Cloud Computing and Services

Chapter 1 : Introduction

Q. 1 What is Cloud Computing? Dec. 15

Ans. :

Definition

"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."

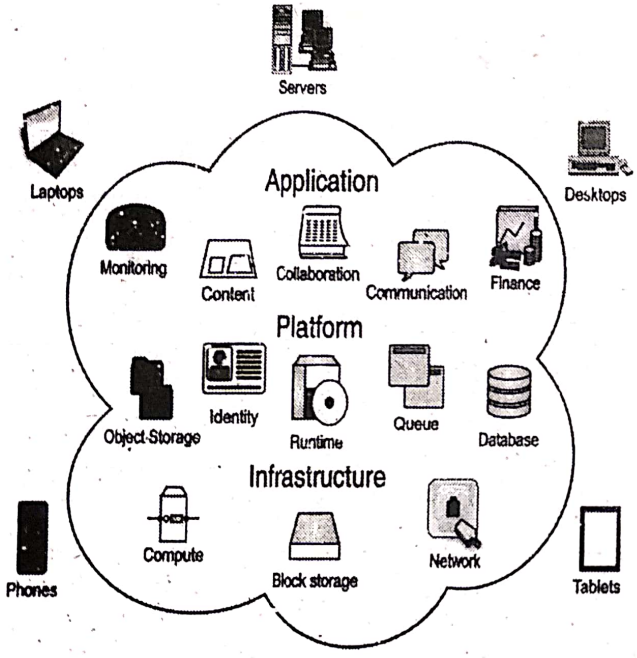


Fig. 1.1 : Cloud computing

Q. 2. Explain the features of cloud in details Dec. 15

Ans. :

Features of the Cloud Computing

1. Resource pooling and elasticity

In cloud computing, resources are pooled to serve a large number of customers. Cloud technology uses multi-tenancy in which different resources are dynamically allocated and de-allocated according to demand. From the user's point of view, it is not possible to know where the resource actually resides. The resource allocation should be elastic that means it should change appropriately and quickly with on demand basis. If the requirement increases suddenly, then the system has to be elastic enough to meet the required result, and it should return to the normal level when the demand decreases.

2. Self-service and on-demand services

Cloud computing is established on self-service and on-demand service based models. It has to allow the user to interact with the cloud to perform the different jobs like building, deploying, managing, and scheduling. The user should be able to access computing capabilities when needed and without any interaction from the cloud-service provider. This would help users to be in control, bringing agility in their work, and to make better decisions on the current and future needs.

3. Pricing

Cloud computing does not have any upfront cost. It is completely based on the custom usage. The user is payable based on the amount of resources he/she used. This will ultimately help the user to track their used resources and minimize the cost. Cloud computing must provide different ways to capture, monitor, and control the used information for accurate billing. The information which is collected should be transparent and readily available to the end users. This will help to make the customer realize the cost benefits that cloud computing brings.

4. Quality of service

Cloud computing must ensure the best service for customers. Services mentioned in the service-level agreements have to include guarantees on round-the-clock availability, sufficient resources, performance, and bandwidth. Any compromise on these guarantees could prove fatal for customers. The decision that is to be taken to choose cloud computing should not be based on the advertise in the industry. The fine understanding of the technology will make sure the user to take proper decisions. Knowing all the features will improve the business users and they will understand and negotiate with the service providers in a positive manner.

Q. 3. Explain the different components in cloud computing.

Ans. :

Components in cloud computing

1. Storage-as-a-Service

This is the kind of component in which we can use or request storage, such as we do it physically using the remote site. It can be also called disk space on demand. This is the main component where even other components will have a base component as Storage-as-a-Service.

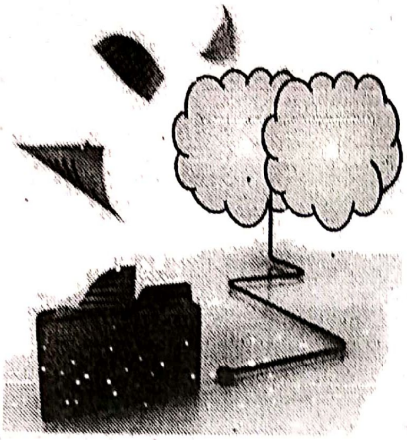


Fig. 1.2 : Storage-as-a-Service

2. Database-as-a-Service

This module acts as a live database from remote site where its functionality and other features works as a physical database present in the local machine. Its main objective is to reduce the cost of database using many software as well as hardware.

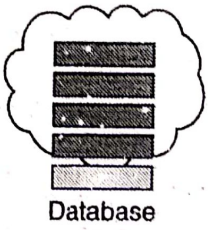


Fig. 1.3 : Database-as-a-Service

3. Information-as-a-Service

Information-as-a-Service is a kind of service which can be accessed remotely. Ultimately the information will be pulled remotely. This includes, for example, live stock prices, internet banking, online news, credit card validation, Generating one time password and so on.

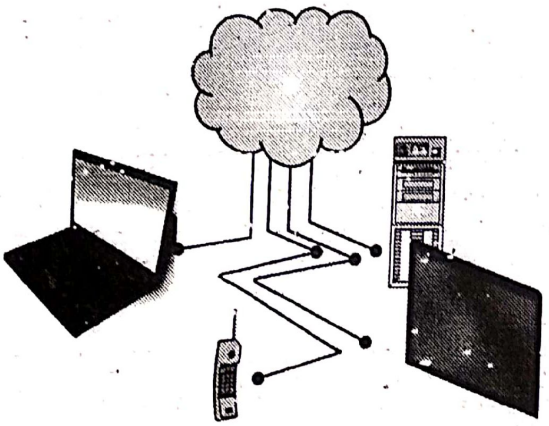


Fig. 1.4 : Information-as-a-Service

4. Process-as-a-Service

This type of service combines various resources such as data and services. This happens when hosted in the same cloud computing resource or remotely. Mainly such kind of service is used for business processes in large industry where various services and information are combined to form one process. This will help in delivery on demand concept. For example mobile networks (internet settings are set up as soon as it is activated).

5. Application-as-a-Service

Application-as-a-Service (also known as SAAS) is the comprehensive application built for the use of the client. This is for end users to use the service and the end users normally use browsers and the internet to access this service. This component is the ultimate front-end for end users. Some of the applications are Salesforce, Gmail, Google calendar and so on.

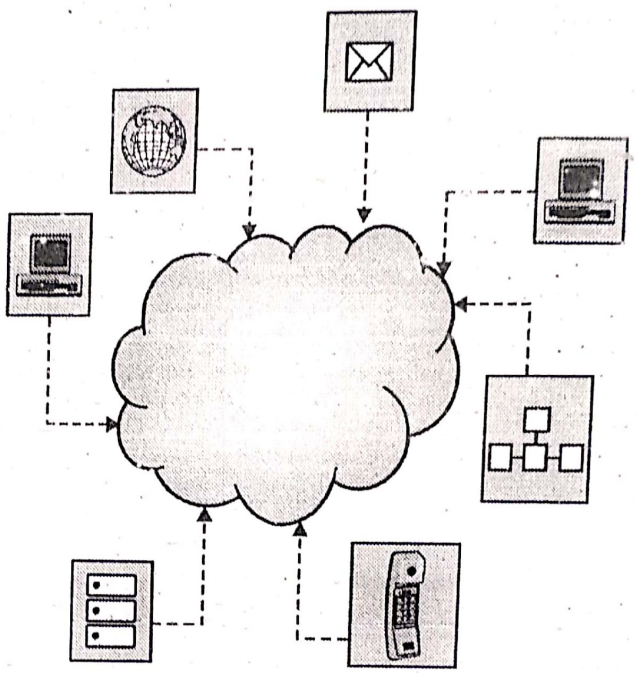


Fig. 1.5 : Application-as-a-Service

6. Platform-as-a-Service

This is the component in which the application is developed and the database is created, implemented, stored and tested. In recent times this component allows creation of industry level applications easily and is very much cost-effective.

7. Integration-as-a-Service

Integration-as-a-Service deals with the component of an application which has been built and it required to be integrated with other different applications. Integration-as-a-service helps in integration between the remote servers with the local machines. Different applications from the cloud are fetched and communicated with local machines. For example saleforce has integrated Google maps into it.

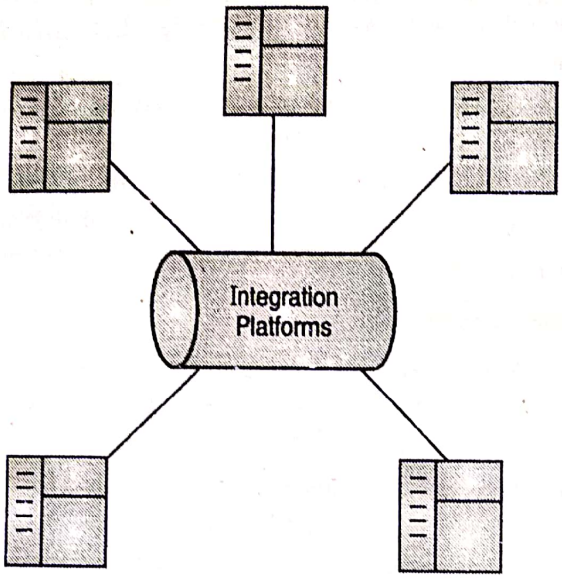


Fig. 1.6 : Integration-as-a-Service

8. Security-as-a-Service

This is the main component in the cloud and many customers ultimately require security as a service. End users who use the cloud platform will always need security features a lot because all the data and operations are handled remotely. There are three-dimensional securities found in cloud platforms.

9. Management-as-a-Service

This is a component which is mainly useful for management of the clouds platforms, which may includes resource utilization on different applications, virtualization and server up and down and down time management. This will be like a small role like an admin.

10. Testing-as-a-Service

Testing-as-a-Service includes the testing of the applications that are hosted remotely, and when there is a requirement to design a database and there is enough security for the applications and so on. This will be tested even with two or three cross clouds. Cross-Cloud Architecture is a type of architecture that offers customers cloud freedom and control its usage. Testing-as-a-service will also act as a component in the development of cloud products.

11. Infrastructure-as-a-Service

This can be called as possible as the taking of all the hardware, software, servers and networking that is completely virtual. In this processes the purchases of resources will take place in the cloud. The processes will execute but we can't see what's happening at the backend. This avoids the running of multiple servers, heat, cold, temperature and so on.

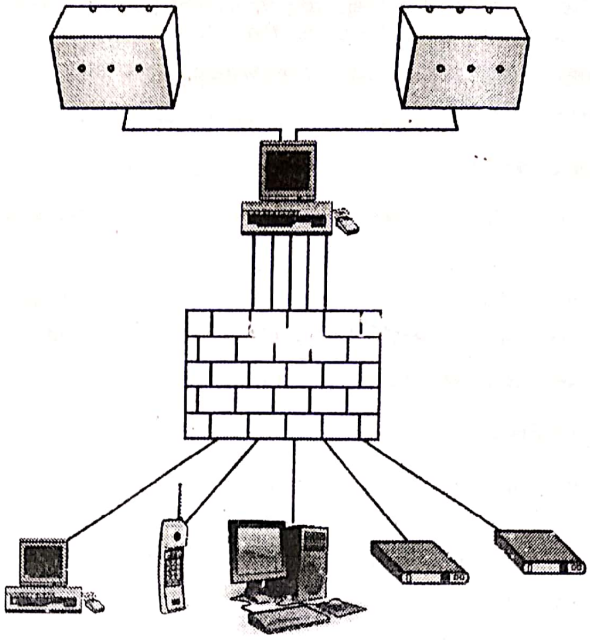


Fig. 1.7 : Infrastructure as a Service

Q. 4. Explain the five major elements of NIST cloud computing

Ans. :

Elements of NIST cloud computing

1. Cloud Consumer

The cloud consumer is the vital stakeholder in the cloud computing that provides the relevant services. A cloud consumer represents a person or association and it will maintain a business relationship with, and uses the service from, a cloud provider. A cloud consumer uses the service registry from a cloud provider, requests the appropriate service, sets up service contracts with the cloud provider, and uses the service. The cloud consumer who uses the service may be payable for the service provisioned, and hence they need to arrange payments as per the usage of service. Depending on which services has been requested, the activities and usage scenarios can be different among cloud consumers.

2. Cloud Provider

A cloud provider's responsibility is to make service available for cloud consumers who can be a person, an organization, or an entity. A cloud provider who develops the requested software/platform/ infrastructure services manages the technical infrastructure which is required for providing the services, provisions the services at agreed-upon service levels, and protects the security and privacy of the services. The cloud providers agree to execute the different tasks for providing the various service models. For Cloud Software as a Service platform, the cloud provider deploys and configures the settings as per the requirements, maintains, and updates the different operation of the software applications on a cloud infrastructure so that the services will be provisioned at the expected service levels to cloud consumers.

The provider of SaaS takes the responsibilities in managing and controlling the applications and the infrastructure, and the cloud consumers have restricted administrative control of the applications.

3. Cloud Auditor

A cloud auditor is a party which can perform an independent examination of cloud service controls. Audits are performed to verify the standards through review. A cloud auditor always evaluates the services provided by a cloud provider in terms of security controls, privacy impact, performance, etc.

4. Cloud Broker

Cloud computing involves integration of cloud services because of which it may be more complex for cloud consumers to manage all the settings related to the cloud infrastructure. A cloud consumer can request cloud services with the help of a cloud broker, as a substitute of contacting a cloud provider directly. A cloud broker is an entity which manages the use of cloud as per the requirement, and delivery of cloud services and he negotiates dealings between cloud providers and cloud consumers.

A cloud broker improves given service by adding some specific capability and also provides value-added services to cloud consumers. A cloud broker integrates various services into one or adds new services. The broker gives integration of data and make sure that the secure data movement can happen in between the cloud consumer and multiple cloud providers. There is another concept of service arbitrage, it is very much similar to service aggregation besides that the services which are aggregated are not permanent. Service arbitrage means a broker can take the decision to choose services from several agencies.

5. Cloud Carrier

A cloud carrier is an intermediate service which gives the connectivity and transport of cloud services between cloud consumers and cloud providers. Cloud carriers give the access to users with the help of network, telecommunication and other accessible devices.

Q. 5. What are the characteristics of cloud? May 18

Ans. :

Characteristics of Cloud

1. On-demand self-service

A cloud consumer can be unilaterally agrees computing capabilities, which can include server time and network storage. When needed it can be used without the human interface with each service provider.

2. Broad network access

Broad network access will indicates the consumers regarding resources which are hosted in a private cloud (operated within a company's firewall) that are available for access from a variety of devices, such as tablets, PCs, Macs and smart phones. These resources will also be available from a wide range of locations that offer online access.

Companies that are involved in the broad network access in a cloud networks need to deal with security issues that may occur. Many times, large companies prefer private cloud service because they deal with the probability for information leaks through the gaps left open outside networks in a public cloud.

3. Resource pooling

The provider's computing resources are pooled to provide multiple end users using a multi-tenant model. This may involve many physical and virtual resources which are dynamically assigned and reassigned according to users demand. There is logic of location independence, in such a case the user generally has no access or knowledge about the exact location of the provided resources but he may be able to identify location at a higher level of abstraction (e.g., country, state, or datacenter). Examples of resources include storage, processing, memory, network bandwidth, and virtual machines.

4. Rapid elasticity

Capabilities can be quickly and elastically provisioned, in some situations automatically, the reason is to quickly scale out. For the consumer, the capabilities accessible are often unlimited and can be purchased in any quantity at any time.

5. Measured service

The cloud environment will automatically organize and optimize resource use as per capability; hence at some level of abstraction it is appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource consumption can be monitored, controlled, and reported by providing transparency for both the provider and user of the utilized service.

Q. 6 What is cloud cube model ?

Ans. : Cloud cube model

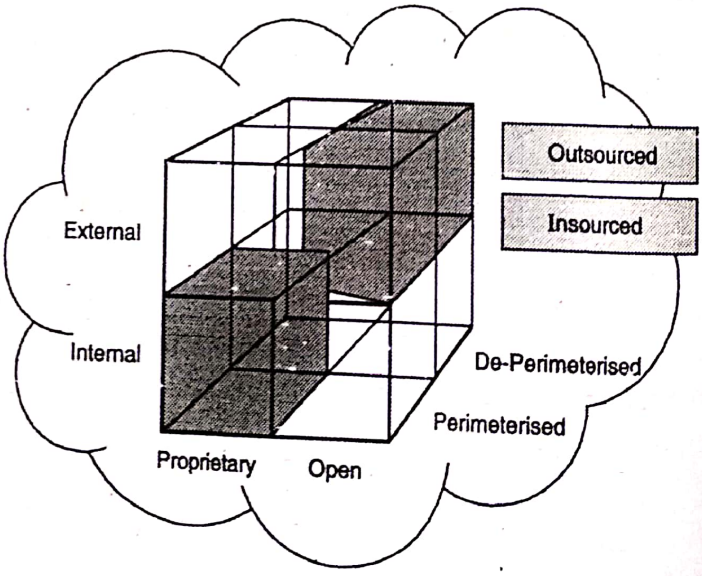
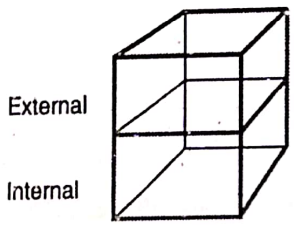


Fig. 1.8 : Cloud Cube Model

The Cloud Cube Model has following four dimensions to differentiate cloud formations :

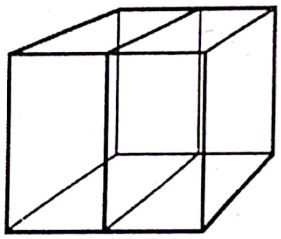
1. The External/Internal dimension

The external or internal dimensions define the physical location of the data. So the question arise is; Does the data will exist outside or inside the industry boundaries? For example, information which is inside a data center via a private cloud deployment can be measured as internal, and data that resided on Amazon EC2 would be measured as external.



2. The Proprietary/Open

The proprietary/open dimension can define the level of ownership of the cloud infrastructure, services, and interfaces. This type of dimensions will indicate the degree of interoperability, and by enabling "data/application transportability" between individual systems and other different cloud forms. This will ultimately useful to move data without any constraint. The meaning of Proprietary is that the organization providing the service is maintaining the means of provision under their ownership. The different clouds are open; this means that they are using technology that is not proprietary. This ultimately means that there are more suppliers, and user is not constrained to share the data and collaborate with selected parties using the same open technology.



Proprietary Open

3. The Perimeterised/De-Perimeterised

The perimeterised / De-perimeterised dimension is mainly deals with architectural mindset. So the question arises is that; whether we are operating inside traditional IT mindset or outside it? De-perimeterisation refers to the concept of steady removal, shrinking, and collapse of the traditional based IT perimeter. Perimeterised indicates continuing to operate within the traditional IT perimeter, often by "network firewalls". When working with the perimeterised areas, this can simply extend organization's perimeter outside cloud computing field by using a VPN and operating the virtual server in IP domain, making use of directory services to control access.

De-perimeterised will guarantees that the system perimeter is architected which follows the principles outlined in the Jericho Forums and Collaboration Oriented Architectures Framework. In de-perimeterised dimensions the data can be encapsulated with the combination of meta-data and this mechanism will protect the data from inappropriate usage.

The working can be divided into four parts viz :

(i) Physical Location of Data

The location of data that may decide the internal or external aspect of the data which ultimately defines the organization's boundary.

(ii) Ownership

Ownership is proprietary or open. It is a capacity for ownership of technology and its interoperability, which uses the data and data-transfer process.

(iii) Security Range

This is parameterized or de-parameterized. This type of dimension will always measure that the operations are inside or outside the security boundary, firewall, etc.

(iv) Sourcing

In-sourcing or out-sourcing : It defines whether the customer or the service provider provides the service correctly or not.

Q. 7 Explain Public Clouds with its advantages and disadvantages

Ans. :

Public Cloud

Public Cloud allows the various types of cloud based systems and services to be simply accessible to common public. The number of IT giants like Google, Zoho, Amazon, Salesforce, Microsoft, Yahoo etc. offer cloud services through the Internet. The Public Cloud Model is illustrated in the Fig. 1.9

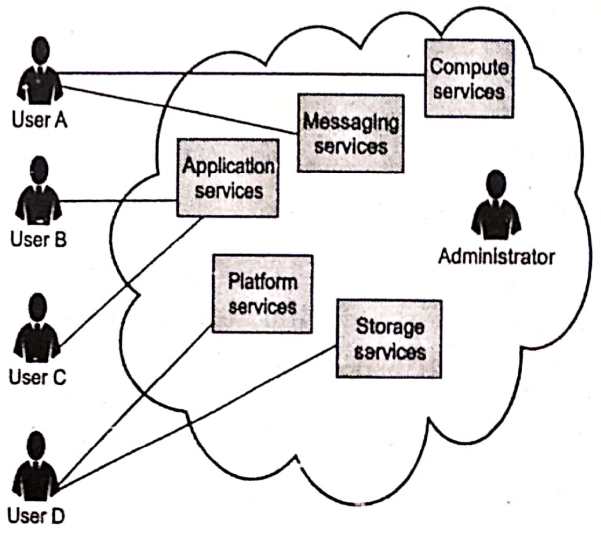


Fig. 1.9 : Public Cloud

Advantages of Public Cloud

1. **Cost Effective**

In public cloud the IT resources are shared by large number of customers, hence it is possible for provider to keep them cost effective.

2. **Reliability**

A large number of resources are employed by the public cloud at various locations hence if failure occurs in any of the resource, another resource is employed by the public cloud.

3. **Flexibility**

Public cloud has ability to integrate with private cloud easily. This provides much better flexibility to customer.

4. **Location Independence**

As services of public cloud are delivered through internet, it is completely location independent.

5. **Utility Style Costing**

Pay-per-use model is available in public cloud and resources made available to customer only when there is requirement.

6. **High Scalability**

As per demand, the cloud resources can be scaled up or down from the pool of resources.

Disadvantages of public cloud

1. **Low Security**

In this model the data hosting is done off site and public sharing of resources is done, which does not ensure strong security.

2. **Less Customizable**

As compared to private cloud, public cloud is less customizable.

Q. 8 Explain the term Community Clouds with its advantages and disadvantages.

Ans. :

Community Cloud

Community Cloud allows the various types of cloud based systems and services to be simply accessible to group of organizations. An infrastructure is shared between various organizations which are of specific community. It is managed either by internally or by any contracted third party.

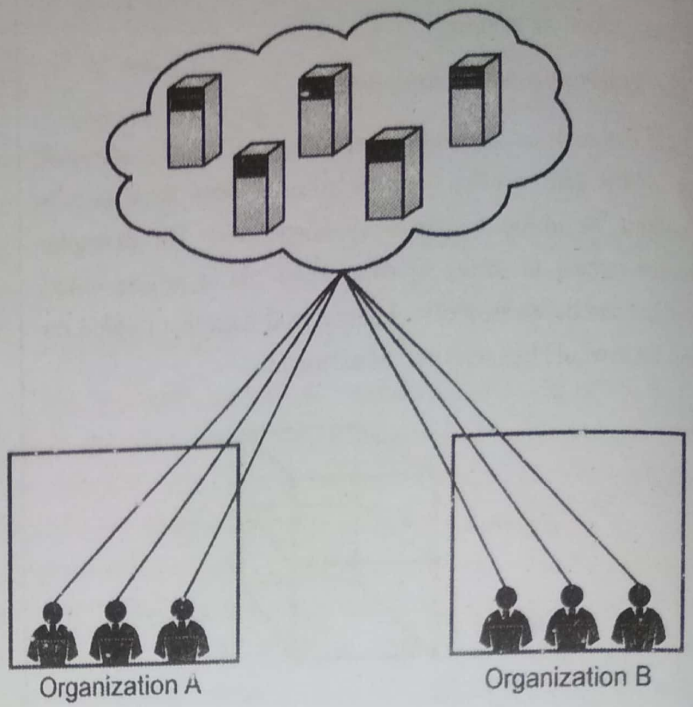


Fig. 1.10 : Community Cloud

Advantages of Community Clouds

1. **Cost Effective**

In community cloud the IT resources are shared by number of organizations, hence it is possible for provider to keep them cost effective.

2. **Sharing Among Organizations**

Sharable infrastructure is provided by the Community cloud for sharing of cloud resources among the various organizations.

3. **Security**

The community cloud is secure as compared to the public cloud but it is less secured as compared to the private cloud.

Disadvantages of Community Cloud

1. **Security issue**

The entire data is stored at one place, hence it may arise security concern as it might be accessible to others.

2. **Sharing of Responsibilities and Cost issue**

There may be confusion while assigning responsibilities of governance and security among organizations. Also the cost sharing is difficult.

Q. 9 Explain the term Private Clouds with its advantages and disadvantages.

Ans. :

Private Cloud

Private Cloud is implemented by an organization in its own private premises. The cloud based IT resources and services are accessible within the organization only. This cloud may be

managed by the organization itself or by any other contracted third-party. The private cloud model is shown in the Fig. 1.11

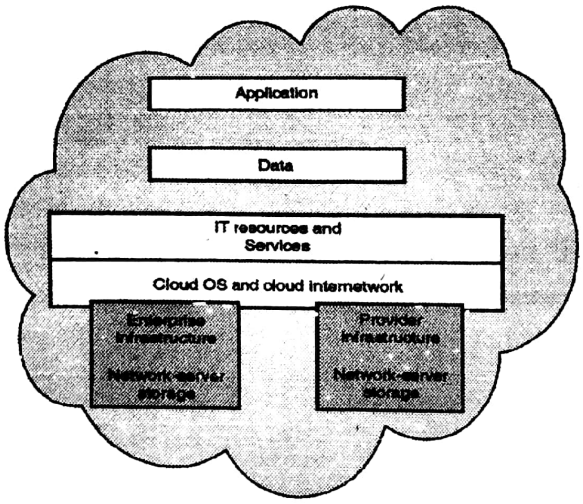


Fig. 1.11 : Private Cloud

Advantages of Private Cloud

1. **High Security and Privacy**

   The operations performed in Private Cloud are not exposed to public and also the resource sharing is done from distinct pool of resources, hence a high security and privacy is ensured.

2. **More Control**

   As the accessibility is only within the boundary of an organization, the control of Private Cloud on the resources and hardware is more than the Public Cloud.

3. **Energy Efficiency**

   The energy efficiency of Private Cloud is more than the Public Cloud.

Disadvantages of Private Cloud

1. **Restricted Area of Operation**

   The accessibility of IT resources and service of Private cloud is only within the boundary of an organization.

2. **High Priced**

   Costing of hardware is the responsibility of the organization alone.

3. **Limited Scalability**

   The scaling is possible within the capacity of internal hosted resources.

4. **Require Additional Skills**

   High level skilled employees are required to manage the private cloud.

Q. 10 Compare public and private cloud.

Ans. :

Parameter	Public Cloud	Private Cloud	Hybrid Cloud
Description	Multi-tenant environment with pay-as-you-grow scalability.	Scalability plus the enhanced security and control of a single-tenant environment.	Connect the public cloud to private cloud or dedicated servers; even in personal data center.
Physical hardware	Shared	Dedicated	Shared + Dedicated
Best for	Non-sensitive, public-facing operations and unpredictable traffic.	Sensitive, business-critical operations.	Combine public, private and/or dedicated servers, for the best of each.

Q. 11 Write a note on Hybrid Clouds and its advantages and disadvantages.

Ans. : Hybrid Cloud

A hybrid cloud is a mixture of two or more types of cloud deployment models. For example, a cloud consumer may want to deploy cloud services which process important data to private cloud and other cloud services which process less important data to a public cloud. Such combination is considered as Hybrid Cloud.

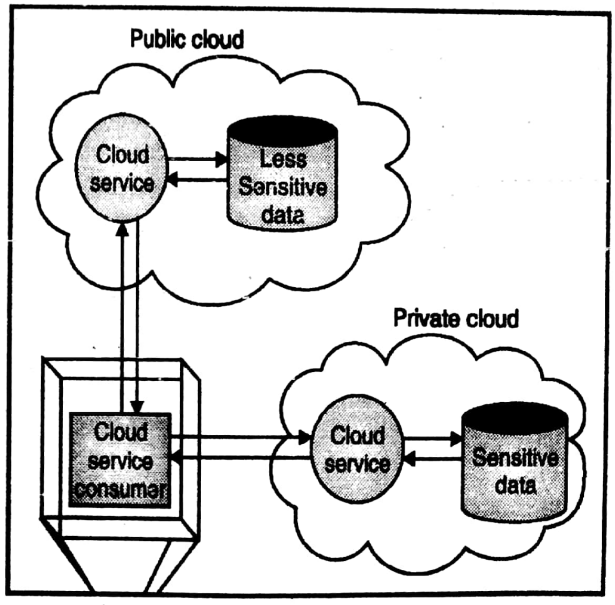


Fig. 1.12 : Hybrid Clouds

Advantages of Hybrid Cloud

1. **Scalability**

   Both public and private scalability is provided by Hybrid Model.

2. **Flexibility**

   Both secure and scalable resources are available.

3. **Cost Efficiency**

   As compared to Private Cloud, it is cost effective.

4. **Security**

   The private part of hybrid cloud ensures strong security.

Disadvantages of Hybrid Cloud

1. **Networking Issues**

   Maintaining network between private and public cloud is complicated.

2. **Security Compliance**

   The involvement of public Cloud leads to security concerns.

3. **Infrastructure Dependency**

   The dependency on internal IT infrastructure of Hybrid cloud is more.

Q. 12 Explain the IaaS model with advantages and disadvantages. Dec. 17

Ans. :

Infrastructure-as-a-Service

Infrastructure-as-a-Service is a model which provides access to primary resources like physical machines, virtual machines, virtual storage, etc.

In addition to these resources, the IaaS also provides following facilities :

(i) Virtual machine disk storage

(ii) Software bundles

(iii) Virtual local area network (VLANs)

(iv) IP addresses

(v) Load balancers

The concept of server virtualization is used to make available these resources to the user. The extent of access rights gives feeling of owner of these resources to the end user.

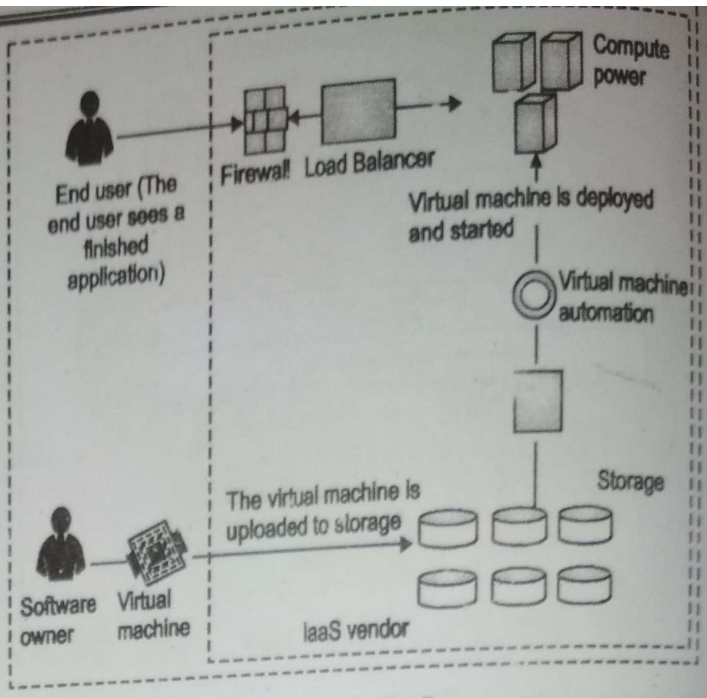


Fig. 1.13 : IaaS

Advantages of IaaS

1. IaaS helps the cloud provider to freely place the infrastructure over the Internet in a cost-effective manner.
2. Through administrative level access to VMs, a complete control of the computing resources is provided.
3. Using the administrative access, the customer can access computing resources in the following way :
4. If the end user wants to run the virtual machine or store data on cloud based server, then he issues an administrative command to cloud provider.
5. Administrative command is given by the customer to virtual machines to start the service to web server to install new applications.

(i) **The renting of computer hardware is very flexible as well as efficient**

Number of IT resources like virtual machines, IP addresses, storage devices, monitoring services, bandwidth, firewalls, etc. made available to the customers on lease. The payment of the service is depending upon the time for which the resources are retained by the customer. Also using the administrative access to virtual machines, number of software can be executed by the customer.

(ii) **Portability and interoperability is provided with legacy applications**

A legacy can be maintained between applications and workloads within IaaS clouds. For example the network applications like web or email server which generally run on customer side server can be run on VMs in IaaS cloud.

Disadvantages of IaaS

1. **Compatibility with legacy security vulnerabilities**

   As the legacy software of customer is run in provider's infrastructure, the software gets exposed to all of the security vulnerabilities.

2. **Virtual Machine sprawl**

   IaaS gives permission to customer to make use of virtual machines in running, suspended and off state modes; hence the Virtual Machine may be out-of-date with respect to security updates.

3. **Robustness of VM-level isolation**

   IaaS provides an environment in isolated form to the customers through the software hypervisor.

   The Hypervisor is an application layer which has hardware support for virtualization to divide a physical computer system into several virtual machines.

4. **Data erase practices**

   The virtual machines use the common disk resources offered by the cloud provider. After releasing the resource by customer, the data may remain on the virtual machine.

Q. 13 Explain the PaaS model with advantages and disadvantages.

Ans. : Platform-as-a-Service

Platform-as-a-Service provides a readymade runtime environment for different types of applications. It also offers various tools regarding development and deployment which are necessary to develop applications. PaaS provides a very important feature of point-and-click tool which is very useful for the non-developers to create various types of web applications as per their requirements.

Fig. 1.14 illustrates that how PaaS provides an API and development tools to the developers and how it guide the user to access the business applications.

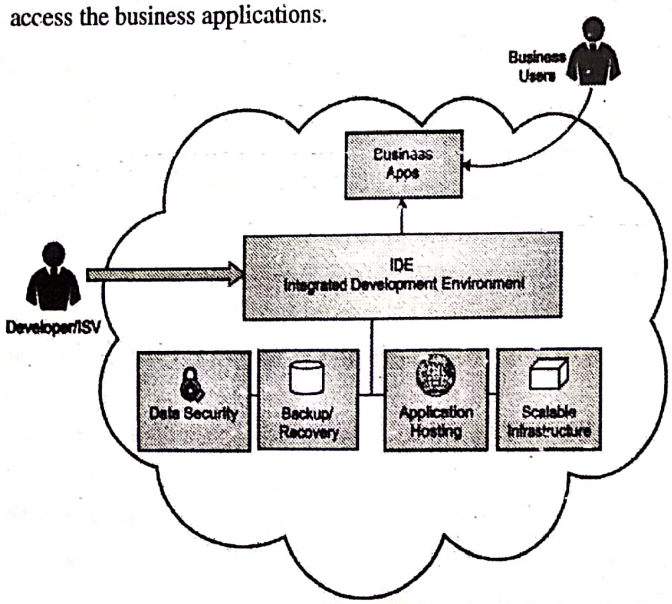


Fig. 1.14 : *PaaS*

Advantages of PaaS model

1. **The overhead regarding administration are very low**

   As administration is the responsibility of cloud provider, it is not headache for customer.

2. **Overall total cost of ownership is very less**

   For the customer, there is no need to purchase expensive hardware, servers, data storage and power.

3. **Scalable solutions are available**

   It is very simple and flexible to scale the available resources up or down automatically, depending on their requirement.

4. **Latest system software**

   It is the responsibility of the cloud provider to maintain and keep advanced and latest software versions.

Disadvantages of PaaS

1. **Lack of portability**

   Lack of portability between PaaS clouds.

2. **Resource Constraints**

   Event based processor scheduling which constitutes resource constraints on the applications, i.e. time limitation to answer a request.

3. **Dependency on network**

   PaaS applications are completely reliant on network, hence they have to explicitly use cryptography and manage the upcoming security exposures.

Q. 14 Discuss SaaS maturity models with advantages and disadvantages.

Ans. :

Software-as-a-service

This model is basically used to provide software application as a service to the end users. It refers to any specific software which has been deployed on a host server and can be accessed through Internet. There are various types of SaaS applications available which are listed below :

1. Billing and invoicing system
2. Help desk applications
3. Customer Relationship Management (CRM) applications
4. Human Resource (HR) solutions

It is not necessary that all the SaaS applications should be customizable, for example Microsoft Office Suite. For customized application development, SaaS provides Application Programming Interface (API) to the user.

Advantages of SaaS

1. Modest software tools

For the SaaS application deployment, there is no need of software installation on client side. This results in the following benefits :

1. No need of any complex software packages to be installed at client side.
2. Zero risk of configuration at client side.
3. Low distribution cost.

2. Efficient use of software licenses

Single license copy can be used on multiple computers which may be at different locations. This lowers the licensing cost. As well, there is no need of license servers since the software runs in the infrastructure of service provider.

3. Centralized management and data

The data is saved centrally by the cloud provider. This helps to manage the data effectively. But sometimes to maintain the redundancy and reliability, the data may be in decentralized manner.

4. Platform responsibilities managed by providers

All platform responsibilities are performed by the cloud provider. These responsibilities include backups of data, maintenance of the system, security, hardware updates, power management, etc.

No need for the customer to bother about them.

5. Multitenant solutions

Multitenant solutions enable several users to share single instance of multiple resources in virtual isolation. It is possible for the customer to customize the application without disturbing the core functionality.

Disadvantages of SaaS

1. Browser based risks.
2. Network dependence.
3. Lack of portability between SaaS clouds.

Q. 15 Write characteristics of SaaS model. (2 Marks)

Ans. :

Characteristics of SaaS

1. SaaS makes available various types of software over the Internet.
2. Vendor has the responsibility to maintain the software.
3. The license of the software is available either subscription based or on usage based. And on the basis of recurring it is charged.
4. User do not have any software, hence it is cost effective.
5. They are anytime anywhere available on demand.
6. They can be scaled up or down on demand.
7. Automatically up gradation and updation is available.

SaaS provides shared data model. Hence, several users can share single instance of infrastructure at a time. There is no need of hard coding for functionality for any specific user.

Q. 16 Write a note on : Infrastructure Constraints for cloud computing architecture. Dec. 15, May 16

Ans. :

Infrastructural Constraints

The Fundamental constraints of the cloud infrastructure are shown in the Fig. 1.15

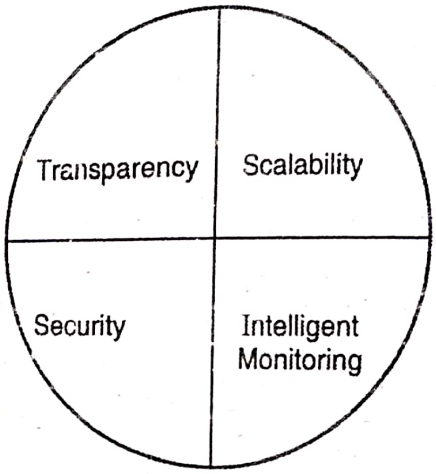


Fig. 1.15 : Infrastructure Constraints

1. Transparency

Virtualization is the main concept to share resources in cloud environment. But it is not difficult to assure the demand with single resource or server. And hence, there must be transparency in resources, load balancing and applications, so that we can scale them on demand.

2 Scalability

Scaling the whole application delivery solution is difficult task as compared to the scaling of application because it includes the configuration part and sometimes re-architecting the network also required. Hence, application delivery resolution will need to be scalable which requires the virtual infrastructure so that resource can be provisioned and de-provisioned easily.

3. Intelligent Monitoring

For achieving transparency and scalability, application solution delivery will always need to be capable of intelligent monitoring.

4. Security

The data center in the cloud should be securely architected. Also the control node, an entry point in data center, also needs to be secure.

Q. 17 Define advantages of Cloud computing. May 17

Ans. :

Advantages of cloud computing

1. Reduced Investments and Proportional Costs

Shopping Malls purchase products in bulk with lower prices from companies and make them available to general public in lower prices. Using the same logics, the public cloud providers purchase IT resources in bulk with lower prices and make them available to consumer IT companies with attractive low priced leasing packages. This opens the door for various small scale organizations to gain access to costly strong infrastructure without any need to purchase it. For the consumer organizations, the main goal of taking cloud service is to reduce the up-front IT investments, for example hardware and software purchases and also the ownership costs. Use of cloud replaces the anticipated higher capital expenditures by the lower operational expenditures.

This helps to eliminate or minimize the up-front financial costs and allows enterprise owners to start small and accordingly increase IT resource allocation as per the requirement. The saved cost can be redirected to the core business investment. In its most basic form, chance to minimize costs are derived from the process of deployment and operation of large-scale data centres by the various major providers of cloud. Usually these data centres are deployed in such destinations where availability of IT professionals, network bandwidth, and offices are available at low cost which helps to support both capital and operational savings. The same principle is applied to operating systems, middleware or platform software, and application software. Pooled IT resources are made available which can be utilized by the various cloud consumers to implement maximum possible utilization.

Common measurable benefits to cloud consumers

On-demand access - pay-as-you-go to various types of IT resources on a short-term basis (For example processors by the hour), and the capacity to release these IT resources when there is no longer any need. The feeling of unlimited computing resources availability, thereby avoiding the requirement to prepare for provisioning. At a fine-grained level it is possible to add or remove the cloud based IT resources, such as updating existing storage disk space by increment of say five gigabytes. Infrastructure is abstracted; hence applications are not locked into devices or locations which keep the option open to move the business anytime anywhere.

2. Increased Scalability

Cloud provides pools of IT resources with the support of technologies which can control them collectively. The IT resources can be instantly and dynamically allocated as per the requirement. This allows the cloud consumers to scale their cloud-based IT resources to manage the fluctuations in processing and access these resources automatically or manually. In the same manner, it is possible to release cloud-based IT resources automatically or manually if there is decrease in processing demand. A simple example of fluctuations in the usage demand in one day is provided in Fig. 1.16. The built-in feature of clouds to provide flexible option of scaling of IT resources gives effective and proportional benefit.

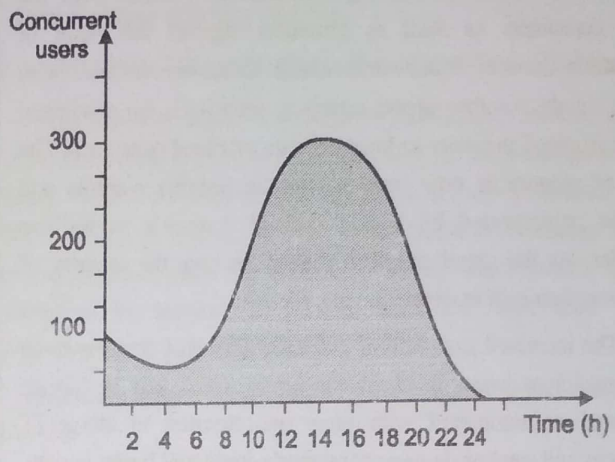


Fig. 1.16 : Fluctuations in usage demand

Besides the financial benefit, it also increase the ability of business to fulfill the unpredictable usage demands of IT resources which avoids a potential loss which may occur because of lack of this ability.

3. Increased Availability and Reliability

The profit of business is completely depends upon the availability and reliability of IT resources. If any IT resource is not available then it's unavailability for customers may affect the revenue generation of the business. Also runtime failure of any IT resource during high level usage period may lead to some loss. These issues affect the service provided to the customers. The main advantages of cloud based environment is its intrinsic ability to give extensive support for increasing the availability of IT resource to decrease or even remove outages.

For improving its reliability so as to decrease the effect of various runtime failure conditions :

A cloud based IT resource can be accessible for longer periods of time. For example near about 22 hours in a day. A cloud based IT resource having increased reliability is able to better avoid and recover in failure condition. The cloud environments have modular architecture which provides a strong failover support to enhance the reliability.

Q. 18 Define disadvantages of Cloud computing.

Ans. :

Disadvantages of cloud computing

1. Increased Security Vulnerabilities

When important business data is shifted to cloud, the concern of security get arise. The usage of various IT resources remotely needs a strong trust by the cloud consumer to involve the external cloud. It is little bit complicated to establish such a strong security architecture without introducing vulnerabilities, unless both the cloud consumers as well as providers support the same or compatible security frameworks which is mostly difficult with public clouds. Another aspect regarding security is the privileged access of cloud provider to business data of cloud consumer. The level of security is now restricted to the security controls and policies implemented by both the cloud consumer as well as provider. As the cloud provides sharing feature, the security of consumer data is in trouble.

The increased exposure of consumer data may provide some other malicious issues to cloud consumers which may be human generated or automated with more opportunities to attack IT resources and steal or damage consumer's important business data. Fig. 1.17 illustrates a scenario where two different businesses accessing the common cloud service, are need to increase their respective trust boundaries to the cloud which may overlap the trust boundaries. It is definitely challenging for the cloud provider to provide such a security mechanism which can accommodate the security concerns of both the consumers of cloud service.

2. Reduced Operational Governance Control

In general there is level of governance control allotted to cloud consumers. This level is always lower than the on-premise IT resources. This low level of governance control may include some risks associated with the operative method of cloud provider, and also outside connections which are necessary for the communication of cloud provider and consumer.

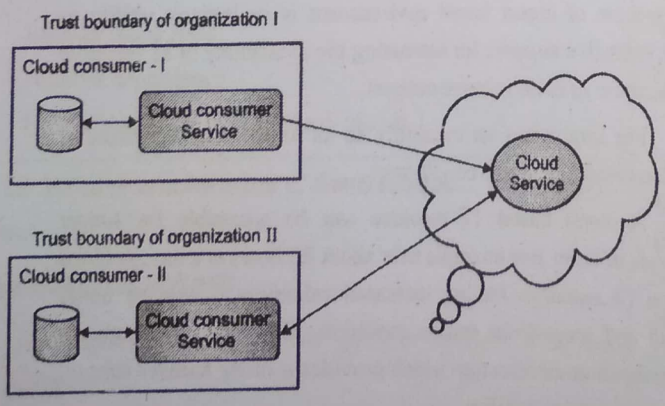


Fig. 1.17 : Reduced Operational Governance Control

Consider the following examples :

If the cloud provider is not reliable, then he may not maintain the guarantee which is made in the SLA (Service-level agreement,) which [illegible] cloud consumer solutions [illegible] services. If the geographic distance between the cloud consumer and cloud provider is longer, then there is need of additional network hops which may lead to fluctuating latency and potential bandwidth constraints.

The latter scenario is illustrated in Fig. 1.18

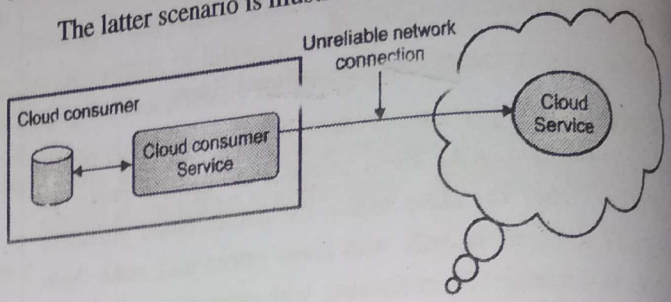


Fig. 1.18 : An unreliable network connection

3. Limited Portability between Cloud Providers

In the industry of Cloud computing, there is lack of established industry standards. Hence the public clouds are usually proprietary to large extents. Some cloud consumers have customized built solutions with dependencies on such types of proprietary environments. In such case it becomes very difficult for a cloud consumer to move from one cloud provider to another.

Portability is considered as a measure which helps to determine the effect of moving cloud consumer IT resources and data from one cloud provider to another. A cloud consumer's application may have low level of portability in moving to another cloud as second cloud provider does not support the same environment as of the first

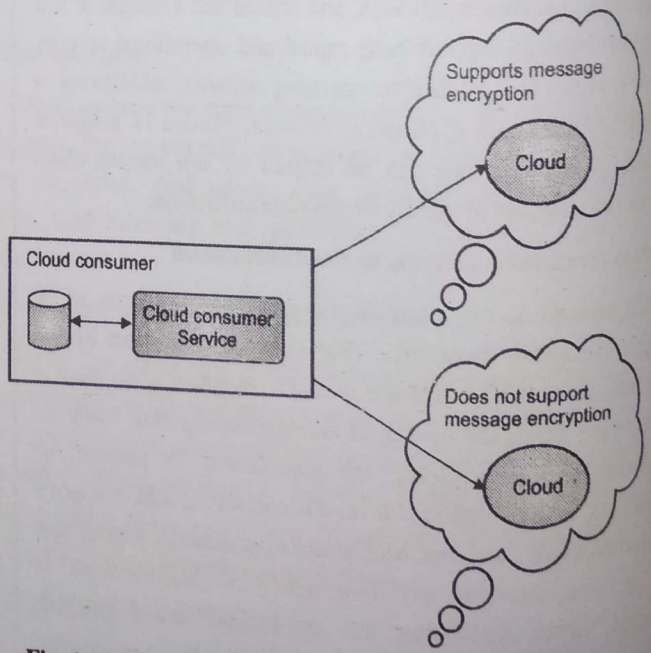


Fig. 1.19 : Limited Portability between Cloud Providers

4. Multi-Regional Regulatory and Legal Issues

Third-party cloud providers always like to establish such data centers which are affordable or convenient as per the geographical

locations. Sometimes the cloud consumers do not know the actual physical locations of public clouds from which they are accessing the IT resources. This can pose serious legal issues regarding the industry or local government rules and regulations that state policies of data privacy and storage. Another important legal issue is regarding the accessibility and disclosure of data. Different countries have different laws regarding the disclosure to extent of data. The cloud consumer has responsibility of the security, integrity, and storage of their own data, even though it is held by cloud provider.

Chapter 2 : Virtualization

Q. 1 What is virtualization? Dec. 15, May 17

Ans. :

Definition

In computing, **virtualization** refers to the act of creating a virtual (rather than actual) version of something, including virtual computer hardware platforms, storage devices, and computer network resources.

Q. 2 Explain is the need of virtualization in the context of cloud computing. Dec. 17

Ans. :

Need of virtualization

1. Resource optimization

Now a day, the computer resources are very powerful with excess capacity. The hardware and allocating parts of it can be virtualized depending upon the actual requirements of users and applications. This leads to much more effective use of available computing power, storage space as well as the network bandwidth.

In this case the computers no longer required to be idle or performing lower than their capabilities. Isolated, constrained and test environments are made available to software developers by the Virtual machines. Instead of buying dedicated physical hardware, virtual machines can be generated on the available hardware.

2. Consolidation

Usually individual computers are dedicated to a single application. If small amount of processing power is used by the several applications, then it is possible to consolidate multiple computers into single server executing several virtual environments. In case of organizations which needs thousands of servers, consolidation can effectively minimize the requirement of floor space, HVAC, A/C power as well as the co-location resources. This leads to significant decrease in cost of ownership, as less physical servers, floor as well as rack space are needed.

3. Maximizing Uptime

Agility is the capacity to respond to frequently changing requirements in a quick and flexible manner. Virtualization provides new openings to data center administration, which allow users to have: Assured uptime of servers and applications; very fast disaster recovery in case of large scale failures. Template images helps to deploy new virtual machines as well as aggregated pools of virtual machines

Elasticity ; On demand provision of resources.

Reconfiguration of computing environments which are executing without affecting the users.

4. Automatically Protect Applications from Server Failure

Virtualization helps to implement redundancy without any need to buy additional hardware. Redundancy, is the mechanism of running single application on several servers, is a safety measure: if there is failure of server. Another server which is executing the same application takes the control by itself, which avoids the interruption in service. In Virtual machines, such type of redundancy works in two ways :

In case of failure of one virtual system, another virtual system takes over.

Against physical hardware failure, better protection can be provided by running the redundant virtual machines on different physical hardware.

5. Easily Migrate Workloads as Needs Change

Migration means shifting the server environment to another location. In virtualization, it is easy to move a virtual machine from one physical machine to another physical machine. In case of physical servers, this migration is possible only if both physical machines are running on the common hardware, operating system and processor. In the virtual world, the migration of server is possible in between physical hosts which may have completely different hardware configurations.

The purpose of migration is to improve reliability as well as availability in case of failure in the hardware, it is possible to move the guest system c to a healthy server with limited downtime, if any. It is also helpful in the situation when a virtual machine is required to scale beyond the physical capabilities of the existing host.

6. Save resources and money

Profit is the most important aspect of any organization. Saving expenses can also be termed as profit. Virtualization minimizes or may completely omit the need of maintaining servers, desktop and data storage machines. Hence all the costing which may be required for the maintenance of these multiple resources is directly cut down.

7. Simplified management of data centre

Just by managing few resources, virtualization helps to handle huge amount of data. There is no need to manage multiple hard drives and data cables.

8. Increased IT productivity and efficiency

Now without any hassle as well as wariness of IT management for big firms, all the advancements in technical and software areas can be implemented with more efficiency.

9. Easy disaster recovery

If any event regarding system crash occurs, then with virtualization it is very simple to detect the loophole because of the simplification of network or data system in just 2-3 layers instead of a complicated web of hard wires and connection.

10. Enhanced Security

As the level of complexity is dropped, the security level enhancement is easy to implement more effectively.

Q. 3 Explain Characteristics of Virtualized Environment.

Ans. :

Characteristics of virtualized environment

1. Increased Security

The capacity to handle the execution of a guest in an entirely transparent way leads to deliver secure as well as controlled execution environment. An emulated environment is represented by the virtual machine where the guest is executed. Usually each and every operation of the guest is carried out against the virtual machine, which further does the processing of translating and applying them to the host. With the help of level of indirection the virtual machine manager is able to control as well as filter the respective activity regarding the guest, thus avoiding some destructive operations from being carried out.

Resources which have been uncovered by the host can then be hidden or get protection from the guest. Additionally, sensitive data which is stored in the host can be obviously hidden without the requirement of installation of any complex security policies. There is need of increased security when there exist un-trusted code.

For example, applets which have been downloaded online execute in a sandboxed version of the JVM (Java Virtual Machine), which offers them with restricted access to the hosting OS resources. Both of the JVM as well as the .NET runtime offers wide range of security policies for the purpose of customizing the execution environment of applications.

2. Managed Execution

Virtualization of the execution environment provides increased security as well as a rich set of features. The most relevant features are sharing, aggregation, emulation, and isolation.

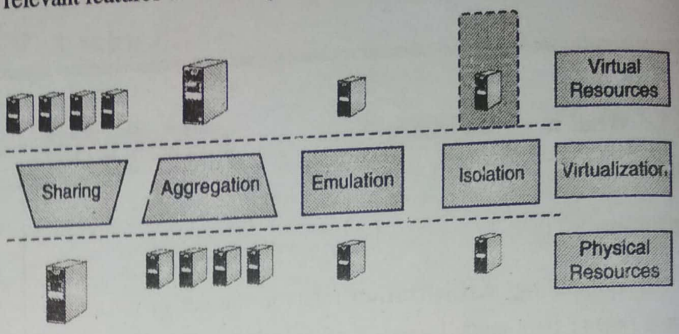


Fig. 2.1 : Functions enabled by managed execution.

i. Sharing

Virtualization helps to generate separate computing environments within the context of a single host. It leads to utilize capabilities of a powerful guest completely, which would otherwise be underutilized. In virtualized data centers Sharing is considered as an important feature, where this basic feature helps to decrease the number of active servers and restrict power consumption.

ii. Aggregation

With sharing ability virtualization also supports aggregation, which is considered as the opposite process.

A number of distinct hosts can be joined together and represented as a single virtual host to the respective guests. This task is done in middleware for distributed computing, with a good example demonstrated by cluster management software that binds the physical resources of identical machines and represents them as a single resource.

iii. Emulation

The execution of guest programs is done within an environment which is handled by the virtualization layer, which finally is a program. It helps to control as well as tune the environment which has been exposed to guests. For example, it is possible to emulate an entirely different environment with regards to the host, consequently permitting the execution of guest programs which need particular characteristics which are not available in the physical host. This feature is considered as very helpful for testing purposes in which a particular guest has to be validated on several platforms or architectures and the numerous options are not simply accessible through development.

Also, hardware virtualization solutions can offer virtual hardware and imitate a specific type of device like SCSI (Small Computer System Interface) for file I/O, with no such hardware installed on the hosting machine. Old and legacy software which does not fulfill the necessities of current systems can be executed on emulated hardware without any necessity to update the code.

This can be done either by the way of emulating the necessary hardware architecture or within environment of a particular OS sandbox such as the MS-DOS mode in Windows 95 or windows 98. One more example of emulation is an arcade-game emulator which enables to play arcade games on a simple desktop.

iv. Isolation

Virtualization offers guests an entirely separate environment for their execution. Those guests may be OSs, applications, or other entities. The guest program carries its activity by the w.. of communicating with an abstraction layer that gives access to the several available underlying resources. There are number of advantages of Isolation; for example, it allows more than one guests to execute on the single host without disturbing each other. Second, it offers a separation among the host and the guest. The virtual machine can keep watch on the activities of the guest and avoid unsafe operations against the host.

v. Portability

There are different ways to apply the concept of portability based on the specific type of virtualization considered. In the case of a hardware virtualization solution, it is possible to package the guest into a virtual image which in several cases can be securely moved as well as run on top of different virtual machines. Except for the file size, this occurs with the similar ease with which one is able to display an image on different computers.

Virtual images are usually considered as proprietary formats which need a particular virtual machine manager to be executed. In the case of programming-level virtualization, as carried out by the JVM (Java Virtual Machine) or the Dot NET runtime, the binary code which represents the application components (such as jars or assemblies) can be executed with no any recompilation on any implementation of the consequent virtual machine. Because of this the application development cycle becomes more flexible and deployment of respective application extremely straightforward: Most of the times one version of the respective application can be executed on different platforms without need of any changes.

Q. 4 Explain Type 1 and Type 2 Virtualization. Dec. 17

Ans. : There are two types of hypervisors

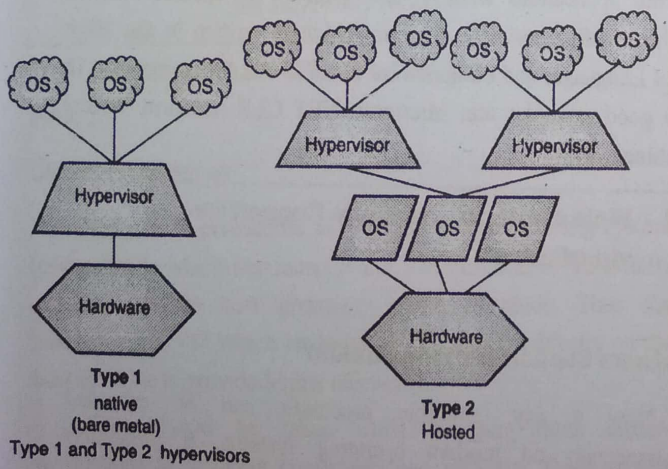


Fig. 2.2 : Types of Hypervisors

Type-1, native or bare-metal hypervisors : Features

Type-1 Hypervisor is also called as Bare Metal or Embedded or Native Hypervisor. It works directly on the hardware of the host and can monitor operating systems that run above the hypervisor. It is totally independent of the Operating System. The size of this hypervisor is small because its main function is to share and manage hardware resources between various operating systems. A major advantage in using Type-1 hypervisor is that any problems occurred in one virtual machine or guest operating system are not going to affect the other guest operating systems running on the hypervisor.

Examples

(i) VMware ESXi Server

(ii) Microsoft Hyper-V

(iii) Citrix/Xen Server

Type-2 or hosted hypervisors : Features

Type-2 Hypervisor is also known as Hosted Hypervisor.

These hypervisors run on a conventional operating system (OS) just as other computer programs do. A guest operating system runs as a process on the host. Type-2 hypervisors abstract guest operating systems from the host operating system. It is totally depends upon the host Operating System for its operations. If any problems arise in the base operating system, then it affects the entire system.

Examples

(i) VMware Workstation

(ii) Microsoft Virtual PC

(iii) Oracle Virtual Box

Q. 5 What are the levels used for virtualization? May 17

Ans. :

Virtualization Level

Usually the virtualization layers includes following levels :

1. Instruction set architecture (ISA) level
2. Hardware level
3. Operating system level
4. Library support level
5. Application level.

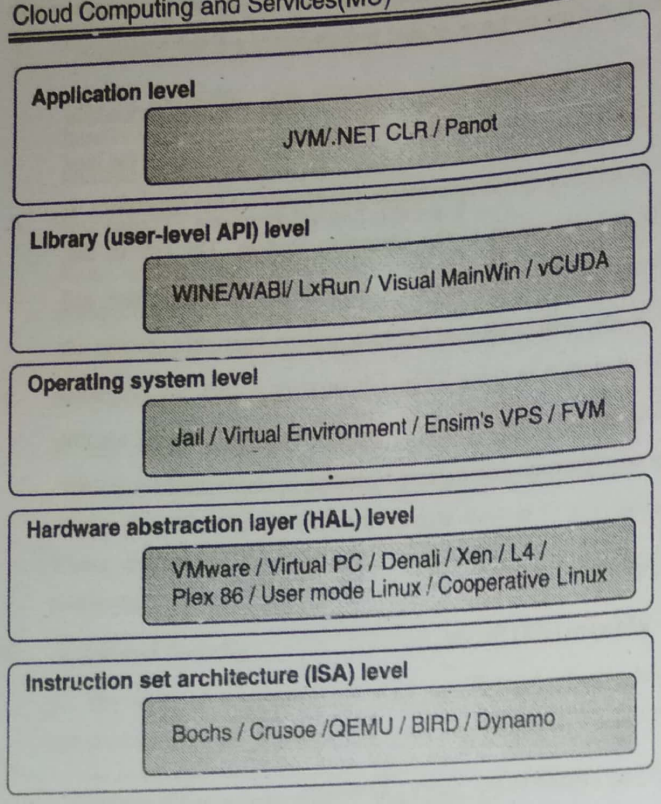


Fig. 2.3 : Implementation Levels of Virtualization

1. Instruction Set Architecture Level (ISA)

In the ISA level, the given ISA is emulated by the ISA of the host machine to carry out the virtualization. For example, we can execute MIPS binary code on an x86-based host machine by the use of ISA emulation. This approach helps to execute plenty of legacy binary code which is written for various processors on any given new hardware host machine. The virtual ISAs are generated on any hardware machine by the Instruction set emulation.

Code interpretation is the basic mechanism for emulation. The source code is interpreted one by one by the interpreter program. To perform its function, there may be need of hundreds of native target instructions for a single source instruction. Hence this process is relatively slow. Dynamic binary translation is required for the better performance. The basic blocks of dynamic source instructions are translated to target instructions. For increasing the efficiency, it is also possible to extend the basic block to program traces or super blocks. There is need of binary translation and optimization for the emulation of instruction set. In this way, virtual instruction set architecture (V-ISA) needs inclusion of a processor-specific software translation layer to the compiler.

2. Hardware Abstraction Level

Hardware-level virtualization process is carried out right on top of the bare hardware. With the help of this approach, two things can be achieved; first a virtual hardware environment is generated for a VM and second underlying hardware can be managed through virtualization.

The main aim of this approach is to virtualized different resources of a computer like its processors, memory, and I/O devices. It can lead to up gradation of hardware utilization rate by the multiple users simultaneously.

3. Operating System Level

This approach basically refers to an abstraction layer among traditional OS and the user applications. Isolated containers are created on a single physical server by the Operating System level virtualization. It also creates OS instances which are used to utilize the hardware and software available in data centres. The behaviour is just like as they are real servers. The Operating System level virtualization is generally used in the creation of virtual hosting environments for the purpose of allocating hardware resources among a large number of mutually distrusting users. Rarely it can also be used for consolidation of server hardware by shifting services on separate hosts into various types of containers or VMs on one server.

4. Library Support Level

Mostly applications use APIs which are exported by user-level libraries instead of lengthy system calls by the OS. As there are well-documented APIs in most of the systems, they can be used as an interface for virtualization. Virtualization using library interfaces is achievable by controlling the communication link between applications and the rest of a system. This is done with the help of API hooks. This approach is implemented by the software tool WINE for the support of Windows applications on top of UNIX hosts.

5. User-Application Level

In the User-Application Level approach, an application is virtualized as a VM. Usually an application executes as a process on traditional OS. Hence the User-Application Level virtualization is also called process-level virtualization. In User-Application Level, the virtualization layer resides as an application program on top of the OS. This layer exports an abstraction of a VM which can execute applications written and compiled for specific abstract machine definition. Any program which is written in the High Level Languages and compiled for this VM can be executed on it. Two good examples are; Microsoft .NET CLR and Java Virtual Machine (JVM).

Q. 6 Write a note on : Hardware Support for virtualization.

Ans. :

Hardware Support for Virtualization

Now a day, multiple processes can be executed simultaneously on modern operating systems. If protection mechanism is not provided in a processor, then the hardware will get accessed by the instructions of different processes. This may

lead to system crash. Hence all processors provide minimum two modes; user mode and supervisor mode, to make sure control over the access of critical hardware. Instructions which executes in supervisor mode are known as privileged instructions. All other instructions are known as unprivileged instructions.

In a virtualized environment, it is very complicated to execute operating systems and applications properly since there are multiple layers in the machine stack. Now a day number of hardware virtualization products are available in the market. The VMware Workstation is a VM software suite for x86 and x86-64 computers. This software suite is used to set up many x86 and x86-64 virtual computers. These VMS can be used concurrently with the host operating system.

Example : Hardware Support for Virtualization in the Intel x86 Processor

As the software dependent virtualization techniques are considered as difficult and also generates performance overhead, a hardware-assist technique is provided by the Intel to ease the process of virtualization and improve performance. Fig. 2.4 illustrates the entire overview of Intel's full virtualization techniques. Intel provides VT-x or VT-i technique for processor virtualization. Automatically all the sensitive instructions are trapped by this enhancement. Intel provides EPT for memory virtualization. To improve performance it translates the virtual address to the physical addresses. VT-d and VT-c are offered by Intel for I/O virtualization.

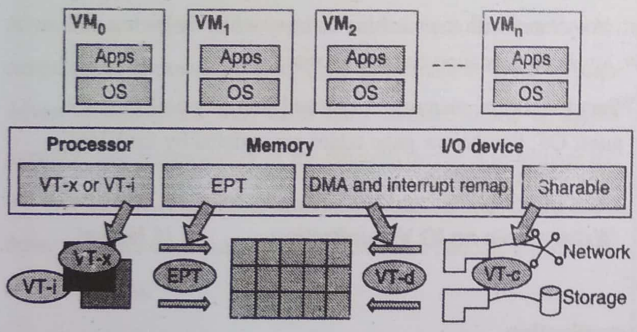


Fig. 2.4 : Hardware Support for Virtualization in the Intel x86 Processor

Q. 7 Write a note on CPU virtualization.

Ans. :

CPU Virtualization

VM can be considered as a duplicate of an existing system (computer) in which maximum of the VM instructions are usually executed on the host processor in native mode. Thus the instructions of VM which are unprivileged, execute directly on the host machine to provide higher efficiency.

Care should be taken while handling other critical instructions to maintain correctness and stability. These critical instructions are divided into three categories :

1. Privileged instructions
2. Control-sensitive instructions
3. Behavior-sensitive instructions.

Privileged instructions are executed in a privileged mode and if executed outside this mode, then get trapped. Control-sensitive instructions are used to make change in the configuration of resources used. Behavior-sensitive instructions show different behaviors which depends upon the configuration of resources and also the load as well as store operations over the virtual memory.

A CPU architecture can be considered as virtualizable on one condition that if it gives support to the ability to execute the VM's privileged as well as unprivileged instructions in the user mode of CPU when the VMM is running in supervisor mode. There is possibility of trapping the instructions in VMM when privileged instructions containing control sensitive and behavior sensitive instructions of a VM get executed. In such case the VM works as a mediator for the access of hardware from various VMs to make sure the correctness and stability of the whole system.

However, it is not possible to virtualize all the CPU architectures. For example RISC CPU architectures are easily virtualized since all control sensitive as well as behavior sensitive instructions are of type privileged instructions. On the other hand, x86 CPU architectures cannot be virtualized easily because near about 10 sensitive instructions in it are not privileged instructions. These instructions cannot be trapped when executed in virtualization.

Hardware-Assisted CPU Virtualization

The full or para-virtualization is complicated; hence this technique is used to simplify virtualization. An additional mode known as privilege mode level or Ring-1 is added by the Intel and AMD to x86 processors. Hence operating systems can be executed on Ring 0 while the hypervisor can be executed on Ring 1. The automatic trapping of all privileged as well as sensitive instructions is done in the hypervisor. This technique helps to avoid the complexity of implementation of binary translation of full virtualization. It also allows the OS to run in VMs without need of any modification.

Example : Intel Hardware-Assisted CPU Virtualization

Initially the x86 processors were not virtualizable, but later on great efforts are taken to virtualize them. x86 processors are widely used in comparison with RISC processors. VT-x technology of Intel is a good example of hardware-assisted virtualization, as shown in Fig. 2.5. Intel gives call to the privilege level of x86 processors the VMX Root Mode.

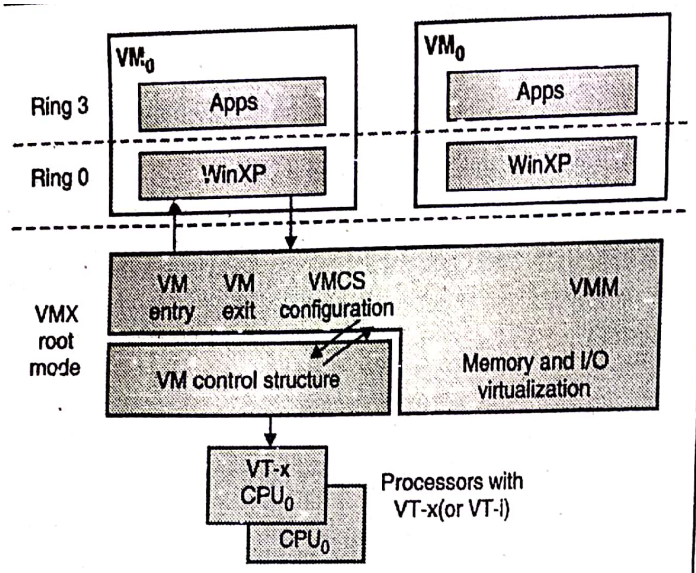


Fig. 2.5 : Intel Hardware-Assisted CPU Virtualization

A collection of additional instructions is added to control the start and stop of a VM and a memory page is allocated to maintain the CPU state for VMs. High efficiency is expected from hardware-assisted virtualization. However, high overhead switches between processor modes may get incurred because of the transition from the hypervisor to the guest OS. This may affects the performance of binary translation. For this reason, now a day, virtualization systems like VMware uses a hybrid approach, in which a small amount of tasks are offloaded to the hardware but remaining are executed with software. Also for performance improvement, the two virtualization; para-virtualization and hardware-assisted virtualization can be combined.

Q. 8 Write a note on Memory Virtualization.

Ans. :

Memory Virtualization

Memory virtualization is a same process as of the virtual memory support which is provided by modern operating systems. In a traditional execution environment, the mappings of virtual memory to machine memory were maintained by the OS with the help of page tables. This was a one step process of mapping from virtual memory to machine memory. For the optimization of virtual memory performance, now a day all modern x86 CPUs contains MMU (Memory Management Unit) and TLB (Translation Look aside Buffer).

In the virtualization of memory, the physical system memory in RAM is shared and dynamically allocated to the VM's physical memory. That means the guest OS and the VMM maintains the two-stage mapping process; first virtual memory to physical memory and then in next phase physical memory to machine memory. The MMU virtualization which is transparent to the guest OS should also be supported. The mapping of virtual addresses to the physical memory addresses of VMs is further controlled by the guest OS. But the actual machine memory is not directly accessible to guest OS. The mapping of guest physical memory to the actual machine memory is responsibility of the VMM.

Fig. 2.6 shows the two-level memory mapping procedure.

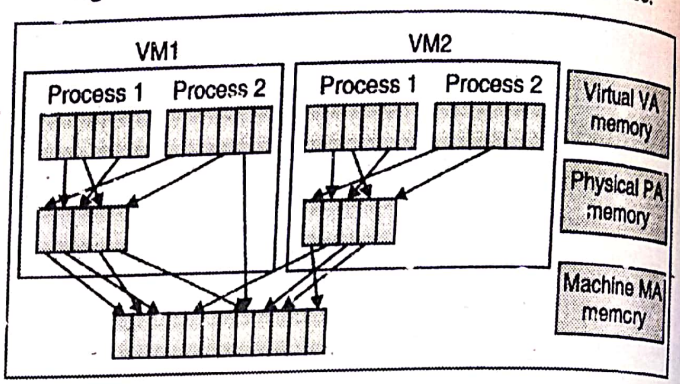


Fig. 2.6 : Two level memory mapping procedure

As each page table in the guest Operating System has a separate page table in the VMM related to it, the VMM page table is known as shadow page table. One more layer of indirection to virtual memory is added by the nested page tables. The virtual-to-physical translations are handled by the MMU as defined by the OS. Another set of page tables defined by the hypervisor translates the physical memory addresses to machine addresses.

A set of page tables for every process is maintained by modern operating systems, hence the shadow page tables will get flooded. It leads to high performance overhead as well as cost of memory. For virtual memory to machine memory address translation, shadow page tables are used by the VMware. Processors take help of TLB hardware for the process of mapping the virtual memory with the machine memory which helps to avoid the two levels of translation on each access.

When the virtual memory is changed into physical memory by the guest OS, the shadow page tables are updated by the VMM for enabling of direct lookup.

Q. 9 Write a note on IO Virtualization. (4 Marks)

Ans. :

I/O Virtualization

I/O virtualization is used to manage the routing of various types of I/O requests in between virtual devices and the shared physical hardware.

There are three ways to implement I/O virtualization

1. Full device emulation
2. Para-virtualization
3. Direct I/O.

Full device emulation is considered as a first approach for I/O virtualization. Generally, well-known, real-world devices are emulated by this approach.

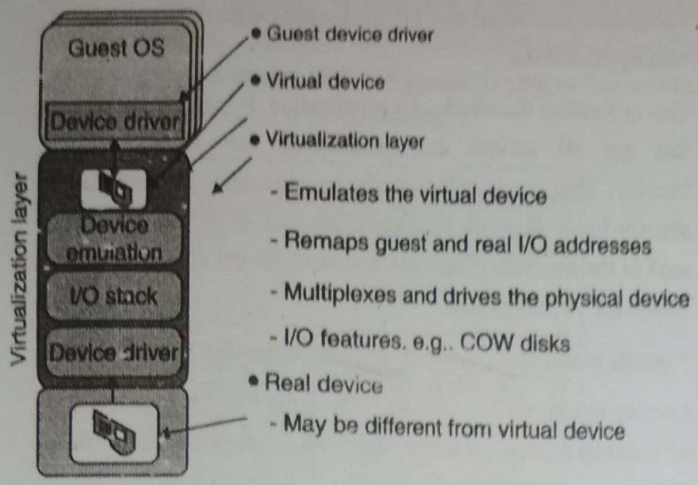


Fig. 2.7 : Device emulation for I/O virtualization

All types of functions of a device or bus infrastructure like identification, interrupts, device enumeration are simulated in software. This software works as a virtual device and placed in the VMM. The I/O access requests of the guest OS which communicates with the different types of I/O devices get trapped in the VMM. The full device emulation approach is shown in Fig. 2.7. Multiple VMs can share common hardware device simultaneously.

The execution of software emulation is slower than the hardware which is emulated by it. In Xen, usually the para-virtualization method of I/O virtualization is used. It is also called as the "split-driver-model" which contains frontend and backend driver. The execution of frontend driver is done in Domain U while execution of backend driver is done in Domain 0. Both of these drivers communicate with each other through block of shared memory. The responsibility of the frontend driver is to manage the I/O requests of the guest operating systems while the backend driver manages the actual I/O devices and also handles the I/O data of various VMs.

The device performance of para-I/O-virtualization is better than full device emulation, but it has higher CPU overhead. The VM can access devices directly by the direct I/O virtualization. Close-to-native performance can be achieved by it by avoiding high CPU costs.

Q. 10 Write a note on Virtualization and Cloud computing.

Ans. :

Virtualization and Cloud Computing

In the context of cloud computing, virtualization plays a significant role as it allows for the suitable degree of customization, security, isolation, and manageability which are considered as fundamentals for the process of delivering IT services on demand. Previously the use of Virtualization technologies was limited to offer configurable computing environments and storage. Network virtualization is a considered as a complementary feature, which is naturally required to build virtual computing systems. The most significant is the role of virtual computing environment as well as execution virtualization techniques. In cloud computing, among several virtualization techniques, hardware and programming language virtualization are mostly used.

Hardware virtualization is considered as a significant aspect for solutions in the IaaS (Infrastructure-as-a-Service) market segment. The programming language virtualization technology is used in Platform-as-a-Service (PaaS) offerings. In all these two cases, the ability of offering a customizable and sandboxed environment provides pretty good business opportunity for organizations featuring a big computing infrastructure which can sustain as well as process huge workloads. Furthermore, virtualization also provides isolation and a better control, thus making simple the leasing of services and their accountability on the vendor side.

Virtualization is considered as an enabler for computation on demand, additionally it also provides the chance to design more competent computing systems through consolidation, which is performed transparently to cloud computing service users. As virtualization provides the way to create isolated and controllable environments, it becomes easy to serve these environments with the same resource without any need to interfere with each other's work. Also if there exist capable underlying resources, no evidence of such sharing can be seen. This option is specifically useful when resources are underutilized, since it allows dropping the number of active resources by the way of aggregating virtual machines over few resources that become completely utilized.

The name for this practice is server consolidation, whereas name for movement of virtual machine instances is virtual machine migration. Since virtual machine instances are considered as controllable environments, it is possible to apply consolidation with a minimum impact, either by provisionally stopping its execution and shifting its data to other resources or by the way of performing a finer control and shifting the instance during its execution. This second techniques is called as live migration and usually considered as more complex to implement but also more efficient as there is no disturbance of the activity of the virtual machine instance.

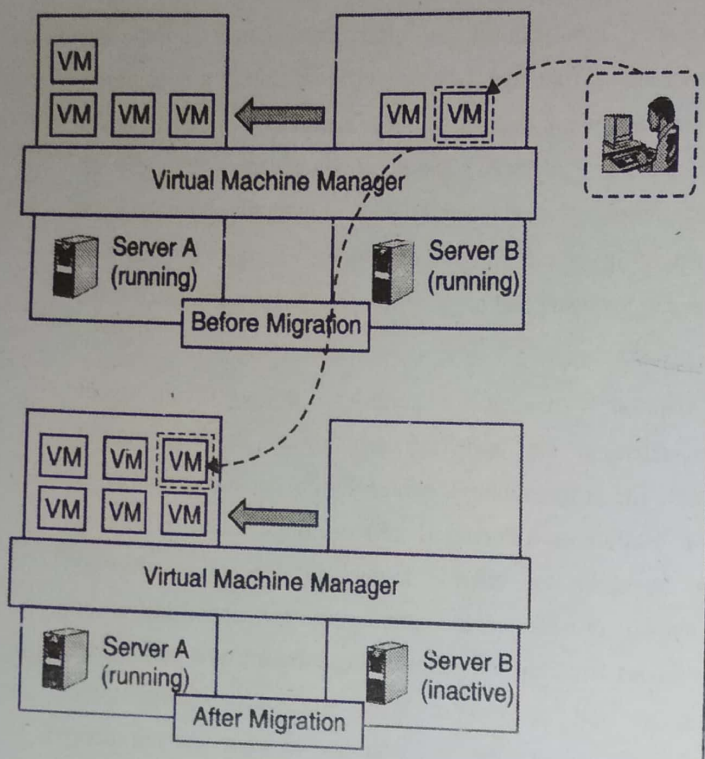


Fig. 2.8 : Live migration and server consolidation

In hardware virtualization, server consolidation and virtual machine migration are mostly preferred, even if it is also technically possible to use them in programming language virtualization. Storage virtualization is a good opportunity provided by virtualization technologies, often considered as complementary to the execution of virtualization. Still in this situation, vendors backed by huge computing infrastructures offering large storage facilities can exploit those facilities into a virtual storage service, which can be effortlessly partitionable into slices. These slices can be dynamic and it is possible to offer them as a service.

More ever, facilities to secure and protect the hosting infrastructure are offered, as are techniques for easy accountability of those services. At the end, cloud computing restores the concept of desktop virtualization, which was basically introduced in the mainframe era. The capability to regenerate the whole computing stack from infrastructure to application services on demand provides the way to getting an absolute virtual computer which is hosted on the infrastructure owned by the provider and accessed by a thin client with the help of capable Internet connection.

Q. 11 Discuss disadvantages of virtualization.

Ans. :

Disadvantages of Virtualization

1. **It can be expensive**

   One of the important things in case of virtualization is the cost. Virtualization can be quite a pricey investment upfront. For installing the virtual server one-time heavy investment is required which is more than the cost of a traditional server.

2. **Virtualization might not be compatible with other servers and applications**

   This is another drawback of virtualization. It may be possible that not all servers and applications are virtualization friendly. This can be a big headache when an investment has already been made on number of servers or if the software used in the business process is not an upgraded version which allows for virtualization.

3. **It needs training to network administrators**

   Another drawback of virtualization is the necessity to spend for training purpose of the network administrator which is an additional expense.

4. **It still has limitations**

   It is not possible that all applications or servers can work within an environment of virtualization. Hence there is need of hybrid environment to function properly. Since not all the vendors support virtualization and few may stop supporting it later on, there is always a level of uncertainty to implement this system completely.

5. **It creates a security risk**

   In virtualization system, sometimes the maintaining security of data gets difficult.

6. **It creates an availability issue**

   It is little bit uncertain that every time there will be availability of resources, hence at crucial point if resources not get available, then it affect work efficiency as well as the credential of company.

7. **It creates a scalability issue**

   Sudden demand or access of large number of virtualized resources by ay growing business may affect the availability of resources for other small businesses.

8. **It requires several links in a chain that must work together cohesively**

   There is need of proper functioning of all the links in a chain of virtualization otherwise simple task like saving file may also become tedious for user.

Q. 12 Explain architecture of KVM.

Ans. :

Architecture of KVM

The Kernel-based Virtual Machine (KVM) is a full native virtualization solution for Linux on x86 hardware containing virtualization extensions (Intel VT or AMD-V). Limited support for para-virtualization is also available for Linux and Windows guests in the form of a para-virtual network driver. KVM is currently designed to interface with the kernel via a loadable kernel module. Operating system versions supported include a wide

variety of guest operating systems like Linux, BSD, Solaris, Windows, Haiku, ReactOS, and AROS Research Operating System. A patched version of KVM (qemu) is able to run on Mac OS X. Fig. 2.9 shows the KVM architecture.

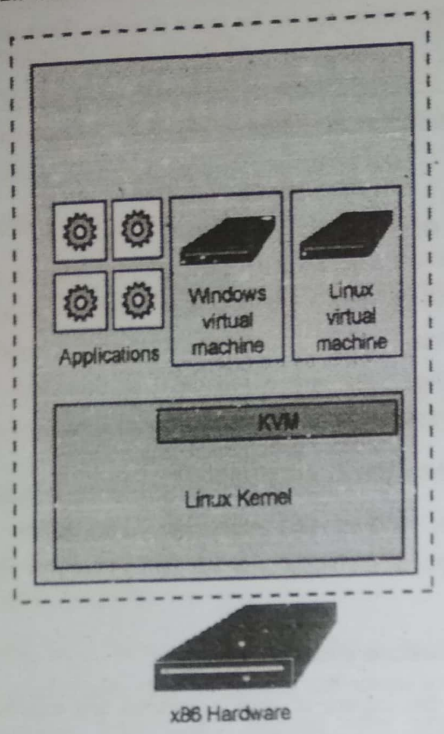


Fig. 2.9 : The KVM architecture

In the KVM architecture, the virtual machine is implemented as regular Linux process, scheduled by the standard Linux scheduler. In fact, each virtual CPU appears as a regular Linux process. This allows KVM to benefit from all the features of the Linux kernel. Device emulation is handled by a modified version of qemu that provides an emulated BIOS, PCI bus, USB bus, and a standard set of devices such as IDE and SCSI disk controllers, network cards, etc.

Q. 13 What are the features of KVM.

Ans. :

Features of KVM

The following features are key to KVM.

1. **Security**

Since a virtual machine is implemented as a Linux process, it leverages the standard Linux security model to provide isolation and resource controls. The Linux kernel uses SELinux (Security-Enhanced Linux) to add mandatory access controls, multi-level and multi- category security, and to handle policy enforcement. SELinux provides strict resource isolation and confinement for processes running in the Linux kernel.

The SVirt project: a community effort attempting to integrate Mandatory Access Control (MAC) security and Linux-based virtualization (KVM) builds on SELinux to provide an infrastructure to allow an administrator to define policies for virtual machine isolation. Out of the box, SVirt ensures that a virtual machines resources cannot be accessed by any other process (or virtual machine); this can be extended by the sysadmin to define fine-grained permissions; for example, to group virtual machines together to share resources.

2. **Memory Management**

KVM inherits powerful memory management features from Linux. The memory of a virtual machine is stored the same as memory is for any other Linux process and can be swapped, backed by large pages for better performance, shared, or backed by a disk file. NUMA support (Non-Uniform Memory Access, memory design for multiprocessors) allows virtual machines to efficiently access large amounts of memory.

KVM supports the latest memory virtualization features from CPU vendors with support for Intel's Extended Page Table (EPT) and AMD's Rapid Virtualization Indexing (RVI) to deliver reduced CPU utilization and higher throughput. Memory page sharing is supported through a kernel feature called Kernel Same-page Merging (KSM). KSM scans the memory of each virtual machine and where virtual machines have identical memory pages, KSM merges these into a single page that it shares between the virtual machines, storing only a single copy. If a guest attempts to change this shared page, it will be given its own private copy.

3. Storage

KVM is able to use any storage supported by Linux to store virtual machine images, including local disks with IDE, SCSI and SATA, Network Attached Storage (NAS) including NFS and SAMBA/CIFS, or SAN with support for iSCSI and Fibre Channel. Multipath I/O may be used to improve storage throughput and to provide redundancy. Again, because KVM is part of the Linux kernel, it can leverage a proven and reliable storage infrastructure with support from all leading storage vendors; its storage stack has a proven record in production deployments. KVM also supports virtual machine images on shared file systems such as the Global File System (GFS2) to allow virtual machine images to be shared between multiple hosts or shared using logical volumes.

Disk images support thin provisioning allowing improved storage utilization by only allocating storage when it is required by the virtual machine rather than allocating the entire storage upfront.

The native disk format for KVM is QCOW2 which includes support for snapshots allowing multiple levels of snapshots, compression, and encryption.

4. **Live Migration**

KVM supports live migration which provides the ability to move a running virtual machine between physical hosts with no interruption to service. Live migration is transparent to the user, the virtual machine remains powered on, network connections remain active, and user applications continues to run while the virtual machine is relocated to a new physical host.

5. Device Drivers

KVM supports hybrid virtualization where para-virtualized drivers are installed in the guest operating system to allow virtual machines to use an optimized I/O interface rather than emulated devices to deliver high performance I/O for network and block devices. The KVM hypervisor uses the VirtIO standard developed by IBM and Red Hat in conjunction with the Linux community for para-virtualized drivers; it is a hypervisor-independent interface for building device drivers allowing the same set of device drivers to be used for multiple hypervisors, allowing for better guest interoperability.

Q. 14 Explain Xen architecture in detail. May 16

Ans. :

Xen Architecture

Xen is an open source hypervisor program which is developed by Cambridge University. Xen hypervisor is of type microkernel, which is used to separate the policy from the mechanism. All the mechanisms are implemented by the Xen hypervisor, and policy handling is the responsibility of Domain 0 as shown in Fig. 2.10.

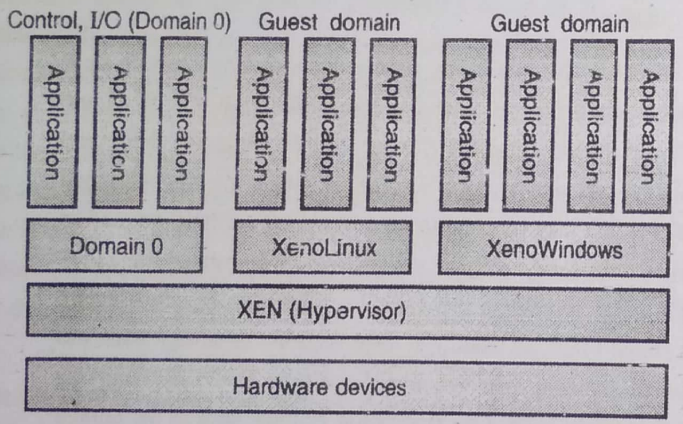


Fig. 2.10 : Xen Architecture

In Xen, no device drivers are included natively. Just a mechanism is provided by Xen with the help of which the guest OS can have direct access to the physical devices. This helps to keep the size of Xen hypervisor effectively small. A virtual environment is provided by Xen between the hardware and the OS. Now a day there are number of vendors who are in process of developing commercial Xen hypervisors. Some of them are Citrix XenServer and Oracle VM. The most important components of a Xen system are considered as the hypervisor, kernel, and applications. These three components should be organized in proper manner.

Like different virtualization systems, number of guest operating systems can be executed on top of the hypervisor. However, not all guest operating systems are created with similar functionality, and one in particular situation can control the others. The guest OS, which can control other operating systems is known as Domain while the others are known as Domain U. Domain 0 is considered as a privileged guest OS of Xen. Initially Domain 0 is loaded when Xen boots without the availability of any file system drivers. The basic aim behind design of Domain 0 is to access hardware directly as well as manage devices. Hence allocating and mapping hardware resources for the guest domains (Domain-U) is responsibility of Domain 0.

Q. 15 Explain functionality of Hyper-V.

Ans. :

Functionality of Hyper-V

1. Establish or expand a private cloud environment

Provide more flexible, on-demand IT services by moving to or expanding your use of shared resources and adjust utilization as demand changes.

2. Use your hardware more effectively

Consolidate servers and workloads onto fewer, more powerful physical computers to use less power and physical space.

3. Improve business continuity

Minimize the impact of both scheduled and unscheduled downtime of your workloads.

4. Establish or expand a virtual desktop infrastructure (VDI)

Use a centralized desktop strategy with VDI can help you increase business agility and data security, as well as simplify regulatory compliance and manage desktop operating systems and applications.

5. Make development and test more efficient

Reproduce different computing environments without having to buy or maintain all the hardware you'd need if you only used physical systems.

Q.16 What are the features of Hyper-V

Ans. :

Features of Hyper-V

1. Computing Environment

A Hyper-V virtual machine includes the same basic parts as a physical computer, such as memory, processor, storage, and networking. All these parts have features and options that you can configure different ways to meet different needs. Storage and networking can each be considered categories of their own, because of the many ways you can configure them.

2. Disaster Recovery and Backup

For disaster recovery, Hyper-V Replica creates copies of virtual machines, intended to be stored in another physical location, so you can restore the virtual machine from the copy. For backup, Hyper-V offers two types. One uses saved

states and the other uses Volume Shadow Copy Service (VSS) so you can make application-consistent backups for programs that support VSS.

3. **Optimization**

   Each supported guest operating system has a customized set of services and drivers, called integration services, that make it easier to use the operating system in a Hyper-V virtual machine.

4. **Portability**

   Features such as live migration, storage migration, and import/export make it easier to move or distribute a virtual machine.

5. **Remote Connectivity**

   Hyper-V includes Virtual Machine Connection, a remote connection tool for use with both Windows and Linux. Unlike Remote Desktop, this tool gives you console access, so you can see what's happening in the guest even when the operating system isn't booted yet.

6. **Security**

   Secure boot and shielded virtual machines help protect against malware and other unauthorized access to a virtual machine and its data.

Chapter 3 : Cloud Computing Services

Q. 1 Explain XaaS with its advantages.

Ans. :

Anything as a Service

Anything as a service (XaaS) describes a wide range of services associated with cloud computing and remote access. With cloud computing technologies, vendors offer organizations different types of services over the web or similar networks. This idea started with the basic SaaS (software as a service) with cloud providers providing individual software applications.

Some other terms such as IaaS (infrastructure as a service) and CaaS (communications as a service) were added as cloud services evolved. With number of different kinds of IT resources now delivered this way, XaaS is a somewhat ironic term for the proliferation of cloud services. Anything as a service is also termed as X as a service or everything as a service.

The basic thought behind XaaS and related cloud services is that organizations can cut costs and get particular kinds of personal resources by the way of purchasing services from providers on a subscription basis. Before the emergence of XaaS and cloud services, businesses often had to buy the licensed software products and install them on site. They had to buy hardware and link it together to create expanded networks. They had to do all security work on site, and they had to provide expensive server setups and other infrastructure for all of their business processes.

By contrast, with XaaS, businesses simply buy what they need, and pay for it as they need it.

This allows businesses to drastically change service models over time. Using multi-tenant approaches, cloud services can provide a lot of flexibility. Concepts like resource pooling and rapid elasticity support these services where business leaders can simply add or subtract services as necessary. XaaS services are typically governed by something called a service level agreement (SLA), where client and vendor work closely to understand how services will be provided.

Advantages of XaaS

1. When speaking about XaaS as it relates to cloud computing, there are a number of benefits:
2. Lower costs.
3. Flexibility. This also includes easier scalability.
4. Maintenance is done by the provider. This frees up the customer's resources and allows them to focus on what they do best.
5. Easy access to new technologies (which are being developed rapidly).
6. New business services are able to debut quickly (think weeks instead of months).
7. Allows for quick responses to market developments. "With constant availability to resources, data and other services through XaaS, businesses can respond in a faster way to any change in the business environment and enjoy better profit figures".

There are several examples of XaaS, but the most common encompass the three general cloud computing models : Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS).

Q. 2 Write a note on "Security as a Service". What are its advantages?

Ans. :

Security as a Service

Security as a service (SECaaS) is a business model in which service providers integrates their security services into a corporate infrastructure on a subscription basis more cost effectively than most individuals or corporations can provide on their own, when total cost of ownership is considered. SECaaS is inspired by the "software as a service" model as applied to information security type services and does not require on-premises hardware, avoiding

substantial capital outlays. These security services often include authentication, antivirus, antimalware/spyware, intrusion detection and security event management, among others. Outsourced security licensing and delivery is boasting a multibillion-dollar market.

SECaaS provides users with Internet security services providing protection from online threats and attacks such as DDoS that are constantly searching for access points to compromise websites. As the demand and use of cloud computing skyrockets, users are more vulnerable to attacks due to accessing the Internet from new access points. SECaaS serves as a buffer against the most persistent online threats.

Advantages of Security as a Service

Security as a service offers a number of benefits, including :

1. **Cost-cutting :** SECaaS eases the financial constraints and burdens for online businesses, integrating security services without on-premises hardware or a huge budget. Using a cloud-based security product also bypasses the need for costly security experts and analysts.
2. **Consistent and uniform protection** : SECaaS services provide continued protection as databases are constantly being updated to provide up-to-date security coverage. It also eases the issue of having separate infrastructures, instead combining all elements in one manageable system.
1. Constant virus definition updates that are not reliant on user compliance.
2. Greater security expertise than is typically available within an organization.
3. Faster user provisioning.
4. Outsourcing of administrative tasks, such as log management, to save time and money and allow an organization to devote more time to its core competencies.
5. A web interface that allows in-house administration of some tasks as well as a view of the security environment and ongoing activities.

Q. 3 Explain "Database as a Service" with its advantages.

Ans. :

Database as a Service

Database as a service (DBaaS) is a cloud computing service model which offers users with specific form of access to a database without any requirement of setting up physical hardware, installing software or configuring for performance. The service provider is responsible for each and every administrative task as well as maintenance. Hence the user or application owner can easily use the database. Sometimes if the customer wants more control over the database, then that option is also provided and vary based on the provider.

DBaaS builds on the concept that the database can be provided on demand to the user irrespective of geographic or organizational separation of provider and the consumer (end user). An IT organization deploys DBaaS which helps users (developers) to provision a database as per requirement from a catalog of available databases. In the list there may be popular relational as well as non-relational databases and the IT organization is able to configure the DBaaS to support particular releases of these software titles. It is possible for the IT organization to confine the configurations that particular users can provision (for instance, developers can just provision with little memory footprint, with conventional disks while devops can offer higher capacity servers with SSD's).

Ultimately, the IT organization can build policies for standard database operations such as backups to make sure that the data is appropriately saved from time to time for the purpose of recovery if needed. Usually an end user is able to access the DBaaS system with the help of a portal which allows selecting from several database titles, and in a wide range of different configuration options. Just with the help of a few clicks the requested database will be provisioned for the respective users. The DBaaS system promptly provisions the database

Advantages of Database as a Service

1. Developer Agility

When a developer expects to provision a database, the steps necessary are provisioning compute, storage and networking components, configuring them properly and then installing database software. Finally, it is necessary to configure the database software properly for the purpose of utilizing the underlying infrastructure components. In this multi-step process there are number of opportunities for errors, omissions and non-standard modes of operation. When the thing that is being provisioned (a database) is the "system of record", this is unacceptable.

In the process of configuring the DBaaS, the organization sets the standards through which databases will be provisioned. By the way of standardizing the provisioning model, DBaaS makes it sure that a single operation is sufficient to provision the databases, and those databases are provisioned in a consistent manner, and in a way which is aligned with the top practices for that specific database and business. Once in operation, complex database operations such as resizing a cluster are now becomes just a simple API call and the developer do not have to worry regarding the details of how the respective operation should be carried out for the particular database and version.

The abstraction offered by the DBaaS manages all of that and lets the developer to concentrate his or her energy on the application instead of the underlying database. Finally, the developer activities are usually iterative and involve spinning up, using, and then destroying database servers.

2. DBA Productivity

When an enterprise handles several instances of number of different databases, substantial resources get consumed on maintenance and upkeep. It involves things such as tuning, configuration, patching, periodic backups, and so on; all these things are necessary for DBAs to keep databases in proper working order. DBaaS solutions offers abstractions which lets DBAs to handle groups of databases and perform operations such as upgrades and configuration changes on a fleet of databases in an easy way. This helps DBAs to concentrate more on activities such as setting the standards of operation for the organization and verifying that they have the best tools available for themselves as well as for the developers.

3. Application Reliability, Performance and Security

Databases are often considered as the "system of record" and are the repository of valuable data of the enterprise. A database outage surely has catastrophic impact. By the way of automation as well as standardization, DBaaS makes it sure that there is consistency in all of the common workflows which are involved in the provisioning, configuration, management, and operation of databases. With the help of this standardization, a DBaaS guarantees that the way of operations of all the databases is same, and in keeping with the best practices set by the IT organization.

This helps DBAs to concentrate more on important things such as the application and innovation instead of running a database. It is essential to understand that most of the organizations today operate applications which need many different database technologies. With this diversity in database technologies, DBaaS solutions helps IT organizations to guarantee application reliability, performance as well as data security whichever the database solution is in use, without necessity that the IT organization or the developer team have in-depth knowledge regarding the finer points related to all the technologies in use. DBaaS solutions summarize such best practices and codify the appropriate way to deploy, manage as well as operate all of the distinct technologies by the way of freeing up the DBAs and developers from these chores.

Q. 4 Explain Storage as a Service.

Ans. :

Storage as a Service

There are number of benefits of Cloud storage over traditional data storage. The data kept on cloud is accessible from any location having Internet access. There is no need of using the same computer to access data and no need to carry physical storage devices. Also, if any company has branch offices, cloud makes it easy to access data from any branch. There are several cloud storage systems available in market in which few are very particular in what they do. Some focus on specific market and store only email or digital pictures, while some can store any type of data. Some providers are comparatively very small, while some are huge and are able to fill an entire warehouse.

In the cloud storage system, at the most basic level, there is need of only single data server which is connected to the Internet. Files are stored by the subscriber on the server. A subscriber copies files to the server over the Internet, in which records are stored. Whenever client needs the data, he or she has access to the respective data server with a web-based interface. The client can get the data from the server directly or get permission from server to access as well as manipulate [illegible].

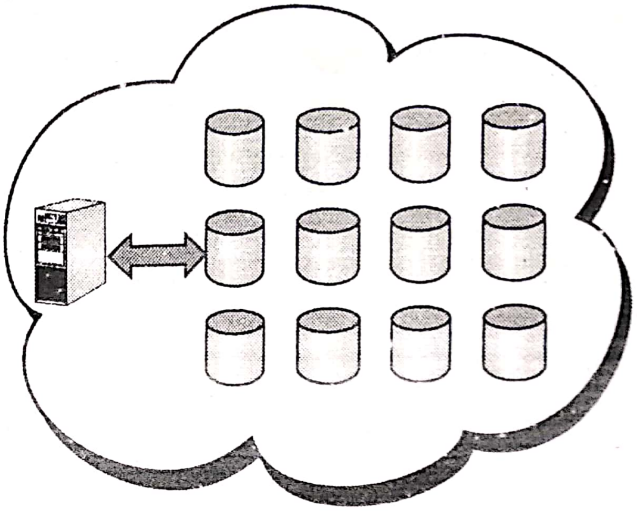


Fig. 3.1 : More commodity hard drives can be added by the provider to enhance capacity

More specifically, on the other hand, several data servers are used by the cloud storage systems. As there is need of maintenance or repair to the servers, the data must be stored on more than one machines enabling redundancy. In the absence of redundancy, it is difficult for cloud storage systems to guarantee clients that their data will be accessible at any given time. Number of systems uses different power supplies so as to store the same data on servers which helps the clients to access their data in case of failure of power supply also. Number of clients prefer cloud storage not as they've run out of room locally, but for the purpose of safety. If there is any bad incidence with their building occurs, then they haven't lost all their data. The term **Storage as a Service** indicates that space on their storage is made available by a third-party provider on rent to end users facing the problem of budget or capital budget to pay for it on their own.

It is also considered as best when there is unavailability of technical personnel or knowledge is inadequate for the purpose of implementing and maintaining the storage infrastructure. The Storage service providers offer the complexity of current backup, replication, and disaster recovery needs because of which the service is in huge demand, mostly among small and medium-sized businesses. The most important advantage of SaaS is cost savings.

Providers rent the storage through a cost-per-gigabyte-stored or cost-per-data-transferred model. There is no need to the end user to pay for infrastructure; they just have to pay for the amount of

data which they have transferred and stored on the provider's servers. Client software is utilized by the customer to mention the backup set and then move the data across a WAN.

If there is data loss, customer has option to get the lost data from the service provider.

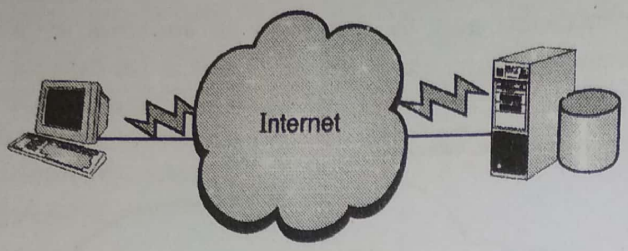


Fig. 3.2 : Clients rent storage capacity from cloud storage vendors

Q. 5 Explain security in cloud storage.

Ans. :

Security in Cloud

For security purpose most systems prefer combination of techniques :

Encryption : Information is encoded with the help of a complex algorithm. Encryption key is used to decode the encrypted files.

Despite the fact that it is probable to crack encrypted data, it is very difficult for most of the hackers since they do not have access to the amount of computer processing power which is required to crack the code.

1. **Authentication processes :** It needs a user to generate a name and password.
2. **Authorization practices :** Lists are created by the client regarding the people who should be able to access data stored on the cloud system.

Number of times there is multiple levels of authorization.

For example, there may be restricted access to a front-line employee for the data stored on the cloud and the access right of head of the IT department will be full and have free access to everything.

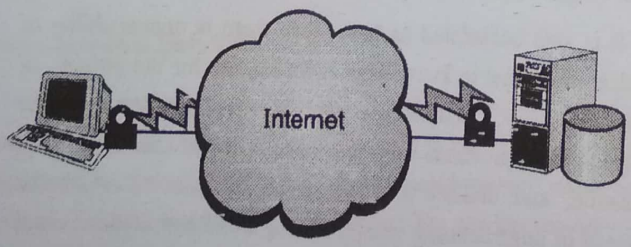


Fig. 3.3 : Encryption and authentication : security measures to keep data safe on a cloud storage.

But in spite of all these measures, there are still concerns that the information present on a remote system is vulnerable. One threat is always there that a hacker may find a way to enter into the secure system to access the data. One another aspect is that the employees who are disgruntled may provide harm to the data with their access credentials.

Q. 6 Explain advantages of cloud storage.

Ans. :

Advantages of Cloud Storage

Day by day, the attraction about cloud storage is increasing drastically in organizations. The reason is; cloud storage helps to place data on the Web, stored across storage systems instead of a designated corporate hosting site. The server loads are balanced by the cloud storage providers; they shift data among several datacenters, ensuring quick access of the data. Data storage on cloud is considered as advantageous, as it protects the user data in case of a disaster.

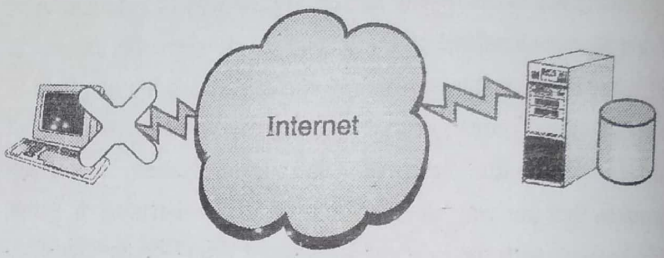


Fig. 3.4 : In case of catastrophe at organization, data is safe on cloud

Q. 7 Which cautions have to taken in cloud storage ?

Ans. :

Cautions in Cloud Storage

A mixed approach is considered as the best way to embrace the cloud, because cloud storage is still not completely developed. It indicates that one should not store everything on the cloud rather use it for a few, noncritical purposes. Big organizations might have trouble with vendors such as Google or Amazon, since they are strained to rewrite solutions for their applications while portability is not seen. A vendor named 3tera, on the other hand, supports applications developed in LAMP, Solaris, Java, or Windows.NET. Also one more concern is that the vendor should assure best deal with quality service.

Legal issue is another important aspect. Consider, users' data is copyrighted such as music or video then there may not be any option for licensing reasons. Users should examine the accountability of storage provider. Vendors offer several assurances regarding the maintenance of data. Service may be offered by them, but user has to see what will be their solution or enumeration in case of loss of data. The best solution is considers as having more than one redundant systems : local and offsite backup; sync and archive.

Q. 8 Write a note on "Collaboration as a Service".

Ans. :

Collaboration as a Service

Cloud collaboration enables people to work simultaneously on documents that live 'in the cloud' so you can access files from anywhere with an internet connection. The start of a cloud collaboration process involves one user creating a file or document and giving access to other members of the team. Anyone who has access can make changes to the document at any time, including when other people are editing or viewing it. Any changes that you make save and sync so every user sees the same version of the project whenever (and wherever) they view it.

The cloud has made collaboration easy. Rather than chasing down details, sifting through dozens of emails, and consolidating pockets of information, you can head to the cloud, which centralizes all important information in one location where anyone can view it and make changes at any time. For enterprises, cloud-based collaboration has become key for profitability, growth, and cost reduction. A cloud-based system allows employees to work together on documents and projects, which are kept outside of a company's own server system and firewall. The cloud also enables virtually unlimited storage of important historical documents and data, easily retrievable as needed. Cloud collaboration has become more sophisticated as vendors try to attract customers.

It is common for a collaboration tool to include a way for project participants to see who else is viewing the document and to communicate with each other while working, such as through comments or a chat function.

Tools also often allow users to set up email alerts for when a file is changed. These and other functions help to increase worker efficiency and productivity. Employee's motivations for using cloud collaboration tools vary, but the drive is often that workers find the cloud tool to be better in some way than an old tool.

Employees may think the cloud collaboration tool is faster, looks nicer, is easier to use and more. Desire for a better collaboration tool can lead employees to choose and use a tool without prior approval of IT, a practice known as shadow IT. IT departments should be on the lookout for this, but they should also be open to the positive impact a cloud collaboration tool can have on group communication and teamwork.

The best cloud collaboration tools :

1. Use real-time commenting and messaging features to enhance speed of project delivery.
2. Allow users to set permissions and manage other users' activity profiles.
3. Allow users to set personal activity feeds and email alert profiles to keep abreast of latest activities per file or user.
4. Allow users to collaborate and share files with users outside the company firewall.
5. Comply with company security and compliance framework.
6. Ensure full auditability of files and documents shared within and outside the organization.
7. Reduce workarounds for sharing and collaboration on large files.

Q. 9 What are the features of "Cloud Collaboration"?

Ans. :

Features of Cloud Collaboration

Cloud collaboration technology offers a wealth of user-centric features that can transform the communication experience :

1. **Universal user access** - The full suite of collaboration tools can be made available anywhere, anytime, with applications for desktop, mobile and tablet.
2. **IP voice and video** - A feature rich alternative to face-to-face meetings and traditional audio conferences, with support for HD voice and video calling in all its forms on all devices, from smartphones to room-based set ups.
3. **Sharing and conferencing** - Collaboration can happen in real-time, thanks to the ability to easily connect and share content wherever and whenever, with the freedom to share applications and desktops, white boards and annotations, regardless of device.
4. **Rich presence** - This gives users the option to select the optimum way of communicating with colleagues dependent on their presence status.
5. **Instant messaging** - IM is a platform designed for quick questions and fast responses, using presence indication and one-to-one and group chat functionality to transform communication speeds and accelerating decision-making.
6. **Group chat** - Group chat replicates the ease and speed of the messaging medium for multiple parties across diverse locations.
7. **Unified messaging** - A single inbox for emails/voicemails/text/messages streamlines communications handling, boosting personal productivity and efficiency.
8. **Single number reach** - The ability to be reached via the same number regardless of end device increases personal effectiveness and overall responsiveness.
9. **Click to dial audio and video calling** - Users can make audio calls using 'click to dial' from Outlook or a web browser, with the option to seamlessly upgrade to a video call.
10. **Group video conferencing** - Users can benefit from full video conferencing capability from the comfort of their desks or via their tablets or smartphones.

Q. 10 Explain the advantages and disadvantages of term "Compliance as a Service".

Ans. :

Advantages of Compliance as a Service (CaaS)

1. In cloud, Encryption is considered as quite difficult to track. It is simplified by the Compliance as a Service. Cloud provider's service can be used to complete the requirements of end user and organizations regarding governance including compliance. These services help to deliver pre-built behaviors with particular regulations, such as needed encryption levels.
2. Compliance as a Service is configurable which is cost effective for the enterprises and reduces the maintenance along with changing regulations, as well as internal and external policies of the corporations.

Disadvantages of Compliance as a Service (CaaS)

1. Cloud service consumers are in general considered as responsible for any issues with the compliance services. Hence it is necessary for the customer to validate the compliance services so as to make sure that there are no issues.
2. It is very difficult for "Compliance as a Service" providers to support each and every regulation among all the countries in the world. Additionally since all the services are based upon cloud, one risk is always there that the service providers may break providing the services at any time for the reason of low uses of their services This makes the end-users and enterprises completely dependent on service providers.

Q. 11 What is "Monitoring as a Service? Explain in brief.

Ans. :

Monitoring as a Service

Cloud Monitoring as a Service is referred to a type of on demand IT service that provides cloud monitoring and management tools for monitoring cloud based platforms, websites, servers, IT Infrastructure etc. Cloud monitoring as a service provides a fully managed cloud monitoring service for cloud and virtualization environments in organizations. Typically, cloud monitoring as a service is delivered through a SaaS based cloud monitoring software that monitors and detects performance issues across the cloud infrastructure. The performance statistics and issues are reported to the cloud administrators for reviewing in a central dashboard or through email, SMS and other alerts and notifications.

The potential use of MaaS would ensure

1. Server Uptime.
2. Will make error reporting and handling easier.
3. Utilization of the resources to the maximum extent possible.
4. Automated system allows greater throughput.
5. Cheaper than the existing conventional human based monitoring service.
6. Easy for consumer to monitor the situation of his application on the go.

Much notice needs to be given to the inquiry of how to supervise all the cloud services, especially in the case where the service might be combined with applications running in the data center.

The idea of a monitoring tool that is delivered as a service so that one can log onto the central web based instrument panel which is hosted by the vendor of the monitoring service and see and control that all is going on with all of the applications no matter where they are located.

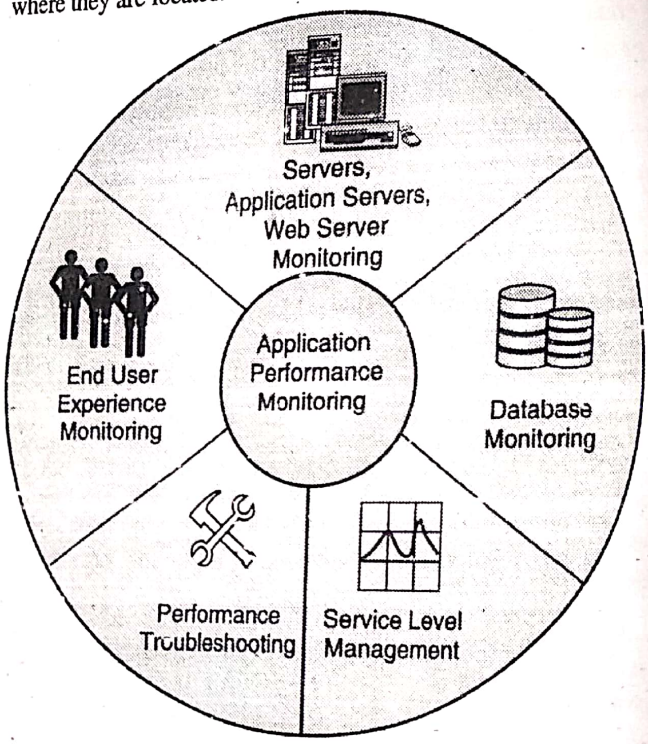


Fig. 3.5 : Monitoring as a Service

Q. 12 Explain advantages of "Monitoring as a Service.

Ans. :

Advantages of Monitoring as a Service

1. **Ready to Use Monitoring Tool Login**

   The vendor takes care of setting up the hardware infrastructure, monitoring tool, configuration and alert settings on behalf of the customer. The customer gets a ready to use login to the monitoring dashboard that is accessible using an internet browser. A mobile client is also available for the MaaS dashboard for IT administrators.

2. **Inherently Available 24x7x365**

   Since MaaS is deployed in the cloud, the monitoring dashboard itself is available 24x7x365 that can be accessed anytime from anywhere. There are no downtimes associated with the monitoring tool.

3. **Easy Integration with Business Processes**

MaaS can generate alert based on specific business conditions. MaaS also supports multiple levels of escalation so that different user groups can get different levels of alerts.

4. **Cloud Aware and Cloud Ready**

Since MaaS is already in the cloud, MaaS works well with other cloud based products such as PaaS and SaaS. MaaS can monitor Amazon and Rackspace cloud infrastructure. MaaS can monitor any private cloud deployments that a customer might have.

5. **Zero Maintenance Overheads**

As a MaaS customer, user doesn't need to invest in a network operations centre. Neither do he needs to invest an in-house team of qualified IT engineers to run the monitoring desk since the MaaS vendor is doing that on behalf of the customer.

Q. 13 Write a note on "Communication as a Service".

Ans. :

Communication as a Service

Communications as a Service (CaaS) is considered as an outsourced organization communications solution which is possible to lease from a single vendor. Such communications regarding the organization include voice over IP (VoIP or Internet telephony), instant messaging (IM), collaboration and video-conference applications with the help of fixed as well as mobile devices. The development of CaaS has been evolved with the same lines as SaaS (Software as a Service). The responsibility of all hardware as well software management is of CaaS vendor and also he has to provide assured Quality of Service (QoS). CaaS helps organizations to exclusively deploy communications devices and modes on the foundation of pay-as-you-go, as-needed basis.

This approach helps to avoid the huge capital investment and constant overhead for a system capacity which may frequently exceed or fall short of present demand. CaaS provides flexibility as well as expandability which might be otherwise non-affordable for small and medium-sized business, giving flexibility for the introduction of new devices, modes or coverage as per requirement. It is possible to change the network capacity and feature set in a frequent manner if required so that functionality keeps pace with demand and no wastage of resources. There is no any possibility of risk of the system becoming obsolete and demanding periodic major upgrades or even replacements.

Q. 14 Explain "Network as a Service" with its advantages.

Ans. : Network as Service

Network as a service (NaaS) is a business model developed for the purpose of providing enterprise-wide area network services in the form of virtual manner on subscription basis. In general there are some complicated tasks such as configuring and operating routers with protocols, WAN optimizers and additional components like firewalls or software-defined-WAN endpoints.

In the context of NaaS, third-party provider is responsible for those activities which then further made available to enterprise customers. The overall functionality regarding the infrastructure may be covered in one NaaS flat fee, or the organization may select to subscribe separately to different services. Those services contain optimization, firewall or other security and SD-WAN which is basically dependent on the service provider. Some NaaS providers have particular focus areas, such as ultra-secure connectivity, ultra-simple configuration, or offering services to mobile and temporary locations. The classic buyers of NaaS are small or midsize organizations, especially those who do not have any investment in a WAN.

NaaS is considered as an attractive option by the new business owners since it evades a huge capital investment expense for network hardware. NaaS also helps to lessen the amount of staff time necessary for maintenance of the network and reduces the level of training as well as skill needed by the network staff.

With NaaS, the network fundamentally turns into one more utility we pay for, such as the electricity, water or heat. In the business model of NaaS, the enterprise's network is controlled by IT staff using just a portal instead of through a headache of network management tools as well as stacks of hardware. It is possible to add new location easily to the enterprise's WAN by the way of connecting it to the NaaS provider's nearest point of presence (POP) either directly by using the leased line to a nearby data center or over the internet.

Advantages of Network as a Service

1. **Independence :** Every customer is independent and it is possible for him to segregate the network.
2. **Bursting :** The NaaS customers have to pay for the high-capacity network only when there is necessity.
3. **Resilience :** For complex and critical applications NaaS offers reliability treatments.
4. **Analytics :** For highly sensitive applications NaaS offers data protection solutions.
5. **Ease of Adding New Service Elements :** It is a simple task to introduce new service element in the present network.
6. **Support Models :** NaaS provides several support models to reduce operation cost.
7. **Isolation of Customer Traffic**

Q. 15 Explain advantages of "Disaster Recovery as a Service"

Ans. :

Advantages of Disaster Recovery as a Service

1. **IT team can focus on core operations**

   When in-house IT team is assigned with the maintenance, testing and IT support associated with disaster recovery planning, they don't have the time to focus on other, critical IT functions. DRaaS simplifies IT management and frees up IT staff to do what they do best.

2. **Organization will be up and running more quickly**

   When it comes to disaster recovery planning, user can't afford to delay implementation. With DRaaS, user won't need to wait for months while hardware installations are taking place and being tested.

3. **Save money**

   In-house disaster recovery programs are expensive primarily because of the recurring costs for maintenance and IT support. Although DRaaS does represent an investment, business will reduce costs over the long term.

4. **User (Organization) won't pay for something he never use**

   With an in-house solution, user (organization) will inevitably have storage space he don't use. With a cloud-based, DRaaS solution, user only pays for what he have actually used. If user needs increase over time, he can upgrade service efficiently and quickly.

5. **Recovery time will be faster**

   The longer it takes for business to recover following a disaster, the more money business will lose. Whereas in-house solutions can lead to protracted recovery times, a DRaaS solution will typically have user back in business quickly, often in 15 minutes or less.

6. **User will have greater access**

   Because DRaaS is a cloud-based solution, user will be able to access his system from any location which has an internet connection. If a natural disaster makes his office unusable, for example, he will still be able to do business from another location.

7. **User will maintain in-house control**

   DRaaS doesn't mean user's business will lose control of his IT environment. User's in-house team will still be able to manage data storage, run reports, and recover lost data on their own.

8. **User won't be responsible for hardware protection**

   One of the big costs of data recovery plans is that associated with data protection for hardware. When user moves to a DRaaS solution, the service provider is responsible for hardware-related data protection.

9. **Data center will be secure**

   It's important to choose a service provider which can provide business with comprehensive data security. The best DRaaS providers ensure that their data centers are secure with state-of-the-art features, from CCTV cameras to electronic fencing, personals IDs and security-coded doors.

10. **User will have expert help and guidance**

    Reputable service providers will typically have deeper experience managing data security and disaster recovery planning than in-house team, in part because this is central to what they do. When problems occur, the best providers will be able to handle them quickly and efficiently.

Q. 16 Explain "Analytics as a Service" with advantages.

Ans. :

Analytic as a Service

Analytics as a service (AaaS) refers to the offerings of analytics software and operations by means of web-delivered technologies.

Those solutions offer organizations a substitute in establishing internal hardware setups to carry out business analytics.

To put analytics as a service in context, this type of service is considered as a part of a several services having similar names and similar ideas, including :

(i) Software as a service (SaaS)

(ii) Platform as a service (PaaS)

(iii) Infrastructure as a service (IaaS)

The common thing in all such services is that the service model substitutes internal systems with web-delivered services. In analytics as a service context, a service provider might offer access to a remote analytics platform on the basis of monthly rent. This permits a client to use that specific analytics software for as long as he wants, and to stop using the respective software and stop paying for the same at any time. Nowadays Analytics as a service is proved to be a helpful option for organizations since setting up analytics processes can be a work-intensive process. Organizations that require doing more analytics may necessitate more servers and other types of hardware, and they may require more IT staff for the implementation and maintenance of these programs.

Instead if the business is able to use analytics as a service, it can bypass these new costs and new business process requirements. Beside the option of complete outsourcing that analytics as a service offers, there is the option of selecting a hybrid system in which organizations use available resources for analytics and outsource other components through the web. All of this provides the modern organizations with more options and more particular solutions for changing business requirements in markets which work mainly on the availability of big data.

Advantages of Analytics as a Service

The important benefit of Analytics as a Service is that it permits users to concentrate on exploring and analyzing data, a high-value activity. Rather than having to set up servers, configure data analysis tools and script reports as organizations would require to do with on-premises analytics options. IT teams can utilize their time formulating hypotheses and discussing insights with stake holders.

Q. 17 Write a note on "Backup as a Service."

Ans. :

Backup as a Service

Online backup service, also known as cloud backup or backup as a service (BaaS), is a method of offsite data storage in which files, folders, or the entire contents of a hard drive are regularly backed up by a service vendor to a remote secure cloud-based data repository over a network connection. The purpose of online backup is simple and straightforward: to protect the information whether its business data or personal from the risk of loss associated with user error, hacking, or any other kind of technological disaster. Instead of performing backup with a centralized, on-premises IT department, BaaS connects systems to a private, public, or hybrid cloud managed by the outside provider. Backup as a service is easier to manage than other offsite services. Instead of worrying about rotating and managing tapes or hard disks at an offsite location, data storage administrators can offload maintenance and management to the provider.

How Does Backup as a Service Work?

In employing backup as a service, the first step is to purchase and sign up for the service. Next, you select the services you want to back up. You make those selections only once. After the initial setup, changes to data you've selected, as well as new data added to the services you've selected, are backed up automatically and, with most online backup services, almost instantly.

Why Is Backup as a Service Important?

Data is the essence of any organization. A staggering 60% of companies that lose critical data shut down within 6 months of the loss. Data loss is often a major concern for software-as-a-service (SaaS) customers because SaaS vendors' backup policies cannot guarantee a complete and speedy restore of lost data. Data can be put in jeopardy by user error, hacking, sync issues, or malicious insiders. Data loss, and the worry that surrounds it, can be easily avoided by pairing SaaS applications with a complete BaaS backup and recovery solution.

Q. 18 Write advantages of "Backup as a Service."

Ans. :

Advantages of Backup as a Service

1. **Convenience**

   The convenience offered by BaaS solutions is indisputable. BaaS is automated - once it's set up, information is saved automatically as it streams in. You don't have to proactively save, label, and track information. Rather, the convenience of BaaS allows you to concentrate on your work without worrying about data loss.

2. **Safety**

   Because your data is stored in the BaaS, you are not subject to the typical threats of hackers, natural disasters, and user error. In fact, data that is stored in the BaaS is encrypted, which minimizes the risks your data can incur.

3. **Ease of recovery**

   Due to multiple levels of redundancy, if data is lost or deleted (most frequently through individual user error or deletion), backups are available and easily located. Multiple levels of redundancy means that your BaaS stores multiple copies of your data in locations independent of each other. The more levels you have stored is better, because each level ensures that your data is safeguarded against loss as much as possible, allowing you to access a backed-up version of your data if it ever gets lost.

4. **Affordability**

   BaaS can be less expensive than the cost of tape drives, servers, or other hardware and software elements necessary to perform backup; the media on which the backups are stored; the transportation of media to a remote location for safekeeping; and the IT labor required to manage and troubleshoot backup systems.

Chapter 4 : Cloud, Implementation, Programming and Mobile Cloud Computing

Q. 1 Explain conceptual Architecture of OpenStack. Dec. 15

Ans. : Architecture of OpenStack

In the field of cloud computing, OpenStack is a free and open-source software platform which is mainly deployed as IaaS (infrastructure-as-a-service) in which virtual servers and various important resources are made available to customers. Interrelated components are available in this system. These components are used to control various hardware pools regarding processing, storage, and networking based resources across a data center. For handling this, there are different options for users like using web-based dashboard, via command-line tools, or with the help of

RESTful web services. OpenStack is a set of software tools for building and managing cloud computing platforms for public and private clouds. Backed by some of the biggest companies in software development and hosting, as well as thousands of individual community members, many think that OpenStack is the future of cloud computing.

OpenStack is managed by the OpenStack Foundation, a non-profit that oversees both development and community-building around the proje. The cloud is all about providing computing for end users in a remote environment, where the actual software runs as a service on reliable and scalable servers rather than on each end-user's computer. Cloud computing can refer to a lot of different things, but typically the industry talks about running different items "as a service" software, platforms, and infrastructure. OpenStack falls into the latter category and is considered Infrastructure as a Service (IaaS). Providing infrastructure means that OpenStack makes it easy for users to quickly add new instance, upon which other cloud components can run. Typically, the infrastructure then runs a "platform" upon which a developer can create software applications that are delivered to the end users.

OpenStack has a modular architecture with various code names for its components

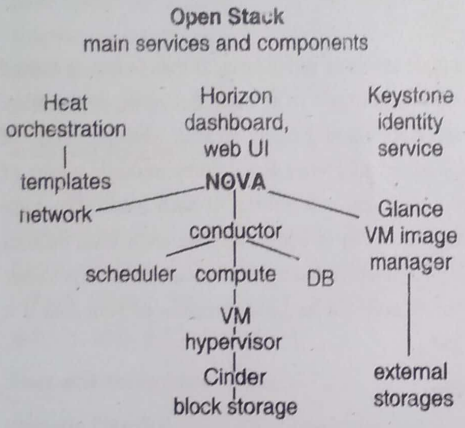


Fig. 4.1 : OpenStack Architecture

Q. 2 Explain the components of OpenStack.

Ans. :

Components of OpenStack

1. OpenStack Compute (Nova)

Nova is the primary computing engine behind OpenStack. It is used for deploying and managing large numbers of virtual machines and other instances to handle computing tasks. In IaaS system, the OpenStack Compute (Nova) is an important part which is a cloud computing fabric controller. Pools of computer resources can be managed and automated by the OpenStack Compute. It can work with advanced virtualization technologies, and also with HPC (high-performance computing). The core language of OpenStack Compute is Python. Number of external libraries are also used like Eventlet (for simultaneous programming), SQLAlchemy (for database access), etc. OpenStack Compute can implement horizontal scaling on standard hardware without the requirement of proprietary hardware or software. It also provides capability to integrate with legacy systems as well various types of third-party technologies.

2. Swift

Swift is a storage system for objects and files. Rather than the traditional idea of a referring to files by their location on a disk drive, developers can instead refer to a unique identifier referring to the file or piece of information and let OpenStack decide where to store this information. This makes scaling easy, as developers don't have the worry about the capacity on a single system behind the software. It also allows the system, rather than the developer, to worry about how best to make sure that data is backed up in case of the failure of a machine or network connection.

3. Cinder

Cinder is a block storage component, which is more analogous to the traditional notion of a computer being able to access specific locations on a disk drive. This more traditional way of accessing files might be important in scenarios in which data access speed is the most important consideration. Persistent block-level storage devices are provided by the OpenStack Block Storage (Cinder) for use with OpenStack compute instances. The management of creation, attaching and detaching of the block devices to servers is done by the block storage system.

Block storage volumes are completely integrated into the system of OpenStack Compute and the Dashboard which allows the users to manage their storage needs. OpenStack provides local Linux server storages as well as some other storage platforms like Ceph, CloudByte, Coraid, and Pure Storage. Block storage is suitable scenarios where performance is an important aspect such as database storage, expandable file systems.

4. Neutron

Neutron provides the networking capability for OpenStack. It helps to ensure that each of the components of an OpenStack deployment can communicate with one another quickly and efficiently.

5. Horizon

Horizon is the dashboard behind OpenStack. It is the only graphical interface to OpenStack, so for users wanting to give OpenStack a try, this may be the first component they actually "see." Developers can access all of the components of OpenStack individually through an application programming interface (API), but the dashboard provides system administrators a look at what is going on in the cloud, and to manage it as needed.

6. Keystone

Keystone provides identity services for OpenStack. It is essentially a central list of all of the users of the OpenStack cloud, mapped against all of the services provided by the cloud, which they have permission to use. It provides multiple means of access, meaning developers can easily map their existing user access methods against Keystone.

7. Glance

Glance provides image services to OpenStack. In this cas "images" refers to images (or virtual copies) of hard disks. Glance allows these images to be used as templates when deploying new virtual machine instances.

8. Ceilometer

Ceilometer provides telemetry services, which allow the cloud to provide billing services to individual users of the cloud. It also keeps a verifiable count of each user's system usage of each of the various components of an OpenStack cloud. Think metering and usage reporting.

9. Heat

Heat is the orchestration component of OpenStack, which allows developers to store the requirements of a cloud application in a file that defines what resources are necessary for that application.

Q. 3 What are the features of OpenStack?

Ans. :

Features of OpenStack

1. Compatibility and Portability

Besides its open source nature, OpenStack provides several advantages for cloud users. For new users, OpenStack is agile as well as easy to deploy; it has support for both private and public clouds, but usually organizations choose it to build the former. OpenStack APIs are compatible with AWS (Amazon Web Services), hence there is no need for users to rewrite applications for AWS. This compatibility also helps applications and storage to shift from private clouds to public cloud providers or vice versa.

2. Security

One of the major bottlenecks for cloud adoption is that whosoever the service provider is, the security concerns are always there. To calm those worries of organizations, OpenStack provides a robust security system which has support for multiple forms of identification.

3. Management and Visibility

Horizon dashboard of the open source cloud provides administrators an overview regarding their cloud environment containing resources as well as instance pools.

4. Cloud Storage

OpenStack provides unrestricted number of storage pools and supports block-IO from different vendors, as well as object file storage.

Its built-in storage management automatically recovers failed drives or nodes. Replication and erasure coding with Ceph provides strong data integrity. To avoid the effects of drive failures, users can take advantage of pre-emptive drive checking. Additionally, OpenStack's scaling capabilities enable users to add servers and storage elastically. As the necessity to handle big data in the cloud rises, flexibility of OpenStack is considered as an added bonus. Users have option to execute Hadoop apps and Web pages for the purpose of big data analytics, media files and standard block-IO.

5. Quality Control

Since code base of OpenStack is evolving, its release process is broken down into blocks approximately 4 to 6 months apart. This guarantees quality control and release stabilization.

6. Piecing together the OpenStack Services Puzzle

Just like a complex puzzle, OpenStack has several modular pieces which fit together. Each module developed independently and OpenStack allows the community to introduce new code modules, as per necessity. In the beginning, OpenStack offered Nova for compute, Glance for images and Swift for object storage. However, nowadays the replacement of Swift is done by Ceph to a great extent which is an outside open source unified storage stack.

Q. 4 Explain modes of operation of Open Stack.

Dec. 15

Ans. : Multi-Host and Single-Host Networking

The nova-network service has the ability to operate in a multi-host or single-host mode. Multi-host is when each compute node runs a copy of nova-network and the instances on that compute node use the compute node as a gateway to the Internet. The compute nodes also host the floating IPs and security groups for instances on that node.

Single-host is when a central server-for example, the cloud controller runs the nova-network service. All compute nodes forward traffic from the instances to the cloud controller. The cloud controller then forwards traffic to the Internet. The cloud controller hosts the floating IPs and security groups for all instances on all compute nodes in the cloud. There are benefits to both modes.

Single-node has the downside of a single point of failure. If the cloud controller is not available, instances cannot communicate on the network. This is not true with multi-host, but multi-host requires that each compute node has a public IP address to communicate on the Internet. If you are not able to obtain a significant block of public IP addresses, multi-host might not be an option.

Q. 5 Write a note on Google app engine. Dec. 15

Ans. :

Google App Engine

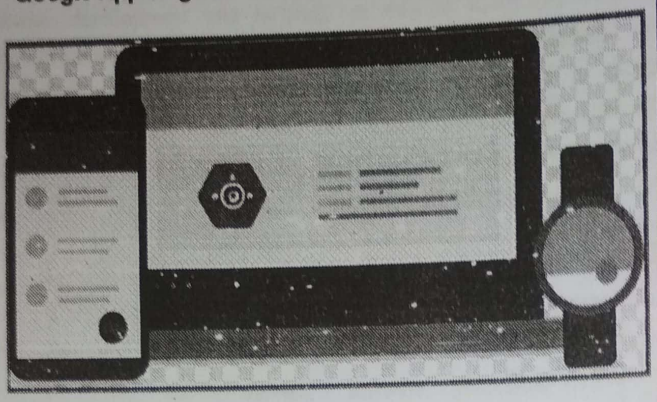


Fig. 4.2 : Google App engine

Google App engine is also called as GAE or just App. Engine. It is considered as framework of web and cloud computing platform used to develop and host various types of web applications in Google-managed data centers. These applications are executed on multiple servers.

For an application if number of requests increases, automatic scaling is provided by the App Engine. For such web applications, to handle increasing demand more resources are allocated by the App Engine automatically.

For certain level, Google App Engine provides free usage of resources. Afterwards, fees are applied for additional storage, bandwidth, or any other resources essential to the application.

Google App Engine is released in April 2008 as a preview version and as final in September 2011.

GAE supports the following major features

GAE allows to run web applications on Google's infrastructure. Dynamic Web services based on common standards. Easy to build. Automatic scaling as well as load balancing. Easy to maintain. Authentication is provided with the help of Google's Accounts API. Easy to scale when there is increase in traffic and storage needs. Persistent storage, with features like query access sorting and transaction management. Task queues and task scheduling. A client-side development environment is provided for the purpose of simulating GAE on local system.

Java

App Engine executes the JAVA based apps on a JAVA 7 virtual machine.

JAVA Servlet standards are used for the web applications :

1. WAR (Web Applications ARchive) directory structure.
2. Servlet classes.
3. Java Server Pages (JSP).
4. Static and data files.
5. Deployment descriptor (web.xml)
6. Other configuration files.

Python

Uses WSGI (Web Server Gateway Interface) standard.

Python applications can be written using :

1. Webapp2 framework
2. Django framewo...
3. Any python code that uses the CGI (Common Gateway Interface) standard.

PHP (Experimental support)

Local development servers are available to anyone for developing and testing local applications. Only white-listed applications can be deployed on Google App Engine.

Through Google App Engine, programming support is given by Google to cloud environment with the help of multiple technology solutions :

1. Google File System (GFS)
2. Big Table
3. Chubby

Q. 6 Write a note on GFS. May 17

Ans. :

Google File System

Google File System (GFS) is developed by Google Inc. to hold Google's increasing data processing requirements. The Google File System is considered as one of the scalable distributed file system (DFS). Google File System is improved to hold the data used by Google and their requirement of storage, like search engine, which produce a large amounts of data that needs to be stored.GFS is also called as GoogleFS. The main purpose behind the design of GFS is to hold the Google's huge cluster requirements without making extra load on applications. In GFS files can be stored in hierarchical directories which can be identified with the help of path names.

It contains the Metadata - such as namespace, access control data, and mapping information and is handled by the master, which communicates with and examines the status updates of each chunk server through timed heartbeat messages.

GFS has following features :

1. Fault Tolerance
2. Critical Data Replication
3. Automatic and efficient data recovery
4. High aggregate throughput

5. Reduced client and master interaction because of large chunk server size
6. Namespace management and locking
7. High availability

Q. 7 Explain architecture of Google File System.

May-18

Ans. :

Architecture of Google File System

The Google File System is structured into clusters of computers. A cluster is nothing but network of different computers. Every cluster contains many computers connected to each other such as it may be hundreds or thousands of computers.

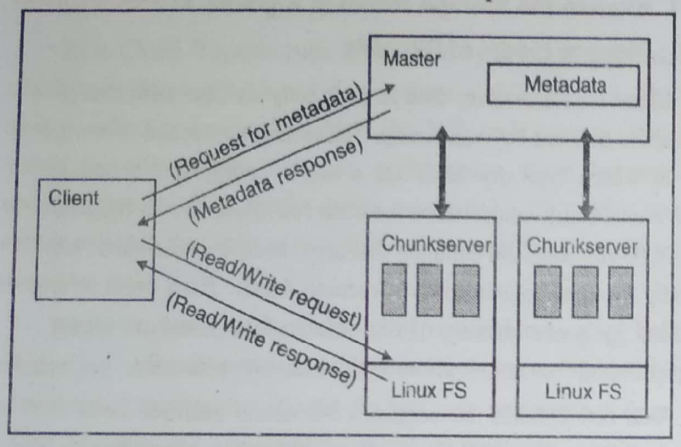


Fig. 4.3 : Google File System Architecture

The Google File System clusters contain three kinds of entities they are as follow :

1. Clients

The term "client" may be any entity which requests a file. Requests can vary from accessing and changing the existing files to creating new files on the system. The Clients may be computers or any computer applications. You can consider clients as the customers of the Google File System.

2. Master Servers

The master server is the main server and it behaves as the controller for the cluster. The job of master servers is to maintain an **operation log**, which keeps track of the activities of the master's cluster. The operation log helps out to keep service disturbance to least - for example if the master server crashes, a replacement server that has monitored the operation log can take its place. Another job of master server is to keep the track of **metadata**, which is nothing but the information that illustrates chunks. The metadata inform the master server that chunks belongs to which files and in the whole file where it should be placed. In the startup, the master **intimates** all the chunk servers present in its cluster. The available chunk servers give response to master server which contains the contents of their inventories. From this point, the master server starts keeping the track of the location of chunks resides in the cluster.

There is only one master server active at a time per cluster. This is very effective because managing thousands of computers by a single server resolves the problem of traffic jam. The master server is not responsible to handle the file data. It can be handled by the chunk servers.

3. Chunk Servers

Chunk servers are the main component of the GFS. Chunk servers are capable of storing the 64-MB file chunks. It sends the requested chunks to the clients rather than sending it to the master server.

The Google File System can copy every chunk several times and it can be stored on different chunk servers. Each copy of chunk is called a **replica**. Minimum three copies of each chunk can be created by the GFS by default, but users can also make more or fewer copies of the chunk if they needs.

Q. 8 What are the features of Google file system?

May-16

Ans. :

Features of Google File System

1. GFS provides the high availability and fault tolerance making use of replication.
2. The GFS have simple and well-organized centralized design with a single master. It delivers good performance for what it was designed i.e. large sequential reads.
3. Simultaneous writes to the same file region are not serializable. Thus replicas might have duplicates but there is no interleaving of records. To make sure data integrity each chunk server confirms integrity of its own copy using checksums.
4. Atomic append operations make sure that there is no need of synchronization at client end.
5. No caching removes cache coherence issues.
6. Decoupling of flow of data from flow of control allows you to use network efficiently.
7. Parentless chunks are automatically collected using garbage collection.
8. GFS master continuously supervise each chunk server with the help of heartbeat messages.

Q. 9 What are the disadvantages of GFS? (3 Marks)

Ans. : Disadvantages of GFS

1. Master memory is one of the limitations.
2. If the garbage is not collected quickly then it can become a problem where the files are dynamic. When there is several deletion operations are performed but not reclaimed the

storage used by them then it might become a problem for new file creations.

3. Small files can contain the small number of chunks; sometime as small as one chunk. This can lead to chunk servers storing these files to become hotspots in case of several client requests.
4. When the numbers of writers are increased then performance will be slow down.

Q. 10 Explain Big Table as Google's NoSQL system in details **Dec. 15**

Ans. : Bigtable

Cloud Bigtable is a sparsely populated table that can scale to billions of rows and thousands of columns, enabling user to store terabytes or even petabytes of data. A single value in each row is indexed; this value is known as the row key. Cloud Bigtable is ideal for storing very large amounts of single-keyed data with very low latency. It supports high read and write throughput at low latency, and it is an ideal data source for MapReduce operations. Cloud Bigtable is exposed to applications through multiple client libraries, including a supported extension to the Apache HBase library for Java. As a result, it integrates with the existing Apache ecosystem of open-source Big Data software.

Cloud Bigtable's powerful back-end servers offer several key advantages over a self-managed HBase installation :

1. **Incredible Scalability :** Cloud Bigtable scales in direct proportion to the number of machines in the cluster. A self-managed HBase installation has a design bottleneck that limits the performance after a certain QPS (Queries per second) is reached. Cloud Bigtable does not have this bottleneck, and so user can scale the cluster up to handle more queries.
2. **Simple Administration :** Cloud Bigtable handles upgrades and restarts transparently, and it automatically maintains high data durability. To replicate the data, simply add a second cluster to the instance, and replication starts automatically. No more managing masters or regions; user has to just design table schemas, and Cloud Bigtable will handle the rest for user.
3. **Cluster resizing without downtime :** User can increase the size of a Cloud Bigtable cluster for few hours to handle a large load, then reduce the cluster's size again, all without any downtime. After user changes a cluster's size, it typically takes just a few minutes under load for Cloud Bigtable to balance performance across all of the nodes in the cluster.

Cloud Bigtable is ideal for applications that need very high throughput and scalability for non-structured key/value data, where each value is typically no larger than 10 MB. Cloud Bigtable also excels as a storage engine for batch MapReduce operations, stream processing/analytics, and machine-learning applications.

User can use Cloud Bigtable to store and query all of the following types of data :

1. Time-series data, such as CPU and memory usage over time for multiple servers.
2. Marketing data, such as purchase histories and customer preferences.
3. Financial data, such as transaction histories, stock prices, and currency exchange rates.

Internet of Things data, such as usage reports from energy meters and home appliances.

Graph data, such as information about how users are connected to one another.

Q. 11 Explain the Storage Model of Bigtable.

Ans. : Storage model of Bigtable

Cloud Bigtable stores data in massively scalable tables, each of which is a sorted key/value map. The table is composed of *rows*, each of which typically describes a single entity, and *columns*, which contain individual values for each row. Each row is indexed by a single *row key*, and columns that are related to one another are typically grouped together into a *column family*. Each column is identified by a combination of the column family and a *column qualifier*, which is a unique name within the column family.

Each row/column intersection can contain multiple *cells* at different timestamps, providing a record of how the stored data has been altered over time. Cloud Bigtable tables are sparse; if a cell does not contain any data, it does not take up any space. For example, suppose user is building a social network for United States presidents let's call it Prezzy. Each president can follow posts from other presidents.

The Fig. 4.4 shows a Cloud Bigtable table that tracks who each president is following on Prezzy :

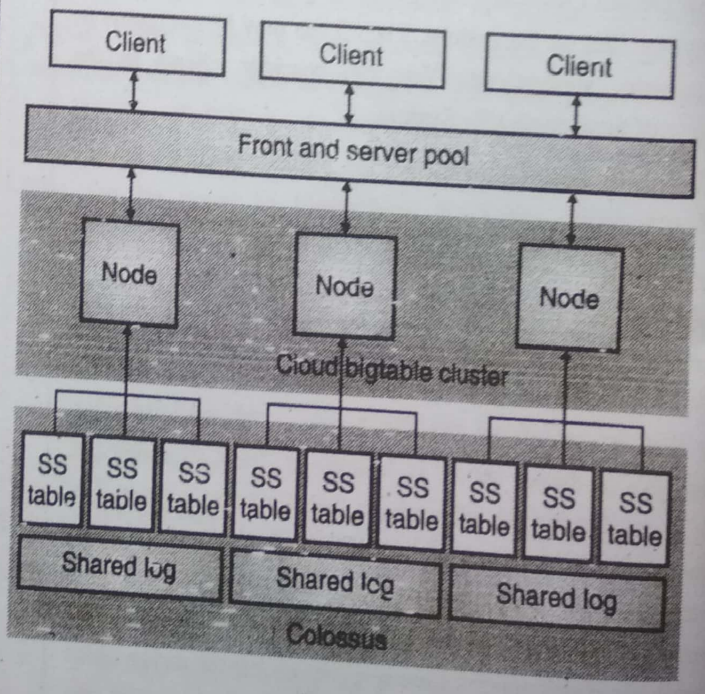


Fig. 4.4

A few things to notice in this illustration :

The table contains one column family, the follows family. This family contains multiple column qualifiers.

Column qualifiers are used as data. This design choice takes advantage of the sparseness of Cloud Bigtable tables, and the fact that new column qualifiers can be added on the fly.

The username is used as the row key. Assuming usernames are evenly spread across the alphabet, data access will be reasonably uniform across the entire table.

Q. 12 Write a note on Load Balancing in Bigtable.

Ans. :

Load Balancing

Each Cloud Bigtable zone is managed by a master process, which balances workload and data volume within clusters. The master splits busier/larger tablets in half and merges less-accessed/smaller tablets together, redistributing them between nodes as needed. If a certain tablet gets a spike of traffic, the master will split the tablet in two, then move one of the new tablets to another node.

Cloud Bigtable manages all of the splitting, merging, and rebalancing automatically, saving users the effort of manually administering their tablets. To get the best write performance from Cloud Bigtable, it's important to distribute writes as evenly as possible across nodes. One way to achieve this goal is by using row keys that do not follow a predictable order. For example, usernames tend to be distributed more or less evenly throughout the alphabet, so including a username at the start of the row key will tend to distribute writes evenly.

At the same time, it's useful to group related rows so they are adjacent to one another, which makes it much more efficient to read several rows at the same time. For example, if user is storing different types of weather data over time, his/her row key might be the location where the data was collected, followed by a timestamp

(for example, WashingtonDC#201803061617).

This type of row key would group all of the data from one location into a contiguous range of rows. For other locations, the row would start with a different identifier; with many locations collecting data at the same rate, writes would still be spread evenly across tablets.

Supported data types

Cloud Bigtable treats all data as raw byte strings for most purposes. The only time Cloud Bigtable tries to determine the type is for increment operations, where the target must be a 64-bit integer encoded as an 8-byte big-endian value.

Empty cells

Empty cells in a Cloud Bigtable table do not take up any space. Each row is essentially a collection of key/value entries, where the key is a combination of the column family, column qualifier and timestamp. If a row does not include a value for a specific key, the key/value entry is simply not present.

Column qualifiers

Column qualifiers take up space in a row, since each column qualifier used in a row is stored in that row. As a result, it is often efficient to use column qualifiers as data.

Compactions

Cloud Bigtable periodically rewrites user's tables to remove deleted entries, and to reorganize user's data so that reads and writes are more efficient. This process is known as a *compaction*. There are no configuration settings for compactions Cloud Bigtable compacts the data automatically.

Mutations and deletions

Mutations, or changes, to a row take up extra storage space, because Cloud Bigtable stores mutations sequentially and compacts them only periodically. When Cloud Bigtable compacts a table, it removes values that are no longer needed. If user updates the value in a cell, both the original value and the new value will be stored on disk for some amount of time until the data is compacted.

Data compression

Cloud Bigtable compresses user's data automatically using an intelligent algorithm. User cannot configure compression settings for his/her table. However, it is useful to know how to store data so that it can be compressed efficiently :

Random data cannot be compressed as efficiently as patterned data. Patterned data includes text

Compression works best if identical values are near to each other, either in the same row or in adjoining rows. If user arranges the row keys so that rows with identical chunks of data are next to each other, the data can be compressed efficiently.

Data durability

When user uses Cloud Bigtable, the data is stored on Colossus, Google's internal, highly durable file system, using storage devices in Google's data centers. User does not need to run an HDFS cluster or any other file system to use Cloud Bigtable.

If user's instance uses replication, Cloud Bigtable maintains two copies of the data in Colossus, with each copy located in a different zone, further improving durability. Behind the scenes, Google uses proprietary storage methods to achieve data durability above and beyond what's provided by standard HDFS three-way replication. In addition, it creates backups of user's data to protect against catastrophic events and provide for disaster recovery.

Security

Access to user's Cloud Bigtable tables is controlled by his/her Google Cloud Platform project and the Cloud Identity and

Access Management roles that user assign to end-users. For example, user can assign Cloud IAM roles that prevent individual users from reading from tables, writing to tables, or creating new instances. If someone does not have access to the project or does not have a Cloud IAM role with appropriate permissions for Cloud Bigtable, they cannot access any of the tables. User can manage security at the project level and instance level. Cloud Bigtable does not support table-level, row-level, column-level, or cell-level security restrictions.

Q. 13 Write a note on Advantages of BigTable. May 18

Ans. :

Advantages of BigTable

1. High availability over multiple clusters.
2. High performance in data storage, retrieval and processing
3. Provides consistency, reliability and scalability over highly distributed/networked systems.
4. Supports dynamic control over data layout and format.
5. Allows clients to reason about the locality properties of the data represented in the underlying storage.
6. Supports both structured and semi-structured data.
7. Its schema parameters let clients to dynamically control whether to serve data out of memory or from disk.

Q. 14 Write a note on Chubby.

Ans. : Chubby

Chubby is a distributed lock service. The main functionality of Chubby is the coarse-grained synchronization of various types of activities within distributed systems. Now a day Chubby is considered as primary internal name service of Google. For system like MapReduce, chubby is commonly used mechanism. The storage systems like Google File System and Bigtable takes help of Chubby to elect a primary from redundant replicas; and it is also considered as a standard repository for the files which needs high availability, just like access control lists. The primary goals of Chubby included reliability, availability to a moderately large set of clients, and throughput and storage capacity were considered secondary.

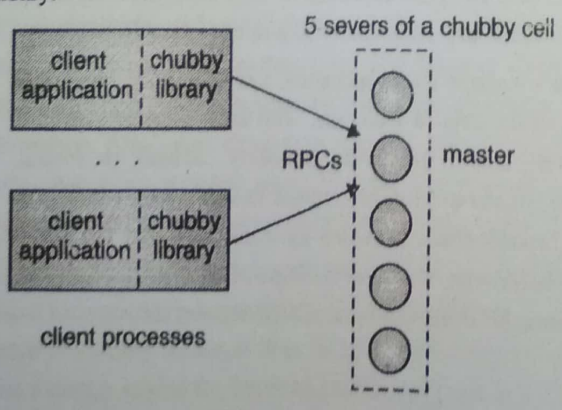


Fig. 4.5 : System Structure of Chubby

Chubby has two main components that communicate via RPC : a server, and a library that client applications link against. All communication between Chubby clients and the servers is mediated by the client library. An optional third component, a proxy server may there. A Chubby cell consists of a small set of servers (typically five) known as replicas, placed so as to reduce the likelihood of correlated failure (for example, in different racks).

The replicas use a distributed consensus protocol to elect a master; the master must obtain votes from a majority of the replicas, plus promises that those replicas will not elect a different master for an interval of a few seconds known as the master lease. The master lease is periodically renewed by the replicas provided the master continues to win a majority of the vote.

The replicas maintain copies of a simple database, but only the master initiates reads and writes of this database. All other replicas simply copy updates from the master, sent using the consensus protocol. Clients find the master by sending master location requests to the replicas listed in the DNS. Non-master replicas respond to such requests by returning the identity of the master. Once a client has located the master, the client directs all requests to it either until it ceases to respond, or until it indicates that it is no longer the master.

Write requests are propagated via the consensus protocol to all replicas; such requests are acknowledged when the write has reached a majority of the replicas in the cell. Read requests are satisfied by the master alone; this is safe provided the master lease has not expired, as no other master can possibly exist. If a master fails, the other replicas run the election protocol when their master leases expire; a new master will typically be elected in a few seconds.

If a replica fails and does not recover for a few hours, a simple replacement system selects a fresh machine from a free pool and starts the lock server binary on it. It then updates the DNS tables, replacing the IP address of the failed replica with that of the new one. The current master polls the DNS periodically and eventually notices the change. It then updates the list of the cell's members in the cell's database; this list is kept consistent across all the members via the normal replication protocol. In the meantime, the new replica obtains a recent copy of the database from a combination of backups stored on file servers and updates from active replicas.

Once the new replica has processed a request that the current master is waiting to commit, the replica is permitted to vote in the elections for new master. Files, directories, and handles Chubby exports a file system interface similar to, but simpler than that of UNIX. It consists of a strict tree of files and directories in the usual way, with named components separated by slashes.

Locks and sequencers

Each Chubby file and directory can act as a reader-writer lock : either one client handle may hold the lock in exclusive (writer)

mode, or several client handles may hold the lock in shared (reader) mode. Like the mutexes known to most programmers, locks are advisory. That is, they conflict only with other attempts to acquire the same lock : holding a lock called F neither is necessary to access the file F, nor prevents other clients from doing so.

Events

Chubby clients may subscribe to a range of events when they create a handle. These events are delivered to the client asynchronously via an up-call from the Chubby library.

Events include :

1. File contents modified - Often used to monitor the location of a service advertised via the file.
2. Child node added, removed, or modified - Used to implement mirroring.
3. Chubby master failed over - Warns clients that other events may have been lost, so data must be rescanned.
4. A handle (and its lock) has become invalid - This typically suggests a communications problem.
5. Lock acquired - Can be used to determine when a primary has been elected.
6. Conflicting lock request from another client - Allows the caching of locks.

Q. 15 Write a note on Google API.

Ans. :

Google API

Google APIs is a set of application programming interfaces (APIs) developed by Google which allow communication with Google Services and their integration to other services. Examples of these include Search, Gmail, Translate or Google Maps. Third-party apps can use these APIs to take advantage of or extend the functionality of the existing services. The APIs provide functionality like analytics, machine learning as a service (the Prediction API) or access to user data (when permission to read the data is given). Another important example is an embedded Google map on a website, which can be achieved using the Static maps API, Places API or Google Earth API.

Authentication and authorization

Usage of some of the APIs requires authentication and authorization using the OAuth 2.0 protocol. OAuth 2.0 is a simple protocol. To start, it is necessary to obtain credentials from the Developers Console. Then the client app can request an access token from the Google Authorization Server, and uses that token for authorization when accessing a Google API service sastha velan.

Client libraries

There are client libraries in various languages which allow developers to use Google APIs from within their code, including Java, JavaScript, .NET, Objective-C, PHP and Python. The Google Loader is a JavaScript library which allows web developers to easily load other JavaScript APIs provided by Google and other developers of popular libraries. Google Loader provides a JavaScript method for loading a specific API (also called module), in which additional settings can be specified such as API version, language, location, selected packages, load callback and other parameters specific to a particular API. Dynamic loading or auto-loading is also supported to enhance the performance of the application using the loaded APIs

Google Apps Script

Google Apps Script is a cloud-based JavaScript platform which allows developers to write scripts that can manipulate API services such as Calendar, Docs, Drive, Gmail, and Sheets and easily create Add-Ons for these services with chromium based applications.

Q. 16 Write a note on Mobile cloud computing.

May 16, Dec. 17

Ans. :

Mobile Cloud Computing

There are two interrelated statements :

1. The cloud is going to drive mobile applications.
2. Mobile applications will drive the growth of the cloud.

In future, there will be explosive growth of Cloud-based mobile applications.

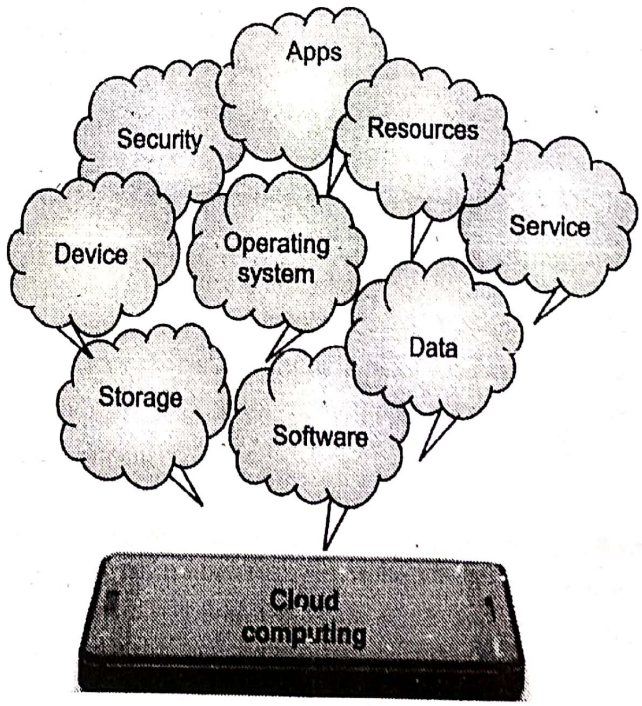


Fig. 4.6 : Cloud and Mobile

Mobile Cloud Computing (MCC) is the combination of cloud computing, mobile computing and wireless networks to bring rich computational resources to mobile users, network operators, as well as cloud computing providers. The ultimate goal of MCC is to enable execution of rich mobile applications on a plethora of mobile devices, with a rich user experience. MCC provides business opportunities for mobile network operators as well as cloud providers.

More comprehensively, MCC can be defined as "a rich mobile computing technology that leverages unified elastic resources of varied clouds and network technologies toward unrestricted functionality, storage, and mobility to serve a multitude of mobile devices anywhere, anytime through the channel of Ethernet or Internet regardless of heterogeneous environments and platforms based on the pay-as-you-u principle".

Q. 17 Explain architecture of Mobile Cloud Computing

Ans. :

Architecture of Mobile Cloud Computing

MCC uses computational augmentation approach (computations are executed remotely instead of on the device) which resource-constraint mobile devices can utilize computation resources of varied cloud-based resources. In MCC, there are fo types of cloud-based resources, namely distant immobile cloud proximate immobile computing entities, proximate mobi computing entities, and hybrid (combination of the other thr model).

Giant clouds such as Amazon EC2 are in the distant immobile groups whereas cloudlet or surrogates are members of proxima immobile computing entities. Smartphones, tablets, handheld devices, and wearable computing devices are part of the third group cloud-based resources which are proximate mobile computing entities.

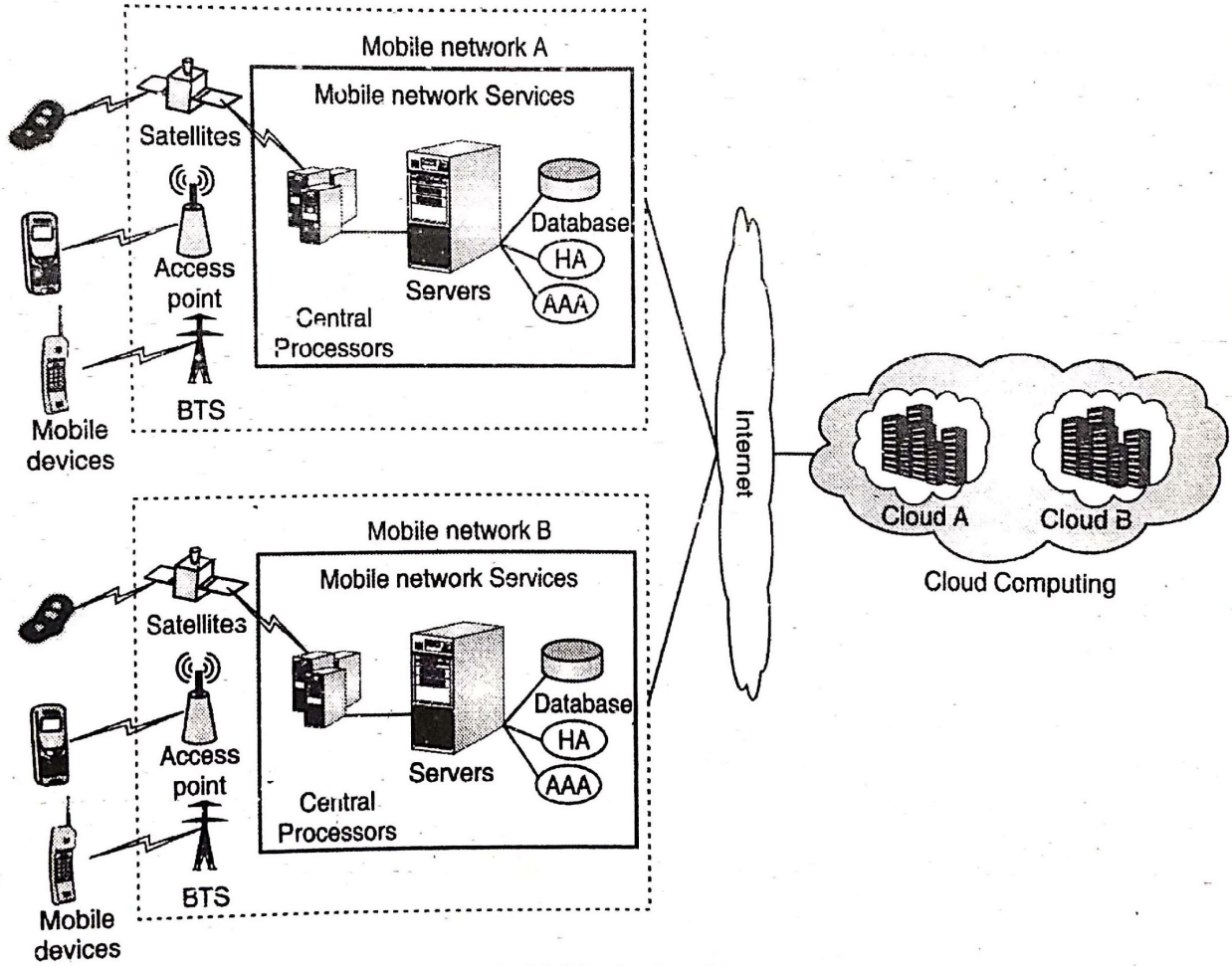


Fig. 4.7 : Mobile cloud architecture

Mobile devices connect to network services through any satellite, access point or BTS (base transceiver station (BTS) which pas request to server providing services. Server provides services like AAA (Authentication, Authorization, and Accounting) based on HA HA is a home agent that works as a router on a mobile devices' home network that maintains information about the device's current location. The home agent uses mechanisms to forward Internet traffic so that the device's IP address do not have to be change every time it connects from a different location. That mechanism is known as tunneling. Any data or request is submitted on database. This all processing is still on mobile network itself. Request by user is then passed to cloud through internet. Cloud controller process the request to provide required data to user.

Q. 18 Explain benefits of Mobile Cloud Computing.

Ans. :

Benefits of Mobile Cloud Computing

1. **Flexibility**

   Mobile cloud computing allows accessing data from anywhere in the world. As long as you are connected to the internet, you can access the application and mobile data from any mobile device.

2. **Multiple Platform Support**

   Mobile cloud computing offers multiple platform support. You can easily access applications stored in the cloud, regardless of the platform.

3. **Cost-Efficient**

   Cloud computing is one of the most cost-efficient methods to be used and maintained. Mobile cloud computing has a minimal upfront cost depending on the usage. Also, there are no hefty fees charged for licensing and upgrades.

4. **Real-Time Data Availability**

   You can go real-time with the mobile cloud computing. Since all your data is managed externally, you can access and update your data in real-time on your mobile device. Documents can also be simultaneously managed by multiple persons.

5. **Backup and Recovery**

   Data backup and restoring is much easier when all your data is stored in the cloud. Cloud disaster recovery is a strategy that involves storing and maintaining copies of digital records in a cloud computing environment as a security measure.

Q. 19 What are challenges regarding Mobile Cloud Computing?

Ans. :

A. Challenges Regarding Mobile Communication

1. **Low Bandwidth Problem :** In communication network, bandwidth is considered as the most important aspect as the radio resource regarding the wireless networks are transmitted over networks based on the available bandwidth for transferring the content in the network.

2. **Lack of Resource of Mobile Devices :** When mobile device is compared with desktop PC, it can be observed that how the cost feature of mobility is being achieved. Because of lack of resources, it becomes difficult to adopt mobile cloud computing in usual conditions.

B. Challenges of Network

1) **Challenges of Wireless Network and Access Control Policies**

Wireless network is considered as the base for implementing the cloud computing which has its own intrinsic nature and constraints. Consistent network bandwidth is very important for getting better performance. Besides it, variable data rates, longer latency and connectivity with gaps in coverage are considered as the major issues associated with network in the MCC. Few factors which are beyond control are also responsible such as weather for varying bandwidth capacity and coverage.

2) **Seamless Connection Handover**

The running application may terminate or it show error message if one shifts from one access point of network to another point or from Wi-Fi network to 4G-based cellular network. This is because the shifting leads to the situation of communication failure and connection reestablishment.

C. Challenges Related To Mobile Applications

1. **Interoperability :** There are number of mobile devices which are running on different platforms such has iPhone, Android phones, BlackBerry, etc.

   Such devices with different platforms are used by employees in the same enterprise or a group of people who are sharing single network.

   In this case interoperability issue will be a major challenge in transmitting data across multiple devices.

2. **Mobile Cloud Convergence :** Data distribution is considered as significant aspect for achieving benefit of mobility by making incorporation of cloud computing with mobile world. For using the application of cloud computing services with mobile devices, there are some problems with computation of data, battery life as well as performance of these devices in distributed platform.

D. Challenges Regarding Security

1. **Information Security Devices Privacy**

Cloud computing provides all types of services, data storage and processing. These things are implemented remotely, because of which security becomes an important concern for all the stakeholders. In Mobile Cloud Computing it is essential to check the security regarding the mobile devices along with cloud computing platform, which is considered as a key concern in this area. This is because if in case the device (mobile) get stolen or misplaced, it will lead to crucial data to be compromised.

2. **Security Attacks and Hacking**

All the networking activates are considered as vulnerable to one or more types of malicious attacks. As there is possibility of browsing malicious code web sites, security is in concern.

Chapter 5 : Exploring the Components of Amazon Web Services

Q. 1 Write a note on Amazon Web Services. May 18

Ans. :

Amazon web services

Amazon.com has provided a subsidiary known as **Amazon Web Services (AWS).** AWS provides cloud computing platforms for various elements like individuals, companies and governments on demand basis. AWS gives a free trial option for one year. AWS has a full-fledged virtual cluster of computers which it makes available to subscribers via internet. The virtual computers of AWS provide most of the features of real computers such as hardware, software (OS, web servers, databases, CRM etc) and networking.

Console I/O (keyboard, display, and mouse) is also virtualized by the AWS which lets the subscribers to have connection with AWS system with the help of a modern browser. In virtual computer, the browser can be considered as a window which helps subscribers to login, configure and utilize the virtual systems just like real physical computers. The subscribers can provide internet-based services to their customers using AWS system. The charges are depending upon the various elements like usage, hardware, Operating System, software, features regarding networking.

There are various options for subscribers as per their need like only one virtual computer or a cluster of VMs. It is responsibility of Amazon to manage and upgrade the system as well as provide industry-standard security. Since 2016 Amazon provides 70 services including computing, storage, networking, database, analytics, application services, deployment, management, mobile, developer tools, and tools for the Internet of Things. EC2 (Amazon Elastic Compute Cloud) and S3 (Amazon Simple Storage Service) are the two most popular services.

Most of the AWS services are not directly exposed to the subscribers; rather their functionality is made available with the help of various APIs. The AWS services are accessed over HTTP, by means of the REST architectural style and SOAP (Simple Object Access Protocol) protocol. The basic aim of Amazon to build AWS is that users should get large scale computing capacity in a quick and cost effective manner as compare to building an actual physical server farm. Virtual machines can share the computing resources safely and flexibly. The IaaS model of cloud is adopted by Amazon for the purpose of providing public cloud services.

Fig. 5.1 illustrates the AWS architecture.

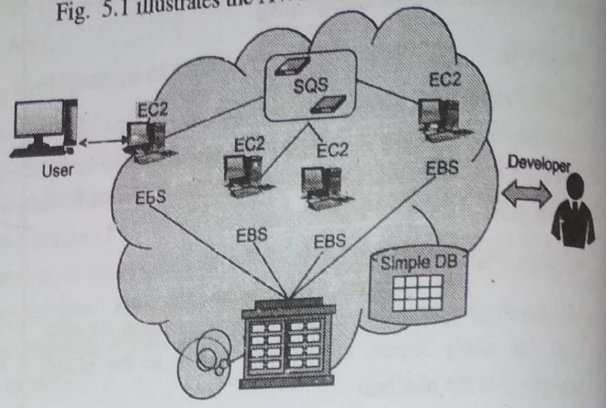


Fig. 5.1 : AWS Architecture

EC2 (Amazon Elastic Compute Cloud) provides virtualized platforms for the host Virtual Machines where the cloud application can be executed. Simple Storage Service (S3) provides the storage service which is OOP based for users. Block storage interface is provided by the Elastic Block Service (EBS), which supports the traditional applications. SQS (Simple Queue Service) is used to guarantee a reliable message service in between two different processes. It is possible to keep the message reliably even if the execution of processes is stopped. The objects can be retrieved by the user with the help of SOAP by using browsers or applications which support the SOAP standards.

Queuing and notification services like SQS and SNS are also provided by Amazon. These services are implemented in the AWS cloud. In cloud, the brokering systems are generally executed in efficient manner which provides office support of smart-phones and tablets. For development of cloud applications, Amazon provides more flexible cloud computing platform. Amazon cloud provides platform for small and medium-size companies. Through AWS these companies can provide service to large numbers of Internet users and also can generate revenue through those paid services.

The incoming application traffic is automatically distributed by the EJB across multiple Amazon EC2 instances. It helps user to avoid the nodes which are currently non-operating and equalize load on functioning images. CloudWatch enables the autoscaling as well as ELB to monitor the running instances. CloudWatch is a web service which is used to monitor AWS cloud resources. CloudWatch helps user to improve resource utilization and overall performance of operation with demand patterns. It also enable user to concentrate on CPU utilization, disk reads / writes and most importantly the network traffic.

A RDS (Relational Database Service) is provided by Amazon with messaging interface. The capability of Elastic MapReduce is same as of the Hadoop running on the basic EC2 offering. It is possible to transfer large volumes of data to and from EC2 with the

help of shipping of physical disks by the AWS Import/Export. A content distribution network is implemented by the Amazon CloudFront. Amazon provides an easy billing and account management service known as Amazon DevPay. This service helps user to sell the applications which are built and executed on the top of AWS.

For payment by customers, Amazon provides commercial system known as FPS (Flexible Payments Service) which gives an easy payment gateway. The customer information which is already available on Amazon like login credentials, address for shipping, and payment ways, can be used by the customers for payment of services. Amazon provides another service known as FWS to access fulfilment capabilities of Amazon using a simple web service interface. On behalf of customer, merchants can send order information to Amazon.

Q. 2 Write a note on EC2.

Ans. :

EC2

In cloud computing platform of Amazon i.e. AWS, the Amazon Elastic Compute Cloud (EC2) is the main central part. It allows the subscribers to take the VMs on rent to run their own applications. The applications can be deployed in scalable manner with EC2. For this purpose, it provides web services to boot an Amazon Machine Image (AMI) so as to configure a virtual machine. It is called as instance which contains the required software. The server instances can be created, launched as well as terminated as per the requirement. Hence the "elastic" word is included in EC2. The geographical location of instances can be controlled with EC2 which helps in latency optimization and redundancy of high levels. To use EC2 and AWS, a website is launched by Amazon in November 2010.

Q. 3 Explain various features of EC2.

Ans. :

Features of EC2

1. Persistent Storage

a) "Instance-store" disk as a root device

b) Use an EBS volume as a root device.

The first option "Instance-store" is a temporary form of storage. In case of rebooting of an EC2 instance, the data is survived but the stoppage or termination of the instance leads to loss of data. The second option EBS (Amazon Elastic Block Store) gives raw block devices. The Amazon EC2 instances can be attached with these raw block devices. Then these block devices can be utilized as of raw block devices. EBS also supports various types of advanced storage features such as snap-shooting and cloning. The maximum size of EBS volumes is 1TB.

In EBS failure of any single component does not lead to loss of data as the Volumes of EBS are built on replicated storage. Amazon introduces EBS in 2008 publically. The act of EBS volumes is similar to hard drives of a real server. The persistence storage provided by the EBS is independent of the lifetime of the EC2 instance. Amazon's disk arrays back the EBS which appeared as block devices to the OS. Device can be used by the OS as per need. In general the loading of file system is implemented and the volume works as a hard drive. In another use, two or more EBS volumes can be combined to creates RAID arrays which helps to increase the speed and as well as reliability of EBS. The storage volumes in the range of 1GB to 1TB can be set up and managed by the users. Snapshots from a GUI tool or the API are supported by the volumes. From instances, the attachment or detachment of EBS volumes can be done in running mode or when moved from one instance to another.

S3 stands for Simple Storage Service which is a storage system where the data is accessible to EC2 instances, or directly over the network. This communication is done over HTTP. In the same region, there is no charge for communications between EC2 instances and S3 storage. Normal rates are applied when S3 data is accessed in different regions. For linux also S3 file-systems are available. This system mounts a remote S3 file store on an EC2 image just same as of the local storage.

2. Elastic IP addresses

In traditional data centres, there is a feature called as static IP address which resembles with Amazon's elastic IP address feature. The mapping of elastic IP address with any virtual machine instance can be done without the help of network administrator. It indicates that an Elastic IP Address is concerned with the account and not to the instance of virtual machine. It remains unless and until it is not removed explicitly, and also be associated with the account even if there is no instance associated with it.

3. Amazon CloudWatch

Amazon CloudWatch is a web service which is basically designed to provide real-time monitoring service for the customers of Amazon's EC2 on the utilization of various resources like CPU, disk and network. CloudWatch requires additional software on the instance to provide memory, disk space, or load average metrics. Example scripts is provided by the Amazon for Linux instances. The management console of AWS is used to aggregate and provide the data. If customer wants to monitor the EC2 resources with the help of their own enterprise monitoring software, then command line tools and Web API's can be used to access data. The auto-scaling feature is enables by the metrics collected by Amazon CloudWatch which helps to add remove EC2 instances dynamically. The number of monitoring instances is considered for the charges to customer.

4. Automated scaling

This feature of EC2 enables the automatic adaption of computing capacity to site traffic. The two auto scaling mechanisms; schedule-based (e.g. time-of-the-day) and rule-based (e.g. CPU utilization thresholds) are provides feature like simple to use and efficiency. But there is an important problem that VMs may require lot of time to be ready to use. This is problematic when there is a time binding. Image size, VM type, data center locations are factors responsible for VM start-up times.

However, one potential problem is that VMs may take up to several minutes to be ready to use, which are not suitable for time critical applications. The VM start-up times are dependent on image size, VM type, data center locations, etc.

5. Reliability

Availability Zones are engineered by the Amazon to make EC2 more fault-tolerant. The Availability zones have different infrastructures. Higher availability is achieved by the applications which execute on multiple availability zones. The geographical location of instances can be controlled by the uses through EC2. It helps for optimization of latency and high levels of redundancy. For example, downtime can be minimized server instances can be set up in more than one zone which are insulated from each other for most causes of failure such that one backs up the other..

Q. 4 Write a note on Life Cycle of Instances in EC2.

Ans. :

Life cycle of instances in EC2

Fig. 5.2 illustrates the life cycle of Instances in EC2

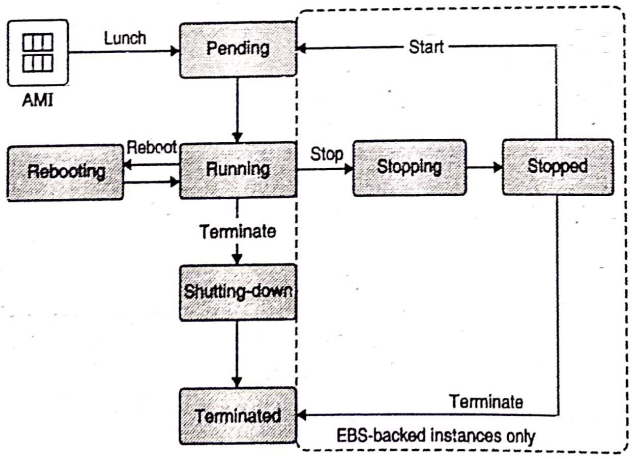


Fig. 5.2 : Life Cycle of Instances

1. **Pending :** The instance is getting ready to enter the running state. An instance is said to be entered in the pending state when it has been launched for the first time, or when it is restarted after being in the stopped state.
2. **Running :** The instance is
3. **Stopping :** The instance is preparing to be stopped or stop-hibernated.
4. **Stopped :** The instance is shut down and it cannot be further used. The instance can be restarted at any time.
5. **Shutting-down :** The instance is preparing to be terminated.
6. **Terminated :** The instance has been permanently deleted and cannot be restarted.

Now we will discuss the actions of instance life cycle :

1. **Instance Launch**

When an instance is launched, it enters the **pending state**. The instance type which has been specified at the time of launching decides the hardware of the host computer for the respective instance.

Here we consider Amazon Machine Image (AMI) specified at launch for the purpose of booting the instance. When the instance is ready to use, it enters the **running state**. Here user can connect to the respective running instance and use it just like a computer placed in front. As soon as the instance enters in the running state, billing get starts.

2. **Instance Stop and Start (Amazon EBS-Backed Instances Only)**

If there is failure in instance status check or the instance is unable to run the applications as expectations, it is possible to stop and start the instance to try to fix the problem. When the instance is stopped, it enters the stopping state, and then the stopped state. When instance is started, it enters the pending state, and most of the times, the instance is shifted to a new host computer. When an instance is stopped and restarted, user loses any data on the instance store volumes of the earlier host computer. The instance retains its private IPv4 or IPv6 address.

3. **Instance Hibernate (Amazon EBS-Backed Instances Only)**

When user hibernate an instance, the OS is signaled to carry hibernation (suspend-to-disk), which copies the data from the instance memory (RAM) to the Amazon EBS root volume. Instance's Amazon EBS root volume and any of the present attached Amazon EBS data volumes are persisted by the system. When instance is restarted, then there is restoring of Amazon EBS root volume to its prior state and reloading of the RAM contents is done.

The reattachment of data volumes is done which were previously attached and the instance retains its instance ID. When instance is hibernated, it enters the stopping state, and then the stopped state. When hibernated instance is restarted, it enters the pending state, and most of the times it is shifted to a new host computer. The instance retains its private IPv4 or IPv6 address.

4. Instance Reboot

It is possible to reboot the instance with the help of the Amazon EC2 console, a command line tool, and the Amazon EC2 API. Amazon EC2 is always recommending rebooting the instance rather than running the OS *reboot* command from the respective instance. Rebooting of an instance is considered as equivalent to rebooting any OS (operating system).

The ... of the ...tance remains same host computer and it preserves its public DNS name, private IP address, and most importantly any data on its instance store volumes. Usually it requires a few minutes for the reboot for completion, but it depends on the instance configuration.

5. Instance Retirement

An instance will be retired if AWS detects that the failure is beyond repair of the underlying hardware which is hosting the instance. When scheduled retirement date of an instance is reached, AWS stop or terminate it. If the instance root device is an Amazon EBS volume, and the instance being used is stopped, it is possible to restart it at any time. But if the respective instance root device is an instance store volume, and the instance being used is stopped, it is not possible to restart it again.

6. Instance Termination

If the instance is no longer required, it can be terminated. If the termination protection is enabled, then it is not possible to terminate the instance through the console, CLI, or API. After termination of an instance, it remains visible in the console for a short period of time, and then the entry of the instance is deleted automatically.

Q. 5 Write a note on Amazon Glacier.

Ans. :

Amazon Glacier

Amazon Glacier is extremely low cost, secure, and durable storage service for data archiving and backup. It is designed to keep the cost low and optimized for the cold data where the retrieval time is 3 to 4 hours. Within Glacier, the user can reliably store the small and large amount of data. In AWS Glacier, there is no limit for the data user stores. Moreover, the data is secure and can be accessed easily.

Amazon Glacier helps to protect the data by redundantly storing it on multiple devices using multiple facilities. AWS Glacier has a Data Integrity Check which regularly monitors the data in the Glacier. It also provides security and fine-grained access to the data of the user with AWS Access Management policies.

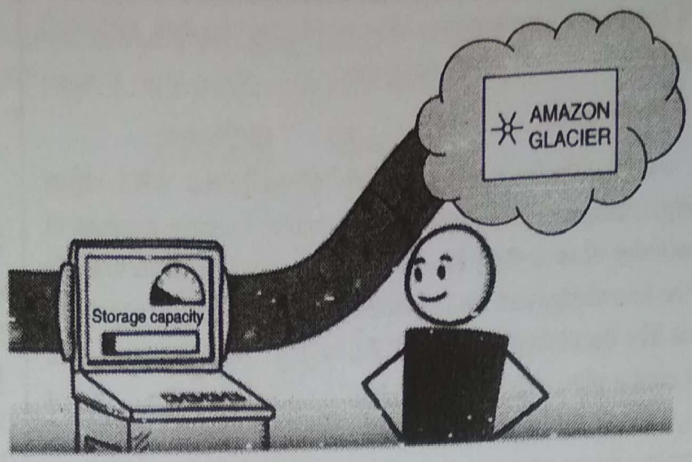


Fig. 5.3 : Amazon Glacier

It automatically encrypts the data at rest with 256-bit advanced encryption standard. The user also gets the benefit of the storage location as he can choose the most suitable location for the regulatory and business criteria. The tools such as SDK which are available to store data and manage AWS also help a lot. Amazon SDK helps to upload the data directly to the Glacier. While using Amazon S3 the user can use Amazon S3 lifecycle policies to automatically load data to Amazon Glacier.

It also helps such that if an industry has a storage facility they can use Amazon import-export to transfer data to AWS Glacier. Third party tools and gateways are also available through which the user can transfer the data to the AWS Glacier. It does not consist of any up-front cost and one can modify their use up and down.

Q. 6 What are advantages of Amazon Glacier ?

Ans. :

Advantages of Amazon Glacier

a. Great Durability and Scalability

Amazon Glacier runs on the world's largest international cloud infrastructure and was designed for 99% of strength. Knowledge automatically distributes across a minimum of 3 physical accessibility zones that are geographically separated inside an AWS Region, and AWS Glacier may automatically replicate knowledge to the other AWS Region.

b. Comprehensive and Compliance Capabilities

Amazon Glacier offers subtle integration with AWS CloudTrail to log, monitor and retain storage API call activities for auditing, and supports totally different sorts of encryption. AWS Glacier additionally supports security standards and compliance certifications together.

c. Quick Retrievals

Amazon Glacier provides 3 retrieval choices to suit user's use case. Facilitated retrievals generally return information in 1-5 minutes, and are better for Active Archive use cases. Normal retrievals generally complete between 3-5 hours work, and work

well for fewer time-sensitive desires like backup data, media re-writing, or semi-permanent analytics.

d. Economical

AWS Glacier intends to very cheap priced AWS object storage category, permitting user to archive massive amounts of knowledge at an awfully low price. This makes it possible to retain all the knowledge and the information the user would like to use in cases like data lakes, analytics, IOT, machine learning, compliance, and media plus archiving. User has to pay just for what he would like, with no minimum commitments or up-front fees.

Q. 7 Write a advantages of Amazon EBS.

Ans. :

Advantages of Amazon EBS

1. **Reliable, Secure Storage**

   Each Amazon EBS volume provides redundancies within its Availability Zone to protect against failures. Encryption and access control policies deliver a strong defence-in-depth security strategy for the data.

2. **Consistent, Low-Latency Performance**

   Amazon EBS General Purpose volumes and Amazon EBS Provisioned IOPS volumes deliver low-latency through SSD technology and consistent I/O performance scaled to the needs of the application.

3. **Backup, Restore, Innovate**

   Protect user's data by taking point-in-time snapshots of user's Amazon EBS volumes providing long-term durability for the data. Boost the agility of user's business by using Amazon EBS snapshots to create new EC2 instances.

4. **Quickly Scale Up, Easily Scale Down**

   Amazon EBS allows user to optimize the volumes for capacity, performance, or cost giving user the ability to dynamically adapt to the changing needs of user's business.

5. **Geographic Flexibility**

   Amazon EBS provides the ability to copy snapshots across AWS regions, enabling geographical expansion, data centre migration, and disaster recovery providing flexibility and protecting for user's business.

6. **Optimized Performance**

   An Amazon EBS–optimized instance provides dedicated network capacity for Amazon EBS volumes. This provides the best performance for user's EBS volumes by minimizing network contention between EBS and user's instance.

Q. 8 Explain types of EBS Volumes.

Ans. :

Types of ESB Volumes

A. General Purpose SSD (gp2) Volumes

General Purpose SSD (gp2) volumes offer cost-effective storage that is ideal for a broad range of workloads. These volumes deliver single-digit millisecond latencies and the ability to burst to 3,000 IOPS for extended periods of time. Between a minimum of 100 IOPS (at 33.33 GiB and below) and a maximum of 16,000 IOPS (at 5,334 GiB and above), baseline performance scales linearly at 3 IOPS per GiB of volume size. AWS designs gp2 volumes to deliver 90% of the provisioned performance 99% of the time. A gp2 volume can range in size from 1 GiB to 16 TiB.

The performance of gp2 volumes is tied to volume size, which determines the baseline performance level of the volume and how quickly it accumulates I/O credits; larger volumes have higher baseline performance levels and accumulate I/O credits faster. I/O credits represent the available bandwidth that user's gp2 volume can use to burst large amounts of I/O when more than the baseline performance is needed. The more credits user's volume has for I/O, the more time it can burst beyond its baseline performance level and the better it performs when more performance is needed.

The Fig. 5.4 shows the burst-bucket behavior for gp2.

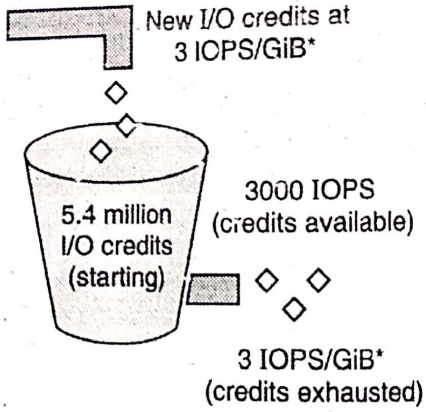


Fig. 5.4 : GP2 Burst Bucket

B. Provisioned IOPS SSD (io1) Volumes

Provisioned IOPS SSD (io1) volumes are designed to meet the needs of I/O-intensive workloads, particularly database workloads, that are sensitive to storage performance and consistency. Unlike gp2, which uses a bucket and credit model to calculate performance, an io1 volume allows user to specify a consistent IOPS rate when user create the volume, and Amazon EBS delivers within 10 percent of the provisioned IOPS performance 99.9 percent of the time over a given year. An io1 volume can range in size from 4 GiB to 16 TiB.

User can provision from 100 IOPS up to 64,000 IOPS per volume on Nitro system instance families and up to 32,000 on other instance families. The maximum ratio of provisioned IOPS to requested volume size (in GiB) is 50:1. For example, a 100 GiB volume can be provisioned with up to 5,000 IOPS. On a supported

instance type, any volume 1,280 GiB in size or greater allows provisioning up to the 64,000 IOPS maximum (50 × 1,280 GiB = 64,000).

C. Throughput Optimized HDD (st1) Volumes

Throughput Optimized HDD (st1) volumes provide low-cost magnetic storage that defines performance in terms of throughput rather than IOPS. This volume type is a good fit for large, sequential workloads such as Amazon EMR, ETL, data warehouses, and log processing. Bootable st1 volumes are not supported. Throughput Optimized HDD (st1) volumes, though similar to Cold HDD (sc1) volumes, are designed to support *frequently* accessed data. This volume type is optimized for workloads involving large, sequential I/O, and it is recommended that customers with workloads performing small, random I/O use gp2. Like gp2, st1 uses a burst-bucket model for performance.

Volume size determines the baseline throughput of user's volume, which is the rate at which the volume accumulates throughput credits. Volume size also determines the burst throughput of user's volume, which is the rate at which user can spend credits when they are available. Larger volumes have higher baseline and burst throughput. The more credits user's volume has, the longer it can drive I/O at the burst level.

The Fig. 5.5 shows the burst-bucket behavior for st1

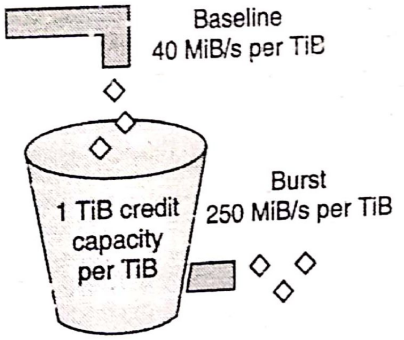


Fig. 5.5 : ST1 Burst Bucket

D. Cold HDD (sc1) Volumes

Cold HDD (sc1) volumes provide low-cost magnetic storage that defines performance in terms of throughput rather than IOPS. With a lower throughput limit than st1, sc1 is a good fit ideal for large, sequential cold-data workloads. If user requires infrequent access to his data and is looking to save costs, sc1 provides inexpensive block storage. Bootable sc1 volumes are not supported. Cold HDD (sc1) volumes, though similar to Throughput Optimized HDD (st1) volumes, are designed to support infrequently accessed data. Like gp2, sc1 uses a burst-bucket model for performance.

Volume size determines the baseline throughput of user's volume, which is the rate at which the volume accumulates throughput credits. Volume size also determines the burst throughput of user's volume, which is the rate at which user can spend credits when they are available. Larger volumes have higher baseline and burst throughput. The more credits user's volume has, the longer it can drive I/O at the burst level.

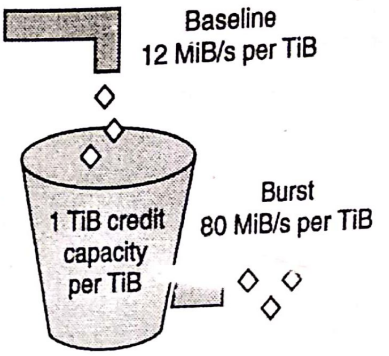


Fig. 5.6 : SC1 Burst Bucket

E. Magnetic (standard)

Magnetic volumes are backed by magnetic drives and are suited for workloads where data is accessed infrequently and scenarios where low-cost storage for small volume sizes is important. These volumes deliver approximately 100 IOPS on average, with burst capability of up to hundreds of IOPS, and they can range in size from 1 GiB to 1 TiB. Magnetic is a Previous Generation Volume. For new applications it is not recommended.

Q. 9 Write a note on Virtual Amazon Cloud.

Ans. :

Virtual Amazon Cloud

Amazon Virtual Private Cloud (Amazon VPC) enables developers to establish a virtual network for the purpose of launching resources in a section of the Amazon Web Services cloud which is totally isolated. AWS users has facility to connect to Amazon VPC using an Internet gateway, an on-premises data-centre via the Hardware Virtual Private Network (VPN) Connection Tool or via several type of AWS tools as well as other vendor VPCs. Better granular control of the cloud network is possible with the help of Amazon VPC that provides an additional layer of security for the purpose of workloads and data.

It is easy for users to define network configurations like IP address range and route tables, and handle network gateways and subnets; subnets are minor independent parts of the entire network. With the help of Amazon VPC, developer is able to generate security groups to fix limits on inbound as well as outbound traffic to Amazon Elastic Compute Cloud (EC2) instances and network access control lists to allow or deny traffic to subnets.

While generating an EC2 instance, users can set an IP address to the particular instance until it is in the IP address range of the related subnet, not assigned to any other interface and not held in reserve by Amazon. VPC routers are used to set communication between instances in various subnets. Routers also enable communication between subnets, Internet gateways and virtual private gateways. Internet gateways enable communication between instances and EC2 resources which reside outside of a VPC and in different regions. AWS provides various options to

link EC2 instances in the environment of VPC to Amazon Simple Storage Service.

AWS offers a "Start VPC Wizard," that provides four options of basic network architectures which dictate whether the category of subnets is public or private and whether the user likes to get access through the Hardware VPN. VPCs have ability to span more than one AZ (Availability Zones), but it is necessary that the subnets are in one AZ. User my additionally prefer the deployment of Amazon CloudWatch and Auto Scaling within an Amazon VPC for the purpose of monitoring resources and let them to meet spikes in workload demand. When there is provision of EC2 resources by the AWS users first, for their launching default VPC is considered if the subnet ID is not specified.

The depth of security as well as network control provided by default VPCs is similar to regular Amazon VPCs, but one important difference is that they enable user to create and manage resources with the help of AWS Management Console, EC2-Classic command line or API. The size of each VPC is restricted by AWS; user does not have facility to change the size after the VPC has been created. Also there is limit of Amazon VPC of two hundred subnets per VPC, all of them are able to support at least fourteen IP addresses. AWS has further restrictions per account / per region, containing restrictive number of VPCs to 5, the number of Elastic IP addresses to 5, the number of Internet gateways per VPC to 1, the number of virtual private gateways to 5and the number of customer gateways to fifty.

Q. 10 Write a note on Subnets.

Ans. :

Subnet

A subnet is a sub-network inside a VPC. An example of a subnet inside a VPC (10.123.X.Y) is 10.123.1.A/24. It indicates that any instance which belongs to this particular subnet will have an IP address 10.123.1.A where *A* will be in the range of 2 to 254.

These are also called as CIDR notations. An instance always belongs to a subnet. It is not possible to have an instance inside a VPC which is not belonging to any subnets. While generating instances inside AWS-VPC, it is necessary to specify which subnet the instance should belong to.

Q. 11 Write a note on Route Tables.

Ans. :

Route Tables

Routing tables are used to dictate network traffic of instances inside a subnet.

An example routing table is :

CIDR --- target

10.123.0.0/16 --- local

0.0.0.0/0 - igw (internet gateway)

This table indicates that any traffic intended for 10.123.X.Y IP (where **X** and **Y** will be in the range of 2 to 254) will be sent directly. The rest of the traffic will be directed to igw.

Now, it's very essential to recognize that a subnet is always associated with only single routing table. Hence, if an instance is spawned inside a subnet which has the above-mentioned routing table associated with it, the instance still won't be accessible from outside VPC since it does not possess a public ip.

It is possible to link an elastic ip (which is a reusable public ip) to this instance and later on access it. In turn the instance is able to access the internet. We have to note that for an instance to be directly obtainable from the internet, it must possess an elastic ip and it should be within a subnet having a routing table in which non-local traffic is routed by means of an internet gateway.

It shows that an *elastic ip* and an *igw* in the routing table are two important criterions regarding an instance to be available directly from the internet. Subnets with such routing tables which are associated with them are also called as public subnets (non-local traffic routed to internet gateway), since any instance having an elastic ip can be publicly obtainable from this subnet.

Conversely, it is possible to mention a NAT (a gateway) instance as a target for non-local traffic witnin a routing table. Also the NAT box can be placed in a public subnet having an elastic ip associated with it. At this moment any subnet having such type of routing table associated turn out to be a private subnet since it cannot be exposed publicly. Even if an elastic ip is assigned, it won't be publicly available.

Here's an example of a private subnet :

CIDR --- target

10.123.0.0/16 --- local

0.0.0.0/0 - i-abcdef (instance ip of the NAT box)

Q. 12 Write a note on ENIs.

Ans. :

Elastic Network Interface

An Elastic Network Interface (ENI) is a virtual network interface which can be associated with an instance in an Amazon VPC. The existence of ENIs is only within an Amazon VPC, and they are linked with a subnet after formation. ENIs can possess single public IP address and more than one private IP addresses.

If private IP addresses are more than one then one of them will be primary. If an instance is assigned second network interface to trough an ENI then it will be dual-homed (possess network existence in different subnets). An ENI which has been generated independently of a specific instance persists irrespective of the lifetime of that instance to which it is associated; if there is failure in an underlying instance, it is possible to preserve the IP by the way of attaching the ENI to a replacement instance.

ENIs helps to generate a management network, use the generated network and security appliances in the respective Amazon VPC, generate dual-homed instances with workloads/roles on distinct subnets, or generate a low-budget, high-availability solution.

A network interface can include the following attributes :

1. A primary private IPv4 address from the IPv4 address range of the VPC.
2. One or more secondary private IPv4 addresses from the IPv4 address range of the VPC.
3. One Elastic IP address (IPv4) per private IPv4 address.
4. One public IPv4 address.
5. One or more IPv6 addresses.
6. One or more security groups.
7. A MAC address.
8. A source/destination check flag.
9. A description.

Q. 13 What is 'security groups'? What is its significance in amazon AWS cloud computing environment? Dec. 16.

Ans. :

Security Groups

A security group acts as a virtual firewall for the respective instance to manage inbound as well as outbound traffic. After launching an instance in a VPC, user is able to assign maximum of 5 security groups to the instance. The level to act for security groups is the instance level; it cannot act at the subnet level. Hence all of the instances in a subnet in the respective VPC could be allocated to another set of security groups.

If at launching time, particular group is not mentioned then the instance is allocated to the default security group for the VPC. For all of the security groups, different set of rules are added by user which handles the inbound and outbound traffic to instances.

Characteristics of Security Groups for VPC

Following are the basic characteristics of security groups for VPC :

1. User has to set limits for the number of security groups to be created per VPC, the number of rules to be added to each security group, and the number of security groups to be associated with a network interface.
2. User has facility to specify *allow rules*, but not *deny rules*.
3. User has option to set different rules for inbound and outbound traffic.
4. When security group is created by user, there are not inbound rules to it. Hence, no inbound traffic generating from another host to user's instance is permitted unless user include inbound rules to the security group.
5. By default, there is presence of an outbound rule in security group which permits all outbound traffic. User has facility to eliminate the rule and add outbound rules which permit particular outbound traffic only. If there are no outbound rules in security group, then no outbound traffic generating from user's instance is permitted.
6. Security groups are state-full - if user forwards a request from his instance, the response traffic for the respective request is permitted to flow in irrespective of inbound security group rules. Responses to allowed inbound traffic are permitted to flow out, irrespective of outbound rules.
7. Instances attached with a security group cannot interact with each other unless rules are added by user allowing it.
8. Security groups are linked to network interfaces. After launching an instance, user has option to change the security groups attached with the instance, which leads to change in the security groups attached to the primary network interface.

Q. 14 Explain the term ACL in detail.

Ans. :

Access Control List

1. A *network access control list (ACL)* is considered as an optional layer regarding security for user's VPC which works as a firewall for managing traffic in and out of one or multiple subnets.
2. It is possible for a user to set up network ACLs with rules same as per his security groups so as to introduce an extra layer of security to his VPC.
3. User's VPC automatically has a modifiable default network ACL.
4. By default, it permits all inbound as well as outbound IPv4 or IPv6 traffic.
5. User can generate a custom network ACL and link it with a subnet. By default, all of the custom networks ACL do not allow all inbound as well as outbound traffic unless rules are not added by the user.
6. It is necessary for user to associate each subnet in the VPC to a network ACL. If user does not do it then the subnet is automatically associated with the default network ACL.
7. User can link a network ACL with more than one subnet; however at a time, association of a subnet can be done only with one network ACL.
8. When a network ACL is associated with a subnet, the earlier association is removed.
9. A network ACL possess a numbered list of rules which is assessed in a sequence, beginning with the lowest numbered

rule, to verify that whether traffic is permitted in or out of any subnet linked with the network ACL.

10. The inbound and outbound rules of a network ACL are separate, and those rules can either allow or deny traffic.

Q. 15 Explain types of ELB.

Ans. :

Types of Elastic Load balancer

1. **Application Load Balancer**

Application Load Balancer is best suited for load balancing of HTTP and HTTPS traffic and provides advanced request routing targeted at the delivery of modern application architectures, including micro-services and containers.

Operating at the individual request level, Application Load Balancer routes traffic to targets within Amazon Virtual Private Cloud (Amazon VPC) based on the content of the request.

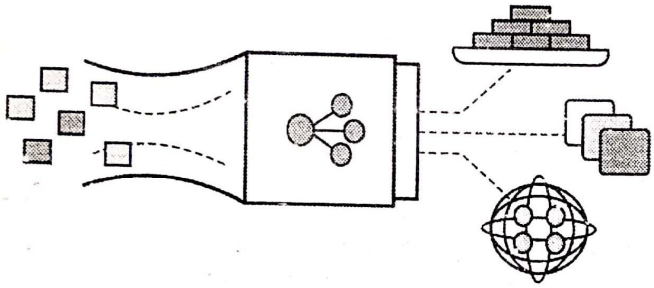


Fig. 5.7 : Application Load Balancer

2. **Network Load Balancer**

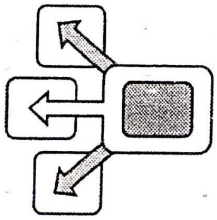


Fig. 5.8 : Network Load Balancer

Network Load Balancer is best suited for load balancing of TCP traffic where extreme performance is required. Operating at the connection level, Network Load Balancer routes traffic to targets within Amazon Virtual Private Cloud (Amazon VPC) and is capable of handling millions of requests per second while maintaining ultra-low latencies. Network Load Balancer is also optimized to handle sudden and volatile traffic patterns.

3. **Classic Load Balancer**

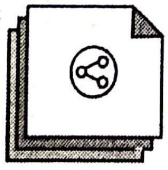


Fig. 5.9 : Classic Load Balancer

Classic Load Balancer provides basic load balancing across multiple Amazon EC2 instances and operates at both the request level and connection level. Classic Load Balancer is intended for applications that were built within the EC2-Classic network.

Q. 16 What are the advantages of Elastic Load Balancer ?

Ans. :

Advantages of Elastic Load Balancer

1. **Highly Available**

Elastic Load Balancing automatically distributes incoming traffic across multiple targets - Amazon EC2 instances, containers, and IP addresses in multiple Availability Zones and ensures only healthy targets receive traffic. Elastic Load Balancing can also load balance across a Region, routing traffic to healthy targets in different Availability Zones.

2. **Secure**

Elastic Load Balancing works with Amazon Virtual Private Cloud (VPC) to provide robust security features, including integrated certificate management, user-authentication, and SSL decryption. Together, they give the flexibility to centrally manage SSL settings and offload CPU intensive workloads from user's applications.

3. **Elastic**

Elastic Load Balancing is capable of handling rapid changes in network traffic patterns. Additionally, deep integration with Auto Scaling ensures sufficient application capacity to meet varying levels of application load without requiring manual intervention.

4. **Flexible**

Elastic Load Balancing also allows using IP addresses to route requests to application targets. This offers flexibility in how user virtualizes application targets, allowing hosting more applications on the same instance. This also enables these applications to have individual security groups and use the same network port to further simplify inter-application communication in micro-services based architecture.

5. **Robust Monitoring and Auditing**

Elastic Load Balancing allows monitoring the applications and their performance in real time with Amazon CloudWatch metrics, logging, and request tracing. This improves visibility in the behaviour of user's applications, uncovering issues and identifying performance bottlenecks in the application stack at the granularity of an individual request.

6. **Hybrid Load Balancing**

Elastic Load Balancing offers ability to load balance across AWS and on-premises resources using the same load

balancer. This makes it easy for the user to migrate, burst, or failover on-premises applications to the cloud.

Q. 17 Explain Amazon cloud watch and Auto Scaling.

Ans. :

Amazon CloudWatch

Amazon CloudWatch is a web service which is basically designed to provide real-time monitoring service for the customers of Amazon's EC2 on the utilization of various resources like CPU, disk and network. CloudWatch requires additional software on the instance to provide memory, disk space, or load average metrics. Example scripts is provided by the Amazon for Linux instances.

The management console of AWS is used to aggregate and provide the data. If customer wants to monitor the EC2 resources with the help of their own enterprise monitoring software, then command line tools and Web API's can be used to access data. The auto-scaling feature is enables by the metrics collected by Amazon CloudWatch which helps to add remove EC2 instances dynamically. The number of monitoring instances is considered for the charges to customer.

Automated scaling

This feature of EC2 enables the automatic adaption of computing capacity to site traffic. The two auto scaling mechanisms; schedule-based (e.g. time-of-the-day) and rule-based (e.g. CPU utilization thresholds) are provides feature like simple to use and efficiency.

But [illegible] is an important problem that VMs may require lot of time to be ready to use. This is problematic when there is a time binding. Image size, VM type, data center locations are factors responsible for VM start-up times.

However, one potential problem is that VMs may take up to several minutes to be ready to use, which are not suitable for time critical applications. The VM start-up times are dependent on image size, VM type, data center locations, etc.

Chapter 6 : Cloud Backup and Solutions

Q. 1 Enlist the different cloud backup benefits.

Ans. :

Benefits of cloud backup services

If the volume of backup data is low then there is reduction in the costs. The amount of data storage used by the customer is the basis for cloud providers to charge customers. So this technique will be less expensive than buying own storage servers. The amount of data that will be needed for backing purpose can vary. As the organization grows, storage requirements will increase and, if there is occasional need for data backup for projects, then there is necessity of temporary backup of the data. A good cloud service provider will let the users to increase their storage capacity on 'as needed' basis, as a result the organization is enabled to scale up with growth or to cover short-term needs.

Most cloud service providers keep the data at multiple locations which store several copies of backups at different data centers. So, if a fire takes out a whole data centre, one of the copies stored in another data center can be brought online immediately.

The cloud vendor such as Mozy generally offers free of charge cloud backup up to a certain data limit. The cloud backup provider generally offers a high availability service that is guaranteed to stay online. The data sets which are increasing are simply backed up in the cloud platforms. The cloud backup is a technique in which service vendors always take care of variety of the tasks which are required with some other forms of backup. They are normally securely aligned with ransom-ware attacks as they are operated outside of the office network.

Q. 2 What are the different cloud backup solutions?

Ans. :

Solutions for cloud backup

Backups can be categorized as following types

1. **Full system or Image Backups**

Backup techniques are very important for industry success because the organizations are always looking forward for solutions which allow for high availability. When comparing with a file backup vs. image backup, image solution works better than the file backup. An image backup or full system backup creates a copy of whole data volume, which includes all system files, the boot record files, and any other data contained on the disk. For creating an image backup of an active system, it needs to stop all applications for the backup purpose. An image backup allows a system to do what is referred to as a bare metal restore. Ghost is an example of software that provides full system or image backup.

Image Backups are simply as the name suggests. An image can be the entire operating system, which includes files, executable programs and OS configurations. Professional backup solutions can create full or additional images of the hard drive in an automated manner. With the help of an image backup, it is possible to restore a single file, directory or entire disk to hardware or to a virtual machine. It is also possible to backup to different onsite or offsite devices like an external USB, network connected hard drives or Fire-wire devices. In the image backup solution data should be strongly encrypted so that it can meet the requirements.

2. **Point-in-time (PIT) or Snapshots Backup**

In this technique the data is backed up, and then every frequent change is amended to the backup and that can be referred

to as an incremental backup. This type of backup allows restoring the data to a point in time and it always saves multiple copies of any file that has been changed. Generally 10 to 30 copies of older versions of files can be saved. The first backup is moderately slow over an internet connection, but the next backup can be relatively fast. For example, software like Carbonite can take number of days to backup a system, but it may take few minutes to create the snapshot. The total time required to backup a system is referred to as its backup window.

3. Differential and Incremental Backups

A differential backup is associated with an incremental backup. An incremental backup is a type of backup in which any altered files are copied to the backup storage and their archive attribute can be cleared by the incremental backup technique. In a differential backup, all the altered files as the last complete backup are copied by the backup software, and always require that the software has to set archive bit ON for any differential backup, since only a full backup can clear all files' archive bit.

The purpose of using an archive bit which is used by backup software is to specify whether a file should be backed up or not. The bit required to set on for backup purpose and it can be cleared when backup has copied the file. An archive bit is a command to the software. The archive bit comes into the picture in backup technique when an incremental backup solution must inspect the full backup data and then analyze all subsequent increments to find the latest file(s). In this type of backup, the software can gain the latest backup from the last full backup and also the last incremental backup. Files in overriding incremental backups can be taken as provisional or scratch versions. As compared to others, incremental backups are faster and more efficient from a storage perspective, and they are also less fault-tolerant.

4. Reverse Delta backup

A reverse delta backup initially creates a full backup and then periodically synchronizes the full copy with the live version. The older versions of files that need to change are archived and hence the historical record of the backup exists. The example of software that uses reverse delta backup system is Apple's Time Machine and the RDIFF-BACKUP utility.

5. Continuous Data Protection (CDP) or Mirroring

The goal of continuous data protection (CDP) backup system is to create a cloned copy of present data. This type of technique is a cloud storage system which contains a certain built-in latency, so when the original data set is inactive, the copied data lags behind the original in concurrency.

6. Open file Backup

The applications such as database systems and messaging systems are very critical applications and that cannot be shut down before backed up. An open file backup is a technique which analyzes the transactions which are in progress. It compares the file(s) which are at the start of the backup and the file(s) which are at the end of the backup, and it will creates a backup which represents a complete file as it would exist at the time the backup started and completes after all the transactions have been processed. Open file backup systems are costly and highly customized to a particular application such as SQL Server.

7. Data Archival

The concept of data archiving is mainly used to indicate the data migration which is no longer in use to secondary or tertiary long-term data storage for retention. The main purpose of using an archive is for legal agreement or it can provide a long-term historical record.

Q. 3 What are the major cloud backup services ?

Ans. :

Major cloud backup services

Following are the cloud data backup vendors

1. Acronis

A cloud service which offers its backup plans to create a hybrid cloud and local backup service. Acronis Backup to Cloud platforms recovers data files, folders that need to back up, applications or a complete system. Data and metadata are generally encrypted before the data is sent to Acronis data centers. Acronis Backup supports backup to Cloud from PC and VMware to cloud

2. Arcserve

The main motive of this type of service is to protect from cloud disaster recovery and handle backup. The cloud protection is targeted at the midmarket. The arceserve has expanded its Unified Data Protection (UDP) contribution with purchase of Zetta.

3. Backblaze

This service offers individual and business cloud backup. Backblaze cloud service stores data on its open source Storage Pods hardware and cloud-based Backblaze Vault file system. Backup data through Backblaze can be accessible through a particular web browser on mobile devices and computers.

4. Carbonite

It provides service to consumers, SMBs and small enterprises. This type of service offers the backup which includes back up documents, email, music, photos and is available for Windows and Mac users. The vendor has two cloud data backup plans: *Carbonite Personal* which is available for individual persons, households and home offices and *Carbonite for business*, which is available for cloud and software-based backup plans for the enterprise.

5. Druva

This cloud backup features has two major products :

The enterprise-level Druva which is targeted at endpoints and backs up data across physical and public cloud storage. And the other is Phoenix which is a software mediator and is used to back up and restore data in the cloud which are based on the distributed physical and virtual servers. This vendor is creating a move into the data management market, and its latest Apollo SaaS product protects workloads in AWS through the Druva Cloud Platform.

6. **JDrive**

This cloud backup deal with consumers and small business processes and supports snapshots, synchronizing service and hybrid protection of data.

7. **Microsoft Azure Backup**

This cloud backup service automatically sends backups to the Azure cloud. Azure Site Recovery will automate duplication of data to back up private Windows infrastructure.

8. **Mozy (by Dell)**

This type of service has three products :

1. MozyEnterprise for enterprises
2. MozyPro for smaller businesses
3. MozyHome for consumers

This backup service vendor provides many key features, which includes the Mozy synchronization of file, synchronization of file system and the Mozy Data Shuttle seeding service.

9. **Unitrends**

This cloud backup service allows customers to back up the data without any limitations to its private cloud. To use this type of service customers must have installed Unitrends' Recovery Series backup hardware or Enterprise Backup.

10. **Hybrid cloud backup**

Hybrid cloud backup providers connect traditional backups to the cloud. The hybrid cloud backup is used in the organizations that generate a large volume of data and need quick restore access. The hybrid cloud uses the approach - a network-attached storage (NAS) application which serves as a local backup and it synchronizes the backup data to the cloud. Suppose an organization requires a quick restoration of data, the data is available in the on-site NAS. If there is loss of data to its primary site, the cloud backup is still available. In another hybrid approach, an institute can use both the public and private clouds for backup. Data consistency with hybrid cloud backup is somewhat difficult, when the data transfer takes a long time.

Q. 4 Explain the concept of CDMI in details.

Ans. :

Cloud data management interface

An open cloud storage management standard is the Storage Networking Industry Association's Cloud Data Management Interface (CDMI). CDMI operates with the storage domain model shown in Fig. 6.1 which allows the interoperation between different cloud systems, and those cloud systems can be on public, private, or hybrid cloud. CDMI has the commands that permit the different applications to access cloud storage platforms and will create, retrieve, update, and delete data objects as per the requirements. It also provides data object discovery and enables storage of data systems to correspond with one another in the cloud infrastructure domain.

The CDMI provides security using standard storage protocols, monitoring and billing methods as well as authentication methods. CDMI uses the similar authorization and authentication technique as NFS (Network File System) does. In the Cloud Data Management Interface (CDMI), the storage area is divided into units called containers. A container can store a set of data and serves as object for the naming purpose and with the help of that data different service operations are performed. The CDMI data object can manage CDMI containers, as well as containers that are accessible in cloud storage through other supported protocols.

Fig. 6.1 shows the SNIA cloud management storage model. In the Fig. 6.1 XAM stands for the Extensible Access Method and XAM is a storage API which is developed for accessing the content on the storage device. VIM stands for Vendor Interface Modules; the purpose of this interface is to convert the XAM request into the native commands which are generally supported by the storage operating system in the cloud platforms.

CDMI can access objects which are stored in the cloud infrastructure by using the standard HTTP command protocol and the REST (Representational State Transfer) protocol. The other functionality of CDMI is to discover objects and those objects can be exported and managed as part of a storage space called as container. CDMI also provides an interface by which system can get entrée to the storage objects in a container over the Web. Other features of CDMI are controlling the access for the system, usage accounting, and the ability to present containers in such a manner that applications will able to see these containers.

CDMI is useful for accessing the metadata for HTTP protocols, system, user, and storage media attributes for accessing them through an interface which is standard and uses a schema that is known as the Resource Oriented Architecture (ROA).

In this technique, every source is identified by a standardized URI (Uniform Resource Identifier) that may be translated into both hypertext (HTTP) and other forms. CDMI uses the SNIA EXtensible Access Method (XAM) to discover and access metadata associated with each data object. Metadata is stored not only for data objects, but for data containers so that any data can be placed into a container.

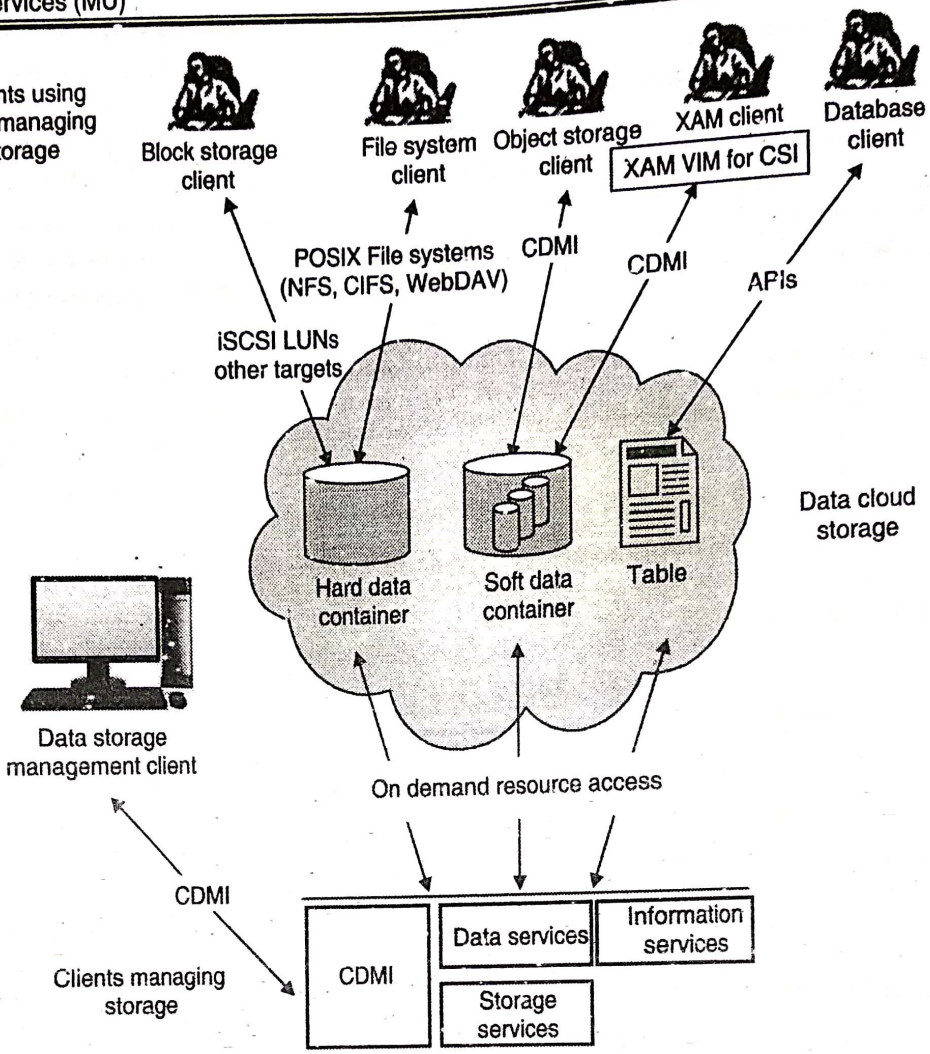


Fig. 6.1 : Cloud Storage for Cloud Computing"

In CDMI concept, resources are recognized so that they can use attributes in the form of key-value pairs, and hence actions can be performed based on the attributes.

The actions include the CRUD operations which are as follows :

Create, Retrieve, Update, and Delete. These CRUD operations are transmitted into the standard HTTP actions such as POST, GET, PUT, and DELETE. The commands like HEAD and OPTIONS provide a wrapper for metadata and operational instructions.A typical action that can be performed on CDMI which includes PUT or GET operation is as follows :

PUT http://www.cloudy.com/store/<myfile>

GET http://www.cloudy.com/compute/<myfile>

The domain which is mentioned above "cloudy.com "would be the service provider, myfile is the name which can provide the instance, and compute is nothing but the folder containing the file. PUT operation will create the container (store) if it didn't exist previously. A range of KEY/VALUE pairs which describes the object attributes in CDMI is defined by the standard attributes. In a protected networking technique, cloud-based computing always depend on the idea of backing up, or sending data to and receiving data from, a secure remote location. It can be said that the cloud data management interface will be acting as a location for using cloud services.

Developers of CDMIs implement the design in such a way that they provide superior products and services to cloud infrastructure. The main advantage of working with CDMI is that it deals with how data is sent, stored and used. One of the examples is the use of metadata, which is nothing but "data about data," for any data being transferred or stored in cloud-based systems. The use of metadata is one of the usual elements of creating, maintaining and presenting CDMIs. The Cloud Data Management Interface is the interface for the applications that is used to create, retrieve, update and delete data elements from the cloud. The interface required for the CDMI is also used by administrative and management applications to manage containers in the CDM, accounts, security access and monitoring/billing information, even for storage that is accessible by other protocols.

Object Model for CDMI

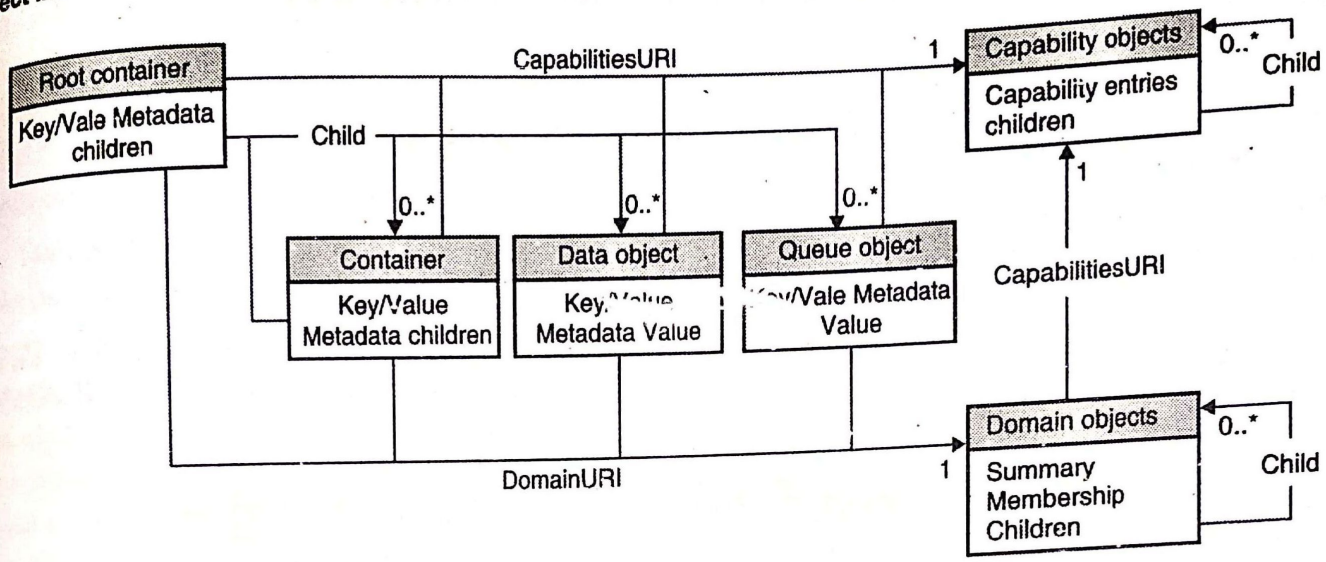


Fig. 6.2 : CDMI Object Model

For the storage operations in the object model of CDMI, the client of the interface only needs to know about container objects and data objects. Using the CDMI object model as shown in Fig. 6.2 the client can send a PUT command via CDMI to the new container URI and create a new container with some specified name. The metadata which will be acting as metadata for CDMI are optional and are expressed as a series of name-value pairs. After creating a container, a client can send a PUT command to create a data object within the newly created container. A succeeding GET command will take the data object, including the value field.

CDMI Metadata Concept

CDMI uses many different types of metadata as follows :

1. HTTP metadata,
2. Data system metadata,
3. User metadata,
4. Storage system metadata.

HTTP metadata is a kind of metadata that is related to the use of the HTTP protocol. In CDMI the metadata like user metadata, storage system metadata are defined in the form of name- value pairs. Service provider defines data system metadata and storage system metadata names which shall begin with the reverse domain name of the vendor.

Data system metadata is a kind of metadata that is preliminary defined by a CDMI client and this metadata is module of objects. Data system metadata conceptually defines the data necessities associated which are included in the data services that are deployed in the cloud storage system. User metadata is a type of metadata which includes the user-defined JSON strings, arrays, and objects that are stored in the metadata field. The namespace which is required for user metadata is self-defined, and user metadata names should not begin with the prefix "cdmi_." Storage system metadata is a kind of metadata which is created by the storage services in the cloud system (e.g., creation time, size) that provides very useful information to a CDMI client.

Object ID for CDMI

Every object which is stored within a CDMI system should have a worldwide unique object identifier (ID) which is given at the creation time. The CDMI object ID is a string with necessities for how it is generated and how it gains its uniqueness. Every cloud service that implements CDMI can generate such identifiers so that the possibility of getting contradictory with identifiers which are generated by other cloud services and the possibility of generating an identifier that has already been used is effectively zero. Each cloud storage system will allow object ID based access to the stored objects which enables the object's ID to append to the root container URI.

If the data object "MyDataObject.txt", which is located in root container, has an object ID of "00006FFD001001CCE3B2B4F602032653", the following pair of URIs access the same data object :

http://cloud.example.com/root/MyDataObject.txt

http://cloud.example.com/root/cdmi_objectid/00006FFD001001CCE3B2B4F602032653

Generally the containers are supported and they are also accessible by object ID.

If the container "My Container", located in the root container, has an object ID of "00006FFD0010AA33D8CEF9711E0835CA", the following pairs of URIs access the same object :

http://cloud.example.com/root/MyContainer/

http://cloud.example.com/root/cdmi_objectid/00006FFD0010AA33D8CEF9711E0835CA/

http://cloud.example.com/root/MyContainer/MyDataObject.txt

http://cloud.example.com/root/cdmi_objectid/00006FFD0010AA33D8CEF9711E0835CA

CDMI object ID format

The cloud services create the object ID. The object ID has to be worldwide unique and the format for the object definition has to follow the format as shown in Fig. 6.3. The format of an object ID is a variable-length byte format and it should be a maximum length of 40 bytes. A user can treat object IDs as byte strings.

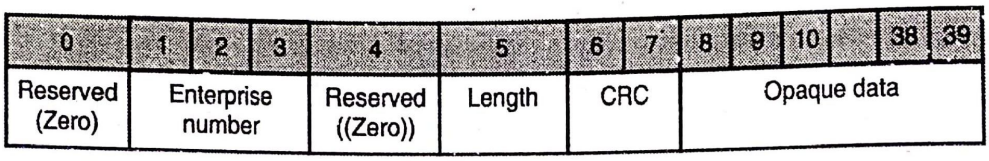


Fig. 6.3 : CDMI Object Id format

The fields shown in Fig. 6.3 are defined as follows.

1. The reserved bytes which are mentioned in the Fig. 6.3 are set to zero.
2. The Enterprise Number field is the SNMP enterprise number of the organization that developed the system which has created the object ID in network byte order.
3. The byte which is present at offset 5 can contain the full length of the object ID in bytes.
4. The CRC field should contain a 2-byte (16-bit) CRC in network byte order.
5. The CRC field enables the object ID to be validated for integrity

Security Objectives

Security concept in the CDMI always refers to the preventing techniques in managing and accessing data and storage.

The objectives that are mentioned have the following attributes :

1. It always makes sure that the interactions between a CDMI client and server cannot be read or modified by a third party.
2. It must allow CDMI clients and servers to assure their identity.
3. It has to permit CDMI client to perform actions on a CDMI server.
4. It also allows the data to be generated for actions performed by a CDMI client on a CDMI server.
5. It eliminates data in a controlled manner.

Security measures within CDMI are summarized as

Discovers the security capabilities of a particular implementation.

1. Transport security.
2. User and entity authentication.
3. Authorization and access controls.
4. Data integrity.
5. Data and media sanitization.
6. Data retention.
7. Protections against malware.
8. Data at-rest encryption.
9. Security capabilities.

Q. 5 Write a short note on Cloud Storage Gateways.

Dec. 15, May 17

Ans. :

Cloud storage gateway

It is a hardware or software which is placed on the customer premise that is an association between local applications and remote cloud-based storage.

The cloud storage gateways are implemented on a machine which is local or application to facilitate data transfer between incompatible base protocols, security and compression services. A cloud storage gateway can provide the protocol translation and effortless connectivity which allows the technology which is incompatible to communicate transparently. A cloud storage gateway can also be termed as a cloud storage controller or cloud storage appliance. A cloud storage gateway is designed in such a manner that it can provide interoperability between different data protocols used in a client/server cloud infrastructure. The gateway can be a separate device or it can be a virtual machine (VM) image

which provides protocol conversion and connection between the devices that allows incompatible technologies to communicate transparently. The need for a cloud storage systems and enterprise applications arises because of an incompatibility between the protocols which are used for public cloud platforms and legacy storage systems platforms.

Many public cloud providers are always depend on Internet protocols, usually HTTP, rather than conventional storage area network (SAN) or network-attached storage (NAS) protocols. Many of the today's cloud storage gateways provide the data which is de duplicated and compress the capabilities so that the available bandwidth can be used efficiently and the data can be moved as quickly as possible. By reducing the footprint which is digitalized can also lower the cost, as the cloud vendors charge for transfers of the data as well as for storage space. The other features can include snapshots and controlling the different versions, the ability to use local storage as a cache, automated storage concept and encryption concept. As the demand of the cloud storage has increased drastically, some of the cloud providers have changed the word "gateway" by "controller" to highlight the idea that their gateway products do more than just serve as a bridge.

The cloud storage allows interoperability among the cloud application programming interface (API) and that interface is REST/SOAP-based on the data storage and Internet SCSI (iSCSI), Fiber Channel (FC) and other cloud storage server system protocols. The systems for the cloud are implemented as gateway of software which gives the services for data transfer and retrieval between remote cloud storage servers. It also includes data compression for faster and easier transfer, management of version and control of entire storage system and encryption which is performed at run time, so it makes secure data transmission.

Q. 6 What is AWS storage gateway?

Ans. :

AWS storage gateway

In the year of 2006, Amazon Web Services (AWS) has started the services in the market which provides the web services, and this technology now termed as cloud computing. Nowadays AWS vendors provide a highly consistent, scalable, minimum infrastructure platform in the cloud that powers multitude of businesses. AWS Storage Gateway provides integration between the IT environment and the AWS storage infrastructure. The user store the data in the AWS cloud which provides data security features and cost-efficient storage. AWS Gateway has the following two types of storage, i.e. volume based and tape based.

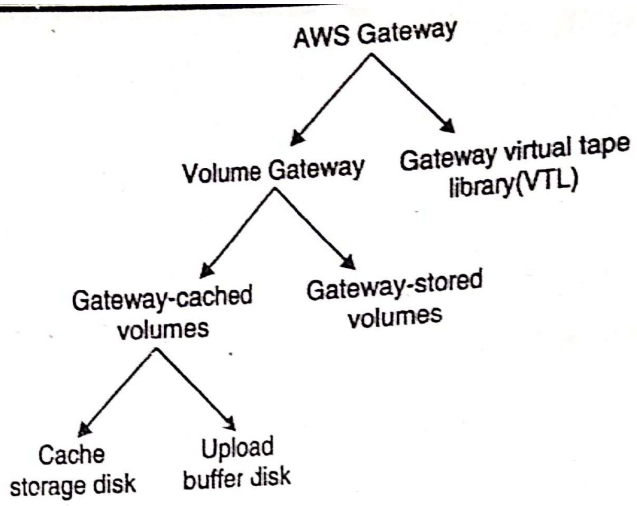


Fig. 6.4 : AWS Gateway

Volume Gateways

This type of storage gateway provides cloud-backed storage volumes which include Internet Small Computer System Interface (iSCSI) procedure from the application servers.

Gateway-cached Volumes

This type of AWS Storage Gateway always stores all the application data in a storage volume in Amazon S3. The range is from 1GB to 32 TB and up to 20 volumes with a total storage of 150TB. It is of two categories -

1. **Cache Storage Disk**

All the software applications need storage volumes so that they can store their data. This kind of storage type is generally used to store data on primary basis when it is to be written to the storage volumes in AWS. The data from the cache storage disk is uploaded to Amazon service from the upload buffer. The cache disk keeps the data which is most recently accessed. When any of the application requires that data, the cache storage disk will be checked before checking Amazon cloud service. The user has to follow guidelines to determine the quantity of disk space to be allocated for cache storage. The allocation should be at least 20% of the available file store size as cache storage.

2. **Upload Buffer Disk**

This kind of storage disk is used to store the data before it is uploaded to Amazon S3 over SSL connection. This type of storage gateway uploads the data from the upload buffer over AWS. In some of the cases there is need to back up storage volumes in Amazon. These backups are incremental and are known as snapshots. Incremental backup is nothing but a new snapshot is backing up the data that has been changed since the last snapshot is changed. The snapshots can be taken either at a scheduled interval or as per the requirement.

Gateway-stored Volumes

Virtual Machine (VM) is being activated when the gateway volumes are created and mapped to the storage disks. Since, the

applications can write/read the data from the gateway storage volumes, it can read and write the data from and to the mapped disk. A gateway stored volume will keep the data to store preliminary data locally and provides the applications with minimum access to entire datasets. The range is from 1 GB to 16 TB in size and supports up to 12 volumes per gateway with a maximum storage of 192 TB.

Gateway-Virtual Tape Library (VTL)

This storage type provides an infrastructure which is in the form of virtual tape and that scales effortlessly with the business requirements and also eliminates the burden of provisioning the operations for scaling purpose, and maintaining a physical tape infrastructure. Here the gateway VTL is preconfigured with media changer and different tape drives that are available with the existing client backup applications as iSCSI devices.

Q. 7 What are the challenges in cloud data storage.

Ans. : Challenges in cloud data storage

Following are the challenges in cloud data storage

1. **How Does the Solution Prevent Data Leakage?**

The cloud is an environment, in which the resources are shared. Cloud can be accessed by outside organization. Hence sharing such a data with hardware and placing data in the hands of a vendor that looks like, to be risky. In addition, controlling the data over the internet is very important. Since data is accessed by different agencies, a malicious hacker attack or even an accident may occur. Data leakage would be a major security concern or privacy violation. The best strategy needs to make sure that the cloud provider should exchange only encrypted files. The users always need to use the strongest encryption. User doesn't need to depend on the cloud provider or an intermediary to encrypt those files over the network. With the cloud use, all data and metadata has to be encrypted before it proceeds for the processing.

2. **Will Your Organization Have Unique Cloud Credentials?**

Access for cloud storage is based on credentials, and if there is another similar customers and they share the identical credentials, then there is a risk that one of them could obtain credentials of other customer and access the data. So one of the solutions is user needs to secure own unique credentials.

3. **How Secure Will Your Data be in Transit?**

If strong encryption and unique credentials is not provided, files can be damaged in the cloud, and also there is risk during data transmission.

4. **Who Holds the Crypto Keys?**

The main solution behind this is encryption should be automatic. So when there is no insecure mode, then there is less chance of sending unencrypted keys, to the unsecure data on cloud. Keys should also be securely escrowed, and difficult to retrieve, so that no outside party can obtain that key to access the data.

5. **Will Performance Suffer?**

A strong security approach is a requirement for cloud data storage, but it should not impact performance. Encryption of data that is sent to the cloud, and decryption of the data files which are called back from the cloud should happen with little or no impact on the user experience. In an ideal world, this process should happen without coming in notice of user.

Q. 8 Explain the comparison between different cloud platforms.

Ans. : Comparison between different cloud platforms

Cloud computing is the on-demand delivery of computation power, storage, web applications, and other IT resources through a cloud platform via internet. Amazon Elastic Compute Cloud (Amazon EC2) is a web service popularly called as Amazon Web Service (AWS) that provides resizable compute capacity in the cloud. Amazon EC2's simple web service interface allows user to configure capacity. Amazon's model is such that user pays only for capacity used, allowing users to quickly scale up or down capacity, as computing requirements change.

For example, during year-end sale the e-commerce website may experience higher than average traffic and hence it can buy additional capacity and only pay for that capacity during peak-traffic period. Open-Stack is an open source cloud computing platform that supports all types of cloud environments. Open-Stack aims for simple implementation, scalability, and a set of features.

As name suggests, Cloud computing experts from around the world contribute to the project of Open-Stack. Open-Stack is cloud operating system that controls compute, storage and networking resources. It also provides dashboard for administrators to manage resources using a web interface. Open-Stack provides a set of services by means of an Infrastructure-as-a-Service (IaaS) solution. Each service provides an Application Programming Interface (API) in order to integrate. Basically, Open-Stack offers almost all features as that of Amazon EC2 with only significant difference in price model and the fact that Open-Stack is open source version of Cloud Computing.

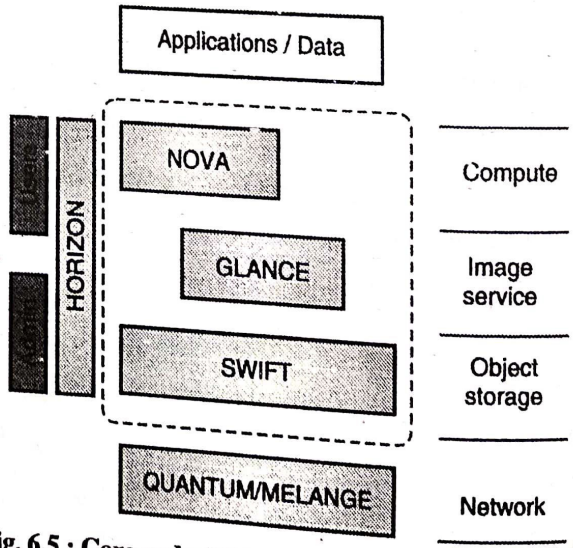


Fig. 6.5 : Core and additional component of open stack

As shown in Fig. 6.5. Open-Stack generally built from core of the technologies. As shown in the Fig. 6.5 on the left side of the dashboard, there is a user interface for managing OpenStack services for both users and administrators. Nova (compute) gives a computer platform for supporting the provisioning and management of large numbers of servers and virtual machines

The Swift components generally implement an extremely scalable object system for the storage technique with internal redundancy. At the bottom in the Fig. 6.5 there are Quantum and Melange components present, and they are for the implementation of the network connectivity as a service. The Glance components implement a repository for virtual disk images. Open-Stack is nothing but the collection of projects that as a whole provide a complete IaaS solution.

The Open-Stack can be represented by following three core open source projects :

1. Nova (compute),
2. Swift (object storage),
3. Glance (VM repository).

Nova, or Open-Stack Compute provides the VM instances across a network of servers for the management purpose. The application programming interfaces (APIs) for the Open Stack structure provides the compute for the condition that attempts to be physical hardware. The Nova vendors provide the Open Stack API for management but also provide the Amazon EC2-compatible API for those comfortable with that interface.

The Nova supports proprietary hypervisors for organizations that use them, but more importantly, it also supports following hypervisors :

1. Xen
2. Kernel Virtual Machine (KVM)
3. Operating system virtualization such as Linux

How is Open-Stack used in a cloud environment?

The cloud is nothing but providing computing environment for end users in a remote system, in which the actual software runs as a service on consistent and scalable servers rather than on each end-user's computer. Cloud computing refers to a lot of things, but characteristically the organization can talks about the operating different items "as a service" software, platforms, and infrastructure. The Open-Stack falls into the category of Infrastructure as a Service (IaaS). And hence the open stack provides the infrastructure which will be easy for users to rapidly add fresh instance, upon which other cloud components can run. Normally, the infrastructure runs a "platform" and depending upon that a developer can create software applications that are delivered to the end users.

Q. 9 Compare the Open Stack and Amazon Web Service.

Ans. :

Comparison between open stack and amazon service

Parameter	OpenStack	Amazon Web Service
Service Model	It Supports IaaS	It Supports IaaS
Deployment OS	Linux	Linux, Windows
Compute	In openstack it can be Named as 'Instance' Compute mainly consists of virtual machine with memory, CPU and storage. Each request from end-user usually spins at least one Compute Node i.e. Virtual Machine. For example, when end-user tries to login, one virtual machine is responsible for logic spins automatically. When another end-user tries to reset password, another virtual machine is responsible for reset password spins automatically	In AWS it can be named as 'Virtual Machine'
Networking: Networking provides	Networking as a service is called 'Neutron' in OpenStack	Networking as a service is called 'Networking' in Amazon Web Service
Networking Service	One can create networks and networking functions, eg. L3 forwarding, NAT, edge firewails, IPsec VPN.	Virtual routers or switches can be added if one uses AWS VPC, a virtual public cloud.

Parameter	OpenStack	Amazon Web Service
Load Balancing:	OpenStack LBaaS (Load Balancing as a Service) balances traffic from network to application services. This is the mechanism to balance 'above average' load/traffic without failure.	ELB (Elastic Load Balancing) distributes incoming traffic across Amazon instances.
Object Storage:	Named as 'Swift'. It offers cloud storage software so that user can store and retrieve data with a simple API. Data is stored in the form of objects - logical groups, along with meta-data and identifier.	Named as Simple Storage Service (S3). Amazon S3 provides management features so users can organize their data and configure access controls to meet specific organizational needs
Monitoring:	Monitoring component is called Ceilometer	Monitoring component is called Cloudwatch
Cost : Cost of using cloud service	Usually consists of an upfront license cost, annual support costs and a subsequent license renewal.	Usually billing is by the minute/hour
Services provided	Compute service Storage concepts Object Storage service Block Storage service Shared File Systems service Networking service Dashboard Identity service Image service	Compute Database Storage Migration Network and Content Delivery Security and Identity Compliance Management Tools
Components	Compute (Nova) Image Service (Glance) Object Storage (Swift) Dashboard (Horizon) Identity Service (Keystone) Networking (Neutron) Block Storage (Cinder) Telemetry (Ceilometer)	Elastic Compute Cloud Simple Storage Service Elastic Block Storage Amazon Virtual Private Cloud
Types of Deployment	OpenStack-based Public Cloud On-premises distribution Hosted OpenStack Private Cloud OpenStack-as-a-Service Appliance based OpenStack	AWS Elastic Beanstalk AWS CloudFormation AWS OpsWorks AWS CodeCommit AWS CodePipeline AWS CodeDeploy