The characteristics of cloud computing are given below:

1) Agility

The cloud **works in a distributed computing environment**. It shares resources among users and works very fast.

2) High availability and reliability

The availability of servers is high and more reliable because the **chances of infrastructure failure are minimum**.

3) High Scalability

Cloud offers **"on-demand" provisioning of resources on a large scale**, without having engineers for peak loads.

4) Multi-Sharing

With the help of cloud computing, **multiple users and applications can work more efficiently** with cost reductions by sharing common infrastructure.

5) Device and Location Independence

Cloud computing enables the users to access systems using a web browser regardless of their location or what device they use e.g. PC, mobile phone, etc. **As infrastructure is off-site** (typically provided by a third-party) **and accessed via the Internet, users can connect from anywhere**.

6) Maintenance

Maintenance of cloud computing applications is easier, since they **do not need to be installed on each user's computer and can be accessed from different places**. So, it reduces the cost also.

7) Low Cost

By using cloud computing, the cost will be reduced because to take the services of cloud computing, **IT company need not to set its own infrastructure** and pay-as-per usage of resources.

8) Services in the pay-per-use mode

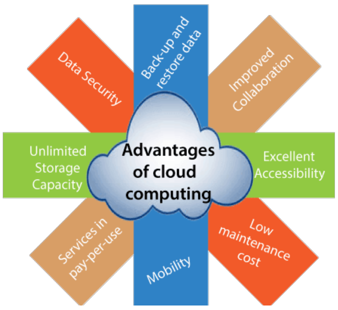
Application Programming Interfaces **(APIs) are provided to the users so that they can access services on the cloud** by using these APIs **and pay the charges as per the usage of services**.

Advantages and Disadvantages of Cloud Computing

Advantages of Cloud Computing

As we all know that Cloud computing is trending technology. Almost every company switched their services on the cloud to rise the company growth.

Here, we are going to discuss some important advantages of Cloud Computing-



1) Back-up and restore data

Once the data is stored in the cloud, it is easier to get back-up and restore that data using the cloud.

2) Improved collaboration

Cloud applications improve collaboration by allowing groups of people to quickly and easily share information in the cloud via shared storage.

3) Excellent accessibility

Cloud allows us to quickly and easily access store information anywhere, anytime in the whole world, using an internet connection. An internet cloud infrastructure increases organization productivity and efficiency by ensuring that our data is always accessible.

4) Low maintenance cost

Cloud computing reduces both hardware and software maintenance costs for organizations.

5) Mobility

Cloud computing allows us to easily access all cloud data via mobile.

6) IServices in the pay-per-use model

Cloud computing offers Application Programming Interfaces (APIs) to the users for access services on the cloud and pays the charges as per the usage of service.

7) Unlimited storage capacity

Cloud offers us a huge amount of storing capacity for storing our important data such as documents, images, audio, video, etc. in one place.

8) Data security

Data security is one of the biggest advantages of cloud computing. Cloud offers many advanced features related to security and ensures that data is securely stored and handled.

Disadvantages of Cloud Computing

A list of the disadvantage of cloud computing is given below -

1) Internet Connectivity

As you know, in cloud computing, every data (image, audio, video, etc.) is stored on the cloud, and we access these data through the cloud by using the internet connection. If you do not have good internet connectivity, you cannot access these data. However, we have no any other way to access data from the cloud.

2) Vendor lock-in

Vendor lock-in is the biggest disadvantage of cloud computing. Organizations may face problems when transferring their services from one vendor to another. As different vendors provide different platforms, that can cause difficulty moving from one cloud to another.

3) Limited Control

As we know, cloud infrastructure is completely owned, managed, and monitored by the service provider, so the cloud users have less control over the function and execution of services within a cloud infrastructure.

4) Security

Although cloud service providers implement the best security standards to store important information. But, before adopting cloud technology, you should be aware that you will be sending all your organization's sensitive information to a third party, i.e., a cloud computing service provider. While sending the data on the cloud, there may be a chance that your organization's information is hacked by Hackers

Cloud Computing Architecture

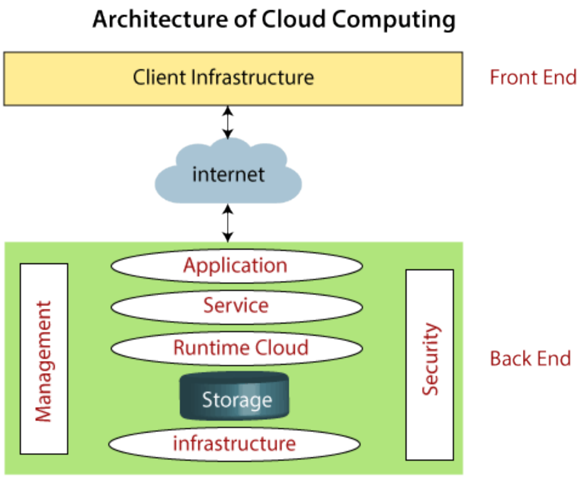
As we know, cloud computing technology is used by both small and large organizations to **store the information** in cloud and **access** it from anywhere at anytime using the internet connection.

Cloud computing architecture is a combination of **service-oriented architecture** and **event-driven architecture**.

Cloud computing architecture is divided into the following two parts -

- Front End
- Back End

The below diagram shows the architecture of cloud computing -



Front End

The front end is used by the client. It contains client-side interfaces and applications that are required to access the cloud computing platforms. The front end includes web servers (including Chrome, Firefox, internet explorer, etc.), thin & fat clients, tablets, and mobile devices.

Back End

The back end is used by the service provider. It manages all the resources that are required to provide cloud computing services. It includes a huge amount of data storage, security mechanism, virtual machines, deploying models, servers, traffic control mechanisms, etc.

Note: Both front end and back end are connected to others through a network, generally using the internet connection.

Components of Cloud Computing Architecture

There are the following components of cloud computing architecture -

1. Client Infrastructure

Client Infrastructure is a Front end component. It provides GUI (Graphical User Interface) to interact with the cloud.

2. Application

The application may be any software or platform that a client wants to access.

3. Service

A Cloud Services manages that which type of service you access according to the client's requirement.

Cloud computing offers the following three type of services:

i. Software as a Service (SaaS) – It is also known as **cloud application services**. Mostly, SaaS applications run directly through the web browser means we do not require to download and install these applications. Some important example of SaaS is given below –

Example: Google Apps, Salesforce Dropbox, Slack, Hubspot, Cisco WebEx.

ii. Platform as a Service (PaaS) – It is also known as **cloud platform services**. It is quite similar to SaaS, but the difference is that PaaS provides a platform for software creation, but using SaaS, we can access software over the internet without the need of any platform.

Example: Windows Azure, Force.com, Magento Commerce Cloud, OpenShift.

iii. Infrastructure as a Service (IaaS) – It is also known as **cloud infrastructure services**. It is responsible for managing applications data, middleware, and runtime environments.

Example: Amazon Web Services (AWS) EC2, Google Compute Engine (GCE), Cisco Metapod.

4. Runtime Cloud

Runtime Cloud provides the **execution and runtime environment** to the virtual machines.

5. Storage

Storage is one of the most important components of cloud computing. It provides a huge amount of storage capacity in the cloud to store and manage data.

6. Infrastructure

It provides services on the **host level**, **application level**, and **network level**. Cloud infrastructure includes hardware and software components such as servers, storage, network devices, virtualization software, and other storage resources that are needed to support the cloud computing model.

7. Management

Management is used to manage components such as application, service, runtime cloud, storage, infrastructure, and other security issues in the backend and establish coordination between them.

8. Security

Security is an in-built back end component of cloud computing. It implements a security mechanism in the back end.

9. Internet

The Internet is medium through which front end and back end can interact and communicate with each other.

Cloud Computing Technologies

A list of cloud computing technologies are given below -

- Virtualization
- Service-Oriented Architecture (SOA)
- Grid Computing
- Utility Computing

Virtualization

Virtualization is the process of creating a virtual environment to run multiple applications and operating systems on the same server. The virtual environment can be anything, such as a single instance or a combination of many operating systems, storage devices, network application servers, and other environments.

The concept of Virtualization in cloud computing increases the use of virtual machines. A virtual machine is a software computer or software program that not only works as a physical computer but can also function as a physical machine and perform tasks such as running applications or programs as per the user's demand.

Types of Virtualization

A list of types of Virtualization is given below -

i. Hardware virtualization
ii. Server virtualization
iii. Storage virtualization
iv. Operating system virtualization
v. Data Virtualization

Service-Oriented Architecture (SOA)

Service-Oriented Architecture (SOA) allows organizations to access **on-demand** cloud-based computing solutions according to the change of business needs. It can work without or with cloud computing. The advantages of using SOA is that it is easy to maintain, platform independent, and highly scalable.

Service Provider and Service consumer are the two major roles within SOA.

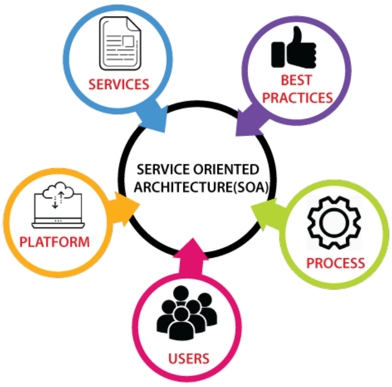
Applications of Service-Oriented Architecture

There are the following applications of Service-Oriented Architecture -

- It is used in the healthcare industry.

- It is used to create many mobile applications and games.
- In the air force, SOA infrastructure is used to deploy situational awareness systems.

The service-oriented architecture is shown below:



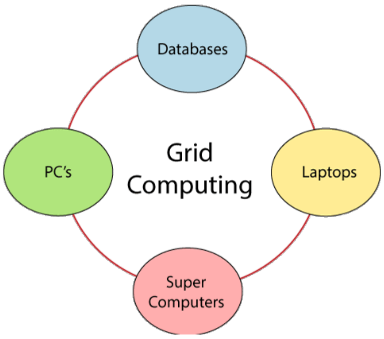
Grid Computing

Grid computing is also known as **distributed computing**. It is a processor architecture that combines various different computing resources from multiple locations to achieve a common goal. In grid computing, the grid is connected by parallel nodes to form a computer cluster. These computer clusters are in different sizes and can run on any operating system.

Grid computing contains the following three types of machines -

1. **Control Node:** It is a group of server which administrates the whole network.
2. **Provider:** It is a computer which contributes its resources in the network resource pool.
3. **User:** It is a computer which uses the resources on the network.

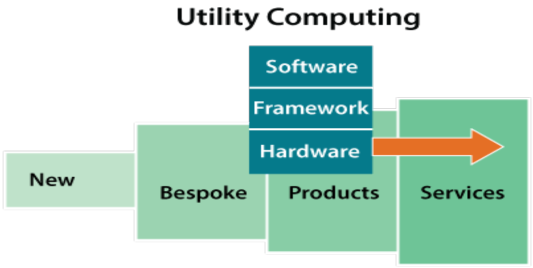
Mainly, grid computing is used in the **ATMs, back-end infrastructures,** and **marketing research**.



Utility Computing

Utility computing is the most trending IT service model. It provides on-demand computing resources (computation, storage, and programming services via API) and infrastructure based on the **pay per use** method. It minimizes the associated costs and maximizes the efficient use of resources. The advantage of utility computing is that it reduced the IT cost, provides greater flexibility, and easier to manage.

Large organizations such as **Google** and **Amazon** established their own utility services for computing storage and application.



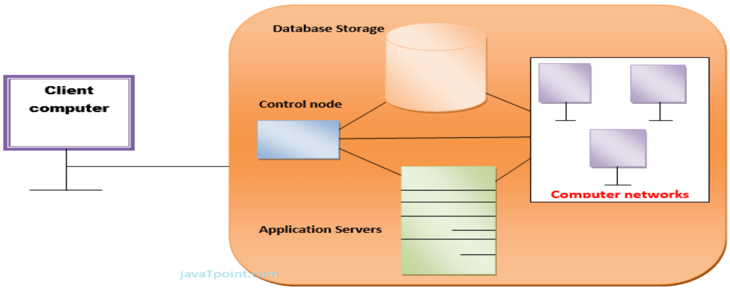
Note: Grid computing, Cloud computing, as well as managed IT services follow the concept of utility computing.

Cloud Computing	Grid Computing
Cloud Computing follows client-server computing architecture.	Grid computing follows a distributed computing architecture.
Scalability is high.	Scalability is normal.
Cloud Computing is more flexible than grid computing.	Grid Computing is less flexible than cloud computing.
Cloud operates as a centralized management system.	Grid operates as a decentralized management system.
In cloud computing, cloud servers are owned by infrastructure providers.	In Grid computing, grids are owned and managed by the organization.
Cloud computing uses services like Iaas, PaaS, and SaaS.	Grid computing uses systems like distributed computing, distributed information, and distributed pervasive.
Cloud Computing is Service-oriented.	Grid Computing is Application-oriented.
It is accessible through standard web protocols.	It is accessible through grid middleware.

How does cloud computing work

Assume that you are an executive at a very big corporation. Your particular responsibilities include to make sure that all of your employees have the right hardware and software they need to do their jobs. To buy computers for everyone is not enough. You also have to purchase software as well as software licenses and then provide these softwares to your employees as they require. Whenever you hire a new employee, you need to buy more software or make sure your current software license allows another user. It is so stressful that you have to spend lots of money.

But, there may be an alternative for executives like you. So, instead of installing a suite of software for each computer, you just need to load one application. That application will allow the employees to log-in into a Web-based service which hosts all the programs for the user that is required for his/her job. Remote servers owned by another company and that will run everything from e-mail to word processing to complex data analysis programs. It is called cloud computing, and it could change the entire computer industry.

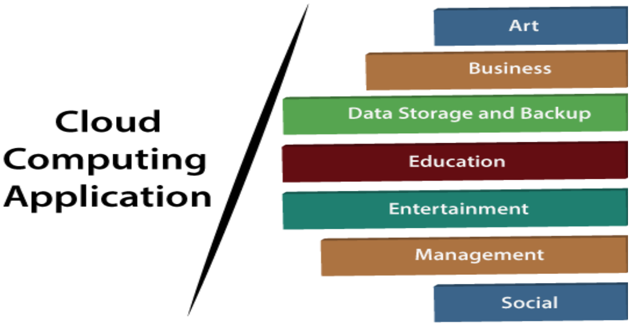


In a cloud computing system, there is a significant workload shift. Local computers have no longer to do all the heavy lifting when it comes to run applications. But cloud computing can handle that much heavy load easily and automatically. Hardware and software demands on the user's side decrease. The only thing the user's computer requires to be able to run is the cloud computing interface software of the system, which can be as simple as a Web browser and the cloud's network takes care of the rest.

Cloud Computing Applications

Cloud service providers provide various applications in the field of art, business, data storage and backup services, education, entertainment, management, social networking, etc.

The most widely used cloud computing applications are given below -



1. Art Applications

Cloud computing offers various art applications for quickly and easily design **attractive cards, booklets,** and **images**. Some most commonly used cloud art applications are given below:

i Moo

Moo is one of the best cloud art applications. It is used for designing and printing business cards, postcards, and mini cards.

ii. Vistaprint

Vistaprint allows us to easily design various printed marketing products such as business cards, Postcards, Booklets, and wedding invitations cards.

iii. Adobe Creative Cloud

Adobe creative cloud is made for designers, artists, filmmakers, and other creative professionals. It is a suite of apps which includes PhotoShop image editing programming, Illustrator, InDesign, TypeKit, Dreamweaver, XD, and Audition.

2. Business Applications

Business applications are based on cloud service providers. Today, every organization requires the cloud business application to grow their business. It also ensures that business applications are 24*7 available to users.

There are the following business applications of cloud computing -

i. MailChimp

MailChimp is an **email publishing platform** which provides various options to **design, send,** and **save** templates for emails.

iii. Salesforce

Salesforce platform provides tools for sales, service, marketing, e-commerce, and more. It also provides a cloud development platform.

iv. Chatter

Chatter helps us to **share important information** about the organization in real time.

v. Bitrix24

Bitrix24 is a **collaboration** platform which provides communication, management, and social collaboration tools.

vi. Paypal

Paypal offers the simplest and easiest **online payment** mode using a secure internet account. Paypal accepts the payment through debit cards, credit cards, and also from Paypal account holders.

vii. Slack

Slack stands for **Searchable Log of all Conversation and Knowledge**. It provides a **user-friendly** interface that helps us to create public and private channels for communication.

viii. Quickbooks

Quickbooks works on the terminology "**Run Enterprise anytime, anywhere, on any device**." It provides online accounting solutions for the business. It allows more than 20 users to work simultaneously on the same system.

3. Data Storage and Backup Applications

Cloud computing allows us to store information (data, files, images, audios, and videos) on the cloud and access this information using an internet connection. As the cloud provider is responsible for providing security, so they offer various backup recovery application for retrieving the lost data.

A list of data storage and backup applications in the cloud are given below -

i. Box.com

Box provides an online environment for **secure content management, workflow,** and **collaboration**. It allows us to store different files such as Excel, Word, PDF, and images on the cloud. The main advantage of using box is that it provides drag & drop service for files and easily integrates with Office 365, G Suite, Salesforce, and more than 1400 tools.

ii. Mozy

Mozy provides powerful **online backup solutions** for our personal and business data. It schedules automatically back up for each day at a specific time.

iii. Joukuu

Joukuu provides the simplest way to **share** and **track cloud-based backup files**. Many users use joukuu to search files, folders, and collaborate on documents.

iv. Google G Suite

Google G Suite is one of the best **cloud storage** and **backup** application. It includes Google Calendar, Docs, Forms, Google+, Hangouts, as well as cloud storage and tools for managing cloud apps. The most popular app in the Google G Suite is Gmail. Gmail offers free email services to users.

4. Education Applications

Cloud computing in the education sector becomes very popular. It offers various **online distance learning platforms** and **student information portals** to the students. The advantage of using cloud in the field of education is that it offers strong virtual classroom environments, Ease of accessibility, secure data storage, scalability, greater reach for the students, and minimal hardware requirements for the applications.

There are the following education applications offered by the cloud -

i. Google Apps for Education

Google Apps for Education is the most widely used platform for free web-based email, calendar, documents, and collaborative study.

ii. Chromebooks for Education

Chromebook for Education is one of the most important Google's projects. It is designed for the purpose that it enhances education innovation.

iii. Tablets with Google Play for Education

It allows educators to quickly implement the latest technology solutions into the classroom and make it available to their students.

iv. AWS in Education

AWS cloud provides an education-friendly environment to universities, community colleges, and schools.

5. Entertainment Applications

Entertainment industries use a **multi-cloud strategy** to interact with the target audience. Cloud computing offers various entertainment applications such as online games and video conferencing.

i. Online games

Today, cloud gaming becomes one of the most important entertainment media. It offers various online games that run remotely from the cloud. The best cloud gaming services are Shaow, GeForce Now, Vortex, Project xCloud, and PlayStation Now.

ii. Video Conferencing Apps

Video conferencing apps provides a simple and instant connected experience. It allows us to communicate with our business partners, friends, and relatives using a cloud-based video conferencing. The benefits of using video conferencing are that it reduces cost, increases efficiency, and removes interoperability.

6. Management Applications

Cloud computing offers various cloud management tools which help admins to manage all types of cloud activities, such as resource deployment, data integration, and disaster recovery. These management tools also provide administrative control over the platforms, applications, and infrastructure.

Some important management applications are -

i. Toggl

Toggl helps users to track allocated time period for a particular project.

ii. Evernote

Evernote allows you to sync and save your recorded notes, typed notes, and other notes in one convenient place. It is available for both free as well as a paid version.

It uses platforms like Windows, macOS, Android, iOS, Browser, and Unix.

iii. Outright

Outright is used by management users for the purpose of accounts. It helps to track income, expenses, profits, and losses in real-time environment.

iv. GoToMeeting

GoToMeeting provides **Video Conferencing** and **online meeting apps**, which allows you to start a meeting with your business partners from anytime, anywhere using mobile phones or tablets. Using GoToMeeting app, you can perform the tasks related to the management such as join meetings in seconds, view presentations on the shared screen, get alerts for upcoming meetings, etc.

7. Social Applications

Social cloud applications allow a large number of users to connect with each other using social networking applications such as **Facebook, Twitter, Linkedln,** etc.

There are the following cloud based social applications -

i. Facebook

Facebook is a **social networking website** which allows active users to share files, photos, videos, status, more to their friends, relatives, and business partners using the cloud storage system. On Facebook, we will always get notifications when our friends like and comment on the posts.

ii. Twitter

Twitter is a **social networking** site. It is a **microblogging** system. It allows users to follow high profile celebrities, friends, relatives, and receive news. It sends and receives short posts called tweets.

iii. Yammer

Yammer is the **best team collaboration** tool that allows a team of employees to chat, share images, documents, and videos.

iv. LinkedIn

LinkedIn is a **social network** for students, freshers, and professionals.

What are the Security Risks of Cloud Computing

Cloud computing provides various advantages, such as improved collaboration, excellent accessibility, Mobility, Storage capacity, etc. But there are also security risks in cloud computing.

Some most common Security Risks of Cloud Computing are given below-

Data Loss

Data loss is the most common cloud security risks of cloud computing. It is also known as data leakage. Data loss is the process in which data is being deleted, corrupted, and unreadable by a user, software, or application. In a cloud computing environment, data loss occurs when our sensitive data is somebody else's hands, one or more data elements can not be utilized by the data owner, hard disk is not working properly, and software is not updated.

Hacked Interfaces and Insecure APIs

As we all know, cloud computing is completely depends on Internet, so it is compulsory to protect interfaces and APIs that are used by external users. APIs are the easiest way to communicate with most of the cloud services. In cloud computing, few services are available in the public domain. These services can be accessed by third parties, so there may be a chance that these services easily harmed and hacked by hackers.

Data Breach

Data Breach is the process in which the confidential data is viewed, accessed, or stolen by the third party without any authorization, so organization's data is hacked by the hackers.

Vendor lock-in

Vendor lock-in is the of the biggest security risks in cloud computing. Organizations may face problems when transferring their services from one vendor to another. As different vendors provide different platforms, that can cause difficulty moving one cloud to another.

Increased complexity strains IT staff

Migrating, integrating, and operating the cloud services is complex for the IT staff. IT staff must require the extra capability and skills to manage, integrate, and maintain the data to the cloud.

Spectre & Meltdown

Spectre & Meltdown allows programs to view and steal data which is currently processed on computer. It can run on personal computers, mobile devices, and in the cloud. It can store the password, your personal information such as images, emails, and business documents in the memory of other running programs.

Denial of Service (DoS) attacks

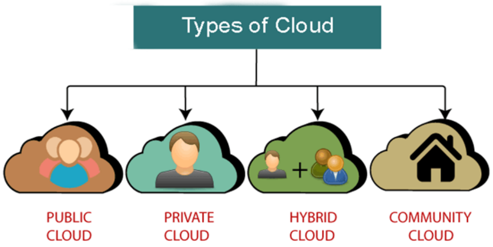
Denial of service (DoS) attacks occur when the system receives too much traffic to buffer the server. Mostly, DoS attackers target web servers of large organizations such as banking sectors, media companies, and government organizations. To recover the lost data, DoS attackers charge a great deal of time and money to handle the data.

Account hijacking

Account hijacking is a serious security risk in cloud computing. It is the process in which individual user's or organization's cloud account (bank account, e-mail account, and social media account) is stolen by hackers. The hackers use the stolen account to perform unauthorized activities.

Types of Cloud

There are the following 4 types of cloud that you can deploy according to the organization's needs-



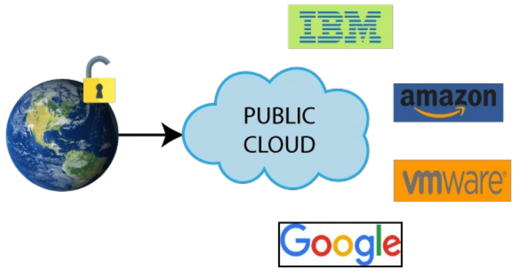
- Public Cloud
- Private Cloud
- Hybrid Cloud
- Community Cloud

Public Cloud

Public cloud is **open to all** to store and access information via the Internet using the pay-per-usage method.

In public cloud, computing resources are managed and operated by the Cloud Service Provider (CSP).

Example: Amazon elastic compute cloud (EC2), IBM SmartCloud Enterprise, Microsoft, Google App Engine, Windows Azure Services Platform.



Advantages of Public Cloud

There are the following advantages of Public Cloud -

- Public cloud is owned at a lower cost than the private and hybrid cloud.
- Public cloud is maintained by the cloud service provider, so do not need to worry about the maintenance.
- Public cloud is easier to integrate. Hence it offers a better flexibility approach to consumers.
- Public cloud is location independent because its services are delivered through the internet.
- Public cloud is highly scalable as per the requirement of computing resources.
- It is accessible by the general public, so there is no limit to the number of users.

Disadvantages of Public Cloud

- Public Cloud is less secure because resources are shared publicly.
- Performance depends upon the high-speed internet network link to the cloud provider.
- The Client has no control of data.

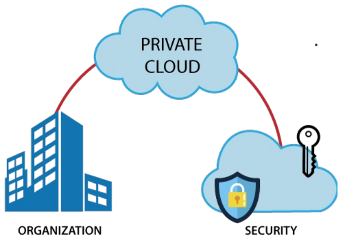
To Read More Click Here

Private Cloud

Private cloud is also known as an **internal cloud** or **corporate cloud**. It is used by organizations to build and manage their own data centers internally or by the third party. It can be deployed using Opensource tools such as Openstack and Eucalyptus.

Based on the location and management, National Institute of Standards and Technology (NIST) divide private cloud into the following two parts-

- On-premise private cloud
- Outsourced private cloud



Advantages of Private Cloud

There are the following advantages of the Private Cloud -

- Private cloud provides a high level of security and privacy to the users.
- Private cloud offers better performance with improved speed and space capacity.
- It allows the IT team to quickly allocate and deliver on-demand IT resources.
- The organization has full control over the cloud because it is managed by the organization itself. So, there is no need for the organization to depends on anybody.
- It is suitable for organizations that require a separate cloud for their personal use and data security is the first priority.

Disadvantages of Private Cloud

- Skilled people are required to manage and operate cloud services.
- Private cloud is accessible within the organization, so the area of operations is limited.
- Private cloud is not suitable for organizations that have a high user base, and organizations that do not have the prebuilt infrastructure, sufficient manpower to maintain and manage the cloud.

To Read More Click Here

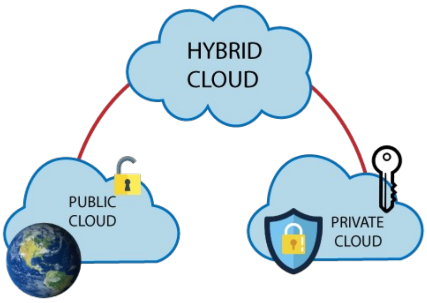
Hybrid Cloud

Hybrid Cloud is a combination of the public cloud and the private cloud. we can say:

Hybrid Cloud = Public Cloud + Private Cloud

Hybrid cloud is partially secure because the services which are running on the public cloud can be accessed by anyone, while the services which are running on a private cloud can be accessed only by the organization's users.

Example: Google Application Suite (Gmail, Google Apps, and Google Drive), Office 365 (MS Office on the Web and One Drive), Amazon Web Services.



Advantages of Hybrid Cloud

There are the following advantages of Hybrid Cloud -

- Hybrid cloud is suitable for organizations that require more security than the public cloud.
- Hybrid cloud helps you to deliver new products and services more quickly.
- Hybrid cloud provides an excellent way to reduce the risk.
- Hybrid cloud offers flexible resources because of the public cloud and secure resources because of the private cloud.

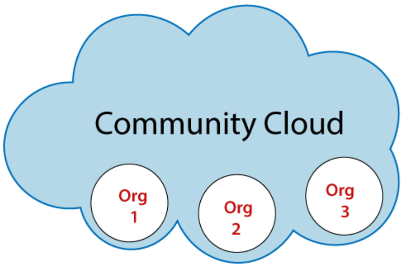
Disadvantages of Hybrid Cloud

- In Hybrid Cloud, security feature is not as good as the private cloud.
- Managing a hybrid cloud is complex because it is difficult to manage more than one type of deployment model.
- In the hybrid cloud, the reliability of the services depends on cloud service providers.

Community Cloud

Community cloud allows systems and services to be accessible by a group of several organizations to share the information between the organization and a specific community. It is owned, managed, and operated by one or more organizations in the community, a third party, or a combination of them.

Example: Health Care community cloud



Advantages of Community Cloud

There are the following advantages of Community Cloud -

- Community cloud is cost-effective because the whole cloud is being shared by several organizations or communities.
- Community cloud is suitable for organizations that want to have a collaborative cloud with more security features than the public cloud.
- It provides better security than the public cloud.
- It provdes collaborative and distributive environment.
- Community cloud allows us to share cloud resources, infrastructure, and other capabilities among various organizations.

Disadvantages of Community Cloud

- Community cloud is not a good choice for every organization.
- Security features are not as good as the private cloud.
- It is not suitable if there is no collaboration.
- The fixed amount of data storage and bandwidth is shared among all community members.

Difference between public cloud, private cloud, hybrid cloud, and community cloud -

The below table shows the difference between public cloud, private cloud, hybrid cloud, and community cloud.

Parameter	Public Cloud	Private Cloud	Hybrid Cloud	Community Cloud
Host	Service provider	Enterprise (Third party)	Enterprise (Third party)	Community (Third party)
Users	General public	Selected users	Selected users	Community members
Access	Internet	Internet, VPN	Internet, VPN	Internet, VPN
Owner	Service provider	Enterprise	Enterprise	Community

Public Cloud

- Public Cloud provides a **shared platform** that is accessible to the **general public** through an Internet connection.
- Public cloud operated on the **pay-as-per-use model** and administrated by the **third party**, i.e., Cloud service provider.
- In the Public cloud, the same storage is being used by multiple users at the same time.
- Public cloud is **owned, managed,** and **operated** by businesses, universities, government organizations, or a combination of them.
- Amazon Elastic Compute Cloud (EC2), Microsoft Azure, IBM's Blue Cloud, Sun Cloud, and Google Cloud are examples of the public cloud.

Advantages of Public Cloud

There are the following advantages of public cloud -

1) Low Cost

Public cloud has a lower cost than private, or hybrid cloud, as it shares the same resources with a large number of consumers.

2) Location Independent

Public cloud is location independent because its services are offered through the internet.

3) Save Time

In Public cloud, the cloud service provider is responsible for the manage and maintain data centers in which data is stored, so the cloud user can save their time to establish connectivity, deploying new products, release product updates, configure, and assemble servers.

4) Quickly and easily set up

Organizations can easily buy public cloud on the internet and deployed and configured it remotely through the cloud service provider within a few hours.

5) Business Agility

Public cloud provides an ability to elastically re-size computer resources based on the organization's requirements.

6) Scalability and reliability

Public cloud offers scalable (easy to add and remove) and reliable (24*7 available) services to the users at an affordable cost.

Disadvantages of Public Cloud

1) Low Security

Public Cloud is less secure because resources are shared publicly.

2) Performance

In the public cloud, performance depends upon the speed of internet connectivity.

3) Less customizable

Public cloud is less customizable than the private cloud.

Private Cloud

- Private cloud is also known as an **internal cloud** or **corporate cloud**.
- Private cloud provides computing services to a **private internal network (within the organization)** and **selected users** instead of the general public.
- Private cloud provides a **high level of security** and **privacy** to data through firewalls and internal hosting. It also ensures that operational and sensitive data are not accessible to third-party providers.
- HP Data Centers, Microsoft, Elastra-private cloud, and Ubuntu are the example of a private cloud.

Advantages of Private cloud

There are the following advantages of Private Cloud -

1) More Control

Private clouds have more control over their resources and hardware than public clouds because it is only accessed by selected users.

2) Security & privacy

Security & privacy are one of the big advantages of cloud computing. Private cloud improved the security level as compared to the public cloud.

3) Improved performance

Private cloud offers better performance with improved speed and space capacity.

Disadvantages of Private Cloud

1) High cost

The cost is higher than a public cloud because set up and maintain hardware resources are costly.

2) Restricted area of operations

As we know, private cloud is accessible within the organization, so the area of operations is limited.

3) Limited scalability

Private clouds are scaled only within the capacity of internal hosted resources.

4) Skilled people

Skilled people are required to manage and operate cloud services.

Hybrid Cloud

- Hybrid cloud is a combination of **public and private** clouds.
  Hybrid cloud = public cloud + private cloud
- The main aim to combine these cloud (Public and Private) is to create a unified, automated, and well-managed computing environment.
- In the Hybrid cloud, **non-critical activities** are performed by the **public cloud** and **critical activities** are performed by the **private cloud**.
- Mainly, a hybrid cloud is used in finance, healthcare, and Universities.
- The best hybrid cloud provider companies are **Amazon, Microsoft, Google, Cisco,** and **NetApp**.

Advantages of Hybrid Cloud

There are the following advantages of Hybrid Cloud -

1) Flexible and secure

It provides flexible resources because of the public cloud and secure resources because of the private cloud.

2) Cost effective

Hybrid cloud costs less than the private cloud. It helps organizations to save costs for both infrastructure and application support.

3) Cost effective

It offers the features of both the public as well as the private cloud. A hybrid cloud is capable of adapting to the demands that each company needs for space, memory, and system.

4) Security

Hybrid cloud is secure because critical activities are performed by the private cloud.

5) Risk Management

Hybrid cloud provides an excellent way for companies to manage the risk.

Disadvantages of Hybrid Cloud

1) Networking issues

In the Hybrid Cloud, networking becomes complex because of the private and the public cloud.

2) Infrastructure Compatibility

Infrastructure compatibility is the major issue in a hybrid cloud. With dual-levels of infrastructure, a private cloud controls the company, and a public cloud does not, so there is a possibility that they are running in separate stacks.

3) Reliability

The reliability of the services depends on cloud service providers.

Community Cloud

Community cloud is a cloud infrastructure that allows systems and services to be accessible by a group of several organizations to share the information. It is owned, managed, and operated by one or more organizations in the community, a third party, or a combination of them.

Example: Our government organization within India may share computing infrastructure in the cloud to manage data.

Advantages of Community Cloud

There are the following advantages of Community Cloud -

Cost effective

Community cloud is cost effective because the whole cloud is shared between several organizations or a community.

Flexible and Scalable

The community cloud is flexible and scalable because it is compatible with every user. It allows the users to modify the documents as per their needs and requirement.

Security

Community cloud is more secure than the public cloud but less secure than the private cloud.

Sharing infrastructure

Community cloud allows us to share cloud resources, infrastructure, and other capabilities among various organizations.

Disadvantages of Community Cloud

There are the following disadvantages of Community Cloud -

- Community cloud is not a good choice for every organization.
- Slow adoption to data
- The fixed amount of data storage and bandwidth is shared among all community members.
- Community Cloud is costly than the public cloud.
- Sharing responsibilities among organizations is difficult.

Cloud Service Models

There are the following three types of cloud service models -

1. Infrastructure as a Service (IaaS)
2. Platform as a Service (PaaS)
3. Software as a Service (SaaS)

Infrastructure as a Service (IaaS)

IaaS is also known as **Hardware as a Service (HaaS)**. It is a computing infrastructure managed over the internet. The main advantage of using IaaS is that it helps users to avoid the cost and complexity of purchasing and managing the physical servers.

Characteristics of IaaS

There are the following characteristics of IaaS -

- Resources are available as a service
- Services are highly scalable
- Dynamic and flexible
- GUI and API-based access
- Automated administrative tasks

Example: DigitalOcean, Linode, Amazon Web Services (AWS), Microsoft Azure, Google Compute Engine (GCE), Rackspace, and Cisco Metacloud.

Platform as a Service (PaaS)

PaaS cloud computing platform is created for the programmer to develop, test, run, and manage the applications.

Characteristics of PaaS

There are the following characteristics of PaaS -

- Accessible to various users via the same development application.
- Integrates with web services and databases.
- Builds on virtualization technology, so resources can easily be scaled up or down as per the organization's need.
- Support multiple languages and frameworks.
- Provides an ability to "**Auto-scale**".

Example: AWS Elastic Beanstalk, Windows Azure, Heroku, Force.com, Google App Engine, Apache Stratos, Magento Commerce Cloud, and OpenShift.

Software as a Service (SaaS)

SaaS is also known as "**on-demand software**". It is a software in which the applications are hosted by a cloud service provider. Users can access these applications with the help of internet connection and web browser.

Characteristics of SaaS

There are the following characteristics of SaaS -

- Managed from a central location
- Hosted on a remote server
- Accessible over the internet
- Users are not responsible for hardware and software updates. Updates are applied automatically.
- The services are purchased on the pay-as-per-use basis

Example: BigCommerce, Google Apps, Salesforce, Dropbox, ZenDesk, Cisco WebEx, ZenDesk, Slack, and GoToMeeting.

Difference between IaaS, PaaS, and SaaS

The below table shows the difference between IaaS, PaaS, and SaaS -

IaaS	Paas	SaaS
It provides a virtual data center to store information and create platforms for app development, testing, and deployment.	It provides virtual platforms and tools to create, test, and deploy apps.	It provides web software and apps to complete business tasks.
It provides access to resources such as virtual machines, virtual storage, etc.	It provides runtime environments and deployment tools for applications.	It provides software as a service to the end-users.
It is used by network architects.	It is used by developers.	It is used by end users.
IaaS provides only Infrastructure.	PaaS provides Infrastructure+Platform.	SaaS provides Infrastructure+Platform +Software.

Infrastructure as a Service | IaaS

Iaas is also known as **Hardware as a Service (HaaS)**. It is one of the layers of the cloud computing platform. It allows customers to outsource their IT infrastructures such as servers, networking, processing, storage, virtual machines, and other resources. Customers access these resources on the Internet using a pay-as-per use model.

In traditional hosting services, IT infrastructure was rented out for a specific period of time, with pre-determined hardware configuration. The client paid for the configuration and time, regardless of the actual use. With the help of the IaaS cloud computing platform layer, clients can dynamically scale the configuration to meet changing requirements and are billed only for the services actually used.

IaaS cloud computing platform layer eliminates the need for every organization to maintain the IT infrastructure.

IaaS is offered in three models: public, private, and hybrid cloud. The private cloud implies that the infrastructure resides at the customer-premise. In the case of public cloud, it is located at the cloud computing platform vendor's data center, and the hybrid cloud is a combination of the two in which the customer selects the best of both public cloud or private cloud.

IaaS provider provides the following services -

1. **Compute:** Computing as a Service includes virtual central processing units and virtual main memory for the Vms that is provisioned to the end- users.
2. **Storage:** IaaS provider provides back-end storage for storing files.
3. **Network:** Network as a Service (NaaS) provides networking components such as routers, switches, and bridges for the Vms.
4. **Load balancers:** It provides load balancing capability at the infrastructure layer.

IaaS
Compute
1
Storage
2
3
Network
Load balancers
4

Advantages of IaaS cloud computing layer

There are the following advantages of IaaS computing layer -

1. Shared infrastructure

IaaS allows multiple users to share the same physical infrastructure.

2. Web access to the resources

Iaas allows IT users to access resources over the internet.

3. Pay-as-per-use model

IaaS providers provide services based on the pay-as-per-use basis. The users are required to pay for what they have used.

4. Focus on the core business

IaaS providers focus on the organization's core business rather than on IT infrastructure.

5. On-demand scalability

On-demand scalability is one of the biggest advantages of IaaS. Using IaaS, users do not worry about to upgrade software and troubleshoot the issues related to hardware components.

Disadvantages of IaaS cloud computing layer

1. Security

Security is one of the biggest issues in IaaS. Most of the IaaS providers are not able to provide 100% security.

2. Maintenance & Upgrade

Although IaaS service providers maintain the software, but they do not upgrade the software for some organizations.

3. Interoperability issues

It is difficult to migrate VM from one IaaS provider to the other, so the customers might face problem related to vendor lock-in.

Some important point about IaaS cloud computing layer

IaaS cloud computing platform cannot replace the traditional hosting method, but it provides more than that, and each resource which are used are predictable as per the usage.

IaaS cloud computing platform may not eliminate the need for an in-house IT department. It will be needed to monitor or control the IaaS setup. IT salary expenditure might not reduce significantly, but other IT expenses can be reduced.

Breakdowns at the IaaS cloud computing platform vendor's can bring your business to the halt stage. Assess the IaaS cloud computing platform vendor's stability and finances. Make sure that SLAs (i.e., Service Level Agreement) provide backups for data, hardware, network, and application failures. Image portability and third-party support is a plus point.

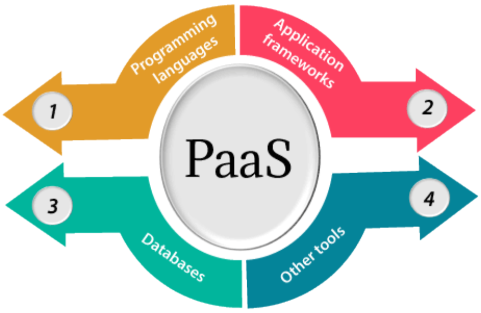
The IaaS cloud computing platform vendor can get access to your sensitive data. So, engage with credible companies or organizations. Study their security policies and precautions.Platform as a Service | PaaS

Platform as a Service (PaaS) provides a runtime environment. It allows programmers to easily create, test, run, and deploy web applications. You can purchase these applications from a cloud service provider on a pay-as-per use basis and access them using the Internet connection. In PaaS, back end scalability is managed by the cloud service provider, so end- users do not need to worry about managing the infrastructure.

PaaS includes infrastructure (servers, storage, and networking) and platform (middleware, development tools, database management systems, business intelligence, and more) to support the web application life cycle.

Example: Google App Engine, Force.com, Joyent, Azure.

PaaS providers provide the Programming languages, Application frameworks, Databases, and Other tools:



1. Programming languages

PaaS providers provide various programming languages for the developers to develop the applications. Some popular programming languages provided by PaaS providers are Java, PHP, Ruby, Perl, and Go.

2. Application frameworks

PaaS providers provide application frameworks to easily understand the application development. Some popular application frameworks provided by PaaS providers are Node.js, Drupal, Joomla, WordPress, Spring, Play, Rack, and Zend.

3. Databases

PaaS providers provide various databases such as ClearDB, PostgreSQL, MongoDB, and Redis to communicate with the applications.

4. Other tools

PaaS providers provide various other tools that are required to develop, test, and deploy the applications.

Advantages of PaaS

There are the following advantages of PaaS -

1) Simplified Development

PaaS allows developers to focus on development and innovation without worrying about infrastructure management.

2) Lower risk

No need for up-front investment in hardware and software. Developers only need a PC and an internet connection to start building applications.

3) Prebuilt business functionality

Some PaaS vendors also provide already defined business functionality so that users can avoid building everything from very scratch and hence can directly start the projects only.

4) Instant community

PaaS vendors frequently provide online communities where the developer can get the ideas to share experiences and seek advice from others.

5)Scalability

Applications deployed can scale from one to thousands of users without any changes to the applications.

Disadvantages of PaaS cloud computing layer

1) Vendor lock-in

One has to write the applications according to the platform provided by the PaaS vendor, so the migration of an application to another PaaS vendor would be a problem.

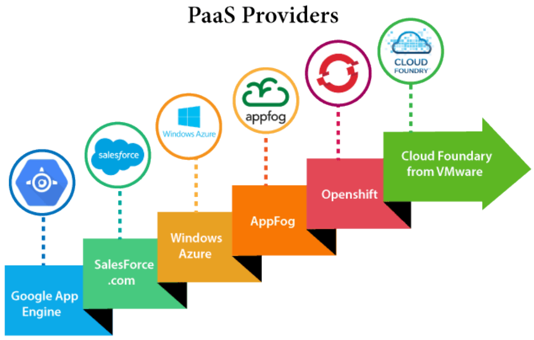
2) Data Privacy

Corporate data, whether it can be critical or not, will be private, so if it is not located within the walls of the company, there can be a risk in terms of privacy of data.

3) Integration with the rest of the systems applications

It may happen that some applications are local, and some are in the cloud. So there will be chances of increased complexity when we want to use data which in the cloud with the local data.

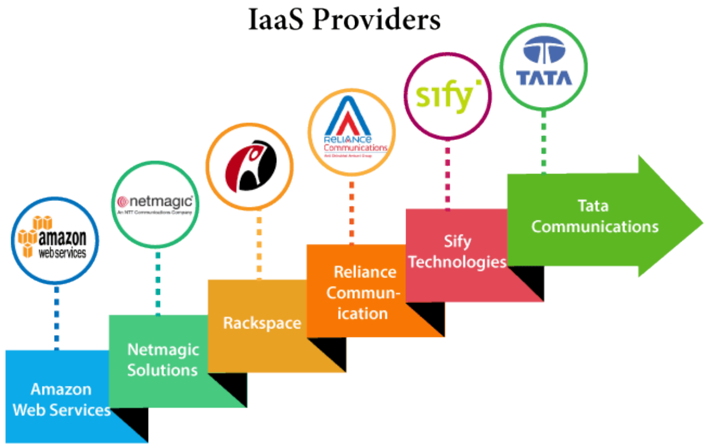
Popular PaaS Providers



The below table shows some popular PaaS providers and services that are provided by them -

Providers	Services
Google App Engine (GAE)	App Identity, URL Fetch, Cloud storage client library, Logservice
Salesforce.com	Faster implementation, Rapid scalability, CRM Services, Sales cloud, Mobile connectivity, Chatter.
Windows Azure	Compute, security, IoT, Data Storage.
AppFog	Justcloud.com, SkyDrive, GoogleDocs
Openshift	RedHat, Microsoft Azure.
Cloud Foundry from VMware	Data, Messaging, and other services.

Top Iaas Providers who are providing IaaS cloud computing platform



IaaS Vendor	Iaas Solution	Details
Amazon Web Services	Elastic, Elastic Compute Cloud (EC2) MapReduce, Route 53, Virtual Private Cloud, etc.	The cloud computing platform pioneer, Amazon offers auto scaling, cloud monitoring, and load balancing features as part of its portfolio.
Netmagic Solutions	Netmagic IaaS Cloud	Netmagic runs from data centers in Mumbai, Chennai, and Bangalore, and a virtual data center in the United States. Plans are underway to extend services to West Asia.
Rackspace	Cloud servers, cloud files, cloud sites, etc.	The cloud computing platform vendor focuses primarily on enterprise-level hosting services.
Reliance Communications	Reliance Internet Data Center	RIDC supports both traditional hosting and cloud services, with data centers in Mumbai, Bangalore, Hyderabad, and Chennai. The cloud services offered by RIDC include IaaS and SaaS.
Sify Technologies	Sify IaaS	Sify's cloud computing platform is powered by HP's converged infrastructure. The vendor offers all three types of cloud services: IaaS, PaaS, and SaaS.
Tata Communications	InstaCompute	InstaCompute is Tata Communications' IaaS offering. InstaCompute data centers are located in Hyderabad and Singapore, with operations in

Software as a Service | SaaS

SaaS is also known as "**On-Demand Software**". It is a software distribution model in which services are hosted by a cloud service provider. These services are available to end-users over the internet so, the end-users do not need to install any software on their devices to access these services.

There are the following services provided by SaaS providers -

Business Services - SaaS Provider provides various business services to start-up the business. The SaaS business services include **ERP** (Enterprise Resource Planning), **CRM** (Customer Relationship Management), **billing**, and **sales**.

Document Management - SaaS document management is a software application offered by a third party (SaaS providers) to create, manage, and track electronic documents.

Example: Slack, Samepage, Box, and Zoho Forms.

Social Networks - As we all know, social networking sites are used by the general public, so social networking service providers use SaaS for their convenience and handle the general public's information.

Mail Services - To handle the unpredictable number of users and load on e-mail services, many e-mail providers offering their services using SaaS.

Business Services
Document Management
1
2
SaaS
3
4
Social Networks
Mail Services

Advantages of SaaS cloud computing layer

1) SaaS is easy to buy

SaaS pricing is based on a monthly fee or annual fee subscription, so it allows organizations to access business functionality at a low cost, which is less than licensed applications.

Unlike traditional software, which is sold as a licensed based with an up-front cost (and often an optional ongoing support fee), SaaS providers are generally pricing the applications using a subscription fee, most commonly a monthly or annually fee.

2. One to Many

SaaS services are offered as a one-to-many model means a single instance of the application is shared by multiple users.

3. Less hardware required for SaaS

The software is hosted remotely, so organizations do not need to invest in additional hardware.

4. Low maintenance required for SaaS

Software as a service removes the need for installation, set-up, and daily maintenance for the organizations. The initial set-up cost for SaaS is typically less than the enterprise software. SaaS vendors are pricing their applications based on some usage parameters, such as a number of users using the application. So SaaS does easy to monitor and automatic updates.

5. No special software or hardware versions required

users will have the same version of the software and typically access it through the web browser. SaaS reduces IT support costs by outsourcing hardware and software maintenance and support to the IaaS provider.

6. Multidevice support

SaaS services can be accessed from any device such as desktops, laptops, tablets, phones, and thin clients.

7. API Integration

SaaS services easily integrate with other software or services through standard APIs.

8. No client-side installation

SaaS services are accessed directly from the service provider using the internet connection, so do not need to require any software installation.

Disadvantages of SaaS cloud computing layer

1) Security

Actually, data is stored in the cloud, so security may be an issue for some users. However, cloud computing is not more secure than in-house deployment.

2) Latency issue

Since data and applications are stored in the cloud at a variable distance from the end-user, there is a possibility that there may be greater latency when interacting with the application compared to local deployment. Therefore, the SaaS model is not suitable for applications whose demand response time is in milliseconds.

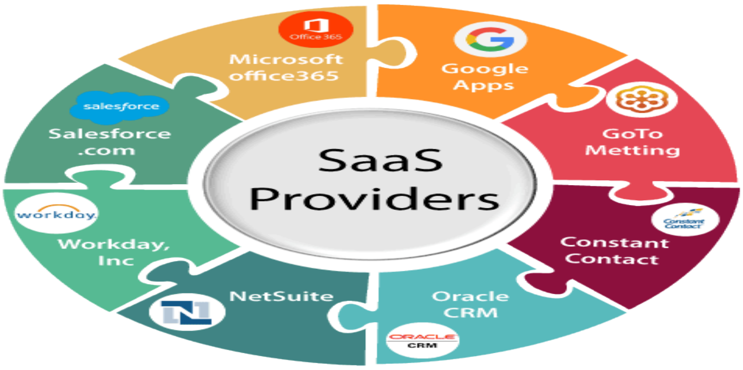
3) Total Dependency on Internet

Without an internet connection, most SaaS applications are not usable.

4) Switching between SaaS vendors is difficult

Switching SaaS vendors involves the difficult and slow task of transferring the very large data files over the internet and then converting and importing them into another SaaS also.

Popular SaaS Providers



The below table shows some popular SaaS providers and services that are provided by them -

Provider	Services
Salseforce.com	On-demand CRM solutions
Microsoft Office 365	Online office suite
Google Apps	Gmail, Google Calendar, Docs, and sites
NetSuite	ERP, accounting, order management, CRM, Professionals Services Automation (PSA), and e-commerce applications.
GoToMeeting	Online meeting and video-conferencing software
Constant Contact	E-mail marketing, online survey, and event marketing
Oracle CRM	CRM applications
Workday, Inc	Human capital management,

Virtualization in Cloud Computing

Virtualization is the "creation of a virtual (rather than actual) version of something, such as a server, a desktop, a storage device, an operating system or network resources".

In other words, Virtualization is a technique, which allows to share a single physical instance of a resource or an application among multiple customers and organizations. It does by assigning a logical name to a physical storage and providing a pointer to that physical resource when demanded.

What is the concept behind the Virtualization?

Creation of a virtual machine over existing operating system and hardware is known as Hardware Virtualization. A Virtual machine provides an environment that is logically separated from the underlying hardware.

The machine on which the virtual machine is going to create is known as **Host Machine** and that virtual machine is referred as a **Guest Machine**

Types of Virtualization:

1. Hardware Virtualization.
2. Operating system Virtualization.
3. Server Virtualization.
4. Storage Virtualization.

1) Hardware Virtualization:

When the virtual machine software or virtual machine manager *(VMM) is directly installed on the hardware system* is known as hardware virtualization.

The main job of hypervisor is to control and monitoring the processor, memory and other hardware resources.

After virtualization of hardware system we can install different operating system on it and run different applications on those OS.

Usage:

Hardware virtualization is mainly done for the server platforms, because controlling virtual machines is much easier than controlling a physical server.

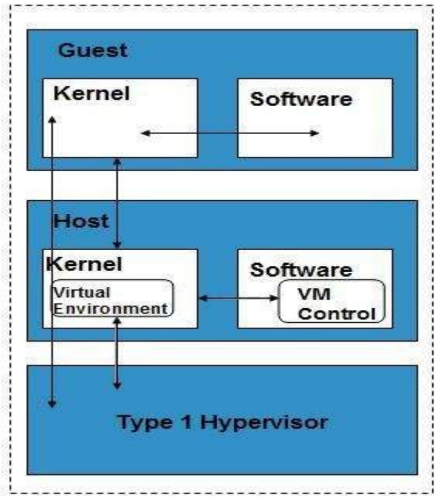
Types of Hardware Virtualization

Here are the three types of hardware virtualization:

- Full Virtualization
- Emulation Virtualization
- Paravirtualization

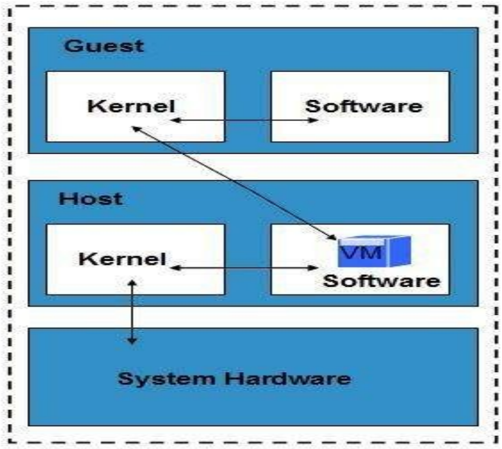
Full Virtualization

In **full virtualization,** the underlying hardware is completely simulated. Guest software does not require any modification to run.



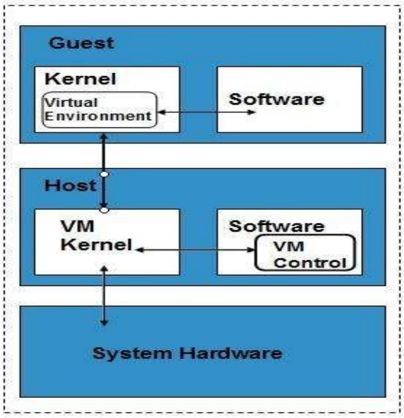
Emulation Virtualization

In **Emulation,** the virtual machine simulates the hardware and hence becomes independent of it. In this, the guest operating system does not require modification.



Paravirtualization

In **Paravirtualization,** the hardware is not simulated. The guest software run their own isolated domains.



VMware vSphere is highly developed infrastructure that offers a management infrastructure framework for virtualization. It virtualizes the system, storage and networking hardware.

2) Operating System Virtualization:

When the virtual machine software or virtual machine manager *(VMM) is installed on the Host operating system* instead of directly on the hardware system is known as operating system virtualization.

Usage:

Operating System Virtualization is mainly used for testing the applications on different platforms of OS.

3) Server Virtualization:

When the virtual machine software or virtual machine manager *(VMM) is directly installed on the Server system* is known as server virtualization.

Usage:

Server virtualization is done because a single physical server can be divided into multiple servers on the demand basis and for balancing the load.

4) Storage Virtualization:

Storage virtualization is the *process of grouping the physical storage from multiple network storage devices so that it looks like a single storage device*.

Storage virtualization is also implemented by using software applications.

Usage:

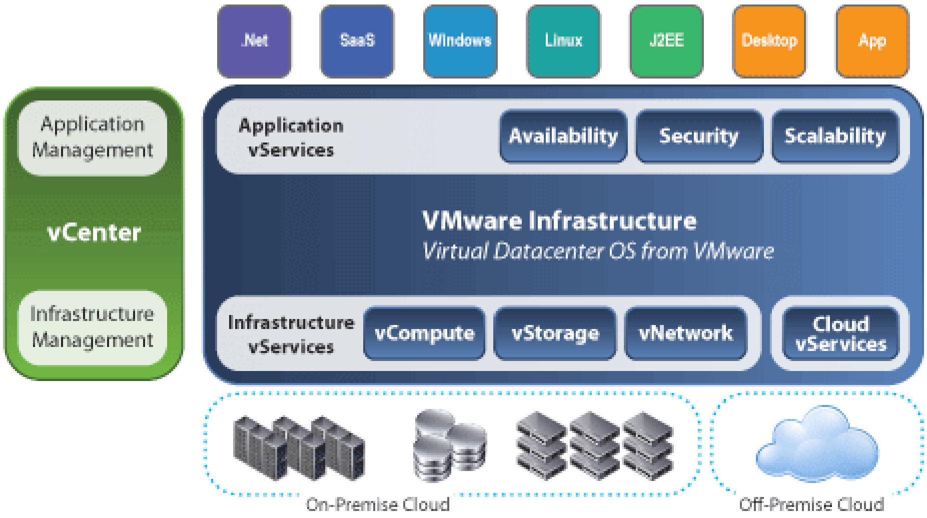
Storage virtualization is mainly done for back-up and recovery purposes.

How does virtualization work in cloud computing?

Virtualization plays a very important role in the cloud computing technology, normally in the cloud computing, users share the data present in the clouds like application etc, but actually with the help of virtualization users shares the Infrastructure.

The **main usage of Virtualization Technology** is to provide the applications with the standard versions to their cloud users, suppose if the next version of that application is released, then cloud provider has to provide the latest version to their cloud users and practically it is possible because it is more expensive.

To overcome this problem we use basically virtualization technology, By using virtualization, all severs and the software application which are required by other cloud providers are maintained by the third party people, and the cloud providers has to pay the money on monthly or annual basis.



Conclusion

Mainly Virtualization means, running multiple operating systems on a single machine but sharing all the hardware resources. And it helps us to provide the pool of IT resources so that we can share these IT resources in order get benefits in the business.

Data Virtualization

Data virtualization is the process of retrieve data from various resources without knowing its type and physical location where it is stored. It collects heterogeneous data from different resources and allows data users across the organization to access this data according to their work requirements. This heterogeneous data can be accessed using any application such as web portals, web services, E-commerce, Software as a Service (SaaS), and mobile application.

We can use Data Virtualization in the field of **data integration, business intelligence,** and **cloud computing**.

Advantages of Data Virtualization

There are the following advantages of data virtualization -

- It allows users to access the data without worrying about where it resides on the memory.
- It offers better customer satisfaction, retention, and revenue growth.
- It provides various security mechanism that allows users to safely store their personal and professional information.
- It reduces costs by removing data replication.
- It provides a user-friendly interface to develop customized views.
- It provides various simple and fast deployment resources.
- It increases business user efficiency by providing data in real-time.
- It is used to perform tasks such as data integration, business integration, Service-Oriented Architecture (SOA) data services, and enterprise search.

Disadvantages of Data Virtualization

- It creates availability issues, because availability is maintained by third-party providers.
- It required a high implementation cost.
- It creates the availability and scalability issues.
- Although it saves time during the implementation phase of virtualization but it consumes more time to generate the appropriate result.

Uses of Data Virtualization

There are the following uses of Data Virtualization -

1. Analyze performance

Data virtualization is used to analyze the performance of the organization compared to previous years.

2. Search and discover interrelated data

Data Virtualization (DV) provides a mechanism to easily search the data which is similar and internally related to each other.

3. Agile Business Intelligence

It is one of the most common uses of Data Virtualization. It is used in agile reporting, real-time dashboards that require timely aggregation, analyze and present the relevant data from multiple resources. Both individuals and managers use this to monitor performance, which helps to make daily operational decision processes such as sales, support, finance, logistics, legal, and compliance.

4. Data Management

Data virtualization provides a secure centralized layer to search, discover, and govern the unified data and its relationships.

Data Virtualization Tools

There are the following Data Virtualization tools -

1. Red Hat JBoss data virtualization

Red Hat virtualization is the best choice for developers and those who are using micro services and containers. It is written in **Java**.

2. TIBCO data virtualization

TIBCO helps administrators and users to create a data virtualization platform for accessing the multiple data sources and data sets. It provides a builtin **transformation** engine to combine non-relational and un-structured data sources.

3. Oracle data service integrator

It is a very popular and powerful data integrator tool which is mainly worked with Oracle products. It allows organizations to quickly develop and manage data services to access a single view of data.

4. SAS Federation Server

SAS Federation Server provides various technologies such as scalable, multi-user, and standards-based data access to access data from multiple data services. It mainly focuses on securing data.

5. Denodo

Denodo is one of the best data virtualization tools which allows organizations to minimize the network traffic load and improve response time for large data sets. It is suitable for both small as well as large organizations.

Industries that use Data Virtualization

- **Communication & Technology**
  In Communication & Technology industry, data virtualization is used to increase revenue per customer, create a real-time ODS for marketing, manage customers, improve customer insights, and optimize customer care, etc.
- **Finance**
  In the field of finance, DV is used to improve trade reconciliation, empowering data democracy, addressing data complexity, and managing fixed-risk income.
- **Government**
  In the government sector, DV is used for protecting the environment.
- **Healthcare**
  Data virtualization plays a very important role in the field of healthcare. In healthcare, DV helps to improve patient care, drive new product innovation, accelerating M&A synergies, and provide a more efficient claims analysis.
- **Manufacturing**
  In manufacturing industry, data virtualization is used to optimize a global supply chain, optimize factories, and improve IT assets utilization.

Hardware Virtualization

Previously, there was *"one to one relationship"* between physical servers and operating system. Low capacity of CPU, memory, and networking requirements were available. So, by using this model, the costs of doing business increased. The physical space, amount of power, and hardware required meant that costs were adding up.

The **hypervisor** *manages shared the physical resources of the hardware between the guest operating systems and host operating system*. The physical resources become abstracted versions in standard formats regardless of the hardware platform. The abstracted hardware is represented as actual hardware. Then the virtualized operating system looks into these resources as they are physical entities.

Virtualization means abstraction. Hardware virtualization is accomplished by abstracting the physical hardware layer by use of a hypervisor or VMM (Virtual Machine Monitor).

When the virtual machine software or virtual machine manager (VMM) or hypervisor software is directly installed on the hardware system is known as hardware virtualization.

The main **job of hypervisor** is to control and monitoring the processor, memory and other hardware resources.

After virtualization of hardware system we can install different operating system on it and run different applications on those OS.

Usage of Hardware Virtualization

Hardware virtualization is mainly done for the server platforms, because controlling virtual machines is much easier than controlling a physical server.

Advantages of Hardware Virtualization

The main benefits of hardware virtualization are more efficient resource utilization, lower overall costs as well as increased uptime and IT flexibility.

1) More Efficient Resource Utilization:

Physical resources can be shared among virtual machines. Although the unused resources can be allocated to a virtual machine and that can be used by other virtual machines if the need exists.

2) Lower Overall Costs Because Of Server Consolidation:

Now it is possible for multiple operating systems can co-exist on a single hardware platform, so that the number of servers, rack space, and power consumption drops significantly.

3) Increased Uptime Because Of Advanced Hardware Virtualization Features:

The modern hypervisors provide highly orchestrated operations that maximize the abstraction of the hardware and help to ensure the maximum uptime. These functions help to migrate a running virtual machine from one host to another dynamically, as well as maintain a running copy of virtual machine on another physical host in case the primary host fails.

4) Increased IT Flexibility:

Hardware virtualization helps for quick deployment of server resources in a managed and consistent ways. That results in IT being able to adapt quickly and provide the business with resources needed in good time.

Hardware Virtualization

Previously, there was *"one to one relationship"* between physical servers and operating system. Low capacity of CPU, memory, and networking requirements were available. So, by using this model, the costs of doing business increased. The physical space, amount of power, and hardware required meant that costs were adding up.

The **hypervisor** *manages shared the physical resources of the hardware between the guest operating systems and host operating system*. The physical resources become abstracted versions in standard formats regardless of the hardware platform. The abstracted hardware is represented as actual hardware. Then the virtualized operating system looks into these resources as they are physical entities.

Virtualization means abstraction. Hardware virtualization is accomplished by abstracting the physical hardware layer by use of a hypervisor or VMM (Virtual Machine Monitor).

When the virtual machine software or virtual machine manager (VMM) or hypervisor software is directly installed on the hardware system is known as hardware virtualization.

The main **job of hypervisor** is to control and monitoring the processor, memory and other hardware resources.

After virtualization of hardware system we can install different operating system on it and run different applications on those OS.

Usage of Hardware Virtualization

Hardware virtualization is mainly done for the server platforms, because controlling virtual machines is much easier than controlling a physical server.

Advantages of Hardware Virtualization

The main benefits of hardware virtualization are more efficient resource utilization, lower overall costs as well as increased uptime and IT flexibility.

1) More Efficient Resource Utilization:

Physical resources can be shared among virtual machines. Although the unused resources can be allocated to a virtual machine and that can be used by other virtual machines if the need exists.

2) Lower Overall Costs Because Of Server Consolidation:

Now it is possible for multiple operating systems can co-exist on a single hardware platform, so that the number of servers, rack space, and power consumption drops significantly.

3) Increased Uptime Because Of Advanced Hardware Virtualization Features:

The modern hypervisors provide highly orchestrated operations that maximize the abstraction of the hardware and help to ensure the maximum uptime. These functions help to migrate a running virtual machine from one host to another dynamically, as well as maintain a running copy of virtual machine on another physical host in case the primary host fails.

4) Increased IT Flexibility:

Hardware virtualization helps for quick deployment of server resources in a managed and consistent ways. That results in IT being able to adapt quickly and provide the business with resources needed in good time.

Software Virtualization

Managing applications and distribution becomes a typical task for IT departments. Installation mechanism differs from application to application. Some programs require certain helper applications or frameworks and these applications may have conflict with existing applications.

Software virtualization is just like a virtualization but *able to abstract the software installation procedure and create virtual software installations*.

Virtualized software is an application that will be "installed" into its own self-contained unit.

Example of software virtualization is *VMware software, virtual box* etc. In the next pages, we are going to see how to install linux OS and windows OS on VMware application.

Advantages of Software Virtualization

1) Client Deployments Become Easier:

Copying a file to a workstation or linking a file in a network then we can easily install virtual software.

2) Easy to manage:

To manage updates becomes a simpler task. You need to update at one place and deploy the updated virtual application to the all clients.

3) Software Migration:

Without software virtualization, moving from one software platform to another platform takes much time for deploying and impact on end user systems. With the help of virtualized software environment the migration becomes easier.

Server Virtualization

Server Virtualization is the process of dividing a physical server into several virtual servers, called **virtual private servers**. Each virtual private server can run independently.

The concept of Server Virtualization widely used in the IT infrastructure to minimizes the costs by increasing the utilization of existing resources.

Types of Server Virtualization

1. Hypervisor

In the Server Virtualization, Hypervisor plays an important role. It is a layer between the operating system (OS) and hardware. There are two types of hypervisors.

- Type 1 hypervisor (also known as bare metal or native hypervisors)
- Type 2 hypervisor (also known as hosted or Embedded hypervisors)

The hypervisor is mainly used to perform various tasks such as allocate physical hardware resources (CPU, RAM, etc.) to several smaller independent virtual machines, called "**guest**" on the host machine.

2. Full Virtualization

Full Virtualization uses a **hypervisor** to directly communicate with the CPU and physical server. It provides the best isolation and security mechanism to the virtual machines.

The biggest disadvantage of using hypervisor in full virtualization is that a hypervisor has its own processing needs, so it can slow down the application and server performance.

VMWare ESX server is the best example of full virtualization.

3. Para Virtualization

Para Virtualization is quite similar to the Full Virtualization. The advantage of using this virtualization is that it is **easier to use**, **Enhanced performance**, and **does not require emulation overhead**. Xen primarily and UML use the Para Virtualization.

The difference between full and pare virtualization is that, in para virtualization hypervisor does not need too much processing power to manage the OS.

4. Operating System Virtualization

Operating system virtualization is also called as system-lever virtualization. It is a **server virtualization technology** that divides one operating system into multiple isolated user-space called **virtual environments**. The biggest advantage of using server visualization is that it reduces the use of physical space, so it will save money.

Linux OS Virtualization and **Windows OS Virtualization** are the types of Operating System virtualization.

FreeVPS, **OpenVZ**, and **Linux Vserver** are some examples of System-Level Virtualization.

Note: OS-Level Virtualization never uses a hypervisor.

5. Hardware Assisted Virtualization

Hardware Assisted Virtualization was presented by **AMD and Intel**. It is also known as **Hardware virtualization**, **AMD virtualization**, and **Intel virtualization**. It is designed to increase the performance of the processor. The advantage of using Hardware Assisted Virtualization is that it requires less hypervisor overhead.

6. Kernel-Level Virtualization

Kernel-level virtualization is one of the most important types of server virtualization. It is an **open-source virtualization** which uses the Linux kernel as a hypervisor. The advantage of using kernel virtualization is that it does not require any special administrative software and has very less overhead.

User Mode Linux (UML) and **Kernel-based virtual machine** are some examples of kernel virtualization.

Advantages of Server Virtualization

There are the following advantages of Server Virtualization -

1. Independent Restart

In Server Virtualization, each server can be restart independently and does not affect the working of other virtual servers.

2. Low Cost

Server Virtualization can divide a single server into multiple virtual private servers, so it reduces the cost of hardware components.

3. Disaster Recovery<

Disaster Recovery is one of the best advantages of Server Virtualization. In Server Virtualization, data can easily and quickly move from one server to another and these data can be stored and retrieved from anywhere.

4. Faster deployment of resources

Server virtualization allows us to deploy our resources in a simpler and faster way.

5. Security

It allows uses to store their sensitive data inside the data centers.

Disadvantages of Server Virtualization

There are the following disadvantages of Server Virtualization -

1. The biggest disadvantage of server virtualization is that when the server goes offline, all the websites that are hosted by the server will also go down.
2. There is no way to measure the performance of virtualized environments.
3. It requires a huge amount of RAM consumption.
4. It is difficult to set up and maintain.
5. Some core applications and databases are not supported virtualization.
6. It requires extra hardware resources.

Uses of Server Virtualization

A list of uses of server virtualization is given below -

- Server Virtualization is used in the testing and development environment.
- It improves the availability of servers.
- It allows organizations to make efficient use of resources.
- It reduces redundancy without purchasing additional hardware components.

Storage Virtualization

As we know that, there has been a strong link between the physical host and the locally installed storage devices. However, that paradigm has been changing drastically, almost local storage is no longer needed. As the technology progressing, more advanced storage devices are coming to the market that provide more functionality, and obsolete the local storage.

Storage virtualization is a major component for storage servers, in the form of functional RAID levels and controllers. Operating systems and applications with device can access the disks directly by themselves for writing. The controllers configure the local storage in RAID groups and present the storage to the operating system depending upon the configuration. However, the storage is abstracted and the controller is determining how to write the data or retrieve the requested data for the operating system.

Storage virtualization is becoming more and more important in various other forms:

File servers: The operating system writes the data to a remote location with no need to understand how to write to the physical media.

WAN Accelerators: Instead of sending multiple copies of the same data over the WAN environment, WAN accelerators will cache the data locally and present the re-requested blocks at LAN speed, while not impacting the WAN performance.

SAN and NAS: Storage is presented over the Ethernet network of the operating system. NAS presents the storage as file operations (like NFS). SAN technologies present the storage as block level storage (like Fibre Channel). SAN technologies receive the operating instructions only when if the storage was a locally attached device.

Storage Tiering: Utilizing the storage pool concept as a stepping stone, storage tiering analyze the most commonly used data and places it on the highest performing storage pool. The lowest one used data is placed on the weakest performing storage pool.

This operation is done automatically without any interruption of service to the data consumer.

Advantages of Storage Virtualization

1. Data is stored in the more convenient locations away from the specific host. In the case of a host failure, the data is not compromised necessarily.
2. The storage devices can perform advanced functions like replication, reduplication, and disaster recovery functionality.
3. By doing abstraction of the storage level, IT operations become more flexible in how storage is provided, partitioned, and protected.

OS Virtualization

With the help of OS virtualization nothing is pre-installed or permanently loaded on the local device and no-hard disk is needed. Everything runs from the network using a kind of virtual disk. This virtual disk is actually a disk image file stored on a remote server, SAN (Storage Area Network) or NAS (Non-volatile Attached Storage). The client will be connected by the network to this virtual disk and will boot with the Operating System installed on the virtual disk.

How does OS Virtualization works?

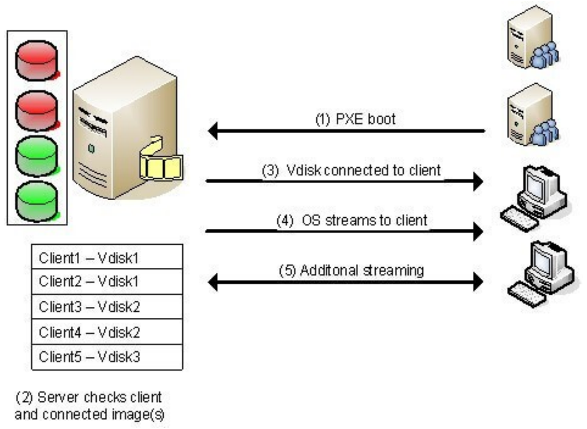
Components needed for using OS Virtualization in the infrastructure are given below:

The first component is the OS Virtualization server. This server is the center point in the OS Virtualization infrastructure. The server manages the streaming of the information on the virtual disks for the client and also determines which client will be connected to which virtual disk (using a database, this information is stored). Also the server can host the storage for the virtual disk locally or the server is connected to the virtual disks via a SAN (Storage Area Network). In high availability environments there can be more OS Virtualization servers to create no redundancy and load balancing. The server also ensures that the client will be unique within the infrastructure.

Secondly, there is a client which will contact the server to get connected to the virtual disk and asks for components stored on the virtual disk for running the operating system.

The available supporting components are database for storing the configuration and settings for the server, a streaming service for the virtual disk content, a (optional) TFTP service and a (also optional) PXE boot service for connecting the client to the OS Virtualization servers.

As it is already mentioned that the virtual disk contains an image of a physical disk from the system that will reflect to the configuration and the settings of those systems which will be using the virtual disk. When the virtual disk is created then that disk needs to be assigned to the client that will be using this disk for starting. The connection between the client and the disk is made through the administrative tool and saved within the database. When a client has a assigned disk, the machine can be started with the virtual disk using the following process as displayed in the given below Figure:



1) Connecting to the OS Virtualization server:

First we start the machine and set up the connection with the OS Virtualization server. Most of the products offer several possible methods to connect with the server. One of the most popular and used methods is using a PXE service, but also a boot strap is used a lot (because of the disadvantages of the PXE service). Although each method initializes the network interface card (NIC), receiving a (DHCP-based) IP address and a connection to the server.

2) Connecting the Virtual Disk:

When the connection is established between the client and the server, the server will look into its database for checking the client is known or unknown and which virtual disk is assigned to the client. When more than one virtual disk are connected then a boot menu will be displayed on the client side. If only one disk is assigned, that disk will be connected to the client which is mentioned in step number 3.

3) VDisk connected to the client:

After the desired virtual disk is selected by the client, that virtual disk is connected through the OS Virtualization server . At the back-end, the OS Virtualization server makes sure that the client will be unique (for example computer name and identifier) within the infrastructure.

4) OS is "streamed" to the client:

As soon the disk is connected the server starts streaming the content of the virtual disk. The software knows which parts are necessary for starting the operating system smoothly, so that these parts are streamed first. The information streamed in the system should be stored somewhere (i.e. cached). Most products offer several ways to cache that information. For examples on the client hard disk or on the disk of the OS Virtualization server.

5) Additional Streaming:

After that the first part is streamed then the operating system will start to run as expected. Additional virtual disk data will be streamed when required for running or starting a function called by the user (for example starting an application available within the virtual disk).

Cloud Service Provider Companies

Cloud Service providers (CSP) offers various services such as **Software as a Service**, **Platform as a service**, **Infrastructure as a service**, **network services**, **business applications**, **mobile applications**, and **infrastructure** in the cloud. The cloud service providers host these services in a data center, and users can access these services through cloud provider companies using an Internet connection.

There are the following Cloud Service Providers Companies -

Amazon Web Services (AWS)

AWS (Amazon Web Services) is a **secure cloud service platform** provided by **Amazon**. It offers various services such as database storage, computing power, content delivery, Relational Database, Simple Email, Simple Queue, and other functionality to increase the organization's growth.

Features of AWS

AWS provides various powerful features for building scalable, cost-effective, enterprise applications. Some important features of AWS is given below-

- AWS is **scalable** because it has an ability to scale the computing resources up or down according to the organization's demand.
- AWS is **cost-effective** as it works on a **pay-as-you-go** pricing model.
- It provides various flexible storage options.
- It offers various **security services** such as infrastructure security, data encryption, monitoring & logging, identity & access control, penetration testing, and DDoS attacks.
- It can efficiently manage and secure Windows workloads.

---

2. Microsoft Azure

Microsoft Azure is also known as **Windows Azure**. It supports various operating systems, databases, programming languages, frameworks that allow IT professionals to easily build, deploy, and manage applications through a worldwide network. It also allows users to create different groups for related utilities.

Features of Microsoft Azure

- Microsoft Azure provides **scalable**, **flexible**, and **cost-effective**
- It allows developers to quickly manage applications and websites.
- It managed each resource individually.
- Its IaaS infrastructure allows us to launch a general-purpose virtual machine in different platforms such as Windows and Linux.
- It offers a **Content Delivery System (CDS)** for delivering the Images, videos, audios, and applications.

---

3. Google Cloud Platform

Google cloud platform is a product of **Google**. It consists of a set of physical devices, such as computers, hard disk drives, and virtual machines. It also helps organizations to simplify the migration process.

Features of Google Cloud

- Google cloud includes various **big data services** such as Google BigQuery, Google CloudDataproc, Google CloudDatalab, and Google Cloud Pub/Sub.
- It provides various services related to **networking**, including Google Virtual Private Cloud (VPC), Content Delivery Network, Google Cloud Load Balancing, Google Cloud Interconnect, and Google Cloud DNS.

- It offers various **scalable** and **high-performance**
- GCP provides various **serverless services** such as Messaging, Data Warehouse, Database, Compute, Storage, Data Processing, and Machine learning (ML)
- It provides a free cloud shell environment with Boost Mode.

---

4. IBM Cloud Services

IBM Cloud is an open-source, faster, and more reliable platform. It is built with a suite of advanced data and AI tools. It offers various services such as Infrastructure as a service, Software as a service, and platform as a service. You can access its services like compute power, cloud data & Analytics, cloud use cases, and storage networking using internet connection.

Feature of IBM Cloud

- IBM cloud improves operational efficiency.
- Its speed and agility improve the customer's satisfaction.
- It offers Infrastructure as a Service (IaaS), Platform as a Service (PaaS), as well as Software as a Service (SaaS)
- It offers various cloud communications services to our IT environment.

---

5. VMware Cloud

VMware cloud is a Software-Defined Data Center (SSDC) unified platform for the Hybrid Cloud. It allows cloud providers to build agile, flexible, efficient, and robust cloud services.

Features of VMware

- VMware cloud works on the **pay-as-per-use** model and **monthly subscription**
- It provides better customer satisfaction by protecting the user's data.
- It can easily create a new VMware **Software-Defined Data Center (SDDC)** cluster on AWS cloud by utilizing a RESTful API.
- It provides flexible storage options. We can manage our application storage on a per-application basis.
- It provides a dedicated high-performance network for managing the application traffic and also supports multicast networking.
- It eliminates the time and cost complexity.

---

6. Oracle cloud

Oracle cloud platform is offered by the **Oracle Corporation**. It combines Platform as a Service, Infrastructure as a Service, Software as a Service, and Data as a Service with cloud infrastructure. It is used to perform tasks such as moving applications to the cloud, managing development environment in the cloud, and optimize connection performance.

Features of Oracle cloud

- Oracle cloud provides various tools for build, integrate, monitor, and secure the applications.
- Its infrastructure uses various languages including, Java, Ruby, PHP, Node.js.
- It integrates with Docker, VMware, and other DevOps tools.
- Oracle database not only provides unparalleled integration between IaaS, PaaS, and SaaS, but also integrates with the on-premises platform to improve operational efficiency.
- It maximizes the value of IT investments.
- It offers customizable Virtual Cloud Networks, firewalls, and IP addresses to securely support private networks.

---

7. Red Hat

Red Hat virtualization is an open standard and desktop virtualization platform produced by Red Hat. It is very popular for the Linux environment to provide various infrastructure solutions for virtualized servers as well as technical workstations. Most of the small and medium-sized organizations use Red Hat to run their organizations smoothly. It offers higher density, better performance, agility, and security to the resources. It also improves the organization's economy by providing cheaper and easier management capabilities.

Features of Rad Hat

- Red Hat provides secure, certified, and updated container images via the Red Hat Container catalog.
- Red Hat cloud includes **OpenShift,** which is an app development platform that allows developers to **access**, **modernize**, and **deploy apps**
- It supports up to 16 virtual machines, each having up to 256GB of RAM.
- It offers better reliability, availability, and serviceability.
- It provides flexible storage capabilities, including very large SAN-based storage, better management of memory allocations, high availability of LVMs, and support for particularly roll-back.
- In the Desktop environment, it includes features like New on-screen keyboard, GNOME software, which allows us to install applications, update application, as well as extended device support.

---

8. DigitalOcean

DigitalOcean is the unique cloud provider that offers computing services to the organization. It was founded in 2011 by Moisey Uretsky and Ben. It is one of the best cloud provider that allows us to manage and deploy web applications.

Features of DigitalOcean

- It uses the KVM hypervisor to allocate physical resources to the virtual servers.
- It provides high-quality performance.
- It offers a digital community platform that helps to answer queries and holding feedbacks.
- It allows developers to use cloud servers to quickly create new virtual machines for their projects.
- It offers one-click apps for droplets. These apps include MySQL, Docker, MongoDB, Wordpress, PhpMyAdmin, LAMP stack, Ghost, and Machine Learning.

---

9. Rackspace

Rackspace offers cloud computing services such as hosting web applications, Cloud Backup, Cloud Block Storage, Databases, and Cloud Servers. The main aim to designing Rackspace is to easily manage private and public cloud deployments. Its data centers operating in the USA, UK, Hong Kong, and Australia.

Features of Rackspace

- Rackspace provides various tools that help organizations to collaborate and communicate more efficiently.
- We can access files that are stored on the Rackspace cloud drive, anywhere, anytime using any device.
- It offers 6 globally data centers.
- It can manage both virtual servers and dedicated physical servers on the same network.
- It provides better performance at a lower cost.

---

10. Alibaba Cloud

Alibaba Cloud is used to develop data management and highly scalable cloud computing services. It offers various services, including Elastic Computing, Storage, Networking, Security, Database Services, Application Services, Media Services, Cloud Communication, and Internet of Things.

Features of Alibaba Cloud

- Alibaba cloud offers a suite of global cloud computing services for both international customers and Alibaba Group's e-commerce ecosystem.
- Its services are available on a pay-as-per-use basis.
- It globally deals with its 14 data centers.
- It offers scalable and reliable data storage.

Network Function Virtualization (NFV) Architecture

Author 5G, Cloud Computing

Classical MNO’s network is crowded with a variety of proprietary hardware elements e.g. routers, switches, Packet Core nodes, and Access nodes. Whenever it wants to launch a new network service it often requires yet another hardware element. Finding the space and power to accommodate this new hardware is becoming increasingly difficult, compounded by the increasing costs of energy, capital investment challenges and the rarity of skills (necessary to design, integrate and operate increasingly complex hardware-based appliances).

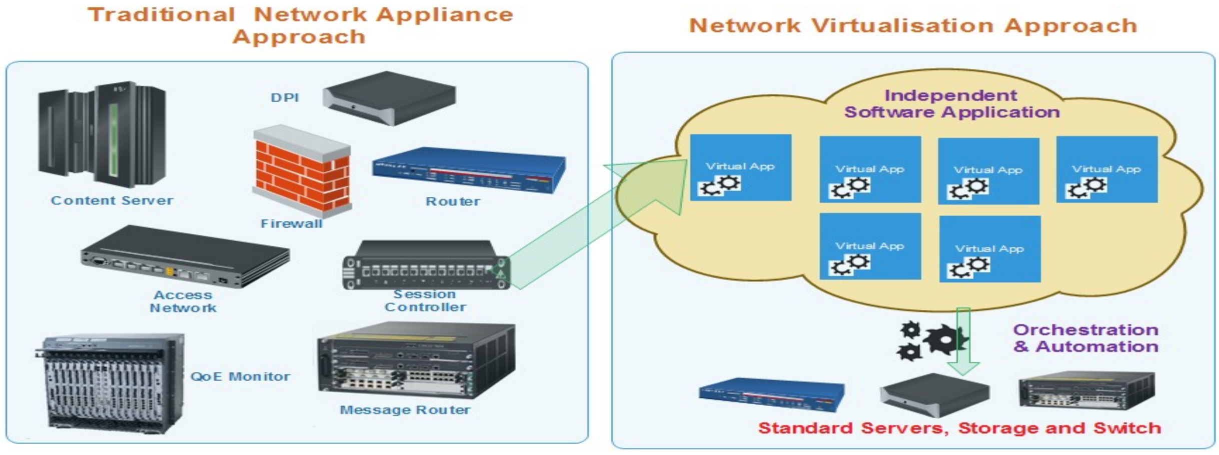
Moreover, hardware-based appliances have an end of life i.e. 5 years or 10 years, which puts an additional burden of a procure-design-integrate-deploy cycle with little or no revenue benefits on the service provider. Hardware life cycles are becoming shorter as technology and services innovation accelerates, slow down the roll out of new revenue earning network services and restricting innovations in a network-centric connected world.

Table of Contents

NFV Definition

The **Network Functions Virtualization** (**NFV**) is a network architecture or concept that utilizes the IT technology fundamentals to virtualize entire network node functions onto industry standard high volume servers, switches and storage, which could be located in Data centers or centralized locations. Network Nodes are in the end user premises to create communication services and illustrated in Figure #1.

It involves implementing network functions in a software that can run on a range of industry standard server hardware, and that can be moved to, or instantiated in, various locations in the network as in when required, without the need to install new hardware equipment.



Traditional Network Appliance Approach
DPI
Content Server
Firewall
Router
Access Network
Session Controller
QoE Monitor
Message Router
Network Virtualisation Approach
Independent Software Application
Virtual App
Virtual App
Virtual App
Virtual App
Virtual App
Virtual App
Orchestration & Automation
Standard Servers, Storage and Switch

Figure #1

ETSI NFVI Architecture

ETSI has created different standards, the one provided below is one of the most important, which illustrates how the NFVI help us to decouple the hardware and software.

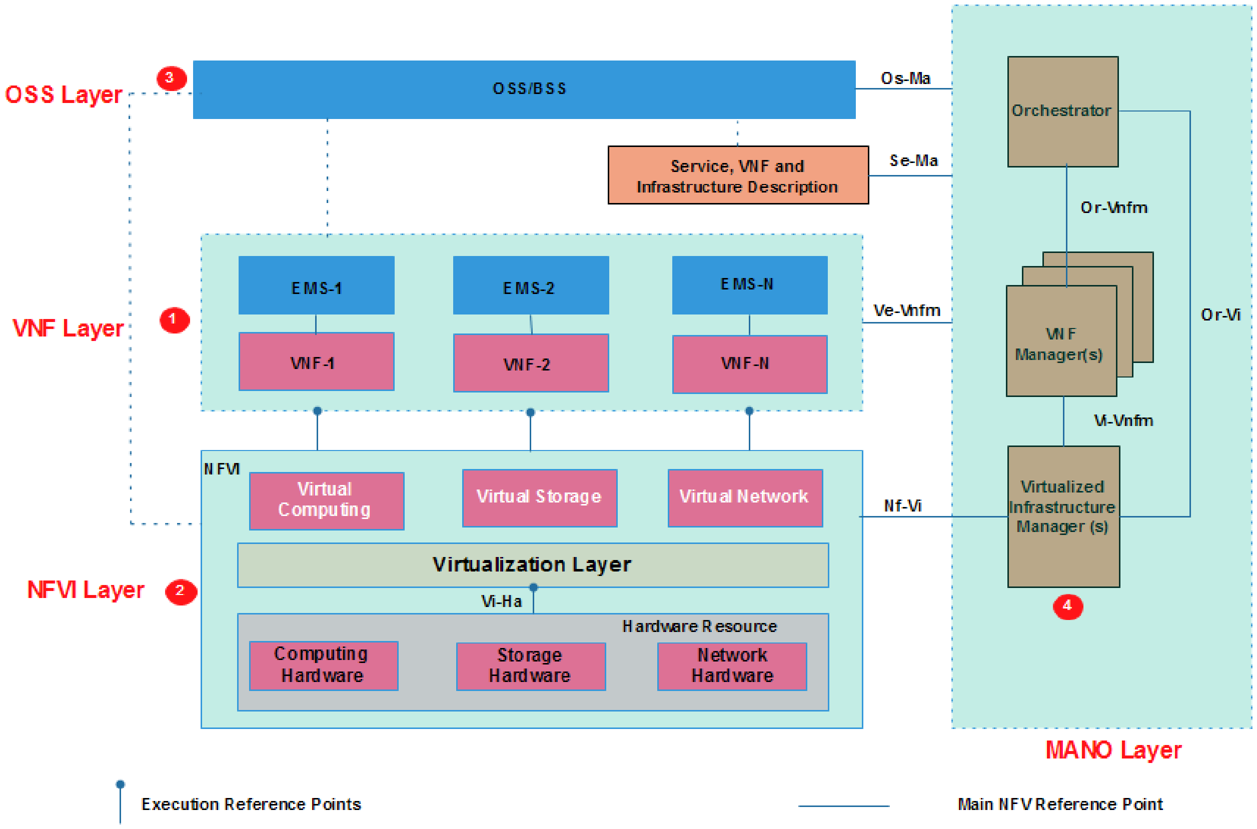


Figure #2

NFV blocks are shown in Figure #2. It can be divided into four layers:

1. Virtualization Network Function (VNF) Layer
2. NFV Infrastructure (NFVI) Layer
3. Operation Support Subsystem (OSS) Layer
4. Management and Orchestration (MANO) Layer

1. Virtualization Network Function (VNF) Layer

It has two subsections **Virtual Network Function** (VNF) and **Element Management System** (EMS)

A **Virtual Network Function** (VNF) is the basic block in NFV Architecture. It virtualized network function. e.g. when a router is virtualized, we call it Router VNF and when a base station is virtual we call it as base station VNF, similarly, it can be DHCP server VNF and Firewall VNF. Even when one sub-function of a network element is virtualized, it is called VNF. For example in Evolved Packet Corer case, various sub-functions like MME, Gateways, and HSS can be separate VNFs which together function as virtual EPC.

A VNFs are deployed on Virtual Machines (VMs). A VNF can be deployed on multiple VMs where each VM hosts a single function of VNF. However, the whole VNF can also be deployed be on a single VM as well.

Element Management System (EMS) is responsible for the functional management of VNF. The management functions include Fault, Configuration, Accounting, Performance and Security Management. An EMS may manage the VNFs through proprietary interfaces. There may be one EMS per VNF or one EMS that can manage multiple VNFs. EMS itself can be deployed as Virtual Network Function (VNF).

2. NFV Infrastructure (NFVI) Layer

NFV Infrastructure is the totality of hardware and software components which build up the environment in which VNFs are deployed, managed and executed. NFV infrastructure physically can span across several locations, the network provides connectivity between these locations to be part of NFV infrastructure.

NFV Infrastructure includes following

- Hardware Resources

- Virtualization Layer
- Virtual Resources

From VNF point of view, the virtualization layer and hardware resources shall be a single entity providing it the desired resource.

Hardware Resource includes computing, storage and network the provides processing, storage and connectivity to VNFs through virtualization (hypervisor) layer. Computing and storage resources are commonly used in a pool.The network resource comprises of switching functions e.g. router, wired or wireless network.

Virtualization Layer also known as **a** hypervisor, it abstracts the hardware resources and decouples the VNF software from the underlying hardware to ensure a hardware independent life cycle for VNFs. It is mainly responsible for following:

- Abstracting and logically partitioning physical resources, commonly as hardware abstraction layer
- Enabling the software to implement the VNF to use the underlying Virtualization Infrastructure
- Providing the virtualised resources to VNF, so that latter can be executed

The virtualization layer in middle ensures VNFs are decoupled from hardware resource and therefore software can be deployed on different physical resources.

Virtual Resources

Virtualization layer abstracts the computing, storage, and network from hardware layer make available as **Virtual Resources.**

3. Operation Support Subsystem (OSS)/Business Support System (BSS) Layer

OSS/BSS refers to OSS/BSS of an operator. OSS deals with network management, fault management, configuration management and service management. BSS deals with customer management, product management and order management etc.

In the NFV architecture, the decoupled BSS/OSS of an operator may be integrated with the NFV Management and Orchestration using standard interfaces.

4. Management and Orchestration (MANO) Layer

Management and Orchestration Layer is also abbreviated as MANO and it includes three components:

- Virtualized Infrastructure Manager(s)
- VNF Manager(s)
- Orchestrator

MANO interacts with both NFVI and VNF layer. MANO layer manages all the resources in the infrastructure layer, it also creates and deletes resources and manages their allocation of the VNFs.

Virtualised Infrastructure Manager (VIM) comprises the functionalities that are used to control and manage the interaction of a VNF with computing, storage and network resources under its authority, as well as their virtualisation. Virtualised infrastructure Manager performs the following:

- Inventory of software, computing, storage and network resources dedicated to NFV infrastructure
- Management of infrastructure resource and allocation e.g. increasing the VMs, increasing energy efficiency etc.
- Allocation of VMs on hypervisors, Compute resources, storage, and relevant network connectivity
- Root cause analysis of performance issues from the NFV infrastructure perspective
- Collection of infrastructure fault information
- Collection of information for capacity planning, monitoring, and optimization

VNF Manager is responsible for VNF life cycle management which includes installation, updates, query, scale up/down and termination. A VNF manager may be deployed for each VNF or a single VNF manager may be deployed to serve multiple VNFs.

Orchestrator is in charge of the orchestration and management of NFV infrastructure and software resources and realizing network services

There is one more independent block know as **Service, VNF and Infrastructure apart** from above building blocks.This includes data-sets that provide information regarding VNF deployment template, VNF forwarding graphs, service related information and NFV infrastructure information models.

Cloud Deployment

What is cloud deployment?

Cloud deployment is the process of deploying an application through one or more hosting models—software as a service (SaaS), platform as a service (PaaS) and/or infrastructure as a service (IaaS)—that leverage the cloud. This includes architecting, planning, implementing and operating workloads on cloud.

What are the business benefits of cloud deployment?

With an effective cloud deployment model, an organization achieves numerous benefits, including:

- **Faster and simplified deployments.** Automate builds that deploy code, databases and application releases, including resource provisioning.
- **Cost savings.** Control costs using consumption-based pricing and eliminate capex-heavy on-premises environments.
- **Platform for growth.** Leverage the global infrastructure provided by cloud service providers (CSPs) to seamlessly expand the business into other geographies.
- **New digital business models.** Exploit the continuous release of features and services by CSPs, incubate new technologies and innovate digital business models.
- **Business resiliency.** Architect for the availability and fault-tolerance CSPs offer and ensure disaster recovery and business continuity of applications to make the business resilient.
- **Agility and scalability.** Use autoscaling and scalability to meet peak demands of the business without provisioning for excess capacity.
- **Geographic reach.** Access applications from any location, on any device, leveraging the connectivity backbone of CSPs.
- **Operational efficiency.** Use the inherent automation enabled by cloud to increase operational efficiency and reduce human effort.
- **A competitive edge.** Leverage infrastructure as code and development, security and operations (DevSecOps) to reduce the time to market for new features and stay ahead of the competition.
- **Empowered users.** Increase productivity by empowering users with self-service options on cloud, such as portals, DevOps pipelines and executive and operational dashboards.

What are some challenges in deploying applications to the cloud?

Some key challenges when migrating applications range from high CapEx for hosting infrastructure to slower deployments, complex and costly migrations, insufficient monitoring methodologies, complex system integrations, dynamic and seasonal workloads, lock-in periods for infrastructure hosting and with application vulnerabilities.

To address these challenges, look for the following in a cloud services provider:

- A cost-saving pay-per-use model
- Rapid provisioning of systems
- Best-in-class technical operations
- Self-services for non-production systems
- Transparent metering and resource inspection
- High-availability solutions integrated with software-as-a-service options, auto-scaling, infrastructure flexibility and portability
- Managed cloud platform security
- A robust cloud management platform

Deployment to the Cloud

Cloud deployment refers to the enablement of SaaS (software as a service), PaaS (platform as a service) or IaaS (infrastructure as a service) solutions that may be accessed on demand by end users or consumers. A cloud deployment model refers to the type of cloud computing architecture a cloud solution will be implemented on. Cloud deployment includes all of the required installation and configuration steps that must be implemented before user provisioning can occur.

SaaS Deployment & Cloud Deployment Models

Cloud deployment can be viewed from the angle of management responsibility for the deployment of the SaaS, PaaS and/or IaaS solutions in question. From this perspective, there are two possible approaches: the cloud solution(s) may be deployed by a third party (under a community cloud, public cloud or private cloud deployment model) or the cloud solution(s) may be deployed by a single entity (under a private cloud deployment model).

SaaS deployment is a type of cloud deployment that is typically initiated using a public cloud or a private cloud deployment model, however SaaS deployment may also be initiated using a hybrid cloud deployment model, when hybrid cloud resources are owned and/or managed by the same entity. Expanding on this theme is the existence of virtual private clouds that can be used for SaaS deployment as well. Virtual private clouds are technically public clouds that function the same as private clouds, since only trusted entities may gain access to the virtual private cloud resources.

Regardless of whether or not a SaaS solution is deployed in a public cloud, a private cloud , a virtual private cloud or a hybrid cloud; many SaaS solutions provide automatic deployment for the cloud services being delivered. SaaS deployment provides many additional benefits over the traditional model of software deployment, including scalability, where application users can be added or subtracted on demand without concerns over capital investments in additional hardware or software. SaaS deployment also provides above average up-time for enterprise applications as compared to on premise software deployment.

After cloud deployment has been completed for a SaaS, PaaS or IaaS solution, user provisioning can occur based on user permissions, where access is provided for cloud resources based on the consumer's classification as either a trusted or untrusted entity. Trusted entities may receive access permission to managed cloud, private cloud or hybrid cloud resources. Untrusted entities may receive access permission to public cloud, managed cloud or hybrid cloud resources. The key difference between trusted and untrusted entities is that untrusted entities never receive access permission to private cloud resources.

How to Build a Private Cloud

If you're nervous about running your business applications on a public cloud, many experts recommend that you opt for a private cloud instead. But building a private cloud within your data center is not just another infrastructure project.

An internal, on-premise private cloud begins with data center consolidation, rationalization of OS, hardware and software platforms, and virtualization up and down the stack servers, storage, and network. Elasticity and pay-as-you-go pricing are guiding principles that allow for the standardization, automation, and commoditization of IT. But it goes beyond infrastructure and provisioning resources. It's also about application building and the user's experience with IT. Despite all the hype, internal clouds are still at an early stage. Only 5% of large enterprises are even capable of running an internal cloud, and only about half of those actually do. If you're interested in being at the forefront of this movement, here's what you need to know about how to build a private cloud.

First Steps: Standardization, Automation, Shared Resources

To go forward with building a private cloud on-premises, you must have standardized and documented procedures for operating, deploying, and maintaining that cloud environment.

Standardized operating procedures that allow efficiency and consistency are critical for automation, which enables self-service capabilities. In terms of the private cloud, self-service means that an enterprise has established an automated workflow whereby resource requests go through an approvals process.

Once approved, the cloud platform automatically deploys the specified environment. Depending on their needs, developers typically specify the parameters for VMs, storage volume, and bandwidth.

Understand Your Services

Many enterprises misguidedly think about building a private cloud from a product perspective before they consider services and service requirements, but services need to be considered first. Whether a workload has affinity with a private, public, or hybrid model depends on a number of attributes, including obvious ones like compliance and security but also things like latency and interdependencies of components in applications.

If you're going to commit to building a private cloud, you need to know what your services are, and what the service-level agreements, costs, and road maps are for each of those. Common services with relatively static interfaces, even if your business is highly reliant on them, are those you should be considering for cloud-style computing. E-mail is one example: You may use it frequently, but instead of wanting it to be integrated tightly with the company, you want to make it as separate as possible, easy to use, and available from self-service interface. If you've customized this type of service over time, you've got to make it as standard as possible. Once you understand which services are right for the cloud and how long it will take to get them to a public-readiness state, you'll be ready to start to look at building a private cloud from a technology perspective.

Four tiers of components for building a private cloud

First is the resource tier comprising infrastructure, platforms, or software. Raw virtualization comes to mind immediately. Rapid re-provisioning technology is another option. Above the resource pool sits the resource management tier, where the pool is managed in an automated manner.

These two levels are fairly mature. Next comes the service management tier. Here you want something that lets you do service governance and convert pools of resources into service levels. You ultimately need to be able to present to the user some kind of service-level interface that says "performance" or "availability" and have the services management tier delivering on that.

Sitting atop it all is the access management tier, which is all about the user self-service interface. It presents a service catalog, gives users all the knobs to turn, and lets you manage subscribers. The interface has to be tied in some way to costing and chargeback, or at least metering"?at that level, it ties to the service management tier.

It’s all about the business

While building a private cloud means you need to think in terms of elasticity, automation, self-service, and chargeback, you shouldn’t be too rigid about the distinctions at this stage of cloud’s evolution. You might get to SaaS eventually, and in the meantime do as much automation as you can, introducing concepts slowly so your organization has time to adapt to the cloud model. The bottom line is, you have to think about the value the cloud will bring to your organization. Cloud platform providers such as Apprenda have been noted for their ability to make multi-tenancy less complex, to make architecture more mature, and to allow businesses to direct their energy toward efficiency and innovation.

Cloud service models and cloud deployment models

Before we start on the actual topic (the Azure platform), we should clarify some terms related to cloud computing. Knowing these concepts, we will then be in a position to identify individual parts of the Azure platform.

Let's start.

Cloud service models

The first term we will look at is **cloud service models**.

All workloads in a cloud scenario use resources from an extremely large resource pool that is operated (managed) by you or a cloud service provider. These resources include servers, storage, networks, applications, services, and much more.

The cloud service models describe to what extent your resources are managed by yourself or by your cloud service providers.

Let's look at the available service models. In the following diagram, you will find a comparison of the models and the existing management responsibilities. Areas that are colored in blue are managed by you: all others are the responsibility of your provider:

The offers are mainly categorized into the following service models:

- **On-premises**: On-premises describes a model in which the user manages all resources alone.
- **Infrastructure as a Service** (**IaaS**): IaaS describes a model in which the cloud provider gives the consumer the ability to create and configure resources from the computing layer upwards. This includes virtual machines, containers, networks, appliances, and many other infrastructure-related resources.
- **Platform as a Service** (**PaaS**): PaaS gives the consumer an environment from the operating system upwards. So the consumer is not responsible for the underlying infrastructure.
- **Software as a Service** (**SaaS**): SaaS is the model with the lowest levels of control and required management. A SaaS application is reachable from multiple clients and consumers, and the owning consumer doesn't have any control over the backend, except for application-related management tasks.

Cloud deployment models

The second term we will look at is **cloud deployment models**.

Cloud deployment models describe the way in which resources are provided in the cloud.

Which cloud deployment models are available?

Let's look at the following diagram first:

The deployment model based on the on-premises service model is called the **private cloud**. A private cloud is an environment/infrastructure, built and operated by a single organization, which is only for internal use.

In the context of this book, you should know that the Windows Azure Pack (a free add-on for the Windows server) gives you the opportunity to deploy Azure technologies in a private cloud environment.

The deployment model based on the IaaS and the PaaS service model is called the **public cloud**. A public cloud is an offer from a service provider (for example, Microsoft Azure), that can be accessed by the public. This includes individuals as well as companies.

> **Note**
>
> Note: When we talk about Azure in this book, it always means the public cloud model.

There is still a third deployment model available, which is the **hybrid cloud**. A hybrid cloud combines parts of the private and public clouds. It is defined as a private cloud environment at the consumer's site, as well as the public cloud infrastructure that the consumer uses.

In the context of this book, you should know that Azure Stack (a new offering from Microsoft) gives you the opportunity to build a hybrid cloud environment:

Choosing a cloud service model

Cloud-service model can be chosen from the *cloud stack*, which comprises of a *trio of cloud computing (also distinct business) models*, that are differentiated on the basis of key players, resources, value-created, costs, and revenue streams:

Software as a Service (SaaS) is a model where the software application is delivered as a service over the internet, and businesses access the service through a web browser. The great advantage of this model is the ability to serve multiple businesses from a virtual environment, and the ease of delivering any changes, upgrades, and modifications to the software through a click-to-deploy model. In a SaaS model, businesses don’t get locked into expensive long-term contracts for software support and maintenance, and the vendor secures a recurring stream of subscription revenue, which is valued far more than one-time licensing income.

Platform as a Service (PaaS) is a service model that provides a virtual platform to develop, deploy, and manage application lifecycle for solutions that are consumed over the internet. In this model of cloud computing, one can access on-demand environment for rapid development, testing, delivery and maintenance of software applications, in other words the entire platform from software development to delivery. PaaS caters to the engineering /product development needs of a business, and is a variant of SaaS with additional architectural and utility components, and is typically used for rapid development and deployment of mobile and web-based apps.

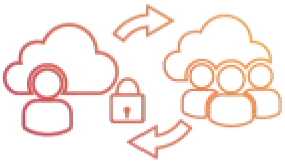
Infrastructure as a Service (IaaS) is the most basic cloud-service model that provides computing infrastructure (servers, storage, network bandwidth, software licenses etc.), as a service in a subscription mode. IaaS serves the needs of the IT organization, and dispenses with the need for businesses to make upfront investments in the technology infrastructure. This is an asset-light model, where businesses don’t have to worry about technology obsolescence, as it is the responsibility of the service provider to ensure flexibility and scalability of the technology infrastructure.

Choosing a cloud-deployment model

An appropriate *cloud-deployment model* must be selected for delivering your cloud services:

Private Cloud, is a mode of deployment where the cloud computing infrastructure is operated exclusively for a single business or customer. In this model, cloud computing services are delivered through a private network, and the associated infrastructure can be either located physically with the business or can also be hosted by a third-party service provider.

Public Cloud, is where the computing services are delivered and accessed through a public network that is open for all. In this deployment model, a third-party service provider owns and supports all the underlying infrastructure including all hardware, software, and network bandwidth. *Amazon Web Services (AWS), Microsoft Azure, and Google Cloud* are some of the well-known Public Clouds.



Hybrid cloud is a composition of two or more clouds (*private, community or public*) that remain distinct entities but are bound together, offering the benefits of multiple deployment models. In this deployment model, sharing of the underlying infrastructure and seamless service delivery across public and private networks is facilitated by technology. Hybrid cloud is increasingly becoming popular for its flexibility, and for some businesses, offers the added comfort of*multi-tiered security and data protection*.

Cloud Deployment Models: Explaining and Comparing the 5 Main Models

What are cloud deployment models?

A cloud deployment model defines where the servers you're using are and who manages them. It defines what your cloud infrastructure looks like, what you can change yourself, and whether the services are provided to you or you need to build everything yourself. Cloud deployment models also define relationships between the infrastructure and your users (what users are allowed to change or implement).

Whenever you hear about the "cloud" or "cloud computing," you think about computing resources that someone else manages. But that's just one of the few cloud deployment models. There are others, too. Typically, when we talk about the cloud, we mean the "public cloud." That's one of the cloud deployment models in which a cloud provider owns and manages all the servers (and other hardware resources).

However, say you use a public cloud but also have some physical servers you own, and you wish to use both as one system. Then we're talking about a "hybrid cloud"—another cloud deployment model. Even if you don't use the public cloud at all, you could still have "a cloud." Your own data center could become a "private cloud" if deployed and managed in a specific way.

All of these options are different cloud deployment models. Basically, the way you use and provision your cloud infrastructure defines which cloud deployment model you use. But it's important to mention that from the user's perspective, there should be little difference between all models. For example, a "private cloud" in your data center has to provide similar options and features as a public cloud. Similarly, if you use a public cloud and your own data center separately, then it's not a hybrid cloud.

Why are there different cloud deployment models?

You may ask, why do we have all these different cloud deployment models, and which one is good for me? Well, we have these models because cloud computing is very efficient and has become very popular.

At the same time, companies try to use their existing data centers with the same efficiency and features. Some companies can't just move to the public cloud for different reasons. For example, compliance and data protection laws may bar them from using the public cloud. Or they may be reluctant to move to the public cloud simply because they previously spent gobs of money on their own servers, and they want to get use out of them. That's why we have a few cloud deployment models to facilitate all the possible scenarios.

To determine which cloud deployment model could be suitable for you, we need to understand all five models first.

1. Public cloud

The public cloud deployment model is the most popular type of cloud. It's also the one that people think about when they say "cloud." The basic principle is that with a public cloud, you don't own any hardware. All the resources are provided to you by a cloud service provider. So to start using the public cloud, the only thing you need to do is to create an account. "Public" in this model means that such a cloud is available for the general public, and resources are shared between all users.

The biggest advantages of the public cloud are scalability, efficiency, and that you don't need to purchase your own hardware. Imagine you build a platform that occasionally experiences a high load. Without a cloud, you'd have to make some sacrifices. One option would be to buy enough servers to handle the load at peak. But that would mean that most of the time, all those servers would be underutilized. Another option would be to buy only enough servers to handle the average load, but then your application would be performing poorly with occasional spikes. With the public cloud, you can have both—enough resources for load spikes without significant upfront investments. In addition, **you're billed only for the resources you use**, and you can provision resources on an ad-hoc basis when needed and even have load-based autoscaling. Cloud providers also offer many public cloud services besides simple virtual machines and storage.

Amazon Web Services (AWS), Microsoft Azure, IBM Cloud, and Google Cloud are just a few examples of a public cloud.

2. Private cloud

The private cloud deployment model is the opposite of the public cloud. It's a dedicated environment for one user (customer). You don't share the hardware with any other users—in fact, most commonly, all the hardware is yours. What's the difference between a "typical/ordinary" on-premises data center and a private cloud, then? The difference is in the way you manage all the hardware.

A private cloud is when you manage your data center in a similar way as the public cloud providers do. You create an abstraction layer on top of your physical servers. This gives you flexibility similar to a public cloud. If you add new servers to your data center, with a private cloud you won't have to worry about configuring them—they'll (semi)automatically become a part of the cluster. You can also get a private cloud from a public cloud provider. This means that a cloud provider will isolate some resources from its cloud and make them available only to you. But no matter if you have your private cloud in your data center or from a cloud provider, the point is that resources are dedicated to a single organization.

Red Hat OpenStack, Rackspace, IBM Bluemix Private Cloud, Microsoft Azure Stack, and VMware Private Cloud are a few examples of a private cloud.

3. Hybrid cloud

As you may have guessed, a hybrid cloud deployment model is the combination of a public and private cloud. It's the second most popular model since many companies already have some hardware of their own and would like to use it. Creating a hybrid cloud means that a company is using the public cloud but also owns on-premises systems, and there is a connection between the two. They work as one system. This is a very useful model that allows for a smooth transition into the public cloud over a longer period of time. Due to security requirements or data protection, some companies can't operate only in the public cloud, so they may choose the hybrid cloud to combine the requirements with the benefits of a public cloud. They run mission-critical applications with sensitive data on-premises while having all the rest in the public cloud.

4. Multi-cloud

Another cloud deployment model on our list is multi-cloud. In this model, as the name suggests, we’re talking about using more than one cloud provider at a time. It’s similar to the hybrid cloud deployment model, where you use both the public and private cloud. In multi-cloud, however, instead of combining private with public, you’d use more than one public cloud. Why would you do that, you ask? Mainly for redundancy. Public cloud providers offer many options to increase the reliability of their services, but accidents still happen. It’s very unlikely you’d have an incident at the same time in two different clouds. Therefore, multi-cloud deployment gives you even better high availability of your services. Another reason for using multi-cloud is when you need a specific service from public cloud X and another specific service from public cloud Y.

5. Community cloud

The last cloud deployment model we’ll discuss is a community cloud. Maybe you haven’t even heard about it before, and there’s a reason for that. This cloud is dedicated to a few organizations from the same “community.” Thus, it’s not a public cloud because it’s not open for everyone, but it’s also not a private cloud because there is more than one user/organization using it. An example of a community cloud could be a cloud that a few different banks use. The biggest advantage of a community cloud is the fact that it can be tailored to requirements for a specific “community.”

Cloud service models

So far, we’ve discussed different cloud deployment models. They define how you provision and manage hardware. But no matter how you do this part, there are different cloud service models available as the next step for your cloud environment.

What does it mean? Imagine that you need, for example, a MySQL server in a cloud environment. You could create a virtual machine and install MySQL on it yourself. You would have to take care of all the configurations and upgrades in the future. Another option would be to request a MySQL server directly from the cloud service provider. A cloud service provider would install, configure, and manage a MySQL server for you. These are two examples of cloud service models.

Simply put, the cloud service model defines which layer of service you manage and which layer the cloud service provider manages. All the models have their pros and cons, so let’s discuss all three so you can decide which one is best for you. Also, we need to mention here that you don’t need to pick one service model for everything. You can pick different models for different components of your cloud infrastructure.

Infrastructure as a Service (IaaS)

IaaS is a cloud service model in which the cloud provider manages the hardware (servers, storage, and networking), and you manage the rest. It means that you don’t have to worry about placing servers in the data center. Nor do you have to worry about connecting those servers to the network and attaching any storage to them. Basically, the cloud provider will make sure that the hardware is ready to use. You’ll get a virtual machine with the operating system you pick. You’ll have full access to the machine on the OS level and full control over what software to install on it. When you create computing resources, for example, on AWS, Oracle Cloud Infrastructure, Google Cloud, Azure, etc., that’s IaaS.

What are the advantages of IaaS? Simplicity and flexibility are the biggest. With one click of a button, you can get a virtual machine ready to be used within a matter of minutes. Do you need to reinstall the operating system? Another few simple clicks or API calls, and your machine is ready again. Another advantage: since you have full control over such a machine, you can configure it as you like or install any custom software you may need. With IaaS you can pretty much clone any existing IT infrastructure, creating, for example, test environments or disaster recovery solutions. Cons? Well, you have to maintain everything yourself. If you only need a MySQL server, you have to secure your operating system, install your MySQL server, and configure it.

Platform as a Service (PaaS)

PaaS is when you don’t manage the operating system and software installed on it. In PaaS, a cloud provider also manages these. You’re getting ready to use a cloud platform—for example, managed Kubernetes or Kafka. In this model, you’re not limited to one specific application (for example, if you get PaaS Kubernetes, you can deploy anything you want on it), but you are limited to one specific platform. The biggest advantage of the PaaS model is that you don’t have to handle all the installation and maintenance efforts of the cloud platform. Installing and configuring a Kubernetes or Kafka cluster can take a few hours. With PaaS, you can get it in a few minutes. Cons? Since a cloud provider manages the platform, you’re a bit limited. It may not be possible to get a very specific, customized configuration for your platform.

Software as a Service (SaaS)

SaaS provides you with an even higher level of abstraction. With SaaS, a cloud provider manages pretty much all layers of cloud infrastructure. For example, consider managed databases. If you use SaaS MySQL, you only need to care about the data in that database. You neither need to create a virtual machine nor install MySQL on it. All of that (together with future upgrade and maintenance) will be done by a cloud provider.

The difference between PaaS and SaaS is that SaaS limits you to one specific application (as mentioned, MySQL). The advantage of SaaS is that it offloads most of the engineering effort from you. You literally can just deploy a MySQL database and start writing data to it in a matter of minutes. With PaaS, you get a platform that does nothing on its own. It only enables you to create something on the platform. With SaaS, you don't need to do anything else to start using it. The disadvantage is that usually, SaaS offerings are a bit more expensive since the cloud provider needs to do all that work for you.

Deploying to the cloud

Now that you know all the cloud deployment models and cloud service models, let's talk about software deployment. At the end of the day, that's what really matters. Picking the right cloud deployment model and service model helps you use the resources optimally. But the business benefits come from effective software deployment. It won't matter that you can deploy a platform in mere minutes if your deployment process takes an hour.

There are a few ways you can deploy your software. Nowadays, the ability to deploy software quickly and often creates real business value. Companies that can't deploy new features or bug fixes at least once daily will fall behind the competition. Some companies are afraid to deploy software so often. This is due to possible issues and downtime. They choose the safer option of deploying less often with more testing and preparation upfront.

But avoiding downtime and unexpected problems doesn't mean you won't be able to deploy often. There are ways of deploying software often and safely. Both canary launches and dark launches let you limit the risk of the new deployment. The canary launch means that you deploy new software to only a small percentage of users first. You test whether everything works correctly, then gradually roll out the change to the rest of the users. This way, if something goes wrong, it affects only a small percentage of users.

A canary launch is a type of a dark launch. But a dark launch can also include deploying a feature to production for internal testers while hiding the feature from users. The very basic example of the dark launch of a new homepage `index.html` would be to deploy it with a different name, like `index-v2.html`. All users would still access `index.html` while you, and maybe your testing team, would use `index-v2.html`. As you can see, the risk of deploying software can be greatly minimized.

LaunchDarkly's feature management platform allows teams to use feature flags to perform dark launches and canary launches on a large scale and with a great deal of sophistication.

Summary

The cloud has changed drastically over the years. At first, it was just an exotic option without many variations. Today it comes in many flavors, and it's even possible to create your own private cloud in your data center. You learned about different cloud deployment models and cloud service models available. It's important to remember that, nowadays, the public cloud isn't the only option. In fact, for some, running a private cloud in your own data center is probably the best way to manage your IT infrastructure. No matter what cloud deployment model will suit you best, you still need to pick the right software deployment method. To make good decisions here, learn how to deploy software to the cloud fast and fearlessly via canary launches and dark launches (enabled by LaunchDarkly). Also, learn how to use LaunchDarkly feature flags to perform smooth, uneventful database migrations to the cloud.

Difference Between Private Cloud and Data Center

• Categorized under Business,Technology | Difference Between Private Cloud and Data Center

Advances in technology and its use in furthering business have left business owners with no option but to look for platforms to meet their business goals. This has brought platforms such as private cloud and data center into the limelight with the business owners left to decide which one works best for them. But what exactly is private cloud and data center? Let us look at their differences and applicability below.

What is Private Cloud?

A private cloud refers to computing services offered over the internet but only for a single customer instead of the general public. It is also referred to as a corporate or internal cloud. Data privacy is provided through firewalls and internal hosting. Third-party providers are denied access to operational and sensitive data.

Features of a Private Cloud

Cloud computing refers to the availability of computer systems and resources on the internet instead of locally on your computer such as storage.

- Businesses benefit from cloud computing in terms of its scalability, availability, instant provisioning, virtualized resources, and storage.
- Cloud computing is divided into three: private, hybrid, and public cloud computing. Hybrid cloud refers to as mixed computing, storage, and services environment. It combines both private and public cloud computing. Public cloud computing refers to computing services offered by a third-party provider and shared with multiple organizations using the public internet. These offer different kinds of software and their security is different.
- Private cloud, as for all cloud computing, is off-premise meaning data is stored online on the internet so that a user can access it whenever necessary.
- Private cloud allows restricted use to a single customer meaning other people cannot access the data, unlike public cloud where anyone can access the data.
- Private cloud offers certain security advantages over the other two types of cloud computing, though it still poses some security risks such as outdated VM images, rogue admins/ service providers, and data loss.
- Data maintenance is done by service providers in the private cloud.

What is Data center?

A data center refers to a large group of networked servers usually in a building or a space between buildings that organizations use for storage and distribution of data and applications. Its components include switches, servers, routers, storage systems, firewalls, and application delivery controllers.

Features of a Data Center

- A data center is on-premise computing meaning software and applications are stored locally in the organization’s database and are present near the organization.
- Only the organization can access the data meaning the data is more secure in a data center compared to the cloud.
- Data maintenance is done by developers within an organization who are trained on how to maintain the organization’s database. These developers are often updated on new development to cope with any technological changes that may suffice over time.
- The servers in data centers are expensive to install, unlike cloud computing which is available on the internet.

Similarities of a Private Cloud and a Data Center

- They are both avenues through which data is stored and made available to users.
- Both platforms are maintained by trained IT experts; private cloud by service providers, data center by developers.
- Both the private cloud and data center offer services to one user, Private cloud for a single customer and data center for one particular organization.
- They are both advances in technology and can be used to benefit businesses.

Differences between private cloud and data center

Location

A private cloud is off-premise while a data center is on-premise. A private cloud is off-premise because it’s accessed from the internet. A data center is on-premise as the applications are located near the organization.

Object 3

Scalability

A private cloud is easily scalable requiring only a small amount of investment while a data center is not easily scalable and needs a huge investment of servers.

User-friendliness

A private cloud environment is simple and easily understandable even for non-professionals while data center architectural design is not easy and is only understood by developers.

Costs

Private cloud has low costs as there’s no need for physical servers while data center incurs high costs of the server installation.

Maintenance

In a private cloud, maintenance is done by service providers while in a data center maintenance is done by developers who manage the organization’s database.

Performance and reliability

Performance and reliability in a private cloud are dependent on the cloud provider while in a data center performance is dependent on the organization.

Security

Though a private cloud is said to be fairly secure, there are still some possible security risks with its use. It is therefore not recommended for critical projects. A data center, on the other hand, is more secure. Hence, it’s recommended for critical projects.

Availability

Private cloud services are available immediately after subscription while the data center takes time to install. It is therefore not easily available after the subscription.

Upgrades

For the Private cloud, upgrades are more automatic from the internet while in the data center upgrades can take time and cause an interruption in business.

Storage considerations

Large amounts of data can be stored in a private cloud. It’s recommended to store small amounts of data in a data center as it takes more time to store large amounts of data.

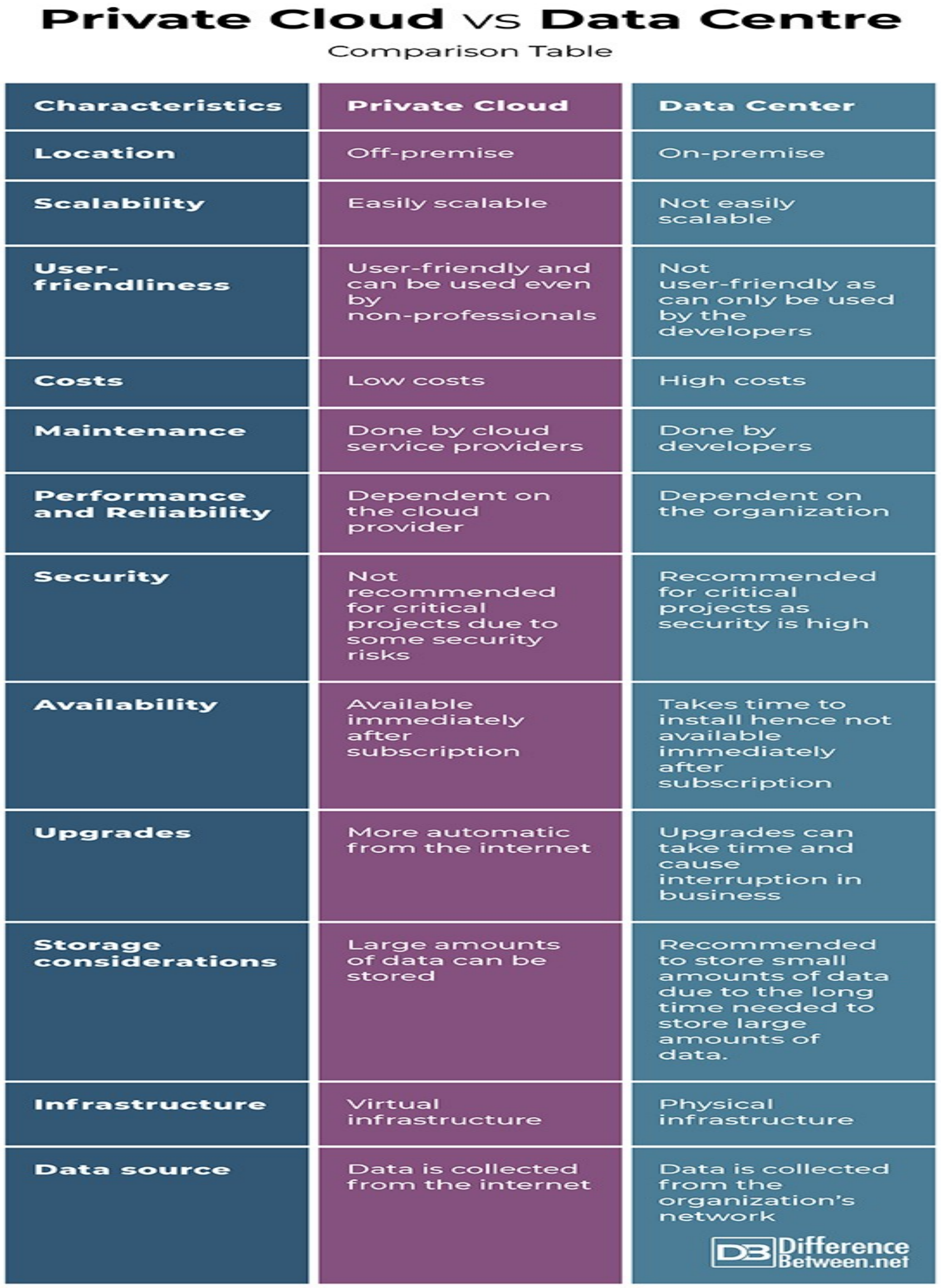
Infrastructure

A private cloud is a virtual infrastructure while a data center is physical infrastructure.

Data Source

In the private cloud data is collected from the internet. In the data center, data is collected from the organization’s network.

Private Cloud vs. Data Centre: Comparison Table



Private Cloud vs Data Centre

Comparison Table

Characteristics	Private Cloud	Data Center
Location	Off-premise	On-premise
Scalability	Easily scalable	Not easily scalable
User-friendliness	User-friendly and can be used even by non-professionals	Not user-friendly as can only be used by the developers
Costs	Low costs	High costs
Maintenance	Done by cloud service providers	Done by developers
Performance and Reliability	Dependent on the cloud provider	Dependent on the organization
Security	Not recommended for critical projects due to some security risks	Recommended for critical projects as security is high
Availability	Available immediately after subscription	Takes time to install hence not available immediately after subscription
Upgrades	More automatic from the internet	Upgrades can take time and cause interruption in business
Storage considerations	Large amounts of data can be stored	Recommended to store small amounts of data due to the long time needed to store large amounts of data.
Infrastructure	Virtual infrastructure	Physical infrastructure
Data source	Data is collected from the internet	Data is collected from the organization's network

Conclusion of Private Cloud vs. Data Center

A private cloud refers to computing services offered online to a single user and is off-premise. A data center refers to a network of servers within a building that an organization uses to store its data and other applications. It is on-premise meaning it is physical and can only be assessed by the organization. Which one is better between a private cloud and a data center? This one entirely depends on the individual or organization needs, whereby the business owner assesses all the considerations and makes the decision of which one suits his/her business needs.

Q&A

Is private cloud data center?

No, a private cloud is different from a data center in that a private cloud is off-premise while a data center is on-premise. The private cloud's infrastructure is virtual while the data center's infrastructure is physical.

The private cloud serves a single customer while the data center serves an organization.

A private cloud can be used even by non-professionals while a data center is more complex used only by developers within an organization.

When should I use a private cloud?

When the data you are storing is not too critical due to possible security risks. If what you are storing is too sensitive for an organization, then the data center is a better resource.

What is a private cloud example?

- Ubuntu
- Managed Private Cloud
- Elastra-private cloud.
-

Mware vSphere Hypervisor 7.0 U3 Download Center

Benefits of hypervisors

There are several benefits to using a hypervisor that hosts multiple virtual machines:

- **Speed**: Hypervisors allow virtual machines to be created instantly, unlike bare-metal servers. This makes it easier to provision resources as needed for dynamic workloads.
- **Efficiency**: Hypervisors that run several virtual machines on one physical machine's resources also allow for more efficient utilization of one physical server. It is more cost- and energy-efficient to run several virtual machines on one physical machine than to run multiple underutilized physical machines for the same task.
- **Flexibility**: Bare-metal hypervisors allow operating systems and their associated applications to run on a variety of hardware types because the hypervisor separates the OS from the underlying hardware, so the software no longer relies on specific hardware devices or drivers.
- **Portability**: Hypervisors allow multiple operating systems to reside on the same physical server (host machine). Because the virtual machines that the hypervisor runs are independent from the physical machine, they are portable. IT teams can shift workloads and allocate networking, memory, storage and processing resources across multiple servers as needed, moving from machine to machine or platform to platform. When an application needs more processing power, the virtualization software allows it to seamlessly access additional machines.

Why use a hypervisor?

Hypervisors make it possible to use more of a system's available resources and provide greater IT mobility since the guest VMs are independent of the host hardware. This means they can be easily moved between different servers. Because multiple virtual machines can run off of one physical server with a hypervisor, a hypervisor reduces:

- Space
- Energy
- Maintenance requirements

Types of hypervisors

There are two main hypervisor types, referred to as “Type 1” (or “bare metal”) and “Type 2” (or “hosted”). A **type 1 hypervisor** acts like a lightweight operating system and runs directly on the host’s hardware, while a **type 2 hypervisor** runs as a software layer on an operating system, like other computer programs.

The most commonly deployed type of hypervisor is the type 1 or bare-metal hypervisor, where virtualization software is installed directly on the hardware where the operating system is normally installed. Because bare-metal hypervisors are isolated from the attack-prone operating system, they are extremely secure. In addition, they generally perform better and more efficiently than hosted hypervisors. For these reasons, most enterprise companies choose bare-metal hypervisors for data center computing needs.

While bare-metal hypervisors run directly on the computing hardware, hosted hypervisors run on top of the operating system (OS) of the host machine. Although hosted hypervisors run within the OS, additional (and different) operating systems can be installed on top of the hypervisor. The downside of hosted hypervisors is that latency is higher than bare-metal hypervisors. This is because communication between the hardware and the hypervisor must pass through the extra layer of the OS. Hosted hypervisors are sometimes known as client hypervisors because they are most often used with end users and software testing, where higher latency is less of a concern.

Hardware acceleration technology can create and manage virtual resources faster by boosting processing speed for both bare-metal and hosted hypervisors. A type of hardware accelerator known as a **virtual Dedicated Graphics Accelerator (vDGA)** takes care of sending and refreshing high-end 3-D graphics. This frees up the main system for other tasks and greatly increases the display speed of images. For industries such as oil and gas exploration, where there is a need to quickly visualize complex data, this technology can be very useful.

Both types of hypervisors can run multiple virtual servers for multiple tenants on one physical machine. Public cloud service providers lease server space on the different virtual servers to different companies. One server might host several virtual servers that are all running workloads for different companies. This type of resource sharing can result in a “noisy neighbor” effect, when one of the tenants runs a large workload that interferes with the server performance for other tenants. It also poses more of a security risk than using a dedicated bare-metal server.

A bare-metal server that a single company has full control over will always provide higher performance than a virtual server that is sharing a physical server’s bandwidth, memory and processing power with other virtual servers. The hardware for bare-metal servers can also be optimized to increase performance, which is not the case with shared public servers. Businesses that need to comply with regulations that require physical separation of resources will need to use their own bare-metal servers that do not share resources with other tenants.

What is a cloud hypervisor?

As cloud computing becomes pervasive, the hypervisor has emerged as an invaluable tool for running virtual machines and driving innovation in a cloud environment. Since a hypervisor is a software layer that enables one host computer to simultaneously support multiple VMs, hypervisors are a key element of the technology that makes cloud computing possible. Hypervisors make cloud-based applications available to users across a virtual environment while still enabling IT to maintain control over a cloud environment’s infrastructure, applications and sensitive data.

Digital transformation and rising customer expectations are driving greater reliance on innovative applications. In response, many enterprises are migrating their virtual machines to the cloud. However, having to rewrite every existing application for the cloud can consume precious IT resources and lead to infrastructure silos. Fortunately, as an integral part of a virtualization platform, a hypervisor can help migrate applications to the cloud quickly. As a result, enterprises can reap the cloud’s many benefits, including reduced hardware expenditures, increased accessibility and greater scalability, for a faster return on investment.

How does a hypervisor work?

Hypervisors support the creation and management of virtual machines (VMs) by abstracting a computer’s software from its hardware. Hypervisors make virtualization possible by translating requests between the physical and virtual resources. Bare-metal hypervisors are sometimes embedded into the firmware at the same level as the motherboard basic input/output system (BIOS) to enable the operating system on a computer to access and use virtualization software.

Container vs hypervisor

Containers and hypervisors are both involved in making applications faster and more efficient, but they achieve this in different ways.

Hypervisors:

- Allow an operating system to run independently from the underlying hardware through the use of virtual machines.

- Share virtual computing, storage and memory resources.
- Can run multiple operating systems on top of one server (bare-metal hypervisor) or installed on top of one standard operating system and isolated from it (hosted hypervisor).

Containers:

- Allow applications to run independently of an operating system.
- Can run on any operating system—all they need is a container engine to run.
- Are extremely portable since in a container, an application has everything it needs to run.

Hypervisors and containers are used for different purposes. Hypervisors are used to create and run virtual machines (VMs), which each have their own complete operating systems, securely isolated from the others. In contrast to VMs, containers package up just an app and its related services. This makes them more lightweight and portable than VMs, so they are often used for fast and flexible application development and movement.

What is a hypervisor?

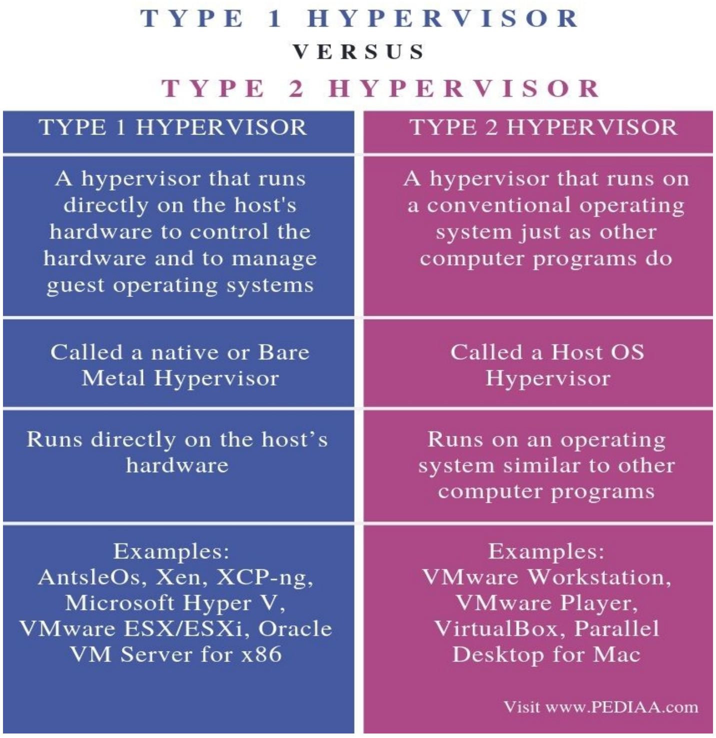
A **hypervisor**, also known as a virtual machine monitor or VMM, is software that creates and runs virtual machines (VMs). A hypervisor allows one host computer to support multiple guest VMs by virtually sharing its resources, such as memory and processing.

Next-Gen Virtualization

What is the Difference Between Type 1 and Type 2 Hypervisor

The **main difference** between Type 1 and Type 2 Hypervisor is that **Type 1 Hypervisor runs directly on the host's hardware while Type 2 Hypervisor runs on an operating system similar to other computer programs**.

Running applications on individual systems cause resource wastage. Virtualization provides a solution to this issue. In fact, virtualization is the process of creating a virtual version of a server, operating system, network or a storage device. It also divides resources between multiple execution environments. Moreover, a hypervisor is related to virtualization. It is a Virtual Machine Monitor (VMM). In other words, it creates and runs virtual machines. There are two types of hypervisors as Type 1 and Type 2.



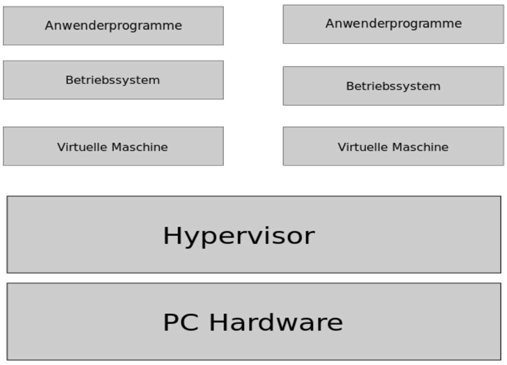
TYPE 1 HYPERVISOR VERSUS TYPE 2 HYPERVISOR

TYPE 1 HYPERVISOR	TYPE 2 HYPERVISOR
A hypervisor that runs directly on the host's hardware to control the hardware and to manage guest operating systems	A hypervisor that runs on a conventional operating system just as other computer programs do
Called a native or Bare Metal Hypervisor	Called a Host OS Hypervisor
Runs directly on the host's hardware	Runs on an operating system similar to other computer programs
Examples: AntsleOs, Xen, XCP-ng, Microsoft Hyper V, VMware ESX/ESXi, Oracle VM Server for x86	Examples: VMware Workstation, VMware Player, VirtualBox, Parallel Desktop for Mac

Visit www.PEDIAA.com

What is Type 1 Hypervisor

A computer on which the hypervisor runs single or multiple virtual machines is called a host machine. In addition, each virtual machine is a guest machine. Type 1 Hypervisor is called a **Bare Metal Hypervisor** or **native Hypervisor**. It runs directly on the host hardware. Furthermore, it manages the guest operating systems and controls hardware.

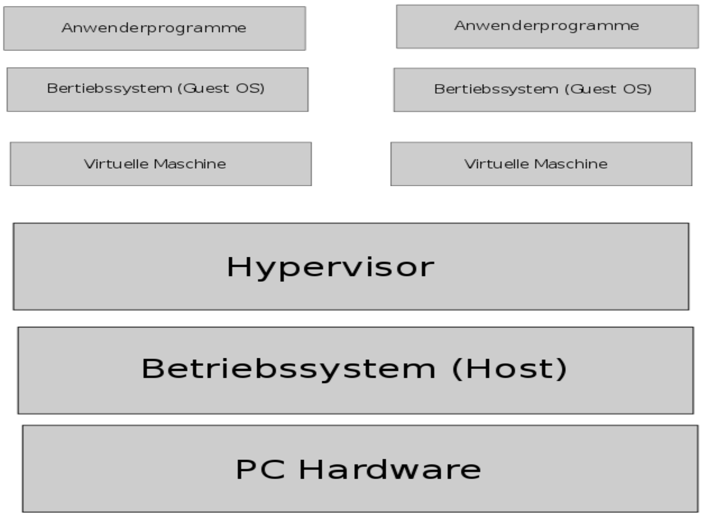


Hypervisor Typ 1

Moreover, the first hypervisors developed by IBM were native hypervisors. These included SIMMON test software. Furthermore, it also had CP/CMS operating system. AntsleOs, Xen, XCP-ng, Microsoft Hyper V, VMware ESX/ESXi, Oracle VM Server for x86 are some examples for Type 1 Hypervisors.

What is Type 2 Hypervisor

Type 2 Hypervisor is called a **Host OS Hypervisor**. These hypervisors execute on an operating system similar to other computer programs. For example, assume that there is an operating system. There is a hypervisor on top of the OS. It provides an emulator environment to run another operating system. In other words, a guest operating system runs as a process on the host. Moreover, VMware Workstation, VMware Player, VirtualBox, Parallel Desktop for Mac are some examples for Type 2 Hypervisors.



Hypervisor Typ 2

Difference Between Type 1 and Type 2 Hypervisor

Definition

Type 1 hypervisor is a hypervisor that runs directly on the host's hardware to control the hardware and to manage guest operating systems while Type 2 hypervisors run on a conventional operating system just as other computer programs do. Thus, this is the main difference between Type 1 and Type 2 Hypervisor.

Synonyms

Type 1 Hypervisor is called a native or Bare Metal Hypervisor while type 2 Hypervisor is called a Host OS Hypervisor.

Functionality

Functionality is another difference between Type 1 and Type 2 Hypervisor. Type 1 Hypervisor runs directly on the host's hardware while Type 2 Hypervisor runs on an operating system similar to other computer programs.

Examples

AntsleOs, Xen, XCP-ng, Microsoft Hyper V, VMware ESX/ESXi, Oracle VM Server for x86 are some examples for Type 1 Hypervisors while VMware Workstation, VMware Player, VirtualBox, Parallel Desktop for Mac are some examples for Type 2 Hypervisors.

Conclusion

In conclusion, Hypervisor is capable of creating and executing virtual machines. There are two types of hypervisors as Type 1 and Type 2. The main difference between Type 1 and Type 2 Hypervisor is that Type 1 Hypervisor runs directly on the host's hardware while Type 2 Hypervisor runs on an operating system similar to other computer programs.

The hypervisor manages the virtualization technique and creates, runs, and monitors multiple virtual machines (guest) simultaneously, on single computer hardware (host).

So, hypervisors regulate the virtualization process, creates multiple virtual machines that allow you to work on several computing instances at once. This is the key difference between Virtualization and Hypervisors.

The Virtual Machine Monitor or VMM or a Hypervisor acts as a supervisor. It's implemented on computer hardware as code embedded in a system's firmware or as a software layer.

Hypervisors create, start, stop, and reset multiple VMs while virtually sharing its resources like RAM and Network interface controller.

VMM governs the guest operating systems and manages execution on a virtual operating platform. It furthermore separates Virtual Machines (VMs) from each other logically, so even if one OS crashes for some reason, the other VMs can function unhindered.

Two Types of Hypervisor: Type 1 and Type 2

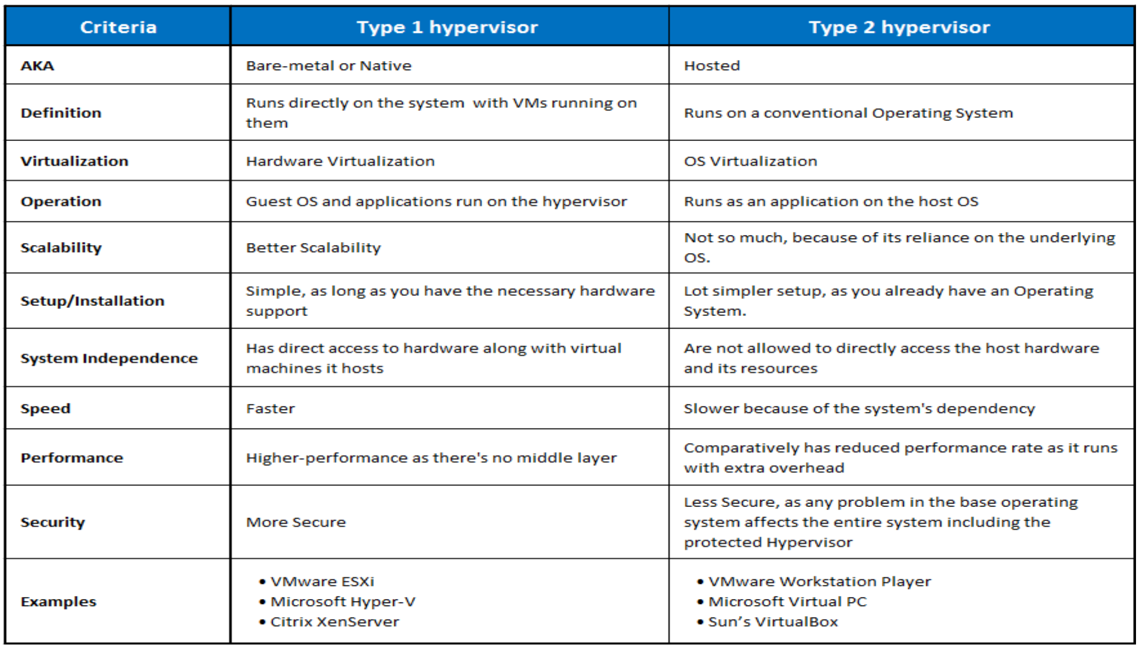
Based on their working system Hypervisors are divided into two categories-

- **Type 1 – Bare Metal hypervisor and Type 2 – Hosted hypervisor**

The primary contributor to why hypervisors are segregated into two types is because of the presence or absence of the underlying operating system.

Type 1 runs directly on the hardware with Virtual Machine resources provided. Type 2 runs on the host OS to provide virtualization management and other services.

Hypervisor Type 1 vs. Type 2 in Tabular Form



Criteria	Type 1 hypervisor	Type 2 hypervisor
AKA	Bare-metal or Native	Hosted
Definition	Runs directly on the system with VMs running on them	Runs on a conventional Operating System
Virtualization	Hardware Virtualization	OS Virtualization
Operation	Guest OS and applications run on the hypervisor	Runs as an application on the host OS
Scalability	Better Scalability	Not so much, because of its reliance on the underlying OS.
Setup/Installation	Simple, as long as you have the necessary hardware support	Lot simpler setup, as you already have an Operating System.
System Independence	Has direct access to hardware along with virtual machines it hosts	Are not allowed to directly access the host hardware and its resources
Speed	Faster	Slower because of the system's dependency
Performance	Higher-performance as there's no middle layer	Comparatively has reduced performance rate as it runs with extra overhead
Security	More Secure	Less Secure, as any problem in the base operating system affects the entire system including the protected Hypervisor
Examples	• VMware ESXi • Microsoft Hyper-V • Citrix XenServer	• VMware Workstation Player • Microsoft Virtual PC • Sun's VirtualBox

Native v/s Hosted Hypervisor: Which is the better option of the two?

For enterprise applications and cloud computing, the Bare-metal hypervisors are preferable, primarily because of its independence from the host operating system.

For the same reason, type 1 generates lesser overhead, and any malfunction in an individual VM does not harm the rest of the system.

The native hypervisors are a more secure option. Unlike the hosted hypervisor, they do not depend upon the underlying OS.

So if under attack, you have better chances with the bare-metal hypervisor (Type 1). This dependency also costs the type 2 server, a little bit of its efficiency, performance, and speed.

Type 2 does not have direct access to the host hardware and resources, so this may make a certain degree of latency inevitable. The already present OS manages the requirements for memory, storage, and network resources.

Although this is not the case for more straightforward scenarios, Hosted Hypervisors are still popular for personal use and SMBs.

For some developer environments, like where access to multiple OSs and their variants is required, Type 2 hypervisors are a better option. On devices not dedicated to the VMs Host role, hosted hypervisors are recommended.

Why is the Cloud not secure?

Posted by Sid Shetye

We get this question all the time from our customers and many companies think they can leverage their existing security mechanisms in the Cloud. However, in reality, the Cloud is an entirely different arena. At Crypteron, we often have to remind customers of the security risks of being in the cloud; and to do that we must look at why things are so different in the Cloud.

Traditionally, companies are used to having their own datacenter with their own hardware running only their application. Or perhaps they use a co-location facility (termed CoLo in the industry) with their hardware sitting in a locked cage physically separating their servers and databases from other Co-Lo customers. In this environment, you are not sharing hardware with others and in theory, only you have access to the hardware equipment. This physical separation and physical security isn't complete in itself but does offer a layer of protection that is otherwise missing in the cloud.

Now, moving to the Cloud, everything is shared. And you own nothing. Not only does the hardware belong to another company (the cloud provider), but that hardware is likely being shared by other organizations too. It is hard, often impossible, to map a 1:1 relationship between physical resource like CPU cores, storage drives, network interfaces etc and their virtual counterparts. It is possible that your data resides on the same physically media as your competitor or another cloud customer currently being investigated by a government agency for questionable behavior. If the government investigation team (eg: FBI, NSA etc) requests a copy of that physical drive, your sensitive data suddenly becomes part of the collateral damage without you ever knowing it.

Even if we leave law enforcement aside, the fact remains that it's the cloud provider who owns the cloud equipment and you are merely renting it. This implies that there is usually an administrator on the cloud provider's side who always has access to all resources just to ensure that everything is up and running. This is especially true as we step into the next evolution of cloud technologies via 'Platform as a service' where the service provider own not just the physical hardware and the virtualized hardware but also the operating system hosting the PaaS application. So even if the Cloud providing company has no interest in your data, a disgruntled employee from the Cloud provider's team can ruin your company via data leaks. Worse of all, there will always be someone outside your organization who has access to your Cloud data.

These are just few of the reasons why it is absolutely critical to have data encryption in the Cloud. Very strong encryption! In addition, compliance requirements also make it illegal to operate in the cloud without adequate protection for your sensitive data. That is a topic in itself so we'll save that for another blog post.

This is why we exist today. Our military-grade, cloud data security solutions ensure that you have the highest level of security so your IT department can focus on the things that actually make your business unique from the competition.