Assignment of Cloud Computing-<CSI ZG527 / SS ZG527 / SE ZG527>

Question1:- Which are the different layers that define cloud architecture?

Question 2:- What are the security aspects provided with the cloud?.

Question 3:- What is the requirement of virtualization platform in implementing cloud?

Question 4:- Explain what are the different modes of software as a service (SaaS)? .

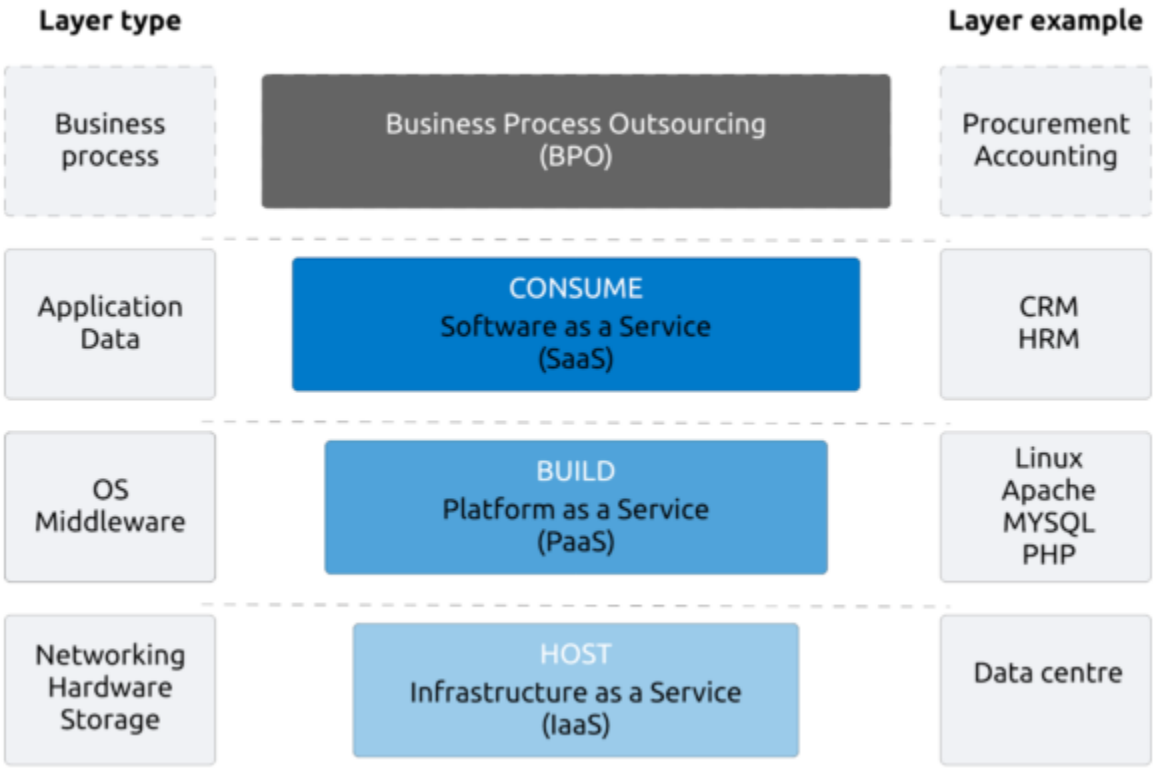
Question 5:- Before going for cloud computing platform what are the essential things to be taken in concern by users?

Question 6:- State the list of a need of virtualization platform in implementing cloud?

Assignment Submitted by: **Satish Kumar Sharma, ID Number: 2022MT93327**

Question 1. Which are the different layers that define cloud architecture?

Ans: Cloud computing services are divided in to 3 types of classes/layers according to abstraction level of the capability provided and the service model of providers. Cloud architecture is not as simple as it first seems. Cloud is the outcome of several layers of cloud architecture intelligently placed over one another. Before moving towards the various layers, look at the more general picture of cloud layers below



- **Hardware Layer:** This bottoms most layer of cloud architecture, the hardware layer, primarily deals with all the hardware powering clouds. The hardware includes but is not restricted to routers, servers, switches, power, and cooling systems.

- **Infrastructure Layer:** Also called the virtualization layer, the infrastructure layer is where all the servers are pooled together into one.
- **Platform Layer:** The platform layer comprises the operating system and other requisition structures and is based over the infrastructure layer.
- **Application Layer:** As the name suggests, the application layer - the topmost layer - contains applications that directly interact with the end-user.

These abstraction levels can be viewed as a layered architecture where services of a higher layer can be composed from services of the underlying layer.

Cloud computing architecture is made of **several layers for better operational efficiency.** Cloud controller or CLC is at the top and is used to manage virtualized resources like **servers, network, and storage.**

- Walrus is the next layer and used as a storage controller to manage the demands of the users.
- Cluster Controller or CC manages the virtual networking between Virtual machines and external users.
- Storage Controller or SC is a block-form storage device dynamically attached by Virtual machine.
- The next layer is NC or Node Controller. It acts as a hypervisor and controls the Virtual machines activities such as execution, management, and termination of many instances.

Cloud Computing is of the Following three types:

Infrastructure as a Service (IaaS): A cloud service is said to be IaaS when the provider is responsible for creating the entire virtualization environment for the client. The provider will setup the cloud, pool resource of the server together, turn on the lights and hand the keys of the cloud to the client. It is the bottom most service that can be sold to the client.

Platform as a Service (PaaS): - Platform as a Service. When the provider itself configures an operating system on the infra, creating a ready platform to be used for various needs, it is called the Platform as a Service (PaaS) PaaS is mostly used by web developers for launching VMs as it gives them a ready-made platform to start developing applications as per their needs.

Software as a Service (SaaS): - is the topmost service layer that can be sold among various layers of cloud architecture. Of all types of cloud computing, this one involves the end-user and the underlying hardware the least. In SaaS, the client is not at all concerned with the layers underpinning the cloud and only works at the topmost layer.

Question 2. What are the security aspects provided with the cloud?

Ans: Security of the Cloud

Technology has developed but with it the activities of the cyber criminals also have advanced. DDoS attacks can cripple the functioning of a business. Strong firewalls and anti-malware solutions can reduce the severity of the risk.

Another solution is the encryption of data while it is being transmitted from the client to provider. The consumers should be kept in individual compartments to make sure that if one account is compromised the other users will not be affected.

The five elements of cloud security are

1. **A secure architecture,**
2. **Enforcing compliance,**
3. **Practicing due diligence,**
4. **Monitoring the network,**
5. **Incorporating solid authentication protocol.**

- **Physical Security.**
- **Software Security.**
- **Infrastructure Security.**

Access control: permissions have to be provided to the users so that they can control the access of other users who are entering the in the cloud environment. Authorization and authentication: provision should be made to allow the authorized and authenticated people only to access and change the applications and data.

What security benefits does the cloud provide?

Cloud computing security helps to continuously monitor, identify, analyze, and mitigate DDoS attacks. The built-in redundancies, customizability, flexibility, scalability, and intelligence of such solutions can prevent volumetric, low, and slow attacks.

Request-based Access

- Users must authenticate themselves to get access to the organization's data that run on the cloud. This is a federated identity service which integrates the identity management of an organization and cloud service provider

- Users must check the policies and then assess to decide which cloud hosting providers would suit their requirements of security, reliability etc.

Some of the salient features of cloud computing that are beneficial to every organization include on-demand resource availability, resource pooling, rapid elasticity, metered services and access via the internet.

Some of the Risks Include:

- Data loss or leakage could damage the business reputation as well as create a doubt or suspicion that could affect employer/employee relationship.

- It will create huge financial losses to the business. This can be mitigated by having a control on access to data only by authorized personal.

The data is stored away from the business premises of the customer. This has been the primary concern of every CIO.

Key Points that Take care of the Cloud Security

People mostly ask what the security aspects are provided with cloud computing provides. Cloud security is nothing without its key technologies that makes it more secured. Such technologies are-

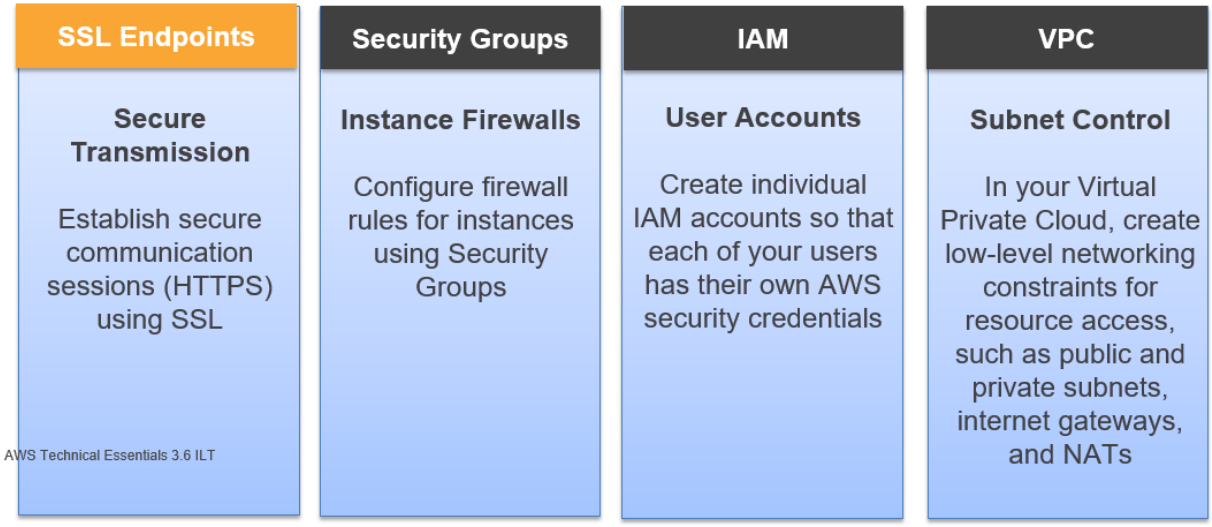
Encryption- It is a technology that makes data being understood only by the concerned authority. Its only motive is to make the format of the data that cannot be easily interpreted. Such technology or process is termed encryption. Cloud technology relies a lot on encryption to keep the data secured. Some data if unencrypted can be a cause of great hazards to a company. Due to encryption, there are unexpected aspects of data security in cloud computing.

Firewall- security aspects of cloud computing are not just limited to encryption. A firewall is a very secure way of keeping the data safe by creating an additional layer of protection. It makes sure that all it blocks all the malicious attacks. Such malicious attacks are very frequent through web traffic. Cloud firewalls are hosted over the cloud, unlike traditional firewalls that were not efficient as they stayed on-premises.

Security Policies- Aspects of data security in cloud computing knows no bounds. Security policies are applied throughout the complete cloud infrastructure. For better cloud security, there must be a proper configuration of security settings through strict security policies. When a

company does not take its security policies seriously then they end up going through data breaches.

Backup Plans- Data security also asks for backup plans so that not a single bit of data is inside the realm of risk. To avoid any kind of data loss, data should be backed either on-premises or on any other cloud. There should be always a plan B to cover any losses that may occur during data loss. To be more sure about data security, cloud technology has come up with multi-cloud and hybrid cloud infrastructure.



Some of the security architecture standards to be compliant with

1. SE-CMM (System Security Engineering Capability Maturity model)
2. ISO/IEC 27001-27006
3. ENISA (European network and information security agency)
4. ITIL security management
5. COBIT
6. NIST

Takeaway

To make cloud services secure, security applications are deployed in two or more layers.

- The first layer comprises of the firewall. Note that firewall can be both hardware and application based. The function of this security system is to avoid entry and exit of phony data packets in and out of the system.

- Request-based access also stands at the network entry. It filters out most unwanted intruders by denying access straightaway.

- Antivirus and anti-spyware comprise predominantly the second layer. It eliminates threats that have somehow crept into the system.

Some firewalls also stand guard at the network exit points. This is perhaps the last line of defense. Any threat that may have successfully evaded the system and the antivirus should be identified and blocked here. Exit firewall buttresses the security of the cloud.

Question 3. What is the requirement of virtualization platform in implementing cloud?

Ans: Virtualization is the main requirement to implement cloud computing. The entire concept is based on **virtually parting the resource i.e. no physical alteration but making the platform to segregate resource by itself**, which is only possible if the architecture undergoes virtualization.

Requirements of virtualization platform from a cloud vendor perspective

1. **Partitioning:** Virtualization through VMs Help running multiple OS on a single hardware=> cloud vendor can enable multiple users running multiple applications on a single hardware
2. **Security isolation:** Cloud vendors can offer fault and security isolation at the hardware level
3. **Encapsulation:** Cloud vendors can offer moving and copying files from one VM to another without any hassle including to file
4. **Hardware independence:** Cloud vendor can secure the data by supporting migration of virtual machine to any physical server

5. **Scalability:** It is easy to scale services being provided through virtualization instead of building independent server resources

Requirements of virtualization platform from a cloud user perspective

1. Identifying the cloud vendor who uses virtualization because that's is the vendor who can provide cost effective solutions
2. Hassle free maintenance as there is no need to maintain the hardware, platforms etc. based on the service model opted
3. As a user, if one is providing a scalable application services, I do not wish to invest in capex for the ad-hoc requests for the customers whose life time value would be less
4. It helps the user to use multiple service models (IaaS, PaaS, SaaS) which could not be possible without having enabled virtualization
5. Creating a light weight application on lift weight OS/hardware would be easier and cost effective

Going in more details:

- Virtualization separates the back-end level and user level for creation of a seamless environment between the two. Virtualization is used for deployment of models of cloud hosting services including Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS) among others.
- Virtualization software allows multiple operating systems and applications to run on the same server at the same time, and, as a result, **lowers costs and increases efficiency of a company's existing hardware**. It's a fundamental technology that powers Everything-as-a-Service model of computing.
- Virtualization in Cloud Computing is **making a virtual platform of server operating system and storage devices**. This will help the user by providing multiple machines at the same time it also allows sharing a single physical instance of resource or an application to multiple users.

- Virtualization in cloud computing **allows a provider to virtualize servers, storage, or other physical hardware or data center resources**, which can then, in turn, allow them to provide numerous services such as infrastructure, software, and platforms

The basic infrastructure of the cloud is empowered by virtualization. It enables delivery of intricate cloud services that is easily scalable in a cost-effective manner. The cloud computing users can run virtual machines without the need to invest and maintain the hardware, bandwidth, and other data center infrastructure.

Virtualization has enabled dealing with infrastructure that cannot be touched and is used to deploy the three major components of cloud computing that include Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS).

One fundamental attribute of virtualization is the concept of partitioning. This enables supporting of multiple operating systems under one single server. This, in turn, ensures more segregation and seclusions to the machines from one another and effectively isolates them from an infected machine.

Your server is not affected even if a neighbor machine is hacked or infected with a virus. Being in an individually enclosed environment assures of enhanced security without being intruded by the other machines being served in the environment. Being housed in an encapsulated form identifies and preserves individuality from other applications.

Yet another feature of virtualization is its ability to share the hardware on the Linux and Windows operating systems. It also enables shifting of operating systems over different hardware when multiple applications are running. Virtualization has enabled the cloud to be sold as a commodity based on utility. Users can choose any platform without being locked in to any one vendor and they pay only for what they use.

Question 4. Explain what are the different modes of software as a service (SaaS)?

Ans: Software as a service (SaaS) is a cloud computing model where a third-party provider offers software applications to consumers over the internet. The services are scalable and can be modified by the users as they find necessary for their business. The SaaS applications can be accessed and used by multiple consumers simultaneously. The users are reduced of the infrastructure costs and the expenses are shared among the multiple users. The main purpose is to share the data resources between multiple users while maintaining data isolation between the users.

The services are delivered in two modes:

a). Simple Multi-Tenancy or Cross-Grain Multi-Tenancy: It is a hosted service model where the users have their own resources that are independent of other users. It is not instantly scalable, and users have to be content with low margins due to high competition. The advantage is it is simple and does not require any code modifications.

b). Fine Grain Multi-Tenancy: This again involves sharing of the same database among multiple users. The data is kept separate although the computing resources are shared. It is easily scalable and offers efficiency in services.

The above described are the two different modes of software as a service (SaaS) in which the service provider offers the software applications to the customer via the internet. SaaS applications can be effectively handled by multiple users making them the top choice for the companies using software through the cloud.

Both the SaaS modes mentioned above are known for offering the best working environment and thus companies choose them more often. If

you are a budding business, then going with any mode of SaaS will easily solve your problem and you will not face any issues.

- Customer Relationship Management (CRM) Software.
- Enterprise Resource Planning (ERP) Software.
- Accounting Software.
- Project Management Software.
- Email Marketing Software.

Question 5. Before going for cloud computing platform what are the essential things to be taken in concern by users?

Ans: Following are the essential things that must be followed before going for the cloud computing platform:

- Uptime.
- Loss of data.
- Data storage.
- Compliance.
- Business continuity.
- Data integrity in cloud computing.

- Determine why your business needs to move to the cloud
- Manage location and security of data
- Define in which ways the work culture of your business will change
- Find out how cloud migration will impact IT and business performance
- Align your move with your hardware life cycle
- Find the right cloud provider
- Determine the realistic costs and timelines

a). Determine why your business needs to move to the cloud

This is the very first question to address, as you do not want to make this move just because it is a “cool” thing to do. You need to have a bird’s eye view of your business to determine which areas could benefit from migration. As the chart below suggests, the reasons for transition to the cloud range from enhanced security to better IT performance, but you need to determine what’s in it for you.

b). Manage location and security of data

You are responsible for both your clients’ and your own valuable, confidential data. At any time, you need to know where it is and be sure that it is safe. For certain industries, such as the legal and finance sectors, data security is a make-or-break issue. According to a recent study, nearly 80% of businesses suffered at least one cloud breach in the past 18 months, and 43% experienced ten or more breaches over the same time period.

That is why you need to always be aware of both data locations and the laws that govern it. You need to stay informed about data regulations and be aware if your data is subject to government surveillance.

In order to make sure your data is governed properly; you first need to align the governance and security requirements of applications with the security provisions of your potential cloud platforms. This is because you need to make sure that your applications and data will be securely guarded, yet fully accessible and auditable.

Your next step is to make sure you are always able to manage access to data. That means you need to control what services are being used, at what cost, and by whom. This way cloud costs will not spiral out of control.

c). Define in which ways the work culture of your business will change

A move to the cloud is not just a business or technology strategy but is a massive organizational change in itself. It requires a change of perspective, learning new skills – primarily cloud-computing skills – and forgetting a few old ones.

Often, it creates an entirely new organizational culture and new workplace collaboration, and it often necessitates applying new HR methods and solutions such as agent supervisor tools. In other words, it is not just a tech issue – it affects all the areas in the chart below.

Migrating to a cloud is a major business shift and stakeholders should receive an explanation of why it is done and how it will change the organization.

A lot of procedures within an organization would change – starting from data storage and ending up with the outreach strategy and the organization of the sales process. Stakeholders must be informed of how their roles will change as a result of such a transition.

D). Find out how cloud migration will impact IT and business performance

The only way to minimize disruption from cloud migration and preserve business continuity is to understand how, when, and why your teams use applications. You can do this via various collaboration tools. In addition, you need to look into the way the move to the cloud will affect various aspects of your IT infrastructure.

e). Align your move with your hardware life-cycle

How old is your hardware? If you have recently invested in new hardware, then financially it would not be advisable to move your IT infrastructure to the cloud.

The perfect time to make the move is when your hardware is three or more years old. This is because any money you would spend on replacing the equipment would be better invested in cloud migration.

If you can align your migration to the cloud with your hardware life-cycle policy, you will be able to optimize the use of existing hardware-related resources until they are on the verge of becoming obsolete. Only after that would it make sense to make that crucial decision on whether server data should be moved to the cloud.

f). Find the right cloud provider

If you believe cloud migration is a great idea for your business, you need to choose the right cloud provider. Often, when you look into your business needs, you realize that different applications have different requirements.

That is why, for most organizations, a hybrid, multi-cloud approach that involves a range of private cloud, public cloud, and SaaS providers will be optimal. That said, such a hybrid approach might entail certain challenges in terms of management.

In order to see which specific solution would work for you, you need to conduct due diligence. Collect references from people you know, focusing on the key characteristics such as:

Technical competency

Experience

Customer satisfaction

Market leadership

Reputation

Once you zero in on a list of cloud vendors, you need to dig deeper to look into their specific capabilities. Here is what you should keep in mind:

Quality of data centers

Quality of engineering team

Approach to data safety

The number of customers already using their services

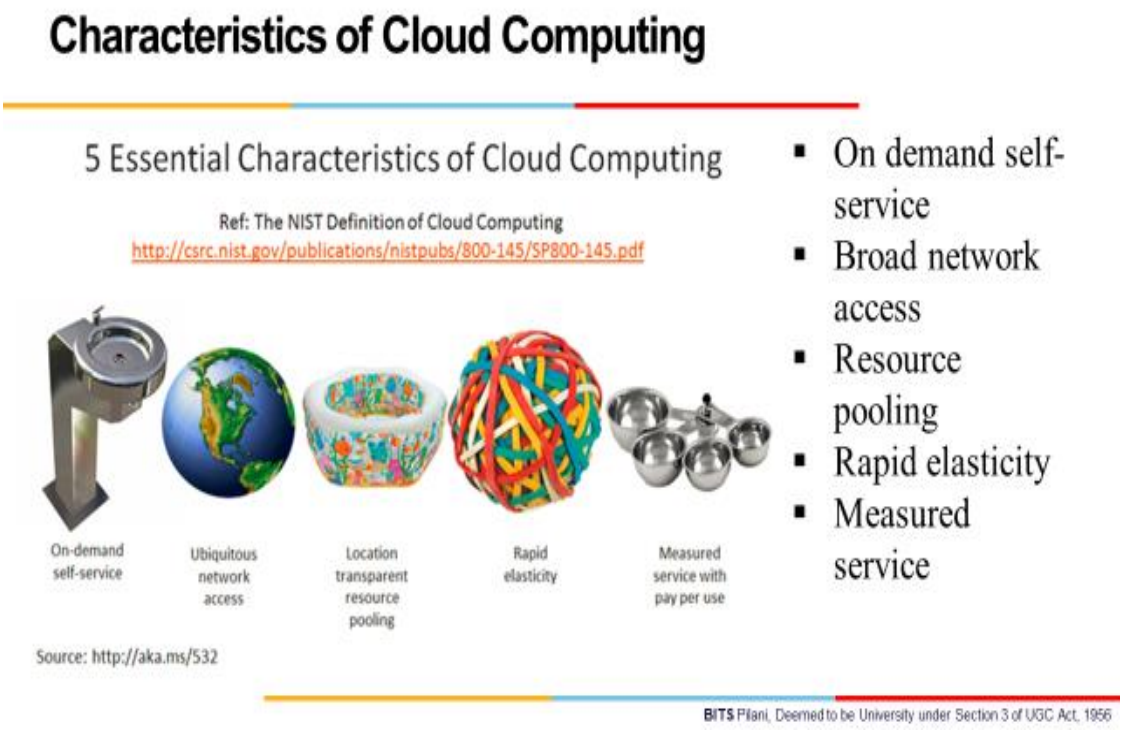
Their solutions for managing updates and patches

Customer support

You need to answer all these questions in order to avoid making a cloud blunder. While a move to the cloud makes perfect business sense, you need to be absolutely sure that this move fits your business growth model and your needs in the future.

g). Determine the realistic costs and timelines

Once you have decided that cloud computing is a great solution for you and have chosen the appropriate provider, here is the next issue to consider. You need to have a realistic idea of costs and timelines – and the way it fits your budget. The needs and resources of financial service providers would differ from those of ecommerce platforms, and so would their perception of appropriate cloud migration costs.



That is why, even if migrating to the cloud makes perfect sense for your business, both the price of this move and the length of time it takes to do it might pose insurmountable problems.

Question 6. State the list of a need of virtualization platform in implementing cloud?

Ans: Virtualization is the foundation of cloud computing. It **enables creation of an intelligent layer of abstraction to hide the intricacies of the software or hardware that is underlying beneath the layer**.

Virtualization can **increase IT agility, flexibility and scalability while creating significant cost savings**. Greater workload mobility, increased performance and availability of resources, automated operations – they're all benefits of virtualization that make IT simpler to manage and less costly to own and operate.

Need for Virtualization platform from vendor perspective

1. Scalability/**economics of scale**
- Vendor can support multiple users and can scale up the services because of efficient utilization of hardware and operating systems/applications which results in economic benefits
2. Reduction in licensing fees/bargaining power
- Efficient utilization of OS/DB etc. makes per user/ per resource licensing cost reduction
3. Reduction in the operational cost/OpenX
4. Efficient utilization of hardware/licensed software's etc.

Need for Virtualization platform from user/customer perspective

Single-minded servers: Virtualization delivers an easy and cost-effective way that helps organizations separate their databases, emails, and web servers.

Expedited deployment and redeployment: In an organization, if the physical server gets crashed, the availability of extra backup is not always there. Also, in such cases, the clone of the server image is not always available. The redeployment process is very time-consuming and laborious. Therefore, if the data center is virtualized, then this process is easy and will be done in a short period.

To slash Capex/ IT expenses: If you are working in a non-virtualized environment, it can be inefficient. Because when you are not consuming the application on the server, the computing is idle and cannot be used for other applications. A single physical server can transform into multiple virtual machines (VM) with Virtualization. Further, VM having different OS can run various applications, all hosted on a single server. Overall it also saves money on power consumption

Increase efficiency and productivity: Virtualization helps the organization of greater efficiency and productivity. With fewer servers, the IT team will need less time for hardware maintenance which automatically saves operating time. Therefore, fewer time requirements are helping the IT environment to increase productivity.

Control independence and DevOps: Because of Virtualization, your IT developers can quickly spin up a VM without impacting a productive IT environment. Moreover, with a virtualized environment, developers can easily clone virtual machines. Also, testers can test the background without any difficulty

Pay as per use: You can pay as per use and save lot of capex/OpenX on licensing fees etc.

Reliability and availability

Real-estate savings, compliance savings etc.

No hassle as no need of maintenance etc.

Flexibility in selecting o/s, dbs applications on the fly etc.

Advantages of Virtualization

- **Instant provisioning - fast scalability**
- **Live Migration is possible**
- **Load balancing and consolidation in a Data Center is possible.**

- **Low downtime for maintenance**
- **Virtual hardware supports legacy operating systems efficiently**
- **Security and fault isolation**

Thank You

Name: Satish Kumar Sharma
ID Number: 2022MT93327