Name :Muhammad Tahir

I.D=12712

Q1:

When each of the following deployment models should be used?

• Public Cloud

• Private Cloud

• Community Cloud

Hybrid Cloud

Answer:>

1. **Public Cloud**

The name speaks for itself: public clouds are available to the general public, and data are created and stored on third-party servers.

Server infrastructure belongs to service providers that manage it and administer pool resources, which is why there is no need for user companies to buy and maintain their own hardware. Provider companies offer resources as a service both free of charge or on a pay-per-use basis via the Internet. Users can scale resources as required.

The public cloud deployment model is the first choice for businesses with low privacy concerns. When it comes to popular public cloud deployment models, examples are Amazon Elastic Compute Cloud (Amazon EC2 — the top service provider according to ZDNet), Microsoft Azure, Google App Engine, IBM Cloud, Salesforce Heroku and others.

The Advantages of a Public Cloud

Hassle-free infrastructure management. Having a third party running your cloud infrastructure is convenient: you do not need to develop and maintain your software because the service provider does it for you. In addition, the infrastructure setup and use are uncomplicated.

High scalability. You can easily extend the cloud's capacity as your company requirements increase.

Reduced costs. You pay only for the service you use, so there's no need to invest in hardware or software.

24/7 uptime. The extensive network of your provider's servers ensures your infrastructure is constantly available and has improved operation time.

The Disadvantages of a Public Cloud

Compromised reliability. That same server network is also meant to ensure against failure But often enough, public clouds experience outages and malfunction, as in the case of the 2016 Salesforce CRM disruption that caused a storage collapse.

Data security and privacy issues give rise to concern. Although access to data is easy, a public deployment model deprives users of knowing where their information is kept and who has access to it.

The lack of a bespoke service. Service providers have only standardized service options, which is why they often fail to satisfy more complex requirements.

2. Private Cloud

There is little to no difference between a public and a private model from the technical point of view, as their architectures are very similar. However, as opposed to a public cloud that is available to the general public, only one specific company owns a private cloud. That is why it is also called an internal or corporate model.

The server can be hosted externally or on the premises of the owner company. Regardless of their physical location, these infrastructures are maintained on a designated private network and use software and hardware that are intended for use only by the owner company.

A clearly defined scope of people have access to the information kept in a private repository, which prevents the general public from using it. In light of numerous breaches in recent years, a growing number of large corporations has decided on a closed private cloud model, as this minimizes data security issues.

Compared to the public model, the private cloud provides wider opportunities for customizing the infrastructure to the company's requirements. A private model is especially suitable for companies that seek to safeguard their mission-critical operations or for businesses with constantly changing requirements.

Multiple public cloud service providers, including Amazon, IBM, Cisco, Dell and Red Hat, also provide private solutions.

The Benefits of a Private Cloud

All the benefits of this deployment model result from its autonomy. They are the following:

Bespoke and flexible development and high scalability, which allows companies to customize their infrastructures in accordance with their requirements

High security, privacy and reliability, as only authorized persons can access resources

The Drawbacks of a Private Cloud

The major disadvantage of the private cloud deployment model is its cost, as it requires considerable expense on hardware, software and staff training. That is why this secure and flexible computing deployment model is not the right choice for small companies.

3. Community Cloud

A community deployment model largely resembles the private one; the only difference is the set

of users. Whereas only one company owns the private cloud server, several organizations with similar backgrounds share the infrastructure and related resources of a community cloud.

If all the participating organizations have uniform security, privacy and performance requirements, this multi-tenant data center architecture helps these companies enhance their efficiency, as in the case of joint projects. A centralized cloud facilitates project development, management and implementation. The costs are shared by all users.

The Strengths of a Community Cloud

Cost reduction

Improved security, privacy and reliability

Ease of data sharing and collaboration

The Shortcomings of a Community Cloud

High cost compared to the public deployment model

Sharing of fixed storage and bandwidth capacity

Not commonly used yet

4. Hybrid Cloud

As is usually the case with any hybrid phenomenon, a hybrid cloud encompasses the best features of the abovementioned deployment models (public, private and community). It allows companies to mix and match the facets of the three types that best suit their requirements.

As an example, a company can balance its load by locating mission-critical workloads on a secure private cloud and deploying less sensitive ones to a public one. The hybrid cloud deployment model not only safeguards and controls strategically important assets but does so in a cost- and resource-effective way. In addition, this approach facilitates data and application portability.

The Benefits of a Hybrid Cloud

Improved security and privacy

Enhanced scalability and flexibility

Reasonable price

However, the hybrid deployment model only makes sense if companies can split their data into mission-critical and non-sensitive.

Q2

Which layer of Cloud Computing Architecture is responsible for? Answer in oneword.

Resource Scheduling:

Connection with the cloud:

Hardware Resources:

Load Balancing:

Answer

Access layer

Q3

How Cloud Architectures can be made secured?

Answer:>

SECURE CLOUD ARCHITECTURE

we propose cloud security architecture, which protect organization against security threats and attacks. The key points for this architecture based on our analysis of existing security technologies are:

Single Sign-on (SSO)

Currently, Users are having multiple accounts in various Service Providers with different usernames accompanied by different password. Therefore the vast majority of network users tend to use the same password wherever possible, posing inherent security risks. Theinconvenience of multiple authentications not only causes users to lose productivity, but also imposes more administrative overhead. Enterprises today are seriously considering the use of Single Sign On (SSO) technology [27] to address the password explosion because they promise to cut down multiple network and application passwords to one.To overcome this

problem, it is suggested that, to streamline security management and to implement strong authentication within the cloud, organizations should implement Single SignOn for cloud users. This enables user to access multiple applications and services in the cloud computing environment through a single login,thus enabling strong authentication at the user level.

Defence in depth Security Approach

As enterprise networking technology has evolved, so too has enterprise security. What began simply as setting up a perimeter around the network via fairly basic security tools like firewalls and email gateways, has evolved into adding an array of virtual private networks (VPNs), virtual local area network (VLAN) segmentation, authentication, and intrusion detection systems (IDS) —necessary to handle the consistently growing number of threats to the corporate network.Virtual firewall appliances should be deployed instead of first-generation firewalls. This allows network administrators to inspect all levels of traffic, which includes basic web browser traffic,to peer-to-peer applications traffic and encrypted web traffic in the SSL tunnel .Intrusion Prevention Systems (IPS) should be installed to protect networks from internal threats from insiders.

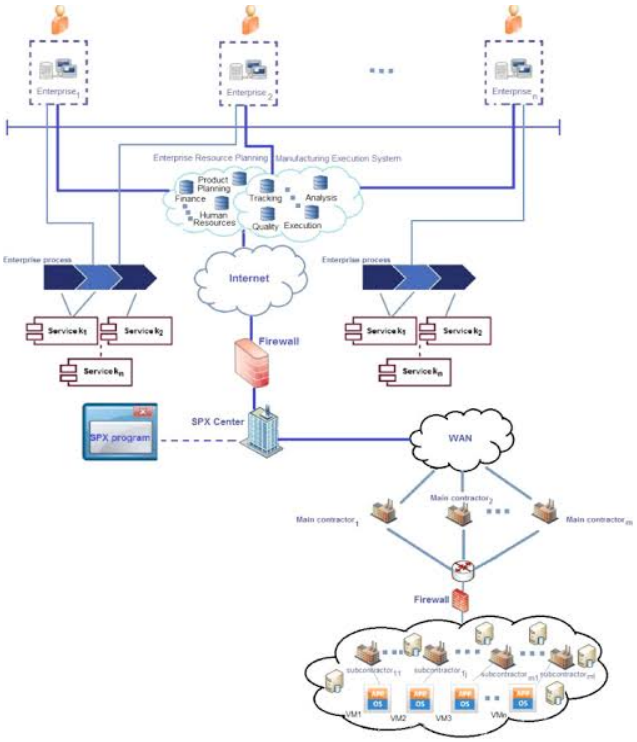
Increase Availability

Availability is a reoccurring and a growing concern in software intensive systems. Cloud systems services can be turned offline due to conservation, power outages or possible denial of service invasions. Fundamentally, its role is to determine the time that the system is up and running correctly; the length of time between failures and the length of time needed to resume operation after a failure. Availability needs to be analyzed through the use of presence information, forecasting usage patterns and dynamic resource scaling [28]. Access to cloudservice should be available all the time, even during maintenance. This makes critical businessdata stored in the cloud to be always available to cloud users, reducing network down time,thereby increasing business profits. This can be done by implementing high availability technologies such as active/active clustering, dynamic server load balanced and ISP load balancing within the network infrastructure.

Data Privacy

Cloud data privacy problem will be found at every stage of the life cycle. For the data storage and use, Mow bray et al. [29] proposed a client-based privacy management tool that provides a user-centric trust model to help users control their sensitive information during the cloud storage and use.

Data loss prevention (DLP) tools can help control migration of data to the cloud and also find sensitive data leaked to the cloud. Data loss prevention (DLP) is a strategy for making sure that end users do not send sensitive or critical information outside of the corporate network. DLP help a network administrator control what data end users can transfer.



Data Integrity

As a result of large scale data communication cost, the users don't want to download data but verify its correctness. Therefore, users need to retrieve the little cloud data through some kinds of agreements or knowledge's which are the probability of analytical tools with high confidence level to determine whether the remote data integrity. User can do the increase and decrease of the data capacity in the cloud server with the help of CSP(cloud serviceprovider) in his request. This storage level must be with flexible and durability condition as far as its entire design or structure is concerned. Thus it should be claimed extra storage space concerning future process in data exchange.

Virtual Machine Protection

You can't just install your firewall or antivirus software on a cloud-based virtual machine.Physical firewalls aren't designed to inspect and filter the vast amount of traffic originating from a hypervisor running 10 virtualized servers. Because VMs can start, stop and move from hypervisor to hypervisor at the click of a button, whatever protection you've chosen has to handle these activities with ease. Plus, as the number of VMs increases in the data center, it becomes harder to account for, manage and protect them. And if unauthorized people gain access to the hypervisor, they can take advantage of the lack of controls and modify all the VMshoused there.These virtual machines are vulnerable like their physical counterparts. Hence, to adequately

protect virtual machines, they should he isolated from other network segments and deep inspection at the network level should be implemented to prevent them both from internal and external threats. Illegal internal access should be restricted by implementing intrusion prevention systems and unauthorized external access should be protected by using secure remote ess technologies like IPSec or SSL VPN.

CONCLUSION

In this research paper we have discussed the characteristics of a cloud security that contains threats/attacks and vulnerabilities. Organizations that are implementing cloud computing by expanding their on-premise infrastructure, should be aware of the security challenges faced by cloud computing. To protect against the compromise of the compliance integrity and security of their applications and data, defense in depth approach must be applied. This line of defense includes firewall, Intrusion detection and prevention, integrity monitoring, log inspection, and malware protection. Proactive organizations and service providers should apply this protection on their cloud infrastructure, to achieve security so that they could take advantage of cloud computing ahead of their competitors. In this paper, a physical cloud computing security architecture has been presented. In future, the proposed architecture may be modified with the advancement of security technologies used for implementing this physical cloud security architecture. By considering the contributions from several IT industries worldwide, it's obvious that cloud computing will be one of the leading strategic and innovative technologies in the near future.

Q5:>

Why do we need Infrastructure as a Service (IaaS)?

While the cloud now dominates all aspects of computing end use—from providing personal email to managing enterprise-level company CRM software—the industry is seeing more and more of the larger companies turn to infrastructure as a service (IaaS) for servers, data storage, hardware management, and bandwidth. IaaS, where businesses make use of pay-as-you-go cloud infrastructure from a service provider, was the largest cloud computing growth area in 2016, and it seems like 2017 will continue this trend. IaaS allows enterprise-level companies to function more effectively, using virtual machines to create data networks, manage large, international business networks, and create apps and software.

IaaS allows users to control virtual machines:

There are three key elements of the cloud computing stack: software as a service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS). IaaS is the aspect of the stack that allows companies the management of their own platform at an architectural level. With IaaS, users manage and control applications, data, middleware, and operating systems, while providers managing servers, hard drives, and storage. IaaS allows users to design and implement their own IaaS software from virtual machines, while the provider manages IaaS hardware. Whereas SaaS and PaaS are commonly used for all levels of computer use—Google apps, for example, hosts millions of personal and professional users—IaaS is specifically keyed

toward enterprise-level companies that operate on a large-scale. In other words, IaaS providers like Amazon AWS and Google Compute Engine maintain the systems that allow companies to, for example, create digital communication technology or customer relations management software. IaaS can also offer momentary benefits with hybrid on-premises/cloud use (‘cloud bursting’), in which businesses can off-load tasks to the cloud when necessary.

Additionally, IaaS providers are beginning to move up the stack, offering databases, messaging queues, and other services. Tech analysts call these services, IaaS+ services, where users can access the initial IaaS services with other platform services. Crucially, these services are more modular; a company can have the provider manage databases or email, for example, while still allowing their employees to manage raw code to create software.

Crucial benefits of IaaS computing:

Cost savings: one of the pivotal reasons why companies choose IaaS is cost. IaaS allows businesses to start with and maintain lower infrastructure costs. By using IaaS, not only does a business not need to invest initial capital in creating servers, hardware, and storage infrastructure from the start, IaaS also reduces maintenance fees and IT services. These kinds of savings are especially productive for mid-range companies; IaaS manages startup cost and provides a pay-as-you-go system that can be cost to scale.

Scaling and flexibility: IaaS offers dynamic scaling and flexibility. Because IaaS providers keep the physical hardware, servers, and storage, companies can add or subtract necessary infrastructure based on their current needs. Companies that see spikes in server usage do not need to allocate infrastructure for their maximum amount of usage. Instead, the IaaS provider can offer the necessary amount of infrastructure at any time. Additionally, IaaS provides flexibility, allowing access in any location or space.

Reducing and innovating IT support: IaaS providers take care of server IT support, letting users focus their IT support on their own software and platform. IaaS allows IT to shift focus to innovating and maintaining applications rather than working with servers and storage. Moreover, IaaS makes hardware more efficient across industries, allowing a minimum amount of hardware to be responsible for a maximum number of businesses and organizations.

Full control of the VM: Because customers control their own virtual machines, they have the flexibility to build their own VM and run any software they'd like. Essentially, users have maximum control over their virtual infrastructure without the overhead costs or large-scale maintenance that hardware requires. In other words, IaaS allows a company to tailor their virtual infrastructure to their needs, framing the architecture in ways that are most proactive and efficient for their company.

There are, of course, specific challenges to working with an IaaS provider. Companies must be able to manage their platforms, applications, and other aspects of their virtual infrastructure. For enterprise-grade businesses, however, IaaS is undeniably the emerging choice for large

scale companies.

Infrastructure as a service (IaaS) can provide dynamic, flexible servers, storage, and hardware for companies that seek to create, modify, and run their own software platforms and applications. IaaS allows companies to use a virtual infrastructure without the large-scale startup costs, IT personnel, and storage space needed to maintain local infrastructure. While IaaS requires businesses to maintain their own platforms and applications, IaaS provides storage, network, and computational hardware for enterprise-level cloud-based computing, available to any amount of users at any time.

Q4:>

Present DC Function Rooms diagrammatically with explanation

Menu

Cart

Home › Archived › What are Data Centers?

WHAT ARE DATA CENTERS?

Oct 05, 2012

SHARE THIS POST

print sharing buttonemail sharing buttonfacebook sharing buttontwitter sharing buttonpinterest sharing buttonsms sharing buttonsharethis sharing button

Data Centers house critical computing resources in controlled environment and under centralized management, which enable enterprises to operate around the clock or according to their business needs.

These computing resources include:

Mainframes

Web and application servers

File and printer servers

Messaging servers

Application software and the operating systems that run them

Storage subsystems

Network Infrastructure (IP or Storage-Area Network (SAN))

Applications range from internal financial and human resources to external e-commerce and business-to-business applications.

Additionally, a number of servers support network operations and network-based applications.

Network operation applications include:

Network Time Protocol (NTP)

TN3270

FTP

Domain Name System (DNS)

Dynamic Host Configuration Protocol (DHCP)

Simple Network Management Protocol (SNMP)

TFTP

Network File System (NFS)

Network-based applications include:

IP telephony

Video streaming over IP

IP video conferencing

and so on …

Virtually, every enterprise has one or more Data Centers. Some have evolved rapidly to accommodate various enterprise application environments using distinct operating systems and hardware platforms. The evolution has resulted in complex and disparate environments that are expensive to manage and maintain.

In addition to the application environment, the supporting network infrastructure might not have changed fast enough to be flexible in accommodating ongoing redundancy, scalability, security, and management requirements.

A Data Center network design lacking in any of these areas risks not being able to sustain the expected service level agreements (SLAs). Data Center downtime, service degradation, or the inability to roll new services implies that SLAs are not met, which leads to a loss of access to critical resources and a quantifiable impact on normal business operation. The impact could be as simple as increased response time or as severe as loss

Data Centers house critical computing resources in controlled environment and under centralized management, which enable enterprises to operate around the clock or according to their business needs.

These computing resources include:

Mainframes

Web and application servers

File and printer servers

Messaging servers

Application software and the operating systems that run them

Storage subsystems

Network Infrastructure (IP or Storage-Area Network (SAN))

Applications range from internal financial and human resources to external e-commerce and business-to-business applications.

Additionally, a number of servers support network operations and network-based applications.

Network operation applications include:

Network Time Protocol (NTP)

TN3270

FTP

Domain Name System (DNS)

Dynamic Host Configuration Protocol (DHCP)

Simple Network Management Protocol (SNMP)

TFTP

Network File System (NFS)

Network-based applications include:

IP telephony

Video streaming over IP

IP video conferencing

and so on ...

Virtually, every enterprise has one or more Data Centers. Some have evolved rapidly to accommodate various enterprise application environments using distinct operating systems and hardware platforms. The evolution has resulted in complex and disparate environments that are expensive to manage and maintain.

In addition to the application environment, the supporting network infrastructure might not have

changed fast enough to be flexible in accommodating ongoing redundancy, scalability, security, and management requirements.

A Data Center network design lacking in any of these areas risks not being able to sustain the expected service level agreements (SLAs). Data Center downtime, service degradation, or the inability to roll new services implies that SLAs are not met, which leads to a loss of access to critical resources and a quantifiable impact on normal business operation. The impact could be as simple as increased response time or as severe as loss of data.

>> DATA CENTER GOALS

The benefits provided by a Data Center include traditional business-oriented goals such as the support for business operations around the clock (resiliency), lowering the total cost of operation and the maintenance needed to sustain the business function (total cost of ownership), and the rapid deployment of applications and consolidation of computing resources (flexibility).

These business goals generate a number of information technology (IT) initiatives, including:

Business continuance

Increased security in the Data Center

Application, server, and Data Center consolidation

Integration of applications whether client/server and multitier (n-tier), or web services –related applications

Storage consolidation

These IT initiatives are a combination of the need to address short-term problems and establishing a long-term strategic direction, all of which require an architectural approach to avoid unnecessary instability if the Data Center network is not flexible enough to accommodate future changes.

The design criteria are:

Availability

Scalability

Security

Performance

Manageability

These design criteria are applied to these distinct functional areas of a Data Center network:

Infrastructure services – Routing, switching, and server-farm architecture

Application services – Load balancing, Secure Socket Layer (SSL) offloading, and caching

Security services – Packet filtering and inspection, intrusion detection, and intrusion prevention

Storage services – SAN architecture, Fibre Channel switching, backup, and archival

Business continuance – SAN extension, site selection, and Data Center interconnectivity

>> DATA CENTER FACILITIES

Because Data Centers house critical computing resources, enterprises must make special arrangements with respect to both the facilities that house the equipment and the personnel required for a 24-by-7 operation.

These facilities are likely to support a high concentration of server resources and network infrastructure. The demands posed by these resources, coupled with the business criticality of the applications, create the need to address the following areas:

Power capacity

Cooling capacity

Cabling

Temperature and humidity controls

Fire and smoke systems

Physical security: restricted access and surveillance systems

Rack space and raised floors

>> ROLES OF DATA CENTERS IN THE ENTERPRISE

Figure 1-1 presents the different building blocks used in the typical enterprise network and illustrates the location of the Data Center within that architecture.

The building blocks of this typical enterprise network include:

Campus network

Private WAN

Remote access

Internet server farm

Extranet server farm

Intranet server farm

image

Data Centers typically house many components that support the infrastructure building blocks, such as the core switches of the campus network or the edge routers of the private WAN.

Data Center designs can include any or all of the building blocks in Figure 1-1, including any or all server farm types. Each type of server farm can be a separate physical entity, depending on the business requirements of the enterprise.

For example, a company might build a single Data Center and share all resources, such as servers, firewalls, routers, switches, and so on. Another company might require that the three server farms be physically separated with no shared equipment.

Enterprise applications typically focus on one of the following major business areas:

Customer relationship management (CRM)

Enterprise Resource Planning (ERP)

Supply chain management (SCM)

Sales force automation (SFA)

Order processing

E-commerce

> DATA CENTER ARCHITECTURE

The enterprise Data Center architecture is inclusive of many functional areas, as presented earlier in Figure 1-1.

The focus of this section is the architecture of a generic enterprise Data Center connected to the Internet and supporting an intranet server farm.

Other types of server farms follow the same architecture used for intranet server farms yet with different scalability, security, and management requirements.

Figure 1-5 *Topology of an Enterprise Data Center Architecture*

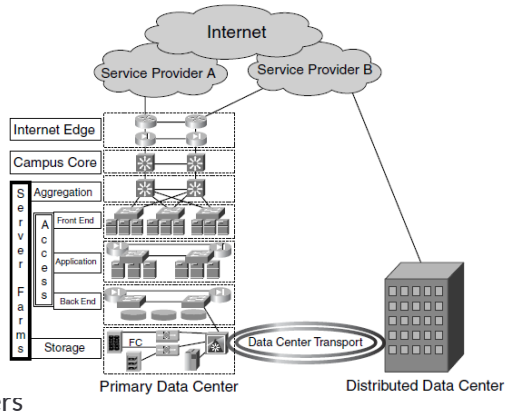


Figure 1-5 sh ting the following areas:

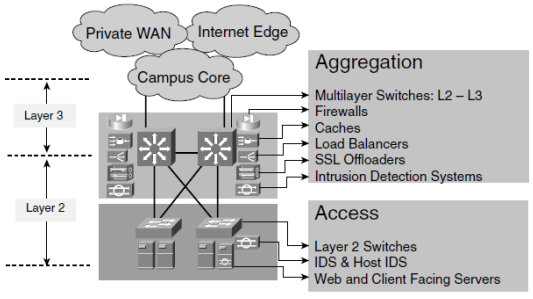
No single-poi

Redundant Data Centers

The core connectivity functions supported by Data Centers are Internet Edge connectivity, campus connectivity, and server-farm connectivity, as presented by Figure 1-5.

> AGGREGATION LAYER

Figure 1-6 *Aggregation and Access Layers*



T ices that provide services to all server farms. These c ancers, and other devices that typically support s

T ion switches because of the aggregation function t ver farms. Specific server farms are likely to span

multiple access switches for redundancy, thus making the aggregation switches the logical connection point for service devices, instead of the access switches.

As depicted in Figure 1-6, the aggregation switches provide basic infrastructure services and connectivity for other service devices. The aggregation layer is analogous to the traditional distribution layer in the campus network in its Layer 3 and Layer 2 functionality.

The aggregation switches support the traditional switching of packets at Layer 3 and Layer 2 in addition to the protocols and features to support Layer 3 and Layer 2 connectivity.