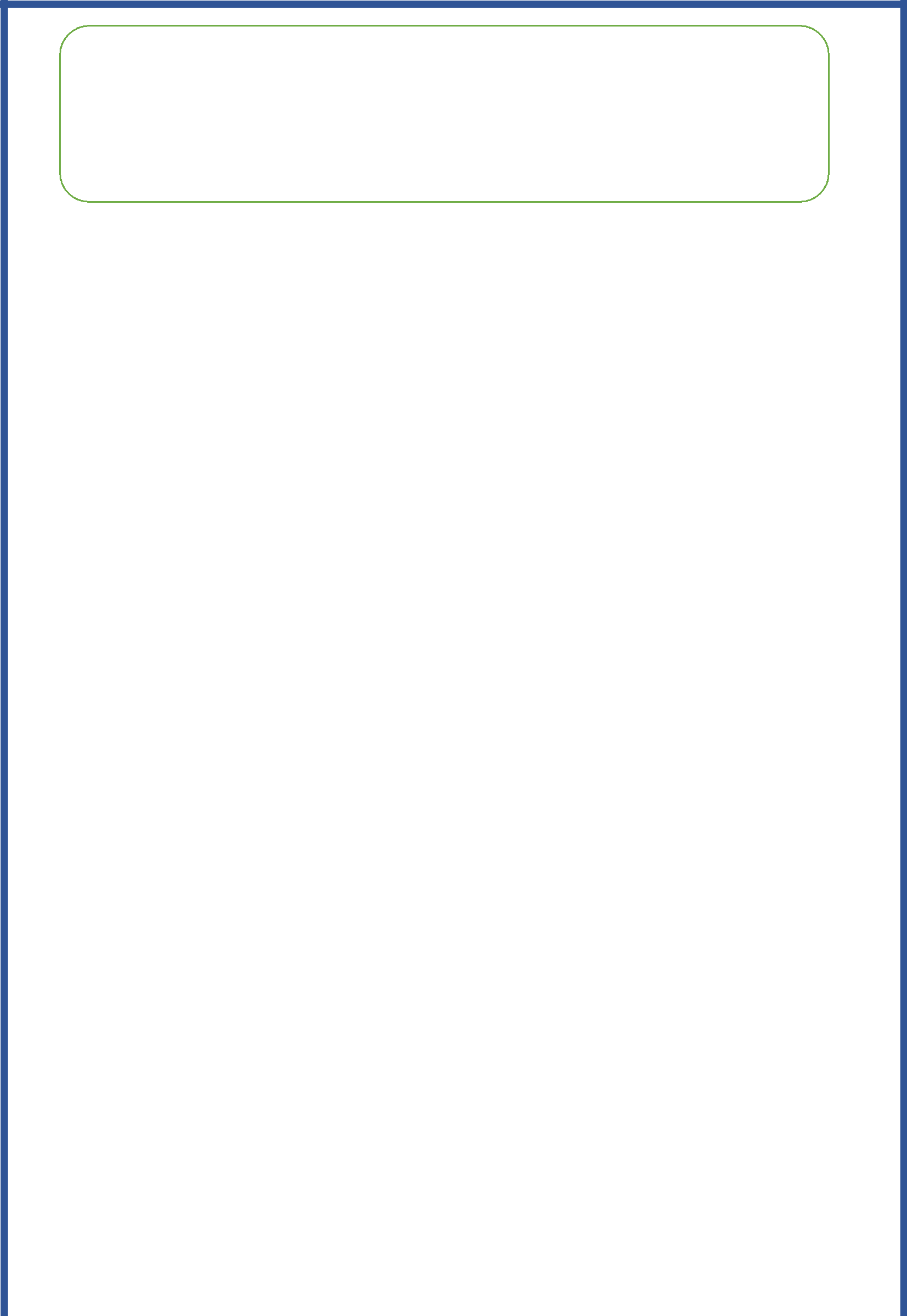
**CLOUD COMPUTING ASSIGNMENT**

**G.S.S.SRI HARSHA** **CSE-B8**

**2210316814**

**1)Write about technology innovations for cloud computing?**

1. **Clustering**
2. **Grid computing**
3. **Virtualizaton**

Ans)

**Clustering**

Server clustering refers to a group of servers working together on one system to provide users with higher availability. These clusters are used to reduce downtime and outages by allowing another server to take over in the event of an outage. Here’s how it works. A group of servers are connected to a single system. The moment one of these servers experiences a service outage, the workload is redistributed to another server before any downtime is experienced by the client. Clustered servers are generally used for applications with frequently updated data with file, print, database and messaging servers ranking as the most commonly used clusters. Overall, clustering servers offer clients a higher level of availability, reliability, and scalability than any one server could possibly offer.

There are three types of server clusters that are classified based on the way in which the cluster system (referred to as a node) is connected to the device responsible for storing configuration data. The three types include a single (or standard) quorum cluster, a majority node set cluster and a single node cluster and are reviewed in more detail below.

1. Single (or Standard) Quorum Cluster: The most commonly used, this cluster is comprised of multiple nodes with one or more cluster disk arrays that utilize a single connection device (called a bus). One server manages and owns each of the individual cluster disk arrays within the cluster.
2. Majority Node Set Cluster: Similar to the above cluster, this model differs in that each of the nodes owns its own copy of the cluster’s configuration data, and this data is consistent across all nodes. This model works best for clusters with individual servers that are located in different geographic locations.
3. Single Node Cluster: Most often used for testing purposes, this model contains a single

node.

**Grid computing**

Grid computing is a distributed architecture of large numbers of computers connected to solve a complex problem. In the grid computing model, servers or personal computers run

independent tasks and are loosely linked by the Internet or low-speed networks. Computers may connect directly or via scheduling systems.

The grid computing architecture can bring massive processing power to bear on a problem, as SETI and other similar projects have shown. Middleware makes creating and controlling grids easier. SETI@home, for example, uses BOINC open source grid computing software. Projects build on these tools by adding user-friendly GUIs and a mechanism to distribute raw data and receive and store results.

The grid computing concept differs from parallel computing in supercomputers. Supercomputers run highly connected applications, rather than independently functional nodes. They operate over high-speed networks, and are typically housed in one specialized data center. Grid computers, on the other hand, exchange little or no data and feed the project over Internet connections from geographically dispersed locations.

**Virtualization**

Virtualization is the creation of a [virtual](https://searchservervirtualization.techtarget.com/definition/virtual) -- rather than actual -- version of something, such as an [operating system,](https://whatis.techtarget.com/definition/operating-system-OS) a [server,](https://whatis.techtarget.com/definition/server) a storage device or network resources.

You probably know a little about virtualization if you have ever divided your [hard drive](https://searchstorage.techtarget.com/definition/hard-disk-drive) into different partitions. A [partition](https://searchstorage.techtarget.com/definition/partition) is the logical division of a hard disk drive to create, in effect, two separate hard drives.

**The evolution of virtualization**

Operating system virtualization is the use of software to allow a piece of hardware to run multiple operating system images at the same time. The technology got its start on mainframes decades ago, allowing administrators to avoid wasting expensive processing power.

1. **Write short notes on the following a)goals and benefits of cloud computing b)risks and challenges of cloud computingans) Ans)**

**Benefits of Cloud Computing in Business**

**Secure**

Best-in-class cloud management and business solutions provide maximum security for customers' peace of mind and digitalization opportunities.

**Flexible**

Cloud integration strategies offer adaptable and customized transformations to the cloud based on the timeframes and methods our customers choose.

**Scalable**

Operational benefits of cloud include reducing time-to-market and connecting distributed, cross-disciplinary teams while improving effectiveness and efficiency at any scale.

**Simple**

Cloud managed PLM provides seamless integrations and operations. Our cloud software portfolio resolves complex issues with sophisticated yet unintimidating cloud technology.

**Affordable**

Economic benefits of the cloud translate to new revenue streams. Small businesses can grow while maintaining the bottom line, while large enterprises can build and extend cloud investments.

**Innovative**

Digitalization in cloud computing helps drive business forward with both speed and agility while continuing to maintain the highest of quality standards.

Challenges and Risks in Cloud Computing

**Cloud Migration**

Cloud migration is the process of moving data, applications, and other important information of an organization from its on-premises either desktops or servers to the cloud infrastructure, and this can also involve in moving data between different cloud setups.

Cloud migration enables all the computing capabilities those were performed earlier by devices installed on-premises. Cloud migration is a big challenge as many companies when they require to migrate from on-premises to cloud or from one cloud to another, they partner with experienced cloud service provider.

**Incompatibility:**

During moving workloads from on-premises to the cloud, the common issue the incompatibility between on-premises infrastructure and the services which are companies going to buy from the public cloud providers. In last current years, most CSPs tried to create “connectors of sort” to make practices more standardize and homogenous.

**Data security:**

CSPs are responsible to provide clouds’ security, but they’re not responsible for your apps, servers, and security of data. As per CDW 2013 State of the Cloud Report, “46 percent of respondents face security of data or applications as a significant challenge.”

When your CSP ensure you about the complete compliance and regulation, don’t consider it as 100% compliant and yielding. You still require to encrypt and secure your own data and should invest in buying suite of tools from your CSP to protect your data from cyber-attacks.

Following questions may be asked before engaging with your cloud service provider.

* Can you ensure protection of my data?
* How will you protect my data from corruption?
* Do you have experts and professionals on board if something happens wrong?

**Lack of expertise:**

With the quick advancements and improvements in cloud technologies, more and more organizations are clouds to place their workloads. However, they face difficulties to keep up with the tools which require particular expertise. Organizations can deal with this challenge by providing cloud technologies training to their sys admins along with development staff.

By adding cloud specialists to IT teams may be costly too for small and medium businesses (SMBs). Luckily, various routine activities that specialists perform can be automated using automated tools. Now, many organizations are also moving to DevOps tools, like Puppet and Chef due to their multi-tasking and automation capabilities such as monitoring resource usage, automating backups etc. These automating tools considerably contribute to cloud optimization for cost, security, and governance.

**Downtime:**

Businesses suppose complete data accessibility and availability when their data is stored on cloud anytime from anywhere. The main challenge most organizations face is they can access their data from cloud only through internet connection. So, poor internet connection can disrupt cloud services and higher risks of data accessibility.

**Bandwidth Cost:**

Though organizations and businesses can save money on hardware using cloud, but they have to pay extra for the bandwidth they use to access their workloads. However, it doesn’t charge much for smaller apps, but data-intensive apps need more bandwidth which can costs higher.

**3 . write about multitenant technology and service technology**

**Ans)**

**multi-tenant cloud**

A multi-tenant [cloud](https://searchstorage.techtarget.com/definition/cloud-storage) is a cloud computing architecture that allows customers to share computing resources in a [public](https://searchcloudcomputing.techtarget.com/definition/public-cloud) or [private cloud.](https://searchcloudcomputing.techtarget.com/definition/private-cloud) Each tenant's data is isolated and remains invisible to other tenants.

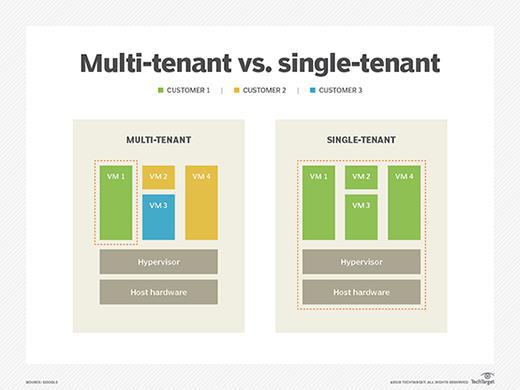
In a multi-tenant cloud system, users have individualized space for storing their projects and data. Each section of a cloud network with multi-tenant architecture includes complex permissions with the intention of allowing each user access to only their stored information along with security from other cloud tenants. Within the [cloud infrastructure,](https://searchcloudcomputing.techtarget.com/definition/cloud-infrastructure) each tenant's data is inaccessible to all other tenants, and can only be reached with the cloud provider's permissions.

**Multi-tenant cloud vs single-tenant cloud**

In a single-tenant cloud, only one customer is hosted on a server and is granted access to it. Due to multi-tenancy architectures hosting multiples customers on the same servers, it is important to fully understand the security and performance the provider is offering. Single-tenant clouds give customers more control over the management of data, storage, security and performance.

**Benefits of multi-tenant cloud**

Multi-tenant cloud networks provide increased storage and improved access compared to [single-tenancy](https://searchcloudcomputing.techtarget.com/definition/single-tenancy) clouds that include limited access and security parameters. Multi-tenancy in cloud computing makes a greater pool of resources available to a larger group of people without sacrificing privacy and security or slowing down applications. The [virtualization](https://searchservervirtualization.techtarget.com/definition/virtualization) of storage locations in cloud computing allows for flexibility and ease of access from almost any device or location.



**Service technology** refers to the use of **service**s for software development, where a **service** isan autonomous, platform agnostic software component that operates within an ecosystem of **service**s. The ecosystem is governed by a **service**-oriented architecture, which relies on the composition of loosely coupled **service**s to achieve complex functionality.

**4)** **Describe about cloud usage monitor and resource replication?**

Cloud monitoring is the process of evaluating, monitoring, and managing cloud-based services, applications, and infrastructure. Companies utilize various [application monitoring](https://stackify.com/application-performance-management-tools/) [tools](https://stackify.com/application-performance-management-tools/) to monitor cloud-based applications. Here’s a look at how it works and best practices for success.

Types of Cloud Services to Monitor

There are multiple types of cloud services to monitor. Cloud monitoring is not just about monitoring servers hosted on AWS or Azure. For enterprises, they also put a lot of importance into monitoring cloud-based services that they consume. Including things like Office 365 and others.

* **SaaS** –Services like Office 365, Salesforce and others
* **PaaS** –Developer friendly services like SQL databases, caching, storage and more
* **IaaS** –Servers hosted by cloud providers like Azure, AWS, Digital Ocean, and others
* **FaaS** –New serverless applications like AWS Lambda and Azure Functions
* **Application Hosting** –Services like Azure App Services, Heroku, etc

Many of these can be monitored usually traditional [application performance](https://stackify.com/what-is-application-performance-monitoring/) [monitoring](https://stackify.com/what-is-application-performance-monitoring/) tools. However, [cloud monitoring has some unique requirements](https://stackify.com/cloud-monitoring-vs-server-monitoring/) over basic [server monitoring tools.](https://stackify.com/top-server-monitoring-tools/) There are also companies like [Exoprise](https://www.exoprise.com/) who focus on monitoring Office 365, Salesforce and other services.

Resource replication

Replication in computing can refer to:

* *data replication*, where the same data is stored on multiple[storage devices](https://en.wikipedia.org/wiki/Data_storage_device)
* *computation replication*, where the same computing task is executed many times.Computational tasks may be:

o *replicated in space*, where tasks are executed on separate devices

o *replicated in time*, where tasks are executed repeatedly on a single device

Replication in space or in time is often linked to scheduling algorithms.[[1]](https://en.wikipedia.org/wiki/Replication_(computing)#cite_note-1)

Access to a replicated entity is typically uniform with access to a single non-replicated entity. The replication itself should be [transparent](https://en.wikipedia.org/wiki/Transparency_(human-computer_interaction)) to an external user. In a failure scenario, a [failover](https://en.wikipedia.org/wiki/Failover) of replicas should be hidden as much as possible with respect to [quality of](https://en.wikipedia.org/wiki/Quality_of_service) [service](https://en.wikipedia.org/wiki/Quality_of_service) (QoS)[.[2]](https://en.wikipedia.org/wiki/Replication_(computing)#cite_note-2)

Computer scientists further describe replication as being either:

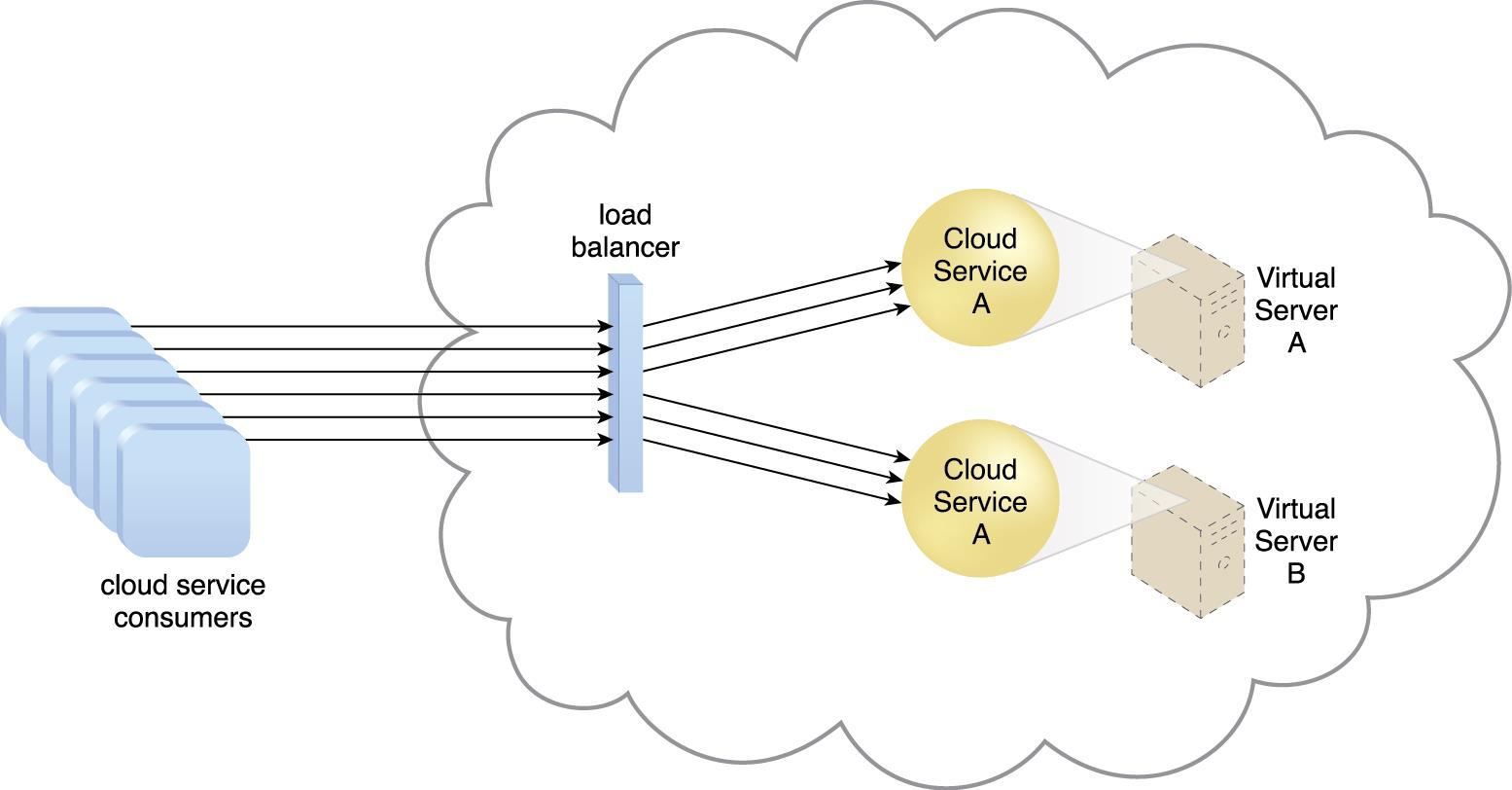
* *active replication*, which is performed by processing the same request at every replica
* *passive replication*, which involves processing every request on a single replica andtransferring the result to the other replicas

When one master replica is designated to process all the requests, the system is using a primary-backup or [master-slave](https://en.wikipedia.org/wiki/Master-slave_(computers)) scheme, which is predominant in [high-availability clusters.](https://en.wikipedia.org/wiki/High-availability_cluster) In comparison, if any replica can process a request and distribute a new state, the system is using a multi-primary or [multi-master](https://en.wikipedia.org/wiki/Multi-master_replication) scheme. In the latter case, some form of [distributed](https://en.wikipedia.org/wiki/Distributed_concurrency_control) [concurrency control](https://en.wikipedia.org/wiki/Distributed_concurrency_control) must be used, such as a [distributed lock manager.](https://en.wikipedia.org/wiki/Distributed_lock_manager)

**5 ) fundalmental cloud architechtures:**

**Workload Distribution Architecture**

1. IT resources can be horizontally scaled by adding one or more identical IT resources, and a load balancer provides runtime logic to distribute the workload among the available IT resources (Figure 11.1).
2. The resulting ***workload distribution architecture*** *reduces both IT resource* *overutilization* and under-utilization to an extent dependent upon the sophisticationof the load balancing algorithms and runtime logic.



* **Figure 1 A redundant copy of Cloud Service A is implemented on Virtual Server B. The load balancer intercepts cloud service consumer requests and directs them to both Virtual Servers A and B to ensure even workload distribution.** This fundamental

architectural model can be applied to any IT resource, with workload distribution commonly carried out in support of distributed virtual servers, cloud storage devices, and cloud services.

* Load balancing systems applied to specific IT resources usually produce specialized variations of this architecture that incorporate aspects of load balancing, such as:
  + the service load balancing architecture
  + the load balanced virtual server architecture
  + the load balanced virtual switches architecture

Load balancing also can be applied to the virtual server and Cloud storage device. The following mechanisms can also be part of this cloud architecture:

* ***Audit Monitor*** *–**When distributing runtime workloads, the type and*geographicallocation of the IT resources that process the data can determine whether monitoring is necessary to fulfil legal and regulatory requirements.
* ***Cloud Usage Monitor*** *–**Various monitors can be involved to carry out*runtimeworkload tracking and data processing.
* ***Logical Network Perimeter*** *–**The logical network perimeter isolates cloud*consumernetwork boundaries in relation to how and where workloads are distributed.
* ***Resource Cluster*** *–**Clustered IT resources inactive/active mode are*commonly used tosupport workload balancing between different cluster nodes.
* ***Resource Replication*** *–**This mechanism can generate new instances of*virtualized ITresources in response to runtime workload distribution demands.

**Redundant Storage Architecture**

Cloud storage devices are occasionally subject to failure and disruptions that are caused by network connectivity issues, controller or general hardware failure, or security breaches.

A compromised cloud storage device’s reliability can have a ripple effect and cause impact failure across all of the services, applications, and infrastructure components in the cloud that are reliant on its availability.

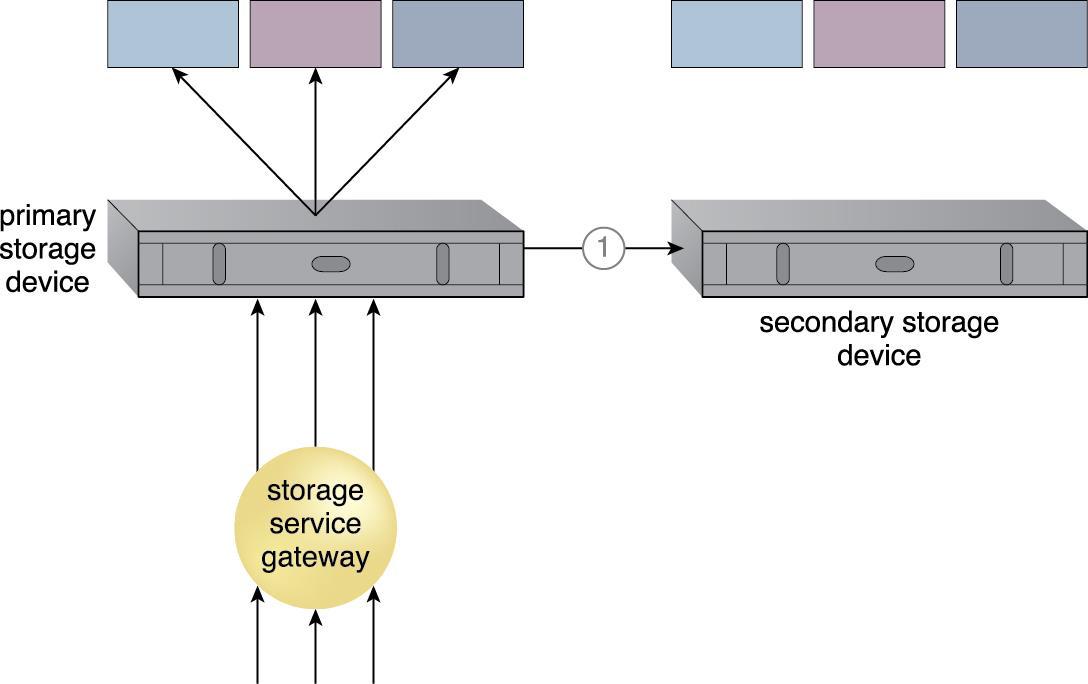
LUN: A logical unit number (LUN) is a logical drive that represents a partition of a physical drive.

Service Gateway: The storage service gateway is a component that acts as the external interface to cloud storage services, and is capable of automatically redirecting cloud consumer requests whenever the location of the requested data has changed.

The *redundant storage architecture introduces a secondary duplicate cloud* storage device as part of a failover system that synchronizes its data with the data in the primary cloud storage deviceLUN: A logical unit number (LUN) is a logical drive that represents a partition of a physical drive.

Storage Service Gateway: The storage service gateway is a component that acts as the external interface to cloud storage services, and is capable of automatically **redirecting cloud** **consumer requests whenever the location of the requested data has changed.**

A storage service gateway diverts cloud consumer requests to the secondary device whenever the primary device fails (Figures 11.16 and 11.17).



**Figure 11.16. The primary cloud storage device is routinely replicated to the secondary cloud storage device (1).**

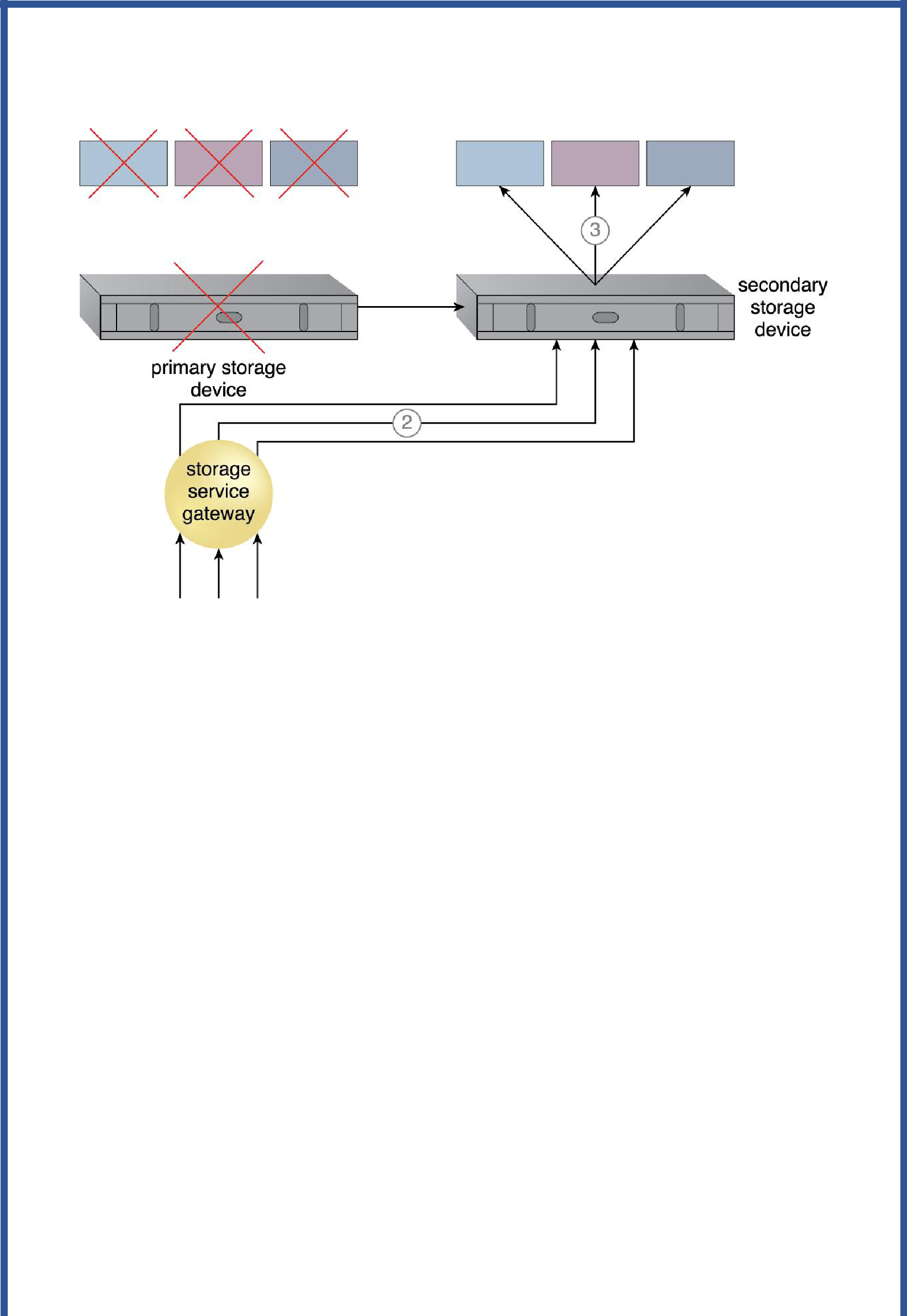


Figure 11.17. The primary storage becomes unavailable and the storage service gateway forwards the cloud consumer requests to the secondary storage device (2). The secondary storage device forwards the requests to the LUNs, allowing

cloud consumers to continue to access their data (3).

* This cloud architecture primarily relies on a **storage replication system** that keeps the primary cloud storage device synchronized with its duplicate secondary cloud storage devices (Figure 11.18).
* **Storage Replication:** Storage replication is a variation of the resource replicationmechanisms used to synchronously or asynchronously replicate data from a primary storage device to a secondary storage device. It can be used to replicate partial and entire LUNs.

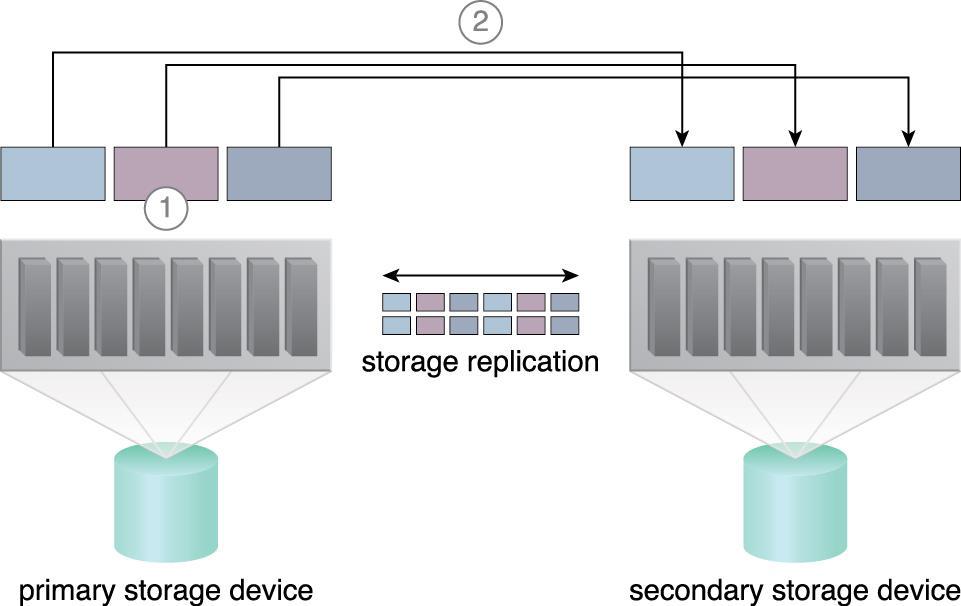


Figure 11.18. Figure 11.18. Storage replication is used to keep the redundant storage device synchronized with the primary storage device.

Cloud providers may locate secondary cloud storage devices in a different geographical region than the primary cloud storage device, usually for economic reasons.

However, this can introduce legal concerns for some types of data.

The location of the secondary cloud storage devices can dictate the protocol and method used for synchronization, as some replication transport protocols have distance restrictions.

Some cloud providers use storage devices with dual array and storage controllers to improve device redundancy, and place secondary storage devices in a different physical location for cloud balancing and disaster recovery purposes.

In this case, cloud providers may need to lease a network connection via a third-party cloud provider in order to establish the replication between the two devices.

**6. Building IaaS Environments**

The virtual server and cloud storage device mechanisms are the two most fundamental IT resources that are delivered as part of a standard rapid provisioning architecture within IaaS environments.

They are offered in various standardized configurations that are defined by the following properties:

* operating system
* primary memory capacity
* processing capacity
* virtualized storage capacity
* Memory and virtualized storage capacity is usually allocated with increments of 1 GB to simplify the provisioning of underlying physical IT resources.
* When limiting cloud consumer access to virtualized environments, IaaS offerings are pre-emptively assembled by cloud providers via virtual server images that capture the pre-defined configurations.
* Some cloud providers may offer cloud consumers direct administrative access to physical IT resources, in which case the bare-metal provisioning architecture may come into play.
* Snapshots can be taken of a virtual server to record its current state, memory, and configuration of a virtualized IaaS environment for backup and replication purposes, in support of horizontal and vertical scaling requirements.
* For example, a virtual server can use its snapshot to become reinitialized in another hosting environment after its capacity has been increased to allow for vertical scaling.
* The snapshot can alternatively be used to duplicate a virtual server.
* The remote administration system mechanism manages the virtual server images.

* Cloud providers support importing and exporting options for custom-built virtual server images in both proprietary and standard formats.
* Data Centers:
* Cloud providers can offer IaaS-based IT resources from multiple geographically diverse data centers, which provides the following primary benefits:
* Multiple data centers can be linked together for increased resiliency.
* Each data center is placed in a different location to lower the chances of a single failure forcing all of the data centers to go offline simultaneously.
* Connected through high-speed communications networks with low latency, data centers can perform load balancing, IT resource backup and replication, and increase storage capacity, while improving availability and reliability.

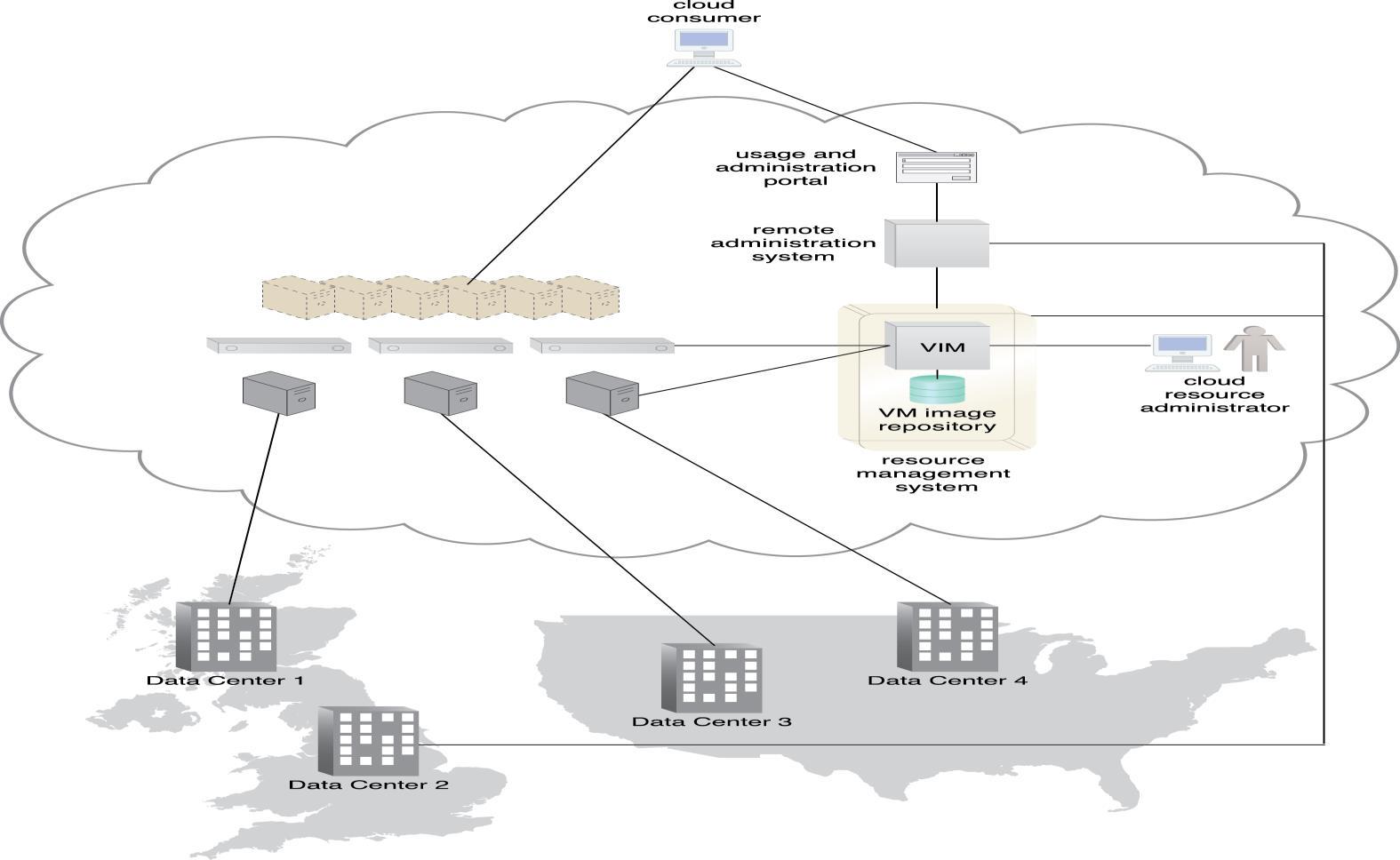


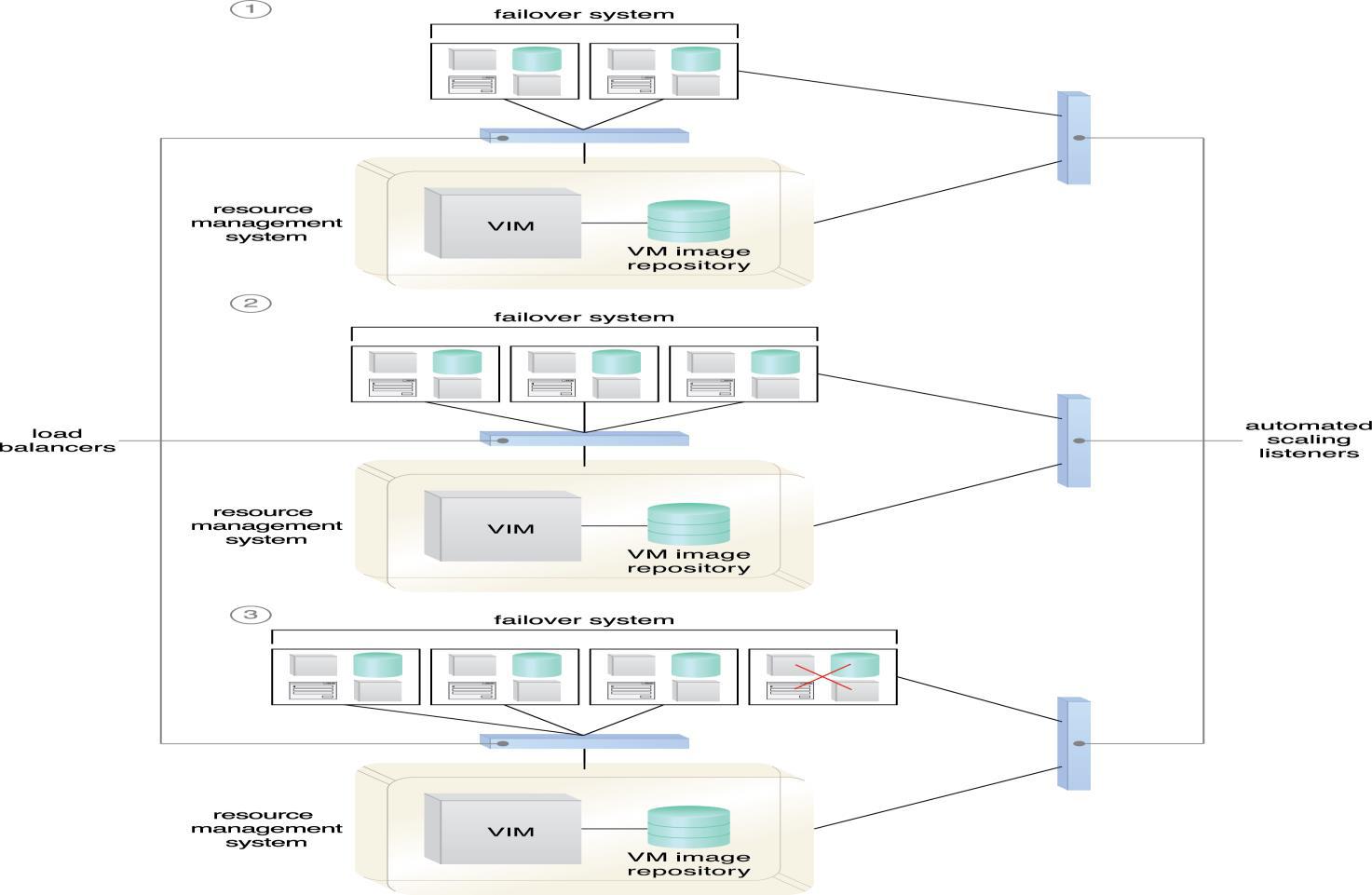
Figure 14.1: provides an example of a cloud provider that is managing four data centers that are split between two different geographic regions.

Equipping PaaS Environments

* PaaS environments selects the application development and deployment platforms in order to accommodate different programming models, languages, and frameworks.

* A separate ready-made environment is created for each programming stack that contains the necessary software to run applications specifically developed for the platform.
* Each platform is accompanied by a matching SDK and IDE, which can be custom-built or enabled by IDE plugins supplied by the cloud provider.
* IDE toolkits can simulate the cloud runtime locally within the PaaS environment and usually include executable application servers.
* The security restrictions that are inherent to the runtime are also simulated in the development environment, including checks for unauthorized attempts to access system IT resources.
* Cloud providers often offer a resource management system mechanism that can create and control customized virtual server images with ready-made environments.
* This mechanism also manages deployed applications and configuring multitenancy.
* Cloud providers further rely on a variation of the rapid provisioning architecture known as platform provisioning, which is designed specifically to provision ready-made environments.
* Scalability and Reliability
* The scalability requirements of cloud services and applications that are deployed within PaaS environments are generally addressed via dynamic scalability and workload distribution architectures by using native automated scaling listeners and load balancers.
* The resource pooling architecture is further utilized to provision IT resources from resource pools made available to multiple cloud consumers.
* Cloud providers can evaluate network traffic and server-side connection usage against the instance’s workload, when determining how to scale an overloaded application as per parameters and cost limitations provided by the cloud consumer.
* Alternatively, cloud consumers can configure the application designs to customize the incorporation of available mechanisms themselves.
* The reliability of ready-made environments and hosted cloud services and applications can be supported with standard failover system mechanisms (Figure 14.2), and non-disruptive service relocation architecture, to shield cloud consumers from failover conditions.
* The resource reservation architecture offers exclusive access to PaaS-based IT resources.
* As with other IT resources, ready-made environments can also span multiple data centers and geographical regions to further increase availability and resiliency.
* Security

* The PaaS environment, by default, does not usually introduce the need for new cloud security mechanisms beyond those that are already provisioned for IaaS environments.



•

**Monitoring**

Specialized cloud usage monitors in PaaS environments are used to monitor the following:

* ***Ready-Made Environment Instances*** *–**The applications of these instances*are recorded bypay-per-use monitors for the calculation of time-based usage fees.
* ***Data Persistence*** *–*This statistic is provided by pay-per-use monitors*that record the number**of objects, individual occupied storage sizes, and database transactions* per billing period.
* ***Network Usage*** *–**Inbound and outbound network usage is tracked for pay-per-*use monitorsand SLA monitors that track network-related QoS metrics.
* ***Failure Conditions*** *–*SLA monitors that track*the QoS metrics of IT resources need to capture**failure statistics.*
* ***Event Triggers*** *–*This metric is primarily used by audit monitors that need to*respond to**certain types of events*.

1. **Working with IaaS Environments**
   * Virtual servers are accessed at the operating system level through the use of remote terminal applications.
   * Accordingly, the type of client software used directly depends on the type of operating system that is running at the virtual server, of which two common options are:
   * ***Remote Desktop (or Remote Desktop Connection) Client*** *–**for Windowsbased*environments and presents a Windows GUI desktop
   * ***SSH Client*** *–**for Mac and other Linux-based environments to allow for*secure channelconnections to text-based shell accounts running on the server OS
   * Figure 14.4 illustrates a typical usage scenario for virtual servers that are being
   * offered as IaaS services after having been created with management interfaces.

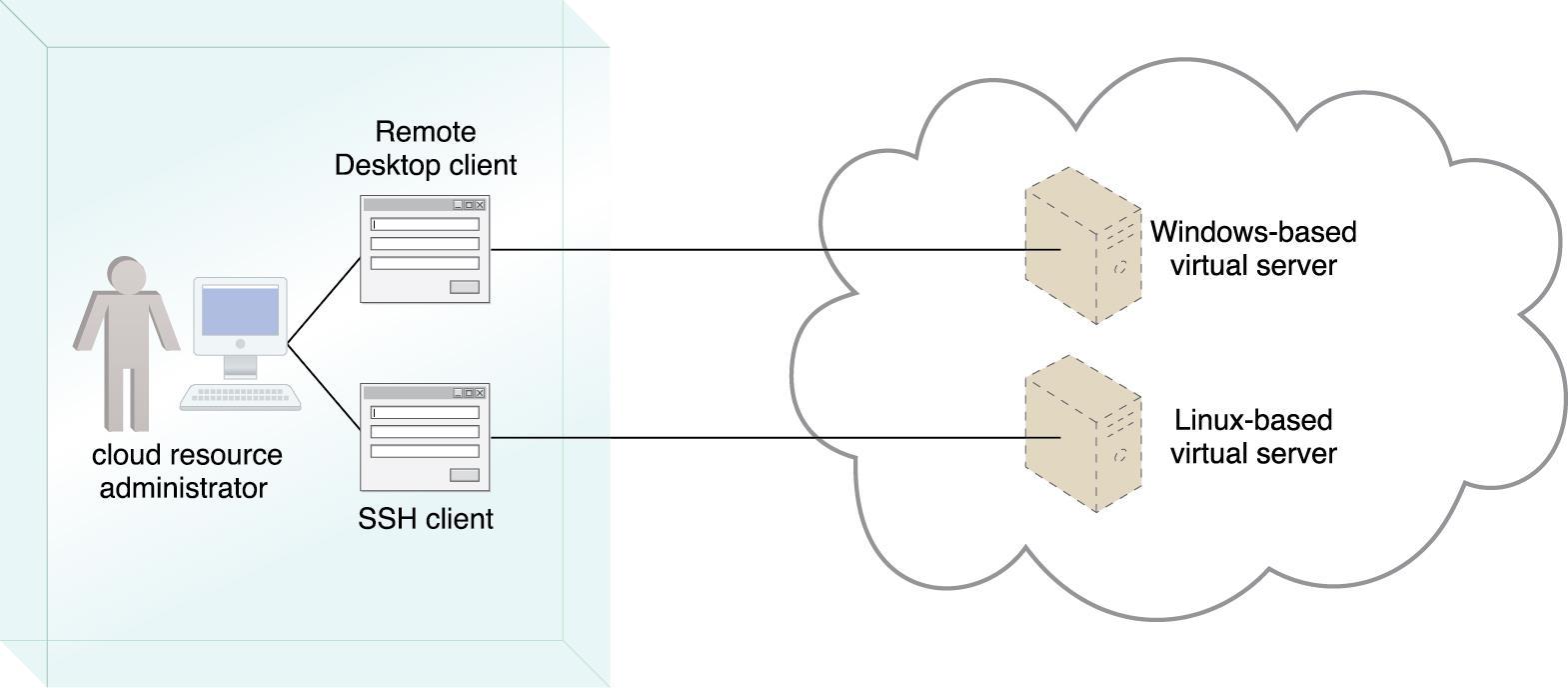


Figure 14.4. A cloud resource administrator uses the Windows-based Remote Desktop client to administer a Windows-based virtual server and the SSH client for the Linux-based virtual server.

A cloud storage device can be attached directly to the virtual servers and accessed through the virtual servers’ functional interface for management by the operating system.

Alternatively, a cloud storage device can be attached to an IT resource that is being hosted outside of the cloud, such as an on-premise device over a WAN or VPN.

In these cases, the following formats for the manipulation and transmission of cloud storage data are commonly used:

*Networked File System – System-based storage access, whose rendering of* files is similar tohow folders are organized in operating systems (NFS, CIFS)

* *Storage Area Network Devices – Block-based storage access collates and* formatsgeographically diverse data into cohesive files for optimal network transmission (iSCSI, Fibre Channel)
* *Web-Based Resources – Object-based storage access by which an interface* that is notintegrated into the operating system logically represents files, which can be accessed through a Web-based interface (Amazon S3)

**IT Resource Provisioning Considerations**

Cloud consumers have a high degree of control over how and to what extent IT resources are provisioned as part of their IaaS environments.

For example:

* controlling scalability features (automated scaling, load balancing)
* controlling the lifecycle of virtual IT resources (shutting down, restarting, powering up of virtual devices)
* controlling the virtual network environment and network access rules (firewalls, logical network perimeters)
* establishing and displaying service provisioning agreements (account conditions, usage terms)
* *Web-Based Resources – Object-based storage access by which an interface* that is notintegrated into the operating system logically represents files, which can be accessed through a Web-based interface (Amazon S3)

**IT Resource Provisioning Considerations**

Cloud consumers have a high degree of control over how and to what extent IT resources are provisioned as part of their IaaS environments.

For example:

* controlling scalability features (automated scaling, load balancing)
* controlling the lifecycle of virtual IT resources (shutting down, restarting, powering up of virtual devices)
* controlling the virtual network environment and network access rules (firewalls, logical network perimeters)
* establishing and displaying service provisioning agreements (account conditions, usage terms)

**Working with PaaS Environments**

* A typical PaaS IDE can offer a wide range of tools and programming resources, such as software libraries, class libraries, frameworks, APIs, and various runtime capabilities that emulate the intended cloud-based deployment environment.
* These features allow developers to create, test, and run application code within the cloud or locally (on-premise) while using the IDE to emulate the cloud deployment environment.
* Compiled or completed applications are then bundled and uploaded to the cloud, and deployed via the ready-made environments.
* This deployment process can also be controlled through the IDE.
* PaaS also allows for applications to use cloud storage devices as independent data storing systems for holding development-specific data (for example in a repository that is available outside of the cloud environment).
* Both SQL and NoSQL database structures are generally supported.

**IT Resource Provisioning Considerations**

* PaaS environments provide less administrative control than IaaS environments, but still offer a significant range of management features.

For example:

* establishing and displaying service provisioning agreements, such as account conditions and usage terms
* selecting software platform and development frameworks for ready-made environments
* selecting instance types, which are most commonly frontend or backend instances
* selecting cloud storage devices for use in ready-made environments
* controlling the lifecycle of PaaS-developed applications (deployment, starting, shutdown, restarting, and release)
* controlling the versioning of deployed applications and modules
  + The usage and administration portal that is used to access PaaS management features can provide the feature of pre-emptively selecting the times at which an IT resource is started and stopped.
  + For example, a cloud resource administrator can set a cloud storage device to turn itself on at 9:00AM then turn off twelve hours later.
  + Building on this system can enable the option of having the readymade environment self-activate upon receiving data requests for a particular application and turn off after an extended period of inactivity.

**Working with SaaS Services**

* Because SaaS-based cloud services are almost always accompanied by refined and generic APIs, they are usually designed to be incorporated as part of larger distributed solutions.

* A common example of this is Google Maps, which offers a comprehensive API that enables mapping information and images to be incorporated into Web sites and Web-based applications.
* Many SaaS offerings are provided free of charge, although these cloud services often come with data collecting sub-programs that harvest usage data for the benefit of the cloud provider.
* When using any SaaS product that is sponsored by third parties, there is a reasonable chance that it is performing a form of background information gathering.
* Reading the cloud provider’s agreement will usually help shed light on any secondary activity that the cloud service is designed to perform.
* For example:
* • managing security-related configurations
* • managing select availability and reliability options
* • managing usage costs
* • managing user accounts, profiles, and access authorization
* • selecting and monitoring SLAs
* • setting manual and automated scalability options and limitations

**8 ) Cloud deployment models**

Cloud is the future of computing. It is about outsourcing of IT services and infrastructure to make them accessible remotely via the Internet. Utilizing cloud-computing models boosts not only productivity but also provide a competitive edge to organizations. The growing popularity of cloud computing has given rise to different types of cloud service deployment models and strategies. Therefore, today there exists a variety of enterprise cloud solutions depending on the degree of desired outsourcing needs.

So, read on as we cover the various cloud computing deployment and service models. It is along with their customization flexibility, control, and data management within the organization. Further, it involves the pooling of specialized human and technical resources to effectively manage existing systems and applications as it helps in meeting the requirements of organizations and users.

**Different Types Of Cloud Computing Deployment Models:**

Most cloud hubs have tens of thousands of servers and storage devices to enable fast loading. It is often possible to choose a geographic area to put the data “closer” to users. Thus, deployment models of cloud computing are categorized based on their location. To know which deployment model would best fit the requirements of your organization, let us first learn about the types of cloud deployment models.



**Private Cloud**

It is a cloud-based infrastructure used by stand-alone organizations. It offers greater control over security. The data is backed up by a firewall and internally, and can be hosted internally or externally. Private clouds are perfect for organizations that have high-security requirements, high management demands, and availability requirements.

**Public Cloud**

This type of cloud services is provided on a network for public use. Customers have no control over the location of the infrastructure. It is based on a shared cost model for all the users, or in the form of a licensing policy such as pay per user. Public deployment models in the cloud are perfect for organizations with growing and fluctuating demands. It is also popular among businesses of all sizes for their [web applications,](https://www.rishabhsoft.com/web-application) webmail, and storage of non-sensitive data.

**Community Cloud**

It is a mutually shared model between organizations that belong to a particular community such as banks, government organizations, or commercial enterprises. Community members generally share similar issues of privacy, performance, and security. This type of deployment model of cloud computing is managed and hosted internally or by a third-party vendor.

**Hybrid Cloud**

This model incorporates the best of both private and public clouds, but each can remain as separate entities. Further, as part of this deployment of cloud computing model, the internal, or external providers can provide resources. A hybrid cloud is ideal for scalability, flexibility, and security. A perfect example of this scenario would be that of an organization who uses the private cloud to secure their data and interacts with its customers using the public cloud.

