

**Lecture Note
On
Cloud Computing**

CONTENTS

SL No.	TOPICS	PAGE
1	INTRODUCTION TO CLOUD COMPUTING	1-14
2	CLOUD COMPUTING ARCHITECTURE	15-21
3	SCALABILITY AND FAULT TOLERANCE	22-28
4	CLOUD MANAGEMENT AND VIRTUALISATION TECHNOLOGY	28-33
5	VIRTUALISATION	33-38
6	CLOUD SECURITY	39-43
7	CLOUD COMPUTING SECURITY ARCHITECTURE	44-51
8	MARKET BASED MANAGEMT OF CLOUDS	52-56
9	HADOOP	57-58

UNIT-1

Introduction to Cloud Computing

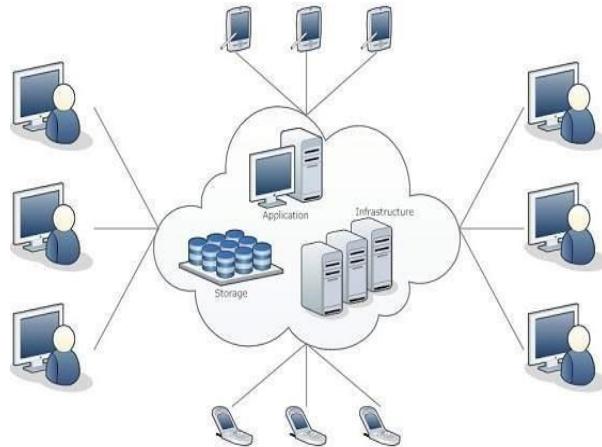
Cloud Computing is the combination of **Network** with **Internet**. It is a technology which is **manipulating, configuring, and accessing** the hardware and software resources remotely. It offers online data storage, infrastructure, and application. It is the on-demand delivery of IT resources over the Internet.

Instead of buying, owning, and maintaining physical data centres and servers, one can access technology services, such as computing power, storage, and databases, on an as-needed basis from a cloud server.

Cloud computing offers **platform independency**, that means software is not required to be installed in a local PC.

In a cloud computing system the Remote Servers are responsible for running everything from e-mail to word processing to complex data analysis programs for the client users and all the computing process owned by another company.

Cloud can provide services over public and private networks, i.e., WAN, LAN or VPN. Applications like e-mail, web conferencing, customer relationship management (CRM) executes on cloud.



Advantages of Cloud Computing

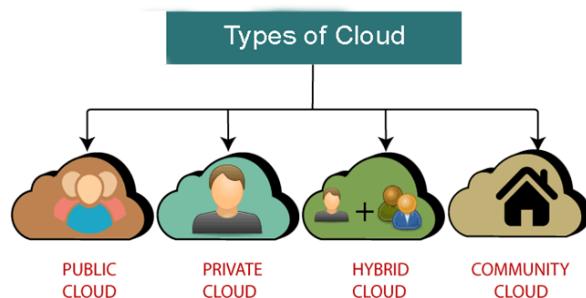
- Back-up and restore data: Once the data is stored in the cloud, it is easier to get back-up and restore that data using the cloud computing technology.
- Improved collaboration: Cloud applications have improved collaboration by allowing groups of people to share information in the cloud quickly and easily.
- Excellent accessibility: It allows us to access and store data or information quickly and easily from anywhere and anytime using internet connection. Ultimately it increases the productivity and efficiency of the organization.
- Low maintenance cost: Cloud computing reduces both hardware and software maintenance costs for an organization.
- Mobility: Cloud computing allows us to easily access all cloud data while on roaming.
- Unlimited storage capacity: Cloud offers us a huge amount of storage capacity for storing our data such as documents, images, audio, video, etc. in one place.
- Data security: Data security is one of the biggest advantages of cloud computing. Cloud offers many advanced features related to security and ensures that the data is safe.

Disadvantages of Cloud Computing

- Internet Connectivity: Cloud Server can be accessed only through internet. So if there is no good internet connectivity or no internet connection, than the data cannot be accessed properly.
- Vendor lock-in: Vendor lock-in is the biggest disadvantage of cloud computing. Organizations may face problems when transferring their services from one vendor to another. As different vendors provide different platforms, that creates a problem to move data from one cloud to another.
- Limited Control: As we know, cloud infrastructure is completely owned, managed, and monitored by the service provider, so the cloud users have less control on the cloud servers.
- Security: Although cloud service providers implement the best security standards, but before adopting cloud technology, the organization must be aware that they are handing over all the organization's sensitive information to a third party, which is a cloud computing service provider. While sending the data on the cloud, there may be a chance that your organization's information is hacked by Hackers.

Types of Cloud

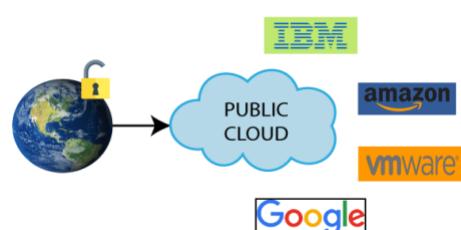
There are the following 4 types of cloud that you can deploy according to the organization's requirements.



Public Cloud

Public cloud is **open to all** to store and access information through Internet using the pay-per-usage method. In public cloud, computing resources are managed and operated by the Cloud Service Provider (CSP).

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



Advantages of Public Cloud

- Public cloud is owned at a lower cost than the private and hybrid cloud.
- Public cloud is maintained by the cloud service provider, so do not need to worry about the maintenance.
- Public cloud is easier to integrate. Hence it offers a better flexibility approach to consumers.
- Public cloud is location independent because its services are delivered through the internet.

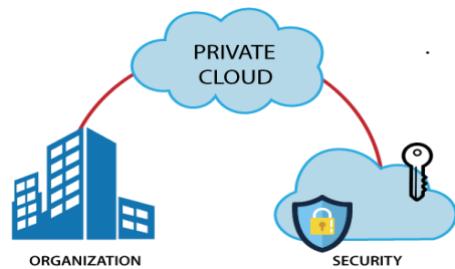
Disadvantages of Public Cloud

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

Private Cloud

Private cloud is also known as an **internal cloud** or **corporate cloud**. It is used by organizations to build and manage their own data centres internally or by the third party.

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



- On-premise private cloud
- Outsourced private cloud

Advantages of Private Cloud

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

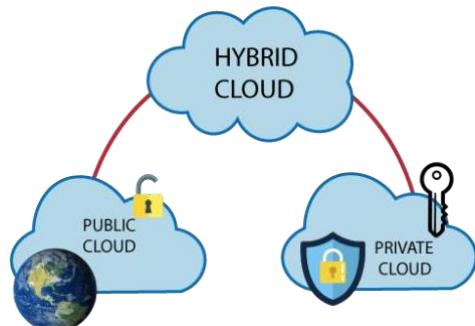
Disadvantages of Private Cloud

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

Hybrid Cloud

Hybrid Cloud is a combination of the public cloud and the private cloud.

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



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

Advantages of Hybrid Cloud

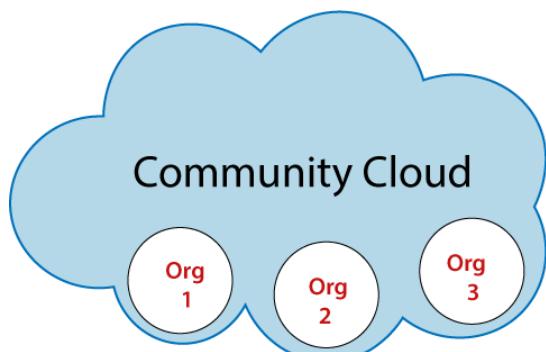
- Hybrid cloud is suitable for organizations that require more security than the public cloud.
- Hybrid cloud helps you to deliver new products and services more quickly.
- Hybrid cloud provides an excellent way to reduce the risk.
- Hybrid cloud offers flexible resources because of the public cloud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

Disadvantages of Hybrid Cloud

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

Community Cloud

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



Example: Health Care community cloud

Advantages of Community Cloud

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

Disadvantages of Community Cloud

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

Historical development

History of Cloud Computing

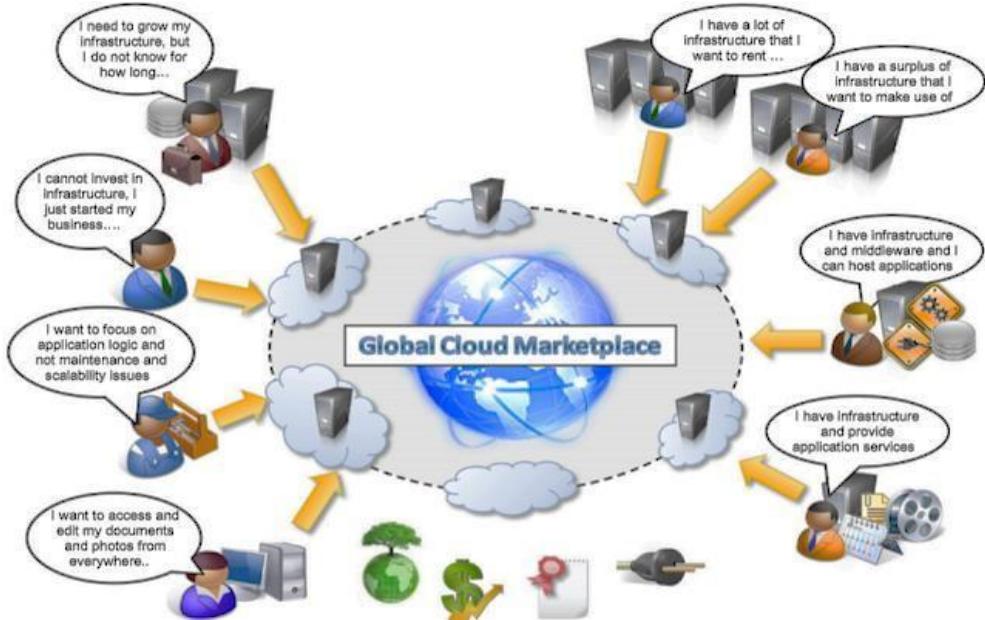
Before cloud computing, there was Client/Server computing which is basically a centralized storage in which all the software applications, all the data and all the controls reside on the server side. If a single user wants to access specific data or run a program, he/she needs to connect to the server and then gain appropriate access, and then he/she can do his/her business.

The concept of **Cloud Computing** came into existence in the year 1950 with implementation of mainframe computers, accessible via **thin/static clients**. Since then, cloud computing has evolved from static clients to dynamic ones and from software to services.

Vision of Cloud Computing

The vision of cloud computing are

1. Cloud computing provides the facility of virtual hardware, runtime environment and services to an individual or an organization.
2. The service of the cloud server can be accessed as long as the user needs it. There is no requirement of any upfront commitment.
3. The entire collection of computing systems is transformed into a collection of utilities, which can be provisioned and composed together to deploy systems in hours rather than days, with no maintenance costs.



4. The long term vision of cloud computing is that IT services and business can be traded as utilities in an open market without any technological and legal barriers.
5. Due to the existence of a global platform for trading cloud services will also help service providers to potentially increase their revenue.
6. A cloud provider can also become a consumer of a competitor service in order to fulfil its promises to customers.

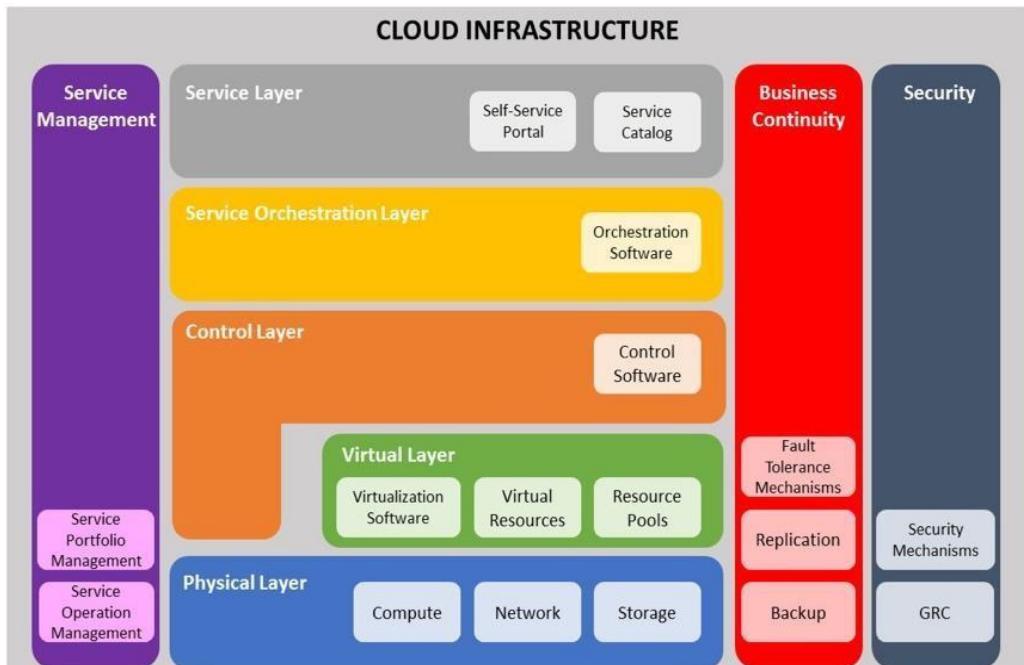
Characteristics of Cloud computing

According to NIST (National institute of standards) there are five essential characteristics of cloud computing:

- 1. On Demand Self Service:** User gets on demand computer services like email, applications etc. without interacting with the service provider. Some of the cloud service providers are- Amazon Web Service, Microsoft, IBM, Salesforce.com
- 2. Broad network access:** Cloud services is available over the network and can be accessed by different clients through Cell phone, IPAD, TAB, Laptops etc.
- 3. Resource pooling:** Same resources can be used by more than one customer at a same time. For example- storage and network bandwidth can be used by any number of customers and without knowing the exact location of that resource.
- 4. Rapid elasticity:** On users demand cloud services can be available and released. Cloud service capabilities are unlimited and can be accessed at any time.
- 5. Measured service:** Resources used by the users can be monitored, controlled. The reports are available for both cloud providers and consumers. On the basis of this measured reports cloud system automatically controls and optimizes the resources based on the type of services.

Cloud computing Reference model

The cloud computing reference model is a conceptual model that characterizes and standardizes the functions of a cloud computing environment by partitioning it into conceptual layers and cross-layer functions. This reference model groups the cloud computing functions and activities into five logical layers and three cross-layer functions.



Cloud computing layers

Physical Layer

- It is the Foundation layer of the cloud infrastructure.
- It Specifies entities that operate at this layer : Compute systems, network devices and storage devices. Operating environment, protocol, tools and processes.
- It executes the request which is generated by the virtualization and control layer.

Virtual Layer

- Deployed on the physical layer.
- It Specifies the entities that operate at this layer like Virtualization software, resource pools, virtual resources.
- It Executes the requests generated by the control layer.

Control Layer

- Deployed either on virtual layer or on physical layer
- It controls and manages the required software
- It enables resource configuration, resource pool configuration and resource provisioning. Executes requests generated by the service layer.

Service Orchestration Layer

- Specifies the entities that operate at this layer i.e. Orchestration software.
- It provides workflows for executing automated tasks.

Service Layer

- Consumers interact and consume cloud resources via this layer.
- It specifies the entities that operate at this layer : Service catalogue and self-service portal.
- Functions of service layer : It stores information about cloud services in service catalogue and presents them to the consumers. It enables consumer to access and manage cloud services via a self-service portal.

Cross-layer function

Business continuity

It is responsible for any kind faults as well as responsible for data replication and backup.

Security

It provides secure data transmission between Cloud and consumer. It protects consumer's information

Service Management

Specifies adoption of activities related to service portfolio management and service operation management.

Service portfolio management :

- Define the service roadmap, service features, and service levels
- Assess and prioritize where investments across the service portfolio are most needed
- Establish budgeting and pricing
- Deal with consumers in supporting activities such as taking orders, processing bills, and collecting payments

Service operation management :

- Enables infrastructure configuration and resource provisioning
- Enable problem resolution
- Enables capacity and availability management
- Enables compliance conformance
- Enables monitoring cloud services and their constituent elements

Cloud computing environment

In a **cloud environment**, consumers can deploy and run their software applications on a sophisticated infrastructure that is owned and managed by **cloud** providers (e.g., Amazon Web Services, Microsoft Azure, and Google **Cloud** Platform). Following are the Cloud Computing Environments.

1. **Application development:** Cloud computing provides application services that are the same as the behaviour of desktop applications that are completely hosted and managed by the cloud services providers. Example- Web Browsing, Email, Online Purchase etc.
2. **Infrastructure and system development:** It is a technology that integrates cloud resources like Cloud Server, Cloud Network etc. with the consumer's network so that the user will access data and information from the cloud server. It also provides the solutions to add and remove resources.
3. **Computing platforms and technologies:** It provides the benefit to different platforms and frameworks that provide different types of services. Some of the cloud computing platforms and technologies are:
 - Amazon web services (AWS): Provides customers with a wide array of cloud services.
 - Google AppEngine: For developing and hosting web applications in Google-managed data centres.
 - Salesforce.com: It is a cloud computing SaaS company that specializes in customer relationship management (CRM).

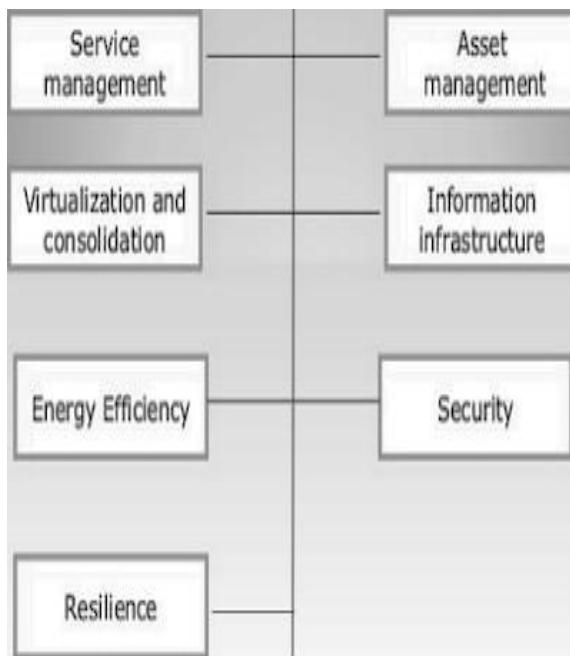
Cloud Service requirements

1. **Efficiency / cost reduction:** By using cloud infrastructure, you don't have to spend huge amounts of money on purchasing and maintaining equipment.
2. **Data security:** Cloud offers many advanced security features that secure the stored data. Cloud storage providers implement baseline protections for their platforms like authentication, access, control, and encryption.
3. **Scalability:** Different companies have different IT needs -- a large enterprise of 1000+ employees won't have the same IT requirements as a start-up. Using the cloud is a great solution because it enables enterprise to efficiently and quickly adapt to their business demands.
4. **Mobility:** Cloud computing allows mobile access to corporate data through smartphones and devices, which is a great way to ensure that no one is ever left out of the network. Staff with busy schedules, or away from the corporate office, can use this feature to keep instantly up-to-date with clients and co-workers.
5. **Disaster recovery:** Data loss is a major concern for all organizations, along with data security. Storing the data in the cloud guarantees that data is always available, even if the client equipment like laptops or PCs, is damaged. Cloud-based services provides quick data recovery for all kinds of emergency situation.

6. **Control:** Cloud enables you complete visibility and control over the data. One can easily decide which users have what type of data can be accessed.
7. **Market reach:** The development of cloud technology ensures the Market reach very easily and quickly for the new IT companies.
8. **Automatic Software Updates:** Cloud-based applications automatically refresh and update themselves.

Cloud and Dynamic Infrastructure

1. **Service management:** This type of services is provided to the IT based companies by the cloud service providers. This facility includes automation and control of the IT company.
2. **Asset-Management:** In this the assets or the property which is involved in providing the cloud services are getting managed.
3. **Virtualization and consolidation:** Consolidation is an effort to reduce the cost of a technology by improving its operating efficiency and effectiveness. It means migrating from large number of resources to fewer one, which is done by virtualization technology.
4. **Information Infrastructure:** It helps the business organizations to achieve the various Information like compliance, availability of resources, preservation and security objectives.
5. **Energy-Efficiency:** Due to energy efficiency, it is not likely to damage or effect any other things of the IT infrastructure or organization.
6. **Security:** The Cloud infrastructure is responsible for the risk management. Risk management Refers to the risks involved in the services which are being provided by the cloud-service providers.
7. **Resilience (Flexibility):** Due to flexibility the infrastructure is safe from all sides and the IT operations will not be easily get affected.



Cloud Adoption

Cloud adoption means adopting a service or technology from another cloud service provider.

Here Cloud means the environment of cloud where the cloud services are being operated. Adoption term states that accepting the services of new Technology.

- The Cloud adoption is suitable for low priority business applications.
- It supports some interactive applications that combines two or more data sources. For example:-if a company requires to grow his business in the whole country in a short span of time then it must need a quick promotion or short promotion across the country adopting cloud technology.
- Cloud Adoption is useful when the recovery management, backup recovery based implementations are required.
- It will work well with research and development projects. It means the testing of new services, design models and also the applications that can be get adjusted on small servers.
- Applications which requires different level of infrastructure throughout the day or throughout the month should be deployed Through the cloud.



Cloud applications

Cloud Computing has its applications in almost all the fields such as business, entertainment, data storage, social networking, management, entertainment, education, art and GPS (**Global Positioning System**), etc. Some of the widely famous cloud computing applications are

- **Business Applications**

Cloud computing has made businesses more collaborative and easy by incorporating various apps such as **MailChimp**, **Chatter**, **Google Apps for business**, and **Quickbooks**.

- **MailChimp:** MailChimp is an **email publishing platform** which provides various options to **design, send, and save templates for emails**.
- **Chatter:** Chatter helps us to **share important information** about the organization in real time.

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

- **Data Storage and Backup**

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

- **Box.com:** Box provides an online environment for **secure content management, workflow, and collaboration.** It allows us to store different files such as Excel, Word, PDF, and images on the cloud. The main advantage of using box is that it provides drag & drop service for files and easily integrates with Office 365, G Suite, Salesforce, and more than 1400 tools.
- **Mozy:** Mozy provides powerful **online backup solutions** for our personal and business data. It schedules automatically back up for each day at a specific time.
- **Oukuu:** Joukuu provides the simplest way to **share and track cloud-based backup files.** Many users use joukuu to search files, folders, and collaborate on documents.
- **Google G Suite:** Google G Suite is one of the best **cloud storage and backup** application. It includes Google Calendar, Docs, Forms, Google+, Hangouts, as well as cloud storage and tools for managing cloud apps. The most popular app in the Google G Suite is Gmail. Gmail offers free email services to users.

- **Management Applications**

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

- **Toggl:** Toggl helps users to track allocated time period for a particular project.
- **Evernote:** Evernote allows you to sync and save your recorded notes, typed notes, and other notes in one convenient place. It is available for both free as well as a paid version. It uses platforms like Windows, macOS, Android, iOS, Browser, and Unix.
- **Outright:** Outright is used by management users for the purpose of accounts. It helps to track income, expenses, profits, and losses in real-time environment.
- **GoToMeeting:** GoToMeeting provides Video Conferencing and online meeting apps, which allows you to start a meeting with your business partners from anytime,

anywhere using mobile phones or tablets. Using GoToMeeting app, you can perform

the tasks related to the management such as join meetings in seconds, view presentations on the shared screen, get alerts for upcoming meetings, etc.

- **Social Applications**

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

Following are some of cloud based social applications -

- **Facebook:** Facebook is a **social networking website** which allows active users to share files, photos, videos, status, more to their friends, relatives, and business partners using the cloud storage system. On Facebook, we will always get notifications when our friends like and comment on the posts.
- **Twitter:** Twitter is a **social networking** site. It is a **microblogging** system. It allows users to follow high profile celebrities, friends, relatives, and receive news. It sends and receives short posts called tweets.
- **Yammer:** Yammer is the **best team collaboration** tool that allows a team of employees to chat, share images, documents, and videos.
- **LinkedIn:** LinkedIn is a **social network** for students, freshers, and professionals.

- **Art Applications**

Cloud computing offers various art applications for quickly and easily design **attractive cards, booklets, and images**.

Some most commonly used cloud art applications are given below:

- **Moo:** Moo is one of the best cloud art applications. It is used for designing and printing business cards, postcards, and mini cards.
- **Vistaprint:** Vistaprint allows us to easily design various printed marketing products such as business cards, Postcards, Booklets, and wedding invitations cards.
- **Adobe Creative Cloud:** Adobe creative cloud is made for designers, artists, filmmakers, and other creative professionals. It is a suite of apps which includes PhotoShop image editing programming, Illustrator, InDesign, TypeKit, Dreamweaver, XD, and Audition.

- **Education Applications**

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

These are the following education applications offered by the cloud -

- **Google Apps for Education:** Google Apps for Education is the most widely used platform for free web-based email, calendar, documents, and collaborative study.
- **Chromebooks for Education:** Chromebook for Education is one of the most important Google's projects. It is designed for the purpose that it enhances education innovation.
- **Tablets with Google Play for Education:** It allows educators to quickly implement the latest technology solutions into the classroom and make it available to their students.
- **AWS in Education:** AWS cloud provides an education-friendly environment to universities, community colleges, and schools.

- **Entertainment Applications**

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

- **Online games:** Today, cloud gaming becomes one of the most important entertainment media. It offers various online games that run remotely from the cloud. The best cloud gaming services are GeForce Now, Vortex, Project xCloud, and PlayStation Now.
- **Video Conferencing Apps:** Video conferencing apps provides a simple and instant connected experience. It allows us to communicate with our business partners, friends, and relatives using a cloud-based video conferencing. The benefits of using video conferencing are that it reduces cost, increases efficiency, and removes interoperability.

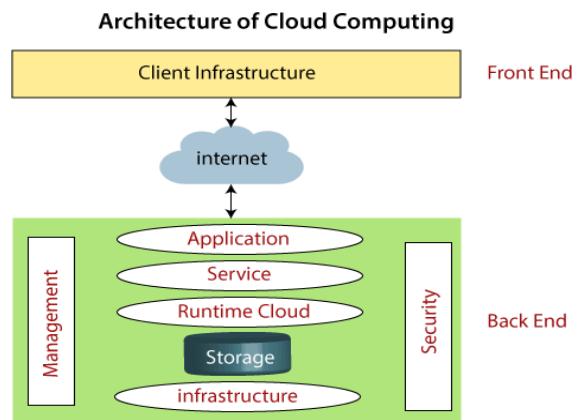


Cloud Computing Architecture

Cloud computing architecture is a combination of **service-oriented architecture** and **event-driven architecture**. Cloud computing architecture is divided into the following two parts

- Front End
- Back End

The below diagram shows the architecture of cloud computing -



Front End

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

Back End

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

Components of Cloud Computing Architecture

These are the following components of cloud computing architecture -

- 1. Client Infrastructure:** Client Infrastructure is a Front end component. It provides GUI (Graphical User Interface) to interact with the cloud.
- 2. Application:** The application may be any software or platform that a client wants to access.
- 3. Service:** A Cloud Services manages that which type of service you access according to the client's requirement.

Cloud computing offers the following three type of services:

- i. Software as a Service (SaaS)** – It is also known as **cloud application services**. Mostly, SaaS applications run directly through the web browser means we do not require to download and install these applications. **Example:** Google Apps, Salesforce, Dropbox, Slack, Hubspot, Cisco WebEx.

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

iii. Infrastructure as a Service (IaaS) – It is also known as **cloud infrastructure services**. It is responsible for managing applications data, middleware, and runtime environments. **Example:** Amazon Web Services (AWS) EC2, Google Compute Engine (GCE), Cisco Metapod.

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

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

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

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

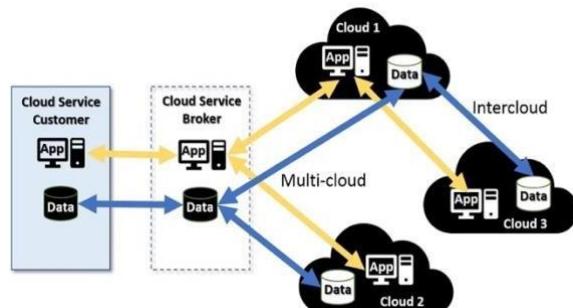
8. Security: Security is an in-built back end component of cloud computing. It implements a security mechanism in the back end.

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

Cloud Interoperability and standards

Cloud interoperability refers to the ability of customers to use the same management tools, server images and other software with a variety of cloud computing providers and platforms.

The Cloud Standards Customer Council (CSCC) has defined five major cloud interoperability scenarios for cloud customers. These are:



Switching cloud service providers : the customer wants to move an application and data from Cloud 1 to Cloud 2

Use of multiple cloud service providers : the customer subscribes to the same or different services from two or more clouds (Clouds 1 and 2 in the diagram);

Directly linked cloud services: the customer needs Cloud 1 to be linked to Cloud 3 to make use of its services.

Hybrid cloud configuration: the customer connects legacy systems to an internal private cloud (e.g., Cloud 1) which is linked to a public cloud service (e.g., Cloud 3); and

Cloud migration: the customer moves one or more in-house applications and/or data to Cloud 1.

Cloud computing Interoperability use cases

Use cases in the context of cloud computing refer to typical ways in which cloud consumers and providers interact. NIST (National Institute of Standards and Technology) defined 21 use cases classified into three groups.

These use cases are listed below:

- Cloud Management Use Cases
 - Open an Account
 - Close an Account
 - Terminate an Account
 - Copy Data Objects into a Cloud
 - Copy Data Objects out of a Cloud
 - Erase Data Objects on a Cloud
 - VM [virtual machine] Control: Allocate VM Instance
 - VM Control: Manage Virtual Machine Instance State
 - Query Cloud-Provider Capabilities and Capacities
- Cloud Interoperability Use Cases
 - Copy Data Objects Between Cloud-Providers
 - Dynamic Operation Dispatch to IaaS Clouds
 - Cloud Burst from Data Centre to Cloud
 - Migrate a Queuing-Based Application
 - Migrate (fully-stopped) VMs from One Cloud Provider to Another
- Cloud Security Use Cases
 - Identity Management: User Account Provisioning
 - Identity Management: User Authentication in the Cloud
 - Identity Management: Data Access Authorization Policy Management in the Cloud
 - Identity Management: User Credential Synchronization Between Enterprises and the Cloud
 - eDiscovery
 - Security Monitoring
 - Sharing of Access to Data in a Cloud

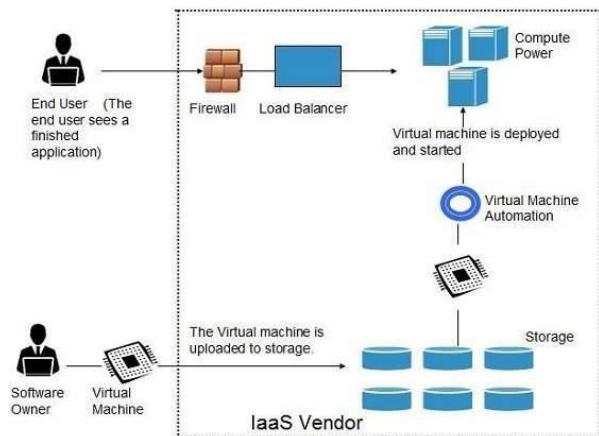
Role of standards in Cloud Computing environment

Various standards in Cloud computing are:

Infrastructure as a Service (IaaS)

Infrastructure-as-a-Service provides access to fundamental resources such as physical machines, virtual machines, virtual storage, etc. Apart from these resources, the IaaS also offers:

- Virtual machine disk storage
- Virtual local area network (VLANs)
- Load balancers
- IP addresses
- Software bundles



All of the above resources are made available to end user via **server virtualization**. Moreover, these resources are accessed by the customers as if they own them.

Benefits

IaaS allows the cloud provider to freely locate the infrastructure over the Internet in a cost-effective manner. Some of the key benefits of IaaS are listed below:

- Full control over computing resources: IaaS allows the customer to access computing resources using administrative rights from virtual machines in the following manner:
- Flexible and efficient renting of computer hardware: IaaS resources such as virtual machines, storage devices, bandwidth, IP addresses, firewalls, etc. are made available to the customers on rent. Also with administrative access to virtual machines, the customer can run any type of software.
- Portability, interoperability: It is possible to switch between applications and resources between IaaS clouds. For example, network applications such as web server or e-mail server that normally runs on customer-owned server hardware can also run from VMs in IaaS cloud.

Issues

The various issues of IaaS are-

- Compatibility with legacy security vulnerabilities: Because IaaS offers the customer to run legacy software in provider's infrastructure, it exposes customers to all of the security vulnerabilities.
- Virtual Machine sprawl: The VM can become out-of-date with respect to security updates because IaaS allows the customer to operate the virtual machines in running, suspended and off state. However, the provider can automatically update such VMs, but this mechanism is hard and complex.

- Robustness of VM-level isolation: IaaS offers an isolated environment to individual customers through hypervisor. Hypervisor is a software layer that includes hardware support for virtualization to split a physical computer into multiple virtual machines.
- Data erase practices: The customer uses virtual machines that in turn use the common disk resources provided by the cloud provider. When the customer releases the resource, the cloud provider must ensure that next customer to rent the resource does not observe data residue from previous customer.

Characteristics

Here are the characteristics of IaaS service model:

- Virtual machines with pre-installed software.
- Virtual machines with pre-installed operating systems such as Windows, Linux, and Solaris.
- On-demand availability of resources.
- Allows to store copies of particular data at different locations.
- The computing resources can be easily scaled up and down.

Platform as a Service (PaaS)

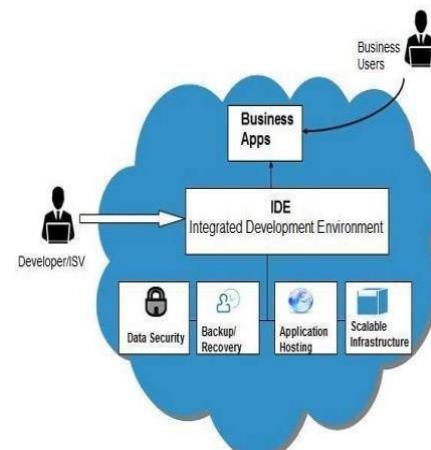
Platform-as-a-Service offers the runtime environment for applications. It also offers development and deployment tools required to develop applications. PaaS has a feature of **point-and-click** tools that enables non-developers to create web applications.

App Engine of Google and **Force.com** are examples of PaaS offering vendors. Developer may log on to these websites and use the **built-in API** to create web-based applications.

Benefits

Following are the benefits of PaaS model:

- Lower administrative overhead: Customer need not bother about the administration because it is the responsibility of cloud provider.
- Lower total cost of ownership: Customer need not purchase expensive hardware, servers, power, and data storage.
- Scalable solutions: It is very easy to scale the resources up or down automatically, based on their demand.
- More current system software: It is the responsibility of the cloud provider to maintain software versions and patch installations.



Issues

PaaS has significant burdens on customer's browsers to maintain reliable and secure connections to the provider's systems. However, there are some specific issues associated with PaaS are-

- Lack of portability between PaaS clouds: Although standard languages are used, yet the implementations of platform services may vary. For example, file, queue, or hash table interfaces of one platform may differ from another, making it difficult to transfer the workloads from one platform to another.
- Event based processor scheduling: The PaaS applications are event-oriented i.e., they have to answer a request in a given interval of time.
- Security engineering of PaaS applications: Since PaaS applications are dependent on network, they must have to use cryptography and manage security exposures.

Characteristics

Here are the characteristics of PaaS service model:

- PaaS offers **browser based development environment**. It allows the developer to create database and edit the application code either via Application Programming Interface or point-and-click tools.
- PaaS provides **built-in security, scalability, and web service interfaces**.
- PaaS provides built-in tools for defining **workflow, approval processes**, and business rules.
- It is easy to integrate PaaS with other applications on the same platform.
- PaaS also provides web services interfaces that allow us to connect the applications outside the platform.

Software as a Service (SaaS)

Software-as-a-Service (SaaS) model allows to provide software application as a service to the end users. It refers to a software that is deployed on a host service and is accessible via Internet. There are several SaaS applications listed below:

- Billing and invoicing system
- Customer Relationship Management (CRM) applications
- Help desk applications
- Human Resource (HR) solutions

Characteristics

Here are the characteristics of SaaS service model:

- SaaS makes the software available over the Internet.
- The software applications are maintained by the vendor.

- The license to the software may be subscription based or usage based. And it is billed on recurring basis.

- SaaS applications are cost-effective since they do not require any maintenance at end user side.
- They are available on demand.
- They can be scaled up or down on demand.
- They are automatically upgraded and updated.
- SaaS offers shared data model. Therefore, multiple users can share single instance of infrastructure. It is not required to hard code the functionality for individual users.
- All users run the same version of the software.

Benefits

Using SaaS has proved to be beneficial in terms of scalability, efficiency and performance. Some of the benefits are listed below:

- Modest software tools: The SaaS application deployment requires a little or no client side software installation, which results in the following benefits:
 - No requirement for complex software packages at client side
 - Little or no risk of configuration at client side
 - Low distribution cost
- Efficient use of software licenses: The customer can have single license for multiple computers running at different locations which reduces the licensing cost. Also, there is no requirement for license servers because the software runs in the provider's infrastructure.
- Centralized management and data: The cloud provider stores data centrally. However, the cloud providers may store data in a decentralized manner for the sake of redundancy and reliability.
- Platform responsibilities managed by providers: All platform responsibilities such as backups, system maintenance, security, hardware refresh, power management, etc. are performed by the cloud provider. The customer does not need to bother about them.

Issues

There are several issues associated with SaaS, some of them are listed below:

Browser based risks: If the customer visits malicious website and browser becomes infected, the subsequent access to SaaS application might compromise the customer's data. To avoid such risks, the customer can use a specific browser to access SaaS applications or can use virtual desktop while accessing the SaaS applications.

Network dependence: The SaaS application can be delivered only when network is continuously available. Also network should be reliable but the network reliability cannot be guaranteed either by cloud provider or by the customer.

Lack of portability between SaaS clouds: Transferring workloads from one SaaS cloud to another is not so easy because work flow, business logics, user interfaces, support scripts can be provider specific.



Introduction

Fault tolerance in cloud computing is very important to continue the service whenever a few devices or components are down or unavailable. This helps the service provider to evaluate their infrastructure requirements, and provide services when the associated devices are unavailable due to some cause.

Scalability and Fault Tolerance

- Cloud Scalability is the ability to scale on-demand the facilities and services as and when they are required by the user.
- Cloud Fault Tolerance is tolerating the faults by the cloud that are done by mistake by the user.
- Cloud middleware is designed on the principle of scalability along with different dimensions in mind e.g.: performance, size and load.
- The cloud middleware manages a huge number of resources and users which depends on the cloud.
- So in this overall scenario the ability to tolerate the failure is normal but sometimes it becomes more important than providing an efficient & optimized system.
- The overall conclusion says that “it is a challenging task for the cloud providers to develop such high scalable and fault tolerance systems and at the same time they will have to provide a competitive performance.

Main Concepts behind Fault Tolerance in Cloud Computing System

Replication: The fault-tolerant system works on the concept of running several other replicates for each and every service. Thus, if one part of the system goes wrong, than the other instances that can be placed instead of it to keep it running.

Redundancy: When any system part fails or moves towards a downstate, then it is important to have backup type systems.

Existence of Fault Tolerance in Cloud Computing

System Failure: This may be either software or hardware issue. The software failure results in a system crash situation that may be due to data overflow or other reasons. Any improper maintenance of the physical hardware machines will result in hardware system failure.

Security Breach Occurrences: There are several reasons why fault tolerance occurs due to security failures. The hacking of the server negatively impacts the server and results in a data lost. Other reasons for the necessity of fault tolerance in the form of security cracks include phishing, virus attack, etc.

Cloud solutions

Any cloud-based solution refers to provide Applications SOFTWARE, Storage Space, On-Demand services, Computer networks, and other resources that are associated with cloud computing.

Benefits of Cloud Solution

- Cloud-based solutions offer benefits for both businesses and end-users.
- Cloud providers use a pay-as-you-go model, so that the client can pay to cloud as per the requirements only. This is very much helpful for start-ups.
- For end-users, cloud computing means they can access everything like Files, Emails, Business applications and many more from any device and from anywhere if there is an internet connection irrespective of place and environment.
- As the cloud-based technology is growing and the SOFTWARE as A SERVICE (SaaS) solution is available in affordable price. So the clients of a Small Business (SMB) are interested in cloud computing.

Cloud Ecosystem

A cloud ecosystem is a complex system of inter-dependent components that all work together to enable the cloud services. In cloud computing, the ecosystem consists of hardware and software as well as cloud customers, cloud engineers, consultants, integrators and partners.

A robust ecosystem provides a cloud provider's customers with an easy way to find and purchase business applications and respond to changing business needs. When the apps are sold through a provider's app store such as AWS (Amazon Web Services) Marketplace, Microsoft Azure Marketplace (for cloud software) or Microsoft AppSource (for business applications), the customer access the catalogue of different vendors' software and services that have already been scrutinized and reviewed for security, risk and cost.

The benefits of a cloud ecosystem

- Companies can use a cloud ecosystem to build new business models. They can promote their business using cloud ecosystem than they sell their product to the customer. Specially in medical equipment.
- In a cloud ecosystem, it is also easier to review data and analyse how each part of the system affects the other parts. For example a doctor can examine a patient over the cloud because all the previous data and present problems of the patient available in the cloud.
- Cloud ecosystem is helpful for complex system of interdependent components that work together to enable the cloud services.
- The centre of a cloud ecosystem is a public cloud provider. It might be an IaaS provider such as Amazon Web Services (AWS) or a SaaS vendor such as Salesforce.
- There is no vendor lock-in in the cloud ecosystem. That means a client can switch over

its business one cloud to other cloud without any restriction. Ex. Mobile No. portability.

Cloud Business process management

Cloud business process management is usually a platform-as-a-service (PaaS) solution that allows the client to create workflows and use the software. Without installing a single Mb of software in the client computer, user can use these cloud-based software solutions to streamline and optimise everyday business activities.

Reasons of Cloud BPM

Minimized errors: Cloud BPM solutions helps the user to minimize the error rate. Less paperwork. Multiple records are also eliminated since changes in data synchronized and visible to every team member with access facility.

Anywhere, anytime access: Cloud BPM, stores information in a centralized database thereby making access possible any time from any location. Further, stakeholders can access the application from any device.

Secure data: Data security is most essential factor for any organization. Cloud BPM application comes with a wide range of security features such as role-based access, conditional visibility, data encryption, and more.

Reputed cloud business process management service providers host their applications on reliable platforms such as Amazon Web Services or Google Cloud Platform, which in turn improves the security of sensitive information.

Reliable, consistent experience: In older client-server system users were constantly threatened by the possibility of server downtime and virus or malware attacks. With cloud BPM, vendors provide ample backup to ensure that there's minimal downtime and protect data using built-in firewalls.

Better collaboration: Collaboration is incredibly easy with cloud BPM, irrespective of whether the users are in the same office or at different offices . Centralized documentation, digital checklists, and automated process flow make it possible for information to be accessed by stakeholders whenever the need arises.

Improved insights: Cloud BPM applications feature has capabilities to store all in a central database. It becomes simpler to monitor and analyse the data.

Portability and Interoperability

Cloud computing is important for many organizations, with use of a wide range of cloud services and the transition of both data and applications to cloud computing environments.

The goal of cloud portability and interoperability is to enable cloud service users to avoid vendor- lock- in and allow for customers to make best use of multiple cloud services.

Basic scenarios

The Cloud Standards Customer Council (CSCC) guide to cloud portability and interoperability has identified five major scenarios requiring interoperability and portability:

Switching cloud service providers: the customer can move an application and data from one Cloud to other Cloud.

Use of multiple cloud service providers: the customer subscribes to the same or different services from two or more cloud service provider.

Directly linked cloud services: the customer needs Cloud 1 to be linked to Cloud 3 to make use of its services

Hybrid cloud configuration: the customer connects traditional systems to an internal private cloud which is linked to a public cloud service.

Cloud migration: the customer moves one or more in-house applications and/or data to Cloud.

Cloud portability is the ability to transfer applications between **cloud** environments without losing any data. Several **cloud** providers have **portability** facility.

Cloud interoperability refers to the ability of customers to use the same management tools, server images and other software with a variety of cloud computing providers and platforms.

The cloud computing portability and interoperability categories are:

- **Data Portability:** is the ability to easily transfer data from one cloud service to another cloud service.
- **Application Portability:** Cloud application portability is the ability to easily transfer an application or application components from one cloud service to another cloud service.
- **Application Interoperability:** It is the interoperability between application components and client devices using various standards like SaaS, PaaS, IaaS. An application component may be a huge application, or a part of the distributed application.
- **Management Interoperability:** Management interoperability is an interoperability between cloud services (SaaS, PaaS, or IaaS) and connected clients.

Cloud Service management

It is the responsibility of cloud service provider to manage resources and their performance. Management of resources includes several aspects of cloud computing such as load balancing, performance, storage, backups, capacity, deployment, etc. The management is essential to access full functionality of resources in the cloud. The cloud provider performs a number of tasks to ensure efficient use of cloud resources. Here, we will discuss some of them:

Data Flow of the System: The managers are responsible to develop a technology for data flow. This process describes the movement of data between the organization and the cloud server.

Vendor Lock-In Awareness and Solutions: The managers must know the procedure to exit from services of a particular cloud provider. The procedures must be defined to enable the cloud managers to export data of an organization from their system to another cloud provider.

Knowing Provider's Security Procedures: The managers should know the security plans of the provider for the following services:

- Multi users
- E-commerce processing
- Employee screening
- Encryption policy

Monitor Audit Log Use: In order to identify errors in the system, managers must audit the logs on a regular basis.

Solution Testing and Validation: When the cloud provider offers a solution, it is essential to test it in order to ensure that it gives the correct result and it is error-free. This is necessary for a system to be robust and reliable.

Cloud Offerings

It offers various servers, storage, databases, networking, software, analytics, and intelligence over the Internet ("the **cloud**") to the client **in an innovative**, faster and flexible way. The various offerings are:

1. Cloud Environment: It describes the hosting environments of cloud in detail.

The various environments are:

- **Elastic Infrastructure:** It is responsible for hosting of virtual servers, disk storage, and configuration of network connectivity.
- **Elastic Platform:** It is a middleware for the execution of customer's application, their communication, and data storage
- **Environment-based Availability:** A cloud provider offers an Elastic Infrastructure or Platform on which customers may deploy various application software. The availability of this environment helps the customer to achieve their requirements.

2. Processing Offerings: It describes how computing can be performed in the cloud.

- **Hypervisor:** In this process the time required to access and terminate server is reduced through hardware virtualization.
- **Execution Environment:** It executes common application components and provides common functionality for data storages, communication etc.
- **Map Reduce:** Large data sets to be processed are divided into smaller data chunks and distributed among users. Individual results are later consolidated.

3. Storage Offerings: It describes how data can be stored in the cloud

- **Block or Mass Storage:** It is responsible for storing data centrally which is large hard disk that is connected to the server.

- **Blob Storage:** A large amount of data can be stored just like a file system. That means data can be stored in a specified folder assigned for a particular type of file like Audio Folder, Video Folder, Image Folder etc.
 - **Strict Consistency:** Data is stored at different locations (replicas) to improve response time and to avoid data loss in case of failures while consistency of replicas is ensured at all times.
4. **Communication Offering:** It is responsible for describing how data can be exchanged in the cloud.
- **Virtual Networking:** It is responsible for how can the physical networking resources, such as networking interface cards, switches, routers etc. can be used in a virtual mode . These Virtual Networking resources may share the same physical networking resources.
 - **Message-oriented Middleware:** Communication partners exchange information asynchronously. The message-oriented middleware handles the message and sends to the destination using available communication resources.
 - **Timeout-based Delivery:** It assures that a message is properly received and it is not deleted immediately after it has been read by the client. After the client has successfully read the message, it sends an acknowledgement to the message queue. After receiving the acknowledgement the message is deleted.

Testing under Control

Cloud testing typically involves monitoring and reporting on real-world user traffic conditions as well as load balance and stress testing for a range of simulated usage conditions.

Load and performance testing conducted on the applications and services provided via cloud computing in order to ensure maximum performance and scalability under a wide variety of conditions.

Testing under the cloud decreases the manual intervention of technical persons for testing the network condition.

Advantages of Cloud Testing:

- Reduces capital investment and operational costs and without effecting the business targets.
- Offers new and attractive services to the clients and provides an opportunity to speed cycles of innovations and improve the solution quality.

Cloud service Controls

Service Controls allow customers to address threats such as data theft, accidental data loss, and excessive access to data stored in Cloud.

In Other words it is a firewall for Google Cloud Service (GCS), BigQuery, Bigtable and other supported services. It gives information security teams peace of mind that no-one can access data contained in these services from unauthorized networks.

Virtual desktop Infrastructure

Virtual desktop infrastructure (VDI) is defined as the hosting of desktop environments on a central server. It is a form of desktop virtualization. In this process the desktop images run within server and are delivered to clients over a network.

Virtual Desktop Infrastructure (VDI) is a concept in which a server based computing model used to deliver applications to remote users.

Virtual Desktop Infrastructure or VDI is the name given to a collection of technologies and processes that extends the concept of a remote desktop.

The idea behind the Virtual desktop infrastructure is that, companies can virtualize their desktop operating systems like Windows XP or Vista and run the same OS in the desktops from and within the secured datacentre.



Cloud Management and Virtualisation Technology

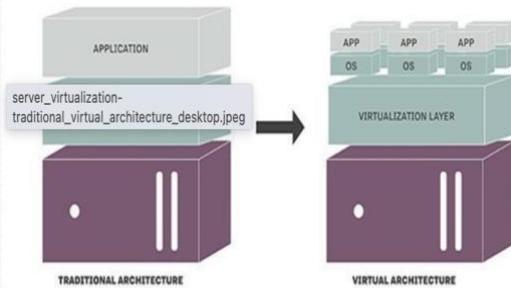
Virtualization is a technique, which allows to share a single physical demand of a resource or an application among multiple customers and organizations.

Virtualization is the "creation of a virtual (rather than actual) version of Server, Desktop, Storage device, Operating system or network resources".

Create a virtualised Architecture

A virtualization architecture is a conceptual model specifying the arrangement and interrelationships of the particular components involved in delivering a virtual rather than physical version like Server, Desktop, Storage device, Operating system or network resources.

TRADITIONAL AND VIRTUAL ARCHITECTURE



Virtualization is commonly hypervisor-based. The hypervisor (**In hypervisor process the time required to access and terminate server is reduced through hardware virtualization**) isolates operating systems and applications from the underlying computer hardware so that the host machine can run multiple virtual machines.

Data Centre

A **Virtual Datacentre** is a huge **cloud** infrastructure designed for enterprise business needs. **Virtual Datacentres** are hosted in the public **cloud** which provides full compatibility with any environment.

In cloud computing, Virtual Datacentre is known as Infrastructure as a Service (IaaS). Using **virtualized data centre** a service provider provides quick service to its clients.

A **virtualized data centre** is a logical software abstraction of a physical **data centre** that provides a collection of **cloud** infrastructure components including servers, storage clusters, and other networking components, to business enterprises

Resilience

Resilient means "having the ability to spring back. "Resiliency is the ability of a server, network, storage system, or an entire data centre, to recover quickly and continue operating even when there has been an equipment failure, power outage or other disruption.

Data centre resiliency is a planned part of a cloud architecture and is usually associated with other disaster planning and data centre disaster-recovery like data protection.

Agility

Cloud agility refers to the addition of business value. When it comes to the cloud context, agility is all about the ability of an organization to rapidly develop, test, and launch software applications that drive business growth.

key benefits of agility in the cloud:

Greater Business Continuity and Flexibility: Due to Agility Cloud services can be rolled up or down as per business requirements without increasing the bunch of IT equipment. For example, you can start with a 10 node cluster and then easily increase to 50 nodes as your requirements change.

Infrastructure Agility: Cloud allows companies to significantly decrease the time it takes to provision and de-provision IT infrastructure.

Automated allocation of resources: It simplifies provisioning, de-provisioning and re-deploying resources through automation and easy-to-use APIs (Application Program Interface) and web consoles. The time for an IT systems administrator spent on managing and supporting cloud infrastructure is reduced.

Storage

Cloud Storage is a service that allows to save data on offsite storage system managed by third-party and is made accessible through **web based API**.

Storage Devices

Block Storage Devices: The **block storage devices** offer raw storage to the clients. These raw storage are partitioned to create volumes.

File Storage Devices: The **file Storage Devices** offer storage to clients in the form of files, maintaining its own file system. This storage is in the form of Network Attached Storage (NAS).

Cloud Storage Classes

Cloud storage can be broadly classified into two categories:

Unmanaged Cloud Storage: Unmanaged cloud storage means the storage is preconfigured for the customer. The customer can neither format, nor install his own file system or change drive properties.

Managed Cloud Storage: Managed cloud storage offers online storage space on-demand. The managed cloud storage system appears to the user to be a raw disk that the user can partition and format.

Provisioning

Cloud provisioning is the allocation of a cloud provider's resources and services to a customer. Cloud provisioning is the key feature of the cloud computing model, relating to how a customer procures cloud services and resources from a cloud provider. Cloud provision includes infrastructure as a service (IaaS), software as a service (SaaS) and platform as a service (PaaS).

Types of cloud provisioning

- **Advanced provisioning:** With advanced provisioning, the customer signs a formal contract of service with the cloud provider. The provider then prepares the agreed-upon resources or services for the customer and delivers them. The customer is charged a flat fee or is billed on a monthly basis.

- **Dynamic provisioning:** With dynamic provisioning, cloud resources are deployed flexibly to match a customer's fluctuating demands.
- **User self-provisioning:** With user self-provisioning, also called *cloud self-service*, the customer buys resources from the cloud provider through a web interface or portal. This usually involves creating a user account and paying for resources with a credit card.

Asset Management

Cloud asset management (CAM) is a component of **cloud management services** focused on the management of business in cloud environment, such as the products or services that are used in cloud. Cloud asset management delivers visibility and control of all the assets and infrastructure that make up your cloud environment. It's a crucial first step towards a better optimised, more secure cloud.

Concept of Map Reduce

A MapReduce is a data processing tool which is used to process the data parallelly in a distributed form. It was developed in 2004. Usage of MapReduce

- It can be used in various application like document clustering, distributed storage and web link.
- It can be used for distributed pattern-based searching.
- We can also use MapReduce in machine learning.
- It was used by Google to regenerate Google's index of the World Wide Web.
- It can be used in multiple computing environments such as multi-cluster, multi-core, and mobile environment.

Cloud Governance

Cloud Governance is a set of rules. It applies specific policies or principles to the use of cloud computing services. This model aims to secure applications and data even if located distantly. The best Cloud Governance solutions include People, Processes, and Technology. It basically refers to the decision making processes, criteria, and policies involved in the planning, architecture, acquisition, deployment, operation, architecture, acquisition, implementation, operation, and management of a Cloud computing capability. Cloud Governance best practices help to optimize the organization's:

- Operations: Doing it efficiently
- Risk and compliance: Doing it securely
- Financial: Doing more with less

Load Balancing

Cloud load balancing is the process of distributing workloads and computing resources in a cloud computing environment. Load balancing allows enterprises to manage application or workload demands by allocating resources among multiple computers, networks or servers. Cloud load balancing involves hosting the distribution of workload traffic and demands that reside over the Internet. Cloud load balancing helps enterprises achieve high performance levels for potentially lower costs than traditional on-premises load balancing technology. Cloud load balancing takes advantage of the cloud's scalability and agility to meet rerouted workload demands and to improve overall availability. In addition to workload and traffic distribution, cloud load balancing technology can provide health checks for cloud applications.

High Availability

High availability is a type of computing infrastructure that allows to continue the functioning of computer even when some of its components fail. This is very important for a cloud customer who cannot tolerate interruption in service, and any downtime can cause damage or result in financial loss.

High Availability in the cloud is achieved by creating clusters. A high availability cluster is a group of servers that act as a single server to provide continuous service. These servers have common access to the same shared storage space for data. So if a server is unavailable, the other servers pick up the load. A high availability cluster can be anything from two to dozens of servers. As well as providing failover, high availability clusters also allow load balancing of workloads so that anyone server within the cluster will not get overloaded and you can provide more consistent performance.

The basic elements of high availability

The following three elements are essential to a highly available system:

- **Redundancy**—ensuring that any elements critical to system operations have an additional, redundant component that can take over in case of failure.
- **Monitoring**—collecting data from a running system and detecting when a component fails or stops responding.
- **Failover**—a mechanism that can switch automatically from the currently active component to a redundant component, if monitoring shows a failure of the active component.

Disaster Recovery

Cloud disaster recovery (cloud DR) is a combination of strategies and services intended to back up data, applications and other resources to public cloud or dedicated service providers. When disaster occurs, the affected data, applications and other resources can be restored to the local data centre or a cloud provider and resume normal operation for the enterprise.

Cloud disaster recovery is primarily an infrastructure as a service (IaaS) solution that backs up designated system data on a remote offsite cloud server. It provides updated recovery point objective (RPO) and recovery time objective (RTO) in case of a disaster or system restore.

Cisco Data Centre Network architecture

The data centre is home to the computational power, storage, and applications necessary to support an enterprise business. The data centre infrastructure is central to the IT architecture, from which all content is sourced or passes through. Proper planning of the data centre infrastructure design is critical, and performance, resiliency, and scalability need to be carefully considered.

Cisco is the only vendor that delivers a complete architecture with advanced services, support, and industry-leading products. Cisco can help design the optimal end-state data centre architecture and meet each tactical deployment phase of network evolution with the best products and services to achieve it.

A complete architecture that enables IT executives to:

- Consolidate and virtualize computing, storage and network resources
- Deliver secure and optimized employee, partner and customer access to information and applications
- Protect and rapidly recover IT resources and applications

Cisco Service-Oriented Network Architecture (SONA), the enterprise implementation of the Intelligent Information Network (IIN) technology vision. Cisco SONA emphasizes the value of the interactive services provided in the networked infrastructure, such as application optimization, security, and server and storage fabric switching, to enhance business applications.

Benefits

- Lower-priced server and storage infrastructure
- Increased business agility and adaptability
- Ability to meet regulatory compliance standards with integrated network security and support for business continuance
- Tested and verified design and extensive service offerings for lower implementation costs and reduced risk
- Investment protection for core data centre platforms offering multiyear deployment lifecycles
- Rapid application development and time to market of business-critical services



Virtualisation

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 to share the physical resource and an application to multiple users.

Cloud Virtualizations also manage the workload by transforming traditional computing and make it more scalable, economical and efficient. One of the important features of virtualization is that it allows sharing of applications to multiple customers and companies. The various type of Virtualizations are:

Network Virtualisation: Network virtualization helps to manage and monitor the entire computer network as a single administrative entity. Admins can keep a track of various components of network infrastructure such as routers and switches through a single software-based administrator's console. Network virtualization helps the network for transferring data perfectly, flexibly, reliably and securely. It improves the overall network's productivity and efficiency. It becomes easier for administrators to allocate and distribute resources conveniently and ensure high and stable network performance.

Desktop Virtualisation: Desktop virtualization is when the host server can run virtual machines using a hypervisor (a software program). A hypervisor can directly be installed on the host machine or over the operating system (like Windows, Mac, and Linux). Virtualized desktops don't use the host system's hard drive; instead, they run on a remote central server. This type of virtualization is useful for development and testing teams who need to develop or test applications on different operating systems.

Local desktop Virtualisation : Local desktop virtualization means the operating system runs on a client device using local hardware virtualization. This type of desktop virtualization works well when users do not need a continuous network connection and can meet application computing requirements with local system resources. However, this technique can be implemented locally only.

Remote Desktop Virtualization: Remote desktop virtualization is a common use of virtualization that operates in a client/server computing environment. This allows users to run operating systems and applications from a server inside a data centre on a client device. This client device could be a laptop, thin client device, or a smartphone.

Application Virtualisation: The process of installing an application on a central server that can virtually be operated on multiple systems is known as application virtualization. For end users, the virtualized application works exactly like a original application installed on a physical machine. With application virtualization, it's easier for organizations to update, maintain, and fix applications centrally. Admins can control and modify access permissions to the application without logging in to the user's desktop. Another benefit of application virtualization is portability. It allows users to access virtualized applications even on non-Windows devices, such as iOS or Android.

Server Virtualisation: Server virtualization is a process of partitioning the resources of a single server into multiple virtual servers. These virtual servers can run as separate machines. Server virtualization allows businesses to run multiple independent tasks with different configurations using a single (host) server. The process also saves the hardware cost involved in keeping a host of physical servers.

Block and File level Storage Virtualisation: Storage virtualization is a series of servers that are managed by a virtual storage system. The servers aren't aware of exactly where their data is stored. This technology manages the storage of data from multiple users and utilized as a single storage system. Storage virtualization software maintains smooth operations and consistent performance despite changes, break down and differences in the connected equipment.

Data virtualization: This is a kind of virtualization in which the data is collected from various sources and managed that in a single server without knowing more about the technical information like how data is collected, stored & formatted. Then the stored data can be arranged in such a way so that its virtual view can be accessed by interested users by using the various cloud services remotely. Many big giant companies are providing their services like Oracle, IBM, At scale, Cdata etc.

Desktop as a service (DaaS)

Desktop as a service (DaaS) is a cloud-based desktop virtualization service hosted by a third party enterprise. The third party cloud provider manages all back-end resources, such as desktop storage, compute, and networking, including the virtual cloud machines that run the desktop operating systems. The provider streams the virtual desktops to end-user devices, allowing anytime, anywhere access to desktops and applications. There are two kinds of desktops available in DaaS. These are:

1. **Persistent desktop:** Users have the ability to customize and save the desktop so that it will look the same way each time when a particular user logs in. Persistent desktop requires more storage than non-persistent desktop.
2. **Non-persistent desktop:** Desktops are wiped each time the user logs out—they are merely a way to access shared cloud services.

DaaS advantages:

- Easy platform migration
- Total cost reduction
- Minimized complexity
- Disaster recovery
- Uninterrupted connectivity
- Increased performance
- Personalization
- Reliability
- Data security

Virtual Machine Monitor

A virtual machine (VM) is a virtual environment that works like a computer within a computer. It runs on a partition of its host computer with its own resources of CPU power, memory, an operating system (e.g. Windows, Linux, macOS), and other resources. This allows end-users to run applications on VMs and use them as they normally would on their workstation.

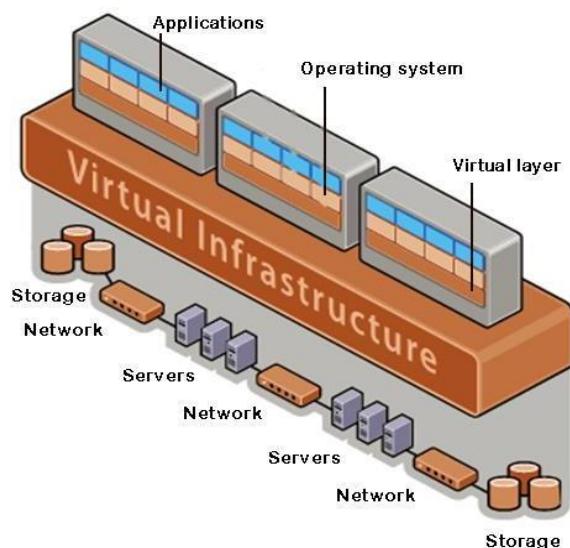
VMs are made possible through virtualization technology. Virtualization uses software to simulate virtual hardware that allows multiple VMs to run on a single machine. The physical machine is known as the host while the VMs running on it are called guests.

This process is managed by software known as a hypervisor. The hypervisor is responsible for managing and provisioning resources like memory and storage from the host to guests.

Infrastructure Requirements

In virtualization, the server and the software application which are required by the **cloud providers** maintain by the third party and in this, the cloud provider gives some amount to the third party.

With the help of Hypervisor software, the cloud customer can access the server. Hypervisor software is a connectivity between the server and the virtual environment and distributes the resources between different virtual environments.



Virtualisation benefits

- **Security:** During the process of virtualization **security** is one of the important factor. The security can be provided with the help of firewalls, which will help to prevent unauthorized access and will keep the data confidential. Moreover, with the help of firewall and security, the data can protect from harmful viruses malware and other cyber threats.
- **Flexible operations:** With the help of a virtual network, the work of IT professional is becoming more efficient and active. The network switch implement today is very easy to use, flexible and saves time.

With the help of virtualization in Cloud Computing, technical problems can solve in physical systems. It eliminates the problem of recovering the data from crashed or corrupted devices and hence saves time.

- **Economical:** Virtualization in **Cloud Computing**, save the cost for a physical system such as hardware and servers. It stores all the data in the virtual server, which are quite economical. It reduces the wastage, decreases the electricity bills along with the maintenance cost. Due to this, the business can run multiple operating system and apps in a particular server.
- **Eliminates the risk of system failure:** While performing some task there are chances that the system might crash down at the wrong time. This failure can cause damage to the company but the virtualizations help you to perform the same task in multiple devices at the same time.

It is possible because the data is stored in the cloud and it can be retrieve anytime and with the help of any device. Moreover, there is two working server side by side which makes the data accessible every time. Even if a server crashes with the help of the second server the customer can access the data.

- **Flexible transfer of data:** The data can transfer to the virtual server and retrieve anytime. The customers or cloud provider don't have to waste time finding out hard drives to find data. With the help of virtualization, it will very easy to locate the required data and transfer them to the allotted authorities.

Virtual Local Area Network (VLAN)

A virtual local area network (VLAN) is a logical group of workstations, servers and network devices that appear to be on the same LAN despite their geographical distribution. A VLAN allows a network of computers and users to communicate in a simulated environment as if they exist in a single LAN and are sharing a single broadcast and multicast domain. VLANs are implemented to achieve scalability, security and ease of network management and can quickly adapt to changes in network requirements and relocation of workstations and server nodes.

A VLAN allows several networks to work virtually as one LAN. One of the most beneficial elements of a VLAN is that it removes latency in the network, which saves network resources and increases network efficiency. In addition, VLANs are created to provide segmentation and assist in issues like security, network management and scalability. Data Traffic can also easily be controlled by using VLANs.

The key benefits of implementing VLANs are:

- Allowing network administrators to apply additional security to network communication
- Making expansion of a network or a network device easier
- Providing flexibility to configure devices in a centralized environment while the devices might be located in different geographical locations
- Decreasing the latency and traffic load on the network and the network devices, offering increased performance

VLANs also have some disadvantages and limitations as listed below:

- High risk of virus issues because one infected system may spread a virus through the whole logical network
- It requires additional routers in very large networks to control the network and workload

Virtual Storage Area Network (VSAN)

A virtual storage area network (VSAN) is a logical partitioning created within a physical storage area network. This implementation model of a storage virtualization technique divides and allocates some or an entire storage area network into one or more logical SANs to be used by internal or external IT services and solutions.

A virtual storage area network (VSAN) is primarily implemented in cloud computing and virtualization environments. A VSAN allows end users to create a logical storage area network in the physical SAN (Storage Area Network) through storage virtualization.

A VSAN provides similar services and features as a typical SAN, but because it is virtualized, it allows for the addition and relocation of subscribers without changing the network's physical layout. It also provides flexible storage capacity that can be increased or decreased over time.

Differences between VLAN and VSAN

Sl No.	VLAN(Virtual Local Area Network)	VSAN(Virtual Storage Area Network)
1	VLAN is a network technology used to logically separate large broadcast domains using layer 2 devices.	VSAN is a logical partition in a storage area network.
2	It divides the network into different virtual sub-networks reduces unnecessary traffic and improve performance.	VSANS allow traffic to be isolated within specific portions of a storage area network.
3	VLANs are implemented to achieve scalability, security and ease of network management.	The use of multiple VSAN's can make a system easier to configure and scale out.
4	VLAN's can quickly adapt the physical change in the network.	VSAN subscribers can be added or relocated without the need for changing the physical layout.
5	The purpose of implementing a VLAN is to improve the performance of a network.	The VSANs minimizes the total system's vulnerability, security is improved. VSANs also offer the possibility of data redundancy, minimizing the risk of unexpected data loss.



Cloud Security

Cloud security refers to the technologies, policies, controls, and services that protect cloud data, applications, and infrastructure from hackers and threats. Cloud security is essential for many users who are concerned about the safety of their data which is stored in the cloud. Data stored in the cloud is more secured because cloud service providers have superior security measures, and their employees are highly security experts.

Cloud Security Fundamentals

Information security is a complex and collective of techniques, technologies, regulations, and behaviours that collaboratively protect the computing systems and data. IT security's main aim to defend against threats from both malicious intent and unintentional user errors. The fundamental security terms relevant to cloud computing are

- **Confidentiality:** Confidentiality is the characteristic of something being made accessible only to authorized users. Within cloud environments, confidentiality primarily pertains to restricting access to data in transit and storage. The message issued by the cloud consumer to the cloud service is considered confidential only if it is not accessed or read by an unauthorized party.
- **Integrity:** Data integrity in the cloud is that the cloud service provider can be guaranteed that the data transmission between the user and the server must be secure. Integrity can extend to how data is stored, processed, and retrieved by cloud services and cloud-based IT resources.
- **Authenticity:** Authenticity means data can be provided through some authorized source. This concept ensures the non-rejection of data.
- **Availability:** Availability is the characteristic of being accessible and usable during a specified time period. In typical cloud environments, the availability of cloud services can be a responsibility that is shared by the cloud provider and the cloud carrier.
- **Vulnerability:** A vulnerability is a weakness that can be exploited due to insufficient security controls. IT resource vulnerabilities can have a range of causes, including configuration deficiencies, security policy weaknesses, user errors, hardware or firmware flaws, software bugs, and poor security architecture.
- **Risk:** Risk is the possibility of loss or harm arising while performing an activity. Risk is typically measured according to its threat level and the number of possible or known vulnerabilities.

Cloud security services

Authentication : Authentication is the testing or reconciliation of evidence of a user's identity. It establishes the user's identity and ensures the authenticity of the user. For example, an user provides the user ID in the login screen and then has to provide a password. The computer system authenticates the user by verifying that the password for the provided user ID.

Authorization : Authorization refers to rights and privileges granted to an individual user to access the computer resources and information. Once a user's identity and authentication are established, authorization levels determine the extent of system rights to the authorised user.

Auditing: To maintain the operational process in cloud , organizations use two basic methods:

1. system audits and monitoring. These methods can be employed by the cloud customer, the cloud provider, or both, depending on the architecture and deployment of the cloud computing. A system audit is a one-time or periodic event to evaluate security.
2. Information technology (IT) audit: This audit is often divided into two types: internal and external. Internal auditors are typically performing their task inside the organization, whereas external auditors are auditing the external network infrastructure.

Accountability: Accountability is the ability to determine the actions and behaviours of a single individual within a cloud system. Accountability can be fixed on an individual employ. Employ's performance can be tracked and judged through accountability.

Design Principles

The NCSC (National Cyber Security Centre) published some cloud security principles. These principles are designed to give guidance to cloud service providers in order to protect their customers.

Data in transit protection: User data which is transitioning between networks should be protected against any interference.

Asset protection and resilience: User data, and the assets storing or processing it, should be protected against physical tampering, loss, damage or seizure.

Separation between users: If a user of a service is compromised by malicious software, this should not affect the service or data of another user.

Governance framework: A Security Governance Framework should be followed by the service provider, in order to internally coordinate its management of the service.

Operational security: In order to prevent and detect attacks, the service must be operated securely.

Secure development: Services should be designed with security in mind.

Personnel security: Service provider personnel should be thoroughly screened, followed by in-depth training to reduce the possibility of accidental or malicious compromise.

Supply chain security: The service provider should ensure that their supply chain adheres to all of the same security principles.

Secure user management: Service provider should ensure that the client should have the relevant tools to securely manage the use of their services.

Identity and authentication: Access to the service interfaces should only be granted to specific individuals and should all be guarded by adequate authentication measures – two way authentication if possible.

External interface protection: Any external or less trustworthy service interfaces must be identified and defended appropriately.

Secure service administration: If a cloud service is compromised through its administration system, important company data could be stolen or manipulated. It is vital that these services are secure.

Audit information for users: A service provider should supply their customers with the audit record to monitor the service and who is able to access your data. This is vital as it gives you a means to identify inappropriate or malicious activity.

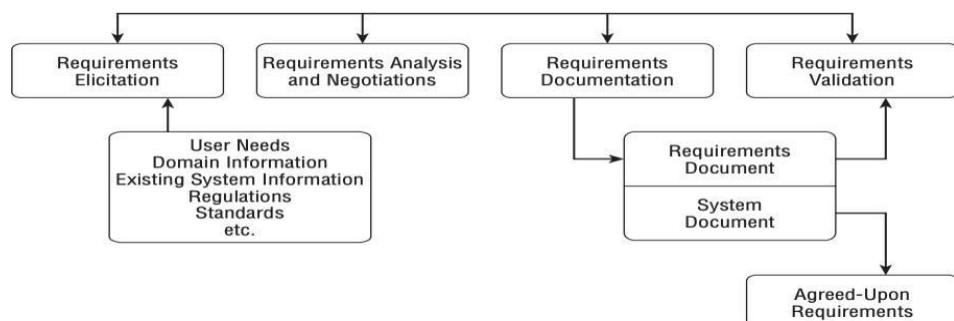
Secure use of service: You have a responsibility to ensure the service is used properly, to ensure your data is kept safe and protected.

Secure Cloud software requirements

The requirements for secure cloud software are concerned with non-functional issues such as minimizing or eliminating vulnerabilities and ensuring that the software will perform as required, even under attack.

- It must be dependable under anticipated operating conditions, and remain dependable under unfriendly operating conditions.
- It must be trustworthy in its own behaviour and it should be able to handle the outside attack
- It must be robust enough to recover quickly to full operational capability with a minimum of damage to itself, the resources and data it handles, and the external components with which it interacts.

Below figure illustrates the major elements of the software requirements engineering process.



Policy Implementation

Security policies are the foundation of a sound cloud system security implementation. According to the Data and Analysis Centre for Software (DACS), three main objectives common to all system security policies and the mechanisms and countermeasures used to enforce those policies:

- They must allow authorized person to connect and access the system to prevent unauthorized access or connections, especially by unknown or suspicious user.
- They must be allowed to read, modify, destroy or delete of data while preventing unauthorized users
- They must block the entry of content like user input, executable code, system commands, etc. suspected of containing attack patterns or malicious logic that could threaten the system's ability to operate according to its security policy and its ability to protect the information.

Implementation Issues : Before implementing the security policy it is very much important to consider the following security issues.

- Access controls
- Data protection
- Confidentiality
- Integrity
- Identification and authentication
- Communication security and Accountability

Cloud Computing Security Challenges

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

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

*API is an application program interface that allows the end user to interact with a **cloud provider's service***

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

hackers.

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

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

Cloud Computing Security Architecture

Cloud security architecture describes all the hardware and technologies designed to protect data, workloads, and systems within cloud platforms. The security architecture design in cloud computing may change just from the company to the company based on their requirement. Nowadays several enterprises are willing to adapt hybrid cloud security architecture. It is an advanced version of the cloud security architecture that helps to reduce the workload and exposure of data.

Architectural Considerations

A variety of factors affect the implementation and performance of cloud security architecture. There are general issues involving regulatory requirements, adherence to standards, security management, information classification, and security awareness. A variety of topics influence and directly affect the cloud security architecture. They include such factors as compliance, security management, controls, and security awareness.

Compliance: In a public cloud environment, the provider does not normally inform the clients about the storage location of their data. In fact, the distribution of processing and data storage is one of the cloud's fundamental characteristics. However, the cloud provider should cooperate to consider the client's data location requirements. In addition, the cloud vendor should provide transparency to the client by supplying information about storage used, processing characteristics, and other relevant account information.

Security Management: Security architecture involves effective security management to realize the benefits of cloud computation. Proper cloud security management and administration should identify management issues in critical areas such as access control, vulnerability analysis, fault tolerance, and disaster recovery and business continuity planning.

Controls: The objective of cloud security controls is to reduce vulnerabilities to a tolerable level and minimize the effects of the data hack.

Security Awareness: The purpose of computer security awareness, training, and education is to enhance security by adopting the following steps:

- Improving the awareness on how to protect System & Resource.
- Developing skills and knowledge so that the computer users can perform their jobs more securely
- Building in-depth knowledge, as needed, to design, implement, or operate security programs for organizations and systems

Information Classification:

The information that an organization processes must be classified according to the organization's sensitivity to its loss or disclosure. The information system owner is responsible for defining the sensitivity level of the data. Classification according to a defined classification scheme enables security controls to be properly implemented. The information classification process also supports disaster recovery planning and business continuity planning.

Information Classification Benefits

- It executives' organization's security policies.
- It helps to identify that which information is the most sensitive to the organization.
- It supports the data confidentiality, integrity, and availability.
- It helps to identify those which protections is applicable for which information.

Classification Criteria

Several criteria may be used to determine the classification of an information object:

- **Value** — Value is the number one commonly used criterion for classifying data in the private sector. If the information is valuable to an organization or its competitors, then it needs to be classified.
- **Age** — The classification of information might be lowered if the information's value decreases over time. In the U.S. Department of Defence, some classified documents are automatically declassified after a predetermined time period has passed.
- **Useful life** — If the information has been made obsolete due to new information, substantial changes in the company, or other reasons, the information can often be declassified.
- **Personal association** — If information is personally associated with specific individuals or is addressed by a privacy law, it might need to be classified. For example, investigative information that reveals informant names might need to remain classified.

Information Classification Procedures

There are several steps in establishing a classification system. These are the steps in priority order:

1. Identify the appropriate administrator and data custodian. The data custodian is responsible for protecting the information, running backups, and performing data restoration.
2. Specify the criteria for classifying and labelling the information.
3. Classify the data by its owner, who is subject to review by a supervisor.
4. Specify and document any exceptions to the classification policy.
5. Specify the termination procedures for declassifying the information or for transferring custody of the information to another entity.
6. Create an enterprise awareness program about the classification controls.

Virtual Private Networks

VPN stands for "Virtual Private Network" and describes the opportunity to establish a protected network connection when using public networks. VPNs encrypt your internet traffic and disguise your online identity. This makes it more difficult for third parties to track your activities online and steal data.

Working principle of VPN

A VPN hides the IP address of the user and control the network through a specially configured remote server run by a VPN host. This means that if you surf online with a VPN, the VPN server becomes the source of your data. This means your Internet Service Provider (ISP) and other third parties cannot see which websites you visit or what data you send and receive online. A VPN works like a filter that turns all your data into "garbage". Even if someone were to get their hands on your data, it would be useless. A VPN connection hides your data traffic online and protects it from external access.

Features of VPN

- **Encryption of IP address:** The primary job of a VPN is to hide the IP address from the ISP and other third parties. This allows you to send and receive information online without the risk of anyone but you and the VPN provider seeing it.
- **Encryption of protocols:** A VPN should also prevent you from leaving any proof, in the form of internet history, search history and cookies. The encryption of cookies is especially important because it prevents third parties from gaining access to confidential information such as personal data, financial information and other content on websites.
- **Kill switch:** If your VPN connection is suddenly interrupted, your secure connection will also be interrupted. A good VPN can detect this sudden downtime and terminate all the activities of the user.
- **Two-factor authentication:** By using a variety of authentication methods, a strong VPN checks everyone who tries to log in. For example, you might be prompted to enter a password, after which a code is sent to your mobile device. This makes it difficult for uninvited third parties to access your secure connection.

Benefits of a VPN connection

- **Secure encryption:** With the help of a VPN, online activities can be hidden even on public networks.
- **Disguising your whereabouts :** VPN servers essentially act as your proxies on the internet. Because the actual location cannot be determined. In addition, most VPN services do not store logs of your activities.
- **Access to regional content:** Regional web content is not always accessible from everywhere. Services and websites often contain content that can only be accessed from certain parts of the world. Standard connections use local servers in the country to determine your location. This means that you cannot access content at home while traveling, and you cannot access international content from home.

- **Secure data transfer:** If you work remotely, you may need to access important files on your company's network. For security reasons, this kind of information requires a secure connection. To gain access to the network, a VPN connection is often required. VPN services connect to private servers and use encryption methods to reduce the risk of data leakage.

Key management

Key management refers to managing cryptographic keys within a cryptosystem. It deals with generating, exchanging, storing, using and replacing keys as needed at the user level. A key management system will also include key servers, user procedures and protocols, including cryptographic protocol design. The security of the cryptosystem is dependent upon the successful key management.

When designing a Key Management System, a system designer may not necessarily be a member of the organization that will be using the system. Therefore, he may not have access to the policies of the organization. Often the designer will create a set of policies and features that are commonplace for the organization's market. The designer will normally then provide documentation to explain how these policies and features are used within the Security Policy.

Key Management Compliance

This includes the following individual compliance domains:

- **Physical security** – the most visible form of compliance, which may include locked doors to secure system equipment and surveillance cameras. These safeguards can prevent unauthorized access to printed copies of key material and computer systems that run key management software.
- **Logical security** – protects the organization against the theft or unauthorized access of information. This is where the use of cryptographic keys comes in by encrypting data, which is then rendered useless to those who do not have the key to decrypt it.
- **Personnel security** – this involves assigning specific roles or privileges to personnel to access information on a strict need-to-know basis. Background checks should be performed on new employees along with periodic role changes to ensure security.

Problems and Challenges of Key Management

Managing keys can be a challenge, especially for larger organizations that rely upon cryptography for various applications. The primary problems that are associated with managing cryptographic keys include:

- Using the correct procedure to update system certificates and keys
- Updating certificate and keys before they expire
- Dealing with proprietary issues when keeping track of crypto updates with legacy systems
- Locating remote devices that need to be updated

Ten Security Tips for a Key Management System

1. Document the Security Policy so that it is easily understood.
2. Maintain malware protection
3. Patch vulnerabilities and turn off non-essential services on servers and devices
4. Perform third-party penetration testing
5. Make the system easy to use
6. Set up remote monitoring
7. Define appropriate crypto-periods for keys
8. Assign key management system roles and responsibilities
9. Meet the goals of the organization's information security policies
10. Define and classify cryptographic zones

Public Key and Encryption Key management

Public key

Public key is a class of cryptographic protocol based on algorithms. This method of cryptography requires two separate keys, one that is private or secret, and one that is public. Public key cryptography uses a pair of keys to encrypt and decrypt data to protect it against unauthorized access or use. Network users receive a public and private key pair from certification authorities. If other users want to encrypt data, they get the intended recipient's public key from a public directory. This key is used to encrypt the message, and to send it to the recipient. When the message arrives, the recipient decrypts it using a private key, to which no one else has access.

Public key cryptography remains the most secure protocol (over private key cryptography) because users never need to transmit or reveal their private keys to anyone, which lessens the chances of cyber criminals discovering an individual's secret key during the transmission.

Encryption key management

Encryption is the process of pushing the data so that only the intended party/organization can access it. This process is done through the use of security tools known as encryption keys or cryptographic keys. Each key consists of a randomly generated string of bits that are used to encrypt (and/or decrypt) data.

Encryption key management is administering the full lifecycle of cryptographic keys. This includes: generating, using, storing, archiving, and deleting of keys. Protection of the encryption keys includes limiting access to the keys physically, logically, and through user/role access.

Encryption key management involves:

- Developing and implementing a variety of policies, systems, and standards that govern the key management process
- Performing necessary key functions such as key generation, pre-activation, activation, expiration, post-activation etc.
- Securing physical and virtual access to the servers.
- Limiting user/role access to the encryption keys.

Digital certificates

A **Digital Certificate** is an electronic "password" that allows a person, organization to exchange data securely over the Internet using the public key infrastructure (PKI). Digital Certificate is also known as a **public key certificate** or **identity certificate**.

Digital certificates are used in public key cryptography functions. They are most commonly used for initializing secure SSL (**Secure Sockets Layer**) connections between web browsers and web servers. Digital certificates are also used for sharing keys to be used for public key encryption and authentication of digital signatures.

SSL (Secure Sockets Layer): Secure Sockets Layer (SSL) is a networking protocol designed for securing connections between web clients and web servers over an insecure network, such as the Internet.

Digital certificates are used by all major web browsers and web servers to provide assurance that published content has not been modified by any unauthorized actors, and to share keys for encrypting and decrypting web content. Digital certificates are also used in other contexts, both online and offline, for providing cryptographic assurance and privacy of data.

Types of Digital Certificates

There are three types of Digital Certificates; namely

1. **TLS/SSL Certificate:** TLS/SSL (Transport Layer Security/Secure Socket Layer) Certificates are installed on the server. The purpose of these certificates is to ensure that all communication between the client and the server is private and encrypted.
2. **Code Signing Certificate:** Code Signing Certificates are used to sign software or files that are downloaded over the internet. They're signed by the developer/publisher of the software. Their purpose is to guarantee that the software or file is genuine and comes from the publisher
3. **Client Certificate:** Client Certificates or Digital IDs are used to identify one user to another, a user to a machine, or a machine to another machine. One common example is emails, where the sender digitally signs the communication, and the recipient verifies the signature. Client certificates authenticate the sender and the recipient.

Memory Cards

Memory cards provide non-volatile storage of information, but they do not have any processing capability. A memory card stores encrypted passwords and other related identifying information. A telephone calling card (SIM CARD) and an ATM card are examples of memory cards.

Implementing Identity Management

Identification and authentication are the keystones of most access control systems. Identification is the act of a user admitting an identity to a system, usually in the form of a username or user logon ID to the system. Authentication is a process that verifies the user's identity by implementing password technic at the time of logon. Authentication is based on the following three factor:

- Type 1 — Something you know, such as a personal identification number (PIN) or password
- Type 2 — Something you have, such as an ATM card or smart card
- Type 3 — Something you are (physically), such as a finger print or retina scan

Identity management includes....

- Establishing a database of identities and credentials
- Managing users' access rights
- Enforcing security policy
- Developing the capability to create and modify accounts
- Setting up monitoring of resource accesses
- Installing a procedure for removing access rights
- Providing training in proper procedures

Controls and Autonomic System

Controls

Controls are implemented to manage the risk factor. Controls provide accountability for individuals who are accessing sensitive information in a cloud environment. This accountability is accomplished through access control mechanisms that require identification and authentication, and through the audit function. These controls must be in accordance with and accurately represent the organization's security policy. Control measures can be administrative, logical (also called technical), and physical in their implementation.

- Administrative control includes policies, procedures, security, background checks, work habit checks, and increased supervision.
- Logical or technical controls involve the restriction of access to systems and the protection of information. Examples of these types of controls are encryption, smart cards, access control lists, and transmission protocols.
- Physical controls incorporate guards and building security in general, such as the locking of doors, the securing of server rooms or laptops, the protection of cables, the separation of duties, and the backing up of files.

Autonomic Systems

The autonomic computing system has the goal of performing self-management to maintain correct operations despite alarms to the system. Such a system requires physical inputs, decision-making capability, and the ability to implement various activities to maintain the normal operation.

An Autonomic system controls the following systems.

- Malicious attacks
- Hardware or software faults
- Excessive CPU utilization
- Power failures
- Organizational policies
- Inadvertent operator errors
- Interaction with other systems
- Software updates

The eight autonomic computing concepts are:

- Self-awareness — An autonomic application/system “knows itself” and is aware of its state and its behaviours.
- Self-configuring — An autonomic application/system should be able to configure and reconfigure itself under varying and unpredictable conditions.
- Self-optimizing — An autonomic application/system should be able to detect sub-optimal behaviours and optimize itself to improve its execution.
- Self-healing — An autonomic application/system should be able to detect and recover from potential problems and continue to function smoothly.
- Self-protecting — An autonomic application/system should be capable of detecting and protecting its resources from both internal and external attack and maintaining overall system security and integrity.
- Context-aware — An autonomic application/system should be aware of its execution environment and be able to react to changes in the environment.
- Open — An autonomic application/system must function in a heterogeneous world and should be portable across multiple hardware and software architectures. Consequently, it must be built on standard and open protocols and interfaces.
- Anticipatory — An autonomic application/system should be able to anticipate, to the

extent possible, its needs and behaviours and those of its context, and be able to manage itself proactively.



Market Based Management of Clouds

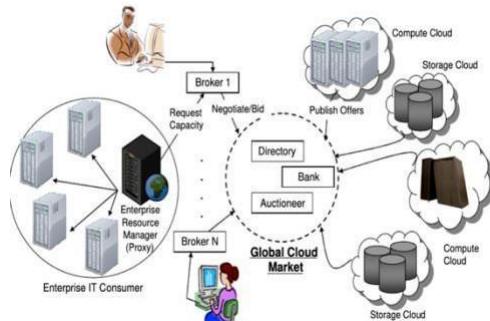
The Real Potential of cloud computing is that, to facilitates the establishment of a market for trading IT utilities. Market oriented cloud computing is a virtual market place where IT Service can be trade.

Reference model of market oriented cloud computing (MOCC)

MOCC originated from the coordination between several users, service providers, and some other entities that make trading between these two groups possible.

There are three major components of cloud exchange are:-

- **Directory**:- The market directory contains a listing of all the published services that are available in the cloud marketplace.
- **Auctioneer**:- The auctioneer is in charge of keeping track of the running auctions in the market place and verifying that the auctions for services are properly conducted and prevented from performing illegal activities.
- **Bank**:-the bank is the component that takes care of the financial aspect of all the operations happening in the virtual market place.



Market oriented architecture for data centres

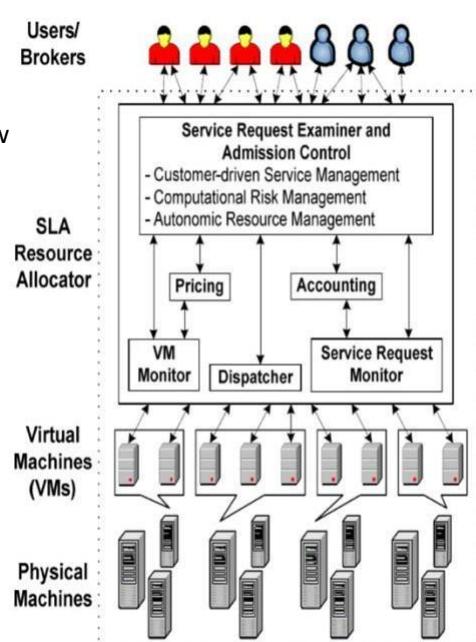
The major components of architecture are:-

Brokers:- They submit their service requests from anywhere in the world to the cloud.

SLA resource allocator:-It is a kind of interface between users and cloud service provider which enable the SLA oriented resource management.

Service request examiner and admission control:-It interprets the submitted request for QoS (Quality Of Service) requirement before determining whether to accept or reject the request.

Pricing:-It is responsible for billing based on the resource utilised.



Accounting:- It is responsible for maintaining the actual resources used by the user, so that the final coat can be charged to the users.

VM monitor:- It keeps the track on the availability of VMs and their resources.

Dispatcher:- The dispatcher mechanism starts the execution of accepted requests on allocated VMs.

Cloud request monitor:- It keeps the track on execution of request with SLA.

Cloud Information security vendors

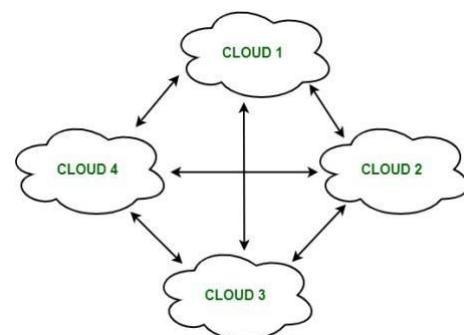
Cloud Security is the set of policies and technologies designed to protect data and infrastructure involved in a cloud computing environment. The top concerns that the cloud security companies are looking into the Identity, Access management, and Data privacy.

Top cloud security companies

- **FireEye**: In October 2019, FireEye announced its FireEye Cloud Security Solution, which includes cloud versions of FireEye Network Security, Detection On Demand security scanning, and the FireEye Helix security operations platform.
- **Lacework**: Lacework is a cloud workload security and compliance solution that is well suited for organizations looking for a visual approach to cloud security.
- **McAfee**: McAfee has a broad set of cloud security capabilities, including CASB, data loss prevention (DLP) and threat prevention.
- **Palo Alto Networks**: Palo Alto Networks has one of the most comprehensive cloud native security platforms in the market, with deep capabilities to help organizations with workload security.
- **Symantec**: Symantec has multiple cloud security functions within its portfolio, including workload protection and CASB.

Cloud Federation, characterization

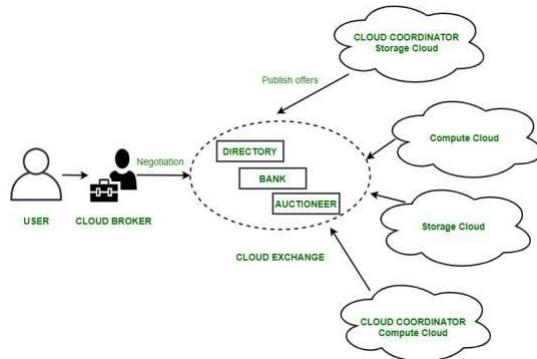
Cloud Federation, also known as Federated Cloud is the deployment and management of several external and internal cloud computing services to match business needs. It is a multi-national cloud system that integrates private, community, and public clouds into scalable computing platforms. Federated cloud is created by connecting the cloud environment of different cloud providers using a common standard.



The architecture of Federated Cloud:

1. Cloud Exchange

The Cloud Exchange acts as a mediator between cloud coordinator and cloud broker. The demands of the cloud broker are taken care by the cloud exchange to the available services provided by the cloud coordinator.



2. Cloud Coordinator

The cloud coordinator assigns the resources of the cloud to the remote users based on the quality of service they demand and the credits they have in the cloud bank. The cloud enterprises and their membership are managed by the cloud controller.

3. Cloud Broker

The cloud broker interacts with the cloud coordinator, analyses the Service-level agreement and the resources offered by several cloud providers in cloud exchange. Cloud broker finalizes the most suitable deal for their client.

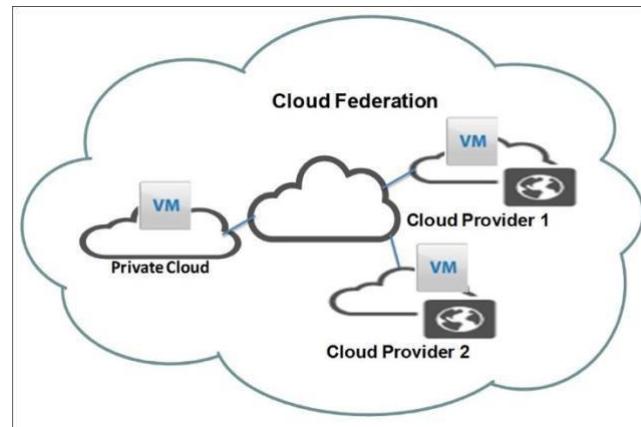
Benefits of Federated Cloud:

1. It minimizes the consumption of energy.
2. It increases reliability.
3. It minimizes the time and cost of providers due to dynamic scalability.
4. It connects various cloud service providers globally. The providers may buy and sell services on demand.

Cloud Federation stack

Cloud federation requires one provider to wholesale or rent computing resources to another cloud provider. Those resources become a temporary or permanent extension of the buyer's cloud computing environment, depending on the specific federation agreement between providers.

Cloud federation offers two big benefits to cloud providers.



First, it allows providers to earn revenue from computing resources which are idle or underutilized.

Second, cloud federation enables cloud providers to expand their geographic area and accommodate more users without establishing a new cloud server.

Third Party Cloud service

The third party cloud services is the services in which user want to acquire when he/she is not getting that service from acquired or hired cloud provider.

Advantages:

1. **Maintenance and support:** If something goes wrong it is the duty of the provider to ensure the problem is fixed.
2. **Security Benefit:** A lot of company feel more secure putting their data in the hands of an experienced cloud computing provider rather than jumping into the unknown and trying to manage the security of their important data themselves.
3. **Cost advantages:** Third party clouds are particularly advantageous for SMBs (Small and Medium Business) because they do not require huge investments.

Disadvantages:

1. **Security worries:** You are entirely responsible for the security of your own data.
2. **Lack of control:** With third party cloud computing you have minimal control over cloud and its management.
3. **Potential cost drawbacks:** If you will access the third party cloud for along period like 5years or more than it is not a cost worthy.

Case study

Google App Engine:

- Google App Engine is An example of Platform as a Service (PaaS).
- Google App Engine provides Web app developers and enterprises with access to Google's scalable hosting and 1-tier Internet service.
- Google App Engine provides a scalable runtime based on the Java and Python programming language.
- Applications in Google app engine stores data in Google BigTable.
- Application in Google app engine uses Google query language.
- If applications are non-compatible to Google app engine, than application needed to be make compatible with Google app engine. All application are not supported by Google app engine.
- Google App Engine also removed some system administration and developmental tasks to make it easier to write scalable applications.

Cost of Google App Engine:

1. Google app engine provides limited resource usage as free of cost.
2. After free resource usage limit users can per day or per minute basis.

There are following reasons to use Google app engine:

Google app engine allows you to build web applications on the same stable and extendable platform which having support facility of Google's large number of applications.

1. Google app engine gives facility to use and run applications in Google's data centre.
2. Google app engine's language Java and Python are easy to understand and implement.
3. This platform is absolutely free; you can purchase additional resources if needed.
4. Using Google accounts you can use Google app engine's services.
5. It is easy to scale up as your data storage and traffic needs grows with time.
6. Google also provides marketing facility to our apps.
7. User can easily write the application code, and can test it on own local system and upload it to Google at the click of a button or with a few lines of command script.
8. There is no need to take approval from system administration to upload or launch a new version of the application.
9. Google takes care of all the apps maintenance and allows users/developers to focus on the features of the application.



Hadoop

Introduction

Hadoop is an open-source java-based software framework sponsored by the Apache Software Foundation for distributed storage and distributed processing of very large data sets on computer clusters built from commodity hardware. It provides storage for big data at a reasonable cost.

Data Source

Hadoop solves two key challenges with traditional databases:

Capacity: Hadoop stores large volumes of data. By using a distributed file system called HDFS (Hadoop Distributed File System), the data is split into chunks and saved across clusters of available servers. As these available servers are built with simple hardware configurations, these are economical and easily scalable for a large amount of data.

Speed: Hadoop stores and retrieves data faster. It uses the MapReduce functional programming model to perform parallel processing across data sets. So, when a query is sent to the database, instead of handling data sequentially, tasks are split and simultaneously run across the distributed servers. Finally, the output of all tasks is collated and sent back to the user. In this way it drastically improves the processing speed.

Data storage and Analysis

Apache Hadoop consist of two major parts:

1. Hadoop Distributed File System (HDFS)
2. MapReduce

Hadoop Distributed File System:

- HDFS is a file system or storage layer of Hadoop. It can store data and can handle very large amount of data.
- When the capacity of a file is large then it is necessary to partition it. And the file systems that manage the storage across a network of machines are called distributed file systems.
- Hadoop keeps data safe by duplicating data across nodes.

MapReduce:

MapReduce is a programming framework. It organizes multiple computers in a cluster in order to perform the calculations. It takes care of distributing the work between computers and putting results together.

Characteristics of Hadoop:

1. Hadoop provides a reliable shared storage(HDFS) and analysis system (Map Reduce).
2. Hadoop is highly scalable. It can contain thousands of servers.
3. Hadoop works on the principles of write once and read multiple times.
4. Hadoop is highly flexible, can process both structured as well as unstructured data

Comparison with other system

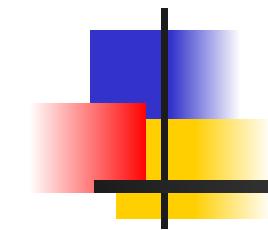
RDBMS (Relational Database Management System): RDBMS is an information management system, which is based on a data model. In RDBMS tables are used for information storage. Each row of the table represents a record and column represents an attribute of data. Organization of data and their manipulation processes are different in RDBMS from other databases. The purpose of RDBMS is to store, manage, and retrieve data as quickly and reliably as possible.

Hadoop: It is an open-source software framework used for storing data and running applications on a group of commodity hardware. It has large storage capacity and high processing power. It can manage multiple concurrent processes at the same time. It is used in predictive analysis, data mining and machine learning. It can handle both structured and unstructured form of data. It is more flexible in storing, processing, and managing data than traditional RDBMS. Unlike traditional systems, Hadoop enables multiple analytical processes on the same data at the same time. It supports scalability very flexibly.

Below is a table of differences between Data Science and Data Visualization:

SI No	RDBMS	HADOOP
1	Traditional row-column based databases, basically used for data storage, manipulation and retrieval.	An open-source software used for storing data and running applications or processes concurrently.
2	In this structured data is mostly processed.	In this both structured and unstructured data is processed.
3	It is best suited for OLTP (Online Transactional Processing) is a type of data processing environment.	It is best suited for BIG data.
4	It is less scalable than Hadoop.	It is highly scalable.
5	Data normalization is required in RDBMS.	Data normalization is not required in Hadoop.
6	It stores transformed and aggregated data.	It stores huge volume of data.
7	It has no latency in response.	It has some latency in response.
8	The data schema of RDBMS is static type.	The data schema of Hadoop is dynamic type.
9	High data integrity available.	Low data integrity available than RDBMS.
10	Cost is applicable for licensed software.	Free of cost, as it is an open source software.



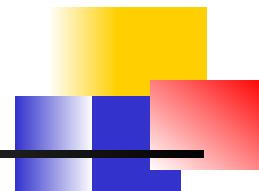


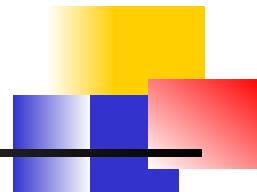
1. Introduction to Computer Security

Introduction to Security

Outline

1. Examples – Security in Practice
2. What is „Security?”
3. Pillars of Security:
Confidentiality, Integrity, Availability (CIA)
4. Vulnerabilities, Threats, and Controls
5. Attackers
6. How to React to an Exploit?
7. Methods of Defense
8. Principles of Computer Security





1. Examples – Security in Practice

Barbara Edicott-Popovsky and Deborah Frincke, CSSE592/492, U. Washington]

From CSI/FBI Report 2002

- 90% detected computer security breaches within the last year
- 80% acknowledged financial losses
- 44% were willing and/or able to quantify their financial losses.
These 223 respondents reported \$455M in financial losses.
- The most serious financial losses occurred through theft of proprietary information and financial fraud:

26 respondents: \$170M
25 respondents: \$115M

- For the fifth year in a row, more respondents (74%) cited their Internet connection as a frequent point of attack than cited their internal systems as a frequent point of attack (33%).
- 34% reported the intrusions to law enforcement. (In 1996, only 16% acknowledged reporting intrusions to law enforcement.)

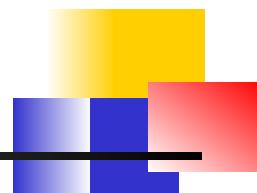
More from CSI/FBI 2002

- 40% detected external penetration
- 40% detected denial of service attacks.
- 78% detected employee abuse of Internet access privileges
- 85% percent detected computer viruses.
- 38% suffered unauthorized access or misuse on their Web sites within the last twelve months. 21% didn't know.
[includes insider attacks]
- 12% reported theft of transaction information.
- 6% percent reported financial fraud (only 3% in 2000).

Critical Infrastructure Areas

- Include:

- Telecommunications
- Electrical power systems
- Water supply systems
- Gas and oil pipelines
- Transportation
- Government services
- Emergency services
- Banking and finance
- ...

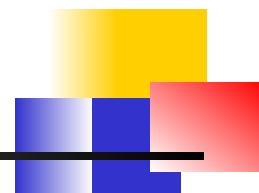


2. What is a “Secure” Computer System?

- To decide whether a computer system is “secure”, you must first decide what “secure” *means to you*, then identify the threats you care about.

You Will Never Own a Perfectly Secure System!

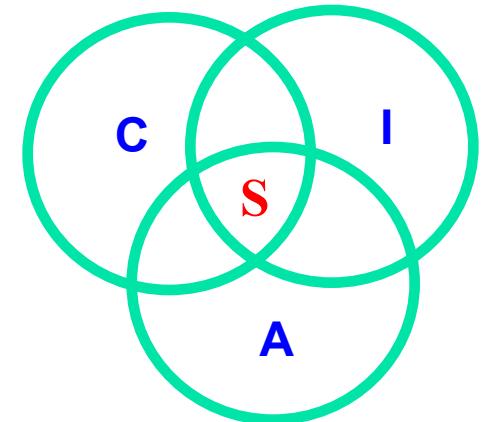
- Threats - examples
 - Viruses, trojan horses, etc.
 - Denial of Service
 - Stolen Customer Data
 - Modified Databases
 - Identity Theft and other threats to personal privacy
 - Equipment Theft
 - Espionage in cyberspace
 - Hack-tivism
 - Cyberterrorism
 - ...



3. Basic Components of Security: Confidentiality, Integrity, Availability (CIA)

■ CIA

- Confidentiality: Who is authorized to use data?
- Integrity: Is data „good?”
- Availability: Can access data whenever need it?

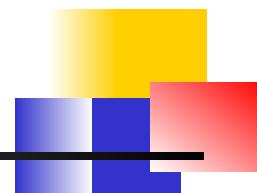


■ CIA or CIAAAN...

(other security components added to

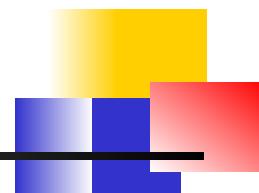
CIA)

- Authentication
- Authorization
- Non-repudiation
- ...



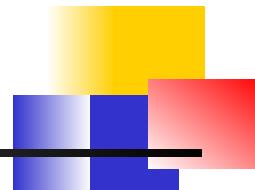
Need to Balance CIA

- Example 1: C vs. I+A
 - Disconnect computer from Internet to increase **confidentiality**
 - **Availability** suffers, **integrity** suffers due to lost updates
- Example 2: I vs. C+A
 - Have extensive data checks by different people/systems to increase **integrity**
 - **Confidentiality** suffers as more people see data, **availability** suffers due to locks on data under verification)



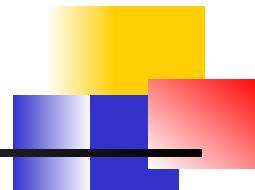
Confidentiality

- “Need to know” basis for data access
 - How do we know who needs what data?
Approach: **access control** specifies *who* can access *what*
 - How do we know a user is the person she claims to be?
Need her **identity** and need to **verify** this identity
Approach: **identification** and **authentication**
- Analogously: “Need to access/use” basis for physical assets
 - E.g., access to a computer room, use of a desktop
- Confidentiality is:
 - difficult to ensure
 - easiest to assess in terms of success (binary in nature:
Yes / No)



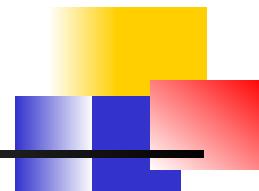
Integrity

- Integrity vs. Confidentiality
 - Concerned with **unauthorized modification** of assets (= resources)
Confidentiality - concerned with access to assets
 - Integrity is more difficult to *measure* than confidentiality
Not binary – degrees of integrity
Context-dependent - means different things in different contexts
Could mean *any subset of* these asset properties:
{ precision / accuracy / currency / consistency / meaningfulness / usefulness / ... }
- Types of integrity—an example
 - Quote from a politician
 - Preserve the quote (data integrity) but misattribute (origin integrity)



Availability (1)

- Not understood very well yet
 - „[F]ull implementation of availability is security's next challenge”
 - E.g. Full implementation of availability for Internet users (with ensuring security)
 - Complex
 - Context-dependent
 - Could mean *any subset* of these asset (data or service) properties :
 - { usefulness / sufficient capacity / progressing at a proper pace / completed in an acceptable period of time / ... }
- [Pfleeger & Pfleeger]



Availability (2)

- We can say that an asset (resource) is **available** if:
 - Timely request response
 - Fair allocation of resources (no starvation!)
 - Fault tolerant (no total breakdown)
 - Easy to use in the intended way
 - Provides controlled concurrency (concurrency control, deadlock control, ...)



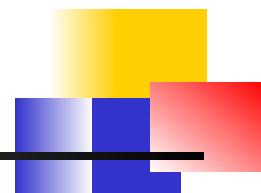
4. Vulnerabilities, Threats, and Controls

- Understanding **Vulnerabilities, Threats, and Controls**
 - **Vulnerability** = a weakness in a security system
 - **Threat** = circumstances that have a *potential* to cause harm
 - **Controls** = means and ways to block a threat, which tries to exploit one or more vulnerabilities
 - Most of the class discusses various controls and their effectiveness

[Pfleeger & Pfleeger]

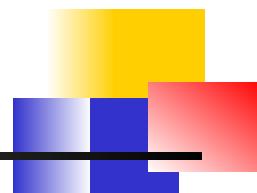
- Example - **New Orleans disaster (Hurricane Katrina)**
 - Q: What were city vulnerabilities, threats, and controls?
 - A: **Vulnerabilities**: location below water level, geographical location in hurricane area, ...
Threats: hurricane, dam damage, terrorist attack, ...
Controls: dams and other civil infrastructures, emergency response plan, ...

- **Attack** (materialization of a vulnerability/threat combination)
 - = exploitation of one or more vulnerabilities by a threat; tries to defeat controls
 - Attack may be:
 - *Successful* (a.k.a. an *exploit*)
 - resulting in a breach of security, a system penetration, etc.
 - *Unsuccessful*
 - when controls block a threat trying to exploit a vulnerability



Threat Spectrum

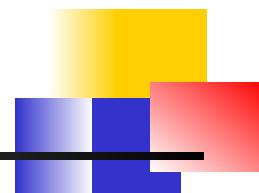
- Local threats
 - Recreational hackers
 - Institutional hackers
- Shared threats
 - Organized crime
 - Industrial espionage
 - Terrorism
- National security threats
 - National intelligence
 - Info warriors



Kinds of Threats

- Kinds of threats:
 - **Interception**
 - an unauthorized party (human or not) gains access to an asset
 - **Interruption**
 - an asset becomes lost, unavailable, or unusable
 - **Modification**
 - an unauthorized party changes the state of an asset
 - **Fabrication**
 - an unauthorized party counterfeits an asset
- Examples?

[Pfleeger & Pfleeger]



Levels of Vulnerabilities / Threats

(reversed order to illustrate interdependencies)

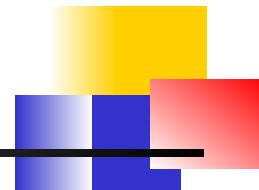
- D) for other assets (resources)
 - including. people using data, s/w, h/w
- C) for data
 - „on top” of s/w, since used by s/w
- B) for software
 - „on top” of h/w, since run on h/w
- A) for hardware



A) Hardware Level of Vulnerabilities / Threats

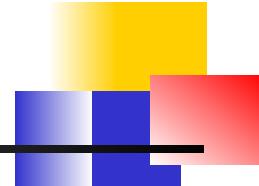
- Add / remove a h/w device
 - Ex: Snooping, wiretapping

Snoop = to look around a place secretly in order to discover things about it or the people connected with it. [Cambridge Dictionary of American English]
 - Ex: Modification, alteration of a system
 - ...
- Physical attacks on h/w => need physical security: locks and guards
 - Accidental (dropped PC box) or voluntary (bombing a computer room)
 - Theft / destruction
 - Damage the machine (spilled coffee, mice, *real* bugs)
 - Steal the machine
 - „Machinicide:“ Axe / hammer the machine
 - ...



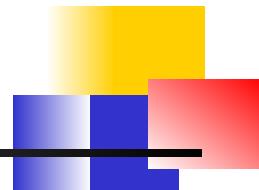
Example of Snooping: Wardriving / Warwalking, Warchalking,

- **Wardriving/warwalking** -- driving/walking around with a wireless-enabled notebook looking for unsecured wireless LANs
- **Warchalking** -- using chalk markings to show the presence and vulnerabilities of wireless networks nearby
 - E.g., a circled "W" -- indicates a WLAN protected by Wired Equivalent Privacy (WEP) encryption



B) Software Level of Vulnerabilities / Threats

- **Software Deletion**
 - Easy to delete needed software by mistake
 - To prevent this: use *configuration management software*
- **Software Modification**
 - Trojan Horses, , Viruses, Logic Bombs, Trapdoors, Information Leaks (via covert channels), ...
- **Software Theft**
 - Unauthorized copying
 - via P2P, etc.



Types of Malicious Code

Bacterium - A specialized *form of virus* which does not attach to a specific file. Usage obscure.

Logic bomb - Malicious *[program] logic* that *activates when specified conditions are met*.

Usually intended to cause denial of service or otherwise damage system resources.

Trapdoor - A hidden *computer flaw known to an intruder*, or a hidden computer mechanism (usually software) installed by an intruder, *who can activate the trap door to gain access to the computer without being blocked by security services or mechanisms*.

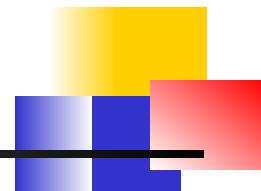
Trojan horse - A computer *program that appears to have a useful function*, but also has a hidden and potentially malicious function that evades security mechanisms, sometimes by exploiting legitimate authorizations of a system entity that invokes the program.

Virus - A hidden, *self-replicating section of computer software*, usually malicious logic, that *propagates by infecting* (i.e., inserting a copy of itself into and *becoming part of*) *another program*. A virus cannot run by itself; it requires that its host program be run to make the virus active.

Worm - A computer *program* that can run independently, *can propagate a complete working version of itself* onto other hosts on a network, and may consume computer resources destructively.

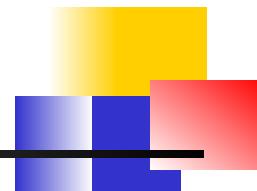
More types of malicious code exist...

[cf. <http://www.ietf.org/rfc/rfc2828.txt>]



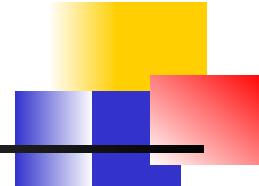
C) Data Level of Vulnerabilities / Threats

- How valuable is your data?
 - Credit card info vs. your home phone number
 - Source code
 - Visible data vs. context
 - „2345“ -> Phone extension or a part of SSN?
- Adequate protection
 - Cryptography
 - Good if intractable for a long time
- Threat of Identity Theft
 - Cf. Federal Trade Commission: <http://www.consumer.gov/idtheft/>



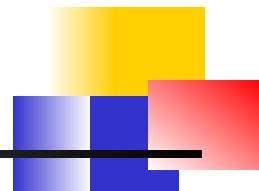
Identity Theft

- Cases in 2003:
 - Credit card skimmers plus drivers license, Florida
 - Faked social security and INS cards \$150-\$250
 - Used 24 aliases – used false id to secure credit cards, open mail boxes and bank accounts, cash fraudulently obtained federal income tax refund checks, and launder the proceeds
 - Bank employee indicted for stealing depositors' information to apply over the Internet for loans
 - \$7M loss, Florida: Stole 12,000 cards from restaurants via computer networks and social engineering
- Federal Trade Commission:
<http://www.consumer.gov/idtheft/>



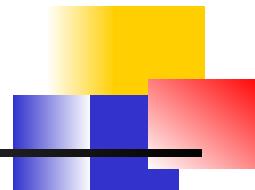
Types of Attacks on Data CIA

- Disclosure
 - Attack on data *confidentiality*
- Unauthorized modification / deception
 - E.g., providing wrong data (attack on data *integrity*)
- Disruption
 - DoS (attack on data *availability*)
- Usurpation
 - Unauthorized use of services (attack on data *confidentiality, integrity or availability*)



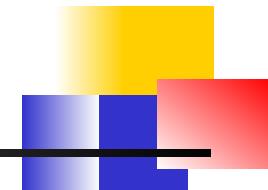
Ways of Attacking Data CIA

- Examples of Attacks on Data Confidentiality
 - Tapping / snooping
- Examples of Attacks on Data Integrity
 - Modification: salami attack -> little bits add up
 - E.g/ „shave off“ the fractions of cents after interest calculations
 - Fabrication: replay data -> send the same thing again
 - E.g., a computer criminal replays a salary deposit to his account
- Examples of Attacks on Data Availability
 - Delay vs. „full“ DoS
- Examples of Repudiation Attacks on Data:
 - Data origin repudiation: „I never sent it“
Repudiation = refusal to acknowledge or pay a debt or honor a contract
(especially by public authorities).
[<http://www.onelook.com>]
 - Data receipt repudiation: „I never got it“



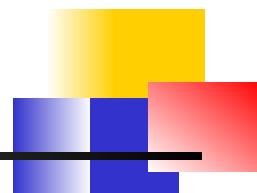
D) Vulnerab./Threats at Other Exposure Points

- **Network** vulnerabilities / threats
 - Networks multiply vulnerabilities and threats, due to:
 - their complexity => easier to make design/impl./usage mistakes
 - „bringing close“ physically distant attackers
 - Esp. wireless (sub)networks
- **Access** vulnerabilities / threats
 - Stealing cycles, bandwidth
 - Malicious physical access
 - Denial of access to *legitimate* users
- **People** vulnerabilities / threats
 - Crucial weak points in security
 - too often, the *weakest* links in a security chain
 - Honest insiders subjected to skillful **social engineering**
 - Disgruntled employees



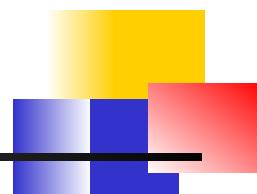
5. Attackers

- Attackers need MOM
 - Method
Skill, knowledge, tools, etc. with which to pull off an attack
 - Opportunity
Time and access to accomplish an attack
 - Motive
Reason to perform an attack



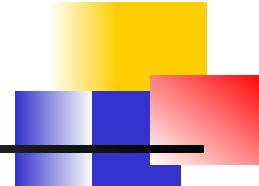
Types of Attackers

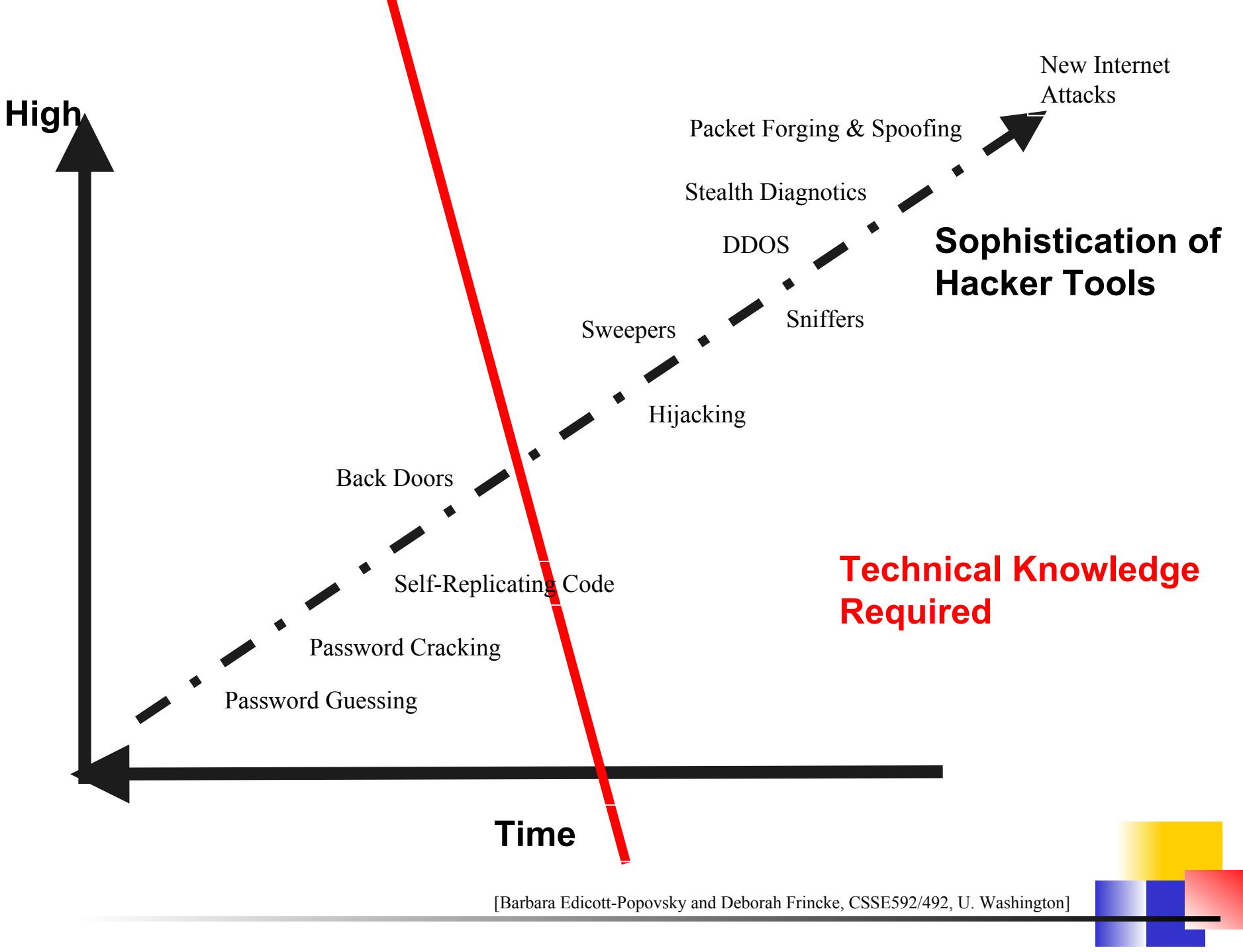
- Types of Attackers - Classification 1
 - Amateurs
 - Opportunistic attackers (use a password they found)
 - Script kiddies
 - Hackers - nonmalicious
 - In broad use beyond security community: also malicious
 - Crackers – malicious
 - Career criminals
 - State-supported spies and information warriors
- Types of Attackers - Classification 2 (cf. before)
 - Recreational hackers / Institutional hackers
 - Organized criminals / Industrial spies / Terrorists
 - National intelligence gatherers / Info warriors



Example: Hacking As Social Protest

- Hactivism
- Electro-Hippies
- DDOS attacks on government agencies
- SPAM attacks as “retaliation”

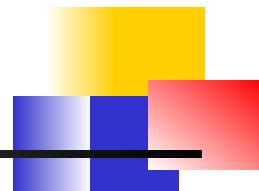




6. Reacting to an Exploit

Exploit = successful attack

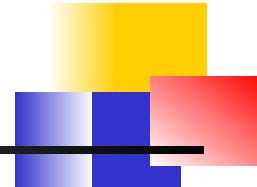
- Report to the vendor first?
- Report it to the public?
 - What will be public relations effects if you do/do not?
- Include source code / not include source code?
- Etc.



“To Report or Not To Report: Tension between Personal Privacy and Public Responsibility

An info tech company will typically lose between ten and one hundred times more money from shaken consumer confidence than the hack attack itself represents if they decide to prosecute the case.

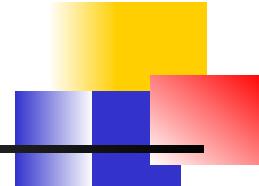
Mike Rasch, VP Global Security, testimony before the Senate Appropriations Subcommittee, February 2000 reported in The Register and online testimony transcript



Further Reluctance to Report

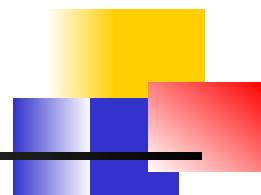
- One common fear is that a crucial piece of equipment, like a main server, say, might be impounded for evidence by over-zealous investigators, thereby shutting the company down.
- Estimate: fewer than one in ten serious intrusions are ever reported to the authorities.

Mike Rasch, VP Global Security, testimony before the Senate Appropriations Subcommittee, February 2000
reported in The Register and online testimony transcript



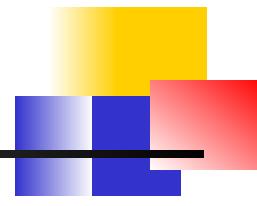
Computer Forensics Against Computer Crime

- Technology
- Law Enforcement
- Individual and Societal Rights
- Judiciary
- ...



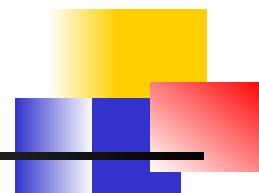
7. Methods of Defense

- Five basic approaches to defense of computing systems
 - Prevent attack
 - Block attack / Close vulnerability
 - Deter attack
 - Make attack harder (can't make it impossible ☺)
 - Deflect attack
 - Make another target more attractive than this target
 - Detect attack
 - During or after
 - Recover from attack

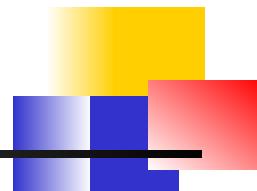


A) Controls

- Castle in Middle Ages
 - Location with **natural obstacles**
 - Surrounding **moat**
 - **Drawbridge**
 - **Heavy walls**
 - Arrow slits
 - Crenellations
 - Strong **gate**
 - Tower
 - Guards / passwords
- Computers Today
 - Encryption
 - Software controls
 - Hardware controls
 - Policies and procedures
 - Physical controls

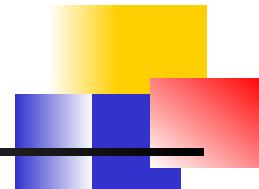


- Medieval castles
 - location (steep hill, island, etc.)
 - moat / drawbridge / walls / gate / guards /passwords
 - another wall / gate / guards /passwords
 - yet another wall / gate / guards /passwords
 - tower / ladders up
- Multiple controls in computing systems can include:
 - **system perimeter** – defines „inside/outside”
 - **preemption** – attacker scared away
 - **deterrence** – attacker could not overcome defenses
 - **faux environment** (e.g. **honeypot**, **sandbox**) – attack deflected towards a worthless target (but the attacker doesn't know about it!)
- à Note **layered defense** /
multilevel defense / **defense in depth** (ideal!)



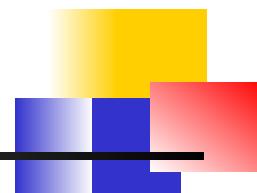
A.1) Controls: Encryption

- Primary controls!
- Cleartext scrambled into ciphertext (enciphered text)
- Protects CIA:
 - confidentiality – by „masking” data
 - integrity – by preventing data updates
 - e.g., checksums included
 - availability – by using encryption-based protocols
 - e.g., protocols ensure availability of resources for different users

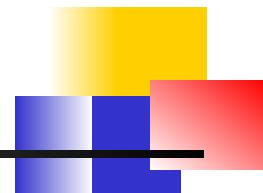


A.2) Controls: Software Controls

- Secondary controls – second only to encryption
- Software/program controls include:
 - OS and network controls
 - E.g. OS: sandbox / virtual machine
 - Logs/firewalls, OS/net virus scans, recorders
 - independent control programs (whole programs)
 - E.g. password checker, virus scanner, **IDS** (intrusion detection system)
 - internal program controls (part of a program)
 - E.g. read/write controls in DBMSs
 - development controls
 - E.g. quality standards followed by developers
 - incl. testing

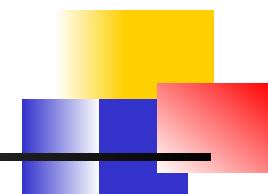


- Considerations for Software Controls:
 - Impact on user's interface and workflow
 - E.g. Asking for a password too often?



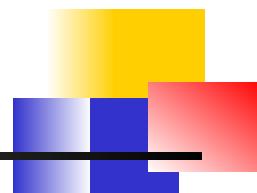
A.3) Controls: Hardware Controls

- Hardware devices to provide higher degree of security
 - Locks and cables (for notebooks)
 - Smart cards, dongles, hardware keys, ...
 - ...

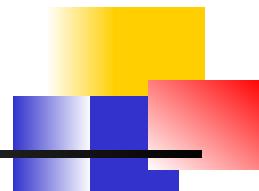


A.4) Controls: Policies and Procedures

- Policy vs. Procedure
 - **Policy:** *What* is/what is not allowed
 - **Procedure:** *How* you enforce policy
- Advantages of policy/procedure controls:
 - Can replace hardware/software controls
 - Can be least expensive
 - Be careful to consider *all* costs
 - E.g. help desk costs often ignored for for passwords (=> look cheap but might be expensive)

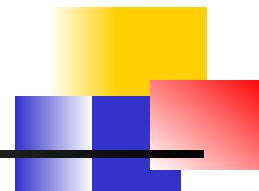


- Policy - must consider:
 - Alignment with users' legal and ethical standards
 - Probability of use (e.g. due to inconvenience)
 - Inconvenient: 200 character password,
change password every week
 - (Can be) good: biometrics replacing passwords
- Periodic reviews
 - As people and systems, as well as their goals, change



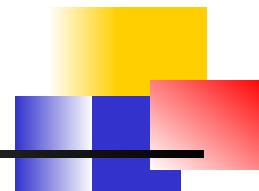
A.5) Controls: Physical Controls

- Walls, locks
- Guards, security cameras
- Backup copies and archives
- Cables and locks (e.g., for notebooks)
- Natural and man-made disaster protection
 - Fire, flood, and earthquake protection
 - Accident and terrorism protection
- ...



B) Effectiveness of Controls

- Awareness of problem
 - People convinced of the need for these controls
- Likelihood of use
 - Too complex/intrusive security tools are often disabled
- Overlapping controls
 - >1 control for a given vulnerability
 - To provide layered defense – the next layer compensates for a failure of the previous layer
- Periodic reviews
 - A given control usually becomes less effective with time
 - Need to replace ineffective/inefficient controls with better ones



8. Principles of Computer Security

[Pfleeger and Pfleeger]

- **Principle of Easiest Penetration** (p.5)

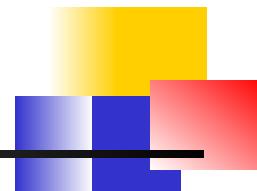
An intruder must be expected to use any available means of penetration.

The penetration may not necessarily be by the most obvious means, nor is it necessarily the one against which the most solid defense has been installed.

- **Principle of Adequate Protection** (p.16)

Computer items must be protected to a degree consistent with their value and only until they lose their value.

[modified by LL]



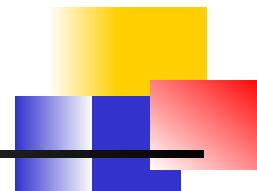
- **Principle of Effectiveness** (p.26)

Controls must be used—and used properly—to be effective.

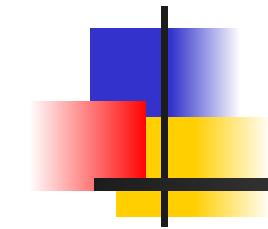
They must be efficient, easy to use, and appropriate.

- **Principle of Weakest Link** (p.27)

Security can be no stronger than its weakest link. Whether it is the power supply that powers the firewall or the operating system under the security application or the human, who plans, implements, and administers controls, a failure of any control can lead to a security failure.



End of Section 1: Introduction



Kubernetes

Docker Vs Kubernetes



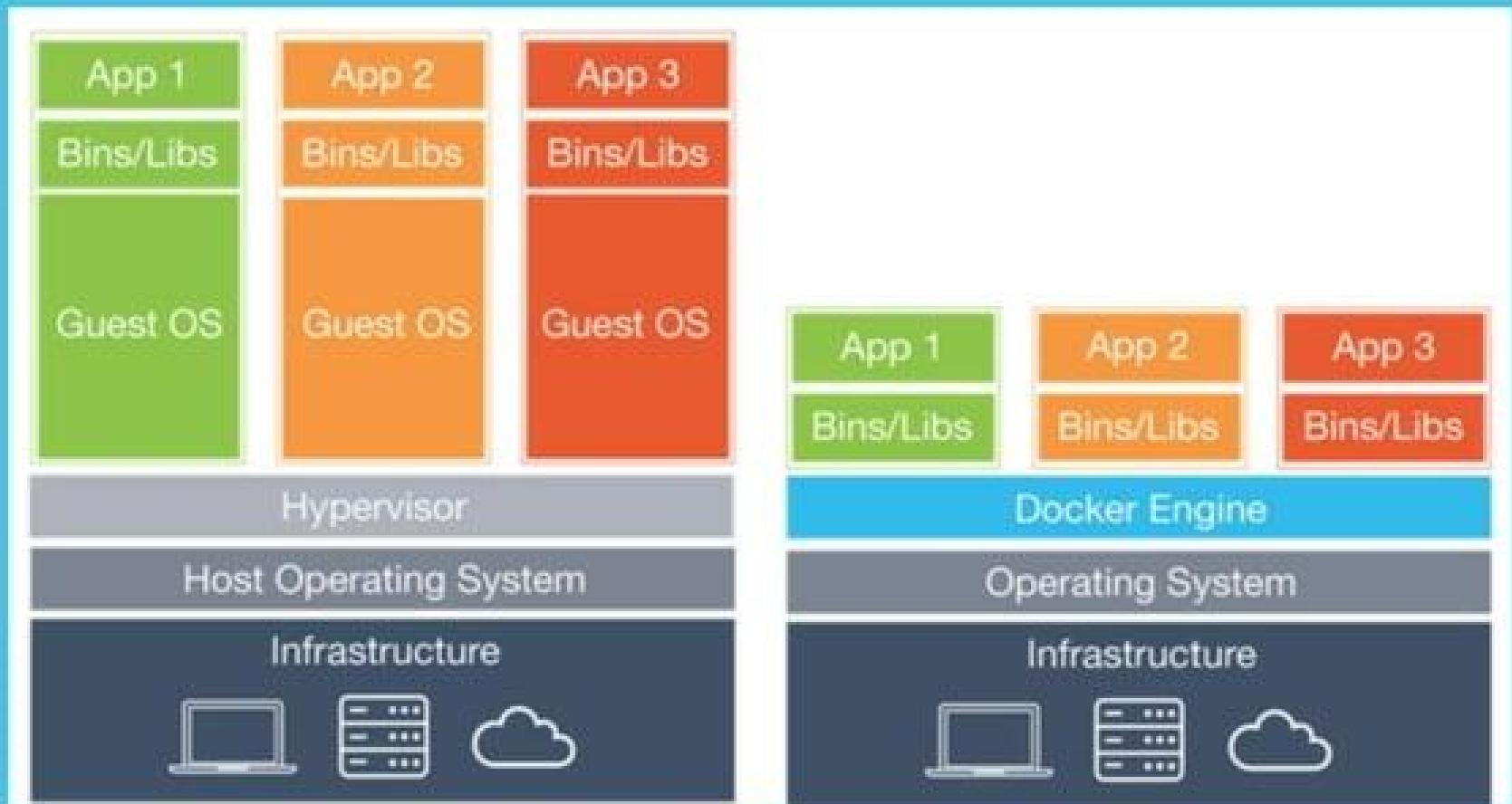


Virtualisation Technologies - VMs vs. Containers

Both are essentially structures for storing and running applications.

- Virtual Machines (VMs) - Isolated at hardware level, higher resource usage.
- Containers - Slightly less isolated, leaner and faster.
 - Docker has ~95% market share in containerisation technology.

Virtualisation Technologies - VMs vs. Containers



You can have 1000's of containers on a server

- Because containers are so lean, you can have a huge number of them on a single server. They allow large monolithic applications to be split into many microservices.
- Each microservice has its own container & controls one feature of the application.
 - **Benefit:** This is an efficient use of resources & can save on hosting costs compared to VMs.
 - **Problem:** How do you manage, rollout, rollback, maintain and repair such a large number of containers?
- The solution: **Kubernetes**

Kubernetes: Definition

- Kubernetes (K8S) is an open source software tool for managing containerised workloads.
- It operates at the container (*not hardware*) level to automate the deployment, scaling and management of applications.
- K8s works alongside a containerisation tool, like Docker. So if containers are the 'ingredients' of an application, then K8S would be the 'chef'.
- As well as managing individual containers, K8s can also manage **clusters**.
 - A cluster is a series of servers connected to run containers.
 - K8s can scale up to 5,000 servers and 150,000 pods in a single cluster.
 - A pod is a group of containers that share resources, a network and can communicate with one another.

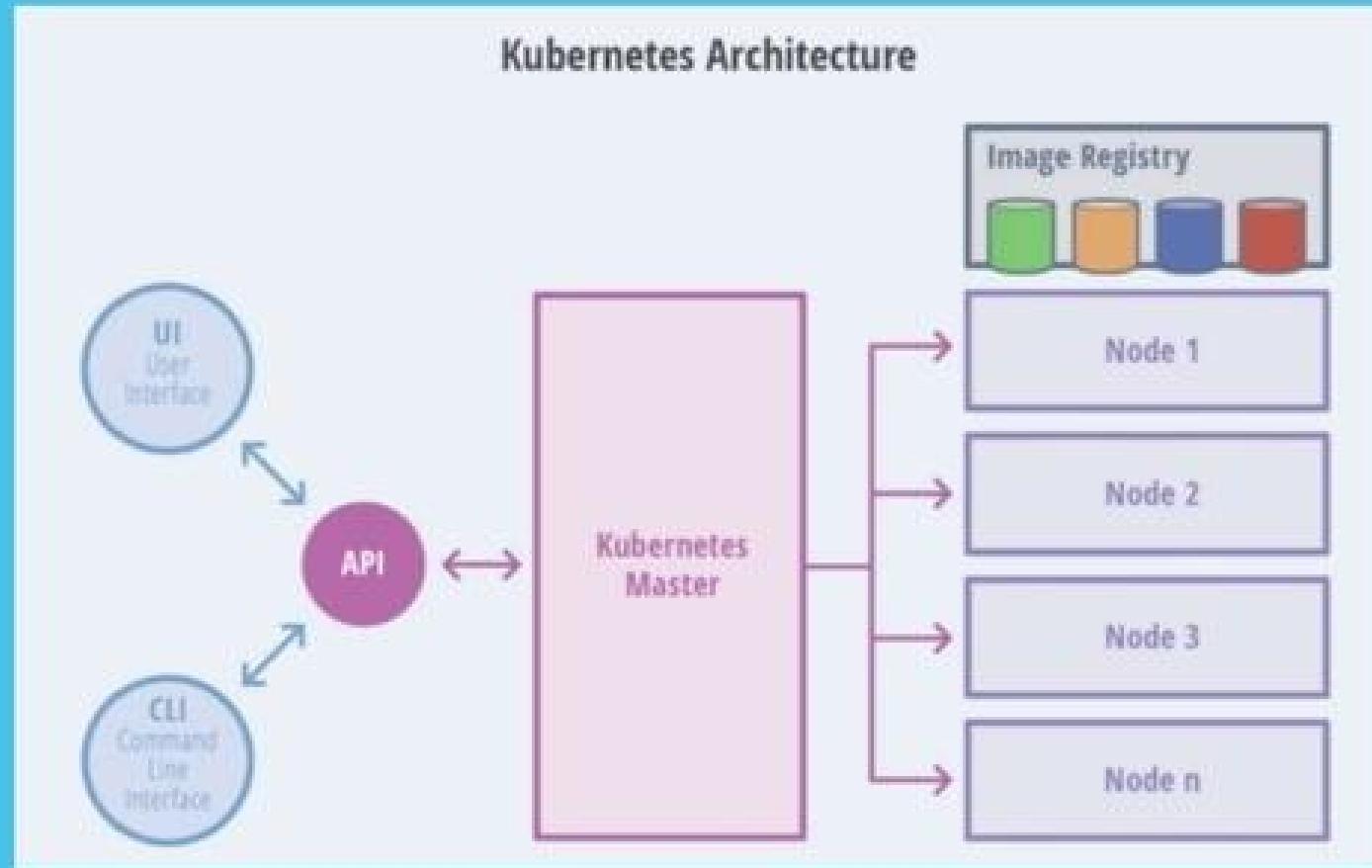
How Does Kubernetes Work?

Kubernetes has a master-slave architecture:

1. **Worker Nodes** (slave) - This is where containers are deployed.
These nodes contain:
 - a. Multiple pods
 - b. Docker engine
 - c. Any add-ons e.g. DNS
 - d. Kubelet - this is an important component as it carries out the instructions from the master node.
2. **Master Node** (master) - This controls the deployment. This node contains:
 - a. API server - this receives inputs from the User Interface (UI) or Command Line Interface (CLI).
 - b. Controller - uses information from the API to drive the application from its current state towards the desired state provided.
 - c. Scheduler
 - d. Etcd - handles configuration management, service discovery etc.

Kubernetes Architecture

To make the last slide easier to visualise, here is a diagram of the architecture:



Nodes 1-n (in purple) are the worker nodes.

Kubernetes Architecture

- Remembering the specific components and their roles isn't important here.
- The architecture has just been outlined to give some background on how Kubernetes is able to orchestrate containers at scale.
- Whilst initially the idea of Kubernetes sounds quite simple, seeing the architecture shows that it is actually fairly complex to work with.
- This is *why* Bytemark want to offer a managed Kubernetes service - so our customers can get the benefits of Kubernetes without worrying about managing and maintaining everything themselves.

Benefits of Kubernetes

- **Self-healing**
 - Clusters can auto-restore from errors by rolling back to the last working version of software. This allows teams to ship quickly without the risk of breaking anything.
- **High Availability**
 - Clusters can be recreated on a working node to avoid downtime during server failure.
- **Simplifies Maintenance**
 - If a server needs to be rebooted, or the host OS needs updating, containers can be moved to another node whilst maintenance is carried out.
- **Automatic Scaling**
 - Uses information from user requests and CPU usage to increase or decrease the number of nodes running to match demand.
- **Efficient**
 - Automatically spins up any new containers on under-utilized nodes.

Things Kubernetes does *not* do...

There are sometimes misconceptions about what Kubernetes can do. Kubernetes does not...

- Provide any comprehensive machine configuration.
- Provide a configuration language/system
- Dictate logging, monitoring or alerting solution
- Build your application
- Provide middleware, data-processing frameworks, databases, caches etc. BUT these components can run on Kubernetes



Where Success is a Tradition

Introduction to Nginx

What is Nginx

- Pronounced as “Engine X”
- Open source web and reverse proxy server
- High performance HTTP, HTTPS, SMTP, IMAP, POP3 server
- Load balancing and HTTP caching
- Asynchronous event-driven architecture

NGINX

NGINX is a powerful web server and uses a non-threaded, event-driven architecture.

It can also do other important things, such as **load balancing**, and **HTTP caching**, or be used as a **reverse proxy**.

Who uses Nginx



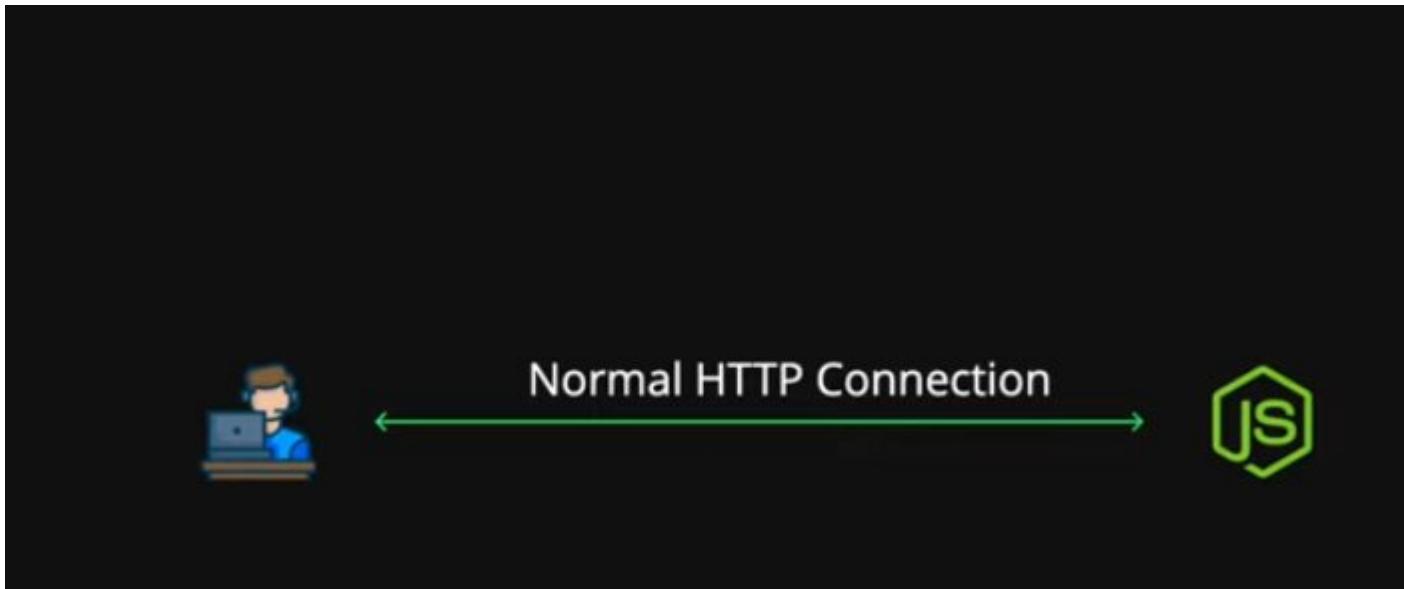
WORDPRESS

NETFLIX

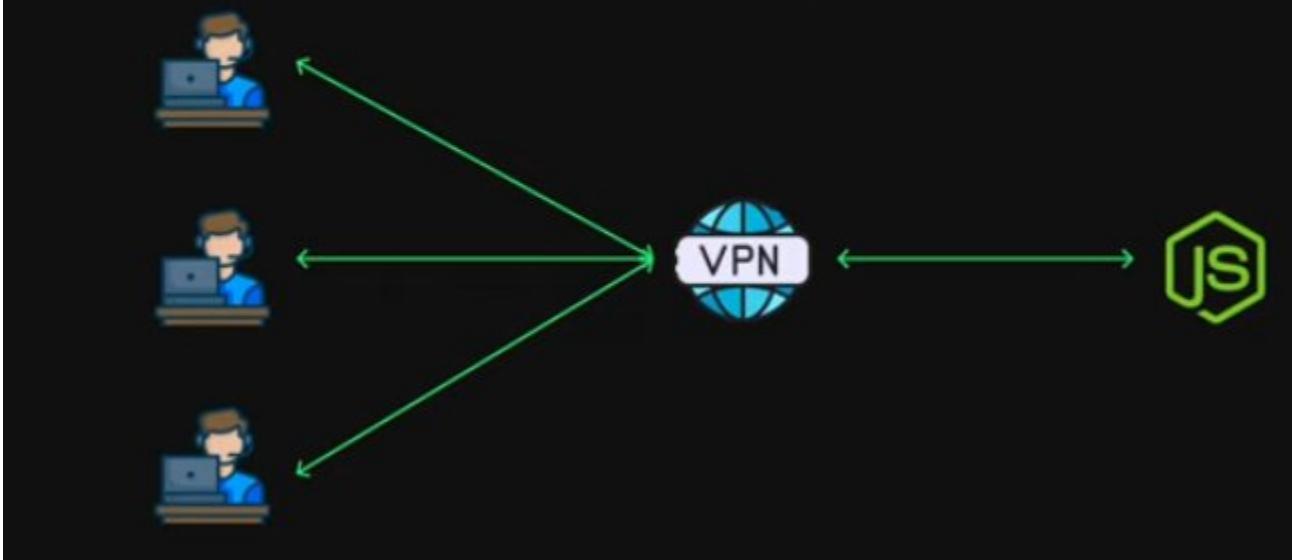


HEROKU

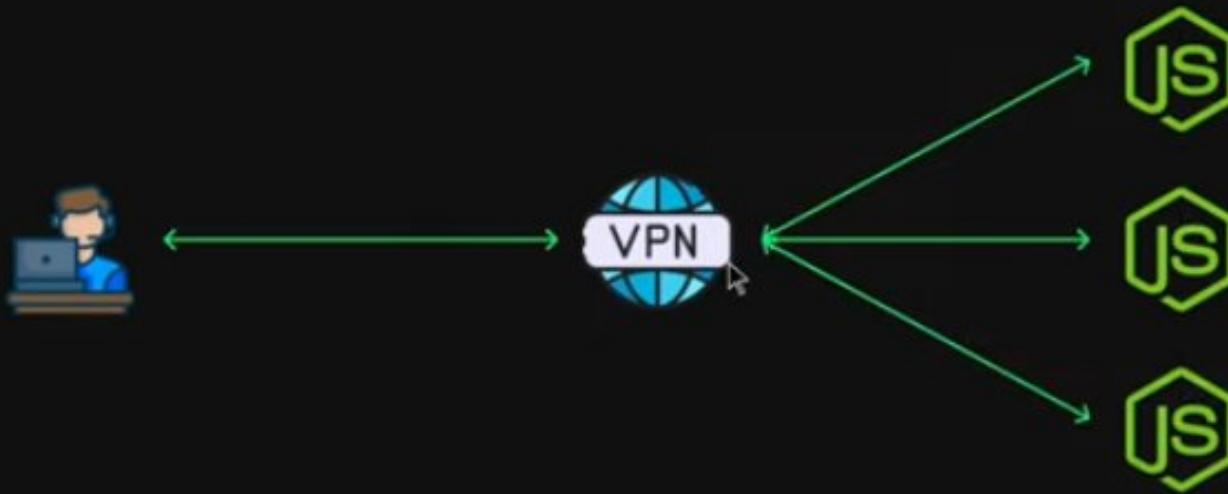




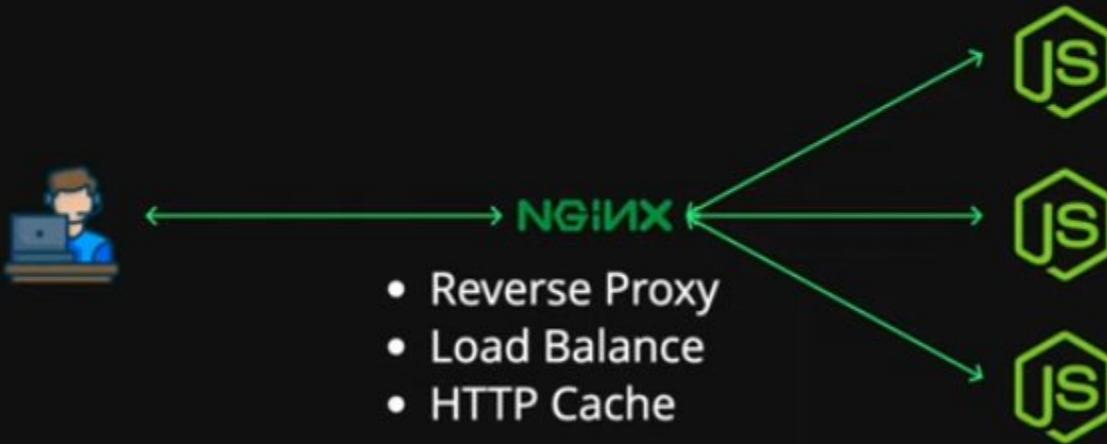
Forward Proxy



Reverse Proxy



Reverse Proxy





NGINX

- Can Handle 10,000 Concurrent Requests
- Cache HTTP Requests
- Act as Reverse Proxy
- Act as Load Balancer
- Act as an API Gateway
- Serve and Cache Static files like images, videos, etc.
- Handle SSL Certificates

Prerequisite



https://www.google.com/maps/@22.6404242,75.8417637,15z?entry=ttu&g_ep=EgoYMDi2MDEyNi4wIKXMDSoKLDeWMDc5MjA2OUgBUAM%3D

Search Google Maps

Restaurants Hotels Things to do Museums Transit Pharmacies ATMs Chat

Silicon City

Heavy traffic in this area
Much slower than usual

Silicon City Rd SHIV CITY NIHALPUR MUNDI SHIV SITI Hindu temple

AB ROAD KANUPRIYA NAGAR THE CHOGALA GURUKUL COLONY NEW NEHRU NAGER Chick Chick Chick Shriram Automall Indore Highway Heaven Restaurant Swaad Anantaa

Chowk Chowk Tatva Cine Wheels Drive-In Theatre By Windasa Machala

Layers

Imagery ©2026, Map data ©2026 India Terms Privacy Send Product Feedback 500 m 20:09 28-01-2026

Teacher : HEMANT KUMAR GUPTA

Class : B.Tech. CST (VI Sem)

Section : B

Subject : Cloud Engineering (Hosting & Deployment) : ACTDCCLD001T



Regenerated QR Code

Class : B.Tech. CST (VI Sem)
Section : B
Subject : Cloud Engineering (Hosting & Deployment) LAB : ACTDCCLD001P



Regenerated QR Code

Teacher : HEMANT KUMAR GUPTA

Class : B.Tech. CST (VI Sem)

Section : B

Subject : Cloud Engineering (Hosting & Deployment) LAB : ACTDCCLD00



Regenerated QR Code



Introduction

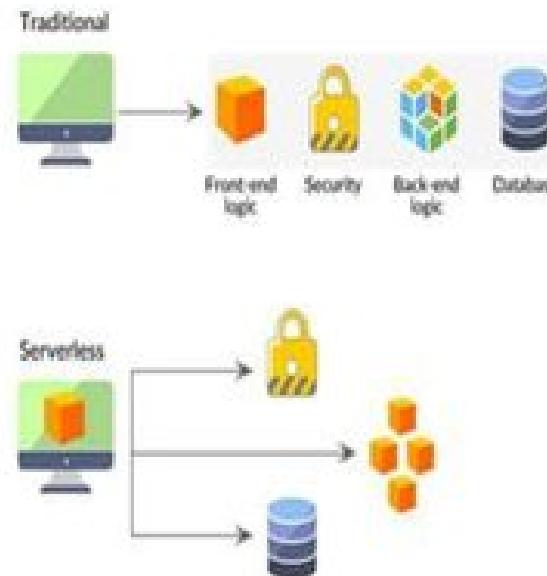
- Serverless Computing (or simply serverless) is emerging as a new and compelling model for the deployment of cloud applications

Server less architecture relies on managed services where you only pay for what you use, without worrying about infrastructure

Introduction

There are many immediate benefits to not managing your own servers:

- You don't have to worry about them randomly rebooting or going down.
- You don't end up with snowflake servers, where you don't know quite what's installed on them but they are mission-critical to your organisation.
- You're not responsible for installing software on them. Even if you use configuration management tools such as Chef or Ansible to automate this, that's still extra code you have to maintain over time.



What is Serverless Computing?

- Serverless Computing is a cloud computing execution model in which the cloud provider dynamically manages the allocation of machine resources, and bills based on the actual amount of resources consumed by an application, rather than billing based on pre-purchased units of capacity..
- The version of serverless that explicitly uses functions as the deployment unit is also called Function-as-a-Service (FaaS).

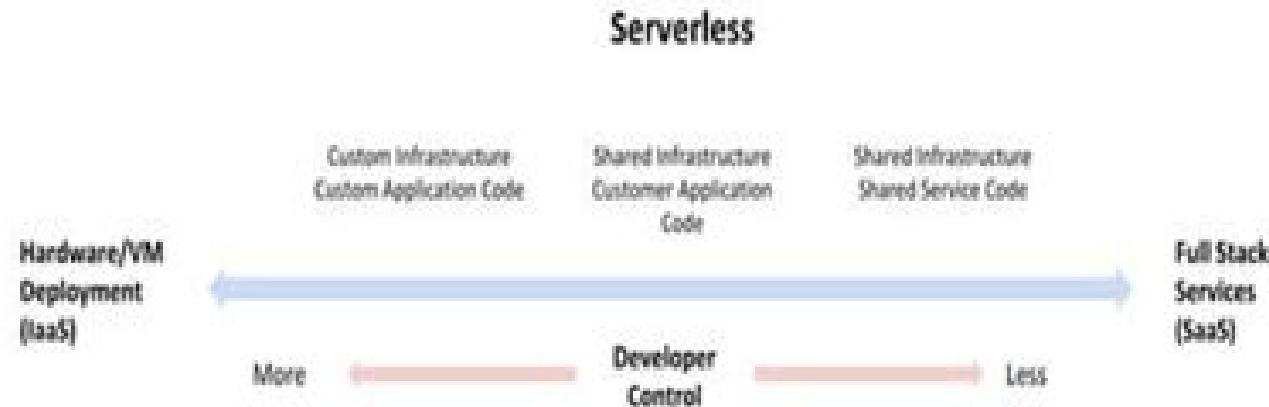
Feature	Server-Based	Serverless
Base Cost	\$20-\$50/month per server	Free for first 1M requests/month
Scaling Cost	Adds more servers, increases cost	Auto-scaling, pay-as-you-go
Maintenance	Manual (OS updates, patches)	Managed by the platform
Setup Time	Hours to days	Minutes
Flexibility	High customization	Limited customization
Application	high-customization, long-running applications	event-driven, cost-sensitive, and scalable applications

What is Serverless Computing?

- The Infrastructure-as-a-Service (IaaS) model is where the developer has the most control over both the application code and operating infrastructure in the cloud
- The developer is responsible for provisioning the hardware or virtual machines.
- Can customize every aspect of how an application gets deployed and executed.
- On the opposite extreme are the PaaS and SaaS models, where the developer is unaware of any infrastructure.
- The developer has access to prepackaged components or full applications. The developer is allowed to host code here, though that code may be tightly coupled to the platform.

Serverless?

- Serverless can be explained by varying level of developer control over the cloud infrastructure.



Serverless : Characteristics

- Independent, server-side, logical functions : small, separate, units of logic that take input arguments, process them in some manner, then return the result.
- Cost : Typically its Pay As You Go
- Simple Deployment : Thanks to the small size of deployment artifacts, in general, deployments are simple and quick. Deployment artifacts are typically idiomatic of the chosen runtime e.g. NuGet packages, npm packages, JAR files
- Ephemeral : designed to spin up quickly, do their work and then shut down again.
- Programming languages : Serverless services support a wide variety of programming languages - Node, Python.
- Stateless : FaaS are stateless, not storing states ,as containers running code will automatically destroy and created by platform.Horizontal Scaling becomes easy...

Serverless : Characteristics

- Scalable by Default
- Event Triggered :Although functions can be invoked directly, they are typically triggered by events from other cloud services, such as incoming HTTP requests,
- Simple Deployment Model.
- Small Deployable Units and More focus on Business Value.
- Managed by third party .
- No more “Works on my Machine”

Commercial platforms

- Amazon's AWS Lambda
- Google's Cloud Functions
- Microsoft Azure Functions
- IBM Cloud Functions
- OpenLambda

Commercial platforms

- Amazon's AWS Lambda
- Google's Cloud Functions
- Microsoft Azure Functions
- IBM Cloud Functions
- OpenLambda

Amazon's AWS Lambda

- Amazon's AWS Lambda was the first serverless platform ,it is a compute service that lets you run code without provisioning or managing servers."
- AWS Lambda executes code only when needed and scales automatically, from a few requests per day to thousands per second.
- Pay only for the compute time.
- Can run code for virtually any type of application or backend service



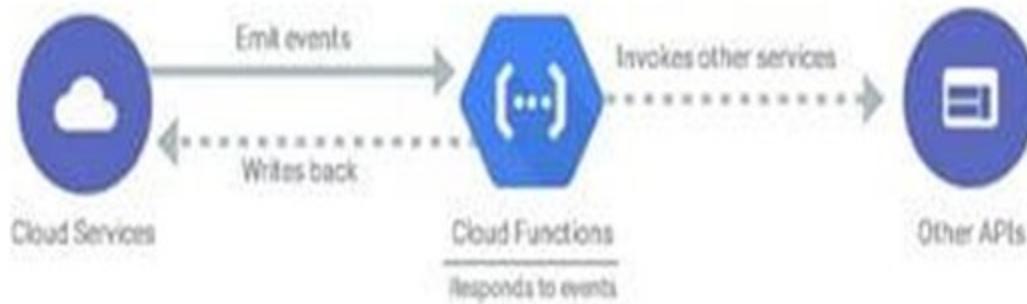
Amazon's AWS Lambda

- Currently AWS Lambda supports Node.js, Java, C# , Go and Python and PowerShell
- AWS Lambda automatically scales application by running code in response to each trigger.
- With AWS Lambda,we are charged for every 100ms



Google's Cloud Functions

- Google Cloud Functions provides basic FaaS functionality to run serverless functions written in Node.js, Go, Python and Java.
- Automatically scales, highly available and fault tolerant.
- No servers to provision, manage, or upgrade
- Pay only while your code runs.



Microsoft Azure Functions

- Microsoft Azure Functions provides HTTP webhooks and integration with Azure services to run user provided functions.
- The platform supports C#, F#, Node.js, Python, java and PowerShell.
- Pay only for the time spent running your code with Consumption plan.
- The runtime code is open-source and available on GitHub under an MIT License.

AWS Lambda, Azure Functions, and Google Cloud Functions are the primary Function-as-a-Service (FaaS) offerings from the top three cloud providers. While they share core serverless principles (automatic scaling, pay-per-use, no server management), they differ significantly in ecosystem integration, developer experience, and specific technical features.

Feature	AWS Lambda	Azure Functions	Google Cloud Functions
Primary Strength	Deepest ecosystem integration, mature tooling, performance optimization	Strong enterprise, hybrid cloud, and .NET integration, stateful workflows via Durable Functions	Simplicity, rapid deployment, designed for real-time data processing and mobile backends
Max Execution Time	15 minutes	10 minutes (Consumption Plan), up to unlimited (Premium Plan)	9 minutes (Gen 1), up to 60 minutes (Gen 2 via Cloud Run)
HTTP Endpoints	Requires a separate service (API Gateway or ELB)	Native HTTP triggers built-in	Automatic HTTPS endpoints built-in
Ideal User	Teams already heavily invested in the AWS ecosystem needing maximum control and broad integrations	Microsoft-centric organizations needing strong identity management and hybrid capabilities	Teams prioritizing simplicity, quick deployments, and seamless integration with GCP or Firebase

OpenLambda

- OpenLambda is an open-source serverless computing platform. The source-code is available in GitHub under an Apache License.
- The Lambda model allows developers to specify functions that run in response to various events.
- OpenLambda will consist of a number of subsystems that will coordinate to run Lambda handlers:

Benefits

- Compared to IaaS platforms, serverless architectures offer different tradeoffs in terms of control, cost, and flexibility.
- The serverless paradigm has advantages for both consumers and providers.
- From the consumer perspective, a cloud developer no longer needs to provision and manage servers, VMs, or containers as the basic computational building block for offering distributed services.
- The stateless programming model gives the provider more control over the software stack, allowing them to, among other things, more transparently deliver security patches and optimize the platform.

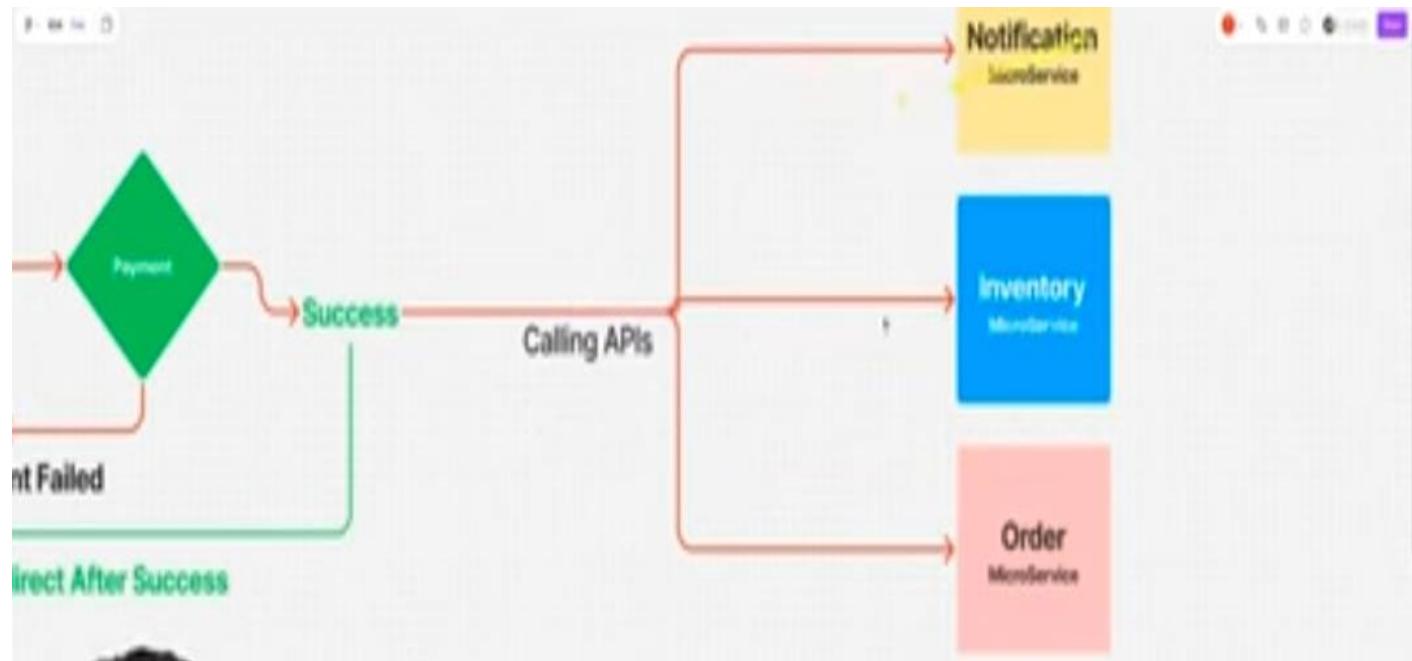
Current state of serverless platforms

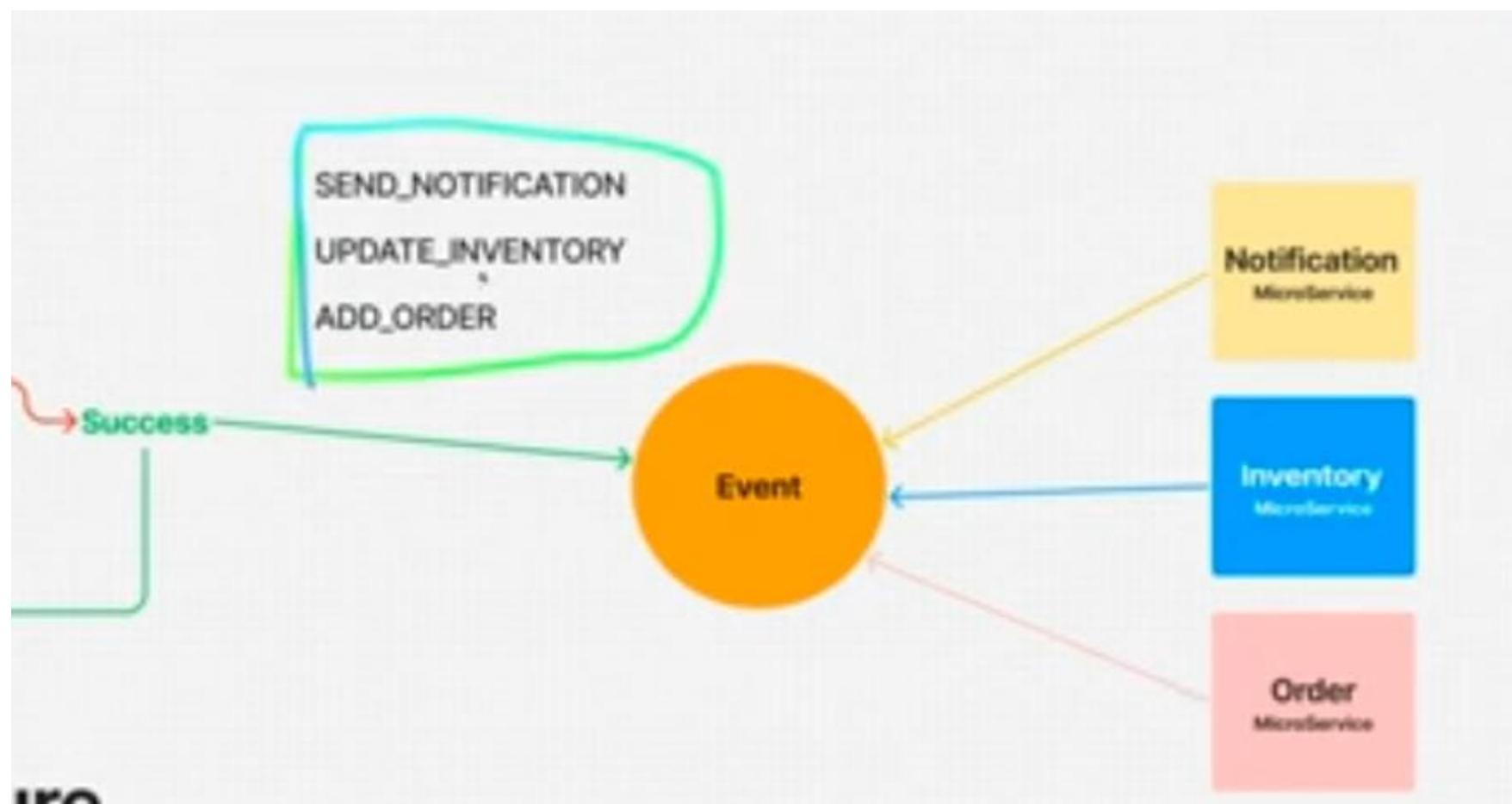
- There are many similarities between serverless platforms.
- They share similar pricing, deployment, and programming models.
- Current serverless platforms only make it easy to use the services in their own ecosystem.
- Open source solutions may work well across multiple cloud platforms.

Event-driven computing

Event-driven computing is a software paradigm where system actions are triggered by events—significant changes in state like user clicks, sensor inputs, or system updates—rather than sequential procedural code. It enables real-time, asynchronous processing, improving responsiveness and scalability, particularly in microservices, GUI applications, and IoT, allowing components to communicate without direct, rigid coupling.







Tightly Coupled (High Dependency)

- **Definition:** Components are deeply dependent on one another; a change in one often requires changes in others.
- **Benefits:** Can offer higher performance, tighter security, and easier, faster communication between modules.
- **Drawbacks:** Difficult to maintain, modify, or scale; changes can cause ripple effects.
- **Example:** A monolith application where the database schema is directly embedded within the user interface code.

Key Differences Summary

- **Interdependence:** High in tight, low in loose.
- **Maintainability:** Easier in loose, harder in tight.
- **Flexibility:** High in loose, low in tight.
- **Scalability:** Better in loose.

Loosely Coupled (Low Dependency)

- **Definition:** Components operate independently, with minimal knowledge of each other's internal workings.
- **Benefits:** High flexibility, easy to test, swap, and reuse components.
- **Use Cases:** Modern microservices, distributed systems, and scalable, maintainable architectures.
- **Example:** A plug-in architecture, where modules can be added or removed without changing the core application.

Disaster

What is it?



Any natural or man-made event that disrupts the operations of a business in such significant way that a considerable and coordinated effort is required to achieve a recovery

(Barnes, 2001)





Not Just Natural Disaster



Power Failures
26%



Software Failures
9%



Hardware Failures
19%



Human Errors
8%



Network Outages
10%



Everything else
30%

Why Downtime Matters



43% of businesses experiencing a disaster never reopen, and almost 30% of those that do close within 2 years

Source : McGladrey and Pullen, LLP – a Consulting Company

93% of businesses that lost their datacenter for 10 days went bankrupt within 1 year

Source : US National Archives and Record Administration

10 Reason why should company consider DR ?



Because you can't afford downtime



Because your customers and prospects expect it



Because you spent a lot in building your brand, and you need to protect it



Because mother nature does not play favorites



Because machine breaks



Because we live in an **always on** world that requires always on capabilities



Because **compliance and regulations** require it



Because you can't predict what data might be lost and the value it had for your company's well being



Because it will **save your money**



Because we're all human

DR Challenges



- Too many moving parts and complexity
- Lack of automation – reliance on manual execution
- Driving without dials – no real time meters to monitor DR service
- DR drills are expensive and impact production





What should I consider?

Costs	Traditional DR	Cloud-based DR
Datacenter for Disaster Recovery (including facilities utility and electrical power source)	Own manage	Cloud Service Provider
Stand-by Hardware System	Own manage	Cloud Service Provider
Manpower – Network Operation	Own manage	Cloud Service Provider
Manpower – System & IT Security Operation	Own manage	Cloud Service Provider
Capacity expansion	Own manage (procurement process + more hardware to manage)	Easily provided through flexibility and agility of Cloud
Expense	1.5 – 2X	1 – 1.2X

Disaster Recovery Considerations

Why Cloud



Traditional DR

- + More control on your server
- + Keeps company data private
- + Data accessible locally

- Increase investment to build H/W and infrastructure
- More spending as company growth
- More space
- Maintenance cost
- Dedicated IT Support
- No uptime guarantees

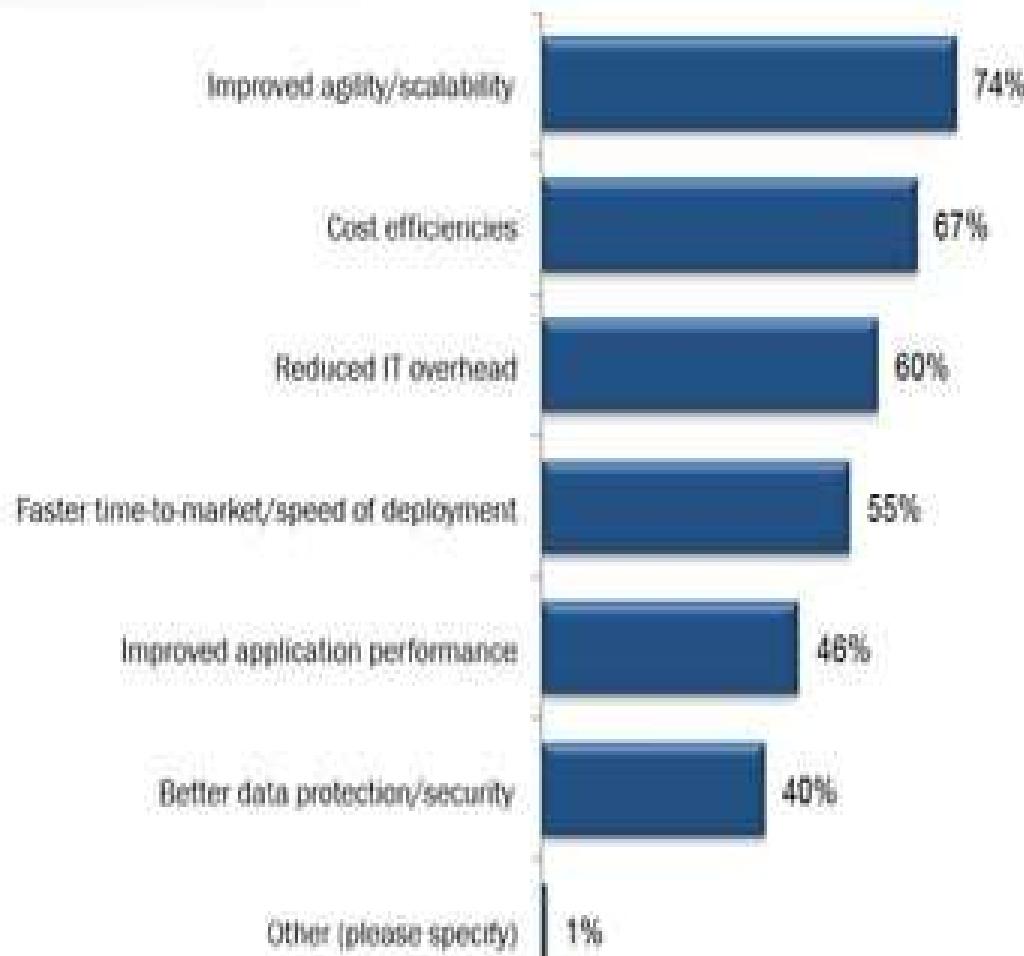
Cloud DR

- + No H/W cost and capital expense
- + Scalable
- + Pay for what you use
- + Easily connect from everywhere, any devices
- + Data can be backup in the cloud regularly and efficiently

- Need internet connection
- Trusting a third party to keep data secure
- Ongoing cost

Disaster Recovery On Cloud

Why cloud ?



Recovery Time and Recovery Point Objective

What is RTO and RPO

Recovery Time Objective

- RTO for an application is the goal for how quickly you need to have that application's information back available after downtime has occurred

Recovery Point Objective

- RPO for an application describes the point in time to which data must be restored to successfully resume processing(often thought of as time between last backup and when a disaster occurred)



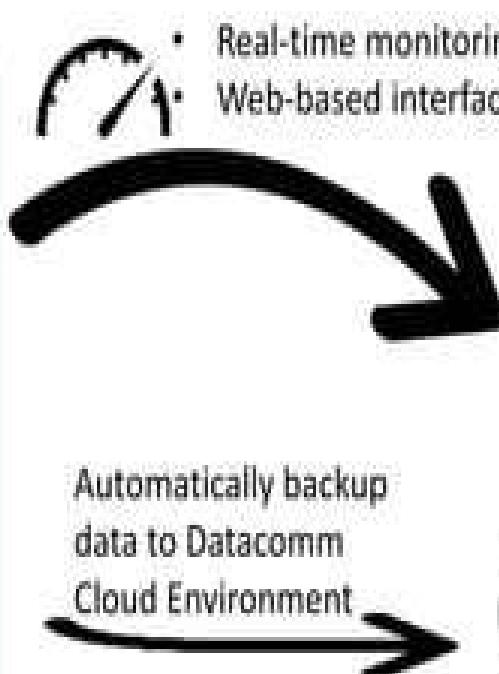
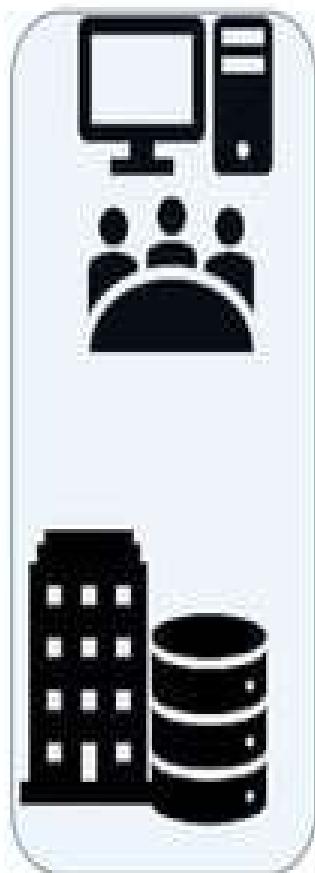
Disaster Recovery On Cloud

Datacomm Disaster Recovery as a Service

	DR Mode	Services Needed	Resources	Failover Scenario	Restore Time	Supported Platform
COLD DR	Backup	BaaS	<ul style="list-style-type: none"> ● Storage ● Compute (unreserved) 	Restore	Up to one day / instance	<ul style="list-style-type: none"> ● Windows ● Linux
WARM DR	Standby (off)	<ul style="list-style-type: none"> ● OS ● IaaS ● BaaS 	<ul style="list-style-type: none"> ● Storage ● Compute 	Boot on VM	4 - 6 hours / instance	<ul style="list-style-type: none"> ● VMware ● Hyper - V
HOT DR	Fully Automated	<ul style="list-style-type: none"> ● OS ● Replication ● IaaS 	Dedicated	Automatically	Less than 10 minutes	<ul style="list-style-type: none"> ● VMware ● Hyper-V

Disaster Recovery On Cloud

Datacomm Disaster Recovery as a Service



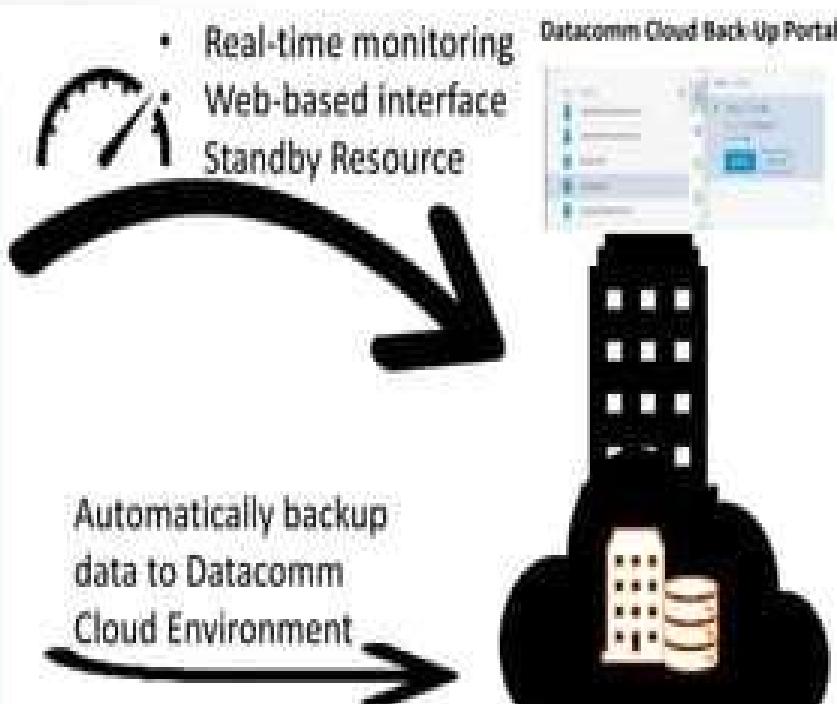
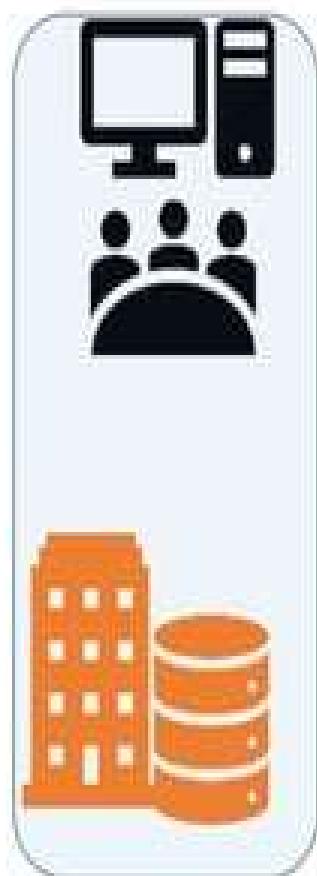
Local Datacenter with Tier III Design, KVM & VMware hypervisors, Multiple OS supported (Microsoft, Linux, Custom OS), 24x7 Support (NOC & SOC),

COLD

- ❖ Based on your capacity expectation
- ❖ Backup to cloud storage
- ❖ Restore as Virtual Machine is an optional
- ❖ Internet-based control portal

Disaster Recovery On Cloud

Datacomm Disaster Recovery as a Service

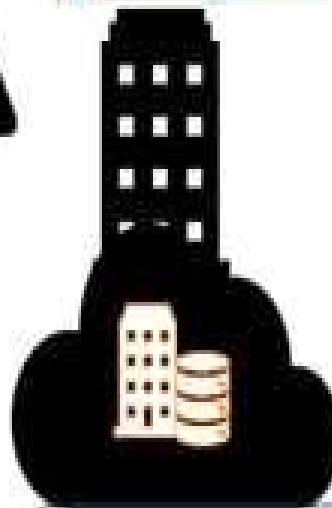


Datacomm Cloud Back-Up Portal



WARM

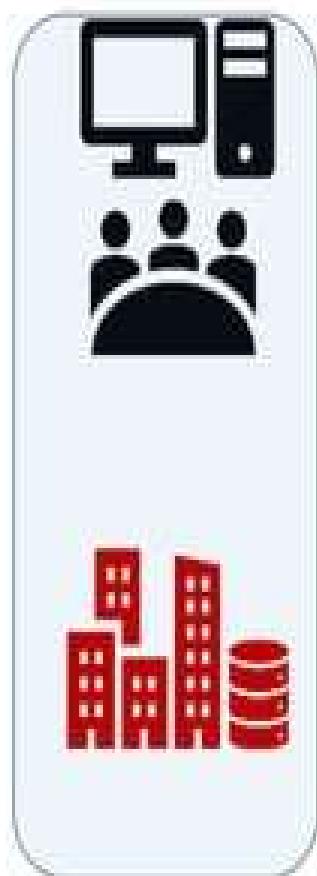
- ❖ Compute resource reservation (standby)
- ❖ Recovery from your own baseline OS template
- ❖ Quick recovery to Datacomm cloud environment



Local Datacenter with Tier III Design, KVM & Vmware hypervisors, Multiple OS supported (Microsoft, Linux, Custom OS), 24x7 Support (NOC & SOC),

Disaster Recovery On Cloud

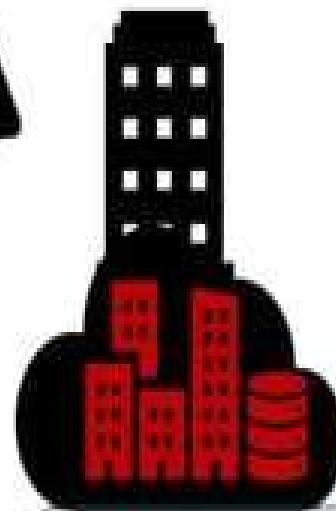
Datacomm Cloud-based Disaster Recovery Solution



- Real-time monitoring
- Web-based interface



Real-time data replication



Local Datacenter with Tier III Design, KVM & Vmware hypervisors, Multiple OS supported (Microsoft, Linux, Custom OS), 24x7 Support (NOC & SOC),

HOT

- ❖ Multi-site datacenter
- ❖ Real-time data replication
- ❖ Up to zero data loss guaranteed
- ❖ Immediately recovery Datacomm cloud environment

Disaster Recovery On Cloud

Key Features

- **High availability** – guaranteed 99.9% SLA data backup availability
- **Physical and virtual systems** – protection of both physical and virtual systems in one service
- **Automatic and scheduled backup** through online control portal
- **Up to zero data loss** guaranteed
- **File and disk image-based backup** - backup of selected files or complete disk images
- **Define your own baseline OS template** for recovery



Disaster Recovery On Cloud

Key features

- **Bare-metal recovery** – recovery to same or dissimilar hardware, even from the cloud
- **Comprehensive** - provides robust replication and offsite backup
- **Local and cloud storage** – support of local and safe cloud storage in our secure and local
- **Recovery reports** document execution of BC/DR processes, for easy auditing and reporting
- ‘**test-before-you-commit**’ function allows test of a specific failover point before committing it, enabling 100% assurance that failover will be successful
- Test failover, including full remote recovery in a **sandboxed zone**



Sandbox for DR Testing



- Non-disruptive DR testing
- Create a test and development environment
- During the test, replication and the production environment is still in process
- Can be done during working days
- No downtime on the production environment

Reporting



Recovery Report for Virtual Protection Group	
Hyper-V (C:\Data\app2)	
Report auto-generated at 10:45 AM on 10/10/2017.	
Recovery Operation Details	
Computer ID	VM-0001 (Windows Server 2012 R2 Standard)
Recovery location	Hyper-V
Read to reuse	Not Enabled (disabled)
Recovery operation start time	2017-10-10 10:45:00
Recovery operation end time	2017-10-10 10:45:00
Size	100 GB
Recovery operation result	Succesful
Run status	Successful (Success/Warning/Failed)
Virtual Protection Group Recovery Settings	
Protected site	My Office
Recovery site	Office Home
Replicate recovery location	Hyper-V (Windows Server 2012 R2 Standard)
Enabled recovery destination	No
Replicate first recovery attempt	Yes
Default recovery location	Hyper-V (Windows Server 2012 R2 Standard)
Default recovery time	00:00:00 (00:00:00 - 00:00:00)

Journal of Business Research (ISSN 0148-296X)
Volume 56, Number 10, October 2003
pp. 1001-1010
© 2003 Elsevier Inc.
0148-296X/\$30.00
doi:10.1016/j.jbusres.2003.07.001
**Published online 20 August 2003 in *ScienceDirect*.
http://www.sciencedirect.com**

—
—
—

Testing Regulations

- PCI
 - ISO
 - SOX
 - HIPAA
 - SEC



THANK
you!



cloud.datacomm.co.id



cloud.datacomm.co.id/blog



facebook.com/Datacomm



linkedin.com/company/datacomm-cloud-business



Privacy and Data Protection

The Concept of Security in Cyberspace

WHAT IS CYBER SECURITY?

Cyber security, also referred to as information technology security, focuses on protecting computers, networks, programs and data from unintended or unauthorized access, change or destruction.



WHY IS CYBER SECURITY IMPORTANT?

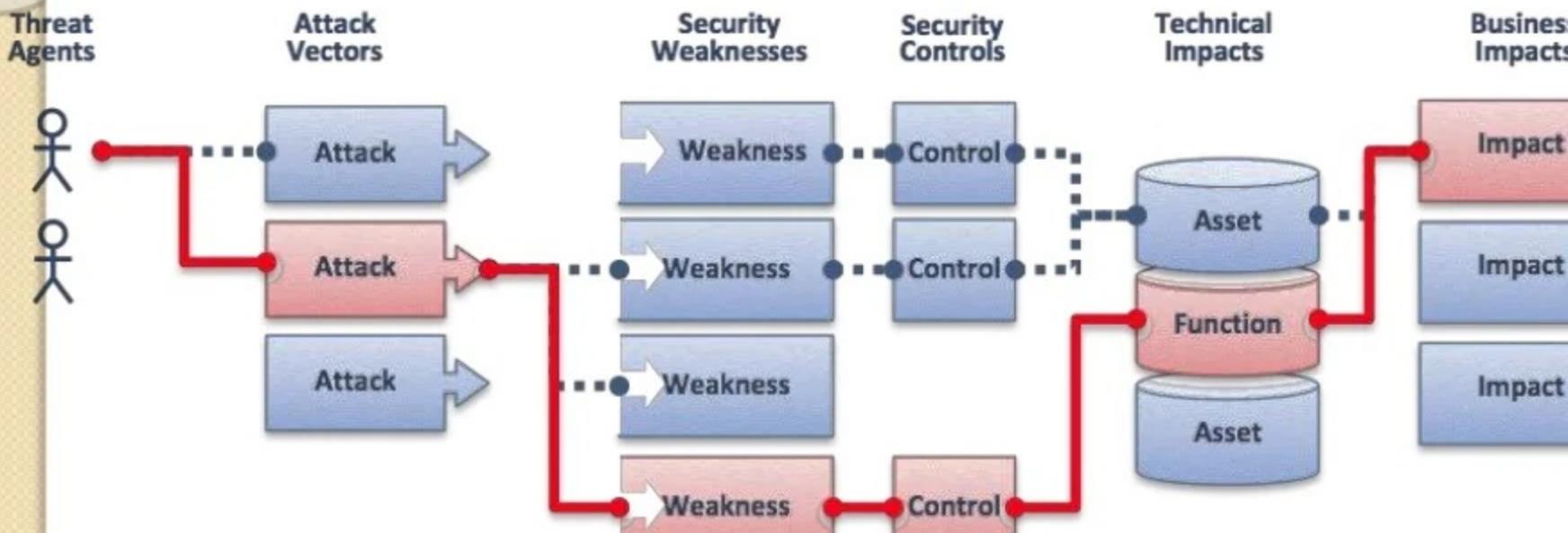
Governments, military, corporations, financial institutions, hospitals and other businesses collect, process and store a great deal of confidential information on computers and transmit that data across networks to other computers. With the growing volume and sophistication of cyber attacks, ongoing attention is required to protect sensitive business and personal information, as well as safeguard national security.

During a Senate hearing in March 2013, the nation's top intelligence officials warned that cyber attacks and

Technological Vulnerability

- In computer security, a **vulnerability** is a weakness which allows an attacker to reduce a system's information assurance.
- Vulnerability is the intersection of three elements: a system susceptibility or flaw, attacker access to the flaw, and attacker capability to exploit the flaw.
- To exploit a vulnerability, an attacker must have at least one applicable tool or technique that can connect to a system weakness. In this frame

Vulnerability and risk factor models



Information Security Audit

Vulnerability Assessment and Penetration Testing Services (VAPT)

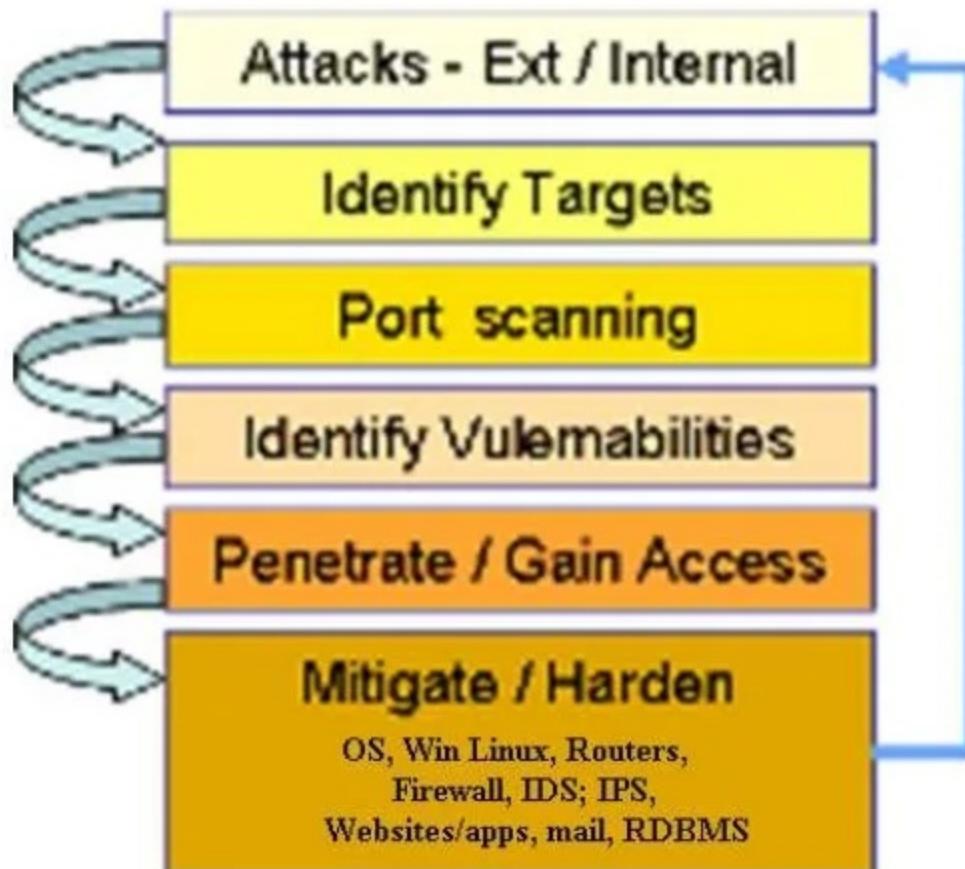
- **Vulnerability Assessments** are a process of identifying, quantifying, and prioritizing vulnerabilities in a system. A vulnerability refers to the inability of the system to withstand the effects of a hostile environment.
- **Penetration Tests** are a method of evaluating computer and network security simulating attacks on a computer system or network from external and internal



NEED OF VAPT

- VAPT is a process in which the Information & Communication Technologies (ICT) infrastructure consists of computers, networks, servers, operating systems and application software are scanned in order to identify the presence of known and unknown vulnerabilities.
- As many as 70% of web sites have vulnerabilities that could lead to the theft of sensitive corporate data such as credit card information, product IP,

Vulnerability Assessment and Penetration Testing



Data Protection Position in India

- **Data protection law in India (Present status):-**

Data Protection law in India is included in the Act under specific provisions. Both civil and criminal liabilities are imposed for violation of data protection.

(1) Section 43 deals with penalties for damage to computer, computer system etc.

(2) Section 65 deals with tampering with computer source documents.

(3) Section 66 deals with hacking with computer system.



BPOs AND THE LEGAL REGIME IN INDIA:

- Business Process Outsourcing (“BPO”) has emerged as the most challenging sector that has not only generated employment potential in India, but has also brought huge inflow of foreign exchange into the country. Today, India is home to some of the world’s leading BPO companies.
- In this context, it is becoming increasingly important to study and examine the legal regime in India pertaining to BPOs and to undertake an

- A BPO takes within its fold various elements such as finance and accounting, customer relationship management, human resources, business process, transcription, and so on. A parent company instead of performing these operations delegates them to a BPO.
- It may be an in house operation or a different company may be engaged to perform a particular task. It may be in the same country or in a different country.
- The BPO sector in India has an extremely advantageous position because of its low cost structure and large pool of skilled manpower.

Child's Privacy Online

- As a parent, you have control over the personal information companies collect online from your kids under 13.
- The Children's Online Privacy Protection Act gives you tools to do that.
- The Federal Trade Commission, the nation's consumer protection agency, enforces the COPPA Rule. If a site or service is covered by COPPA, it has to get your consent before collecting personal information and it has to honor your choices about how that information is used.



What is COPPA?

- The COPPA Rule was put in place to protect kids' personal information on websites and online services — including apps — that are directed to children under 13. The Rule also applies to a general audience site that knows it's collecting personal information from kids that age.
- COPPA requires those sites and services to notify parents directly and get their approval before they collect, use, or disclose a child's personal information. Personal information in the world of COPPA includes a



EVOLVING TRENDS IN DATA PROTECTION AND INFORMATION SECURITY:

- The legal systems which deal with them, have been forced to evolve rapidly. Though the changes in law have had to deal with a number of issues in the broad area of cyber laws, the most vibrant of those have been concerned with privacy, information security, information warfare, egovernance, e-commerce and crimes on the Internet.



Information System Security

Threat, Vulnerabilities and attack



Cyber security threat

A cyber security threat is any potential action or event that could harm digital system , steal data or disrupt operation .

Threat Categorization

➤ Deliberate Threat

- Traffic overload
- Network Failure
- Malicious Software
- Illegal use of Software
- Theft
- Infiltration

Environment

- Earthquakes
- Floods
- Lightning
- Storm
- Tornadoes
- Deterioration

Accidental

- Service Failure
- Hardware Failure
- Human Error
- Design Failure
- Misroute Message
- Transmission Error

Threats to Info. Security

Threat Category	Examples
<i>Acts of human error or failure</i>	<i>Accidents, employee mistakes</i>
Intellectual property compromise	Piracy, copyright infringement
Deliberate espionage or trespass	Unauthorized access, data collection
Deliberate information extortion	Blackmail of info. disclosure
Deliberate sabotage or vandalism	Destruction of systems or info.
Deliberate theft	Illegally taking equipment or info.
<i>Deliberate software attacks</i>	<i>Viruses, worms, denial of service</i>
Forces of nature	Fires, floods, earthquakes
Deviations in service from providers	Power and Internet provider issues
Technological hardware failures	Equipment failure
Technological software failures	Bugs, code problems, unknown loopholes
Technological obsolescence	Antiquated or outdated technologies



Vulnerability



A **vulnerability** is a weakness in the security system

1. Physical Vulnerability
2. Natural Vulnerability
3. Hardware and Software Vulnerability
4. Media Vulnerability
5. Human vulnerability



Vulnerability

A vulnerability scanner software

1. NESSUS
 2. BurpSuite
 3. Qualys
 4. Zenmap
 5. Acunetix Vulnerability Scanner
 6. Netsparker
 7. Intruder
-



Attacks (1)

- Act or action that exploits vulnerability (i.e., an identified weakness) in controlled system
- Accomplished by threat agent which damages or steals organization's information

Attacks (2)

- **Malicious code:** launching viruses, worms, Trojan horses, and active Web scripts aiming to steal or destroy info.
- **Backdoor:** accessing system or network using known or previously unknown mechanism
- **Password crack:** attempting to reverse calculate a password
- **Brute force:** trying every possible combination of options of a password
- **Dictionary:** selects specific accounts to attack and uses commonly used passwords (i.e., the dictionary) to guide guesses

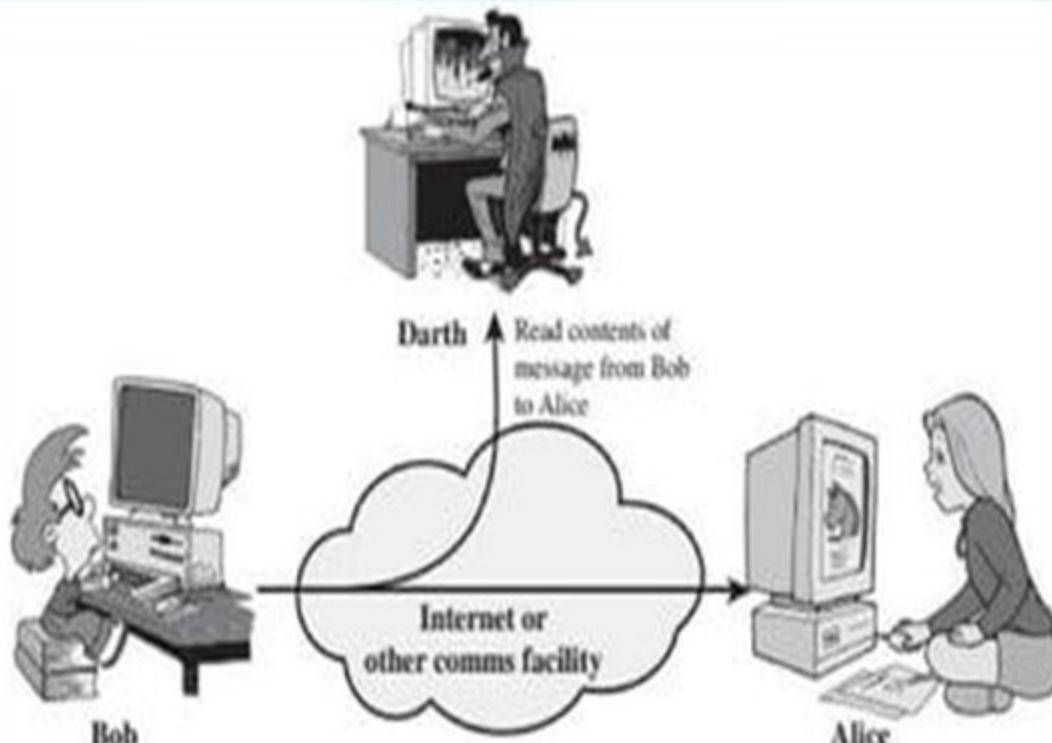
Security Attacks Categories

1. Passive Attacks
2. Active Attacks

A **passive attack** attempts to learn or make use of information from the system but does not affect system resources.

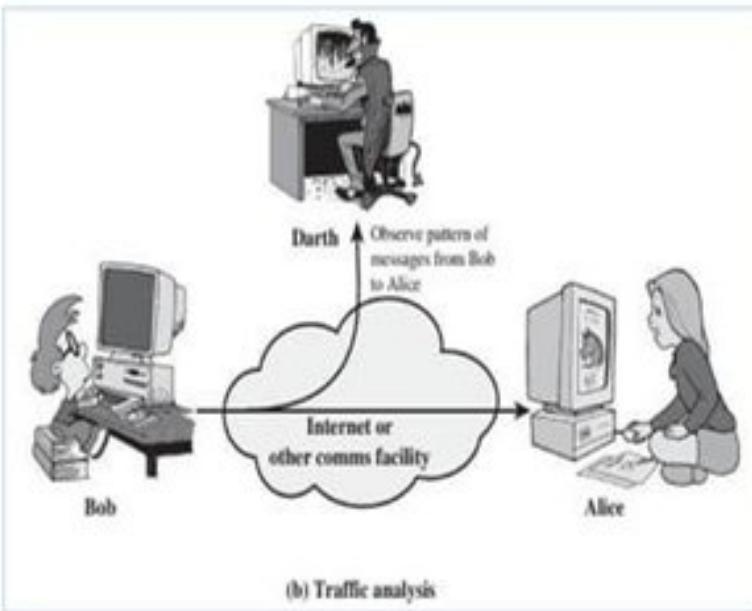
An **active attack** attempts to alter system resources or affect their operation.

Passive Attack #1



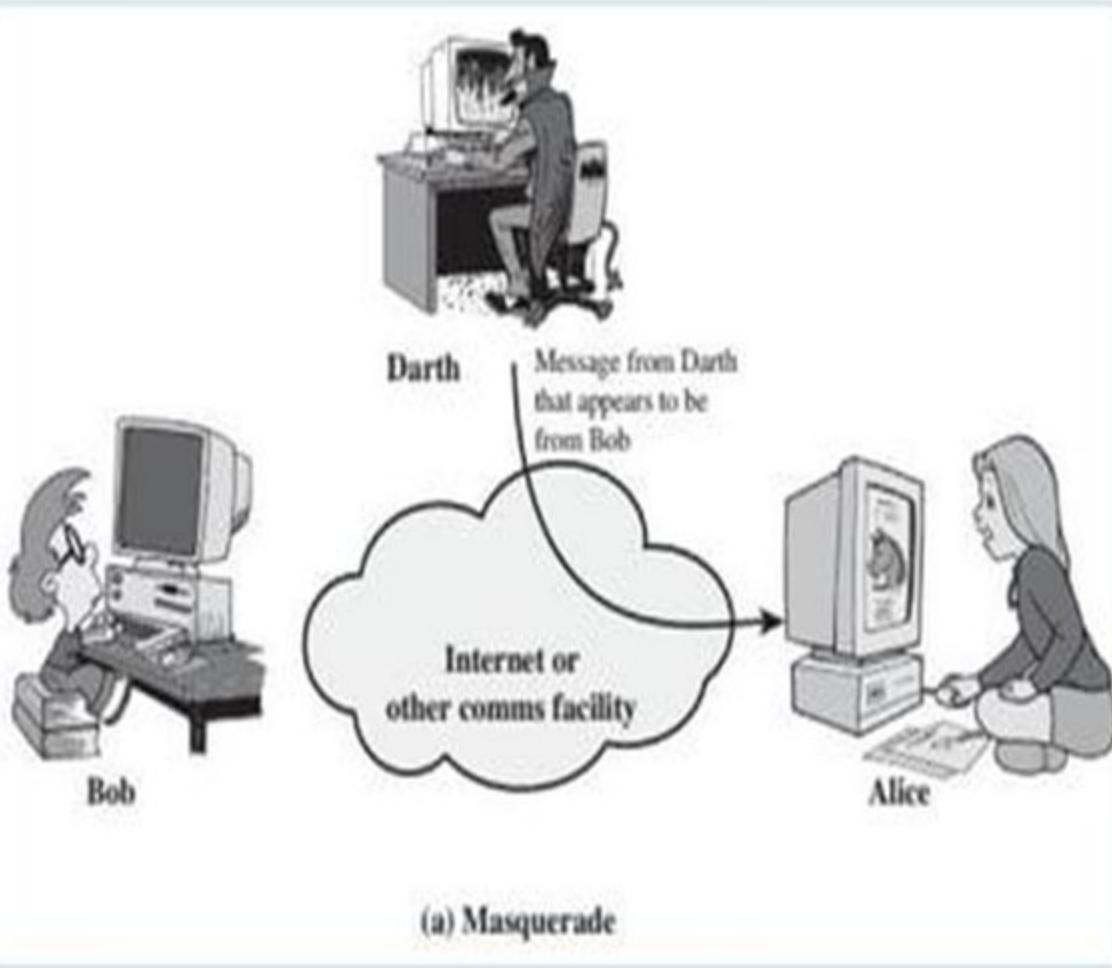
(a) Release of message contents

Passive Attack #2

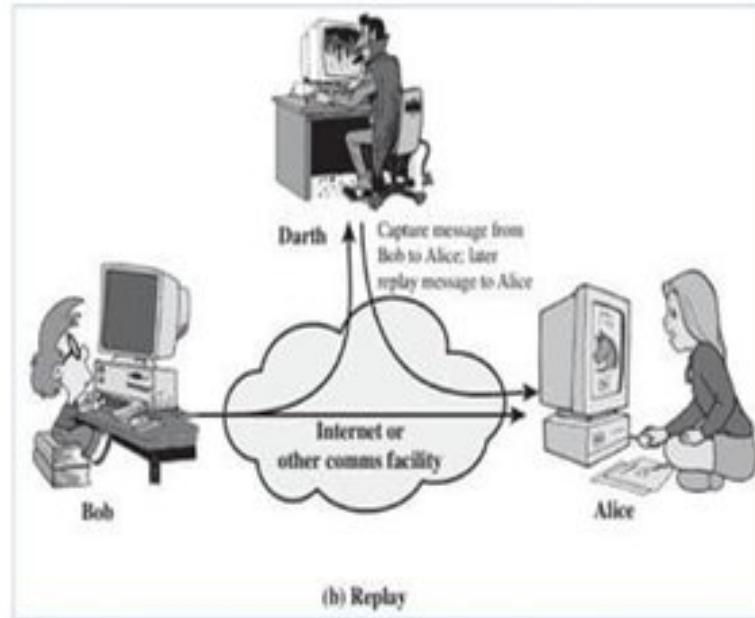


Passive attacks are very difficult to detect, because they do not involve any alteration of the data

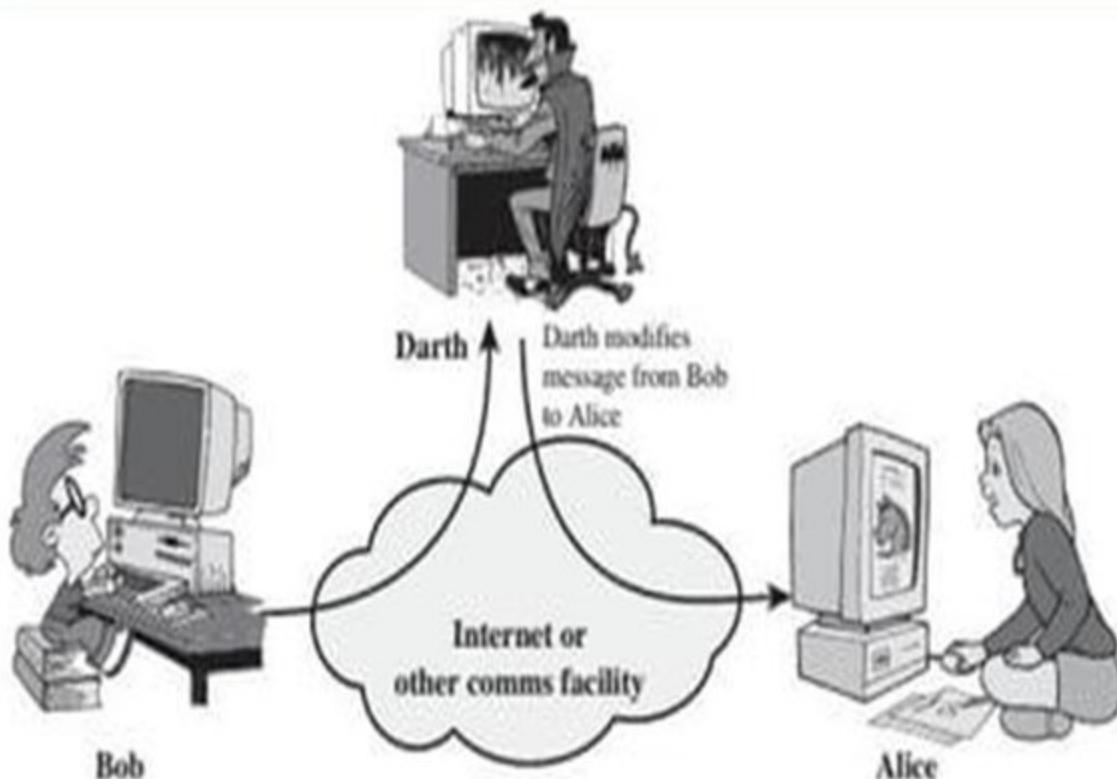
Active Attack #1



Active Attack #2

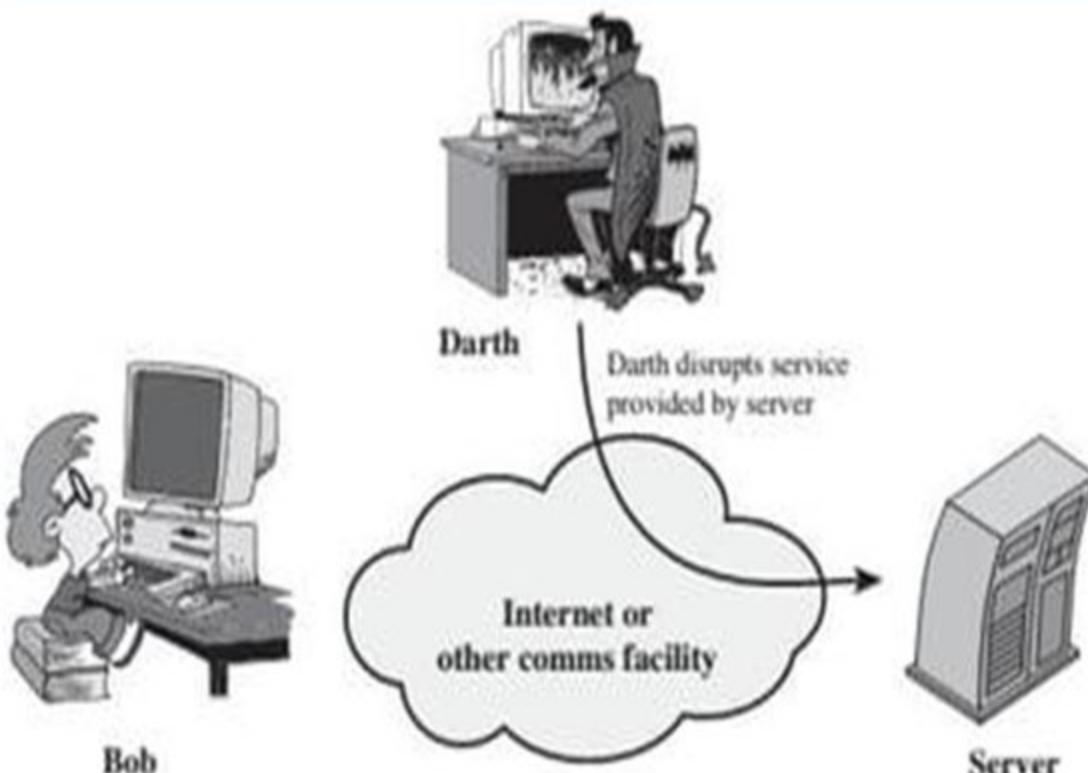


Active Attack #3



(c) Modification of messages

Active Attack #4



(d) Denial of service

3 “Biggest” Common Attack

VIRUS

TROJAN
HORSE

WORM

3 “Biggest” Common Attack

- ✓ The primary vulnerabilities for end-user computers are virus, worm, and Trojan Horse attacks:
- ✓ A virus is malicious software which attaches to another program to execute a specific unwanted function on a computer.
- ✓ A worm executes arbitrary code and installs copies of itself in the memory of the infected computer, which then infects other hosts.
- ✓ A Trojan Horse is an application written to look like something else. When a Trojan Horse is downloaded and opened, it attacks the end-user computer from within.



Disaster Recovery in the Cloud

What You Will Learn

- 1** The Need for Disaster Recovery
- 2** Public, Private and Hybrid Cloud
- 3** DR and the Cloud
- 4** Products from Novell



The Need for Disaster Recovery

Why Downtime Matters

\$41.3 Billion

Total economic damage from disaster in 2009*

\$10.8 Billion

Economic impact felt in the US from disasters in 2009*

**September 2, 2010 , Business Continuity and Disaster Recovery are top IT Priorities for 2010 and 2011 - Forrester*

Better Understanding of Protection

78% of enterprises have indicated that improving disaster recovery capabilities is a high priority*

Critical Priority 30% - High Priority 48%

- Better able to identify and quantify risk
- Better understanding of economic impact
- Less tolerance for downtime and data loss

*Jan. 25, 2010 – *The State of Enterprise IT: 2009 to 2010* - Forrester

Define Your Objectives

Recovery Time Objective (RTO)

- Time between declaration and service availability
- Time to restore services to useable state

Recovery Point Objective (RPO)

- Data in system lost at disaster time
- Amount of data entered since last backup

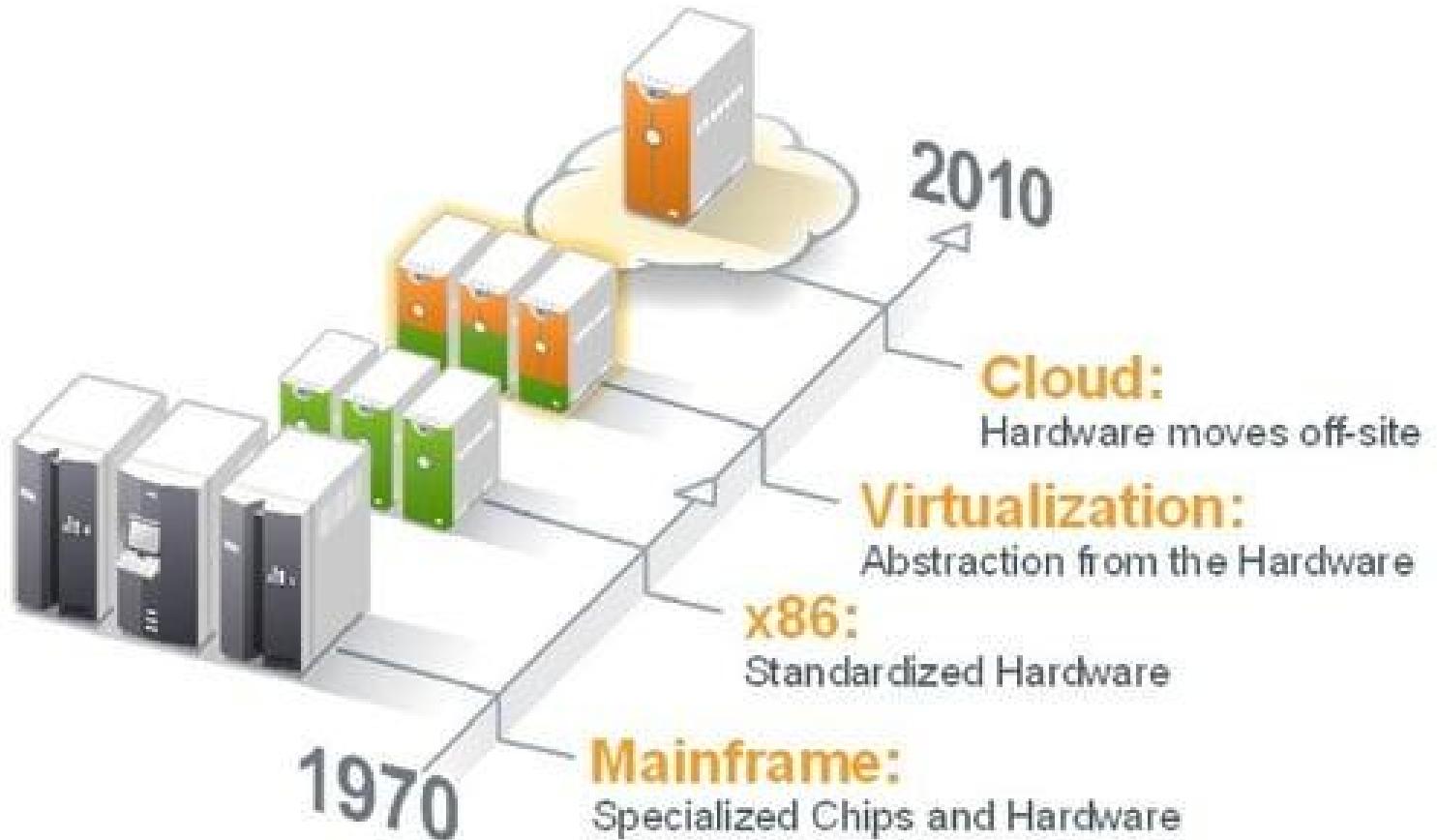
Test Time Objective (TTO)

- Time required to test recovery plans
- Resources used for testing



The Move to the Cloud

From a Big Box to a Big Cloud



Defining Cloud Characteristics

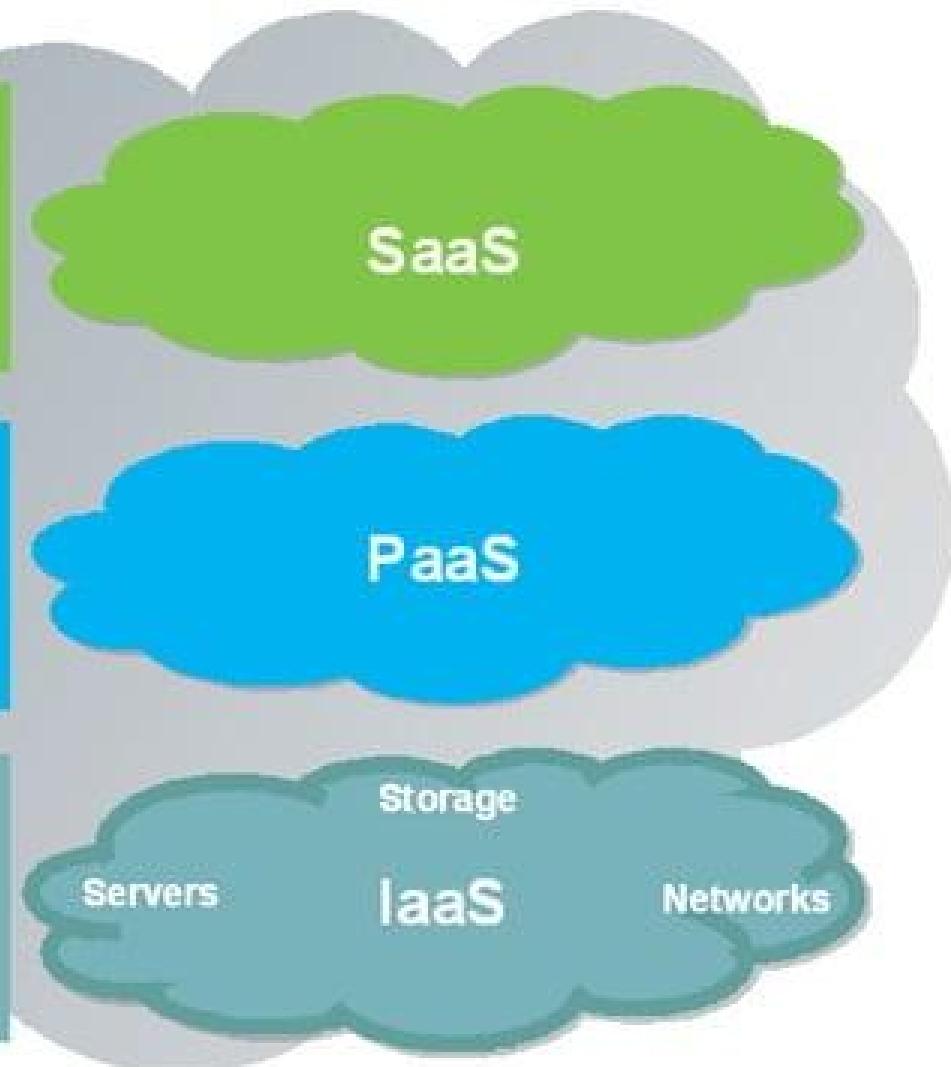


The Cloud Stack

Google Apps, Salesforce.com, online retail, web conferencing, online tax preparation and imaging/printing services

Microsoft Azure, Force.com, Google App Engine, AWS AMI (App runtime environment offered as a service)

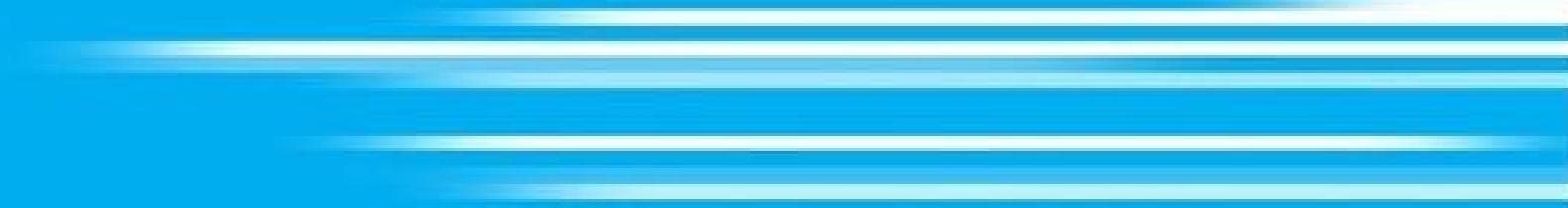
EC2, Rackspace Cloud, Google, Bluelock vCloud, Terremark, BT, AT&T, Verizon, GoGrid, Joyent, SunGard



Your cloud, my cloud

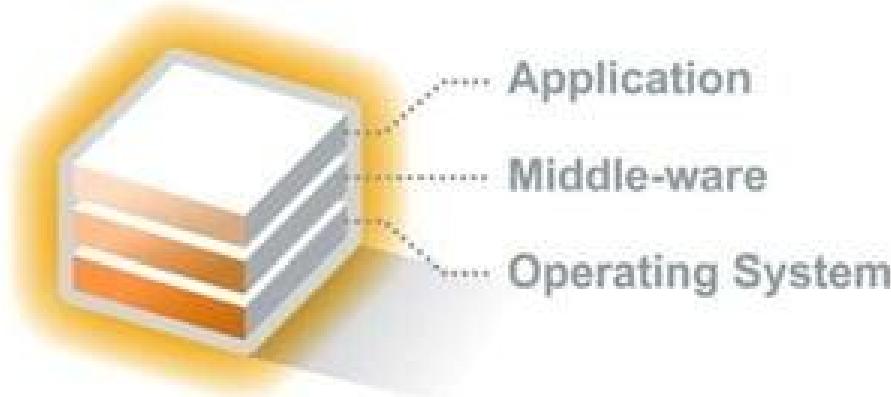
- Public
 - ✓ Scalable and elastic computing services offered to external customers via the Internet.
 - ✓ Typically multi-tenant, where multiple customers are able to share a single set of resources.
- Private
 - ✓ Dynamic and scalable computer services offered to internal customers using equipment the customer owns and delivered over a private network.

DR and the Cloud



What is a Workload?

Workload



A workload is an integrated stack of application, middleware, and operating system that accomplishes a computing task

A workload is portable and platform agnostic—it can run in physical, virtual or cloud computing environments

A workload or a collection of workloads makes up a business service, which is what the end user consumes

Update your DR with Virtualization



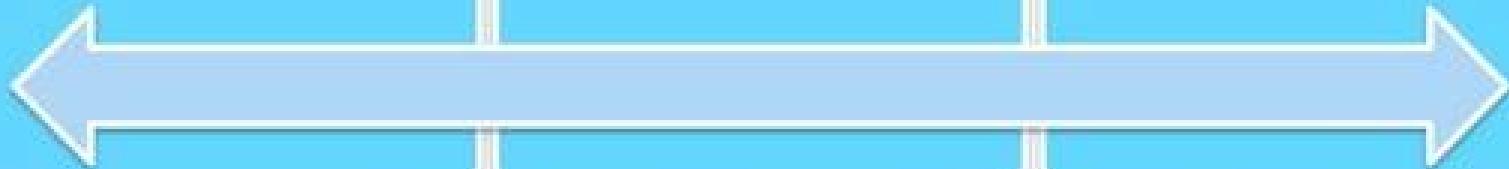
One virtual
server host can
protect several
servers in
production



Eliminate the
Multi-Platform
problem

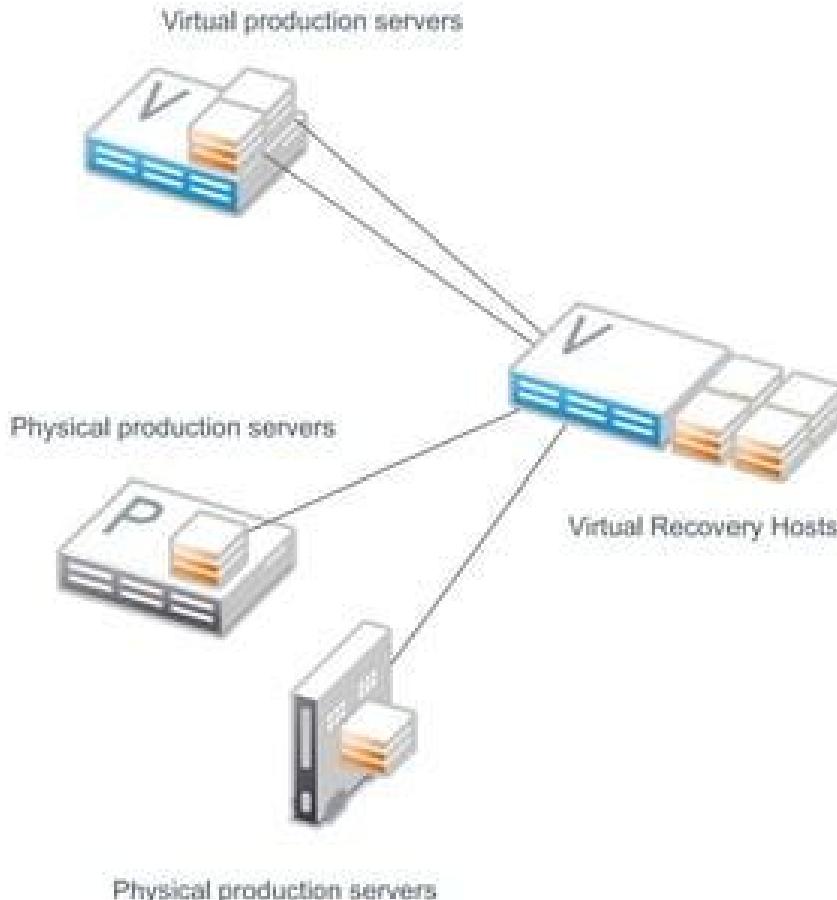


Simplify testing
as Virtual
Machines can
be isolated



Consolidated Recovery

Leveraging Virtual Infrastructure For Protection of All Your Servers



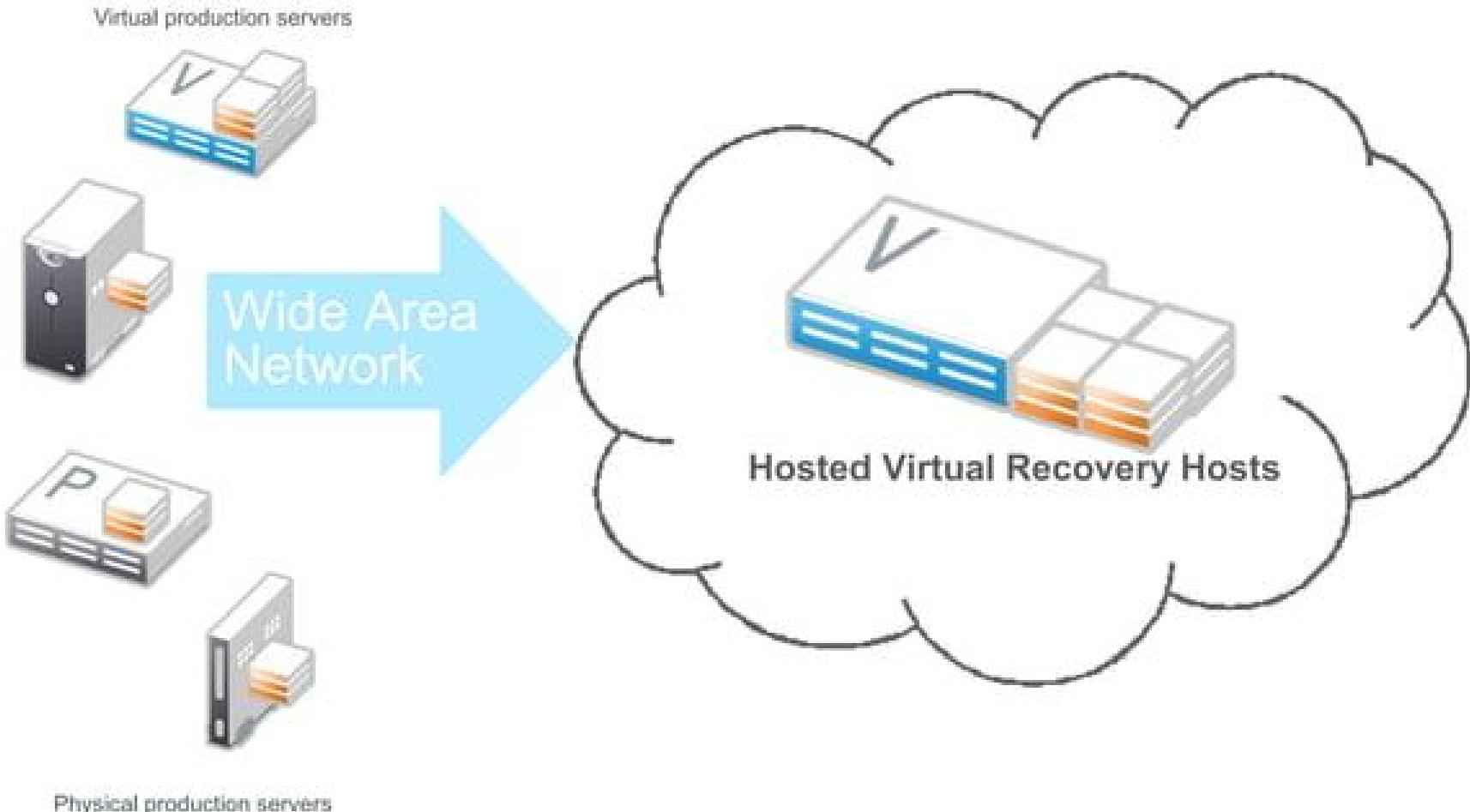
Solution

- Replicate workload into an off-line virtual machine
- One click failover
- One click test restore
- Flexible fallback

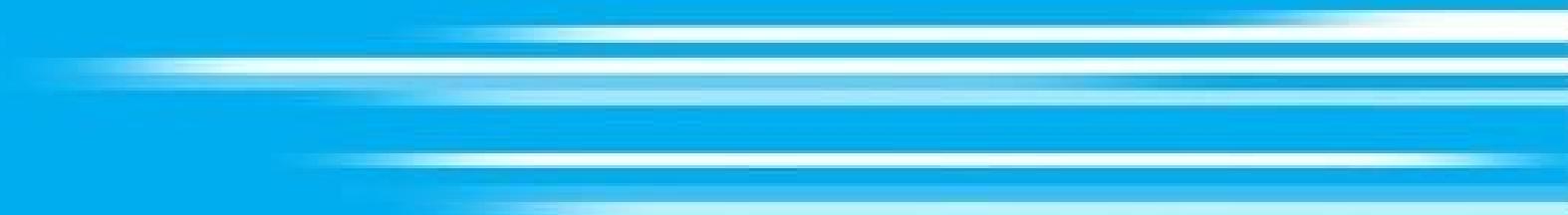
Benefits

- Drastically reduce TCO and achieve whole workload protection
- Simplify testing with bootable backups
- Finally a way to complete your DR architecture

Protect to the Cloud



Products from Novell



PlateSpin Protect

Whole-workload protection for all server workloads.



Backup to
virtual machines

Incremental
replication

Easy to test

One-click
failover

PlateSpin. Forge



World's first disaster recovery hardware appliance with embedded virtualization

Protects up to 25 workloads

Plug In and Protect Solution for :

- Medium enterprises
- Branch or field use for large enterprises
- Hosted recovery

PlateSpin Forge Includes:

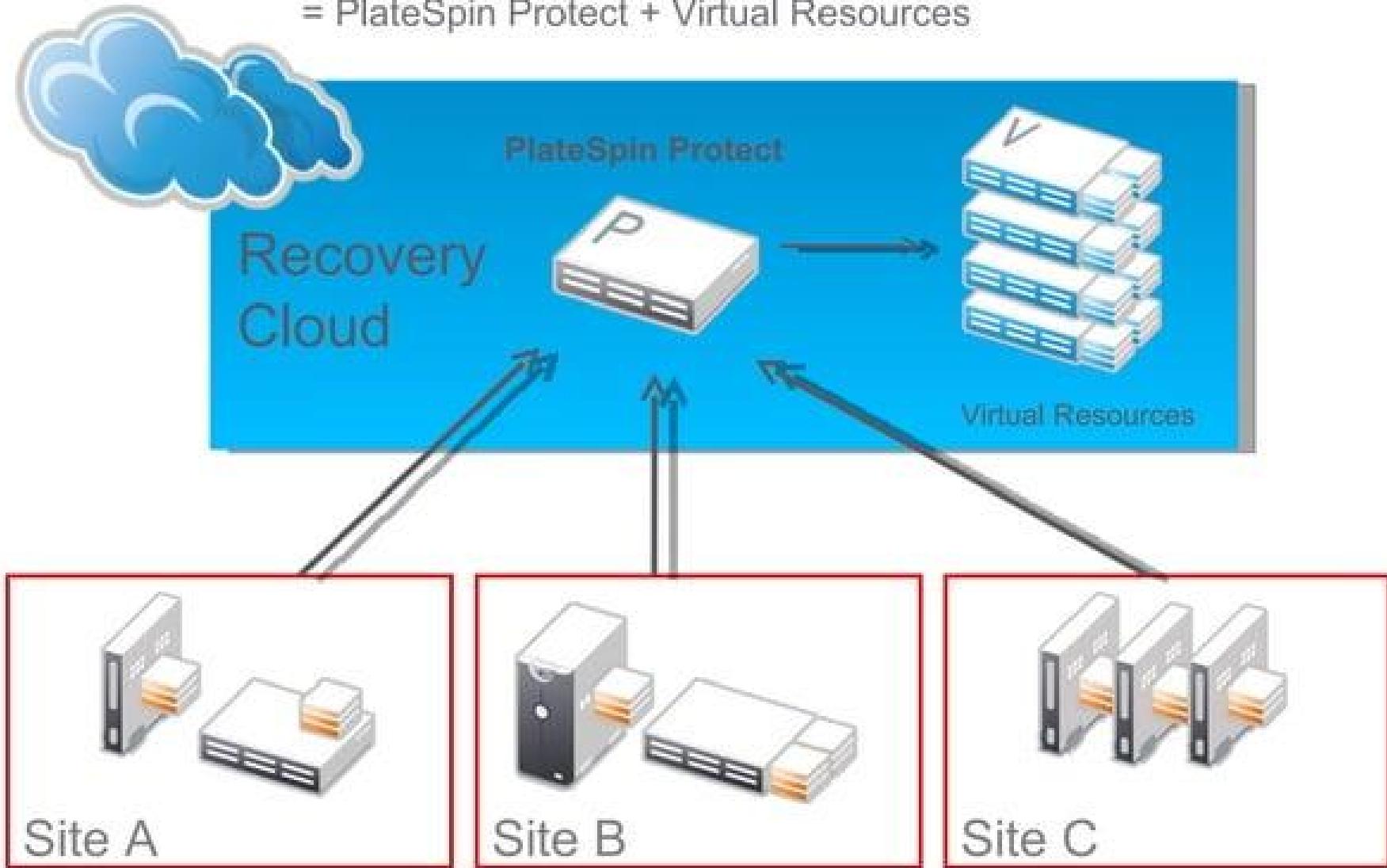
- Storage
- Replication software
- Hypervisor

Build a Protection Cloud



Build a Recovery Cloud

= PlateSpin Protect + Virtual Resources



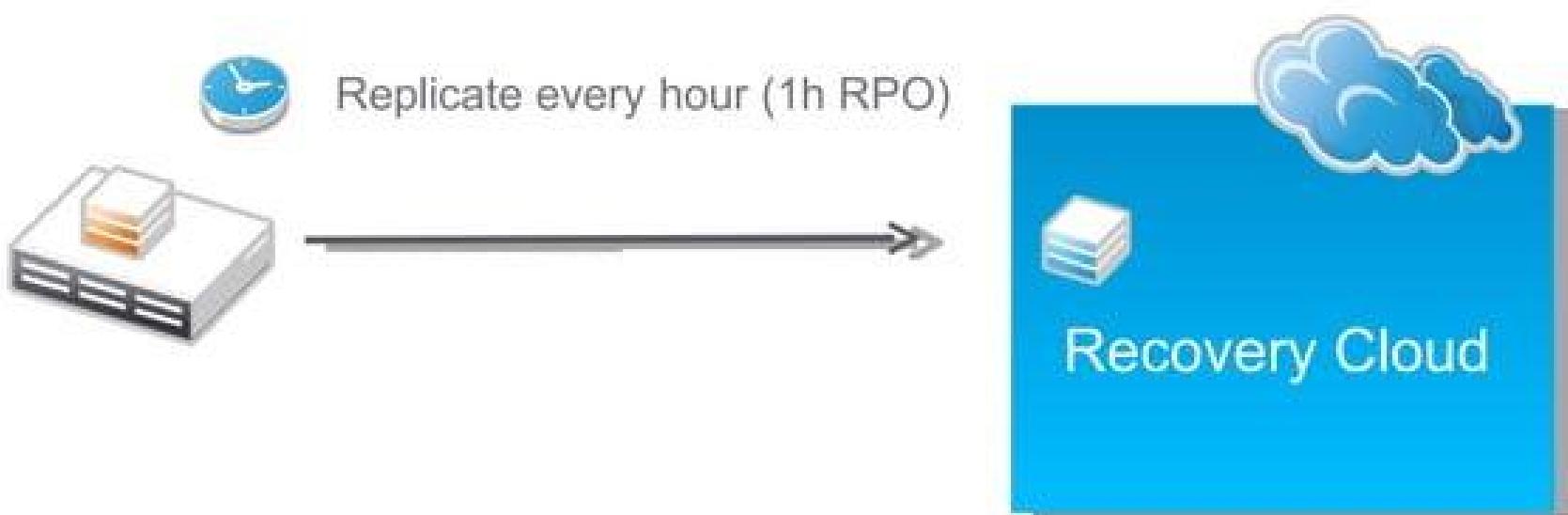
Site A

Site B

Site C

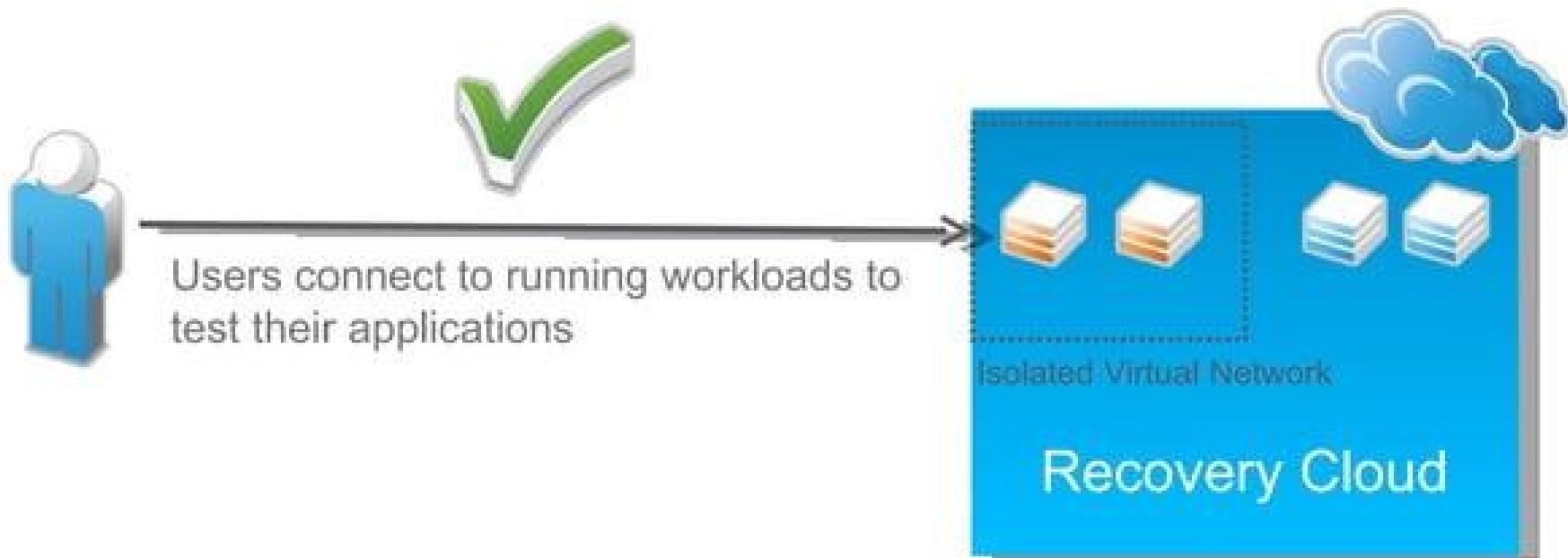
Setup Workload Replications

Scheduled replications: Workload changes are automatically replicated into virtual machines inside the Recovery Cloud



Easy Test Failover

Test Failover: recover workloads in isolated virtual networks to avoid production disruptions



Recover Workloads In Minutes



Offline Detection: PlateSpin Protect sends out notification when the protected workload goes offline

Failover: Workloads are recovered in minutes inside the Recovery Cloud

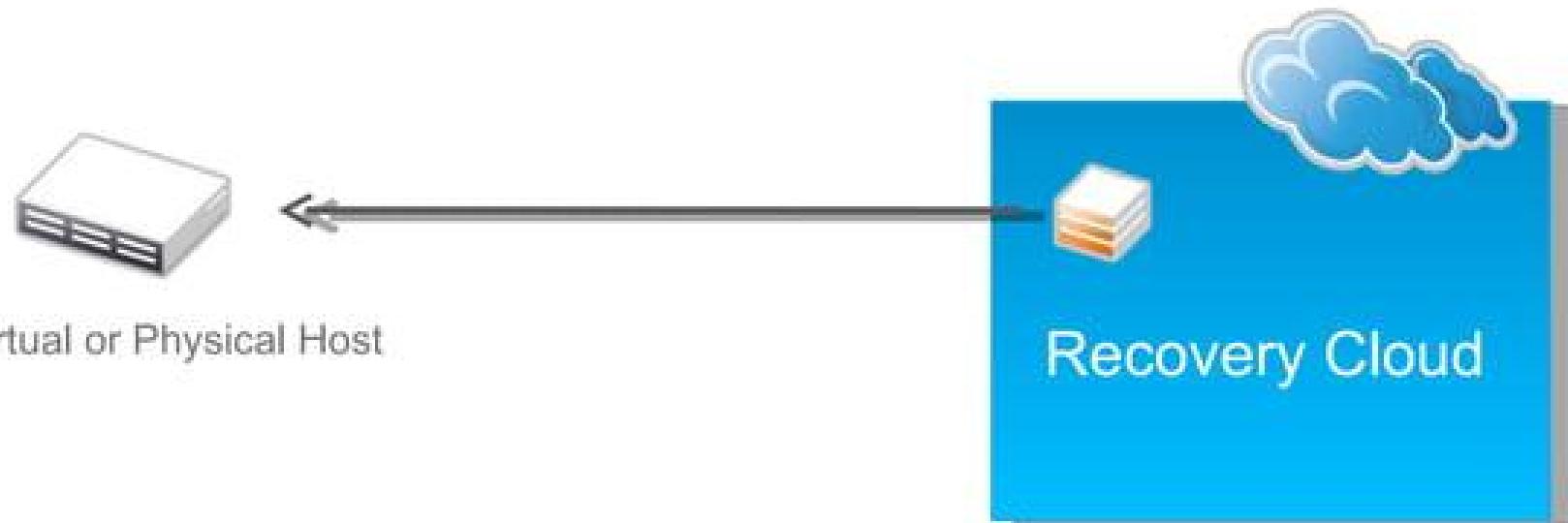


Users connect to workloads running in the Recovery Cloud

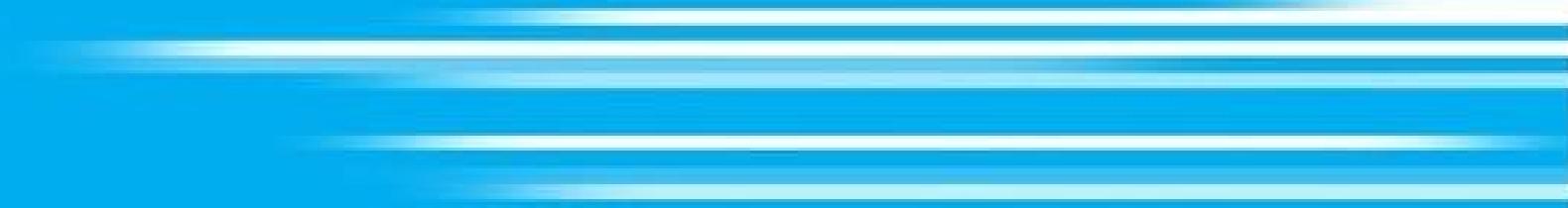


Restore the Production Environment

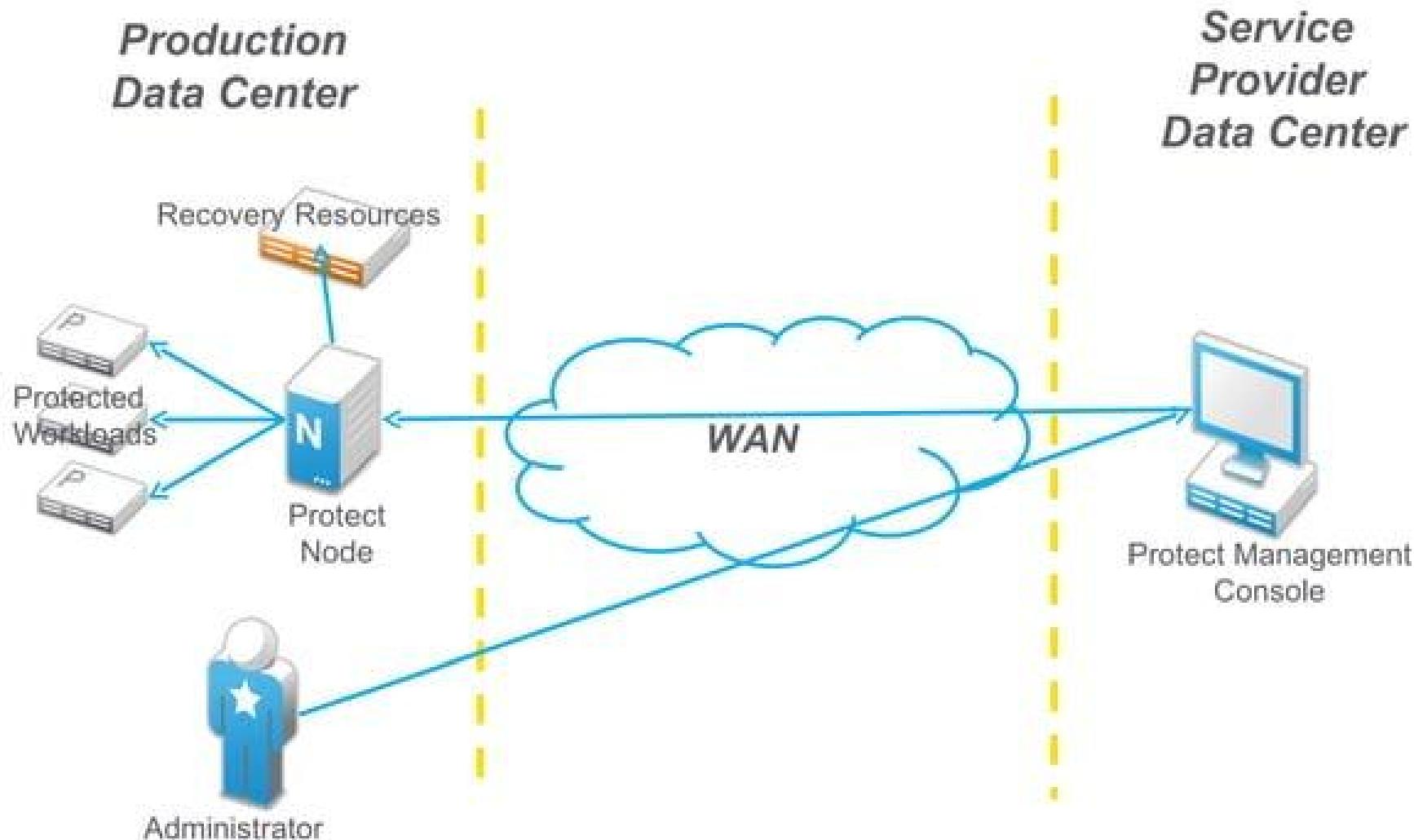
Fallback: move the workload back into production to the same or a different host



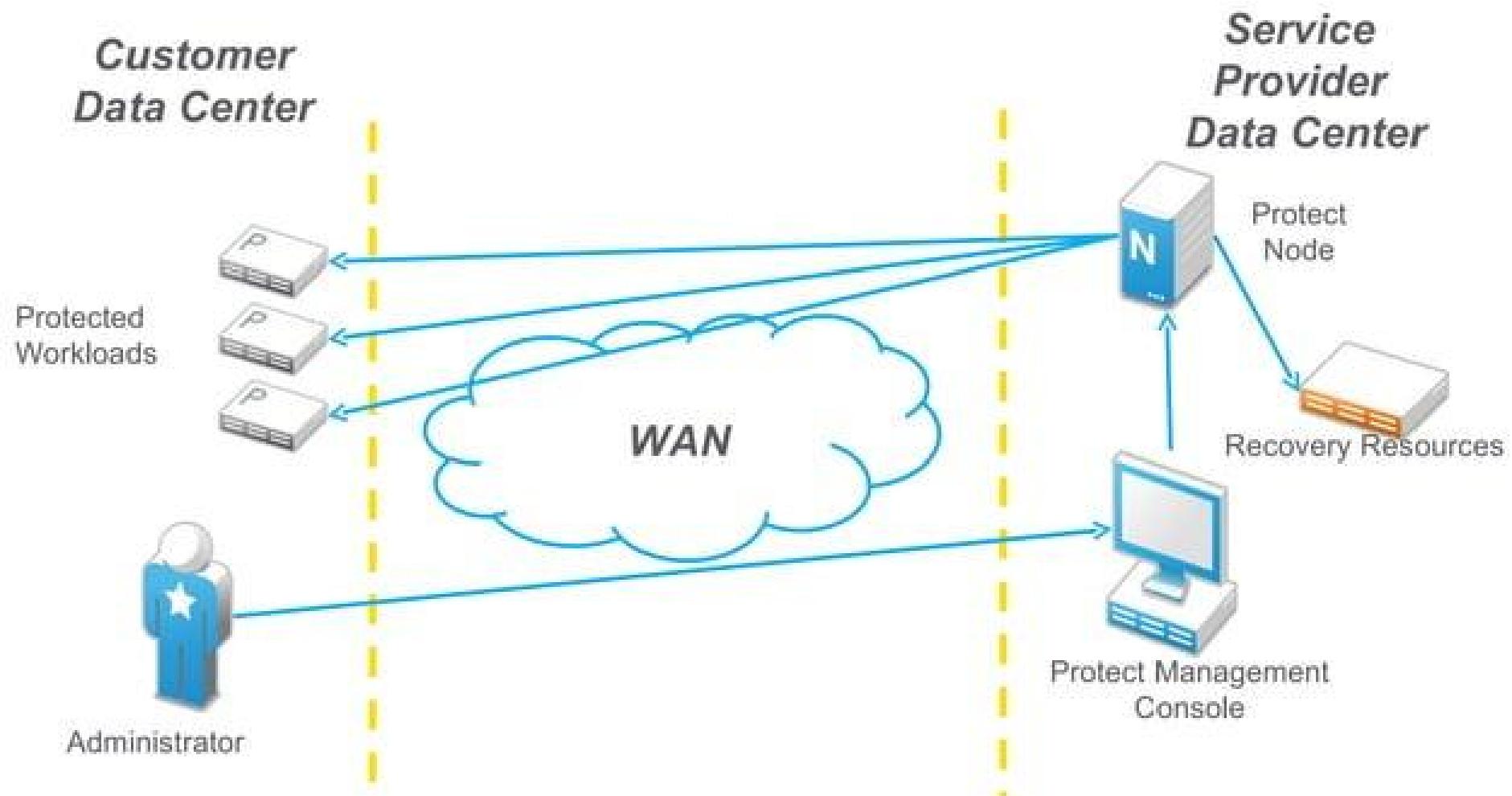
Solution Flexibility



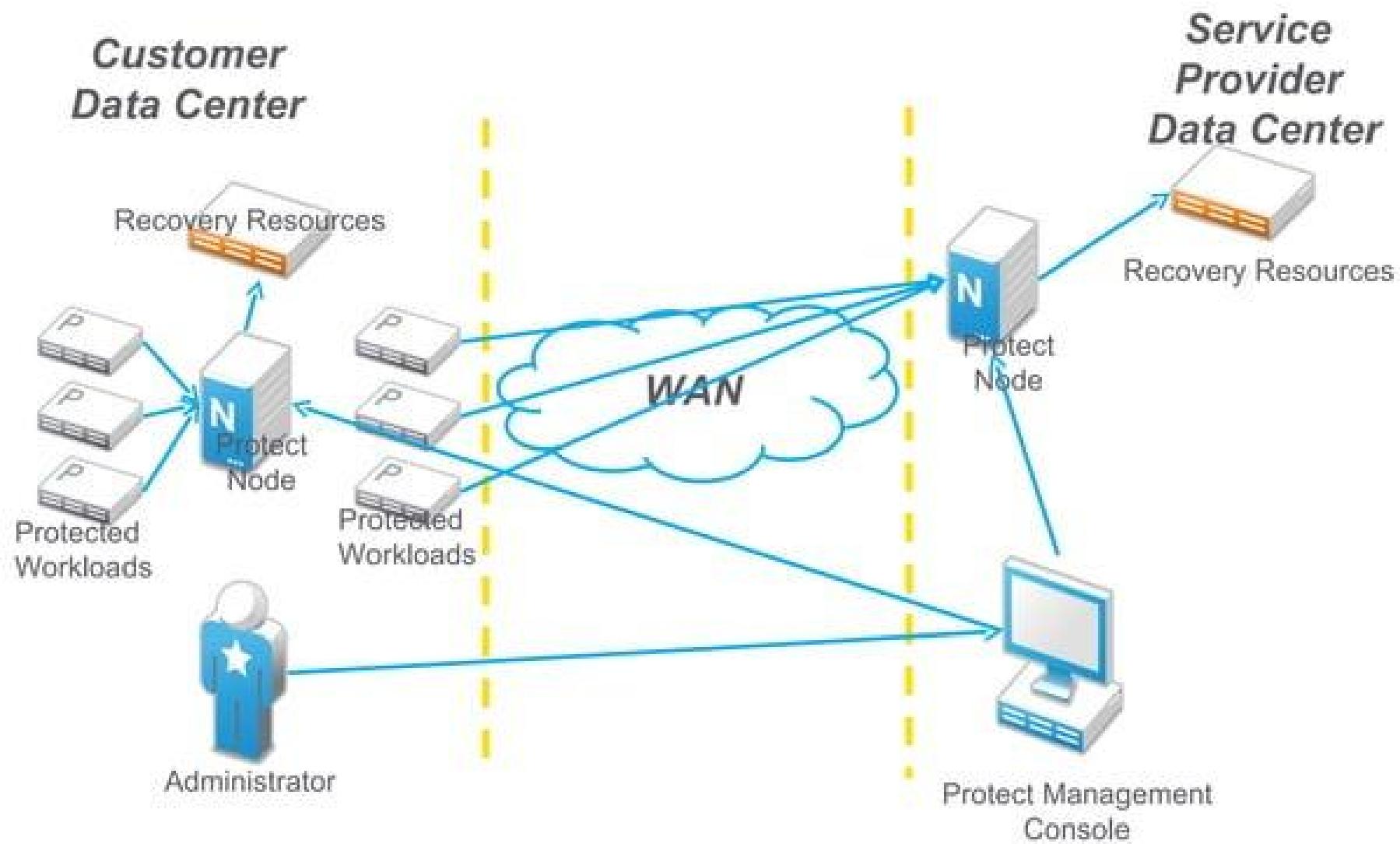
On-Premise



Virtual Private Cloud



Hybrid Model



What do Customers Have to Say?

Customer Results



Nichols College

www.novell.com/success/nichols_college.html

"Disaster recovery solutions can be very complex ... PlateSpin Forge is very straightforward. There's just one piece of hardware to manage. It's low maintenance, and has low overhead. Without it, we certainly would have spent more money on another disaster recovery solution that would have required more resources to support it."

ReedSmith

Reed Smith LLP

http://www.novell.com/success/reed_smith.html

"With PlateSpin Protect, we can recover multiple sites with the same set of hardware quite easily, in a matter of minutes."



Connect

Next Steps

Give it a Try!

- Download a 30 day trial copy of PlateSpin Protect

download.novell.com/index.jsp

Learn More

- Contact Us – 800.529.3400
- Visit
 - www.novell.com/products/forge/
 - www.novell.com/products/protect/



Social Networks Privacy and security

SOCIAL MEDIA BENEFITS AND RISKS



Agenda

- What is Social Media?
- Social Media's Professional Side
- Benefits of Social Media
- Regulatory Risks and Concerns
- Social Media Risks and Concerns
- Reputational and Financial Risks
- Information Security Risks
- Legal Risks
- Business Risks
- Social Media Risks Controls
- UWMC Social Media Policy



What is Social Media

■ Facebook

- 500 million users 2011
- 1 in every 13 people on earth
- 48% of 18 – 34 check Facebook daily

■ Twitter

- 200,000,000+ registered users
- 460,000 new sign-ups daily
- 155,000,000 Tweets per day

■ YouTube

- 100 million + users
- 24 hours of video are uploaded every minute

Social Media's Professional Side



■ LinkedIn

- 100 million + members, March 2011
- 17,800,000 members in Groups
- Groups – Education, finance, healthcare, etc.

■ Plaxo

- 50 million users
- Electronic address book



Benefits of Social Media

■ Marketing

- Selling and promoting the university to students
- Academics, research, sports

■ Brand recognition

- University accomplishments
- Selling and promoting the university to alumni, businesses and potential donors

■ Human resources

- Job postings



Benefits of Social Media

- Communication tool
- Direct customer communication
- Speed of feedback/results
- Low cost
- Reach
- Credibility
- Customer service

Regulatory Risks and Concerns



- FERPA, Family Educational Rights and Privacy Act
- HIPAA, Health Insurance Portability and Accountability Act

- Require the non-disclosure of personal private student and patient data.
- Require notification if personal private data is disclosed

Social Media Risks and Concerns

- Reputational and financial risks
- Information security risks
- Legal risks



Reputational and financial risks



■ Making the news for all the wrong reasons

- Security breaches
- Posting of personal private data
- Posting of embarrassing information (data, reports, photos, videos)
- Re-posting of data: e-mails, memos, reports, employee rants can be resent by recipients to a much larger and unintended audiences.
- “Name squatting” or “Brand hijacking” when a third party uses your company name or logos without your permission in social media.

Reputational and financial risks



Where Success is a Tradition

Consequences

- Cost of corrective actions and damage control
- Loss of donations, grants
- Lawsuits



Information security risks

- Introduction of viruses/malware to the corporate network
 - Security breaches
 - Loss of productivity / downtime
-
- Consequences
 - Reputational damage
 - Regulatory fines



Legal risks

- Disclosure of sensitive or protected information:
 - An employee could unwittingly click on links to spam or phishing schemes or download malicious code on to the university network
- Regulatory violations
- Discovery and preservation issues:
 - Ensure that data can be preserved, retrieved and produced if required
 - Just because an attorney is cc'd, does not make it privileged
 - If a privilege exists, it can be lost:
 - ➥ Once communications are shared with others, any privilege of confidentiality will be lost.



Business Risks

- Here are five primary business risks associated with the use of social media:
 - Introduction of viruses/malware to the corporate network;
 - Brand hijacking, such as a brand being impersonated on Twitter;
 - Unclear or undefined content rights to information posted on social media sites;
 - Unrealistic customer expectations of service through the ability to communicate with companies online 24/7; and
 - Noncompliance with record management regulations because of mismanagement of electronic communications.



Social Media Risk Control

- Policies and procedures address at least:
 - What is social media
 - Acceptable and authorized use of social media
 - Posting rules/requirements for data, videos
 - What is not allowed (rants, threatening, hateful or sexual content, bad mouthing employees, etc.)
 - Rules for friending between employees, supervisors, students and faculty
 - Regulatory requirements
 - Copyright rules
 - Intellectual property rules

Social Media Risk Controls

• Communications:

- Communicate to all personnel (and students) the social media policies and procedures
- Periodic communications regarding social media acceptable use
 - i.e. if an employee uses the university's name for a personal post are they required to include a disclaimer.
- Communicate when and how to notify management of policy violations.



Social Media Risk Control

■ Training

- Social media use training for users that will use social media as part of their job function or for research purposes
- Provide a webinar on social media use, risks, and your policies and procedures
- Social media use and regulatory requirements / restrictions (clearly defining that posting private patient or student is not allowed)



Social Media Risk Control

Information Technology Controls

- Antivirus/malware software
- Firewalls
- Logging and monitoring
- Security controls implemented on your social media site
- Scanning the social media sites for your data
 - >You can set up Google for “Social Mention” alerts when your university or president name is used

SOCIAL MEDIA BENEFITS AND RISKS



Questions

edureka!



Docker Commands

Most Used Docker Commands

docker --version

docker ps

docker commit

docker --help

docker images

docker import

docker pull

docker stop

docker export

docker run

docker kill

docker container

docker build

docker rm

docker compose

docker login

docker rmi

docker swarm

docker push

docker exec

docker service

Basic Docker Commands

`docker --version`

This command returns the version of Docker which is installed



Basic Docker Commands

```
docker --help
```

This command returns a list of commands available in Docker along with the possible flags (options)



Basic Docker Commands

`docker pull`

`$ docker pull ubuntu`

This command pulls a new Docker image from the Docker Hub



Basic Docker Commands

docker images

\$ docker images

This command lists down all the images in your local repo



Basic Docker Commands

`docker run`

`$ docker run ubuntu`

This command executes a Docker image on your local repo & creates a running Container out of it



Basic Docker Commands

docker build

```
$ docker build -t MyUbuntuImage .
```

This command is used to compile the Dockerfile, for building custom Docker images based on the



Basic Docker Commands

docker container

This command is used to perform various operations on the container. Refer to www.docs.docker.com for more info.



\$ docker container logs

\$ docker container kill

\$ docker container rm

\$ docker container run

\$ docker container start

And so on..

Basic Docker Commands

docker login

\$ docker login

This command is used to Login to Docker Hub repo from the CLI



Basic Docker Commands

docker push

\$ docker push vardhanns/MyUbuntuImage

This command pushes a Docker image on your local repo to the Docker Hub



PUSH

Basic Docker Commands

`docker ps`

*This command lists all the running containers in the host
If '-a' flag is specified, shutdown containers are also displayed*



`$ docker ps`

`$ docker ps -a`

Basic Docker Commands

docker stop

\$ docker stop fe6e370a1c9c

This command shuts down the container whose Container ID is specified in arguments. Container is shut down gracefully by waiting for other dependencies to shut



Basic Docker Commands

`docker kill`

`$ docker kill fe6e370a1c9c`

This command kills the container by stopping its execution immediately. Its similar to force kill



Basic Docker Commands

`docker rm`

`$ docker rm fe6e370a1c9c`

This command removes the container whose Container ID is specified in arguments



Basic Docker Commands

```
docker rmi
```

```
$ docker rmi MyUbuntuImage
```

This command removes the image whose name has been specified in arguments



Basic Docker Commands

docker exec

```
$ docker exec -it fe6e370a1c9c bash
```

This command is used to access an already running container and perform operations inside the container



Basic Docker Commands

docker commit

```
$ docker commit fe6e370a1c9c vardhanns/MyModifiedImage
```

This command creates a new image of an edited container on the local repo



COPY & PASTE

Basic Docker Commands

docker export

```
$ docker export --output="latest.tar" mycontainer
```

This command is used to export a Docker image into a tar file in your local system



Basic Docker Commands

docker import

```
$ docker import /home/edureka/Downloads/demo.tgz
```

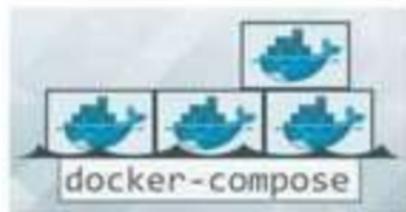
*This command is used to import the contents of a tar file
(usually a Docker image) into your local repo*



Advanced Docker Commands

docker compose

This command is used to power multi-container applications where various services will be hosted inside different containers.



\$ docker-compose build

\$ docker-compose up

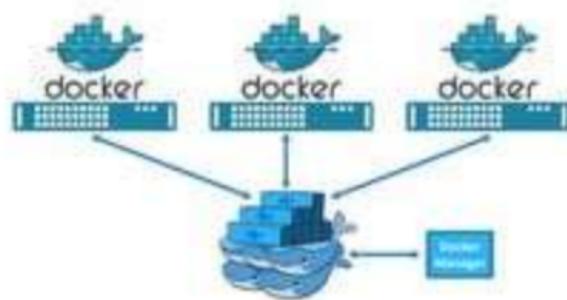
Note: This command is executed in the directory where YAML file is present for building the Compose.

Advanced Docker Commands

docker swarm

```
$ docker swarm init --advertise-addr 192.168.1.100
```

This command creates a network of Docker engines/ hosts to execute containers in parallel (for scaling up & high availability)



\$ docker swarm join

```
$ docker swarm join-token
```

\$ docker swarm leave

And so on..

Advanced Docker Commands

docker service

This command is used to control any existing Docker service
(Containers/Compose/Swarm/Others..)



\$ docker service ls

\$ docker service ps

\$ docker service scale

\$ docker service stop

\$ docker service logs

\$ docker service rm

And so on..



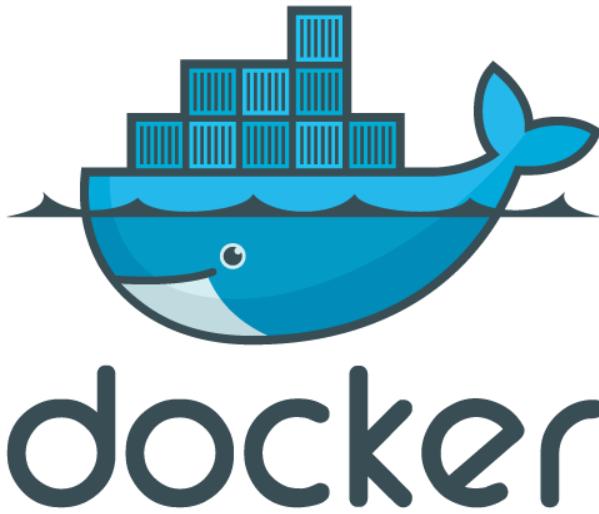
Thank You

Like

Comment

Share

For more information please visit our website
www.edureka.co



Introduction to Docker

Feb, 2019

Agenda

- **What is Docker?**
- **Containers vs. VMs**
- **How Docker works**
- **Why Docker? Docker Benefits**
- **Why Developers Care ?**
- **Docker Architecture**
- **What are Docker Images**
- **What are Docker Containers**
- **How to run Tomcat on Docker Container**
- **What is Docker File**
- **What is Docker Compose**
- **What is Docker Volumes**
- **Docker Swarm**

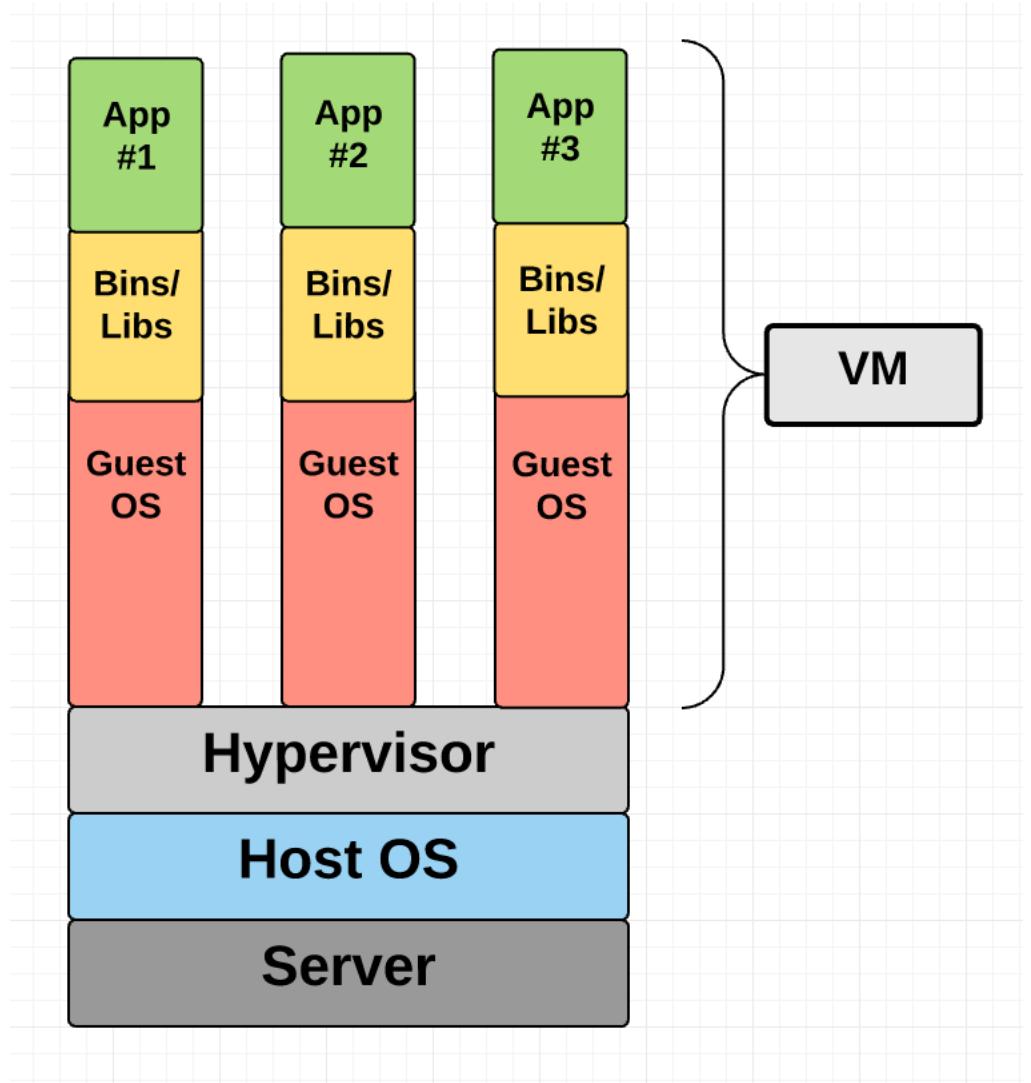


Docker: Containerization for Software

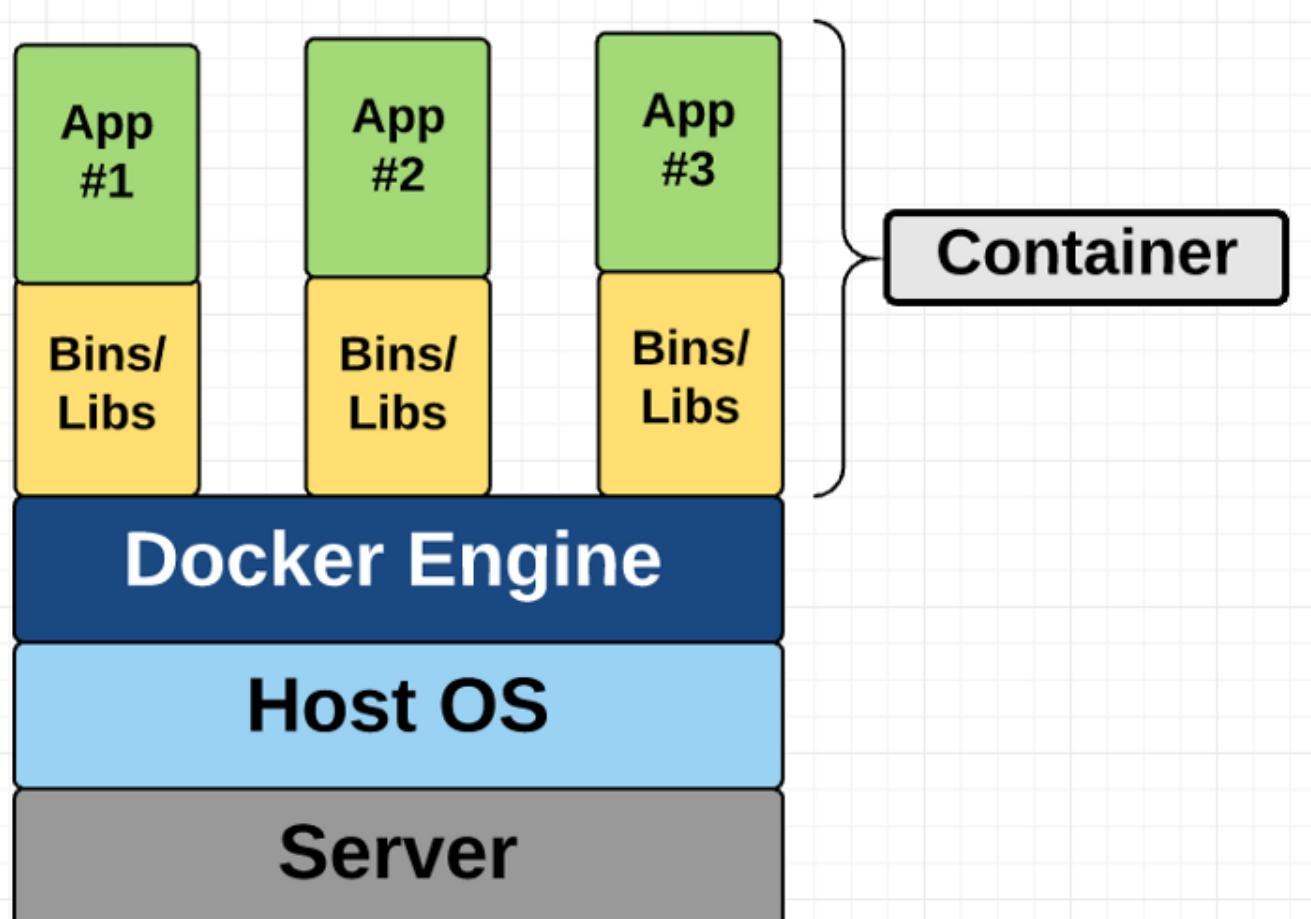


“Docker is an open platform for developers and sysadmins to build, ship, and run distributed applications”

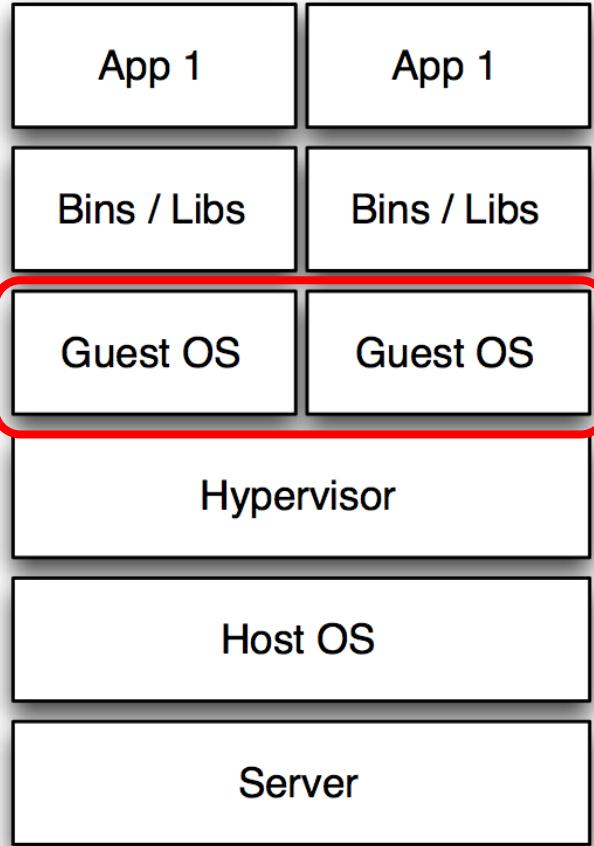
Virtual Machine



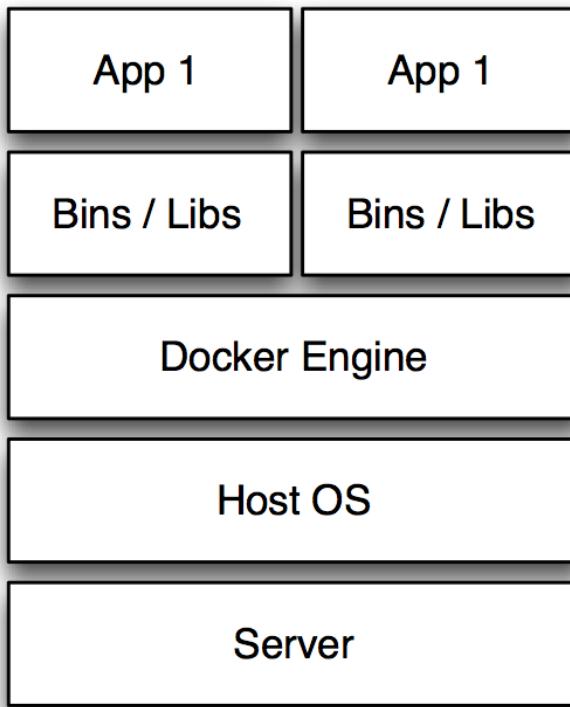
Container



VM vs. Docker (Containers)



Virtual Machines



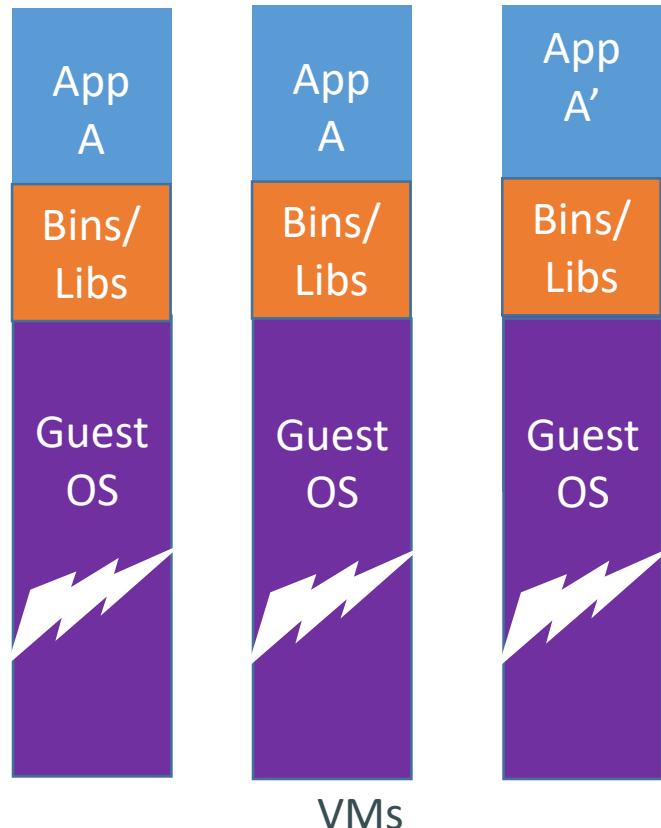
Docker

Docker Engine

Docker engine is the layer on which Docker runs. It's a lightweight runtime and tooling that manages containers, builds, and more.

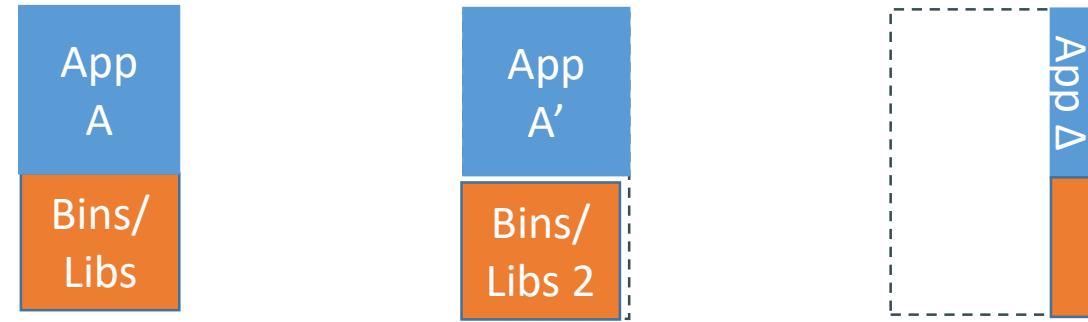
Why are Docker containers lightweight?

VMs



Every app, every copy of an app, and every slight modification of the app requires a new virtual server

Containers



Original App
(No OS to take up space, resources, or require restart)

Copy of App
No OS. Can Share bins/libs

Modified App
Copy on write capabilities allow us to only save the diffs Between container A and container A'

So why Docker?

- **Ease of use.** It allows anyone to package an application on their laptop, which in turn can run unmodified anywhere
 - The mantra is: “build once, run anywhere.”
- **Speed.** Docker containers are very lightweight and fast. Since containers are just sandboxed environments running on the kernel, they take up fewer resources. You can create and run a Docker container in seconds, compared to VMs which might take longer because they have to boot up a full virtual operating system every time.
- **Docker Hub.** Docker users also benefit from the increasingly rich ecosystem of Docker Hub, which you can think of as an “app store for Docker images.” Docker Hub has tens of thousands of public images created by the community that are readily available for use.
- **Modularity and Scalability.** Docker makes it easy to break out your application’s functionality into individual containers. With Docker, it’s become easier to link containers together to create your application, making it easy to scale or update components independently in the future.



Docker Benefits

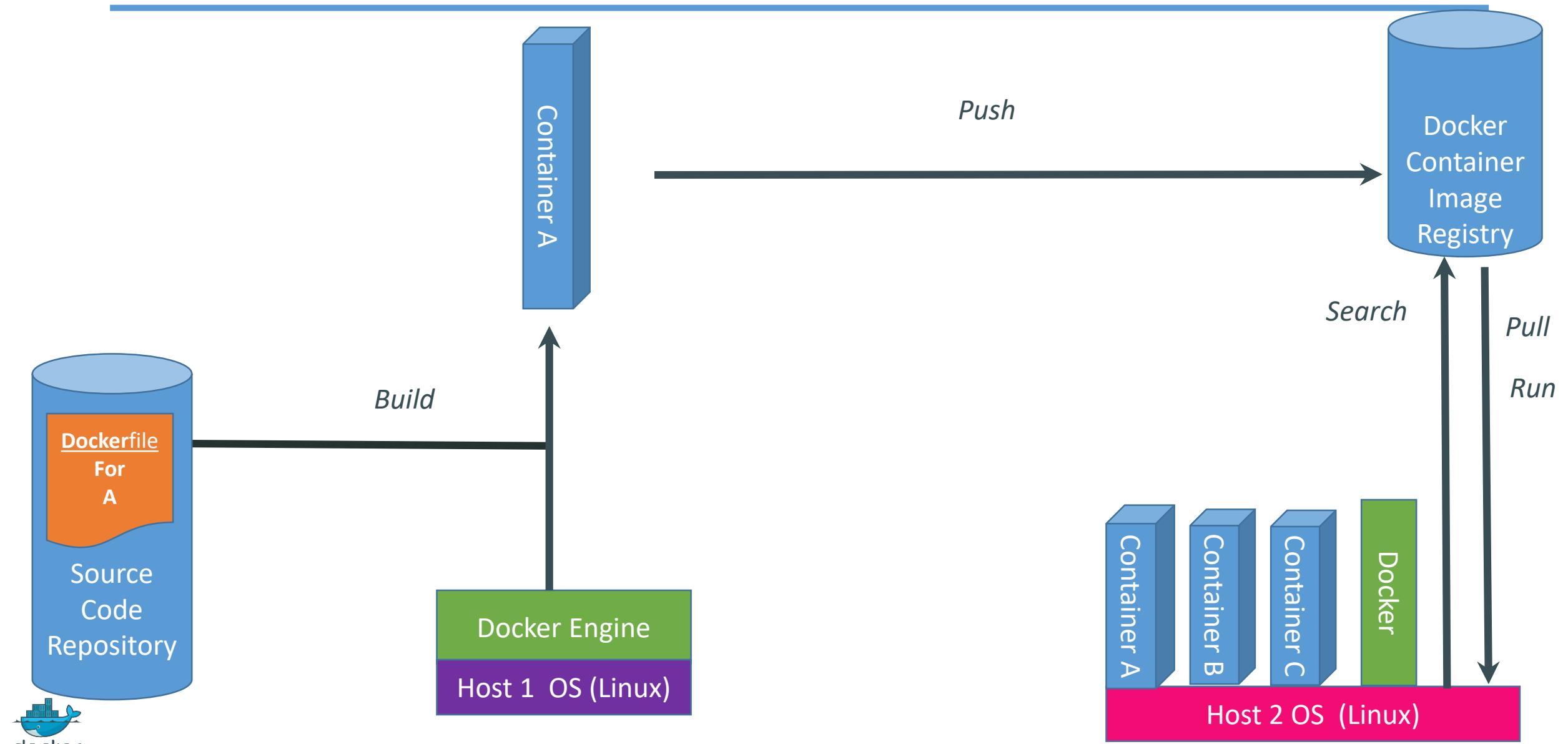
- 1. Local development environments can be set up that are exact replicas of a live environment/server.**
- 2. It simplifies collaboration by allowing anyone to work on the same project with the same settings, irrespective of the local host environment.**
- 3. Multiple development environments can be run from the same host each one having different configurations, operating systems, and software.**
- 4. It gives you instant application portability. Build, ship, and run any application as a portable container that can run almost anywhere.**

Why Developers Care

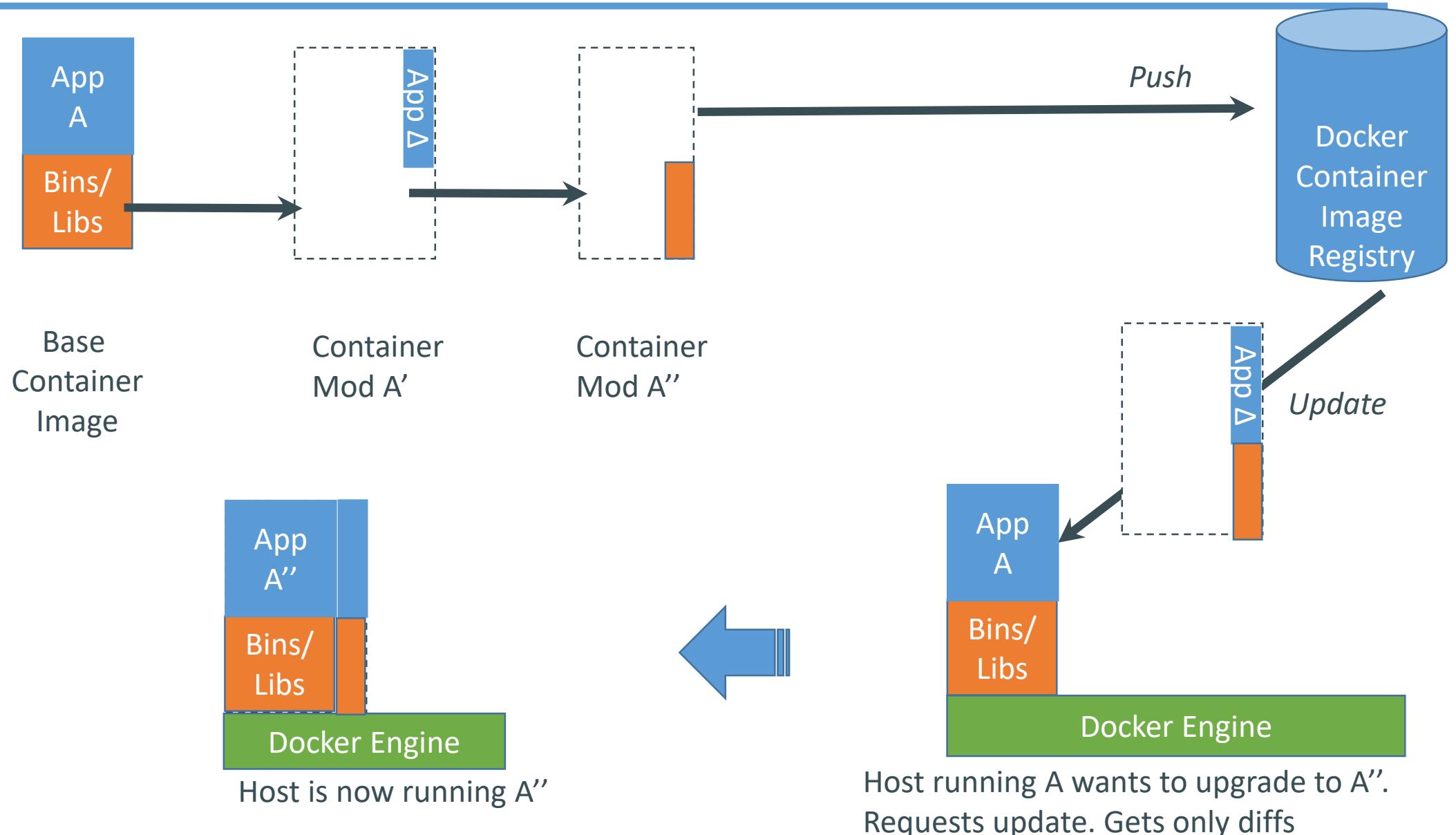
- **Build once... (finally) run anywhere***
 - **A clean, safe and portable runtime environment for your app.**
 - **No worries about missing dependencies, packages and other pain points during subsequent deployments.**
 - **Run each app in its own isolated container, so you can run various versions of libraries and other dependencies for each app without worrying**
 - **Reduce/eliminate concerns about compatibility on different platforms**
 - **Cheap, zero-penalty containers to deploy services. A VM without the overhead of a VM.**



What are the basics of the Docker system?



Changes and Updates



What are Docker Images

- Docker Images are templates used to create Docker containers.
- Where are Images Stored

Registries (e.g. docker hub)

Can be stored locally or remote

COMMANDS :

:docker images --help

:docker pull image

:docker images

:docker images -q

:docker run imageName

:docker rmi imageName

:docker rmi -f imageName

:docker inspect

:docker history imagename



What are Docker Containers

- **Containers are running instances of Docker Images.**
- **A container image is a lightweight, stand-alone, executable package of a piece of software that includes everything needed to run it: code, runtime, system tools, system libraries, settings.**
- **Containers run on the same machine sharing the same Operating system Kernel, this makes it faster**
- **Features of Containers:**
 - **Are lightweight**
 - **Fewer resources are used**
 - **Booting of containers is very fast**
 - **Can start, stop, kill, remove containers easily and quickly**
 - **Operating System resources can be shared within Docker**

Example Commands :

```
:docker run imageName  
:docker start/stop ContainerName/ID  
:docker pause/unpause ContainerName/ID  
:docker stats/attach ContainerName/ID  
:docker kill/rm ContainerName/ID
```



What is Docker File

- Docker can build images automatically by reading the instructions from a Docker file.
- A Docker file is a text document that contains all the commands a user could call on the command line to assemble an image.
- Using docker build users can create an automated build that executes several command-line instructions in succession.
- Each instruction creates one layer:

FROM creates a layer from the ubuntu:15.04 Docker image.

COPY adds files from your Docker client's current directory.

RUN builds your application with make.

CMD specifies what command to run within the container.

COMMANDS :

:docker build

:docker build -t ImageName:Tag directoryOfDockerfile

:docker run image



What is Docker Compose

- **Tool for defining & running multi-container docker applications.**
- **Use yaml files to configure application services (docker-compose.yml)**
- **Can start all services with a single command : docker compose up**
- **Can stop all services with a single command : docker compose down**
- **Can scale up selected services when required**



What is Docker Volumes

- **Volumes are stored in a part of the host filesystem which is managed by Docker.**
- **Non-Docker processes should not modify this part of the filesystem**
- **Bind mounts may be stored anywhere on the host system**
- **A given volume can be mounted into multiple containers simultaneously.**
- **Use of Volumes**

Decoupling container from storage

Share volume (storage/data) among different containers

Attach volume to container

On deleting container, volume is not deleted

Docker Swarm

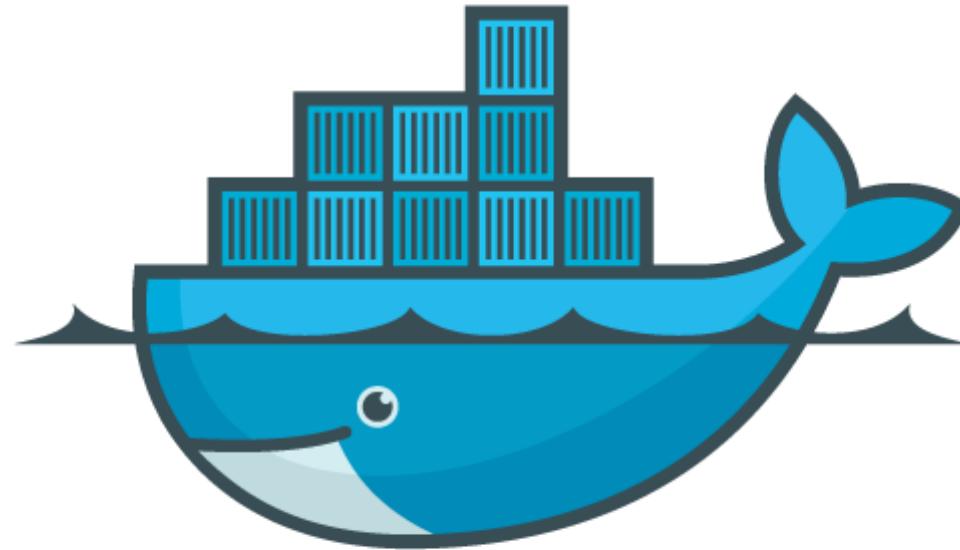
- A swarm is a group of machines that are running Docker and joined into a cluster.
- Docker Swarm is a tool for Container Orchestration.
- Let's take an example You have 100 containers
- You need to do
 - Health check on every container
 - Ensure all containers are up on every system
 - Scaling the containers up or down depending on the load
 - Adding updates/changes to all the containers
- Orchestration - managing and controlling multiple docker containers as a single service
- Tools available - Docker Swarm, Kubernetes, Apache Mesos



Want to learn more?

- [www.docker.io:](http://www.docker.io)
 - Documentation
 - Getting started: interactive tutorial, installation instructions, getting started guide,
 - About: Introductory whitepaper: <http://www.docker.io/the-whole-story/>
- Github: [dotcloud/docker](https://github.com/dotcloud/docker)
- IRC: [freenode/#docker](#)
- Google groups: groups.google.com/forum/#!forum/docker-user
- Twitter: follow [@docker](#)





docker
www.docker.io