ANISH ADNANI
D1713 / 01

ASSIGNMENT 2

1) Explain Network virtualization

→ Network virtualization (NV) refers to abstracting network resources that were traditionally delivered in hardware to software. NV can combine multiple physical networks to one virtual, software based network, or it can divide one physical network into seperate, independent virtual networks.
Network virtualization software allows network administrators to move virtual machine across different domains without reconfiguring the network. The software creates a network overlay that can run seperate virtual network layers on top of the same physical network fabric.

Network virtualization is rewriting the rules for the way services are delivered, from the software-defined data center (SDDC), to cloud, to the edge. This approach moves network from static, inflexible, and inefficient to dynamic, agile and optimized. Network virtualization decouples network services from the underlying hardware and allows virtual provisioning of an entire network. It makes it possible to programmatically create, provision, and manage networks all in software, while continuing to leverage the underlying physical network as the packet-forwarding backplane.
Physical network resources, such as switching, routing, firewalling, load balancing, virtual private network (VPN),

and more, are pooled, delivered in software, and require only Internet Protocol (IP) packet forwarding from the underlying physical network.

Benefits of Network virtualization are:

- Reduce network provisioning time from weeks to minutes
- Achieve greater operational efficiency by automating manual processes
- Place and move workloads independently of physical topology
- Improve network security within the data center.

2) Explain how Storage as a service is different from software as a service.

→ Storage as a service (STaaS)

Storage as a service is a managed service in which the provider supplies the customer with access to a data platform. The service can be delivered on premises from infrastructure that is dedicated to a single customer, or it can be delivered from the public cloud as a shared device service that's purchased by subscription and is billed according to one or more usage metrics.

STaaS customers access individual storage services through standard system interface protocols or applications program interface. Typical offerings

include bare-metal storage capacity; raw storage volumes; network file systems; storage objects; and storage applications that support file sharing and backup lifecycle management.

storage as a service can be used for data transfers and redundant storage, as well as to restore any corrupted or lost data. CIOs may want to use STaaS for the ability to deploy resources at an instant or to replace some existing storage space.

Whereas software as a service (SaaS) is a way of delivering applications over the Internet-as-a service. Instead of installing and maintaining software, you simply access it via the Internet, freeing yourself from complex software and hardware management.
SaaS applications are sometimes called web-based software, on-demand software, or hosted software. Whatever the name, SaaS applications run on a SaaS provider's servers. The provider manages access to the applications, including security, availability, and performance.
SaaS customers have no hardware to buy, install, maintain or update. Access to applications is easy. You just need an internet connection.

3) What is the Walrus storage controller? Explain the working of it is particular module in detail.

→

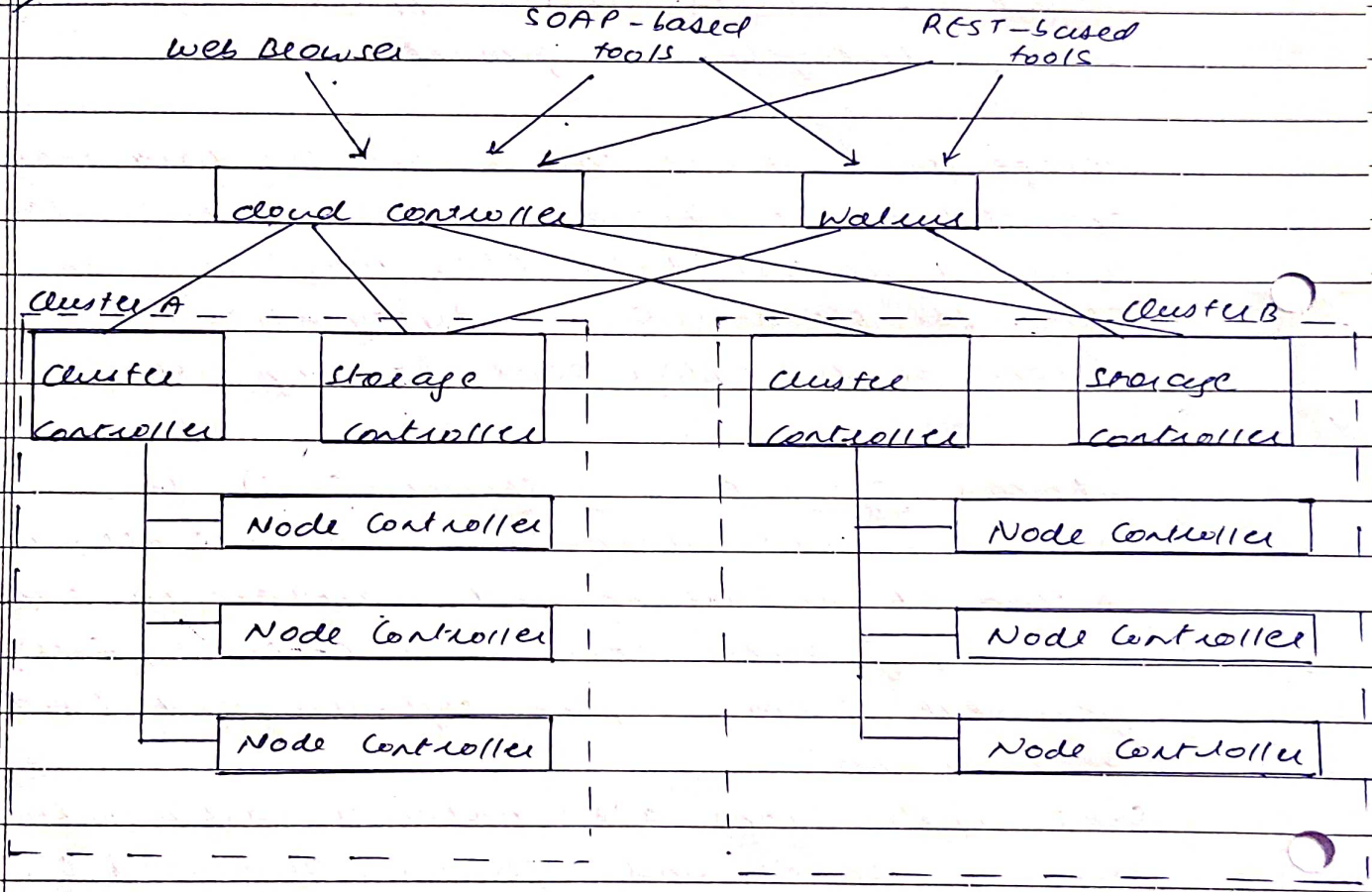


Fig: Eucalyptus and its components

Walrus allows users to store persistent data, organize as buckets and objects. You can use Walrus to create, delete, and list buckets, or to put, get, and delete objects, or to set access control policies.

Walrus is interface compatible with Amazon's simple storage service (S3), providing a mechanism

for storing and accessing virtual machine images and user data.
Basically walrus is a storage controller that provides block storage services with the same interface as Amazon EBS and S3 and can be used to store and retrieve virtual machine images and also application data.

4) List and explain the different services of CSB (Cloud Services Brokerage)

→ Cloud services brokerage (CSB) is an IT role and business model in which a company or other entity adds value to one or more (public or private) cloud services on behalf of the customers of that service via three primary roles including aggregation, integration and customization brokerage

There are three primary areas a cloud service broker can address in accelerating the adoption of the cloud:

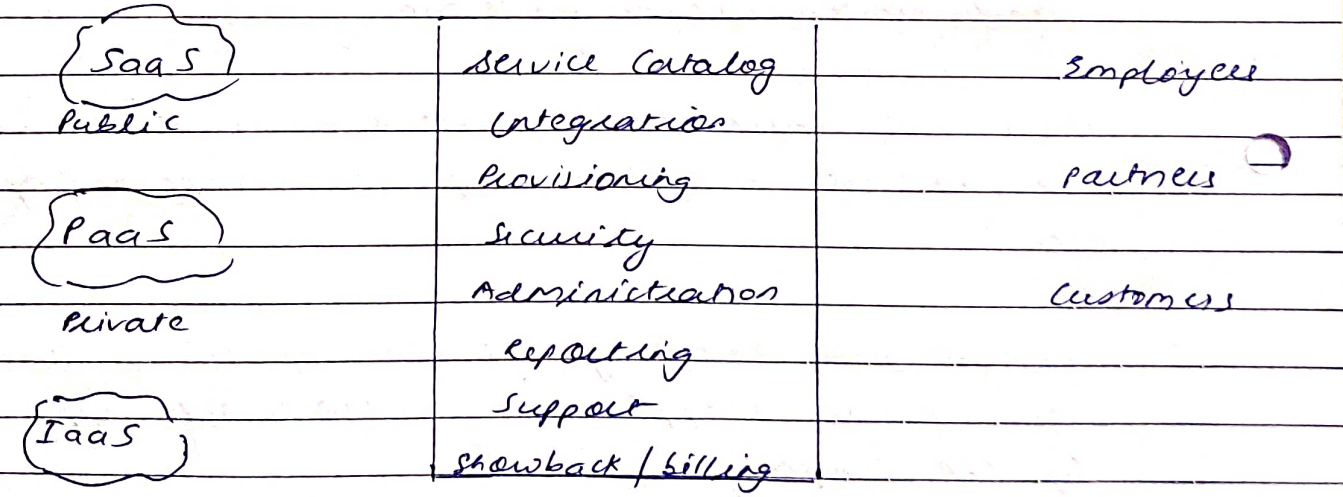
1. Aggregation: enabling the consumption of cloud by end users via cloud application marketplace approved by the company

2. Integration: ensuring cloud applications exchange data with each other and with on-premise applications to orchestrate business processes.

3. customization: augmenting cloud services with changes to data scheme or enhanced security and compliance.

In particular, organizations are looking to augment the cloud and achieve the following:

1. Reduce risk with more robust security and compliance capabilities
2. Add value and visibility with analytics.
3. Centralize functionality for audit trails and policy enforcement
4. Streamline the selection process of cloud services.



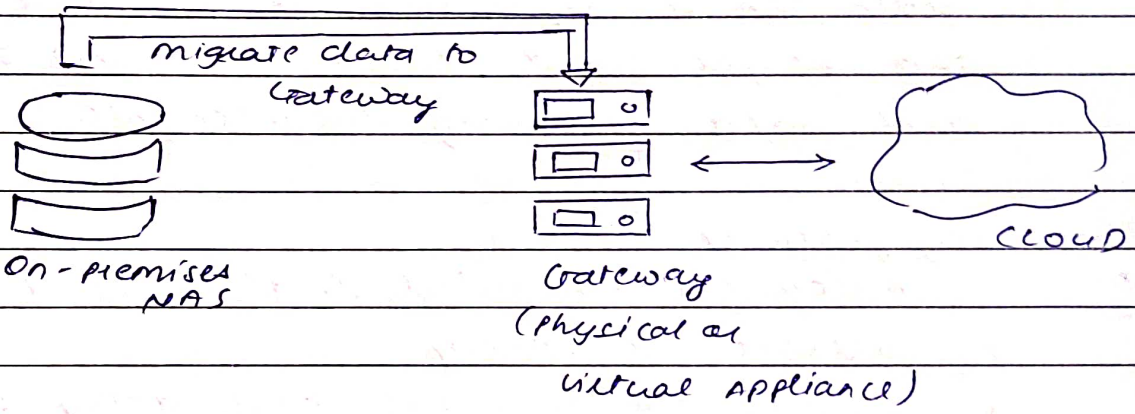
Advantages of CSB:

1) Broader Technical Expertise
2) Lower Total Cost of Ownership - financial returns

3) Operational efficiencies
4) Better options in dealing with risk, compliance and governance.

5) Explain the functioning of cloud storage Gateways with the help of a diagram.

→



A cloud storage gateway is a hardware or software appliance that serves as a bridge between local applications and remote cloud-based storage.
A cloud storage gateway provides basic protocols translation and simple connectivity to allow compatible technologies to communicate. The gateway may be hardware or a virtual machine (VM) image.

The requirement for a gateway between cloud storage and enterprise applications became necessary because of the incompatibility between protocols used for public cloud technologies and legacy storage systems.

Most public cloud providers rely on Internet protocols, usually a RESTful API over HTTP, rather than conventional storage area network (SAN) or network-attached storage (NAS) protocols.

Gateways can also be used for archiving the cloud. This pairs with automated storage tiering, in which data can be replicated between fast, local disk and cheaper cloud storage to balance space, cost, and data archiving requirements.

Key features include
1. Automated scheduled local & cloud backup
2. selective file backup
3. Bandwidth optimized cloud backup with block-level de-duplication
4. Supports windows, linux and mac
5. Application-aware backup for Microsoft Exchange, SQL server, sharepoint and Active Directory
6. Microsoft Hyper-V backup and restore for VMs

6) Describe in detail the working of the AAA model in cloud computing

→ AAA stands for Authentication, Authorization and Accounting.

Authentication is the process of identifying an individual, usually based on a username and

password. Authentication is based on the idea that each individual user will have unique information that sets him or her apart from other users.

Authorization is the process of granting or denying a user access to network resources once the user has been authenticated through the username and password. The amount of information and the amount of services the user has access to depend on the user's authorization level.

Accounting refers to the record-keeping and tracking of user activities on a computer network. For a given time period it is may include, but is not limited to, real-time accounting of time spent accessing the network, the network services employed or accessed, capacity and trend analysis, network cost allocations, etc.

Examples of AAA protocols include:

- Diameter, a successor to Remote Authentication Dial-In User Service (RADIUS)
- Terminal Access Controller Access-Control System (TACACS)
- Terminal Access Controller Access-Control System Plus (TACACS+)

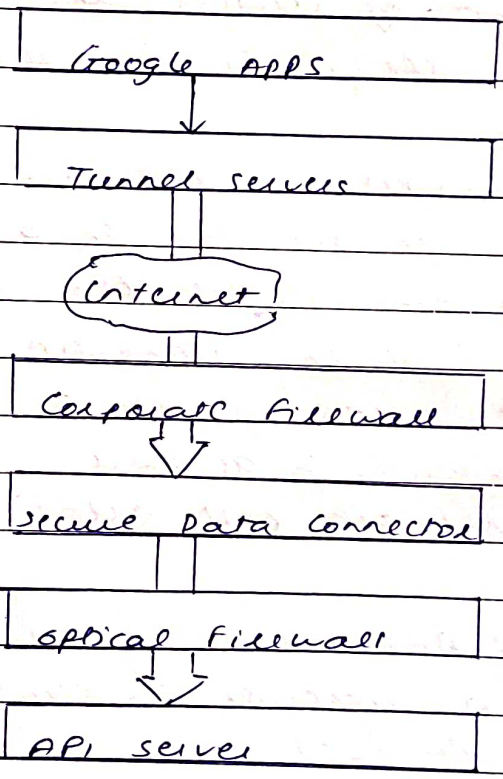
Types of AAA servers include

- Access Network AAA (AN-AAA) which communicates with radio network controllers

- Broker AAA (B-AAA), which manages traffic between roaming partner networks
- Home AAA (H-AAA)

7) Explain the structure of Google App Engine's Data store and its underlying technologies.

→



Google SDC working

1. The Google App Engine provides a powerful distributed data storage service that features a query engine and transaction.
2. An independent third-party auditor, who claims that GAE can be secure under the SAS70 auditing industry standard, issued Google Apps an unqualified SAS70 type II

certificate

3. There is no content addressing the issues of security storage services.
4. The security of data storage is assumed guaranteed using techniques such as by SSL link, based on our knowledge of security method adopted by other services.
5. The above figure is one of the secure services, called Google Secure Data Connector (SDC)
6. The SDC constructs an encrypted connection between the data source and Google Apps.
7. The tunnel servers validate the request identity. If the identity is valid, the tunnel protocol allows the SDC to set up a connection, authenticate, and encrypt the data that flows across the internet.
8. When the request is valid, the SDC performs a network request.
9. The server validates the signed request, checks the credentials, and return the data if the SDC and tunnel server all like the proxy to encrypt connectivity between Google Apps and the internal network.
10. In the signed request, the user has to submit identification information including the owner-id, viewer-id, instance-id, public-key, consumer-key, nonce, token, and signature within the request to ensure the integrity, security, and privacy of the request.