CLOUD COMPUTING ASSIGNMENT

Name :Aniket Bote
Roll Number : 10
Class : D17C

1.)Describe in detail the working of the AAA model in cloud computing

Ans : AAA is a system for tracking user activities on an IP-based network and controlling their access to network resources. AAA is often implemented as a dedicated server. AAA model stands for Authentication, Authorization, and Accounting**.**

Authentication is the process of identifying an individual, usually based on a username and password. It involves every user to have a unique username which becomes a primary Authentication enables confirmation of a user's validity who is requesting a service .It is established using the presentation of an identity and credentials. Ex:passwords, one-time tokens, digital certificates.

Authorization is granting or denying a user access to network resources after the user has been authenticated . The authorization level of the user determines whether the user gets to use a certain resource or not .It may be based on restrictions, for example, time-of-day restrictions, or physical location restrictions, or restrictions against multiple logins by the same user. Ex:IP address filtering, route assignment, encryption,differential services, bandwidth control ,etc.

Accounting is the process of keeping track of a user's activity i.e accessing the network resources, including the amount of time spent in the network, the services accessed and the amount of data transferred during the session.The data from accounting is used for trend analysis, capacity planning, billing, auditing and cost allocation.

Core components of AAA include :
Client
Policy Enforcement Point
Policy Information Point
Policy Decision Point
Accounting and Reporting System

AAA Flow :

1) The client attempts to connect to the network , is challenged for identity information, and sends this information to the PEP . In this example let's assume the client is a laptop with a worker attempting to access an organization's VPN from a remote location.
2) The PEP sends the collected identity information to the PDP. In some cases , the PEP just replays the information to PDP without knowing the information
3) The PDP queries any configured PIP for information about the client and validates the credential provided by the client.

4) The PIP returns a success or failure message from the credential validation step and sends additional information about the client to the PDP for evaluation. This informatioin could be the role of the user, the home location , etc.
5) The PDP evaluates information learned about the client through the client PEP , and PIP, the role of PEP and PIP that service the request and any contextual information against it's configured policies. Based on this information , the PDP makes an authorization decision.
6) The PDP sends PEP the authentication result and any authorization specific to the client . These authorization triggers specific PEP actions to apply to the client. For ex: The authentication data might trigger specific access control lists for client
7) The PDP also sends the results of this transaction to the accounting system
8) The PEP applies the authentication profile learned from PDP and sends the "authentication successful " message to client.
9) The client access production network through PEP

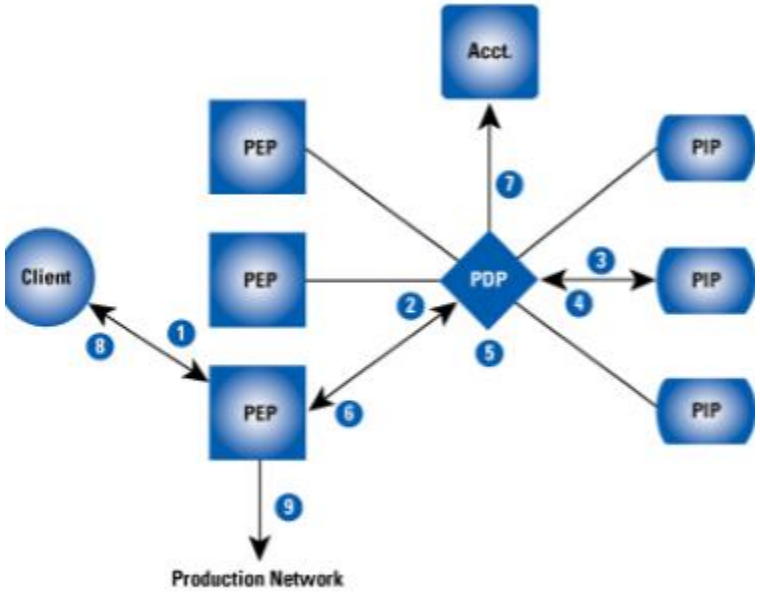


Figure 1: A Client Connects to a AAA-Protected Network

2.)List and explain the different services of CSB

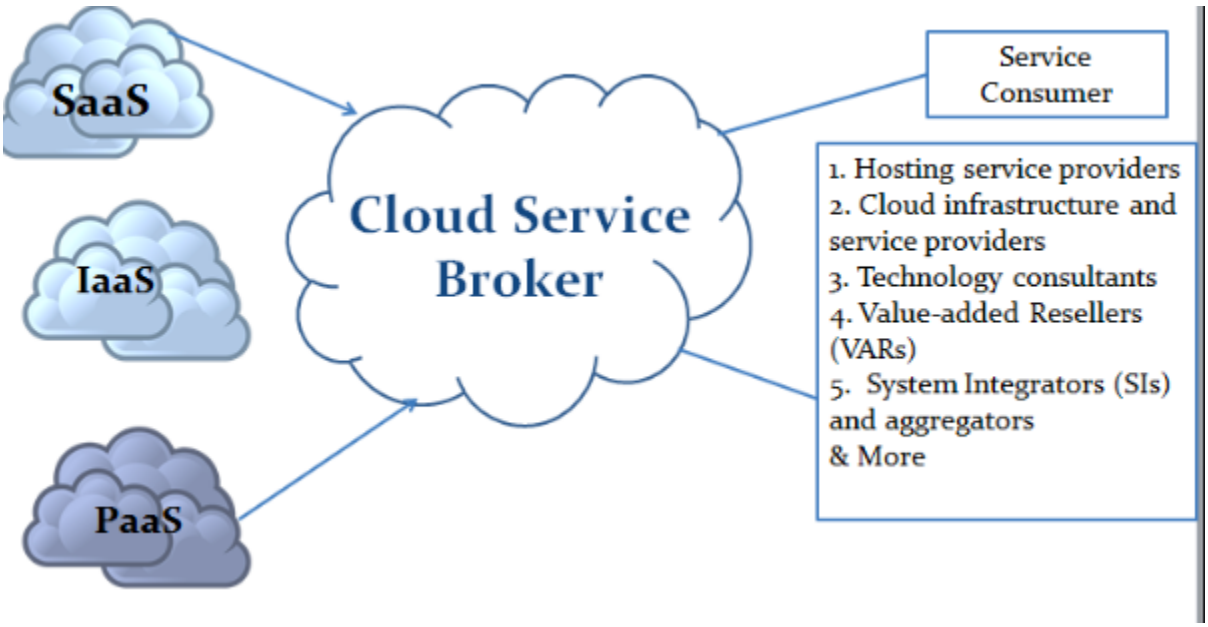
Ans: Cloud service brokerage is an IT role and business model in which a company or other entity adds value to one or more cloud services on behalf of one or more customers of that service via three primary roles including aggregation , integration and customization brokerage .Cloud service broker negotiates between cloud providers and cloud consumer that assist companies in choosing the services and offerings that best suits their needs. They may also assist in the deployment and integration of apps across multiple clouds or provide a choice and possible cost saving function which include multiple competing services from a catalog.Value added services like migration, VM portability, and

API management and normalization from cloud brokerage platforms like ComputeNext also allow end users freedom to move between platforms and keep options available at a variety of cloud vendors. 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 a 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 schema or enhanced security and compliance

The challenge for IT is that the cloud is relatively immature compared to on-premise enterprise software. By adding customized capabilities on top of cloud services, the enterprise can realize the benefits of cloud, while also meeting its other business objectives including data 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



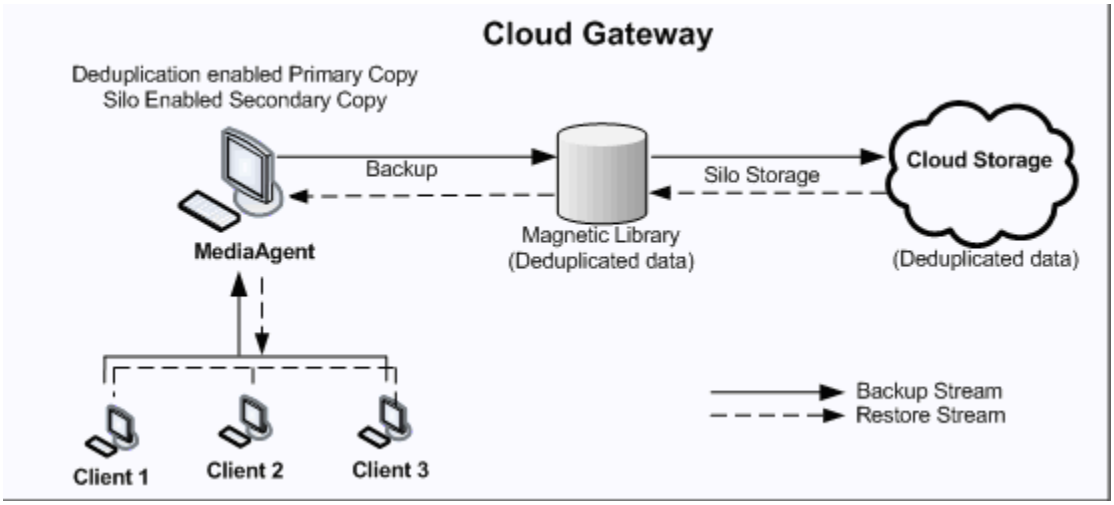
3.)Explain the functioning of cloud storage gateways with the help of diagram

Ans:It is a hardware/software based appliance situated on the client premises which bridges local applications of the customer and remote cloud-based storage. A cloud storage gateway is often called cloud storage controller or cloud storage appliance.

1. It enables basic protocol translation and simple connectivity for the incompatible technologies to be able communicate.
2. The gateway can be a single computing device or a virtual machine image that provides basic protocol translation and connectivity, letting incompatible technologies communicate.
3. Incompatibility between the protocols used for public cloud technologies and legacy
4. In order to use bandwidth efficiently and move data fast , gateways enable de-duplication and compression.
5. It is designed to provide interoperability between different data protocols used in a client/server cloud architecture.
6. It allows interoperability between the application programming interface (API) of a client's REST/SOAP-based data storage and Internet SCSI (iSCSI), Fiber Channel (FC).

Cloud Storage Gateways also include the following:

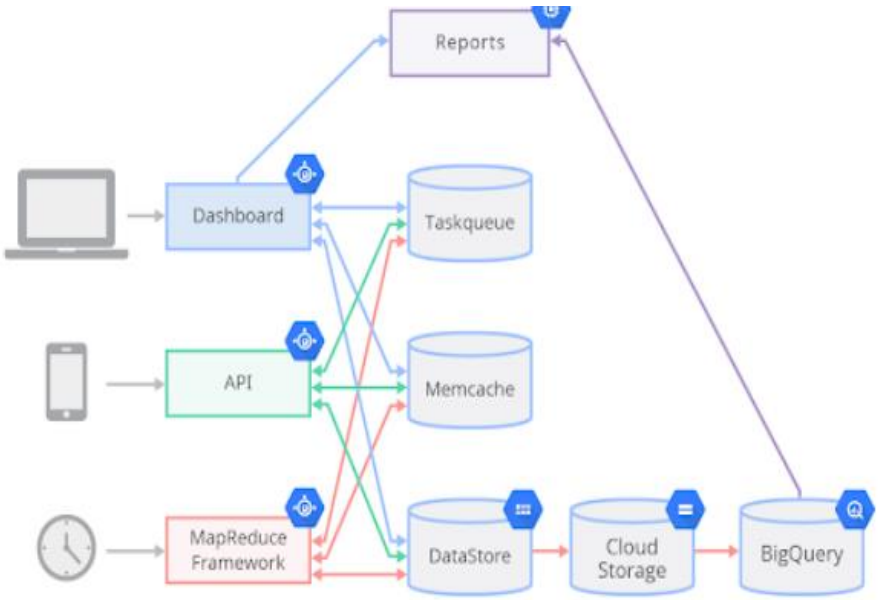
1. Automated scheduled local & cloud backup
2. Selective file backup
3. Supports Windows, Linux and Mac
4. Application-aware backup for Microsoft Exchange, SQL Server, SharePoint and Active Directory
5. Microsoft Hyper-V backup and restore for VMs



4.)Explain Google App Engine Datastore and it’s underlying technologies

Ans:Google App Engine Datastore is a platform as a service and cloud computing platform for web applications in google managed data centers.It provides with a query engines and transactions on a distributed data storage.An independent third-party auiditor , who claims that GAE can be secure under the SAS70 auditing industry standard , issued Google Apps an unclassified SAS70 Type II certification . However from it's online storage technical documents of lower API , there are only some functions such as GET and PUT.It doesnpt have any content addressing the issues of security storage services.The security of data storage is assumed guaranteed using techniques such as SSL Link, based on your knowledge of security method adopted by other services . Google secure data controller based on GAF.The SDC constructs an encrypted connection between the data secure and google apps . As long as data sources are in Google tunnel protocol servers when the user wants to get the data , then she/he will first send authorized data requests to google apps which forwards the request to tunnel server.The tunnel servers validate the requestor's identity . If the ID is valid then tunnel protocols allows the SDC to setup a connection , authenticate and encrypt the data that follows across the internet . At the same time the SDC uses resources to rules to validate whether the user is authorized to access the resource.If the request is valid , it performs a network request.

The server validates the signed request , checks the credentials and returns the data , if the SDC and tunnel server are like the proxy to encrypt between google apps and the internal network . In the signal request , the iser has to submit identification information including owner-id, viewer_id etc along with token and signature within the request to ensure integrity, security and privacy of request .



5)What is Walrus storage controller , explain in detail

Ans:Walrus takes care of storing the virtual machine images, storing the snapshots and serving Files. As with all other public facing Services in Eucalyptus, these Services are based on the Amazon Web Services API.Walrus is also called "WS3" and is the storage service provided by Eucalyptus. It is a

simple storage functionality, which is exposed by ReSTful and Soap APIs. Walrus takes care of storing the virtual machine images, storing the snapshots of data and serving Files.Just like in AWS , Walrus has containers called as “Buckets” which are unique on all accounts. Some naming restrictions are:

1. Containers can contain lowercase letters, numbers, periods (.), underscores (_), and dashes (-)
2. Container Names must start with a number or letter
3. The Length of a Name must be between 3 and 255 characters long
4. It is not allowed to use an IP-Address as Name (e.g., 265.255.5.4)

Walrus allows files to be public or private and the maximum size of file is 5TB.To delete a container in Walrus , all the files in the container must be deleted first before proceeding to delete the container. Uniform Resource Identifiers (URIs) are used to identify Files in walrus .Common Actions performed on the Walrus storage are the creation of containers, store data in containers, download data and grant or deny permissions. The Walrus Storage distinguishes two major read options: consistent read or eventually consistent read. The later one is faster but might server inconsistent data whereas the first one might have higher latency but data is always consistent.