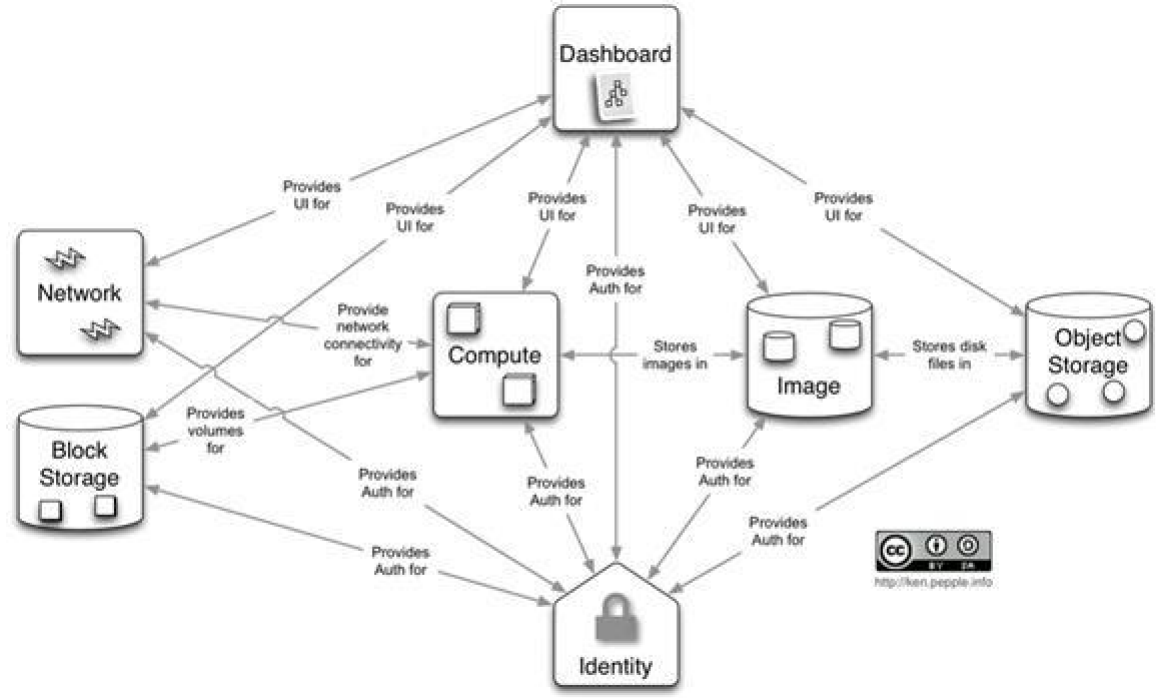
Open Stack

- OpenStack is a free and open-source software platform for cloud computing.
- OpenStack is a virtualization tool to manage your virtual infrastructure.
- **OpenStack consists of multiple components.**
  - Compute (Nova)
  - Image Service (Glance)
  - Object Storage (Swift)
  - Dashboard (Horizon)
  - Identity Service (Keystone)
  - Networking (Neutron)
  - Block Storage (Cinder)
  - Telemetry (Ceilometer)
  - Orchestration (Heat)
  - Workflow (Mistral)
  - Database (Trove)
  - Elastic map reduce (Sahara)
  - Bare metal (Ironic)
  - Messaging (Zaqar)
  - Shared file system (Manila)
  - DNS (Designate)
  - Search (Searchlight)
  - Key manager (Barbican)
  - Root Cause Analysis (Vitrage)
  - Rule-based alarm actions (Aodh)



Compute (Nova)

- OpenStack Compute is also known as OpenStack Nova.
- Nova is the primary compute engine of OpenStack, used for deploying and managing virtual machine.
- OpenStack Compute manages pools of computer resources and work with virtualization technologies.
- Nova can be deployed using hypervisor technologies such as KVM, VMware, LXC, XenServer, etc.

Image Service (Glance)

- OpenStack image service offers storing and retrieval of virtual machine disk images.
- OpenStack Compute makes use of this during VM provisioning.
- Glance has client-server architecture which allows querying of virtual machine image. While
- deploying new virtual machine instances, Glance uses the stored images as templates.
- OpenStack Glance supports VirtualBox, VMWare and KVM virtual machine images.

Object Storage (Swift)

 OpenStack Swift creates redundant (repetition), scalable data storage to store petabytes of accessible data.

 The data can be included,retrieved and updated.

 It has a distributed architecture, providing greater redundancy, scalability, and performance, with no central point of control.

 It helps organizations to store lots of data safely, cheaply and efficiently.

Dashboard (Horizon)

 OpenStack Horizon is a web-based graphical interface that cloud administrators and users can access tomanage OpenStack compute, storage and networking services.

 To service providers it provides services such as monitoring,billing, and other management tools.

Identity Service (Keystone)

 Provides an authentication and authorization service for other OpenStack services. Provides a catalog of OpenStack Services.

 Keystone provides a central list of users, mapped against all the OpenStack services, which they can access.

 Keystone supports various forms of authentication like standard username & password credentials.

Networking (Neutron)

 Neutron provides networking capability like managing networks and IP addresses for OpenStack.

 OpenStack networking allows users to create their own networks and connects devices and servers to one or more networks.

 Neutron also offers an extension framework, which supports deploying and managing of other network services such as virtual private networks (VPN), firewalls, load balancing, and intrusion detection system (IDS)

Block Storage (Cinder)

- Orchestrates multiple composite cloud applications by using templates.
- It creates and manages service that provides persistent data storage to cloud computing applications.
- Provides persistent block storage to running virtual machine.
- Cinder also provides a self-service application programming interface (API) to enable users to request and consume storage resources.
- A cloud user can manage their storage needs by integrating block storage volumes with Dashboard and Nova.
- It is appropriate for expandable file systems and database storage.

Telemetry (Ceilometer)

- It provides customer billing, resource tracking, and alarming capabilities across all OpenStack core components.

Orchestration (Heat)

- Heat is a service to orchestrate (coordinates) multiple composite cloud applications using templates.

Workflow (Mistral)

- Mistral is a service that manages workflows.
- User typically writes a workflow using workflow language and uploads the workflow definition.
  - The user can start workflow manually.

Database (Trove)

- Trove is Database as a Service for OpenStack.
- Allows users to quickly and easily utilize the features of a database without the burden of handling complex administrative tasks.

Elastic map reduce (Sahara)

- Sahara is a component to easily and rapidly provision Hadoop clusters.

 Users will specify several parameters like the Hadoop version number, the cluster topology type, node flavor details (defining disk space, CPU and RAM settings), and others.

Bare metal (Ironic)

 Ironic provisions bare metal machines instead of virtual machines.

Messaging (Zaqar)

 Zaqar is a multi-tenant cloud messaging service for Web developers.

Shared file system (Manila)

 Manila is the OpenStack Shared Filesystems service for providing Shared Filesystems as a service.

 Allows to create, delete, and give/deny access to a file.

DNS (Designate)

 Designate is a multi-tenant API for managing DNS.

Search (Searchlight)

 Searchlight provides advanced and consistent search capabilities across various OpenStack cloud services.

Key manager (Barbican)

 It provides secure storage, provisioning and management of secret data.

 This includes keying material such as Symmetric Keys,Asymmetric Keys and Certificates.

Root Cause Analysis (Vitrage)

 Vitrage is the OpenStack RCA (Root Cause Analysis) service for organizing, analyzing and expanding OpenStack alarms & events, yielding insights regarding the root cause of problems and deducing their existence before they are directly detected.

Rule-based alarm actions (Aodh)

 This alarming service enables the ability to trigger actions based on defined rules against an event data collected by Ceilometer.

Federation in the cloud

Inter cloud:

- The Inter-Cloud is an interconnected global "cloud of clouds" and an extension of the Internet "network of networks" on which it is based.
- Inter-Cloud computing is interconnecting multiple cloud providers' infrastructures.
- The main focus is on direct interoperability between public cloud service providers.
- To provide cloud services as utility successfully, interconnected clouds are required.
- Interoperability and portability are important factors.
- The limitations of cloud are that they have limited physical resources.
- If a cloud has exhausted all the computational and storage resources, it cannot provide service to the clients.
- The Inter-Cloud environment provides benefits like diverse Geographical locations, better application resilience and avoiding vendor lock-in to the cloud client.
- Benefits for the cloud provider are expand-on-demand and better service level agreements (SLA) to the cloud client.

Types of Inter-Cloud

- ✓ Federation Clouds
- ✓ Multi-Cloud

Federation Clouds

- A Federation cloud is an Inter-Cloud where a set of cloud providers willingly interconnect their cloud infrastructures in order to share resources among each other.
- The cloud providers in the federation voluntarily collaborate to exchange resources.
- This type of Inter-Cloud is suitable for collaboration of governmental clouds.

- Types of federation clouds are Peer to Peer and Centralized clouds.

Multi-Cloud

- In a Multi-Cloud, a client or service uses multiple independent clouds.
- A multi-cloud environment has no volunteer interconnection and sharing of the cloud service providers' infrastructures.
- Managing resource provisioning and scheduling is the responsibility of client or their representatives.
- This approach is used to utilize resources from both governmental clouds and private cloud portfolios.
- Types of Multi-cloud are Services and Libraries

Cloud Federation

- Provides Federated cloud ecosystem by connecting multiple cloud computing providers using a common standard.
- The combination of disparate things, so that they can act as one.
- Cloud federation refers to the unionization of software infrastructure and platformservices from disparate networks that can be accessed by a client.
- The federation of cloud resources is facilitated through network gate ways that connect public or external clouds like private or internal clouds
- It is owned by a single entity and/or community clouds owned by several co-operating entities.
- Creating a hybrid cloud computing environment.
- It is important to note that federated cloud computing services still relay on the existing of physical data centers.

Benefits of cloud federation:

- The federation of cloud resources allows client to optimize enterprise IT service delivery.
- The federation of cloud resources allows a client to choose best cloud serviceproviders
- In terms of flexibility cost and availability of services to meet a particular business or technological need within their organization.
- Federation across different cloud resources pools allows applications to run in the

most appropriate infrastructure environments.

- The federation of cloud resources allows an enterprise to distribute workload around the globe and move data between desperate networks and implement innovative security models for user access to cloud resources

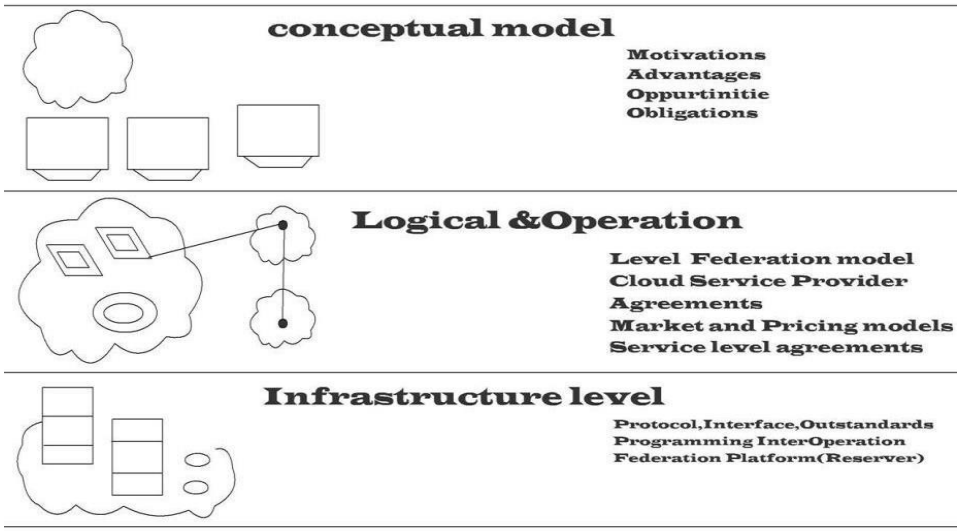
Cloud Federation and Implementation

- One weakness that exist in the federation of cloud resources is the difficulty in programming connectivity.
- Connection between a client and a given external cloud provider is difficult as they each possess their own unique network addressing scheme.
- Cloud providers must grant clients the permission to specify an addressing scheme for each server the cloud provider has external to the internet.
- This provides customers to with the ability to access cloud services without the need for reconfiguration when using resources from different service providers.
- Cloud federation can also be implemented behind a firewall which providing clients with the menu of cloud services provided by one or more trusted entities

5.5.2 Four Levels of Federation:

- Permissive
- Verified
- Encrypted
- Trusted

Permissive Federation:



- Permissive federation occurs when a server accepts a connection from a peer network server without verifying its identity using DNS lookups or certificate checking.
- The lack of verification or authentication may lead to domain spoofing.
- The unauthorized use of a third party domain name in an email message in order to pretend to be someone else), which opens the door to widespread spam and other abuses.

Verified Federation:

- This type of federation occurs when a server accepts a connection from a peer after the identity of the peer has been verified.
- It uses information obtained via DNS and by means of domain-specific keys exchanged beforehand.
- The connection is not encrypted, and the use of identity verification effectively prevents domain spoofing.
- Federation requires proper DNS setup, and that is still subject to DNS poisoning attacks.
- Verified federation has been the default service policy on the open XMPP since the release of the open-source jabberd 1.2 server.
- XMPP-real time communication protocol uses XML.
- Prevent Address spoofing

Encrypted federation:

- Server accepts a connection from a peer if and only if the peer supports Transport Layer Security (TLS) as defined for XMPP in Request for Comments (RFC) 3920.
- The peer must present a digital certificate.
- The certificate may be self-signed, but this prevents using mutual authentication.
- XEP-0220 defines the Server Dialback protocol, which is used between XMPP servers to provide identity verification.
- Server Dialback uses the DNS as the basis for verifying identity.
- The basic approach is that a receiving server receives a server-to- server connection request from an originating server.
- It does not accept the request until it has verified a key with an authoritative server for the domain asserted by the originating server.
- Server Dialback does not provide strong authentication or trusted federation
- Although it is subject to DNS poisoning attacks, it has effectively prevented most instances of address spoofing on the XMPP network

Trusted federation:

- A server accepts a connection from a peer only under the stipulation that the peer supports TLS and the peer can present a digital certificate issued by a root certification authority (CA) that is trusted by the authenticating server.
- The list of trusted root CAs may be determined by one or more factors, such as the operating system, XMPP server software, or local service policy.
- The use of digital certificates results not only in a channel encryption but also in strong authentication.
- The use of trusted domain certificates effectively prevents DNS poisoning attacks.
- But makes federation more difficult, since such certificates have traditionally not been easy to obtain.

5.5.3Federated Services and Applications:

- Clouds typically consist of all the users, devices, services, and applications connected to the network.
- In order to fully leverage the capabilities of this cloud structure, a participant needs the ability to find other entities of interest.
- Such entities might be end users, multiuser chat rooms, real-time content feeds, user directories, data relays, messaging gateways, etc.
- Finding these entities is a process called discovery.
- XMPP uses service discovery (as defined in XEP-0030) to find the aforementioned entities.
- The discovery protocol enables any network participant to query another entity regarding its identity, capabilities, and associated entities.
- When a participant connects to the network, it queries the authoritative server for its particular domain about the entities associated with that authoritative server.
- Then the authoritative server informs the inquirer about services hosted there and may also detail services that are available but hosted elsewhere.
- XMPP includes a method for maintaining personal lists of other entities, known as roster technology, which enables end users to keep track of various types of entities.

Future of Federation:

- The implementation of federated communications is a precursor to building a seamless cloud that can interact with people, devices, information feeds, documents, application interfaces, and other entities.
- It enables software developers and service providers to build and deploy such applications without asking permission from a large, centralized communications operator.
- Many big companies (e.g. banks, hosting companies, etc.) and also many large institutions maintain several distributed data-centers or server-farms, for example to serve to multiple geographically distributed offices, to implement HA, or to guarantee server proximity to the end user. Resources and networks in these distributed data-centers are usually configured as non-cooperative separate elements.
- Many educational and research centers often deploy their own computing infrastructures, that usually do not cooperate with other institutions, except in same punctual situations (e.g. in joint projects or initiatives). Many times, even different departments within the same institution maintain their own non-cooperative infrastructures.
- Cloud end-users are often tied to a unique cloud provider, because of the different APIs, image formats, and access methods exposed by different providers that make very difficult for an average user to move its applications from one cloud to another, so leading to a vendor lock-in problem.
- Many SMEs have their own on-premise private cloud infrastructures to support the internal computing necessities and workloads. These infrastructures are often over-sizedto satisfy peak demand periods, and avoid performance slow-down. Hybrid cloud (orcloud bursting) model is a solution to reduce the on-premise infrastructure size, so that it can be dimensioned for an average load, and it is complemented with external resources from a public cloud provider to satisfy peak demands.
- The cloud consumer is often presented with "take-it-or-leave-it standard contracts that might be cost-saving for the provider but is often undesirable for the user". The commission aims to develop with "stakeholders model terms for cloud computing service level agreements for contracts".