__/__/____

Cloud Networks

Cloud networking is the service or science in which companies networking procedure is hosted on public or private cloud. It is in demand for their speedy, fast processing dependable ~~transfer~~ transmission of information without any loss and pocket friendly setup.

Advantages

1. on demand self service
2. high scalability
3. Multisharing
4. low cost
5. Services according to pay per use
6. High availability
7. Maintainance

Protocols

Protocols are the set of rules that allow ~~to~~ two electronic items to connect and exchange information to one another.

There are many protocols :-

1. Gossip protocol → It is communication protocol It is used for failure detection, monitoring and messaging.

(2) Connectionless network protocol → It works on layer 3 protocol OSI model. It works on the mechanism of fragmentation.

(3) State routing protocol → A router communicate with each other used to choose path to route information.

(4) Internet group management protocol → Communication protocol used to multicast the data to nodes in network via router. It is used for streaming video, games over cloud.

(5) Secure shell protocol → Network protocol that allows remote login securely over internet.

(6) Coverage enhanced ethernet protocol → It solves network and packet loss issues.

(7) Extensible messaging and presence protocol → It is used for video and file transfer in cloud.

(8) Advanced message queing protocol → consist of wireless protocols, provides discription format of data sent on network.

Enhanced interior gateway routing protocol → It supports load balancing.

Media Transfer protocol → It transfers the media files, audio files and meta data to form portable devices over cloud.

Types of cloud Network

Cloud network is of three types
- Network Management
- Network Communication
- Network Security

Architecture of Software defined Networking with open stack

Three layers
- Application layer
- control layer
- Infrastructure layer

Application layer → It contains typical applications like firewall and load balancing.

Control layer → It consists of SDN controller which acts as a brain of network, it also allows hardware abstraction to applications.

Infrastructure layer → It consists of physical switches which forms data planes and carries actual movement of data packet.

__/__/____

Network function Virtualization

NFV is a network architecture which aims to accelerate service deployment for network operators and reduce cost by operating functions like firewall or encryption from dedicated hardware and moving them to virtual servers which reduces overall costs.

NFV is ~~provi~~ targeted at service providers or operators.
NFV helps service providers or operators to virtualize functions like load balancing, routing and policy management by transferring network functions from dedicated appliances to virtual servers.
There is no protocol determined for NFV.
NFV applications run on industry standards servers.
There are various cases for which NFV's are being used

(i) Network Virtualization → It helps them reduce there spendings on bulky physical hardware and cost associated with running, maintaining and repairing it.

(ii) Mobile edge computing → Using NFV, allows edge computing devices to perform computational services

__/__/____

and by generating and utilising single or multiple virtual machines. It translates various components of mobile like radio towers, data centres from hardware to software.

) Orchestration engines :- It uses programming to manage connections between network function and services.

) video analytics :- It reduces bandwidth upto 90%.

Security :- Firewalls protect VMS.

Network slicing :- It slice physical network to multiple networks.

SDN (software defined networking)

It is networking architecture which aims to improve overall network performance and make network agile and flexible by enabling a dynamic and programmatically efficient network configuration.

(i) SDN networks mainly focus on data centres.
(ii) SDN uses open flow as a communication protocol.
(iii) SDN reduces cost of network because there is no need of expensive switches and routers.

Applications → (i) networking
(ii) cloud orchestration

Cloud monitoring

Cloud monitoring uses automated and manual tools to manage, monitor and evaluate cloud computing architecture, infrastructure and services. It incoporates overall cloud management strategy allowing administrators to monitor status of cloud based resources.

It helps you identify ~~merging~~ emerging defects and troubling patterns so you can prevent minor issues from turning into significant problems.

Tools for cloud monitoring are
(i) Solarwinds
(ii) App dynamics
(iii) Microsoft cloud monitoring
(iv) Amazon cloud watch

cloud management

cloud management is management of cloud computing products and services. Public clouds are managed by public cloud service providers. which include public cloud environment's server, storage, networking and data centre operations. Users may also opt to manage their public cloud services with third party cloud management tool

Characteristics of cloud management :-

(i) provisioning and orchestration
(ii) Automation
(iii) Security and compliance
(iv) Cost managent and optimisation

Cloud maintenance

Cloud based computerised maintenance management system can be accessed by web browser or app. This mean maintenance staff can retrieve relevant information wherever they are located. Maintenance can be planned, scheduled, monitored and automated from a web browser.

__/__/____

Troubleshooting

It is a systematic approach to solving problems. The goal of troubleshooting is to determine why something doesn't work as expected and explain how to resolve the problem.

for eg:- when a laptop don't boot up, first step is to check whether power cable is working, once common issues are ruled out troubleshooters must run through a checklist of components to identify where failure is happening.

Backup

Backup ~~of the process~~ refers to copying and archiving of computer data so it may be used to restore original data after a data loss event. Cloud backup is a service in which data and applications on a business server can back up & stored on a remote server. Business opt to backup to cloud to keep files and data readily available in event of system failure, outage or natural disaster.

Recovery

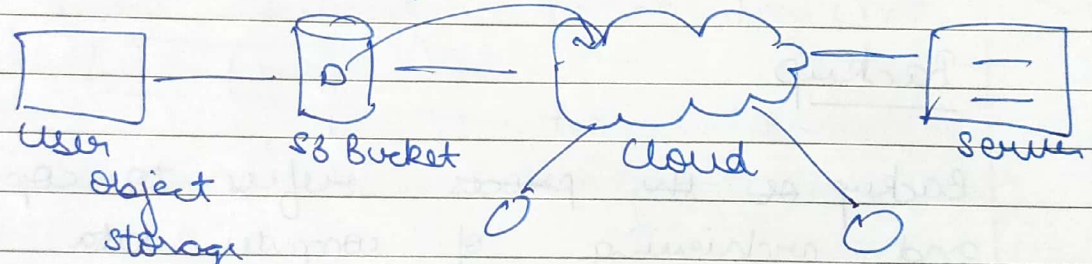
Data recovery is a process of restoring data that has been lost, accidently deleted

corrupted or made inaccessible. Cloud disaster recovery is a service that enables backup and recovery of remote machines on a cloud based platform. It is a primarily on IAAS solution that backup designated system data on a remote offsite cloud server.

Explain SLA (Service level Agreement), monitoring and management related to cloud.

Cloud lab

S3 Simple Storage service



Object storage service

→ optimise cost, configure data, organise data

Functions :-

Control access data
Optimise cost
Replicate data to a region
Protect & secure your data

Storage class

__/__/____

2/2 check passed

Public ipv4 addres copy and paste on browser

→ It availabl to all (setting change)

Service level Agreement (SLA)

SLA is the bound for performance negotiated between cloud service providers and clients. SLA are standarised until a client becomes a large consumer of cloud services. SLA are defined at different levels :-

1) customer based SLA
2) Server based SLA
3) Multi level SLA

Few service level agreements are enforced as contracts but mostly are agreements or contracts which are more along the lines of operating level agreement and may not have any restriction of law.

SLA specifies some parameters :-

1) availability of service
2) latency or response time
3) Service components reliability
4) Each part accountability
5) Warrenties

__/__/____

Cloud security

Cloud computing security or cloud security refers to the broad set of policies, technologies, applications and controls utilised to protect virtualised IP, data, applications, services and associated infrastructure of cloud computing.

Cloud security ensures data and applications are readily available to authorised users.
for eg:- In AWS, cloud security provides services that helps protect your data, accounts and workloads from unauthorised access. AWS data protection services provide encryption and key management and threat detection that continuously monitors and protect your accounts and workloads.

Cloud security is set of rules, policies, controls and procedures that work together to protect cloud infrastructure and data.

Attacks:-

1) Cloud Malware injection attack :- It is done to take control of users information in cloud. For this purpose hackers add an infected service to SaaS or PaaS implementation module.

2) ~~Att~~ Abuse of cloud services :- Hackers can use cheap cloud services to arrange

DoS (Denial of Service) and brute force attacks on target users, companies and either other cloud providers.

3) Denial of Service attack :- These attacks are dangerous for cloud computing system as many users may suffer as result of flooding even a single cloud server.

4) Site channel attack :- A site channel ~~attack~~ hack is arranged by hackers when they place a melacious virtual machine on same host as target.

5) Insider attack :- It is initiated by legitimate user who is purposefully violating security policy.

Network Security

It is a set of rules and ~~configurations~~ configurations designed to protect integrity, confidentiality and ~~assess~~ accessibility of computer ~~not~~ network and data using both software and hardware technologies.

There are three components of network security

1) Hardware - servers or devices that perform
2) ~~Software~~ security functions within networking environment.

2) Software :- Software includes antivirus applications, antivirus app. can be installed on devices and nodes.

3) Cloud services :- It does the work of scanning and blocking potential threats before traffic is allowed onto network.

Threats

1) Misconfiguration :- Many organisations are unfamiliar with securing cloud infrastructure and often have multi cloud deployments. It is easy for misconfiguration or security over site to leave an organisation's cloud based resources exposed to hackers.

2) Unauthorised access :- While this is an asset accessible from public network it makes easier for attackers to gain access to an organisation's cloud based resources.

3) Insecure API :- It creates potential issues if customer has not properly secured interfaces for cloud based infrastructure.

4) Hijacking of accounts :- Many people have extremely weak password security including password reuse and attack with employee's credentials can access sensitive

data or functionality and give full control over their online account.

5) Lack of visibility :- An organisation's cloud based resources are located outside of cooperate network and run on infrastructure that company doesn't own. This can limit an organisation's ability to monitor their cloud based resources and protect them against attack.

6) External sharing of data :- While easy data sharing is an asset it can also be a cloud security issue. The shared link can be forwarded to someone else, stolen as a part of cyber attack or cyber criminal provides unauthorised access to shared resource.

Assignment -2

Q1. What is edge computing ? Explain with example.

Q2. Explain containers and edge computing with open stack.

Gartners seven cloud computing security risk

There are following security risks gartner say that customers should raise with vendors before selecting a cloud vendor.

(1) privileged user access :- Sensitive data brings inherit level of risk so get as much information as you can about people who manage your data.

(2) regular compliance :- customers are responsible for security and integrity of their own data.

(3) data location :- when you use cloud you don't know where data is hosted, ask your providers if they commit to storing and processing data in specific jurisdiction and whether they make commitment to obey local privacy requirements.

(4) data segregation :- Encryption is effective but isn't sure. One needs to find out what is done to segregate data to rest.

(5) Recovery :- A cloud provider should tell what will happen to your data and service in case of disaster.

Also ~~also~~ ask about ability to complete restoration and how much time it will take.

(6) Investigative support :- Cloud services are difficult ~~to~~ to investigate because logging and data for multiple customers maybe located at and spread across everchanging set of locations.

(7) long ~~term~~ term viability :- Ask potential providers how would you get your data back and if it would be in a format that one could ~~import~~ import into replacement application.

Data lifecycle management (DLM)

It is a policy based approach to managing the flow of an informations system data throughout its lifecycle from creation and initial storage to when it becomes ~~obsolete~~ ~~obsolete~~ obsolete and is deleted.

There are three main goals of DLM strategy

(1) data security and confidentiality :- data should be stored securily to ensure private, confidential and sensitive information

(2) data integrity :- data must be accurately stored

(3) data availability :- approved users should be able to access data when and where they need access without disruption.

Data management experts stress that DLCM is not a product but a comprehensive approach to manage an organisation's data, involving procedures and practice as well as application.

Five phases of DLCM

(1) generate and collect data
(2) store and manage data
(3) use and share data
(4) archieve data
(5) destroy data