Welcome To:
Module 7

Networking, Services and System Updates

Internet Access to VM

- Open **Virtualbox Manager**
- Select the machine you cannot get internet on in the left pane
- Click the **Settings** button in the top menu
- Click **Network** in the left pane in the settings window
- Switched to **Bridged Adaptor** in the **Attached to** drop-down menu
- Hit **OK** to save your changes
- Start your VM

Network Components

- IP
- Subnet mask
- Gateway
- Static vs. DHCP

- Interface
- Interface MAC.

Network Files and Commands

- Interface Detection
- Assigning an IP address
- Interface configuration files
  - /etc/nsswitch.conf
  - /etc/hostname
  - /etc/sysconfig/network
  - /etc/sysconfig/network-scripts/ifcfg-nic
  - /etc/resolv.conf

- Network Commands
  - **`ping`**
  - **`ifconfig`**
  - **`ifup or ifdown`**
  - **`netstat`**
  - **`tcpdump`**

NIC Information

NIC = Network Interface Card

Example:

```
ethtool enp0s3
```

Other NICs

`lo` = The loopback device is a special interface that your computer uses to communicate with itself. It is used mainly for diagnostics and troubleshooting, and to connect to servers running on the local machine

`virb0` = The virbr0, or "Virtual Bridge 0" interface is used for NAT (Network Address Translation). Virtual environments sometimes use it to connect to the outside network

NIC Bonding

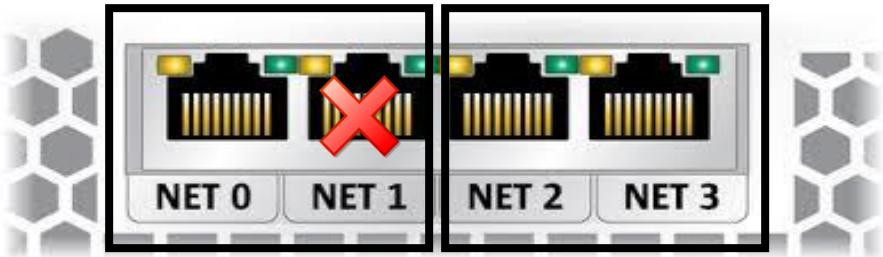
NIC = Network Interface Card (PC or laptop)

NIC(Network Interface Card) bonding is also known as Network bonding. It can be defined as the aggregation or combination of multiple NIC into a single bond interface.

It's main purpose is to provide high availability and redundancy

2G

1G + 1G

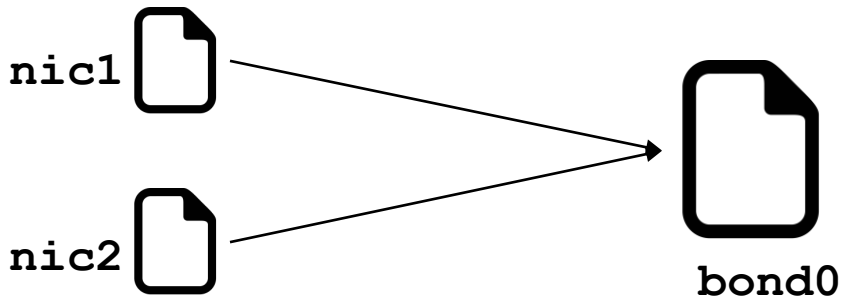


Redundancy

High Availability
Link Aggregation

NIC Bonding Procedure

- modprobe bonding
- modinfo bonding
- Create /etc/sysconfig/network-scripts/ifcfg-bond0
- Edit /etc/sysconfig/network-scripts/ethernet1
- Edit /etc/sysconfig/network-scripts/ethernet2



- Restart network = systemctl restart network

System Updates and Repos

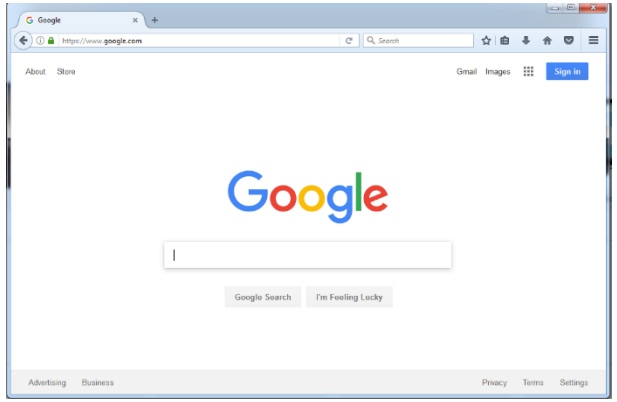
- yum (CentOS), apt-get (other Linux)
- rpm (Redhat Package Manager)

Advance Package Management

- Installing packages
- Upgrading
- Deleting
- View package details information
- Identify source or location information
- Packages configuration files

Download Files or Apps

- Example of Windows browser



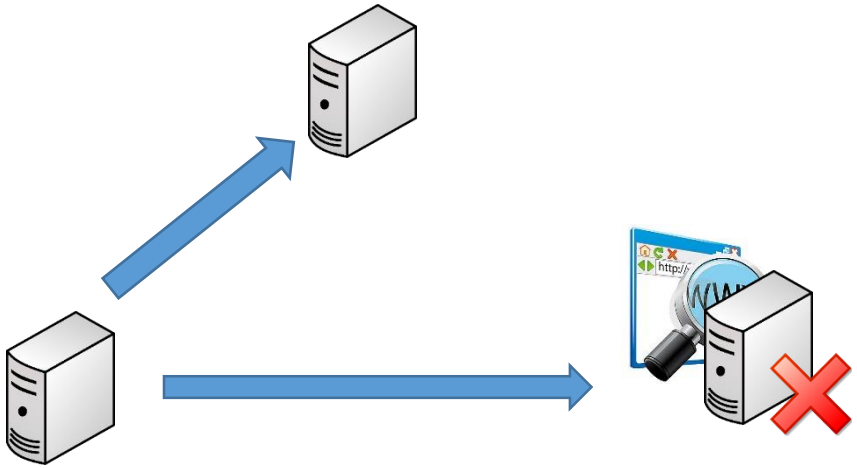
- Linux = **`wget`**

- Example in Linux:

`wget` `http://website.com/filename`

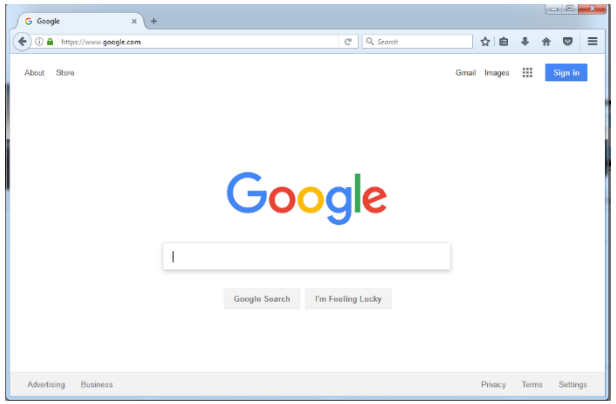
- **Why???**

Most of the servers in corporate environment do **NOT** have internet access



curl and ping Commands

- Example of Windows browser



- Linux = **curl**
- **Linux = ping**

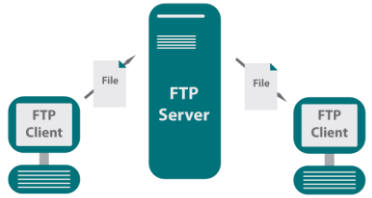
- Example in Linux:

```
curl http://website.com/filename
curl -O http://website.com/filename

ping www.google.com
```

FTP – File Transfer Protocol

- The File Transfer Protocol is a standard network protocol used for the transfer of computer files between a client and server on a computer network. FTP is built on a client-server model architecture using separate control and data connections between the client and the server. *(Wikipedia)*

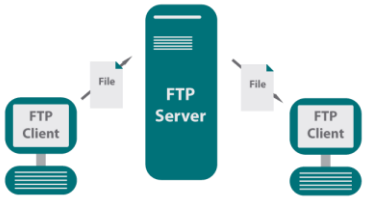


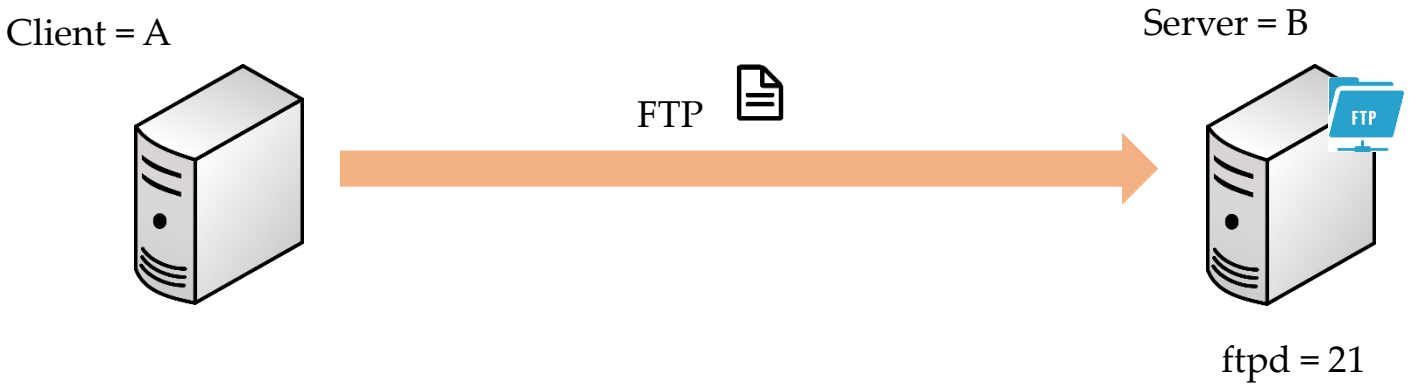
- Protocol = Set of rules used by computers to communicate

- Default FTP Port = 21

- For this lecture we need 2 Linux machines
  - **`Client = MyFirstLinuxVM`**
  - **`Server = LinuxCentOS7`**

FTP – File Transfer Protocol

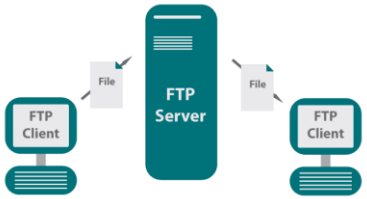




By: Imran Afzal

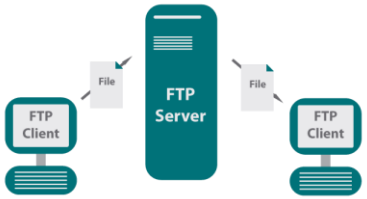
FTP – File Transfer Protocol

- Install and Configure FTP on the remote server
  - **# Become root**
  - **# rpm -qa | grep ftp**
  - **# ping www.google.com**
  - **# yum install vsftpd**
  - **# vi /etc/vsftpd/vsftpd.conf** ***(make a copy first)***



  - Find the following lines and make the changes as shown below:
  - ## Disable anonymous login ##
    - ***anonymous_enable=NO***
  - ## Uncomment ##
    - ***ascii_upload_enable=YES***
    - ***ascii_download_enable=YES***
  - ## Uncomment - Enter your Welcome message - This is optional ##
    - ***ftpd_banner=Welcome to UNIXMEN FTP service.***
  - ## Add at the end of this file ##
    - ***use_localtime=YES***
  - **# systemctl start vsftpd**
  - **# systemctl enable vsftpd**
  - **# systemctl stop firewalld**
  - **# systemctl disable firewalld**
  - **# useradd iafzal** *(if the user does not exist).*

FTP – File Transfer Protocol



- Install FTP client on the client server
  - `# Become root`
  - `# yum install ftp`
  - `# su - iafzal`
  - `$ touch kruger`

  - Commands to transfer file to the FTP server:
  - `ftp 192.168.1.x`
  - `Enter username and password`
  - `bi`
  - `hash`
  - `put kruger`
  - `bye.`

SCP – Secure Copy Protocol

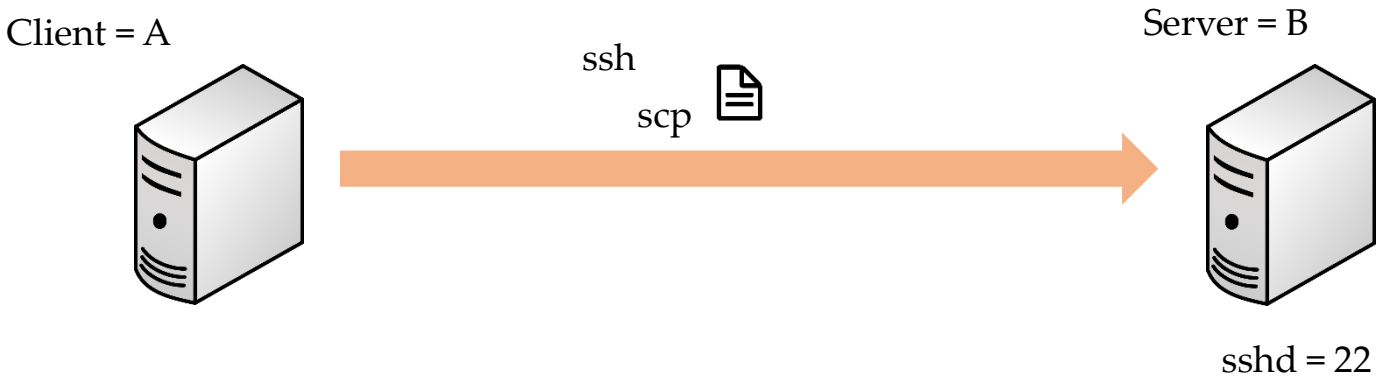
- The Secure Copy Protocol or "SCP" helps to transfer computer files securely from a local to a remote host. It is somewhat similar to the File Transfer Protocol "FTP", but it adds security and authentication

- Protocol = Set of rules used by computers to communicate

- Default SCP Port = 22 (same as SSH)

- For this lecture we need 2 Linux machines
  - **`Client = MyFirstLinuxVM`**
  - **`Server = LinuxCentOS7`**

SCP – Secure Copy



By: Imran Afzal

SCP – Secure Copy

- SCP commands to transfer file to the remote server:
  - **Login as yourself (iafzal)**
  - **touch jack**
  - **scp jack iafzal@192.168.1.x:/home/iafzal**
  - **Enter username and password**

rsync – Remote Synchronization

- **rsync** is a utility for efficiently transferring and synchronizing files within the same computer or to a remote computer by comparing the modification times and sizes of files

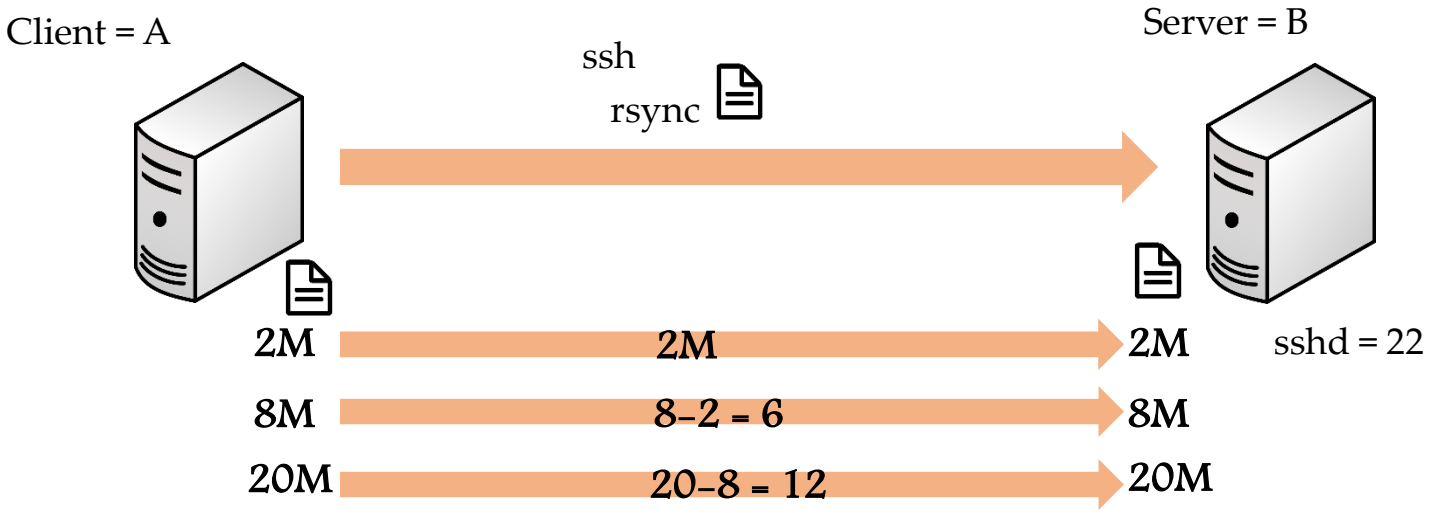
- rsync is a lot faster than ftp or scp

- This utility is mostly used to backup the files and directories from one server to another

- Default rsync Port = 22 (same as SSH)

- For this lecture we need 2 Linux machines
  - **`Client = MyFirstLinuxVM`**
  - **`Server = LinuxCentOS7`**

rsync – Remote Synchronization



By: Imran Afzal

rsync – Remote Synchronization

- Basic syntax of rsync command
  - **# rsync options source destination**

- Install rsync in your Linux machine *(check if it already exists)*
  - **# yum install rsync** *(On CentOS/Redhat based systems)*
  - **# apt-get install rsync** *(On Ubuntu/Debian based systems)*

- rsync a file on a local machine
  - **$ tar cvf backup.tar .** *(tar the entire home directory (/home/iafzal)*
  - **$ mkdir /tmp/backups**
  - **$ rsync -zvh backup.tar /tmp/backups/**

- rsync a directory on a local machine
  - **$ rsync -azvh /home/iafzal /tmp/backups/**

- rsync a file to a remote machine
  - **$ mkdir /tmp/backups** *(create /tmp/backups dir on remote server)*
  - **$ rsync -avz backup.tar iafzal@192.168.1.x:/tmp/backups**

- rsync a file from a remote machine
  - **$ touch serverfile**
  - **$ rsync -avzh iafzal@192.168.1.x:/home/iafzal/serverfile /tmp/backups**

System Upgrade/Patch Management

- Two type of upgrades

  Major version = 5, 6, 7

  Minor version = 7.3 to 7.4

Major version = yum command

Minor version = yum update

Example:

```
yum update -y
```

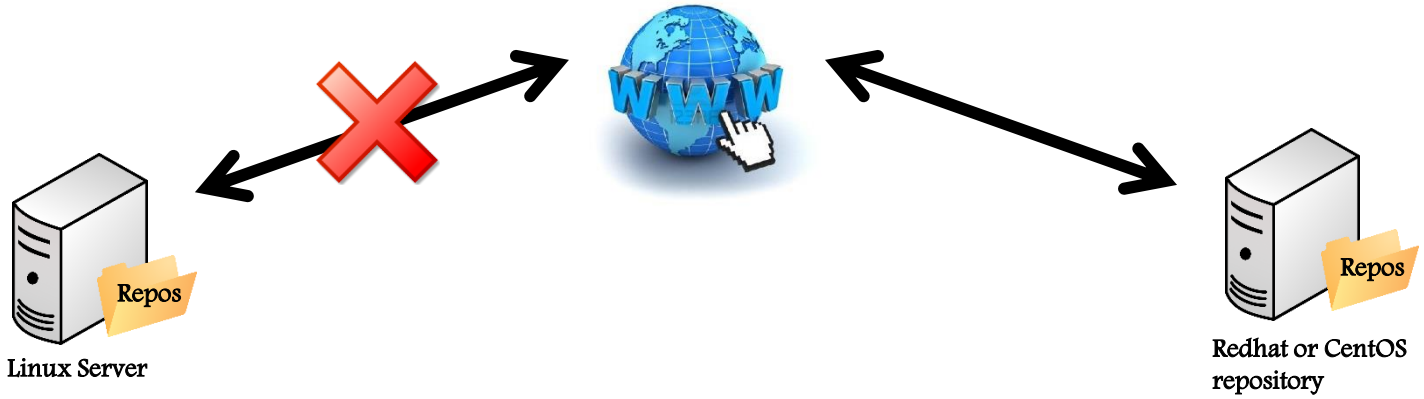
yum update vs. upgrade

upgrade = delete packages

update = preserve

Create Local Repository from DVD

- What is local repository?



- Command

  `createrepo`

SSH and Telnet

- Telnet = Un-secured connection between computers
- SSH = Secured

- Two type of packages for most of the services
  - Client package
  - Server package

SSH without a Password

- SSH is a secure way to login from host A to host B
- Repetitive tasks require login without a password

What we will learn…

- How to generate SSH keys on the server
- Add SSH keys to the client
- Verify by logging through SSH.

By: Imran Afzal

DNS = Domain Name System

- Purpose?

  Hostname to IP (A Record)

  IP to Hostname (PTR Record)

  Hostname to Hostname (CNAME Record)

- Files

  /etc/named.conf

  /var/named

- Service

  systemctl restart named

Download, Install and Configure DNS

- Create a snapshot of your virtual machine
- Setup:
  - Master DNS
  - Secondary or Slave DNS
  - Client

- Domain Name = lab.local
- IP address = My local IP address on enp0s3

- Install DNS package
  - `yum install bind bind-utils -y`
- Configure DNS **(Summary)**
  - `Modify /etc/named.conf`
  - `Create two zone files (forward.lab and reverse.lab)`
  - `Modify DNS file permissions and start the service`

- Revert back to snapshot

By: Imran Afzal

Hostname/IP Lookup

- Commands used for DNS lookup
  - **`nslookup`**
  - **`dig`**

NTP

- **Purpose?**

  Time synchronization

- **File**

  /etc/ntp.conf

- **Service**

  systemctl restart ntpd

- **Command**

  ntpq

chronyd

- Purpose? = Time synchronization
- Package name = chronyd
- Configuration file = /etc/chronyd.conf
- Log file = /var/log/chrony
- Service = systemctl start/restart chronyd
- Program command = chronyd.

Sendmail

- Purpose?

  Send and receive emails

- Files

  /etc/mail/sendmail.mc

  /etc/mail/sendmail.cf

  /etc/mail

- Service

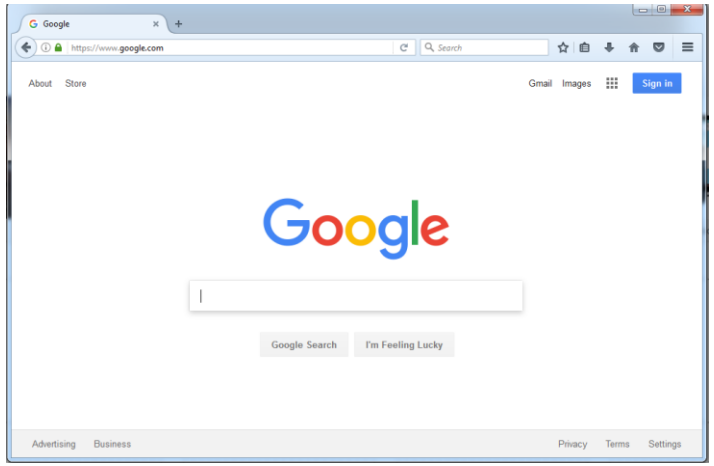
  systemctl restart sendmail

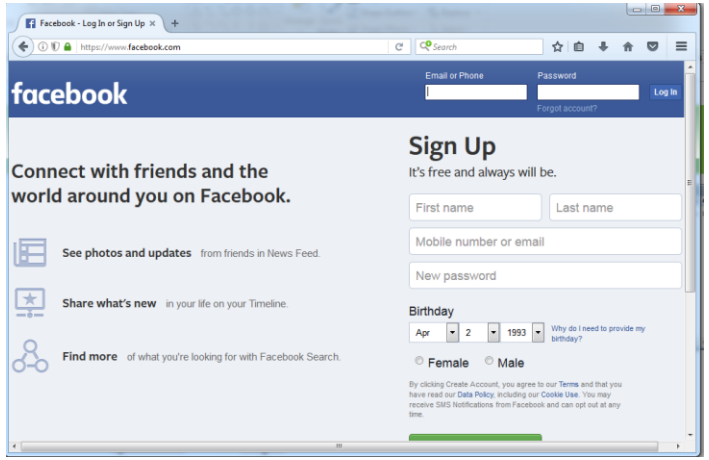
- Command

  mail –s “subject line” email@mydomain.com

Web Server (httpd)

- Purpose = Serve webpages





- Service or Package name = **`httpd`**

- Files = **`/etc/httpd/conf/httpd.conf`**
  = **`/var/www/html/index.html`**

- Log Files = **`/var/log/httpd/`**

- Service

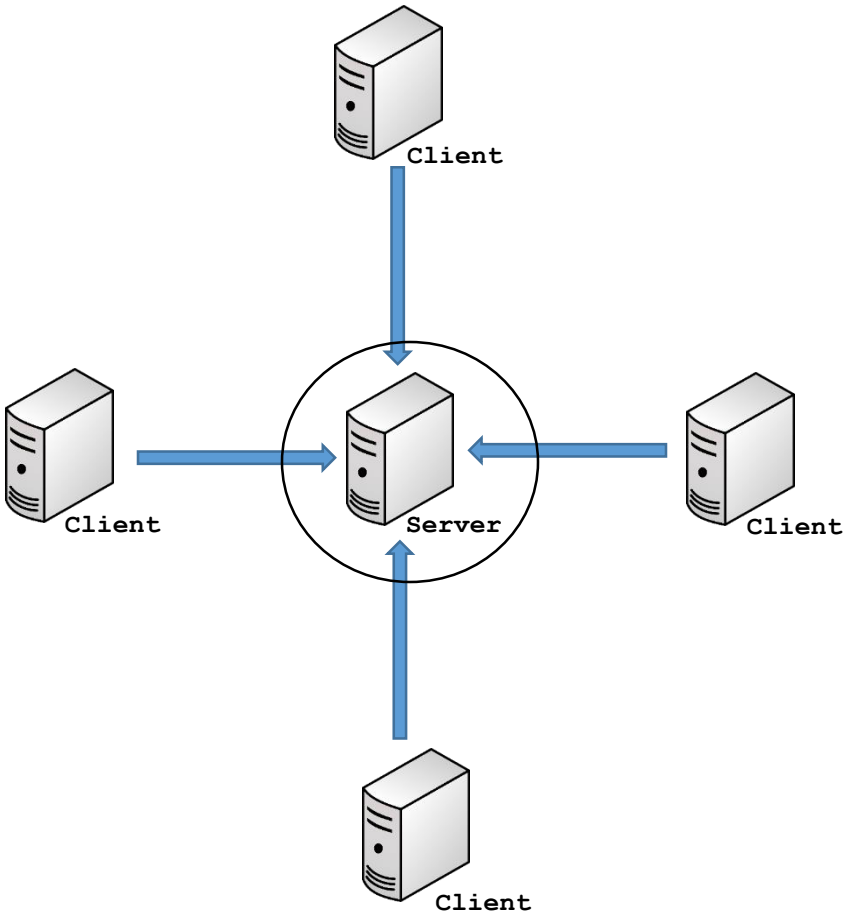
```
systemctl restart httpd
systemctl enable httpd
```

By: Imran Afzal

Central Logger (rsyslog)

- Purpose = Generate logs or collect logs from other servers
- Service or package name = **`rsyslog`**
- Configuration file= **`/etc/syslog.conf`**
- Service

```
systemctl restart rsyslog
systemctl enable rsyslog
```



Network File System (NFS)

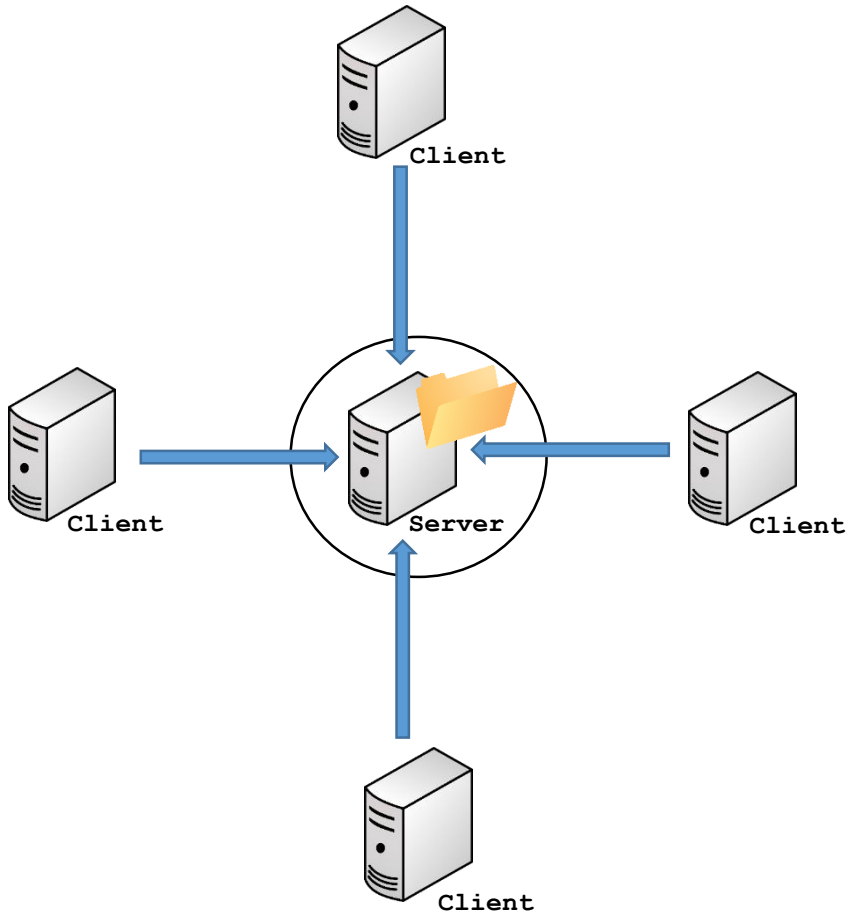
- Purpose = Share files or directories (filesystem)
- Service or package name = **nfs-utils**
- Configuration file =

  /etc/fstab, /etc/exports, /etc/sysconfig/nfs

- Service

  systemctl restart nfs-server

  systemctl enable nfs-server



Linux OS Hardening

- User Account
- Remove un-wanted packages
- Stop un-used Services
- Check on Listening Ports
- Secure SSH Configuration
- Enable Firewall (iptables/firewalld)
- Enable SELinux
- Change Listening Services Port Numbers
- Keep your OS up to date (security patching)

OpenLDAP Installation

- What is OpenLDAP?
- OpenLDAP Service
  - `slapd`
- Start or stop the service
  - `systemctl start slapd`
  - `systemctl enable slapd`
- Configuration Files
  - `/etc/openldap/slapd.d`

Trace Network Traffic (traceroute)

- The traceroute command is used in Linux to map the journey that a packet of information undertakes from its source to its destination. One use for traceroute is to locate when data loss occurs throughout a network, which could signify a node that's down.
- Because each hop in the record reflects a new server or router between the originating PC and the intended target, reviewing the results of a traceroute scan also lets you identify slow points that may adversely affect your network traffic.

- Example

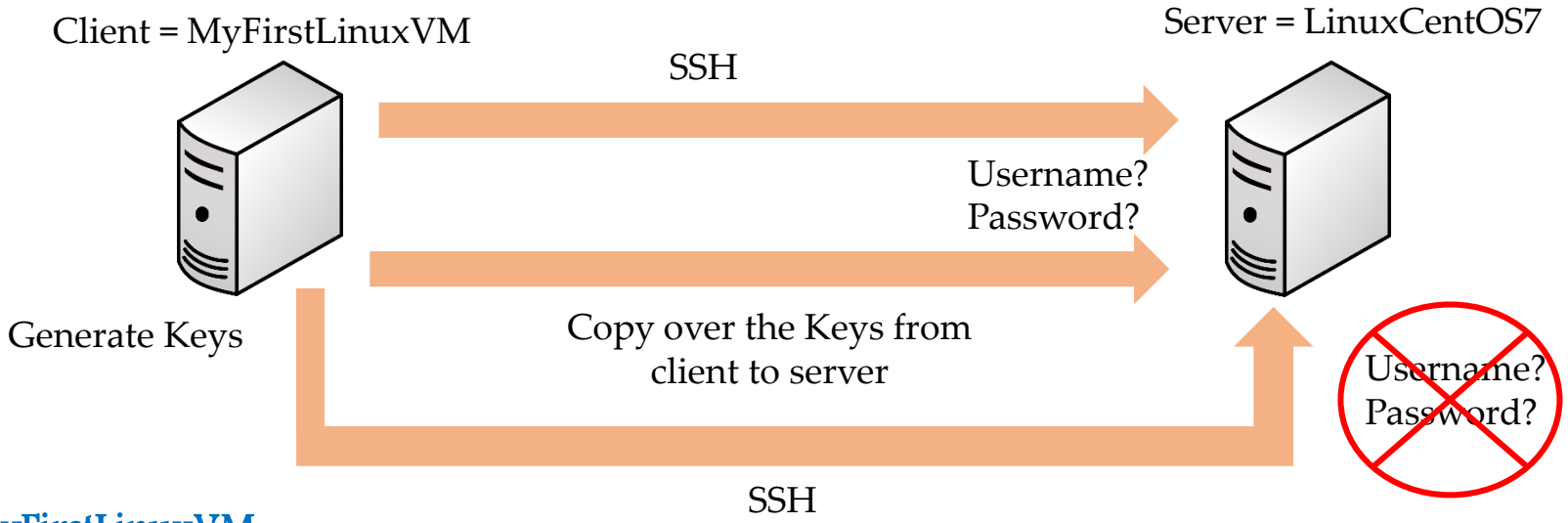
```
# traceroute www.google.com
```

Access Remote Server without Password (SSH-Keys)

- Two reasons to access a remote machine
  - Repetitive logins
  - Automation through scripts

- Keys are generated at user level
  - iafzal
  - root

Access Remote Server without Password (SSH-Keys)



Client = MyFirstLinuxVM

Step 1 — Generate the Key

```
# ssh-keygen
```

Step 2 — Copy the Key to the server

```
# ssh-copy-id root@192.168.1.x
```

Step 3 — Login from client to server

```
# ssh root@192.168.1.x
# ssh -l root 192.168.1.x
```