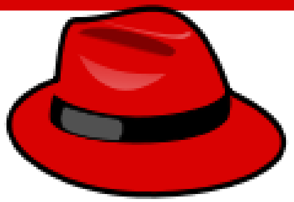
Red Hat

Welcome to Section 3

Redhat System Administration (RH124)

By: Imran Afzal
www.utclisolutions.com

Get started with Red Hat Enterprise Linux



Linux is everywhere, cloud, smart phones, airplanes, smart TV, gadgets etc.

We will learn…

- Open source
- Linux distributions
- Red Hat Enterprise Linux

Get started with Red Hat Enterprise Linux

- **Open source**
  - Open-source software is computer software that is released under a license in which the copyright holder grants users the rights to use, study, change, and distribute the software and its source code to anyone and for any purpose *(Wikipedia)*

  - Open source software is developed in a decentralized and collaborative way, relying on peer review and community production. Open source software is often cheaper, more flexible, and has more longevity than its proprietary peers because it is developed by communities rather than a single author or company

  - Linux is a free, open source operating system (OS), released under the GNU General Public License (GPL). It's also become the largest open source software project in the world

  - Red Hat Enterprise Linux is built from open source components. The kernel itself and the supporting software are all open source. However, Red Hat has built infrastructure, support, and a suite of services that will let you license their branded version of enterprise Linux and use it in production.

Get started with Red Hat Enterprise Linux

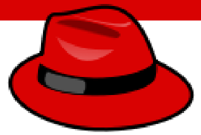
- **Linux distribution**
  - A Linux distribution is an operating system composed of the Linux kernel, GNU tools, additional software and a package manager.

Example of Linux distribution OS

Red Hat
ubuntu
fedora
CentOS
suse
KALI LINUX

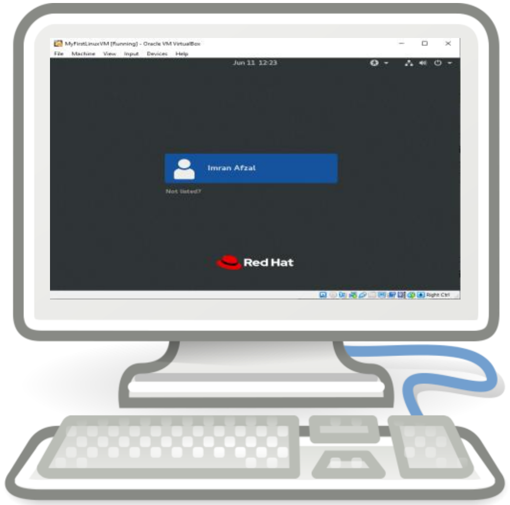
By: Imran Afzal
www.utclisolutions.com

Get started with Red Hat Enterprise Linux

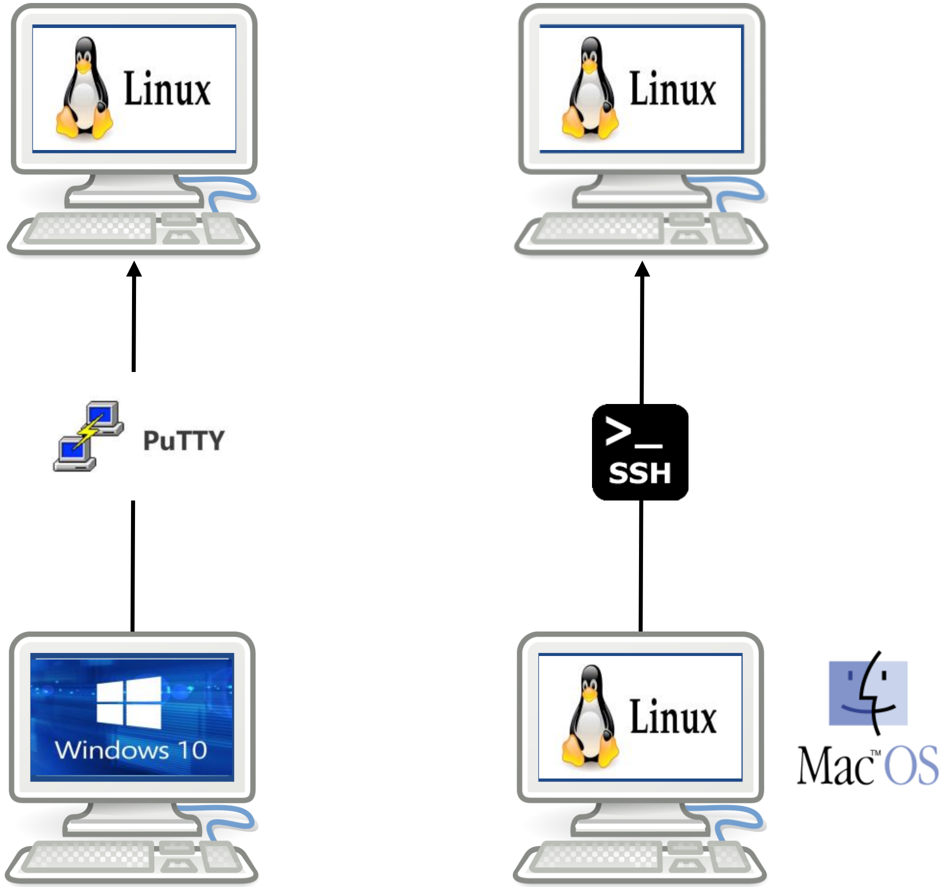


- **Red hat Linux**
  - Red Hat is one of the leading contributors to the Linux kernel and associated technologies in the greater open source community
  - IBM acquired Red hat in 2018 for $34billion
  - Red hat Linux current version is 8
  - Product Lifecycle of 10 years
  - Download and use any supported version of the Red Hat Enterprise Linux software, meaning that you may upgrade to the latest version for no additional cost
  - Allows live kernel patching, avoiding the need for a system reboot
  - Access to Red Hat Enterprise Linux documentation
  - Access to Red Hat Customer Portal Labs.

Linux System Access (Command Line and GUI)



Console



By: Imran Afzal
www.utclisolutions.com

Manage Files From The Command Line

Introduction to Filesystem

- What is a Filesystem?
    - It is a system used by an operating system to manage files. The system controls how data is saved or retrieved

Manage Files From The Command Line

Introduction to Filesystem

- What is a Filesystem?
  - It is a system used by an operating system to manage files. The system controls how data is saved or retrieved

Shirts

Accessories

Skirts

Jackets

Shoes

Pants

Manage Files From The Command Line

Introduction to Filesystem

- Operating system stores files and directories in an organized and structured way
  - System configuration file = Folder A
  - User files = Folder B
  - Log files = Folder C
  - Commands or scripts = Folder D and so on

- There are many different types of filesystems. In general, improvements have been made to filesystems with new releases of operating systems and each new filesystem has been given a different name
  - e.g. **ext3, ext4, xfs, NTFS, FAT etc.**

Manage Files From The Command Line

Directory Listing Attributes

Total columns = 9

Type	# of Links	Owner	Group	Size	Month	Day	Time	Name
drwxr-xr-x.	21	root	root	4096	Feb	27	13:33	var
lrwxrwxrwx.	1	root	root	7	Feb	27	13:15	bin
-rw-r—r--	1	root	root	0	Mar	2	11:15	testfile

The second column is the number of hard links to the file. For a directory, the number of hard links is the number of immediate subdirectories it has plus its parent directory and itself

By: Imran Afzal
www.utclisolutions.com

Manage Files From The Command Line

Creating Files and Directories

- Creating Files
  - ✓ **`touch`**
  - ✓ **`cp`**
  - ✓ **`vi`**

- Creating Directories
  - ✓ **`mkdir`**

Manage Files From The Command Line

File Maintenance Commands

- cp
- rm
- mv
- mkdir
- rmdir or rm -r
- chgrp
- chown

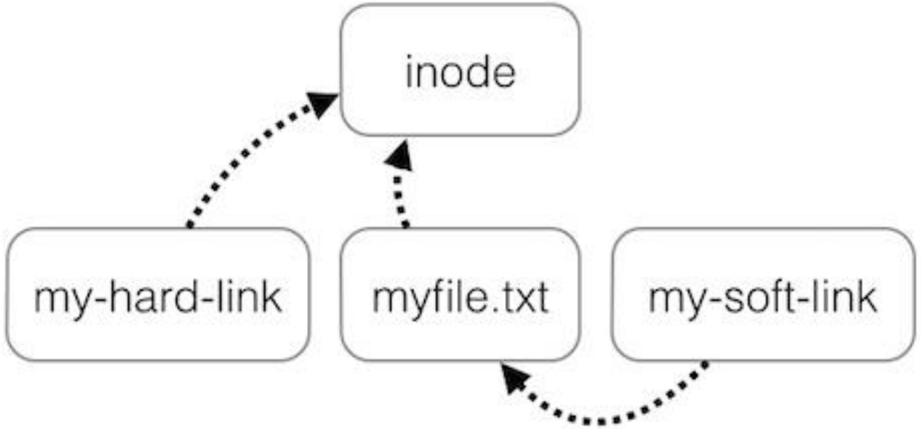
By: Imran Afzal
www.utclisolutions.com

Manage Files From The Command Line

Soft and Hard Links

- inode = Pointer or number of a file on the hard disk
- Soft Link = Link will be removed if file is removed or renamed
- Hard Link = Deleting renaming or moving the original file will not affect the hard link

  - ln
  - ln -s



By: Imran Afzal
www.utclisolutions.com

Manage Files From The Command Line

Input and Output Redirects

- There are 3 redirects in Linux
  1. Standard input (**`stdin`**) and it has file descriptor number as 0
  2. Standard output (**`stdout`**) and it has file descriptor number as 1
  3. Standard error (**`stderr`**) and it has file descriptor number as 2

- Output (**stdout**) - 1
  - By default when running a command its output goes to the terminal
  - The output of a command can be routed to a file using > symbol
    - E.g.

      ```
      ls -l > listings
      pwd > findpath
      ```
  - If using the same file for additional output or to append to the same file then use >>
    - E.g.

      ```
      ls -la >> listings
      echo “Hello World”  >> findpath.
      ```

Manage Files From The Command Line

Input and Output Redirects

- Input (**stdin**) - 0
  - Input is used when feeding file contents to a file
    - E.g.

```
cat < listings
mail -s "Office memo" allusers@abc.com < memoletter
```

- Error (**stderr)** - 2
  - When a command is executed we use a keyboard and that is also considered (stdin -0)
  - That command output goes on the monitor and that output is (stdout – 1)
  - If the command produced any error on the screen then it is considered (stderr – 2)
    - We can use redirects to route errors from the screen
      - E.g

```
ls -l /root 2> errorfile
telnet localhost 2> errorfile.
```

By: Imran Afzal
www.utclisolutions.com

Manage Files From The Command Line

Pipes (|)

- A pipe is used by the shell to connect the output of one command directly to the input of another command.

The symbol for a pipe is the vertical bar (|). The command syntax is:

```
command1 [arguments]  |  command2 [arguments]
```

Manage Files From The Command Line

Pipes (|)

```
ls -l          |          more
```

By: Imran Afzal
www.utclisolutions.com

Get Help in Red Hat Enterprise Linux

- There are 3 types of help commands
  - **`whatis`** command
  - command **`--help`**
  - **`man`** command

Create, View, and Edit Text Files

Linux File Editor

- A text editor is a program which enables you to create and manipulate data (text) in a Linux file

- There are several standard text editors available on most Linux systems

• vi	-	Visual editor
• ed	-	Standard line editor
• ex	-	Extended line editor
• emacs	-	A full screen editor
• pico	-	Beginner's editor
• vim	-	Advance version of vi

- Our editor = vi (available in almost every Linux distribution)

Create, View, and Edit Text Files

Introduction to vi Editor

- vi supplies commands for:
  - Inserting and deleting text
  - Replacing text
  - Moving around the file
  - Finding and substituting strings
  - Cutting and pasting text

- Most common keys:
  - `i – insert`
  - `Esc – Escape out of any mode`
  - `r – replace`
  - `d – delete`
  - `:q! – quit without saving`
  - `:wq! – quit and save`

User Account Management

Commands

- useradd
- groupadd
- userdel
- groupdel
- usermod

Files

- /etc/passwd
- /etc/group
- /etc/shadow

Example:

```
useradd -g superheros -s /bin/bash -c “user description” -m -d
/home/spiderman spiderman
```

The /etc/login.def File

- The chage command – per user
  - **Example**

```
chage [-m mindays] [-M maxdays] [-d lastday] [-I inactive] [-E
expiredate] [-W warndays] user
```

- File = /etc/login.def
  - PASS_MAX_DAYS   99999
  - PASS_MIN_DAYS   0
  - PASS_MIN_LEN   5
  - PASS_WARN_AGE   7

Manage Local Users and Groups

The chage Command

- The chage command – per user

  - **Example**

```
chage [-d lastday] [-m mindays] [-M maxdays] [-W warndays] [-I
inactive] [-E expiredate] user
```

-d = 3. Last password change (lastchanged) : Days since Jan 1, 1970 that password was last changed
-m = 4. Minimum : The minimum number of days required between password changes i.e. the number of days left before the user is allowed to change his/her password
-M = 5. Maximum : The maximum number of days the password is valid (after that user is forced to change his/her password)
-W = 6. Warn : The number of days before password is to expire that user is warned that his/her password must be changed
-I = 7. Inactive : The number of days after password expires that account is disabled
-E = 8. Expire : days since Jan 1, 1970 that account is disabled i.e. an absolute date specifying when the login may no longer be used.

By: Imran Afzal
www.utclisolutions.com

Switch Users and sudo Access

Commands

- `su - username`
- `sudo command`
- `visudo`

File

- `/etc/sudoers`

Control Access to Files

File Permissions

- UNIX is a multi-user system. Every file and directory in your account can be protected from or made accessible to other users by changing its access permissions. Every user has responsibility for controlling access to their files.

- Permissions for a file or directory may be restricted to by types
- There are 3 type of permissions
  - r - read
  - w - write
  - x - exeawke = running a program
- Each permission (rwx) can be controlled at three levels:
  - u - user = yourself
  - g - group = can be people in the same project
  - o - other = everyone on the system
- File or Directory permission can be displayed by running ls –l command
  - -rwxrwxrwx
- Command to change permission
  - chmod

Monitor and Manage Processes

- When an operating system boots up many programs get loaded into system memory. These processes or programs need to be managed and monitored because they consume mainly 3 system resources like CPU, memory and disk space
- Here are a few monitoring commands to manage system resources
  - **`df`**
  - **`du`**
  - **`uptime`**
  - **`top`**
  - **`free`**
  - **`lsof`**
  - **`tcpdump`**
  - **`netstat`**
  - **`ps`**
  - **`kill`**
  - **`Some other commands are vmstat, iostat, iftop etc.`**

By: Imran Afzal
www.utclisolutions.com

Control Services and Daemons

- Service or application when started creates processes and when those processes run continuously in the background, they become daemons
- Most services are daemons
- Services are controlled by systemctl
- systemctl is a systemd utility that is responsible for controlling the systemd system and service manager
- systemd is a collection of system management daemons, utilities, and libraries which serves as a replacement of System V init daemon
- systemd is the parent process of most of the daemons
- The command to control services = **`systemctl.`**

Control Services and Daemons

- Check if systemd installed in your system

```
systemctl --version
```

- Check if systemd is running

```
ps -ef | grep system
```

- Check all running services

```
systemctl --all
```

- To check the status, start, stop and restart a service

```
systemctl status|start|stop|restart application.service
```

- To reload the configuration of a service

```
systemctl reload application.service
```

- To enable or disable a service at boot time

```
systemctl enable|disable application.service
```

- To enable or disable a service completely (upon another service dependency)

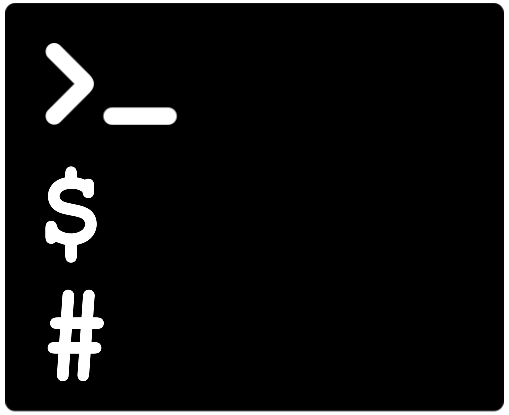
```
systemctl mask|unmask application.service
```

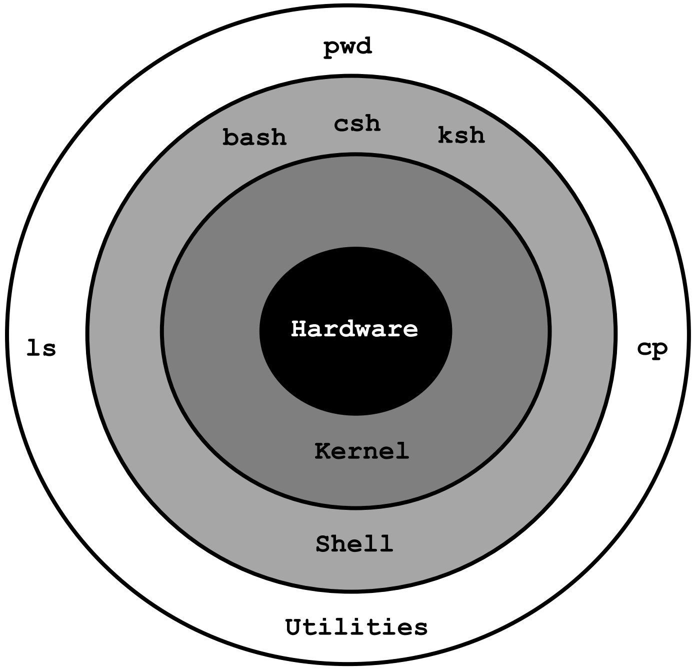
By: Imran Afzal
www.utclisolutions.com

Configure and Secure SSH

- **SSH**
  - SSH stands for secure shell

provides you with an interface to the Linux system. It takes in your commands and translate them to kernel to manage hardware





- Open SSH is a package/software
- Its service daemon is sshd
- SSH port # 22

Configure and Secure SSH

- SSH itself is secure, meaning communication through SSH is always encrypted, but there should be some additional configuration can be done to make it more secure
- Following are the most common configuration an administrator should take to secure SSH

✓ Configure Idle Timeout Interval

Avoid having an unattended SSH session, you can set an Idle timeout interval

- Become root
- Edit your **`/etc/ssh/sshd_config`** file and add the following line:
- **`ClientAliveInterval 600`**
- **`ClientAliveCountMax 0`**
- **`# systemctl restart sshd`**

The idle timeout interval you are setting is in seconds (600 secs = 10 minutes). Once the interval has passed, the idle user will be automatically logged out

Configure and Secure SSH

✓ **Disable root login**

Disabling root login should be one of the measures you should take when setting up the system for the first time. It disable any user to login to the system with root account

- Become root
- Edit your **`/etc/ssh/sshd_config`** file and replace PermitRootLogin yes to no
- **`PermitRootLogin no`**
- **`# systemctl restart sshd`**

Configure and Secure SSH

✓ **Disable Empty Passwords**

You need to prevent remote logins from accounts with empty passwords for added security.

- Become root
- Edit your **`/etc/ssh/sshd_config`** file and remove # from the following line
- **`PermitEmptyPasswords no`**
- **`# systemctl restart sshd`**

Configure and Secure SSH

✓ Limit Users’ SSH Access

To provide another layer of security, you should limit your SSH logins to only certain users who need remote access

- Become root
- Edit your **`/etc/ssh/sshd_config`** file and add
- **`AllowUsers user1 user2`**
- **`# systemctl restart sshd`**

Configure and Secure SSH

✓ **Use a different port**

By default SSH port runs on 22. Most hackers looking for any open SSH servers will look for port 22 and changing can make the system much more secure

- Become root
- Edit your **`/etc/ssh/sshd_config`** file and remove # from the following line and change the port number
- **`Port 22`**
- **`# systemctl restart sshd`**

By: Imran Afzal
www.utclisolutions.com

Configure and Secure SSH

- ✓ **SSH-Keys - Access Remote Server without Password**

Watch the next video

Configure and Secure SSH

Access Remote Server without Password (SSH-Keys)

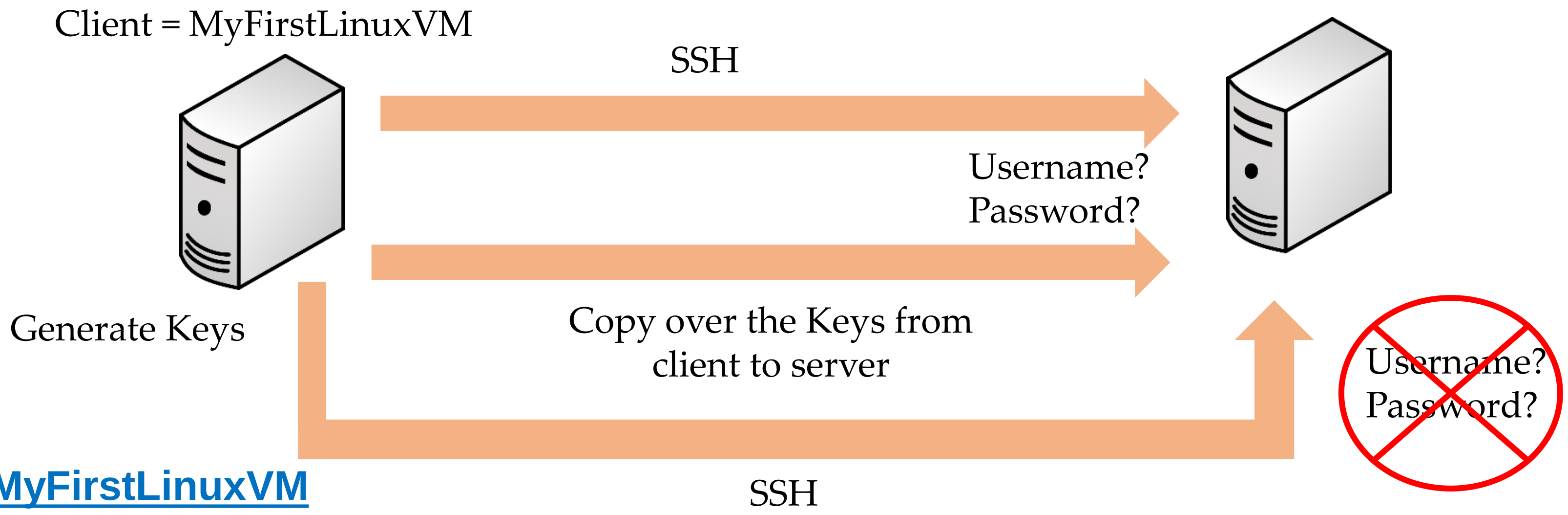
- Two reasons to access a remote machine
  - Repetitive logins
  - Automation through scripts

- Keys are generated at user level
  - iafzal
  - root

By: Imran Afzal
www.utclisolutions.com

Configure and Secure SSH

Access Remote Server without Password (SSH-Keys)



Client = MyFirstLinuxVM

Step 1 — Generate the Key

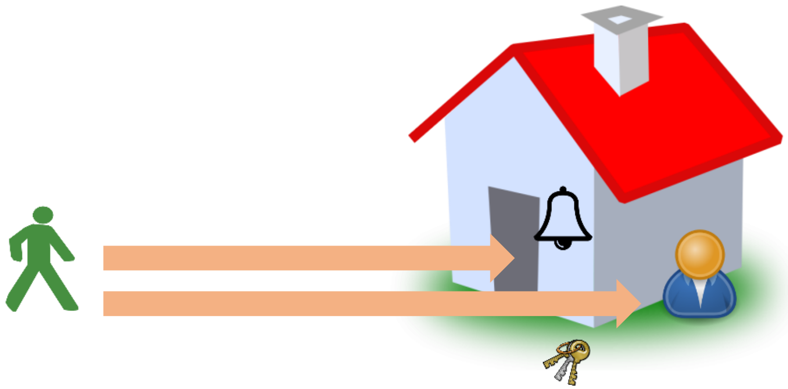
```
# ssh-keygen
```

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
```



By: Imran Afzal
www.utclisolutions.com

Analyze and Store logs

Log Monitoring

Another and most important way of system administration is log monitor

Log Directory = `/var/log`

- `boot`
- `chronyd = NTP`
- `cron`
- `maillog`
- `secure`
- `messages`
- `httpd`

Analyze and Store logs

Maintaining Accurate Time

- Maintaining accurate system time is critical for log file analysis across multiple systems
- Also having accurate time on a system is requirement for sensitive applications such as database in production environment
- The network time protocol (NTP) is a standard way for machines to provide and synchronize the time to the NTP server
- An NTP server is a dedicated machine/computer which responds to clients for time synchronization
- chronyd is a NTP service used for time synchronization in the newer Linux versions.

Analyze and Store logs

Maintaining Accurate Time

- Command to show system time/date
  - `date`
- Command for time/date and NTP setting
  - `timedatectl`
- To get help
  - `timedatectl --help`
- To view list of time zones
  - `timedatectl list-timezones`
- To set a time zone
  - `timedatectl set-timezone America/New_York`
- To set time or to set time and date
  - `timedatectl set-time HH:MM:SS`
  - `timedatectl set-time ‘2021-08-18 20:15:50’`
- To enable NTP synchronization
  - `timedatectl set-ntp true`

Analyze and Store logs

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.

Manage Linux Networking

What we will learn in this lecture…

- Static vs. dynamic IP
- OS network components (Network interface, subnet mask, gateway, MAC address etc.)
- Getting started with NetworkManager
- Network configuration methods
  - **`nmtui, nmcli, nm-connection-editor and GNOME Settings`**
- Network files and basic commands.

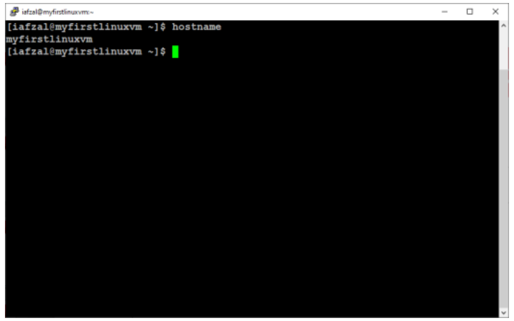
Manage Linux Networking

✓ Static IP vs. DHCP

- IP stands for internet protocol which is assigned to your computer so it can access the network. Private IP is assigned for internal communication and public is for the internet/external communication

- Static → does not change
- Dynamic → changes after system reboot

- Let's look at our Linux machine…



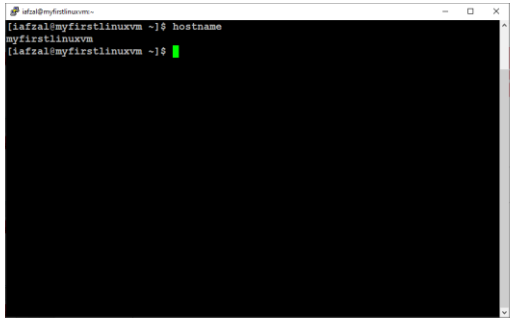
```
[iafzal@myfirstlinuxvm ~]$ hostname
myfirstlinuxvm
[iafzal@myfirstlinuxvm ~]$
```

Manage Linux Networking

✓ OS Network Components

- Network interface
- MAC address
- Subnet mask
- Gateway
- DNS (Domain name system)

- Let’s look at our Linux machine…



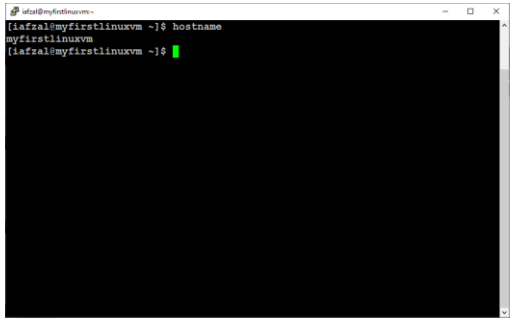
```
[iafzal@myfirstlinuxvm ~]$ hostname
myfirstlinuxvm
[iafzal@myfirstlinuxvm ~]$
```

Manage Linux Networking

✓ Getting started with `NetworkManager`

- NetworkManager is a service and set of tools designed specifically to make it easier to manage the networking configuration on Linux systems and is the default network management service on RHEL 8
- It makes network management easier
- It provides easy setup of connection to the user
- NetworkManager offers management through different tools such as **`GUI, nmtui, and nmcli`**

- Let's practice in our Linux machine…



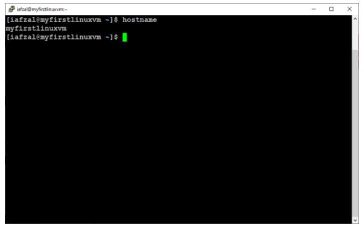
```
[iafzal@myfirstlinuxvm ~]$ hostname
myfirstlinuxvm
[iafzal@myfirstlinuxvm ~]$
```

Manage Linux Networking

✓ Network configuration methods

- **`nmcli`** – Short for network manager command line interface. This tool is useful when access to a graphical environment is not available and can also be used within scripts to make network configuration changes
- **`nmtui`** – Short for network manager text user interface. This tool can be run within any terminal window and allows changes to be made by making menu selections and entering data
- **`nm-connection-editor`** - A full graphical management tool providing access to most of the NetworkManager configuration options. It can only be accessed through the desktop or console
- **`GNOME Settings`** - The network screen of the GNOME desktop settings application allows basic network management tasks to be performed

- Let's practice in our Linux machine…



```
[iafzal@myfirstlinuxvm ~]$ hostname
myfirstlinuxvm
[iafzal@myfirstlinuxvm ~]$
```

Manage Linux Networking

✓ Network Files and Basic Commands

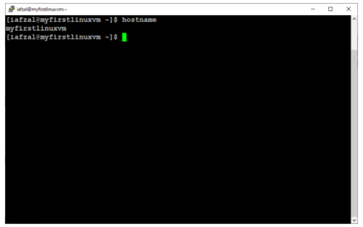
Files:

```
/etc/sysconfig/network-scripts
/etc/hosts
/etc/hostname
/etc/resolv.conf
/etc/nsswitch.conf
```

Commands:

```
ping
ifconfig or ip
ifup or ifdown
netstat
traceroute
tcpdump
nslookup or dig
ethtool
```

- Let’s practice in our Linux machine…



```
[iafzal@myfirstlinuxvm ~]$ hostname
myfirstlinuxvm
[iafzal@myfirstlinuxvm ~]$
```

Archive and Transfer Files

- ✓ tar, compress and uncompress
- ✓ ftp
- ✓ scp

Archive and Transfer Files

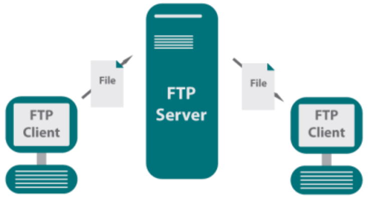
Compress and un-Compress Files

- `tar`
- `gzip`
- `gzip –d OR gunzip`

Archive and Transfer Files

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)*



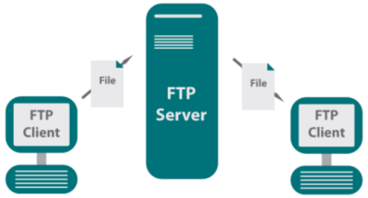
- Protocol = Set of rules used by computers to communicate

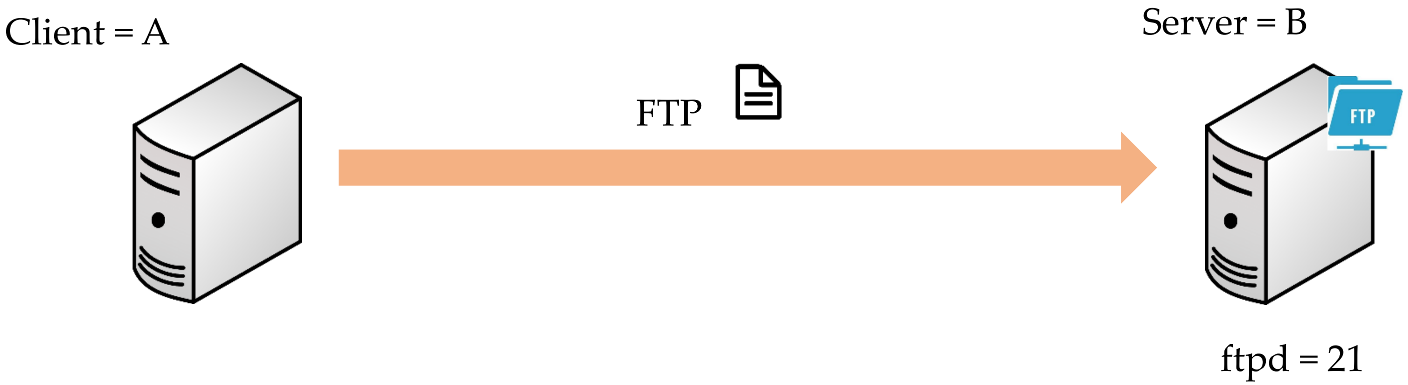
- Default FTP Port = 21

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

Archive and Transfer Files

FTP – File Transfer Protocol




Client = A

FTP

Server = B

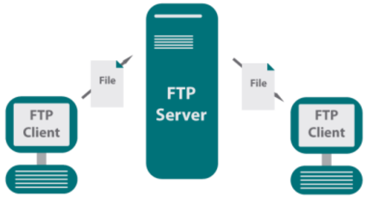
ftpd = 21

By: Imran Afzal

Archive and Transfer Files

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*

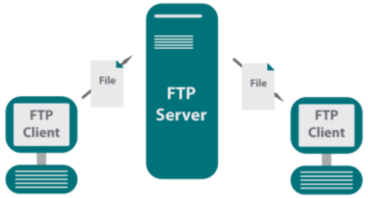
  - ## Uncomment - Enter your Welcome message - This is optional ##
    - *ftpd_banner=Welcome to UNIXMEN FTP service.*

  - ## 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).*

Archive and Transfer Files

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.`

By: Imran Afzal

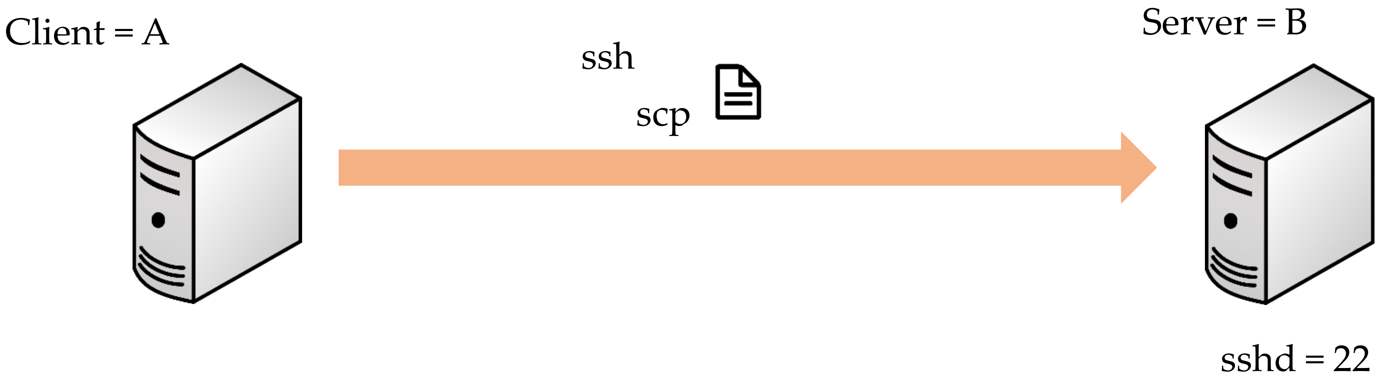
Archive and Transfer Files

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`**

Archive and Transfer Files

SCP – Secure Copy Protocol



By: Imran Afzal

Archive and Transfer Files

SCP – Secure Copy Protocol

- 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`

Install and Update Software Packages

- Software is any application that you run on your computer
- Package is a container that contain the software related programs, files and executables

We will learn…

✓ Linux package management using **`yum/dnf`** and **`rpm`** command

✓ System update and patch management (yum update vs. upgrade)

✓ Advance package management

System Updates and Repos

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

Install and Update Software Packages

System Upgrade/Patch Management

- Two type of upgrades

  Major version = 5, 6, 7

  Minor version = 7.3 to 7.4

Major version = yum ✗ mmand

Minor version = yum update ✓

Example:

```
yum update -y
```

```
yum update vs. upgrade
```

`upgrade` = delete packages

`update` = preserve

Access Linux files systems

- Filesystem is a structured way where all files and directories are stored
- To access those files, we need navigation tools
- Following are the basic tools or commands to access Linux file system

    - **`ls`**
    - **`cd`**
    - **`pwd`**
    - **`df`**
    - **`du`**
    - **`fdisk`**
    - **`Absolute and relative path`** (absolute path always begins with /)
    - **`Tilde ~`**
    - **`. and ..`**

Analyze Servers and get Support

- Anytime you have an issue with your Linux Redhat server you will have to through the monitoring commands such as top, free, df, du etc. A system administrator should also review the system logs in `/var/log` directory and then reach out to Redhat technical support for more help
- Redhat has made it easier for system administrator to use a web-based application named **Cockpit** to manage and analyze server
- To get support from Redhat, a system administrator can run the utility `sosreport` or in newer version `"sos report"` on Linux system as root which will collect the logs and configuration file and then transfer them over to Redhat support server. Now with Cockpit application, the report can be generated at the web-based portal
- Cockpit web-based interface provides many other functionality aside from monitoring and getting support from Redhat

- Let's deep dive into Cockpit in the next slide…

Analyze Servers and get Support

Cockpit

- Cockpit is a server administration tool sponsored by Red Hat, focused on providing a modern-looking and user-friendly interface to manage and administer servers
- Cockpit is the easy-to-use, integrated, glanceable, and open web-based interface for your servers
- The application is available in most of the Linux distributions such as, CentOS, Redhat, Ubuntu and Fedora
- It is installed in Redhat 8 by default and it is optional in version 7
- It can monitor system resources, add or remove accounts, monitor system usage, shut down the system and perform quite a few other tasks all through a very accessible web connection

Analyze Servers and get Support

Install, Configure and Manage Cockpit

- Check for network connectivity
  - `ping www.google.com`

- Install cockpit package as root
  - `yum/dnf install cockpit -y` *(For RH or CentOS)*
  - `apt-get install cockpit` *(For Ubuntu)*

- Start and enable the service
  - `systemctl start|enable cockpit`

- Check the status of the service
  - `systemctl status cockpit`

- Access the web-interface
  - `https://192.168.1.x:9090`

By: Imran Afzal
www.utclisolutions.com