**CHAPTER 9** **Controlling service with SYSTEMD**

Concept is similar to MS-Windows Services where we performed task.

(**stop, start, restart**, **Boot up** --> **Automatic, Manual, Diabled**)

**What is SYSTEMD:**

1. Introduced in RHEL 7

2. Used to managed services as same concept as MS-Windows service

3. PID=1

4. Increaces boot up speed

5. Service dependencies (what other services that need to be started before the main serices starts)

6. Tracking Method from Linux cgroup

7. The main command is "**systemctl**"

8. used to manage many "UNITS" such as "services", "devices", "mount", "socket", "slice", "target".

9. Example, to specify use "**systemctl --type=service**"

**Compare to MS-Windows:**

1. enabled = Automatic

2. disable = Manual

3. mask/unmask = Disable

**CHAPTER 10** **Configuring and securing ssh**

--> ssh Protocol used for remote access into RHEL/Linux/Unix/Windows servers using commandline

**Covered Sections:**

1. **ssh concept**

2. **ssh passwordless login** (for use of some implementation such for **Nagios Monitoring Product**)

3. **hardening sshd server**

**SSH Concept:**

1. Client will use the command "ssh" or "Putty.exe" from MS-Windows

--> "ssh username@hostname" or "ssh usename@ip\_address(172.25.250.9)"

2. **There will be an exhange of PKI(Public Key Infratructure)** --> RSA or DSA (public and private key) --> By default RHEL uses RSA keys.

3. We can also generate RSA or DSA keys and have it copy over to the sshd server for passwordless login.

**SSH Passwordless login:**

1. generate rsa or dsa key

"**ssh-keygen -t dsa**"

--> Will be added into the ~/.ssh/\*

2. Copy the newly created keys into the sshd server(servera)

--> "**ssh-copy-id username@servera**"

3. Test the passwordless login

--> **ssh username@servera** (you should get passwordless login)

**SSHD hardering:**

1. ssh protocol is the only primary method used for remote access into RHEL/Unix/sshd server.

2. configure the file "**/etc/ssh/sshd\_config**" on the sshd server. Ie servera or serverb

--> Prevent "**root**" user from being able to ssh into servera or serverb

--> Prevent password login (every users that exist in servera or serverb cannot login)

3. sshd service restart on either one of those two server where the "/etc/ssh/sshd\_config" file has been configured.

4. Test the newly harderned servera or serverb

**CHAPTER 11** **Anaylsing and Storing logs**

Similiar Concept to MS-Windows-Event-Viewer

**Covered Topics:**

1. How to analyse logs files

2. How to configure rsyslog

3. Introduction to Journald (journalctl command)

4. Configuring NTP using Chrony

**How to Anaylyse Logs:**

1. **systemctl status rsyslog.service**

2. config file for rsyslog is **/etc/rsyslog.conf**

3. locations of all the log files **/var/log/\*.\***

4. to prevent the log directory from grown to big --> **/var/log/\*.\*** --> **/etc/logrotate.conf**

5. The first log files to analyse is "**/var/log/messages**" --> Always

**Introduction to Journald**

1. Comes together with **systemd as of RHEL 7.x**

2. Its **NOT** a replacement for **rsyslog**

3. It compliment rsyslog

4. It provides a mechanism for easy to analyse your rsyslog files with **/var/log/\*.\***

5. The main command is "**journalctl**"

**Configuring NTP with Chronyd:**

What is NTP(**Network Time Protocol**)?

--> Mechanise to maintain acurate time for all you servers, apps, etc

--> Network base

--> Every NTP server set up is typical an NTP client of other NTP servers out in the internet.

--> NTP Stratum

1. **systemctl status chronyd.service**

2. the config file is found in

3. Add an external NTP server to the existing NTP list within that config file.

4. Restart chronyd service

5. use command "**chronyc sources -v**" to verify the new NTP server that you 've just added