Red Hat System Administration I

UNIT 10

Analyzing and Storing Logs

Objectives

- Describe the basic syslog architecture in Red Hat Enterprise Linux 7.
- Interpret entries in relevant syslog files to troubleshoot problems or review system status.
- Find and interpret log entries in the systemd journal to troubleshoot problems or review system status.
- Configure systemd-journald to store its journal on disk rather than in memory.
- Maintain accurate time synchronization and time zone configuration to ensure correct timestamps in system logs.

System logging

Log file	Purpose
/var/log/messages	Most syslog messages are logged here. The exceptions are messages related to authentication and email processing, that periodically run jobs, and those which are purely debugging-related.
/var/log/secure	The log file for security and authentication-related messages and errors.
/var/log/maillog	The log file with mail server-related messages.
/var/log/cron	The log file related to periodically executed tasks.
/var/log/boot.log	Messages related to system startup are logged here.

Sample rules section of rsyslog.conf

```
#### RULES ####

# Log all kernel messages to the console.
# Logging much else clutters up the screen.
#kern.*                                                 /dev/console

# Log anything (except mail) of level info or higher.
# Don't log private authentication messages!
*.info;mail.none;authpriv.none;cron.none                /var/log/messages

# The authpriv file has restricted access.
authpriv.*                                              /var/log/secure

# Log all the mail messages in one place.
mail.*                                                  -/var/log/maillog
```

Finding events with journalctl

- journalctl
  - -n 5
  - -p err
  - -f
  - --since today --until "2014-2-14 12:00:00"
  - -o verbose
  - _SYSTEMD_UNIT=sshd.service _PID=1182

Store the system journal permanently

```
[root@serverX ~]#mkdir /var/log/journal
[root@serverX ~]#chown root:systemd-journal /var/log/journal
[root@serverX ~]#chmod 2755 /var/log/journal
Send the USR1 signal to the systemd-journald or reboot serverX.
[root@serverX ~]#killall -USR1 systemd-journald
[root@serverX ~]#ls /var/log/journal/4513ad59a3b442ffa4b7ea88343fa55f
system.journal user-1000.journal
```

Set local clocks and time zone

- timedatectl
- timedatectl list-timezones
- timedatectl set-timezone America/P
- timedatectl set-time 9:00:00
- timedatectl set-ntp true

Configuring and monitoring chronyd

- vim /etc/chrony.conf
  - server classroom.example.com iburst
- systemctl restart chronyd
- chronyc sources -v

Lab

<lab 1>
Your serverX machine has been relocated to Jamaica. Change the time zone on the serverX machine to Jamaica and verify the time zone has been changed properly
<lab 2>
Display all systemd journal entries recorded in the last 30 minutes on serverX
<lab 3>
Configure rsyslogd by adding a rule to the newly created configuration file /etc/rsyslog.d/auth-errors.conf to log all security and authentication messages with the priority alert and higher to the/var/log/auth-errors file as well. Test the newly added log directive with the logger command.

That's all