AINUX

— TASTE OF LINUX —

WELCOME TO THE WORLD OF LINUX

DAY - 16

CREATED BY : ARYAN M.P

AINUX
TASTE OF LINUX

Analyzing and Storing Logs

System log:

Processes and the OS kernel need to be able to record the event logs. These logs can be useful for auditing the system and troubleshooting problems. These logs are stored into ***"/var/log"*** directory.

In RHEL 7, syslog messages are handled by two services, "**systemd-journald**" and **"rsyslog"**. Previous Linux versions uses **"rsyslog"** service and "**systemd-journald**" is introduced in RHEL 7.

"**rsyslog**" service configuration file is **"/etc/rsyslog.conf"** and stores the log into **"/var/log/"** directory.

The "/var/log" directory holds various log files mentioned below

Log File Name	Description
/var/log/messages	Most syslog messages are logged here. Run jobs log stored here.
/var/log/secure	Security and authentication related logs stored here.
/var/log/maillog	Mail server related log stored here.
/var/log/cron	Periodically executed task log stored here.
/var/log/boot.log	System start-up related log stored here.

AINUX
TASTE OF LINUX

Analyzing and Storing Logs

Log File rotation:

Log are rotated by the "**logrotate**" utility. When a log file is rotated, it is renamed with an extension indicating the date.

Monitor a log with tail command:

Example: - # tail /var/log/secure

To restart rsyslog service

systemctl restart rsyslog

"**Jorunalctl**" commands shows the full system based logs.

To display system based log

journalctl
journalctl -n 10
journalctl -f

To display system based log day wise

journalctl --since today
~~# journalctl --since "2017-02-10" --untill "2017-03-10"~~

AINUX
TASTE OF LINUX

Analyzing and Storing Logs

To display your current time zone

timedatectl

To display list of time zone

timedatectl list-timezones

To set a specific time zone

timedatectl set-timezone Asia/Kolkata | # tzselect

To set date and time

timedatectl set-time "YYYY-MM-DD hh:mm:ss"

To disable set time from NTP server

timedatectl set-ntp false

To enable set time from NTP server

timedatectl set-ntp true

NTP server configuration files stored into ***"/etc"*** directory as ***"chrony.conf"***

To restart the ntp service at the server end

systemctl restart chronyd

To display your ntp setup details at client end

chronyc sources -v

AINUX

TASTE OF LINUX

THANK YOU

CREATED BY : ARYAN M.P