System Administration 2

1 System Log

1.1

I choose Ubuntu 12.04-32bit for problems in 1.1

(1)

pid/name:433/rsyslogd

package:bsdutils

#netstat -anp | grep /dev/log

Reference:

http://www.serverwatch.com/tutorials/article.php/3924816/Use-Logger-to-Write-Messages-to-Log-Files.htm

(2)

#logger first attempt

#tail -f /var/log/syslog

```
May 14 16:21:36 os-VirtualBox os: first attempt
```

(3)

a:/var/log/mail.err and /var/log/syslog

b:/var/log/auth.log

c:/var/log/syslog

(find at /etc/rsyslog.d/50-default.conf)

“rsyslogd” cannot tell the difference between user and system service messages. An approach is to change the “init” process to “systemd”. Then, it will be clear by using the following two commands:

#journalctl --user

#journalctl --system

Reference:

http://man7.org/linux/man-pages/man1/logger.1.html

1.2

I choose Ubuntu 16.04-64bit for problems in 1.2

(1)

```
systemd@systemd-VirtualBox:~/Desktop$ systemctl --version
systemd 229
+PAM +AUDIT +SELINUX +IMA +APPARMOR +SMACK +SYSVINIT +UTMP +LIBCRYPTSETUP +GCRYPT +GNUTLS +ACL +XZ -LZ4
+SECCOMP +BLKID +ELFUTILS +KMOD -IDN
```

(2)

#vim /etc/systemd/journald.conf

edit a line : Storage=persistent

(3)

#journalctl -b -1 -k

(4)
#journalctl -u ssh.service
(5)
#less /etc/passwd
#journalctl _UID=1000 _UID=106(1000 is for current user and 106 is for dbus)
(6)
#journalctl /usr/bin/sudo

Reference for 1.2:

[1]https://www.digitalocean.com/community/tutorials/how-to-use-journalctl-to-view-and-manipulate-systemd-logs
[2]Reference:https://www.digitalocean.com/community/tutorials/how-to-use-journalctl-to-view-and-manipulate-systemd-logs

2 Network Log

#vim /etc/rsyslog.d/iptables.conf
put the following text into the file:
:msg, startswith, "iptables: " -/var/log/iptables.log
& ~
#iptables -A FORWARD -j LOG
#iptables -A INPUT -i eth1 -j LOG(assume that “eth1" which is the second network interface for the firewall connects to the private network)

Reference:

[1]https://blog.shadypixel.com/log-iptables-messages-to-a-separate-file-with-rsyslog/
[2]http://linux.vbird.org/linux_server/0250simple_firewall.php#netfilter

Discuss:

顏毓均
王冠鈞