Лаборатория работа 15

Настройка сетевого журналирования

ПОДГОТОВИЛА: КИМ РЕАЧНА
ГРУППА: НПИБД-02-20

Цель работы:

Получение навыков по работе с журналами системных событий.

Задание:

- Настройка сервера сетевого журнала
- Настройка клиента сетевого журнала
- Просмотр журнала
- Внесение изменений в настройки внутреннего окружения виртуальных машин

Настройка сервера сетевого журнала

```
[kreachna@server.kreachna.net ~]$ sudo -i
[sudo] password for kreachna:
[root@server.kreachna.net ~]# cd /etc/rsyslog.d
[root@server.kreachna.net rsyslog.d]# touch netlog-server.conf
```

```
rpc.mount 1113                          root    5u     IPv4              22706       0t0        TCP *:mountd (LISTEN)
rpc.mount 1113                          root    7u     IPv6              22721       0t0        TCP *:mountd (LISTEN)
dovecot   1116                          root   21u     IPv4              23145       0t0        TCP *:pop3 (LISTEN)
dovecot   1116                          root   22u     IPv6              23146       0t0        TCP *:pop3 (LISTEN)
dovecot   1116                          root   23u     IPv4              23147       0t0        TCP *:pop3s (LISTEN)
dovecot   1116                          root   24u     IPv6              23148       0t0        TCP *:pop3s (LISTEN)
dovecot   1116                          root   40u     IPv4              23164       0t0        TCP *:imap (LISTEN)
dovecot   1116                          root   41u     IPv6              23165       0t0        TCP *:imap (LISTEN)
dovecot   1116                          root   42u     IPv4              23166       0t0        TCP *:imaps (LISTEN)
dovecot   1116                          root   43u     IPv6              23167       0t0        TCP *:imaps (LISTEN)
smbd      6650                          root   35u     IPv4              40199       0t0        TCP mail.kreachna.net:m
icrosoft-ds->client.kreachna.net:46774 (ESTABLISHED)
rsyslogd  6806                          root    4u     IPv4              40995       0t0        TCP *:shell (LISTEN)
rsyslogd  6806                          root    5u     IPv6              40996       0t0        TCP *:shell (LISTEN)
rsyslogd  6806 6807 in:imtcp            root    4u     IPv4              40995       0t0        TCP *:shell (LISTEN)
rsyslogd  6806 6807 in:imtcp            root    5u     IPv6              40996       0t0        TCP *:shell (LISTEN)
rsyslogd  6806 6809 in:imjour           root    4u     IPv4              40995       0t0        TCP *:shell (LISTEN)
rsyslogd  6806 6809 in:imjour           root    5u     IPv6              40996       0t0        TCP *:shell (LISTEN)
rsyslogd  6806 6810 rs:main             root    4u     IPv4              40995       0t0        TCP *:shell (LISTEN)
rsyslogd  6806 6810 rs:main             root    5u     IPv6              40996       0t0        TCP *:shell (LISTEN)
rsyslogd  6806 6811 in:imtcp            root    4u     IPv4              40995       0t0        TCP *:shell (LISTEN)
rsyslogd  6806 6811 in:imtcp            root    5u     IPv6              40996       0t0        TCP *:shell (LISTEN)
rsyslogd  6806 6812 in:imtcp            root    4u     IPv4              40995       0t0        TCP *:shell (LISTEN)
rsyslogd  6806 6812 in:imtcp            root    5u     IPv6              40996       0t0        TCP *:shell (LISTEN)
rsyslogd  6806 6813 in:imtcp            root    4u     IPv4              40995       0t0        TCP *:shell (LISTEN)
rsyslogd  6806 6813 in:imtcp            root    5u     IPv6              40996       0t0        TCP *:shell (LISTEN)
rsyslogd  6806 6814 in:imtcp            root    4u     IPv4              40995       0t0        TCP *:shell (LISTEN)
rsyslogd  6806 6814 in:imtcp            root    5u     IPv6              40996       0t0        TCP *:shell (LISTEN)
```

Настройка клиента сетевого журнала

```
[kreachna@client.kreachna.net ~]$ sudo -i
[sudo] password for kreachna:
[root@client.kreachna.net ~]# cd /etc/rsyslog.d
[root@client.kreachna.net rsyslog.d]# touch netlog-client.conf
```

```
[root@client.kreachna.net rsyslog.d]# vim /etc/rsyslog.d/netlog-client.conf
[root@client.kreachna.net rsyslog.d]# cat /etc/rsyslog.d/netlog-client.conf
*.* @@server.kreachna.net:514
```

Просмотр журнала

```
[kreachna@server.kreachna.net ~]$ sudo -i
[sudo] password for kreachna:
[root@server.kreachna.net ~]# tail -f /var/log/messages
Dec 30 17:22:26 client rsyslogd[559]: [origin software="rsyslogd" swVersion="8.2102.0-105.el9" x-pid="559" x-info="http
s://www.rsyslog.com"] exiting on signal 15.
Dec 30 17:22:26 client systemd[1]: rsyslog.service: Deactivated successfull
Dec 30 17:22:26 client systemd[1]: Stopped System Logging Service.
Dec 30 17:22:26 client systemd[1]: Starting System Logging Service...
Dec 30 17:22:26 client systemd[1]: Started System Logging Service.
Dec 30 17:22:26 client rsyslogd[5534]: [origin software="rsyslogd" swVersio
tps://www.rsyslog.com"] start
Dec 30 17:22:26 client rsyslogd[5534]: imjournal: journal files changed, re
ww.rsyslog.com/e/0 ]
Dec 30 17:22:46 server systemd[5787]: Started VTE child process 6855 launch
Dec 30 17:22:52 server systemd[1]: Starting Hostname Service...
Dec 30 17:22:52 server systemd[1]: Started Hostname Service.
Dec 30 17:23:04 client NetworkManager[4441]: <info>  [1672410184.5317] dhcp
92.168.1.30
Dec 30 17:23:04 server dhcpd[1092]: DHCPREQUEST for 192.168.1.30 from 08:00
Dec 30 17:23:04 server dhcpd[1092]: DHCPACK on 192.168.1.30 to 08:00:27:83:
Dec 30 17:23:22 server systemd[1]: systemd-hostnamed.service: Deactivated s
Dec 30 17:23:29 server systemd[1]: Starting Cleanup of Temporary Directorie
Dec 30 17:23:29 server systemd[1]: systemd-tmpfiles-clean.service: Deactiva
Dec 30 17:23:29 server systemd[1]: Finished Cleanup of Temporary Directorie
Dec 30 17:24:31 server systemd[5787]: Started VTE child process 6935 launch
```

Processes | Resources | File Systems

Process Name	User	% CPU	ID	Memory	Disk read tota	Disk write tot	Disk read	Disk write	Priority
at-spi2-registryd	kreachna	0.00	5904	421.9 kB	274.4 kB	N/A	N/A	N/A	Normal
at-spi-bus-launcher	kreachna	0.00	5873	106.5 kB	94.2 kB	N/A	N/A	N/A	Normal
bash	kreachna	0.00	6706	1.8 MB	6.9 MB	N/A	N/A	N/A	Normal
bash	kreachna	0.00	6855	2.0 MB	2.6 MB	N/A	N/A	N/A	Normal
bash	kreachna	0.00	6935	1.6 MB	N/A	N/A	N/A	N/A	Normal
dbus-broker	kreachna	0.00	5811	1.2 MB	270.3 kB	N/A	N/A	N/A	Normal
dbus-broker	kreachna	0.00	5879	299.0 kB	N/A	N/A	N/A	N/A	Normal
dbus-broker-launch	kreachna	0.00	5810	167.9 kB	426.0 kB	N/A	N/A	N/A	Normal
dbus-broker-launch	kreachna	0.00	5878	188.4 kB	N/A	N/A	N/A	N/A	Normal
dconf-service	kreachna	0.00	6020	315.4 kB	262.1 kB	20.5 kB	N/A	N/A	Normal
evolution-addressbook-factory	kreachna	0.00	6028	1.2 MB	4.6 MB	36.9 kB	N/A	N/A	Normal
evolution-alarm-notify	kreachna	0.00	6213	4.7 MB	14.6 MB	N/A	N/A	N/A	Normal
evolution-calendar-factory	kreachna	0.00	5997	N/A	2.3 MB	N/A	N/A	N/A	Normal
evolution-source-registry	kreachna	0.00	5987	1.0 MB	3.4 MB	N/A	N/A	N/A	Normal
gjs	kreachna	0.00	6106	3.0 MB	2.3 MB	N/A	N/A	N/A	Normal
gjs	kreachna	0.00	6230	3.1 MB	167.9 kB	N/A	N/A	N/A	Normal
gnome-keyring-daemon	kreachna	0.00	5799	356.4 kB	N/A	N/A	N/A	N/A	Normal
gnome-session-binary	kreachna	0.00	5802	1.3 MB	9.5 MB	N/A	N/A	N/A	Normal
gnome-session-binary	kreachna	0.00	5920	N/A	2.9 MB	4.1 kB	N/A	N/A	Normal
gnome-session-ctl	kreachna	0.00	5918	237.6 kB	28.7 kB	N/A	N/A	N/A	Normal
gnome-shell	kreachna	25.61	5941	138.2 MB	252.8 MB	8.2 kB	21.3 KiB/s	N/A	Normal
gnome-shell-calendar-server	kreachna	0.00	5970	N/A	4.8 MB	N/A	N/A	N/A	Normal
gnome-software	kreachna	0.00	6228	34.1 MB	55.2 MB	1.4 MB	N/A	N/A	Normal
gnome-system-monitor	kreachna	21.45	6971	14.3 MB	19.3 MB	N/A	N/A	N/A	Normal
gnome-terminal-server	kreachna	0.00	6679	11.2 MB	10.7 MB	N/A	N/A	N/A	Normal
goa-daemon	kreachna	0.00	5993	N/A	18.9 MB	N/A	N/A	N/A	Normal

Внесение изменений в настройки внутреннего окружения виртуальной машины

nfs.sh | netlog.sh | netlog.sh | Vagrantfile

```
#!/bin/bash

echo "Provisioning script $0"

echo "Copy configuration files"
cp -R /vagrant/provision/server/netlog/etc/* /etc
restorecon -vR /etc

echo "Configure firewall"
firewall-cmd --add-port=514/tcp
firewall-cmd --add-port=514/tcp

echo "Start rsyslog service"
systemctl restart rsyslog
```

s.sh | netlog.sh | netlog.sh | Vagrantfile

```
#!/bin/bash

echo "Provisioning script $0"

echo "Install needed packages"
dnf -y install lnav

echo "Copy configuration files"
cp -R /vagrant/provision/client/netlog/etc/* /etc
restorecon -vR /etc

echo "Start rsyslog service"
systemctl restart rsyslog
```

Вывод

Получила навыков по работе с журналами системных событий.

Спасибо за внимание!