Lab 8: Syslog Server

Objective: To help students to learn

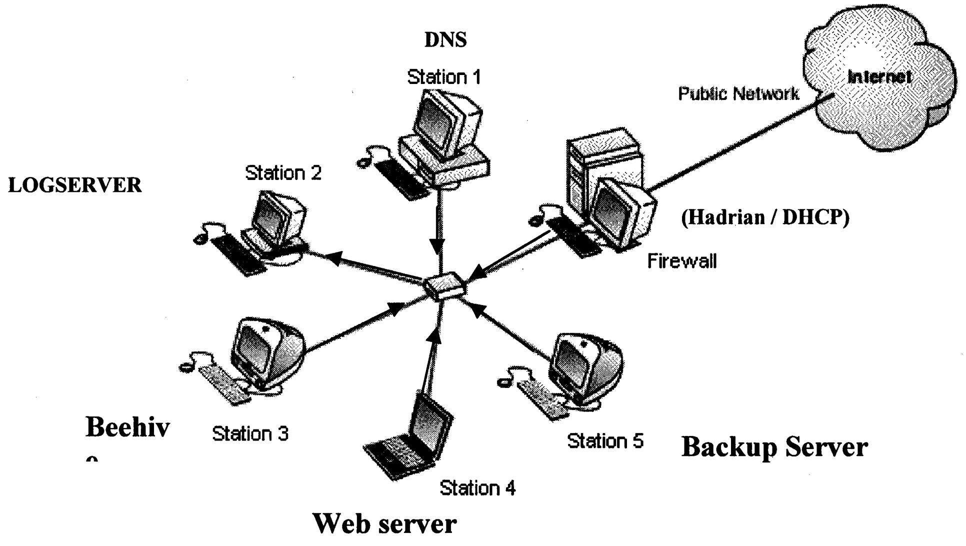
- Understand how syslog server works.

Scenario:

- **Domain: coyote365.net**
- **Systems administrator: Daniel McKay (dmckay)**
- **Servers:**

Server Name:	IP Address:	Function:
hadrian	192.168.1.1	Gateway
ns	192.168.1.2	DNS1
ns2	192.168.1.3	DNS2
www, web	192.168.1.4	Web server
beehive	192.168.1.5	NFS
chango	192.168.1.6	Backup
acme / logsver	192.168.1.7	log Server
lin-0 ~ lin-99	192.168.1.100 ~ 192.168.1.199	Linux Workstations
win-0 ~ lin-54	192.168.1.200 ~ 192.168.1.254	Windows Workstations

LOGSERVER will receive all log messages from other servers:



[1] Setup syslog Server:

Stop syslog service:

```
[root@logsver ~root]# service syslog stop
```

Edit /etc/sysconfig/syslog

```
[root@logsver ~root]# vi /etc/sysconfig/syslog
```

Replace the line

```
SYSLOGD_OPTIONS=”-m 0”
```

with

```
SYSLOGD_OPTIONS=”-rm 0”
```

Re-start the syslog service:

```
[root@logsver ~root]# service syslog restart
```

Check the log:

```
[root@logsver ~root]# tail /var/log/messages
```

You will find:

```
syslogd 1.4.1: restart (remote reception).
```

Add a Firewall Rule for accepting remote syslog reception:

```
[root@logsver ~root]# iptables -L
[root@logsver ~root]# iptables -I RH-Firewall-1-INPUT -p udp -i eth0 -s 192.168.1.0/24 \
-d 192.168.1.7 --dport 514 -j ACCEPT
[root@logsver ~root]# iptables-save > /etc/sysconfig/iptables
[root@logsver ~root]# service iptables restart
[root@logsver ~root]# iptables -L
```

NOTE:
192.168.1.0/24 are clients (loghosts)
192.168.1.7 is server (logsver)

Configure the syslog Clients:

```
[root@loghost ~root]# vi /etc/syslog.conf
```

Add following line:

```
*.* @192.168.1.7
```

Re-start the syslog service:

```
[root@loghost ~root]# service syslog restart
```

Add a Firewall Rule for accepting remote syslog reception:

```
[root@loghost ~root]# iptables -L
[root@loghost ~root]# iptables -I OUTPUT -p udp -s 192.168.1.0/24 -d 192.168.1.7 --dport 514 -j
ACCEPT
[root@loghost ~root]# iptables-save > /etc/sysconfig/iptables
[root@loghost ~root]# service iptables restart
[root@loghost ~root]# iptables -L
```

Check the log from syslog Server:

```
[root@logsver ~root]# tail -f /var/log/messages  (CTRL + C to escape)
```

```
[root@loghost ~root]# ssh 192.168.1.2  ( try to fail in deferent terminal )

[root@logsver ~root]# tail -f /var/log/secure (CTRL + C to escape)
[root@loghost ~root]# ssh 192.168.1.4  ( try to fail in deferent terminal)

[root@logsver ~root]# tail -f /var/log/alert (CTRL + C to escape)
[root@loghost ~root]# nmap 192.168.1.0 ( try in deferent terminal)
```

Set crontab to send you a notification via email.

Lab 8 Report:

[1] Why do we need log server?

[2] What port is needed to open on syslog server?

[3] Why do you replace "-m 0" to "-rm 0" as following?

> *Replace the line*
> **SYSLOGD_OPTIONS="-m 0"**
> *with*
> **SYSLOGD_OPTIONS="-rm 0"**

[4] Why following firewall rule is important on syslog server?

```
iptables -I RH-Firewall-1-INPUT -p udp -i eth0 -s 192.168.1.0/24 -d 192.168.1.3 --dport 514 -j ACCEPT
```

[5] Explain above firewall rule?

[6] How to save current firewall rule sets?

[7] How to make your syslog server become web-based so that you can check syslog from anywhere with secure manner?

[8] What did you learn from this lab?