LAB Exercise Ubuntu SYSLOG

Pre requested software

- Ubuntu 18.04
- Virtual Box – Server (192.168.10.38)
- Virtual Box – Client (192.168.10.37)
- Putty for SSH

  Note: enable putty and ssh and continue your lab exercise.

Server Configuration (Rsyslog)

Step 01 Update the repository - Ubuntu

```
# sudo apt-get update
```

Step 02 Installation of rSyslog and mibs

```
#sudo apt install rsyslog
#sudo apt-get install snmp-mibs-downloader
#sudo apt install grep
```

Step 03 verify the status.

```
# sudo systemctl start rsyslog
# sudo systemctl status rsyslog
```

Step 04 Allow firewall

```
#  sudo ufw enable
#  sudo ufw allow 514/udp
#  sudo ufw allow 514/tcp
#  sudo ufw allow openssh
#  sudo ufw reload
```

Step 05 Backup the existing "rsyslog.conf" file

```
# sudo cp /etc/rsyslog.conf /etc/rsyslog.conf.orig
```

Step 06 Uncomment the lines for udp and tcp port binding:

```
#  sudo nano /etc/rsyslog.conf
```

```
# provides UDP syslog reception
module(load="imudp")
input(type="imudp" port="514")

# provides TCP syslog reception
module(load="imtcp")
input(type="imtcp" port="514")
```

# Create a new template for receiving remote messages

Add the following lines: (copy and paste using ssh)

```
$template RemoteLogs,"/var/log/%HOSTNAME%/%PROGRAMNAME%.log"
*.* ?RemoteLogs
& ~
```

save and exit. (ctrl+o and ctrl+x)

Step 08 restart the services

```
# sudo systemctl restart rsyslog
```

Step 09 Verify the service is listening on configured ports

```
# sudo ss -tulnp | grep “rsyslogd”
```

Now log on to client host

Client Configuration (Rsyslog)

Step 01 Update the repository - Ubuntu

```
# sudo apt-get update

# sudo systemctl status rsyslog
```

Step 02 Backup the existing “rsyslog.conf” file

```
# sudo cp /etc/rsyslog.conf /etc/rsyslog.conf.orig
```

Step 03 Add the rules: (server IP and port no)

```
# sudo nano /etc/rsyslog.conf
```

```
    *.* @@192.168.10.38:514
    auth. * @@192.168.10.38:514
```

Step 04 Service restart

```
#  sudo systemctl restart rsyslog
```

Note : now log on to server and continue

Final step

Step 05 Monitoring

```
# sudo ls -l /var/log/


# Directory Access (Your syslog file name)

# sudo ls -l /var/log/rsys
```