LAB: Log Management Lab - syslog-ng

Please follow the lab guide to login to the VM.

Note:

- Commands preceded with `$` imply that you should execute the command as a general user - not as root.
- Commands preceded with `#` imply that you should be working as root.
- If a command line ends with `\` this indicates that the command continues on the next line and you should treat this as a single line.

1. Install syslog-ng

Update the package index for the APT package manager and install `syslog-ng`:

```
$ sudo apt-get update
$ sudo apt-get install syslog-ng syslog-ng-core
```

Verify installed version of syslog-ng:

```
$ syslog-ng --version
syslog-ng 3 (3.13.2)
Config version: 3.13
Installer-Version: 3.13.2
```

2. Configure syslog-ng

The default configuration file is `/etc/syslog-ng/syslog-ng.conf`. To allow logs from another machine or device we need to do the following changes:

```
$ sudo vi /etc/syslog-ng/syslog-ng.conf
```

Find the lines:

```
source s_src {
    system();
    internal();
};
```

Add `udp();` and it will look like below:

```
source s_src {
    system();
    internal();
    udp();
};
```

Save the file and exit.

Since the last line in the `syslog-ng.conf` config file (`/etc/syslog-ng/syslog-ng.conf`) is `@include "/etc/syslog-ng/conf.d/"` , all configuration files in the folder `conf.d` will be processed, too.

```
$ sudo vi /etc/syslog-ng/conf.d/router.conf

filter f_routers { facility(local0); };

log {
    source(s_src);
    filter(f_routers);
    destination(routers);
};

destination routers {
    file("/var/log/apnic/$HOST/$YEAR/$MONTH/$HOST-$YEAR-$MONTH-$DAY.log"
    owner(root) group(root) perm(0644) dir_perm(0755) create_dirs(yes)
    template("$YEAR $DATE $HOST $MSG\n"));
};
```

As all the logs will be stored in `/var/log/apnic` ; we need to create the folder:

```
$ sudo mkdir -p /var/log/apnic
```

Restart syslog-ng:

```
$ sudo systemctl restart syslog-ng
```

Check the status

```
$ sudo service syslog-ng status
● syslog-ng.service - System Logger Daemon
Loaded: loaded (/lib/systemd/system/syslog-ng.service; enabled; vendor preset: enable
d)
Active: active (running) since Mon 2020-12-28 03:10:25 AEDT; 16s ago
    Docs: man:syslog-ng(8)
Main PID: 50157 (syslog-ng)
    Tasks: 2 (limit: 9323)
CGroup: /system.slice/syslog-ng.service
        └─50157 /usr/sbin/syslog-ng -F
```

The default port for syslog is `udp/514` ; we can check the same from `netstat` command:

```
$ sudo netstat -4altunp|grep 514
udp        0      0 0.0.0.0:514             0.0.0.0:*                           5685/
syslog-ng
```

3. Configure router to send syslog

Login to your group router and add the following configuration. Replace `X` with your group number:

```
(config)# logging 192.168.X.10
(config)# logging facility local0
(config)# logging userinfo
(config)# exit
# write memory
```

Run `show logging` to verify

```
Trap logging: level informational, 60 message lines logged
    Logging to 192.168.X.10  (udp port 514, audit disabled,
          link up),
          14 message lines logged,
          0 message lines rate-limited,
          0 message lines dropped-by-MD,
          xml disabled, sequence number disabled
          filtering disabled
    Logging Source-Interface:       VRF Name:

Log Buffer (8192 bytes):
```

Logs are stored in `/var/log/apnic/` folder. There will be folder for each host. If you hvae noticed the log location is defined in the `/etc/syslog-ng/conf.d/router.conf` file which is `/var/log/apnic/$HOST/$YEAR/$MONTH/$HOST-$YEAR-$MONTH-$DAY.log`.

```
$ more /var/log/apnic/192.168.10.1/2020/12/192.168.10.1-2020-12-28.log
2020 Dec 28 12:51:36 192.168.10.1 Logging to host 192.168.10.10 port 514 started - CL
I initiated
2020 Dec 28 12:51:37 192.168.10.1 Configured from console by apnic on vty0 (100.101.0
.91)
2020 Dec 28 12:51:38 192.168.10.1 GRUB configuration is being updated on disk. Please
 wait...
2020 Dec 28 12:51:38 192.168.10.1 GRUB configuration was written to disk successfully
.
2020 Dec 28 13:06:19 192.168.10.1 Line protocol on Interface Loopback0, changed state
 to up
2020 Dec 28 13:06:20 192.168.10.1 Configured from console by apnic on vty0 (100.101.0
.91)
2020 Dec 28 13:06:21 192.168.10.1 GRUB configuration is being updated on disk. Please
 wait...
2020 Dec 28 13:06:22 192.168.10.1 GRUB configuration was written to disk successfully.
```

End of Lab