LAB: Log Management Lab - rsyslog

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. Verify port

Before installing `rsyslog` please check if any other syslog service is installed or not and running on port `514`

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

In this example syslog-ng is running. We need to stop `syslog-ng` first.

```
$ sudo systemctl stop syslog-ng
```

Verify that `syslog-ng` is not running

```
$ sudo systemctl status syslog-ng
● syslog-ng.service - System Logger Daemon
Loaded: loaded (/lib/systemd/system/syslog-ng.service; enabled; vendor preset:
enabled)
Active: inactive (dead) since Mon 2020-12-28 23:14:13 AEST; 5s ago
    Docs: man:syslog-ng(8)
Process: 5685 ExecStart=/usr/sbin/syslog-ng -F $SYSLOGNG_OPTS (code=exited,
status=0/SUCCESS)
Main PID: 5685 (code=exited, status=0/SUCCESS)
Status: "Shutting down... (Mon Dec 28 23:14:13 2020"
```

2. Install rsyslog

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

```
$ sudo apt-get update
$ sudo apt-get install rsyslog
```

After installing `rsyslog`, you can check the version of `rsyslog` with the following command:

```
$ rsyslogd -v
rsyslogd 8.32.0, compiled with:
        PLATFORM:                               x86_64-pc-linux-gnu
        PLATFORM (lsb_release -d):
        FEATURE_REGEXP:                         Yes
        GSSAPI Kerberos 5 support:              Yes
        FEATURE_DEBUG (debug build, slow code): No
        32bit Atomic operations supported:      Yes
        64bit Atomic operations supported:      Yes
        memory allocator:                       system default
        Runtime Instrumentation (slow code):    No
        uuid support:                           Yes
        systemd support:                        Yes
        Number of Bits in RainerScript integers: 64
```

You can also check the status of Rsyslog with the following command:

```
$ sudo systemctl status rsyslog

● rsyslog.service - System Logging Service
Loaded: loaded (/lib/systemd/system/rsyslog.service; enabled; vendor preset:
enabled)
Active: active (running) since Mon 2020-12-28 23:15:36 AEST; 1min 30s ago
    Docs: man:rsyslogd(8)
        http://www.rsyslog.com/doc/
Main PID: 6437 (rsyslogd)
    Tasks: 4 (limit: 4601)
CGroup: /system.slice/rsyslog.service
        └─6437 /usr/sbin/rsyslogd -n
```

3. Configure rsyslog

Rsyslog is now installed and running. Next, you will need to configure it to run in a server mode. You can do it by editing the file `/etc/rsyslog.conf`:

```
$ sudo vi /etc/rsyslog.conf
```

First, you will need to define the protocol either UDP or TCP or both.
To use both UDP and TCP connections at the same time search and uncomment the lines below:

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

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

Save and close the file when you are finished. Then, check the Rsyslog configuration for any syntax error with the following command:

```
$ sudo rsyslogd -f /etc/rsyslog.conf -N1
```

You should see the following output:

```
rsyslogd: version 8.32.0, config validation run (level 1), master config
/etc/rsyslog.conf
rsyslogd: End of config validation run. Bye.
```

Finally, restart Rsyslog service with the following command:

```
$ sudo systemctl restart rsyslog
```

Now, verify that Rsyslog is listening on TCP/UDP with the following command:

```
$ sudo netstat -4altunp | grep 514
```

You should get the following output:

```
tcp        0      0 0.0.0.0:514             0.0.0.0:*               LISTEN
6634/rsyslogd
udp        0      0 0.0.0.0:514             0.0.0.0:*
6634/rsyslogd
```

4. 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/syslog` file.

```
$ sudo tail -f /var/log/syslog
Dec 28 23:23:24 192.168.10.1 80: .Dec 28 13:23:23.284: %GRUB-5-CONFIG_WRITING:
GRUB configuration is being updated on disk. Please wait...
Dec 28 23:23:24 192.168.10.1 81: .Dec 28 13:23:23.896: %GRUB-5-CONFIG_WRITTEN:
GRUB configuration was written to disk successfully.
Dec 28 23:24:06 192.168.10.1 82: .Dec 28 13:24:05.863: %SYS-5-CONFIG_I:
Configured from console by apnic on vty0 (100.101.0.91)
Dec 28 23:24:06 192.168.10.1 83: .Dec 28 13:24:06.520: %GRUB-5-CONFIG_WRITING:
GRUB configuration is being updated on disk. Please wait...
Dec 28 23:24:07 192.168.10.1 84: .Dec 28 13:24:07.009: %LINK-5-CHANGED: Interface
Loopback0, changed state to administratively down
Dec 28 23:24:07 192.168.10.1 85: .Dec 28 13:24:07.132: %GRUB-5-CONFIG_WRITTEN:
GRUB configuration was written to disk successfully.
Dec 28 23:24:07 192.168.10.1 86: .Dec 28 13:24:08.009: %LINEPROTO-5-UPDOWN: Line
protocol on Interface Loopback0, changed state to down
```

5. Sending log from server

If you would like to send server log to the rsyslog server, create a file called `/etc/rsyslog.d/99-syslog-server.conf` with the following contents:

```
$ sudo vi /etc/rsyslog.d/99-syslog-server.conf

##Enable sending of logs over UDP add the following line:
*.*  @192.168.X.10:514
```

Save and close the file. Then, restart Rsyslog server to apply the configuration changes:

```
$ sudo systemctl restart rsyslog
```

Now all the server logs will be send to the syslog server.

End of Lab