

Project: System-to-System Log Forwarding using Rsyslog on Ubuntu



By: Afroz Shaikh



Email: afrozshaikh8086@gmail.com



Overview

This project demonstrates how to configure **log forwarding** from one Ubuntu system to another using **rsyslog**. This technique is commonly used in **SOC environments**, **log management systems**, and **SIEM platforms** to centralize and monitor logs from multiple sources.



Prerequisites

- Ubuntu OS installed on both systems.
- **rsyslog** service enabled (default on most Ubuntu installs).
- Network connectivity between the source and destination systems.
- Root or sudo access.



Step-by-Step Configuration

1. Launch Terminal

Start by opening the terminal on your Ubuntu system.

2. Navigate to Configuration Directory

*Run the following command to go to the `/etc` directory:

```
splunk123@hackerzone: /etc
```

```
splunk123@hackerzone:/etc$ cd /etc
```

This folder contains system-wide configuration files, including those for **rsyslog**.

3. Locate rsyslog Configuration

Use `ls` to verify the presence of the configuration files:

```
splunk123@hackerzone: /etc
```

```
splunk123@hackerzone:/etc$ cd /etc
splunk123@hackerzone:/etc$ ls
adduser.conf      cryptsetup-initramfs  gshadow-      libnl-3        nanorc        ppp            sgml            tmpfiles.d
alternatives      crypttab              hdparm.conf   locale.alias   needrestart   profile        shadow          ubuntu-advantage
apparmor          dbus-1               host.conf     locale.conf    netconfig    rc0.d          shadow-        ucf.conf
apparmor.d        debconf.conf         hostname      locale.gen     netplan      rc1.d          shells         udev
appport           debian_version       hosts         localtime      network      rc2.d          skel           udisks2
apt              default              hosts.allow   logcheck       networkd-dispatcher  python3        snort          ufw
bash.bashrc       deluser.conf         hosts.deny    login.defs     newt         rc3.d          sos            update-manager
bash_completion   depmod.d             init.d        logrotate.conf nftables.conf rc4.d          ssh            update-motd.d
bash_completion.d dhcpd.conf           initramfs-tools  logrotate.d    nsswitch.conf rc5.d          ssl            update-notifier
bindresvport.blacklist  dpkg                iproute2       lsb-release   oinkmaster.conf rc6.d          subgid         UPower
binfmt.d          e2scrub.conf         iscsi          lvm            opt           rc7.d          subgid-        usb_modeswitch.conf
byobu             environment          issue          magic          overlayroot.conf rc8.d          subuid         usb_modeswitch.d
ca-certificates   ethertypes           issue.net      magic.mime     PackageKit   resolv.conf    sudo.conf     vconsole.conf
ca-certificates.conf  fonts               kernel         manpath.config pam.conf      rmt            sudoers.d     vim
cloud             fstab                landscape      mdadm          mime.types   rsyslog.conf   sudoers.d     vmware-tools
console-setup     fuse.conf            ldap           mke2fs.conf   ModemManager passw.d        sudo_logd.conf  vtrgb
credstore          fwupd               ld.so.cache   modprobe.d    modules      rsyslog.d      supercat       wgetrc
credstore.encrypted  gai.conf            ld.so.conf    modprobe.d    modules-load.d  screenrc      sysctl.conf   X11
cron.d            gnutils             ld.so.conf.d  modules        mtab          security       sysctl.d      xattr.conf
cron.daily        groff               legal          mtap           multipath      selinux        syslogd       xdg
cron.hourly       grub.d              libaudit.conf mtab           multipath.conf pki            systemd       xml
cron.monthly      grub.d              libblockdev   multipath      pollinate      sensors3.conf  systemd      zsh_command_not_found
cron.tab          gshadow             libibverbs.d  multipath.conf
cron.weekly
cron.yearly
```

Look for:

- **rsyslog.conf**
- **rsyslog.d/ directory**

4. Edit the rsyslog Configuration

Open the config file with elevated privileges:

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

Add the following line at the end of the file:

```
*.* @192.168.1.9:514
```

- *.* → forward all logs from all facilities and severity levels
- @ → indicates use of **UDP** (use @@ for **TCP**)
- 192.168.1.9:514 → destination IP and port of the log collector

```
splunk123@hackerzone: /etc
GNU nano 7.2 /etc/rsyslog.conf *
module(load="imuxsock") # provides support for local system logging
#module(load="immark") # provides --MARK-- message capability

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

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

# provides kernel logging support and enable non-kernel klog messages
module(load="imklog" permitnonkernelfacility="on")

#####
#### GLOBAL DIRECTIVES ####
#####

# Filter duplicated messages
$RepeatedMsgReduction on

#
# Set the default permissions for all log files.
#
$FileOwner syslog
$FileGroup adm
$FileCreateMode 0640
$DirCreateMode 0755
$Umask 0022
$PrivDropToUser syslog
$PrivDropToGroup syslog

#
# Where to place spool and state files
#
$WorkDirectory /var/spool/rsyslog

#
# Include all config files in /etc/rsyslog.d/
#
$IncludeConfig /etc/rsyslog.d/*.conf
*.* @192.168.1.9:514
```

5. Save and Exit

- Press `Ctrl + X`
- Press `Y` to confirm
- Hit `Enter` to save

```
*. * @192.168.1.9:514
Save modified buffer?
Y Yes
N No      ^C Cancel
```

6. Restart rsyslog Service

```
sudo systemctl restart rsyslog
```

```
splunk123@hackerzone:/etc$ sudo nano /etc/rsyslog.conf
[sudo] password for splunk123:
splunk123@hackerzone:/etc$ sudo ./splunk restart rsyslog
```

Output

Now, logs from your system will be **forwarded in real time** to the destination system or SIEM platform for centralized analysis and monitoring.

Notes

- Ensure that port 514 is open on the destination.
 - Use `firewall-cmd` or `ufw` to allow traffic if needed.
 - Recommended: monitor `/var/log/syslog` to verify forwarding is working.
-

Use Cases

- Security Operations Centers (SOC)
 - SIEM integration
 - Lab-based log collection projects
 - Centralized log monitoring
-