

# Configuring System-to-System Log Forwarding Using rsyslog on Ubuntu

 To begin the configuration process, **launch the terminal** on your Ubuntu system.

Once the terminal is open, **navigate to the system configuration directory** by executing the command to enter the /etc path.

 This directory contains important **configuration files**, including those necessary for managing rsyslog services used for log forwarding.

```
splunkufw@splunkufw:/s cd /etc
```

 Next, use the ls command within the /etc directory to list and locate the rsyslog configuration files.

This step helps **verify the presence** of rsyslog-related files such as rsyslog.conf

```
plunkufw@plunkufw:~/etc$ cd /etc  
duser.conf      cryptsetup-initramfs  gshadow-    libnl-3      nanorc      ppp          sqmll      tmpfiles.d  
lternatives     crypttab        libnl.alias   needrestart  profile      shadow       ubuntu-advantage  
lparmor        dbus-1          locale.alias  netconfig    profile.d    shadow-  
lparmor.d      default.conf     locale.conf   netplm       profile.d    shadow-  
lparmor.d      default.conf     host.conf    network     protocols    shells  
lparmor.d      default        hostname     nmap        protocols    shells  
lparmor.d      default        hosts       logcheck    network-dispatcher python3.12  snort  
ash.bashrc      deluser.conf    hosts.allow  login.defs networks    rc0.d      sos       update-manager  
ash_completion  depmod.d      hosts.deny  logrotate.conf newt       rc1.d      ssh       update-motd.d  
ash_completion.d dhcp          init.d      logrotate.d  nftables.conf  rc2.d      ssh       update-notifier  
ashesport.blacklist  dhclient.conf  inputrc    logrotate.d  nfqueue.conf  rc3.d      ssh       update-ua  
infmit.d      dpkg          iproute2   machine-id  oinkmaster.conf  rc4.d      subgid-  usb_modemswitch.conf  
yobu          e2scrub.conf  iproute2   magic       os-release   rc5.d      subuid-  usbmodeswitch.d  
a-certificates environment  iscsi       magic.mime  overlayroot.conf  rc6.d      subuid-  vconsole.conf  
a-certificates.conf ethertypes  issue      manpath.conf  overlayroot.conf  rc7.d      sudo.conf  vim  
fntab          kernel       iscsi.net   manpath.config  overlayroot.conf  rc8olv.conf  sudoers  vmsave-tools  
onsole-setup  fstab         kernel     mtab       pam.confd   rc9.d      sudoers.d  vt100  
redstore      fuse.conf    landscape  mime.types  pam.confd   rmt       sudoers.d  vtgb  
redstore.encrypted  fuppd      ldap       mkefcfs.conf  paesswd    rpc       sudo.logrsvd.conf  wgetrc  
ron.d          gal.conf     ld.so.cache  ModemManager  paesswd    rsyslog.conf  supercat  X11  
ron.daily     gnats       ld.so.conf   NetworkManager  paesswd    rsyslogd    systemctl.conf  
ron.hourly    gnats       ld.so.conf.d  NetworkManager-gtk  perl      rsyslogd    sysctl.conf  
ron.monthly   group      ld.so.conf.d  modules     pki       security    systemd  
rontab        group      libaudit.conf  modules-load.d  Plymouth    security    systemd  
ron.weekly    grub.d      libblkdev    multipath   pm       selinux     systemd  
ron.yearl     grub.d      libibverbs.d  multipath.conf  polkit-1  sensors    terminfo  
plunkufw@plunkufw:/etc$ sudo nano rsyslog.conf  
plunkufw@plunkufw:/etc$ sudo password for plunkufw: [REDACTED]
```

or the rsyslog.d directory, which are essential for configuring log forwarding and centralized logging.

 At this stage, we need to **access the rsyslog configuration file or directory with elevated privileges**.

 Since the /etc directory and its contents are protected system files, you will be **prompted to enter the Ubuntu user password** when executing commands with sudo.

 This ensures **secure access** to modify rsyslog settings necessary for

```
splunkufw@splunkufw:/$ cd /etc
splunkufw@splunkufw:/etc$ ls
alternatives      cryptsetup-initramfs  gshadow-      libnl-3      nanorc      ppp        sgml        tmpfiles.d
apparmor          crypttab             gss          locale.alias  needrestart  profile    shadow      ubuntu-advantage
apparmor.d        dbus-1               hparm.conf   locale.conf   netconfig    profile.d   shadow-
apparmor.d        debconf.conf        host.conf    locale.gen    netplan     protocols  shells
apport            debian_version     hostname    localtime   network    python3    skeI
apt              default             hosts       logcheck    networkd-dispatcher  python3.12  snort
bash.bashrc       deluser.conf       hosts.allow  login.defs  networks   rc0.d      sos
bash_completion   depmod.d           hosts.deny  logrotate.conf newt      rc1.d      ssh
bash_completion.d dhcpc               init.d      logrotate.d  nftables.conf  rc2.d      ssl
bindresvport.blacklist dhpcd.conf     initramfs-tools  lsb-release  nsswitch.conf  rc3.d      subgid
binfmt.d          dpkg               inputrc    lvm         oinkmaster.conf  rc4.d      subgid-
byobu            e2scrub.conf      iproute2   machine-id  opt       rc5.d      subuid
ca-certificates   environment       iscsi        magic      os-release  rc6.d      subuid-
ca-certificates.conf ethertypes       issue       magic.mime  overlayroot.conf  rcS.d      sudo.conf
cloud            fonts              issue.net   manpath.config PackageKit  resolv.conf sudoers
console-setup     fstab              kernel      mime.types  pam.conf   rmt       sudoers.d
credstore         fuse.conf         landscape  mke2fs.conf  passwd    rpc       sudoers.d
credstore.encrypted  fwupd             ldap       ModemManager  passwd-   syslogd  supercat
cron.d           gai.conf          ld.so.cache  ld.so.conf  modprobe.d perl      screenrc  sysctl.conf
cron.daily        gnutls            ld.so.conf.d ld.so.conf.d modules   pki       security
cron.hourly       groff            ld.so.conf.d ld.so.conf.d modules-load.d plymouth
cron.monthly      group             legal       mtab      multipath  polkit-1 sensors3.conf terminfo
cron.tab          group-            libaudit.conf libblockdev  multipath  pollinate sensors.d thermal
cron.weekly       grub.d            libibverbs.d libibverbs.d  multipath.conf pollinate sensors.d thermal
cron.yearly       gshadow          libibverbs.d
splunkufw@splunkufw:/etc$
```

system-to-system log forwarding.

 Once the rsyslog.conf file is opened in the **Nano text editor**, you will be able to **view and edit its contents**.

 At this point, specific **configuration lines** need to be added or

modified to define the **destination IP address** of the second system to which logs will be forwarded.

➡ This second system acts as an **intermediary**, receiving logs from the source machine and subsequently forwarding them to a centralized **enterprise log server or SIEM platform**  for further analysis and storage.

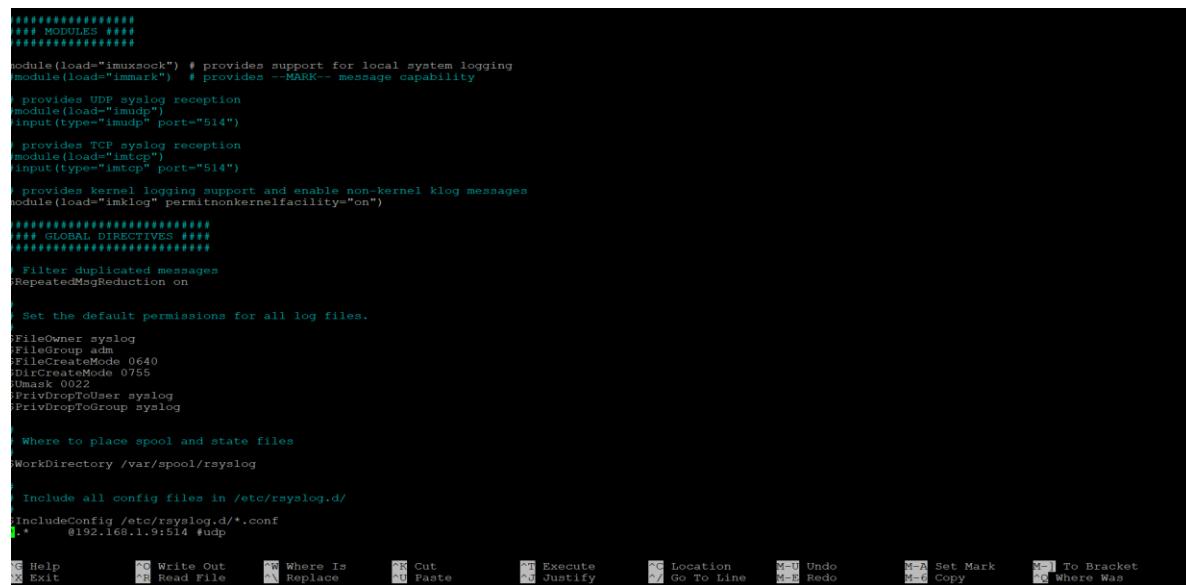
💡 At this point, you will need to **insert a specific configuration directive** into the rsyslog.conf file.

📝 An example of such a directive is:

\*.\* @192.168.1.9:514

👉 This line instructs rsyslog to **forward all log messages**—across all facilities and severity levels—to the **remote system** identified by the IP address 192.168.1.9 using **UDP on port 514** .

🚀 This setup is essential for enabling **real-time log transmission** from the local system to a remote **log collector or server** .



```
#####
## MODULES ##
#####

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" perm=nonkernelfacility="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 udp
```

- ⚙️ In the configuration syntax, the @ symbol signifies that the log messages should be forwarded using **UDP (User Datagram Protocol)** .
- 💡 If **TCP** is preferred for more reliable transmission, the @@ symbol should be used instead.
- 💾 After entering or modifying the required configuration line, **save the changes** in the Nano editor by:
  - ◆ Pressing Ctrl + X to exit
  - ◆ Pressing Y to confirm saving the changes
  - ◆ Hitting Enter to finalize and return to the terminal .

