

How to Configure Multi-Hop Log Forwarding with rsyslog from Kali Linux to Splunk via Ubuntu

Submitted by: Faizanullah Syed

Use Case: Centralized Log Collection in SOC using rsyslog

Systems Used:

- **Kali Linux** (Log Source)
- **Ubuntu Server** (Intermediate Forwarder)
- **Enterprise Server** (Log Collector)

✓ Objective

To configure centralized log forwarding where logs are sent:

Kali Linux (Client) → Ubuntu Server (Forwarder) → Enterprise Server (Collector)

This method is essential in Security Operations Centers (SOCs) where intermediate forwarders are used to centralize logs before sending them to SIEMs or log analysis tools.

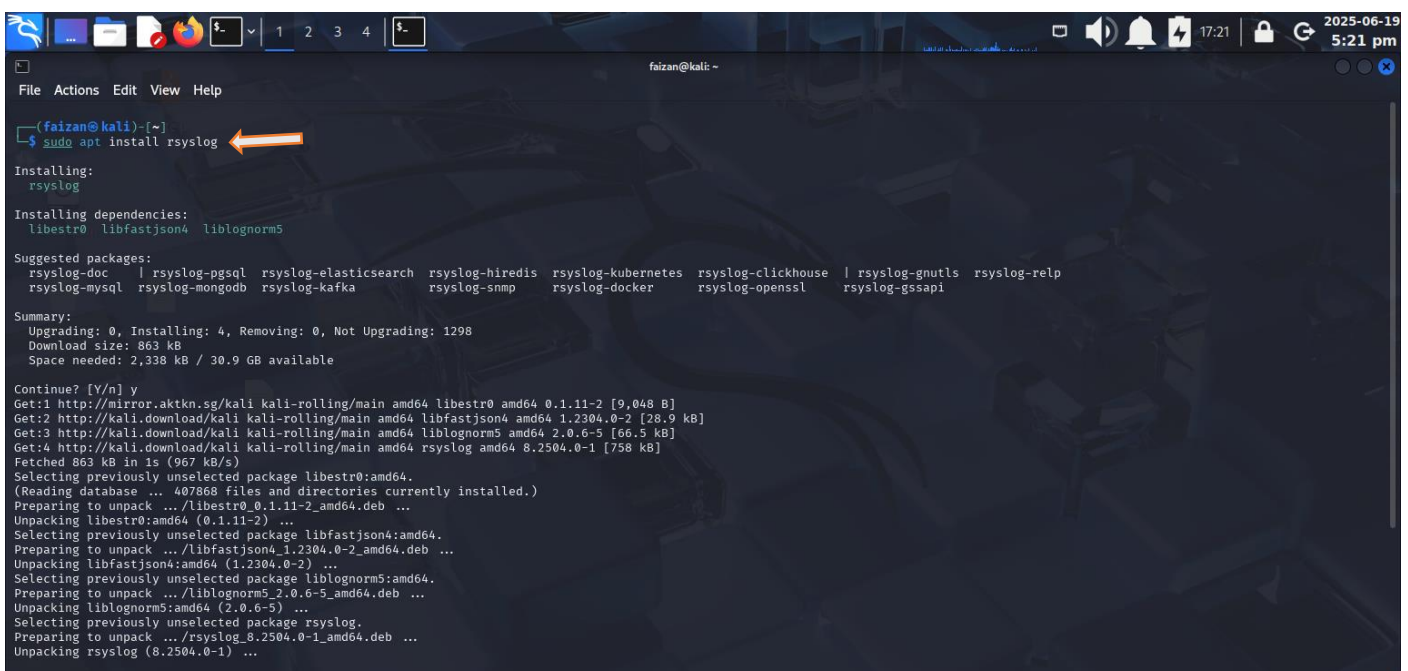
Implementation Steps:

◆ Step 1: Install **rsyslog** on All Machines

Run the following on **Kali**, **Ubuntu**, and **Enterprise Server**:

```
# sudo apt update
```

```
# apt install rsyslog sudo
```

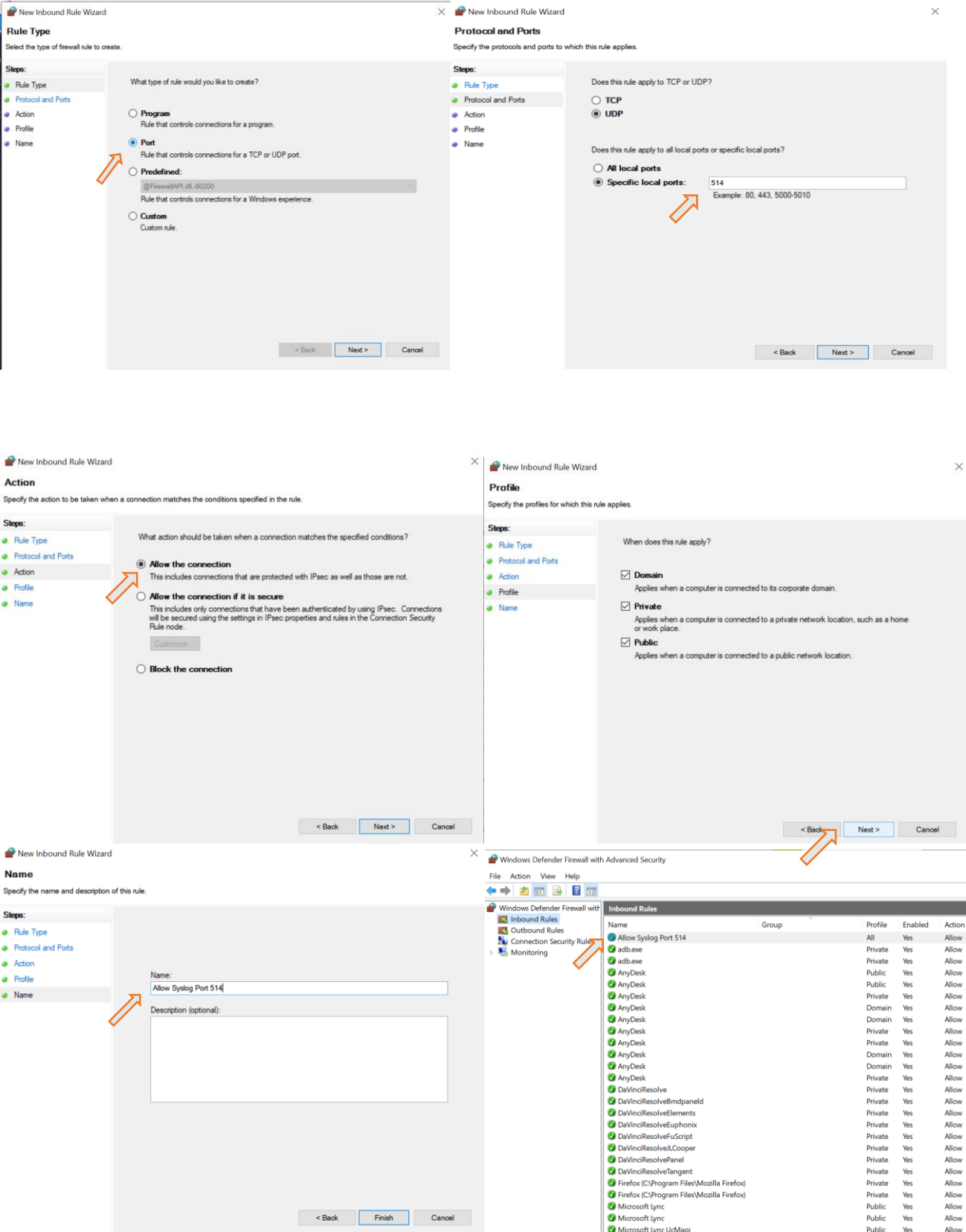


```
faizan@kali: ~  
$ sudo apt install rsyslog  
Installing:  
  rsyslog  
Installing dependencies:  
  libestr0 libfastjson4 liblognorm5  
Suggested packages:  
  rsyslog-doc | rsyslog-pgsql rsyslog-elasticsearch rsyslog-hiredis rsyslog-kubernetes rsyslog-clickhouse | rsyslog-gnutls rsyslog-relp  
  rsyslog-mysql rsyslog-mongodb rsyslog-kafka rsyslog-snmp rsyslog-docker rsyslog-openssl rsyslog-gssapi  
Summary:  
  Upgrading: 0, Installing: 4, Removing: 0, Not Upgrading: 1298  
  Download size: 863 kB  
  Space needed: 2,338 kB / 30.9 GB available  
Continue? [Y/n] y  
Get:1 http://mirror.aktkn.sg/kali kali-rolling/main amd64 libestr0 amd64 0.1.11-2 [9,048 B]  
Get:2 http://kali.download/kali kali-rolling/main amd64 libfastjson4 amd64 1.2304.0-2 [28.9 kB]  
Get:3 http://kali.download/kali kali-rolling/main amd64 liblognorm5 amd64 2.0.6-5 [56.5 kB]  
Get:4 http://kali.download/kali kali-rolling/main amd64 rsyslog amd64 8.2504.0-1 [758 kB]  
Fetched 863 kB in 1s (967 kB/s)  
Selecting previously unselected package libestr0:amd64.  
(Reading database ... 407868 files and directories currently installed.)  
Preparing to unpack .../libestr0_0.1.11-2_amd64.deb ...  
Unpacking libestr0:amd64 (0.1.11-2) ...  
Selecting previously unselected package libfastjson4:amd64.  
Preparing to unpack .../libfastjson4_1.2304.0-2_amd64.deb ...  
Unpacking libfastjson4:amd64 (1.2304.0-2) ...  
Selecting previously unselected package liblognorm5:amd64.  
Preparing to unpack .../liblognorm5_2.0.6-5_amd64.deb ...  
Unpacking liblognorm5:amd64 (2.0.6-5) ...  
Selecting previously unselected package rsyslog.  
Preparing to unpack .../rsyslog_8.2504.0-1_amd64.deb ...  
Unpacking rsyslog (8.2504.0-1) ...
```

Step 2: Configure Enterprise Server to Receive Logs

On the **Enterprise Server** :

- 1) First need to create inbound rule in windows firewall & network protection where Splunk Enterprise server installed.



The following screenshots illustrate the steps to create a new inbound rule in Windows Firewall:

- Rule Type:** Select **Port** (Rule that controls connections for a TCP or UDP port).
- Protocol and Ports:** Select **UDP**. Does this rule apply to TCP or UDP? **UDP**. Does this rule apply to all local ports or specific local ports? **Specific local ports:** 514 (Example: 80, 443, 5000-5010).
- Action:** Select **Allow the connection** (This includes connections that are protected with IPsec as well as those are not).
- Profile:** Select **Domain**, **Private**, and **Public** (Applies when a computer is connected to its corporate domain, a private network location, such as a home or work place, and a public network location).
- Name:** Name: Allow Syslog Port 514. Description (optional):

The final screenshot shows the **Windows Defender Firewall with Advanced Security** console. The **Inbound Rules** list includes the newly created rule: **Allow Syslog Port 514**.

Name	Group	Profile	Enabled	Action
Allow Syslog Port 514		All	Yes	Allow
adb.exe		Private	Yes	Allow
adb.exe		Private	Yes	Allow
AnyDesk		Public	Yes	Allow
AnyDesk		Private	Yes	Allow
AnyDesk		Domain	Yes	Allow
AnyDesk		Domain	Yes	Allow
AnyDesk		Private	Yes	Allow
AnyDesk		Domain	Yes	Allow
AnyDesk		Domain	Yes	Allow
AnyDesk		Private	Yes	Allow
AnyDesk		Domain	Yes	Allow
AnyDesk		Private	Yes	Allow
DaVinciResolve		Private	Yes	Allow
DaVinciResolveEbmpanel		Private	Yes	Allow
DaVinciResolveElements		Private	Yes	Allow
DaVinciResolveEuphonix		Private	Yes	Allow
DaVinciResolveFuScript		Private	Yes	Allow
DaVinciResolveILCooper		Private	Yes	Allow
DaVinciResolvePanel		Private	Yes	Allow
DaVinciResolveTangent		Private	Yes	Allow
Firefox (C:\Program Files\Mozilla Firefox)		Private	Yes	Allow
Firefox (C:\Program Files\Mozilla Firefox)		Private	Yes	Allow
Microsoft Lync		Public	Yes	Allow
Microsoft Lync		Public	Yes	Allow
Microsoft Lync Ucmapi		Public	Yes	Allow

2) Configured splunk Enterprise server settings to listen a port UDP:514.

Settings → Data inputs → UDP → New local UDP

The screenshot shows the Splunk Settings page. The left sidebar has a search bar and a list of settings categories. The 'Settings' menu is open, and the path 'Data inputs' → 'UDP' is highlighted with orange arrows. The main content area shows a table of data input types. The 'UDP' row is selected, and the 'New Local UDP' button is visible in the top right corner.

Type	Inputs	Actions
Local event log collection Collect event logs from this machine.	-	Edit
Remote event log collections Collect event logs from remote hosts. Note: this uses WMI and requires a domain account.	1	+ Add new
Files & Directories Index a local file or monitor an entire directory.	19	+ Add new
Local performance monitoring Collect performance data from local machine.	0	+ Add new
Remote performance monitoring Collect performance and event information from remote hosts. Requires domain credentials.	0	+ Add new
HTTP Event Collector Receive data over HTTP or HTTPS.	0	+ Add new
TCP Listen on a TCP port for incoming data, e.g. syslog.	0	+ Add new
UDP Listen on a UDP port for incoming data, e.g. syslog.	0	+ Add new

The screenshot shows the 'New Local UDP' button in the top right corner of the 'UDP' settings page. An orange arrow points to the button.

The screenshot shows the 'Add Data' wizard for UDP. The 'Review' step is active, showing the configuration details for the new UDP input. The 'Port' field is set to 514, and the 'Source Type' is set to syslog_kail. The 'Host' field is set to (IP address of the remote server). The 'Index' field is set to main. The 'Submit' button is visible in the top right corner.

Review

Input Type UDP Port
Port Number 514
Source name override N/A
Restrict to Host N/A
Source Type syslog_kail
App Context launcher
Host (IP address of the remote server)
Index main

◆ Step 3: Configure Kali Linux machine to forward log to Receive Logs

On the **kali linux machine** :

1. Open the config file:

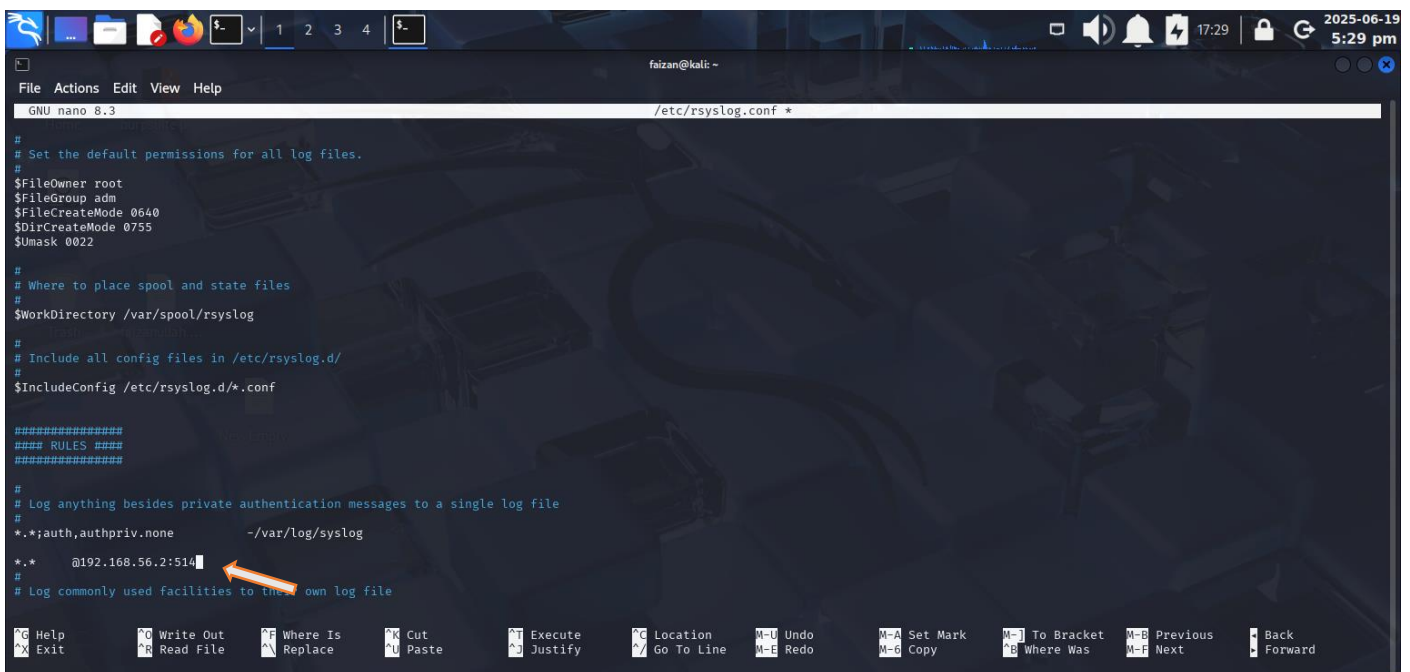
```
# sudo nano /etc/rsyslog.conf
```

2. Add this line to forward logs to the Enterprise Server:

```
*.* @<ENTERPRISE_SERVER_IP>:514
```

3. Save and restart:

```
# sudo systemctl restart rsyslog
```



```
GNU nano 8.3 /etc/rsyslog.conf *

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

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

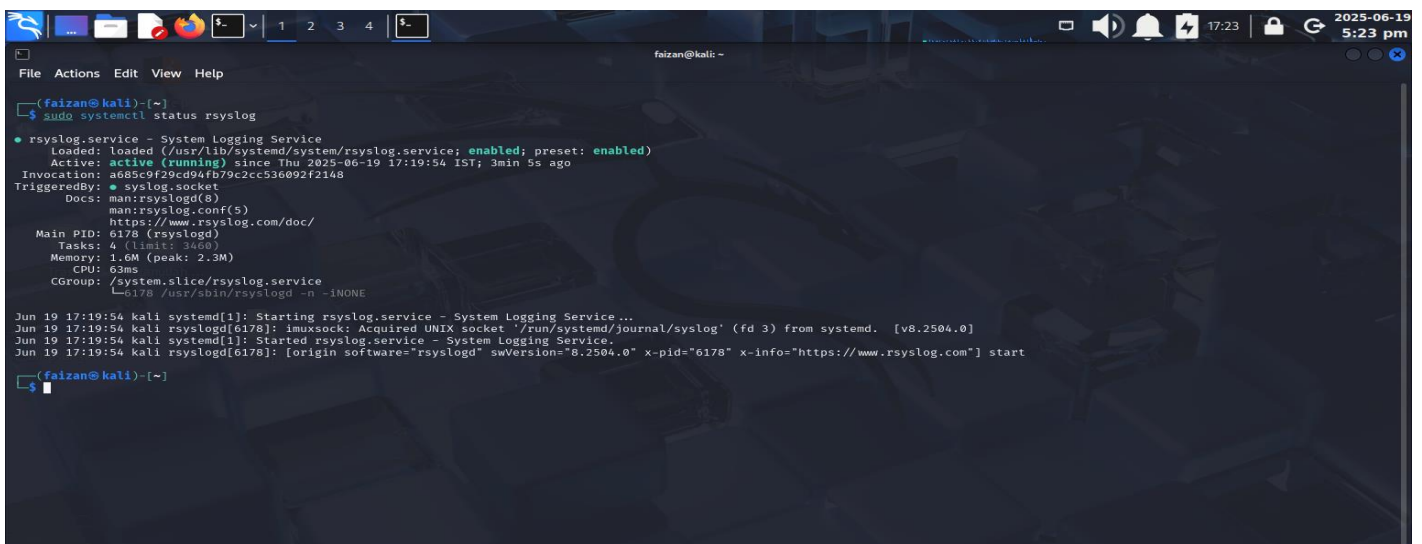
# Include all config files in /etc/rsyslog.d/
#
$IncludeConfig /etc/rsyslog.d/*.conf

#####
### RULES ###
#####

# Log anything besides private authentication messages to a single log file
#
*.*;auth,authpriv.none -/var/log/syslog

*.* @192.168.56.2:514
#
# Log commonly used facilities to their own log file
```

4. Check rsyslog Status: # sudo Systemctl status rsyslog.



```
(faizan@kali)-[~]
$ sudo systemctl status rsyslog

● rsyslog.service - System Logging Service
   Loaded: loaded (/usr/lib/systemd/system/rsyslog.service; enabled; preset: enabled)
   Active: active (running) since Thu 2025-06-19 17:19:54 IST; 3min 5s ago
   Invocation: ad85c9f29cd94fb79c2cc536092f2148
   TriggeredBy: ● syslog.socket
     Docs: man:rsyslogd(8)
           man:rsyslog.conf(5)
           https://www.rsyslog.com/doc/
   Main PID: 6178 (rsyslogd)
     Tasks: 4 (limit: 3460)
    Memory: 1.6M (limit: peak: 2.3M)
       CPU: 63ms
    CGroup: /system.slice/rsyslog.service
           └─6178 /usr/sbin/rsyslogd -n -iNONE

Jun 19 17:19:54 kali systemd[1]: Starting rsyslog.service - System Logging Service...
Jun 19 17:19:54 kali rsyslogd[6178]: imuxsock: Acquired UNIX socket '/run/systemd/journal/syslog' (fd 3) from systemd. [v8.2504.0]
Jun 19 17:19:54 kali systemd[1]: Started rsyslog.service - System Logging Service.
Jun 19 17:19:54 kali rsyslogd[6178]: [origin software="rsyslogd" swVersion="8.2504.0" x-pid="6178" x-info="https://www.rsyslog.com"] start

(faizan@kali)-[~]
$
```

◆ Step 4: Configure Ubuntu (Intermediate) to Forward Logs to Enterprise

On the **Ubuntu Server** (Intermediate):

```
splunk_uf@splunkufserver: ~  
splunk_uf@splunkufserver:~$ sudo apt install rsyslog  
[sudo] password for splunk_uf:  
Reading package lists... Done  
Building dependency tree... Done  
Reading state information... Done  
rsyslog is already the newest version (8.2312.0-3ubuntu9.1).  
rsyslog set to manually installed.  
0 upgraded, 0 newly installed, 0 to remove and 1 not upgraded.  
splunk_uf@splunkufserver:~$
```

1. Open the config file:

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

2. Add this line to forward logs to the Enterprise Server:

```
*.* @<ENTERPRISE_SERVER_IP>:514
```

3. Save and restart:

```
# sudo systemctl restart rsyslog
```

```
splunk_uf@splunkufserver: ~  
GNU nano 7.2 /etc/rsyslog.conf *  
#  
$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  
*.* @192.168.100.5:514  
^G Help ^O Write Out ^W Where Is ^K Cut ^T Execute ^C Location  
^X Exit ^R Read File ^\ Replace ^U Paste ^J Justify ^_ Go To Line
```

4. Check rsyslog Status: # sudo Systemctl status rsyslog

```
splunk_uf@splunkufserver: ~  
● rsyslog.service - System Logging Service  
   Loaded: loaded (/usr/lib/systemd/system/rsyslog.service; enabled; preset: >  
   Active: active (running) since Thu 2025-06-19 17:04:50 UTC; 4h 39min left  
TriggeredBy: ● syslog.socket  
   Docs: man:rsyslogd(8)  
         man:rsyslog.conf(5)  
         https://www.rsyslog.com/doc/  
   Process: 762 ExecStartPre=/usr/lib/rsyslog/reload-apparmor-profile (code=ex>  
   Main PID: 828 (rsyslogd)  
     Tasks: 4 (limit: 2246)  
   Memory: 4.0M (peak: 5.1M)  
     CPU: 568ms  
   CGroup: /system.slice/rsyslog.service  
           └─828 /usr/sbin/rsyslogd -n -iNONE  
  
Jun 19 17:08:02 splunkufserver rsyslogd[828]: action 'action-8-builtin:omfwd' r>  
Jun 19 17:08:02 splunkufserver rsyslogd[828]: omfwd/udp: socket 7: sendto() err>  
Jun 19 17:08:02 splunkufserver rsyslogd[828]: omfwd: socket 7: error 101 sendin>  
Jun 19 17:08:02 splunkufserver rsyslogd[828]: action 'action-8-builtin:omfwd' s>  
Jun 19 17:08:02 splunkufserver rsyslogd[828]: action 'action-8-builtin:omfwd' r>  
Jun 19 17:08:02 splunkufserver rsyslogd[828]: omfwd/udp: socket 7: sendto() err>  
Jun 19 17:08:02 splunkufserver rsyslogd[828]: omfwd: socket 7: error 101 sendin>  
Jun 19 17:08:02 splunkufserver rsyslogd[828]: action 'action-8-builtin:omfwd' s>  
lines 1-23
```

Step 5: Configure Kali Linux to Send Logs to Ubuntu

On the **Kali Linux** system:

- Add this line to forward logs to the Ubuntu Forwarder in /etc/rsyslog.conf file .

```

#####
### RULES ###
#####

#
# Log anything besides private authentication messages to a single log file
#
*.;auth,authpriv.none -/var/log/syslog
#*. * @192.168.XX.X:514
#*. * @192.168.100.6:514
# Log commonly used facilities to their own log file
auth,authpriv.* /var/log/auth.log
cron.* /var/log/cron.log
kern.* /var/log/kern.log
mail.* /var/log/mail.log
user.* /var/log/user.log

#
# Emergencies are sent to everybody logged in.
#
*.emerg :omusrmsg:*

```

Save and restart: `# sudo systemctl restart rsyslog.`

◆ Step 6: Configure Splunk Universal Forwarder to Monitor and Forward /var/log/syslog

To forward logs from your Ubuntu system to a Splunk Enterprise server, follow these commands using the **Splunk Universal Forwarder (UF)**.

1. **Check Current Forward Servers:**
sudo ./splunk list forward-server

It shows both:

- **Active Forwards:** Working forwarder IPs
 - **Inactive Forwards:** Configured but not working
2. **Add a Forward Server (Enterprise Splunk Server)**
#sudo ./splunk add forward-server 192.168.100.5:9997
Output confirms: Added forwarding to: 192.168.100.5:9997
 3. **Add Monitor for /var/log/syslog**
#sudo ./splunk add monitor /var/log/syslog
Output: Added monitor of '/var/log/syslog'.

```
splunk_uf@splunkufserver:~$ cd /opt/splunkforwarder/bin
splunk_uf@splunkufserver:/opt/splunkforwarder/bin$ sudo ./splunk list forward-server
[sudo] password for splunk_uf:
Warning: Attempting to revert the SPLUNK_HOME ownership
Warning: Executing "chown -R splunkfwd:splunkfwd /opt/splunkforwarder"
Your session is invalid. Please login.
Splunk username: admin
Password:
Active forwards:
None
Configured but inactive forwards:
192.168.100.10:9997
192.168.100.3:9997
192.168.19.106:9997
192.168.19.196:9997
192.168.202.196:9997
192.168.56.2:9997
splunk_uf@splunkufserver:/opt/splunkforwarder/bin$ sudo ./splunk add forward-server 192.168.100.5:9997
Warning: Attempting to revert the SPLUNK_HOME ownership
Warning: Executing "chown -R splunkfwd:splunkfwd /opt/splunkforwarder"
Added forwarding to: 192.168.100.5:9997.
splunk_uf@splunkufserver:/opt/splunkforwarder/bin$ sudo ./splunk add monitor /var/log/syslog
Warning: Attempting to revert the SPLUNK_HOME ownership
Warning: Executing "chown -R splunkfwd:splunkfwd /opt/splunkforwarder"
Added monitor of '/var/log/syslog'.
splunk_uf@splunkufserver:/opt/splunkforwarder/bin$ _
```

127.0.0.1:8000/en-US/app/search/search?q=search%20host%3Dsplunkufserver&sid=1750337462.320&display.page.search.mode=smart&dispatc...

host=splunkufserver

✓ 288 events (6/18/25 5:30:00.000 PM to 6/19/25 6:21:02.000 PM) No Event Sampling

Events (288) Patterns Statistics Visualization

Timeline format Zoom Out Zoom to Selection Deselect

Format Show: 50 Per Page View: List

Time	Event
6/19/25 6:20:35.011 PM	2025-06-19T12:58:35.011982+00:00 splunkufserver kernel: [UFW BLOCK] IN=enp0s3 OUT= MAC=01:00:5e:00:00:01:b0:53:65:3b:23:18:08:00 SRC=192.168.100.1 DST=224.0.0.1 LEN=32 TOS=0x00 PREC=0xc0 TTL=1 ID=0 DF PROTO=2 host = splunkufserver source = /var/log/kern.log sourcetype = kern-too_small
6/19/25 6:20:35.011 PM	2025-06-19T12:58:35.011982+00:00 splunkufserver kernel: [UFW BLOCK] IN=enp0s3 OUT= MAC=01:00:5e:00:00:01:b0:53:65:3b:23:18:08:00 SRC=192.168.100.1 DST=224.0.0.1 LEN=32 TOS=0x00 PREC=0xc0 TTL=1 ID=0 DF PROTO=2 host = splunkufserver source = /var/log/syslog sourcetype = syslog
6/19/25 6:20:35.011 PM	2025-06-19T12:58:35.011982+00:00 splunkufserver kernel: [UFW BLOCK] IN=enp0s3 OUT= MAC=01:00:5e:00:00:01:b0:53:65:3b:23:18:08:00 SRC=192.168.100.1 DST=224.0.0.1 LEN=32 TOS=0x00 PREC=0xc0 TTL=1 ID=0 DF PROTO=2 host = splunkufserver source = /var/log/ufw.log sourcetype = ufw-too_small
6/19/25 6:20:28.722 PM	2025-06-19T12:58:28.722945+00:00 splunkufserver kernel: [UFW BLOCK] IN=enp0s3 OUT= MAC=08:00:27:47:ba:c7:08:00:27:23:87:85:08:00 SRC=192.168.100.10 DST=192.16.8.100.6 LEN=120 TOS=0x00 PREC=0x00 TTL=64 ID=37541 DF PROTO=UDP SPT=40073 DPT=514 LEN=100 host = splunkufserver source = /var/log/kern.log sourcetype = kern-too_small
6/19/25 6:20:28.722 PM	2025-06-19T12:58:28.722945+00:00 splunkufserver kernel: [UFW BLOCK] IN=enp0s3 OUT= MAC=08:00:27:47:ba:c7:08:00:27:23:87:85:08:00 SRC=192.168.100.10 DST=192.16.8.100.6 LEN=120 TOS=0x00 PREC=0x00 TTL=64 ID=37541 DF PROTO=UDP SPT=40073 DPT=514 LEN=100 host = splunkufserver source = /var/log/ufw.log sourcetype = ufw-too_small

127.0.0.1:8000/en-US/app/search/search?q=search%20host%3D%27192.168.100.6%27&sid=1750336478.300&display.page.search.mode=smart&dispatc...

host="192.168.100.6"

✓ 22 events (6/18/25 5:30:00.000 PM to 6/19/25 6:04:38.000 PM) No Event Sampling

Events (22) Patterns Statistics Visualization

Timeline format Zoom Out Zoom to Selection Deselect

Format Show: 50 Per Page View: List

Time	Event
6/19/25 6:00:41.000 PM	Jun 19 18:00:41 192.168.100.6 Jun 19 12:30:40 splunkufserver snort[1081]: WARNING: No preprocessors configured for policy 0. host = 192.168.100.6 source = udp:514 sourcetype = syslog_kali
6/19/25 6:00:40.000 PM	Jun 19 18:00:40 192.168.100.6 Jun 19 12:30:39 splunkufserver sudo: pam_unix(sudo:auth): authentication failure; logname=splunk_uf uid=1000 euid=0 tty=/dev/tty1 ruser=splunk_uf rhost= user=splunk_uf host = 192.168.100.6 source = udp:514 sourcetype = syslog_kali
6/19/25 6:00:40.000 PM	Jun 19 18:00:40 192.168.100.6 Jun 19 12:30:35 splunkufserver snort[1081]: message repeated 25 times: [WARNING: No preprocessors configured for policy 0.] host = 192.168.100.6 source = udp:514 sourcetype = syslog_kali
6/19/25 6:00:18.000 PM	Jun 19 18:00:18 192.168.100.6 Jun 19 12:30:17 splunkufserver snort[1081]: WARNING: No preprocessors configured for policy 0. host = 192.168.100.6 source = udp:514 sourcetype = syslog_kali
6/19/25 6:00:18.000 PM	Jun 19 18:00:18 192.168.100.6 Jun 19 12:30:16 splunkufserver sudo: pam_unix(sudo:session): session opened for user root(uid=0) by splunk_uf(uid=1000) host = 192.168.100.6 source = udp:514 sourcetype = syslog_kali

Result

You now have:

- ✓ Logs generated on **Kali Linux**
- ✓ Forwarded to **Ubuntu**
- ✓ Finally relayed to **Enterprise Server**

All via secure and structured `rsyslog` configurations.

