# Linux - Setting up a Logging Server

> Last verified: October 2026 against the RHEL 9 remote logging guide and the current rsyslog documentation.

# Summary

This is to setup a logging server to capture logs from any servers on your network.

# Prerequisites

Install of a RedHat or Rocky Linux minimal install (RHEL 9 / Rocky Linux 9 or later)

# Configuration

You will need to edit the file "/etc/rsyslog.conf"

## Editing the file

```
vi /etc/rsyslog.conf
```

You will need to change to the following to allow port 514 to be open

```
# Provides UDP syslog reception
# for parameters see http://www.rsyslog.com/doc/imudp.html
module(load="imudp") # needs to be done just once
input(type="imudp" port="514")

# Provides TCP syslog reception
# for parameters see http://www.rsyslog.com/doc/imtcp.html
module(load="imtcp") # needs to be done just once
```

```
input(type="imtcp" port="514")
```

Open port 514 in the firewall (skip if firewalld is disabled), check the configuration and then restart the rsyslog daemon

```
firewall-cmd --permanent --add-port=514/tcp
firewall-cmd --permanent --add-port=514/udp
firewall-cmd --reload
rsyslogd -N1
systemctl restart rsyslog
```

Port 514 is already labelled `syslogd_port_t` in the default SELinux policy. If you use a different port, add it with `semanage port -a -t syslogd_port_t -p tcp <port>` (and `-p udp` for UDP).

Multi Host Logging to one server

```
vi /etc/rsyslog.conf
```

Add the following

Before this entry "#### RULES ####"

```
$template RemoteLogs,"/var/log/%HOSTNAME%/%PROGRAMNAME%.log"
*.* ?RemoteLogs
& stop
```

This will enable for all host/servers to log to their own folders

The entry should look like this

```
# Provides TCP syslog reception
# for parameters see http://www.rsyslog.com/doc/imtcp.html
module(load="imtcp") # needs to be done just once
input(type="imtcp" port="514")

#custom
$template RemoteLogs,"/var/log/%HOSTNAME%/%PROGRAMNAME%.log"
*.* ?RemoteLogs
& stop

#### RULES ####
```

The directive $template tells the rsyslog daemon to write the received messages to separate logs under /var/log, based on the hostname (client machine name) and the program/application that generated the message, as defined in the template RemoteLogs. The second line “*.* ?RemoteLogs” means record messages from all facilities at all severity levels using the RemoteLogs template. The third line “& stop” stops further processing of those messages, so they are not also written to the default log files. Because this block sits before the RULES section, the server's own messages are also written to /var/log/<its hostname>/.

> Older guides use `& ~` here. The `~` discard action is deprecated and logs a warning on current rsyslog; use `& stop` instead.

# Setup Log Rotate

Create a log file configuration file

```
vi /etc/logrotate.d/remote-hosts
```

then add the following, and change the folder name pattern(s) to match your host names. Each line must match the log files inside the per-host folders.

```
/var/log/server*/*.log
/var/log/web*/*.log
/var/log/vcenter*/*.log
{
    rotate 2
    maxsize 200k
    daily
}
```

Run to make sure the config is good

```
logrotate -d /etc/logrotate.d/remote-hosts
```

# Setup Host Servers

This is what to setup on the servers you wish to log to one server

You must login to the server and then edit the following file

```
vi /etc/rsyslog.conf
```

Once opened, add one of the following lines at the end of the file to send everything (use only one, TCP is recommended). Replace 192.168.x.x with your logging server's IP or hostname, then run `systemctl restart rsyslog`.

```
*.* @192.168.x.x:514    # use @ for UDP protocol
*.* @@192.168.x.x:514   # use @@ for TCP protocol
```

You can also setup specific logging by doing the following

```
auth.* @@192.168.x.x:514   # only for authentication based records
```

# Results

This is what your folder will look like with the host name of the server or device

```
drwx------  2 root   root       42 Aug 29 22:30 router01
drwx------  2 root   root       82 Aug 29 22:32 server01
drwx------  2 root   root       87 Aug 29 22:32 web01
```

This is a look within a folder of a server

```
[/var/log]# cd server01/


root@server01.example.com : Linux : Thu Aug 29 22:35:01 :
[/var/log/server01]# ls -lrt
total 16
-rw------- 1 root root 850 Aug 29 22:30 rsyslogd.log
-rw------- 1 root root  56 Aug 29 22:32 sssd_kcm.log
-rw------- 1 root root 948 Aug 29 22:32 systemd.log
-rw------- 1 root root 251 Aug 29 22:32 CROND.log
```

# Sources

- https://docs.redhat.com/en/documentation/red_hat_enterprise_linux/9/html/security_hardening/assembly_configuring-a-remote-logging-solution_security-hardening
- https://docs.rsyslog.com/doc/configuration/actions.html
- https://docs.rsyslog.com/doc/configuration/converting_to_new_format.html
- https://docs.rsyslog.com/doc/faq/common-config-mistakes.html

---

Revision #1
Created 30 August 2024 00:36:28 by Admin
Updated 24 October 2026 14:10:46 by Admin