

Rsyslog

Tutorials

- [Remote Syslogging with rsyslog on Red Hat Enterprise Linux - Red Hat Customer Portal](#)
- [Chapter 23. Viewing and Managing Log Files Red Hat Enterprise Linux 7 | Red Hat Customer Portal](#)
- [The Definitive Guide to Centralized Logging with Syslog on Linux \(devconnected.com\)](#)
- [????? - ???????????????? \(vbird.org\)](#)

????

```
# Validate the rsyslog configuration
rsyslogd -N 2 -f /etc/rsyslog.conf

# Restart the rsyslog
systemctl restart rsyslog
```

??????????

???: ??????

?????? rsyslog ??????????????????????

```
/etc/rsyslog.d/myapp.conf
```

```
# Save db2audit log to db2audit
# Test command:
# logger -t db2audit -p user.info "Hello, This is Test Message"
if $programname == 'db2audit' then action(type="omfile" file="/var/log/db2audit")
& stop
```



TIP: `user.*`

???: ?????

???????????????????? rsyslog ??????????????????????

`/etc/rsyslog.d/myapp.conf`

```
$ModLoad imfile

$InputFileName /app/your-file.log
$InputFileTag   your-tag
$InputFileStateFile    your-tag
$InputFileSeverity    info
$InputFileFacility    local7
$InputRunFileMonitor

$InputFilePersistStateInterval 1000

local7.* @remote-rsyslog-server:port
```

??????????????

????? (/var/log/messages) ??????????

```
Jul 24 08:50:01 example.com systemd: Created slice user-0.slice.
Jul 24 08:50:01 example.com systemd: Starting Session 150 of user root.
Jul 24 08:50:01 example.com systemd: Started Session 150 of user root.
Jul 24 09:00:01 example.com systemd: Created slice user-0.slice.
Jul 24 09:00:02 example.com systemd: Starting Session 151 of user root.
Jul 24 09:00:02 example.com systemd: Started Session 151 of user root.
```

`/etc/rsyslog.d/ignore-systemd-session-slice.conf`

```
if $programname == "systemd" and ($msg contains "Starting Session" or $msg contains "Started
Session" or $msg contains "Created slice" or $msg contains "Starting user-" or $msg contains
"Starting User Slice of" or $msg contains "Removed session" or $msg contains "Removed slice
User Slice of" or $msg contains "Stopping User Slice of") then stop
```

Central Log Server

Server Configuration

```
/etc/rsyslog.d/10-from-remote.conf
```

```
# Avoid the duplicate messages from local syslog
$template RemoteLogs, "/var/log/%HOSTNAME%/%PROGRAMNAME%.log"
if ($fromhost != "local-server-hostname" ) then ?RemoteLogs
& stop
```

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

```
# 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")
```

Client Configuration

```
/etc/rsyslog.d/10-to-remote.conf
```

```
# remote host is: name/ip:port, e.g. 192.168.0.1:514, port optional
# Use @@ for TCP protocol, @ for UDP protocol
*. * @10.4.1.77:514;RSYSLOG_SyslogProtocol23Format
```

Restrict access to the log server (on Server)

```
/etc/rsyslog.d/9-acl.conf
```

```
# Restrict access to the log server that is sent from
# $AllowedSender <type>, ip[/bits], ip[/bits]
$AllowedSender TCP, 127.0.0.1, 10.15.9.31
```

FAQ

????????????????????

???????????????????? rsyslog ??????????

AIX: ?? AIX ??? syslog ?????????? IP

???AIX syslog ?????? Log Server ?????????? "Message forwarded by \$hostname"
????????????????????? syslogd ??????? -n?

```
startsrc -s syslogd -a "-n"
```

Revision #21

Created 2023-12-14 11:07:58 CST by A-Lang (Admin)

Updated 2025-03-20 11:30:29 CST by A-Lang (Admin)