

8. Linux Syslog

→sudo bash→cat /etc/rsyslog.conf

```
lubuntu@desktop:~$ sudo bash
root@desktop:/home/lubuntu# cat /etc/rsyslog.conf
```

```
vim@(    syslogs    IP):514
wq
```



```
# Use traditional timestamp format.
# To enable high precision timestamps, comment out the following line.
#
$ActionFileDefaultTemplate RSYSLOG_TraditionalFileFormat

# 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

# Epower
*.* @go.sopdom.com:514
```

61,8

底端

```
# Use traditional timestamp format.
# To enable high precision timestamps, comment out the following line.
#
$ActionFileDefaultTemplate RSYSLOG_TraditionalFileFormat

# 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

# Epower
*.* @go.sopdom.com:514
:wq
```

/etc/init.d/rsyslog restart,

```
root@desktop:/home/lubuntu# vi /etc/rsyslog.conf
root@desktop:/home/lubuntu# /etc/init.d/rsyslog restart
Restarting rsyslog (via systemctl): rsyslog.service.
```

, librenms Overview→Syslog→ Syslog

Overview

Devices

Services

Ports

Health

Alerts

admin

Global Search

Syslog

All Devices

All Programs

All Priorities

2021-11-21 09:24

2021-11-22 09:24

Filter

Q

Search

50

Timestamp	Level	Hostname	Program	Message	Prior
2021-11-22 09:24:39	info	www.sopdom.com	SSHD	Disconnected from authenticating user root 114.55.209.81 port 33796 [preauth]	info
2021-11-22 09:24:39	info	www.sopdom.com	SSHD	Received disconnect from 114.55.209.81 port 33796:11: Bye Bye [preauth]	info
2021-11-22 09:24:39	info	www.sopdom.com	RC.LOCAL	www.sopdom.com,5600035FF012,198.13.58.97,10.0.0.203,Intel Core Processor (Skylake, IBRS) #1#2.0,1004316#659952,23775232#22265344#1509888#94%,2.0.4,2028848.43,2.8 GB,8.4 GB	info
2021-11-22 09:24:38	info	www.sopdom.com	SSHD	Failed password for root from 114.55.209.81 port 33796 ssh2	info
2021-11-22 09:24:35	notice	www.sopdom.com	SSHD	pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=114.55.209.81 user=root	notice
2021-11-22 09:24:28	info	www.sopdom.com	RC.LOCAL	www.sopdom.com,5600035FF012,198.13.58.97,10.0.0.203,Intel Core Processor (Skylake, IBRS) #1#0.0,1004316#657856,23775232#22265344#1509888#94%,2.0.4,2028837.38,2.8 GB,8.4 GB	info
2021-11-22	info	www.sopdom.com	SSHD	Disconnected from invalid user hadoop 114.55.209.81 port 56548 [preauth]	info