5. NXLog Linux

Linux Syslog rsyslog.conf

NXLog Community Edition syslog

---

1. rsyslog.conf

```
lubuntu@pc-71:~$ sudo bash
root@pc-71:/home/lubuntu# vi /etc/rsyslog.conf
```

---

2. rsyslog.conf

```
#################
#### 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" permitnonkernelfacility="on")
###########################
#### GLOBAL DIRECTIVES ####
###########################
#
# 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

*.* @192.168.31.16:1514
```

Esc :wq

3. rsyslog

```
root@pc-71:/home/lubuntu# /etc/init.d/rsyslog restart
```

Graylog

Revision #18
Created 26 October 2021 00:42:48 by Epower
Updated 1 November 2021 00:57:31 by Epower