Syslog

Server Information

OS: Ubuntu 24.04.1 LTS

IP-Adresse: 192.168.2.55

Domäne: lab.local

SSH-Verbindung: ssh [Benutzername@IP-Adresse / syslog.lab.local]

Service

graylog-server: Web UI für alle Logs des Syslog Server logs sind unter /var/log/graylog-server/server.log zu finden

syslog-ng: Zentrale verwaltung für Logfiles von allen Servern

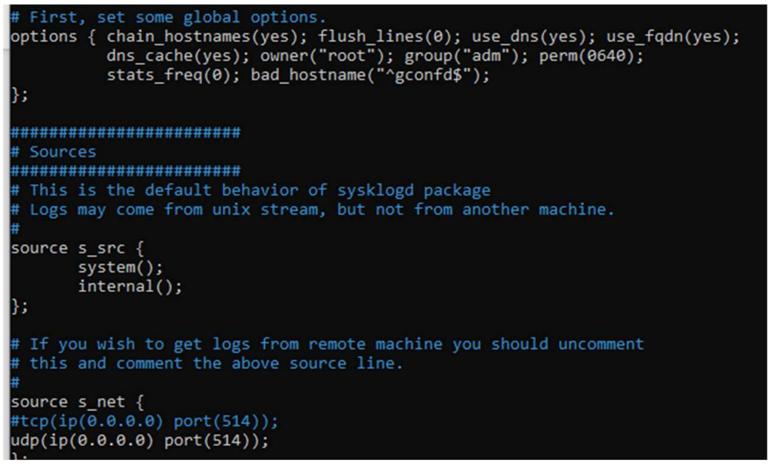
Pfad zu log: /var/log/centralized/$HOST/$YEAR-$MONTH-$DAY.log nach Hostname und Datum jeder Server

Log files: über diese Server gibt es Log files **ansible bitwarden db git git-runner idm idm2 monitoring nodejs npm ovpn syslog.lab.local ubunut www**

Pfad zum Config file

pfad & settings: /etc/syslog-ng/syslog-ng.conf ablegungs Pfad von Logfiles und Port listening 514 udp

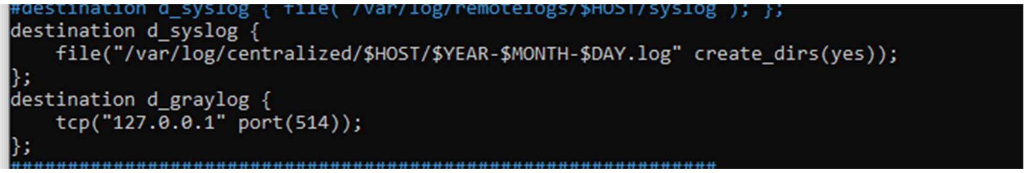
orignial file : /etc/syslog-ng/syslog-ng.conf.orignial



```
# First, set some global options.
options { chain_hostnames(yes); flush_lines(0); use_dns(yes); use_fqdn(yes);
          dns_cache(yes); owner("root"); group("adm"); perm(0640);
          stats_freq(0); bad_hostname("^gconfd$");
};

########################
# Sources
########################
# This is the default behavior of sysklogd package
# Logs may come from unix stream, but not from another machine.
#
source s_src {
       system();
       internal();
};

# If you wish to get logs from remote machine you should uncomment
# this and comment the above source line.
#
source s_net {
#tcp(ip(0.0.0.0) port(514));
udp(ip(0.0.0.0) port(514));
};
```



```
#destination d_syslog { file("/var/log/remotelogs/$HOST/syslog"); };
destination d_syslog {
    file("/var/log/centralized/$HOST/$YEAR-$MONTH-$DAY.log" create_dirs(yes));
};
destination d_graylog {
    tcp("127.0.0.1" port(514));
};
#############################################################
```