

Syslog-NG

```
wget -q0 - https://ose-repo.syslog-ng.com/apt/syslog-ng-ose-pub.asc | sudo apt-key add -  
echo "deb https://ose-repo.syslog-ng.com/apt/ stable debian-bookworm" | sudo tee -a  
/etc/apt/sources.list.d/syslog-ng-ose.list  
apt update  
apt-get install syslog-ng-core syslog-ng-scl
```

A10 Thunder NAT logging

```
nano /etc/syslog-ng/conf.d/A10CGNat.conf
```

```
# Вхідні джерела  
source s_tcp_a10nat_log {  
    network(ip("0.0.0.0") port(1515) transport(tcp) ip-protocol(4));  
};  
  
# Фільтр для перевірки наявності слова "nat"  
filter f_a10nat_cgnat {  
    message("(?i)nat");  
};  
  
# Журнал на виході у форматі JSON  
destination d_a10nat_json {  
    file(  
        "/var/log/syslog-ng/jnat/${SOURCEIP}/${SOURCEIP}_${YEAR}-${MONTH}-${DAY}--${HOUR}-${MIN}.json"  
        template("${format-json --pair UNIXTIME=$R_UNIXTIME --pair PROGRAM=$PROGRAM --pair HOST=$HOST --pair  
SOURCEIP=$SOURCEIP --pair MSG=$MSGONLY}\n")  
        create_dirs(yes)  
    );  
};
```

```
};  
  
# Логічне об'єднання джерела та призначення  
log {  
    source(s_tcp_al0nat_log);  
    filter(f_al0nat_cgnat);  
    destination(d_al0nat_json);  
    flags(flow-control);  
};
```

```
systemctl restart syslog-ng
```

From:

<https://ndp.pp.ua/> - my NoDeny Wiki

Permanent link:

<https://ndp.pp.ua/doku.php/debian/syslog-ng?rev=1721917314>

Last update: **2024/07/25 17:21**

