

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

On A10 Thunder

```
nat-0>show config cgnv6  
!Section configuration: 2296 bytes  
!  
cgnv6 server syslog1 172.16.0.37  
    health-check-disable  
    port 1515 tcp  
!  
  
cgnv6 service-group syslog tcp  
    member syslog1 1515  
!  
  
cgnv6 template logging lsn_logging  
    facility local7  
    severity informational  
    batched-logging-disable  
    service-group syslog  
    source-address  
        ip 172.16.0.6
```

```
disable-log-by-destination
icmp
!
```

On Syslog-NG server

```
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" у назві програми
filter f_a10nat_cgnat {
    program("(?i)nat");
};

# Журнал на виході у форматі JSON. Основне призначення
destination d_a10nat_json_main {
    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)
    );
};

# Журнал на виході у форматі JSON. Запасне призначення
destination d_a10nat_json_backup {
    file(
        "/var/log/syslog-ng/jnat_backup/${SOURCEIP}/${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, фільтра та призначень з умовою для використання запасного каталогу
log {
    source(s_tcp_al0nat_log);
    filter(f_al0nat_cgnat);
    destination(d_al0nat_json_main);
    flags(flow-control);
};

log {
    source(s_tcp_al0nat_log);
    filter(f_al0nat_cgnat);
    destination(d_al0nat_json_backup);
    when not exists("/var/log/syslog-ng/jnat");
    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=1721939343>

Last update: **2024/07/25 20:29**

