

Syslog-NG

Install 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
```

test message from localhost

```
# logger --server 127.0.0.1 -p local0.info -t test "This is a test message"
```

A10 Thunder NAT logging

Syslog-NG server configuration for A10

```
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_al0nat_json_main {
    file(
        "/var/log/syslog-ng/jnat/${SOURCEIP}/${SOURCEIP}_${S_YEAR}-${S_MONTH}-${S_DAY}--${S_HOUR}-${S_MIN}.json"
        template("${(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_al0nat_json_backup {
    file(
        "/var/log/syslog-ng/jnat_backup/${SOURCEIP}/${SOURCEIP}_${S_YEAR}-${S_MONTH}-${S_DAY}--${S_HOUR}-${S_MIN}.json"
        template("${(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_a10nat_json_backup);  
when not exists("/var/log/syslog-ng/jnat");  
flags(flow-control);  
};
```

```
systemctl restart syslog-ng
```

test message from remote linux host

```
# logger --server 172.16.0.37 --port 1515 --tcp --rfc3164 --tag NAT-TCP "This is a test message FROM nat"
```

A10 Thunder Configuration

```
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
```

!

Скрипт міграції логів

```
nano /usr/local/bin/move_jnat_to_nfs
```

```
#!/bin/bash
```

```
# Перевірка, чи основний каталог доступний
```

```
if mountpoint -q /nfs/syslog; then
```

```
    echo "Основний каталог доступний. Переміщую логи старші за 2 хвилини..."
```

```
    find /var/log/syslog-ng/jnat/172.29.100.6/ -type f -mmin +2 -exec mv {} /nfs/syslog/jnat/172.29.100.6/ \;
```

```
    find /var/log/syslog-ng/jnat/172.29.101.6/ -type f -mmin +2 -exec mv {} /nfs/syslog/jnat/172.29.101.6/ \;
```

```
else
```

```
    echo "Основний каталог не доступний. Логи залишаються в запасному каталозі."
```

```
fi
```

```
chmod +x /usr/local/bin/move_jnat_to_nfs
```

```
crontab -e
```

```
*/5 * * * * /usr/local/bin/move_jnat_to_nfs
```

From:

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

Permanent link:

<https://ndp.pp.ua/doku.php/debian/syslog-ng?rev=1721943858>

Last update: **2024/07/26 00:44**

