

Syslog-NG

Install Syslog-NG

```
wget -q0 - https://ose-repo.syslog-ng.com/apt/syslog-ng-ose-pub.asc | gpg --dearmor > /usr/share/keyrings/ose-repo-syslog-ng-keyring.gpg
cat <EOF > /etc/apt/sources.list.d/syslog-ng-ose.list
deb [ signed-by=/usr/share/keyrings/ose-repo-syslog-ng-keyring.gpg ] https://ose-repo.syslog-ng.com/apt/ stable
debian-bookworm
EOF

apt update
apt-get install syslog-ng-core syslog-ng-scl
syslog-ng -V
```

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_al0nat_cgnat {
    program("(?i)nat");
};

# Журнал на виході у форматі JSON. Основне призначення
destination d_al0nat_json_main {
    file(
        "/nfs/syslog/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/${SOURCEIP}/${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_al0nat_json_backup);  
    when not exists("/nfs/syslog/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
```

DNS query logging

```
apt-get install syslog-ng-mod-python
```

```
cat <<EOT > /etc/syslog-ng/conf.d/source_net_udp_514.conf
```

```
source source_net_udp_514 {
    tcp(ip(0.0.0.0) port(514));
};
EOT
cat <<EOT > /etc/syslog-ng/conf.d/source_net_tcp_514.conf
source source_net_tcp_514 {
    tcp(ip(0.0.0.0) port(514));
};
EOT
```

```
cat <<EOT > /etc/syslog-ng/conf.d/dnsdist.conf
#rewrite r_round_min_10 {
#    set("${subst("\\((\\d*)(\\d)$)", "\\1\\10\\", $(env MIN)))" value("R_MIN_10"));
#};

#rewrite r_round_min_10 {
#    subst("^((\\d)(\\d)$)", "${1}0", value("MIN") type("pcre") flags(global) condition(filter(f_dns)));
#    set("${MIN}" value("R_MIN_10")); # Копіюємо MIN → R_MIN_10 після округлення останньої цифри
#};

# Округлення хвилин до 10
rewrite r_round_min_10 {
    # Використовуємо pcre для заміни останньої цифри на 0
    set("$R_MIN_10" value("env $MIN"));
    subst("^[0-9]?([0-9])$", "$1\\0", value("R_MIN_10"));
};

parser p_json {
    json-parser(prefix(".json."));
};

template t_full_dnsdist {
    template("${.json.timestamp},${.json.ip_version},${.json.client_ip},${.json.protocol},${.json.query_type},${.json
.query_name}\\n");
}
```

```
};

template t_custom_dnsdist {
    template("${.json.timestamp},${.json.client_ip},${.json.query_name}\n");
};

destination d_dns_csv {
    file("/var/log/syslog-ng/tmpfs/dnsdist/${YEAR}/${MONTH}/${DAY}/${HOUR}_${R_MIN_10}_queries.csv"
#template("${.json.timestamp},${.json.ip_version},${.json.client_ip},${.json.protocol},${.json.query_type},${.json.query_name}\n")
    template(t_custom_dnsdist)
    template-escape(yes)
    create-dirs(yes)
    flush-lines(100)
    #flush-timeout(1000)
    log-fifo-size(2048)
    disk-buffer(
        mem-buf-size(10000)          # Або mem-buf-size, але краще length, залежно від версії
        disk-buf-size(1073741824)    # 1 GB у байтах
        reliable(yes)
        dir("/var/log/syslog-ng/tmpfs/buffer")
    )
    #init("echo 'timestamp,client_ip,query_name' > $FILENAME");
    flags(no-multi-line)
};

destination d_debug_all {
    file("/var/log/syslog-ng/debug/all.log"
    template("${ISODATE} ${HOST} ${PROGRAM} [${PID}]: ${MSG}\n")
    template-escape(no)
    create-dirs(yes)
    flush-lines(1)
    );
```

```
};  
  
#log {  
#    source(source_net_udp_514);  
#    destination(d_debug_all);  
#};  
  
log {  
    source(source_net_udp_514);  
    rewrite(r_round_min_10);  
    parser(p_json);  
    destination(d_dns_csv);  
};  
EOT
```

Налаштування продуктивності syslog-ng

- `flush_lines` - кількість рядків перед записом
- `time_reopen` - час перед повторним відкриттям
- `log_fifo_size` - розмір черги
- `threaded` - багатопотоковий режим

```
cat << EOF > /etc/syslog-ng/conf.d/performance.conf  
options {  
    flush_lines(1000);  
    time_reopen(10);  
    log_fifo_size(10000);  
    stats_freq(0);  
    threaded(yes);  
    use_dns(no);  
    use_fqdn(no);  
    chain_hostnames(off);  
    keep_hostname(yes);  
};
```

EOF

Перевіримо правильність конфігурацій

```
syslog-ng -s -f /etc/syslog-ng/syslog-ng.conf
```

Перезапуск служб

```
systemctl restart syslog-ng
```

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

Permanent link:
<https://ndp.pp.ua/doku.php/debian/syslog-ng?rev=1746008775>

Last update: **2025/04/30 10:26**

