Linux Syslog-ng ???????

使用 **OpenObserve**時，需要用 **AxoSyslog**來傳送 **LOG**，而 **Synology**和 **OpenWrt**內建只有基本 **Syslog-ng**而不是加強版 **AxoSyslog**

若要升級到 **AxoSyslog**也非常麻煩 **(**不支援或重新編譯 **)**，可以將 **Synology**和 **OpenWrt Syslog** 指向已安裝 **AxoSyslog**的設備讓它來一併轉發

編輯 **/etc/syslog-ng/syslog-ng.conf**

```
options { keep-hostname(yes);chain_hostnames(off); flush_lines(0); use_dns(no); use_fqdn(no);
          dns_cache(no); owner("root"); group("adm"); perm(0640);
          stats(freq(0)); bad_hostname("^gconfd$");
};
########################################################## options內新增keep-hostname(yes); 轉發保留原設備名稱
destination d_openobserve_http {
    openobserve-log(
        url("http://192.168.100.1")
        port(5080)
        organization("default")
        stream("syslog-ng")
        user("root@example.com")
        password("b5wE158wERFTaxe0X")
    );
};



log {
    source(s_src);
    destination(d_openobserve_http);
    flags(flow-control);
};
########################################################## 上面為原本openobserve設定
source s_test {
    udp(ip(192.168.100.100) port(514));
};
log {
    source(s_test);
```

```
    destination(d_openobserve_http);
};
########################################################## 新增本機收到 udp 514 port 的log並轉發到openobserve
```

過濾設定

```
filter f_filter {
    not (
        (program("CRON") and message("/root/temp1.sh"))
    or (facility("authpriv") and message("cron:session"))
    or (program("systemd-logind") and message("suspend"));
        )
};
########################################
以上範例過濾
CRON 進程 關於 訊息包含 "/root/temp1.sh"
facility 為"authpriv" 訊息包含 "cron:session"
systemd-logind 進程 訊息包含 "suspend"




log {
    source(s_src);
    filter(f_filter);
    destination(d_remote);
};
########################################
再轉發設定中加入filter, 這樣關於過濾的訊息不會被轉送到Server
```

Revision #3
Created 19 November 2025 03:06:18 by Jason
Updated 19 November 2025 07:58:53 by Jason