

rsyslog

remote log server

do no log twice

[Rsyslog - prevent local host logging twice](#)

```
module(load="imudp")
input(type="imudp" port="514" ruleset="remote")
ruleset(name="remote"){
    $template RemoteLogs, "/var/log/devices/%HOSTNAME%.log"
    *.* ?RemoteLogs
}
```

dump vars rule

```
$template
DUMP_ALL_VAR, "/rsyslog/dump_hostname=%HOSTNAME%, fromhost=%FROMHOST%, fromhost
-ip=%FROMHOST-IP%, syslogtag=%SYSLOGTAG%, programname=%PROGRAMNAME%, app-
name=%APP-NAME%"
*.* ?DUMP_ALL_VAR
```

rule for TP-Link switch

```
$template TPLinkSwitch, "/rsyslog/%FROMHOST%/syslog.log"
if ($msg contains "T2600G-28TS") then {
    ?TPLinkSwitch
    stop
}
```

From:

<https://niziak.spox.org/wiki/> - niziak.spox.org

Permanent link:

<https://niziak.spox.org/wiki/linux:sw:rsyslog>

Last update: **2023/09/14 09:54**

