Windows Агент NXLog

NXLog Community Edition ????? ?????????????? ? ???????? ?????????????? ?????? ??? ????? ? ???????? ??????? ? ?????? ??? Event ???????? Windows, ???? ????? ??????? ??????????? ??? ???? ????????:

Сбор с файлов

- ????????? ?????: https://nxlog.co/products/nxlog-community-edition/download
- ?????? ?? ?????? ???? ??????: https://docs.nxlog.co/refman/v5.5/im/file.html
- ??? ?????? ??????: `C:\Program Files\nxlog\data\nxlog.log`
- ??????????? ?????? ????????? ?? ????: `C:\Program Files\nxlog\conf\nxlog.conf`

> ????? ?????? ?????? ??????????? ????????? ????????????? ?????? ?????? NXLog

???? ?????? ??????????? ?????? ?? c???e ??????? ? ?????? ???????? WIndows DHCP ? DNS ? ????????? ?? ?????????? KUMA ?? ????????? TCP:

```
<Input win_dhcp_file>
    Module  im_file
    File    "C:\dhcp\Dhcp*.log"
    #File    "C:\Windows\System32\dhcp\DhcpSrvLog*log"
</Input>

<Input win_dns_file>
    Module  im_file
    File    "C:\dns\dns.log"
</Input>

<Output to_kuma_dhcp>
    Module        om_tcp
    Host          10.68.85.125
    Port          5177
</Output>

<Output to_kuma_dns>
    Module        om_tcp
    Host          10.68.85.125
    Port          5178
</Output>

<Route file_to_tcp>
    Path          win_dhcp_file => to_kuma_dhcp
    Path          win_dns_file => to_kuma_dns
</Route>
```

Чтение и отправка Event журналов

???? ?????? ???????????? ?????? ?? c???e ??????? ? ???????? WIndows EventLog ? ???????? ?? HTTP:

```
<Extension xml>
    Module      xm_xml
</Extension>

<Input win_log>
    Module  im_msvistalog
    #Module  im_mseventlog
    Exec    to_xml();
</Input>

<Output to_kuma>
    Module  om_http
    URL     http://10.68.85.129:5140/input
</Output>

<Route to_collecor>
    Path          win_log => to_kuma
</Route>
```

Revision #4
Created 2023-10-30 10:28:36 UTC by Boris Rzr
Updated 2024-11-14 09:49:22 UTC by Koala