

NXLog агент

Альтернатива агента KUMA

- [Windows Агент NXLog](#)
- [Linux Агент NXLog](#)

Windows Агент NXLog

NXLog Community Edition может использоваться в качестве альтернативного агента для сбора и отправки событий с файлов или Event журналов Windows, ниже будут примеры конфигураций для этих настроек:

Сбор с файлов

- Загрузить Агент: <https://nxlog.co/products/nxlog-community-edition/download>
- Детали по маскам пути файлов: <https://docs.nxlog.co/refman/v5.5/im/file.html>
- Лог ошибок агента: `C:\Program Files\nxlog\data\nxlog.log`
- Конфигурация агента находится по пути: `C:\Program Files\nxlog\conf\nxlog.conf`

После каждой правки конфигурации необходимо перезагружать службу агента NXLog

Ниже пример конфигурации агента по сборе событий с файлов журналов Windows DHCP и DNS с отправкой на коллектора KUMA по протоколу 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

Ниже пример конфигурации агента по сборе событий с журналов Windows EventLog и отправка по 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_collector>

```
Path      win_log => to_kuma
```

</Route>

Linux Агент NXLog

NXLog Community Edition может использоваться в качестве альтернативного агента для сбора и отправки событий с файлов на ОС Linux.

- Необходимые пакеты для установки агента:

<https://box.kaspersky.com/f/ca3202dbb39b4b5c929c/>

- Загрузить Агент (для установки на Oracle Linux используйте RHEL пакет):

<https://nxlog.co/products/nxlog-community-edition/download>

- Конфигурация агента находится по пути: `/etc/nxlog/nxlog.conf`
- Конфигурация сервиса находится по пути: `/etc/systemd/system/multi-user.target.wants/nxlog.service`
- Опции запуска:
 - `ExecStartPre=/usr/bin/nxlog -v`
 - `ExecStart=/usr/bin/nxlog -f`
 - `ExecStop=/usr/bin/nxlog -s`
 - `ExecReload=/usr/bin/nxlog -r`