

Продолжаю тему мониторинга различных систем и метрик серверов с помощью известной и бесплатной системы мониторинга заббикс. Сегодня я расскажу, как настроить мониторинг openvpn подключений в zabbix с помощью автообнаружения конфигов пользователей. Способ придуман не мной, приведу ссылку на github страницу проекта.

Содержание:

- 1 Введение
- 2 Настройка zabbix-agent на openvpn сервере
- 3 Мониторинг openvpn подключений в zabbix
- 4 Заключение

Заказать настройку Zabbix от 1000 р.

## Введение

Идея настроить мониторинг openvpn подключений с помощью zabbix витала у меня давно, но никак не доходили руки. Когда выбрал время и сел настраивать, сходу не придумал, а как же лучше это сделать. Так как в задаче много нюансов, то и подходов тоже может быть несколько.

Изначально я думал как-нибудь распарсить лог openvpn и вытаскивать подключенных пользователей оттуда. После того, как внимательно посмотрел на основной лог, понял, что это не самая простая задача, пришлось бы повозиться, чтобы все отладить.

Перед настройкой решил погуглить и посмотреть, что уже есть из готового. И сразу же нашел вот этот проект — <https://github.com/Grifagor/zabbix-openvpn>. Идею быстро понял, оценил все плюсы и минусы и решил не заморачиваться сам, а взять готовое, благо тут все в комплекте:

- Скрипты
- Конфиги

- Шаблон с автообнаружением, графиками и триггерами.

Шаблон имеет следующие элементы в своем составе:

1. Итемы для мониторинга за полученным и переданным трафиком пользователя.
2. Итемы для мониторинга за статусом подключения, отключения пользователя.
3. Триггер со срабатыванием на подключение и отключение пользователя.
4. График полученных, отправленных данных в байтах.
5. График со статусом подключения пользователя.
6. Количество подключенных пользователей к openvpn серверу.

Все эти итемы, графики и триггеры создаются автоматически для каждого пользователя.

Минус один и весьма существенный — добавление итемов в виде отдельных пользователей работает через автообнаружение конфигураций пользователей в директории с `ssd`. Для того, чтобы приведенный способ мониторинга openvpn подключений работал, у вас должны существовать индивидуальные конфигурации пользователей, заданные в конфиге openvpn параметром **client-config-dir**.

Сами конфигурации пользователей могут быть пустыми. Их содержимое не используется. Они нужны только для того, чтобы получить имя пользователя и затем по этому имени анализировать лог файл состояния openvpn, настроенный с помощью параметра **status** в конфигурации openvpn сервера.

В принципе, скрипт обнаружения пользователей можно переделать и искать логины по сертификатам, если они у вас хранятся на сервере. Но с этим тоже есть нюансы. Какие-то сертификаты могут быть отозваны, либо вообще не храниться на сервере. Им там, по большому счету, делать нечего.

С учетом указанных особенностей мониторинга openvpn, переходим к настройке. Возможно, у меня что-то не будет совпадать точь в точь с тем, что есть в репозитории github, так как редактировал под свои реалии, причем достаточно давно. Нюансов уже не помню, буду приводить свои конфиги как есть.

Если у вас еще нет своего сервера для мониторинга, то рекомендую материалы на эту тему. Для тех, кто предпочитает систему CentOS:

1. Установка CentOS 7.
2. Настройка CentOS 7.
3. Установка и настройка zabbix сервера.

То же самое на Debian 9, если предпочитаете его:

1. Установка Debian 9.
2. Базовая настройка Debian 9.
3. Установка и настройка zabbix на debian.

## Настройка zabbix-agent на openvpn сервере

Для настройки мониторинга за openvpn подключениями, создадим скрипт автообнаружения пользователей. У меня директория для ccd файлов следующая — `/etc/openvpn/ccd-users-udp`. В связи с этим делаем скрипт `/etc/zabbix/scripts/discover_vpn.sh`

```
#!/bin/bash

path=/etc/openvpn/ccd-users-udp

users=`ls -F $path | sed 's/\\///g'` # array of users name

echo "{"
echo "\"data\":["

comma=""
for user in $users
do
    echo "    $comma{\"#VPNUSER\": \"$user\"}"
    comma=","
done

echo "]"
echo "}"
```

Сохраняем его, назначаем владельца zabbix и делаем исполняемым.

```
# chown zabbix. discover_vpn.sh && chmod +x discover_vpn.sh
```

Запустите файл и проверьте, что он выводит список пользователей из директории ccd в json формате.

```
[root@xs-gate scripts]# ./discover_vpn.sh
{
  "data": [
    {"#VPNUSER": "a1", "device": "g"},
    {"#VPNUSER": "b", "device": "kina_v"},
    {"#VPNUSER": "b", "device": "v"},
    {"#VPNUSER": "b", "device": "router"},
    {"#VPNUSER": "b", "device": "mp"},
    {"#VPNUSER": "e", "device": "a"},
    {"#VPNUSER": "e", "device": "ev_s"},
    {"#VPNUSER": "g", "device": ""},
    {"#VPNUSER": "g", "device": "n"},
    {"#VPNUSER": "k", "device": "rich_a"},
    {"#VPNUSER": "k", "device": "ova_a"},
    {"#VPNUSER": "n", "device": "router"},
    {"#VPNUSER": "n", "device": "s_ml"},
    {"#VPNUSER": "n", "device": "s_st"},
    {"#VPNUSER": "p", "device": "eva_y"},
    {"#VPNUSER": "p", "device": "v"},
    {"#VPNUSER": "p", "device": "ra_e"},
    {"#VPNUSER": "r", "device": ""},
    {"#VPNUSER": "r", "device": ""},
    {"#VPNUSER": "s", "device": "va_t"},
    {"#VPNUSER": "s", "device": "a_e"},
    {"#VPNUSER": "s", "device": "ov_i"},
    {"#VPNUSER": "z", "device": "ev_router"},
    {"#VPNUSER": "z", "device": "ev_v"},
    {"#VPNUSER": "z", "device": "t"}
  ]
}
```

Далее создаем конфиг с Userparameters — `/etc/zabbix/zabbix_agentd.d/openvpn.conf` следующего содержания:

```
UserParameter=discovery.openvpn,/etc/zabbix/scripts/discover_vpn.sh
UserParameter=user_status.openvpn[*], cat /var/log/openvpn/status-users-udp.log | grep $1, >/dev/null && echo 1 || echo 0
UserParameter=num_user.openvpn, cat /var/log/openvpn/status-users-udp.log | sed -n '/Connected Since/,/ROUTING/p' | sed -e 'ld' -e 'fd' | wc -l
UserParameter=user_byte_received.openvpn[*], if [ "`grep -c $1, /var/log/openvpn/status-users-udp.log`" != "0" ]; then cat /var/log/openvpn/status-users-udp.log | grep $1, | tr ", " "\n" | sed -n '3p' ; else echo "0" ; fi
UserParameter=user_byte_sent.openvpn[*], if [ "`grep -c $1, /var/log/openvpn/status-users-udp.log`" != "0" ]; then cat /var/log/openvpn/status-users-udp.log | grep $1, | tr ", " "\n" | sed -n '4p' ; else echo "0" ; fi
```

Не забудьте в конфиге поменять пути к status логу. У меня он живет по адресу `/var/log/openvpn/status-users-udp.log`.

Перезапускаем zabbix-agent.

```
# systemctl restart zabbix-agent
```

Проверяем работу итемов.

```
# zabbix_agentd -t discovery.openvpn
```

Вы должны увидеть вывод в формате json, как и при запуске скрипта в консоли. Если это не так, то разбирайтесь, в чем проблема. Возможно права на скрипт не дали или ошиблись в конфигурации агента.

Далее можно взять какого-нибудь пользователя, который в данный момент подключен к openvpn серверу и посмотреть по нему информацию.

```
# zabbix_agentd -t user_status.openvpn[ovpn_user1]
user_status.openvpn[ovpn_user1] [t|1]
```

Агент возвращает 1, что значит, что пользователь подключен. Таким же образом можете проверить все остальные **UserParameter**. После того, как убедитесь, что все работает, можете переходить к настройке zabbix сервера для мониторинга за openvpn подключениями.

## Мониторинг оренvpn подключений в zabbix

На сервере zabbix никакой особой настройки для мониторинга оренvpn подключений делать не надо. Достаточно просто импортировать готовый шаблон. Вы можете его взять на гитхабе, либо скачать у меня. Насколько я помню, не менял в нем ничего. Но это не 100%. В любом случае, если изменения и есть, то косметические. Например, интервалы обновления, либо перевод названий.

[Скачать шаблон для оренvpn подключений](#)

После добавления шаблона, прикрепите его к хосту с оренvpn сервером, где ранее настроили zabbix-agent. После этого данные начнут поступать на сервер мониторинга. Проверить это, как обычно, можно в **Latest data**.





<input type="checkbox"/>	openvpn byte_sent po	01/04/2019 06:08:08 PM	0 b/s		<a href="#">Graph</a>
<input type="checkbox"/>	openvpn byte_sent ra	01/04/2019 06:08:09 PM	0 b/s		<a href="#">Graph</a>
<input type="checkbox"/>	openvpn byte_sent ru	01/04/2019 06:09:43 PM	0 b/s		<a href="#">Graph</a>
<input type="checkbox"/>	openvpn byte_sent se	01/04/2019 06:08:10 PM	0 b/s		<a href="#">Graph</a>
<input type="checkbox"/>	openvpn byte_sent sa	01/04/2019 06:08:11 PM	0 b/s		<a href="#">Graph</a>
<input type="checkbox"/>	openvpn byte_sent sc	01/04/2019 06:08:12 PM	0 b/s		<a href="#">Graph</a>
<input type="checkbox"/>	openvpn byte_sent za	01/04/2019 06:08:13 PM	0 b/s		<a href="#">Graph</a>
<input type="checkbox"/>	openvpn byte_sent za	01/04/2019 06:08:14 PM	155 b/s	+44 b/s	<a href="#">Graph</a>
<input type="checkbox"/>	openvpn byte_sent zy	01/04/2019 06:09:00 PM	0 b/s		<a href="#">Graph</a>
<input type="checkbox"/>	openvpn num_user	01/04/2019 06:09:30 PM	1		<a href="#">Graph</a>
<input type="checkbox"/>	openvpn user_status openvpn alex	01/04/2019 06:08:15 PM	0		<a href="#">Graph</a>
<input type="checkbox"/>	openvpn user_status openvpn belk	01/04/2019 06:08:16 PM	0		<a href="#">Graph</a>
<input type="checkbox"/>	openvpn user_status openvpn bob	01/04/2019 06:08:17 PM	0		<a href="#">Graph</a>
<input type="checkbox"/>	openvpn user_status openvpn bob	01/04/2019 06:08:18 PM	0		<a href="#">Graph</a>
<input type="checkbox"/>	openvpn user_status openvpn bob	01/04/2019 06:08:19 PM	0		<a href="#">Graph</a>
<input type="checkbox"/>	openvpn user_status openvpn epis	01/04/2019 06:08:20 PM	0		<a href="#">Graph</a>
<input type="checkbox"/>	openvpn user_status openvpn evs	01/04/2019 06:08:21 PM	0		<a href="#">Graph</a>

serveradmin.ru

После подключения какого-нибудь пользователя, вы получите уведомление и увидите информацию об этом на дашборде.



Problems						
Time	Info	Host	Problem • Severity	Duration	Ack	Actions
03:38:36 PM		xs	Пользователь VPN z...ev_v	2h 34m 28s	No	Done 1
Today						
12/30/2018 03:01:30 PM		xл		5d 3h 11m	No	Done 2
12/29/2018 01:15:30 PM		xs		6d 4h 57m	No	Done 2
12/28/2018 12:48:58 PM		xs		7d 5h 24m	No	Done 2
12/27/2018 10:21:06 AM		m		8d 7h 51m	No	Done 2
December						
11/20/2018 12:19:06 AM		xs		1m 15d 17h	No	Done 2

Если вам это не нужно, то отключите в шаблоне триггер. Если сам триггер все же нужен, но не нужны уведомления о подключениях пользователей, отключите уведомления по триггеру в общем правиле по отправке оповещений, если оно используется.



### Actions

Action Operations Recovery operations Acknowledgement operations

Name

Type of calculation  A and B and C

Conditions	Label	Name	Action
			<a href="#">Remove</a>
			<a href="#">Remove</a>
	C	Trigger name not like Пользователь VPN	<a href="#">Remove</a>

New condition

[Add](#)

Enabled

serveradmin.ru

В общем, кастомизируйте данный шаблон на свой вкус. На этом по самой настройке мониторинга за openvpn пользователями на сервере zabbix все.

## Заключение

Не понравилась статья и хочешь научить меня администрировать? Пожалуйста, я люблю учиться. Комментарии в твоём распоряжении. Расскажи, как сделать правильно!

Описанный способ мониторинга за подключениями openvpn пользователей не идеальный. Надежнее не привязываться к готовому списку пользователей, а напрямую анализировать лог файл openvpn. Иначе, если по какой-то причине пользователя не будет в списке, который формируется правилом автообнаружения, вы ничего не узнаете о подключениях. Особенно это актуально, когда мониторинг используется не просто для сбора информации, а для целей обеспечения безопасности, где важно фиксировать абсолютно все подключения.

В данной статье рассмотрен только мониторинг за подключениями пользователей. Если вам нужно мониторить работу самой службы openvpn, то можете это сделать по другой моей статье — мониторинг работы служб linux.

[Заказать настройку Zabbix от 1000 р.](#)

Помогла статья? Есть возможность отблагодарить автора