



Я чаще всего использую стандартные уведомления от zabbix на почтовый ящик, это позволяет спокойно спать. Тем не менее, решил пойти в ногу со временем и попробовать настроить отправку оповещений из zabbix в популярный мессенджер telegram. К тому же я постоянно активно пользуюсь этим мессенджером и считаю его очень удобным.

Онлайн-курс по "**Архитектор высоких нагрузок**" – Best Practice по HighLoad и отказоустойчивости веб-приложений. Самый полный русскоязычный курс по очень востребованным и хорошо оплачиваемым навыкам. Курс для профессионалов – нужно пройти .

Содержание:

- 1 Введение
- 2 Создание бота в telegram
- 3 Скрипт для отправки оповещений
- 4 Настройка zabbix на отправку уведомлений в телеграм
- 5 Отправка оповещений в группу
- 6 Отправка графиков из zabbix в telegram
- 7 Заключение

Введение

Способов настройки уведомлений из заббикса в телеграм существует несколько. Их можно разделить по информативности:

- Отправка только текстовых оповещений
- Отправка графиков

Так же можно разделить по типу реализации:



- Использовать готового бота
- Создать своего бота для уведомлений
- Отправлять оповещения себе лично или в группу

Я постараюсь разобрать все возможные варианты. Идти будем от простого к сложному. Сначала настроим текстовые оповещения, потом добавим графики. Отправлять будем как в личку, так и в группу.

Кстати, еще один способ отправки уведомлений из zabbix — с помощью звонка через asterisk. Если вам это интересно, читайте соответствующий материал — оповещения zabbix через asterisk.

Я буду настраивать все в zabbix 3.4, установленный на Centos 7. Принципиального значения это не имеет, решение будет одинаково работать практически на всех дистрибутивах linux.

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 10, если предпочитаете его:

1. Установка Debian 10.
2. Базовая настройка Debian.
3. Установка и настройка zabbix на debian.

Приступим к реализации.

Создание бота в telegram

Первым делом создадим бота, через которого будем слать оповещения из заббикса. Для этого добавляем себе в контакты @BotFather и пишем ему сначала /start, потом /newbot.



Мы создали бота для оповещений и получили для него **token**, который нам понадобится далее. Теперь нужно добавить в свой список контактов созданного бота. Для этого найдите его по имени. В моем случае имя @serveradmin_zabbix_bot.

Теперь проверим, как работает отправка уведомлений через нашего бота. Для этого в консоли сервера набираем примерно такую команду:

```
# curl --header 'Content-Type: application/json' --request 'POST' --data '{"chat_id":"210806260","text":"Проверяю отпавку оповещений ботом"}' "https://api.telegram.org/bot526250249:AAFtAqy4ln0BqK5vtU_9IoSlLduhtl8IaGg/sendMessage"
```

Бот пришлет оповещение.



В моем запросе изменяемые данные следующие:

210806260	id моего аккаунта. Чтобы его узнать, добавьте бота @my_id_bot и напишите ему /start
Проверяю работу бота	Текст сообщения
bot526250249:AAFtAqy4ln0BqK5vtU_9IoSlLduhtl8IaGg	Слово bot и дальше token бота. Пишется все в одно слово.

Если все в порядке, двигаемся дальше. Это самая простая часть, тут не должно быть затруднений.

Скрипт для отправки оповещений

Напишем очень простой скрипт, который будет использовать zabbix для отправки оповещений в telegram. Стандартная настройка для директории со скриптами, которые использует заббикс для отправки уведомлений — /usr/lib/zabbix/alertscripts. Поменять ее можно в параметре AlertScriptsPath. Создадим скрипт.

```
# mcedit /usr/lib/zabbix/alertscripts/telegram.sh
```



```
#!/bin/bash

token='526250249:AAftAqy4ln0BqK5vtU_9IoSlLduhtl8IaGg'
chat="$1"
subj="$2"
message="$3"

/usr/bin/curl -s --header 'Content-Type: application/json' --request 'POST' --data
"{\"chat_id\": \"${chat}\", \"text\": \"${subj}\\n${message}\"} \"https://api.telegram.org/bot${token}/sendMessage"
```

Сохраняем файл и делаем исполняемым.

```
# chmod +x /usr/lib/zabbix/alertscripts/telegram.sh
```

Проверим отправку сообщений с помощью нашего скрипта. Для этого запустим его и передадим 3 параметра:

```
# /usr/lib/zabbix/alertscripts/telegram.sh 210806260 Тест 'Проверяю отправку оповещений ботом'
```

Вы должны получить сообщения в телеграме. Если этого не происходит, разберитесь с ошибками, прежде чем двигаться дальше.

Настройка zabbix на отправку уведомлений в телеграм

Идем в web интерфейс zabbix и добавляем новый способ оповещений. Для этого переходим в раздел [Администрирование -> Способы оповещений](#) и создаем новый.



Заполняем необходимые поля.





В данном случае {ALERT.SENDTO}, {ALERT.SUBJECT} и {ALERT.MESSAGE} этот как раз наши параметры, которые мы будем передавать скрипту.

Добавим новый способ оповещения пользователю, для которого они будут добавляться. В моем примере только один пользователь администратор, ему я и добавлю. Для этого идем в раздел [Администрирование -> Пользователи](#). Выбираем нужного пользователя и добавляем ему новый тип оповещений — Telegram.



В поле «Отправлять на» вводим свой Telegram ID. Все, этого достаточно, если у вас используются дефолтные настройки действий разделе [Настройка -> Действия](#). По-умолчанию, там есть действие, которое отправляет администраторам при срабатывании любого триггера оповещение по всем указанным каналам связи.



Я обычно для проверки использую тестовый триггер, который срабатывает, если на сервер подключится по ssh 2 и более юзеров. Сделаю это на своем сервере и посмотрю результат. Когда триггер сработает, на дашборде будет информация.



В телеграме бот пришлет уведомление.



Когда условие срабатывания триггера будет прекращено, я получаю еще одно оповещение о том, что теперь все в порядке.



Скорее всего, вам не понадобится получать уведомления в телеграм на все события, которые происходят в системе. Вам нужно вручную настроить действия, на которые вы хотите получать уведомления. Для этого надо отредактировать дефолтное правило и оставить там только email оповещения. А для телеграма сделать отдельные действия.

Я покажу как это сделать на отдельном примере. Я оставил в дефолтном правиле уведомления только по email. В телеграм я буду получать сообщения



только о срабатывании одного триггера. В данном случае это будет упоминаемый раньше тестовый триггер, срабатывающий на кол-во подключенных ssh пользователей. Вы можете выбрать абсолютно любой триггер из имеющихся в наличии.

Идем в [Настройка -> Действия](#) и создаем новое действие. На первой вкладке «Действие» указываем имя и условие срабатывания.



На вкладке «Операции» добавляем нужное действие. Я выбрал отправку сообщения всей группе администраторов zabbix.






Это же действие продублировал для операций восстановления и подтверждения. Сохраняем действие и проверяем. Вы должны получить следующие оповещения:



Отправка оповещений в группу

Рассмотрим ситуацию, когда мы хотим отправлять уведомления из zabbix не конкретным людям, а сразу в группу, где будут несколько пользователей. Никаких особых настроек для этого не надо. Просто создайте группу в Телеграме, добавьте в эту группу бота @my_id_bot и напишите /start. Так вы узнаете ID группы. В эту же группу добавьте своего бота.

Теперь ID группы надо использовать в способе оповещения пользователя. Там, где мы раньше использовали ID пользователя, теперь ставим ID группы. Можете либо отредактировать предыдущий способ, либо добавить новый. Я добавлю новый, конкретно проделав следующие действия:

1. Создал 2 способа оповещения: Telegram private и Telegram group. 
2. Добавил оба этих способа пользователю администратор, указав соответствующие ID. 
3. Добавил оба эти способа в Действия. 



Хочу обратить внимание, что ID группы начинается с тире, например -288179672. Я этот момент упустил и долго не мог сообразить, почему в группу не отправляются оповещения. Не знал, что этот символ является неотъемлемой частью.

После этого оповещения стали приходят как в приват, так и в общую группу. Можно настраивать разные сообщения на разные события и отправлять их по разным каналам. Это все настраивается под конкретные обстоятельства.

Отправка графиков из zabbix в telegram

Выше я рассказал, как вручную самостоятельно настроить отправку простых текстовых оповещений. В интернете мне попался скрипт на питоне, который умеет все это делать, плюс прикреплять к сообщениям графики. Сейчас я вам расскажу, как это все настроить. Если вам графики не нужны, то настраивать только оповещения все же проще так, как я сделал выше. Получается и понятнее, и быстрее, и питон не надо ставить на сервер, хотя обычно он там и так есть. По крайней мере в centos 7.

Речь идет вот об этом скрипте — <https://github.com/ableev/Zabbix-in-Telegram>. Скопируем себе исходники.

```
# cd /usr/src && git clone https://github.com/ableev/Zabbix-in-Telegram
```

Для его работы, как я уже сказал выше, у вас должен быть установлен в системе python версии 2.6.0. Именно такая версия указана у разработчика скрипта. У меня нормально работает на 2.7.5. Так же для работы необходим pip модуль **requests**. Если у вас его нет, то надо сначала установить pip:

```
# cd /usr/src && wget https://bootstrap.pypa.io/get-pip.py  
# python get-pip.py
```

а потом и сам модуль:

```
# pip install requests
```

Копируем в директорию `/usr/lib/zabbix/alertscripts` файлы `zbxtg.py` и `zbxtg_settings.example.py` из скачанного с github проекта. Последний переименовываем в `zbxtg_settings.py`. Приводим содержимое `zbxtg_settings.py` примерно к такому виду.



```
# -*- coding: utf-8 -*-

tg_key = "526250249:AAFtAqy4ln0BqK5vtU_9IoSLLduhtl8IaGg" # telegram bot api key

zbx_tg_prefix = "zbx_tg" # variable for separating text from script info
zbx_tg_tmp_dir = "/var/tmp/" + zbx_tg_prefix # directory for saving caches, uids, cookies, etc.
zbx_tg_signature = False

zbx_tg_update_messages = True
zbx_tg_matches = {
    "problem": "PROBLEM: ",
    "ok": "OK: "
}

zbx_server = "http://zabbix.server.ru/" # zabbix server full url
zbx_api_user = "zabbix"
zbx_api_pass = "password"
zbx_api_verify = False # True - do not ignore self signed certificates, False - ignore

zbx_basic_auth = False
zbx_basic_auth_user = ""
zbx_basic_auth_pass = ""

proxy_to_zbx = None
proxy_to_tg = None

#proxy_to_zbx = "proxy.local:3128"
#proxy_to_tg = "proxy.local:3128"

google_maps_api_key = None # get your key, see https://developers.google.com/maps/documentation/geocoding/intro

zbx_tg_daemon_enabled = False
```




```
zbx_tg_daemon_wl_ids = [210806260, ]
zbx_tg_daemon_wl_u = ["zeroxzed", ]

zbx_db_host = "localhost"
zbx_db_database = "zabbix"
zbx_db_user = "zabbix"
zbx_db_password = "password"

emoji_map = {
    "OK": "✅",
    "PROBLEM": "❌",
    "info": "ℹ️",
    "WARNING": "⚠️",
    "DISASTER": "🚨",
    "bomb": "💣",
    "fire": "🔥",
    "hankey": "🐔",
}
```

Жирным я выделил те параметры, что нужно поменять. Вам необходимо указать token от бота, который мы ранее создавали, полный url адреса сервера с zabbix, учетную запись к нему. Лучше всего сделать отдельную учетку с доступом только на чтение. Она нужна для получения графиков. Так же вам нужно будет указать telegram id и логин. Они нам не понадобятся, так как мы не будем использовать локальную слежку телеграма, но если поля оставить пустыми, то скрипт ругается на ошибку в конфиге. Поэтому заполняем своими данными. И в конце нужно будет указать параметры доступа к базе данных зabbixа.

Сохраняем конфиг и проверяем работу скрипта. Если вы только создали бота, то не забудьте ему написать личное сообщение, для настройки персональных сообщений, либо из группы, чтобы он мог слать оповещения в группу. Проверим из консоли работу скрипта.

```
# /usr/lib/zabbix/alertscripts/zbx_tg.py "@zeroxzed" "тест" "тестовое сообщение" --debug
```

В личку телеграма должно прийти тестовое сообщение, а в консоли появиться примерно такой вывод.



То же самое сделаем с группой.

```
# /usr/lib/zabbix/alertscripts/zbxtg.py "serveradmin_zabbix_group" "тест" "тестовое сообщение" --debug --group
```

Если все в порядке, двигаемся дальше. Если будут ошибки, сразу разбирайтесь, в чем может быть проблема.

Идем в web интерфейс и добавляем 2 новых способа оповещения: один для частных сообщений, второй для группы. Делаем все то же самое, что и раньше.



Я добавляю ключ **--debug** на время отладки, чтобы лог работы и картинки сохранялись в */var/tmp/*. Это может быть полезно. Потом надо убрать. После этого добавляем новые способы оповещения пользователю. Все то же самое, что делали для первого способа.



Название учетки и группы я указал в виде имени, а не ID. С именами тоже работает, плюс так удобнее.

Теперь создаем новое действие, которое будет использовать созданные только что способы оповещения. Вот мой пример такого действия с использованием графиков и иконок emoji в сообщениях.



Тема по умолчанию {{WARNING}} Проблема: Превышено число SSH пользователей



Сообщение по умолчанию

```
Последнее значение: {ITEM.VALUE1} ({TIME})
zbxtg;graphs
zbxtg;graphs_period=1800
zbxtg;itemid:{ITEM.ID1}
zbxtg;title:{HOST.HOST} — {TRIGGER.NAME}
Важность триггера: {TRIGGER.SEVERITY}
Host: {HOSTNAME} ({HOST.IP})
Описание:
{TRIGGER.DESCRPTION}
```

- {{WARNING}} — макрос для выставления иконки с восклицательным знаком
- zbxtg;graphs — указывает, что будем отправлять график
- zbxtg;itemid:{ITEM.ID1} — параметр автоматически определяет itemid для графика на основании информации об итеме в триггере, можно указать нужный itemid вручную
- zbxtg;title — задает имя для заголовка графика

Все остальное понятно по смыслу. Вот полный список параметров, которые поддерживает скрипт:

zbxtg;graphs	включает отправку графиков
zbxtg;graphs_period=10800	период за который строится график
zbxtg;graphs_width=700	ширина графика
zbxtg;graphs_height=300	высота графика
zbxtg;itemid:{ITEM.ID1}	выбор itemid для графика на основе триггера
zbxtg;title:{HOST.HOST} — {TRIGGER.NAME}	заголовок графика
zbxtg;debug	включает режим отладки, некоторая дополнительная информация сохраняется в tmp_dir
zbxtg;channel	включает возможность отправки оповещения в telegram channel

Для операции восстановления я нарисовал примерно такой шаблон.



Тема по умолчанию {{OK}} Решено: Превышено число SSH пользователей



Сообщение по умолчанию

Server: {HOSTNAME} ({HOST.IP})
Описание:
Проблема устранена!
Время устранения проблемы: {DATE} {TIME}

И для подтверждения.



Тема по умолчанию {{OK}} Подтверждено: Превышено число SSH пользователей

Сообщение по умолчанию {USER.FULLNAME} подтвердил проблему {ACK.DATE} {ACK.TIME} со следующим сообщением:
{ACK.MESSAGE} Текущее состояние проблемы {EVENT.STATUS}

Сохраняем действие, активируем и проверяем. При срабатывании тестового триггера я получаю следующие оповещения с графиком в telegram.



Получилось красиво и наглядно. Если нажать на картинку, то она откроется в большом размере.



Обращаю внимание. Для того, чтобы отправлялся график в telegram, он должен существовать в системе мониторинга. Если его нет, то вы будете получать ошибку, вместо графика. Но текстовое оповещение будет приходить нормально.

Если у вас возникают ошибки с отправкой графиков, то проверить их работу можно в консоли. Вот пример запроса.

```
# # sudo -u zabbix ./zbxtg.py zeroxxed test "$(echo -e 'zbxtg;graphs:
\nzbxtg;graphs_period=3600\nzbxtg;itemid:23301\nzbxtg;title:ololo')"
```

zbxtg.py: Bad Request: PHOTO_INVALID_DIMENSIONS
zbxtg.py: Zabbix user couldn't get graph (probably has no rights to get data from host), check script manually, see



<https://github.com/ableev/Zabbix-in-Telegram/wiki/Graphs>

Это нормальный вывод ошибки, которая указывает на то, что выбран itemid 23301, которого либо не существует, либо к нему нет доступа, либо для него нет графика. Если выбрать правильный itemid, то после выполнения скрипта никакого вывода не будет, а в телеграм будет отправлен выбранный график.



Можете теперь настраивать по своему усмотрению графики, триггеры, события с отправкой оповещений и графиков в telegram.

Заключение

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

Теперь у нас zabbix работает современно, модно, молодежно :) Использует telegram для отправки оповещений с графиками. Функционал удобный и настраивается достаточно просто. У меня практически не было затруднений, когда разбирал тему. Возьму себе на вооружение и буду по необходимости использовать. Хотя сам не люблю оповещения в телеграме, и чаще всего их отключаю, как и от остальных программ. Не нравится, когда меня в каждую минуту могут отвлечь какие-то события. Проверка почты раз в 30 минут самая подходящая интенсивность для меня.

Тем не менее, при работе коллектива, оповещения в общую группу могут быть очень удобны. Особенно, если только на мониторинге сидят отдельные люди, в чью задачу входит оперативная реакция на события.

Практикум по Kali Linux

Курс для тех, кто интересуется проведением тестов на проникновение и хочет практически попробовать себя в ситуациях, близких к реальным. Курс рассчитан на тех, у кого еще нет опыта в информационной безопасности. Обучение длится 3 месяца по 4 часа в неделю. Что даст вам этот курс:



- Искать и эксплуатировать уязвимости или изъяны конфигурации в корпоративных сетях, web сайтах , серверах. Упор на пентест ОС Windows и на безопасность корпоративного сегмента.
- Изучение таких инструментов, как metasploit, sqlmap, wireshark, burp suite и многие другие.
- Освоение инструментария Kali Linux на практике - с ним должен быть знаком любой специалист по ИБ.

Проверьте себя на вступительном тесте и смотрите подробнее программу по .

Помогла статья? Есть возможность отблагодарить автора