

Принципы эффективной работы со службой поддержки Zabbix



Кузюткина Элина Леонидовна

ZABBIX Инженер технической поддержки, тренер

ZABBIX 2019
Conference

RUSSIA

Внимание!

Все персонажи и описываемые
события являются вымышленными.
Любое совпадение с реальными
людьми или событиями - случайно

Вредные советы создания обращений в техподдержку

ZABBIX 2019
Conference
RUSSIA

Никогда не рассказывайте подробностей
проблемы!



Название проблемы: **ОЧЕНЬ ВАЖНО!!!**
Описание проблемы: У нас ничего не работает

Если вы нашли ошибку
Напишите в техподдержку.
Заголовок лучше CAPS-ом:
«ВСЕ СЛОМАЛОСЬ, КАК ТАК ЖИТЬ!!»
Текст в таком письме не нужен,
Подпись так же будет лишней,
Вставьте больше адресатов
И нажмите «Отослать».

Автор, к сожалению, не известен

Название проблемы: Нет данных по хосту.

Описание проблемы: Нет данных по хосту.
Пожалуйста проверьте.



Название проблемы: Ошибка на комплексном экране

Описание проблемы: Срочно нужна удаленная сессия

Не стоит тратить время на форматирование обращения!

Если вывела программа
Очень длинный текст ошибки,
Текст в письмо вставлять не нужно,
Лучше сделайте скриншот.
А потом картинку эту
Поместите в файл Word-а,
Запакуйте ZIP-архивом
И... забудьте приложить.

Автор, к сожалению, не известен

Важность тикетов всегда выбирайте
максимально доступную!

Начинайте описание проблемы с конца!
Вы же уже нашли вариант решения, но
что-то пошло не так?
Спросите «почему?», не озвучивая
корневую причину

Проблема: Как сделать timeout в настройках Zabbix агента больше чем 30 секунд?

Есть скрипт, выполнение которого занимает более 30 секунд. Но вместо обхода ограничения на таймаут, где в случае успеха, могут быть проблемы производительности, следует посмотреть в сторону перехода на связку Zabbix sender + Zabbix траппер как элемент данных.

Не сохраняйте никакой информации
после проблемы!

Всегда достаточно просто спросить
почему такое могло случиться

Никогда не читайте документацию.
Ее писали для слабаков!



Проблема: Триггер переходит в состояние проблема, но даже при выполненных условиях не возвращается в состояние ОК

Выражение проблемы:

```
{app1:log[/logs/catalina.out,"Exception",,,,].regexp(Exception)}=1
```

Выражение восстановления:

```
{app1:log[/logs/catalina.out,"Exception",,,,].nodata(600)}=1
```

Руководство по Zabbix-> Настройка-> Триггеры-> Настройка триггера

*Выражение
восстановления*

Логическое **выражение**, используемое для определения условий, когда проблема решена.
Выражение восстановления вычисляется только после того, как выражение проблемы будет вычислено как ЛОЖЬ. Невозможно решить проблему с помощью выражения восстановления, если условие проблемы всё ещё присутствует.
Это поле опционально и доступно только, если в *Формирование ОК событий* выбрано 'Выражение восстановления'.
Поддерживается начиная с Zabbix 3.2.0.

Обратите внимание, что выражение восстановления будет вычислено только при первом решении события о проблеме. Невозможно решить проблему при помощи выражения восстановления, если условие проблемы всё еще присутствует.

Тогда как правильно? Выражение проблемы:

```
{app1:log[/logs/catalina.out,"Exception",,,,].regexp(Exception)}=1  
and {app1:log[/logs/catalina.out,"Exception",,,,].nodata(600)}=0
```

Проблема: Триггер странно себя ведет

Неправильно выбраны параметры функций, например:

```
min(#3600)
```

```
last(10m)
```


Руководство по Zabbix-> Приложения -> Поддерживаемые функции

| last (<сек #кол-во>,<сдвиг_времени>) | | |
|---|---|--|
| Самое новое значение. | сек (игнорируется, равно #1) или #кол-во (опционально) - N-ое самое новое значение сдвиг_времени (опционально) - смотри avg() | Поддерживаемые типы значений: float, int, str, text, log Обратите внимание, что #кол-во здесь работает иначе, чем во многих других функциях. Например: last() всегда идентичен last(#1) last(#3) - третье самое новое значение (<i>не</i> три последних значения) Zabbix не гарантирует точный порядок значений, если в истории существуют более двух значений менее чем за секунду.. Параметр #кол-во поддерживается начиная с Zabbix 1.6.2. Параметр сдвиг_времени поддерживается начиная с Zabbix 1.8.2. |

Тогда как правильно?

min(3600)

min\max(10m)

last(#10)

Проблема: С недавнего времени Zabbix неприлично тормозит

Использовался MySQL в качестве движка базы данных Zabbix

Документация отнимет много времени,
если вы решили обновиться!
Особенно, если обновление между
мажорными версиями

Перестал работать Java мониторинг после обновления с 3.2 до 4.0

В версии 3.4 протокол Java Gateway изменился,
НО
Java Gateway не был обновлен

Обновление до последней версии заняло 6 часов (время простоя)

Изменения в структуре больших таблиц

Ошибка обновления Zabbix 3.4 до 4.2. Процесс обновления прошел успешно, но после запуска веб-интерфейс не доступен.

В логах несоответствие версий фронтенда и схемы БД. Есть инициализация обновления БД, но нет % завершения обновления схемы

MySQL также был обновлен, но `mysql_upgrade` не выполнен.

Collation и кодировка для части таблиц были заданы неверно.

Настройки сервера БД большей частью по умолчанию

innodb_buffer_pool_size (Хранение данных и индексов) только пятая часть от доступной памяти

Включено кеширование запросов

Включен "index_condition_pushdown"

Всегда используйте настройки по умолчанию!

Внезапно остановился Zabbix сервер

В логах причина. Конфигурация просто выросла из той памяти, что выделяется по умолчанию

```
25552:20180419:110323.811 __mem_malloc: skipped 31 asked 108424 skip_min 304 skip_max 98176
```

```
25552:20180419:030323.811 [file:dbconfig.c,line:90] zbx_mem_realloc(): out of memory (requested 108424 bytes) 25552:20180419:110323.811 [file:dbconfig.c,line:90] zbx_mem_realloc(): please increase CacheSize configuration parameter
```

```
25548:20180419:110323.813 One child process died (PID:25552,exitcode/signal:1). Exiting ...
```

Постоянно висит проблема «Zabbix housekeeper processes more than 75% busy»

Filter ▲

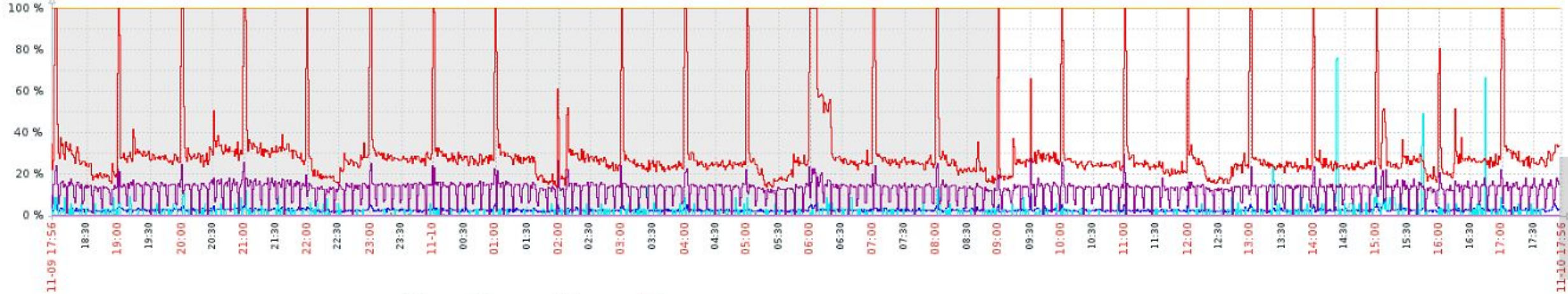
Zoom: 5m 15m 30m 1h 2h 3h 6h 12h 1d 3d 7d 14d 1m 3m 6m All

2016-11-09 17:56 - 2016-11-10 17:56 (now)

<< 6m 1m 7d 1d 12h 1h 5m | 5m 1h 12h 1d 7d 1m 6m >>

1d fixed

Zabbix server: Zabbix internal process busy % (1d)



| | last | min | avg | max |
|--|---------------|---------|------------|---------|
| Zabbix busy timer processes, in % | [avg] 0 % | 0 % | 0.03 % | 0.86 % |
| Zabbix busy escalator processes, in % | [avg] 2.76 % | 1.25 % | 2.53 % | 10.74 % |
| Zabbix busy housekeeper processes, in % | [avg] 100 % | 100 % | 100 % | 100 % |
| Zabbix busy alerter processes, in % | [avg] 0 % | 0 % | 1.43 % | 76.09 % |
| Zabbix busy configuration syncer processes, in % | [avg] 15.06 % | 0 % | 12.55 % | 48.82 % |
| Zabbix busy db watchdog processes, in % | [avg] 0.05 % | 0 % | 0.009626 % | 0.12 % |
| Zabbix busy history syncer processes, in % | [avg] 33.49 % | 13.42 % | 29.14 % | 100 % |
| Zabbix busy self-monitoring processes, in % | [avg] 0 % | 0 % | 0.002591 % | 1.04 % |

Data from Zabbix. Processed in 0.41

Размер базы данных >1,5ТБ

Все компоненты Zabbix установлены на одном сервере с 4 CPU и 8ГБ RAM

Для работы mysql используется конфигурационный файл по умолчанию

НЕ оптимизируйте настройки базы данных для лучшей производительности

НЕ оптимизируйте конфигурацию Zabbix сервера

НЕ настраивайте очистку истории

НЕ создавайте собственные шаблоны

НЕ оптимизируйте настройки базы данных для лучшей производительности

НЕ оптимизируйте конфигурацию Zabbix сервера

НЕ настраивайте очистку истории

НЕ создавайте собственные шаблоны

**НЕ рассказывайте
подробностей проблемы!**

НЕ форматируйте сообщения!

**НЕ указывайте реальную
важность проблемы!**

НЕ читайте документацию!

НЕ рассказывайте
подробностей проблемы!

НЕ форматируйте сообщения!

НЕ указывайте реальную
важность проблемы!

НЕ читайте документацию!

Если ты себя с размаху
Молотком по пальцу — бац!
Не вини того, кто гвозди,
Нам на горе, изобрёл,
Потому что, несомненно,
Виноват в твоей беде
Не гвоздей изобретатель,
А создатель молотка.

Все можно починить простой
перезагрузкой!

Очередь Zabbix содержит много элементов данных?

Частые пропуски данных на графиках?
Отсутствует часть данных?

Срабатывают триггеры с временными функциями?

Не отвечает веб-интерфейс?



Определить проблему и локализовать ее

Найти основную причину и исправить

Оптимизировать

Определить проблему и локализовать ее

База данных: медленные запросы

Zabbix: Шаблоны "Template App Zabbix Server\проху", очередь

Веб интерфейс: режим отладки

Сеть и ОС: инструменты проверки доступности, качества сети, состояния дисковой подсистемы, загрузки CPU\RAM

База данных

LogSlowQueries

```
# grep slow /var/log/zabbix/zabbix_server.log  
slow query: 11.511997 sec, "delete from history where itemid=282492  
limit 5000"  
slow query: 6.043998 sec, "insert into history (itemid,clock,ns,value)  
values ...  
slow query: 19.254535 sec, "delete from history where itemid=488976  
limit 5000"
```

База данных

LogSlowQueries

```
# grep slow /var/log/zabbix/zabbix_server.log  
slow query: 8.501505 sec, "update hosts set lastaccess=1421211815  
where hostid...  
slow query: 37.949541 sec, "select i.itemid, i.hostid, h.proxy_hostid,  
i.type, i.data_type...  
slow query: 70.877295 sec, "select distinct t.triggerid, t.description,  
t.expression, t.error..."
```


База данных

Статистика базы данных, **innotop**, **pg_top**

Инструменты позволяющие исследовать метрики производительности базы данных в реальном времени

```
[R0] Query List (? for help) localhost, 3h, 2.67k QPS,
```

| When | Load | Cxns | QPS | Slow | Se/In/Up/De% | QCacheHit | KCacheHit | BpsIn | BpsOut |
|-------|------|------|-------|-------|--------------|-----------|-----------|---------|--------|
| Now | 0.10 | 413 | 2.67k | 0 | 59/ 6/ 3/ 0 | 0.00% | 100.00% | 774.40k | 8.44M |
| Total | 0.00 | 800 | 1.36k | 1.86k | 51/ 8/ 2/ 0 | 0.00% | 100.00% | 451.79k | 4.81M |

| Cmd | ID | State | User | Host | DB | Time | Query |
|--------|--------|--------------------|--------|------|--------|--------------|---|
| Daemon | 1 | Waiting for next a | | | | 03:16:07.030 | |
| Query | 383981 | Copying to tmp tab | zabbix | | zabbix | 34:23.130 | SELECT DISTINCT t.triggerid FROM triggers t,functions f,items i,hosts_groups hg |
| Query | 386985 | Copying to tmp tab | zabbix | | zabbix | 33:05.811 | SELECT DISTINCT t.triggerid FROM triggers t,functions f,items i,hosts_groups hg |
| Query | 387548 | Copying to tmp tab | zabbix | | zabbix | 32:52.015 | SELECT DISTINCT t.triggerid FROM triggers t,functions f,items i,hosts_groups hg |
| Query | 397535 | Copying to tmp tab | zabbix | | zabbix | 29:37.209 | SELECT DISTINCT t.triggerid FROM triggers t,functions f,items i,hosts_groups hg |
| Query | 398569 | Copying to tmp tab | zabbix | | zabbix | 29:18.436 | SELECT DISTINCT t.triggerid FROM triggers t,functions f,items i,hosts_groups hg |
| Query | 401813 | Copying to tmp tab | zabbix | | zabbix | 28:30.742 | SELECT DISTINCT t.triggerid FROM triggers t,functions f,items i,hosts_groups hg |
| Query | 402601 | Copying to tmp tab | zabbix | | zabbix | 28:17.560 | SELECT DISTINCT t.triggerid FROM triggers t,functions f,items i,hosts_groups hg |
| Query | 404458 | Copying to tmp tab | zabbix | | zabbix | 27:45.404 | SELECT DISTINCT t.triggerid FROM triggers t,functions f,items i,hosts_groups hg |
| Query | 415576 | Copying to tmp tab | zabbix | | zabbix | 24:33.079 | SELECT DISTINCT t.triggerid FROM triggers t,functions f,items i,hosts_groups hg |
| Query | 416777 | Copying to tmp tab | zabbix | | zabbix | 24:14.477 | SELECT DISTINCT t.triggerid FROM triggers t,functions f,items i,hosts_groups hg |
| Query | 420551 | Copying to tmp tab | zabbix | | zabbix | 23:14.913 | SELECT DISTINCT t.triggerid FROM triggers t,functions f,items i,hosts_groups hg |
| Query | 432344 | Copying to tmp tab | zabbix | | zabbix | 19:32.040 | SELECT DISTINCT t.triggerid FROM triggers t,functions f,items i,hosts_groups hg |
| Query | 433241 | Copying to tmp tab | zabbix | | zabbix | 19:12.086 | SELECT DISTINCT t.triggerid FROM triggers t,functions f,items i,hosts_groups hg |
| Query | 436055 | Copying to tmp tab | zabbix | | zabbix | 18:12.712 | SELECT DISTINCT t.triggerid FROM triggers t,functions f,items i,hosts_groups hg |
| Query | 442309 | Copying to tmp tab | zabbix | | zabbix | 16:08.446 | SELECT DISTINCT e.eventid,e.objectid,e.clock,e.ns FROM events e,functions f,items |
| Query | 448041 | Copying to tmp tab | zabbix | | zabbix | 14:28.152 | SELECT DISTINCT t.triggerid FROM triggers t,functions f,items i,hosts_groups hg |
| Query | 448926 | Copying to tmp tab | zabbix | | zabbix | 14:07.957 | SELECT DISTINCT t.triggerid FROM triggers t,functions f,items i,hosts_groups hg |
| Query | 451328 | Copying to tmp tab | zabbix | | zabbix | 13:08.678 | SELECT DISTINCT t.triggerid FROM triggers t,functions f,items i,hosts_groups hg |
| Query | 460067 | Copying to tmp tab | zabbix | | zabbix | 09:24.569 | SELECT DISTINCT t.triggerid FROM triggers t,functions f,items i,hosts_groups hg |
| Query | 460892 | Copying to tmp tab | zabbix | | zabbix | 09:03.653 | SELECT DISTINCT t.triggerid FROM triggers t,functions f,items i,hosts_groups hg |
| Query | 463216 | Copying to tmp tab | zabbix | | zabbix | 08:03.100 | SELECT DISTINCT t.triggerid FROM triggers t,functions f,items i,hosts_groups hg |

База данных

SQL Запросы

```
mysql> select max(id)-(select nextid from ids where table_name =  
"proxy_history" limit 1) from proxy_history;
```

```
+-----+  
|  825  |  
+-----+
```

```
+-----+  
| 16825939 |  
+-----+
```

База данных

SQL Запросы

```
mysql> select count(*),source from events group by source;
```

```
+-----+-----+  
| count(*) |source|  
+-----+-----+  
| 21964352 |    0 |  
| 1099901  |    1 |  
| 108361941|    3 |  
+-----+-----+
```

Где можно найти описание полей для составления запроса в базу?

В описании соответствующих объектов документации Zabbix API.

Еще можно найти подсказку в отладочном режиме веб-интерфейса

```
ps ax | grep zabbix_server
```

```
history syncer #1 [synced 1845 items in 0.257111 sec, syncing history]  
history syncer #2 [synced 24 items in 0.060314 sec, idle 4 sec]  
history syncer #3 [synced 0 items in 0.000018 sec, idle 4 sec]  
history syncer #4 [synced 0 items in 0.000009 sec, syncing history]
```

Выполните несколько раз. Значения меняются?

```
ps ax | grep zabbix_server
```

Во время проблемы:

```
history syncer #1 [synced 962 items in 285.198752 sec,  
syncing history]  
history syncer #2 [synced 867 items in 285.177799 sec,  
syncing history]  
history syncer #3 [synced 1000 items in 284.936376 sec,  
syncing history]  
history syncer #4 [synced 988 items in 285.280719 sec,  
syncing history]
```

Веб интерфейс. Режим отладки

ZABBIX Мониторинг Инвентаризация Отчеты Настройка **Администрирование** Поиск [Поддержка](#) [Share](#) [?](#) [Пользователь](#) [Выход](#)

Общие Прокси Аутентификация **Группы пользователей** Пользователи Способы оповещений Скрипты Очередь

Группы пользователей

[Создать группу пользователей](#) [Фильтр](#)

| <input type="checkbox"/> | Имя ▲ | # | Члены группы | Доступ к веб-интерфейсу | Режим отладки | Состояние |
|--------------------------|--------------------|--------------|--------------|--|------------------------------|------------------------------|
| <input type="checkbox"/> | Enabled debug mode | Пользователи | | Системная по умолчанию | Активировано | Активировано |

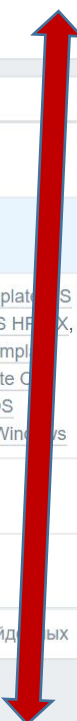
Отображено 1 из 1 найденных

| <input type="checkbox"/> | Имя ▲ | Группы элементов данных | Элементы данных | Триггеры | Графики | Комплексные экраны | Обнаружение | Веб | Присоединенные шаблоны | Присоединен к |
|--------------------------|-----------------------------------|---------------------------|--------------------|-------------|-----------|----------------------|-------------|-----|---|---------------|
| <input type="checkbox"/> | Template App Remote Zabbix proxy | Группы элементов данных 1 | Элементы данных 32 | Триггеры 23 | Графики 4 | Комплексные экраны 1 | Обнаружение | Веб | | |
| <input type="checkbox"/> | Template App Remote Zabbix server | Группы элементов данных 1 | Элементы данных 43 | Триггеры 31 | Графики 6 | Комплексные экраны 1 | Обнаружение | Веб | | |
| <input type="checkbox"/> | Template App Zabbix Agent | Группы элементов данных 1 | Элементы данных 3 | Триггеры 3 | Графики | Комплексные экраны | Обнаружение | Веб | Template OS AIX, Template OS FreeBSD, Template OS HP-UX, Template OS Linux, Template OS Mac OS X, Template OS OpenBSD, Template OS Solaris, Template OS Windows | |
| <input type="checkbox"/> | Template App Zabbix Proxy | Группы элементов данных 1 | Элементы данных 31 | Триггеры 23 | Графики 4 | Комплексные экраны 1 | Обнаружение | Веб | | |
| <input type="checkbox"/> | Template App Zabbix Server | Группы элементов данных 1 | Элементы данных 42 | Триггеры 31 | Графики 6 | Комплексные экраны 1 | Обнаружение | Веб | Zabbix server | |

Отображено 5 из 5 найденных

0 выбрано [Экспорт](#) [Удалить](#) [Удалить и очистить](#)

Zabbix 4.0.7. © 2001–2019, Zabbix SIA [Отладка](#)



Веб интерфейс. Режим отладки

***** Script profiler *****

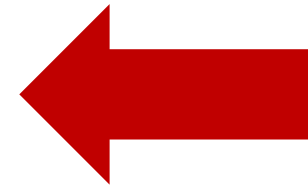
Total time: **10.960905**

Total SQL time: **0.749027**

SQL count: 5636 (selects: 4065 | executes: 1571)

Peak memory usage: 180.5M

Memory limit: 2G



Медленный веб
сервер

Оптимизируйте настройки веб
сервера

Попробуйте nginx =)

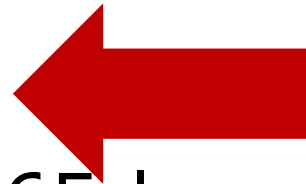
Веб интерфейс. Режим отладки

***** Script profiler *****

Total time: **10.960905**

Total SQL time: **10.749027**

Медленная база
данных

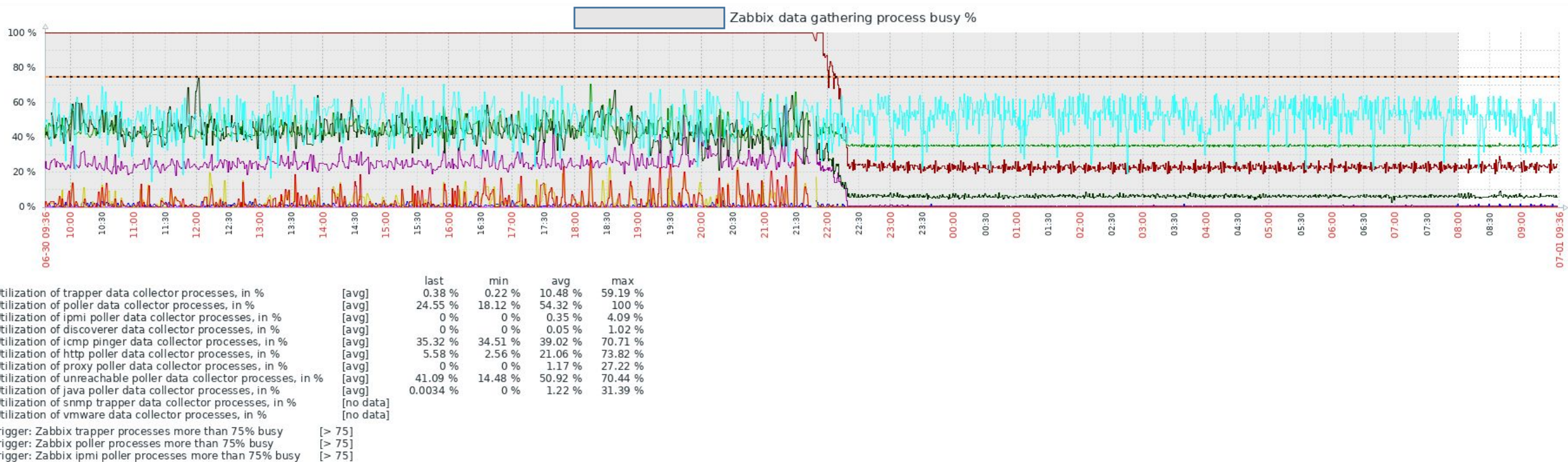


SQL count: 5636 (selects: 4065 | executes: 1571)

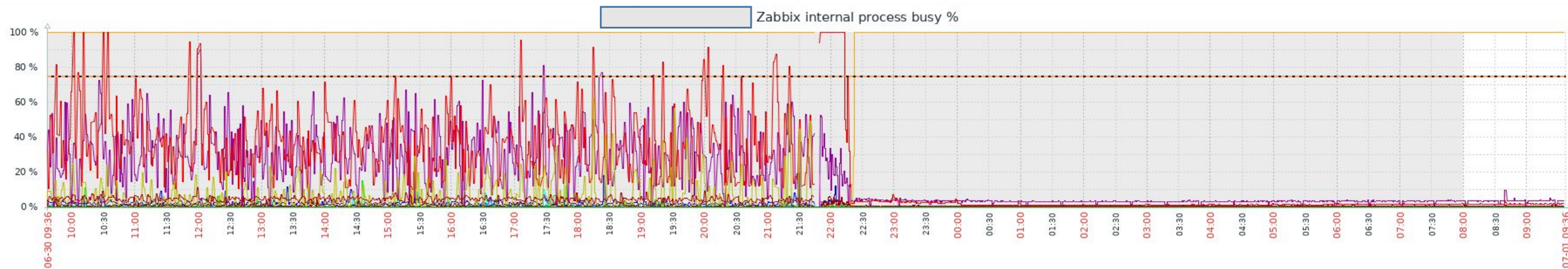
Peak memory usage: 180.5M

Memory limit: 2G

Внутренняя статистика Zabbix

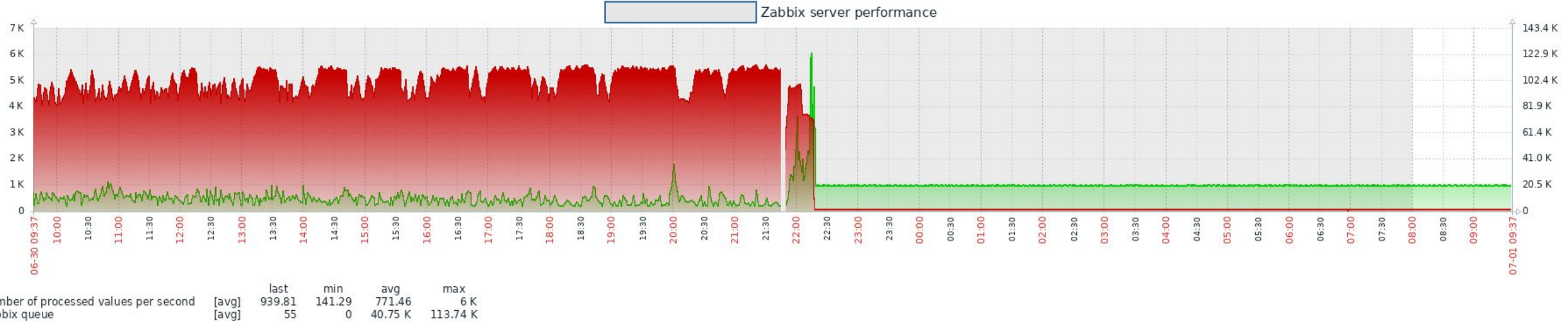


Внутренняя статистика Zabbix



| | last | min | avg | max |
|---|--------------|--------|---------|---------|
| Utilization of timer internal processes, in % | [avg] 0 % | 0 % | 0.16 % | 19.34 % |
| Utilization of escalator internal processes, in % | [avg] 0.05 % | 0 % | 0.96 % | 17.91 % |
| Utilization of housekeeper internal processes, in % | [avg] 100 % | 0 % | 97.06 % | 100 % |
| Utilization of alerter internal processes, in % | [avg] 0 % | 0 % | 0.07 % | 10.08 % |
| Utilization of configuration syncer internal processes, in % | [avg] 3.72 % | 0 % | 14.26 % | 89.89 % |
| Utilization of history syncer internal processes, in % | [avg] 1.78 % | 0.84 % | 17.29 % | 100 % |
| Utilization of self-monitoring internal processes, in % | [avg] 0 % | 0 % | 0.03 % | 18.59 % |
| Utilization of task manager internal processes, in % | [avg] 0 % | 0 % | 0.22 % | 2.95 % |
| Utilization of ipmi manager internal processes, in % | [avg] 0 % | 0 % | 2.48 % | 61.97 % |
| Utilization of alert manager internal processes, in % | [avg] 0.1 % | 0 % | 1.81 % | 11.12 % |
| Utilization of preprocessing manager internal processes, in % | [avg] 0.54 % | 0.1 % | 0.73 % | 9.23 % |
| Utilization of preprocessing worker internal processes, in % | [avg] 0.07 % | 0 % | 0.08 % | 0.58 % |
| Trigger: Zabbix timer processes more than 75% busy | [> 75] | | | |
| Trigger: Zabbix escalator processes more than 75% busy | [> 75] | | | |
| Trigger: Zabbix housekeeper processes more than 75% busy | [> 75] | | | |

Внутренняя статистика Zabbix



Внутренняя статистика Zabbix



Очередь Zabbix

Queue of items to be updated Overview by proxy

| Proxy | 5 seconds | 10 seconds | 30 seconds | 1 minute | 5 minutes | More than 10 minutes |
|-------|-----------|------------|------------|----------|-----------|----------------------|
| | 1 | 0 | 0 | 0 | 0 | 2232 |
| | 0 | 0 | 0 | 0 | 0 | 1572 |
| | 0 | 0 | 0 | 9 | 9 | 1008 |
| | 1418 | 8349 | 4596 | 0 | 1 | 2624 |
| | 0 | 0 | 0 | 0 | 0 | 0 |

Total: 5

Повышение логирования Zabbix процессов

Процессы alerter утилизируются на 100%

```
# zabbix_server -R log_level_increase=alerter
```

Проверяем лог:

```
# grep 23153 /var/log/zabbix/zabbix_server.log
```


Повышение логирования Zabbix процессов

```
23153:20151229:004407.963 In zbx_popen() command:'/usr/  
local/share/zabbix/alertScripts/ZBX_Notifications_1.0.sh 'ZBX'  
'PROBLEM
```

```
23153:20151229:004407.964 End of zbx_popen():6
```

```
23153:20151229:004428.873 In zbx_waitpid()
```

Повешение логирования Zabbix процессов

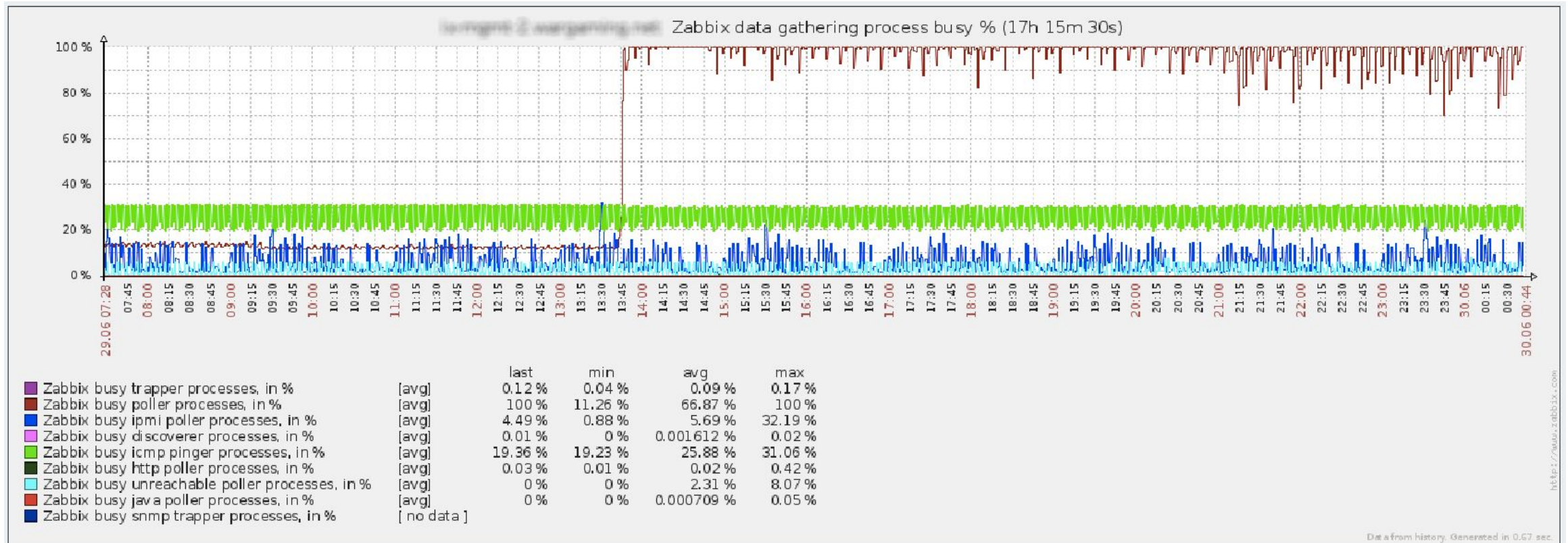
```
23153:20151229:004407.963 In zbx_popen() command:'/usr/  
local/share/zabbix/alertScripts/ZBX_Notifications_1.0.sh 'ZBX'  
'PROBLEM
```

```
23153:20151229:004407.964 End of zbx_popen():6
```

```
23153:20151229:004428.873 In zbx_waitpid()
```

strace

Процессы poller утилизируются на 100%



strace

Процессы poller утилизируются на 100%

Найдем pid интересующего нас процесса

```
# ps aux | grep poller
```

```
# strace -ttT -s 256 -p <poller_pid> -o debug.txt
```

strace

Процессы poller утилизируются на 100%

Roller ждал 25 секунд

```
20:26:56.006121 connect(7, {sa_family=AF_INET,  
sin_port=htons(10050), sin_addr=inet_addr("10.10.10.10")}, 16) = 0  
20:26:56.006280 write(7, "users.online[onlineUsers,server-1]\n", 38)  
= 38 20:26:56.006345 read(7, "ZBXD\1", 5) = 5  
20:27:19.260890 read(7, "\1\0\0\0\0\0\0\0", 8) = 8  
20:27:19.260963 read(7, "0", 2047) = 1
```

tcpdump

Zabbix агент часто недоступен

| Time | Severity | Recovery time | Status | Info | Host | Problem | Duration | Ack | Actions | Tags |
|---------------------|----------|---------------------|----------|------|------|--|----------|-----|---------|------|
| 11:08:01 | High | 11:13:01 | RESOLVED | | | CPU Utilization is over 85% on | 5m | No | | |
| 06:54:06 | Disaster | 06:58:05 | RESOLVED | | | is down | 3m 59s | No | | |
| 06:48:06 | Disaster | 06:57:50 | RESOLVED | | | Zabbix agent on is unreachable for 5 minutes | 9m 44s | No | 2 | |
| 02:39:06 | Disaster | 02:43:05 | RESOLVED | | | is down | 3m 59s | No | | |
| 02:33:06 | Disaster | 02:42:50 | RESOLVED | | | Zabbix agent on is unreachable for 5 minutes | 9m 44s | No | 2 | |
| 2019-06-02 17:59:06 | Disaster | 2019-06-02 18:03:05 | RESOLVED | | | is down | 3m 59s | No | | |
| 2019-06-02 17:53:06 | Disaster | 2019-06-02 18:02:50 | RESOLVED | | | Zabbix agent on is unreachable for 5 minutes | 9m 44s | No | 2 | |
| 2019-06-02 17:09:06 | Disaster | 2019-06-02 17:13:05 | RESOLVED | | | is down | 3m 59s | No | | |
| 2019-06-02 17:03:06 | Disaster | 2019-06-02 17:12:50 | RESOLVED | | | Zabbix agent on is unreachable for 5 minutes | 9m 44s | No | 2 | |
| 2019-06-02 09:29:06 | Disaster | 2019-06-02 09:33:05 | RESOLVED | | | is down | 3m 59s | No | | |
| 2019-06-02 09:23:06 | Disaster | 2019-06-02 09:32:50 | RESOLVED | | | Zabbix agent on is unreachable for 5 minutes | 9m 44s | No | 2 | |
| 2019-06-02 02:14:06 | Disaster | 2019-06-02 02:18:05 | RESOLVED | | | is down | 3m 59s | No | | |
| 2019-06-02 02:08:06 | Disaster | 2019-06-02 02:17:50 | RESOLVED | | | Zabbix agent on is unreachable for 5 minutes | 9m 44s | No | 2 | |
| 2019-06-02 00:49:06 | Disaster | 2019-06-02 00:53:05 | RESOLVED | | | is down | 3m 59s | No | | |
| 2019-06-02 00:43:06 | Disaster | 2019-06-02 00:52:50 | RESOLVED | | | Zabbix agent on is unreachable for 5 minutes | 9m 44s | No | 2 | |

В логах Zabbix сервера встречаются “network error”
Добавим к логу tcpdump

```
tcpdump -w /tmp/zabbix.pcap -npi any port 10050 and host <host_IP>
```

Теперь проанализируем сопоставив события в логе
и дампа

Tcpdump

Нет проблем

| No. | Time | Source | Destination | Protocol | Length | Info |
|------|---------|--------|-------------|----------|--------|--|
| 2161 | 914.757 | | | TCP | 76 | 44024 → 10050 [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 |
| 2162 | 914.757 | | | TCP | 76 | 10050 → 44024 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1260 WS |
| 2163 | 914.757 | | | TCP | 68 | 44024 → 10050 [ACK] Seq=1 Ack=1 Win=14720 Len=0 TSval=356896594 |
| 2164 | 914.758 | | | TCP | 91 | 44024 → 10050 [PSH, ACK] Seq=1 Ack=1 Win=14720 Len=23 TSval=356896594 |
| 2165 | 914.758 | | | TCP | 73 | 10050 → 44024 [PSH, ACK] Seq=1 Ack=24 Win=132096 Len=5 TSval=196226 |
| 2166 | 914.758 | | | TCP | 68 | 44024 → 10050 [ACK] Seq=24 Ack=6 Win=14720 Len=0 TSval=356896594 |
| 2167 | 914.758 | | | TCP | 77 | 10050 → 44024 [FIN, PSH, ACK] Seq=6 Ack=24 Win=132096 Len=9 TSval=196226 |
| 2168 | 914.758 | | | TCP | 68 | 44024 → 10050 [FIN, ACK] Seq=24 Ack=16 Win=14720 Len=0 TSval=356896594 |
| 2169 | 914.758 | | | TCP | 68 | 10050 → 44024 [ACK] Seq=16 Ack=25 Win=132096 Len=0 TSval=196226 |

SYN – устанавливаем
соединение
до хоста на порт 10050

PSH - "push" передаем
данные

FIN – окончание соединения

Linux cooked capture

Packet type: Sent by us (4)

Link-layer address type: 1

Link-layer address length: 6

Source: Vmware_92:22:80 (00:50:56:92:22:80)

Unused: 0000

Protocol: IPv4 (0x0800)

Internet Protocol Version 4, [redacted]

Transmission Control Protocol, [redacted]

Data (23 bytes)

```
0000 00 04 00 01 00 06 00 50 56 92 22 80 00 00 08 00  ....P V.....
0010 45 00 00 4b c8 83 40 00 40 06 fe d2 0a 0a 00 02  E..K..@. @.....
0020 0a 0b 5f 40 ab f8 27 42 d2 e8 d1 b8 5d 4c 19 d9  .._@..'B ....]L..
0030 80 18 00 73 73 94 00 00 01 01 08 0a d4 ba 19 36  ..ss.....f
0040 74 f4 e2 62 5a 42 58 44 01 0a 00 00 00 00 00 00  t..bZBXD .....
0050 00 61 67 65 6e 74 2e 70 69 6e 67                .agent.p ing
```


Tcpdump Нет проблем

tcp.stream eq 199

| No. | Time | Source | Destination | Protocol | Length | Info |
|------|-------------------------|--------|-------------|----------|--------|--|
| 1911 | 2019-04-11 10:07:50,379 | 48612 | 10050 | TCP | 76 | 48612 → 10050 [SYN] Seq=0 Win=14600 Len=0 MSS=1460 |
| 1912 | 2019-04-11 10:07:50,379 | 10050 | 48612 | TCP | 76 | 10050 → 48612 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 |
| 1913 | 2019-04-11 10:07:50,379 | 48612 | 10050 | TCP | 68 | 48612 → 10050 [ACK] Seq=1 Ack=1 Win=14720 Len=0 TS=0 |
| 1914 | 2019-04-11 10:07:50,379 | 48612 | 10050 | TCP | 91 | 48612 → 10050 [PSH, ACK] Seq=1 Ack=1 Win=14720 Len=23 |
| 1917 | 2019-04-11 10:07:50,379 | 10050 | 48612 | TCP | 68 | 10050 → 48612 [ACK] Seq=1 Ack=24 Win=132096 Len=0 |
| 1918 | 2019-04-11 10:08:05,166 | 48612 | 10050 | TCP | 68 | 48612 → 10050 [FIN, ACK] Seq=24 Ack=1 Win=14720 Len=0 |
| 1919 | 2019-04-11 10:08:05,166 | 10050 | 48612 | TCP | 68 | 10050 → 48612 [ACK] Seq=1 Ack=25 Win=132096 Len=0 |
| 1980 | 2019-04-11 10:10:41,304 | 10050 | 48612 | TCP | 73 | 10050 → 48612 [PSH, ACK] Seq=6 Ack=25 Win=132096 Len=23 |
| 1981 | 2019-04-11 10:10:41,304 | 48612 | 10050 | TCP | 56 | 48612 → 10050 [RST] Seq=25 Win=0 Len=0 |
| 1982 | 2019-04-11 10:10:41,304 | 10050 | 48612 | TCP | 77 | 10050 → 48612 [FIN, PSH, ACK] Seq=6 Ack=25 Win=132096 Len=23 |
| 1983 | 2019-04-11 10:10:41,304 | 48612 | 10050 | TCP | 56 | 48612 → 10050 [RST] Seq=25 Win=0 Len=0 |

PSH - "push" передаем данные

PSH - "push" передаем данные (результат проверки Zabbix)

FIN – запрашиваем окончание соединения, не дождавшись данных по проверке Zabbix

SYN – устанавливаем соединение до хоста на порт 10050

Transmission Control Protocol, Src Port: 48612, Dst Port: 10050, Seq: 1, Ack: 1, Len: 23

Data (23 bytes)

Data: 5a425844010a000000000000000006167656e742e70696e67

```
0000 00 04 00 01 00 06 00 50 56 92 22 80 00 00 08 00  . . . . . P V " . . . . .
0010 45 00 00 4b 3b b8 40 00 40 06 8b 9e 0a 0a 00 02  E . K ; @ . @ . . . . .
0020 0a 0b 5f 40 bd e4 27 42 b4 9c be 2a c3 52 68 7c  . _ @ . ' B . . * . Rh |
0030 80 18 00 73 73 94 00 00 01 01 08 0a d4 b5 85 9f  . . . . .
0040 74 f4 6d 3a 5a 42 58 44 01 0a 00 00 00 00 00 00  t : m : Z B X D . . . . .
0050 00 61 67 65 6e 74 2e 70 69 6e 67                . a g e n t . p i n g
```

Tsrdump

Еще один пример

| lo. | Time | Source | Destination | Protocol | Length | Info |
|-----|-------------------------|-------------------|-------------------|----------|--------|-------------------------------|
| 1 | 2016-08-12 23:11:42,087 | 10.[redacted].250 | 10.[redacted].93 | SNMP | 106 | get-request |
| 2 | 2016-08-12 23:11:42,095 | 10.[redacted].93 | 10.[redacted].250 | SNMP | 133 | report 1.3.6.1.6.3.15.1.1.4.0 |
| 3 | 2016-08-12 23:11:42,095 | 10.[redacted].250 | 10.[redacted].93 | SNMP | 167 | encryptedPDU: privKey Unknown |
| 4 | 2016-08-12 23:11:42,103 | 10.[redacted].93 | 10.[redacted].250 | SNMP | 175 | encryptedPDU: privKey Unknown |

[redacted]

Internet Protocol Version 4, Src: 10.[redacted].93, Dst: 10.[redacted].250
User Datagram Protocol, Src Port: 161, Dst Port: 40038
Simple Network Management Protocol

msgVersion: snmpv3 (3)
msgGlobalData
msgAuthoritativeEngineID: 80003a8c04
msgAuthoritativeEngineBoots: 0
msgAuthoritativeEngineTime: 0
msgUserName:

**RFC 2571
EngineID Должно быть
уникально!!**

| Time | Source | Destination | Protocol | Length | Info |
|---------------------------|-------------------|-------------------|----------|--------|-------------------------------|
| 1 2016-08-12 13:45:02,675 | 10.[redacted].250 | 10.[redacted].1 | SNMP | 106 | get-request |
| 2 2016-08-12 13:45:02,675 | 10.[redacted].1 | 10.[redacted].250 | SNMP | 135 | report 1.3.6.1.6.3.15.1.1.4.0 |
| 3 2016-08-12 13:45:02,676 | 10.[redacted].250 | 10.[redacted].1 | SNMP | 306 | encryptedPDU: privKey Unknown |

[redacted]

Internet Protocol Version 4, Src: 10.[redacted].1, Dst: 10.[redacted].250
User Datagram Protocol, Src Port: 161, Dst Port: 40156
Simple Network Management Protocol

msgVersion: snmpv3 (3)
msgGlobalData
msgAuthoritativeEngineID: 80003a8c04
msgAuthoritativeEngineBoots: 0
msgAuthoritativeEngineTime: 0

ВОПРОСЫ?
СПАСИБО!



Кузюткина Элина Леонидовна

ZABBIX Инженер технической поддержки, тренер

ZABBIX 2019
Conference

RUSSIA



twitter.com/zabbix_ru



habr.com/ru/company/zabbix/