3 SNMP трапы

Обзор

Получение SNMP трапов является полной противоположностью запросам к SNMP устройствам.

В этом случае информация отправляется с SNMP устройства и собирается или “ловится” Zabbix'ом.

Обычно трапы отправляются при наступлении некоторых условий и агент подключается на 162 порт сервера (в отличии от 161 порта на стороне агента, который используется для запросов). Использование трапов может помочь обнаружить некоторые кратковременные проблемы, которые происходят между интервалами опроса и могут быть пропущены при запросах данных.

Получение SNMP трапов в Zabbix рассчитано на работу с **snmptrapd** и с одним из встроенных механизмов передачи трапов в Zabbix - либо perl скрипт, либо SNMPTT.

Последовательность действий при получении трапа:

1. **snmptrapd** получает трап
2. snmptrapd передает трап в SNMPTT или вызывает получателя трапов Perl
3. SNMPTT или получатель трапов Perl, форматируют и записывают трап в файл
4. Zabbix SNMP траппер читает и анализирует файл с трапами
5. Zabbix ищет все соответствующие элементы данных с типом “SNMP трап” на интерфейсах узлов сети по каждому трапу, которые совпадают с полученным адресом из трапа. Возьмите на заметку, только выбранный “IP” или “DNS” у интерфейса узла сети используется в процессе поиска совпадения.
6. По каждому найденному SNMP интерфейсу, трап сравнивается со всеми регулярными выражениями из элементов данных “snmptrap[регулярное выражение]”. Если совпадение найдено, трап записывается значением для **всех** совпавших элементов данных. Если совпадений не найдено, но существует элемент данных “snmptrap.fallback”, трап записывается значением для этого элемента данных.
7. Если совпадений не было найдено ни с одним из соответствующих SNMP интерфейсов, Zabbix по умолчанию журналирует несовпавшие трапы. (Это поведение настраивается в “Журналировать не совпадающие SNMP трапы” в Администрирование → Общие → Прочие).

1 Настройка SNMP трапов

Настройка следующих полей в веб-интерфейсе является специфичной для этого типа элементов данных:

- Ваш узел сети должен иметь SNMP интерфейс

В *Настройка → Узлы сети*, в поле **Интерфейсы узла сети** добавьте SNMP интерфейс с корректными IP или DNS адресами. Адрес из каждого полученного трапа сравнивается с IP и DNS адресами всех SNMP интерфейсов для поиска соответствующих узлов сети.

- Настройка элемента данных

В поле **Ключ** используйте один из ключей SNMP трапов:

Ключ		
Описание	**Возвращаемое значение**	**Комментарии**
snmptrap[регулярное выражение]		
Отлов всех SNMP трапов , который совпадают с регулярным выражением, указанном в поле **регулярное выражение**. Если регулярное выражение не указано, принимаются все трапы.	SNMP трап	Этот элемент данных можно привязать только к SNMP интерфейсам. Элемент данных поддерживается начиная с Zabbix **2.0.0**. *Обратите внимание*: Начиная с Zabbix 2.0.5, в параметре этого ключа элемента данных поддерживаются пользовательские макросы и глобальные регулярные выражения.
snmptrap.fallback		
Отлов всех SNMP трапы, которые не совпадают ни с одним из элементов данных snmptrap[] для этого интерфейса.	SNMP трап	Этот элемент данных можно привязать только к SNMP интерфейсам. Элемент данных поддерживается начиная с Zabbix **2.0.0**.

Многострочное совпадение по регулярному выражению в данный момент времени не поддерживается.

Укажите **Тип информации** равным 'Журнал (лог)' для обработки штампов времени. Обратите внимание, что другие форматы, такие как 'Числовой' также приемлемы, но для этого может потребоваться пользовательский обработчик трапов.

Для того чтобы мониторинг SNMP трапов работал, он должен быть сначала корректно настроен.

2 Настройка мониторинга SNMP трапов

Настройка Zabbix сервера/прокси

Для чтения трапов, Zabbix сервер или прокси должны быть настроены на запуск процесса SNMP траппера и должны знать абсолютный путь к файлу с трапами, который заполняется при помощи SNMPTT или получателя трапов Perl. Чтобы это сделать, измените файл конфигурации (zabbix_server.conf или zabbix_proxy.conf):

1. StartSNMPTrapper=1
2. SNMPTrapperFile=[ФАЙЛ С ТРАПАМИ]

Если используется systemd параметр **PrivateTmp**, этот файл вряд ли заработает в */tmp*.

Настройка SNMPTT

Для начала, snmptrapd необходимо настроить на использование SNMPTT.

Для лучшей производительности, SNMPTT необходимо сконфигурировать демоном с использованием **snmptthandler-embedded** для передачи ему трапов. Смотрите инструкции по настройке SNMPTT на его сайте:
http://snmptt.sourceforge.net/docs/snmptt.shtml

При конфигурировании SNMPTT на получение трапов, настройте SNMPTT на журналирование этих трапов:

1. журналирование трапов в файл с трапами, который Zabbix будет читать:
   log_enable = 1
   log_file = [ФАЙЛ С ТРАПАМИ]
2. задайте формат времени/даты:
   date_time_format = %H:%M:%S %Y/%m/%d = [ФОРМАТ ВРЕМЕНИ]

Теперь отформатируйте трапы, чтобы они распознавались Zabbix'ом (измените snmptt.conf):

1. Каждая инструкция FORMAT должна начинаться с “ZBXTRAP [адрес]”, где [адрес] будет сравниваться с IP и DNS адресами у SNMP интерфейсов в Zabbix. Например:
   EVENT coldStart .1.3.6.1.6.3.1.1.5.1 “Status Events” Normal
   FORMAT ZBXTRAP $aA Device reinitialized (coldStart)
2. Подробнее о формате SNMP трапов смотрите ниже.

Не используйте неизвестные трапы - Zabbix может их не распознать. Неизвестные трапы могут быть обработаны, если задать общее событие в snmptt.conf:
EVENT general .* “General event” Normal

Настройка получателя Perl трапов

Требования: Perl, Net-SNMP скомпилированный с --enable-embedded-perl (компилируется по умолчанию начиная с Net-SNMP 5.4)

Получатель трапов Perl (ищите в misc/snmptrap/zabbix_trap_receiver.pl) можно использовать для передачи трапов в Zabbix сервер напрямую с snmptrapd. Для его настройки:

- добавьте perl скрипт в файл конфигурации snmptrapd (snmptrapd.conf), Например:
  perl do "[ПОЛНЫЙ ПУТЬ К СКРИПТУ ПОЛУЧАТЕЛЯ PERL]";
- настройте сам получатель, например:
  $SNMPTrapperFile = '[ФАЙЛ С ТРАПАМИ]';
  $DateTimeFormat = '[ФОРМАТ ДАТЫ/ВРЕМЕНИ]';

Если имя скрипта не заключено в кавычки, snmptrapd откажется запускаться с сообщениями наподобие этих:

```
Regexp modifiers "/l" and "/a" are mutually exclusive at (eval 2) line 1, at
end of line
Regexp modifier "/l" may not appear twice at (eval 2) line 1, at end of line
```

Формат SNMP трапа

Все пользовательские получатели трапов perl и конфигурация SNMPTT трапов должны форматировать трап следующим образом:

[штамп времени] [трап, часть 1] ZBXTRAP [адрес] [трап, часть 2], где

- [штамп времени] - штамп времени используемый в элементах данных типа 'Журнал (лог)'
- ZBXTRAP - заголовок, который указывает, что с этой строки начался новый трап
- [адрес] - IP адрес, используемый для поиска узла сети для этого трапа

Обратите внимание, что “ZBXTRAP” и “[адрес]” при обработке отрезаются из сообщения. Если трап форматируется как-то иначе, Zabbix может разобрать такие трапы неожиданным образом.

Пример трапа:
11:30:15 2011/07/27 .1.3.6.1.6.3.1.1.5.3 Normal “Status Events” localhost - ZBXTRAP 192.168.1.1 Link down on interface 2. Admin state: 1. Operational state: 2
Такое сообщение будет результатом следующего трапа для SNMP интерфейса с IP=192.168.1.1:
11:30:15 2011/07/27 .1.3.6.1.6.3.1.1.5.3 Normal “Status Events” localhost - Link down on interface 2. Admin state: 1. Operational state: 2

3 Требования к системе

Поддержка больших файлов

У Zabbix имеется “Поддержка больших файлов” для файлов SNMP трапов. Максимальный размер файла, который Zabbix может прочитать, это 2^63 (8 Эбайт). Обратите внимание, что файловая система может иметь меньшее ограничение на максимальный размер файлов.

Ротация журнала

Zabbix не предоставляет какую-либо систему ротации журналов - должно быть обработано пользователем. Ротация журналов должна начинаться с переименовывания старого файла и только после этого удалять его, чтобы никакие трапы не пропали:

1. Zabbix открывает файл с трапами с последней известной позиции и переходит к 3 шагу.
2. Zabbix проверяет был ли сротирован в данный момент открытый файл, сравнивая номера inode с заданным у файла трапов номером inode. Если нет открытого файла, Zabbix сбрасывает последнюю позицию и переходит к 1 шагу.
3. Zabbix читает данные из открытого в данный момент файла и устанавливает новую позицию.
4. Обрабатываются новые данные. Если этот файл был ротирован, то он закрывается и Zabbix переходит назад ко 2 шагу.
5. Если не было новых данных, Zabbix засыпает на 1 секунду и возвращается ко 2 шагу.

Файловая система

Из-за реализации файла с трапами, Zabbix'у требуется файловая система с поддержкой inode для того чтобы различать файлы (эта информация берется из вызова stat()).

4 Пример установки

Этот пример использует snmptrapd + SNMPTT для передачи трапов Zabbix серверу. Установка:

1. **zabbix_server.conf** - настройте Zabbix, чтобы запускался SNMP траппер процесс и укажите абсолютный путь к файлу с трапами:
   StartSNMPTrapper=1
   SNMPTrapperFile=/tmp/my_zabbix_traps.tmp
2. **snmptrapd.conf** - добавьте SNMPTT как обработчик трапов:
   traphandle default snmptt
3. **snmptt.ini** - настройте выходной файл и формат времени:
   log_file = /tmp/my_zabbix_traps.tmp
   date_time_format = %H:%M:%S %Y/%m/%d
4. **snmptt.conf** - укажите формат трапов по умолчанию:
   EVENT general .* "General event" Normal
   FORMAT ZBXTRAP $aA $ar
5. Создайте ТЕСТ элемент данных с типом SNMP трап:
   Узел сети с IP адресом SNMP: 127.0.0.1
   Ключ: snmptrap["General"]
   Формат времени журнала: hh:mm:ss yyyy/MM/dd

В результате:

1. Используйте следующую команду для отправки трапа:
   snmptrap -v 1 -c public 127.0.0.1 '.1.3.6.1.6.3.1.1.5.3' '0.0.0.0' 6 33 '55' .1.3.6.1.6.3.1.1.5.3 s "teststring000"
2. Полученный трап:
   15:48:18 2011/07/26 .1.3.6.1.6.3.1.1.5.3.0.33 Normal "General event" localhost - ZBXTRAP 127.0.0.1 127.0.0.1
3. Значение ТЕСТ элемента данных:
   15:48:18 2011/07/26 .1.3.6.1.6.3.1.1.5.3.0.33 Normal "General event" localhost - 127.0.0.1

В этом примере используется SNMPTT как **traphandle**. Для лучшей производительности на продуктивных системах используйте встроенный Perl для передачи трапов от snmptrapd к SNMPTT или напрямую Zabbix'у.

5 Смотрите также

- Руководство по настройке SNMP трапов на CentOS на сайте zabbix.org [en]