3 SNMP трапы

Обзор

Получение SNMP трапов является противоположностью к запросам к SNMP устройствам.

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

Обычно трапы отправляются на некоторые условия и агент подключения на 162 порт сервера (в отличии от 161 порта на стороне агента, который используется для запросов). Использование трапов может 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 одним из встроенных механизмов для 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, форматирует и записывает трап в файл
4. Zabbix SNMP траппер читает и анализирует файл с трапами
5. Для каждого трапа Zabbix ищет все соответствующие SNMP интерфейса на узлах сети по полученными адресам IP или DNS
6. Для каждого найденного SNMP интерфейса, трап сравнивается со всеми регулярными выражениями из элементов данных “snmptrap[регулярное выражение]”. Если найдено, трап устанавливается значением для **всех** совпавших элементов данных. Если не совпадений не найдено, но существует элемент данных “snmptrap.fallback”, трап устанавливается 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 несовпавшие SNMP трапы” в Администрирование → Общие → Другое).

3.1 Настройка SNMP трапов

Настройка соответствующих 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** задайте SNMP интерфейс с корректными IP и 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]		
Ловит все SNMP трапы с соответствующего адреса, которые совпадают с **регулярным выражением**	SNMP трап	Этот элемент данных можно задать только на SNMP устройства. **Этот элемент данных поддерживается начиная с версии 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		
Ловит все SNMP трапы с соответствующего адреса, которые не совпадают ни с одним из элементов данных snmptrap[] для этого интерфейса	SNMP трап	Этот элемент данных можно задать только на SNMP устройства. **Этот элемент данных поддерживается начиная с версии 2.0.0.**

Установите **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 работы мониторинга SNMP трапов, они должны быть сначала корректно заданы.

3.2 Настройка мониторинга SNMP трапов

Настройка Zabbix сервера/прокси

Для чтения трапов, Zabbix сервер или прокси должны быть настроены для запуска процесса SNMP траппера, с указанием файла с трапами, который пишется с помощью SNMPTT или с помощью получателя трапов Perl. Чтобы это сделать, измените файл конфигурации (zabbix_server.conf или zabbix_proxy.conf):

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

Настройка SNMPTT

Для начала, snmptrapd должен быть настроен для использования SNMPTT.

Для лучшей производительности, SNMPTT должен быть настроен 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 настройке SNMPTT на получение трапов, настройке 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. установите 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, задав 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) может быть использован 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 получатель, например:
  $SNMPTrapperFile = '[ФАЙЛ С ТРАПАМИ]';
  $DateTimeFormat = '[ФОРМАТ ДАТЫ/ВРЕМЕНИ]';

Если имя скрипта не заключено в кавычки, snmptrapd откажет в обработке с сообщением в начале, подобных следующих:

```
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 быть отформатированы следующим образом:

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

где

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

Обратите внимание, что “ZBXTRAP” и “[адрес]” при обработке отрезаются. Если трап форматируется инача, Zabbix может разобрать эти трапы неожиданным образом.

Пример строки трапа из файла:

```
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
```

Это будет результатом отформатированного 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
```

3.3 Требования к системе

Ротация журнала

Zabbix не предоставляет какую-нибудь систему ротации журналов - поэтому это должно быть обработано пользователем. Ротация журналов должна сначала переименовать старый файл и только после этого удалить 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, сравнением номера inode с заданным для 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 файл ротируется, то он закрывается и Zabbix переходит назад ко 2 шагу.
5. Если нет 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()).

3.4 Пример установки

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

1. **zabbix_server.conf** - настройте Zabbix для запуска SNMP траппера и задайте файл 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** - определите формат трапа по умолчанию:
   EVENT general .* "General event" Normal
   FORMAT ZBXTRAP $aA $ar
5. Создайте TEST элемент данных типа SNMP:
   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 TEST 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 с snmptrapd в SNMPTT или напрямую Zabbix'y.