Zaredis 12 ноября 2014 в 15:34

Ловим snmp трапы mac-notification с устройств Cisco

PHP

Из песочницы

Несмотря на кажущуюся простоту вопроса, пришлось достаточно долго и нудно собирать информацию по крупицам. В данной публикации я хочу поделиться накопленным опытом.

Итак, mac notification — snmp уведомление, которое будет передавать серверу информацию о mac-адресе устройства на порту коммутатора при включении или отключении этого устройства. Весьма удобная штука, расширяющая возможности мониторинга сети через snmp.

Приступим к настройке

Настройка коммутатора не займет много времени:

```
!В режиме конфигурации
!Добавление новой группы snmp
```

```
snmp-server community имя_группы RO
!Включение mac уведомлений
snmp-server enable traps mac-notification change move threshold
!Показываем, куда отправлять трапы
snmp-server host IP-АДРЕС_СЕРВЕРА имя_группы  mac-notification snmp
!Настройка таблицы уведомлений
mac address-table notification change
mac address-table notification change interval 15
mac address-table notification change history-size 100

!Выбираем нужные порты и включаем отправление трапов при добавлении или о
тключении устройства на портах
int range fa0/1-24
snmp trap mac-notification change added
snmp trap mac-notification change removed
```

Проверить правильность настройки можно в режиме дебага:

```
debug snmp packets
ter mon
```

Если все настроено верно, то мы увидим что-то вроде этого:

```
Nov 11 16:28:51.685: SNMP: Queuing packet to xxx.xxx.xxx.xxx
Nov 11 16:28:51.685: SNMP: V1 Trap, ent cmnMIBNotificationPrefix, addr 1
0.0.28.18, gentrap 6, spectrap 1
 cmnHistMacChangedMsg.37 =
```

```
01 00 XX XX XX XX XX XX 00 14 00
 cmnHistTimestamp.37 = 113588548
Nov 11 16:28:51.937: SNMP: Packet sent via UDP to xxx.xxx.xxx.xxx
```

Рассмотрим подробнее объект cmnHistMacChangedMsg, который передает **шестнадцатеричную строку** из 11 октетов (последние два нуля — всегда конец записи). Первый октет — состояние(01 — устройство добавлено,02 — устройство отключено), следующие 2 октета — номер vlan'a, 6 октетов занимает мак-адрес(в нашем случае он xxxx.xxxx.xxxx), и 2 октета (00 14) — номер порта.
Хочу обратить внимание на следующее: согласно документации, объект cmnHistMacChangedMsg может передавать несколько mac-адресов в одном трапе. В этом случае записи идут подряд, без какого либо разделения, в конец сообщения так же будет дописываться пара нулей.

Настройка сервера состоит из нескольких этапов:

Перед настройкой настоятельно рекомендую проверить, доходят ли udp пакеты до сервера командой tcpdump udp|grep IP_адрес_свича.

1. Установка snmp сервера и стандартных mib:

```
sudo apt-get install snmpd snmp snmptt snmp-mibs-downloader
```

2. Установка нужных MIB-файлов
   По умолчанию, snmp сервер не знает о объекте mac-notification в Cisco. Чтобы сервер смог распознать подобный трап, необходимо скачать .mib файлы с ftp и

положить их в /var/lib/mibs.

Вы должны скачать следующие файлы:

```
CISCO-MAC-NOTIFICATION-MIB
CISCO-QOS-PIB-MIB
CISCO-SMI
CISCO-TC
CISCO-VTP-MIB
```

В случае успешной установки новых mib, на команду

```
snmptranslate -m CISCO-MAC-NOTIFICATION-MIB  .1.3.6.1.4.1.9.9.215
```

сервер ответит

```
CISCO-MAC-NOTIFICATION-MIB::ciscoMacNotificationMIB
```

3. Настройка файлов конфигурации

   - /etc/default/snmpd:
   - /etc/snmp/snmptrapd.conf:
   - /etc/snmp/snmptt.conf:
   - /etc/snmp/snmptt.ini:

Таким образом,snmpd демон слушает порт udp 162 и перенаправляет сообщения на snmptt.Он обрабатывает трап и запускает на исполнение php-скрипт. В конфиге snmptt.ini включен режим дебага, поэтому все входящие трапы будут записываться в /tmp/snmptt.debug.

4. Собственно, сам скрипт обработки(я полагаю, что на сервере уже установлен и настроен php и mysql):
   - /opt/script.php

Данная статья — всего лишь конкретный пример широкого применения snmp трапов. На Cisco ftp можно найти еще больше интересных функций.

Надеюсь, моя публикация помогла вам сэкономить время.

Теги: snmp trap, cisco, сетевые технологии, php

Поделиться публикацией

ПОХОЖИЕ ПУБЛИКАЦИИ

19 июня 2015 в 15:59

Уровень сигнала трансивера через SNMP в Cisco

+11 13,3k 77 3

4 марта 2015 в 04:31

Сетевые технологии SDN – Software Defined Networking

+12 55,9k 135 8

15 августа 2013 в 12:56

Не совсем стандартный подход к организации доступа к WiFi сети (Cisco WLC -> FreeRadius -> PHP -> страничка в сети)

+3 10,1k 31 2

ВАКАНСИИ

Мой круг

PHP Developer | PHP разработчик — от 2000 до 2500 €

App-Smart • Краснодар

PHP программист — от 70000 ₽
Кабель.РФ • Саранск

PHP-разработчик — от 40000 до 80000 ₽
InStat • Возможна удаленная работа

Наставник-репетитор по PHP — от 12000 до 20000 ₽
HTML Academy • Возможна удаленная работа

PHP-разработчик / PHP-Development — от 60000 до 120000 ₽
БюроБюро • Калининград • Возможна удаленная работа

Все вакансии

Комментарии 12

m0ps 12 ноября 2014 в 21:58 −1

Эт конечно все хорошо, но не раскрыто главное — чего в результате добьемся?

Zaredis 12 ноября 2014 в 22:14 0

ЧТО ОБСУЖДАЮТ

Сейчас | Вчера | Неделя

Люди на Луне. Источники

21,1k 109

В результате мы добьемся того, что при каждом включении или выключении устройства на порту, коммутатор будет посылать сообщение(mac-notification) на сервер, где данная информация обрабатывается и хранится в БД.

m0ps 12 ноября 2014 в 22:45 −1

Я эт понял… Практическая сторона какая? Какую задачу позволяет решить описанные в статье телодвижения?
Я просто к чему спрашиваю: У самих стоит switchmap для сбора статистики с коммутаторов (не графики, а маки, вланы, транки, статистика простоя портов и т.д.) плюс arpwatch для оповещения о конфликтах(бывает устройства могут чужие адреса воровать как умышленно, так и случайно).

Zaredis 13 ноября 2014 в 09:48 0

Конкретно мы собираем статистику в связи с требованиями безопасности. Думаю, каждый, кто задумался о сборе подобной статистики, знает, зачем она ему нужна.Я лишь предлагаю один из вариантов. Т.к наша сеть полностью на Cisco, нам удобнее пользоваться встроенными функциями коммутаторов.

m0ps 13 ноября 2014 в 10:15 −1

То-есть вы собираете статистику появления/пропадания мака на порту в целях безопасности? Это в чем может помочь, вычислить кто в момент инцидента был подключен к порту? Что ж Вы так… статью написать не поленились, а описать практическое применение не удосужились…

P.S. PHP-скрипт это встроенные средства коммутатора? :)

Zaredis 13 ноября 2014 в 10:32 0

Встроенное средство коммутатора явно написано в названии статьи)

27 удивительных инструментов VS Code для современных JavaScript-разработчиков
9,9k 12

Почему Senior Developer'ы не могут устроиться на работу
37k 247

Я не настоящий
3k 18

Электромобиль — это не для меня
584 1

Arks 13 ноября 2014 в 03:29 –1

И вот тут то основной вопрос — при чем тут «PHP» в тегах поста(ну кроме скрипта который с тем же успехом можно написать на perl'e, bash'e, e.t.c)?

Zaredis 13 ноября 2014 в 09:52 0

С таким же успехом можно убрать и *Cisco, ведь там всего лишь настройка)

Homas 19 ноября 2014 в 23:17 0

Удивительно, что народ так мало знает про SNMP про SNMP Trap'ы в частности. В особенности поражают фразы про крупицы знаний и «больше интересных функций на ftp Cisco». Информации навалом, даже на хабре есть куча статей о применении SNMP.
BTW MIB-файлы устанавливать совершенно не обязательно, главное знать правильные OIDы.

Zaredis 20 ноября 2014 в 09:24 0

Видимо, более конструктивных комментариев, кроме баянов и придирок к словам, я не увижу)

Homas 20 ноября 2014 в 14:00 0

Если статья «ни о чем», то что Вы вообще желали услышать?
Радуйтесь, что не заминусовали :)

Zaredis 20 ноября 2014 в 14:45 0

Обязательно напишу модераторам песочницы, чтобы не пропускали такие статьи)

Только полноправные пользователи могут оставлять комментарии. Войдите, пожалуйста.

САМОЕ ЧИТАЕМОЕ

Сутки | Неделя | Месяц

Почему Senior Developer'ы не могут устроиться на работу

+71 37k 137 247

Битва за аккаунт. Основатель сети Jeffrey's Coffee подаёт в суд на ВКонтакте

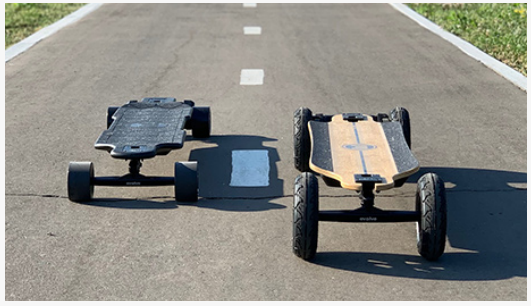
+57 26,6k 49 102

Взломщики подрядчика ФСБ узнали о тайных проектах спецслужб для слежки в интернете

+45 50,7k 40 202

Люди на Луне. Источники

РЕКОМЕНДУЕМ



Серфинг на асфальтовых волнах: тестируем электроскейты Evolve

+68 21,1k 82 109

Онлайн игра с реальными RC роботами в Чернобыле

+132 16,7k 63 110

Одна «Бомба», много докладов и непонятный «Код Рагнерек»: выжимаем сок из РИТ++