Настройка SNMP и Syslog на Juniper SRX

ОПУБЛИКОВАНО 01.10.2015 от admin

Выдалась более-менее свободная неделька чтобы поковырять Juniper. Опять же, закончилась моя эпопея с JTAC и отправкой JFLOW. Внезапно(тм) выяснилось, что слать FLOW аппарат умеет только из Default VR, а сообщить об этом в мануале толи забыли, то ли сделали это так ненавязчиво. что я банально это пропустил.

Под катом самая макотка — вдруг кому пригодится.
Сразу оговорюсь — даже не пытайтесь настраивать control-функии (snmp, syslog, flow, ntp) через VR. Проблем огребете гарантированно, а пользу получите весьма сомнительную. Лучше свести все взаимодействие с коробкой к mng-интерфейсу. Тем более что даже если настроить (вроде бы!) отсылку всевозможных сообщений через VR, то, в самый неподходящий момент, может выясниться, что часть информации кладет болт на ваши настройки и шлет из default VR.

Syslog

Начнем мы с syslog.
syslog-сервер 172.30.5.100
source-address 172.30.2.241 — адрес нашего fxp0 интерфейса.

Директива «*system syslog host*» указывает на syslog-сервер.
Директива «*system syslog file*» указывает, что мы будем писать в локальные логи.

```
set system syslog archive size 100k
set system syslog archive files 3
set system syslog user * any emergency
set system syslog host 172.30.5.100 any any
set system syslog host 172.30.5.100 authorization warning
set system syslog host 172.30.5.100 daemon any
set system syslog host 172.30.5.100 security any
set system syslog host 172.30.5.100 change-log none
set system syslog host 172.30.5.100 interactive-commands none
set system syslog host 172.30.5.100 facility-override local1
set system syslog host 172.30.5.100 source-address 172.30.2.241
set system syslog host other-routing-engine any any
set system syslog host other-routing-engine source-address 172.30.2.241
set system syslog file messages any alert
set system syslog file interactive-commands interactive-commands error
set system syslog file kmd-logs daemon info
set system syslog file kmd-logs match KMD
set system syslog time-format year
set system syslog time-format millisecond
set system syslog source-address 172.30.2.241
```

Отдельно настроим security log: это логи, отсылаемые, непосредственно, с dataplane.

```
set security log cache limit 256
set security log mode stream
set security log format sd-syslog
set security log rate-cap 2000
set security log source-address 172.30.2.241
```

```
set security log stream NOC severity warning
set security log stream NOC format sd-syslog
set security log stream NOC category all
set security log stream NOC host 172.30.5.100
```

SNMP

Казалось бы, проще некуда. Тем более что здесь я все-таки указал VR для опроса железки извне (исторически сложилось так). Запомните, что если к SNMP вы пытаетесь обращаться через VR, то community надо указывать так: BRANCH_VR@public, где BRANCH_VR это имя VR, через который вы идете.
Ну и не забыть явно указать ACL для доступа из VR.

Тут всё просто:

```
set snmp name jpsrx550-X-s10
set snmp description "Juniper SRX 550 2x645AC"
set snmp location "SPb, DataCenter"
set snmp contact "NOC: noc@nixman.info"
```

snmp filter-interfaces interfaces делает одну очень полезную штуку — фильтрует информацию о ненужных вам интерфейсах. Например, ей удобно фильтровать всякие служебные сущности, коих у джунипера полно.

snmp filter-interfaces

Теперь настраиваем ACL для SNMP:

```
set snmp community public authorization read-only
set snmp community public clients 172.20.0.0/24
```

```
set snmp community public routing-instance BRANCH_VR client-list-name MGMT-IP
set snmp community private authorization read-write
set snmp community private clients 172.20.0.0/24
set snmp community private routing-instance BRANCH_VR client-list-name MGMT-IP
set snmp routing-instance-access access-list BRANCH_VR
```

В ACL я указал, что получать информацию по SNMP можно только из сети 172.20.0.0/24 из дефолтного VR и сети из листа MGMT-IP через VR. Последней директивой мы указываем, что получать данные SNMP можно только из BRANCH_VR.
ACL MGMT-IP настраивается так:

```
set policy-options prefix-list MGMT-IP 172.20.0.0/24
```

Теперь настраиваем трапы. Имя trap-group это community, с которым будут отправляться трапы:

```
set snmp trap-options source-address 172.30.2.241
set snmp trap-options enterprise-oid
set snmp trap-group trap version v2
set snmp trap-group trap categories authentication
set snmp trap-group trap categories chassis
set snmp trap-group trap categories link
set snmp trap-group trap categories remote-operations
set snmp trap-group trap categories routing
set snmp trap-group trap categories startup
set snmp trap-group trap categories rmon-alarm
set snmp trap-group trap categories vrrp-events
set snmp trap-group trap categories configuration
set snmp trap-group trap categories services
set snmp trap-group trap categories chassis-cluster
```

```
set snmp trap-group trap categories otn-alarms
set snmp trap-group trap targets 172.30.0.254
```

отдельно отмечу, что часть трапов может приходить вполне с community BRANCH_VR@trap, а не только trap. Почему? Так получилось (с)

На этом, собственно, и все. Советую для начала настроить максимально детальную и полную отсылку событий, а потом, когда уже разберетесь, как и что, уже повышать уровень severity и убирать ненужные категории, дабы не захламлять логи.

Удачи!

Понравилось это:

Загрузка...

Похожее

Juniper SRX и Libreswan (и ещё StrongSwan)
14.12.2017
В "Hard"

IPSec: Mikrotik и Juniper
29.12.2015
В "Mikrotik"

Сам себе почтальон, часть 3: антивирус и антиспам
04.09.2015
В "Linux"

ОПУБЛИКОВАНО В **HARD** juniper snmp srx syslog traps

ПРЕДЫДУЩИЙ ПОСТ
Hotspot для самых маленьких, часть 2: своя страница входа + социальные сети

СЛЕДУЮЩИЙ ПОСТ
Настройка отправки Jflow в Juniper SRX

Будьте первым, кто оставит комментарий

Добавить комментарий

Вы можете войти через социальные сети

Введите свой комментарий...

FOLLOW ME

МЕТКИ

3g apt asterisk bash blog cisco debian debmirror drivers FreeBSD gnome hdd hotspot humor ipsec juniper linux mail mikrotik mirror monitoring nat network nVidia openvpn pbr perl postfix ppp pptp release routing srx stargazer tips ubuntu verlihub virtualization vlan vpn wifi Windows work work xen

РУБРИКИ

FreeBSD

Hard

Linux

Mikrotik

Без рубрики

СВЕЖАК

Настройка Postfix через Yandex relay

Репликация PostgreSQL

Мониторинг с помощью RPM probe в Juniper

Juniper SRX и Libreswan (и ещё StrongSwan)

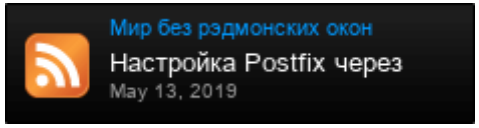
Mikrotik и ansible: устанавливаем сертификаты

ПОДПИСКА

Enter your email address:

Subscribe

Delivered by FeedBurner



↑ Grab this Headline Animator

СЧЕТЧИКИ

COPYRIGHT

ABOUT ME

Добро пожаловать! Я - Алексей, a.k.a. Snake. Основной моей деятельностью является сетевое администрирование. В фокусе - сетевое оборудование различных вендоров (Cisco, Juniper, Mikrotik), а также Linux в различных его проявлениях. Сюда я пишу, как правило, в формате HOWTO, чтобы помочь другим (и себе тоже) в решении разнообразных задач, связанных с настройкой сетевого оборудования и серверов. Я всегда рад комментариям, а также вопросам в почту или личные сообщения в социальных сетях.

Support