Хочу подробно рассмотреть вопрос наблюдения за популярными сетевыми устройствами. Я расскажу, как настроить мониторинг устройств Mikrotik с помощью системы мониторинга Zabbix. За основу будет взят типовой шаблон, плюс мои доработки для мониторинга и оповещений логинов в систему.

Содержание:

Цели статьи

1. Настроить мониторинг базовых метрик сетевых устройств Mikrotik.
2. Настроить отправку основных логов на удаленный сервер.
3. Анализировать логи mikrotik и отправлять уведомления в случае подключения к устройству.

Введение

За основу мониторинга Mikrotik я возьму стандартный шаблон Zabbix от разработчиков. Он очень качественно сделан. Забирает информацию по snmp.

Итемы и триггеры настраиваются через автообнаружение. Вот основные метрики, которые в нем реализованы:

1. Состояние процессоров (загрузка, температура).
2. Статус и характеристика интерфейсов (трафик, активность, ошибки, тип, скорость).
3. Хранилища (общий объем и используемый).
4. Использование оперативной памяти.
5. Проверка доступности пингом.
6. Версия прошивки, модель, система, серийный номер, расположение, описание устройства.
7. Время работы (uptime).

Для всех основных метрик есть графики. На все значимые события настроены триггеры:

- Высокая температура процессора.
- Изменение серийного номера, прошивки.
- Сетевая недоступность по icmp.
- Высокая загрузка памяти или процессора.
- Окончание свободного места на хранилищах.
- Уменьшилась скорость на интерфейсе.
- Высокая утилизация интерфейса.
- Большое количество ошибок на интерфейсе.
- Интерфейс отключился.

Шаблон настолько хорош и полон, что я даже не придумал, чего в нем не хватает. По метрикам есть все. Для полного мониторинга Микротика мне не хватало только оповещений о том, что к нему кто-то подключился. Я реализовал это по своему, о чем расскажу далее подробно. В двух словах мониторинг подключений выглядит так:

1. Mikrotik отправляет логи подключений на удаленный syslog сервер.
2. На syslog сервере логи анализирует zabbix-agent.
3. По определенному шаблону агент определяет имя и ip адрес подключившегося к микротику и отправляет эту информацию в уведомлении.

В целом, никаких сложностей в этой настройке нет. У меня уже есть статьи по сбору логов с микротиков — отправка в elk stack и на удаленный rsyslog сервер. Сегодня я актуализирую эту информацию и опишу еще раз.

Если у вас еще нет своего сервера для мониторинга, то рекомендую материалы на эту тему. Для тех, кто предпочитает систему CentOS:

1. Установка CentOS 8.
2. Настройка CentOS 8.
3. Установка и настройка zabbix сервера.

То же самое на Debian 10, если предпочитаете его:

1. Установка Debian 10.
2. Базовая настройка Debian.
3. Установка и настройка zabbix на debian.

Мониторинг Mikrotik в Zabbix по snmp

Стандартный шаблон собирает все метрики по snmp. Так что нам надо включить его на микротике. Для этого подключаемся к нему по Winbox и идем в раздел **IP -> SNMP**. Настраиваем работу snmp.

Мы включили snmp, выставили версию 2, разрешили подключаться только с ip адреса zabbix server — 10.1.3.29. Не забудьте указать адрес своего сервера.

Сходим теперь на zabbix-server и убедимся, что мы через него можем забирать информацию с mikrotik по snmp. Для этого подключимся к нему по ssh и воспользуемся утилитой **snmpwalk**. Если у вас ее нет, то поставить можно командой:

```
# yum install net-snmp-utils
```

Подключаемся к микротику по snmp.

```
# snmpwalk -v 2c -c public 10.1.3.111
```

Получите кучу значений в консоли. Если хотите удобно их просмотреть, направьте вывод команды в файл и почитайте его. Если подключение прошло

успешно, то переходим в Web интерфейс Zabbix сервера.

Здесь нам нужно будет добавить несколько шаблонов. Для начала загрузите вот этот пак шаблонов — https://share.zabbix.com/official-templates/template-modules-pack и установите несколько штук из него:

- template_module_generic_snmp_SNMPv2_EN.xml
- template_module_interfaces_SNMPv2_EN.xml
- 00template_module_icmp_ping__EN.xml

Вроде все. Но если вдруг чего-то будет не хватать, то при установке основного шаблона, он вам скажет об этом. Загружаем основной шаблон отсюда — https://share.zabbix.com/network_devices/mikrotik/template-net-mikrotik-snmpv2 и устанавливаем на сервер мониторинга. Обратите внимание на вкладку Макросы в шаблоне. Там указаны дефолтные значения, которые используются в триггерах. Лично я немного поднял пороговые значения по температуре.

Теперь нам нужно добавить в систему само устройство Mikrotik. Делаем это как обычно, не забывая указать snmp интерфейс.

И не забудьте ему подключить шаблон **Template Net Mikrotik SNMPv2**. После этого можно идти в Lates Data и проверять поступление информации с устройства в систему мониторинга.

Часть данных увидите сразу, а та, что поступает через правила автообнаружения, появится позже. Надо подождать. После того, как отработают все правила автообнаружения, рекомендую сходить на хост и поотключать то, что вам не нужно. К примеру, если у вас настроен capsman, то в мониторинг с мастера попадут интерфейсы **cap**, которые отключаются, если к точке нет подключенных клиентов по wifi. В итоге будет ненужный спам от мониторинга с точек.

На этом по мониторингу базовых метрик в микротике все. Теперь займемся уведомлениями о подключениях к устройствам через Winbox.

Отправка логов Mikrotik в syslog

Первым делом настроим сбор логов с микротиков на любой syslog сервер. В моем случае это будет сам сервер мониторинга на базе rsyslog и centos 7, но это не принципиально. Главное, чтобы на нем был zabbix-agent, который будет отправлять логи микротиков на заббикс сервер.

Для этого в rsyslog включим возможность слушать udp port 514. Открываем конфиг */etc/rsyslog.conf* и раскомментируем там строки:

```
$ModLoad imudp
$UDPServerRun 514
```

Дальше в этом же файле в самом начале перечисления правил, добавляем свое.

```
$template FILENAME,"/var/log/mikrotik/%fromhost-ip%.log"
if $fromhost-ip != '127.0.0.1' then ?FILENAME
& stop
```

Данное правило будет автоматически раскладывать все логи с удаленных устройств по файлам в директории */var/log/mikrotik* с именами в виде IP адресов. При этом не будет создан лог 127.0.0.1.log, куда бы складывались все локальные лог файлы. В своей предыдущей статье я не учитывал этот нюанс, что приводило к дублированию всех локальных логов. Сейчас я это исправляю.

Сразу же настроим ротацию лог файлов, чтобы они не забили нам весь диск. Для этого создаем конфиг для logrotate в файле */etc/logrotate.d/mikrotik* примерно следующего содержания:

```
/var/log/mikrotik/*.log {
        weekly
        rotate 12
        compress
        olddir /var/log/mikrotik/old
        missingok
        notifempty
        create 0640 root zabbix
```

```
}
```

Я ротирую файлы логов раз в неделю, сразу сжимаю и кладу их в директорию */var/log/mikrotik/old*, где будут храниться 12 последних версий файла.

Не забудьте создать указанные директории и дать пользователю zabbix права на чтение. Потом проследите, чтобы у самих логов тоже были права на чтение для zabbix. Это важно, так как агент должен их читать.

После завершения настройки, надо перезапустить rsyslog.

```
# systemctl restart rsyslog
```

Отправляемся на Mikrotik и настраиваем отправку логов на наш syslog сервер. Для этого переходите в раздел **System -> Logging -> Actions** и добавляйте новое действие.

Дальше открывайте вкладку Rules и добавляйте темы логов, которые вы будете отправлять в Zabbix. Для мониторинга за логинами достаточно темы System.

Чтобы проверить отправку логов, достаточно тут же в Mikrotik открыть новый терминал. Создастся событие в логе, который улетит на удаленный сервер. На сервере с rsyslog будет создан лог файл с содержимым.

Если у вас так же, можно двигаться дальше. Если же логи не поступают на syslog сервер, разбирайтесь в чем может быть причина. Первым делом проверьте настройки firewall. Убедитесь, что доступ к udp порту 514 есть. Дальше проверьте, что ваш rsyslog сервер реально слушает этот порт.

Мониторинг подключений (авторизаций) в Mikrotik

Логи с устройств мы собрали в одном месте. Теперь будем их анализировать и отправлять уведомления при каждом подключении к Mikrotik через Winbox. Я для этого сделал отдельный шаблон, где созданы элементы данных типа **Журнал (лог)** для анализа лог файла от каждого устройства.

Для каждого элемента данных есть триггер, который с помощью регулярного выражения анализирует лог файл и срабатывает тогда, когда видит строки с подключением к микротику через winbox. Имя триггера формируется таким образом, чтобы в нем была информация об имени пользователя и ip адрес, с которого он подключился.

Я не стал делать в шаблоне автообнаружение. Настраивал это в системах до 10-ти точек и мне банально было лень это делать, хотя и не сложно. Я просто копировал и исправлял итемы и триггеры, меняя ip адреса устройств. Для автообнаружения надо скрипт на сервер класть, который будет передавать список логов в мониторинг. А если руками делать, то можно все на сервере в шаблоне добавлять.

Итак, создаем простой итем.

К итему делаем триггер.

```
Mikrotik 10.1.3.110 auth {{ITEM.VALUE}.iregsub("account user (.*)via", "\1")}
```

```
{Template Mikrotik Logs:log[/var/log/mikrotik/10.1.3.111.log].str(logged in from,#1)}=1 and {Template Mikrotik
Logs:log[/var/log/mikrotik/10.1.3.111.log].str(via winbox,#1)}=1
```

Вот и все. Прикрепляйте шаблон к хосту с микротиком и проверяйте. В первую очередь смотрите, чтобы в **Latest Data** появилось содержимое лога.

Если триггеры настроены правильно, то при каждом подключении по Winbox вы будете получать уведомление на почту.

И еще одно после отключения.

Такой несложный механизм мониторинга за подключениями. Я отслеживаю именно подключения по winbox. Вы можете это изменить, добавив и другие типы подключения. Для этого надо изменить регулярное выражение в триггере.

Пример моего шаблона с двумя микротиками — zabbix-mikrotik-logs.xml. Если у вас много устройств, настройте автообнаружение лог файлов, чтобы автоматически создавать итемы и триггеры. Пример настройки автообнаружения в Zabbix можете посмотреть на примере мониторинга openvpn подключений. Там как раз показан очень похожий пример, когда анализируется список файлов в директории и передается в zabbix server.

На этом по мониторингу микротиков в Zabbix у меня все. По идее, рассмотрел все актуальные задачи по этой теме.

Заключение

> Не понравилась статья и хочешь научить меня администрировать? Пожалуйста, я люблю учиться. Комментарии в твоем распоряжении. Расскажи, как сделать правильно!

Если у вас есть замечания или рекомендации по настройке мониторинга Mikrotik, делитесь в комментариях. Так же интересно узнать, есть ли еще какие-то полезные метрики, которые я упустил. Имея на руках лог файлы, можно настроить мониторинг абсолютно всех действий с микротиками. Но лично я не придумал, какая еще информация может быть полезна.

Мониторинг подключений и авторизаций в микротиках настроен в рамках построения простенькой самодельной системы информационной безопасности. Сюда можно будет добавить мониторинг за подключениями по ssh и openvpn. Затем свести все это в единый dashboard.

Так же может быть полезным настройка оповещений в telegram.

Онлайн курсы по Mikrotik

Если у вас есть желание научиться работать с роутерами микротик и стать специалистом в этой области, рекомендую пройти курсы по программе, основанной на информации из официального курса **MikroTik Certified Network Associate**. Помимо официальной программы, в курсах будут лабораторные работы, в которых вы на практике сможете проверить и закрепить полученные знания. Все подробности на сайте . Стоимость обучения весьма демократична, хорошая возможность получить новые знания в актуальной на сегодняшний день предметной области. Особенности курсов:

- Знания, ориентированные на практику;
- Реальные ситуации и задачи;
- Лучшее из международных программ.