Мониторинг локальной сети. Mikrotik + Zabbix

MikroTik

Приветствую, коллеги!

Антон Мороз

Генеральный директор ООО «Реал»

Россия, Москва

www.realsd.ru

С 2005 г. в ИТ области, с 2012 г. на рынке ИТ аутсорсинга.

Сертификаты Mikrotik: MTCNA, MTCWE, MTCTCE, MTCRE, MTCIPv6E, MTCUME

Сертификаты Zabbix: ZCS, ZCP

О чем поговорим?

RealSD™

Сокращенный план презентации

1. Рассмотрим как Zabbix может взаимодействовать с Mikrotik
2. Разберем официальный шаблон для Mikrotik
3. Осветим возможности автоматизации обнаружения и начала сбора метрик
4. Посмотрим примеры мониторинга через разные каналы
5. Настроим мониторинг состояния IPSec в туннельном режиме
6. Поговорим как можно средствами Zabbix контролировать безопасность сети 24x7

1. Зачем мониторить сеть?

MikroTik

1. Зачем мониторить сеть?

RealSD™

Какие задачи решает мониторинг устройств?

1. Уведомление о сбоях и нарушениях качества услуг
2. Проактивное управление проблемами
3. Сбор исторических и статистических данных
4. Наличие дополнительной информации для расследования инцидентов
5. Контроль соблюдения и подсчет показателей SLA
6. Выявление аномальных показаний на сетевом оборудовании

2. Краткий обзор Zabbix

MikroTik

2. Краткий обзор Zabbix

Zabbix - зрелое и легкое решение распределенного мониторинга корпоративного класса для мониторинга миллионов метрик сетей и приложений.

- 21 год опыта на рынке
- 100% открытый код
- 300 000 + инсталляций по всему миру

2. Краткий обзор Zabbix

Плюсы

1. Open Source решение
2. Кроссплатформенность наблюдаемых устройств
3. Дружелюбный Web интерфейс
4. Масштабируемость от нескольких устройств до сотен тысяч
5. Возможность отображения информации на графических картах
6. Наличие API для автоматизации и интеграции с другими системами
7. Возможность использования собственных скриптов для расширения функциональности мониторинга
8. Универсальность применения в компании
9. Территориально распределенный мониторинг

2. Краткий обзор Zabbix

Минусы

1. Пока не умеет определять и автоматически рисовать топологию сети
2. Не самый низкий порог вхождения для ИТ специалистов
3. Вопрос отказоустойчивости и кластеризации из коробки на стартовом этапе. Заявлены изменения по данному вопросу в версии 5.0 (март 2020г.)

3. Типы проверок для мониторинга Mikrotik

MikroTik

3. Типы проверок для мониторинга Mikrotik

1. SNMP

Самый распространенный протокол мониторинга сетевого оборудования.

Поддерживаются все 3 версии протокола, включая шифрование.

Mikrotik поддерживает актуальным MIB файл. Последнее обновление 10 апреля 2019 года.
https://wiki.mikrotik.com/wiki/Manual:SNMP#Management_information_base_.28MIB.29

Заметки

По умолчанию SNMP выключен

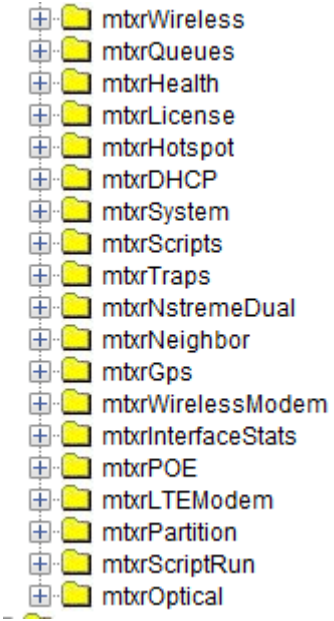
Использует порты UDP: 161 для опросов, 162 для получения трапов

Для корректной работы v3 не забывайте указывать в настройках engine-id

3. Типы проверок для мониторинга Mikrotikй

Возможности мониторинга многих параметров системы:

1. Метрики беспроводных и проводных интерфейсов
2. Метрики очередей
3. Метрики физического состояния устройства
4. Метрики сервиса Hotspot
5. Метрики PoE состояния
6. Возможность запуска системных скриптов и получения от них результатов выполнения
7. И многое другое



3. Типы проверок для мониторинга Mikrotik

2. SSH

Поддерживается авторизация как по логину и паролю так и по ssh ключу.

Возможность запуска любых команд и получения результата вывода команд.

Возможно выполнение действий по триггерам и на основании автообнаружения.

4. Шаблон Mikrotik «из коробки»

MikroTik

4. Шаблон Mikrotik «из коробки»

Факты

1. Шаблон доступен в стандартной установке Zabbix сервера
2. Используется SNMP v2
3. Использует вложенные стандартные шаблоны Template Module Generic SNMPv2 и Template Module Interfaces SNMPv2
4. Не включает мониторинг Hotspot и CAPsMAN метрик

Заметки

Отдельно можно скачать по ссылке

https://www.zabbix.org/mw/images/8/89/Template_Net_Mikrotik_SNMPv2-4.2.0.xml

4. Шаблон Mikrotik «из коробки»

Что можно допилить

1. Лишние метрики

Сразу удалить из шаблона Элемент данных System object ID, так как он возвращает OID с зарегистрированным номером Private Enterprises для Mikrotik в IANA.

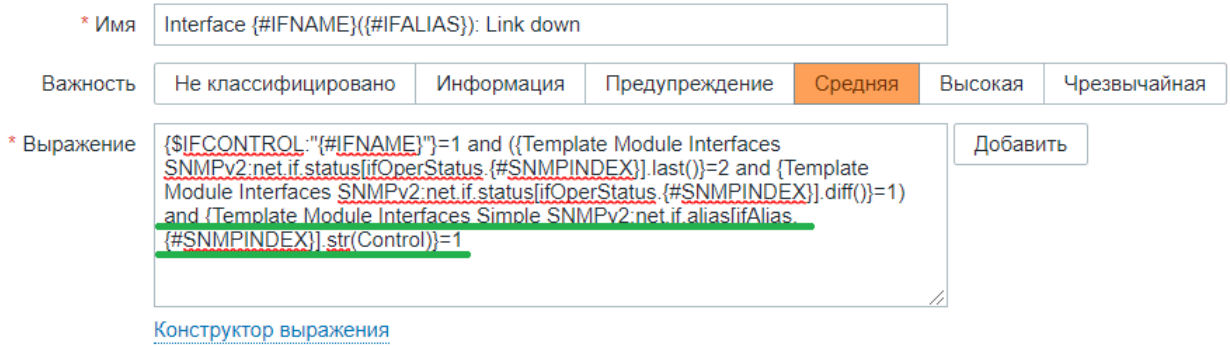
Возвращает: 1.3.6.1.4.1.14988.1 или MIKROTIK-MIB::mikrotikExperimentalModule

Не самая полезная информация и имеет постоянное значение.

4. Шаблон Mikrotik «из коробки»

2. Контроль только критических портов

Чтобы триггеры не срабатывали для всех интерфейсов можно добавить в комментарии интерфейсов суффикс. К примеру в конце указывать «Control». Тогда добавив дополнительное условие в триггер будем получать уведомления только для важных интерфейсов.



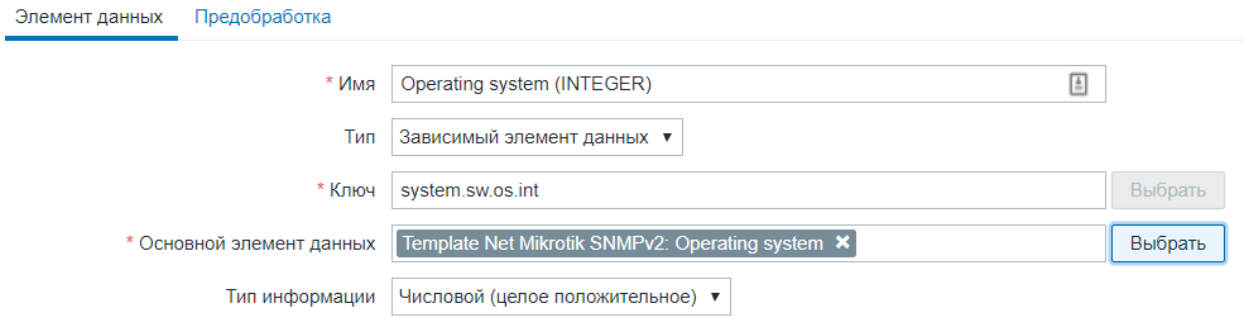
4. Шаблон Mikrotik «из коробки»

3. Больше не забываем обновиться

Добавить контроль соответствия current-firmware и upgrade-firmware

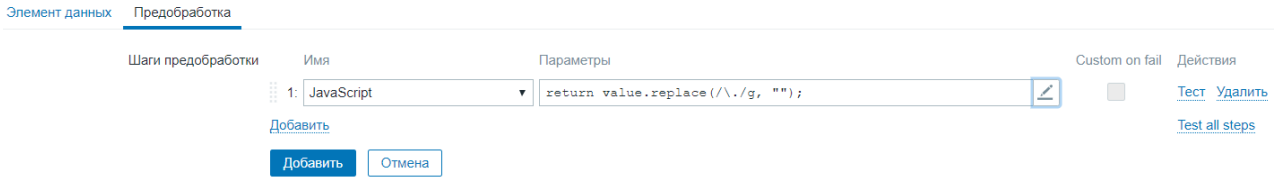
Zabbix не умеет сравнивать строки в триггерах, поэтому придется для начала перевести версии firmware в числовой формат.

Создаем зависимый элемент данных



4. Шаблон Mikrotik «из коробки»

Настраиваем предобработку

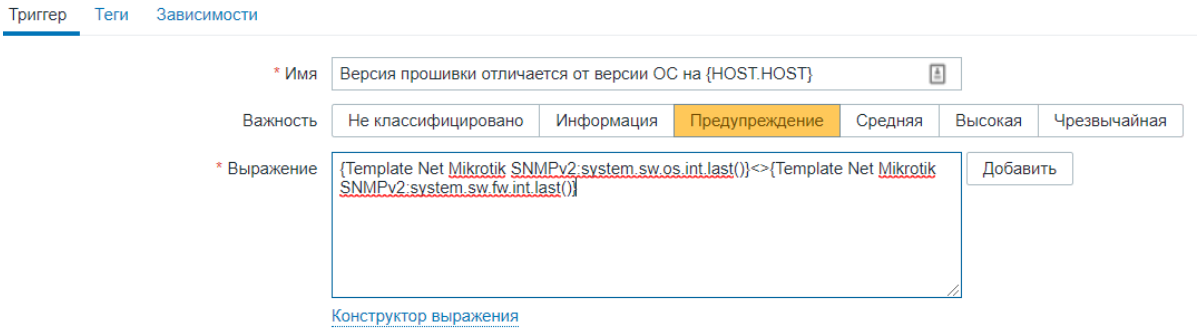


Получаем следующий результат

NET-006-77-01001	**Inventory** (6 элементов данных)			
	Firmware version	05.09.2019 22:01:48	6.44.5	История
	Firmware version (INTEGER)	05.09.2019 22:01:48	6445	График
	Hardware model name	05.09.2019 22:01:49	RouterOS RB4011iGS+	История
	Hardware serial number	05.09.2019 22:01:49	AAAF0997136A	История
	Operating system	05.09.2019 22:01:49	6.44.5	История
	Operating system (INTEGER)	05.09.2019 22:01:49	6445	График

4. Шаблон Mikrotik «из коробки»

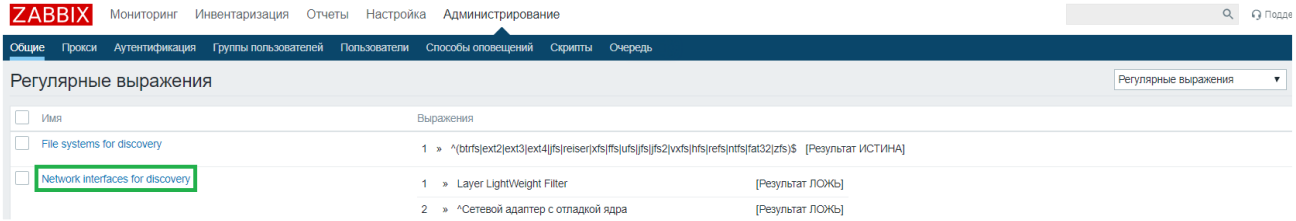
Создаем триггер



4. Шаблон Mikrotik «из коробки»

4. Фильтруем динамические интерфейсы при обнаружения

Исключить из правила обнаружения l2tp/pptp/sstp интерфейсы, добавив регулярное выражение ^<?(l2tp|sstp|pptp).* в набор фильтров



4. Шаблон Mikrotik «из коробки»

Регулярные выражения

Выражения Тест

▼	NET-006-77-01001	**Inventory** (6 элементов данных)			
☐		Firmware version	05.09.2019 22:01:48	6.44.5	История
☐		Firmware version (INTEGER)	05.09.2019 22:01:48	6445	График
☐		Hardware model name	05.09.2019 22:01:49	RouterOS RB4011iGS+	История
☐		Hardware serial number	05.09.2019 22:01:49	AAAF0997136A	История
☐		Operating system	05.09.2019 22:01:49	6.44.5	История
☐		Operating system (INTEGER)	05.09.2019 22:01:49	6445	График

Позволим добавлять важные PPP интерфейсы в систему мониторинга, установив суффикс «–Control» в имени интерфейса и изменив регулярное выражение (?=^<?(l2tp|sstp|pptp).*)(?=.*(?!-Control)$)

5. Автообнаружение устройств Mikrotik

MikroTik

5. Автообнаружение устройств Mikrotik

RealSD™

Возможности обнаружения по сети

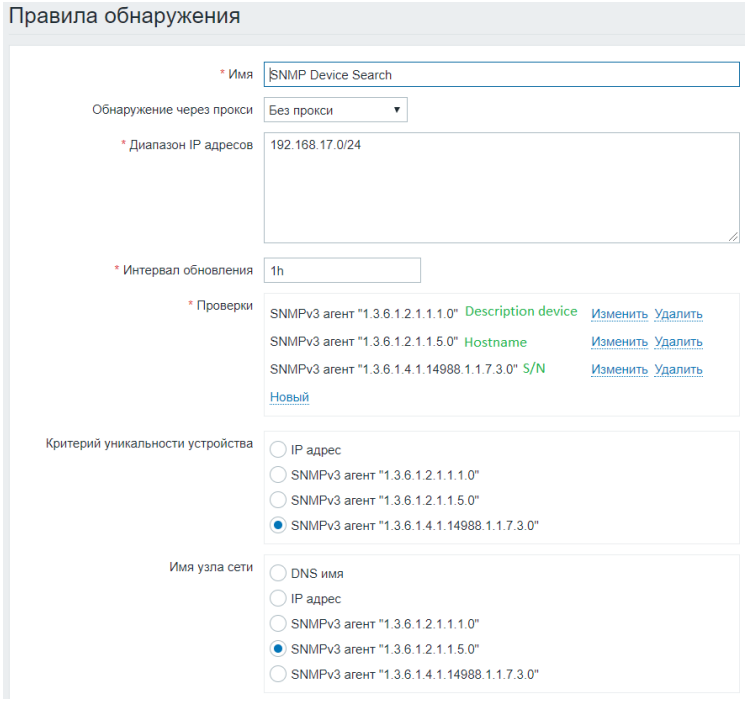
1. Сканирование сети по расписанию
2. Проверка на возможность получения требуемых данных
3. В связки с модулем «Действия» можем автоматически создавать узлы сети и применять к ним подходящие шаблоны
4. Выполнение практически любых действий во время обнаружения или потери устройства в сети

Заметки

Одно правило обнаружения обслуживается только одним процессом, поэтому не стоит добавлять большие подсети, если частота запуска маленькая.

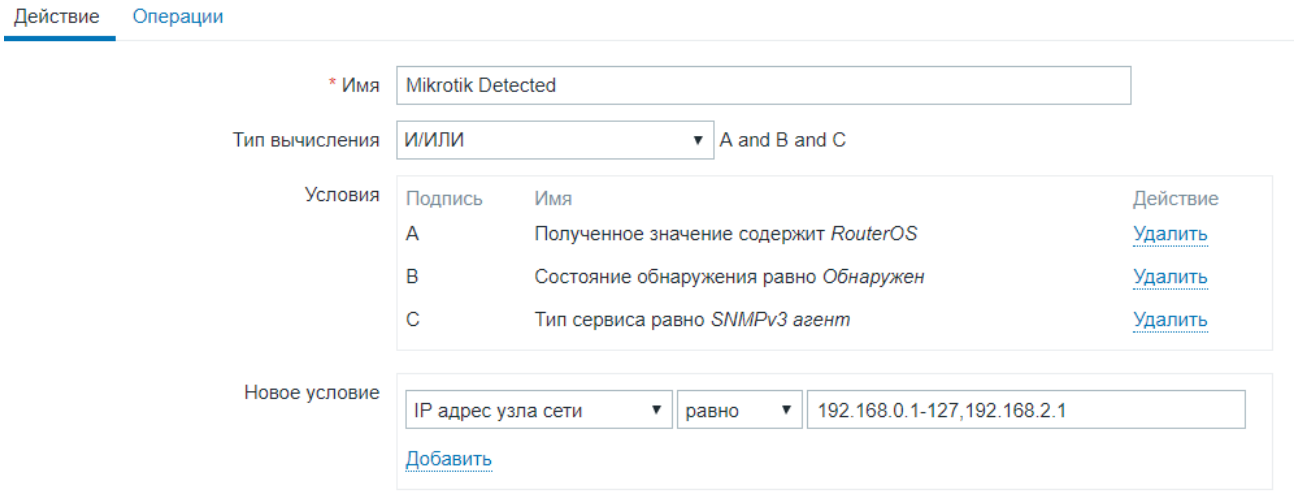
5. Автообнаружение устройств Mikrotik

Настройка правила обнаружения



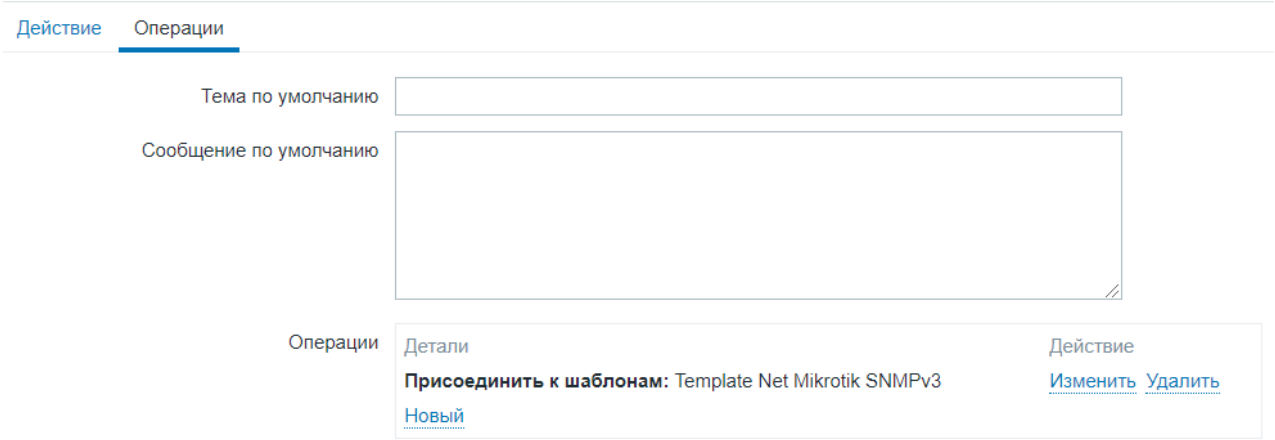
5. Автообнаружение устройств Mikrotik

Настройка присоединения шаблона Mikrotik к обнаруженным устройствам



5. Автообнаружение устройств Mikrotik

Настройка присоединения шаблона Mikrotik к обнаруженным устройствам



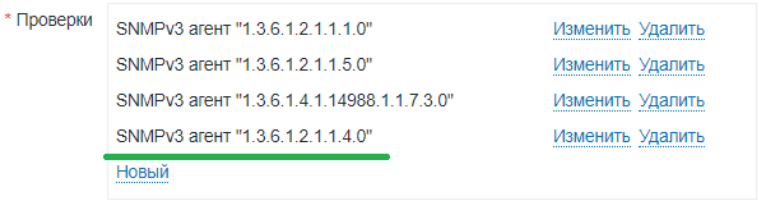
5. Автообнаружение устройств Mikrotik

Что еще можно сделать при обнаружении

На основании полученных данных во время обнаружения принимать решение нужно ли отправлять уведомления о найденном или потерянном устройстве, выбрать тип оповещения, на основании полученных данных.

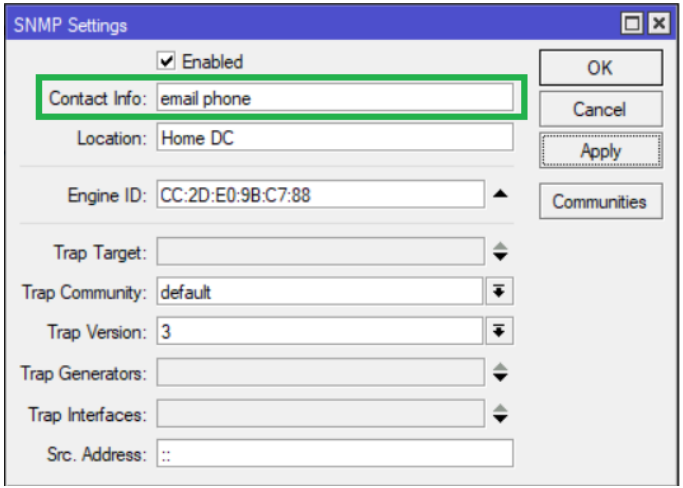
Решение

1. В правило обнаружения добавляем дополнительную проверку для получения значения поля Contact в настройках SNMP (OID 1.3.6.1.2.1.1.4.0)



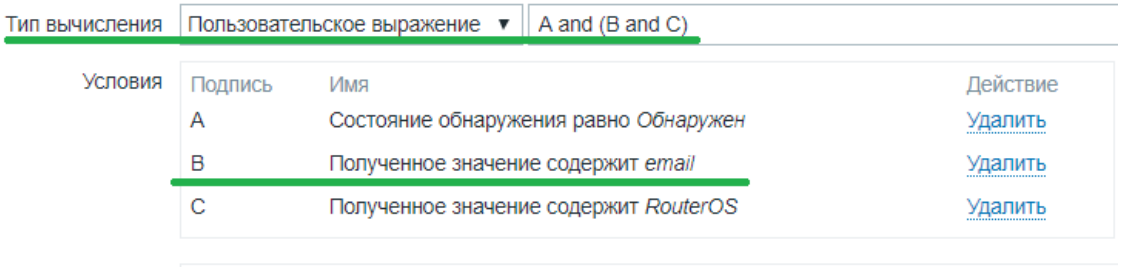
5. Автообнаружение устройств Mikrotik

2. В настройках SNMP можно указать перечень типов оповещения



5. Автообнаружение устройств Mikrotik

3. При создании действия сделать дополнительно условие, чтобы выбрать какое действие выполнить.



6. Примеры получения не стандартных метрик

MikroTik

6. Примеры получения не стандартных метрик

Типы данных, которые мы можем получать

1. Цифры: их можно сравнивать, использовать в агрегированных и вычисляемых элементах данных, строить графики
2. Строки: получение исторических данных, контроль изменения и т.д.
3. JSON формат: используются для правил обнаружения
4. XML формат: для сокращения количества обращений к оборудованию, используется для зависимых элементов данных

6. Примеры получения не стандартных метрик

Скрипт формирования JSON со списком всех активных политик IPSec

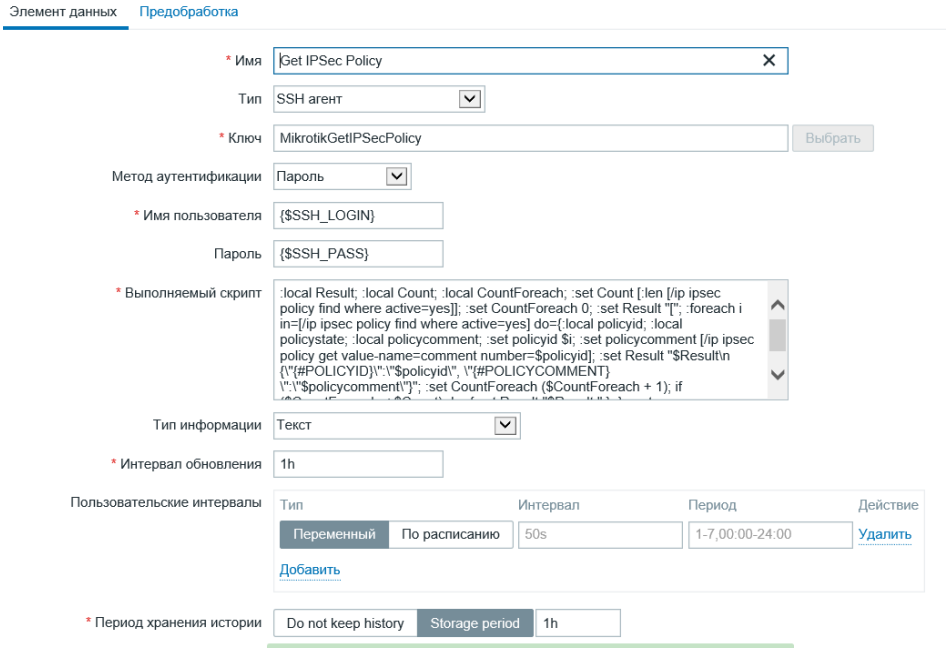
```
:local Result;
:local Count;
:local CountForeach;
:set Count [:len [/ip ipsec policy find where active=yes]];
:set CountForeach 0;
:set Result "[";
:foreach i in=[/ip ipsec policy find where active=yes] do={
    :local policyid;
    :local policycomment;
    :set policyid $i;
    :set policycomment [/ip ipsec policy get value-name=comment number=$policyid];
    :set Result "$Result\n{\"{#POLICYID}\":\"$policyid\", \"{#POLICYCOMMENT}\":\"$policycomment\"}";
    :set CountForeach ($CountForeach + 1);
    if ($CountForeach < $Count) do={
        :set Result "$Result,"
    };
};
:set Result "$Result\n]";
:put $Result;
```

Заметки

Zabbix передает команды построчно, и так как в Mikrotik есть особенность работы с локально объявленными переменными, скрипт в Zabbix необходимо добавлять в одну строку.

6. Примеры получения не стандартных метрик

Создание элемента данных для получения информации от скрипта



6. Примеры получения не стандартных метрик

Результат скрипта записывается в значение элемента данных

[

{"{#POLICYID}":"*1000002", "{#POLICYCOMMENT}":”FromOffice1_ToOffice2"},

{"{#POLICYID}":"*1000011", "{#POLICYCOMMENT}":"FromOffice1_ToOffice3"},

{"{#POLICYID}":"*1000012", "{#POLICYCOMMENT}":"FromOffice1_ToSklad1"},

{"{#POLICYID}":"*1000014", "{#POLICYCOMMENT}":"FromOffice1_ToSklad2"},

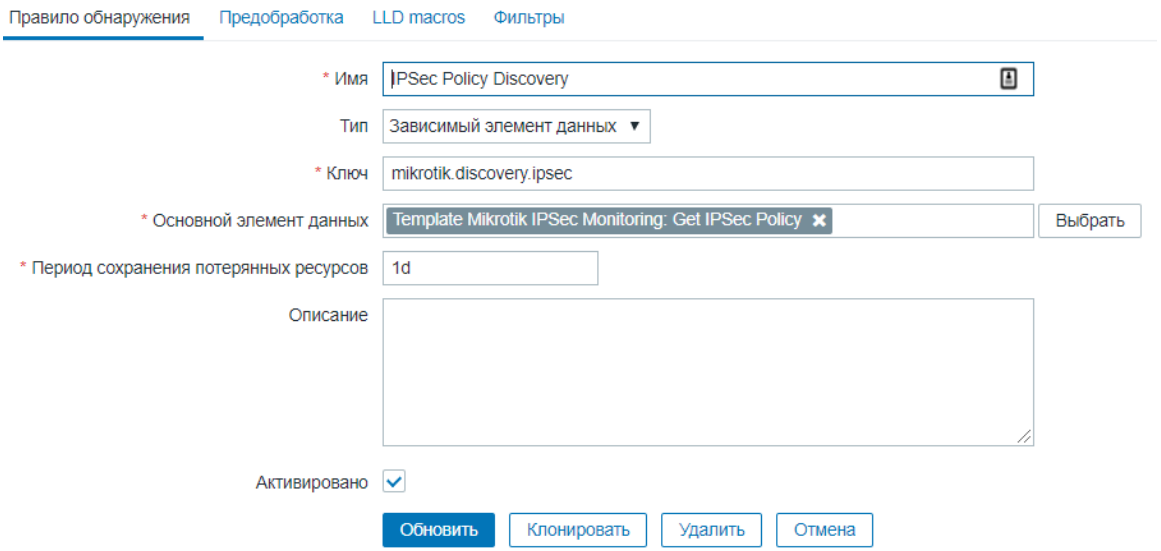
]

Заметки

Из данного JSON мы получим автоматически создаваемые макросы {#POLICYID} и {#POLICYCOMMENT}.

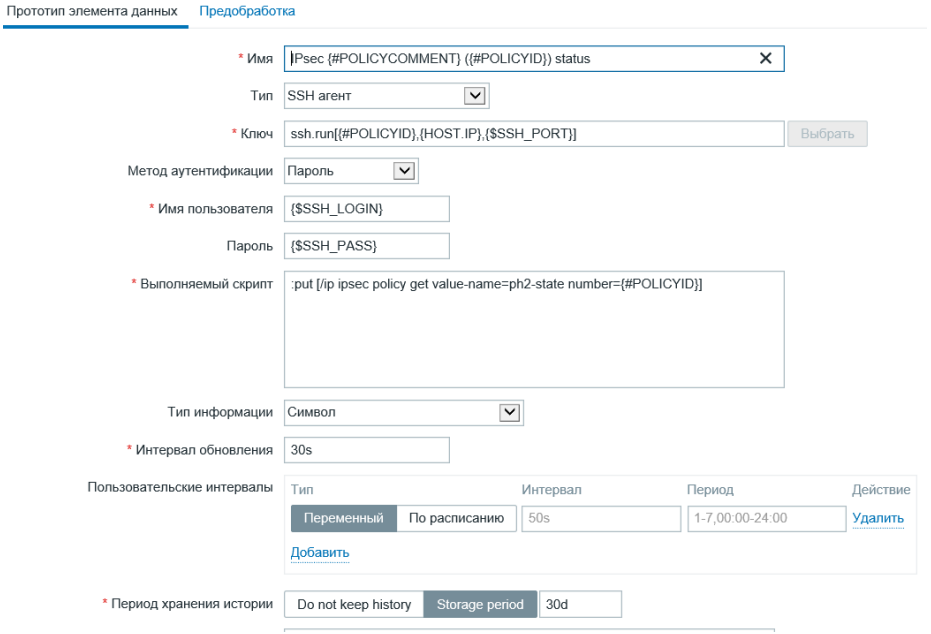
6. Примеры получения не стандартных метрик

Создание правила обнаружения



6. Примеры получения не стандартных метрик

Создание прототипа элемента данных



6. Примеры получения не стандартных метрик

Полученный итог в меню последних данных

Узел сети	Имя ▲	Последняя проверка	Последнее значение	Изменение	
NET-006-77-01001	**IPSec** (6 элементов данных)				
	Get IPSec Policy	17.08.2019 15:46:21	[{"{#POLICYID}":"*10000…		История
	IPsec ipip-real-cloud (*100003F) status	17.08.2019 16:04:54	established		История
	IPsec ipip-varshavskoe (*1000014) status	17.08.2019 16:04:58	established		История
	IPsec ToMainMoscow (*1000011) status	17.08.2019 16:04:55	established		История
	IPsec ToMainMoscow (*1000012) status	17.08.2019 16:04:56	established		История
	IPsec ToMainSpb (*1000002) status	17.08.2019 16:04:54	established		История

Заметки

Остается только создать триггер, оповещающий об отсутствии установленного соединения. Мониторинг состояния IPSec политик готов.

6. Примеры получения не стандартных метрик

Мониторинг использования DHCP Pool

На этом примере рассмотрим как можно использовать сохраненные скрипты в самом Mikrotik. Запускать скрипты будем через SNMP.

Запуск скриптов возможен в двух режимах:

.1.3.6.1.4.1.14988.1.1.8.1.1.3.{#Index} – при установке командой snmpset значения отличного от нуля разово запускает скрипт с соответствующим индексом.

.1.3.6.1.4.1.14988.1.1.18.1.1.2.{#Index} – методом snmpget запускает соответствующий скрипт и получает возвращаемый результат.

Заметки

Для запуска скриптов требуется разрешение на запись в настройках Community в Mikrotik

6. Примеры получения не стандартных метрик

Скрипт получения количества свободных IP в пуле

```
:local poolname default-dhcp
:local minaddress
:local maxaddress
:local pooladdresses
:local poolused
:local poolfree
:local findindex
:local tmpint
:local maxindex
:local poolrange [/ip pool get $poolname range]
#Get min and max addresses
:set findindex [:find [:tostr $poolrange] "-"]
:if ([:len $findindex] > 0) do={
    :set minaddress [:pick [:tostr $poolrange] 0 $findindex]
    :set maxaddress [:pick [:tostr $poolrange] ($findindex + 1) [:len [:tostr $poolrange]]]
} else={
    :set minaddress [:tostr $poolrange]
    :set maxaddress [:tostr $poolrange]
}
#Convert to array of octets (replace '.' with ',')
:for x from=0 to=([:len [:tostr $minaddress]] - 1) do={
    :if ([:pick [:tostr $minaddress] $x ($x + 1)] = ".") do={
        :set minaddress ([:pick [:tostr $minaddress] 0 $x] . "," . [:pick [:tostr $minaddress] ($x + 1) [:len [:tostr $minaddress]]])
    }
}
:for x from=0 to=([:len [:tostr $maxaddress]] - 1) do={
    :if ([:pick [:tostr $maxaddress] $x ($x + 1)] = ".") do={
        :set maxaddress ([:pick [:tostr $maxaddress] 0 $x] . "," . [:pick [:tostr $maxaddress] ($x + 1) [:len [:tostr $maxaddress]]])
    }
}
```

6. Примеры получения не стандартных метрик

Скрипт получения количества свободных IP в пуле

```
#Calculate available addresses for current range
:if ([:len [:toarray $minaddress]] = [:len [:toarray $maxaddress]]) do={
    :set maxindex ([:len [:toarray $minaddress]] - 1)
    :for x from=$maxindex to=0 step=-1 do={
        #Calculate 256^($maxindex - $x)
        :set tmpint 1
        :if (($maxindex - $x) > 0) do={
            :for y from=1 to=($maxindex - $x) do={ :set tmpint (256 * $tmpint) }
        }
        :set tmpint ($tmpint * ([:tonum [:pick [:toarray $maxaddress] $x]] - [:tonum [:pick [:toarray $minaddress] $x]]) )
        :set pooladdresses ($pooladdresses + $tmpint)
    }
}
#Add current range to total pool's available addresses
:set pooladdresses ($pooladdresses + 1)
:set poolused [:len [/ip pool used find pool=[:tostr default-dhcp]]]
:set poolfree ($pooladdresses - $poolused)
:put $poolfree
```

6. Примеры получения не стандартных метрик

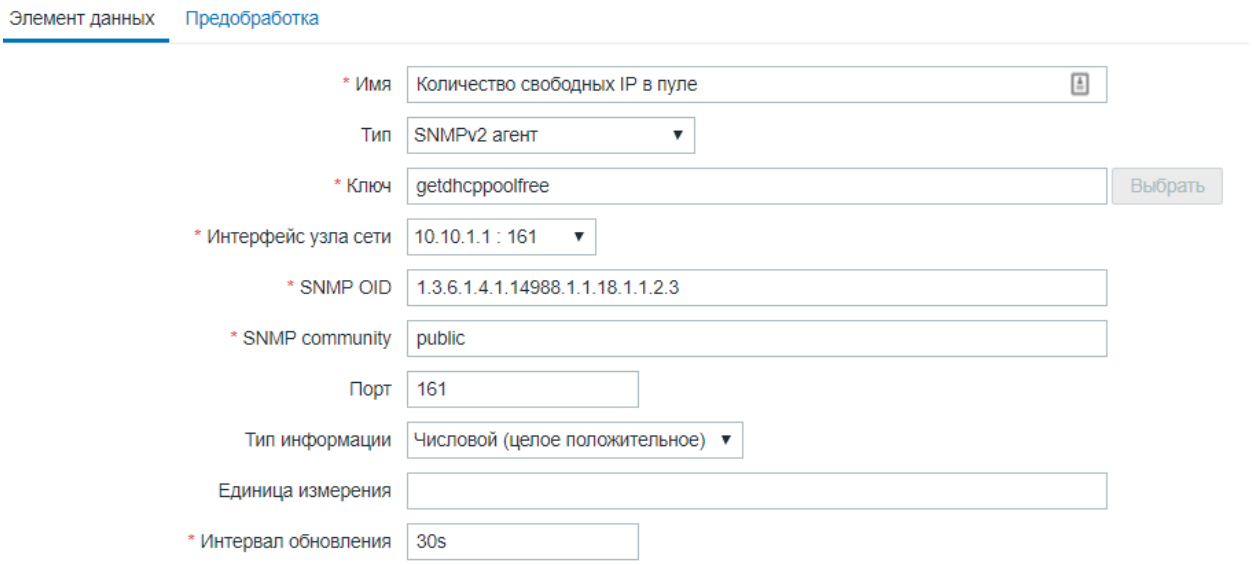
Определяем SNMP Index нашего скрипта

Командой snmpwalk получаем список всех скриптов по oid 1.3.6.1.4.1.14988.1.1.8.1.1

```
MIKROTIK-MIB::mtxrScriptName.1 = STRING: Backup_to_email
MIKROTIK-MIB::mtxrScriptName.2 = STRING: NTPServerUpdate
MIKROTIK-MIB::mtxrScriptName.3 = STRING: Get_DHCP_Pool_Free
```

6. Примеры получения не стандартных метрик

Для получения результатов скрипта создадим элемент данных



7. Контроль безопасности сети средствами мониторинга

MikroTik

7. Контроль безопасности сети средствами мониторинга

1. Контроль выключенных сервисов

Любым понравившимся способом получаем текущее состояние сервисов

:put [ip service get api value-name=disabled]

Заметки

Принимает значения true если сервис выключен и false если включен

7. Контроль безопасности сети средствами мониторинга

2. Контроль открытых портов

Для это используется тип элемента данных «Простая проверка» с ключом net.tcp.service или net.tcp.service

Например net.tcp.service[tcp,{HOST.CONN},8080]

Заметки

Возвращаемые значения 1 при открытом порте, 0 при невозможности установки соединения.

Благодаря распределенной схеме мониторинга с Proxy возможна проверка с разных зон Firewall относительно Mikrotik.

7. Контроль безопасности сети средствами мониторинга

3. Контроль наличия и активности правил файрвола

Легко и просто создать правила мониторинга наличия включенного правила “All Drop”

Например :put [/ip firewall filter get value-name=disabled [find where comment~"drop all from WAN"]]

Заметки

Принимает значения true если правило выключено и false если включено

8. Список материалов для самостоятельного изучения

MikroTik

8. Список материалов для самостоятельного изучения

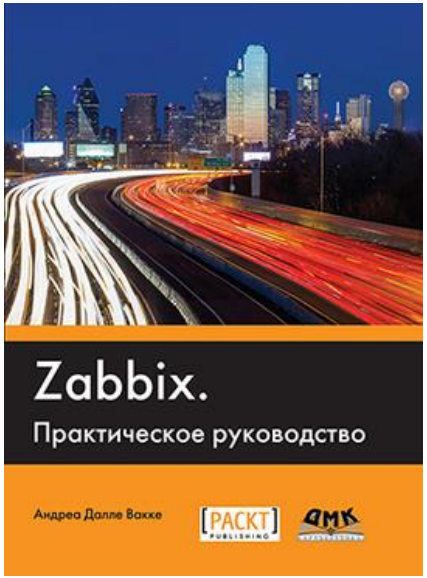
ZABBIX. ПРАКТИЧЕСКОЕ РУКОВОДСТВО

Автор: Далле Вакке А.

Издательство: ДМК Пресс

Дата выхода: октябрь 2016 года

В книге описаны основные понятия и объекты системы, а так же описан процесс установки и настройки. Позволяет проще освоить систему и приступить к внедрению.



8. Список материалов для самостоятельного изучения

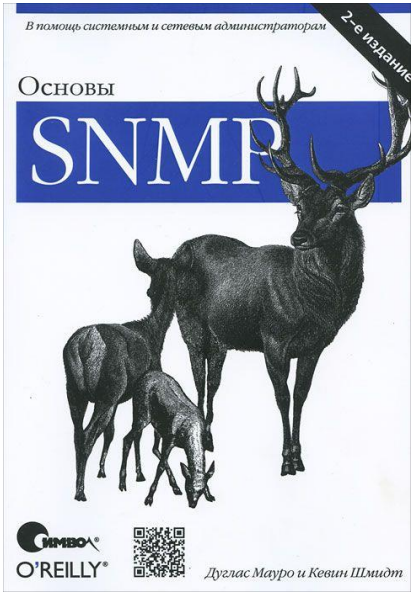
RealSD

Основы SNMP

Автор: Дуглас Мауро, Кевин Шмидт

Издательство: Символ-Плюс

Дата выхода: 2012 года



Книга начинается с объяснения основных принципов SNMP и его работы и охватывает такие технические элементы, как идентификаторы объектов (OID), базы MIB, строки сообщества и ловушки. Внимание авторов сосредоточено на практическом системном и сетевом администрировании.

8. Список материалов для самостоятельного изучения

Онлайн документация

MikroTik Wiki

https://wiki.mikrotik.com/wiki/Main_Page

Zabbix документация

https://www.zabbix.com/documentation/4.2/start

Спасибо за внимание!
Вопросы?

Презентация
https://nc.realclouds.ru/index.php/s/D8rzwmsbPiYrNJt

Контакты

E-mail moroz@llcreal.ru
Telegram https://t.me/AntonMoroz_LLCReal
WhatsApp https://wa.me/74957776832