?????????? ?? ?????????? ? ???????? ????????? Zabbix ?? ????????? SNMPv2

?????????? ?? ?????????? ? ???????? ????????? Zabbix ?? ????????? SNMPv2

В качестве приложения использовалась KATA Central Node версии 6.0.2, а в качестве системы мониторинга использовался Zabbix версии 6.4. Инструкция носит информационный характер и может отличаться от ваших действий.

Готовый шаблон Zabbix с элементами данных: https://box.kaspersky.com/d/179e900f0d29464eaa27/

????????? ?? ??????? Central Node

Вы можете отправлять данные о загрузке центрального процессора и оперативной памяти серверов Central Node и Sensor во внешние системы, поддерживающие протокол SNMP. Для этого вам требуется настроить параметры соединения с протоколом.

Если компонент Central Node развернут в виде кластера, во внешние системы отправляются данные о загрузке центрального процессора и оперативной памяти каждого сервера кластера.

Чтобы настроить параметры соединения с протоколом SNMP на сервере Central Node:

1. В окне веб-интерфейса приложения выберите раздел **Параметры**, подраздел **Общие параметры**.

2. В блоке параметров **SNMP** установите флажок **Использовать SNMP**.

3. В поле **Версия протокола** выберите версию протокола: v2c.

4. В поле **Строка сообщества** укажите пароль, который будет использоваться для подключения к Kaspersky Anti Targeted Attack Platform.

Параметры соединения с протоколом на сервере Central Node будут настроены.

Подробнее: https://support.kaspersky.ru/kata/6.0/247539

????????? ?? ??????? Zabbix

Установите пакет SNMP. На Debian подобных системах:

```
sudo apt install snmp
```

На RHEL подобных системах:

```
sudo yum install net-snmp
```

Запустите команду snmpwalk, чтобы проверить, что все работает. Синтаксис утилиты:

```
snmpwalk -v [версия SNMP] -c [строка сообщества] [IP-адрес/имя хоста устройства] [OID или символьное имя]
```

OID’ы и символьные имена описаны по ссылке: https://support.kaspersky.ru/kata/6.0/233730

Например, рассмотрим OID 1.3.6.1.4.1.2021.9.1.6, где:

- 1.3.6.1.4.1.2021.9.1.6 – это часть OID, определяющая тип объекта (в данном случае, это OID для свойства «dskTotal», которое указывает на размер диска или тома в КБ).
- В конце OID’а должен указываться “instance identifier” или экземпляр данного объекта (в данном случае, это .1 или .2, которые соответствуют дискам /dev/sda2 или /dev/sda3). Таким образом, для объектов, имеющих несколько экземпляров, этот идентификатор позволяет получать данные для каждого отдельного элемента. OID’ы имеющие единственный элемент будут иметь экземпляр .0.

```
root@kedr-ubuntu-demo-lab:~# snmpwalk -v 2c -On -c public 192.168.12.180 laLoad
Bad operator (INTEGER): At line 73 in /usr/share/snmp/mibs/ietf/SNMPv2-PDU
.1.3.6.1.4.1.2021.10.1.3.1 = STRING: 3.50
.1.3.6.1.4.1.2021.10.1.3.2 = STRING: 3.01
.1.3.6.1.4.1.2021.10.1.3.3 = STRING: 2.99
root@kedr-ubuntu-demo-lab:~#
```

На скриншоте выше приведен ещё один пример, где предоставлены OID’ы и значения средней загрузки системы (load average) в течении 1, 5 и 15 минут. Также использовался ключ **-On**, чтобы вывести цифровые идентификаторы, а не символьные имена.

Для дальнейшей настройки нас интересуют конкретные OID’ы, так как Zabbix использует в своей работе утилиту snmpget.

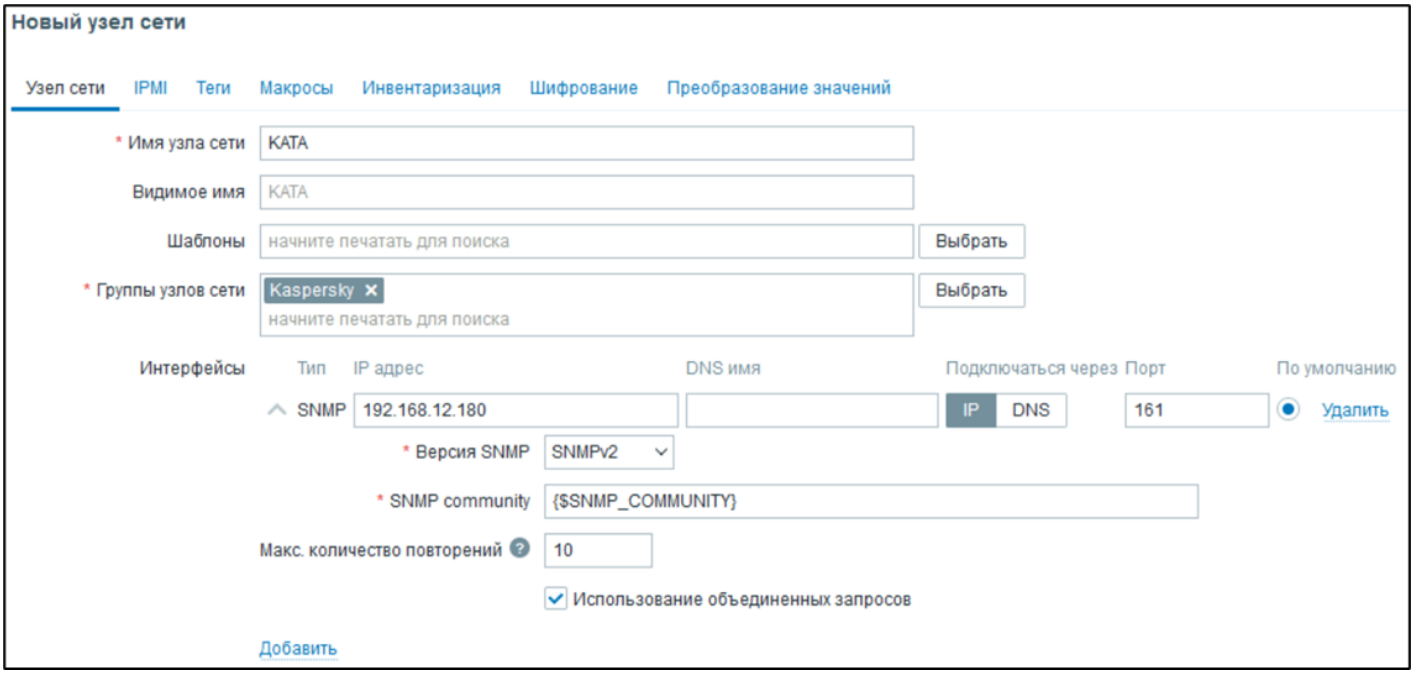
Основное различие, что SNMPGET извлекает значения для конкретных OID, в то время как SNMPWALK рекурсивно проходит по всему поддереву OID, начиная с указанного корневого OID, и извлекает значения для всех соответствующих объектов.

SNMPWALK обычно используется для обнаружения и сбора более широкого набора данных с устройства или для получения общего представления о доступной информации SNMP. SNMPGET же применяется для извлечения конкретных значений OID, когда известно точное расположение требуемых данных.

Далее в веб-консоли Zabbix необходимо добавить Узел сети:

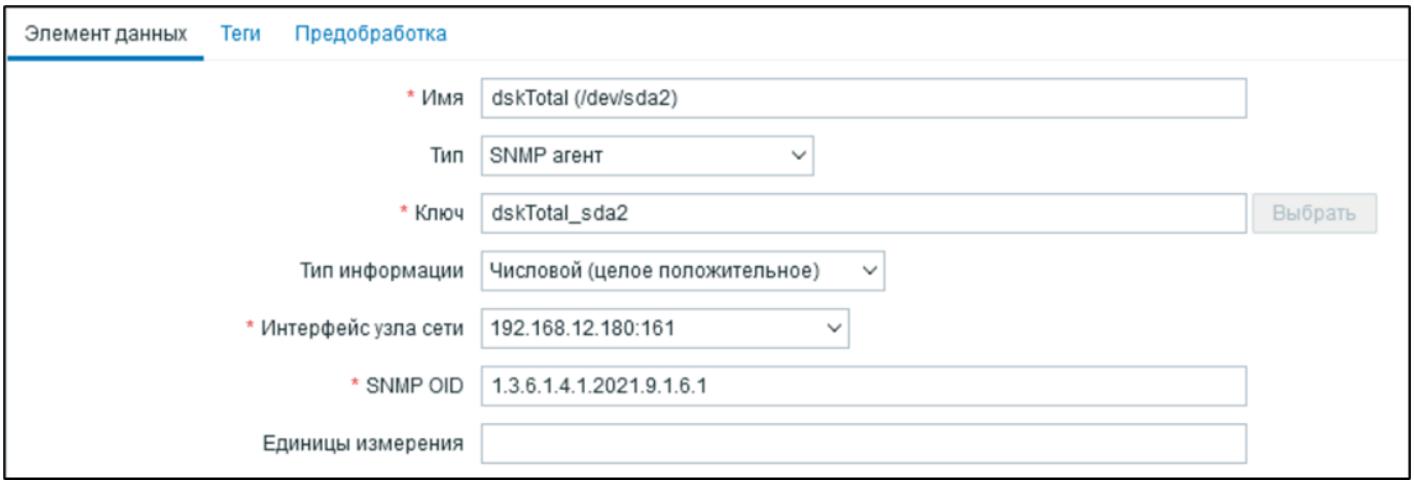
1. Перейдите в раздел **Сбор данных**, подраздел **Узлы сети**.

2. Нажмите на кнопку **Создать узел сети**, укажите произвольное имя и группу узла сети. В разделе **Интерфейсы** нажмите кнопку **Добавить** и выберите **SNMP**. Далее укажите IP адрес узла сети (в данном случае, адрес Central Node) и SNMP community (строка сообщества), если меняли его в Central Node.



3. После добавления узла, переходите в **Элементы данных**

4. Нажмите на кнопку **Создать элемент данных**, укажите произвольное имя, выберите тип **SNMP агент**, укажите ключ (уникальное значение в рамках одного хоста), определите тип информации и укажите SNMP OID.



5. Далее можете нажать кнопку **Тест**, чтобы проверить корректность введенных данных. По завершению нажмите кнопку **Добавить**. С этого момента Zabbix начнет запрашивать данные, согласно указанному интервалу обновления.

6. Добавьте по аналогии нужные элементы данных.

Revision #3
Created 13 August 2025 12:22:55 by Павел
Updated 6 February 2026 11:11:19 by Кирилл