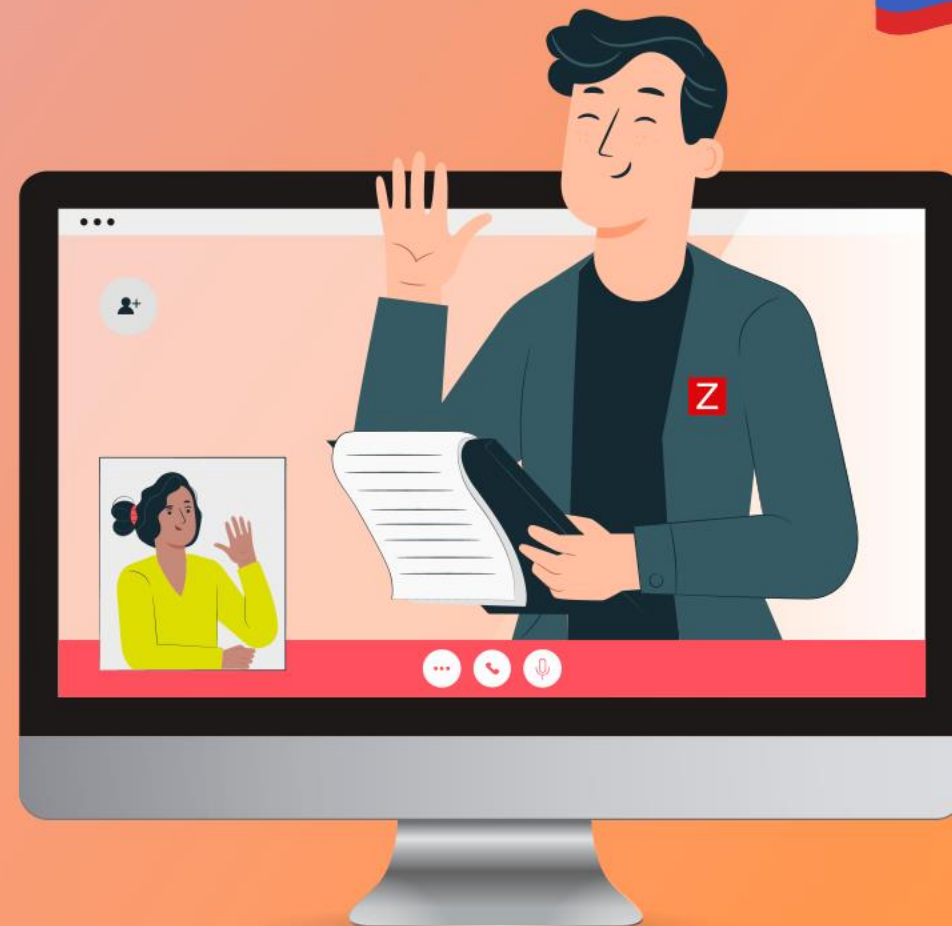


RUSSIAN



MEETUP ONLINE '21



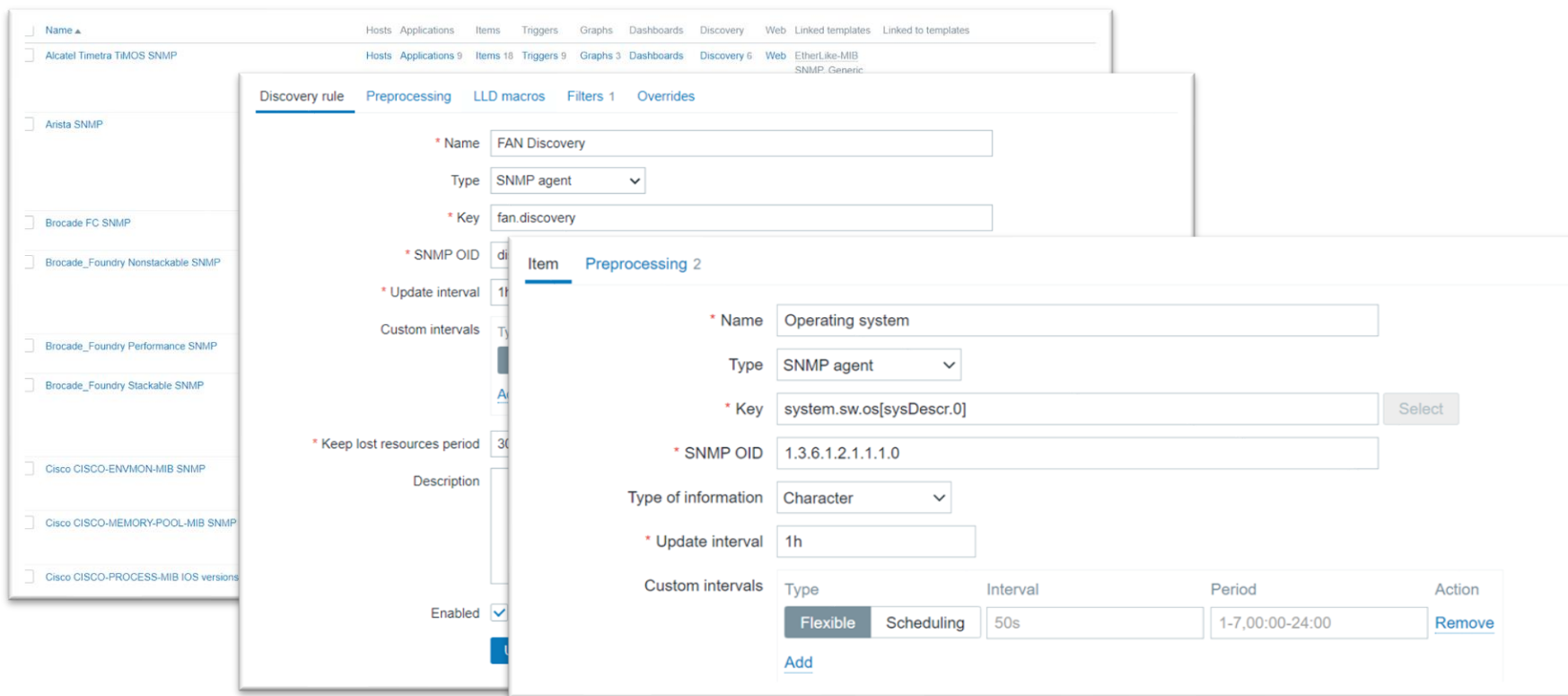
СОЗДАНИЕ ШАБЛОНОВ ДЛЯ SNMP УСТРОЙСТВ

АЛЕКСАНДР ПЕТРОВ-ГАВРИЛОВ
ИНЖЕНЕР ТЕХНИЧЕСКОЙ ПОДДЕРЖКИ

ZABBIX

МОНИТОРИНГ SNMP АГЕНТОВ В ZABBIX

- ✓ Использование шаблонов из коробки или от сообщества
- ✓ Создание элементов данных на основе документации производителя или результатов snmpwalk
- ✓ Использование LLD для обнаружения элементов SNMP



The screenshot displays the Zabbix web interface configuration for SNMP agents. It is divided into two main sections: 'Discovery rule' and 'Item'.

Discovery rule configuration:

- Name: FAN Discovery
- Type: SNMP agent
- Key: fan.discovery
- SNMP OID: [empty]
- Update interval: 1h
- Keep lost resources period: 30m
- Description: [empty]
- Enabled:

Item configuration:

- Name: Operating system
- Type: SNMP agent
- Key: system.sw.os[sysDescr.0] (with a 'Select' button)
- SNMP OID: 1.3.6.1.2.1.1.1.0
- Type of information: Character
- Update interval: 1h
- Custom intervals table:

Type	Interval	Period	Action
Flexible Scheduling	50s	1-7,00:00-24:00	Remove

An 'Add' button is located at the bottom of the custom intervals table.



СОЗДАНИЕ ПОЛЬЗОВАТЕЛЬСКИХ SNMP ШАБЛОНОВ

Я хочу создать свой SNMP шаблон, но с чего начать?

- ☑ Документация производителя будет лучшим началом! (конечно, если она доступна)

coDeviceWirelessInterfaceStatusTable

.1.3.6.1.4.1.18744.5.25.1.2.1

not-accessible

Device wireless interface status attributes.

- coDeviceWirelessInterfaceStatusEntry

.1.3.6.1.4.1.18744.5.25.1.2.1.1

not-accessible

An entry in the coDeviceWirelessInterfaceStatusTable. coDevDisIndex - Uniquely identifies a device in the MultiService Controller. coDevWirIfStaRadioIndex - Uniquely identifies a radio on the device.

- coDevWirIfStaRadioIndex

.1.3.6.1.4.1.18744.5.25.1.2.1.1.1

not-accessible

Specifies the

- coDevWirIfStaRadioIndex

.1.3.6.1.4.1.18744.5.25.1.2.1.1.1

Link to coDevWirIfStaRadioIndex

- coDevWirIfStaRadioIndex

.1.3.6.1.4.1.18744.5.25.1.2.1.1.1

The current

- coDevWirIfStaRadioIndex

.1.3.6.1.4.1.18744.5.25.1.2.1.1.1

Identifies the

Table 2-9 scfCpuInfo(1.3.6.1.4.1.211.1.15.4.1.1.9)

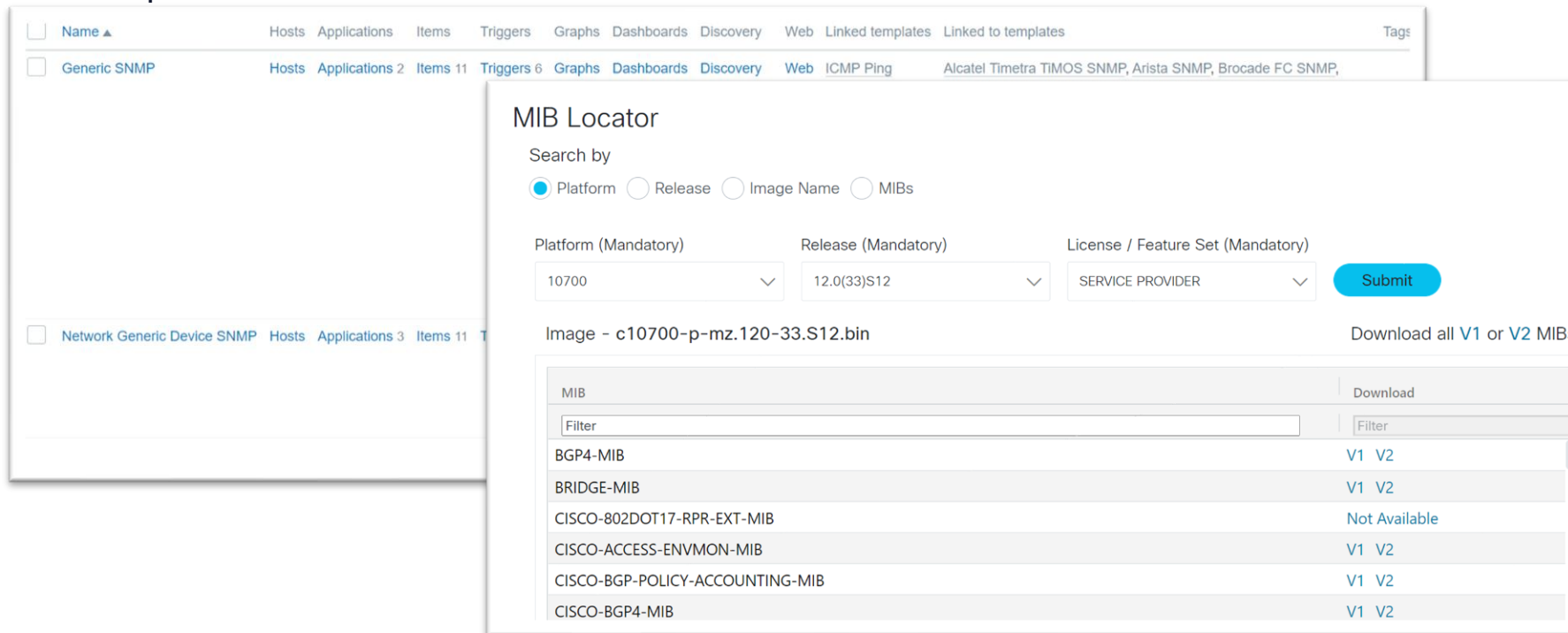
OBJECT-NAME	SUMMARY	OID	INDEX	SYNTAX	MAX-ACCESS
scfCpuNumber	CPU information count (table)	scfCpuInfo.1	.0	Integer32	ro
scfCpuTable	CPU information (table)	scfCpuInfo.2	-	SEQUENCE OF ScfMemoryEntry	na
scfCpuEntry	-	scfCpuTable.1	-	ScfMemoryEntry	na
scfCpuBoardType	Board identity	scfCpuEntry.1	.Parts identifier (*1)	ScfComponentType	ro
scfCpuBoardId	Board number	scfCpuEntry.2	.Parts identifier (*1)	ScfIndex	ro
scfCpuModuleType	Part identity	scfCpuEntry.3	.Parts identifier (*1)	ScfComponentType	ro
scfCpuModuleId	Part number	scfCpuEntry.4	.Parts identifier (*1)	ScfIndex	ro
scfCpuSubType	Part (sub) identity	scfCpuEntry.5	.Parts identifier (*1)	ScfComponentType	ro
scfCpuSubId	Part (sbu) number	scfCpuEntry.6	.Parts identifier (*1)	ScfIndex	ro
scfCpuType	CPU type name	scfCpuEntry.7	.Parts identifier (*1)	DisplayString	ro
scfCpuFrequency	CPU frequency	scfCpuEntry.8	.Parts identifier (*1)	Integer32	ro
scfCpuAdditionalInfo	CPU additional information	scfCpuEntry.9	.Parts identifier (*1)	DisplayString	ro
scfCpuMemoryMode	Memory mirror mode	scfCpuEntry.10	.Parts identifier (*1)	ScfMemoryMirroMode	ro
scfCpuState	CPU operating state	scfCpuEntry.11	.Parts identifier (*1)	ScfStateTC	ro

*1: For "Parts identifier" in INDEX, see "4.1 Parts identifier (OID)".



СОЗДАНИЕ ПОЛЬЗОВАТЕЛЬСКИХ SNMP ШАБЛОНОВ

- ✓ Проверьте были предоставлены производителем MIB файлы (например относящиеся только к их устройствам)
- ✓ SNMP шаблоны доступные из коробки, можно смело совмещать с MIB файлами общего назначения!



The screenshot shows the Zabbix MIB Locator interface. The main window displays a search form with the following fields:

- Search by:** Platform (selected), Release, Image Name, MIBs
- Platform (Mandatory):** 10700
- Release (Mandatory):** 12.0(33)S12
- License / Feature Set (Mandatory):** SERVICE PROVIDER
- Submit** button

Below the search form, the results are displayed as a table:

Image - c10700-p-mz.120-33.S12.bin Download all V1 or V2 MIB:

MIB	Download
BGP4-MIB	V1 V2
BRIDGE-MIB	V1 V2
CISCO-802DOT17-RPR-EXT-MIB	Not Available
CISCO-ACCESS-ENVMON-MIB	V1 V2
CISCO-BGP-POLICY-ACCOUNTING-MIB	V1 V2
CISCO-BGP4-MIB	V1 V2



СОЗДАНИЕ ПОЛЬЗОВАТЕЛЬСКИХ SNMP ШАБЛОНОВ

Хорошо, но как мне организовать среду для тестирования моих шаблонов?

- ❌ Некорректно настроенные шаблоны могут стать причиной всплеска запросов на ваших устройствах
- ❌ Иногда устройство не доступно напрямую во время разработки шаблона

github.com/etingof/snmpsim

SNMP Simulator

pyPI v0.4.7 | python 2.4 | 2.5 | 2.6 | 2.7 | 3.2 | 3.3 | 3.4 | 3.5 | 3.6 | 3.7 | build passing | license BSD

This is a pure-Python, open source and free implementation of SNMP agents simulator distributed under 2-clause BSD license.

Features

- SNMPv1/v2c/v3 support
- SNMPv3 USM supports MD5/SHA/SHA224/SHA256/SHA384/SHA512 auth and DES/3DES/AES128/AES192/AES256 privacy crypto algorithms
- Runs over IPv4 and/or IPv6 transports
- Simulates many EngineID's, each with its own set of simulated objects
- Varies response based on SNMP Community, Context, source/destination addresses and ports
- Can gather and store snapshots of SNMP Agents for later simulation
- Can run simulation based on MIB files, snmpwalk and sapwalk output
- Can gather simulation data from network traffic or tcpdump snoops
- Can gather simulation data from external program invocation or a SQL database
- Can trigger SNMP TRAP/INFORMs on SET operations
- Capable to simultaneously simulate tens of thousands of Agents
- Offers REST API based [control plane](#)
- Gathers and reports extensive activity metrics
- Pure-Python, easy to deploy and highly portable
- Can be extended by loadable Python engine



ПОДГОТОВКА ПРАВИЛЬНЫХ ИНСТРУМЕНТОВ

Симулируем SNMP устройство!

Для начала ещё раз убедимся в правильно подобранных инструментах:

- ✓ CentOS 8
- ✓ Zabbix 5.2
- ✓ Документация Zabbix (SNMP обнаружение)
- ✓ Установленный SNMPSIM
- ✓ Результат snmpwalk команды с нашего устройства
- ✓ Документация производителя
- ✓ MIB файлы устройства



ВЫПОЛНИМ SNMPWALK

- ✓ Выполните snmpwalk на вашем устройстве

```
[root@localhost ~]# snmpwalk -v2c -On -c Meetup
192.168.1.126
.1.3.6.1.2.1.1.1.0 = STRING: 1148VXP
.1.3.6.1.2.1.1.2.0 = OID: .1.3.6.1.4.1.664.1.1416
.1.3.6.1.2.1.1.3.0 = Timeticks: (813572029) 94 days,
3:55:20.29
.1.3.6.1.2.1.1.4.0 = STRING: www.adtran.com
.1.3.6.1.2.1.1.7.0 = INTEGER: 4
.1.3.6.1.2.1.1.8.0 = Timeticks: (0) 0:00:00.00
.1.3.6.1.2.1.2.1.0 = INTEGER: 6160
.1.3.6.1.2.1.2.2.1.1.1 = INTEGER: 1
.1.3.6.1.2.1.2.2.1.1.2 = INTEGER: 2
..1.3.6.1.2.1.2.2.1.1.100001 = INTEGER: 100001
...
```

- ✓ Сохраните результат в отдельный файл



УСТАНОВКА SNMPsim

- ✓ Установите python

```
yum install python3
```

- ✓ Используйте pip (*package installer for Python*) чтобы установить snmpsim

```
pip3 install snmpsim
```

- ✓ Snmpsim не запустится под повышенными правами пользователя
- ✓ Создайте новую группу и пользователей

```
groupadd snmpd  
useradd -g snmpd snmpd
```

- ✓ Создайте директорию для хранения вывода snmpwalk MIB файлов

```
mkdir -p /usr/share/snmpsim/data
```



ЗАПУСТИТЕ SNMPSIM

- ✓ Запустите snmpsim указав IP/Port для прослушивания

```
snmpsimd.py --agent-udp4-endpoint=192.168.1.126:1024
```

- ✓ snmpwalk файл становится именем сообщества (community name)

```
Configuring /usr/share/snmpsim/data/192.168.1.126.raw.snmpwalk controller  
SNMPv1/2c community name: 192.168.1.126.raw  
SNMPv3 Context Name: 6bdad8c3906f65190f7c5f4674434a6c or 192.168.1.126.raw
```



ТЕСТ SNMPSIM

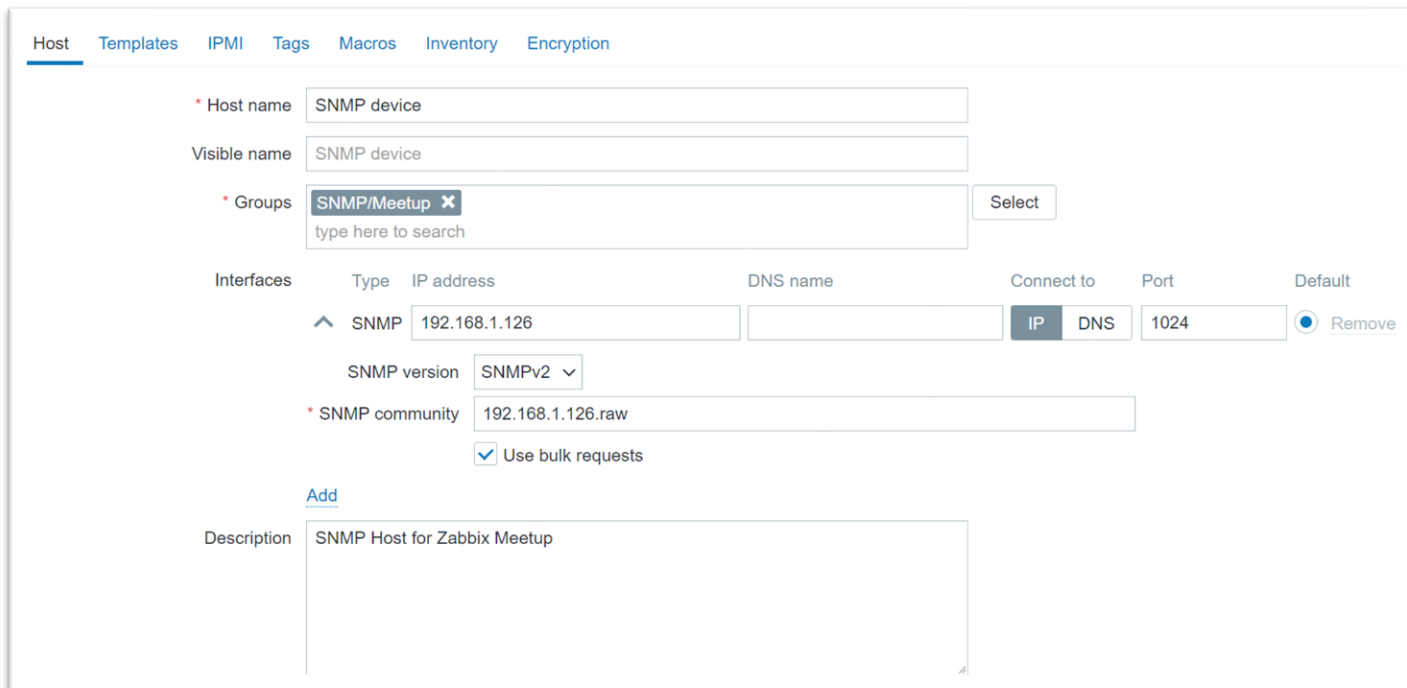
- ✓ Проверим сможем ли мы выполнить snmpwalk до сэмულიрованного устройства

```
[root@localhost ~]# snmpwalk -v2c -c '192.168.1.126.raw' 192.168.1.126:1024
SNMPv2-MIB::sysDescr.0 = STRING: 1148VXP
SNMPv2-MIB::sysObjectID.0 = OID: SNMPv2-SMI::enterprises.664.1.1416
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (813572029) 94 days,
3:55:20.29
SNMPv2-MIB::sysContact.0 = STRING: www.adtran.com
SNMPv2-MIB::sysName.0 = STRING: WINF-OKHR
SNMPv2-MIB::sysLocation.0 = STRING: FM 946 SOUTH @ WINFREY RD
SNMPv2-MIB::sysServices.0 = INTEGER: 4
SNMPv2-MIB::sysORLastChange.0 = Timeticks: (0) 0:00:00.00
IF-MIB::ifNumber.0 = INTEGER: 6160
IF-MIB::ifIndex.1 = INTEGER: 1
```



ПРОВЕРЯЕМ SNMP SIM ИЗ ZABBIX

✓ Теперь попробуем создать узел в Zabbix



The screenshot shows the Zabbix web interface for creating a new host. The 'Host' tab is selected, and the configuration is for an SNMP device. The 'Host name' and 'Visible name' fields are both set to 'SNMP device'. The 'Groups' dropdown is set to 'SNMP/Meetup'. The 'Interfaces' table shows one interface of type 'SNMP' with IP address '192.168.1.126', DNS name empty, 'Connect to' set to 'IP', and 'Port' set to '1024'. The 'SNMP version' is set to 'SNMPv2'. The 'SNMP community' is set to '192.168.1.126.raw', and the 'Use bulk requests' checkbox is checked. The 'Description' field contains 'SNMP Host for Zabbix Meetup'.

Interfaces	Type	IP address	DNS name	Connect to	Port	Default
SNMP	SNMP	192.168.1.126		IP	1024	Remove

✓ И снова – нужно указать правильное имя сообщества, IP адрес и порт! (Имя сообщества = *SNMPWalk* файл)



ПРОВЕРЯЕМ SNMP SIM ИЗ ZABBIX

☑ Давайте попробуем создать элемент данных на нашем SNMP устройстве

Item [Preprocessing 1](#)

* Name	<input type="text" value="Port 7 incoming traffic"/>
Type	<input type="text" value="SNMP agent"/>
* Key	<input type="text" value="ifHCInOctets.103007"/> <input type="button" value="Select"/>
* Host interface	<input type="text" value="192.168.1.126 : 1024"/>
* SNMP OID	<input type="text" value=".1.3.6.1.2.1.31.1.1.1.6.103007"/>
Type of information	<input type="text" value="Numeric (unsigned)"/>
Units	<input type="text" value="Bps"/>
* Update interval	<input type="text" value="1m"/>

☑ Но как я получил числовой OID если вывод SNMPWalk был в текстовом формате?



ПРОВЕРЯЕМ SNMP SIM ИЗ ZABBIX

✓ Текстовый вывод

```
IF-MIB::ifHCInOctets.103007 = Counter64: 7566464822  
IF-MIB::ifHCInOctets.103008 = Counter64: 48097542881  
IF-MIB::ifHCInOctets.103009 = Counter64: 75748849150  
IF-MIB::ifHCInOctets.103010 = Counter64: 25963616931
```

✓ Воспользуемся snmptranslate

```
[root@localhost ~]# snmptranslate -On -IR ifHCInOctets  
.1.3.6.1.2.1.31.1.1.1.6
```

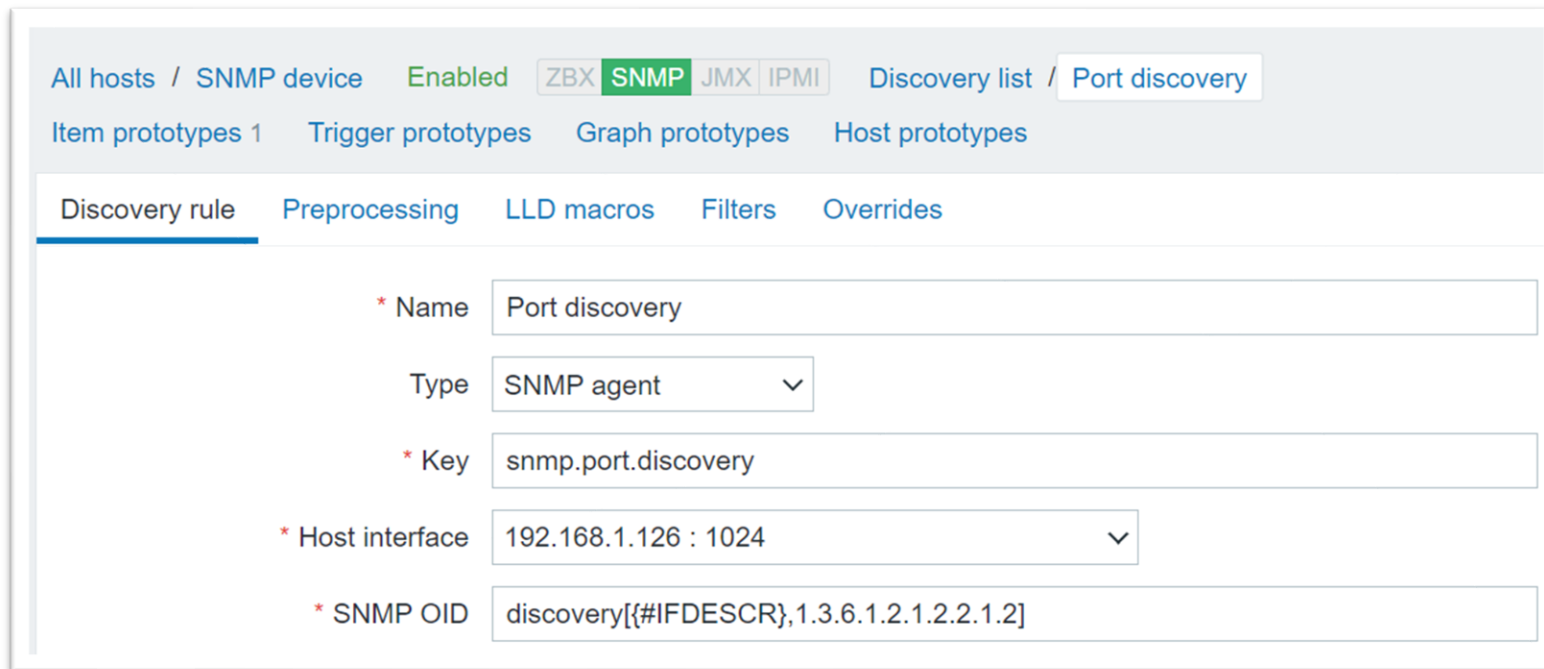
✓ Теперь нам нужно просто добавить индекс – 103007 в конце OID

* Key	<input type="text" value="ifHCInOctets.103007"/>	<input type="button" value="Select"/>
* Host interface	<input type="text" value="192.168.1.126 : 1024"/>	▼
* SNMP OID	<input type="text" value=".1.3.6.1.2.1.31.1.1.1.6.103007"/>	



СОЗДАНИЕ ПРАВИЛА SNMP ОБНАРУЖЕНИЯ

✓ Создайте LLD правило



The screenshot shows the Zabbix configuration interface for creating an LLD rule. The breadcrumb trail is: All hosts / SNMP device Enabled ZBX SNMP JMX IPMI Discovery list / Port discovery. Below this are tabs for Item prototypes 1, Trigger prototypes, Graph prototypes, and Host prototypes. The 'Discovery rule' tab is active, with sub-tabs for Preprocessing, LLD macros, Filters, and Overrides. The configuration fields are:

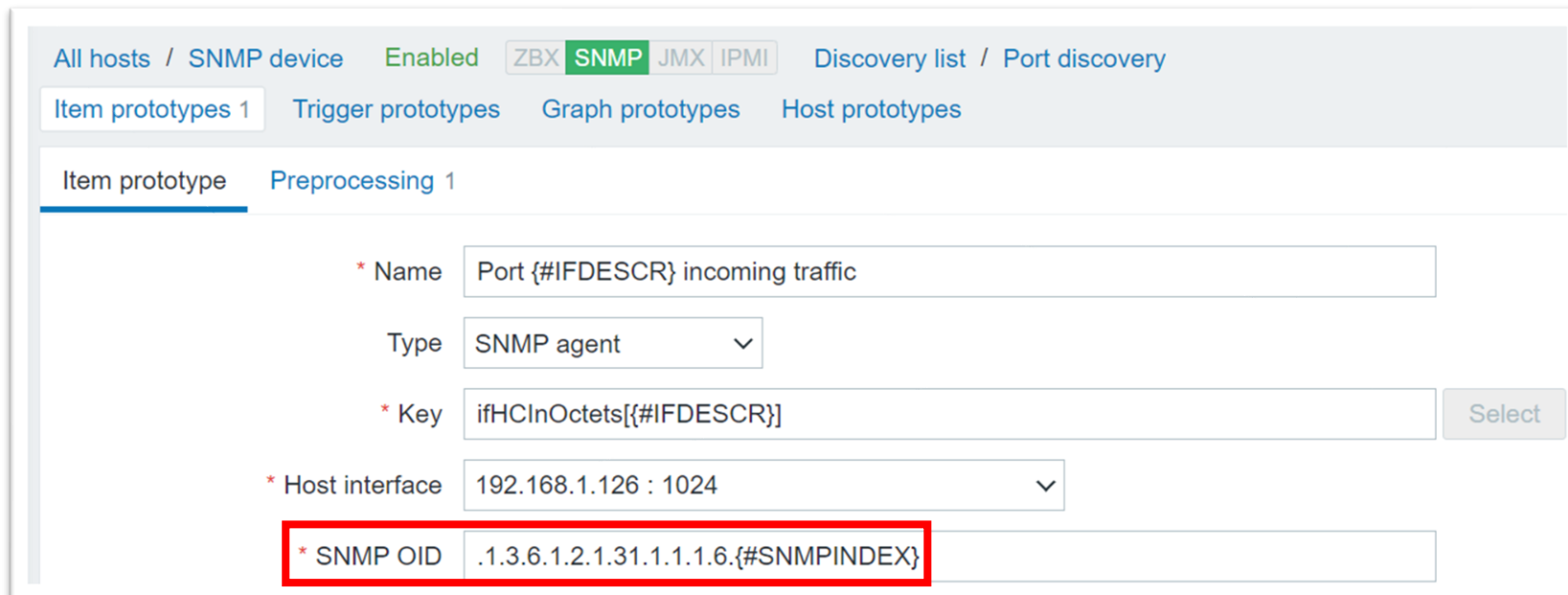
- * Name: Port discovery
- Type: SNMP agent
- * Key: snmp.port.discovery
- * Host interface: 192.168.1.126 : 1024
- * SNMP OID: discovery[#{IFDESCR},1.3.6.1.2.1.2.2.1.2]

- ✓ Мы будем обнаруживать все индексы под 1.3.6.1.2.1.2.2.1.2 (*IFDescr*)
- ✓ Мы так же обнаружим все описание под этими индексами



СОЗДАНИЕ ПРОТОТИПА ЭЛЕМЕНТА ДАННЫХ ДЛЯ SNMP

- ✓ Создайте прототип элемента данных для входящего трафика



The screenshot shows the Zabbix web interface for creating an item prototype. The breadcrumb navigation is "All hosts / SNMP device Enabled ZBX SNMP JMX IPMI Discovery list / Port discovery". The "Item prototypes" tab is active, showing "Preprocessing 1". The configuration fields are:

- * Name: Port {#IFDESCR} incoming traffic
- Type: SNMP agent
- * Key: ifHCInOctets[{#IFDESCR}]
- * Host interface: 192.168.1.126 : 1024
- * SNMP OID: .1.3.6.1.2.1.31.1.1.6.{#SNMPINDEX}

The "SNMP OID" field is highlighted with a red box.

- ✓ Обнаруженные индексы {#SNMPINDEX} будут добавлены в конце OID (*ifHCInOctets*)



ОШИБКА – NO SUCH INSTANCE CURRENTLY EXISTS

Wizard	Name ▲	Triggers	Key	Interval	History	Trends	Type	Applications	Status	Info
	...	Port 7 incoming traffic	ifHCInOctets.103007	1m	90d	365d	SNMP agent		Enabled	
		Port discovery: Port AltInband1 incoming traffic	ifHCInOctets[AltInband1]	1m	90d	365d	SNMP agent		Not supported	
		Port discovery: Port AltInband2 incoming traffic	ifHCInOctets[AltInband2]	1m	90d	365d	SNMP agent		No Such Instance currently exists at this OID	
		Port discovery: Port AltInband3 incoming traffic	ifHCInOctets[AltInband3]	1m	90d	365d	SNMP agent		Not supported	

- ✓ Вызвана наличием большего числа индексов IfDescr в сравнении с ifHCInOctets
- ✓ Решается отфильтровыванием лишних индексов по IfDescr:

All hosts / SNMP device Enabled ZBX SNMP JMX IPMI Discovery list / Port discovery

Item prototypes 1 Trigger prototypes Graph prototypes Host prototypes

Discovery rule Preprocessing LLD macros **Filters 1** Overrides

Filters

Label	Macro	Regular expression	Action
A	{#IFDESCR}	does not match <input type="checkbox"/> (^AltInband ^backplane FXS ^vds ^lpbk ^eth0\$ ^eth1\$	Remove

[Add](#)

[Update](#) [Clone](#) [Execute now](#) [Test](#) [Delete](#) [Cancel](#)

ФИЛЬТР СУЩНОСТЕЙ LLD

RUSSIAN



MEETUP ONLINE '21

☑ Для создания фильтров, попробуйте обнаружить дополнительные OID's (*IFTYPE*)

All templates / Template Adtran TA1148 / Discovery list / ethernet-like Network interfaces dis...
Item prototypes 9 / Trigger prototypes 4 / Graph prototypes 1 / Host prototypes

Discovery rule / Preprocessing / LLD macros / Filters 3 / Overrides

Parent discovery rules: Template Module Interfaces SNMPv2 ethernet-csmacd

* Name: ethernet-like Network interfaces discovery
Type: SNMP agent
* Key: net.if.discovery.ether
* SNMP OID: discovery[#{#IFDESCR},1.3.6.1.2.1.2.2.1.2,#{#IFTYPE},1.3.6.1.2.1.2.2.1.3,#{#IFNAME

Discovery rule / Preprocessing / LLD macros / Filters 3 / Overrides

Type of calculation: And (A and B) and C

Filters	Label	Macro		Regular expression	Action
	A	{#IFTYPE}	matches	{\$ETH.NET.IF.IFTYPE.MATCHES}	Remove
	B	{#IFTYPE}	does not match	{\$ETH.NET.IF.IFTYPE.NOT_MATCHES}	Remove
	C	{#SNMPINDEX}	does not match	{\$ETH.NET.IF.SNMPINDEX.NOT_MATCHES}	Remove



ОШИБКИ – NO VALUE RECEIVED FOR MACRO

⊖ При попытке обнаружить множество значений – {#IFNAME}, {#IFTYPE}, {#IFDESCR}

All hosts / SNMP device Enabled ZBX **SNMP** JMX IPMI Applications Items 56 Triggers Graphs Discovery rules 1 Web scenarios Filter

Host groups Type

Hosts Update interval

Name

Key

Keep lost resources period

<input type="checkbox"/>	Host	Name ▲	Items	Triggers	Graphs	Hosts	Ke
<input type="checkbox"/>	SNMP device	Port discovery	Item prototypes 1	Trigger prototypes	Graph prototypes	Host prototypes	snmp.port.discovery 1m SNMP agent Enabled

Cannot accurately apply filter: no value received for macro "{#IFDESCR}".
 Cannot accurately apply filter: no value received for macro "{#IFDESCR}".
 Cannot accurately apply filter: no value received for macro "{#IFDESCR}".
 Cannot accurately apply filter: no value received for macro "{#IFDESCR}".
 Cannot accurately apply filter: no value received for macro "{#IFDESCR}".
 Cannot accurately apply filter: no value received for macro "{#IFDESCR}".
 Cannot accurately apply filter: no value received for macro "{#IFDESCR}".
 Cannot accurately apply filter: no value received for macro "{#IFDESCR}".
 Cannot accurately apply filter: no value received for macro "{#IFDESCR}".
 Cannot accurately apply filter: no value received for macro "{#IFDESCR}".
 Cannot accurately apply filter: no value received for macro "{#IFDESCR}".
 Cannot accurately apply filter: no value received for macro "{#IFDESCR}".
 Cannot accurately apply filter: no value received for macro "{#IFDESCR}".
 Cannot accurately apply filter: no value received for macro "{#IFDESCR}".
 Cannot accurately apply filter: no value received for macro "{#IFDESCR}".
 Cannot accurately apply filter: no value received for macro "{#IFDESCR}".
 Cannot accurately apply filter: no value received for macro "{#IFDESCR}".
 Cannot accurately apply filter: no value received for macro "{#IFDESCR}".
 Cannot accurately apply filter: no value received for macro "{#IFDESCR}".
 Cannot accurately apply filter: no value received for macro "{#IFDESCR}".
 Cannot accurately apply filter: no value received for macro "{#IFDESCR}".

Displaying 1 of 1 found



ОШИБКА – NO VALUE RECEIVED FOR MACRO

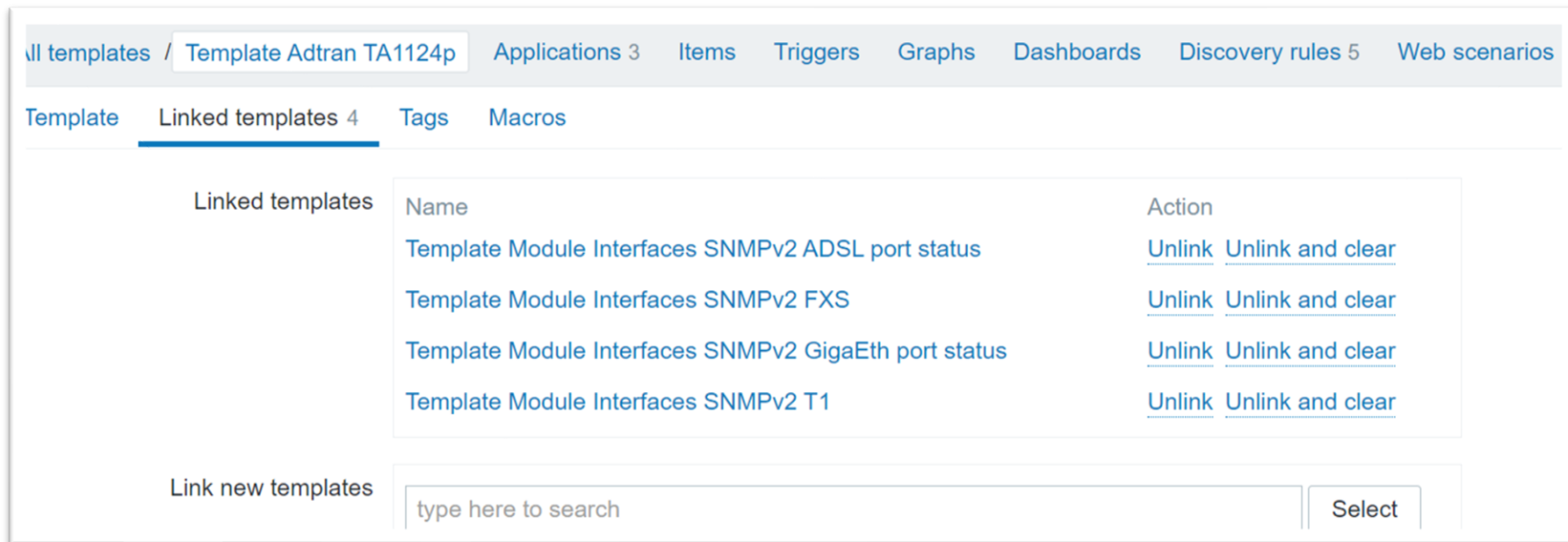
- ☑ Zabbix применяет фильтр ко всем OID в правиле обнаружения

{#IFNAME}	{#IFTYPE}	{#IFDESCR}
1.3.6.1.2.1.31.1.1.1.1.1	1.3.6.1.2.1.2.2.1.3.1	1.3.6.1.2.1.2.2.1.2.1
1.3.6.1.2.1.31.1.1.1.1.2	1.3.6.1.2.1.2.2.1.3.2	1.3.6.1.2.1.2.2.1.2.2
1.3.6.1.2.1.31.1.1.1.1.3	1.3.6.1.2.1.2.2.1.3.3	1.3.6.1.2.1.2.2.1.2.3

- ☑ Индекс 3 отсутствует для {#IFTYPE} и {#IFDESCR}
- ☑ Но попытки отфильтровать {#IFTYPE} и {#IFDESCR} остаются

МОДУЛЬНЫЕ ШАБЛОНЫ И ПРАВИЛА ОБНАРУЖЕНИЯ

✓ Пробуйте создавать модульные шаблоны и правила обнаружения



The screenshot shows a web interface for managing templates. At the top, there is a breadcrumb trail: 'All templates / Template Adtran TA1124p'. Below this, there are several tabs: 'Applications 3', 'Items', 'Triggers', 'Graphs', 'Dashboards', 'Discovery rules 5', and 'Web scenarios'. Underneath, there are sub-tabs: 'Template', 'Linked templates 4', 'Tags', and 'Macros'. The 'Linked templates 4' tab is active. It displays a table with two columns: 'Name' and 'Action'. The table lists four linked templates, each with 'Unlink' and 'Unlink and clear' actions. Below the table, there is a section for 'Link new templates' with a search input field containing the placeholder text 'type here to search' and a 'Select' button.

Name	Action
Template Module Interfaces SNMPv2 ADSL port status	Unlink Unlink and clear
Template Module Interfaces SNMPv2 FXS	Unlink Unlink and clear
Template Module Interfaces SNMPv2 GigaEth port status	Unlink Unlink and clear
Template Module Interfaces SNMPv2 T1	Unlink Unlink and clear

Link new templates:

- ✓ Каждое правило обнаружение создания для интерфейса определённого типа
- ✓ Позволяет Вам отсоединять или присоединять шаблоны для определённых сущностей в родительском шаблоне
- ✓ Вы по прежнему можно отключить или включить правило обнаружения на уровне узла

RUSSIAN



MEETUP ONLINE '21



ВОПРОСЫ?

АЛЕКСАНДР ПЕТРОВ-ГАВРИЛОВ
ИНЖЕНЕР ТЕХНИЧЕСКОЙ ПОДДЕРЖКИ

ZABBIX



RUSSIAN



MEETUP ONLINE '21



СПАСИБО!

АЛЕКСАНДР ПЕТРОВ-ГАВРИЛОВ
ИНЖЕНЕР ТЕХНИЧЕСКОЙ ПОДДЕРЖКИ
ZABVIX

