MikroTik Warsaw
Training Center

MikroTik i Zabbix®

Jak monitorować ?

MikroTik Warsaw Training Center

Michał Filipek

Network Architect
Zabbix Trainer
MikroTik Trainer

/in/michalfilipek

michal@mwtc.pl

Certyfikowane Szkolenia
Zabbix, MikroTik

Sieci IP
Konsultacje, Projektowanie i Wdrożenia

Systemy Monitoringu
Wdrożenia

ZABBIX

Agenda

- SNMP, Simple checks, SSH agent
- Template Net Mikrotik SNMPv2
- LLD – Low Level Discovery
- Zdalne wykonanie skryptu za pomocą SNMP
- Dodawanie wielu hostów
  - Import/export XML
  - Network Discovery
  - API

Simple checks, SSH agent, SNMP

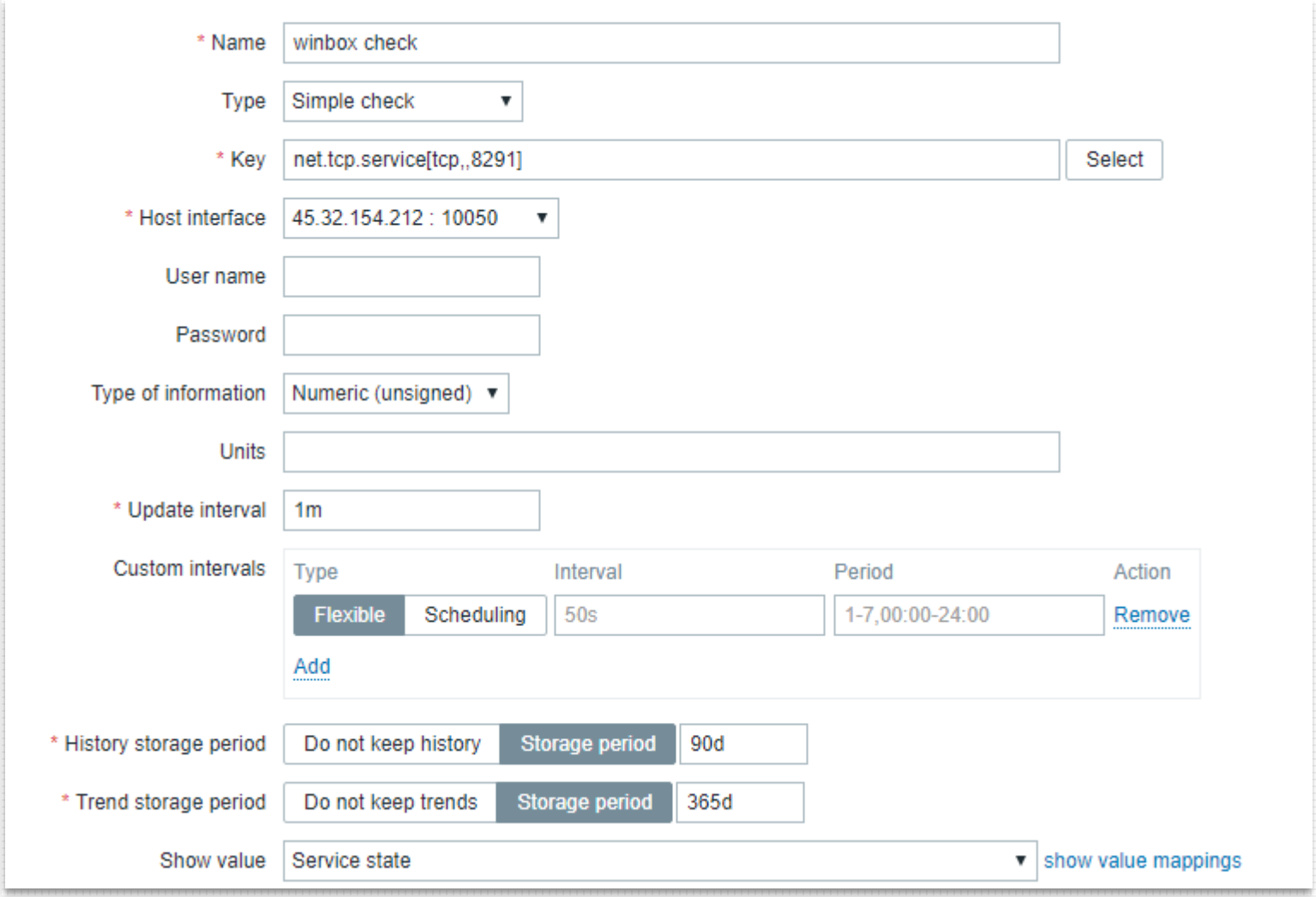
ZABBIX

Simple checks – prosta weryfikacja komunikacji sieciowej (icmp ping, czy dana usługa odpowiada na danym porcie tcp/udp).

SSH agent – umożliwia wykonanie dowolnej komendy na zdalnym urządzeniu. Wynik zwrócony przez komendę zostanie wykorzystany jako metryka dla monitorowanego hosta.

SNMP – wydajny sposób odczytywania metryk z monitorowanego urządzenia. Standard w zakresie monitoringu urządzeń sieciowych.

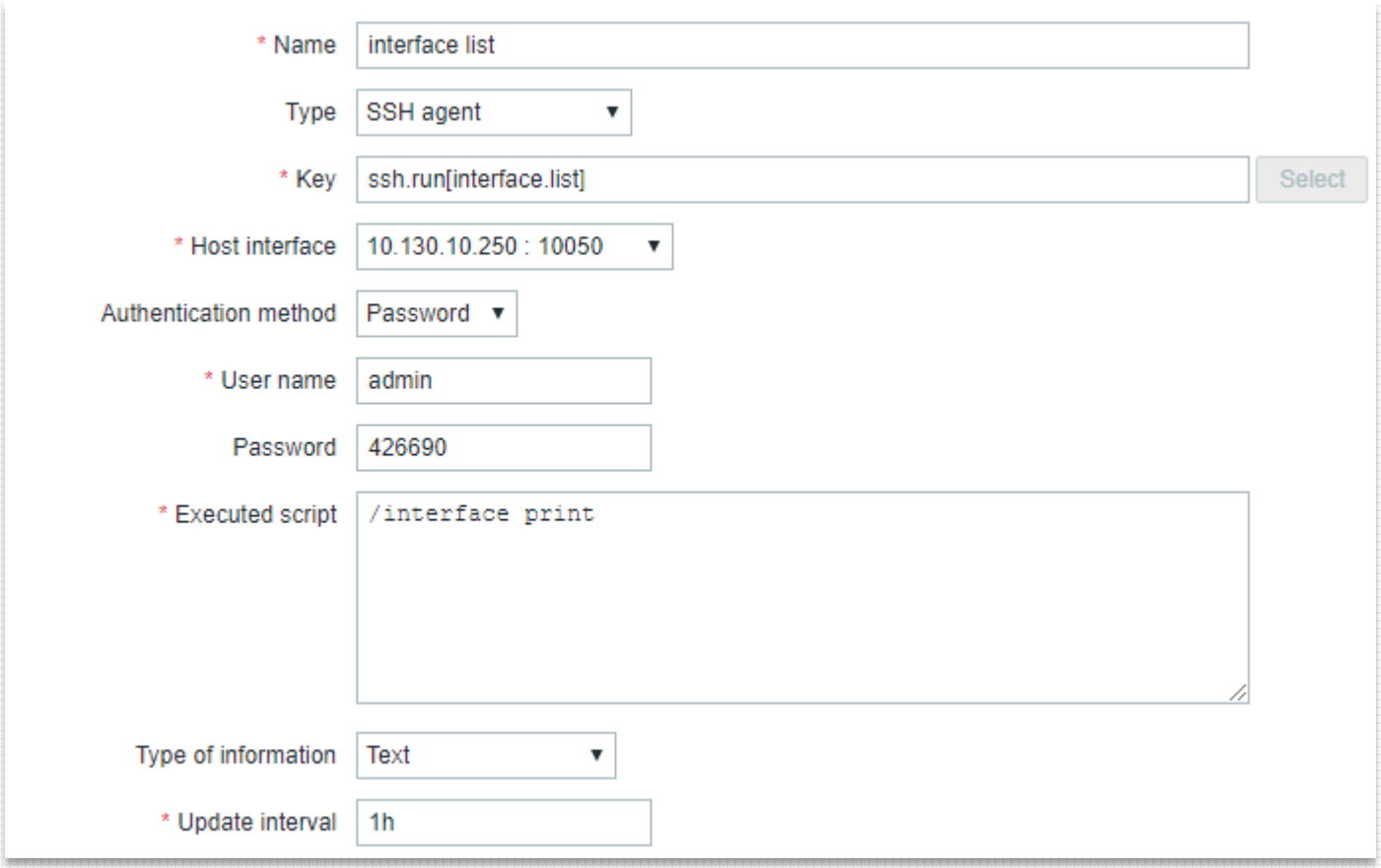
Simple checks



Weryfikacja urządzenie nasłuchuje na porcie 8291/tcp.

Tego typu prosta weryfikacja pozwala na sprawdzenie czy konfiguracja firewall'a została przeprowadzona poprawnie.

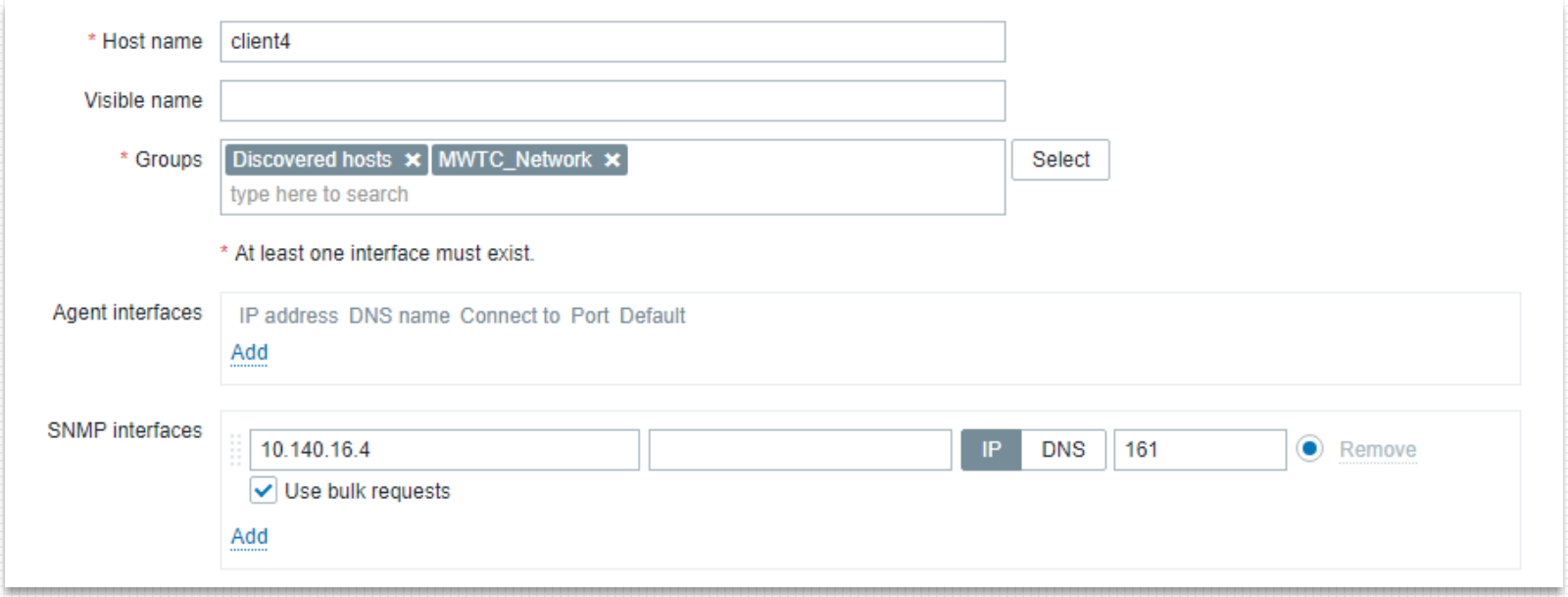
SSH agent



SSH agent może wykonać dowolne poleceniena zdalnym hoście, a jego wynik zapisze jako metrykę (item). Dostępne metody uwierzytelnienia:

- Login + hasło
- Klucze RSA

SNMP



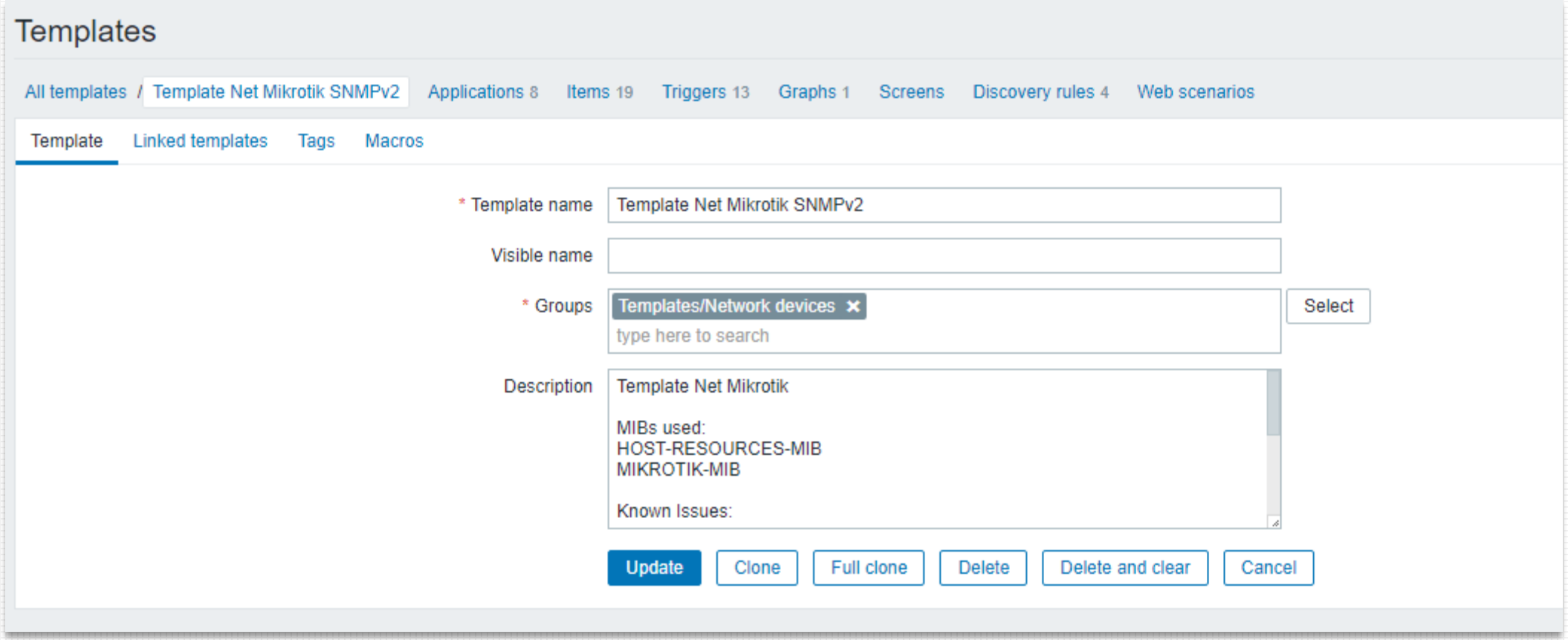
Dostępne wersje SNMP:

- SNMP v1
- SNMP 2c
- SNMP v3

Wersja 2c cechuje się słabym poziomem bezpieczeństwa, wersja v3 oferuje nie tylko autoryzację ale również szyfrowanie.

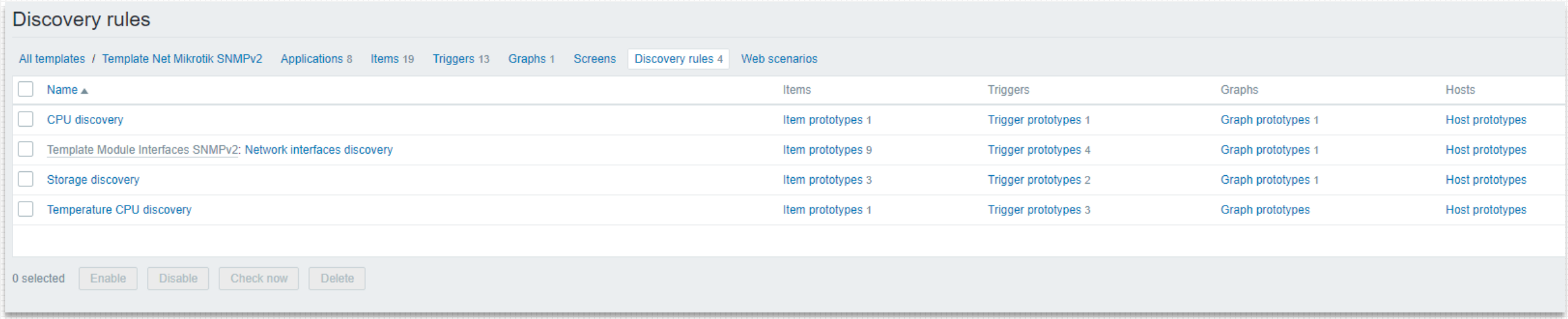
W definicji host'a należy zdefiniować SNMP interface, opcjonalnie zaznaczyć możliwość odpytania o wiele metryk w jednym zapytaniu (**bulk**).

Template Net Mikrotik SNMPv2



Oficjalny Template zawiera wiele istotnych metryk oraz trigger'ów. Można go wykorzystać jako podstawowy sposób monitorowania urządzeń MikroTik.

Template Net Mikrotik SNMPv2



Dodatkowo template zawiera 4 reguły LLD (Low Level Discovery) pozwalające na automatyczne wykrycie:

- rdzeni CPU
- interface'ów sieciowych
- dodatkowych pamięci masowych (np. USB)

Template Net Mikrotik SNMPv2

ZABBIX

Template macros | Inherited and template macros

Macro		Value	Description	
{$CPU.UTIL.CRIT}	⇒	90	description	Remove
{$MEMORY.UTIL.MAX}	⇒	90	description	Remove
{$TEMP_CRIT}	⇒	60	description	Remove
{$TEMP_CRIT:"CPU"}	⇒	75	description	Remove
{$TEMP_CRIT_LOW}	⇒	5	description	Remove
{$TEMP_WARN}	⇒	50	description	Remove
{$TEMP_WARN:"CPU"}	⇒	70	description	Remove
{$VFS.FS.PUSED.MAX.CRIT}	⇒	90	description	Remove
{$VFS.FS.PUSED.MAX.WARN}	⇒	80	description	Remove

Template można w łatwy sposób dostosować do własnych potrzeb. Dopuszczalne poziomy dla większości trigger'ów definiujemy za pomocą makr.

LLD – Low Level Discovery

ZABBIX

Umożliwia automatyczne wykrycie, na monitorowanym hoście, elementów takich jak:

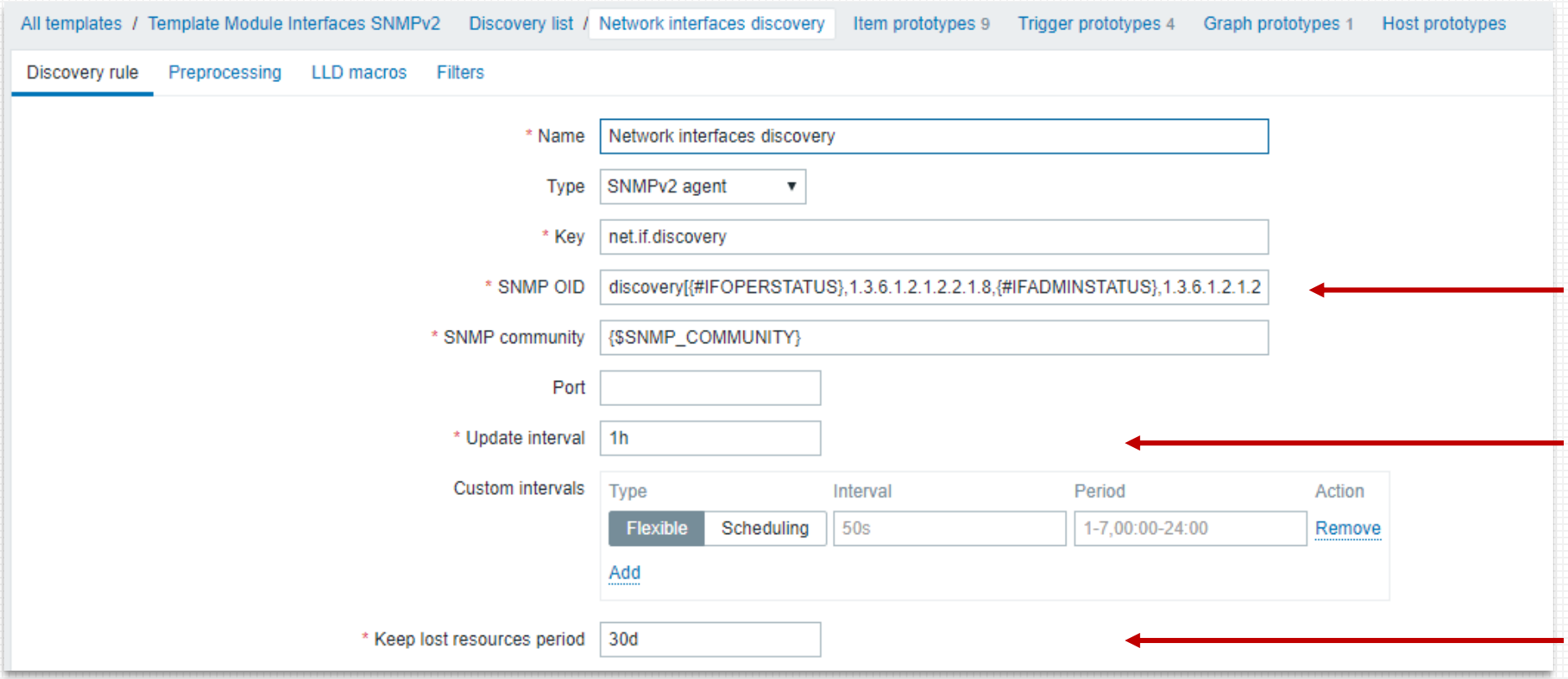
- Interface'y sieciowe
- Rdzenie procesora
- Pamięci masowe (dyski/partycje)
- Bazy danych
- Tabele w bazie danych
- Elementy aplikacji JAVA (JMX)
- ...

Dla każdego z wykrytych elementów utworzone zostaną stosowne metryki (ITEM), Triggery, Grafy

LLD – Low Level Discovery

Metryki jakie zostaną automatycznie utworzone

Triggery jakie zostaną automatycznie utworzone



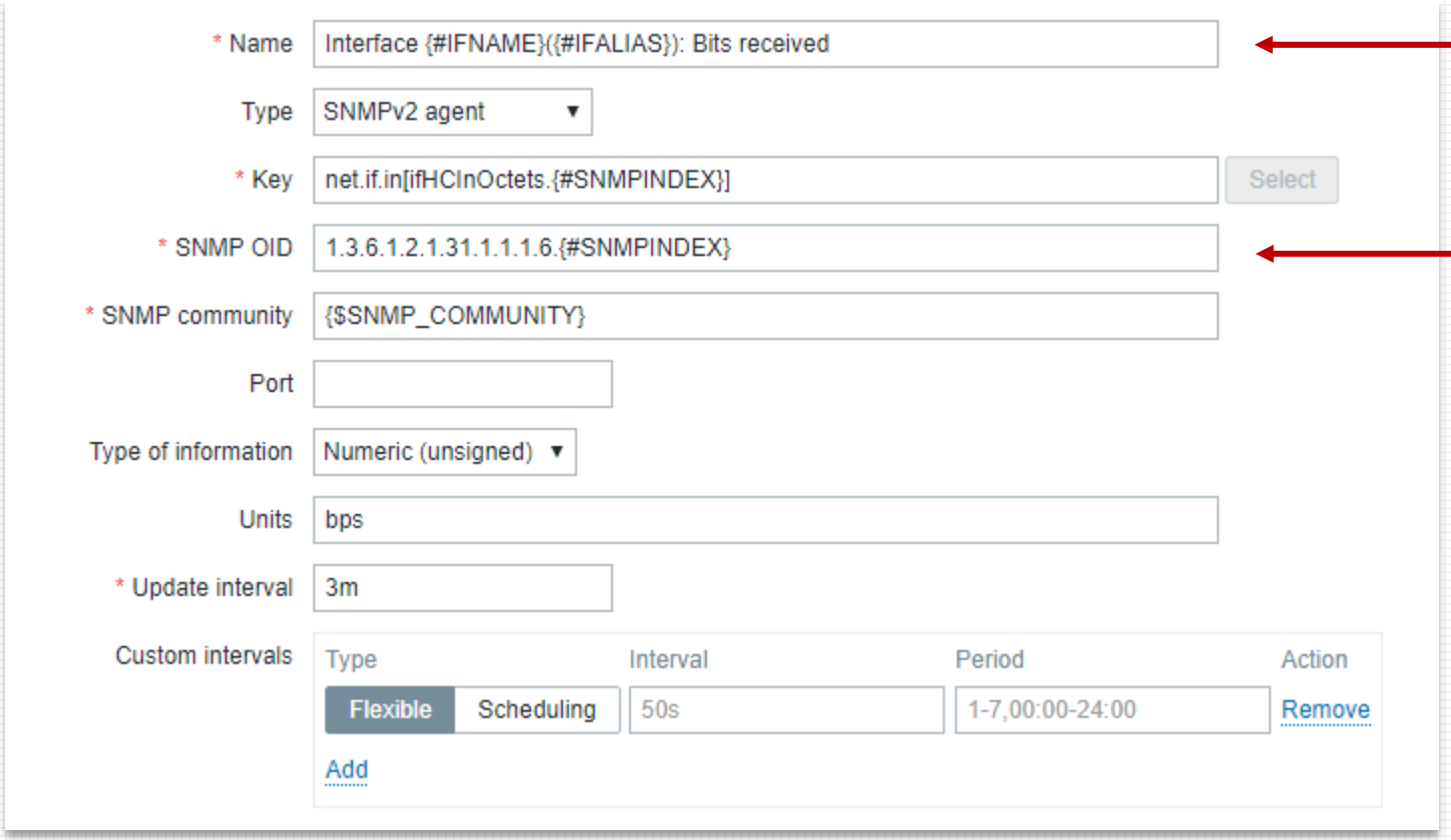
Jakie elementy zostaną wykryte

Jak często reguła powinna być uruchamiana

Po jakim czasie, element, który przestał być wykrywalny powinien zostać usunięty

LLD – Low Level Discovery

ITEM PROTOTYPE

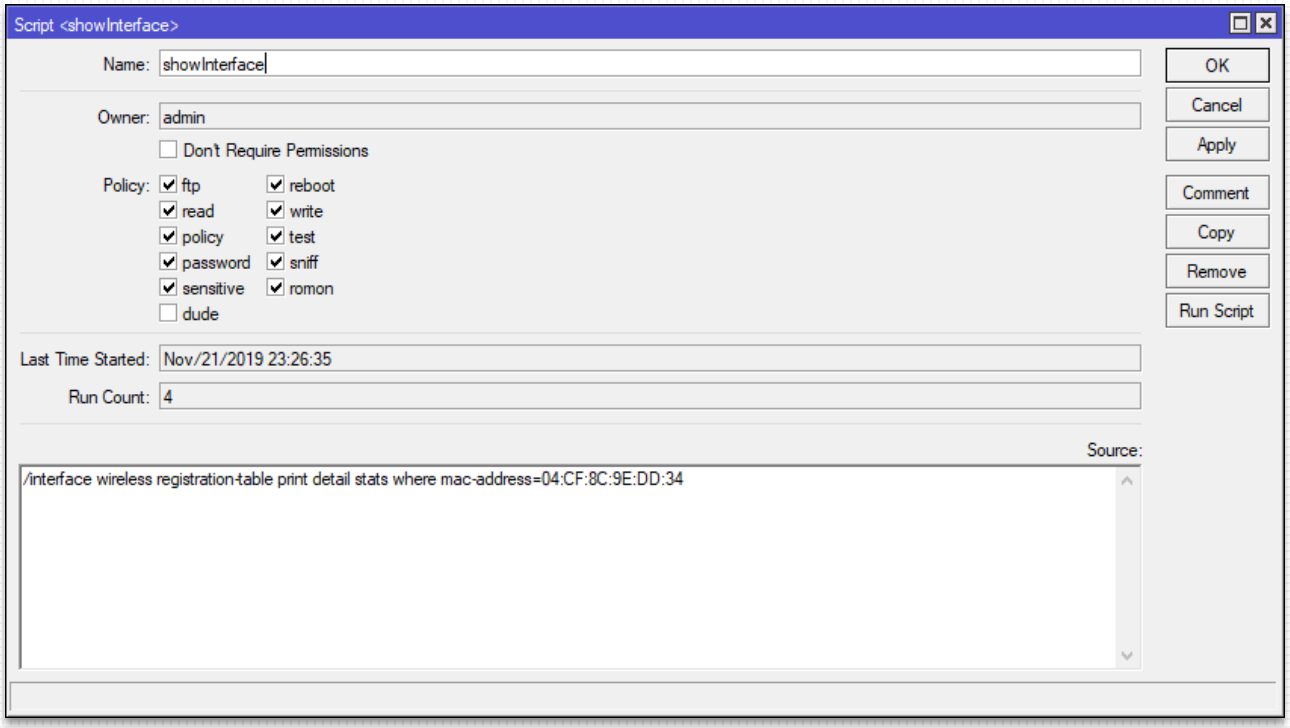


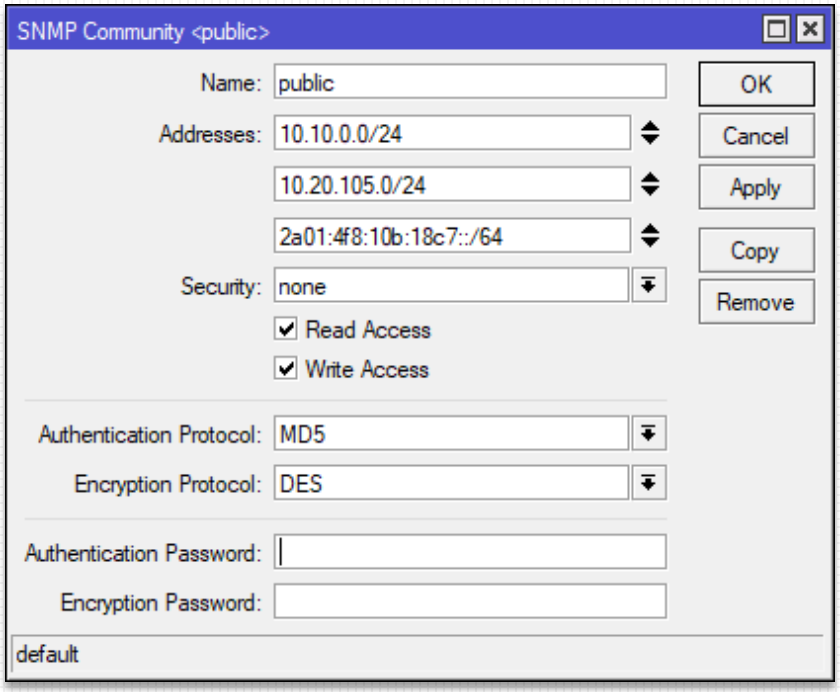
Nazwa metryki (ITEM) powstaje w wyniku rozwinięcia makr

Ostatnia część numeru OID zapisana jest jako parametr stanowiący numer wykrytego elementu

Zdalne wykonanie skryptu - SNMP

W systemie RouterOS istnieje możliwość zdalnego wykonania skryptu poprzez zapytanie SNMP.





Aby wykonać skrypt, należy nadać uprawnienia do zapisu !!!

Zdalne wykonanie skryptu - SNMP

ZABBIX

Dla utworzonego skryptu należy wyszukać OID

snmpwalk -v2c -c public 2001:470:73da:9999::1 -On ***1.3.6.1.4.1.14988.1.1.8***

.1.3.6.1.4.1.14988.1.1.8.1.1.2.1 *= STRING: "showInterface"*

.1.3.6.1.4.1.14988.1.1.8.1.1.3.1 = INTEGER: 0

← Wyszukujemy wszystkie skrypty

OID skryptu, jaki zamierzamy wykonać : *1.3.6.1.4.1.14988.1.1.**8**.1.1.2.1*

W celu wykonania skryptu należy zmodyfikować OID do postaci:

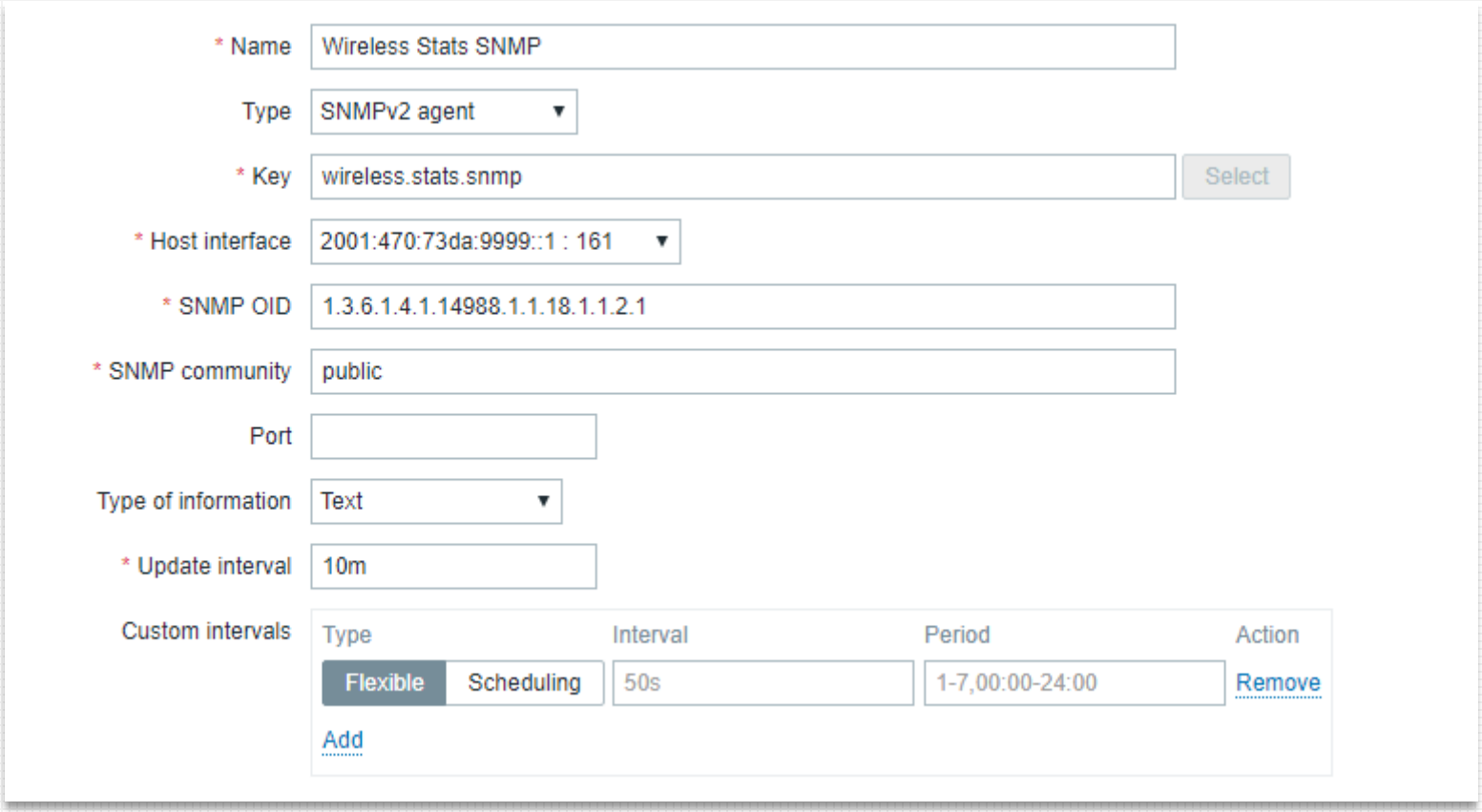
*1.3.6.1.4.1.14988.1.1.**18**.1.1.2.1*

snmpget -v2c -c public 2001:470:73da:9999::1 -On 1.3.6.1.4.1.14988.1.1.18.1.1.2.1

.1.3.6.1.4.1.14988.1.1.18.1.1.2.1 = STRING: " 0 interface=wlan1 mac-address=04:CF:8C:9E:DD:34 ap=no wds=no bridge=no
rx-rate=\"5.5Mbps\" tx-rate=\"24Mbps\" packets=770,750 bytes=61972,59740
frames=770,788 frame-bytes=63714,59350 hw-frames=1997,861
hw-frame-bytes=214289,92558 tx-frames-timed-out=0 uptime=1h53m16s
last-activity=5s240ms signal-strength=-65dBm@1Mbps signal-to-noise=42dB
signal-strength-ch0=-73dBm signal-strength-ch1=-71dBm
strength-at-rates=-65dBm@1Mbps 2h33m50s930ms,-64dBm@2Mbps 1h50m58s920ms,-
65dBm@5.5Mbps 5s280ms,-73dBm@6Mbps 1h53m16s430ms
tx-ccq=70% p-throughput=17953 distance=1 last-ip=192.168.1.13
802.1x-port-enabled=yes authentication-type=wpa2-psk encryption=aes-ccm
group-encryption=aes-ccm management-protection=no wmm-enabled=yes
tx-rate-set=\"CCK:1-11 OFDM:6-54 BW:1x HT:0-7\"

Zdalne wykonanie skryptu - SNMP

Utworzenie ITEM do zbierania danych



Dodanie wielu hostów

Zabbix API

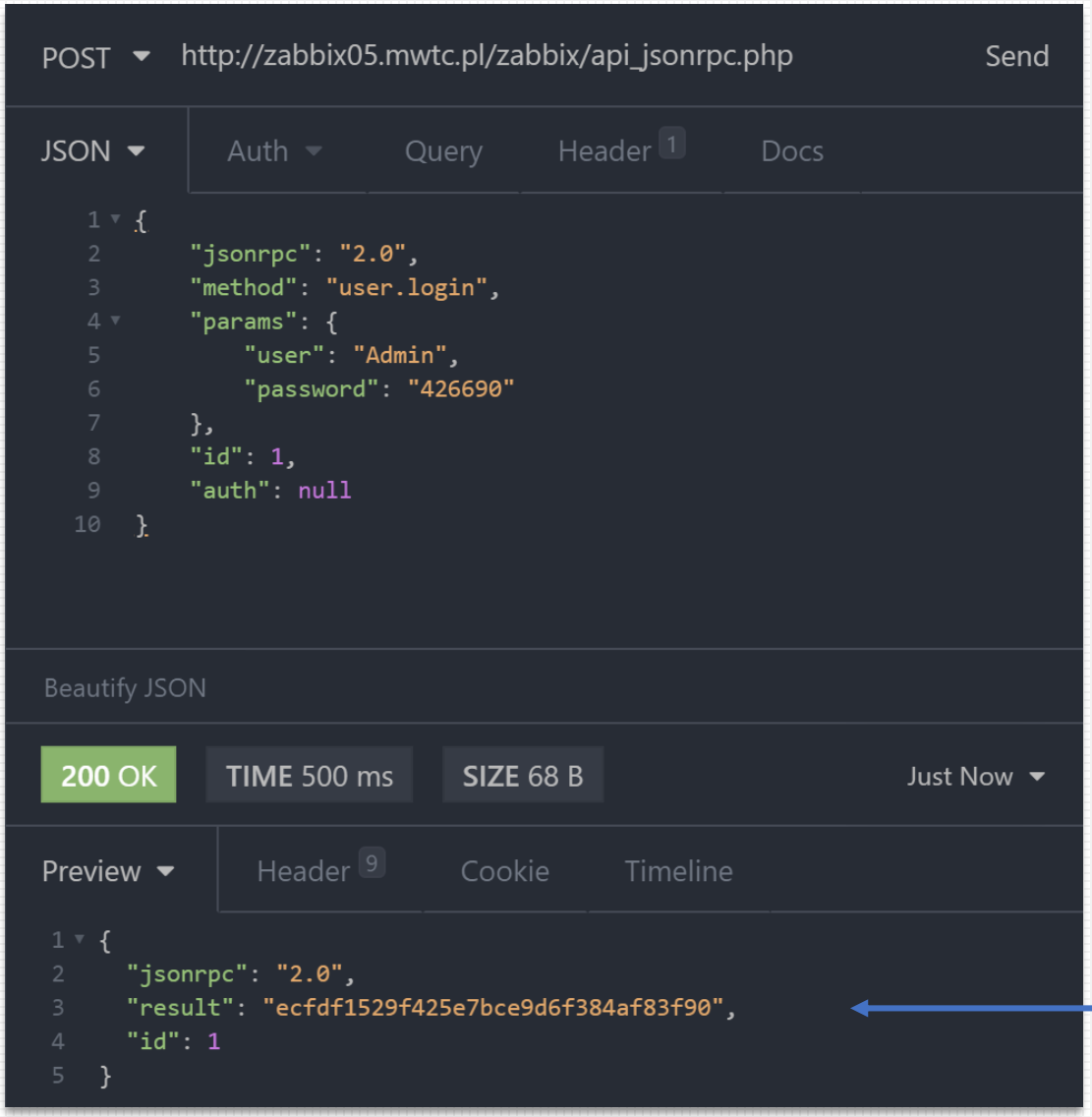
W celu integracji systemu monitoringu z zewnętrznymi aplikacjami udostępnione zostało bardzo rozbudowane API.
Dzięki API możemy:

- modyfikować istniejącą konfigurację
- dodawać /usuwać elementy
- odczytać dane historyczne

https://www.zabbix.com/documentation/4.4/manual/api

Dodanie wielu hostów

Zabbix API – uzyskanie token'a



Po poprawnym zalogowaniu uzyskujemy **token**. Każde kolejne wywołanie JSON będzie wymagało wykorzystania tego **token'a**, ponowne logowanie nie będzie wymagane.

Dodanie wielu hostów

Zabbix API – dodanie host'a

POST http://zabbix05.mwtc.pl/zabbix/api_jsonrpc.php Send

JSON Auth Query Header 1 Docs

```
{
    "jsonrpc": "2.0",
    "method": "host.create",
    "params": {
        "host": "New Mikrotik 1",
        "interfaces": [
            {
                "type": 2,
                "main": 1,
                "useip": 1,
                "ip": "192.168.3.1",
                "dns": "",
                "port": "161",
                "bulk": 1
            }
        ],
        "groups": [
            {
              "groupid": "15"
            }
        ]
    },
    "id": 2,
    "auth": "ecfdf1529f425e7bce9d6f384af83f90"
}
```

200 OK TIME 188 ms SIZE 55 B

Preview Header 9 Cookie

```
{
  "jsonrpc": "2.0",
  "result": {
    "hostids": [
      "10323"
    ]
  },
  "id": 2
}
```

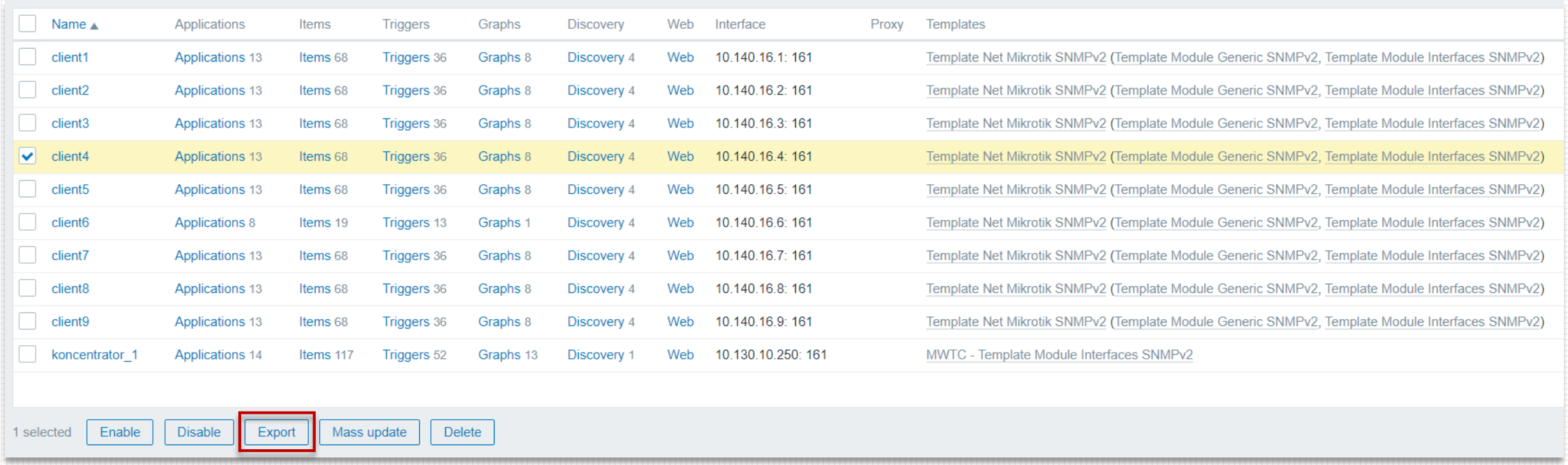
Dodanie wielu hostów

Import/Export XML

W przypadku konieczności dodania do systemu monitoringu wielu hostów, przydatna okaże się funkcja import. Należy uprzednio przygotować odpowiedni plik XML. Aby poznać strukturę tego pliku można wcześniej wykonać export przykładowego hosta.

Dodanie wielu hostów

Export XML



Name ▲	Applications	Items	Triggers	Graphs	Discovery	Web	Interface	Proxy	Templates
client1	Applications 13	Items 68	Triggers 36	Graphs 8	Discovery 4	Web	10.140.16.1: 161		Template Net Mikrotik SNMPv2 (Template Module Generic SNMPv2, Template Module Interfaces SNMPv2)
client2	Applications 13	Items 68	Triggers 36	Graphs 8	Discovery 4	Web	10.140.16.2: 161		Template Net Mikrotik SNMPv2 (Template Module Generic SNMPv2, Template Module Interfaces SNMPv2)
client3	Applications 13	Items 68	Triggers 36	Graphs 8	Discovery 4	Web	10.140.16.3: 161		Template Net Mikrotik SNMPv2 (Template Module Generic SNMPv2, Template Module Interfaces SNMPv2)
client4	Applications 13	Items 68	Triggers 36	Graphs 8	Discovery 4	Web	10.140.16.4: 161		Template Net Mikrotik SNMPv2 (Template Module Generic SNMPv2, Template Module Interfaces SNMPv2)
client5	Applications 13	Items 68	Triggers 36	Graphs 8	Discovery 4	Web	10.140.16.5: 161		Template Net Mikrotik SNMPv2 (Template Module Generic SNMPv2, Template Module Interfaces SNMPv2)
client6	Applications 8	Items 19	Triggers 13	Graphs 1	Discovery 4	Web	10.140.16.6: 161		Template Net Mikrotik SNMPv2 (Template Module Generic SNMPv2, Template Module Interfaces SNMPv2)
client7	Applications 13	Items 68	Triggers 36	Graphs 8	Discovery 4	Web	10.140.16.7: 161		Template Net Mikrotik SNMPv2 (Template Module Generic SNMPv2, Template Module Interfaces SNMPv2)
client8	Applications 13	Items 68	Triggers 36	Graphs 8	Discovery 4	Web	10.140.16.8: 161		Template Net Mikrotik SNMPv2 (Template Module Generic SNMPv2, Template Module Interfaces SNMPv2)
client9	Applications 13	Items 68	Triggers 36	Graphs 8	Discovery 4	Web	10.140.16.9: 161		Template Net Mikrotik SNMPv2 (Template Module Generic SNMPv2, Template Module Interfaces SNMPv2)
koncentrator_1	Applications 14	Items 117	Triggers 52	Graphs 13	Discovery 1	Web	10.130.10.250: 161		MWTC - Template Module Interfaces SNMPv2

Dodanie wielu hostów

Export XML

```xml
<?xml version="1.0" encoding="UTF-8"?>
<zabbix_export>
    <version>4.4</version>
    <date>2019-11-21T15:07:00Z</date>
    <groups>
        <group>
            <name>Discovered hosts</name>
        </group>
        <group>
            <name>MWTC_Network</name>
        </group>
    </groups>
    <hosts>
        <host>
            <host>client4</host>
            <name>client4</name>
            <templates>
                <template>
                    <name>Template Net Mikrotik SNMPv2</name>
                </template>
            </templates>
            <groups>
                <group>
                    <name>Discovered hosts</name>
                </group>
                <group>
                    <name>MWTC_Network</name>
                </group>
            </groups>
            <interfaces>
                <interface>
                    <type>SNMP</type>
                    <ip>10.140.16.4</ip>
                    <port>161</port>
                    <interface_ref>if1</interface_ref>
                </interface>
            </interfaces>
            <inventory_mode>DISABLED</inventory_mode>
        </host>
    </hosts>
</zabbix_export>
```

Plik zawiera listę hostów, wraz ze wszystkimi ustawieniami takimi jak:

- Grupy
- Template'y
- Interface'y

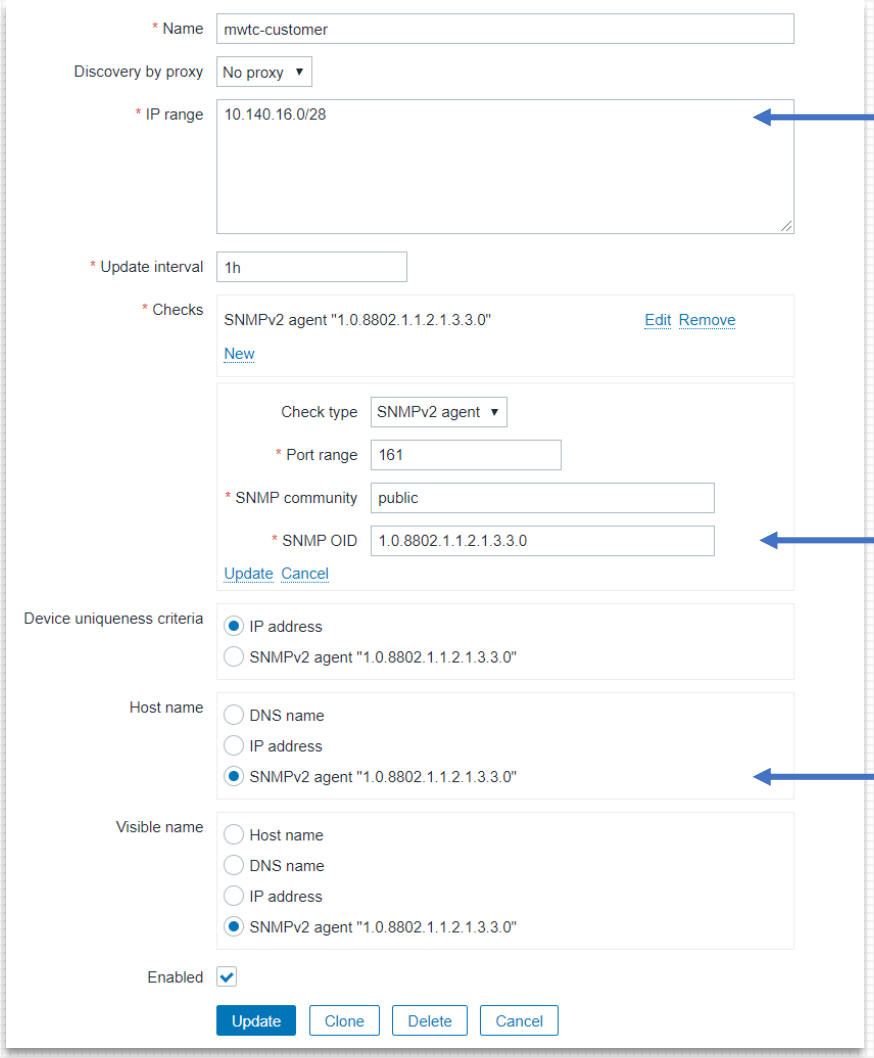
Network Discovery

ZABBIX

Umożliwia automatyczne przeskanowanie sieci w celu wykrycia nowych hostów. Wykryte hosty mogą następnie zostać dodane do monitorowania, dodane do konkretnej grupy, możliwe jest także przypisanie template'a.

Network Discovery

Utworzenie reguły Discovery (*Configuration -> Discovery*)



Zakres adresów jakie zostaną przeskanowane w celu wykrycia nowych hostów

OID przechowujący nazwę urządzenia

W jaki sposób zostanie utworzona nazwa nowo wykrytego urządzenia.

Network Discovery

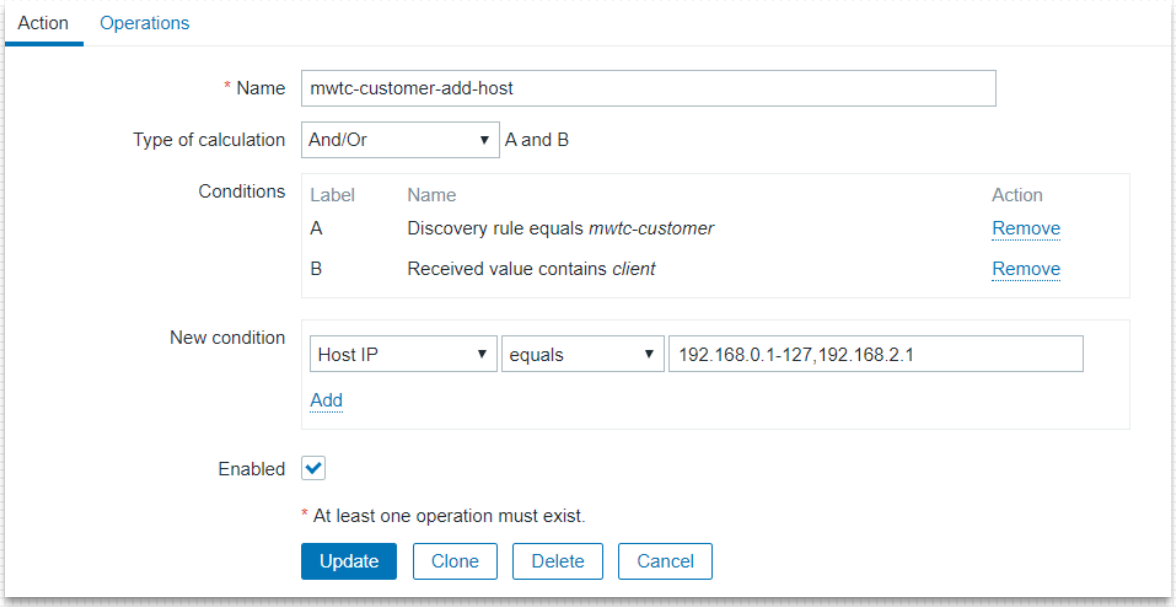
Weryfikacja wykrytych hostów (*Monitoring -> Discovery*)

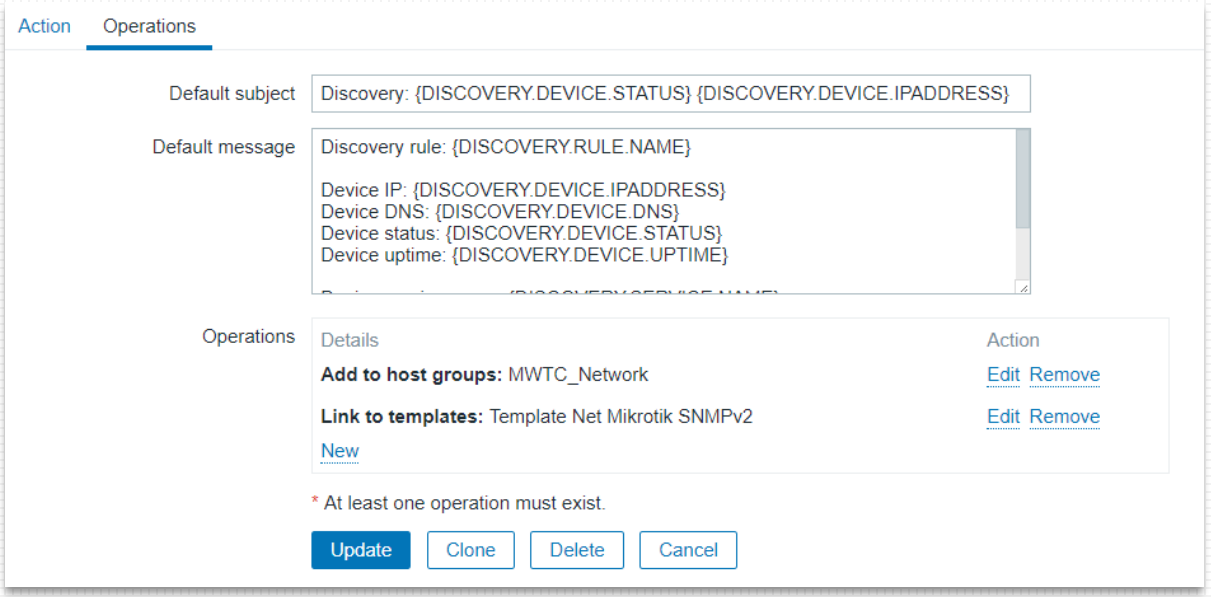
Discovered device ▲	Monitored host	Uptime/Downtime	SNMPv2 agent: 1.0.8802.1.1.2.1.3.3.0
mwtc-customer (9 devices)			
10.140.16.1	client1	15:15:56	15h 15m 56s
10.140.16.2	client2	15:11:12	15h 11m 12s
10.140.16.3	client3	15:11:12	15h 11m 12s
10.140.16.4	client4	14:48:07	14h 48m 7s
10.140.16.5	client5	14:48:07	14h 48m 7s
10.140.16.6	client6	14:51:55	14h 51m 55s
10.140.16.7	client7	15:11:04	15h 11m 4s
10.140.16.8	client8	15:11:03	15h 11m 3s
10.140.16.9	client9	15:03:27	15h 3m 27s

Lista wykrytych hostów, wraz z informacją od kiedy są one wykrywane oraz ewentualnie hosty, które przestały być wykrywalne.

Network Discovery

Akcja dodająca wykryte hosty do monitoringu (*Configuration -> Action*)





Każdy nowy host, wykryty przez regułę **mwtc-customer**, dla którego wartość "1.0.8802.1.1.2.1.3.3.0„ (device name) zawiera słowo **client**.

Zostanie dodany do grupy **MWTC_Network** oraz wykorzystany odpowiedni template **Template Net Mikrotik SNMPv2**

mwtc

Dziękuję za uwagę

https://mwtc.pl
email: info@mwtc.pl
facebook.com/mwtcPL

ZABBIX