



MikroTik Warsaw
Training Center

MikroTik i Zabbix® Jak monitorować ?

MikroTik Warsaw Training Center



Michał Filipek

Network Architect
Zabbix Trainer
MikroTik Trainer



[/in/michalfilipek](#)



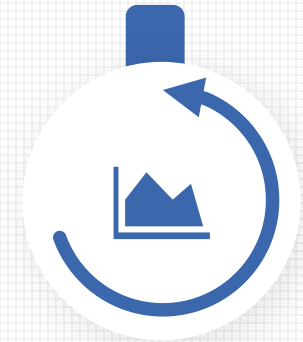
michal@mwtc.pl

**Certyfikowane
Szkolenia**
Zabbix, MikroTik



Sieci IP
Konsultacje,
Projektowanie i
Wdrożenia

**Systemy
Monitoringu**
Wdrożenia



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

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

* Name

Type

* Key

* Host interface

User name

Password

Type of information

Units

* Update interval

Custom intervals

Type	Interval	Period	Action	
<input checked="" type="checkbox"/> Flexible	<input type="text" value="Scheduling"/>	<input type="text" value="50s"/>	<input type="text" value="1-7,00:00-24:00"/>	<input type="button" value="Remove"/>

[Add](#)

* History storage period Do not keep history Storage period

* Trend storage period Do not keep trends Storage period

Show value

Weryfikacja urządzenia następuje na porcie 8291/tcp.

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

SSH agent

* Name	<input type="text" value="interface list"/>
Type	<input type="text" value="SSH agent"/>
* Key	<input type="text" value="ssh.run[interface.list]"/> <input type="button" value="Select"/>
* Host interface	<input type="text" value="10.130.10.250 : 10050"/>
Authentication method	<input type="text" value="Password"/>
* User name	<input type="text" value="admin"/>
Password	<input type="text" value="426690"/>
* Executed script	<input type="text" value="/interface print"/>
Type of information	<input type="text" value="Text"/>
* Update interval	<input type="text" value="1h"/>

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

- Login + hasło
- Klucze RSA

SNMP

* Host name

Visible name

* Groups
type here to search

* At least one interface must exist.

Agent interfaces
[Add](#)

SNMP interfaces

<input type="text" value="10.140.16.4"/>	<input type="text"/>	<input type="text" value="IP"/>	<input type="text" value="DNS"/>	<input type="text" value="161"/>	<input type="button" value="Remove"/>
--	----------------------	---------------------------------	----------------------------------	----------------------------------	---------------------------------------

Use bulk requests

[Add](#)

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

Templates

All templates / **Template Net Mikrotik SNMPv2** Applications 8 Items 19 Triggers 13 Graphs 1 Screens Discovery rules 4 Web scenarios

Template **Linked templates** Tags Macros

* Template name

Visible name

* Groups
type here to search

Description
MIBs used:
HOST-RESOURCES-MIB
MIKROTIK-MIB
Known Issues:

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

Template Net Mikrotik SNMPv2

Discovery rules

All templates / Template Net Mikrotik SNMPv2 Applications 8 Items 19 Triggers 13 Graphs 1 Screens Discovery rules 4 Web scenarios

<input type="checkbox"/> Name ▲	Items	Triggers	Graphs	Hosts
<input type="checkbox"/> CPU discovery	Item prototypes 1	Trigger prototypes 1	Graph prototypes 1	Host prototypes
<input type="checkbox"/> Template Module Interfaces SNMPv2: Network interfaces discovery	Item prototypes 9	Trigger prototypes 4	Graph prototypes 1	Host prototypes
<input type="checkbox"/> Storage discovery	Item prototypes 3	Trigger prototypes 2	Graph prototypes 1	Host prototypes
<input type="checkbox"/> Temperature CPU discovery	Item prototypes 1	Trigger prototypes 3	Graph prototypes	Host prototypes

0 selected

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

Template macros		Inherited and template macros	
Macro	Value	Description	
<input data-bbox="333 454 825 496" type="text" value="{CPU.UTIL.CRIT}"/>	⇒ <input data-bbox="868 454 1462 496" type="text" value="90"/>	<input data-bbox="1480 454 2074 496" type="text" value="description"/>	Remove
<input data-bbox="333 522 825 565" type="text" value="{MEMORY.UTIL.MAX}"/>	⇒ <input data-bbox="868 522 1462 565" type="text" value="90"/>	<input data-bbox="1480 522 2074 565" type="text" value="description"/>	Remove
<input data-bbox="333 591 825 634" type="text" value="{TEMP_CRIT}"/>	⇒ <input data-bbox="868 591 1462 634" type="text" value="60"/>	<input data-bbox="1480 591 2074 634" type="text" value="description"/>	Remove
<input cpu"}"="" data-bbox="333 659 825 702" type="text" value="{TEMP_CRIT:"/>	⇒ <input data-bbox="868 659 1462 702" type="text" value="75"/>	<input data-bbox="1480 659 2074 702" type="text" value="description"/>	Remove
<input data-bbox="333 728 825 771" type="text" value="{TEMP_CRIT_LOW}"/>	⇒ <input data-bbox="868 728 1462 771" type="text" value="5"/>	<input data-bbox="1480 728 2074 771" type="text" value="description"/>	Remove
<input data-bbox="333 796 825 839" type="text" value="{TEMP_WARN}"/>	⇒ <input data-bbox="868 796 1462 839" type="text" value="50"/>	<input data-bbox="1480 796 2074 839" type="text" value="description"/>	Remove
<input cpu"}"="" data-bbox="333 865 825 908" type="text" value="{TEMP_WARN:"/>	⇒ <input data-bbox="868 865 1462 908" type="text" value="70"/>	<input data-bbox="1480 865 2074 908" type="text" value="description"/>	Remove
<input data-bbox="333 933 825 976" type="text" value="{VFS.FS.PUSED.MAX.CRIT}"/>	⇒ <input data-bbox="868 933 1462 976" type="text" value="90"/>	<input data-bbox="1480 933 2074 976" type="text" value="description"/>	Remove
<input data-bbox="333 1002 825 1045" type="text" value="{VFS.FS.PUSED.MAX.WARN}"/>	⇒ <input data-bbox="868 1002 1462 1045" type="text" value="80"/>	<input data-bbox="1480 1002 2074 1045" type="text" value="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

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

All templates / Template Module Interfaces SNMPv2 / Discovery list / Network interfaces discovery / Item prototypes 9 / Trigger prototypes 4 / Graph prototypes 1 / Host prototypes

Discovery rule / Preprocessing / LLD macros / Filters

* Name

Type

* Key

* SNMP OID

* SNMP community

Port

* Update interval

Custom intervals

Type	Interval	Period	Action
<input checked="" type="checkbox"/> Flexible <input type="checkbox"/> Scheduling	<input type="text" value="50s"/>	<input type="text" value="1-7,00:00-24:00"/>	Remove

[Add](#)

* Keep lost resources period

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

* Name

Type

* Key

* SNMP OID

* SNMP community

Port

Type of information

Units

* Update interval

Custom intervals

Type	Interval	Period	Action
<input type="checkbox"/> Flexible <input checked="" type="checkbox"/> Scheduling	<input type="text" value="50s"/>	<input type="text" value="1-7,00:00-24:00"/>	Remove
Add			

Nazwa metryki (ITEM)
powstaje w wyniku
rozwiniecia makr

Ostatnia czesc numeru OID
zapisana jest jako parametr
stanowiacy numer wykrytego
elementu

Zdalne wykonanie skryptu - SNMP

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

Script <showInterface>

Name:

Owner:

Don't Require Permissions

Policy:

- ftp
- read
- policy
- password
- sensitive
- dude
- reboot
- write
- test
- sniff
- romon

Last Time Started:

Run Count:

Source:

```
/interface wireless registration-table print detail stats where mac-address=04:CF:8C:9E:DD:34
```

Buttons: OK, Cancel, Apply, Comment, Copy, Remove, Run Script

SNMP Community <public>

Name:

Addresses:

-
-
-

Security:

Read Access

Write Access

Authentication Protocol:

Encryption Protocol:

Authentication Password:

Encryption Password:

default

Buttons: OK, Cancel, Apply, Copy, Remove

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

Zdalne wykonanie skryptu - SNMP

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

* Name

Type

* Key

* Host interface

* SNMP OID

* SNMP community

Port

Type of information

* Update interval

Custom intervals		Type	Interval	Period	Action
<input checked="" type="checkbox"/>	Flexible	Scheduling	<input type="text" value="50s"/>	<input type="text" value="1-7,00:00-24:00"/>	Remove
Add					

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

Dodanie wielu hostów

Zabbix API – uzyskanie token'a

The screenshot shows a REST client interface with the following details:

- Method: POST
- URL: http://zabbix05.mwtc.pl/zabbix/api_jsonrpc.php
- Request Body (JSON):

```
1 {
2   "jsonrpc": "2.0",
3   "method": "user.login",
4   "params": {
5     "user": "Admin",
6     "password": "426690"
7   },
8   "id": 1,
9   "auth": null
10 }
```
- Status: 200 OK
- Response Time: 500 ms
- Response Size: 68 B
- Response Body (JSON):

```
1 {
2   "jsonrpc": "2.0",
3   "result": "ecfdf1529f425e7bce9d6f384af83f90",
4   "id": 1
5 }
```

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 200 OK TIME 188 ms SIZE 55 B
JSON Auth Query Header 1 Docs Preview Header 9 Cookie
1 {
2   "jsonrpc": "2.0",
3   "method": "host.create",
4   "params": {
5     "host": "New Mikrotik 1",
6     "interfaces": [
7       {
8         "type": 2,
9         "main": 1,
10        "useip": 1,
11        "ip": "192.168.3.1",
12        "dns": "",
13        "port": "161",
14        "bulk": 1
15      }
16    ],
17    "groups": [
18      {
19        "groupid": "15"
20      }
21    ]
22  },
23  "id": 2,
24  "auth": "ecfdf1529f425e7bce9d6f384af83f90"
25 }
```

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

<input type="checkbox"/>	Name ▲	Applications	Items	Triggers	Graphs	Discovery	Web	Interface	Proxy	Templates
<input type="checkbox"/>	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)
<input type="checkbox"/>	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)
<input type="checkbox"/>	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)
<input checked="" type="checkbox"/>	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)
<input type="checkbox"/>	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)
<input type="checkbox"/>	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)
<input type="checkbox"/>	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)
<input type="checkbox"/>	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)
<input type="checkbox"/>	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)
<input type="checkbox"/>	koncentrator_1	Applications 14	Items 117	Triggers 52	Graphs 13	Discovery 1	Web	10.130.10.250: 161		MWTC - Template Module Interfaces SNMPv2

1 selected

Dodanie wielu hostów

Export XML

```
1 <?xml version="1.0" encoding="UTF-8"?>
2 <zabbix_export>
3   <version>4.4</version>
4   <date>2019-11-21T15:07:00Z</date>
5   <groups>
6     <group>
7       <name>Discovered hosts</name>
8     </group>
9     <group>
10      <name>MWTC_Network</name>
11    </group>
12  </groups>
13  <hosts>
14    <host>
15      <host>client4</host>
16      <name>client4</name>
17      <templates>
18        <template>
19          <name>Template Net Mikrotik SNMPv2</name>
20        </template>
21      </templates>
22      <groups>
23        <group>
24          <name>Discovered hosts</name>
25        </group>
26        <group>
27          <name>MWTC_Network</name>
28        </group>
29      </groups>
30      <interfaces>
31        <interface>
32          <type>SNMP</type>
33          <ip>10.140.16.4</ip>
34          <port>161</port>
35          <interface_ref>if1</interface_ref>
36        </interface>
37      </interfaces>
38      <inventory_mode>DISABLED</inventory_mode>
39    </host>
40  </hosts>
41 </zabbix_export>
```

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

- Grupy
- Template'y
- Interface'y

Network Discovery

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*)

* Name

Discovery by proxy

* IP range

* Update interval

* Checks

SNMPv2 agent "1.0.8802.1.1.2.1.3.3.0" [Edit](#) [Remove](#)

[New](#)

Check type

* Port range

* SNMP community

* SNMP OID

[Update](#) [Cancel](#)

Device uniqueness criteria

IP address

SNMPv2 agent "1.0.8802.1.1.2.1.3.3.0"

Host name

DNS name

IP address

SNMPv2 agent "1.0.8802.1.1.2.1.3.3.0"

Visible name

Host name

DNS name

IP address

SNMPv2 agent "1.0.8802.1.1.2.1.3.3.0"

Enabled

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: 1.0.8602.1.1.2.1.3.3.0
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*)

Action Operations

* Name

Type of calculation A and B

Conditions	Label	Name	Action
	A	Discovery rule equals <i>mwtc-customer</i>	Remove
	B	Received value contains <i>client</i>	Remove

New condition

[Add](#)

Enabled

* At least one operation must exist.

Action Operations

Default subject

Default message

Operations

Details	Action
Add to host groups: MWTC_Network	Edit Remove
Link to templates: Template Net Mikrotik SNMPv2	Edit Remove
New	

* At least one operation must exist.

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**



Dziękuję za uwagę

<https://mwtc.pl>

[email: info@mwtc.pl](mailto:info@mwtc.pl)

facebook.com/mwtcPL



ZABBIX