CZWARTY POLSKI ZABBIX MEETUP ONLINE '22

Mateusz Dampc

Starszy administrator ds. monitoringu infrastruktury IT

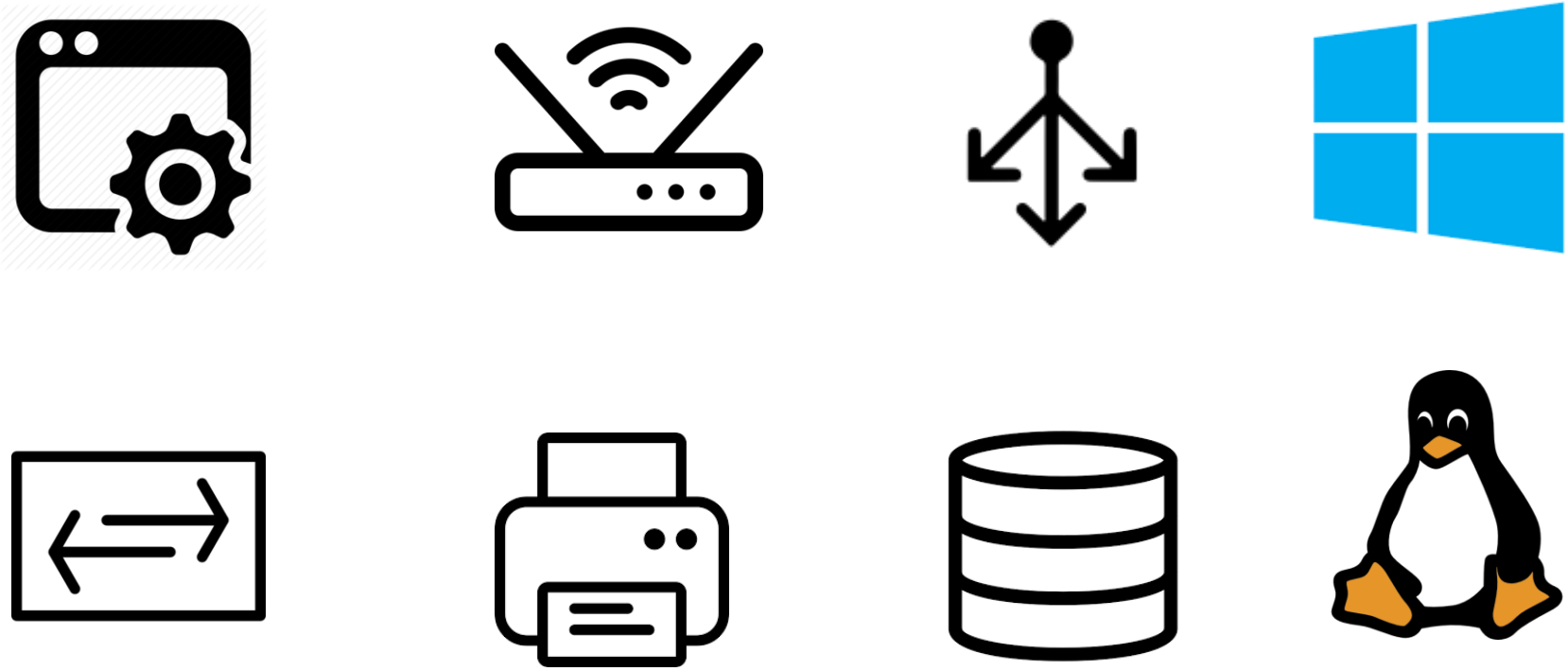
APL!TT

HUMAN FACE OF IT

Co nieco o SNMP Trapach

SNMP

Single Network Management Protocol



APL!TT

ZABBIX PREMIUM PARTNER

HUMAN FACE OF IT

Wersje SNMP

SNMPv1

- Najstarsza wersja protokołu
- Autoryzacja bazująca na podaniu poprawnej wartości community

SNMPv2

- Możliwość uruchomienia żądań zbiorowych

.1.3.6.1.2.1.1.5.0

sysName

SNMPv3

- Sposób szyfrowania protokołem MD5 lub SHA
- Sposób autoryzacji protokołem DES lub AES
- Użytkownik RO/RW

Schemat drzewa

Superior references

- 1.3.6.1.2.1.1.5 - sysName
- 1.3.6.1.2.1.1 - SNMP MIB-2 System
- 1.3.6.1.2.1 - SNMP MIB-2
- 1.3.6.1.2 - IETF Management
- 1.3.6.1 - OID assignments from 1.3.6.1 - Internet
- 1.3.6 - US Department of Defense
- 1.3 - ISO Identified Organization
- 1 - ISO assigned OIDs

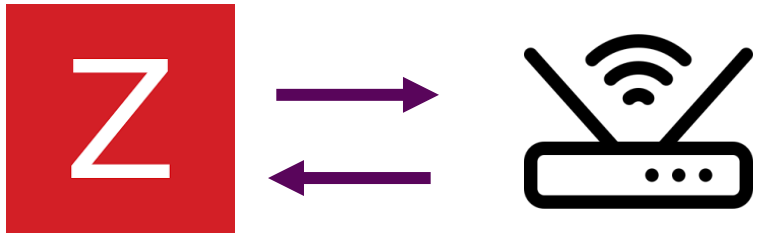
Źródło: https://www.alvestrand.no/objectid/1.3.6.1.2.1.1.5.0.html

APL!TT

ZABBIX PREMIUM PARTNER

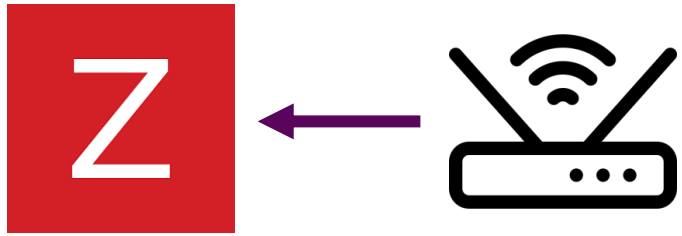
SNMP trap

- **Monitoring SNMP**



Port: 161 TCP/UDP
Domyślnie: UDP

- **Monitoring SNMP trap**



Port: 162 TCP/UDP
Domyślnie: UDP

HUMAN FACE OF IT

APL!TT

ZABBIX PREMIUM PARTNER

Monitorowanie Zabbixem trapów SNMP

- Wymagania (po stronie serwera Zabbix):
  - Zainstalowana biblioteka net-snmp
  - Zainstalowana i uruchomiona usługa snmptrapd
  - Odpowiednia konfiguracja snmptrapd do uruchomienia skryptu zapisującego trap do pliku:
    - perl: (https://github.com/prelegalwonder/zabbix/blob/master/misc/snmptrap/zabbix_trap_receiver.pl)
    - python: https://github.com/OpensourceICTSolutions/zabbix-snmp-trap-parser/blob/master/snmptrap-parser.py
    - bash: https://github.com/OpensourceICTSolutions/zabbix-snmp-trap-parser/blob/master/snmpparser.sh
  - Konfiguracja serwera Zabbix:
    - StartSNMPTrapper=1
    - SNMPTrapperFile=(plik z zbieranymi trapami podany w wybranym skrypcie)

HUMAN FACE OF IT

APL!TT

ZABBIX PREMIUM PARTNER

Przykładowy trap dla skryptu pythonowego

```
06:37:10 2022/02/10 <UNKNOWN>
UDP: [10.11.22.33]:49969->[10.10.10.10]:162
iso.3.6.1.2.1.1.3.0 50:14:26:15.75
iso.3.6.1.6.3.1.1.4.1.0 iso.3.6.1.6.3.1.1.5.3
iso.3.6.1.2.1.2.2.1.1.107 107
iso.3.6.1.2.1.2.2.1.2.107 „Serial1/0/1"
iso.3.6.1.2.1.2.2.1.3.107 6
iso.3.6.1.4.1.9.2.2.1.1.20.107 "down"
```

```
06:38:19 2022/02/10 <UNKNOWN>
UDP: [10.11.22.33]:49969->[10.10.10.10]:162
iso.3.6.1.2.1.1.3.0 50:14:26:16.80
iso.3.6.1.6.3.1.1.4.1.0 iso.3.6.1.6.3.1.1.5.4
iso.3.6.1.2.1.2.2.1.1.107 107
iso.3.6.1.2.1.2.2.1.2.107 „Serial1/0/1"
iso.3.6.1.2.1.2.2.1.3.107 6
iso.3.6.1.4.1.9.2.2.1.1.20.107 "up"
```

HUMAN FACE OF IT

Monitoring Zabbix

- Host:
  - Skonfigurowany interfejs typu: SNMP

- Pozycja:
  - Typ: Pułapka SNMP
  - Klucz:
    - snmptrap.fallback
    - snmptrap[<wyrażenie regularne>]
  - Typ informacji: Tekst

APL!TT

ZABBIX PREMIUM PARTNER

SNMPv3 trap - wymagania

- Odpowiednia konfiguracja interfejsu w Zabbixie:
  - Podany adres połączeniowy IP/DNS
  - Wersja: SNMPv3
  - Skonfigurowany poziom ochrony (NoAuthNoPriv, authNoPriv,authPriv)
  - Podanie prawidłowego użytkownika
  - Podanie haseł (dla zwiększenia bezpieczeństwa w secret makrach lub tajnych sejfach)
  - Protokół uwierzytelniania (przy authNoPriv lub authPriv)
  - Protokół prywatności (przy authPriv)
- Wpis w pliku konfiguracyjnym snmptrapd z id użytkownika wysyłającego trapy:
  - createUser -e "0x800000020100B76BAF2C1B21" trapUser SHA meetup1! DES meetup1!
  - Każda modyfikacja pliku konfiguracyjnego snmptrapd.conf wiąże się z restartem daemona

HUMAN FACE OF IT

APL!TT

ZABBIX
PREMIUM PARTNER

HUMAN FACE OF IT

HUMAN FACE OF IT