Zabbix and the art of SNMP traps

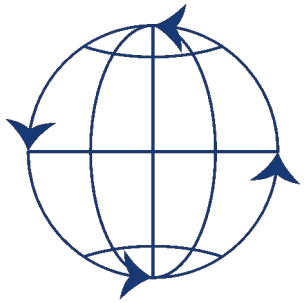
Action = Reaction

whoami

Brian van Baekel

- Zabbix consultant
- Zabbix trainer

- Netherlands
- United Kingdom
- United States



Opensource ICT Solutions

Goal of this talk

- Explain the (very) basics of SNMP polling
- Explain the (very) basics of SNMP trapping
- Explain how to capture traps
- Explain how to react on those traps

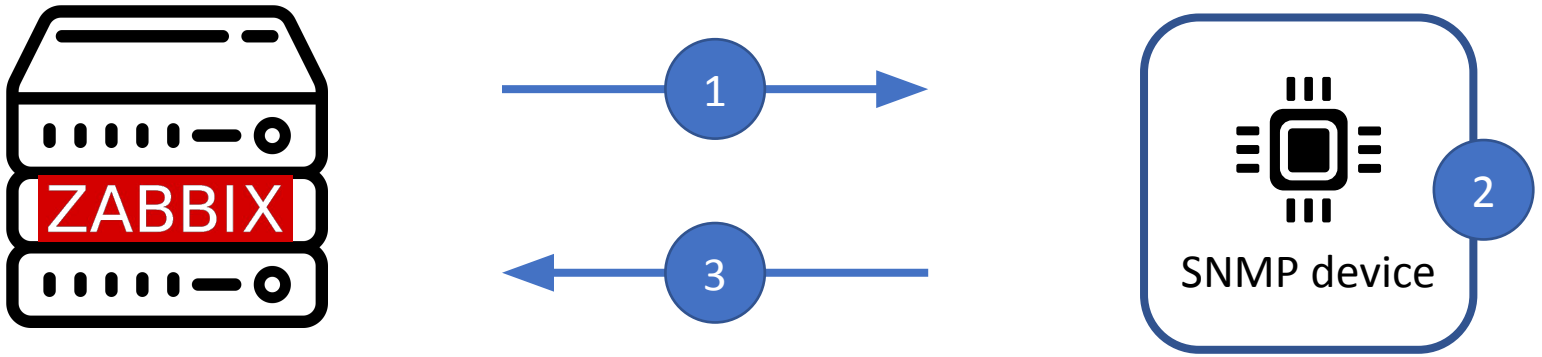
What is SNMP

Simple **N**etwork **M**anagement **P**rotocol

- Introduced early 90s
- 3 version: v1, v2c, v3
- Used to monitor:
  - Routers
  - Switches
  - Firewalls
  - Printers
  - Applications?
  - etc
- Various components:
  - Polling
  - Trapping
  - Commands/Control

Polling

- Zabbix server is requesting data from a remote device
  - Snmpget -> single request, single metric
  - GetBulk -> single request, many metrics



MIB? OID? ?????

- MIB: **M**anagement **I**nformation **B**ase
- OID: **O**bject **ID**entifier

SysUptime MIB

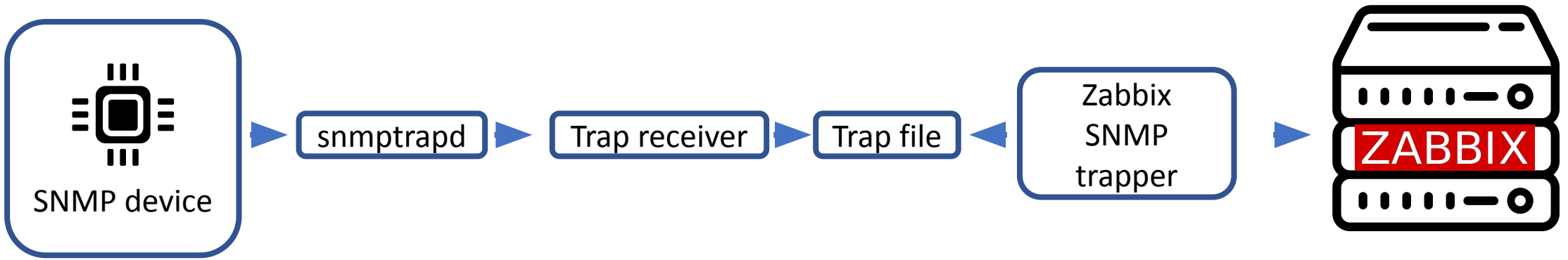
sysUpTime OBJECT-TYPE
SYNTAX TimeTicks
ACCESS read-only
STATUS mandatory
DESCRIPTION
"The time (in hundredths of a second) since the network management portion of the system was last re-initialized."
::= { system 3 }

SysUptime OID

.1.3.6.1.2.1.1.3

Trapping

- Remote device is pushing data to Zabbix
- Event driven
  - Port flapping
  - Temperature too high/low
  - Administrative login
  - etc



How it looks in Zabbix

- Polling:

Name ▲	Triggers	Key	Interval	History	Trends	Type
Network interfaces discovery: Interface lan(Lan): Bits received	Triggers 1	net.if.in[ifHCInOctets.4]	5m	7d	365d	SNMP agent
Network interfaces discovery: Interface lan(Lan): Bits sent	Triggers 1	net.if.out[ifHCOutOctets.4]	5m	7d	365d	SNMP agent
Network interfaces discovery: Interface lan(Lan): Inbound packets discarded		net.if.in.discards[ifInDiscards.4]	5m	7d	365d	SNMP agent
Network interfaces discovery: Interface lan(Lan): Inbound packets with errors	Triggers 1	net.if.in.errors[ifInErrors.4]	5m	7d	365d	SNMP agent
Network interfaces discovery: Interface lan(Lan): Interface type	Triggers 1	net.if.type[ifType.4]	4h	7d	0	SNMP agent
Network interfaces discovery: Interface lan(Lan): Operational status	Triggers 2	net.if.status[ifOperStatus.4]	5m	7d	0	SNMP agent
Network interfaces discovery: Interface lan(Lan): Outbound packets discarded		net.if.out.discards[ifOutDiscards.4]	5m	7d	365d	SNMP agent
Network interfaces discovery: Interface lan(Lan): Outbound packets with errors	Triggers 1	net.if.out.errors[ifOutErrors.4]	5m	7d	365d	SNMP agent
Network interfaces discovery: Interface lan(Lan): Speed	Triggers 2	net.if.speed[ifHighSpeed.4]	5m	7d	0d	SNMP agent

How it looks in Zabbix

- Trapping:

Capture all (fallback)

Name ▲	Triggers	Key	Interval	History	Trends	Type	S
Template Module Generic SNMP: SNMP traps (fallback)		snmptrap.fallback		2w		SNMP trap	E

Capture specific

Name ▲	Triggers	Key	Interval	History	Trends	Type	S
Network interfaces: Link status trap for dmz		snmptrap["(IF-MIB::linkDown|IF-MIB::linkUp)(.|[[:space:]])*dmz"]		90d		SNMP trap	E
Network interfaces: Link status trap for internal		snmptrap["(IF-MIB::linkDown|IF-MIB::linkUp)(.|[[:space:]])*internal"]		90d		SNMP trap	E
Network interfaces: Link status trap for modem		snmptrap["(IF-MIB::linkDown|IF-MIB::linkUp)(.|[[:space:]])*modem"]		90d		SNMP trap	E
Network interfaces: Link status trap for office		snmptrap["(IF-MIB::linkDown|IF-MIB::linkUp)(.|[[:space:]])*office"]		90d		SNMP trap	E

How it looks in Zabbix

Raw trap(tcpdump) :

09:27:01.569250 IP 192.168.1.251.snmp > 192.168.0.3.snmptrap:
Trap(81) .1.3.6.1.6.3.1.1.5 192.168.1.251 linkUp 119078322
.1.3.6.1.2.1.2.2.1.1.1=1 — ifIndex
.1.3.6.1.2.1.2.2.1.7.1=1 — ifAdminStatus (up)
.1.3.6.1.2.1.2.2.1.8.1=1 — ifOperStatus (up)

Zabbix:

Timestamp	Local time	Value

```
2021-11-06 09:27:02  2021-11-06 09:27:01  09:27:01 2021/11/06 PDU INFO:
                                            errorstatus                 0
                                            requestid                   0
                                            messageid                   0
                                            errorindex                  0
                                            receivedfrom                UDP: [192.168.1.251]:161->[192.168.0.3]:162
                                            transactionid               2
                                            version                     0
                                            community                   public
                                            notificationtype            TRAP
                                          VARBINDS:
                                            DISMAN-EVENT-MIB::sysUpTimeInstance type=67 value=Timeticks: (119078322) 13 days, 18:46:23.22
                                            SNMPv2-MIB::snmpTrapOID.0       type=6  value=OID: IF-MIB::linkUp
                                            IF-MIB::ifIndex.1               type=2  value=INTEGER: 1
                                            IF-MIB::ifAdminStatus.1         type=2  value=INTEGER: 1
                                            IF-MIB::ifOperStatus.1          type=2  value=INTEGER: 1
                                            SNMP-COMMUNITY-MIB::snmpTrapAddress.0 type=64 value=IpAddress: 192.168.1.251
                                            SNMP-COMMUNITY-MIB::snmpTrapCommunity.0 type=4  value=STRING: "public"
                                            SNMPv2-MIB::snmpTrapEnterprise.0 type=6  value=OID: SNMPv2-MIB::snmpTraps
```

Conceptual

- Poll frequency should be as low as possible. 10-15 minutes interval?
- Traps are important to get fast status updates
- Don’t rely on traps only

- Upon received trap we want to get all(or a subset) of items updated ASAP.
- Devices are typically not capable to facilitate fast polling

Conceptual

- We can get a status update with the “execute now” function in Zabbix

- We can utilize the API of Zabbix

- Assumption: Zabbix configuration is working already

Configuration

- Make sure all SNMP trap triggers are using tags:

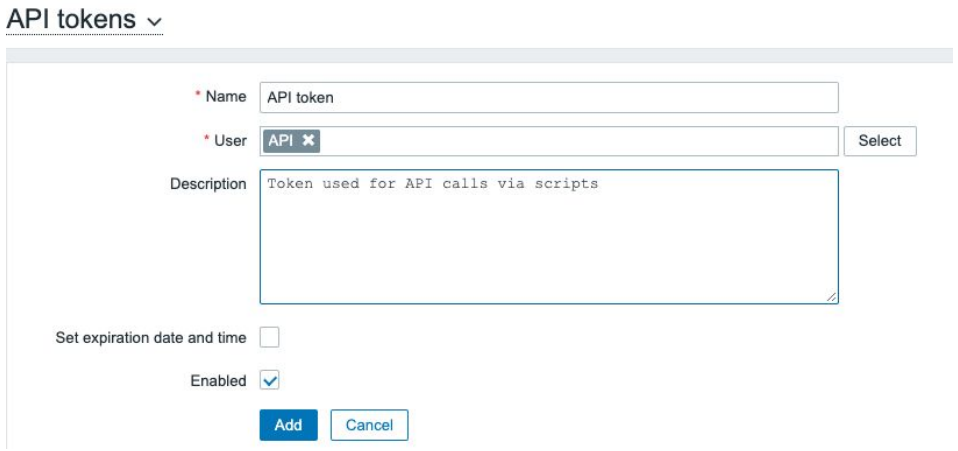
Severity	Value	Name ▲	Operational data	Expression	Status	Info	Tags
Not classified	OK	We received an SNMP trap		**nodata**(/SNMP Device/snmptrap.fallback,10s)=0	Enabled		SNMPtrap: True

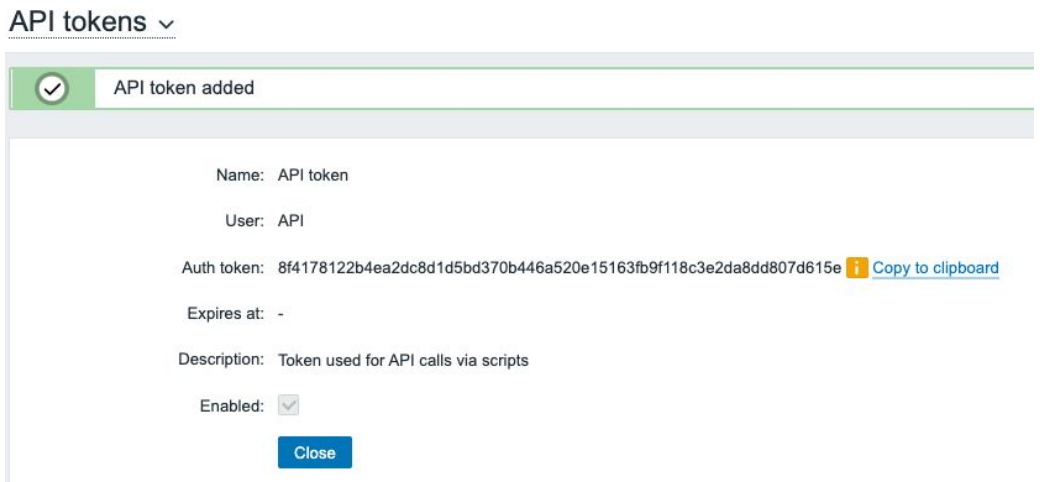
Displaying 1 of 1 found

- Severity can be anything
- Multiple tags are not a problem

Configuration

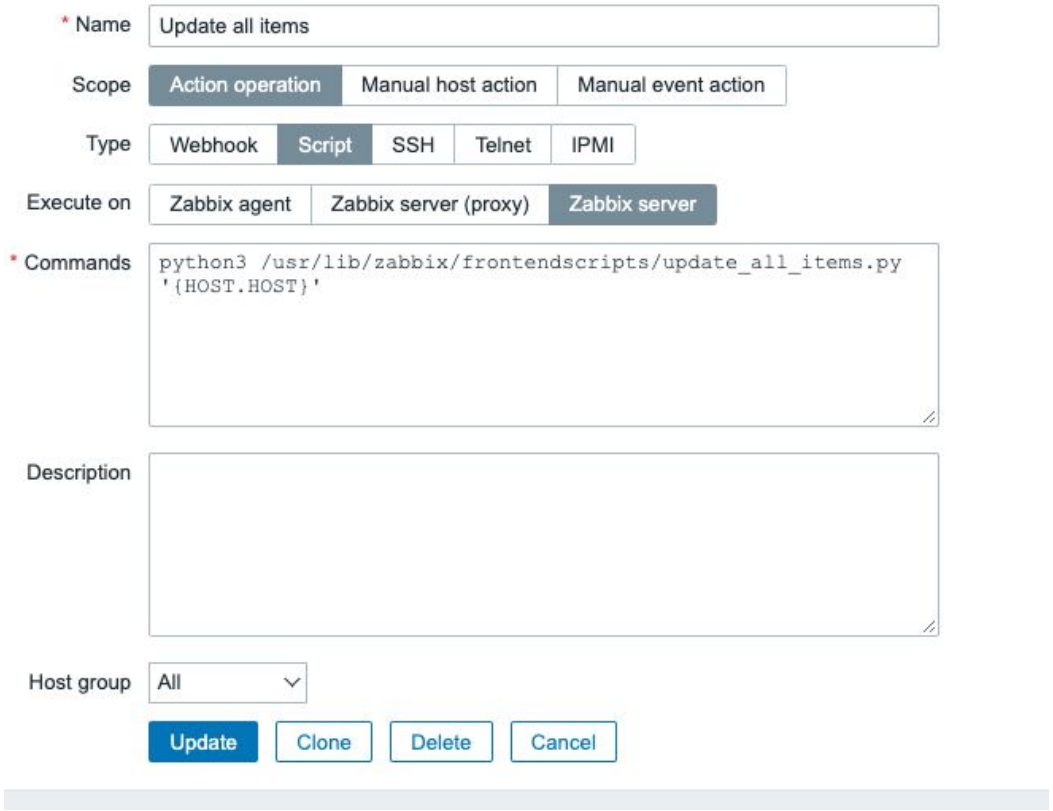
Create an API token(Administration -> General -> API tokens):





Configuration

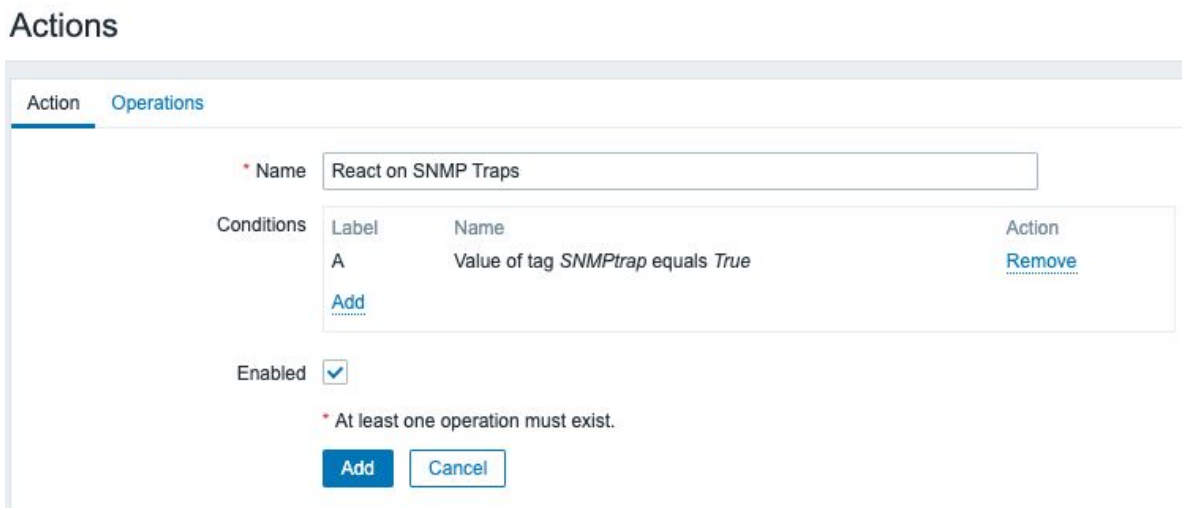
Create a new frontend script(Administration -> Scripts):



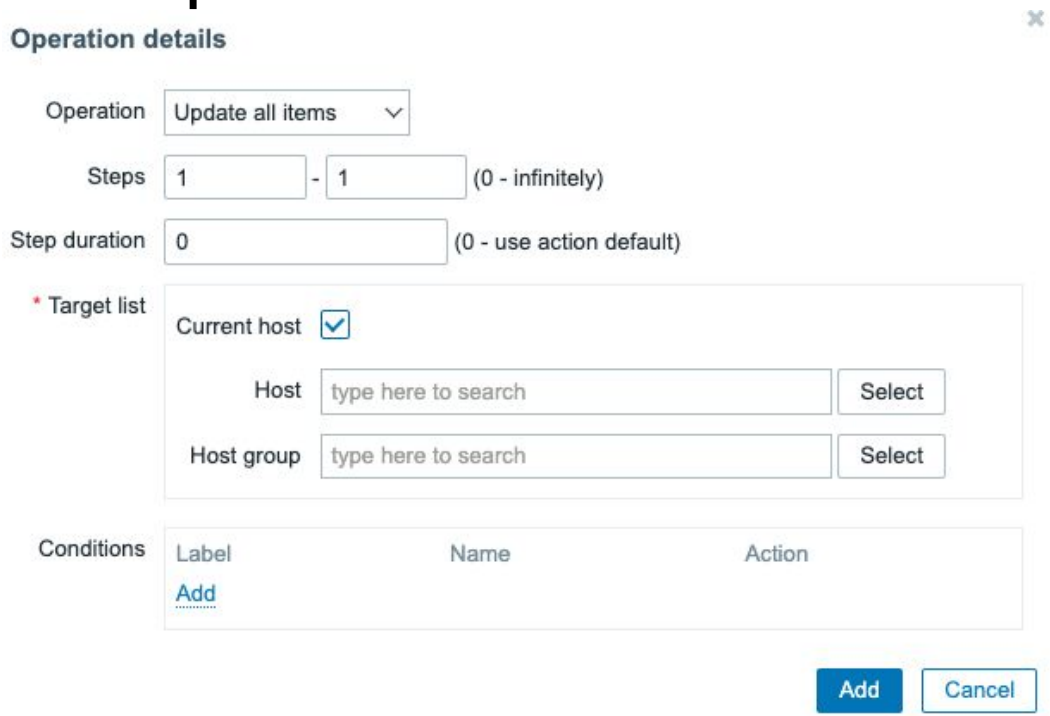
Configuration

Create an action:

Condition:



Operation:



Configuration

- Last but not least, the API script

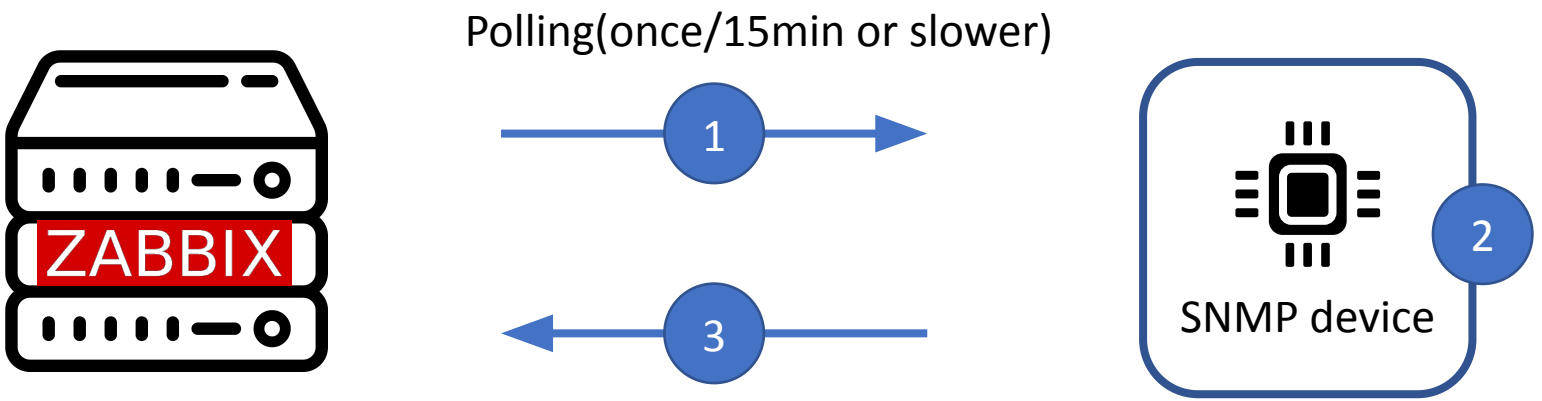
  - Download from https://github.com/OpensourceICTSolutions/zabbix-update_all_items
  - Place it in /usr/lib/Zabbix/frontendscripts/ on your Zabbix server

Prerequisites:

- Python3
- python pip
  - Requests module

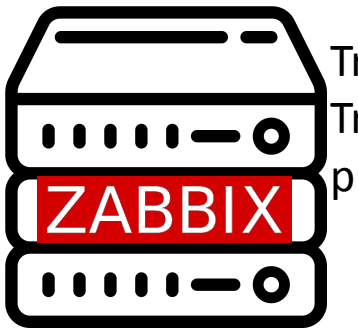
Result

Normal operations



Result

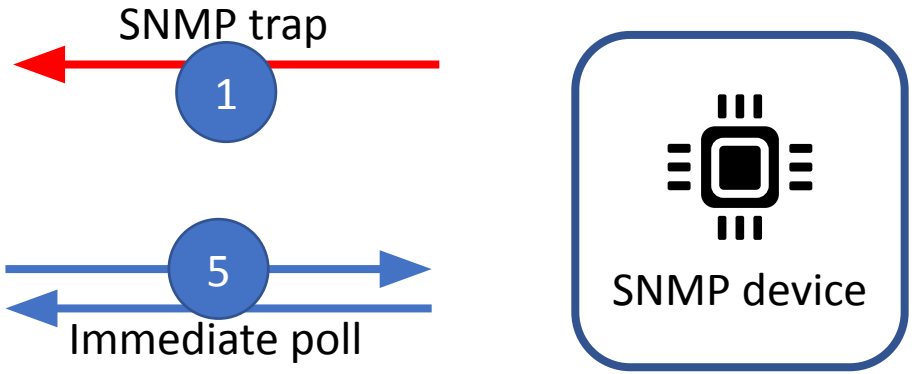
Upon trap receival



2 Trap received. Trigger goes in problem state

3 Action takes place due to problem event: Calling the Python script

4 Python script: execute check now on all items of involved host



6 Within seconds after receiving the trap, we know the exact state of the device as all items are updated

Thank you

Questions?