BUILDING TEMPLATES FOR SNMP DEVICES

ARTŪRS LONTONS
TECHNICAL SUPPORT ENGINEER
ZABBIX
MONITORING SNMP AGENTS WITH ZABBIX

- Use built in or community templates
- Create items based on vendor documentation/snmpwalk results
- Use LLD to discover SNMP entities
I wish to build custom SNMP templates, but where do I start?

✔️ Vendor documentation is your best friend! (If available)
Check for vendor provided, vendor specific MIB files!

Out of the box SNMP templates can also be used with general purpose MIBs!
BUILDING CUSTOM SNMP TEMPLATES

Okay, but how would I create a test environment for my templates?

- Misconfigured templates could cause a spike in SNMP requests on your device
- Sometimes the device is not directly accessible during the development

github.com/etingof/snmpsim
PREPARING THE PROPER TOOLS

Let's simulate an SNMP device!

First, we will need to make sure we have the proper tools:

- CentOS 8
- Zabbix 5.2
- Zabbix documentation (SNMP discovery)
- SNMPSIM software
- snmpwalk command results from our device
- Vendor documentation
- Device MIB files
Perform snmpwalk on your device

[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
...

Store the result in a separate file
INSTALLING SNMPSIM

✔️ Install python

```bash
yum install python3
```

✔️ Use pip (package installer for Python) to install snmpsim

```bash
pip3 install snmpsim
```

✔️ Snmpsim won't run under elevated user permissions

✔️ Create new user group and user accounts

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

✔️ Create a directory for snmpwalk output and MIB file storage

```bash
mkdir -p /usr/share/snmpsim/data
```
RUN SNMPSIM

✓ Run snmpsim and pass the listen IP/Port

```
snmpsimd.py --agent-udpv4-endpoint=192.168.1.126:1024
```

✓ The snmpwalk file name becomes the 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
```
TESTING SNMPSIM

Let's see if we can snmpwalk the simulated device

[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

Don't forget to specify the proper community, IP and port!
TESTING SNMPSIM FROM ZABBIX

✔️ Now let's try and create a host in Zabbix

✔️ Once again – mind the IP, Port and community! (Community = SNMPWalk file name!)
Let's create an item and test if our SNMP device

But how did I obtain the numeric OID form if the SNMPWalk output was textual?
GETTING THE NUMERIC OID FORM

Textual output

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

Let's use snmptranslate

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

No we just need to add the index – 103007 at the end of the OID

* Key: ifHCInOctets.103007

* Host interface: 192.168.1.126 : 1024

* SNMP OID: .1.3.6.1.2.1.31.1.1.1.6.103007
CREATING SNMP AGENT LLD RULE

Create an LLD rule

- We will be discovering all of the indexes on 1.3.6.1.2.1.2.1.2.2.1.2 (*IFDescr*)
- We will also discover all of the available port descriptions
CREATING SNMP AGENT LLD ITEM PROTOTYPE

☑️ Create an item prototype for incoming traffic

☑️ Discovered index {#SNMPINDEX} will be added at the end of the OID (ifHCInOctets)
**ERROR – NO SUCH INSTANCE CURRENTLY EXISTS**

- Caused by having extra indexes in `IfDescr` compared to `ifHCInOctets`
- Fixed by filtering out unnecessary Indexes by `IfDescr`:
LLD ENTITY FILTERING

To make filtering easier, try discovering additional OID's (*IFTYPE*)
ERROR – NO VALUE RECEIVED FOR MACRO

When trying to discover multiple attributes – {#IFNAME}, {#IFTYPE}, {#IFDESCR}
**ERROR – NO VALUE RECEIVED FOR MACRO**

- Zabbix tries to apply filters for all of the OID's in the discovery rule

<table>
<thead>
<tr>
<th>{#IFNAME}</th>
<th>{#IFTYPE}</th>
<th>{#IFDESCR}</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.3.6.1.2.1.31.1.1.1.1.1</td>
<td>1.3.6.1.2.1.2.2.1.3.1</td>
<td>1.3.6.1.2.1.2.2.1.2.1</td>
</tr>
<tr>
<td>1.3.6.1.2.1.31.1.1.1.1.2</td>
<td>1.3.6.1.2.1.2.2.1.3.2</td>
<td>1.3.6.1.2.1.2.2.1.2.2</td>
</tr>
<tr>
<td>1.3.6.1.2.1.31.1.1.1.1.3</td>
<td>1.3.6.1.2.1.2.2.1.3.3</td>
<td>1.3.6.1.2.1.2.2.1.2.3</td>
</tr>
</tbody>
</table>

- Index 3 is missing for {#IFTYPE} and {#IFDESCR}
- Filtering is still attempted by {#IFTYPE} or {#IFDESCR}
MODULAR TEMPLATES AND LLD RULES

- Try creating modular discovery rules or templates
- Each discovery rule is created for specific interface type
- Allows you to link/unlink templates for specific entity types to a parent template
- You can then enable/disable discovery rules on the host level
THANK YOU!

ARTūRS LONTONS
TECHNICAL SUPPORT ENGINEER
ZABBIX