ZABBIX 5.0

SNMPv3 CONFIGURATION AND TROUBLESHOOTING
THE EVOLUTION OF SNMP

COMPARING SNMP VERSIONS
- Benefits of using SNMP v2c/v3
- Which one should I use?
IN THE BEGINNING – SNMPv1

- Standardized in 1988
- Communication is established with SNMP agent on the host device
- Supports only 32 bit counters
- Plaintext Community string is the only security method

```
# snmpget -v1 -cpublic 192.168.1.103 .1.3.6.1.2.1.25.4.2.1.5.3674
# HOST-RESOURCES-MIB::hrSWRunParameters.3674 = STRING: "--color=auto Linux"
```
IMPROVING ON IT – SNMPV2

- New message format and protocol changes – performance improvements
- Devices can be bilingual – support for both snmpv1 and snmpv2
- 64 bit counter support
- Still relies on a plaintext community as the only Authentication measure

```bash
# snmpget -v2c -cpublic 192.168.1.103 1.3.6.1.2.1.31.1.1.1.6.1
# IF-MIB::ifHCInOctets.1 = Counter64: 8768072
```
FOCUSING ON ENCRYPTION—SNMPv3

- Support for message encryption
- Support for multiple contexts on a single device (select MIB according to context)
- MD5/SHA Authentication protocol support
- DES/AES Encryption of SNMP messages

```
# snmpget -v3 -l authPriv -u admin -a SHA -A "AuthPass" -x AES -X "PrivPass" 192.168.1.103 1.3.6.1.2.1.2.2.1.2.2.1.2
IF-MIB::ifDescr.1 = STRING: Adaptive Security Appliance 'v101'
interface
```
WHICH VERSION TO USE WITH ZABBIX

- SNMPv2c almost always trumps SNMPv1 – only reason to choose SNMPv1 is lack of v2c support on the device
- SNMPv3 is a lot more complex to configure
- SNMPv3 devices can cause issues if they’re not RFC compliant (Static EngineBoots time, Non-unique Engine ID)
- SNMPv3 provides immense security improvements over v1/2c
GETTING STARTED WITH SNMP IN ZABBIX
CHANGES IN ZABBIX 5.0

- Community and SNMP version configuration moved to the host level configuration
Changes in Zabbix 5.0

- Ability to reload SNMP cache, clear the SNMP properties (engine time, engine boots, engine id, credentials) for all hosts.

```
# zabbix_server -R snmp_cache_reload
# zabbix_server [7414]: command sent successfully
```
Configure the SNMPv3 interface according to your device configuration:
CREATE **SNMP ITEMS MANUALLY OR VIA LLD**

- Create items pointing at the proper OID files
- If required, use preprocessing to transform data
Discover indexes by pointing your discovery rule at a specific OID

Use filters to Filter out unnecessary data

Specify the OIDs on item prototypes

These OIDs will be populated by discovered indexes
ZABBIX AND SNMPV3 TRAPS

✓ You need to create an SNMPv3 user in your snmpd.conf
✓ The user needs to be linked to the EngineID of the device sending the traps

createUser -e 0x80000000001020304 traptest SHA AuthPass
AES PrivPass
If you want to receive v3 traps (or informs) sent with `noAuthNoPriv`, you'll need to add `noauth` to the `authUser` line:

```
authUser log,execute,net SNMPUser noauth
```

- Log - log the details of the notification
- Execute - pass the details of the trap to a specified handler program
- forward the trap to another notification receiver.
TESTING SNMPV3 TRAPS

You can use the following command to test the SNMPv3 traps locally:

```bash
#snmptrap -v 3 -n «ContextName" -a SHA -A AuthPass -x AES
-X PrivPass -l authPriv -u SNMPUser -e
0x80000634b210008894719abe08 127.0.0.1 0 linkUp.0
```
COMMON ISSUES AND MISCONFIGURATION

SNMPv3 CONFIGURATION AND TROUBLESHOOTING
- Testing your SNMPv3 devices
- Configuring an SNMPv3 interface in Zabbix frontend
- Detecting any potential SNMPv3 issues
DUPLICATE SNMP ENGINE ID

The SNMPv3 device needs to return the following values in accordance with RFC specification:

- **msgAuthoritativeEngineID**: Unique device Engine ID
- **msgAuthoritativeEngineBoots**: Count of Device reboots
- **msgAuthoritativeEngineTime**: Device Uptime
DUPLICATE SNMP ENGINE ID

Devices with authNoPriv or AuthPriv security respond to a get request only if all three of these parameters are correct.

Otherwise, you might see the following entries in your Zabbix

```
# SNMP agent item «TrafficIfIn" on host "SNMPHOST" failed: first network error, wait for 15 seconds
# SNMP agent item «TrafficIfOut" on host "SNMPHOST" failed: another network error, wait for 15 seconds
# temporarily disabling SNMP agent checks on host "SNMPHOST": host unavailable
```
**DUPLICATE SNMP ENGINE ID - DETECTION**

- Multiple approaches to help detect this
- Perform an snmpget for SNMP-FRAMEWORK-MIB::snmpEngineID.0
- Use a script to get the Engine ID’s en masse

```bash
for seq in {1..254};do echo 192.168.1.$seq >> /tmp/engineid.out && snmpget -v 3 -l authPriv -u user -x AES -X 'PRIVPASS' -a SHA -A 'AUTHPASS!' 192.168.1.$seq <OID> >> /tmp/engineid.out ;done
```
DUPLICATE SNMP ENGINE ID - DETECTION

- Try to inspect the packet capture from the Zabbix server or proxy to detect the duplicate engine IDs.

```
Destination Port: 161
Length: 154
Checksum: 0x2cab [unverified]
[Checksum Status: Unverified]
[Stream index: 4554]
[Timestamps]
Simple Network Management Protocol
  msgVersion: snmpv3 (3)
  msgGlobalData
  msgAuthoritativeEngineID: 80001f8880812dfa5b44a4c85b
  msgAuthoritativeEngineBoots: 1
  msgAuthoritativeEngineTime: 623326
```
SNMPv3 INTERFACE MISCONFIGURATION

- Misconfigured security

```
# error reason for "SNMPv3
device:system.contact[sysContact.0]" changed: Cannot connect to "192.168.1.103:161": Unknown user name.
```
Misconfigured Authentication password

# error reason for "SNMPv3 device:system.uptime[sysUpTime.0]"
changed: Cannot connect to "127.0.0.1:161": Authentication failure (incorrect password, community or key).
Misconfigured Privacy password

# SNMP agent item "system.uptime[sysUpTime.0]" on host "SNMPv3 device" failed: first network error, wait for 15 seconds
# SNMP agent item "system.uptime[sysUpTime.0]" on host "SNMPv3 device" failed: another network error, wait for 15 seconds
# SNMP agent item "system.uptime[sysUpTime.0]" on host "SNMPv3 device" failed: another network error, wait for 15 seconds
# temporarily disabling SNMP agent checks on host "SNMPv3 device": host unavailable
SNMP CACHE RELOAD

SNMP cache reload is required for any changes in Authentication protocol, Authentication passphrase, Privacy protocol or Privacy passphrase to take effect.

SNMP cache can be reloaded either by executing the SNMP cache reload command (recommended, added in version 5.0) or restarting the server/proxy.

# zabbix_server -R snmp_cache_reload
# zabbix_server [10738]: command sent successfully
SNMPV3 NOTES AND RECOMMENDATIONS

- If you’re experiencing issues with SNMP checks on a host, try unchecking «Use bulk requests». Some devices can have issues with processing bulk requests.

```
# item "system.uptime[sysUpTime.0]" became not supported: SNMP error: (genError) A general failure occurred
```

- Perform test snmpget or snmptrap requests from the CLI!

```
# snmpwalk -v3 -l authPriv -a MD5 -A AutPass -x DES -X PrivPass -u SnmpUser 192.168.1.103 .1
```
THANK YOU!