

# Common SNMP issues and troubleshooting

---

**Karlis Salins**

Technical support engineer



# SNMP

# SNMP – Simple Network Management Protocol

- ▶ Introduced in 1988
- ▶ Allows access to most network devices
- ▶ Multiple versions available (SNMPv1, SNMPv2, SNMPv3)
- ▶ Zabbix allows monitoring of SNMP
- ▶ SNMP monitoring is done by Zabbix server or proxy



# SNMP communications

---

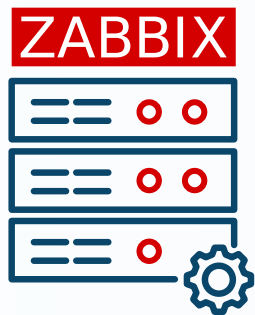
- ▶ SNMP GET
- ▶ SNMP WALK
- ▶ SNMP GETBULK
- ▶ SNMP TRAP
- ▶ SNMP SET



# Monitoring a device using SNMP

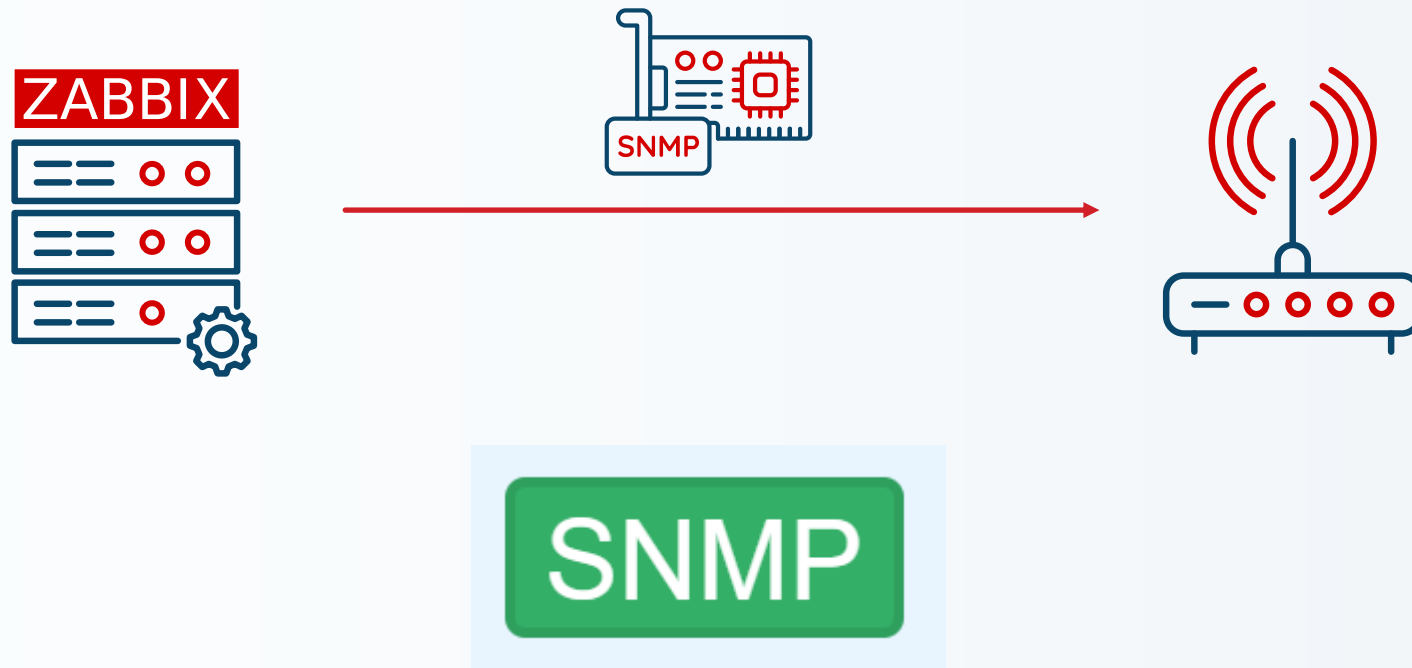
---

- ▶ 1. Create a host
- ▶ 2. Set up SNMP interface on the host
- ▶ 3. Create at least one item with type "SNMP agent"

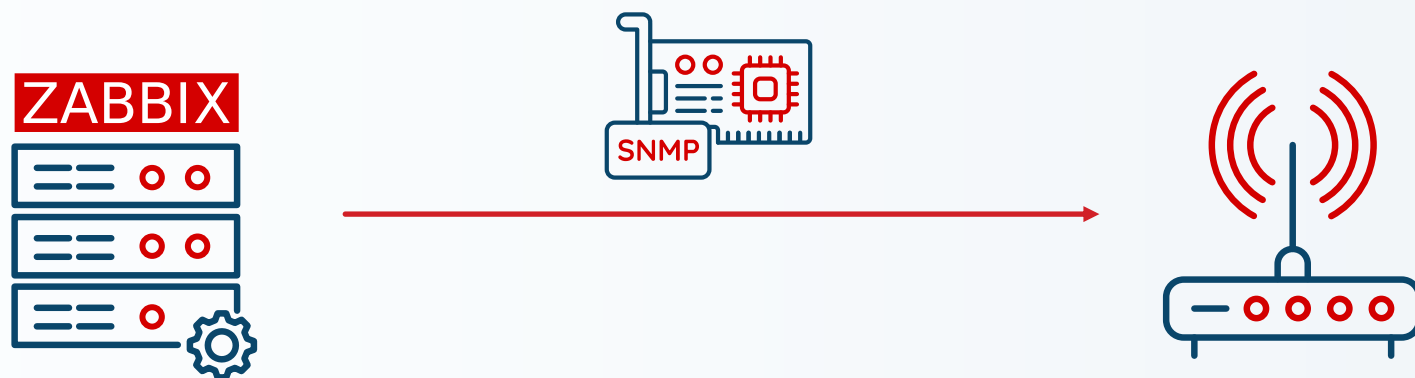


# Successful scenario

---



# Unsuccessful scenario



# Common issues

---

- ▶ Wrong device IP/DNS
- ▶ Wrong credentials
- ▶ Wrong SNMP version
- ▶ Firewall
- ▶ ACL list
- ▶ Device does not support SNMP



# Testing connection from CLI

- ▶ Needs to be done from Zabbix server/proxy to the target device
- ▶ net-snmp-utils library needs to be installed
- ▶ **SNMPv2:**

```
# snmpget -v2c -c<community> <IP/DNS> <OID>  
# IF-MIB::ifHCInOctets.1 = Counter64: 123456
```

- ▶ **SNMPv3:**

```
# snmpget -v3 -l authPriv -u <user> -a SHA -A <apass> -x AES -X <privpass>  
<IP> <OID>  
# IF-MIB::ifHCInOctets.1 = Counter64: 123456
```



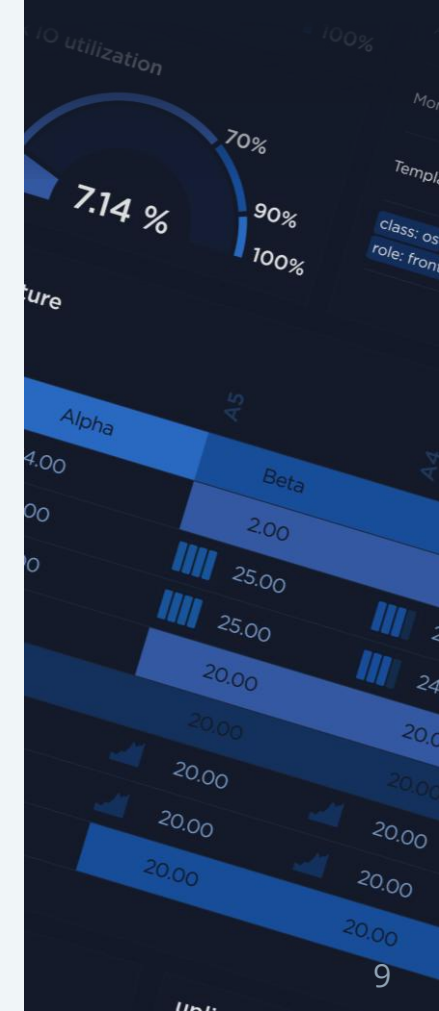


# Wrong credentials (SNMP v3)

---

- ▶ Make sure the credentials are properly set (also SNMP v2 community)
- ▶ SNMP information is stored in SNMP cache
- ▶ SNMP cache is reloaded on Zabbix server/proxy service restart
- ▶ SNMP cache can be forcefully reloaded using runtime command:

```
# zabbix_server -R snmp_cache_reload  
# Runtime control command was forwarded successfully  
# zabbix_proxy -R snmp_cache_reload  
# Runtime control command was forwarded successfully
```



# Uncommon issues

---

- ▶ Duplicate EngineID's ( SNMPv3 )
- ▶ SNMP boots are not persistent ( SNMPv3 )
- ▶ SNMP boot time is static
- ▶ Device is overloaded with requests
- ▶ Device does not allow SNMP GET to retrieve multiple values in one connection
- ▶ Device does not allow more than N values to be retrieved by SNMPBULKGET (walk[] item)



# Duplicate EngineIDs

---

- ▶ RFC 3414 - msgAuthoritativeEngineID
- ▶ All devices need to have unique EngineID's
- ▶ Troubleshooting can be done in two ways:
  - Zabbix server log ( from  $\geq 7.0$  )
  - TCP dump
- ▶ Visible in Zabbix, when multiple hosts turn on and off intermittently
- ▶ Testing from CLI will be successful



# SNMP boots are not persistent

---

- ▶ RFC 3414 - msgAuthoritativeEngineBoots
- ▶ Every single device needs to have a boot counter
- ▶ Restarting the device will increment the counter
- ▶ Testing from CLI will not be successful if using authPriv or authNoPriv security level



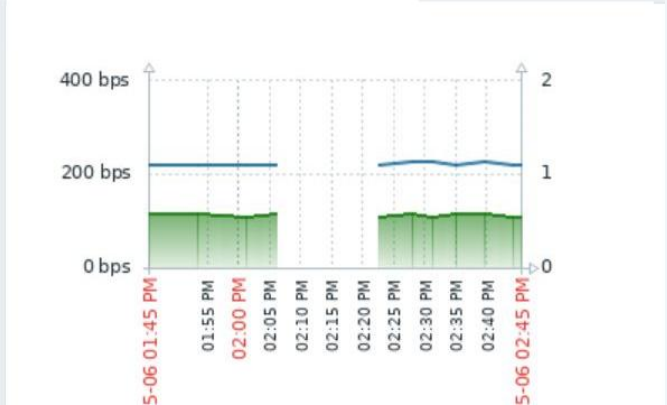
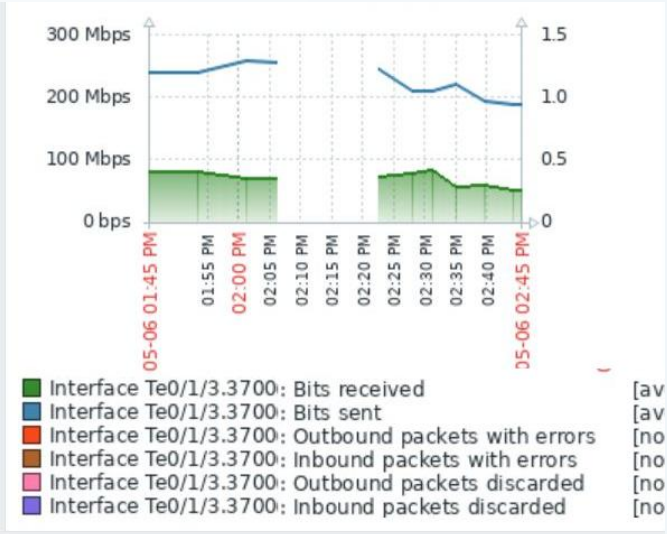
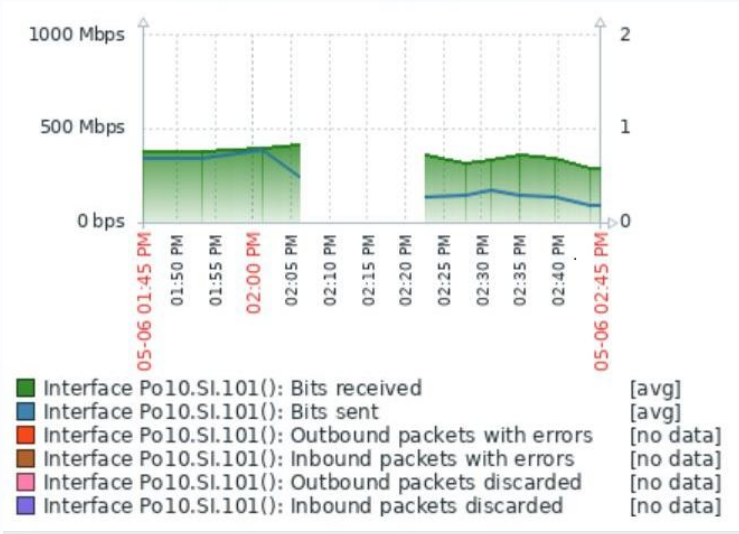
# SNMP boot time is static

---

- ▶ RFC 3414 - msgAuthoritativeEngineTime
- ▶ Every single device needs to have an uptime counter
- ▶ Restarting the device will reset the boot time
- ▶ Testing from CLI will not be successful if using authPriv or authNoPriv security level



# Device is overloaded with requests





# Device is overloaded with requests

## Log entries:

1765:20250512:103712.331 SNMP agent item  
"net.if.in[ifHCInOctets.6]" on host "Karlis switch" failed: first  
network error, wait for 15 seconds

1776:20250512:104050.473 resuming SNMP agent checks on host  
"Karlis switch": connection restored

1774:20250512:104332.050 SNMP agent item  
"net.if.in.errors[ifInErrors.123]" on host "Karlis switch" failed: first  
network error, wait for 15 seconds

1776:20250512:104724.955 resuming SNMP agent checks on host  
"Karlis switch": connection restored



# Device is overloaded with requests

---

- ▶ Happens on devices where lots of metrics are collected at short time intervals
- ▶ Because of overload, device rejects incoming connections
- ▶ Almost exclusively happens to devices which are monitored using “old” SNMP LLD





# Device is overloaded with requests

---

## How to fix it:

- ▶ Convert “old” SNMP LLD to “new” walk item and dependent discovery rule
- ▶ If using “old” SNMP LLD, increasing “Timeout” on Zabbix server/proxy **might help, but not always**
- ▶ If using “old” SNMP LLD, increase individual item polling intervals



# Device does not allow bulk request (SNMP GET)

- ▶ Some devices (mostly older) do not support bulk value retrieval for multiple values at the same time
- ▶ By default, SNMP GET requests are bundled together
- ▶ Fix:

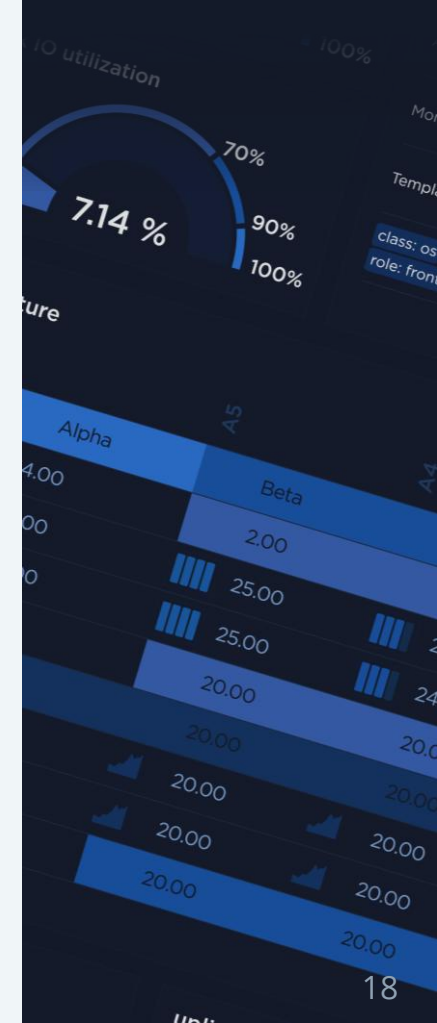
SNMP  karlis-switch.karlis.com IP DNS 161 Remove

\* SNMP version SNMPv2

\* SNMP community { \$SNMP\_COMMUNITY }

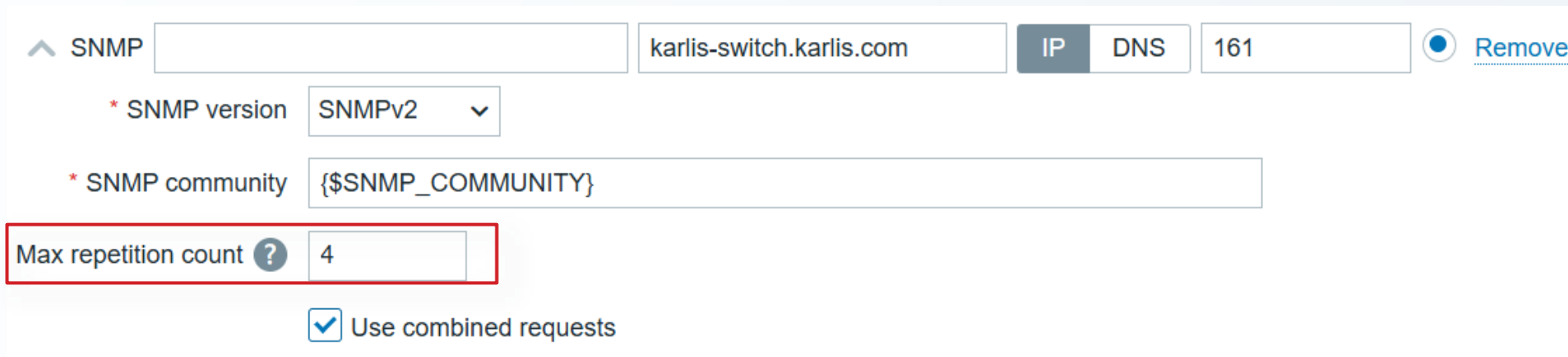
Max repetition count ? 10

☐ Use combined requests



# Device does not allow bulk requests (SNMP GETBULK)

- ▶ SNMP GETBULK retrieves 10 (default) values with each request until there are no values left in the OID table
- ▶ We have observed some occurrences when the value amount needs to be reduced
- ▶ Fix:



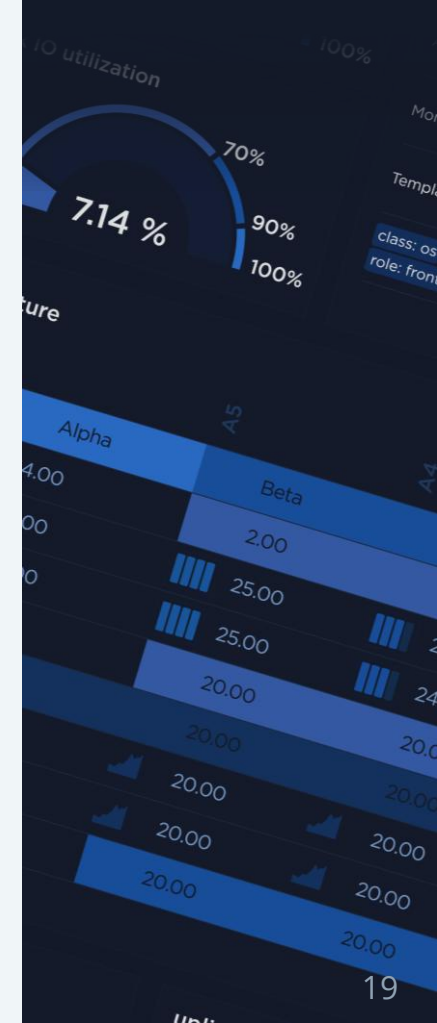
SNMP  IP DNS 161 [Remove](#)

\* SNMP version

\* SNMP community

Max repetition count

☒ Use combined requests



# SNMP trap setup (snmptrapd.conf)

---

- ▶ SNMPv2 traps require community to be set up:

```
authCommunity log,execute,net <community>
```

- ▶ SNMPv3 traps require user and EngineID to be set up:

```
createUser -e <engine id> <user> SHA <password>  
<AESauthuser>  
log,execute <user>
```

- ▶ For SNMPv3 this needs to be done for every device



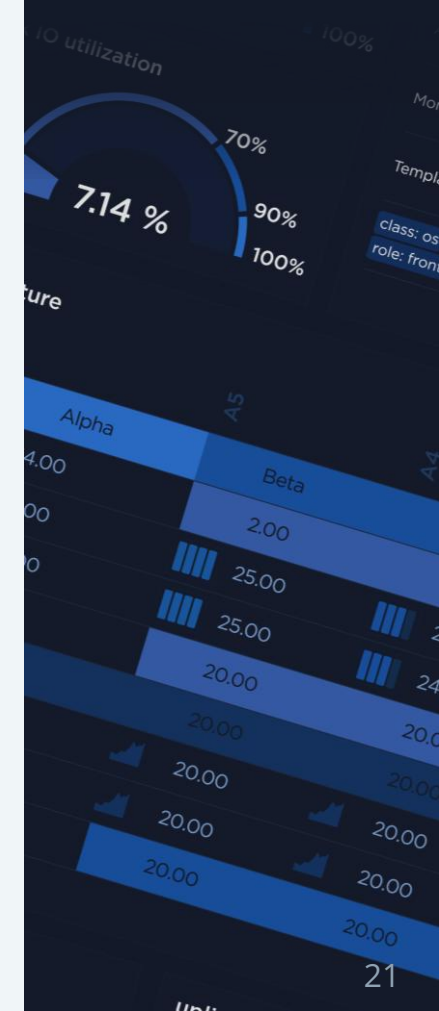
# Issues with SNMP traps

- ▶ Common network issues with SNMP polling
- ▶ Community is wrong for SNMPv2
- ▶ SNMPv3 information is wrong
- ▶ SNMPv2 test trap:

```
snmptrap -v 2c -c <community> localhost " linkUp.0
```

- ▶ SNMPv3 test trap:

```
snmptrap -v 3 -n "" -a SHA -A <apass> -x AES -X <privpass>  
-l authPriv -u <user> -e <engineID> localhost 0 linkUp.0
```



# ZABBIX '25

## CONFERENCE

GERMANY

---

**Karlis Salins**

Technical support engineer

