Troubleshooting guide

How to

Manage SNMP on webrtcgw

Edition	Changes
1.0	Creation
1.1	Add new counters
1.2	Add limitations & infos Invert description between .1.3.6.1.4.1.8072.9999.1.1.2.0 & .1.3.6.1.4.1.8072.9999.1.1.3.0 (chapter 5)
1.3	Add a SNMP trap if the certificate is close to expiring or is expired

Content

1 Introduction

1.1 Context

This document describes how to manage SNMP GET & SNMP TRAP.

Both SNMP v2c and v3 are supported.

1.2 Documents reference

Ref.	Title	Source
1		
2		

2 Description

It is now possible to configure SNMP to retrieve some counters & to send trap on thresholds.

2.1 SNMP GET

Following counters can be collected:

Global:

- Current active calls
- Maximum calls reached since last server reboot
- Number of calls for current day
- Total calls received since last server reboot
- Total of registered users
- Some counters regarding server connection
- Infos on webrtcgw processes (janus / kamailio / otlitemediapillargateway)

Per SIP domain:

- Current active calls
- Maximum calls reached since last server reboot

Standard linux system SNMP are available

- See ANNEX A for some examples

2.2 SNMP TRAP

Following traps are emitted:

- alertCallOverload: number of current actives calls >= defined threshold
- loadavg1min: trap if cpu load (/proc/loadavg 1min) >= defined threshold
  - when such situation occurs, the delay between 2 successive traps can be adjusted
- diskAlert: if disk occupation >= defined threshold
  - when such situation occurs, the delay between 2 successive traps can be adjusted
- diskAlert: trap if used memory >= defined threshold
  - when such situation occurs, the delay between 2 successive traps can be adjusted
- certificateAlert: trap if certificate validity < 30 days

- test: trap for testing

3 Configuration

The command mpsnmp can have following options:

3.1 Stop/start service

mpsnmp on

start SNMP service

- SNMP configuration must be done before starting SNMP service (see SNMP GET configuration & SNMP Trap configuration).

mpsnmp off

stop SNMP service (GET + Trap)

3.2 SNMP Get configuration

SNMP Get is configured with mpsnmp --mode=get

With following options:

--version=v2c or v3

- For v3, some questions related to V3 user creation are asked
- SNMP version be different for Get & Trap

--community="your community"

- For version v2c only
  public community is not recommended

--contact="your contact"

- sysContact information
- Used with OID .1.3.6.1.2.1.1.4.0

--location="your location"

- sysLocation information
- Used with OID .1.3.6.1.2.1.1.6.0

--monitdomains

- This option is used ONLY for webrtcgw shared between Pabxs.
  This allows to have detailed counters (activeCalls + maxCalls) per oxe SIP domain
- Do not activate it if your webrtcgw is linked to only one PABX

--nomonitdomains

- Deactivate SIP domains monitoring

3.3 SNMP Trap configuration

SNMP Trap is configured with mpsnmp --mode=trap

With following options:

--version=v2c or v3

- For v3, some questions related to V3 user creation are asked
- SNMP version be different for Get & Trap

--community=”your community”
- For version v2c only
  public community is not recommended

--traphost=<FQDN or IP>
- Remote trap receiver
  Be sure that no firewall blocks connectivity

--notrap
- Monitoring is stopped. No more automatic trap
  Manual trap emission is still possible.

--thcalls=<number of calls>
- Number of active calls threshold
- Alarm is repeated every 5s (monitoring loop delay) if threshold >= thcalls to inform of persistent overload.

--thcpu=<% of cpu>
- CPU % threshold
- Associated with parameter –delaycpu

---delaycpu=<delay between alarm in seconds>
- If cpu reaches the threshold, alarm could stay active until action.
- delaycpu is the delay before trap repetition

--thdisk=<% of used disk>
- Disk occupation % threshold
- Associated with parameter –delaydisk

--delaydisk=<delay between alarm in seconds>
- If disk reaches the threshold, alarm will stay active until action.
- delaydisk is the delay before trap repetition

--thmem=<% of used memory>
- Memory used % threshold
- Associated with parameter --delaymem

---delaymem=<delay between alarm in seconds>
- If memory reaches the threshold, alarm could stay active until action.
- delaymem is the delay before trap repetition

3.4 SNMP user v3

When SNMP v3 is selected (--version=v3), some information related to security are requested.
Questions are the same between Get & Trap.

Ex:
mpsnmp --mode=get --version=v3
Stopping SNMP service ...
Enter SNMP V3 user for GET:
Enter your password (8 characters minimum):
Confirm your password :
Enter your passphrase (8 characters minimum):
Confirm your passphrase :

Which Authentication protocol is used: MD5 SHA SHA-224 SHA-256 SHA-384 SHA-512 (default SHA)?
What is privacy protocol used: DES AES (default AES)?
SNMP V3 user userV3 created (SHA / AES)
Community is deactivated to prevent SNMP v2c usage
Starting SNMP service ...
SNMP service is started !

- SNMP v3 user can be different for Get & Trap
- Only SecurityLevel "authPriv" (Authentication + Encryption) is supported (most secured level)
- For Get, user information is store in /var/lib/snmp/snmpd.conf
  - password & passphrase are crypted
- For Trap, user information is store in /etc/snmp/snmp.conf
  - You can notice that information is in clear text. This is normal behavior with snmp.

3.5 Check SNMP configuration

You can check if your configuration seems correct:

mpsnmp check

ex:

```
Checking SNMP GET configuration ...
  [OK] SNMP V2C is used for GET
  [OK] Community is "rainbow" in /etc/snmp/snmpd.conf
  [OK] Contact is "admin@labale.bzh" in /etc/snmp/snmpd.conf
  [OK] Location is "Paris / Buidling A / Floor 0" in /etc/snmp/snmpd.conf
  [OK] SIP domains metrics are activated
      [REMINDER] This option must be activated only if many PABXs are using this webrtcgw !

Checking SNMP TRAP configuration ...
  [OK] SNMP Trap is activated
  [OK] SNMP v2c is used for trap
  [OK] Community is "rainbow"
  [OK] REMOTE host is xxx.xxx.xxx.xxx : Check if correct ...

Alerts definition …
  [OK] CPU alert when 85% is reached
  [OK] Memory alert when 85% is reached
  [OK] Memory alert is every 60 seconds
  [OK] Disk alert when 90% is reached
  [OK] Disk alert is every 60 seconds
  [OK] Calls alert when active calls >= 300

Checking SNMP service status ...
  SNMP service is enabled
  SNMP service is active

Trying to send a testing trap with OID .1.3.6.1.4.1.999.3.999.1.3.999 ...
  [OK]  Please check reception on remote party
```

4 Troubleshooting

This chapter describes how to test configuration.

4.1 Get

Some tools are existing for testing SNMP get:
Ex: SnmpB download | SourceForge.net
Free MIB Browser / MIB Browser / SNMP Browser.
Embedded snmpget / snmptrap / snmpbulk …

On webrtcgw itself, you can test Get with snmpget command:
v2c:
snmpget -v2c -c <community> <host> .1.3.6.1.4.1.8072.9999.1.1.1.0 -m ""
v3c:
snmpget -v 3 -u <user v3> -l authPriv -a SHA -A "<password>" -x AES -X "<privacy>" <host> .1.3.6.1.4.1.8072.9999.1.1.1.0 -m ""

SIP domains (if managed) can be discovered using snmpwalk or snmpbulk:
v2c:
snmpwalk -v2c -c <community> <host> .1.3.6.1.4.1.8072.9999.1.2 -m ""
v3c:
snmpwalk -v 3 -u <user v3> -l authPriv -a SHA -A "<password>" -x AES -X "<privacy>" <host> .1.3.6.1.4.1.8072.9999.1.2 -m ""

Ex with OID only: snmpwalk -v2c -c <community> <host> .1.3.6.1.4.1.8072.9999.1.2 -m ""
iso.3.6.1.4.1.8072.9999.1.2.1.1 = STRING: "domain1.labale.bzh"
iso.3.6.1.4.1.8072.9999.1.2.1.2 = INTEGER: 10
iso.3.6.1.4.1.8072.9999.1.2.1.3 = INTEGER: 76
iso.3.6.1.4.1.8072.9999.1.2.2.1 = STRING: "domain2.labale.bzh"
iso.3.6.1.4.1.8072.9999.1.2.2.2 = INTEGER: 4
iso.3.6.1.4.1.8072.9999.1.2.2.3 = INTEGER: 34

Ex with generic MIB name: snmpwalk -v2c -c <community> <host> .1.3.6.1.4.1.8072.9999.1.2
NET-SNMP-MIB::netSnmpExperimental.1.2.1.1 = STRING: "domain1.labale.bzh"
NET-SNMP-MIB::netSnmpExperimental.1.2.1.2 = INTEGER: 10
NET-SNMP-MIB::netSnmpExperimental.1.2.1.3 = INTEGER: 76
NET-SNMP-MIB::netSnmpExperimental.1.2.2.1 = STRING: "domain2.labale.bzh"
NET-SNMP-MIB::netSnmpExperimental.1.2.2.2 = INTEGER: 4
NET-SNMP-MIB::netSnmpExperimental.1.2.2.3 = INTEGER: 34

Ex using RAINBOW-MIB explicitly: snmpwalk -v2c -c <community> <host> .1.3.6.1.4.1.8072.9999.1.2 -M +/opt/mediapillar/cv/MIB/ -m +RAINBOW-MIB
RAINBOW-MIB::RAINBOW-MIB.9999.1.2.1.1 = STRING: "domain1.labale.bzh"
RAINBOW-MIB::RAINBOW-MIB.9999.1.2.1.2 = INTEGER: 10
RAINBOW-MIB::RAINBOW-MIB.9999.1.2.1.3 = INTEGER: 76
RAINBOW-MIB::RAINBOW-MIB.9999.1.2.2.1 = STRING: "domain2.labale.bzh"
RAINBOW-MIB::RAINBOW-MIB.9999.1.2.2.2 = INTEGER: 4
RAINBOW-MIB::RAINBOW-MIB.9999.1.2.2.3 = INTEGER: 34

4.2 Trap

Command “mpsnmp check” is including a trap sending.

You can send manually a trap by:
/opt/mediapillar/cv/send_snmp_trap.sh test

- Note that you don’t need to give user v3 information since it is read from /etc/snmp/snmp.conf

5 Rainbow-MIB

The Rainbow mib file is present in /opt/mediapillar/cv/MIB/RAINBOW-MIB.
This file can be added in your SNMP supervisor tool.

This MIB is based on NET-SNMP MIB and is using extension netSnmpExperimental (.1.3.6.1.4.1.8072.9999) subtree.

Specific Rainbow OID (.1.3.6.1.4.1.8072.9999.1)

OID	Type	Information	Description
.1.3.6.1.4.1.8072.9999.1.1.1.0	Get	Number	Number of current active calls
.1.3.6.1.4.1.8072.9999.1.1.2.0	Get	Number	Number of calls for today
.1.3.6.1.4.1.8072.9999.1.1.3.0	Get	Number	Number of maximum calls since last server reboot
.1.3.6.1.4.1.8072.9999.1.1.4.0	Get	Number	Number of total calls since last server reboot
.1.3.6.1.4.1.8072.9999.1.1.5.0	Get	Number	Number of registered users
.1.3.6.1.4.1.8072.9999.1.1.6.0	Get	Number	Number of daily server connection
.1.3.6.1.4.1.8072.9999.1.1.7.0	Get	Number	Number of failed server connection
.1.3.6.1.4.1.8072.9999.1.1.8.0	Get	Number	Number of total server connection
.1.3.6.1.4.1.8072.9999.1.1.9.0	Get	Number	Number of daily server connection (XMPP)
.1.3.6.1.4.1.8072.9999.1.1.10.0	Get	Number	Number of failed server connection (XMPP)
.1.3.6.1.4.1.8072.9999.1.1.11.0	Get	Number	Number of total server connection (XMPP)
.1.3.6.1.4.1.8072.9999.1.2.x.1	Get	String	SIP Domain name x
.1.3.6.1.4.1.8072.9999.1.2.x.2	Get	Number	Number of current active calls for SIP domain x
.1.3.6.1.4.1.8072.9999.1.2.x.3	Get	Number	Number of calls maximum calls for SIP domain x
.1.3.6.1.4.1.8072.9999.1.3.1	Trap	.1.3.6.1.2.1.1.5.0: server FQDN .1.3.6.1.4.1.8072.9999.1.1.1.0: number of active calls .1.3.6.1.4.1.8072.9999.1.1.100.0: threshold for call .1.3.6.1.4.1.8072.9999.1.1.200: description	active calls reach threshold
.1.3.6.1.4.1.8072.9999.1.3.2	Trap	.1.3.6.1.2.1.1.5.0: server FQDN .1.3.6.1.4.1.8072.9999.1.1.101.0: cpu load .1.3.6.1.4.1.8072.9999.1.1.102.0: threshold for cpu load .1.3.6.1.4.1.8072.9999.1.1.200: description	cpu load reaches threshold
.1.3.6.1.4.1.8072.9999.1.3.3	Trap	.1.3.6.1.2.1.1.5.0: server FQDN .1.3.6.1.4.1.8072.9999.1.1.103.0: disk occupation .1.3.6.1.4.1.8072.9999.1.1.104.0: threshold for disk occupation .1.3.6.1.4.1.8072.9999.1.1.200: description	disk reaches threshold
.1.3.6.1.4.1.8072.9999.1.3.4	Trap	.1.3.6.1.2.1.1.5.0: server FQDN	used memory reaches threshold

		.1.3.6.1.4.1.8072.9999.1.1.105.0: memory occupation .1.3.6.1.4.1.8072.9999.1.1.106.0: threshold for memory occupation .1.3.6.1.4.1.8072.9999.1.1.200: description	
.1.3.6.1.4.1.8072.9999.1.3.5	Trap	.1.3.6.1.2.1.1.5.0: server FQDN .1.3.6.1.4.1.8072.9999.1.1.200: description	Certificate for SIP TLS or HTTPS is close to expiring or is expired Description field gives number of remaining days before expiration
.1.3.6.1.4.1.8072.9999.1.3.999	Trap	.1.3.6.1.2.1.1.5.0: server FQDN .1.3.6.1.4.1.8072.9999.1.1.200: description	Testing

☞ Add the Rainbow MIB in your environment

6 Limitations

1) Using mpsnmp --mode=get/trap will delete existing SNMP manual configuration (if any).
   - Save your own configuration & synchronize it after management with mpsnmp

2) Only one community for get or trap.

3) Only one destination for trap.

4) Regarding “Authentication password” & “Privacy password”, check if your snmp client has restriction with special characters.
   - In case of trouble with get/trap, try with a simple password.

ANNEX A: System Linux SNMP OID

This annex gives some OID values for Linux system (get, walk, bulk).

Description	OID
Load	
1 minute Load	.1.3.6.1.4.1.2021.10.1.3.1
5 minute Load	.1.3.6.1.4.1.2021.10.1.3.2
15 minute Load	.1.3.6.1.4.1.2021.10.1.3.3
CPU	
percentage of user CPU time	.1.3.6.1.4.1.2021.11.9
raw user cpu time	.1.3.6.1.4.1.2021.11.50
percentages of system CPU time	.1.3.6.1.4.1.2021.11.10
raw system cpu time	.1.3.6.1.4.1.2021.11.52
percentages of idle CPU time	.1.3.6.1.4.1.2021.11.11
raw idle cpu time	.1.3.6.1.4.1.2021.11.53
raw nice cpu time	.1.3.6.1.4.1.2021.11.51
Memory Statistics	
Total Swap Size	.1.3.6.1.4.1.2021.4.3
Available Swap Space	.1.3.6.1.4.1.2021.4.4
Total RAM in machine	.1.3.6.1.4.1.2021.4.5
Total RAM used	.1.3.6.1.4.1.2021.4.6
Total RAM Free	.1.3.6.1.4.1.2021.4.11
Total RAM Shared	.1.3.6.1.4.1.2021.4.13
Total RAM Buffered	.1.3.6.1.4.1.2021.4.14
Total Cached Memory	.1.3.6.1.4.1.2021.4.15
Disk Statistics	
Path where the disk is mounted	.1.3.6.1.4.1.2021.9.1.2.1
Path of the device for the partition	.1.3.6.1.4.1.2021.9.1.3.1
Total size of the disk/partion (kBytes)	.1.3.6.1.4.1.2021.9.1.6.1
Available space on the disk	.1.3.6.1.4.1.2021.9.1.7.1
Used space on the disk	.1.3.6.1.4.1.2021.9.1.8.1
Percentage of space used on disk	.1.3.6.1.4.1.2021.9.1.9.1
Percentage of inodes used on disk	.1.3.6.1.4.1.2021.9.1.10.1
Interfaces	
Interface's name	.1.3.6.1.2.1.31.1.1.1.1.1 (lo) .1.3.6.1.2.1.31.1.1.1.1.1.1 (eth0)
Interfaces Input Octets (ifInOctets)	.1.3.6.1.2.1.2.2.1.10
Interfaces Output Octets (ifOutOctets)	.1.3.6.1.2.1.2.2.1.16
Interfaces Output Errors (ifOutErrors)	.1.3.6.1.2.1.2.2.1.20
System	
System Uptime	.1.3.6.1.2.1.1.3
sysLocation	.1.3.6.1.2.1.1.6
sysContact	.1.3.6.1.2.1.1.4
sysDescr	.1.3.6.1.2.1.1.1
Webrtcgw processes	
Janus	.1.3.6.1.4.1.2021.2.1.2.1
Janus minimum instances	.1.3.6.1.4.1.2021.2.1.3.1
Janus maximum instances	.1.3.6.1.4.1.2021.2.1.4.1
Janus number of running instances	.1.3.6.1.4.1.2021.2.1.5.1
Janus error flag (0= no error / 1 = error)	.1.3.6.1.4.1.2021.2.1.100.1
Janus error message (if error=1)	.1.3.6.1.4.1.2021.2.1.101.1
Kamailio	.1.3.6.1.4.1.2021.2.1.2.2
Kamailio minimum instances	.1.3.6.1.4.1.2021.2.1.3.2
Kamailio maximum instances	.1.3.6.1.4.1.2021.2.1.4.2
Kamailio number of running instances	.1.3.6.1.4.1.2021.2.1.4.2
Kamailio error flag (0= no error / 1 = error)	.1.3.6.1.4.1.2021.2.1.100.2
Kamailio error message (if error=1)	.1.3.6.1.4.1.2021.2.1.101.2
nodejs (otlitemediapillargateway)	.1.3.6.1.4.1.2021.2.1.2.3
nodejs (otlitemediapillargateway) minimum instances	.1.3.6.1.4.1.2021.2.1.3.3

nodejs (otlitemediapillargateway) maximum instances	.1.3.6.1.4.1.2021.2.1.4.3
nodejs (otlitemediapillargateway) number of running instances	.1.3.6.1.4.1.2021.2.1.4.3
nodejs (otlitemediapillargateway) error flag (0= no error / 1 = error)	.1.3.6.1.4.1.2021.2.1.100.3
nodejs (otlitemediapillargateway) error message (if error=1)	.1.3.6.1.4.1.2021.2.1.101.3

- This list is not exhaustive.
- Refer to IANA Private Enterprise Numbers (PENs)

- You can list all available OIDs from root with:
  snmpwalk -v2c -c rainbow localhost .1
  snmpwalk -v3 -u <user v3> -l authPriv -a SHA -A <password> -x AES -X <privacy> <host> .1