

SNMP



- SNMP
- SNMPD
 -
- Unknown token: defaultMonitors Unknown token: linkUpDownNotifications
- SNMP
 - : snmpget
 - SNMPv3: snmpusm
 - SNMPv3: snmpvacm
 -
 -
-

$$\vdots$$

- Astra Linux Special Edition .10015-01 (1.7), .10015-10
- Astra Linux Special Edition .10015-17
- Astra Linux Special Edition .10015-37 (7.7)
- Astra Linux Special Edition .10015-03 (7.6)
- Astra Linux Special Edition .10152-02 (4.7)
- Astra Linux Special Edition .10015-01 (1.6)
- Astra Linux Special Edition .10015-16 . 1
- Astra Linux Special Edition .10015-16 . 2
- Astra Linux Special Edition .10265-01 (8.1)
- Astra Linux Common Edition 2.12

SNMP (- Simple Network Management Protocol —) — - IP- TCP/UDP. SNMP , , , . , . SNMP , , .

$$\vdots$$

MIB () . SNMP MIB . , MIB, .

Astra Linux Special Edition.

IP-: 192.168.1.111

IP-: 192.168.1.112

SNMP :

```
sudo apt install snmp
```

SNMPD () :

```
sudo apt install snmpd
```

```
snmp-mibs-downloader MIB-. Debian. :
```

1. Astra Linux Special Edition .10015-01 1.6 snmp-mibs-downloader smstrip:

```
wget http://ftp.de.debian.org/debian/pool/main/libs/libsmi/smstrip_0.4.8+dfsg2-16_all.deb
sudo apt install -y ./smstrip_0.4.8+dfsg2-16_all.deb
```

Astra Linux Special Edition .10015-01 1.7 ;

- ## 2. snmp-mibs-downloader:

- a. Astra Linux Special Edition .10015-01 1.7 2023-1023SE17 (1.7.5) . :

```
sudo apt install snmp-mibs-downloader
```

b. Debian:

```
wget http://ftp.de.debian.org/debian/pool/non-free/s/snmp-mibs-downloader/snmp-mibs-downloader_1.5_all.deb
sudo apt install -y ./snmp-mibs-downloader_*.deb
```

SNMP

/etc/snmp/snmp.conf SNMP MIB, :

```
#mibs :
```

SNMPD

1. /etc/snmp/snmpd.conf agentAddress, . . . :

```
# ( )
#agentAddress udp:127.0.0.1:161

# (IPv4 ** IPv6)
agentAddress udp:161,udp6:[::1]:161
```



IPv6, udp6:[::1]:161.
IPv6 , udp6:[::1]:161, snmpd , , , "Timeout" .

2. %_,, . SNMP . , (MD5 SHA) (8). , (DES AES) (). , .

:

"initial", <_>, MD5 DES. /etc/snmp/snmpd.conf :

1. :

```
createUser initial MD5 <_> DES
```



SNMP : . , .

2. :

```
group MyRWGroup usm initial
```

3. (view) :

```
view viewall included .1
```

4. :

```
access MyRWGroup "" usm priv exact viewall viewall none
```

/etc/snmp/snmpd.conf :

```
createUser initial MD5 <_> DES
group MyRWGroup usm initial
view viewall included .1
access MyRWGroup "" usm priv exact viewall viewall none
```

snmpd:

```
sudo systemctl restart snmpd
```

, OID initial:

```
snmpwalk -u initial -l authPriv -a MD5 -x DES -A <_> -X <_> localhost .
```

/ snmpd:

```
sudo systemctl status snmpd
```

```
snmpd.service - Simple Network Management Protocol (SNMP) Daemon.
  Loaded: loaded (/lib/systemd/system/snmpd.service; enabled; vendor
  preset: enabled)
  Active: active (running) since Fri 2022-03-04 09:22:44 MSK; 8s ago
  Process: 7319 ExecStartPre=/bin/mkdir -p /var/run/agentx (code=exited,
  status=0/SUCCESS)
  Main PID: 7321 (snmpd)
    Tasks: 1 (limit: 4641)
   Memory: 5.2M
    CGroup: /system.slice/snmpd.service
           7321 /usr/sbin/snmpd -Lsd -Lf /dev/null -u Debian-snmp -g Debian-
  snmp -I -smux mteTrigger mteTriggerConf -f -p /run/snmpd.pid

04 09:22:44 se17 systemd[1]: Starting Simple Network Management Protocol
(SNMP) Daemon....
04 09:22:44 se17 systemd[1]: Started Simple Network Management Protocol
(SNMP) Daemon..
04 09:22:44 se17 snmpd[7321]: /etc/snmp/snmpd.conf: line 145: Warning:
Unknown token: defaultMonitors.
04 09:22:44 se17 snmpd[7321]: /etc/snmp/snmpd.conf: line 147: Warning:
Unknown token: linkUpDownNotifications.
04 09:22:44 se17 snmpd[7321]: Turning on AgentX master support.
04 09:22:44 se17 snmpd[7321]: NET-SNMP version 5.7.3
```

Unknown token: defaultMonitors Unknown token: linkUpDownNotifications

snmpd :

```
snmpd[7321]: /etc/snmp/snmpd.conf: line 145: Warning: Unknown token: defaultMonitors.
snmpd[7321]: /etc/snmp/snmpd.conf: line 147: Warning: Unknown token: linkUpDownNotifications.
```

MIB DISMAN (). , , , / /etc/snmp/snmpd.conf.

, , , MIB DISMAN, :

1. /etc/snmp/snmpd.conf defaultMonitors linkUpDownNotifications :

- a. defaultMonitors:

```
monitor -o prNames      -o prErrorMessage "procTable" prErrorFlag  != 0
monitor -o memErrorName -o memSwapErrorMsg "memory"  memSwapError  != 0
monitor -o extNames     -o extOutput       "extTable"  extResult    != 0
monitor -o dskPath      -o dskErrorMsg    "dskTable"  dskErrorFlag != 0
monitor -o laNames      -o laErrMessage   "laTable"    laErrorFlag  != 0
monitor -o fileName     -o fileErrorMsg   "fileTable"  fileErrorFlag != 0
```

- b. linkUpDownNotifications

```
notificationEvent linkUpTrap linkUp ifIndex ifAdminStatus ifOperStatus
notificationEvent linkDownTrap linkDown ifIndex ifAdminStatus ifOperStatus
monitor -r 60 -e linkUpTrap "Generate linkUp" ifOperStatus != 2
monitor -r 60 -e linkDownTrap "Generate linkDown" ifOperStatus == 2
```

2. /etc/systemd/system/snmpd.service.d/override.conf.



:

```
sudo systemctl edit snmpd
```

:

```
[Service]
Environment=
Environment="MIBSDIR=/usr/share/snmp/mibs:/usr/share/snmp/mibs/iana:/usr/share/snmp/mibs/ietf:/usr
/share/mibs/site:/usr/share/snmp/mibs:/usr/share/mibs/iana:/usr/share/mibs/ietf:/usr/share/mibs
/netsnmp"
ExecStart=
ExecStart=/usr/sbin/snmpd -Lsd -Lf /dev/null -u Debian-snmp -g Debian-snmp -I -smux -f -p /run/snmpd.
pid
```

" " . Environment=MIBSDIR etc/systemd/system/snmpd.service, ExecStart etc/systemd/system/snmpd.service, :

```
,mteTrigger,mteTriggerConf"
```

3. sudo systemctl edit, :

```
sudo systemctl daemon-reload
```

4. snmpd:

```
sudo systemctl restart snmpd
```

SNMP

SNMPv3 snmpusm. SNMP:

- snmpget - ;
- snmpset - ;

- snmpwalk - MIB.

net-snmp .

SNMP. :

- -v (version): SNMP.
- -c (community): .
- -u (user-name): ., ., SNMP.
- -l (level): . : noAuthNoPriv (), authNoPriv () authPriv (). , , .
- -a (protocol): , MD5 SHA. , .
- -x (protocol): , DES AES. , . , priv.
- -A (passphrase): .
- -X (passphrase): . , . , priv.

:

```
snmp_command -u <_> -l authPriv -a MD5 -x DES -A <_> -X <_> <IP-> <_>
```

: snmpget

, , initial, :

```
snmpget -u initial -l authPriv -a MD5 -x DES -A <_> -X <_> 192.168.1.112
1.3.6.1.2.1.1.1.0
```

1.3.6.1.2.1.1.1.0 – OID, . , uname -a:

```
SNMPv2-MIB::sysDescr.0 = STRING: Linux se17o1 5.4.0-81-generic #astra34+ci17-Ubuntu SMP Mon Nov 22 13:21:54
UTC 2021 x86_64
```

SNMPv3: snmpusm

snmpusm - , . :

```
snmpusm <_> <_> create <_> <_>
```

(initial) :

```
snmpusm -u initial -l authPriv -a MD5 -x DES -A <_> -X <_> localhost
create admin initial
```

admin. , () , initial, . , () :

```
snmpusm -u initial -l authPriv -a MD5 -x DES -A <_> -X <_> localhost
passwd <_> <_> admin
```

admin <_>.

SNMPv3: snmpvacm

snmpvacm .:

```
snmpvacm -u initial -l authPriv -a MD5 -x DES -A <_> -X <_> localhost
createSec2Group 3 admin rwgrp
```

:

- createSec2Group MODEL SECURITYNAME GROUPNAME .:
 - MODEL - , :

- 1 - SNMPv1;
- 2 - SNMPv2c;
- 3 - User-based Security Model (USM) .
- SECURITYNAME -, (). USM ;
- GROUPNAME -, , . .

:

```
snmpvacm -u initial -l authPriv -a MD5 -x DES -A <_> -X <_> localhost
createAccess rwgrp 3 3 1 viewall viewall none
```

:

- createAccess GROUPNAME [CONTEXTPREFIX] MODEL LEVEL CONTEXTMATCH READVIEW WRITEVIEW NOTIFYVIEW ,
MIB .:
 - GROUPNAME -, ;
 - CONTEXTPREFIX ()-, . CONTEXTMATCH. , "".
 - MODEL -, :
 - 1 - SNMPv1;
 - 2 - SNMPv2c;
 - 3 - User-based Security Model (USM)
 - LEVEL -, :
 - 1 - noAuthNoPriv - ;
 - 2 - authNoPriv - ;
 - 3 - authPriv - ;
 - CONTEXTMATCH - CONTEXTPREFIX:
 - 1 ('exact') - CONTEXTPREFIX;
 - 2 ('prefix') - ;
 - READVIEW - MIB (view , viewall), MIB, ;
 - WRITEVIEW - MIB (view , viewall), MIB, ;
 - NOTIFYVIEW - MIB, MIB, ();

, admin OID. OID :

```
snmpwalk -u admin -l authPriv -a MD5 -x DES -A <_> -X <_> localhost .1
```

- initial, :

```
snmpusm -u admin -l authPriv -a MD5 -x DES -A <_> -X <_> localhost
delete initial
```

, initial snmpd :

```
createUser initial MD5 <_> DES
group MyRWGroup usm initial
```

q2w2e2r2, - 87654321.

```

#!/bin/bash
inipass="q2w2e2r2"
admpass="87654321"
wget http://ftp.de.debian.org/debian/pool/non-free/s/snmp-mibs-downloader/snmp-mibs-downloader_1.5_all.deb
sudo apt update
sudo apt install -y snmp snmpd ./snmp-mibs-downloader_1.5_all.deb
[ -f /etc/snmp/snmp.conf ] && sudo sed -i "s/^s*mibs\s*:/#mibs :/" /etc/snmp/snmp.conf
if [ -f /etc/snmp/snmpd.conf ] ; then
    sudo sed -i.bak "s/^s*agentAddress.*agentAddress udp:161/" /etc/snmp/snmpd.conf
    echo "createUser initial MD5 \"$inipass\" DES" | sudo tee -a /etc/snmp/snmpd.conf
    echo "group MyRWGroup usm initial" | sudo tee -a /etc/snmp/snmpd.conf
    echo "view viewall included .1" | sudo tee -a /etc/snmp/snmpd.conf
    echo "access MyRWGroup \"\" usm priv exact viewall viewall none" | sudo tee -a /etc/snmp/snmpd.conf
    sudo systemctl restart snmpd
fi
snmpwalk -u initial -l authPriv -a MD5 -x DES -A "$inipass" -X "$inipass" localhost .
snmpusm -u initial -l authPriv -a MD5 -x DES -A "$inipass" -X "$inipass" localhost create admin initial
snmpusm -u initial -l authPriv -a MD5 -x DES -A "$inipass" -X "$inipass" localhost passwd "$inipass"
"$admpass" admin
snmpvacm -u initial -l authPriv -a MD5 -x DES -A "$inipass" -X "$inipass" localhost createSec2Group 3 admin
rwgrp
snmpvacm -u initial -l authPriv -a MD5 -x DES -A "$inipass" -X "$inipass" localhost createAccess rwgrp 3 3 1
viewall viewall none
snmpwalk -u admin -l authPriv -a MD5 -x DES -A "$admpass" -X "$admpass" localhost .
snmpusm -u admin -l authPriv -a MD5 -x DES -A "$admpass" -X "$admpass" localhost delete initial
sudo sed -i -e "/^s*createUser\s\+initial.*d" \
-e "/^s*group\s\+MyRWGroup\s\+usm\s\+initial/d" /etc/snmp/snmpd.conf
sudo systemctl restart snmpd

```