

SNMPD (Simple Network Management Protocol)

SNMPD allow you to collecting and organizing information about managed devices on IP networks and for modifying that information to change device behaviour.

Here are the configuration directives, how to configure SNMPD and what are the possible values you can put into text fields.

For learning Net-SNMP go to [here](#).

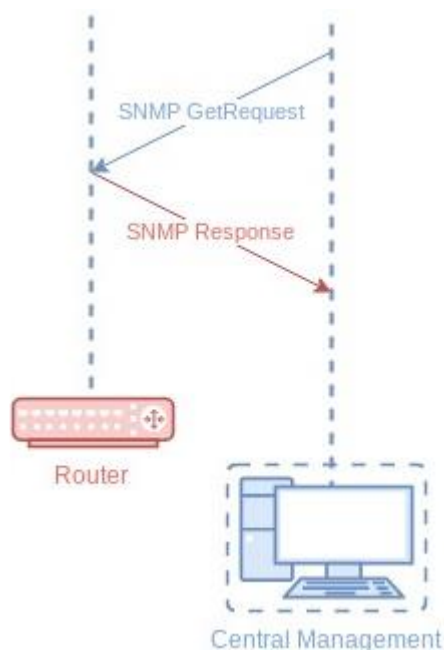


Fig-1: SNMPD

-- SNMPD General Settings --

Enable/Disable SNMP Deamon:

Enable or Disable the SNMPD application.

SNMP EnginID Section:

EngineID: Auto-Generated value and will be available on first start-up.

Useful, if you are configuring SNMPTRAP application (maybe useful for another trap receiver also) in trap mode.

SNMP Agent Profile:

Agentaddress:

- The default agent behaviour (listening on the standard SNMP UDP port on all interfaces) is equivalent to the directive:

`agentaddress udp:161` or simply `agentaddress 161`

- The agent can be configured to only accept requests sent to the local loopback interface (again listening on the SNMP UDP port), using:

`agentaddress localhost:161` # (udp implicit)

or

`agentaddress 127.0.0.1` # (udp and standard port implicit)

- It can be configured to accept both UDP and TCP requests (over both IPv4 and IPv6), using:

`agentaddress udp:161, tcp:161, udp6:161, tcp6:161`

Other combinations are also valid.

System Information:

The full contents of the 'system' group (apart from sysUpTime) can be explicitly configured using:

SysName: It is a device hostname and can be set through Manager.

Note: Setting sysName through manager will not change device hostname. It will only update sysName in system information.

SysContact: Default is blank and can be set through Manager.

SysLocation: Default is blank and can be set through Manager.

SysDescr: Default 'uname -s -n -r -v -m' command output and it is not writable using set request.

-- SNMPD v1/v2c/usm Configuration --

VACM (View-based Access Control Model) on Net-SNMP:

- For Configuring v1/v2c we follow the VACM model.
- The VACM determines whether access to a managed object in a local MIB by a remote principal should be allowed. The VACM makes use of a MIB that defines the access control policy for this agent and makes it possible for remote configuration to be used.
- Net-SNMP uses four keywords to set up VACM:

Com2sec

Access

Group

View

These set up access control to variables on the agent.

- access and view determine what access is being controlled to.
- group and com2sec determine who has this access.

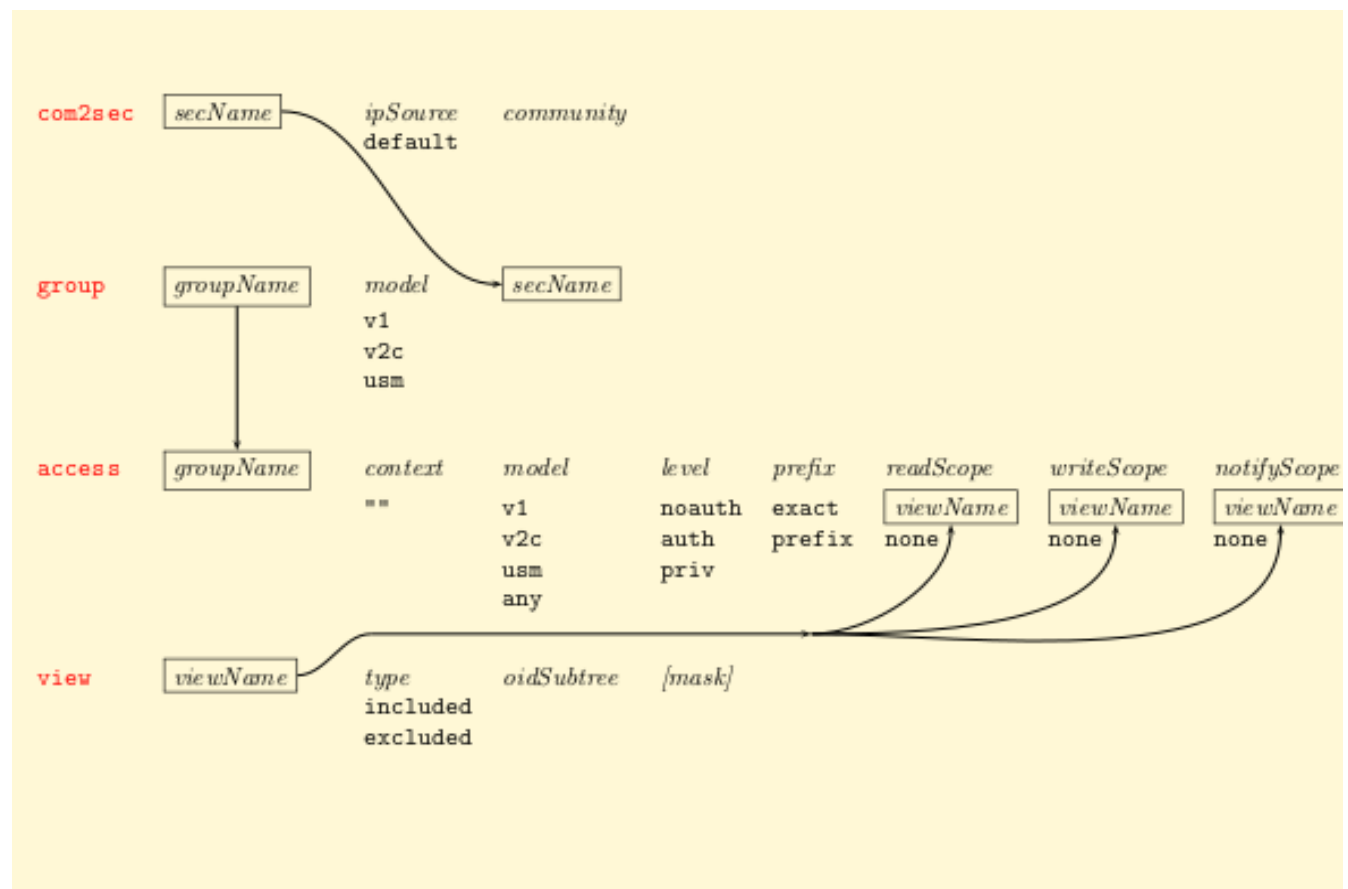


Fig-2: VACM Configuration Model

Com2Sec Configuration:

Maps a community string and a source IP or network address to a security name (username).

Security Name: Username specifies the security name to which this source and community string are to be mapped.

Source: source can be any one-off following,

1. Source can be a restricted source can either be a specific hostname (or address) or
2. A subnet - represented as IP/MASK (e.g. 10.10.10.0/255.255.255.0), or IP/BITS (e.g. 10.10.10.0/24), or the IPv6 equivalents. or
3. The word "default" or "localhost". (default will allow access to all)

Community: community string can be specified in several separate directives and the first source/community combination that matches the incoming request will be selected.

Group Configuration:

Maps pairs of Security Model and Security Name to a group name.

Group Name: Maps a security name (in the specified security model) into a named group. Several *group* directives can specify the same group name, allowing a single access setting to apply to several users and/or community strings.

Version: {v1|v2c|usm}

Security Name: The Security Name is from com2sec configuration as shown in above figure.

- All members of one group have the same access rights.
- A user cannot belong to more than one group for each of the three security models.

Access Configuration:

1. Specifies which group has access to which parts of the tree. It Has 8 parameters.

Group Name: maps from a group of users/communities.

2. **Context:** Default context is the empty string "". Keep "none" for version v1/v2c.

3. **Version:** Can be one of: any, v1, v2c or usm. Should be set to match the SNMP version of clients that will connect to this agent.

4. **Level:** Can be one of noauth , auth, or priv.

Note: that community strings are not counted as authentication, so for SNMP v1 and SNMP v2c we specify noauth.

auth (authNoPriv) means that we use both strong authentication

priv (authPriv) means that we use both strong authentication and encryption.

Match: The prefix parameter to access can be either exact or prefix.

Indicates whether context name needs to match exactly or whether only the first part of the context name needs to match.

The default value is exact.

5. **READ, WRITE** and **NOTIFY** specifies the view to be used for GET*, SET and TRAP/INFORM requests (although the NOTIFY view is not currently used by SNMPD).

Indicate which part of the MIB tree has read access, which part of tree has write access, and which part has permission for access to send notifications (i.e., traps or inform requests).

- Note: For SNMP v1 and SNMP v2c clients
Security Level will be noauth , and context will be empty (the “none” string).

View:

It defines a named "view" - a subset of the overall OID tree. The view determines what part of the MIB access is controlled to.

It uses concept of a subtree. A subtree is a node in the MIB tree and all the elements under that node. In other words, all the MIB elements in a subtree have the same common prefix.

View Name:

Maps from Read, Write, Notify. Several *view* directives can be given with the same view name to build up a more complex collection of OIDs.

Type:

Type is either *included* or *excluded*. which can again define a more complex view (e.g by excluding certain sensitive objects from an otherwise accessible subtree).

included - means that the MIB view includes all the elements of the subtree.

excluded - means that the MIB view excludes all the elements of the subtree.

OID:

The OID defining the root of the subtree to add to (or exclude from) the named view.

E.g. .1 or system or .1.3.6.1.2.1.1.

Mask:

It is a list of hex octets (optionally separated by '.' or ':') with the set bits indicating which sub identifiers in the view OID to match against.

Note: Ignore for now.

--SNMPD v3 Configuration --

Engine ID Configuration:

Please refer [SNMPv3 generic parameters](#) section here for more details.

SNMPv3 with the User-based Security Model (USM):

To use the USM based SNMPv3-specific users, we need to create them. So, let's start to create snmp V3 user by using following directives.

User Name: Name for creating user.

Map VACM configuration here i.e. For v3 username is from security name from VACM table.

Security Level: We have 3 types of security levels as following,

- 1 - NoAuth,NoPriv: Does not have any authentication and Privacy protocol.
- 2 - Auth,NoPriv: Have authentication MD5|SHA but not have Privacy protocol.
- 3 - Auth,Priv: Have authentication MD5|SHA and Privacy protocol as AES|DES.

If Auth,NoPriv or Auth,Priv is used need to configure appropriate protocol and passphrase.