

SNMPTRAPD (Simple Network Management Protocol-TRAP)

Simple Network Management Protocol (SNMP) Traps are alert messages sent from a remote SNMP-enabled device to a central collector, the "SNMP manager".

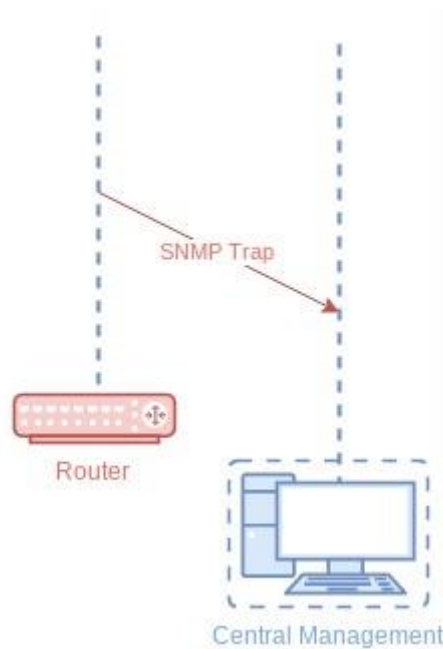


Fig-1: SNMP-TRAP

-- SNMPTRAPD General Settings --

General:

Enable: Enable or Disable the SNMPTRAPD application.

Ignore Authorization Failure: Instructs the receiver to ignore *authentication Failure* traps.

SNMP TRAP Daemon Configuration:

Note: User can configure multiple trap daemon but adding multiple trap daemon lead to multiple notifications.

Version: Select appropriate version.

(For v1 & v2c)

Community: for authorization.

Source: Source field can be used to specify that the configuration should only apply to notifications received from sources

(For v3)

Username: Name for creating user.

Type: Select Trap or Inform.

EngineID: If type is trap then add agent's engineID.

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.

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

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.

Logging Configuration:

Log: Enable/Disable logging.

Logging Location: Specifies where notifications should be logged - to standard output, a specified file or via syslog.

File Path: If Logging Location is specific file then write specific file path so that all logs and notification will be written into that file.

Format1:

Format2:

Specify the format used to display SNMPv1 TRAPs and SNMPv2 notifications respectively. Note that SNMPv2c and SNMPv3 both use the same SNMPv2 PDU format.

Note: If not define format1 and/or format2 then default format provided by net-snmp will be used.

Notifications Processing:

Execute: Pass the details of the trap to a specified handler program.

Execute OID:

Invokes the specified program (with the given arguments) whenever a notification is received that matches the OID token. For SNMPv2c and SNMPv3 notifications, this token will be compared against the snmpTrapOID value taken from the notification. For SNMPv1 traps, the generic and specific trap values and the enterprise OID will be converted into the equivalent OID (following RFC 2576).

Typically, the OID token will be the name (or numeric OID) of a NOTIFICATION-TYPE object, and the specified program will be invoked for notifications that match this OID exactly.

If the OID field is the token “*default*” then the program will be invoked for any notification not matching another (OID specific) *traphandle* entry.

Program: Program name with path specified followed by space separated arguments if any. e.g. /usr/bin/xyz 1 2 3

Net: Forward the trap to another notification receiver.

Note: Do not use this directive for snmp v3 for any security level.

Net OID: Explanation for this Net OID is same as above Execute OID.

Destination: Forwards notifications that match the specified OID to another receiver listening on Destination.