SNMP north plugin

Module description

The PMC/PMP gateway must be monitored via SNMP (Simple Network Management Protocol).

This module must send notifications (traps) related to its operation to the centralized SNMP server.

The system notifications (traps) (CPU, RAM, disk consumption, network, etc...) do not concern this plugin. They will be sent directly by the system SNMP agent to the monitoring tool.

This plugin must use the net-snmp library proposed by the host OS.

The notifications to expect are:

1. Protocol plugin server connection status (offline, in progress, established) (STLNK or STCHA)
2. Protocol plugin client connection status (offline, in progress, established) (STLNK or STCHA)
3. North Protocol plugin service status (stopped, starting, shutting down, running) (STSRV)
4. South Protocol plugin service status (stopped, starting, shutting down, running) (STSRV)
5. Fledge system start (START)
6. Stop the Fledge system (FSTOP)
7. Configuration update (CONCH)
8. Service failure (SRVFL)
9. SNMP v3 authentication failure (SNAUF)
10. INFO event (EVTIF)
11. WARNING event (EVTWA)
12. FATAL event (EVTFA)

The plugin must be able to link audit messages with SNMP traps only by configuration.

Audit Message Reception

The plugin will receive a number of audit messages. These audits represent states, logs or actions reported by the various services. These messages are to be transferred as a trap via the SNMP protocol.

These received audits respect the following description:

Name of the audit message **(SOURCE)**	**Description**	**SEVERITY**	**Variables** **JSON DETAILS**	**Description of the variable**	**Type of the variable**
STLNK (to be created)	State of the protocol link of the north or south services	SUCCESS, FAILURE, WARNING or INFORMATION	nameService	Name of the service sending the notification. (1)	String
			nameLink	Name of the protocol link (name of the PA for example)	String
			valueLink	Link status.	enum : • ON • OFF
STCHA (to be created)	Status of the north or south service protocol channels	SUCCESS, FAILURE, WARNING or INFORMATION	nameService	Name of the service sending the notification. (1)	String
			nameLink	Name of the protocol link	String
			nameChannel	Name of the TCP connection	String
			valueChannel	State of the TCP connection	enum : • ON • OFF
STSRV (to be created)	State of services north or south	SUCCESS, FAILURE, WARNING or INFORMATION	nameService	Name of the service sending the notification. (1)	String
			valueService	State of the service sending the notification. (1)	enum : • stopped • starting • shutting down • running

START	Starting the FLEDGE system	SUCCESS, FAILURE, WARNING or INFORMATION			
FSTOP	Stopping the FLEDGE system	SUCCESS, FAILURE, WARNING or INFORMATION			
CONCH	Configuration update	SUCCESS, FAILURE, WARNING or INFORMATION	nameService	Name of the service sending the notification. (1)	String
SRVFL	Failure of a service (failure to start, crash at runtime...)	SUCCESS, FAILURE, WARNING or INFORMATION	nameService	Name of the service sending the notification. (1)	String
			errorService	Service error in the form of a string	String
SNAUF (to be created)	Authentification failure SNMP v3	SUCCESS, FAILURE, WARNING or INFORMATION			
EVTIF (to be created)	évènement type INFO	SUCCESS, FAILURE, WARNING or INFORMATION	nameService	Name of the service sending the notification. (1)	String
			nameEvent	Name of the event	String
			valueEvent	Description of the event	String
EVTWA (to be created)	évènement type WARNING	SUCCESS, FAILURE, WARNING or INFORMATION	nameService	Name of the service sending the notification. (1)	String
			nameEvent	Name of the event	String
			valueEvent	Description of the event	String
EVTFA (to be created)	évènement type FATAL	SUCCESS, FAILURE, WARNING or INFORMATION	nameService	Name of the service sending the notification. (1)	String
			nameEvent	Name of the event	String
			valueEvent	Description of the event	String

(1) "nameService" the name of the service must show :

- The name of the service type (north or south)
- The instance name of the service
- The name of the protocol

Sending messages via SNMP

All the audits are converted and transferred as a trap to the SNMP server.

The definition of the trap event is as follows:

SNMP trap name	Variable Objet	Description variable objet
Evt (OID)	nameGateway (OID)	Name of the gateway (hostname)
	nameService (OID)	Name of the service
	nameEvent (OID)	Name of the event. Take the name of the audit.
	labelVariable (OID)	Label of the variable
	valueVariable (OID)	Event value (log description, connection status, service status ...)
	severity (OID)	Severity of the audit
	date (OID)	Date of receipt of the audit

Common fields for all traps:

- nameGateway = hostname of the gateway
- date
- severity

Correspondence with audit variables

Name of the audit message	Variables Audit	SNMP trap variable name
STLNK	nameService	nameService
		nameEvent="stateLink"
	nameLink	labelVariable
	valueLink	valueVariable
STCHA	nameService	nameService
		nameEvent="stateChannel"
	nameLink - nameChannel	labelVariable
	valueChannel	valueVariable
STSRV	nameService	nameService
		nameEvent="stateService"
		labelVariable="State of the service"
	valueService	valueVariable
START		nameService= nameGateway
		nameEvent="START"
		labelVariable="State of the gateway"
		valueVariable="ON"
FSTOP		nameService=nameGateway
		nameEvent="FSTOP"
		labelVariable="State of the gateway"
		valueVariable="OFF"
CONCH	nameService	nameService
		nameEvent="CONCH "
		labelVariable=”Configuration”
		valueVariable="UPDATE"
SRVFL	nameService	nameService
		nameEvent="SRVFL "
		labelVariable="Service ERROR"
	errorService	valueVariable
SNAUF		nameService
		nameEvent="SNMPAuthenficationFailure "
		labelVariable="Authentification"
		valueVariable="Failure"
EVTIF	nameService	nameService
		nameEvent="eventinfo "
	nameEvent	labelVariable
	valueEvent	valueVariable
EVTWA	nameService	nameService
		nameEvent="eventwarning "
	nameEvent	labelVariable
	valueEvent	valueVariable

EVTFA	nameService	nameService
		nameEvent="eventfatal "
	nameEvent	labelVariable
	valueEvent	valueVariable

Configuration

The configuration of the plugin allows the link between the audit variables and the SNMP trap objects.

Attributes definition

Attribute	Description	Expected values	Mandatory
oid	OID of the trap or OID of the objects include in the trap	texte value respecting OID format	Yes
"1".."7"	Order index number of the objects include in the trap	"1" to "7"	Yes
dest	name of the object in the trap	string	Yes
origin	origin of the data	"audit", "env", "static"	Yes
value	Value of the data	• audit : data retrieved from the audit message • env : data retrieved from environment variable • static : data entered statically in the configuration	Yes

Configuration :

```
{
   "link_audit_trap": {
      "description":"Correspondence between audit and trap",
      "type":"json",
      "default":"",
      "order":"1",
      "displayName":"Link audit trap"
   }
}
```

The content of the config.json file will be the default value of the link_audit_trap parameter.

Example for an audit :

```
{ "stateLink " : {
        "oid" : "1.3.6.1.4.1.39059.1.1.1.1",
        "1" : {
            "oid" :"1.3.6.1.4.1.39059.1.1.1.1.1",
            "dest": "nameGateway",
            "origin" : "env",
            "value":"hostname"
        }
        "2" : {
            "oid" :"1.3.6.1.4.1.39059.1.1.1.1.2",
            "dest": "nameService",
            "origin" : "audit",
            "value":"detail.nameService"
        },
        "3" : {
            "oid" :"1.3.6.1.4.1.39059.1.1.1.1.3",
            "dest": "nameEvent",
            "origin" : "audit",
            "value":"source"
        },
        "4" : {
            "oid" :"1.3.6.1.4.1.39059.1.1.1.1.4",
            "dest": "libelleVariable",
            "origin" : "audit",
            "value":"detail.nameLink"
        },
        "5" : {
            "oid" :"1.3.6.1.4.1.39059.1.1.1.1.5",
            "dest": "valueVariable",
            "origin" : "audit",
            "value":"detail.valueLink"
        },
        "6" : {
            "oid" :"1.3.6.1.4.1.39059.1.1.1.1.6",
            "dest": "severity",
            "origin" : "audit",
            "value":"severity"
        },
        "7" : {
            "oid" :"1.3.6.1.4.1.39059.1.1.1.1.7",
            "dest": "date",
            "origin" : "audit",
            "value":"timestamp"
        }
    }
}
```

The MIB to load on the SNMP server is PMC-MIB.txt.