SNMP (All-in-One) cloudkod.com

Simple Network Management Protocol (SNMP)

Terminology	Description	UDP port	Configured with
SNMP Manager NMS	Server that runs the SNMP polling software Also called Network Management Server (NMS)	-	-
SNMP Agent	Device that sends SNMP info to NMS	-	-
MIB	Management Information Base (MIB) Structure of objects holding information about the device	-	-
SNMP GET	A NMS directly requests information from an SNMP Agent (read-only) NMS can only poll on specific intervals, so information might be lost	161	snmp-server community … ro
SNMP SET	Allows an NMS to make changes to the device configuration (read/write)	161	snmp-server community … rw
SNMP TRAP (default)	Unacknowledged sent from Agent to NMS Traps are sent when an event occurs and not on a polling interval	162	snmp-server host …. traps
SNMP INFORM	Acknowledged sent from Agent to NMS Informs are sent when an event occurs and not on a polling interval	162	snmp-server host …. informs

SNMP Communities / Users & Groups

- Both v1 and v2 groups are created when configuring a SNMP community
  - The default read view is v1default
  - The default write view is v1default
- Disable the v1 group with the **no snmp-server group public v1** command
- Also disable the Interim Local Management Interface (ILMI) SNMP groups
- The ILMI community itself cannot be deleted
- SNMP community is basically a combination of a username and password
- SNMP users and groups are not only a v3 concept, a combination of the two is basically the same as a community
- It is possible to configure SNMP users/groups for v1 and v2c

SNMP Host

- Only SNMP Traps will be sent to the host, unless you specify the **inform** keyword
- SNMP v1 is the default when not specifying a version

SNMPv3

- The SNMP group security level is a minimum allowed security level
- The actual security level for the user is defined in the **snmp-server** user command.
  - This is the minimum security level for that specific user
- Other users may still connect using the minimum allowed group security level

SNMP Engine-ID

- SNMPv3 user passwords are hashed based on the value of the local Engine-ID
- If the Engine-ID changes, the security digests of SNMPv3 users will be invalid, and the users will have to be reconfigured
- Trailing zeroes will be added automatically to create 24 characters when changing the Engine-ID

Which SNMP versions does Junos OS support?

Junos OS supports SNMP version 1 (SNMPv1), version 2 (SNMPv2c), and version 3 (SNMPv3). By default, SNMP is disabled on a Juniper Networks device.

Which ports (sockets) does SNMP use?

The default port for SNMP queries is port 161. The default port for SNMP traps and informs is port 162.

Does Junos OS support the user-based security model (USM)?

Yes, Junos OS supports USM as part of its support for SNMPv3. SNMPv3 contains more security measures than previous versions of SNMP, including providing a defined USM. SNMPv3 USM provides message security through data integrity, data origin authentication, message replay protection, and protection against disclosure of the message payload.

Does Junos OS support the view-based access control model (VACM)?

Yes, Junos OS supports VACM as part of its support for SNMPv3. SNMPv3 contains more security measures than previous versions of SNMP, including providing a defined VACM. SNMPv3 VACM determines whether a specific type of access (read or write) to the management information is allowed.

Does Junos OS support SNMP informs?

Yes, Junos OS supports SNMP informs as part of its support for SNMPv3. SNMP informs are confirmed notifications sent from SNMP agents to SNMP managers when significant events occur on a network device. When an SNMP manager receives an inform, it sends a response to the sender to verify receipt of the inform.

Can I provision or configure a device using SNMP on Junos OS?

No, provisioning or configuring a device using SNMP is not allowed on Junos OS.

What is a MIB?

A management information base (MIB) is a table of definitions for managed objects in a network device. MIBs are used by SNMP to maintain standard definitions of all of the components and their operating conditions within a network device. Each object in the MIB has an identifying code called an object identifier (OID).

Can the Junos OS be configured for SNMPv1 and SNMPv3 simultaneously?

Yes, SNMP has backward compatibility, meaning that all three versions can be enabled simultaneously.

Can I filter specific SNMP queries on a device?

Yes, you can filter specific SNMP queries on a device using exclude and include statements.

Does SNMP open dynamic UDP ports? Why?

The SNMP process opens two additional ports (sockets): one for IPv4 and one for IPv6. This enables the SNMP process to send traps.

With Junos, you will need to create your user, create your security-group, set the security-model, assign a user and once you have the group created and confirmed you will be able to set the privileges for each of the groups by assigned the MIB views

SECURITY MODEL LEVELS	SECURITY LEVEL	MIB VIEWS
ANY — *ANY SECURITY MODEL* **USM** — *SNMPV3 SECURITY MODEL* **V1** — *SNMPV1 SECURITY MODEL* **V2C** — *SNMPV2C SECURITY MODEL*	**None** — *Provides no authentication and no encryption.* **Authentication** — *Provides authentication but no encryption.* **Privacy** — *Provides authentication and encryption.*	**Notify-view** – *group user is inform of MIB updates* **Read-view** – *the group user can see the MIB updates* **Write-view** – *the group user can make changes to the MIB updates.*

CLI Quick Configuration – v1/2

```
set snmp name “snmp qfabric” description “qfabric0 switch”
set snmp location “Lab 4 Row 11” contact “qfabric-admin@qfabric0”
set snmp community public authorization read-only
set snmp client-list list0 192.168.0.0/24
set snmp community public client-list-name list0
set snmp community public clients 192.170.0.0/24 restrict
set snmp trap-group “qf-traps” destination-port 155 targets 192.168.0.100
```

Minimum SNMPv3 Configuration on a Device Running Junos OS

```
[edit snmp]
view view-name {
oid object-identifier (include | exclude);
}
[edit snmp v3]
notify name {
tag tag-name;
}
notify-filter profile-name {
oid object-identifier (include | exclude);
}
snmp-community community-index {
security-name security-name;
}
target-address target-address-name {
address address;
target-parameters target-parameters-name;
}
target-parameters target-parameters-name {
notify-filter profile-name;
parameters {
message-processing-model (v1 | v2c | v3);
security-level (authentication | none | privacy);
security-model (usm | v1 | v2c);
security-name security-name;
}
}
usm {
local-engine {
user username {
}
vacm {
access {
group group-name {
(default-context-prefix | context-prefix context-prefix){
security-model (any | usm | v1 | v2c) {
security-level (authentication | none | privacy) {
notify-view view-name;
read-view view-name;
write-view view-name;
}
}
security-to-group {
security-model (usm | v1 | v2c) {
security-name security-name {
group group-name;
}
```

JNCIE WORKBOOK EXAMPLE:

SNMP Configuration

In this task you will configure SNMP v3 for secure NMS interactions.

1) Configure SNMP v3 view parameters according to Table 4.

Table 4

Parameter	Value
USM user name	S1
USM user authentication	MD5
USM user authentication password	workbook
VACM security model	usm
VACM user	S1
VACM security level	authentication
VACM read view OID	.1

2) Configure SNMP v3 notification parameters according to Table 5.

Table 5

Parameter	Value
Target address	S1 server IP address
Target processing model	v3
Target security model	usm
Target security level	authentication
Target security name	S1
Notification OID filter	snmpTraps, jnxTraps
Notification type	trap

TABLE:4 Config

- Configure local SNMP engine user with the required authentication that NMS system will use to access the device.

```
[edit snmp v3]
+ usm {
+    local-engine {
+       user S1 {
+          authentication-md5 {
+             authentication-key "$9$mP36AtOBRh.P1RhSMWLxNdgoJZjfQFNd5Qz39CxN-
V4aZGiHmfiHCtuOREgoaUk.P5Q6CtPfSrvMN-YgoGk.n/Cu0ICA"; ## SECRET-DATA
```

- Define the SNMP view that user is allowed to access . Global SNMP Config.

```
[edit snmp]
+ view global-info {
+    oid .1 include;
```

- Configure the VACM access parameters, map group for security model USM with security level authentication to the view named 'global-info'. Below, group name is 'global'.
- Configure VACM security to group mapping. Bind user S1 to the group global.

```
[edit snmp v3]
+ vacm {
+    security-to-group {
+       security-model usm {
+          security-name S1 {
+             group global;
```

```
+    }
+    access {
+       group global {
+          default-context-prefix {
+             security-model usm {
+                security-level authentication {
+                   read-view global-info;
+                }
```

TABLE:5 Config

- Configure the trap notification with a tag that will be used to bind the notification to trap receiver. In below example, notification name is NMS.
- Configure trap receiver target parameters.

```
[edit snmp v3]
+  target-address S1 {
+     address 10.10.10.1;
+     tag-list trap-receiver;
+     target-parameters S1-parameters;
+  }
+  target-parameters S1-parameters {
+     parameters {
+        message-processing-model v3;
+        security-model usm;
+        security-level authentication;
+        security-name S1;
+     }
+  notify NMS {
+     type trap;
+     tag trap-receiver;
+  }
+  notify-filter specific-traps {
+     oid snmpTraps include;
+     oid jnxTraps include;
+  }
```

```
root@Core1> show snmp v3 access
Access control:
Group           Context Security     Read      Write     Notify
                prefix  model/level  view      view      view
global                  usm/authent  global-inf

root@Core1> show snmp v3 users
Engine ID: local
  User                  Auth/Priv  Storage     Status
  S1                    md5/none   nonvolatile  active
root@Core1> show snmp v3 groups
Group name       Security  Security         Storage     Status
                 model     name             type
global           usm       S1               nonvolatile  active

root@Core1> show snmp v3 notify
SNMP Notify:
Notify           Tag            Type       Storage     Status
name                                       type
NMS              trap-receiver  trap       nonvolatile  active
root@Core1> show snmp v3 target
SNMP Target:
Address    Address              Port  Parameters  Storage    Status
name                            name      type
S1         10.10.10.1           162   S1-paramete nonvolatile active

Parameters    Security      Security    Notify  Storage     Status
name          name          model/level  filter  type
S1-parameters  S1           usm/authent        nonvolatile  active
```