



User interaction and design

The Net-SNMP application will be included in the appliance image. It will be disabled by default, requiring users to manually opt-in before using. The default SNMP configuration is located at `/etc/snmp/snmpd.conf`.

By default, SNMP will be configured with the following:

- Support for walking over UDP (ipv4 and ipv6)
- Default OIDS enabled
 - System Information: [.1.3.6.1.2.1.1](#)
 - Interfaces: [.1.3.6.1.2.1.2](#)
 - IPv4 Forwarding: [.1.3.6.1.2.1.4.1.0](#)
 - IPv6 Forwarding: [.1.3.6.1.2.1.4.25.0](#)
 - IP: [.1.3.6.1.2.1.4.34](#)
 - Host Resources: [.1.3.6.1.2.1.25.1](#)
 - ifXTable: [.1.3.6.1.2.1.31.1.1](#)
 - Memory Stats: [.1.3.6.1.4.1.2021.4](#)
 - Disk Stats: [.1.3.6.1.4.1.2021.9](#)
 - CPU Stats: [.1.3.6.1.4.1.2021.11](#)
- Version 2c enabled with default community of *public*
- Version 3 enabled with the following
 - Readonly User: *admin*
 - Password: *changeme*
 - Auth Protocol: *SHA*
 - Privacy Protocol: *AES*
 - Privacy Pass: *changeme*
- The following system information has been defined by default
 - sysDescr: LiveNX Server or LiveNX Node (depending on install)
 - sysObjectID: [.1.3.6.1.4.1.35874.2.1](#)
 - sysContact: LiveAction Support <<https://www.liveaction.com/support/technical-support/>>
 - sysLocation: Data center
 - sysServices: 72

You can walk the current default OIDS by using snmpwalk:

```
SNMP V2C
admin:~$ snmpwalk -v 2c -c public 192.168.121.163 -CE .1.3.6.1.4.1.2021.12

SNMP V3
admin:~$ snmpwalk -v 3 -l authPriv -u admin -a SHA -A changeme -x AES -X
changeme 192.168.121.163
```

Enable SNMP

The SNMP daemon can be enabled by performing the following:

```
admin@livenx:~$ sudo systemctl enable snmpd
Synchronizing state of snmpd.service with SysV service script with /lib/
systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable snmpd
admin@livenx:~$ sudo systemctl start snmpd
```

The status of SNMP can be checked by performing the following:

```
admin@livenx:~$ 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 Wed 2020-03-11 18:21:06 UTC; 4s ago
     Process: 20570 ExecStartPre=/bin/mkdir -p /var/run/agentx (code=exited,
  status=0/SUCCESS)
    Main PID: 20571 (snmpd)
       Tasks: 1 (limit: 4653)
      CGroup: /system.slice/snmpd.service
             └─20571 /usr/sbin/snmpd -Lsd -Lf /dev/null -u Debian-snmp -g
  Debian-snmp -I -smux mteTrigger mteTriggerConf -f

Mar 11 18:21:06 livenx systemd[1]: Starting Simple Network Management
  Protocol (SNMP) Daemon....
Mar 11 18:21:06 livenx systemd[1]: Started Simple Network Management Protocol
  (SNMP) Daemon..
Mar 11 18:21:06 livenx snmpd[20571]: Created directory: /var/lib/snmp/
  mib_indexes
Mar 11 18:21:06 livenx snmpd[20571]: Turning on AgentX master support.
Mar 11 18:21:06 livenx snmpd[20571]: Created directory: /var/agentx
Mar 11 18:21:06 livenx snmpd[20571]: NET-SNMP version 5.7.3
```

Change SNMP v3 admin password

1. Stop the SNMP daemon.


```
admin@livenx:~$ sudo systemctl stop snmpd
```
2. Add the following to `/var/lib/snmp/snmpd.conf`. Please update **passphrase1** and **passphrase2** with desired passphrases.


```
createUser admin SHA "passphrase1" AES passphrase2
```
3. Start the SNMP daemon.


```
admin@livenx:~$ sudo systemctl start snmpd
```

Change SNMP v2 community

1. Edit `/etc/snmp/snmpd.conf` as `sudo`. Change the term `public` to the desired community name.
2.


```
rocommunity public default -V systemonly
rocommunity6 public default -V systemonly
```
3. Restart the SNMP daemon.

```
admin@livenx:~$ sudo systemctl restart snmpd
```

Disable SNMP v2


1. Edit `/etc/snmp/snmpd.conf` as `sudo`. Comment out `rocommunity` and `rocommunity6` entries.
2. # Default access to basic system info
3.



```
#rocommunity public default -V systemonly
#rocommunity6 public default -V systemonly
```
4. Restart the SNMP daemon.




























```
admin@livenx:~$ sudo systemctl restart snmpd
```

Control SNMP through LiveNX Admin

The SNMP daemon has been added to the LiveNX Admin services view:

 Service Details

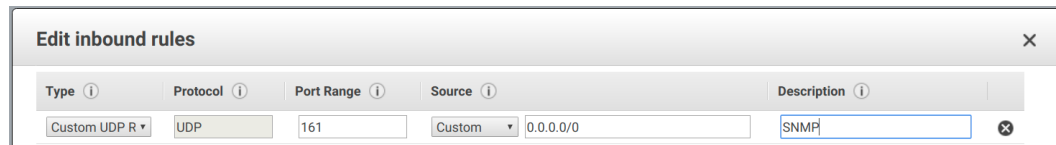
 Refresh

Service	CPU	Memory	PID	Commands
influxdb	0.1 %	0.7 %	1847	  
livenx-server	2.0 %	51.8 %	1873	  
livenx-web	0.2 %	2.3 %	1881	  
mongod	0.3 %	2.0 %	1937	  
samplicator@anyconnect	NA	NA	NA	  
samplicator@netflow	NA	NA	NA	  
samplicator@sflow	NA	NA	NA	  
snmpd	0.1 %	0.2 %	31744	  
ssh	0.0 %	0.1 %	1888	  

Cloud

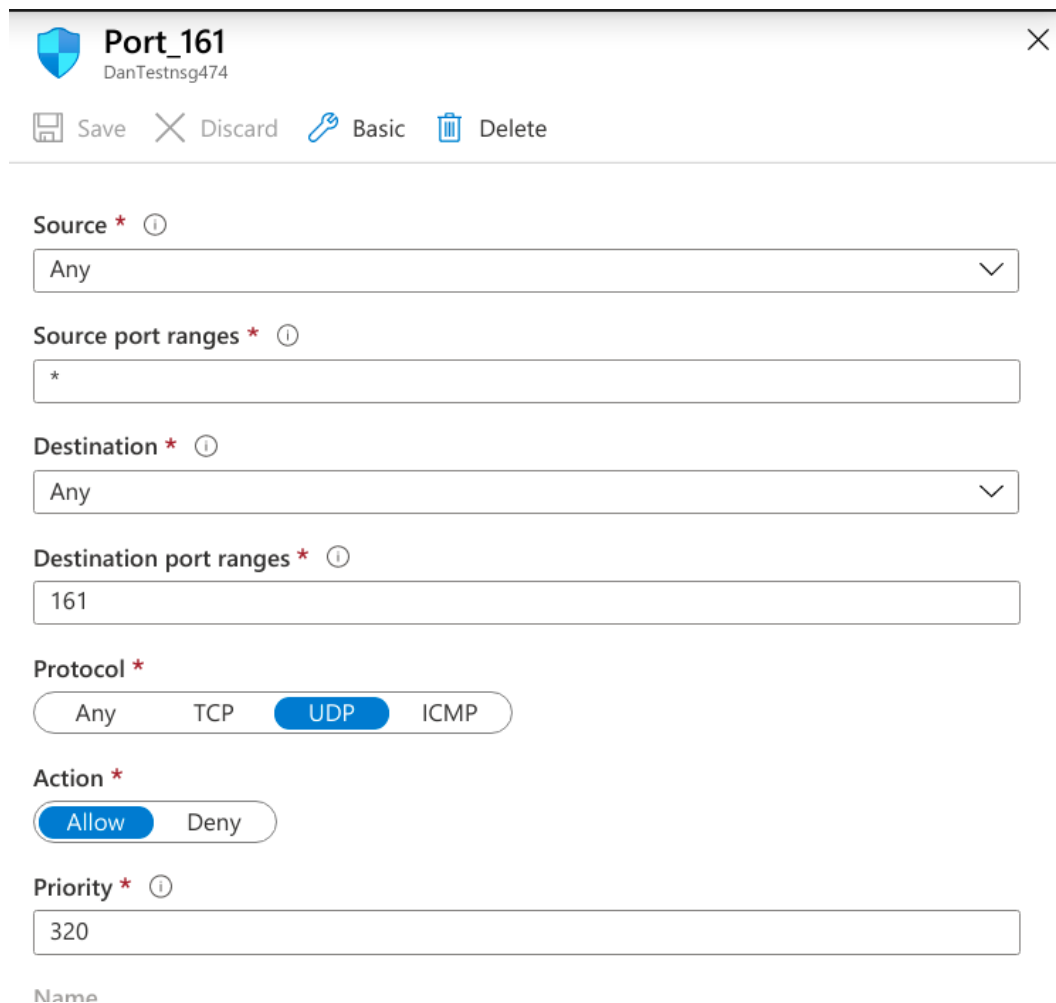
If SNMP needs to be monitored for cloud deployments, the previous steps for enabling/disabling the service still apply. In addition, you will need to open a network port for **161: UDP** bound traffic to be able to successfully monitor the device.

AWS



Type	Protocol	Port Range	Source	Description
Custom UDP R	UDP	161	Custom 0.0.0.0/0	SNMP

Azure



Port_161
DanTestnsg474

Save Discard Basic Delete

Source * ⓘ
Any

Source port ranges * ⓘ
*

Destination * ⓘ
Any

Destination port ranges * ⓘ
161

Protocol *
Any TCP **UDP** ICMP

Action *
Allow Deny

Priority * ⓘ
320

Name