Table Of Contents

Home > Faq > CentOS

Snmpd Listen to Specific IP Address (BIND To Selected Interfaces)

Posted by Vivek Gite <vivek@nixcraft.com>

How do I force SNMP (Simple Network Management Protocol) network management software to listen on public interfaces under RHEL / RedHat / Fedora / CentOS Linux server?

net-snmp comes with snmpd server which is an SNMP agent which binds to a port and awaits requests from SNMP management software. By default it binds to localhost (127.0.0.1) only.

snmpd can be configured to listens for incoming SNMP requests on UDP port 161 on all IPv4 interfaces or selected interface using the -x option. A listening address takes the form:

[1]

[2]

```
[<transport-specifier>:]<transport-address>
```

Few Examples

```
    127.0.0.1:161            listen on UDP port 161, but only on the loopback interface.
                             port specification ":161" is not strictly necessary since th

    TCP:1161                 listen on TCP port 1161 on all IPv4 interfaces.

    ipx:/40000               listen on IPX port 40000 on all IPX interfaces.

    unix:/tmp/local-agent    listen on the Unix domain socket /tmp/local-agent.

    /tmp/local-agent         is  identical  to  the  previous  specification, since the U
  is '/'.

    PVC:161                  listen on the AAL5 permanent virtual circuit with VPI=0 and
                             machine.

    udp6:10161               listen on port 10161 on all IPv6 interfaces.
```

CentOS / RHEL / Fedora Linux Specific Configuration

Edit /etc/sysconfig/snmpd.options, enter:

[3]

```
# vi /etc/sysconfig/snmpd.options
```

Uncomment OPTIONS line. Add -x option as follows to listen on default port 161 and IP 127.0.0.1 and 192.168.1.254

```
OPTIONS="-Lsd -Lf /dev/null -p /var/run/snmpd.pid -a -x 127.0.0.1 192.168.1.254"
```

Save and close the file. Reload the changes:
```
# service snmpd reload
```

Update /etc/sysconfig/iptables firewall configuration to allow communication at udp port 161:
```
# vi /etc/sysconfig/iptables
```

Only accept connection only from 192.168.1.0/24 to UDP port 161, enter:

```
-A RH-Firewall-1-INPUT -p udp s 192.168.1.0/24 -m udp --dport 161 -j ACCEPT
```

Finally, restart iptables service [4]:

```
# service iptables restart
```

You may also need to update your /etc/snmp/snmpd.conf to setup correct public community and other ACL settings. Refer snmpd.conf man page for more details.

4000+ howtos and counting! Want to read more Linux / UNIX howtos, tips and tricks? Subscribe to our daily email newsletter or weekly newsletter to make sure you don't miss a single tip/tricks. Alternatively, subscribe via RSS/XML feed.

Article printed from Frequently Asked Questions About Linux / UNIX: **http://www.cyberciti.biz/faq/**

URL to article: **http://www.cyberciti.biz/faq/linux-unix-bind-snmpd-to-specific-ip-address-interfaces/**

URLs in this post:

[1] Image: **http://www.cyberciti.biz/faq/category/networking/**
[2] Image: **http://www.cyberciti.biz/faq/category/centos/**
[3] Image: **http://www.cyberciti.biz/faq/category/redhat-and-friends/**
[4] restart iptables service: **http://www.cyberciti.biz/faq/howto-rhel-linux-open-port-using-iptables/**