SNMP Trap - Inbound UDP Traffic

Inbound TCP Traffic

These steps explain how to confirm that the Nagios server is receiving SNMP Trap traffic destined for it on the UDP port 162.

In this example, the following applies:

- Remote computer sending SNMP Traps
  - 10.25.5.20
- Nagios server receiving SNMP Traps
  - 10.25.5.30

The purpose of this test is to confirm that the network traffic is hitting the Nagios XI server. TCP dump displays the lower level of network traffic before it is intercepted by the Operating System (OS) firewall rules. The OS firewall rules are not evaluated yet and hence this test allows you to clearly determine if this traffic is hitting the Nagios XI server.

If your tests show that no traffic is being received then there must be other firewall(s) between the sending device and the Nagios XI server that are blocking the traffic.

Install / Update tcpdump

Establish an SSH session to the Nagios server that receives SNMP Traps. Execute the following command to install the tcpdump program, depending on your OS:

**RHEL | CentOS | Oracle Linux**

```bash
yum -y install tcpdump
```

**Debian | Ubuntu**

```bash
apt-get install -y tcpdump
```

Wait while tcpdump is installed/updated.

Watch TCP Traffic - Reverse DNS Lookup

Execute the following command:

```bash
tcpdump src host 10.25.5.20 and udp dst port 162 and dst host 10.25.5.30
```

When an SNMP Trap is received it should produce output like:

```
10:57:34.879662 IP snmpsender.domain.local.40410 > snmpreceiver.domain.local.snmptrap:  V2Trap(180)  ... E:20006.1.3.1.6="Users" E:20006.1.3.1.7=0 E:20006.1.3.1.17="USERS OK - 0 users currently logged in"
```

When you have finished watching the network traffic press **CTRL + C** to kill tcpdump.

Watch TCP Traffic - NO Reverse DNS Lookup

Execute the following command:

```bash
tcpdump -n src host 10.25.5.20 and udp dst port 162 and dst host 10.25.5.30
```

When an SNMP Trap is received it should produce output like:

```
10:59:17.614465 IP 10.25.5.20.43471 > 10.25.5.30.snmptrap:  V2Trap(185)  .1.3.6.1.2.1.1.3.0=155084 ... .1.3.6.1.4.1.20006.1.3.1.7=1 .1.3.6.1.4.1.20006.1.3.1.17="USERS WARNING - 1 users currently logged in"
```

When you have finished watching the network traffic press **CTRL + C** to kill tcpdump.

Troubleshooting

If you receive this message when trying to execute tcpdump:

```
tcpdump: NFLOG link-layer type filtering not implemented
```

Then you will need to define the interface name with the **-i** argument, for example:

```bash
tcpdump -i ens32 src host 10.25.5.20 and udp dst port 162 and dst host 10.25.5.30
```
Conclusion

With these steps you will be able to confirm that the Nagios server is correctly receiving SNMP Trap UDP traffic on port 162 from a remote server.

Your next troubleshooting step would be to confirm the **firewall rules** are in place.

Final Thoughts

For any support related questions please visit the Nagios Support Forums at:

http://support.nagios.com/forum/

Posted by: tlea - Tue, Mar 24, 2015 at 7:52 PM. This article has been viewed 4184 times.

Online URL: https://support.nagios.com/kb/article/snmp-trap-inbound-udp-traffic-86.html