How To: Block SNMP port in ScaleArc if it is required to do so?

Arun Sangameswaran - 2016-05-16 - 0 Comments - in ScaleArc Registered User

How To: Block SNMP port in ScaleArc if it is required to do so?

Release	Classification	Level	DB Platforms	Categories

v3.2 and above	How To		ALL	Security

Table of Contents

What are all the default ports used by SNMP?

What are all the likely causes for disabling these ports?

Will Stopping SNMP Service suffice?

How to achieve SNMP port block in ScaleArc?

What are best practices if SNMP is not being used on ScaleArc?

01. What are all the default ports used by SNMP?

SNMP uses the default UDP port 161 for general SNMP messages and UDP port 162 for SNMP trap messages. At this time ScaleArc does not send trap messages, but we will be

implementing it in future versions.

02. What are all the likely causes for disabling these ports?

If SNMP within ScaleArc appliance is not actively been used then it could be blocked for security reasons to avoid SNMP walks on those ports. It can also be blocked from sending

general statistics messages.

03. Will Stopping SNMP Service suffice?

No. Typical stopping of SNMP service (as shown below) will not suffice in this case as ScaleArc's python service "idb_snmp" will restart snmpd as soon as it detects it being

down.

```
service snmpd stop
chkconfig snmpd off
```

thus will not work to stop SNMP for security reasons. The idb_snmp process cannot be

stopped as it is run internally by ScaleArc processes.

04. How to achieve SNMP port block in ScaleArc ?

Add below 4 iptables rules to block any inbound on ports 161 and 162 within ScaleArc appliance, and prevent potential transmission of data on the broadcast address:

```
iptables -A INPUT -p udp -m udp --dport 161:162 -j DROP
iptables -A INPUT -p tcp -m tcp --dport 161:162 -j DROP
iptables -A OUTPUT -p udp -m udp --dport 161:162 -j DROP
iptables -A OUTPUT -p tcp -m tcp --dport 161:162 -j DROP
```

This will prevent all SNMP traffic coming in or out of ScaleArc. These lines should be added to the end of the /etc/sysconfig/iptables file using an ASCII text editor like vi or vim, and

then the iptables service should be restarted:

```
vi /etc/sysconfig/iptables
service iptables restart
```

Below is an example output of nmap identifying port 161 as open (prior to adding above rules to iptables)

```
# nmap -sU --script snmp-brute  172.10.1.1

Starting Nmap 7.12 ( https://nmap.org ) at 2016-05-13 16:05 PDT
Stats: 0:00:17 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 2.96% done; ETC: 16:15 (0:09:51 remaining)
Stats: 0:16:31 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 99.99% done; ETC: 16:22 (0:00:00 remaining)
Nmap scan report for 172.10.1.1
Host is up (0.0025s latency).
Not shown: 994 closed ports
PORT     STATE         SERVICE
69/udp   open|filtered tftp
123/udp  open          ntp
161/udp  open          snmp
| snmp-brute:
|_  public - Valid credentials
1434/udp open|filtered ms-sql-m
1718/udp open|filtered h225gatedisc
1719/udp open|filtered h323gatestat
```

Below is an example output of nmap identifying port 161 as blocked (after adding above rules to iptables)

```
root# nmap -sU --script snmp-brute  172.10.1.1

Starting Nmap 7.12 ( https://nmap.org ) at 2016-05-13 17:16 PDT
Stats: 0:00:02 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 1.73% done; ETC: 17:18 (0:01:53 remaining)
Nmap scan report for 172.10.1.1
Host is up (0.0029s latency).
Not shown: 993 closed ports
PORT     STATE         SERVICE
69/udp   open|filtered tftp
123/udp  open          ntp
161/udp  open|filtered snmp
162/udp  open|filtered snmptrap
1434/udp open|filtered ms-sql-m
1718/udp open|filtered h225gatedisc
1719/udp open|filtered h323gatestat
Nmap done: 1 IP address (1 host up) scanned in 1085.64 seconds
```

What does "open|filtered" mean?

open|filtered

Nmap places ports in this state when it is unable to determine whether a port is open or filtered. This occurs for scan types in which open ports give no response. The lack of response could also mean that a packet filter dropped the probe or any response it elicited. So Nmap does not know for sure whether the port is open or being filtered. The UDP, IP protocol, FIN, NULL, and Xmas scans classify ports this way.

Below is an example output of snmpwalk (prior to adding above rules to iptables)

```
 # snmpwalk -v2c -c public 172.10.1.1 IDB-MIB::systemStatsData
IDB-MIB::sysCpuUsageLoadBalancer.0 = INTEGER: 0 Percentage
IDB-MIB::sysCpuUsageCache.0 = INTEGER: 0 Percentage
IDB-MIB::sysCpuUsageQueries.0 = INTEGER: 0 Percentage
IDB-MIB::sysCpuUsageConnections.0 = INTEGER: 0 Percentage
IDB-MIB::sysBandwidthInbound.0 = INTEGER: 0 Mb
IDB-MIB::sysBandwidthOutbound.0 = INTEGER: 0 Mb
.....
.....
.....
```

Below is an example output of snmpwalk (after adding above rules to iptables)

```
# snmpwalk -v2c -c public 172.10.1.1 IDB-MIB::systemStatsData
Timeout: No Response from 172.10.1.1
```

05. Best Practice

As a best practice, if SNMP is not used with ScaleArc, rules should be added to block any

inbounds or outbounds on the 2 SNMP ports for both protocols as shown above.

If you are experiencing issues with ScaleArc or with any of it's features, please contact ScaleArc Support. We are available 24x7 by phone at 855 800 7225 or +1 408 412 7315.

For general support inquiries, you can also e-mail us at support@scalearc.com.

Permalink:
https://support.scalearc.com/kb/articles/3398

Tags

block

port

snmpd

Related Pages

How to change a default SNMP community name

How to configure ScaleArc SNMP