[구조]

ㅇSNMP매니저(CLIENT)-> SNMP AGENT(서버:snmpd설정)에 질의하여 MIB정보 수집 (UDP 161)

ㅇ서버/스위치TRAP이벤트설정 -> SNMP매니저(snmptrapd설정) (UDP 162)

[root@web1 network-scripts]# yum install net-snmp

[root@web1 network-scripts]# yum install net-snmp-utils

[root@web1 network-scripts]# vi /etc/snmp/snmpd.conf

1. First, map the community name "public" into a "security name"# sec.name source community

#com2sec notConfigUser default public

com2sec choga88 default public

com2sec choga88 192.168.17.0/24 public

2. Second, map the security name into a group name:

# groupName securityModel securityName

group notConfigGroup v1 notConfigUser

group notConfigGroup v2c notConfigUser

group choga88group v1 choga88

group choga88group v2c choga88

3. Third, create a view for us to let the group have rights to:

# Make at least snmpwalk -v 1 localhost -c public system fast again.

# name incl/excl subtree mask(optional)

view systemview included .1.3.6.1.2.1.1

view systemview included .1.3.6.1.2.1.25.1.1

4. Finally, grant the group read-only access to the systemview view.

# group context sec.model sec.level prefix read write notif

access notConfigGroup "" any noauth exact systemview none none

access choga88group "" any noauth exact all all all

[root@web1 network-scripts]# systemctl restart snmpd

[root@web1 network-scripts]# systemctl status snmpd

● snmpd.service - Simple Network Management Protocol (SNMP) Daemon.

Loaded: loaded (/usr/lib/systemd/system/snmpd.service; disabled; vendor preset: disabled)

Active: active (running) since Sat 2018-03-31 07:04:53 GMT; 1s ago

Main PID: 1879 (snmpd)

CGroup: /system.slice/snmpd.service

└─1879 /usr/sbin/snmpd -LS0-6d -f

Mar 31 07:04:53 web1 systemd[1]: Starting Simple Network Management Protocol (SNMP) ......

Mar 31 07:04:53 web1 snmpd[1879]: NET-SNMP version 5.7.2

Mar 31 07:04:53 web1 systemd[1]: Started Simple Network Management Protocol (SNMP) D...n..

Hint: Some lines were ellipsized, use -l to show in full.

[root@web1 network-scripts]# ps -ef | grep snmpd

root 1879 1 0 07:04 ? 00:00:00 /usr/sbin/snmpd -LS0-6d –f

LS:로그메세지, 0-6는 level정의

|  |  |
| --- | --- |
| 1  2  3  4  5  6  7  8 | 0 or ! for LOG\_EMERG,  1 or a for LOG\_ALERT,  2 or c for LOG\_CRIT,  3 or e for LOG\_ERR,  4 or w for LOG\_WARNING,  5 or n for LOG\_NOTICE,  6 or i for LOG\_INFO, and  7 or d for LOG\_DEBUG. |

[root@web1 network-scripts]# netstat -anlp | grep snmp

tcp 0 0 127.0.0.1:199 0.0.0.0:\* LISTEN 1879/snmpd

udp 0 0 0.0.0.0:161 0.0.0.0:\* 1879/snmpd

[root@web1 network-scripts]# snmpwalk -v 2c -c public localhost system

SNMPv2-MIB::sysDescr.0 = STRING: Linux web1 3.10.0-693.17.1.el7.x86\_64 #1 SMP Thu Jan 25 20:13:58 UTC 2018 x86\_64

SNMPv2-MIB::sysObjectID.0 = OID: NET-SNMP-MIB::netSnmpAgentOIDs.10

DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (71693) 0:11:56.93

SNMPv2-MIB::sysContact.0 = STRING: Root <root@localhost> (configure /etc/snmp/snmp.local.conf)

SNMPv2-MIB::sysName.0 = STRING: web1

SNMPv2-MIB::sysLocation.0 = STRING: Unknown (edit /etc/snmp/snmpd.conf)

SNMPv2-MIB::sysORLastChange.0 = Timeticks: (3) 0:00:00.03

SNMPv2-MIB::sysORID.1 = OID: SNMP-MPD-MIB::snmpMPDCompliance

SNMPv2-MIB::sysORID.2 = OID: SNMP-USER-BASED-SM-MIB::usmMIBCompliance

SNMPv2-MIB::sysORID.3 = OID: SNMP-FRAMEWORK-MIB::snmpFrameworkMIBCompliance

SNMPv2-MIB::sysORID.4 = OID: SNMPv2-MIB::snmpMIB

SNMPv2-MIB::sysORID.5 = OID: TCP-MIB::tcpMIB

SNMPv2-MIB::sysORID.6 = OID: IP-MIB::ip

SNMPv2-MIB::sysORID.7 = OID: UDP-MIB::udpMIB

SNMPv2-MIB::sysORID.8 = OID: SNMP-VIEW-BASED-ACM-MIB::vacmBasicGroup

SNMPv2-MIB::sysORID.9 = OID: SNMP-NOTIFICATION-MIB::snmpNotifyFullCompliance

SNMPv2-MIB::sysORID.10 = OID: NOTIFICATION-LOG-MIB::notificationLogMIB

SNMPv2-MIB::sysORDescr.1 = STRING: The MIB for Message Processing and Dispatching.

SNMPv2-MIB::sysORDescr.2 = STRING: The management information definitions for the SNMP User-based Security Model.

SNMPv2-MIB::sysORDescr.3 = STRING: The SNMP Management Architecture MIB.

SNMPv2-MIB::sysORDescr.4 = STRING: The MIB module for SNMPv2 entities

SNMPv2-MIB::sysORDescr.5 = STRING: The MIB module for managing TCP implementations

SNMPv2-MIB::sysORDescr.6 = STRING: The MIB module for managing IP and ICMP implementations

SNMPv2-MIB::sysORDescr.7 = STRING: The MIB module for managing UDP implementations

SNMPv2-MIB::sysORDescr.8 = STRING: View-based Access Control Model for SNMP.

SNMPv2-MIB::sysORDescr.9 = STRING: The MIB modules for managing SNMP Notification, plus filtering.

SNMPv2-MIB::sysORDescr.10 = STRING: The MIB module for logging SNMP Notifications.

SNMPv2-MIB::sysORUpTime.1 = Timeticks: (3) 0:00:00.03

SNMPv2-MIB::sysORUpTime.2 = Timeticks: (3) 0:00:00.03

SNMPv2-MIB::sysORUpTime.3 = Timeticks: (3) 0:00:00.03

SNMPv2-MIB::sysORUpTime.4 = Timeticks: (3) 0:00:00.03

SNMPv2-MIB::sysORUpTime.5 = Timeticks: (3) 0:00:00.03

SNMPv2-MIB::sysORUpTime.6 = Timeticks: (3) 0:00:00.03

SNMPv2-MIB::sysORUpTime.7 = Timeticks: (3) 0:00:00.03

SNMPv2-MIB::sysORUpTime.8 = Timeticks: (3) 0:00:00.03

SNMPv2-MIB::sysORUpTime.9 = Timeticks: (3) 0:00:00.03

SNMPv2-MIB::sysORUpTime.10 = Timeticks: (3) 0:00:00.03

[root@db1 ~]# snmpwalk -v 2c -c public 192.168.17.203 system -> 다른시스템에서 접근

SNMPv2-MIB::sysDescr.0 = STRING: Linux web1 3.10.0-693.17.1.el7.x86\_64 #1 SMP Thu Jan 25 20:13:58 UTC 2018 x86\_64

SNMPv2-MIB::sysObjectID.0 = OID: NET-SNMP-MIB::netSnmpAgentOIDs.10

DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (79816) 0:13:18.16

SNMPv2-MIB::sysContact.0 = STRING: Root <root@localhost> (configure /etc/snmp/snmp.local.conf)

SNMPv2-MIB::sysName.0 = STRING: web1

SNMPv2-MIB::sysLocation.0 = STRING: Unknown (edit /etc/snmp/snmpd.conf)

SNMPv2-MIB::sysORLastChange.0 = Timeticks: (3) 0:00:00.03

SNMPv2-MIB::sysORID.1 = OID: SNMP-MPD-MIB::snmpMPDCompliance

SNMPv2-MIB::sysORID.2 = OID: SNMP-USER-BASED-SM-MIB::usmMIBCompliance

SNMPv2-MIB::sysORID.3 = OID: SNMP-FRAMEWORK-MIB::snmpFrameworkMIBCompliance

SNMPv2-MIB::sysORID.4 = OID: SNMPv2-MIB::snmpMIB

SNMPv2-MIB::sysORID.5 = OID: TCP-MIB::tcpMIB

SNMPv2-MIB::sysORID.6 = OID: IP-MIB::ip

SNMPv2-MIB::sysORID.7 = OID: UDP-MIB::udpMIB

SNMPv2-MIB::sysORID.8 = OID: SNMP-VIEW-BASED-ACM-MIB::vacmBasicGroup

SNMPv2-MIB::sysORID.9 = OID: SNMP-NOTIFICATION-MIB::snmpNotifyFullCompliance

SNMPv2-MIB::sysORID.10 = OID: NOTIFICATION-LOG-MIB::notificationLogMIB

SNMPv2-MIB::sysORDescr.1 = STRING: The MIB for Message Processing and Dispatching.

SNMPv2-MIB::sysORDescr.2 = STRING: The management information definitions for the SNMP User-based Security Model.

SNMPv2-MIB::sysORDescr.3 = STRING: The SNMP Management Architecture MIB.

SNMPv2-MIB::sysORDescr.4 = STRING: The MIB module for SNMPv2 entities

SNMPv2-MIB::sysORDescr.5 = STRING: The MIB module for managing TCP implementations

SNMPv2-MIB::sysORDescr.6 = STRING: The MIB module for managing IP and ICMP implementations

SNMPv2-MIB::sysORDescr.7 = STRING: The MIB module for managing UDP implementations

SNMPv2-MIB::sysORDescr.8 = STRING: View-based Access Control Model for SNMP.

SNMPv2-MIB::sysORDescr.9 = STRING: The MIB modules for managing SNMP Notification, plus filtering.

SNMPv2-MIB::sysORDescr.10 = STRING: The MIB module for logging SNMP Notifications.

SNMPv2-MIB::sysORUpTime.1 = Timeticks: (3) 0:00:00.03

SNMPv2-MIB::sysORUpTime.2 = Timeticks: (3) 0:00:00.03

SNMPv2-MIB::sysORUpTime.3 = Timeticks: (3) 0:00:00.03

SNMPv2-MIB::sysORUpTime.4 = Timeticks: (3) 0:00:00.03

SNMPv2-MIB::sysORUpTime.5 = Timeticks: (3) 0:00:00.03

SNMPv2-MIB::sysORUpTime.6 = Timeticks: (3) 0:00:00.03

SNMPv2-MIB::sysORUpTime.7 = Timeticks: (3) 0:00:00.03

SNMPv2-MIB::sysORUpTime.8 = Timeticks: (3) 0:00:00.03

SNMPv2-MIB::sysORUpTime.9 = Timeticks: (3) 0:00:00.03

SNMPv2-MIB::sysORUpTime.10 = Timeticks: (3) 0:00:00.03

ㅇtrap전송호스트 설정 : /etc/snmp/snmpd.conf에 trap2sink 192.168.17.210 public 추가

NAME

snmptrap, snmpinform - sends an SNMP notification to a manager

SYNOPSIS

snmptrap -v 1 [COMMON OPTIONS] AGENT enterprise-oid agent generic-trap specific-trap uptime [OID TYPE VALUE]...

snmptrap -v [2c|3] [COMMON OPTIONS] [-Ci] AGENT uptime trap-oid [OID TYPE VALUE]...

snmpinform -v [2c|3] [COMMON OPTIONS] AGENT uptime trap-oid [OID TYPE VALUE]...

ㅇ trap수신설정 -> snmptapd 데몬의 /etc/snmptrap/

[root@web1 network-scripts]# cat /etc/snmp/snmptrapd.conf

# Example configuration file for snmptrapd

#

# No traps are handled by default, you must edit this file!

#

# authCommunity log,execute,net public

# traphandle SNMPv2-MIB::coldStart /usr/bin/bin/my\_great\_script cold

authCommunity log,execute,net public

[root@db1 ~]# systemctl start snmptrapd.service

[root@db1 ~]# systemctl status snmptrapd.service

● snmptrapd.service - Simple Network Management Protocol (SNMP) Trap Daemon.

Loaded: loaded (/usr/lib/systemd/system/snmptrapd.service; disabled; vendor preset: disabled)

Active: active (running) since Sat 2018-03-31 08:04:57 GMT; 4s ago

Main PID: 3348 (snmptrapd)

Memory: 3.9M

CGroup: /system.slice/snmptrapd.service

└─3348 /usr/sbin/snmptrapd -Lsd -f

Mar 31 08:04:57 db1 systemd[1]: Starting Simple Network Management Protocol (SNMP......

Mar 31 08:04:57 db1 snmptrapd[3348]: NET-SNMP version 5.7.2

Mar 31 08:04:57 db1 systemd[1]: Started Simple Network Management Protocol (SNMP)...n..

[root@db1 ~]# netstat -anlp | grep snmptrap

udp 0 0 0.0.0.0:162 0.0.0.0:\* 3348/snmptrapd