Enabling SNMP monitoring in the CA API Gateway

Topic This article will prescribe the process of enabling the SNMP daemon for SNMP-based monitoring. This document assumes that version 8.2.00 or later is in use.

Solution

Background

SNMP is a protocol for monitoring and managing devices or components within a network. SNMP supports three primary monitoring methods: **getting**, **walking**, and **trapping**. An SNMPGET allows a remote monitor or manager to fetch a particular monitored element. An SNMPWALK allows a remote monitor or manager to fetch a range of values within a class. An SNMP trap allows a monitored entity to generate a notification that is sent to a remote monitor based on certain conditions. This article will focus on configuring the Gateway appliance to allow remote monitors to be queried via getting and walking.

Implementation

Leveraging SNMP requires the following changes:

1. Allowing SNMP traffic to traverse the software firewall
2. Setting the initialization parameters for the SNMP daemon
3. Allowing the SNMP daemon to receive requests from outside requestors
4. Setting desired configuration options in the SNMP daemon

Configuring the software firewall

The software firewall used by the Gateway will not allow SNMP traffic through from external requestors. The software firewall must be modified to allow these requests through to the SNMP daemon. The software firewall rules within the host operating system should never be modified. The following procedure should be executed to make this change within the Policy Manager:

1. Log in to the Policy Manager as an administrative user
2. Select **Manage Listen Ports** from the Tasks menu
3. Select **Manage Firewall Rules** from the Manage Listen Ports dialog
4. Select **Create** from the Manage Firewall Rules dialog
5. Create a rule with the following settings

    - Rule Name: Permit SNMP
    - Rule Action: Accept
    - Interface: All
    - Protocol: UDP
    - From Port: 161

Setting the initialization parameters

A configuration file prevents the SNMP daemon from listening on any interface besides the loopback interface. Execute the following procedure to bind the daemon to all interfaces:

1. Log in to the Gateway appliance as the ssgconfig user
2. Select Option #3: Use a privileged shell (root)
3. Open the SNMP daemon parameters file in a text editor: `vi /etc/sysconfig/snmpd`
4. Modify the existing line to read as follows: `OPTIONS="-Lsd -Lf /dev/null -p /var/run/snmpd.pid -a -I -smux"`
5. Save the file and exit the editor

An example configuration file is illustrated as follows:

```
# snmpd command line options
# OPTIONS="-LS0-6d -Lf /dev/null -p /var/run/snmpd.pid"
OPTIONS="-Lsd -Lf /dev/null -p /var/run/snmpd.pid -a -I -smux"
```

Allowing external requestors to access the SNMP daemon

Access to the SNMP daemon is restricted by an access control list. This list must be modified to allow external hosts access to this daemon.

1. Log in to the Gateway appliance as the ssgconfig user
2. Select Option #3: Use a privileged shell (root)
3. Open the SNMP daemon parameters file in a text editor: `vi /etc/hosts.allow`
4. Modify the snmpd line to read as follows: `snmpd: ALL`
5. Save the file and exit the editor

An abridged configuration file is illustrated as follows:

```
snmpd: ALL
sshd: ALL
```

Setting desired configuration options

There are several configuration options that should be set in order to secure the SNMP implementation on the Gateway appliance. It consists of the following goals:

1. Specifying an acceptable IP address or IP range
2. Attaching the address or range to a security group
3. Allowing the security group to access a particular view
4. Permitting read-only access to that specific view

To make these changes, open up the SNMP daemon configuration file (located at /etc/snmp/snmpd.conf) in a text editor. The applicable portions of an example configuration file is displayed below with the applicable changes in bold face.

Specifying an acceptable IP address or range

SNMP requires specifying an IP address or IP range (in CIDR notation) and assign it to a community. The values of *sec.name*, *source*, and *community* can be modified. An example is as follows:

```
# First, map the community name "public" into a "security name"
```

```
#       sec.name        source          community
#com2sec notConfigUser   default         public
com2sec  myNetwork       10.10.50.0/24   ca
```

Attaching the address or range to a security group

A named security group must be created that specifies the SNMP security version to use and assign a named IP address or range to the group. The values of *groupName* and *securityModel* can be modified. The value of *securityName* should reflect the value of *sec.name* set previously. An example is as follows:

```
# Second, map the security name into a group name:
#       groupName       securityModel   securityName
#group   notConfigGroup  v1              notConfigUser
#group   notConfigGroup  v2c             notConfigUser
group   myGroup         v1              myNetwork
group   myGroup         v2c             myNetwork
```

Allowing the security group to access a particular view

A view specifies a container restricting what system information can be accessed. This section permits a group to access a specific view. The values of *name*, and *subtree mask* can be modified but should be set as follows. An example is as follows:

```
# Third, create a view for us to let the group have rights to:
# Open up the whole tree for ro, make the RFC 1213 required ones rw.
#       name            incl/excl       subtree mask(optional)
#view    roview          included        .1
#view    rwview          included        system.sysContact
#view    rwview          included        system.sysName
#view    rwview          included        system.sysLocation
view     systemview      included        system
view     systemview      included        .1.3.6.1.4.1.17304
```

Note that in this step you should add to the view the root nodes for the MIBs you want to be able to view. In the above example, the Layer 7 MIB is added to the view in the second uncommented line. If you also want to see the subtree containing system information (CPU, Memory, disk usage) add the following subtree mask to the view: .1.3.6.1.4.1.2021.

Permitting read-only access to that view

A relationship must be configured between a security group and a view. This relationship controls what information is accessible by which entities. The value of *group* should reflect the value of *groupName* set previously. The value of *read* should reflect the value of *name* set in the previous step. An example is as follows:

```
# 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  roview rwview none
access  myGroup         ""      any       noauth    exact   systemview none none
```

Completing the configuration

All configuration files that have been modified should be saved after they are edited. The Gateway appliance should be restarted after

saving. The changes will manifest after the restart completes and the SNMP daemon initializes.

Workaround

1. There is a second SNMP service running on the gateway (ncsnmpd). This service is the SNMP agent for the internal HSM card. It is configured in such a way that it does not interfere with the main SNMP service.
2. In older versions of the gateway step 1 had to be done through the iptables configuration. This method is no longer recommended. The reccomended method is the one described in this document. If for some reason you require to open the port through iptables you should follow the following steps:

    - Open the iptables configuration file: vi /etc/sysconfig/iptables
    - Locate lines 84-85:

        84 #[0:0] -A INPUT -p tcp -m tcp --dport 161 -j ACCEPT
        85 #[0:0] -A INPUT -p udp -m udp --dport 161 -j ACCEPT

    - Uncomment them
    - Restart the iptables service: service iptables restart
    - **IMPORTANT:** Restart the ssg service: service ssg restart

    This process will open port 161 for outside udp and tcp connections only. If you also require the port to be open for localhost requests to, copy and paste the two rules and add the -i lo flag to them.

Knowledge Base File