SNMP Traps

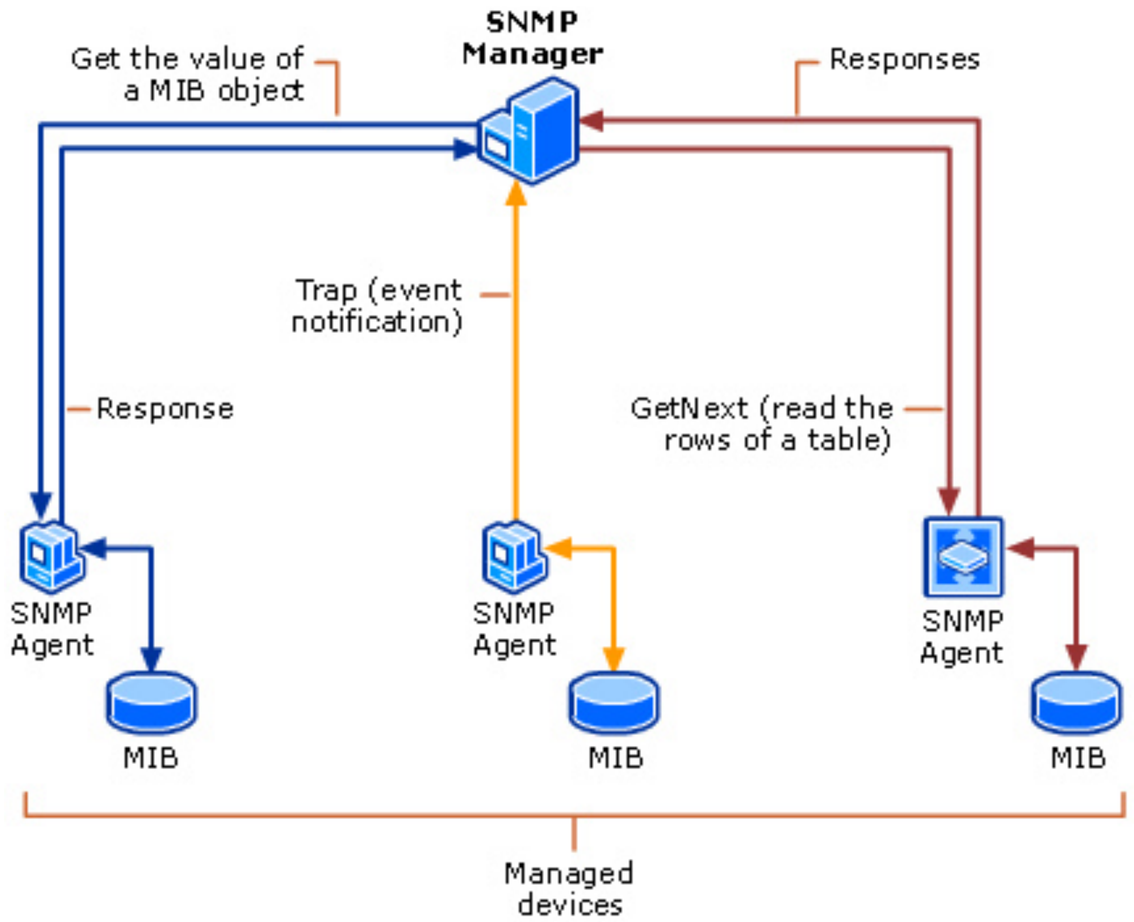
Monitoring and Log Management

Advanced Network Monitoring

- Pre-packaged software can cover basic monitoring needs
- They provide views of the servers, the network devices, and usually some traffic graphics to help you identify when things aren't running as they normally do
- Having full-time system operators watching the monitors is costly, so having a way to tell operations staff when they need to be observing things is valuable

Proactive Monitoring

- Many of the system monitoring tools have some ability to perform automated tasks based on triggers in the gathered data
  - You might have email sent when bandwidth utilization crosses a threshold
  - You might have a text message sent when particular types of traffic are seen, whether or not they are blocked
- SNMP offers traps, which do not require a machine to poll for them because the trap generator initiates transmission of the event message to an automated handler program



Proactive SNMP
Polling vs. Traps

- An SNMP agent can send a trap message (on UDP port 162) to a trap receiver which then takes some action based on the information contained in the trap
- Typical traps are sent for things like reboots, interface up/down events, failed snmp accesses
- Using traps requires MIBs for the sending agent since the MIBs contain the trap definitions for a given agent
- Custom traps can be created by modifying the MIBs on a given trap sender
- The snmptrapd daemon is a commonly used trap receiver

SNMP Traps

- They are seven trap types, with 6 being generic pre-defined notifications in version 1 of SNMP
- The seventh is the enterprise-specific trap which allows any organization to create a complete hierarchy of traps supported by their agents and defined in their MIB
- Version 2c of SNMP does away with these types and moves to the concept of notifications instead of traps using the same basic mechanism as traps but adding acknowledgements
- Version 3 extends version 2c to include authentication and encryption

snmptrapd

- Installed as a separate package from snmpd
- Configured in /etc/snmp/snmptrapd.conf
- The minimum configuration must include authentication directives and can log traps, run programs to handle traps, or forward traps to another trap receiver
- Need to enable snmptrapd in /etc/default/snmpd

snmptrapd.conf

- To handle traps using v1 or v2c SNMP, add
  authCommunity log,execute,net public

- To handle traps using v3 SNMP, add
createUser username SHA "authpassword" AES "encpassword"
authUser log,execute,net username

- To process traps using the execute mode, add
traphandle OID|default program

- To process traps using the net mode, add
forward OID|default destination

Sample Traphandle Script

- This script will format a trap message as a single line of text
- Set this script as a program to run on a traphandle line in snmptrapd.conf

```
authCommunity log,execute,net public
traphandle default /home/ubuntu/snmptraphandler
traphandle default path-to-librenms-snmptrap.php
```

```
#!/bin/sh

read host
read ip
vars=

while read oid val
do
  if [ "$vars" = "" ]
  then
    vars="$oid = $val"
  else
    vars="$vars, $oid = $val"
  fi
done

echo trap: $1 $host $ip $vars
```

Testing Trap Receivers

- snmptrap command can be used to send traps
- snmpinform can be used to send notifications (v2c or 3 only)
- An example of using snmptrap to send a Warm Start trap message to syslog with an enterprise OID and uptime set to defaults might look like this:

```
snmptrap -v 1 -c public localhost '' sourcehostname 1 0 '' .1.3.6.1.4.1.2021.7890.1 s "distroname"
```

Sending Traps

- To send the built-in traps from the snmpd agent, edit the snmpd.conf file
- Add a line for trapsink or trap2sink or informsink to specify that traps are to be sent (more config options are available, see http://www.net-snmp.org/docs/man/snmpd.conf.html)
- Restart snmpd to make the change take effect
- Sending traps from other agents will require using their configuration procedures (e.g. pfsense can be configured using the web administration interface)
- See http://www.net-snmp.org/wiki/index.php/TUT:snmptrap for examples of creating custom traps, mib entries, and additional customization

SNMP Traps Lab

- Trap handler setup on nmshost
- Alerting configured in librenms
- email alerting on traps setup
- Trap sending configured on all VMs