Process Count Monitoring with Net-SNMP

Processes metrics are not available by default via Net-SNMP; therefore the Net-SNMP collection method in Uptime Infrastructure Monitor does not gather process metrics. With a few extra lines added to snmpd.conf and a SNMP Poller monitor, it is possible to set up process count monitoring and alerting for Net-SNMP elements. I'll give the steps first and the logic follows later in the article.

Steps

1. Edit snmpd.conf on the Net-SNMP target system and add the following line (multiple similar "proc" lines can be specified as well)
    - proc java 3 1
2. Restart the Net-SNMP service for the change to be read in
3. In Uptime Infrastructure Monitor, create an SNMP Poller monitor
4. Click Add OID, enter .1.3.6.1.4.1.2021.2.1.5 and click Next
5. Click the Use Table Column radio button, select prNames from the drop down and click Add
6. Set WARN and CRIT threshold:
    - WARN is greater than 1
    - CRIT is less than 1
7. Enter desired alerting intervals and click Finish

This SNMP Poller will pull back the number of occurrences of the processes specified with the proc directive in snmpd.conf. If the occurrence is greater than one, a warning alert will be sent and if it is less than one, a critical alert will be sent.

How it Works

The MIB being leveraged for this SNMP query is UCD-SNMP-MIB, which is usually a regular part of a Net-SNMP install, and the table of interest is the prTable. For a full description of each of the OIDs in the prTable, see http://net-snmp.sourceforge.net/docs/mibs/ucdavis.html#prTable.

The OID specified when configuring the SNMP Poller monitor is UCD-SNMP-MIB::prCount (.1.3.6.1.4.1.2021.2.5). For each of the processes specified in snmpd.conf using the "proc" directive, UCD-SNMP-MIB::prCount.x will contain the number of occurrences of that process.

Two values are required, along with the process name, when adding the proc directive to snmpd.conf. These are max and min values for the number of occurrences of the process. If these values are exceeded, UCD-SNMP-MIB::prErrorFlag will be set to 1 (otherwise it is zero). It is better to allow the SNMP Poller monitor to do the threshold comparison though because the alert messaging will be more clear and the metric can be retained for graphing purposes, if desired.