Thresh — a Data-Directed SNMP Threshold Poller

John Sellens

Certainty Solutions Inc.

jsellens@certaintysolutions.com

LISA 2000

December, 2000

Introduction

- Thresh is a simple SNMP monitoring tool
- Flexible configuration and notification
- Typically used for lower-priority monitoring
- Thresh would typically augment other monitoring tools
  - No claim to solving every monitoring problem

The Basics — Why Monitor?

- What are you trying to accomplish?

  It isn't a service if it isn't monitored. If there is no monitoring then you're just running software.

  — Tom Limoncelli

- What do you need from your monitoring?
  - Alarms, history, trends, notices, nagging, . . .
- Is every problem/issue an emergency?

What is Thresh?

- An SNMP threshold poller
  - Sends notifications if an SNMP variable passes its threshold
- Intended primarily for low to medium priority tracking
- Not (usually) an emergency alarmer
- Not (typically) a history and trend tool
- SNMP only - no (direct) port or service monitoring
- Written in Scotty/Tcl
- No custom network protocols or agents
  - Nothing extra to install on the monitored devices

Why Thresh and Not Something Else?

- Not every problem requires paging you at 3:00am
- Many monitoring systems treat everything as an emergency
- Some monitoring systems can’t do SNMP
- It’s often useful to be able to track configuration and state changes
- It seems to fill an overlooked niche
- Why SNMP? Because you can easily monitor just about anything with it

A Few Examples

- Send me mail when a system or device reboots/resets
- Log an entry when a network interface goes up or down
- Create a trouble ticket when disk use goes above a certain level
- Page someone else if the load average is too high
- Watch for ethernet switch configuration or port state changes
- Restart a daemon if the process dies
  - Though this is a little more complicated

How Thresh Works

- Invoked periodically by cron
- Walks a file/directory tree, querying devices for SNMP variable values
  - Each directory is typically a different device, named for its location in the hierarchy
  - e.g. The directory

    `org/sellens/www`

    is for my web server www.sellens.org
- If a value doesn't satisfy a rule, thresh formats a message and passes it to the current notifier

Configuration Overview

- ASCII text files, in a directory hierarchy
- `DEFAULTS` files set thresh variables to control operation
  - Inherited down the tree until overridden
- Other files list SNMP variables to be queried, along with thresholds and comparison indicators
- `.thresh` subdirectory is used to maintain history and state between runs

Configuration Examples

A sample DEFAULTS file:

```
verbose = true
name = mydomain.net
community = hello
# read an additional SNMP MIB
mib = /usr/local/mibs/ascend.mib
# big network, long timeout
timeout = 20
notifier = threshmail jsellens
syslog = local1.info
```

Configuration Examples

A sample variable file:

```
# this is a comment
S system.sysDescr.0
S system.sysContact.0
I system.sysUpTime.0
C interfaces.ifTable.ifEntry.ifDescr.5
G ucdavis.memory.memTotalReal.0   90000
L loadTable.laEntry.laLoad.1      1.20
L loadTable.laEntry.laLoad.2      1.50
L loadTable.laEntry.laLoad.3      2.00
V snmp.snmpInPkts.0
```

Sample Notification

- The notifier program can be just about anything — mail, cat, syslog, ...
- A sample notification message:

```
errors for node: www.sellens.org
hrStorageEntry.hrStorageUsed.4:
 not less than threshold
  threshold 2000000
  currently 2038055
    The amount of the storage represented
    by this entry that is allocated, in
    units of hrStorageAllocationUnits.
```

Where to Use Thresh

- When you need to be kept informed, but not woken up
- When you need to sometimes perform some simple actions in response to SNMP settings
- When you want to log changes in state
- When you're already using an alarm tool that can't do all the SNMP probing that you want

When Not to Use Thresh

- When your site is large
- When your budget is large
- When fancy graphics are required
- When you need fancy event correlation
  - though the `prune` variable helps

Potential Enhancements

- SNMP support for other than V1
- Integrate syslog into the code, rather than relying on `logger`
- Some form of include file mechanism
- Message comparison that ignores current values
  - e.g. two more bytes added to a filesystem is probably not really a different error

Summary and Conclusions

- Experience with thresh and an ancestor seems to show that thresh is useful in a number of situations
- Seems to be low footprint, and simple to install and operate
- Seems to fill a need that’s not already well addressed

Questions, Availability, etc.?

- Soon at

  http://thresh.sourceforge.net/

- Questions?