Statistical Monitoring with Cacti
Tracking Problems Before They Happen

“Devon, I don’t know what it is about you that makes you do things just differently enough that it becomes a major problem for the rest of us.”
- Dennis Bellinger
Disclaimer

• SNMP v1 is used for most common devices at within the School of Computer Science at the University of Waterloo

• Any SNMP device that requires write access or has sensitive information uses SNMP v3 and is separated on a network level
Our Situation

• 218 “public use” lab Macs
• Various Nettop/specialty labs running Ubuntu
• Various public and non-public printers
• Mixture of Dell, HP and Super Micro servers
• Various services hosted within LXC or VMWare
• Datacenter services (UPS, SPDU, HVAC)
• Environmental Sensors
Our Situation

When running a lab in any school, one thing becomes painfully obvious

Students love to unplug things
Cacti

Created in 2001 by Ian Berry

Current 0.8.8h (May 2016)
What is Cacti?

Cacti is a **passive** monitoring solution*

* Unless you use plugins
What is Cacti?
Why Cacti?

• Simple to install, Open Source
• Not resource hungry
• Configuration and management is similar to other common monitoring platforms such as Nagios
• Difficult to break the entire platform
What is RRDTool?

Data is polled from target machine(s) and stored into different Round Robin Archives (RRAs) that exist within a single Round Robin Database (RRD) file.

Round Robin Archives have a predefined amount of space for data that overwrites itself as it becomes full.

Therefore, the RRD never grows larger in filesize.
Round Robin Archives

Round Robin Archive - RRA
Fixed Time Period
Fixed Amount of Entries

Once the archive is full, when new data is added
the oldest entry is destroyed
Consolidation can be used to reduce the amount of data points stored without much data loss.
Multiple RRAs can be used to provide consolidated data over different time frames.
RRDTool

Daily
(5 Minute Average)

Weekly
(30 Minute Average)

Monthly
(2 Hour Average)

Yearly
(1 Day Average)
RRDTool can then read from the specified RRD files to create a graph.
RRDTool

Graphs from RRDTool are embeddable images that can be placed almost anywhere

cacti/graph_image.php?action=view&local_graph_id=GRAPHID&rra_id=2
Pollers

**cmd.php**
- Written in PHP
- Included in the default Cacti installation
- Makes use of php-snmp libraries

**Spine (cactid)**
- Written in native C
- Uses POSIX threads
- Makes direct use of the net-snmp library for minimal overhead

Default poller interval in Cacti is 5 minutes (300 seconds)
Poll data for all data sources must finish within that interval.
Collection Types

Data Input Methods

• Runs a set script with provided arguments, data returned is stored in RRD
• Useful when querying one specific OID that never changes
• Can support collection methods other than SNMP (e.g. PHP sockets)

Data Queries

• Reads an XML file and queries the target based upon the settings stored in XML
• Useful for querying multiple data sources that have the same information where the amount of sources can’t be defined
• Only SNMP
Management Information Base

XUPS-MIB::xupsBatTimeRemaining.0 = INTEGER: 3885 seconds
XUPS-MIB::xupsBatVoltage.0 = INTEGER: 260 Volts DC
XUPS-MIB::xupsBatCurrent.0 = INTEGER: 0 Amps DC
XUPS-MIB::xupsBatCapacity.0 = INTEGER: 98 percent
XUPS-MIB::xupsBatteryAbmStatus.0 = INTEGER: batteryResting(4)
MIB

Translating from MIB object to direct OID

#: snmptranslate -On GEIST-QUETZAL-MIB::pduChannelWyeTable
   .1.3.6.1.4.1.21239.6.1.99.4

Translating from direct OID to MIB object

#: snmptranslate -m +ALL .1.3.6.1.4.1.21239.6.1.99.4
GEIST-QUETZAL-MIB::pduChannelWyeTable
SNMP Basics
NMS to Target Communication

SNMP Target

SNMP Daemon

snmpd.conf

extend activeConsole .../activeConsole.sh

activeConsole.sh

NMS

Poller

check_activeconsole.sh

snmpwalk/snmpget

GET/SET Request

161 UDP

GET/SET Response

SNMP Basics
NMS to Target Communication

SNMP Target

SNMP Daemon

snmpd.conf

extend activeConsole .../activeConsole.sh

activeConsole.sh

NMS

Poller

check_activeconsole.sh

snmpwalk/snmpget

GET/SET Request

161 UDP

GET/SET Response
NMS Process
From poller to end result

Poller calls a script providing appropriate host variables (hostname, SNMP community, etc).

Script calls `snmpwalk` which queries the target device with a specific OID or OID tree.

Parsing
Data returned from the `snmp` query is parsed and returned.

Data Source
Returned data from script stored into a round robin database.

```
check_mysql.sh
-H mysql.cs
-C Secret

snmpget -v 1 -c Secret
NET-SNMP-EXTEND-MIB:
:nsExtendOutput1Line."mysql"

sed -e 's/.*/\[[[:digit:]]*\]$/\1/'

mysql[Synced |result|_d1850.rrd] seconds ago. | $result
exit 0
```
/etc/snmp/snmpd.conf

SNMP Daemon Configuration

trapcommunity  UofW
authtrapenable  2
syslocation  "School of Computer Science, University of Waterloo"
syscontact  "csi-snmp@cscf.cs.uwaterloo.ca"
sysservices  76

rocommunity  "UofW" 129.97.0.0/16
rocommunity  "UofW" 172.16.0.0/12
rocommunity  "UofW" 10.0.0.0/8
rocommunity  "UofW" 127.0.0.1

disk  "/" MIN=5%

load  20 15 10

file  /var/log/messages 1000000

extend activeConsole  /etc/snmp/scripts/activeConsole.sh
SNMPD
SNMP Daemon Configuration

**macOS**

```
#: sudo launchctl load -w \n/System/Library/LaunchDaemons/org.net.snmp.snmpd.plist
```

**Ubuntu**

```
#: sudo service snmpd start
```
#!/bin/bash
# Author: Devon Merner (dmerner)
# Date: December 9th, 2015

# To anyone trying to read/learn from/modify this code, good luck and godspeed.

TIMEOUT="3600"
IDLETIME=$(ioreg -c IOHIDSystem | sed -e '/HIDIdleTime/!d' -e 't' -e '}s/.* = //g' -e 'q' / 1000000000)
read ACTIVEUSER <<< $(w | tr -s " " | cut -d" " -f1,2,5 | tail -n+3 | grep console | awk '{ print $1; }' | head -n 1)

if [[ $(w -h) == "*console*** ]] then
  if [ $IDLETIME -ge $TIMEOUT ] then
    echo "0"
  else
    echo "1"
  fi
else
  echo "0"
fi

SNMP Extensions
SNMP Extensions

Applications/IDEs that aren’t saved will hang the built in auto logout process in Mac OS X which can be a security risk and may cause false graph data.
SNMP Extensions

https://github.com/CLCMacTeam/IdleLogout
SNMP Extensions

MC 3003 - Console Usage

Users

From 2015/12/15 08:03:07 To 2015/12/16 08:03:07

Current: 2.00

NOT SURE IF GRAPHING SYSTEM INCORRECT

OR STUDENTS STUDYING FOR FINALS
SNMP Extensions

Lab usage graphs *should* go to zero during off-hours
### DC-3558-B7-PDU-1

#### Data Queries

<table>
<thead>
<tr>
<th>State</th>
<th>Label</th>
<th>Energy (kWh)</th>
<th>Real Power (W)</th>
<th>Apparent Power (VA)</th>
<th>Power Factor (%)</th>
<th>Voltage (Vrms)</th>
<th>Peak Voltage (V)</th>
<th>Current (Amps)</th>
<th>Peak Current (A)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>BladeUPS Feed</strong></td>
<td>4367</td>
<td>1034</td>
<td>1185</td>
<td>87</td>
<td>211.6</td>
<td>211.7</td>
<td>5.60</td>
<td>6.35</td>
</tr>
<tr>
<td></td>
<td>Circuit 1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>✔</td>
<td>Outlet 1</td>
<td>2491</td>
<td>756</td>
<td>855</td>
<td>88</td>
<td>212.0</td>
<td>212.2</td>
<td>4.03</td>
<td>4.95</td>
</tr>
<tr>
<td>✔</td>
<td>Outlet 2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>✔</td>
<td>Outlet 3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>✔</td>
<td>Outlet 4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>✔</td>
<td>Outlet 5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>✔</td>
<td>Outlet 6</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>✔</td>
<td>Outlet 7</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>✔</td>
<td>Outlet 8</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>✔</td>
<td>Outlet 9</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>✔</td>
<td>Outlet 10</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>✔</td>
<td>Outlet 11</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>✔</td>
<td>Outlet 12</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>✔</td>
<td><strong>Circuit 2</strong></td>
<td>1854</td>
<td>274</td>
<td>333</td>
<td>82</td>
<td>212.8</td>
<td>213.0</td>
<td>1.57</td>
<td>1.63</td>
</tr>
<tr>
<td>✔</td>
<td>Outlet 13</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>✔</td>
<td>Outlet 14</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>✔</td>
<td>Outlet 15</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>✔</td>
<td>Outlet 16</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>✔</td>
<td>Outlet 17</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>✔</td>
<td>Outlet 18</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>✔</td>
<td>Outlet 19</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>✔</td>
<td>Outlet 20</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>✔</td>
<td>Outlet 21</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>✔</td>
<td>Outlet 22</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>✔</td>
<td>Outlet 23</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>✔</td>
<td>Outlet 24</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---

**Note:** The data displayed is a snapshot of the power consumption and voltage levels for various outlets and circuits. The values are measured in kilowatt-hours (kWh), watts (W), volts (V), and amperes (A).
Data Queries

**pduChannelWyeTable**

- **pduChannelWyeID.1.1** = Gauge32: 1
- **pduChannelWyeID.1.2** = Gauge32: 2
- **pduChannelWyeID.1.3** = Gauge32: 3

- **pduChannelWyeLabel.1.1** = STRING: “BladeUPS Feed”
- **pduChannelWyeLabel.1.2** = STRING: “Circuit 1”
- **pduChannelWyeLabel.1.3** = STRING: “Circuit 2”

- **pduChannelWyeVolts.1.1** = Gauge32: 2116
- **pduChannelWyeVolts.1.2** = Gauge32: 2120
- **pduChannelWyeVolts.1.3** = Gauge32: 2128

- **pduChannelWyeAmps.1.1** = Gauge32: 560
- **pduChannelWyeAmps.1.2** = Gauge32: 403
- **pduChannelWyeAmps.1.3** = Gauge32: 157
<interface>
  <name>Get GEIST Quetzal PDU wye-wired Information</name>
  <description>Queries a host for a list of monitorable devices from the GEIST v4 Power Firmware GEIST-QUETZAL-MIB::pduChannelWyeTable.</description>
  <oid_index>.1.3.6.1.4.1.21239.6.1.99.4.1.1</oid_index>
  <index_order>pduChannelWyeID</index_order>
  <index_order_type>numeric</index_order_type>
  <index_title_format>chosen_order_field</index_title_format>
  <fields>
    ...
  </fields>
</interface>
“input” fields are cached, they are used for labels and legends. “output” fields are queried when the poller runs.
“input” fields are cached, they are used for labels and legends. “output” fields are queried when the poller runs.
Data Queries

entPhySensorTable

entPhySensorValue

200021021 = INTEGER: 8310
entPhySensorValue.200022021 = INTEGER: 8130
entPhySensorValue.200023021 = INTEGER: 8310

entPhySensorTable

200021021 = INTEGER: 200021021

entPhySensorTable

200022021 = INTEGER: 200022021

entPhySensorTable

200023021 = INTEGER: 200023021
Data Queries

“oid_index_parse” can be used to filter out unwanted indexing entries.

<oid_index_parse_OID/REGEXP:^.*\.(\d{2,})$/</oid_index_parse>
Data Queries

entPhySensorTable

entPhySensorValue

200021021

200022021

200023021

entPhySensorValue.200021021 = INTEGER: 8310
entPhySensorValue.200022021 = INTEGER: 8130
entPhySensorValue.200023021 = INTEGER: 8310

entPhySensorTable.200021021 = INTEGER: 200021021
entPhySensorTable.200022021 = INTEGER: 200022021
entPhySensorTable.200023021 = INTEGER: 200023021
Plugins

Aggregate

Allows for the creation of graphs with data sources from different hosts

Single host graph

Multi host graph
Plugins

Autom8

Automates the creation of graphs and graph tree structure.
Plugins

Monitor

Adds a kiosk style page with an overview of all your monitored hosts. Can sound an alarm when one is down.

Only checks if the host is up, not if data returned is correct.
Plugins

Threshold

Mimics the notification checking that services like Nagios provide. Can monitor both a host and its graphed data.

<table>
<thead>
<tr>
<th>Default Alerting Options</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Weekend exemptions</td>
<td></td>
</tr>
<tr>
<td>This is checked, this will not run on weekends.</td>
<td></td>
</tr>
<tr>
<td>Default Trigger Count</td>
<td>1</td>
</tr>
<tr>
<td>Default number of consecutive times the Data Source must be in breach of the Threshold for an Alert to be raised</td>
<td></td>
</tr>
<tr>
<td>Re-Alerting</td>
<td>12</td>
</tr>
<tr>
<td>Repeat Alert after specified number of poller cycles.</td>
<td></td>
</tr>
<tr>
<td>Syslog Support</td>
<td></td>
</tr>
<tr>
<td>These messages will be sent to your local syslog. If you would like these sent to a remote box, you must setup your local syslog to do so</td>
<td></td>
</tr>
<tr>
<td>Syslog Level</td>
<td>Warning</td>
</tr>
<tr>
<td>This is the priority level that your syslog messages will be sent as</td>
<td></td>
</tr>
<tr>
<td>Syslog Facility</td>
<td>Daemon</td>
</tr>
<tr>
<td>This is the facility level that your syslog messages will be sent as</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Emailing Options</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Send Emails with Urgent Priority</td>
<td></td>
</tr>
<tr>
<td>Allows you to set e-mails with urgent priority</td>
<td></td>
</tr>
<tr>
<td>Dead Hosts Notifications</td>
<td></td>
</tr>
<tr>
<td>Enable Dead/Recovering host notification</td>
<td></td>
</tr>
<tr>
<td>Dead Host Notifications Email</td>
<td></td>
</tr>
<tr>
<td>This is the Email Address that the Dead Host Notifications will be sent to if the Global Notification List is selected.</td>
<td></td>
</tr>
<tr>
<td>Down Host Subject</td>
<td></td>
</tr>
<tr>
<td>This is the Email subject that will be used for Down Host Messages.</td>
<td></td>
</tr>
</tbody>
</table>

Host Error: <DESCRIPTION> (<HOSTNAME>) is DOWN
Q & A

Resources
Cacti Main Site
http://cacti.net

Cacti Community Forums
http://forums.cacti.net

RRDTool
http://rrdtool.org

Feedback