



Statistical Monitoring with Cacti

Tracking Problems Before They Happen



UNIVERSITY OF
WATERLOO



Feedback: <https://bit.ly/psumac2016-97>

Devon Merner

IT Support Assistant

University of Waterloo - Computer Science Computing Facility
Infrastructure Support Group

dmerner@uwaterloo.ca

“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



UNIVERSITY OF
WATERLOO

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

The awesome world of
Simple Network Management Protocol

François Joannette – FJ Consultant
Manuel Deschambault – Symbiotic System Design

Feedback <http://j.mp/psumac2015-132>



UNIVERSITY OF
WATERLOO

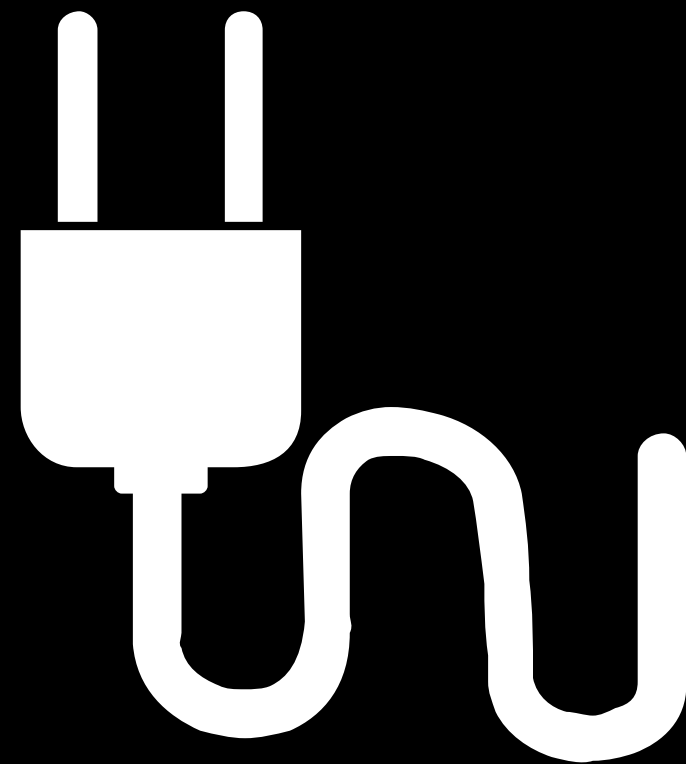
Our Situation

- 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's or VMWare
- Datacenter services (UPS, SPDUE, 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)



UNIVERSITY OF
WATERLOO

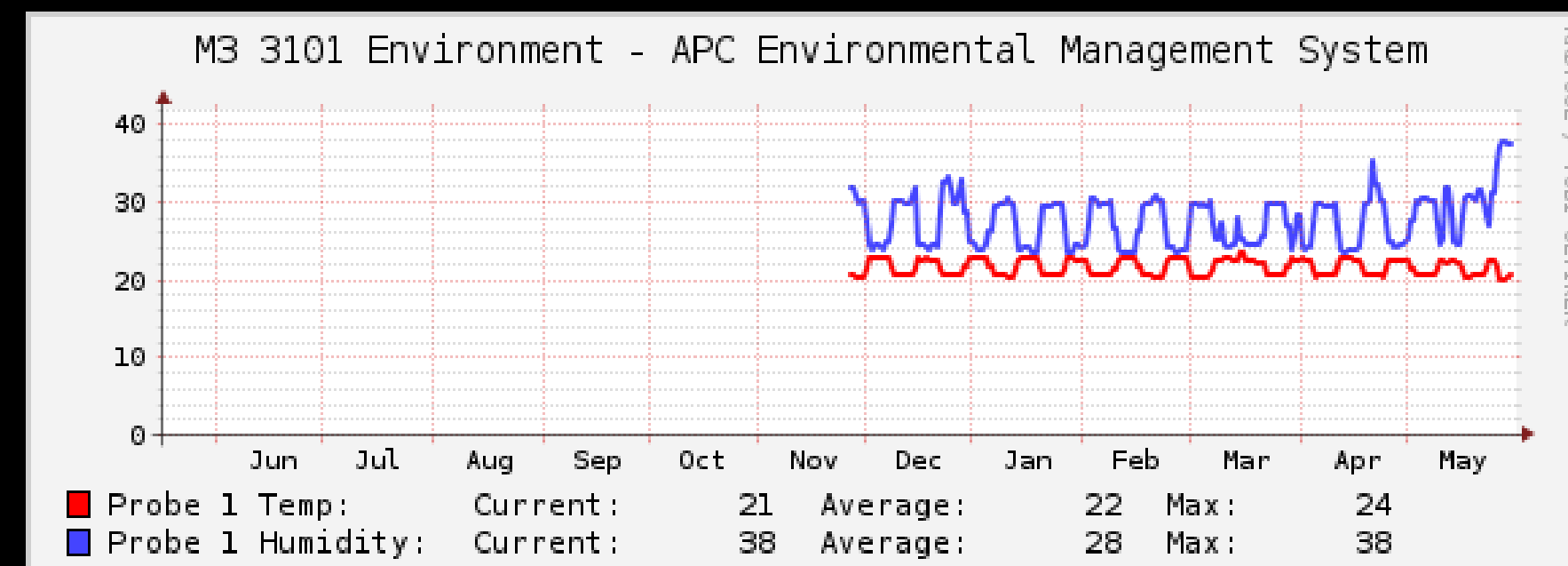
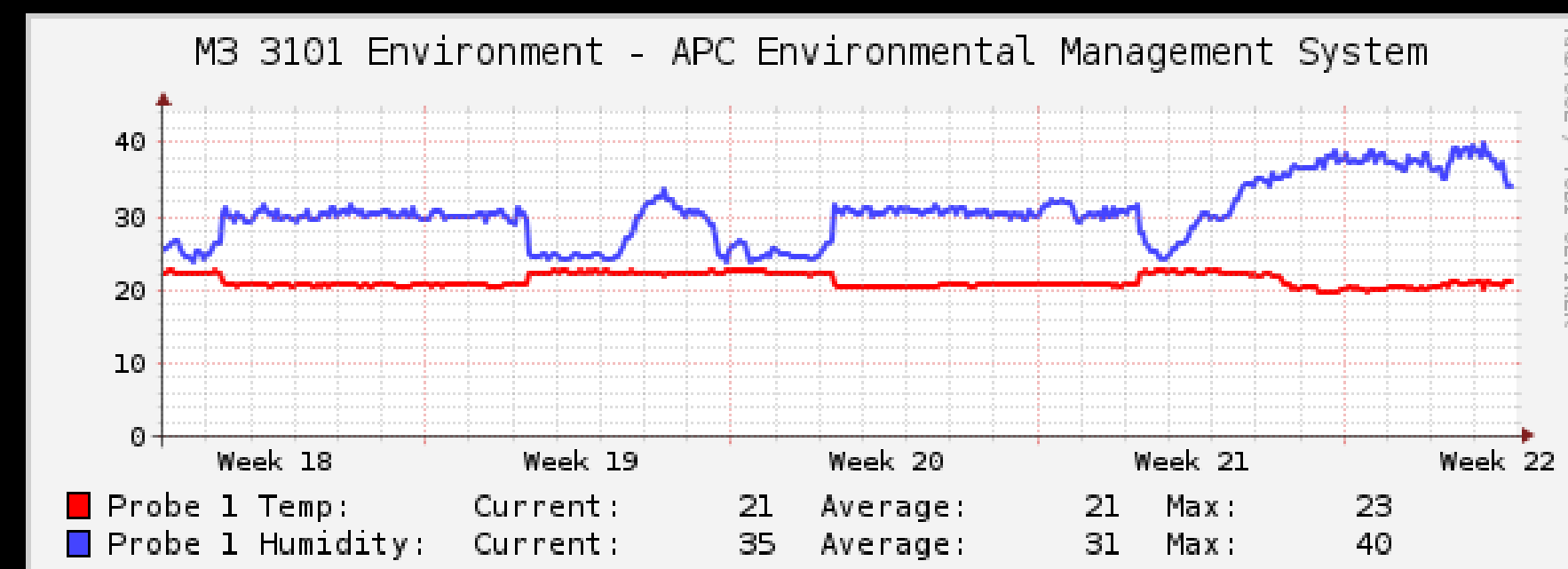
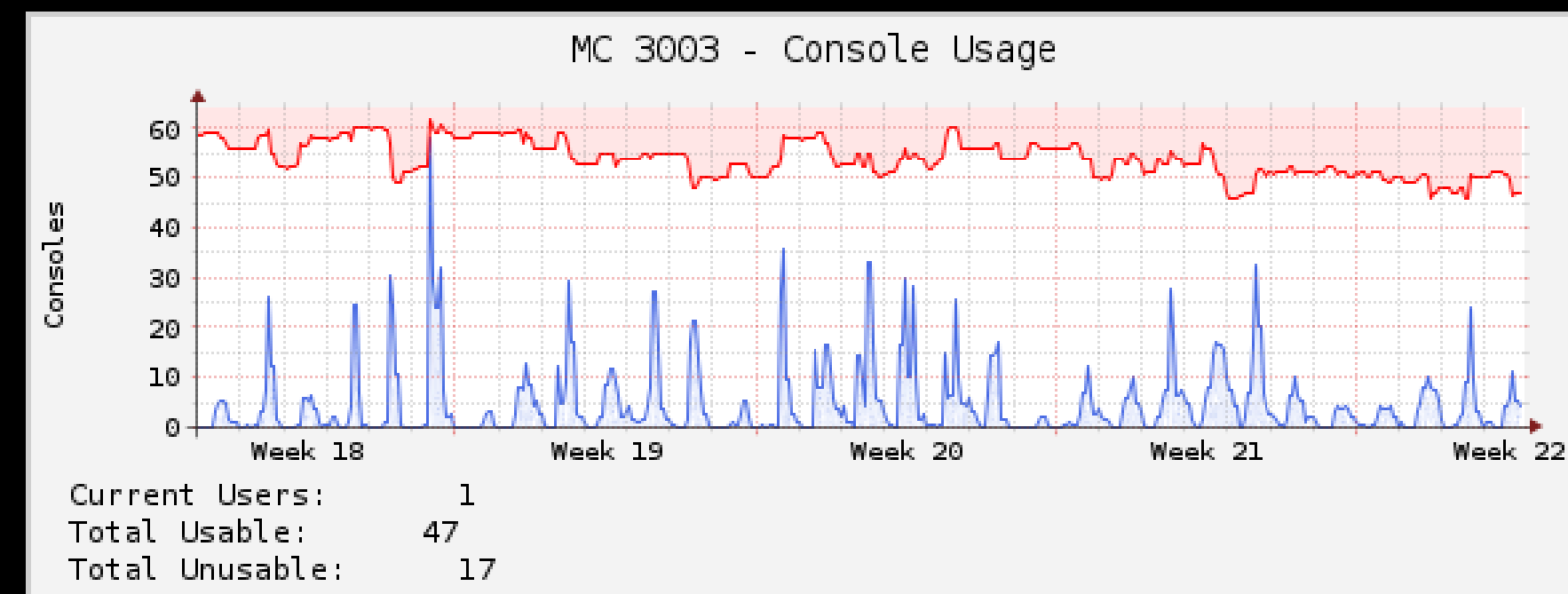
What is Cacti?

Cacti is a passive monitoring solution*



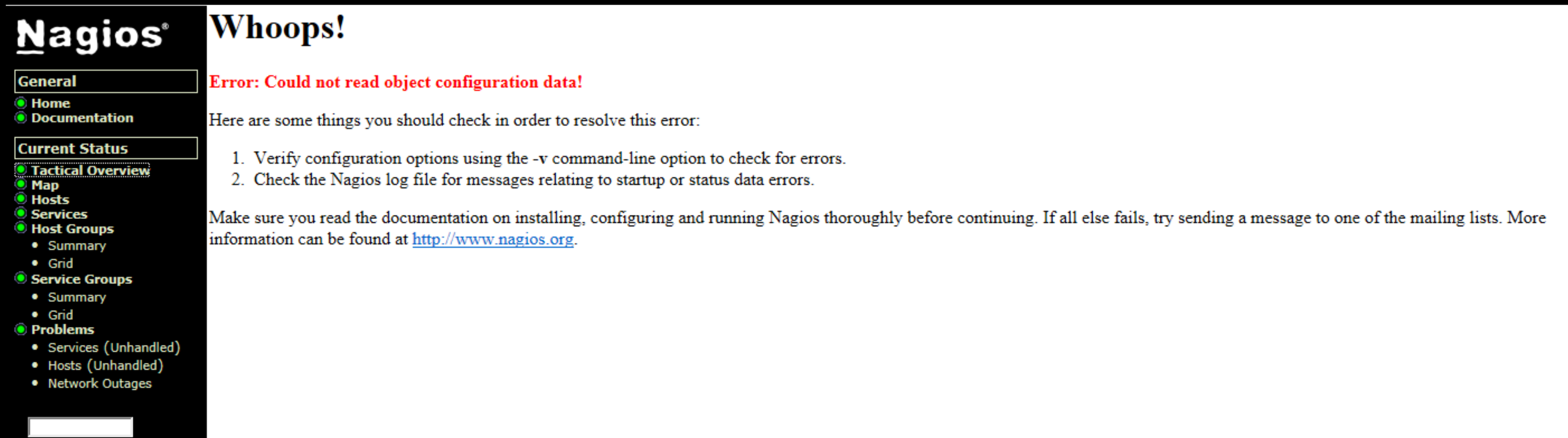
* Unless you use plugins

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



The screenshot shows the Nagios web interface. On the left is a sidebar with the Nagios logo and a navigation menu. The main content area displays an error message. The sidebar menu includes: General, Home, Documentation, Current Status, Tactical Overview, Map, Hosts, Services, Host Groups (with sub-items Summary and Grid), Service Groups (with sub-items Summary and Grid), and Problems (with sub-items Services (Unhandled), Hosts (Unhandled), and Network Outages). The main content area has a heading "Whoops!" followed by a red error message: "Error: Could not read object configuration data!". Below this, it says "Here are some things you should check in order to resolve this error:" and lists two steps: 1. Verify configuration options using the -v command-line option to check for errors. 2. Check the Nagios log file for messages relating to startup or status data errors. At the bottom, it advises reading the documentation and provides a link to <http://www.nagios.org>.

Nagios®

General

- Home
- Documentation

Current Status

- Tactical Overview
- Map
- Hosts
- Services
- Host Groups
 - Summary
 - Grid
- Service Groups
 - Summary
 - Grid
- Problems
 - Services (Unhandled)
 - Hosts (Unhandled)
 - Network Outages

Whoops!

Error: Could not read object configuration data!

Here are some things you should check in order to resolve this error:

1. Verify configuration options using the -v command-line option to check for errors.
2. Check the Nagios log file for messages relating to startup or status data errors.

Make sure you read the documentation on installing, configuring and running Nagios thoroughly before continuing. If all else fails, try sending a message to one of the mailing lists. More information can be found at <http://www.nagios.org>.

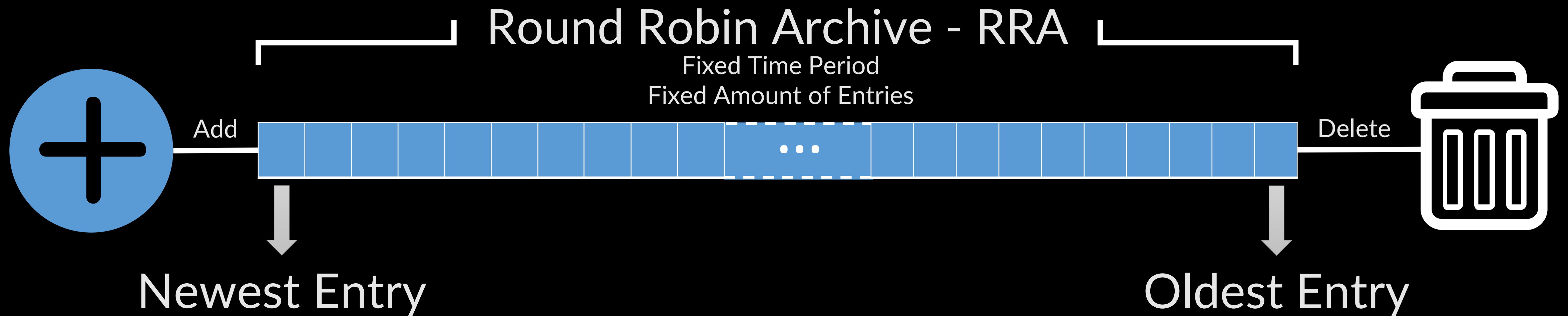
What is RRDTool?

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.

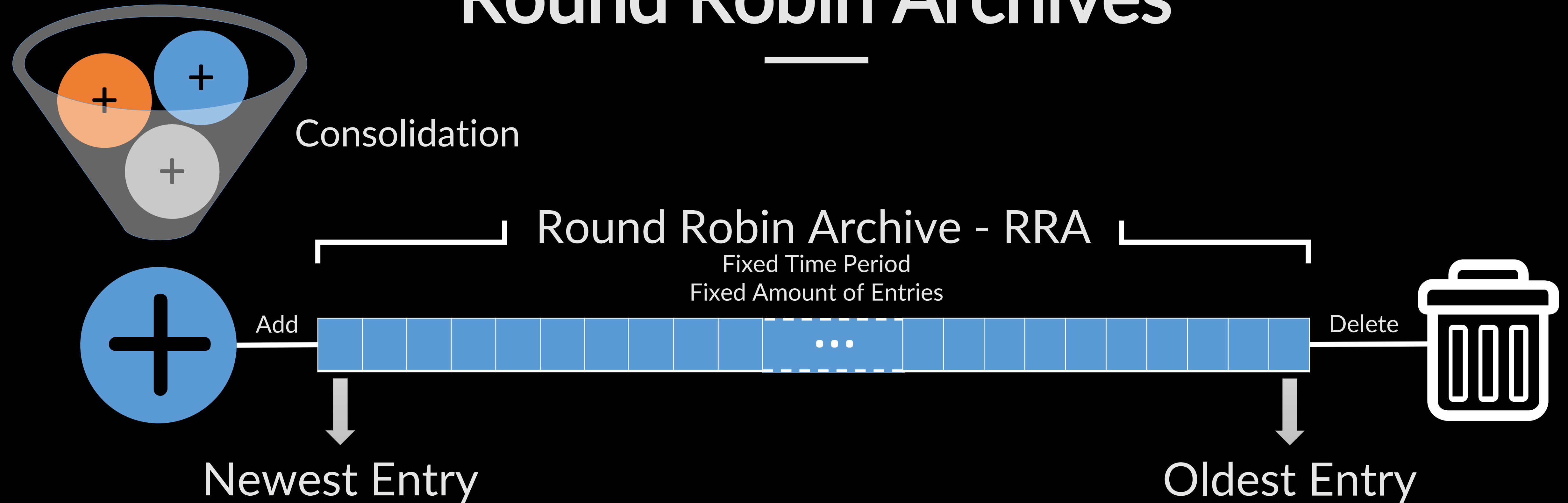
Therefore, the RRD never grows larger in filesize.

Round Robin Archives



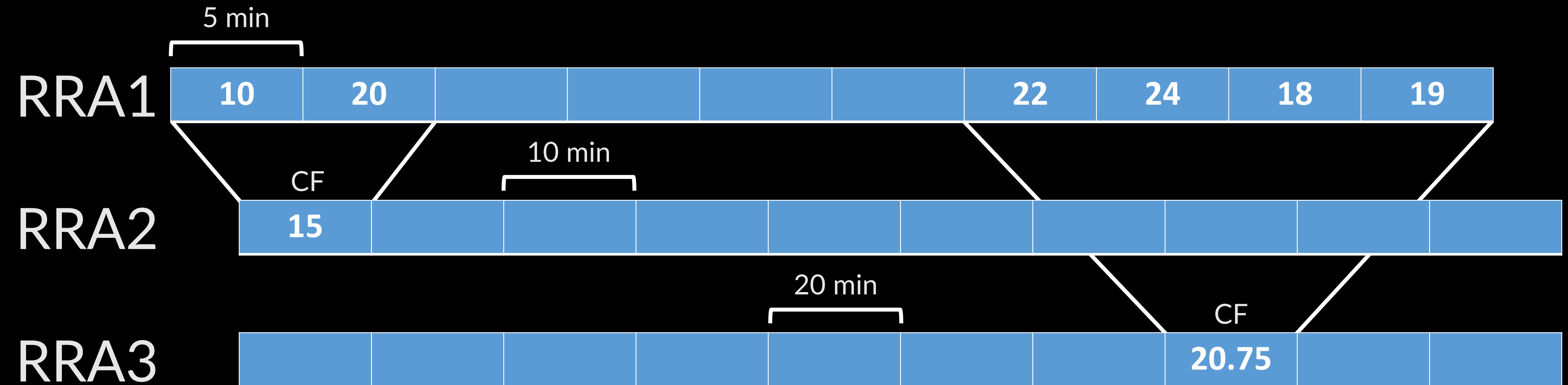
Once the archive is full, when new data is added the oldest entry is destroyed

Round Robin Archives



Consolidation can be used to reduce the amount of data points stored without much data loss.

Round Robin Archives



Multiple RRAs can be used to provide consolidated data over different time frames.

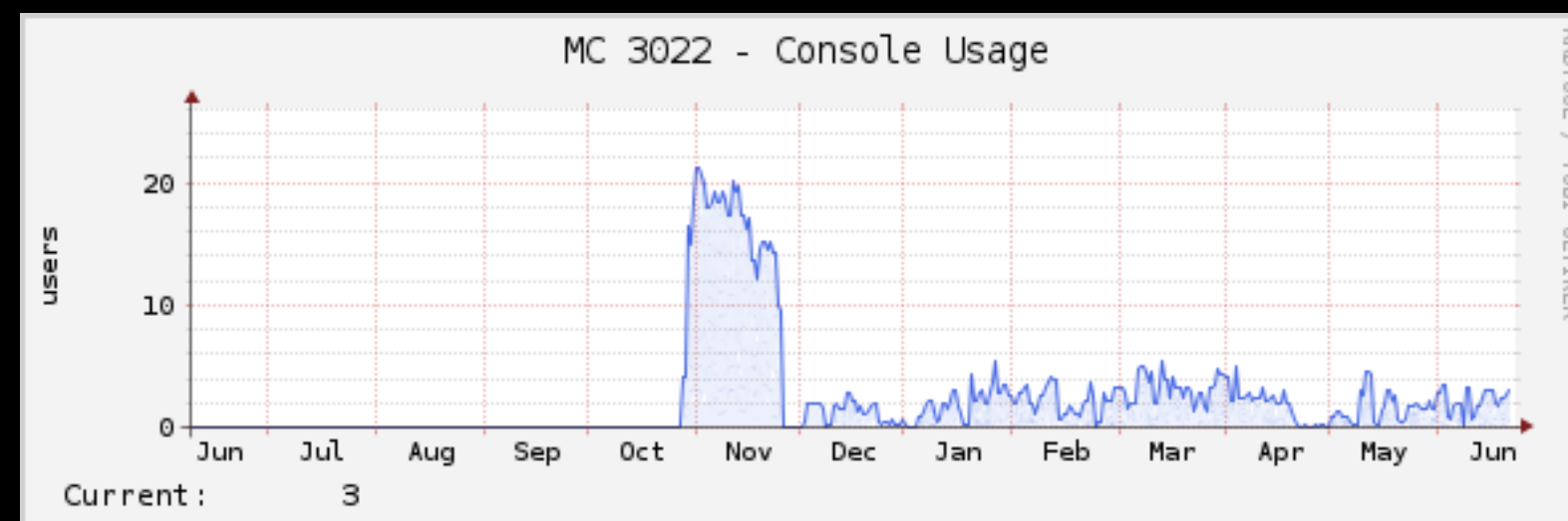
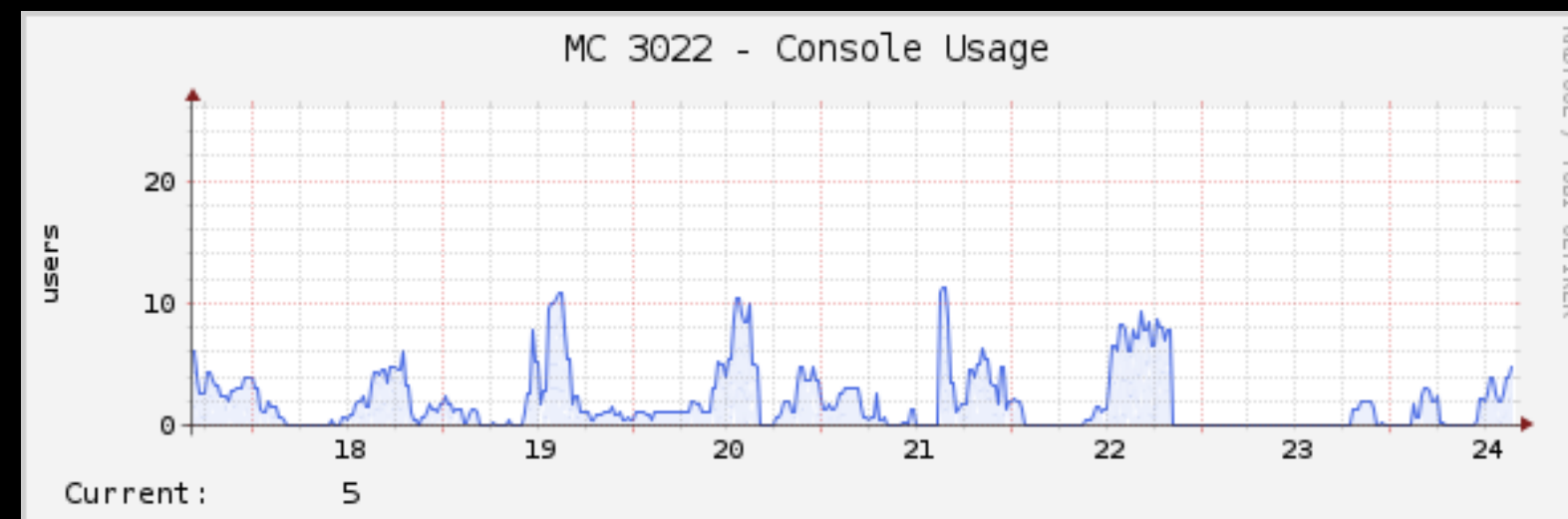
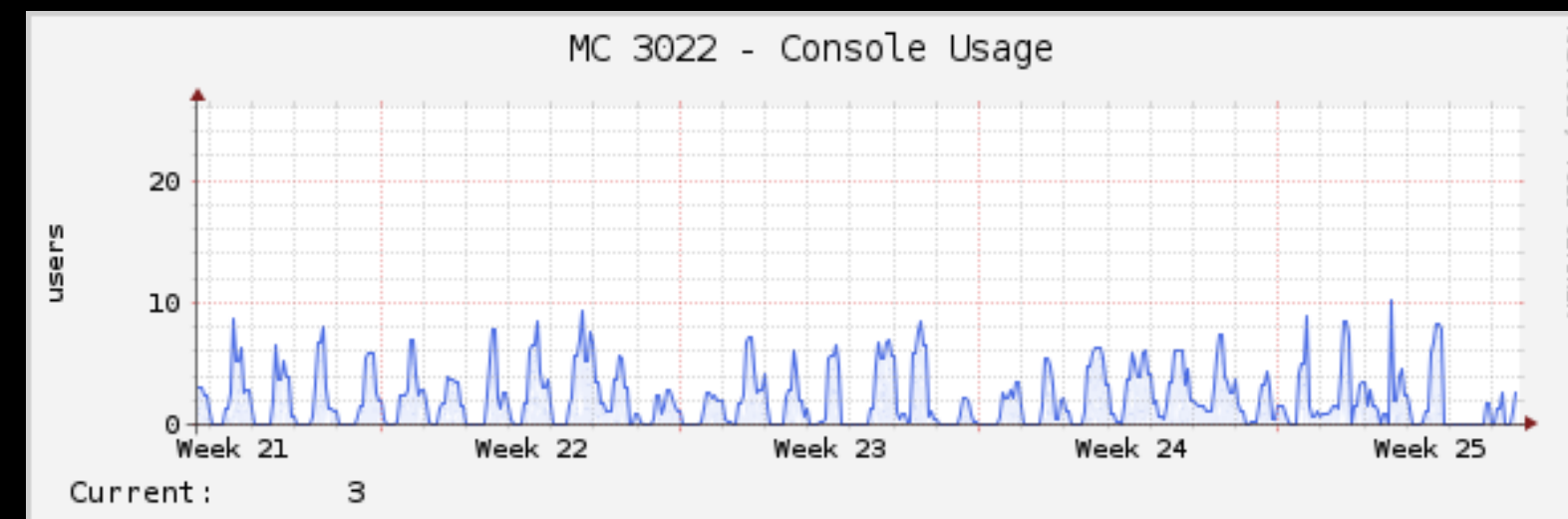
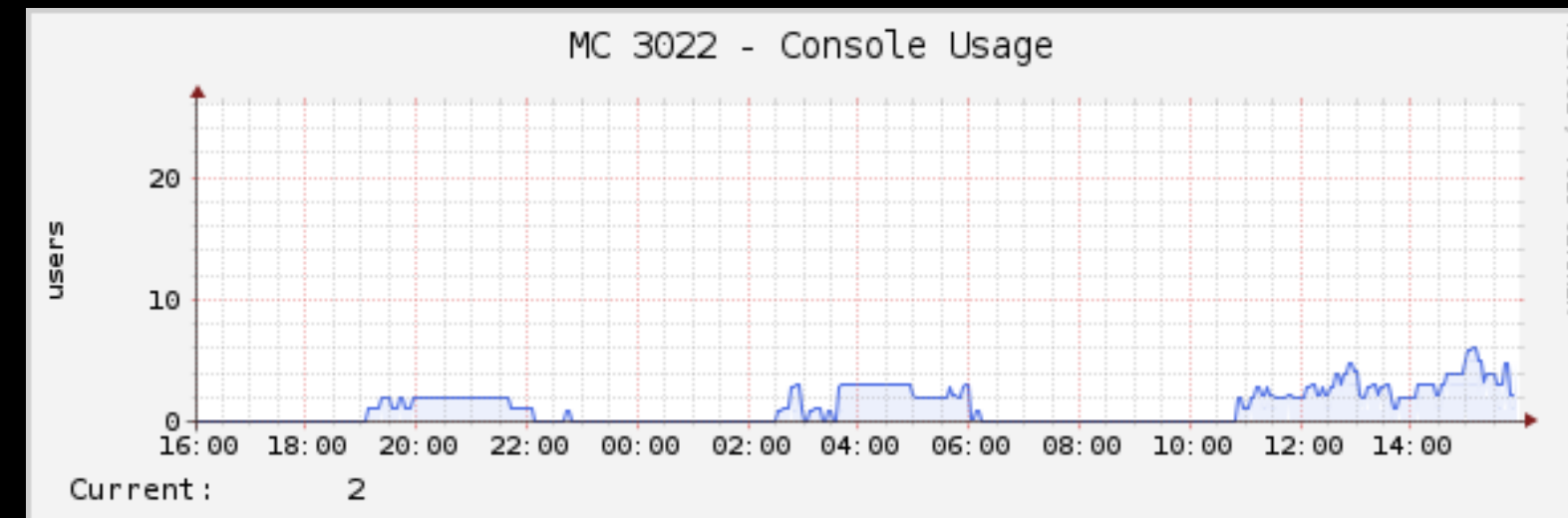
RRDTool

Daily
(5 Minute Average)

Weekly
(30 Minute Average)

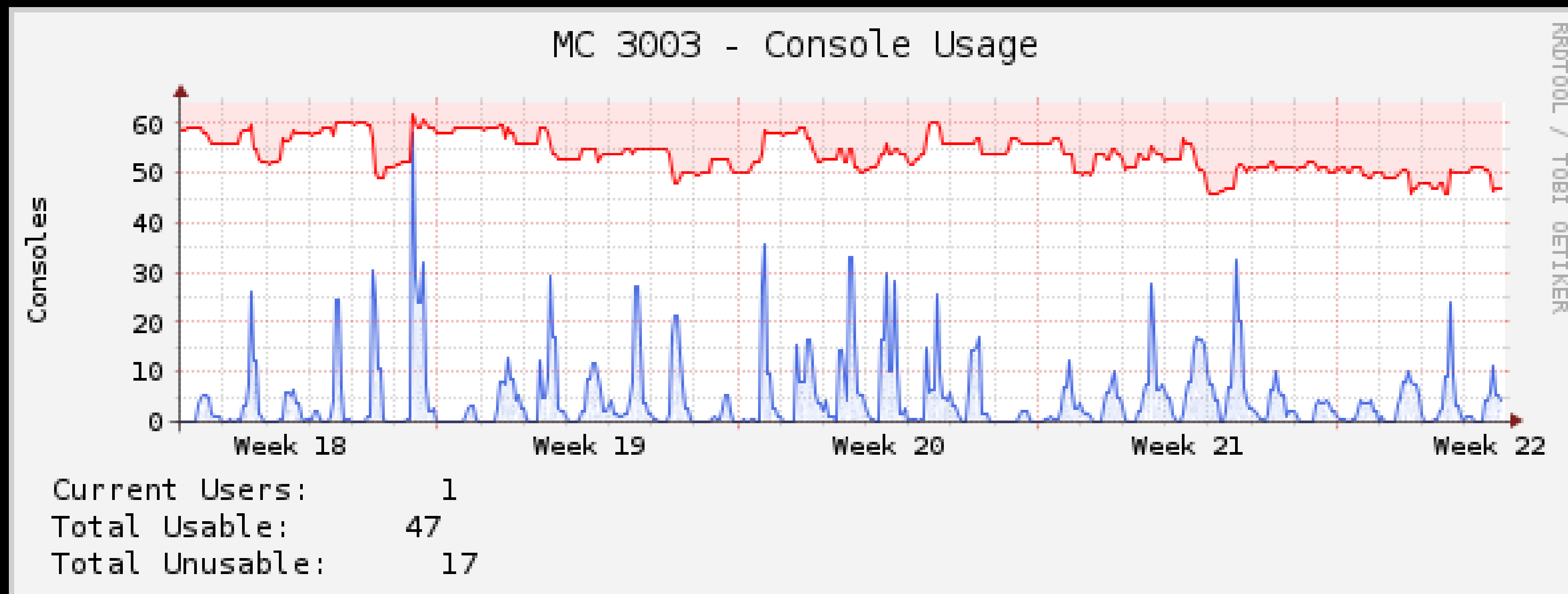
Monthly
(2 Hour Average)

Yearly
(1 Day Average)



RRDTool

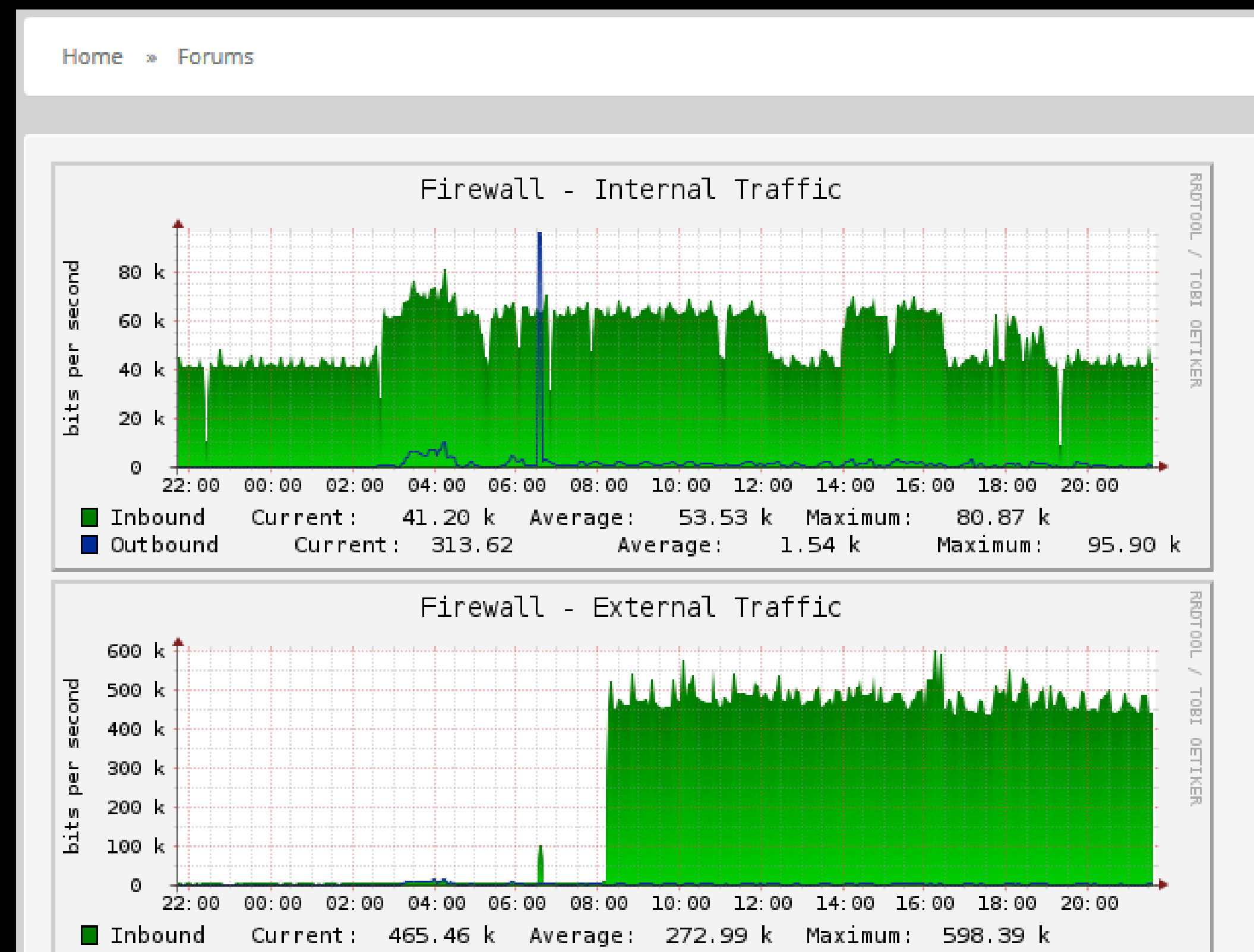
RRDTool can then read from the specified RRD files to create a graph



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

MIB

Management Information Base

XUPS-MIBiso3.Bat4in534m.2in10=0INTEGER88885 seconds
XUPS-MIBiso3.Bat4V.dl534.1.2.INTEGER260.V260 DC
XUPS-MIBiso3.Bat4C.1r534.1.2.INTEGER0ARnps DC
XUPS-MIBiso3.Bat4Cap534.102=4INTEGER08Percent
XUPS-MIBiso3.Bat4ely534m152a50.0 INTEGER4 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

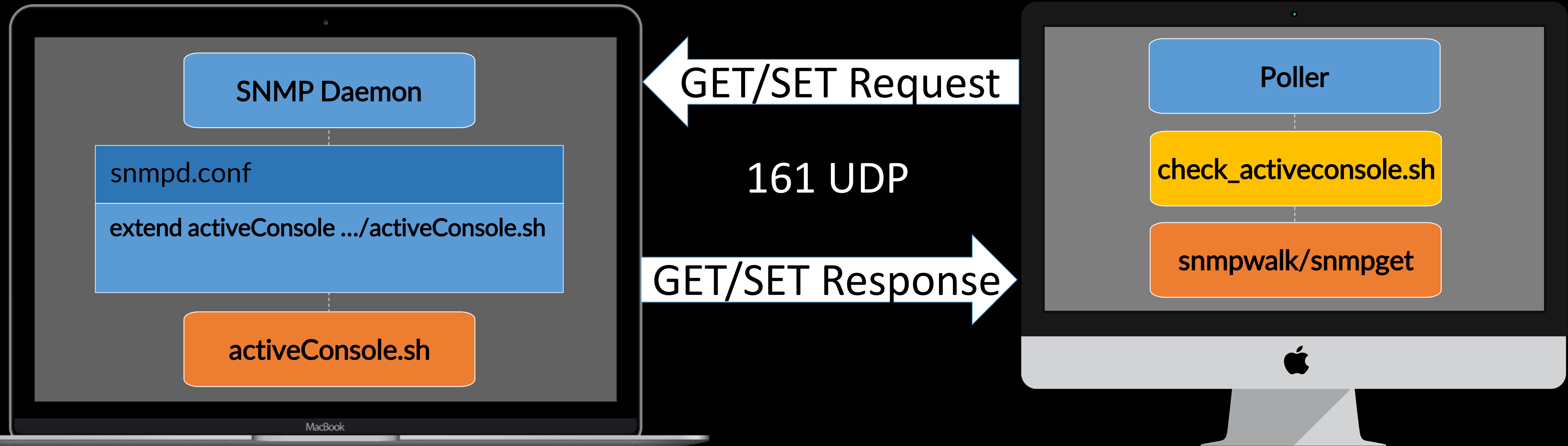
```
#: snmptranslate -m +ALL .1.3.6.1.4.1.21239.6.1.99.4  
GEIST-QUETZAL-MIB::pduChannelWyeTable
```


SNMP Basics

NMS to Target Communication

SNMP Target

NMS



NMS Process

From poller to end result

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

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

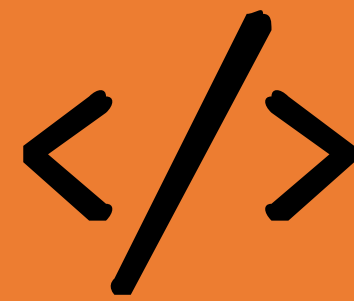
```
sed -e 's/. * \([[:digit:]]*\)$/\1/'
```

```
mysql -s -e 'select $result_4350 seconds ago. | $result'  
exit 0
```



Poller

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



Script

Script calls snmpwalk/snmpget 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 is stored in a round robin database



UNIVERSITY OF
WATERLOO

/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
```



UNIVERSITY OF
WATERLOO

SNMPD

SNMP Daemon Configuration

macOS

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

Ubuntu

```
#: sudo service snmpd start
```



UNIVERSITY OF
WATERLOO

SNMP Extensions

```
#!/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 '}' -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
```

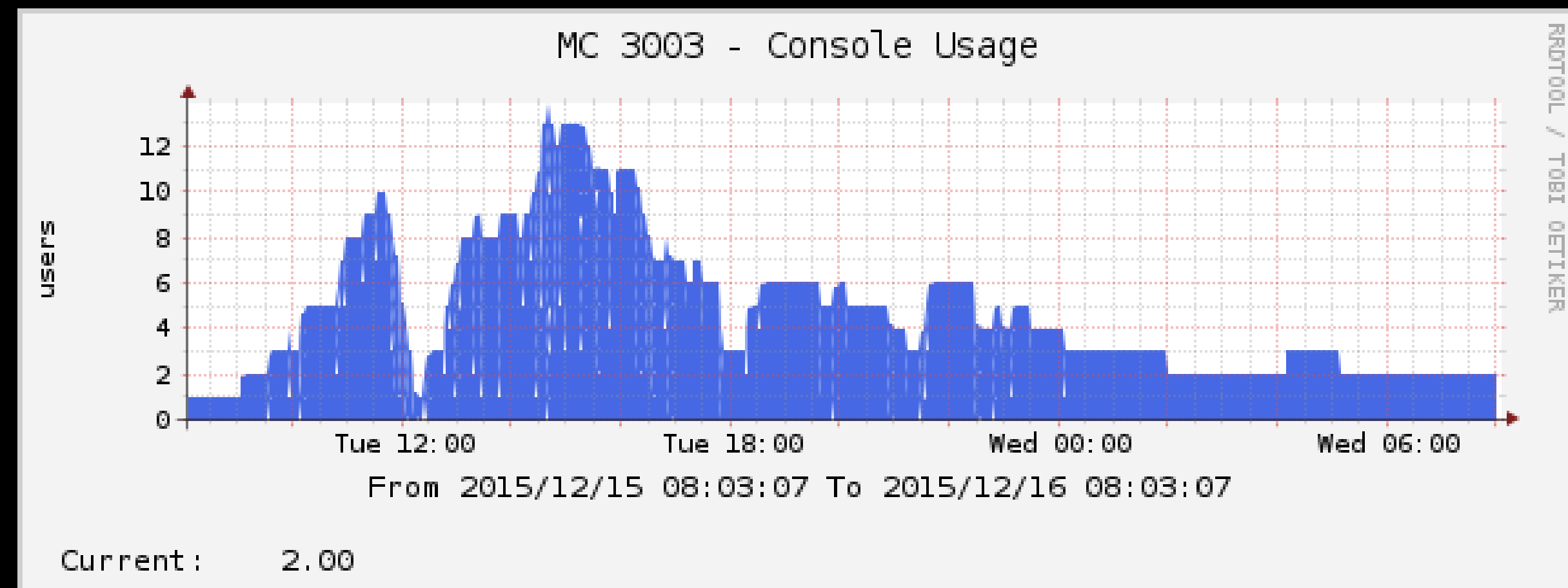
```
        echo "1"
```

```
    fi
```

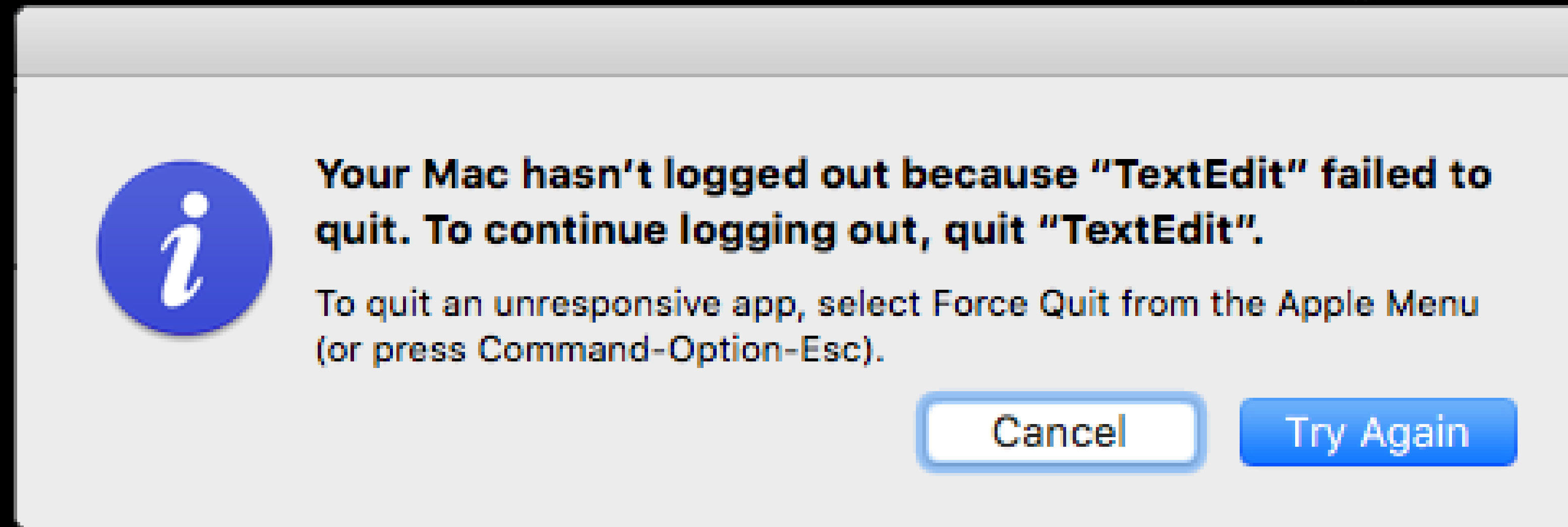
```
else
```

```
    echo "0"
```

```
fi
```

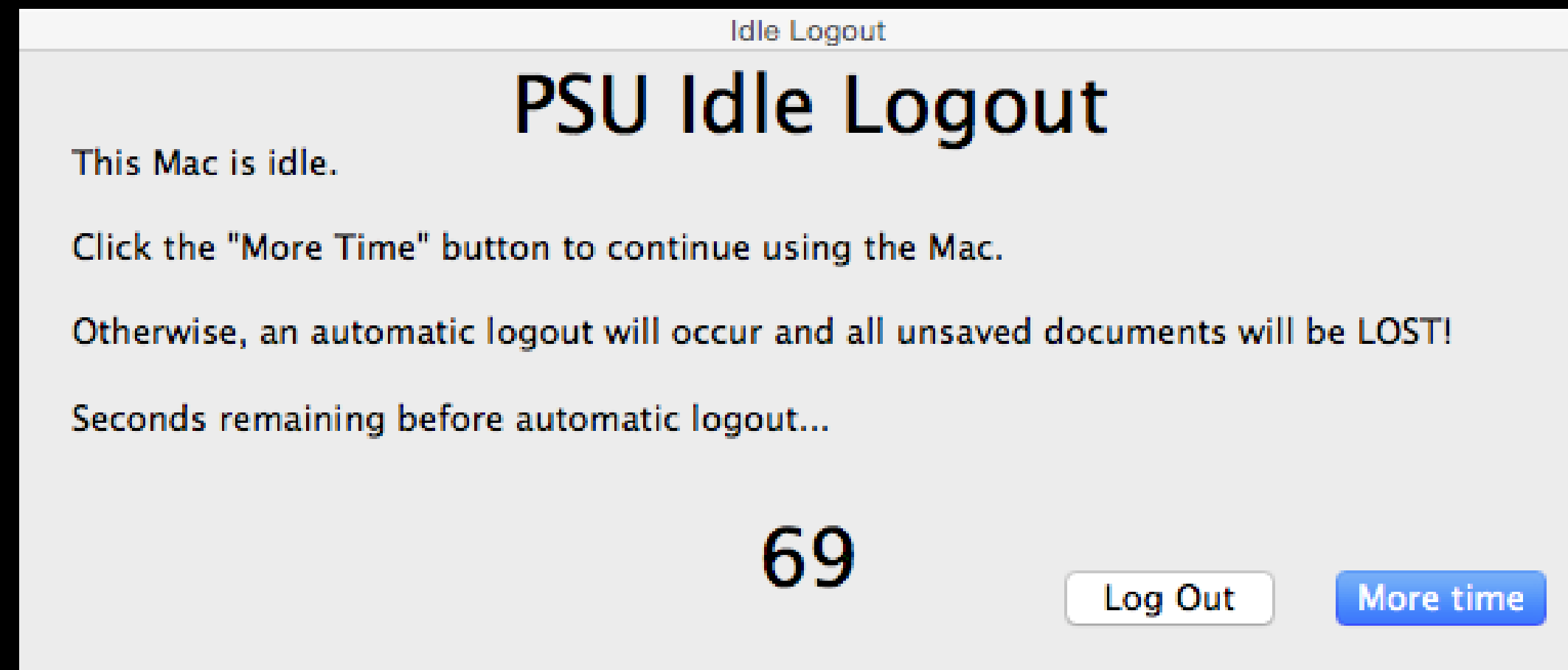


SNMP Extensions



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

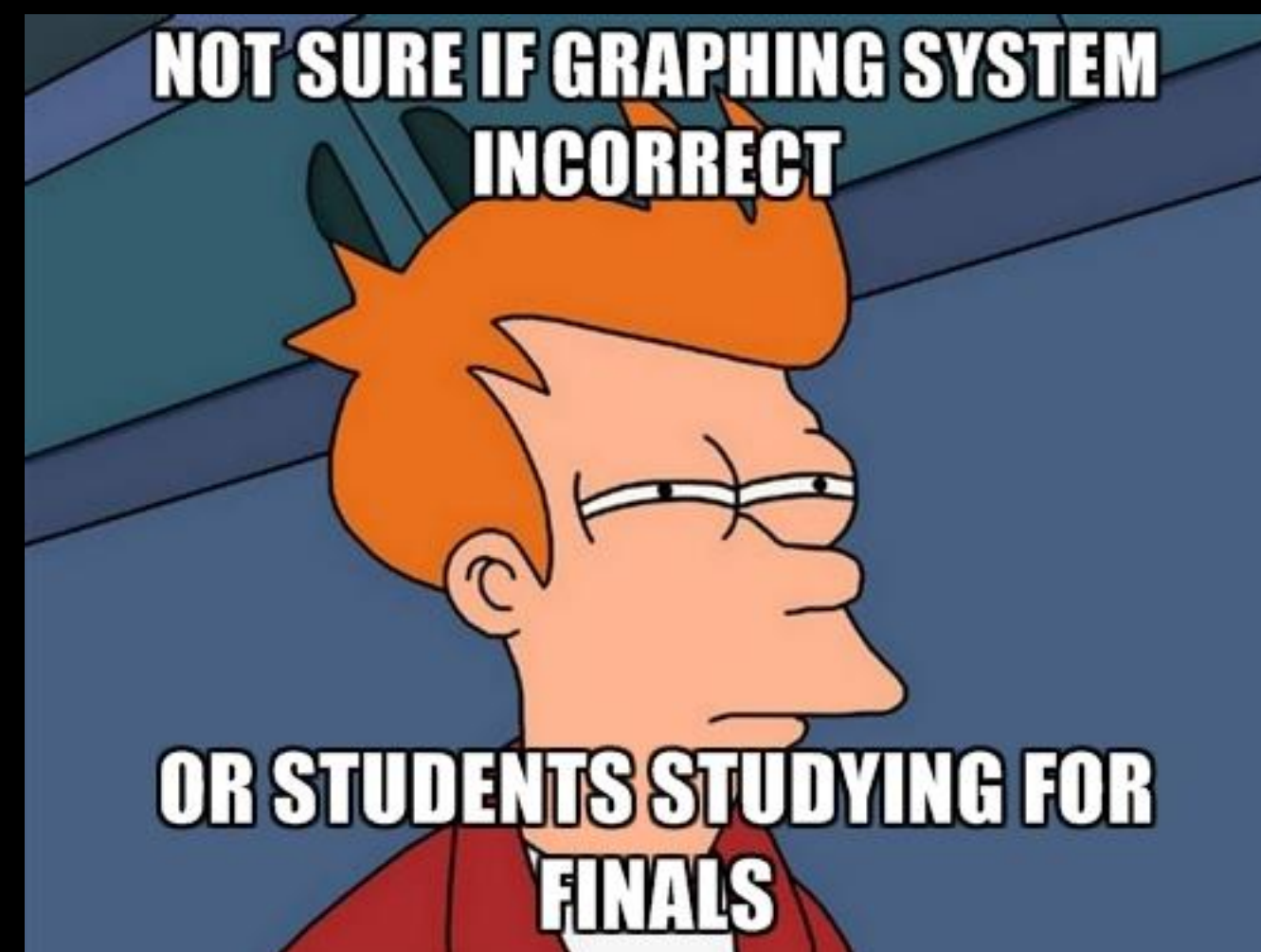
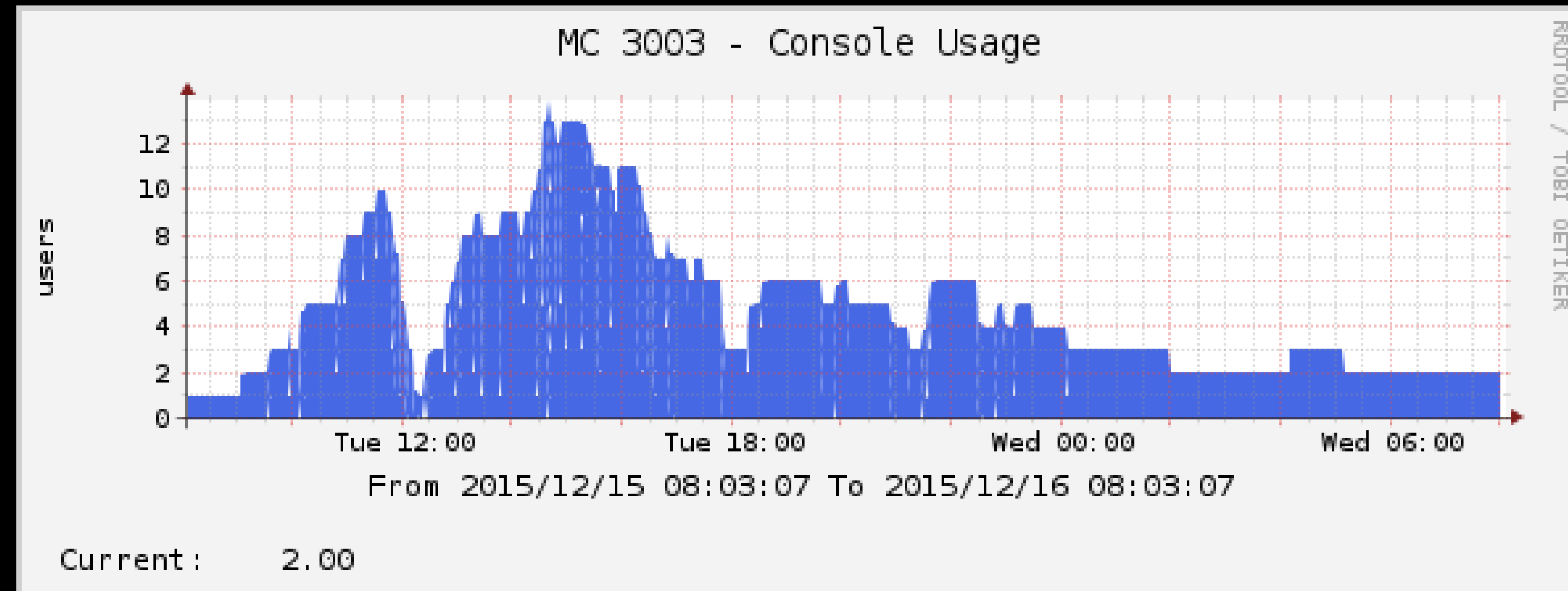


<https://github.com/CLCMacTeam/IdleLogout>

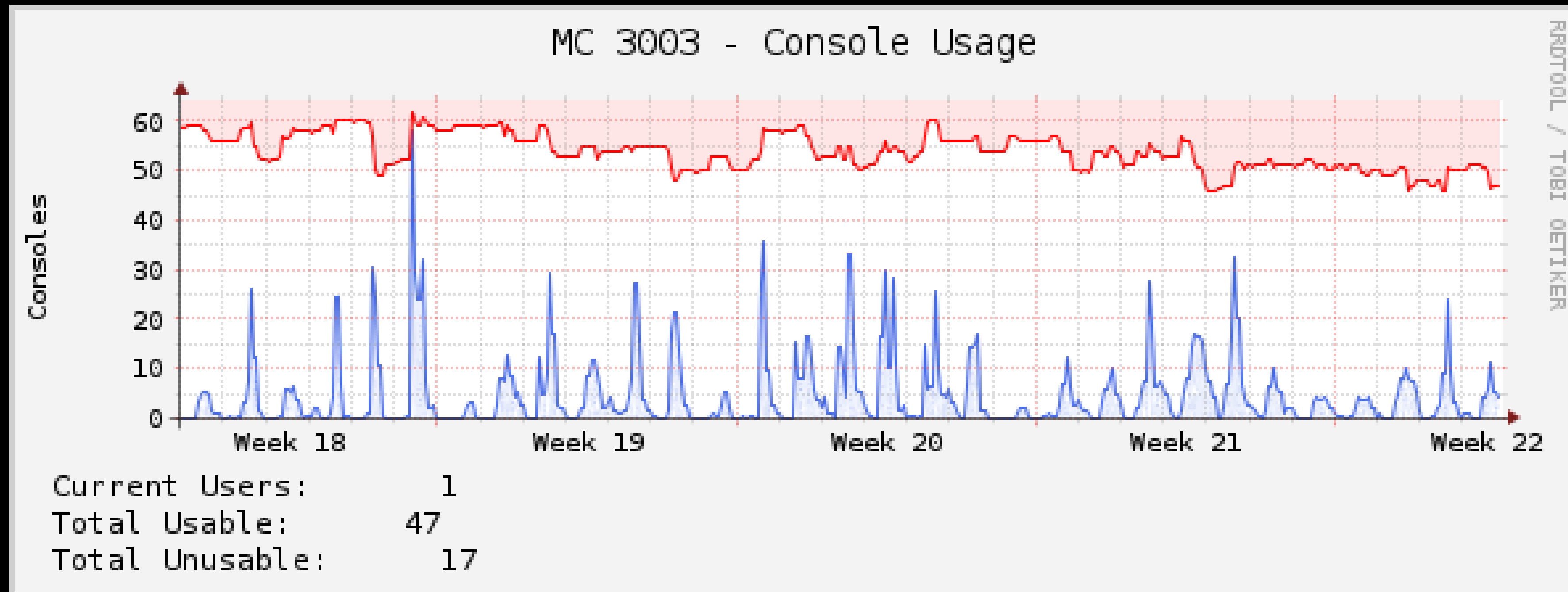


UNIVERSITY OF
WATERLOO

SNMP Extensions































SNMP Extensions





























Lab usage graphs *should* go to zero during off-hours

DC-3558-B7-PDU-1

State		Label	Energy (kWh)	Real Power (W)	Apparent Power (VA)	Power Factor (%)	Voltage (V _{RMS})	Peak Voltage (V)	Current (A _{RMS})	Peak Current (A)
	 	BladeUPS Feed	4367	1034	1185	87	211.6	211.7	5.60	6.35

State		Label	Energy (kWh)	Real Power (W)	Apparent Power (VA)	Power Factor (%)	Voltage (V _{RMS})	Peak Voltage (V)	Current (A _{RMS})	Peak Current (A)
	 	Circuit 1	2491	756	855	88	212.0	212.2	4.03	4.95
✓	 	Outlet 1								
✓	 	Outlet 2								
✓	 	Outlet 3								
✓	 	Outlet 5								
✓	 	Outlet 5								
✓	 	Outlet 6								
✓	 	Outlet 7								
✓	 	Outlet 8								
✓	 	Outlet 9								
✓	 	Outlet 10								
✓	 	Outlet 11								
✓	 	Outlet 12								

	 	Circuit 2	1854	274	333	82	212.8	213.0	1.57	1.63
✓	 	Outlet 13								
✓	 	Outlet 14								
✓	 	Outlet 15								
✓	 	Outlet 16								
✓	 	Outlet 17								
✓	 	Outlet 18								
✓	 	Outlet 19								
✓	 	Outlet 20								
✓	 	Outlet 21								
✓	 	Outlet 22								
✓	 	Outlet 23								
✓	 	Outlet 24								

Data Queries

pduChannelWyeTable

pduChannelWyeIndex

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

pduChannelWyeLabel

pduChannelWyeLabel.1.1 = STRING: "BladeUPS Feed"
pduChannelWyeLabel.1.2 = STRING: "Circuit 1"
pduChannelWyeLabel.1.3 = STRING: "Circuit 2"

pduChannelWyeVolts

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

pduChannelWyeAmps

pduChannelWyeAmps.1.1 = Gauge32: 560
pduChannelWyeAmps.1.2 = Gauge32: 403
pduChannelWyeAmps.1.3 = Gauge32: 157

Data Queries

```
<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>
```

Data Queries

```
<fields>  
  <pduChannelWyeLabel>  
    <name>Label</name>  
    <method>walk</method>  
    <source>value</source>  
    <direction>input</direction>  
    <oid>.1.3.6.1.4.1.21239.6.1.99.4.1.2</oid>  
  </pduChannelWyeLabel>  
</fields>
```

“input” fields are cached, they are used for labels and legends. “output” fields are queried when the poller runs.

Data Queries

Data Query [Mellanox Sensors]				
Showing All Items				
Index	Type	Description	Units	<input type="checkbox"/>
200021021	Fan Sensor	MGMT/FAN1/F1	RPM	<input type="checkbox"/>
200022021	Fan Sensor	MGMT/FAN2/F1	RPM	<input type="checkbox"/>
200023021	Fan Sensor	MGMT/FAN3/F1	RPM	<input type="checkbox"/>
200024021	Fan Sensor	MGMT/FAN4/F1	RPM	<input type="checkbox"/>
200030011	Temperature Sensor	MGMT/BOARD_MONITOR/T1	Celsius	<input type="checkbox"/>
200040011	Temperature Sensor	MGMT/CPU_BOARD_MONITOR/T1	Celsius	<input type="checkbox"/>
200040012	Temperature Sensor	MGMT/CPU_BOARD_MONITOR/T2	Celsius	<input type="checkbox"/>
200050011	Temperature Sensor	MGMT/SX/T1	Celsius	<input type="checkbox"/>
200181011	Temperature Sensor	MGMT/QSFP_TEMP1/T1	Celsius	<input type="checkbox"/>
200182011	Temperature Sensor	MGMT/QSFP_TEMP2/T1	Celsius	<input type="checkbox"/>
200183011	Temperature Sensor	MGMT/QSFP_TEMP3/T1	Celsius	<input type="checkbox"/>

“input” fields are cached, they are used for labels and legends. “output” fields are queried when the poller runs.

Data Queries

entPhySensorTable

entPhySensorValue

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

200021021

entPhySensorTable.200021021 = INTEGER: 200021021

200022021

entPhySensorTable.200022021 = INTEGER: 200022021

200023021

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

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

200021021

entPhySensorTable 200021021 = INTEGER: 200021021

200022021

entPhySensorTable 200022021 = INTEGER: 200022021

200023021

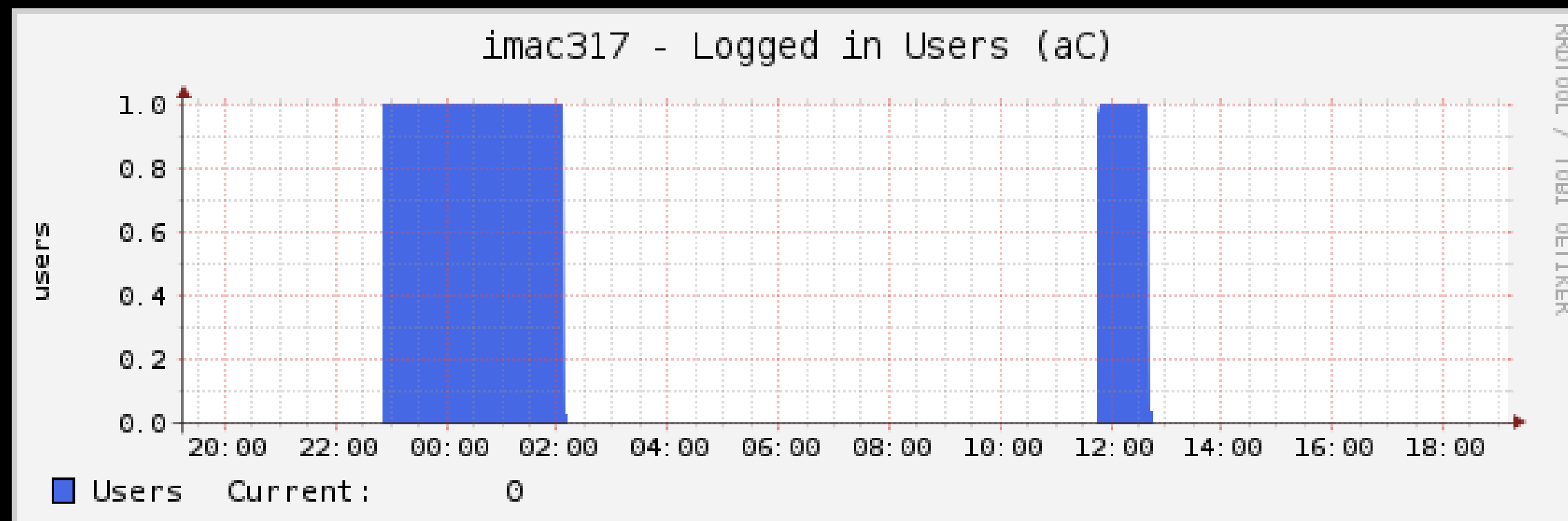
entPhySensorTable 200023021 = INTEGER: 200023021

Plugins

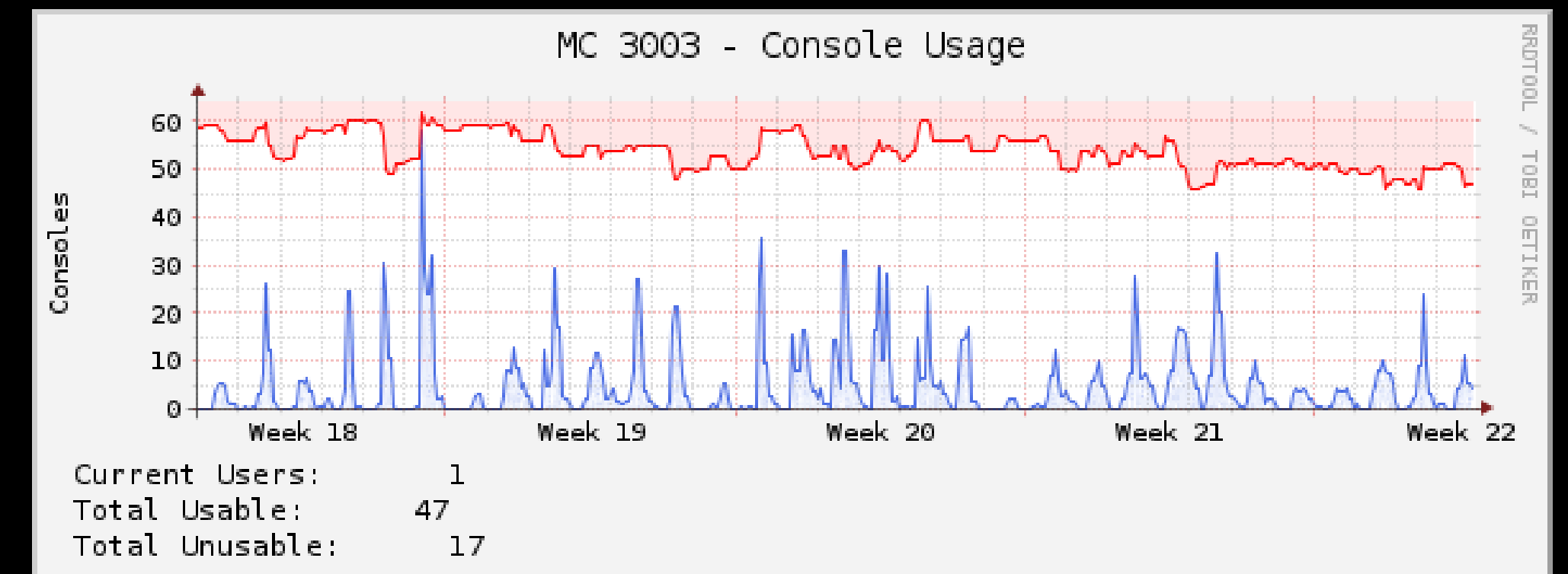
Aggregate

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.

Rule Selection [edit: Traffic - Switch - In/Out (64-bit Counters)]
Name
A useful name for this Rule.
Traffic - Switch - In/Out (64-bit Counters)
REQUIRED: Data Query
Choose a Data Query to apply to this rule.
SNMP - Interface Statistics
REQUIRED: Graph Type
Choose any of the available Graph Types to apply to this rule.
In/Out Bits (64-bit Counters)
Enable Rule
Check this box to enable this rule.
☒ Enable Rule

Rule Items => Eligible Hosts Add

Item	Sequence	Operation	Field	Operator	Pattern		
Item#1	1		host_template.name	contains	HP ProCurve	↕↕	✗
Item#2	2	OR	host_template.name	contains	Mellanox Switch	↕↕	✗

Rule Items => Create Graph Add

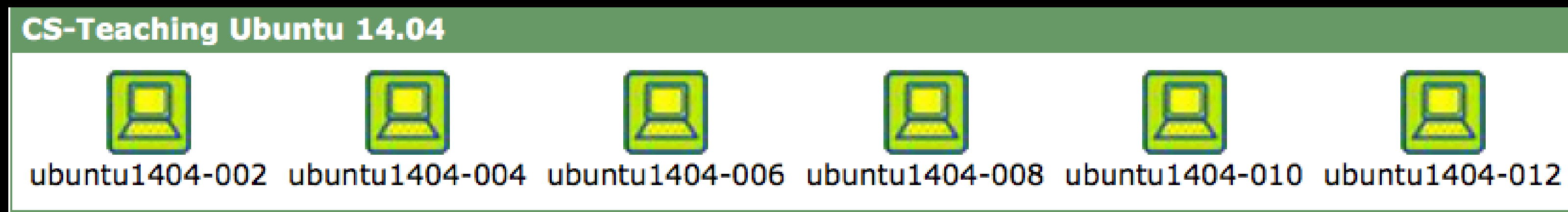
Item	Sequence	Operation	Field	Operator	Pattern		
Item#1	1		IfOperStatus	matches	Up	↕↕	✗
Item#2	3	AND	IfHwAddr	is not empty		↕↕	✗
Item#3	4	AND	IfDescr	does not contain	VLAN	↕↕	✗
Item#4	5	AND	IfSpeed	does not match with	0	↕↕	✗

Cancel Save

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.

Default Alerting Options	
Weekend exemptions If this is checked, thold will not run on weekends.	<input type="checkbox"/> Weekend exemptions
Default Trigger Count Default number of consecutive times the Data Source must be in breach of the Threshold for an Alert to be raised	<input type="text" value="1"/>
Re-Alerting Repeat Alert after specified number of poller cycles.	<input type="text" value="12"/>
Syslog Support 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	<input type="checkbox"/> Syslog Support
Syslog Level This is the priority level that your syslog messages will be sent as.	<input type="text" value="Warning"/>
Syslog Facility This is the facility level that your syslog messages will be sent as.	<input type="text" value="Daemon"/>
Emailing Options	
Send Emails with Urgent Priority Allows you to set e-mails with urgent priority	<input type="checkbox"/> Send Emails with Urgent Priority
Dead Hosts Notifications Enable Dead/Recovering host notification	<input checked="" type="checkbox"/> Dead Hosts Notifications
Dead Host Notifications Email This is the Email Address that the Dead Host Notifications will be sent to if the Global Notification List is selected.	<input type="text"/>
Down Host Subject This is the Email subject that will be used for Down Host Messages.	<input type="text" value="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

<https://bit.ly/psumac2016-97>



UNIVERSITY OF
WATERLOO