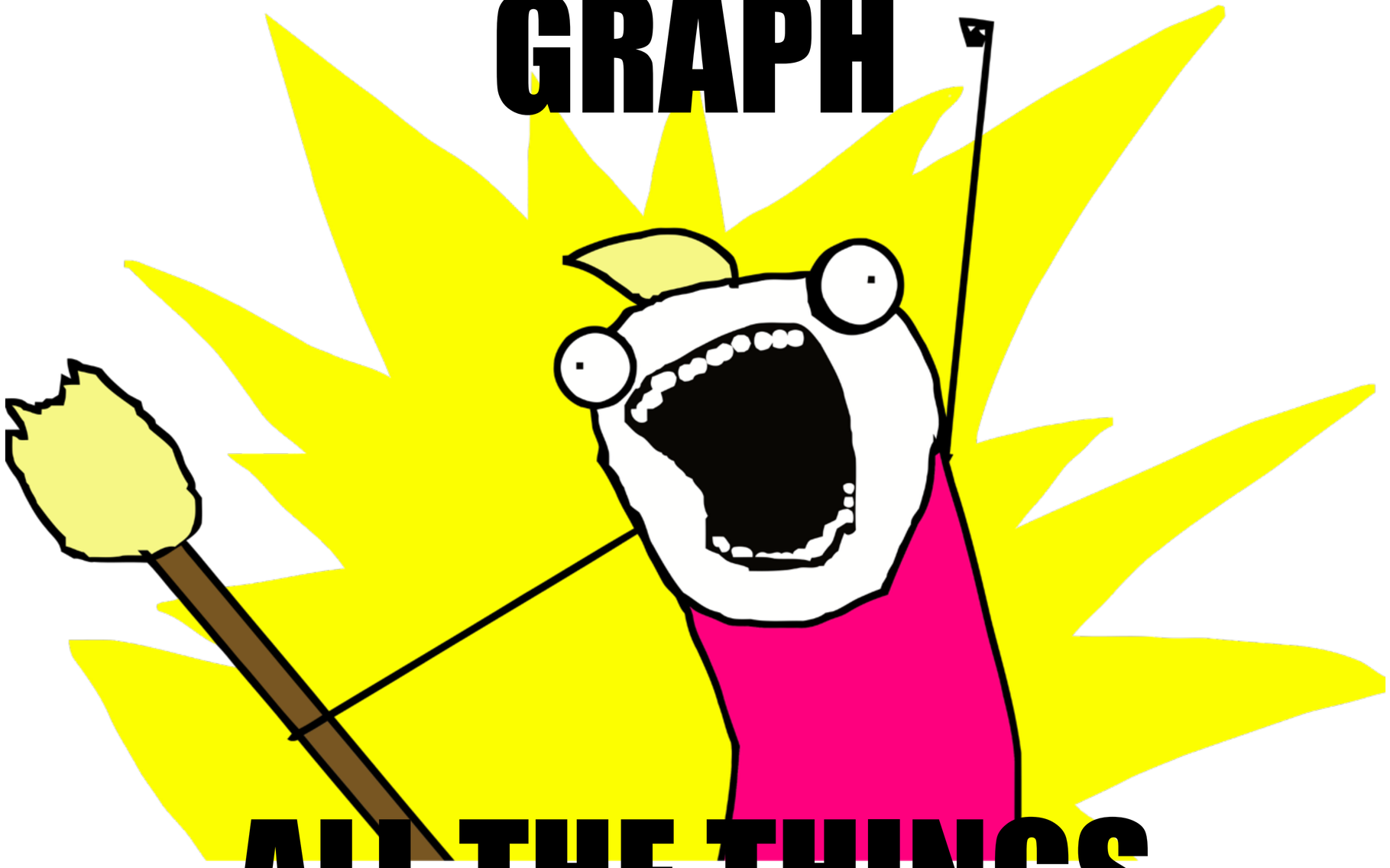
GRAPH



ALL THE THINGS

An SNMP and alerting primer featuring Observium

If you want to learn about moving a datacenter, you’re in the wrong talk.

Go heckle my buddy Steve in 208.

About Me

@refrshingapathy

@refreshingapathy

github.com/rickheil

2016 MACADMINS CONFERENCE AT PENN STATE®

Today's slides and links are available now at
rickheil.com/psu2016

About Me

- Half of the IT team for PARTNERS+simons, an integrated marketing and advertising agency
- Heavy focus on end-user empowerment and self-service
- Munki and Meraki MDM in production
- ~100 employees and growing fast!
- Avid musician, home chef, and motorcyclist

If you see me on your way home, wave!

Overview

- Alerting Theory: Why monitor?
- SNMP: is it actually simple?
- SNMP: really, just one config file?
- SNMP: how do I secure it?
- SNMP: extending your agent
- Observium: overview of centralized monitoring
- Observium: alerting demo
- Q&A

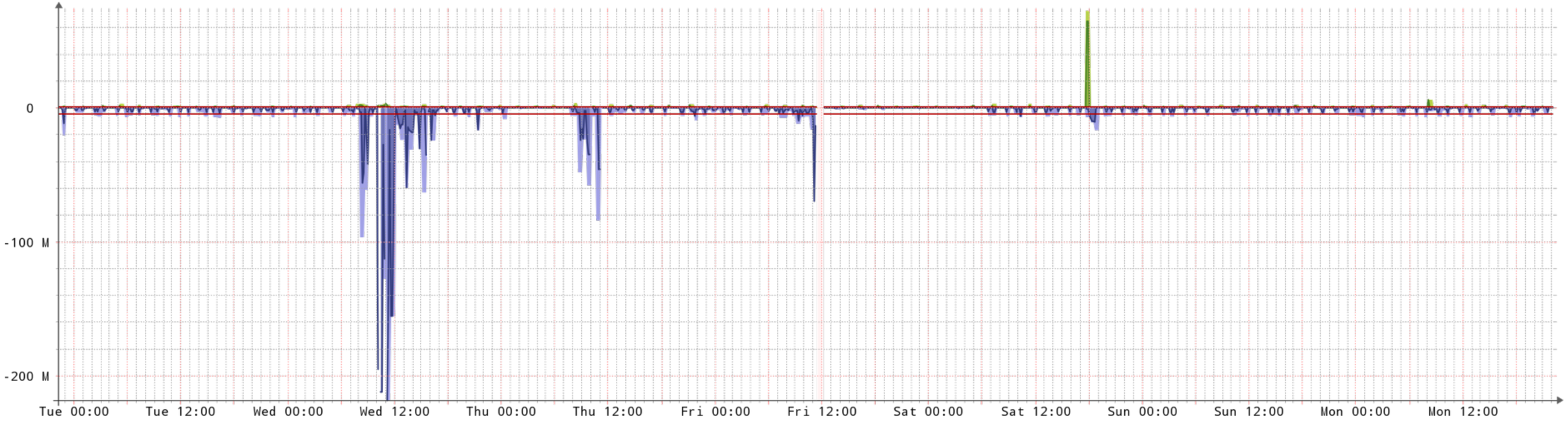
How urgent was the last problem that woke you up?

Should it have woken you up?

Did your alerting wake you up? Or your users?

Why do we monitor?

- Enable proactive problem solving
- Enhance security with historical data
- Reduce support time (cost)
- Look at pretty graphs



Bits/s	Last	Avg	Max	95th
In	18.60k	250.02k	72.30M	1.18M
Out	12.55k	2.53M	218.43M	4.06M

Total 207.52G (In 18.79G Out 189.01G)

Finding your alerting balance

- Spammy emails get ignored
- Over alerting can be just as bad as under-alerting!
- Too many notifications wastes your time, and therefore your money.
- You’re less likely to pick out the problems if you don’t let your alerting system do the sorting for you

How can I streamline my alerts?

The Four Step Alert Test

1. Is the alert impact-based, or does it have a clear reason to be cause-based?
2. Is the alert actionable?
3. Is the alert threshold reasonable?
4. Is the alert notification targeted?

Cause or Impact Based

- Cause based is great information for IT people
- Cause-based data is generally statistical in nature and reflects hardware information
- Impact based is great information for IT to get a sense of the user's experience.
- Impact-based data generally comes from monitoring the end user experience.

Cause or Impact Based

- Both types of data are useful for problem solving
- Alerts that are cause based lend themselves to over-alerting you
- When setting up a new alerting scheme, consider which systems should be cause based and which can be impact based.

Is the alert actionable?

- If an alert is just an FYI… should it really be an alert?
- Alerts should notify you of a problem to solve either now or very shortly in the future.

Is the threshold reasonable?

- Analyze the workload of the system you are monitoring
- Give yourself enough pre-warning to address a problem before it becomes critical
- But don’t let your monitoring cry wolf.
- Don’t be afraid to use trial and error for this!

Is the notification targeted?

- Keep the number of people who need to get each alert to a minimum.
- Reducing alert frequency helps reduce alert fatigue
- Test this by determining if the person getting the alert could fix the problem.

To review…

- We monitor to gather information that makes us more efficient
- Historical data is a huge benefit to your process
- Alerts need to be configured properly to avoid “alert fatigue”

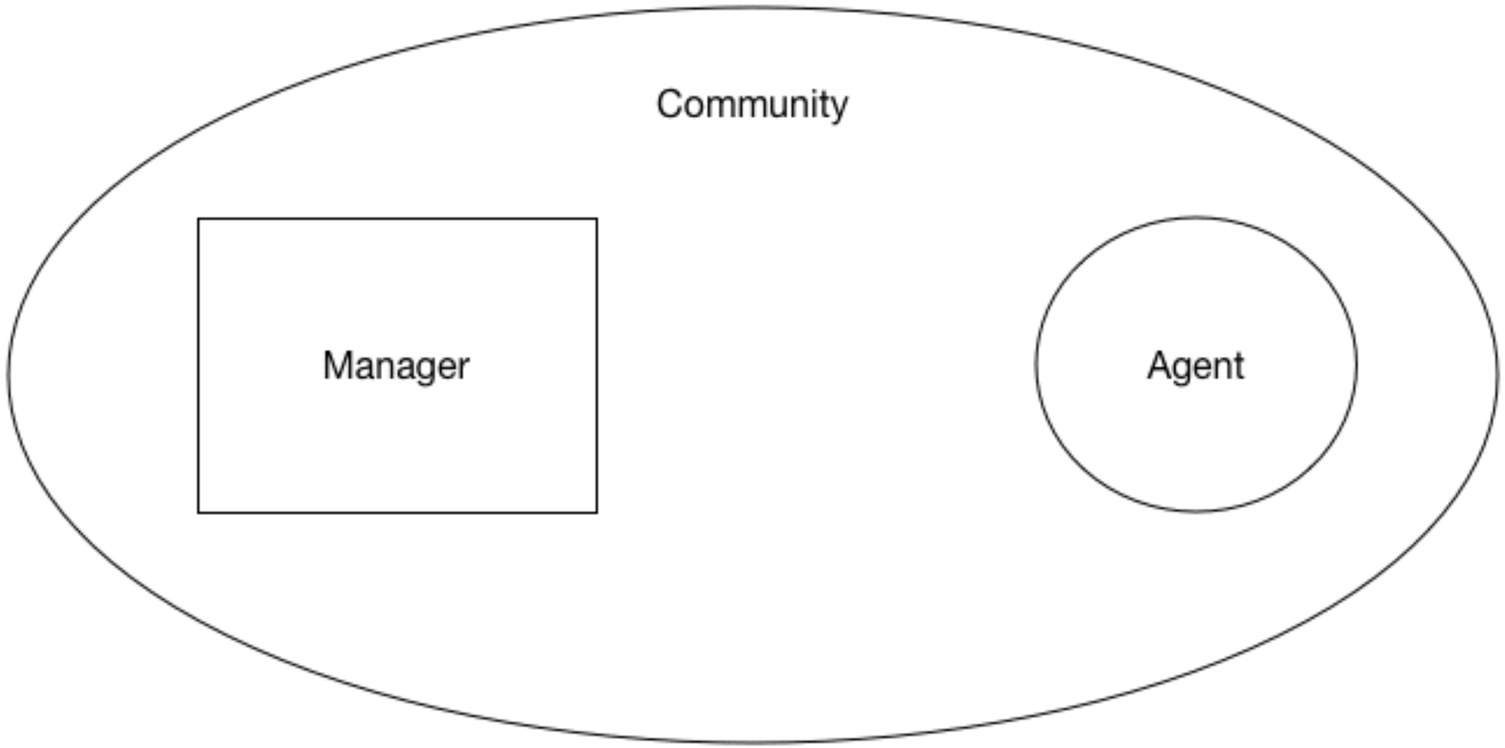
The Four Step Alert Test

1. Is the alert impact-based, or does it have a clear reason to be cause-based?
2. Is the alert actionable?
3. Is the alert threshold reasonable?
4. Is the alert notification targeted?

Simple
Network
Management
Protocol

…actually only a little simple.

Basic SNMP Terminology



Basic SNMP Terminology

- Every **agent** maintains two data sets:
  - Management data, the actual values of configuration or counters, which are labeled by an **Object ID (OID)**
  - **Management Information Base (MIB)**, an index of sorts that describes the management data and parameters (OIDs) available.

TCP-MIB Excerpt

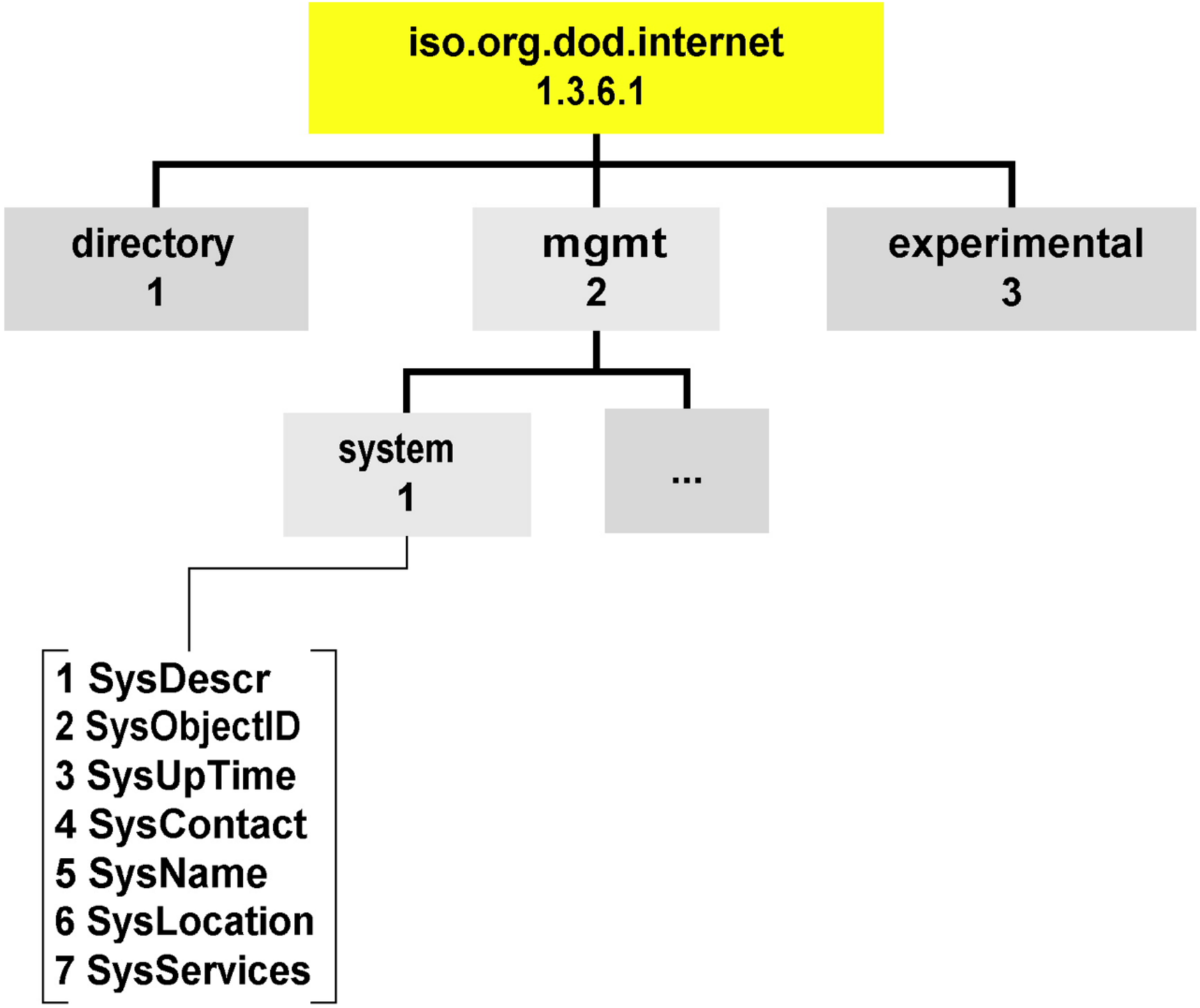
```
tcpHCInSegs OBJECT-TYPE
    SYNTAX      Counter64
    MAX-ACCESS read-only
    STATUS      current
    DESCRIPTION
            "The total number of segments received, including those
             received in error.  This count includes segments received

             on currently established connections.  This object is
             the 64-bit equivalent of tcpInSegs.

             Discontinuities in the value of this counter are
             indicated via discontinuities in the value of sysUpTime."
    ::= { tcp 17 }
```

More about OIDs

- OIDs are unique and linked to a specific piece of data, as described in the MIB
- Scalar OIDs are a single response object - something like the device model number, hostname, a value counter
- Tabular OIDs can be an array of data - something like CPU utilization on a multi-core processor
- OIDs are organized in a tree format to allow categorization and grouping of data

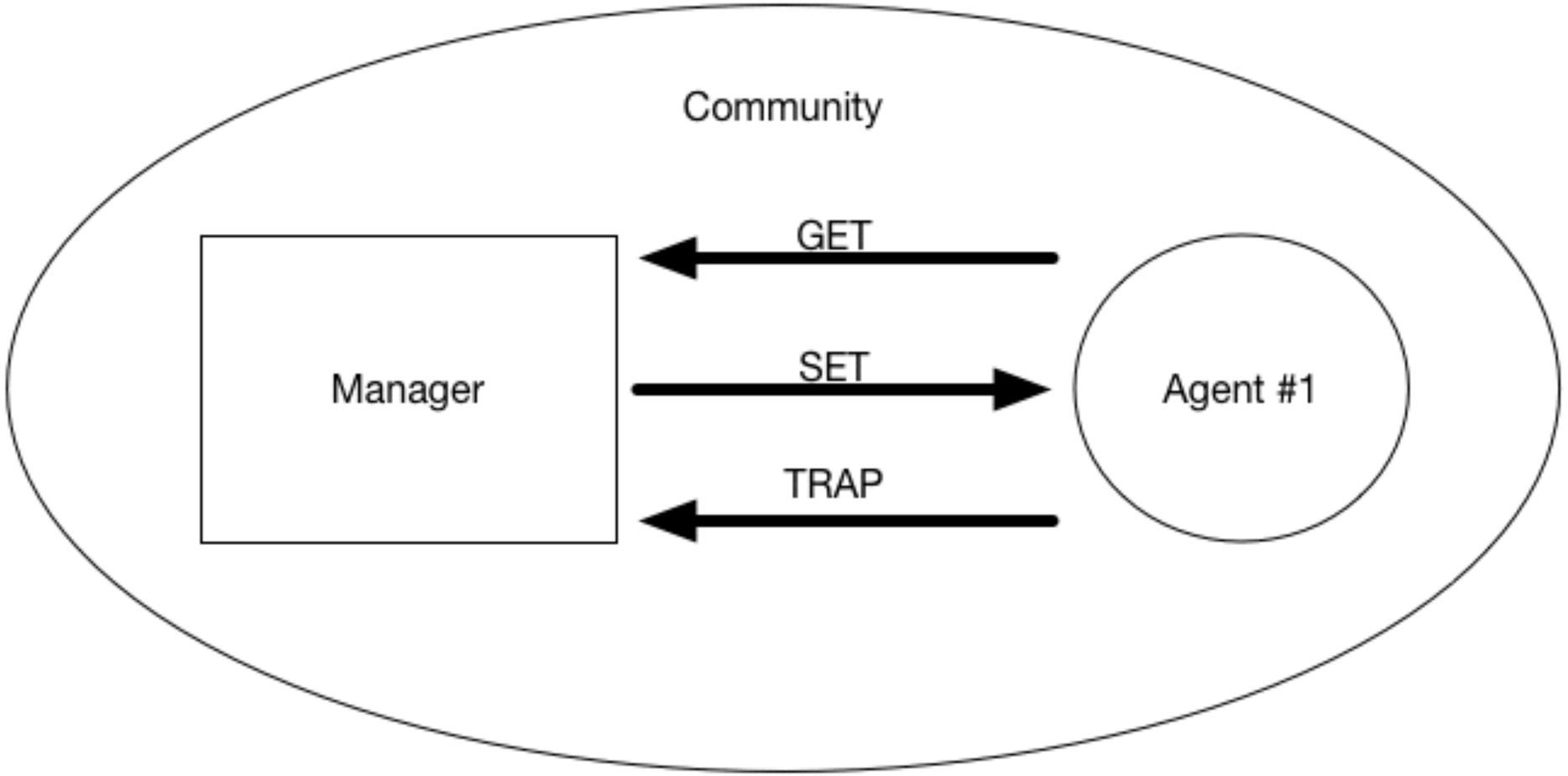

iso.org.dod.internet
1.3.6.1
directory
1
mgmt
2
experimental
3
system
1
...
1 SysDescr
2 SysObjectID
3 SysUpTime
4 SysContact
5 SysName
6 SysLocation
7 SysServices

More about OIDs

- OIDs can be represented in two ways:
  - Text, which generally start with the MIB name and allow you to trace the MIB tree. For example, a counter that shows incoming TCP network traffic is “TCP-MIB::tcpHCInSegs”
  - Numerically, in a series of dotted integers. The same OID from above is “. 1.3.6.1.2.1.6.10.17”
- You can translate between text and numeral OIDs using the snmptranslate command:
  - snmptranslate -On ‘TCP-MIB::tcpHCInSegs’ will return the numerical equivalent
  - snmptranslate -To ‘.1.3.6.1.2.1.6.10.17’ will return the textual equivalent

SNMP Methods

- Manager GETs information about a managed object.
- Manager GETNEXTs information that is next in the tree
- Manager SETs a managed object's value on the agent (if permitted)
- Agent sends a TRAP (alert) to the manager in response to predefined conditions or characteristics
- There are more methods, but these will get you started!


Community
GET
Manager
SET
Agent #1
TRAP

Useful tool: snmpwalk

- snmpwalk “walks” from the top of the MIB tree to the bottom and GETNEXTs all the data available
- Verbose output, but useful for learning and troubleshooting
- Syntax: snmpwalk -v VERSION -c COMMUNITY HOST
- Example: snmpwalk -v 2c -c rick localhost

To review…

- Data is labeled by OID and organized by MIB
- MIBs are laid out in a tree
- A manager GETs the contents of an OID to poll data
- A manager SETs the contents of an OID to alter configurations
- An agent TRAPs to the manager for alerting or notification

Version	Level	Authentication	Encryption	Process
v1	noAuthNoPriv	Community String	No	Community string match
v2 (c)	noAuthNoPriv	Community String	No	Community string match
v3	noAuthNoPriv	Username	No	Username match
v3	AuthNoPriv	MD5 or SHA	No	Auth based on HMAC
v3	authPriv	MD5 or SHA	DES	HMAC auth plus stream encryption

SNMP Versions Cheatsheet

Thanks to François and Manuel for this table from their 2015 talk!

SNMP Security

- Choose the correct version to implement (v1, v2c, v3)
- Set up your community access list to only allow trusted addresses
- Use ACLs or firewall rules as an extra safeguard
- Cisco has an excellent white paper on this (link at the end of these slides)

Making an SNMP Config

Go to your terminal and type in “snmpconf”

Quick Aside: extending SNMP with custom scripts

In your snmpd.conf…

- “Extend” is a powerful tool to return data from non-SNMP aware applications
- Used to execute scripts or pull other metrics in and pass them through SNMP
- Leverages the NET-SNMP-EXTEND-MIB

Example:

- This line in the configuration: exec osversion /usr/local/bin/osversion
- With this script:

```
#!/bin/bash

sw_vers | grep ProductVersion | awk '{print $2}'

exit 0
/usr/local/bin/osversion (END)
```

- Gets us this when we snmpget:

```
[ rickheil@rick-heil ~ ]$ snmpget -v2c -c psumac localhost 'NET-SNMP-EXTEND-MIB::nsExtendOutLine."osversion".1'
NET-SNMP-EXTEND-MIB::nsExtendOutLine."osversion".1 = STRING: 10.11.5
```

To review…

- Use v3 authPriv in production whenever possible
- Firewall / ACL as well as use host/IP range restrictions in config
- snmpconf will walk you through configuration options
- extend is freakin’ awesome
- sorry, no cat on this slide

Management Software

- Many solutions - Cacti, Zenoss, Spiceworks, OpenNMS, Observium
- Pick one that meets your feature needs and your budget
- We prefer Observium because:
  - self hosted
  - written in PHP so I can modify and extend it as needed
  - does a few things and does them well instead of trying to be everything to everyone

Observium demo

Links and Resources

- Securing SNMP - Cisco - http://bit.ly/28ZSoYf
- “Entering the Awesome World of SNMP” talk from 2015: https://www.youtube.com/watch?v=iY1y9DQBvVQ
- Observium: http://www.observium.org

Image Attributions

- Balancing Rock photo from Terry Robinson (CC-BY-SA) https://www.flickr.com/photos/suburbanadventure/15945627666
- Archery Target by Ann Oro (CC-BY-SA) https://www.flickr.com/photos/njtechteacher/7564364494
- Cute cat by Laurinha Lii https://www.flickr.com/photos/mundoworldmonde/5621803163
- SNMP versions table by François Joannette and Manuel Deschambault http://macadmins.psu.edu/wp-content/uploads/sites/24696/2015/07/psumac2015-132-Entering_the_Awesoe_World_of_SNMP.pdf
- Observium mascot from http://www.observium.org

Q&A / Connect with Me

@refrshingapathy

@refreshingapathy

github.com/rickheil

Feedback: bit.ly/psumac2016-96

Today's slides and links are available now at
rickheil.com/psu2016

2016
MACADMINS
CONFERENCE
AT PENN STATE®