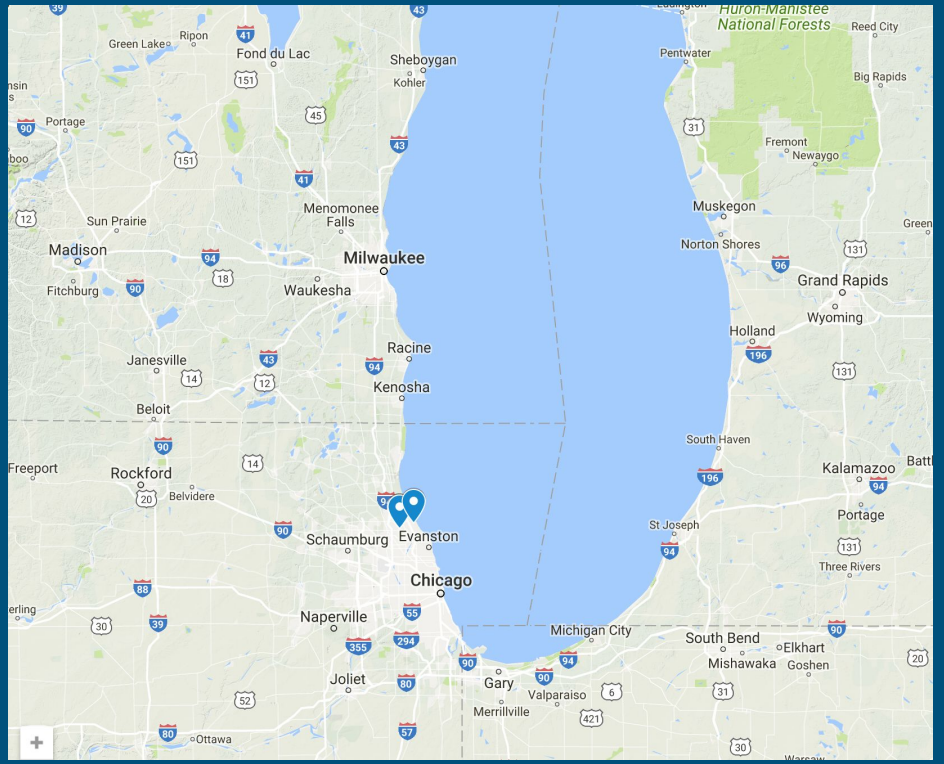
Monitoring systems using Open Source Tools

Randy Saeks, Network Manager
Glencoe School District 35
Glencoe, IL
@rsaeks

Distinguished Educator

Background

- 16-years in K-12 EdTech
- Systems Integration
- Conference Presentations
- iOS Deployment
- G-Suite for Edu Deployment



What is happening

And let us know

What are the trends

And how can we be ready

Why did it occur

And should we be worried

Tools

Alerting via Nagios

Monitoring via Cacti

Logging via ELK

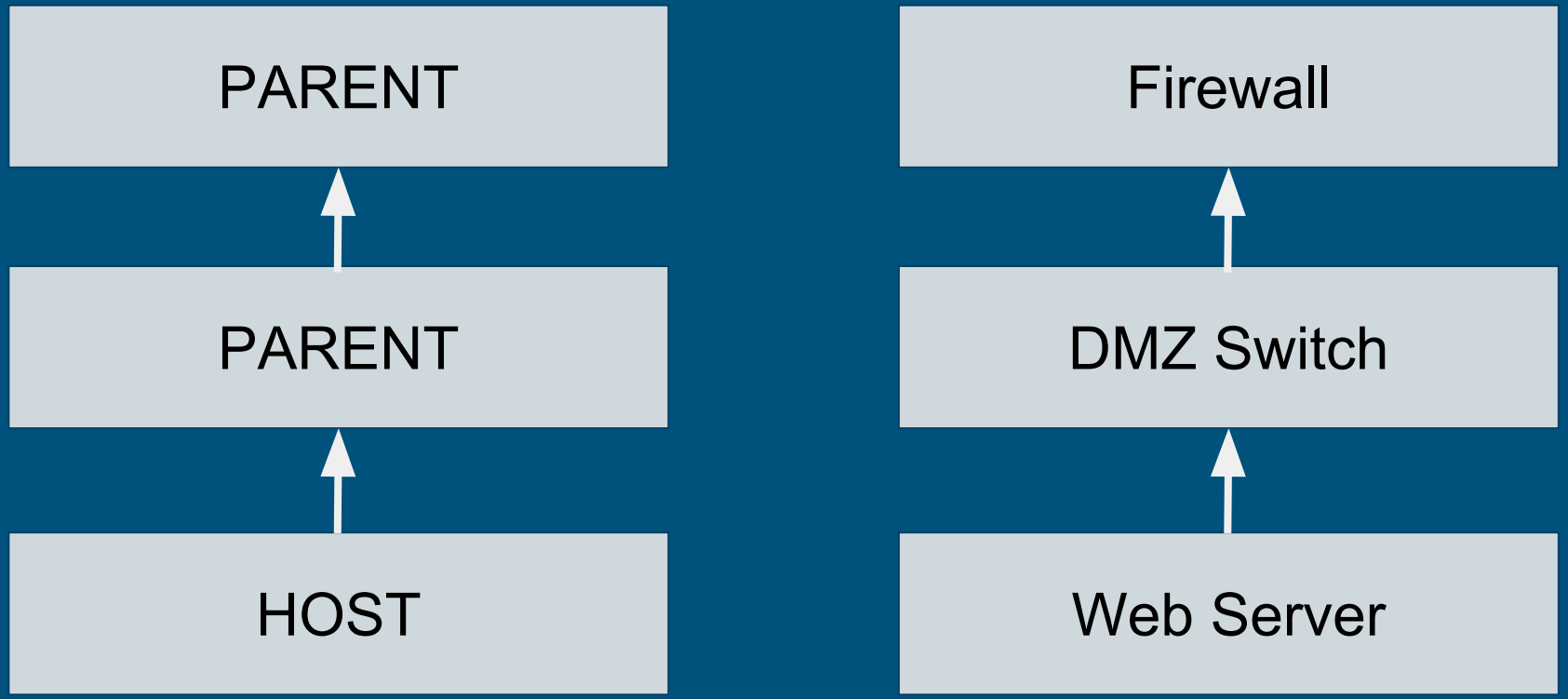
Alerting

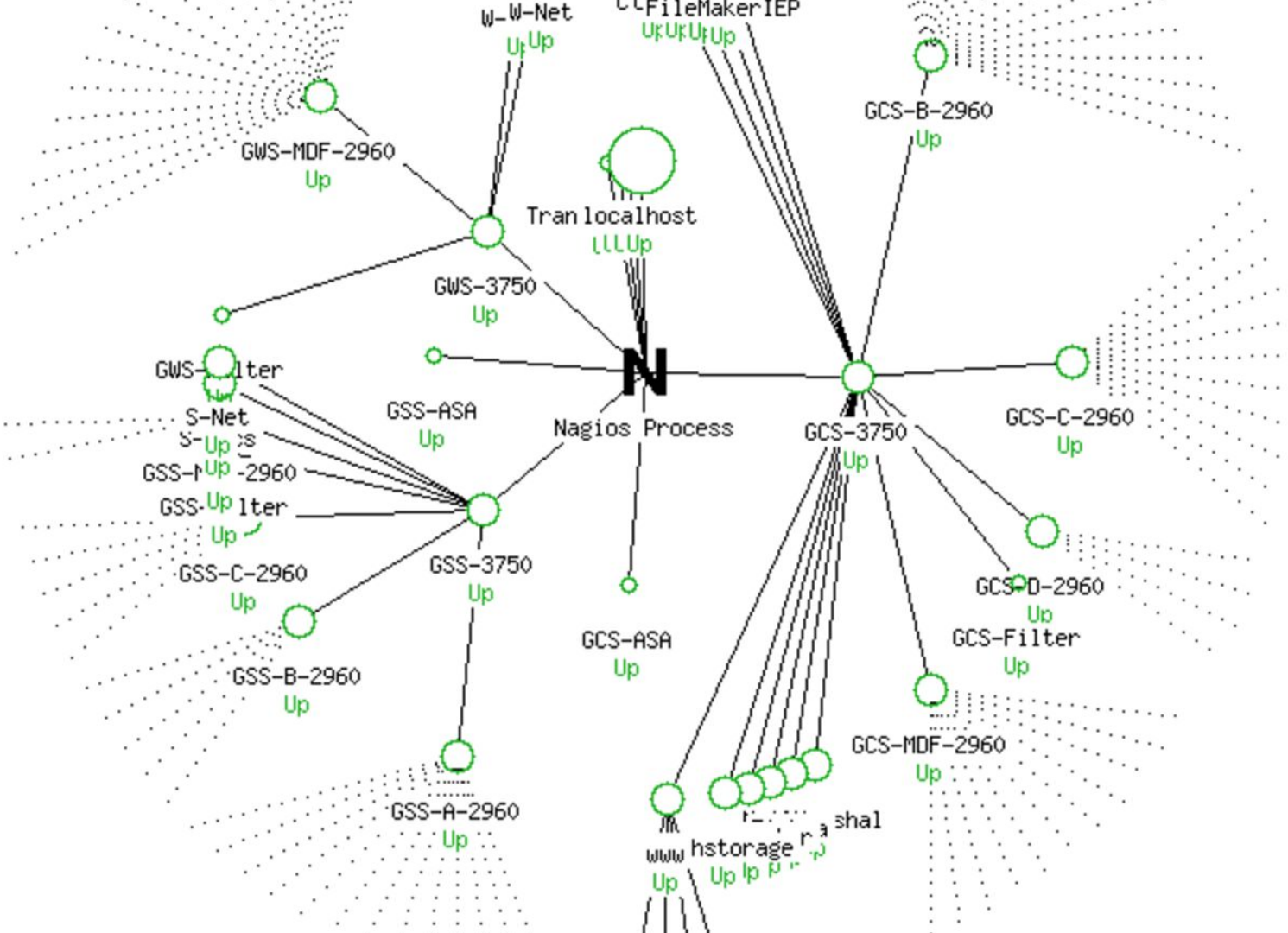
- Focused around current state of operation
- Indicates server or service health
- Functional area notifications

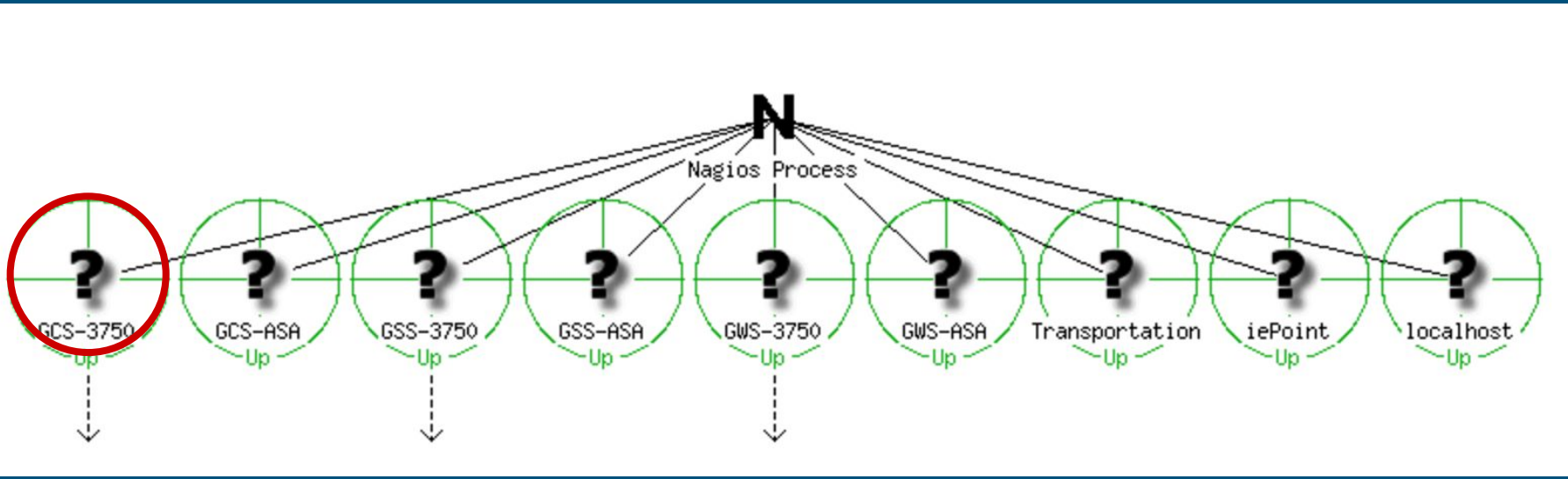
https://media.giphy.com/media/FXGoDrsgrNLj2/giphy.gif

Alerting | NAGIOS

- Create structure
- Extend with service plugins
- Define relevant alerting times
- Basic reporting ability


PARENT
PARENT
HOST
Firewall
DMZ Switch
Web Server


W-W-Net
Up
FileMakerIEP
Up
GCS-B-2960
Up
GWS-MDF-2960
Up
Tran localhost
Up
GWS-3750
Up
GSS-ASA
Up
Nagios Process
GCS-3750
Up
GCS-C-2960
Up
GSS-3750
Up
GSS-C-2960
Up
GSS-B-2960
Up
GCS-ASA
Up
GCS-D-2960
Up
GCS-Filter
Up
GCS-MDF-2960
Up
GSS-A-2960
Up
hstorage
Up

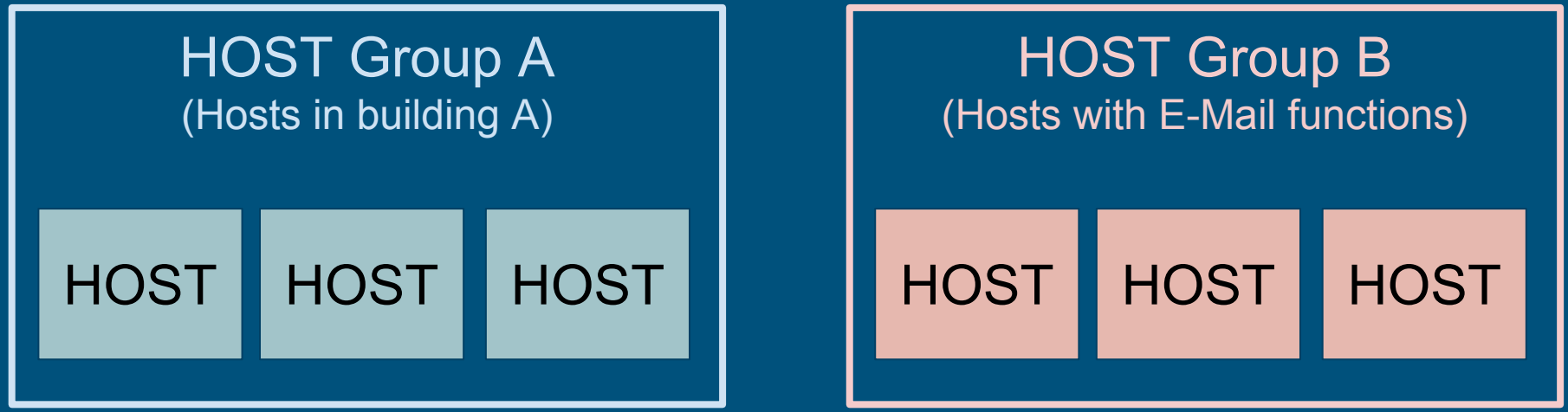

N
Nagios Process
GCS-3750
Up
GCS-ASA
Up
GSS-3750
Up
GSS-ASA
Up
GWS-3750
Up
GWS-ASA
Up
Transportation
Up
iePoint
Up
localhost
Up

Define Host

```
define host {
    host_name           ESXi
    alias               GCS-ESXI-01
    address             192.168.40.24
    parents             GCS-3750
    contact_groups      admins
}
```

Create Structure

```
define hostgroup{
    hostgroup_name    web-servers
    alias             Web Servers
    members     www,glencoecentral,glencoesouth,glencoewest,intranet
}
```

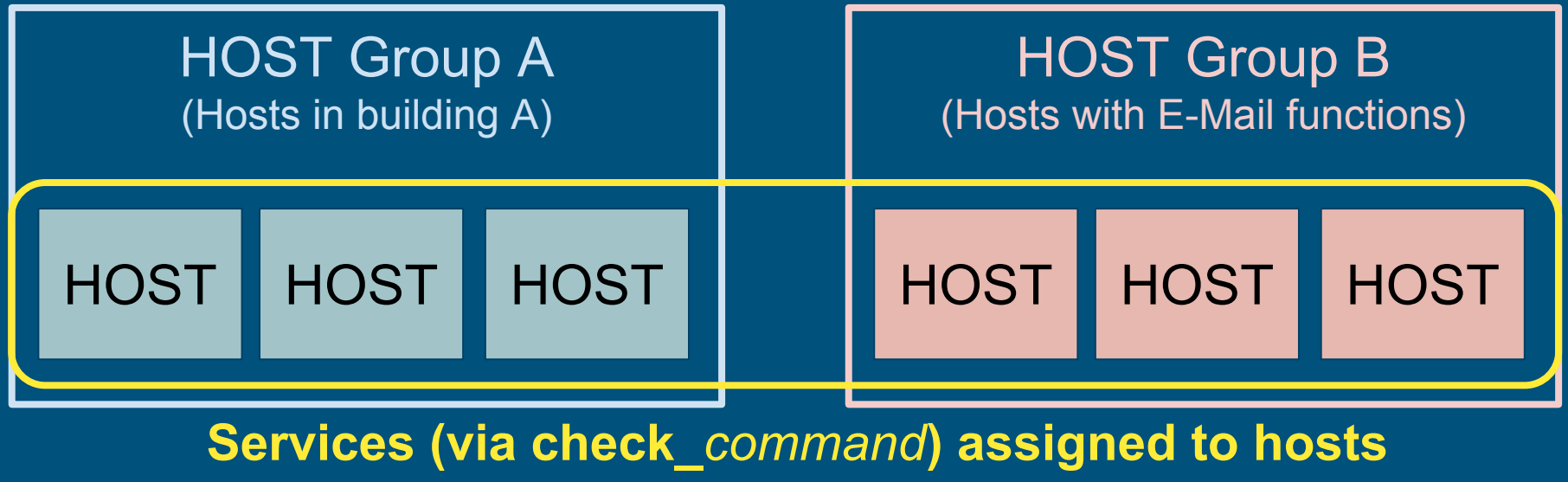

HOST Group A
(Hosts in building A)
HOST
HOST
HOST
HOST Group B
(Hosts with E-Mail functions)
HOST
HOST
HOST

Extend with service plugins

```
define command{
    command_name    check-host-alive
    command_line    $USER1$/check_ping -H $HOSTADDRESS$ -w 3000.0,80% -c 5000.0,100%
}
```

Assign Services to Hosts

```
define service{
    host_name                ns1,S-Net,W-Net
    service_description      DNS
    check_command            check_dns!$HOST$!www.apple.com!.200!.500
    contact_groups           admins
}
```


HOST Group A
(Hosts in building A)
HOST Group B
(Hosts with E-Mail functions)
HOST
HOST
HOST
HOST
HOST
HOST
Services (via check_*command*) assigned to hosts

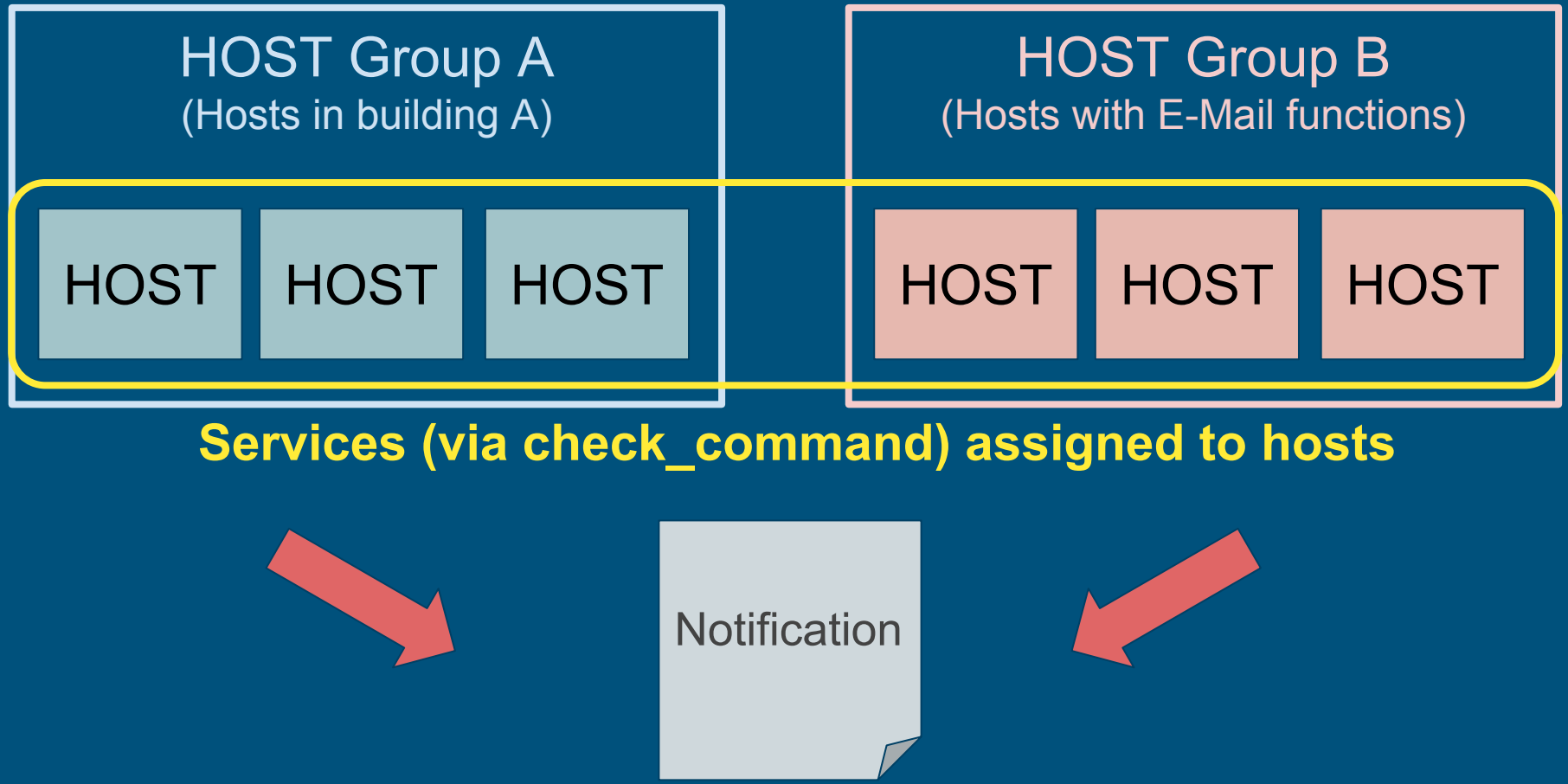
Functional Area Notifications

```
define contact {
    contact_name            saeksr
    alias                   Randy Saeks
    email                   saeksr@glencoeschools.org
}

define contactgroup {
    contactgroup_name       admins
    alias                   Nagios Administrators
    members                 saeksr
}
```

Define relevant alerting times

```
define timeperiod {
    timeperiod_name    InHours
    alias              Included Hours Hours, 7AM - 5PM
    monday             07:00 - 17:00
    tuesday            07:00 - 17:00
    wednesday          07:00 - 17:00
    thursday           07:00 - 17:00
    friday             07:00 - 17:00
}
```


HOST Group A
(Hosts in building A)
HOST Group B
(Hosts with E-Mail functions)
HOST
HOST
HOST
HOST
HOST
HOST
Services (via check_command) assigned to hosts
Notification

Hostgroup 'IDFs' Host State Breakdowns:

Host	% Time Up	% Time Down	% Time Unreachable	% Time Undetermined
GCS-B-2960	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
GCS-C-2960	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
GCS-D-2960	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
GCS-MDF-2960	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
GSS-A-2960	99.376% (99.376%)	0.026% (0.026%)	0.598% (0.598%)	0.000%
GSS-B-2960	99.384% (99.384%)	0.018% (0.018%)	0.597% (0.597%)	0.000%
GSS-C-2960	99.405% (99.405%)	0.003% (0.003%)	0.592% (0.592%)	0.000%
GSS-MDF-2960	99.407% (99.407%)	0.000% (0.000%)	0.593% (0.593%)	0.000%
GWS-MDF-2960	99.422% (99.422%)	0.000% (0.000%)	0.578% (0.578%)	0.000%
Average	99.666% (99.666%)	0.005% (0.005%)	0.329% (0.329%)	0.000%

July 05, 2017 11:00

[07-05-2017 11:01:56] SERVICE ALERT: techstorage;PING;OK;SOFT;2;PING OK - Packet loss = 0%, RTA = 0.43 ms
[07-05-2017 11:01:08] HOST ALERT: techstorage;UP;SOFT;2;PING OK - Packet loss = 0%, RTA = 0.51 ms
[07-05-2017 11:00:04] HOST ALERT: techstorage;DOWN;SOFT;1;CRITICAL - Host Unreachable (192.168.40.23)
[07-05-2017 11:00:02] SERVICE ALERT: techstorage;PING;CRITICAL;SOFT;1;PING CRITICAL - Packet loss = 100%

July 05, 2017 09:00

[07-05-2017 09:00:15] SERVICE ALERT: techstorage;AFP;OK;SOFT;2;TCP OK - 0.000 second response time on 192.168.40.23 port 548

July 05, 2017 08:00

[07-05-2017 08:59:32] HOST ALERT: techstorage;UP;SOFT;2;PING OK - Packet loss = 0%, RTA = 0.30 ms
[07-05-2017 08:58:28] HOST ALERT: techstorage;DOWN;SOFT;1;CRITICAL - Host Unreachable (192.168.40.23)
[07-05-2017 08:58:25] SERVICE ALERT: techstorage;AFP;CRITICAL;SOFT;1;CRITICAL - Socket timeout after 10 seconds

July 05, 2017 00:00

[07-05-2017 00:59:57] SERVICE ALERT: techstorage;PING;OK;SOFT;2;PING OK - Packet loss = 0%, RTA = 0.44 ms
[07-05-2017 00:59:08] HOST ALERT: techstorage;UP;SOFT;2;PING OK - Packet loss = 0%, RTA = 0.43 ms
[07-05-2017 00:58:04] HOST ALERT: techstorage;DOWN;SOFT;1;CRITICAL - Host Unreachable (192.168.40.23)
[07-05-2017 00:58:03] SERVICE ALERT: techstorage;PING;CRITICAL;SOFT;1;PING CRITICAL - Packet loss = 100%

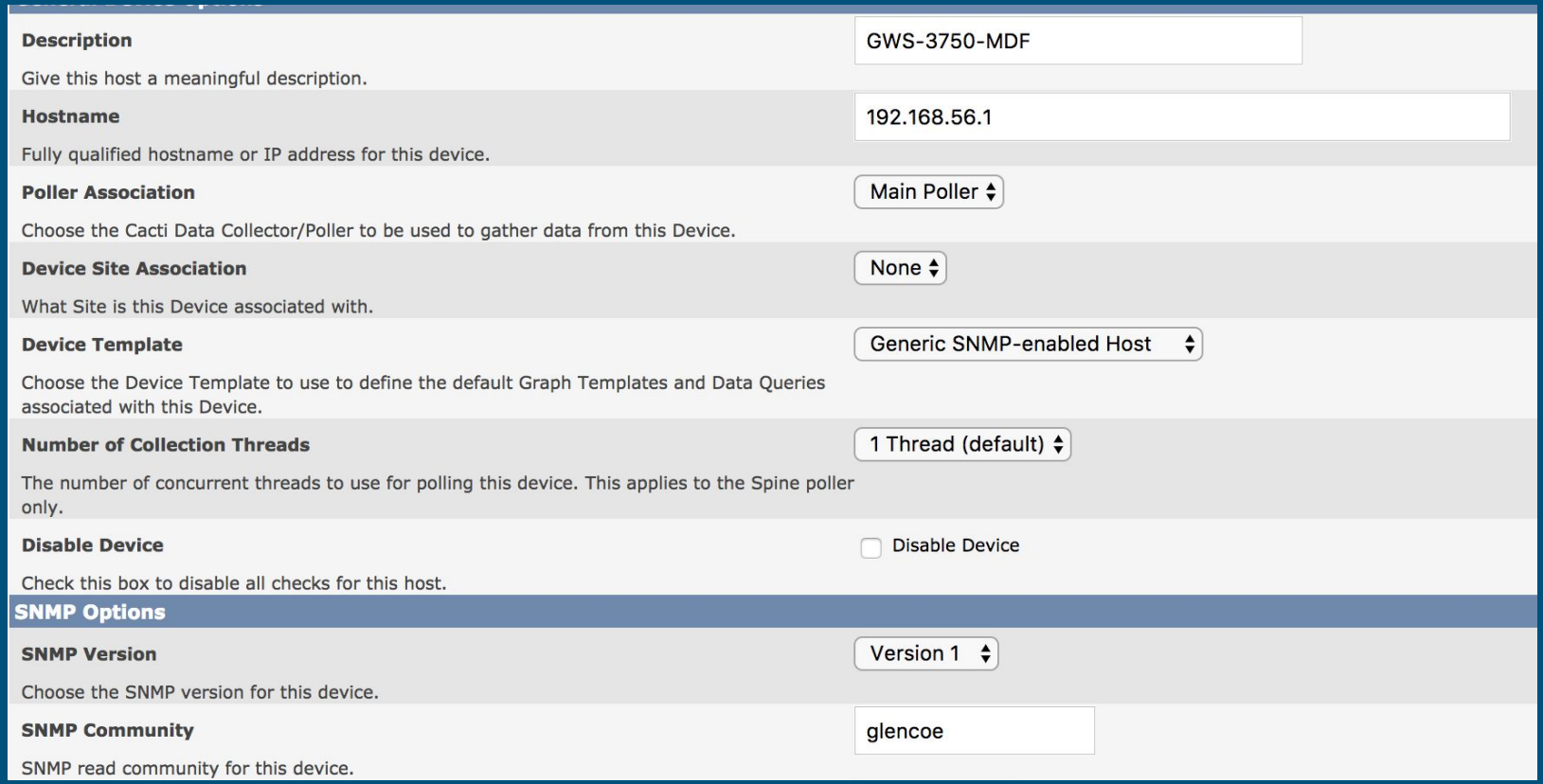
Monitoring vs Alerting

- Alerting can tell us an AP is down
- Monitoring can tell us number of connected clients
- Monitoring can tell us if a network port maxed out

Monitoring | CACTI

- Network device focus
- Numerical data retrieved via SNMP
- Graph basic trends
- GUI based
- Extend with community templates

Step 1: Add a device



New Graphs for [GCS-2960-B (192.168.42.4) Generic SNMP-enabled Host]

Device: GCS-2960-B (192.168.42.4) | Graph Types: All | Rows: Default

* Edit this Device
* Create New Device

Graph Templates

Graph Template Name

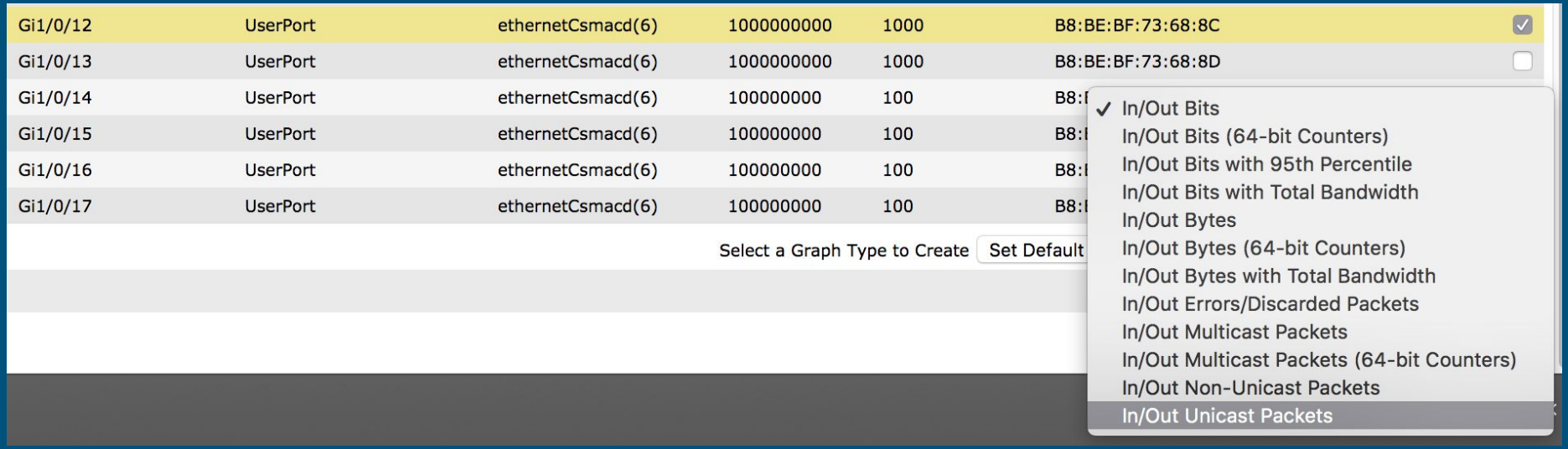
Create (Select a graph type to create)

Data Query [SNMP - Interface Statistics]

1 to 30 of 171 [1 2 3 4 5 ... 6] Next »

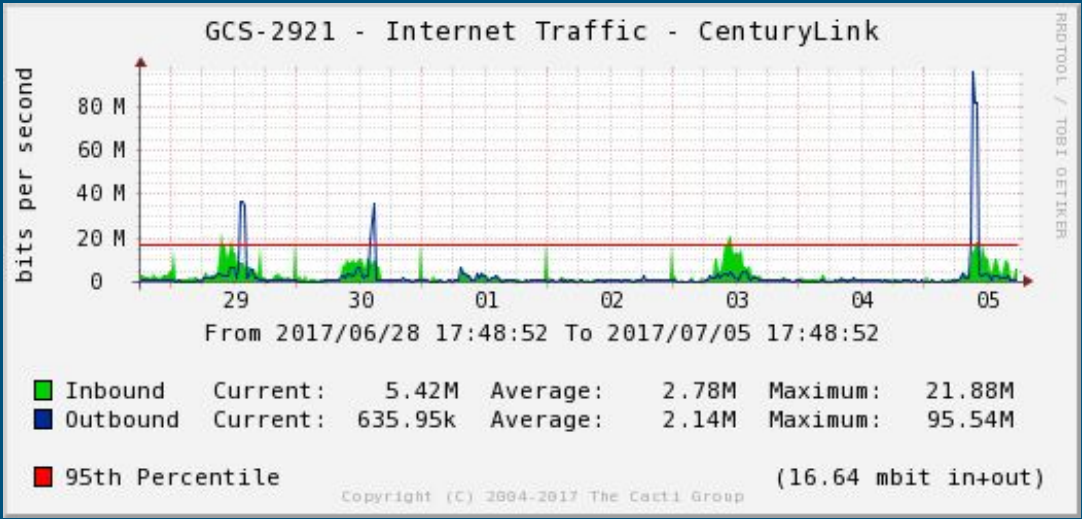
Index	Status	Description	Name (IF-MIB)	Alias (IF-MIB)	Type	Speed	High Speed	Hardware Address	IP Address
1	Up	Vlan1	Vl1		propVirtual(53)	1000000000	1000	44:E4:D9:72:1D:40	
42	Up	Vlan42	Vl42	UserData-B	propVirtual(53)	1000000000	1000	44:E4:D9:72:1D:41	192.168.42.4
142	Up	Vlan142	Vl142	UserVoice-B	propVirtual(53)	1000000000	1000	44:E4:D9:72:1D:42	192.168.142.4
5001	Up	Port-channel1	Po1	GCS-3750-MDF-po22	propVirtual(53)	2000000000	2000	44:E4:D9:72:1D:31	
5137	Up	StackPort1	StackPort1		propVirtual(53)	0	0		
5138	Up	StackSub-St1-1	StackSub-St1-1		propVirtual(53)	0	0		
5139	Up	StackSub-St1-2	StackSub-St1-2		propVirtual(53)	0	0		
5140	Up	StackPort2	StackPort2		propVirtual(53)	0	0		
5141	Up	StackSub-St2-1	StackSub-St2-1		propVirtual(53)	0	0		
5142	Up	StackSub-St2-2	StackSub-St2-2		propVirtual(53)	0	0		
5143	Up	StackPort3	StackPort3		propVirtual(53)	0	0		
5144	Up	StackSub-St3-1	StackSub-St3-1		propVirtual(53)	0	0		
5145	Up	StackSub-St3-2	StackSub-St3-2		propVirtual(53)	0	0		
10101	Up	GigabitEthernet1/0/1	Gi1/0/1	UserPort	ethernetCsmacd(6)	100000000	100	B8:BE:BF:73:68:81	
10102	Up	GigabitEthernet1/0/2	Gi1/0/2	UserPort	ethernetCsmacd(6)	1000000000	1000	B8:BE:BF:73:68:82	
10103	Down	GigabitEthernet1/0/3	Gi1/0/3	UserPort	ethernetCsmacd(6)	10000000	10	B8:BE:BF:73:68:83	

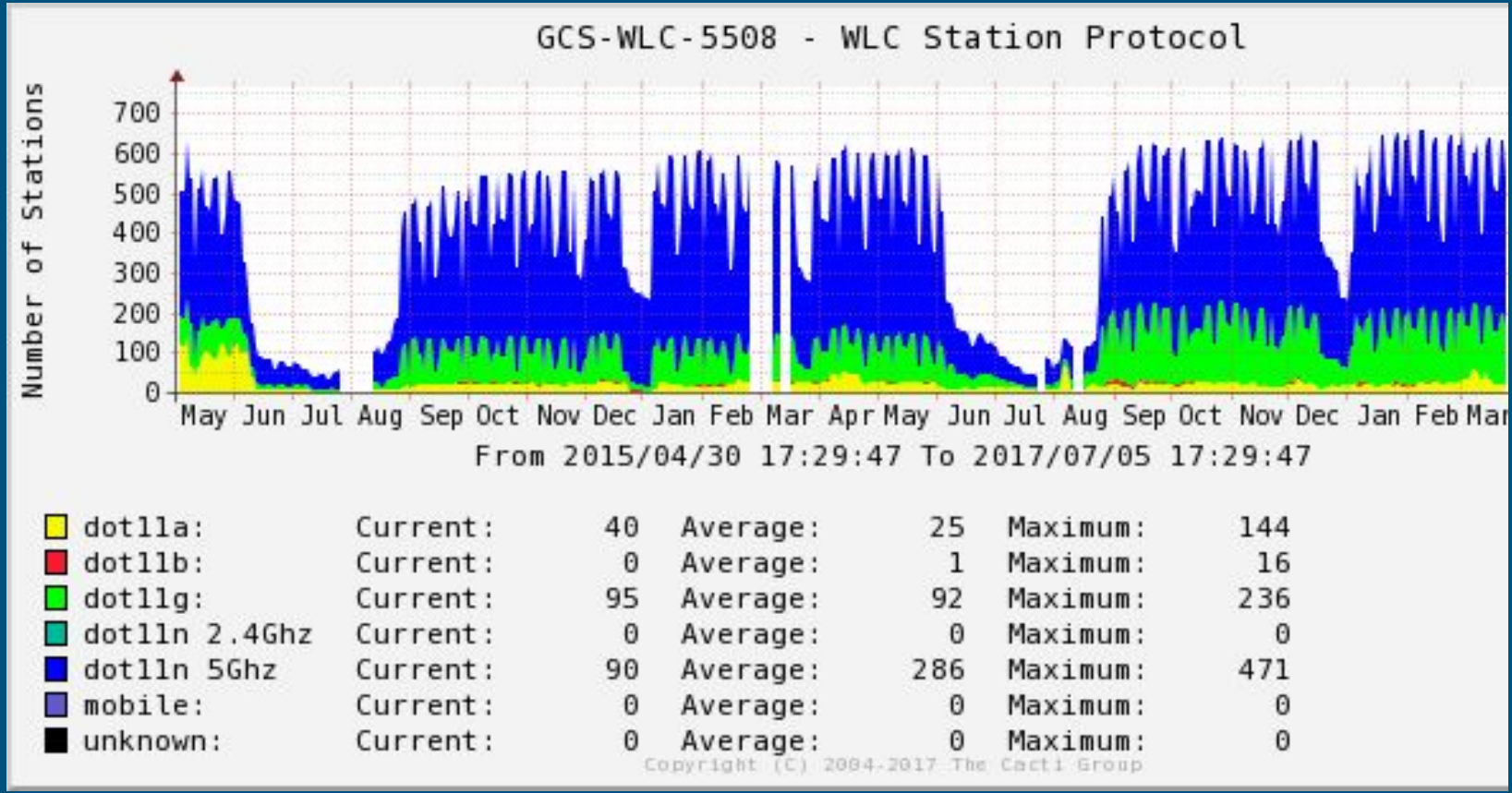
Step 2: Generate visualizations



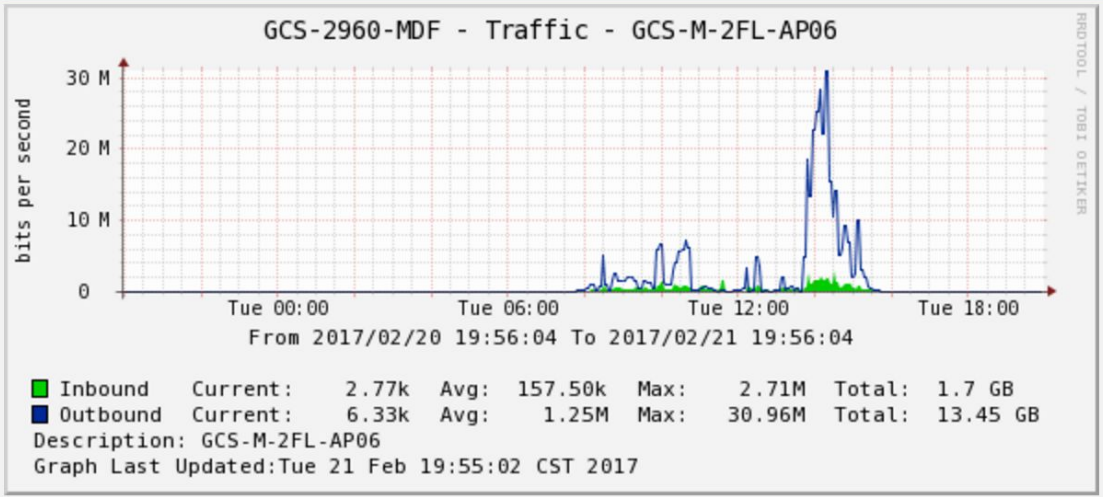
Remember

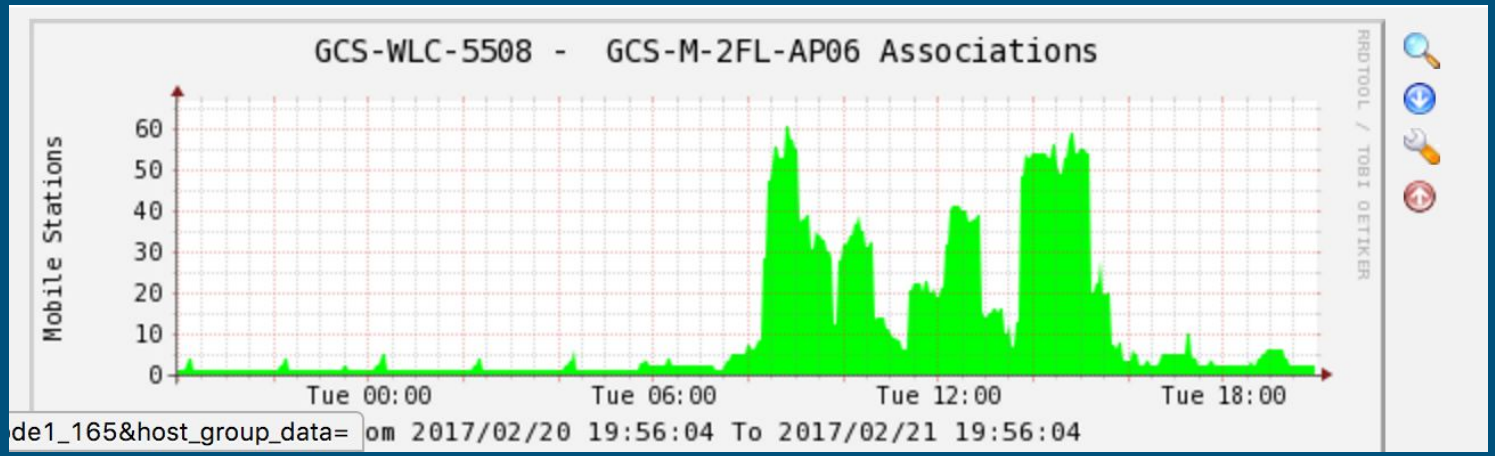
- Understand what the graph is telling us
- Relate information to actual environment




GCS-WLC-5508 - WLC Station Protocol
Number of Stations
700
600
500
400
300
200
100
0
May Jun Jul Aug Sep Oct Nov Dec Jan Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec Jan Feb Mar
From 2015/04/30 17:29:47 To 2017/07/05 17:29:47
dot11a: Current: 40 Average: 25 Maximum: 144
dot11b: Current: 0 Average: 1 Maximum: 16
dot11g: Current: 95 Average: 92 Maximum: 236
dot11n 2.4Ghz Current: 0 Average: 0 Maximum: 0
dot11n 5Ghz Current: 90 Average: 286 Maximum: 471
mobile: Current: 0 Average: 0 Maximum: 0
unknown: Current: 0 Average: 0 Maximum: 0
Copyright (C) 2004-2017 The Cacti Group

AP06


GCS-2960-MDF - Traffic - GCS-M-2FL-AP06
bits per second
30 M
20 M
10 M
0
Tue 00:00
Tue 06:00
Tue 12:00
Tue 18:00
From 2017/02/20 19:56:04 To 2017/02/21 19:56:04
Inbound Current: 2.77k Avg: 157.50k Max: 2.71M Total: 1.7 GB
Outbound Current: 6.33k Avg: 1.25M Max: 30.96M Total: 13.45 GB
Description: GCS-M-2FL-AP06
Graph Last Updated:Tue 21 Feb 19:55:02 CST 2017
RRDTOOL / TOBI OETIKER


GCS-WLC-5508 - GCS-M-2FL-AP06 Associations
Mobile Stations
60
50
40
30
20
10
0
Tue 00:00
Tue 06:00
Tue 12:00
Tue 18:00
de1_165&host_group_data=
om 2017/02/20 19:56:04 To 2017/02/21 19:56:04
RRDTOOL / TOBI OETIKER

What about custom data?

- Determine by manufacturer MIB
- OID represent an element of the device
  - 1.3.6.1.2.1.1.4 - sysContact

Logging | ELASTICSEARCH, LOGSTASH, KIBANA

Logstash

Data collection
Plugin ecosystem

Beats

Shipper from edge machines to Logstash

Elasticsearch

Search, Analyze, Store data

Kibana

Visualize data

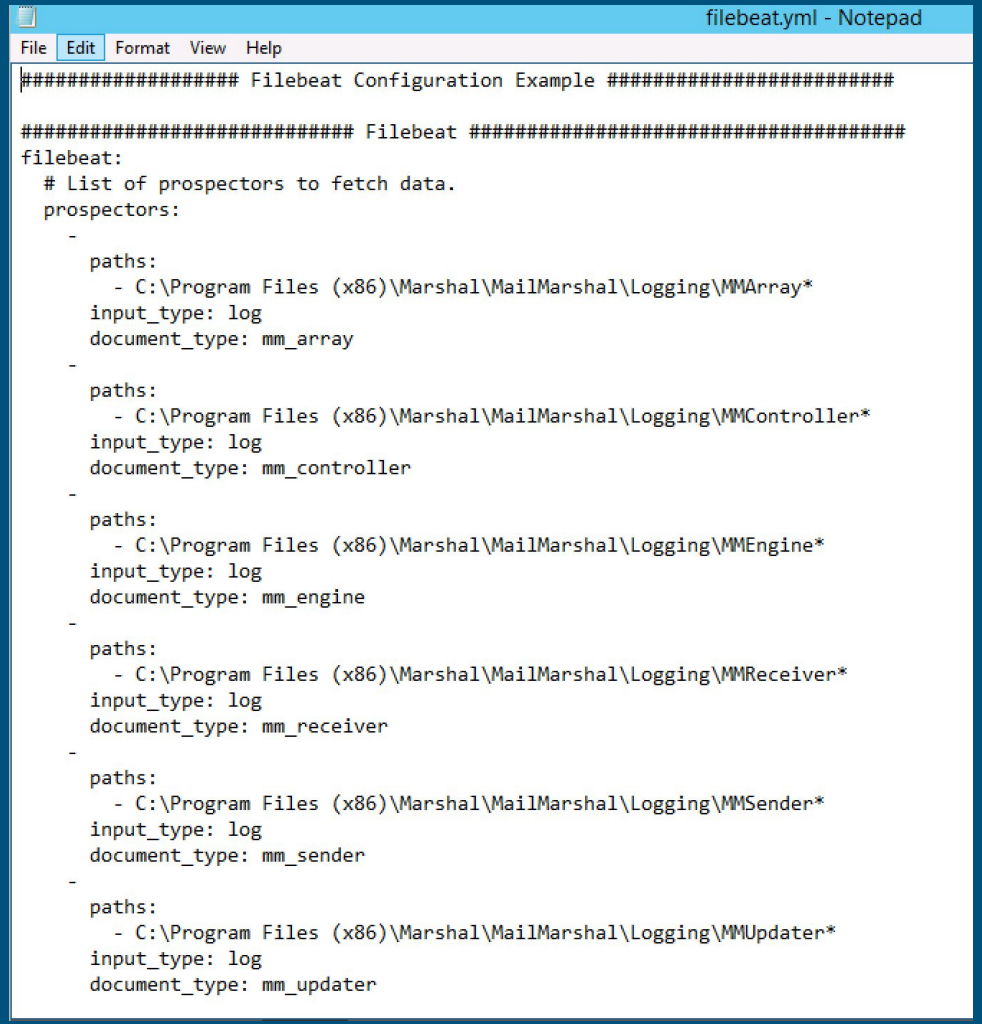
Beats | FILEBEAT

- Installed on edge device
- Configured with log files & paths
- Shipped to Logstash






GNU nano 2.3.1 File:
filebeat:
prospectors:
-
paths:
- /opt/zimbra/log/mailbox.log
- /opt/zimbra/log/access_log*
- /opt/zimbra/log/audit.log
- /opt/zimbra/log/clamd.log
input_type: log
document_type: zimbra-logs
-
paths:
- /var/log/zimbra.log
input_type: log
document_type: postfix
-
paths:
- /var/log/fail2ban.log
input_type: log
document_type: fail2ban
-
paths:
- /opt/zimbra/log/sync.log
input_type: log
document_type: activesync
registry_file: /var/lib/filebeat/registry
output:
logstash:
hosts: ["192.168.40.209:5044"]
bulk_max_size: 1024
index: filebeat
tls:
^G Get Help
^O WriteOut
^R Read Fi
^X Exit
^J Justify
^W Where I


filebeat.yml - Notepad
File Edit Format View Help
################### Filebeat Configuration Example #########################
############################# Filebeat ######################################
filebeat:
List of prospectors to fetch data.
prospectors:
-
paths:
- C:\Program Files (x86)\Marshal\MailMarshal\Logging\MMArray*
input_type: log
document_type: mm_array
-
paths:
- C:\Program Files (x86)\Marshal\MailMarshal\Logging\MMController*
input_type: log
document_type: mm_controller
-
paths:
- C:\Program Files (x86)\Marshal\MailMarshal\Logging\MMEngine*
input_type: log
document_type: mm_engine
-
paths:
- C:\Program Files (x86)\Marshal\MailMarshal\Logging\MMReceiver*
input_type: log
document_type: mm_receiver
-
paths:
- C:\Program Files (x86)\Marshal\MailMarshal\Logging\MMSender*
input_type: log
document_type: mm_sender
-
paths:
- C:\Program Files (x86)\Marshal\MailMarshal\Logging\MMUpdater*
input_type: log
document_type: mm_updater

Logstash

- Learn to ♡ Logstash
- Text-based configuration of Inputs, Filters, Outputs

https://media.giphy.com/media/VNFJZ6mpsvfHO/giphy.gif

Inputs

```
input {
   udp { port => 5514, type => "cisco-switch" }
   udp { port => 5544, type => "cisco-fw" }
   beats { port => 5044 }
}
```

Inputs

```
input {
   file {
      path => "/var/log/remotelogs/wlc.log"
      type => "cisco-wlc"
      start_position => "beginning"
   }
}
```

Filters

Because …

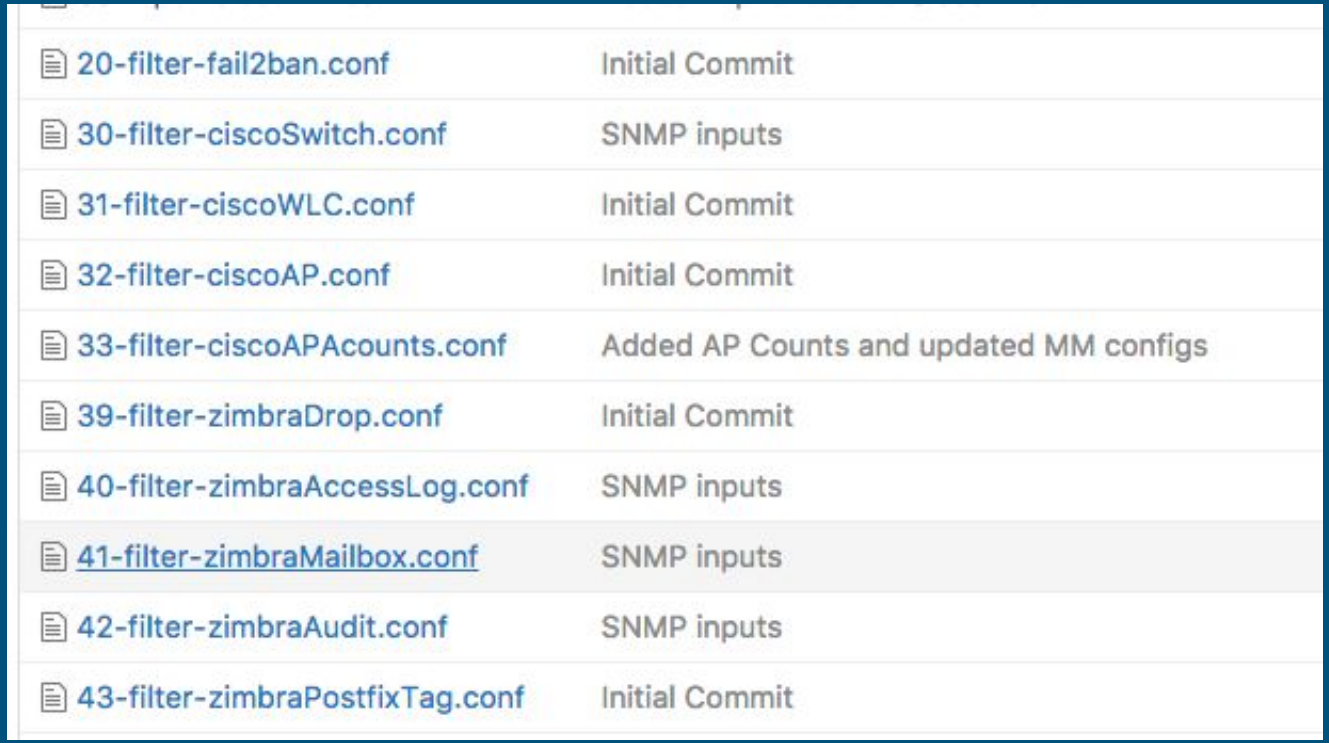
```
15092 10:16:28.939 PTR record for <74.125.82.54> exists
for HELO string <mail-wm0-f54.google.com>, accepting
```

…doesn’t really help us

Logstash Filters

- Format information
- Parse out fields of information
- Use patterns for specific services

Filters



20-filter-fail2ban.conf	Initial Commit
30-filter-ciscoSwitch.conf	SNMP inputs
31-filter-ciscoWLC.conf	Initial Commit
32-filter-ciscoAP.conf	Initial Commit
33-filter-ciscoAPAcounts.conf	Added AP Counts and updated MM configs
39-filter-zimbraDrop.conf	Initial Commit
40-filter-zimbraAccessLog.conf	SNMP inputs
41-filter-zimbraMailbox.conf	SNMP inputs
42-filter-zimbraAudit.conf	SNMP inputs
43-filter-zimbraPostfixTag.conf	Initial Commit

How do we do this?

15092 10:16:28.939 PTR record for <74.125.82.54> exists for HELO string <mail-wm0-f54.google.com>, accepting

```
match => [ “message”,
“%{NUMBER} %{TIME} PTR record for <%{IP:clientip}> exists for
HELO string <%{IP:from_server}>, %{WORD:status}” ]
```

t	clientip	74.125.82.54
t	from_server	mail-wm0-f54.google.com
t	geoip.city_name	Mountain View
t	geoip.continent_code	NA
#	geoip.coordinates	-122.057, 37.419
t	geoip.country_code2	US
t	geoip.country_code3	US
t	geoip.country_name	United States
#	geoip.dma_code	807
💻	geoip.ip	74.125.82.54
#	geoip.latitude	37.419
🌐	geoip.location	-122.0574, 37.419200000000004
#	geoip.longitude	-122.057
t	geoip.postal_code	94043
t	geoip.region_code	CA
t	geoip.region_name	California
t	geoip.timezone	America/Los_Angeles

Filters

```
filter {
   if [type] == "cisco-switch" { }
   if [type] == "cisco-fw" { }
   …
}
```

Construction Example | GROK CONSTRUCTOR

Constructed regular expression so far:

```
\A%{PROG} %{TIME} %{CISCO_REASON}<%{IP}> %{CISCO_REASON}<
```

Already matched	Unmatched rest of the loglines to match
15092 10:16:28.939 PTR record for <74.125.82.54> exists for HELO string <	mail-wm0-f54.google.com>,·accepting

Grok expression	Matches at the start of the rest of the loglines
%{GREEDYDATA} %{JAVALOGMESSAGE}	mail-wm0-f54.google.com>,·accepting
%{NOTSPACE} %{PROG} %{SYSLOG5424PRINTASCII} %{SYSLOGPROG}	mail-wm0-f54.google.com>,
%{EMAILLOCALPART} %{HOSTNAME} %{HTTPDUSER} %{IPORHOST} %{JAVACLASS} %{JAVAFILE} %{SYSLOGHOST} %{URIHOST} %{USER} %{USERNAME}	mail-wm0-f54.google.com
%{MONGO_WORDDASH}	mail-wm0-f54

grokconstructor.appspot.com

Outputs

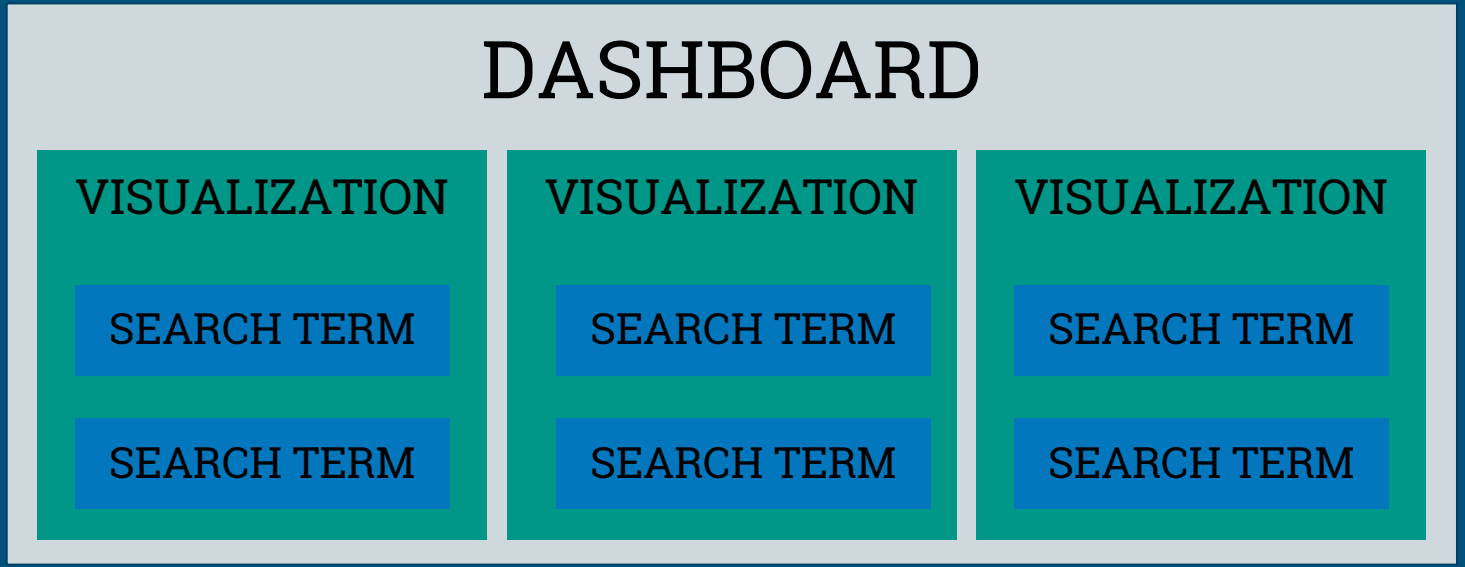
```
output {
 if "beats_input_codec_plain_applied" in [tags] {
   elasticsearch { index => "filebeat-%{+YYYY.MM.dd}"}
 }
 else if "twitter" in [tags] {
   elasticsearch { index => "twitter-%{+YYYY.MM.dd}"}
   file { path => "/tmp/logstash.log" }
 } }
```

Elasticsearch

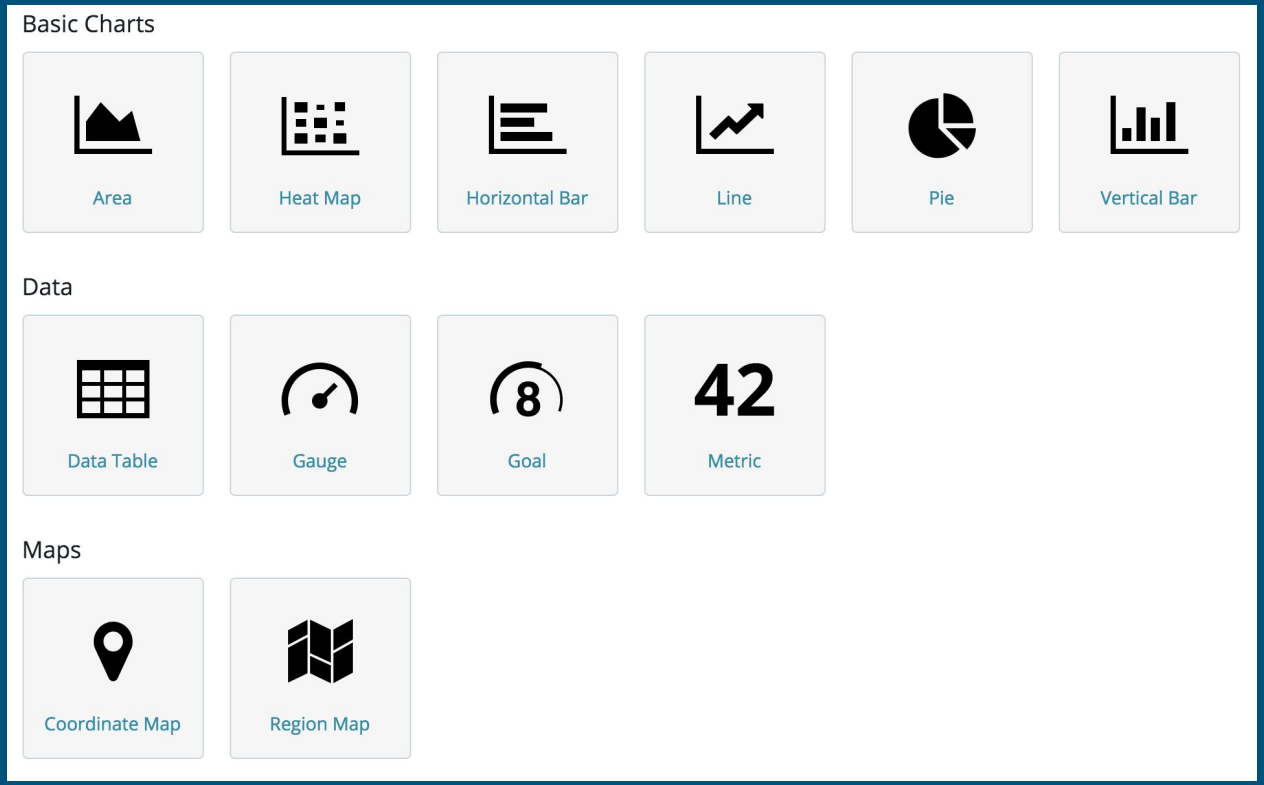
- Central Storage of your data
- Elasticsearch is configured as a logstash output
- Create indices for source-types
- Least amount of time for setup

“Discover the expected, uncover the unexpected”

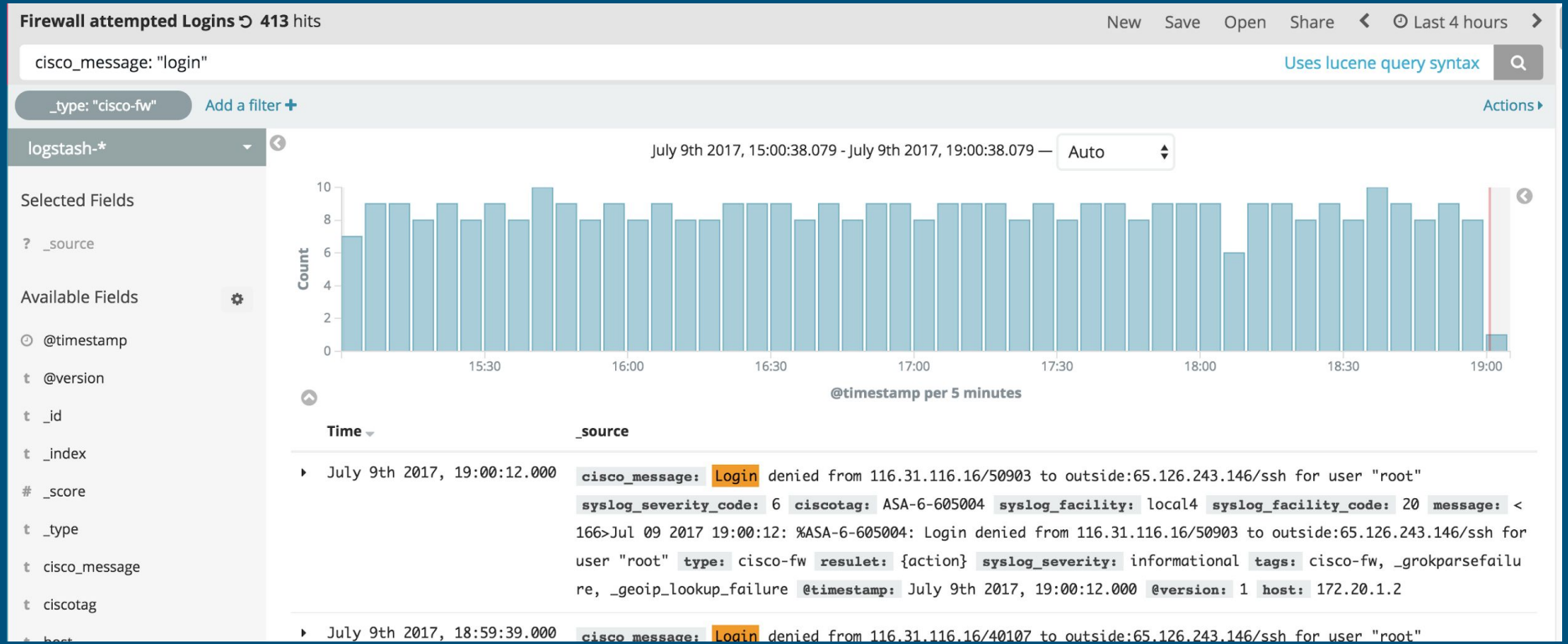
Kibana


DASHBOARD
VISUALIZATION
SEARCH TERM
SEARCH TERM
VISUALIZATION
SEARCH TERM
SEARCH TERM
VISUALIZATION
SEARCH TERM
SEARCH TERM

Visualization



Denied Firewall logins

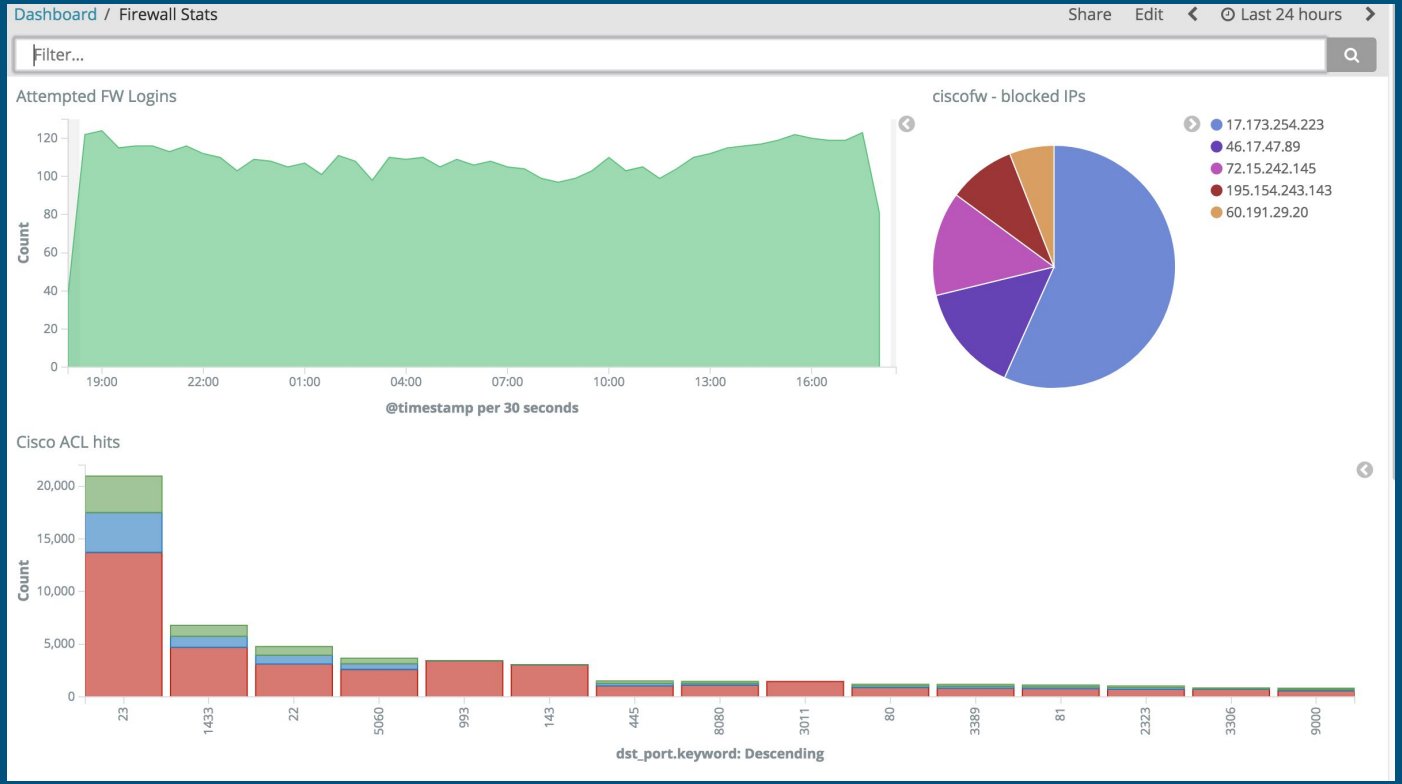


Denied Firewall logins

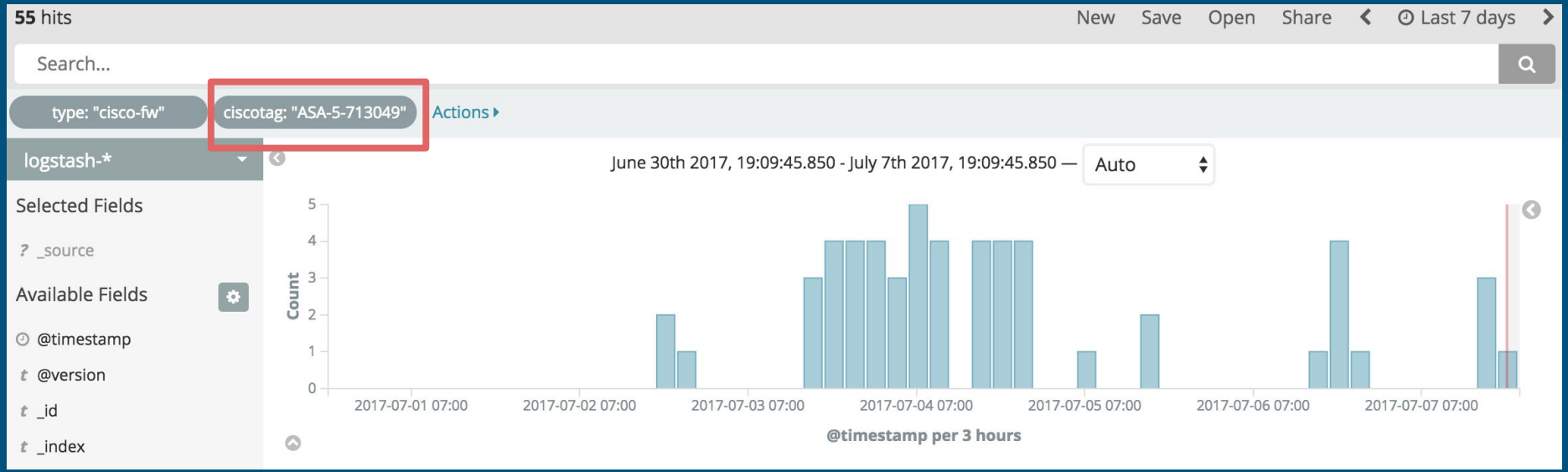
Login denied from 182.100.67.252/18872 to outside:65.126.243.146/ssh for user "root"

Action	Login denied
Source IP	182.100.67.252
Our public IP	65.126.243.146
Service	ssh
Username	root

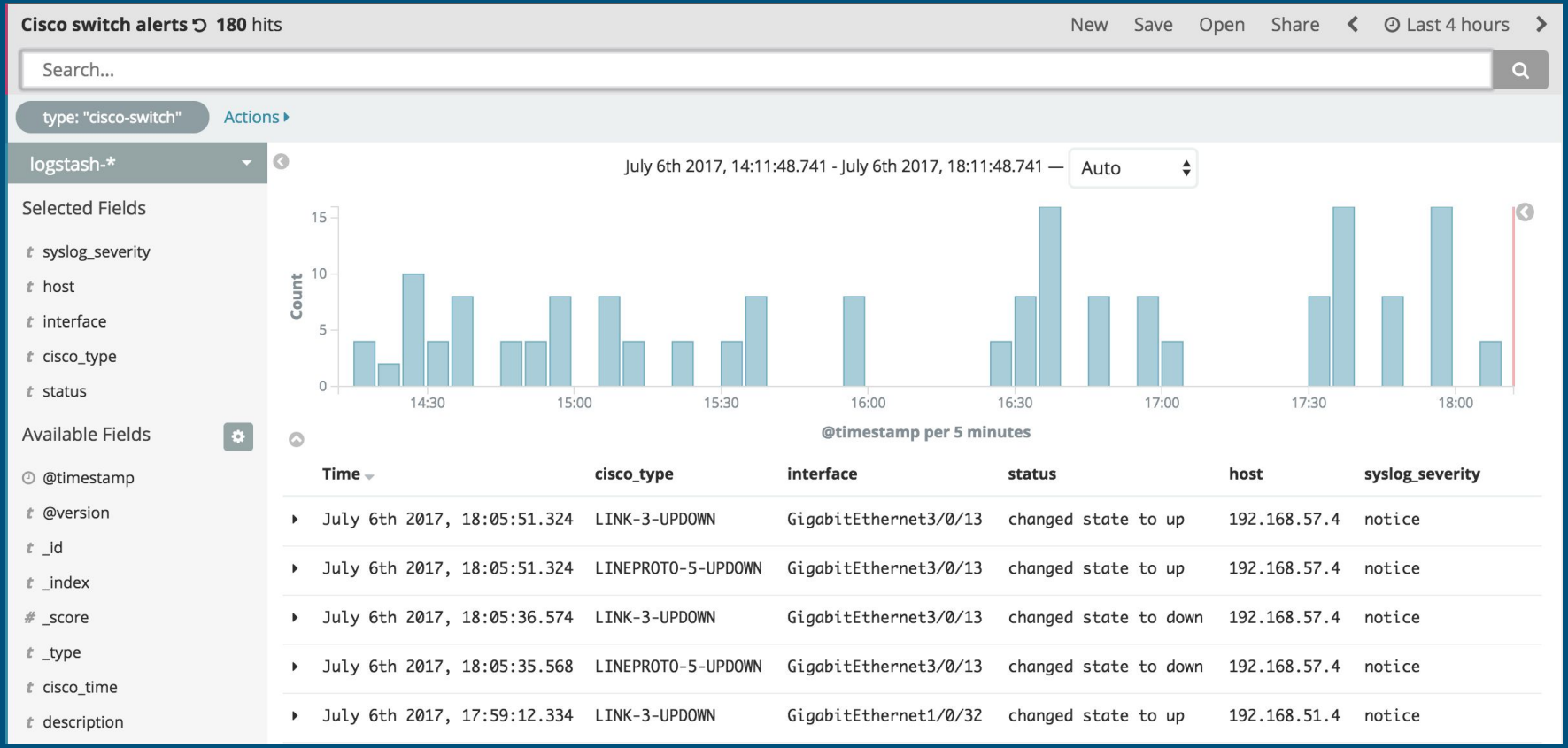
Dashboard - Firewall Events



VPN connections

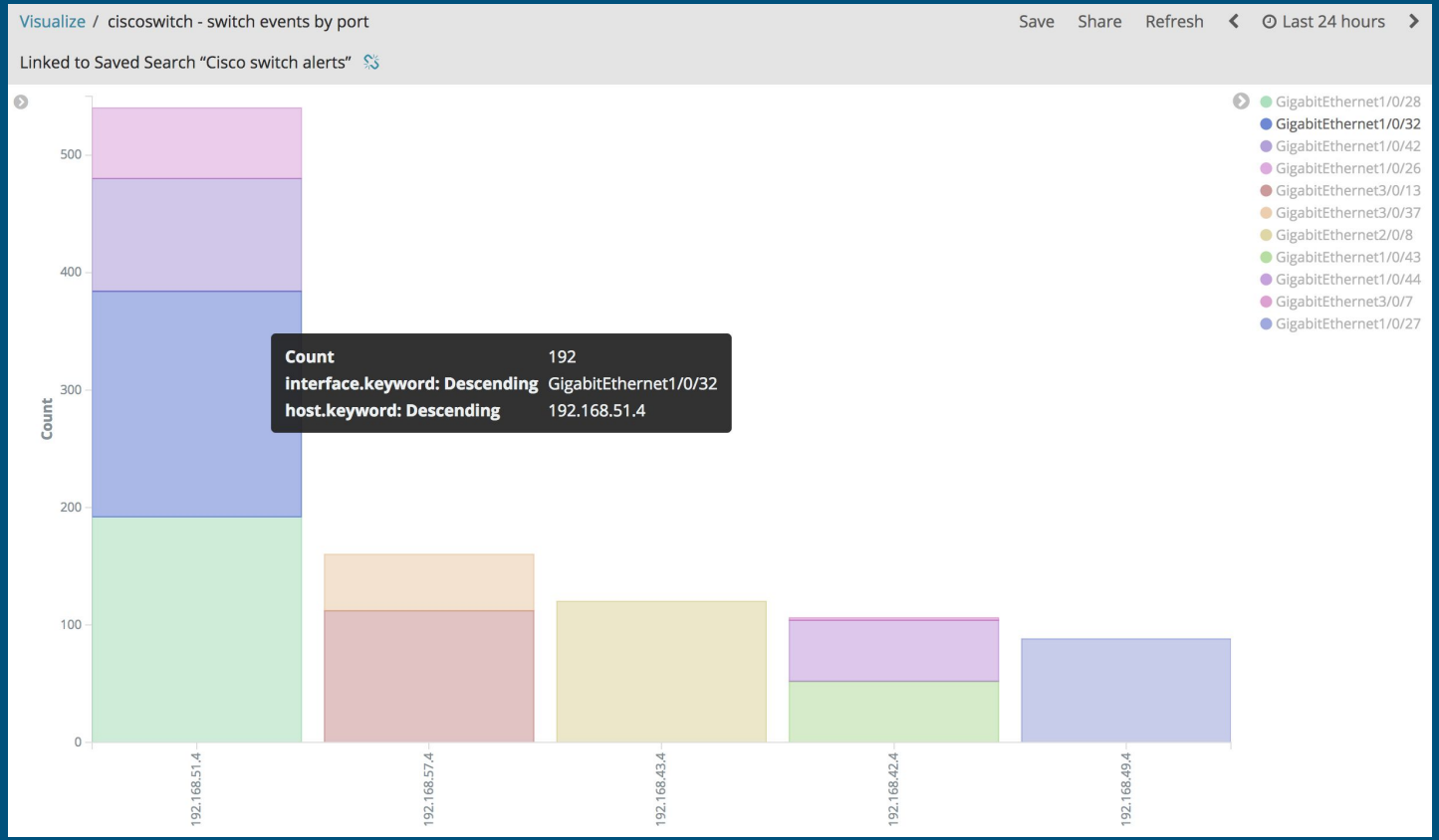


Switch events

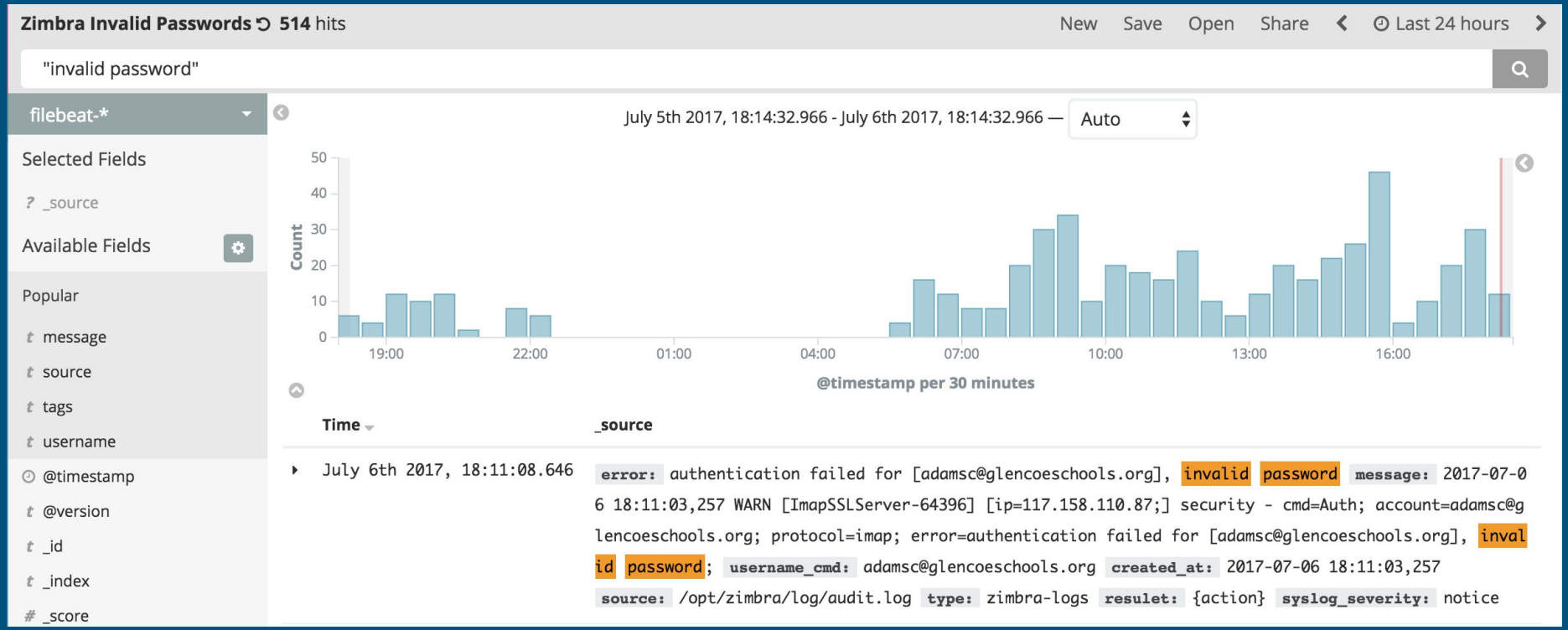


Time	cisco_type	interface	status	host	syslog_severity
July 6th 2017, 18:05:51.324	LINK-3-UPDOWN	GigabitEthernet3/0/13	changed state to up	192.168.57.4	notice
July 6th 2017, 18:05:51.324	LINEPROTO-5-UPDOWN	GigabitEthernet3/0/13	changed state to up	192.168.57.4	notice
July 6th 2017, 18:05:36.574	LINK-3-UPDOWN	GigabitEthernet3/0/13	changed state to down	192.168.57.4	notice
July 6th 2017, 18:05:35.568	LINEPROTO-5-UPDOWN	GigabitEthernet3/0/13	changed state to down	192.168.57.4	notice
July 6th 2017, 17:59:12.334	LINK-3-UPDOWN	GigabitEthernet1/0/32	changed state to up	192.168.51.4	notice

Switch events



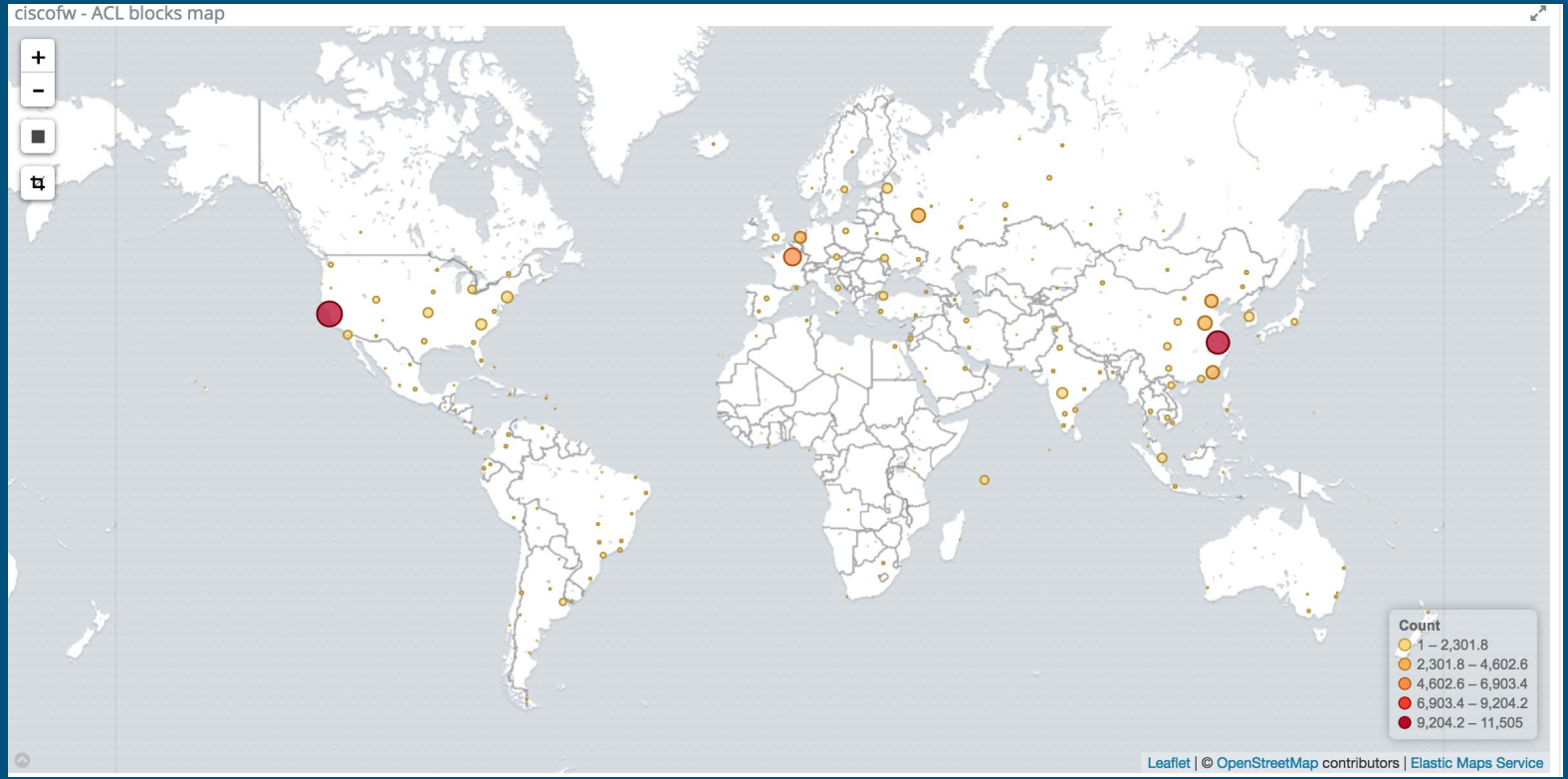
E-Mail Events



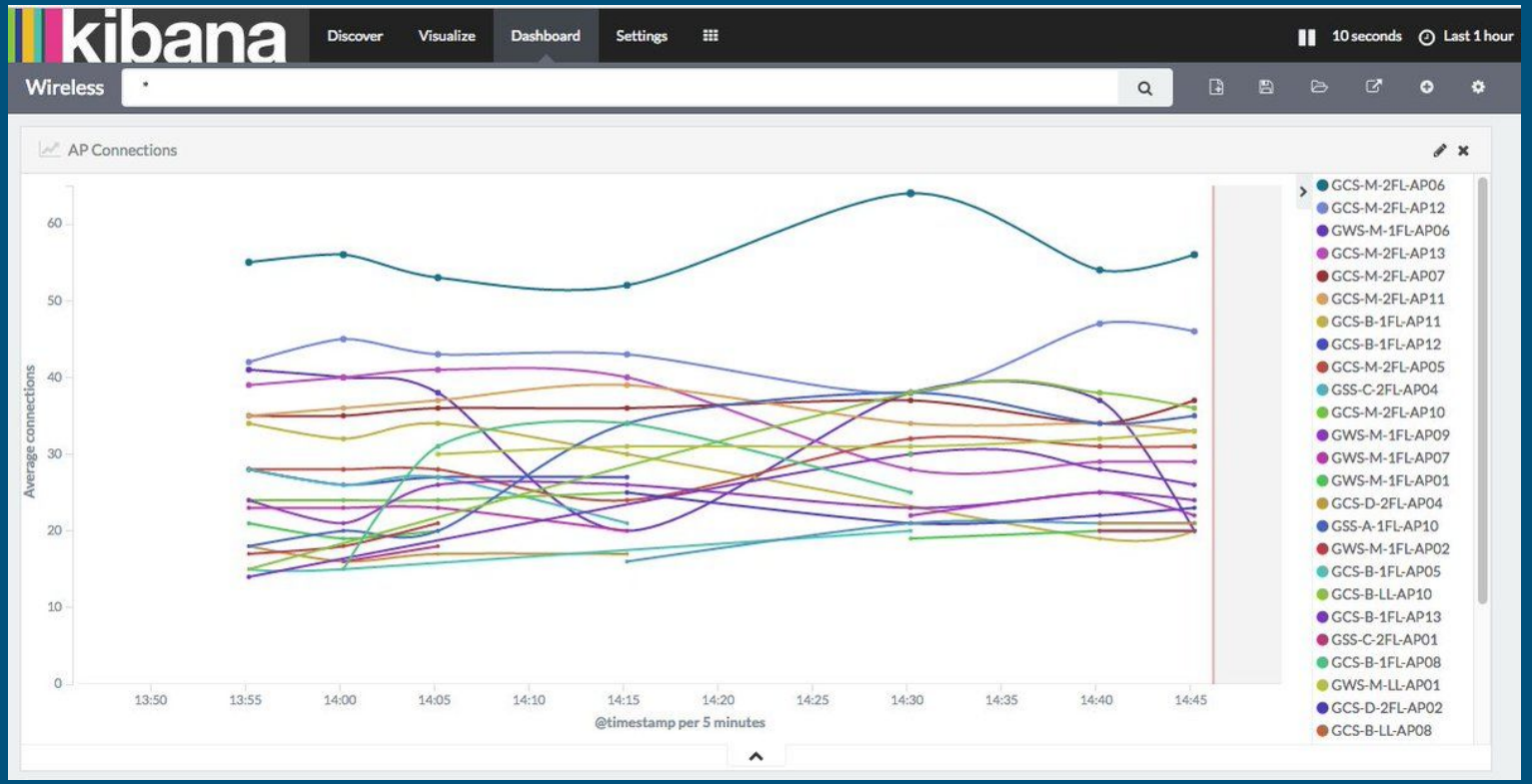
What does the data tell us?

2017-07-06 18:11:03,257 WARN [ImapSSLServer-64396] [ip=117.158.110.87;] security - cmd=Auth; account=USER@glencoeschools.org; protocol=imap; error=authentication failed for [USER@glencoeschools.org], invalid password;

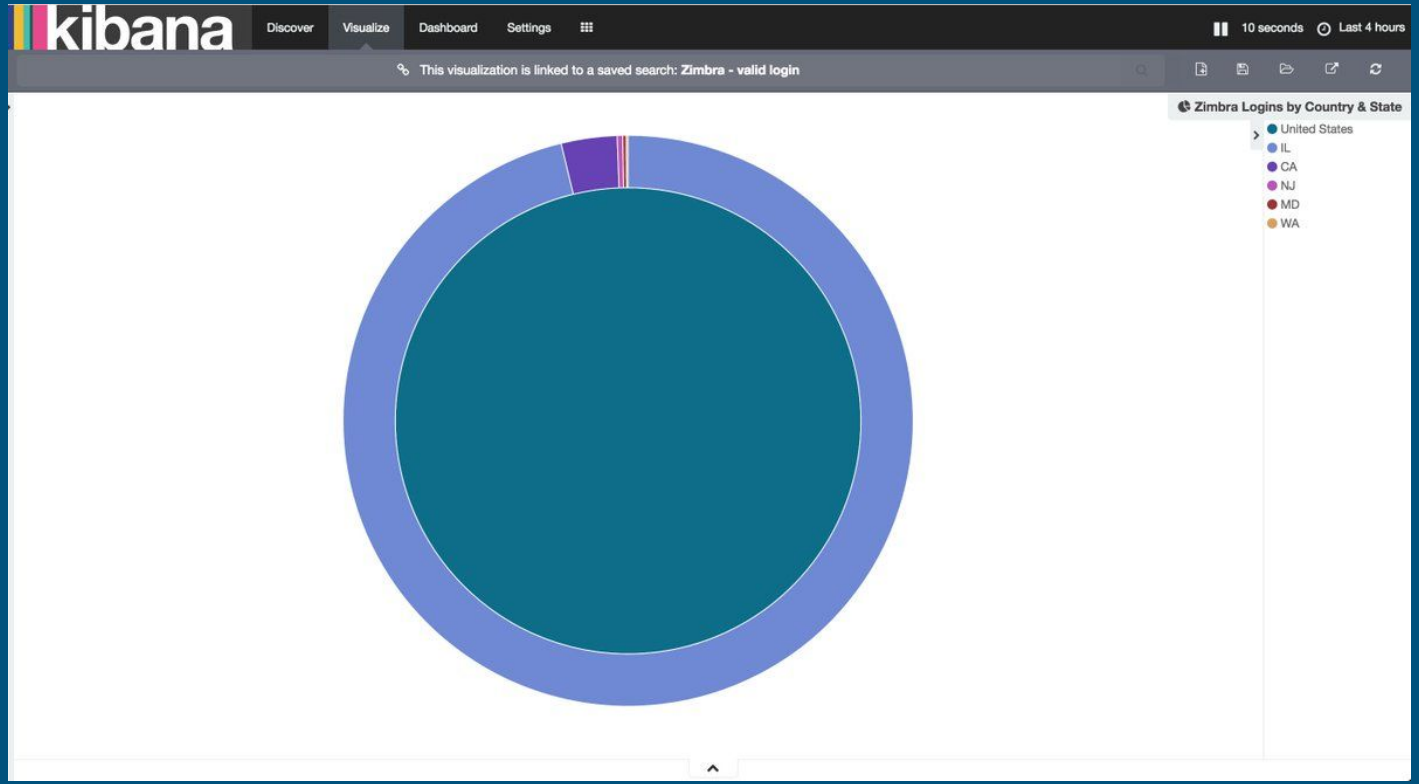
Dashboards


ciscofw - ACL blocks map
Count
1 – 2,301.8
2,301.8 – 4,602.6
4,602.6 – 6,903.4
6,903.4 – 9,204.2
9,204.2 – 11,505
Leaflet | © OpenStreetMap contributors | Elastic Maps Service

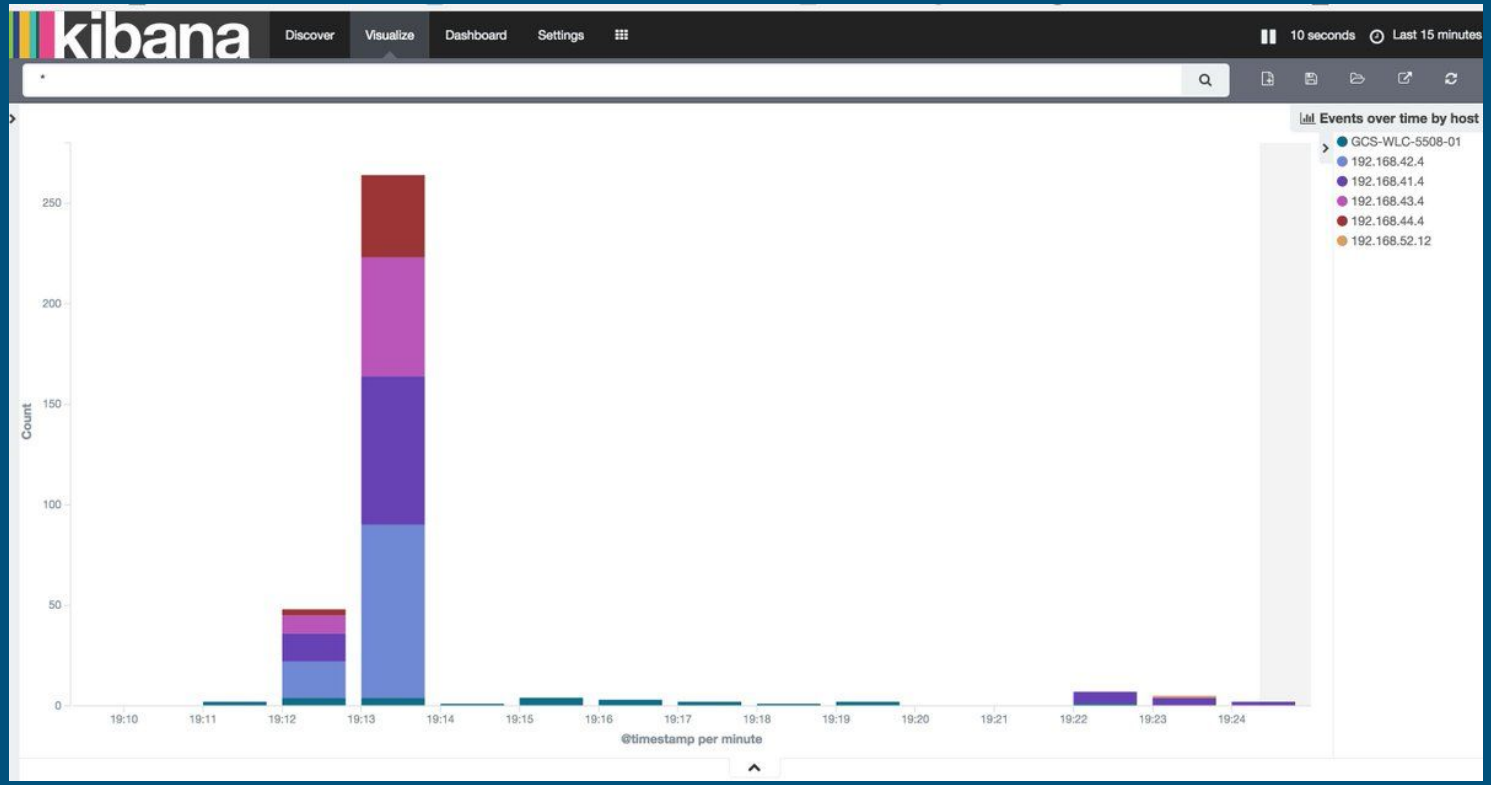
Connections per Access Point



Valid E-Mail logins by Country & State



Do we know why there is a spike?



Other Examples

- Filtering through data example
- Social Media Analytics

That’s how it starts …

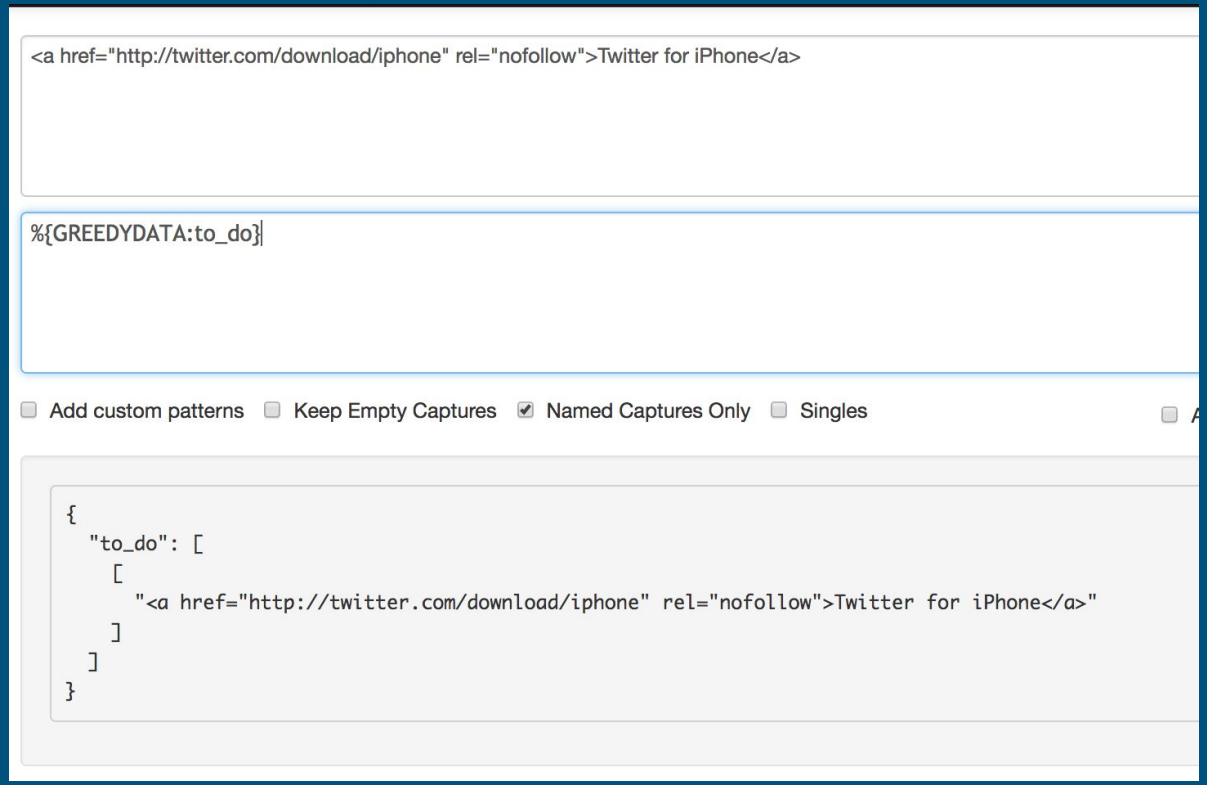
source

```
<a href="http://twitter.com/download/iphone"
rel="nofollow">Twitter for iPhone</a>
```

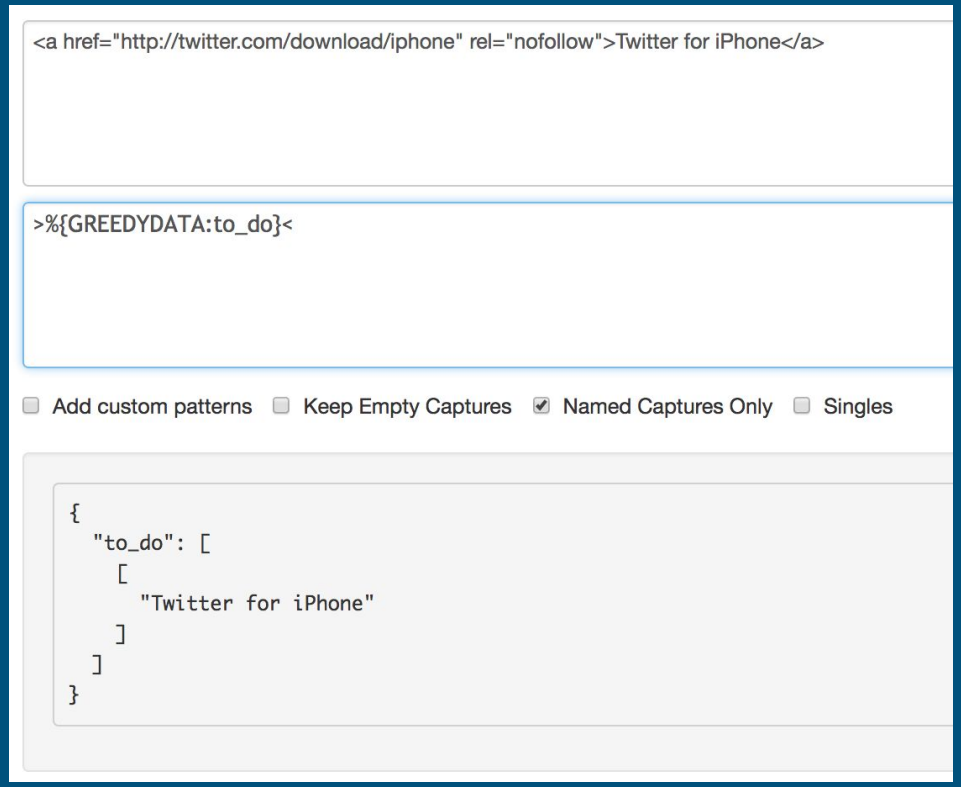
```
<a href="http://twitter.com/download/iphone"
rel="nofollow">Twitter for iPhone</a>
```

```
<a href="http://twitter.com/download/iphone"
rel="nofollow">Twitter for iPhone</a>
```

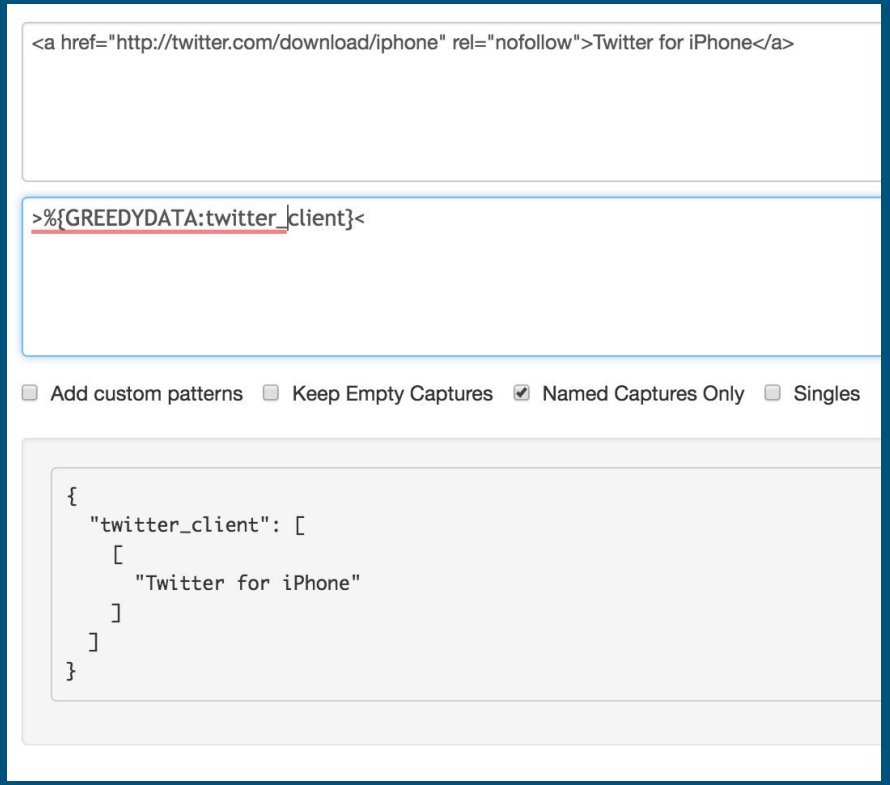
… you check the charts …



… and start to figure it out.



That’s how it starts



Power of dashboards

- Dashboards consolidate information otherwise isolated
- Reduce time searching logs for events
- Once data consolidate we can manipulate
- Dashboards can focus around project-specific metrics
- Use time to troubleshoot instead of discovering

Q&A