The devops approach to monitoring, Open Source and IAC Style

Julien Pivotto

Open World Forum

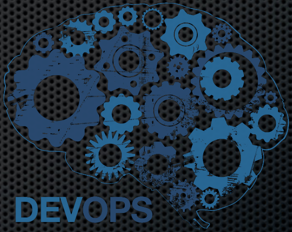
October 4, 2013

whoami

- sysadmin @ inuits
- open-source defender for 7+ years
- devops believer
- @roidelapluie on twitter/github

DevOps

- Culture
- Automation
- Measurement
- Sharing



Damon Edwards and John Willis

OPEN WORLD FORUM

Monitoring is usually an afterthought

ENOTIME, ENOBUDGET

#monitoringsucks

- A movement started in 2011
- http://github.com/monitoringsucks
- A lot of tools and information

Goals

- Find when a service is unavailable
- Understand failure post-mortem

Goals

- Find when a service is unavailable
- Understand failure post-mortem
- Learn from your infrastructure
- Anticipate

Monitor everything

- Servers
- Services
- Usage
- Hardware
- Software
- People

Monitor every environment

- See performance changes in dev
- Fix them before it hits production

Metric

- Time + name + value = metric
- Can be anything

Event

- Time + fields = metric
- Logs become usable data
- Can be transformed into metrics

Metrics + events

- Overview of your infrastructure
- Usage and state of the services
- Combine several metrics
- Extract business values

Automation

- Infrastructure as Code
- Automate everything

⇒ One source of truth

OPEN WORLD FORUM

Deployment

- Definitions of a service includes monitoring
- Deployed ⇔ monitored

Tools

- No all-in-one tool
- No autodiscovery tool
- Text-based configuration
- Scalable

⇒ The Unix philosphy

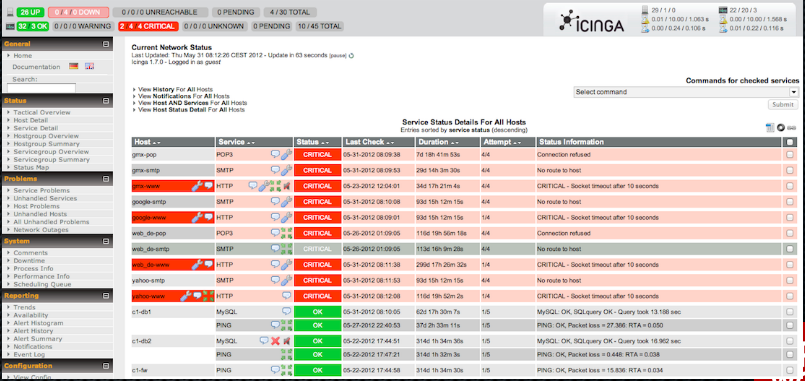
OPEN WORLD FORUM

Icinga

- Fork of nagios
- Large and vibrant community
- Configuration compatible with nagios
- User-friendly interface
- Use Icinga Classic!

Icinga

https://icinga.org



26 UP | 0 / 4 / 0 DOWN | 0 / 0 / 0 UNREACHABLE | 0 PENDING | 4 / 30 TOTAL

32 / 3 OK | 0 / 0 / 0 WARNING | 2 / 4 / 4 CRITICAL | 0 / 0 / 0 UNKNOWN | 0 PENDING | 10 / 45 TOTAL

29 / 1 / 0
0.01 / 10.00 / 1.063 s
0.00 / 0.24 / 0.106 s

22 / 20 / 3
0.00 / 10.00 / 1.568 s
0.01 / 0.22 / 0.116 s

Current Network Status
Last Updated: Thu May 31 08:12:26 CEST 2012 - Update in 63 seconds [pause]
Icinga 1.7.0 - Logged in as *guest*

- View **History** For **All** Hosts
- View **Notifications** For **All** Hosts
- View **Host AND Services** For **All** Hosts
- View **Host Status Detail** For **All** Hosts

Commands for checked services

Service Status Details For All Hosts
Entries sorted by **service status** (descending)

Host	Service	Status	Last Check	Duration	Attempt	Status Information	□
gmx-pop	POP3	CRITICAL	05-31-2012 08:09:38	7d 18h 41m 53s	4/4	Connection refused	□
gmx-smtp	SMTP	CRITICAL	05-31-2012 08:09:53	29d 14h 3m 30s	4/4	No route to host	□
gmx-www	HTTP	CRITICAL	05-23-2012 12:04:01	34d 17h 21m 4s	4/4	CRITICAL - Socket timeout after 10 seconds	□
google-smtp	SMTP	CRITICAL	05-31-2012 08:10:08	93d 15h 12m 15s	4/4	No route to host	□
google-www	HTTP	CRITICAL	05-31-2012 08:09:01	93d 15h 12m 15s	1/4	CRITICAL - Socket timeout after 10 seconds	□
web_de-pop	POP3	CRITICAL	05-26-2012 01:09:05	116d 19h 56m 18s	4/4	Connection refused	□
web_de-smtp	SMTP	CRITICAL	05-26-2012 01:09:05	113d 16h 9m 28s	4/4	No route to host	□
web_de-www	HTTP	CRITICAL	05-31-2012 08:11:38	299d 17h 26m 32s	1/4	CRITICAL - Socket timeout after 10 seconds	□
yahoo-smtp	SMTP	CRITICAL	05-31-2012 08:11:53	93d 15h 12m 15s	4/4	No route to host	□
yahoo-www	HTTP	CRITICAL	05-31-2012 08:12:08	116d 19h 52m 2s	1/4	CRITICAL - Socket timeout after 10 seconds	□
c1-db1	MySQL	OK	05-31-2012 08:10:05	62d 17h 30m 7s	1/5	MySQL: OK, SQLquery OK - Query took 13.188 sec	□
	PING	OK	05-27-2012 22:40:53	37d 2h 33m 11s	1/5	PING: OK, Packet loss = 27.386: RTA = 0.050	□
c1-db2	MySQL	OK	05-22-2012 17:44:51	314d 1h 34m 36s	1/5	MySQL: OK, SQLquery OK - Query took 16.962 sec	□
	PING	OK	05-22-2012 17:47:21	314d 1h 32m 3s	1/5	PING: OK, Packet loss = 0.448: RTA = 0.038	□
c1-fw	PING	OK	05-22-2012 17:44:58	314d 1h 34m 30s	1/5	PING: OK, Packet loss = 15.836: RTA = 0.034	□

Sensu

- Flexibility
- Compatible with nagios plugins
- Connects to your source of trust
- Relies on RabbitMQ

Collectd

- Statistics collection daemon
- A lot of plugins available. . .
- Can send data to graphite
- Simple configuration

Collectd plugins

http://www.flickr.com/photos/juhansonin/3141561416/

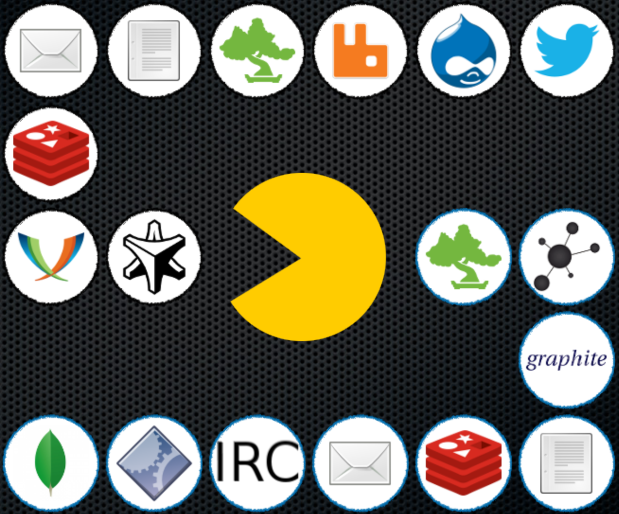
Collectd plugins

AMQP Apache APC_UPS Apple_Sensors Ascent Battery BIND Carbon
ConnTrack ContextSwitch CPU CPUFreq CSV cURL cURL-JSON cURL-XML
DBI DF Disk DNS E-Mail Entropy Exec FileCount FSCache GenericJMX
gmond HDDTemp Interface IPMI IPTables IPVS IRQ Java libvirt Load
LogFile LPAR MadWifi MBMon memcachec memcached Memory Modbus
Monitorus Multimeter MySQL NetApp Netlink Network NFS nginx
Notify_Desktop Notify_Email NTPd NUT olsrd OneWire OpenVPN OpenVZ
Oracle Perl Pinba Ping PostgreSQL PowerDNS Processes Protocols Python
Redis RouterOS RRDCacheD RRDtool Sensors Serial SNMP Swap SysLog
Table Tail Tape TCPConns TeamSpeak2 TED thermal TokyoTyrant UnixSock
Uptime Users UUID Varnish vmem VServer Wireless XMMS
Write_Graphite Write_HTTP Write_MongoDB
Write_Redis Write_Riemann ZFS_ARC

Logstash

- Ship logs from any source
- Filter them
- Index them
- Search them
- Backed with elasticsearch

Logstash



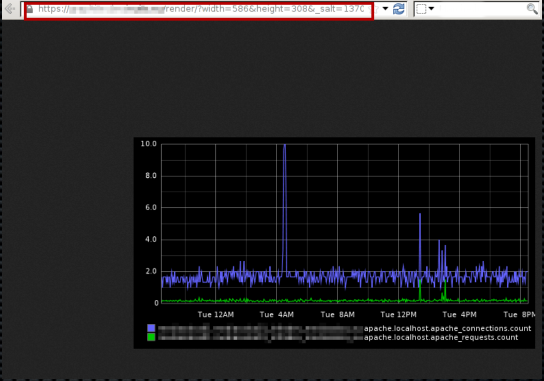
Graphite

- Graphing
- Accept any metric
- Store data in files (whisper)
- A lot of helpers functions
- Listen on UDP and TCP

Send data to graphite

```
echo "stats.sshd.login 1 $(date +%s)" | nc -u graphite.example.com 2003
```

Graphite API



https://[redacted]render/?width=586&height=308&_salt=137(

10.0
8.0
6.0
4.0
2.0
0
Tue 12AM
Tue 4AM
Tue 8AM
Tue 12PM
Tue 4PM
Tue 8PM
🟦 [redacted]apache.localhost.apache_connections.count
🟩 [redacted]apache.localhost.apache_requests.count

OPEN WORLD FORUM

Statsd

- Graphite friend
- Stats aggregation
- Simple counters
- Flushes every XX seconds to graphite
- UDP

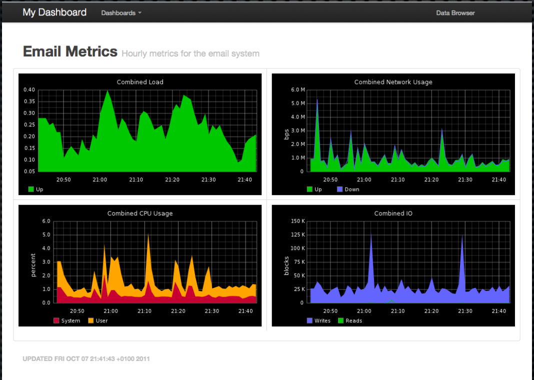
OPEN WORLD FORUM

Feeding statsd

```
echo "stats.sshd.login:1|c" |
nc -u statsd.example.com 8125
```

gdash

https://github.com/ripienaar/gdash

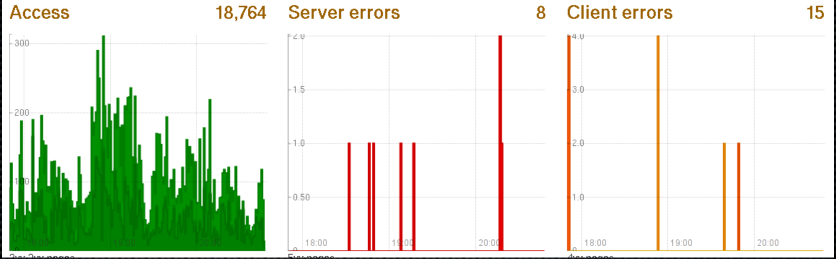


My Dashboard Dashboards ▾ Data Browser

Email Metrics Hourly metrics for the email system

UPDATED FRI OCT 07 21:41:43 +0100 2011

giraffe



Alternative to gdash

Kibana

- Kibana is a web interface for Logstash/ES
- Kibana 1 was written in PHP
- Kibana 2 was written in Ruby
- Kibana 3 is written in AngularJS

Kibana 3

- Everything happens in the browser
- The browser is connected to Elasticsearch
- You can save dashboards into ES
- You can write/template dashboards to files

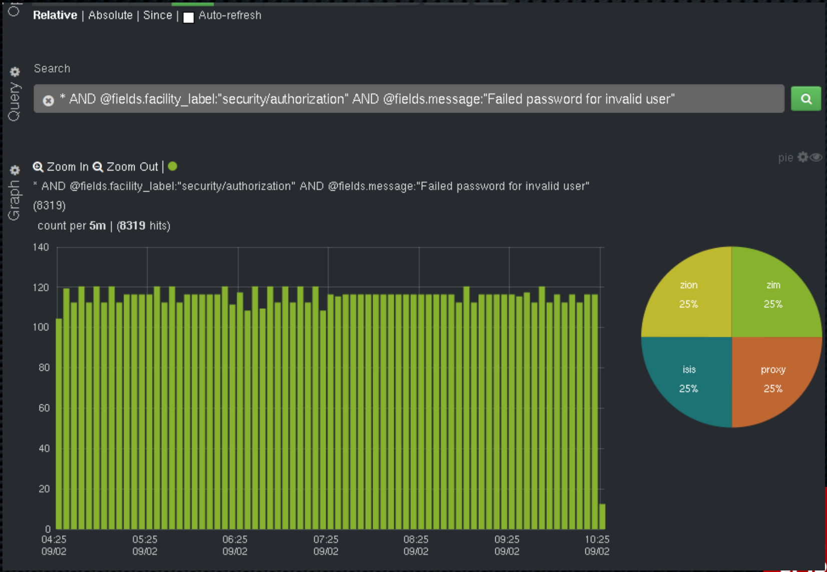
Kibana queries

Example of a kibana query

```
@fields.syslog_program:"httpd" AND
@fields.http_host:"test.example.com" AND
@fields.response:"404"
```

- Lucene query syntax
- Simple and effective
- Point & click web interface

OPEN WORLD FORUM



Relative | Absolute | Since | □ Auto-refresh

Query

Search

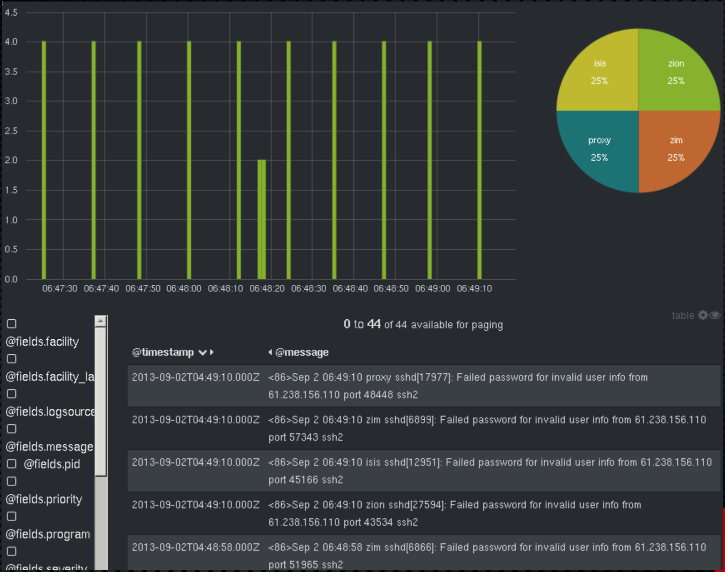
* AND @fields.facility_label:"security/authorization" AND @fields.message:"Failed password for invalid user"

Graph

Zoom In Zoom Out | ●

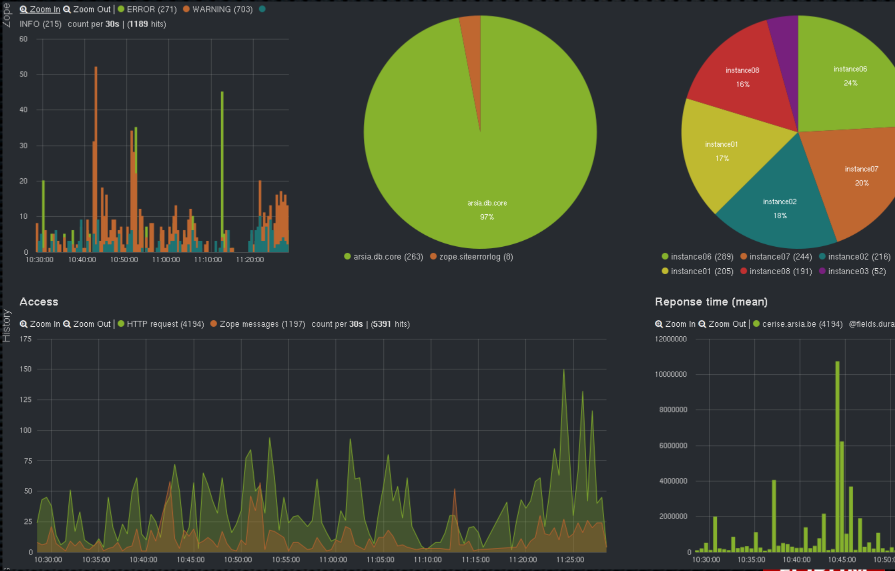
* AND @fields.facility_label:"security/authorization" AND @fields.message:"Failed password for invalid user" (8319)

count per **5m** | (**8319** hits)



0 to 44 of 44 available for paging

@timestamp	@message
2013-09-02T04:49:10.000Z	<86>Sep 2 06:49:10 proxy sshd[17977]: Failed password for invalid user info from 61.238.156.110 port 48448 ssh2
2013-09-02T04:49:10.000Z	<86>Sep 2 06:49:10 zim sshd[6899]: Failed password for invalid user info from 61.238.156.110 port 57343 ssh2
2013-09-02T04:49:10.000Z	<86>Sep 2 06:49:10 isis sshd[12951]: Failed password for invalid user info from 61.238.156.110 port 45166 ssh2
2013-09-02T04:49:10.000Z	<86>Sep 2 06:49:10 zion sshd[27594]: Failed password for invalid user info from 61.238.156.110 port 43534 ssh2
2013-09-02T04:48:58.000Z	<86>Sep 2 06:48:58 zim sshd[6866]: Failed password for invalid user info from 61.238.156.110 port 51965 ssh2


Zope
Zoom In | Zoom Out | ● ERROR (271) ● WARNING (703) ● INFO (215) count per 30s | (1189 hits)
60
50
40
30
20
10
0
10:30:00
10:40:00
10:50:00
11:00:00
11:10:00
11:20:00
arsia.db.core
97%
● arsia.db.core (263) ● zope.siteerrorlog (8)
instance06
24%
instance07
20%
instance02
18%
instance01
17%
instance08
16%
● instance06 (289) ● instance07 (244) ● instance02 (216)
● instance01 (205) ● instance08 (191) ● instance03 (52)
History
Access
Zoom In | Zoom Out | ● HTTP request (4194) ● Zope messages (1197) count per 30s | (5391 hits)
175
150
125
100
75
50
25
0
10:30:00
10:35:00
10:40:00
10:45:00
10:50:00
10:55:00
11:00:00
11:05:00
11:10:00
11:15:00
11:20:00
11:25:00
Reponse time (mean)
Zoom In | Zoom Out | ● cerise.arsia.be (4194) @fields.dura
12000000
10000000
8000000
6000000
4000000
2000000
0
10:30:00
10:35:00
10:40:00
10:45:00
10:50:0

Toolchain example

- Apache ships logs to rsyslog
- Rsyslog ships logs to logstash
- Logstash ships metrics to statsd
- Statsd ships metrics to Graphite
- Icinga query metric from graphite
- https://github.com/etsy/nagios_tools

Reusing Icinga/Nagios perfdata

- Icinga performs various checks
- Icinga sends perfdata to graphite
- Graphite stores the data
- Gdash serves them inside dashboards
- https://github.com/roidelapluie/icinga-to-graphite

Sharing

- Build dashboard: dashing, teamdash
- Share with developers
- Share with managers

Try them yourself

https://github.com/KrisBuytaert/vagrant-graphite

Thank you

Any question?

OPEN WORLD FORUM

Contact

Julien Pivotto
julien@inuits.eu
@roidelapluie

inuits
open source

INUITS bvba
Duboisstraat 50
2060 Antwerp
Belgium
+32 473 441 636
https://inuits.eu

OPEN WORLD FORUM