elasticsearch

openSUSE™

one Center

ZABBIX 2014 Conference

THE BIGGEST INTERNATIONAL EVENT
Dedicated to Zabbix Monitoring Solution

Riga, Latvia | 12-13 September

ZABBIX Monitoring Soltuion

Logitoring :

log-driven monitroing

and

the Rocket science

Eugene Istomin

IT Architect

e.istomin@edss.ee

Cone Center,Tallinn

ZABBIX 2014 Conference

Topic goal:

talking about a common way of delivering, storing and analyzing monitoring/log/trace data flows.

In brief:

Does log-driven monitoring fits all needs?

TOC

Metrics in monitoring and logging

IT Monitoring - sum of methods used to collect defined metrics using checks.

Monitoring ~ protocol/agent, desired data descr, centralized storage, notifications

= Reactive

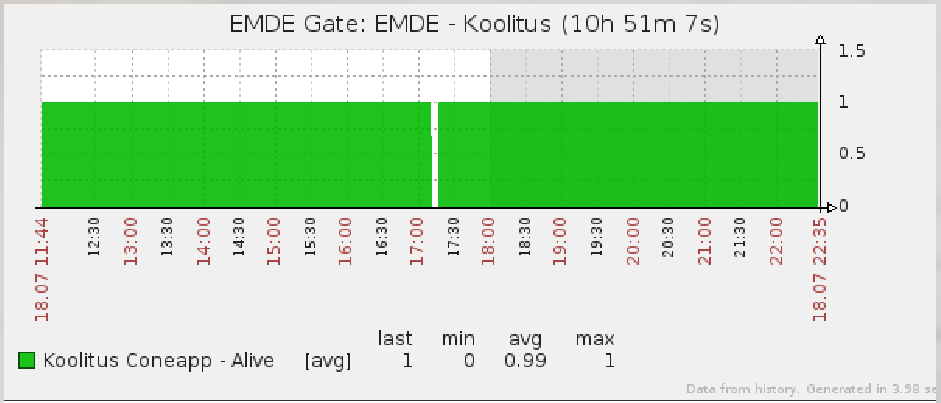
What is the classical monitoring metric?

Numeric! (int/bool/etc)

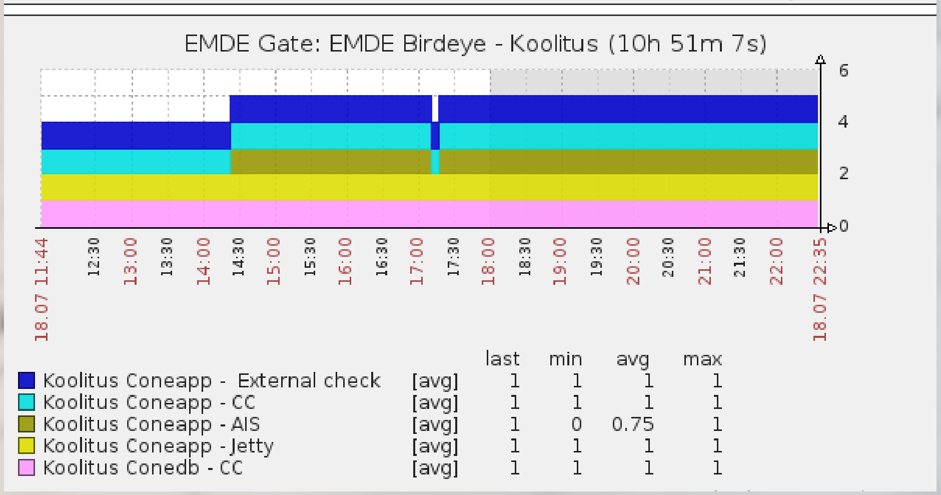
Metrics in monitoring and logging

Classical monitoring interfaces

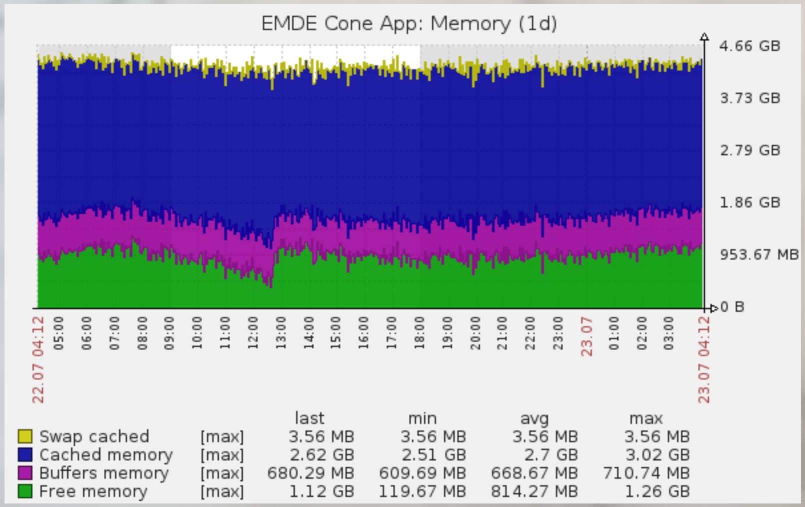
- **Zabbix**
- **Nagios**



		last	min	avg	max
🟩 Koolitus Coneapp - Alive	[avg]	1	0	0.99	1



		last	min	avg	max
🟦 Koolitus Coneapp - External check	[avg]	1	1	1	1
🟦 Koolitus Coneapp - CC	[avg]	1	1	1	1
🟫 Koolitus Coneapp - AIS	[avg]	1	0	0.75	1
🟨 Koolitus Coneapp - Jetty	[avg]	1	1	1	1
🟪 Koolitus Conedb - CC	[avg]	1	1	1	1



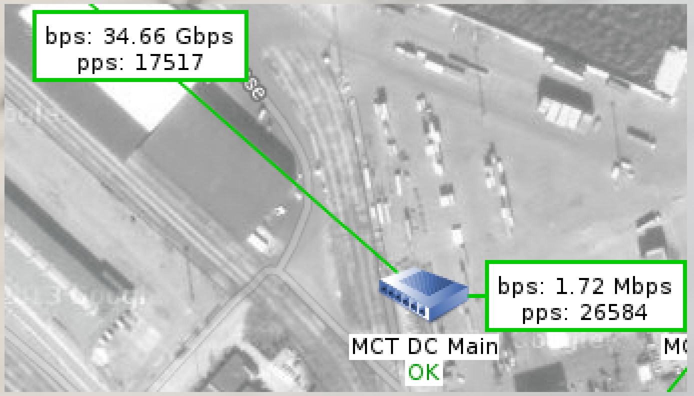
		last	min	avg	max
🟨 Swap cached	[max]	3.56 MB	3.56 MB	3.56 MB	3.56 MB
🟦 Cached memory	[max]	2.62 GB	2.51 GB	2.7 GB	3.02 GB
🟪 Buffers memory	[max]	680.29 MB	609.69 MB	668.67 MB	710.74 MB
🟩 Free memory	[max]	1.12 GB	119.67 MB	814.27 MB	1.26 GB

Metrics in monitoring and logging

Monitoring is usually used for:

- Servers status dashboard creation
- IT-administrators notification
- Numeric info visualization
- IT-inventory

Monitoring In brief:



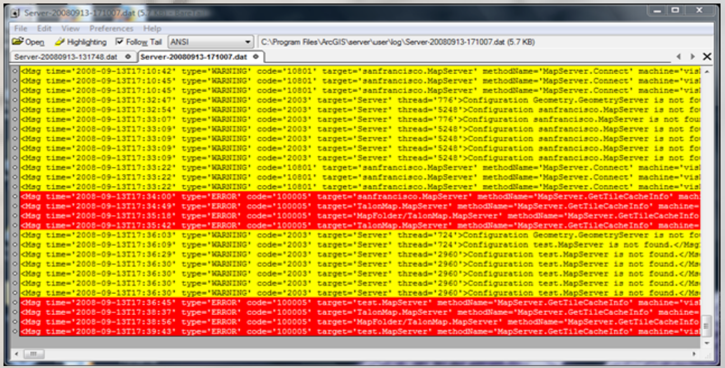
- Schema-based
- Use common network protocols or agents
- Stored data not reusable
- Needs by IT technics/admins

Metrics in monitoring and logging

IT Logging - sum of methods used to collect pass-through flows information.

Logs ~ syslog, pid/severity/ program, transport, centralized storage.

= Proactive


Server-20080913-171007.dat (5.7 KB)
File
Edit
View
Preferences
Help
Open
Highlighting
Follow Tail
ANSI
C:\Program Files\ArcGIS\server\user\log\Server-20080913-171007.dat (5.7 KB)
Server-20080913-131748.dat
Server-20080913-171007.dat

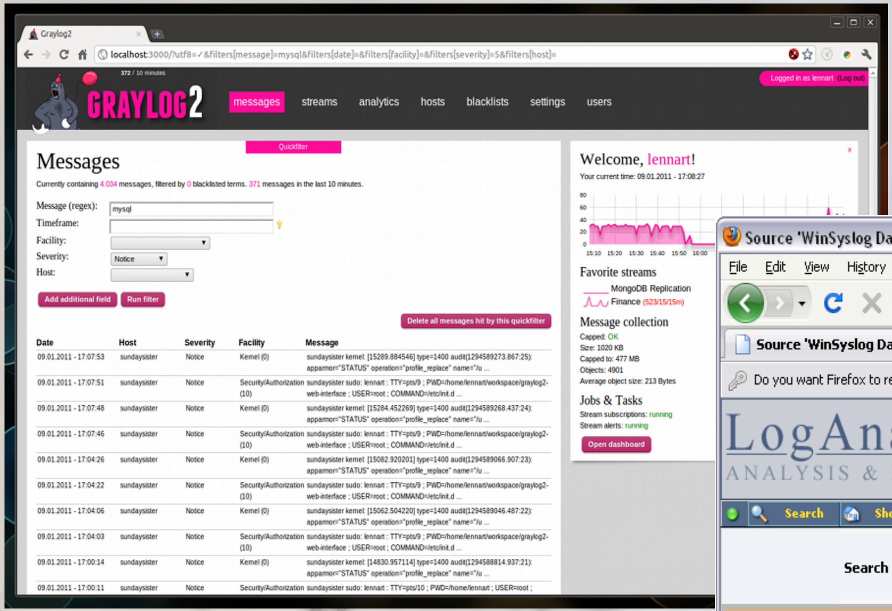
```
<Msg time='2008-09-13T17:10:42' type='WARNING' code='10801' target='sanfrancisco.MapServer' methodName='MapServer.Connect' machine='visi
<Msg time='2008-09-13T17:10:45' type='WARNING' code='10801' target='sanfrancisco.MapServer' methodName='MapServer.Connect' machine='visi
<Msg time='2008-09-13T17:10:45' type='WARNING' code='10801' target='sanfrancisco.MapServer' methodName='MapServer.Connect' machine='visi
<Msg time='2008-09-13T17:32:47' type='WARNING' code='2003' target='Server' thread='776'>Configuration Geometry.GeometryServer is not fo
<Msg time='2008-09-13T17:32:54' type='WARNING' code='2003' target='Server' thread='5248'>Configuration sanfrancisco.MapServer is not fo
<Msg time='2008-09-13T17:33:07' type='WARNING' code='2003' target='Server' thread='776'>Configuration sanfrancisco.MapServer is not fou
<Msg time='2008-09-13T17:33:09' type='WARNING' code='2003' target='Server' thread='5248'>Configuration sanfrancisco.MapServer is not fo
<Msg time='2008-09-13T17:33:09' type='WARNING' code='2003' target='Server' thread='5248'>Configuration sanfrancisco.MapServer is not fo
<Msg time='2008-09-13T17:33:09' type='WARNING' code='2003' target='Server' thread='5248'>Configuration sanfrancisco.MapServer is not fo
<Msg time='2008-09-13T17:33:09' type='WARNING' code='2003' target='Server' thread='5248'>Configuration sanfrancisco.MapServer is not fo
<Msg time='2008-09-13T17:33:22' type='WARNING' code='10801' target='sanfrancisco.MapServer' methodName='MapServer.Connect' machine='visi
<Msg time='2008-09-13T17:33:22' type='WARNING' code='10801' target='sanfrancisco.MapServer' methodName='MapServer.Connect' machine='visi
<Msg time='2008-09-13T17:33:22' type='WARNING' code='10801' target='sanfrancisco.MapServer' methodName='MapServer.Connect' machine='visi
<Msg time='2008-09-13T17:34:00' type='ERROR' code='100005' target='sanfrancisco.MapServer' methodName='MapServer.GetTileCacheInfo' mach
<Msg time='2008-09-13T17:34:49' type='ERROR' code='100005' target='TalonMap.MapServer' methodName='MapServer.GetTileCacheInfo' machine=
<Msg time='2008-09-13T17:35:18' type='ERROR' code='100005' target='MapFolder/TalonMap.MapServer' methodName='MapServer.GetTileCacheInfo
<Msg time='2008-09-13T17:35:42' type='ERROR' code='100005' target='TalonMap.MapServer' methodName='MapServer.GetTileCacheInfo' machine=
<Msg time='2008-09-13T17:36:03' type='WARNING' code='2003' target='Server' thread='724'>Configuration Geometry.GeometryServer is not fo
<Msg time='2008-09-13T17:36:09' type='WARNING' code='2003' target='Server' thread='724'>Configuration test.MapServer is not found.</Msg
<Msg time='2008-09-13T17:36:29' type='WARNING' code='2003' target='Server' thread='2960'>Configuration test.MapServer is not found.</Ma
<Msg time='2008-09-13T17:36:30' type='WARNING' code='2003' target='Server' thread='2960'>Configuration test.MapServer is not found.</Ma
<Msg time='2008-09-13T17:36:30' type='WARNING' code='2003' target='Server' thread='2960'>Configuration test.MapServer is not found.</Ma
<Msg time='2008-09-13T17:36:30' type='WARNING' code='2003' target='Server' thread='2960'>Configuration test.MapServer is not found.</Ma
<Msg time='2008-09-13T17:36:30' type='WARNING' code='2003' target='Server' thread='2960'>Configuration test.MapServer is not found.</Ma
<Msg time='2008-09-13T17:36:45' type='ERROR' code='100005' target='test.MapServer' methodName='MapServer.GetTileCacheInfo' machine='visi
<Msg time='2008-09-13T17:38:37' type='ERROR' code='100005' target='TalonMap.MapServer' methodName='MapServer.GetTileCacheInfo' machine=
<Msg time='2008-09-13T17:38:56' type='ERROR' code='100005' target='MapFolder/TalonMap.MapServer' methodName='MapServer.GetTileCacheInfo
<Msg time='2008-09-13T17:39:43' type='ERROR' code='100005' target='test.MapServer' methodName='MapServer.GetTileCacheInfo' machine='visi
```

What is the classical logs metric?

String!

Metrics in monitoring and logging

Classical logging interfaces



localhost:3000/?utf8=✓&filters[message]=mysql&filters[date]=&filters[facility]=&filters[severity]=5&filters[host]=

372 / 10 minutes

Messages

Currently containing 4.034 messages, filtered by 0 blacklisted terms. 371 messages in the last 10 minutes.

Message (regex): mysql
Timeframe:
Facility:
Severity: Notice
Host:

Date	Host	Severity	Facility	Message
09.01.2011 - 17:07:53	sundaysister	Notice	Kernel (0)	sundaysister kernel: [15289.884546] type=1400 audit(1294589273.867:25): apparmor="STATUS" operation="profile_replace" name="/u ...
09.01.2011 - 17:07:51	sundaysister	Notice	Security/Authorization (10)	sundaysister sudo: lennart : TTY=pts/9 ; PWD=/home/lennart/workspace/graylog2-web-interface ; USER=root ; COMMAND=/etc/init.d ...
09.01.2011 - 17:07:48	sundaysister	Notice	Kernel (0)	sundaysister kernel: [15284.452269] type=1400 audit(1294589268.437:24): apparmor="STATUS" operation="profile_replace" name="/u ...
09.01.2011 - 17:07:46	sundaysister	Notice	Security/Authorization (10)	sundaysister sudo: lennart : TTY=pts/9 ; PWD=/home/lennart/workspace/graylog2-web-interface ; USER=root ; COMMAND=/etc/init.d ...
09.01.2011 - 17:04:26	sundaysister	Notice	Kernel (0)	sundaysister kernel: [15082.920201] type=1400 audit(1294589066.907:23): apparmor="STATUS" operation="profile_replace" name="/u ...
09.01.2011 - 17:04:22	sundaysister	Notice	Security/Authorization (10)	sundaysister sudo: lennart : TTY=pts/9 ; PWD=/home/lennart/workspace/graylog2-web-interface ; USER=root ; COMMAND=/etc/init.d ...
09.01.2011 - 17:04:06	sundaysister	Notice	Kernel (0)	sundaysister kernel: [15062.504220] type=1400 audit(1294589046.487:22): apparmor="STATUS" operation="profile_replace" name="/u ...
09.01.2011 - 17:04:03	sundaysister	Notice	Security/Authorization (10)	sundaysister sudo: lennart : TTY=pts/9 ; PWD=/home/lennart/workspace/graylog2-web-interface ; USER=root ; COMMAND=/etc/init.d ...
09.01.2011 - 17:00:14	sundaysister	Notice	Kernel (0)	sundaysister kernel: [14830.957114] type=1400 audit(1294588814.937:21): apparmor="STATUS" operation="profile_replace" name="/u ...
09.01.2011 - 17:00:11	sundaysister	Notice	Security/Authorization	sundaysister sudo: lennart : TTY=pts/10 ; PWD=/home/lennart ; USER=root ;

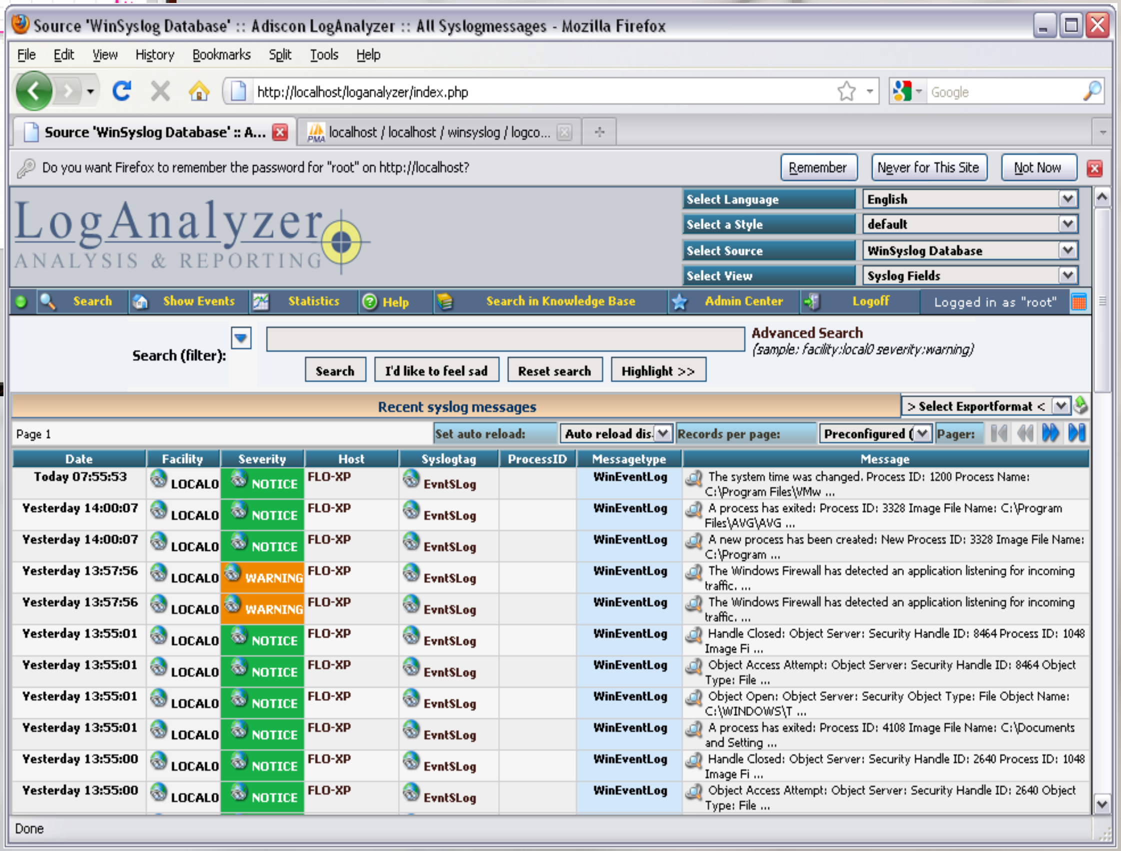
Welcome, lennart!

Your current time: 09.01.2011 - 17:08:27

Favorite streams
MongoDB Replication
Finance (523/15/15m)

Message collection
Capped: OK
Size: 1020 KB
Capped to: 477 MB
Objects: 4901
Average object size: 213 Bytes

Jobs & Tasks
Stream subscriptions: running
Stream alerts: running



Source 'WinSyslog Database' :: Adiscon LogAnalyzer :: All Syslogmessages - Mozilla Firefox

http://localhost/loganalyzer/index.php

Source 'WinSyslog Database' :: A... | localhost / localhost / winsyslog / logco...

Do you want Firefox to remember the password for "root" on http://localhost?

Select Language: English
Select a Style: default
Select Source: WinSyslog Database
Select View: Syslog Fields

Logged in as "root"

Search (filter):

Advanced Search
(sample: facility:local0 severity:warning)

Recent syslog messages

> Select Exportformat <

Page 1
Set auto reload: Auto reload dis
Records per page: Preconfigured (
Pager:

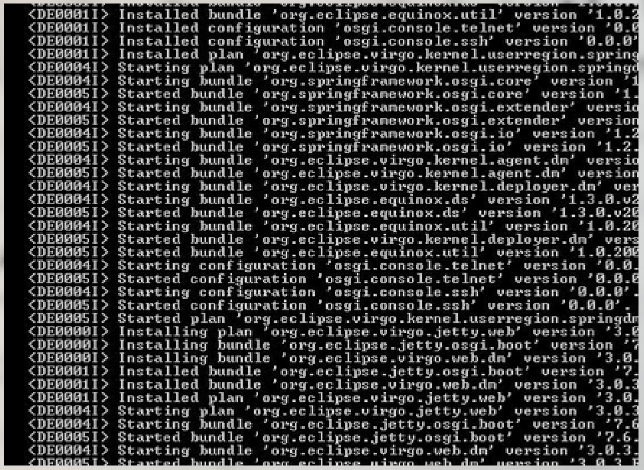
Date	Facility	Severity	Host	Syslogtag	ProcessID	Messagetype	Message
Today 07:55:53	LOCAL0	NOTICE	FLO-XP	EvntSLog		WinEventLog	The system time was changed. Process ID: 1200 Process Name: C:\Program Files\VMw ...
Yesterday 14:00:07	LOCAL0	NOTICE	FLO-XP	EvntSLog		WinEventLog	A process has exited: Process ID: 3328 Image File Name: C:\Program Files\AVG\AVG ...
Yesterday 14:00:07	LOCAL0	NOTICE	FLO-XP	EvntSLog		WinEventLog	A new process has been created: New Process ID: 3328 Image File Name: C:\Program ...
Yesterday 13:57:56	LOCAL0	WARNING	FLO-XP	EvntSLog		WinEventLog	The Windows Firewall has detected an application listening for incoming traffic. ...
Yesterday 13:57:56	LOCAL0	WARNING	FLO-XP	EvntSLog		WinEventLog	The Windows Firewall has detected an application listening for incoming traffic. ...
Yesterday 13:55:01	LOCAL0	NOTICE	FLO-XP	EvntSLog		WinEventLog	Handle Closed: Object Server: Security Handle ID: 8464 Process ID: 1048 Image Fi ...
Yesterday 13:55:01	LOCAL0	NOTICE	FLO-XP	EvntSLog		WinEventLog	Object Access Attempt: Object Server: Security Handle ID: 8464 Object Type: File ...
Yesterday 13:55:01	LOCAL0	NOTICE	FLO-XP	EvntSLog		WinEventLog	Object Open: Object Server: Security Object Type: File Object Name: C:\WINDOWS\T ...
Yesterday 13:55:01	LOCAL0	NOTICE	FLO-XP	EvntSLog		WinEventLog	A process has exited: Process ID: 4108 Image File Name: C:\Documents and Setting ...
Yesterday 13:55:00	LOCAL0	NOTICE	FLO-XP	EvntSLog		WinEventLog	Handle Closed: Object Server: Security Handle ID: 2640 Process ID: 1048 Image Fi ...
Yesterday 13:55:00	LOCAL0	NOTICE	FLO-XP	EvntSLog		WinEventLog	Object Access Attempt: Object Server: Security Handle ID: 2640 Object Type: File ...

- Loganalyzer
- Greylog

Metrics in monitoring and logging

Logging is usually used for:

- Problem resolving
- Debugging & development
- Security access violation events storage



```
<DE0001I> Installed bundle 'org.eclipse.equinox.util' version '1.0.2
<DE0001I> Installed configuration 'osgi.console.telnet' version '0.0
<DE0001I> Installed configuration 'osgi.console.ssh' version '0.0.0'
<DE0001I> Installed plan 'org.eclipse.virgo.kernel.userregion.spring
<DE0004I> Starting plan 'org.eclipse.virgo.kernel.userregion.springd
<DE0004I> Starting bundle 'org.springframework.osgi.core' version '1
<DE0005I> Started bundle 'org.springframework.osgi.core' version '1.
<DE0004I> Starting bundle 'org.springframework.osgi.extender' versio
<DE0005I> Started bundle 'org.springframework.osgi.extender' version
<DE0004I> Starting bundle 'org.springframework.osgi.io' version '1.2
<DE0005I> Started bundle 'org.springframework.osgi.io' version '1.2.
<DE0004I> Starting bundle 'org.eclipse.virgo.kernel.agent.dm' versio
<DE0005I> Started bundle 'org.eclipse.virgo.kernel.agent.dm' version
<DE0004I> Starting bundle 'org.eclipse.virgo.kernel.deployer.dm' ver
<DE0004I> Starting bundle 'org.eclipse.equinox.ds' version '1.3.0.v2
<DE0005I> Started bundle 'org.eclipse.equinox.ds' version '1.3.0.v20
<DE0004I> Starting bundle 'org.eclipse.equinox.util' version '1.0.20
<DE0005I> Started bundle 'org.eclipse.virgo.kernel.deployer.dm' vers
<DE0005I> Started bundle 'org.eclipse.equinox.util' version '1.0.200
<DE0004I> Starting configuration 'osgi.console.telnet' version '0.0.
<DE0005I> Started configuration 'osgi.console.telnet' version '0.0.0
<DE0004I> Starting configuration 'osgi.console.ssh' version '0.0.0'.
<DE0005I> Started configuration 'osgi.console.ssh' version '0.0.0'.
<DE0005I> Started plan 'org.eclipse.virgo.kernel.userregion.springdm
<DE0000I> Installing plan 'org.eclipse.virgo.jetty.web' version '3.0
<DE0000I> Installing bundle 'org.eclipse.jetty.osgi.boot' version '7
<DE0000I> Installing bundle 'org.eclipse.virgo.web.dm' version '3.0.
<DE0001I> Installed bundle 'org.eclipse.jetty.osgi.boot' version '7.
<DE0001I> Installed bundle 'org.eclipse.virgo.web.dm' version '3.0.3
<DE0001I> Installed plan 'org.eclipse.virgo.jetty.web' version '3.0.
<DE0004I> Starting plan 'org.eclipse.virgo.jetty.web' version '3.0.3
<DE0004I> Starting bundle 'org.eclipse.jetty.osgi.boot' version '7.6
<DE0005I> Started bundle 'org.eclipse.jetty.osgi.boot' version '7.6.
<DE0004I> Starting bundle 'org.eclipse.virgo.web.dm' version '3.0.3.
```

Logging In brief:

- Schema-less
- Use syslog or API/REST
- Stored data are reusable
- Needs by developers

Metrics in monitoring and logging

Do the data in monitoring **is the same** as data in logging?

Yes, if:

- the data is <u>well tokenized</u> (known keys)

A=2, TO=me@z.com…

- the data have a <u>common syntax</u> (JSON/CSV)

{ “A”:”2”, “TO”:[“me@z.com”,…] }

Metrics in monitoring and logging

Do the data in monitoring **is the same** as data in logging?

Yes, if:

• the data have known type mapping
(“field TO = string”, “field ID = int”)

{ “A”:”int”, “TO”:”array” }

• storage layer use efficient token/key/hash-based algorithms

“me@z.com”=>“me”,”z”,”com”

Metrics in monitoring and logging

Do the data in monitoring **is the same** as data in logging?

Yes, if:

- user UI/API can ask for mixed fields content using complex expressions (regexp/ranges/sorts)

```
"query_string" : {
        "fields" : ["TO.*"],
        "query" : "a AND com OR z"
    }
```

Metrics in monitoring and logging

Do the data in monitoring have the **same** nature as data in logging?

Yes,

- Monitoring and logging are subsets of events
- Monitoring is mainly reactive
- Logging is mainly proactive

Events is a set includes all possible types of messages (monitoring, logging, JSON data exchange by HTTP or TCP, etc)

TOC

Metrics in monitoring and logging

By log-driven monitoring – to dataflow -driven services.

Rsyslog event transport

Let's try. Live test case

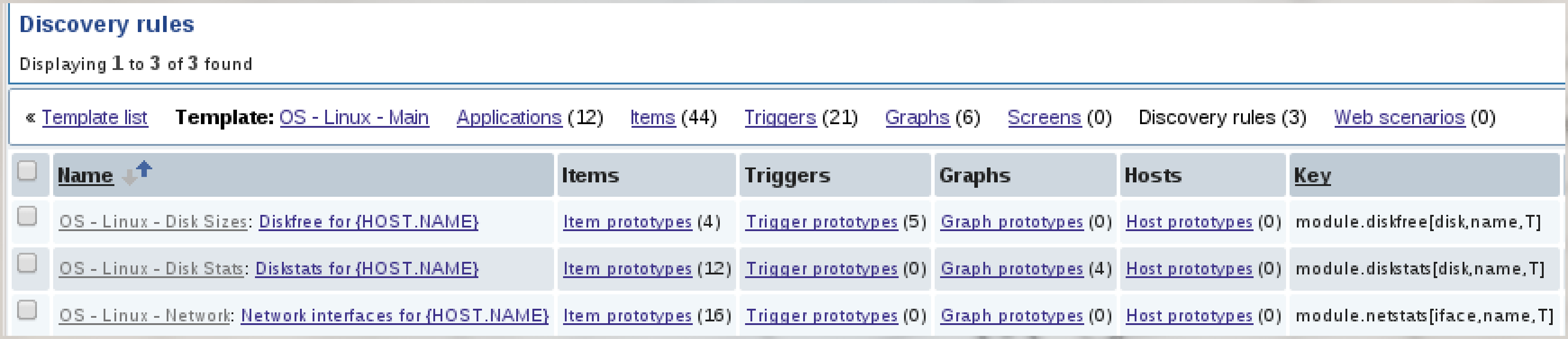
Log-driven monitoring

Log-driven monitoring -
a sum of techniques that provides access to logs events fields from high-level decision-maker application using complex expressions.

```
1. { haproxy_status=503},... { jmx_app1_status=500 }
2. "query_string" : {
       "fields" : ["haproxy_status",”jmx_*_status”],
       "query" : ">=500"
   }
3. action → notify admins
```

Log-driven monitoring

LLD is superb

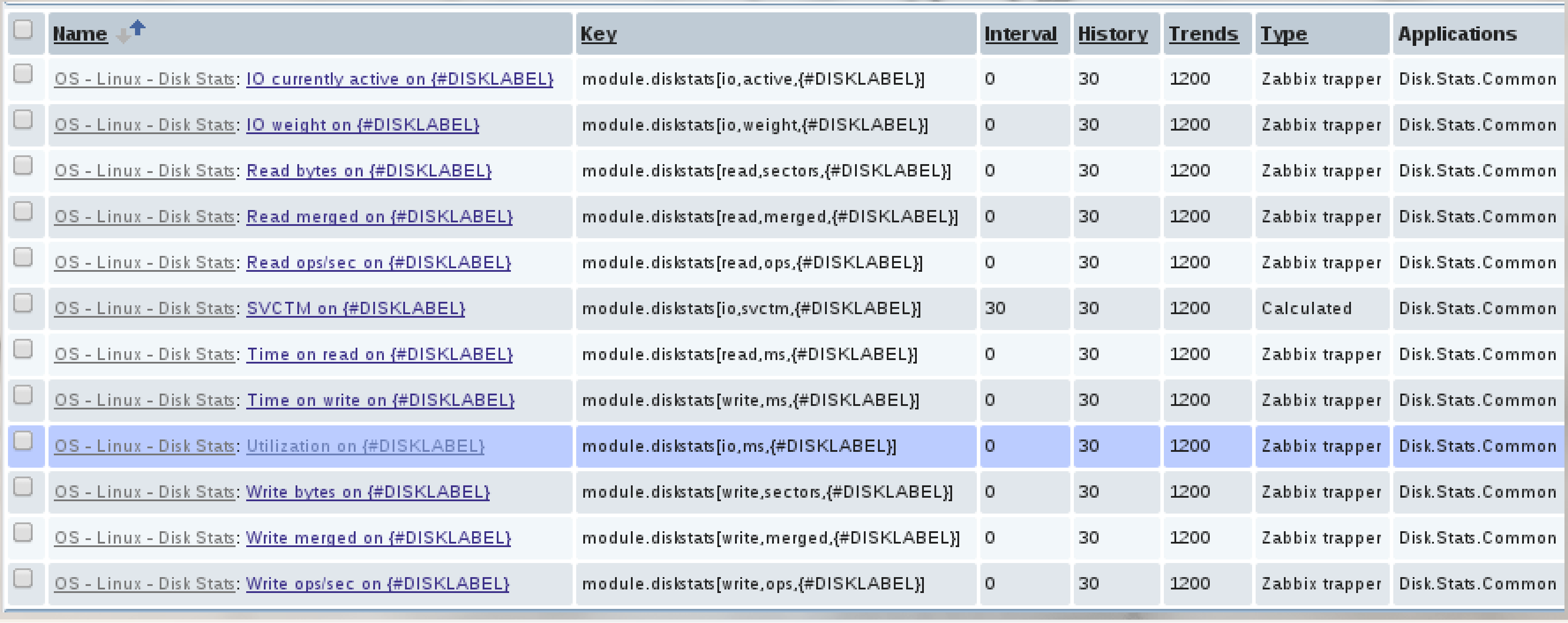


Discovery rules

Displaying **1** to **3** of **3** found

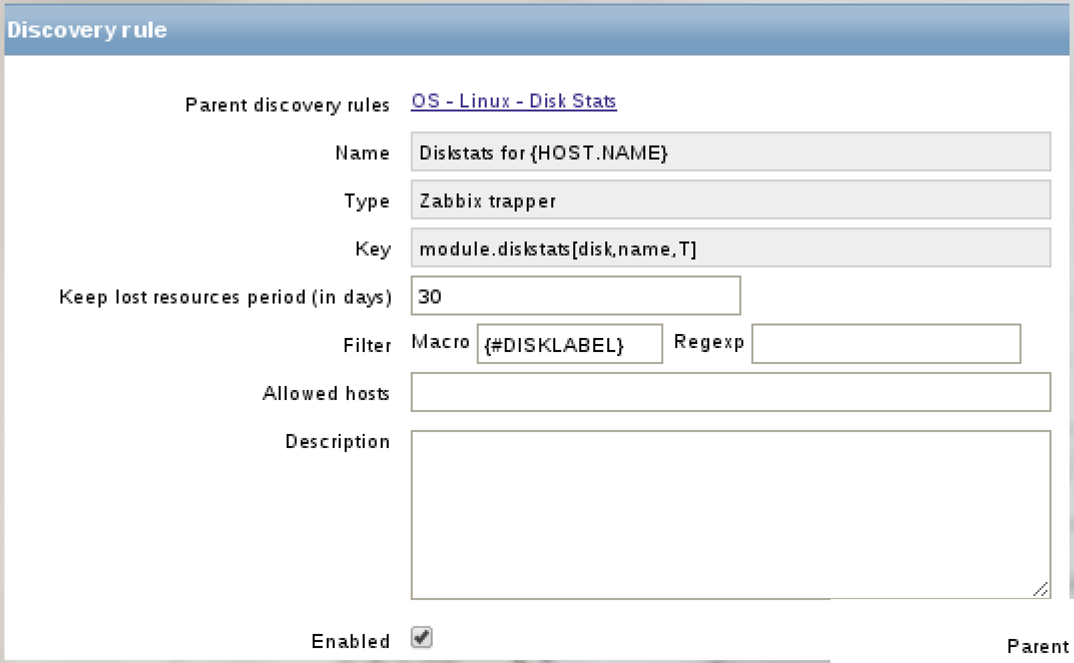
« Template list **Template:** OS - Linux - Main Applications (12) Items (44) Triggers (21) Graphs (6) Screens (0) Discovery rules (3) Web scenarios (0)

☐	Name	Items	Triggers	Graphs	Hosts	Key
☐	OS - Linux - Disk Sizes: Diskfree for {HOST.NAME}	Item prototypes (4)	Trigger prototypes (5)	Graph prototypes (0)	Host prototypes (0)	module.diskfree[disk,name,T]
☐	OS - Linux - Disk Stats: Diskstats for {HOST.NAME}	Item prototypes (12)	Trigger prototypes (0)	Graph prototypes (4)	Host prototypes (0)	module.diskstats[disk,name,T]
☐	OS - Linux - Network: Network interfaces for {HOST.NAME}	Item prototypes (16)	Trigger prototypes (0)	Graph prototypes (0)	Host prototypes (0)	module.netstats[iface,name,T]



☐	Name	Key	Interval	History	Trends	Type	Applications
☐	OS - Linux - Disk Stats: IO currently active on {#DISKLABEL}	module.diskstats[io,active,{#DISKLABEL}]	0	30	1200	Zabbix trapper	Disk.Stats.Common
☐	OS - Linux - Disk Stats: IO weight on {#DISKLABEL}	module.diskstats[io,weight,{#DISKLABEL}]	0	30	1200	Zabbix trapper	Disk.Stats.Common
☐	OS - Linux - Disk Stats: Read bytes on {#DISKLABEL}	module.diskstats[read,sectors,{#DISKLABEL}]	0	30	1200	Zabbix trapper	Disk.Stats.Common
☐	OS - Linux - Disk Stats: Read merged on {#DISKLABEL}	module.diskstats[read,merged,{#DISKLABEL}]	0	30	1200	Zabbix trapper	Disk.Stats.Common
☐	OS - Linux - Disk Stats: Read ops/sec on {#DISKLABEL}	module.diskstats[read,ops,{#DISKLABEL}]	0	30	1200	Zabbix trapper	Disk.Stats.Common
☐	OS - Linux - Disk Stats: SVCTM on {#DISKLABEL}	module.diskstats[io,svctm,{#DISKLABEL}]	30	30	1200	Calculated	Disk.Stats.Common
☐	OS - Linux - Disk Stats: Time on read on {#DISKLABEL}	module.diskstats[read,ms,{#DISKLABEL}]	0	30	1200	Zabbix trapper	Disk.Stats.Common
☐	OS - Linux - Disk Stats: Time on write on {#DISKLABEL}	module.diskstats[write,ms,{#DISKLABEL}]	0	30	1200	Zabbix trapper	Disk.Stats.Common
☐	OS - Linux - Disk Stats: Utilization on {#DISKLABEL}	module.diskstats[io,ms,{#DISKLABEL}]	0	30	1200	Zabbix trapper	Disk.Stats.Common
☐	OS - Linux - Disk Stats: Write bytes on {#DISKLABEL}	module.diskstats[write,sectors,{#DISKLABEL}]	0	30	1200	Zabbix trapper	Disk.Stats.Common
☐	OS - Linux - Disk Stats: Write merged on {#DISKLABEL}	module.diskstats[write,merged,{#DISKLABEL}]	0	30	1200	Zabbix trapper	Disk.Stats.Common
☐	OS - Linux - Disk Stats: Write ops/sec on {#DISKLABEL}	module.diskstats[write,ops,{#DISKLABEL}]	0	30	1200	Zabbix trapper	Disk.Stats.Common

Log-driven monitoring

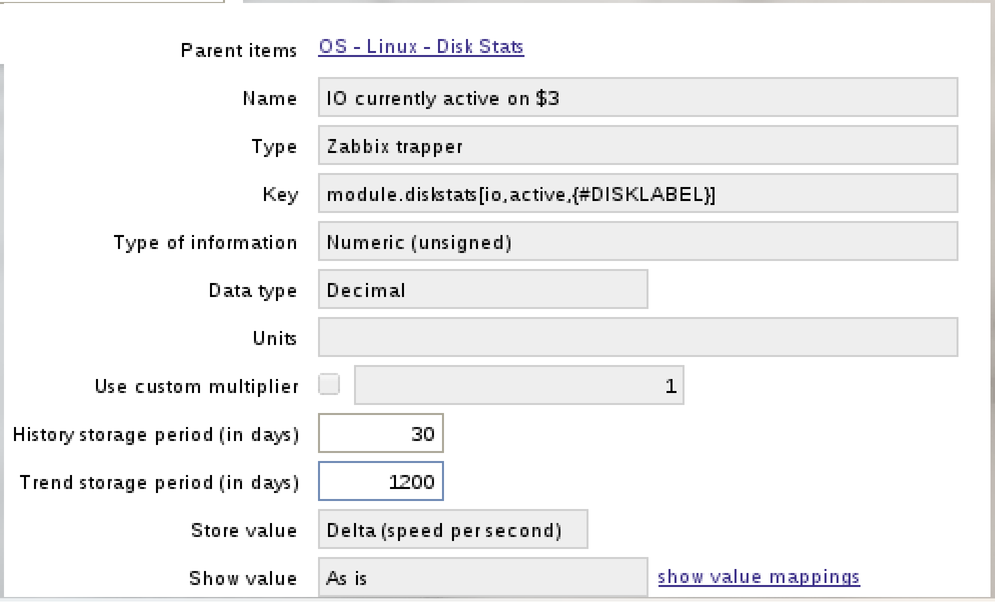


Discovery rule

Parent discovery rules	OS - Linux - Disk Stats
Name	Diskstats for {HOST.NAME}
Type	Zabbix trapper
Key	module.diskstats[disk,name,T]
Keep lost resources period (in days)	30
Filter	Macro {#DISKLABEL} Regexp
Allowed hosts	
Description	
Enabled	✓

LLD is superb

All items are trappers

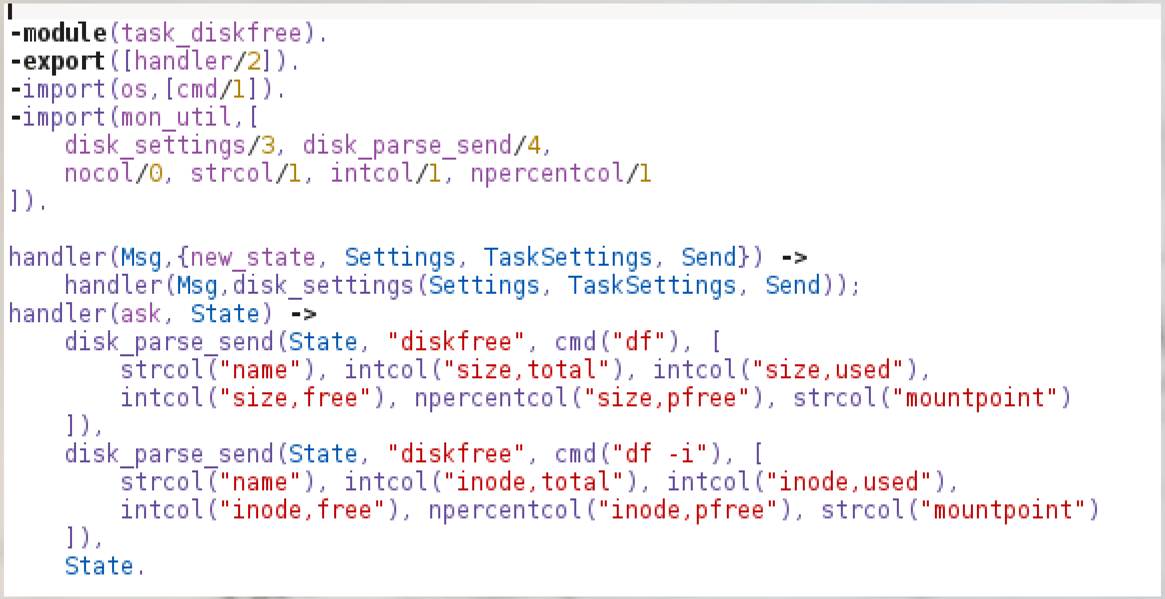


Parent items	OS - Linux - Disk Stats
Name	IO currently active on $3
Type	Zabbix trapper
Key	module.diskstats[io,active,{#DISKLABEL}]
Type of information	Numeric (unsigned)
Data type	Decimal
Units	
Use custom multiplier	☐ 1
History storage period (in days)	30
Trend storage period (in days)	1200
Store value	Delta (speed per second)
Show value	As is show value mappings

Items are created by JSON POST using exernal CMDB database

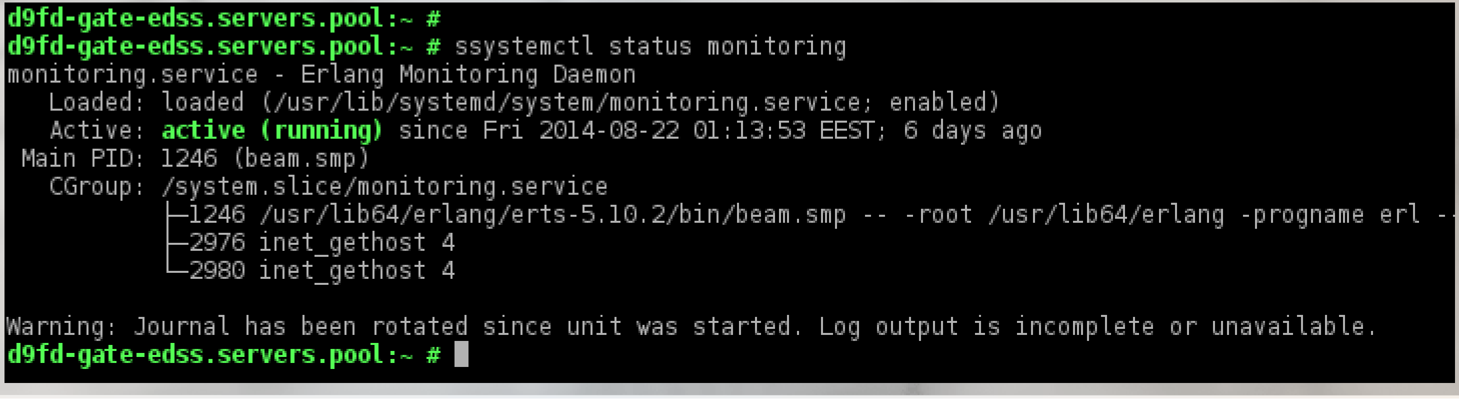
Log-driven monitoring

Fast-as-light Erlang Zabbix sender



```
-module(task_diskfree).
-export([handler/2]).
-import(os,[cmd/1]).
-import(mon_util,[
    disk_settings/3, disk_parse_send/4,
    nocol/0, strcol/1, intcol/1, npercentcol/1
]).

handler(Msg,{new_state, Settings, TaskSettings, Send}) ->
    handler(Msg,disk_settings(Settings, TaskSettings, Send));
handler(ask, State) ->
    disk_parse_send(State, "diskfree", cmd("df"), [
        strcol("name"), intcol("size,total"), intcol("size,used"),
        intcol("size,free"), npercentcol("size,pfree"), strcol("mountpoint")
    ]),
    disk_parse_send(State, "diskfree", cmd("df -i"), [
        strcol("name"), intcol("inode,total"), intcol("inode,used"),
        intcol("inode,free"), npercentcol("inode,pfree"), strcol("mountpoint")
    ]),
    State.
```

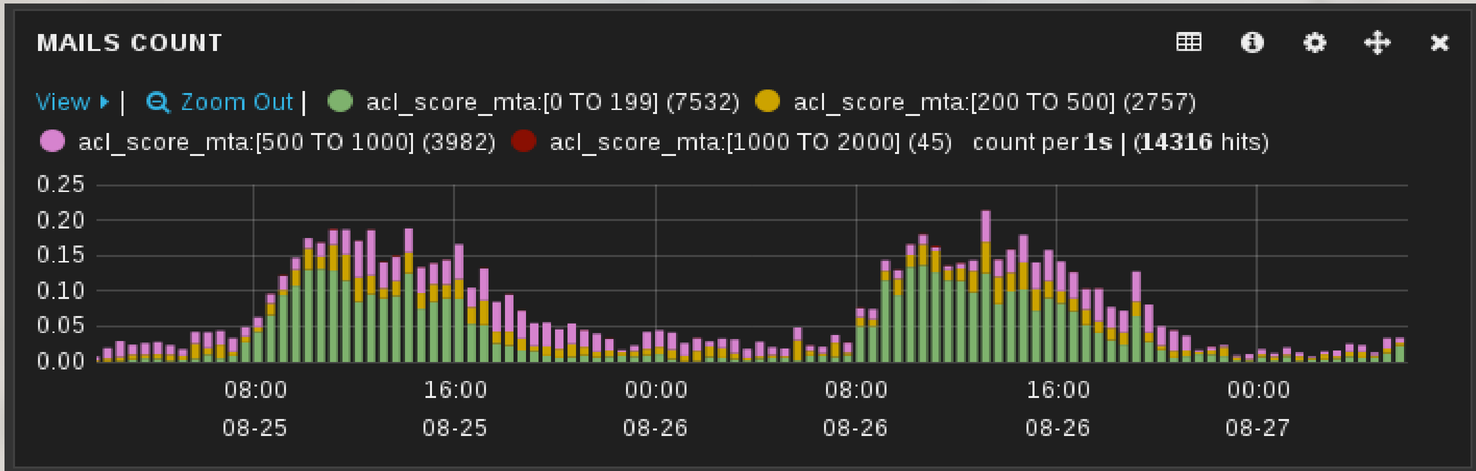
Systemd-based service

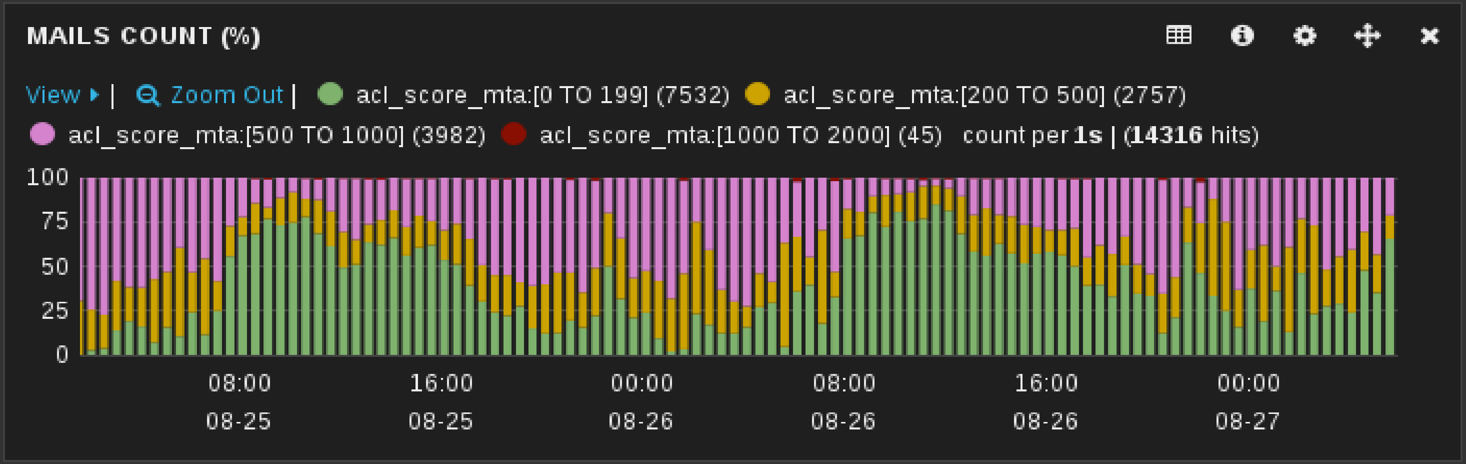


```
d9fd-gate-edss.servers.pool:~ #
d9fd-gate-edss.servers.pool:~ # ssystemctl status monitoring
monitoring.service - Erlang Monitoring Daemon
   Loaded: loaded (/usr/lib/systemd/system/monitoring.service; enabled)
   Active: active (running) since Fri 2014-08-22 01:13:53 EEST; 6 days ago
 Main PID: 1246 (beam.smp)
   CGroup: /system.slice/monitoring.service
           ├─1246 /usr/lib64/erlang/erts-5.10.2/bin/beam.smp -- -root /usr/lib64/erlang -progname erl --
           ├─2976 inet_gethost 4
           └─2980 inet_gethost 4

Warning: Journal has been rotated since unit was started. Log output is incomplete or unavailable.
d9fd-gate-edss.servers.pool:~ #
```

Log-driven monitoring

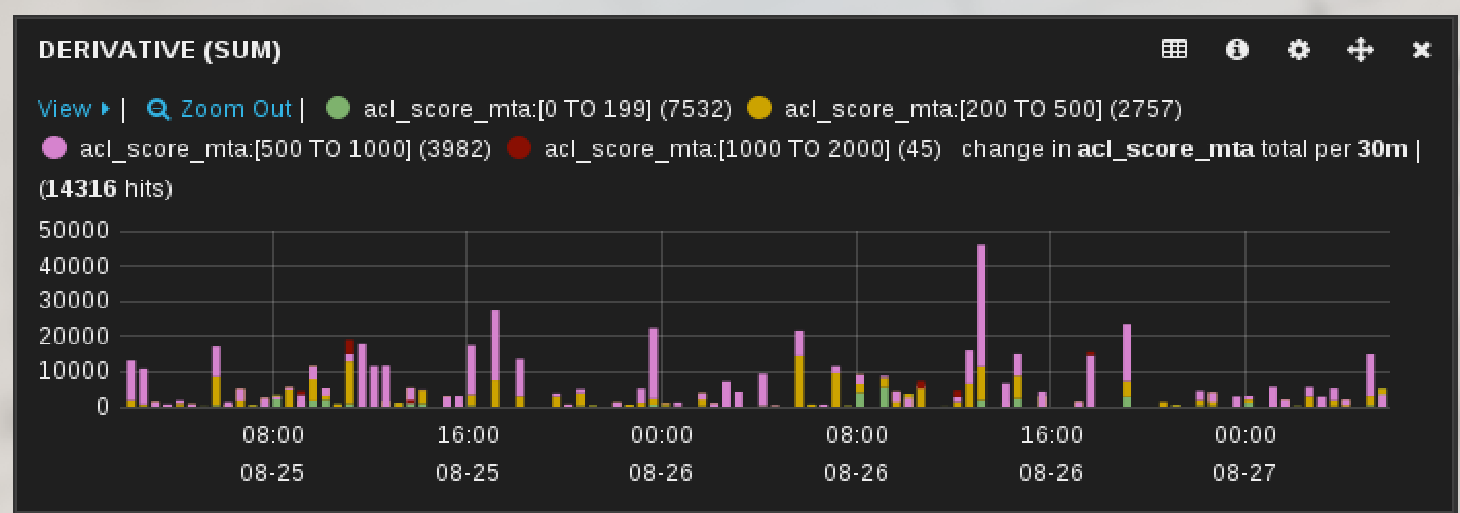
mails count per second in normal & percent grade



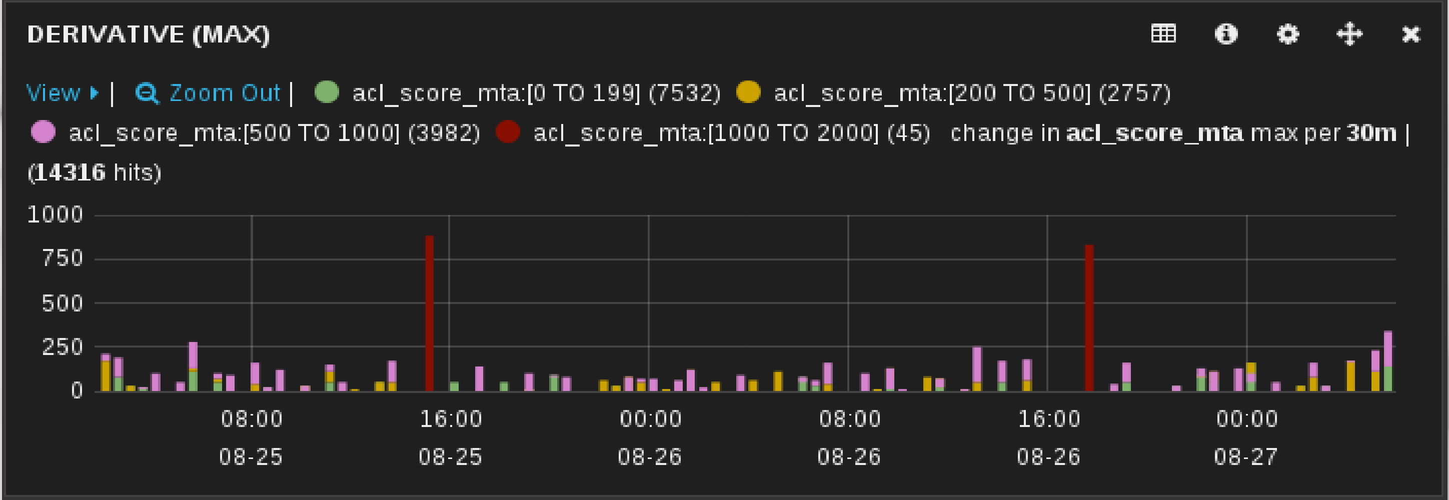


Log-driven monitoring

derivative of mails count per second coerced to spamscore SUM & MAX


DERIVATIVE (SUM)

View ▸ | Zoom Out | ● acl_score_mta:[0 TO 199] (7532) ● acl_score_mta:[200 TO 500] (2757) ● acl_score_mta:[500 TO 1000] (3982) ● acl_score_mta:[1000 TO 2000] (45) change in **acl_score_mta** total per **30m** | (**14316** hits)

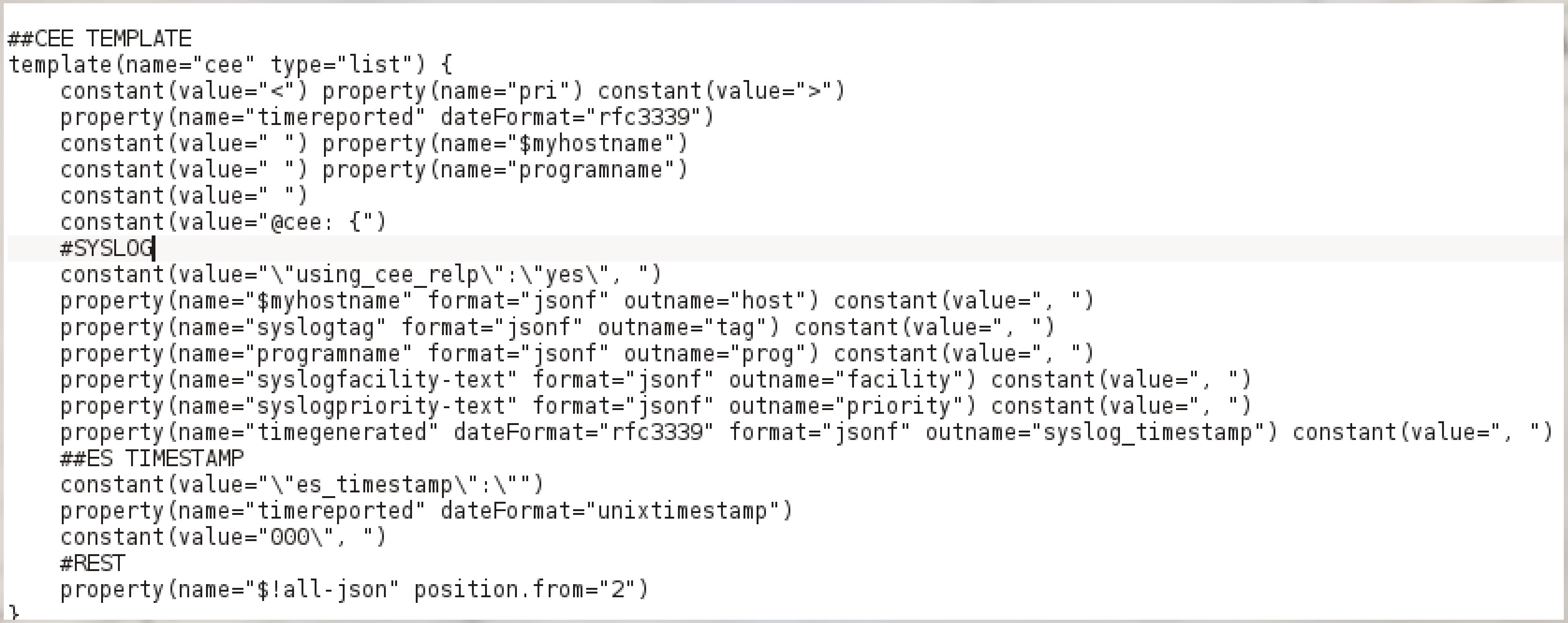

DERIVATIVE (MAX)

View ▸ | Zoom Out | ● acl_score_mta:[0 TO 199] (7532) ● acl_score_mta:[200 TO 500] (2757) ● acl_score_mta:[500 TO 1000] (3982) ● acl_score_mta:[1000 TO 2000] (45) change in **acl_score_mta** max per **30m** | (**14316** hits)

TOC

Rsyslog event transport

Rsyslog templates for CEE logging

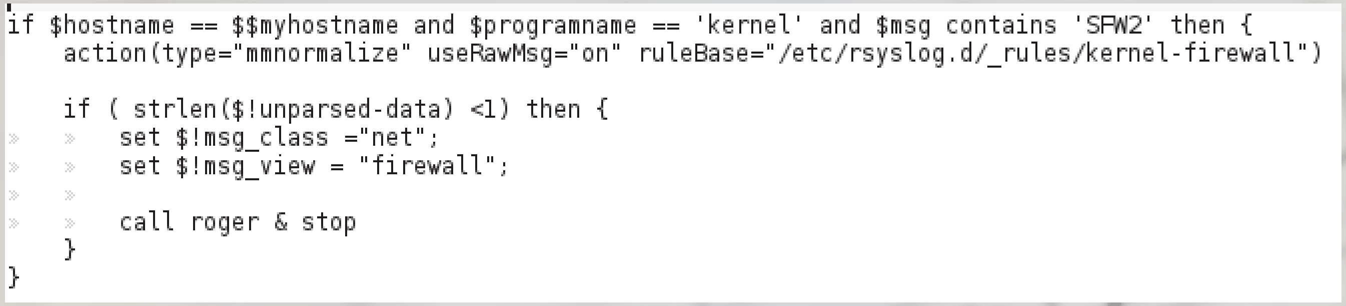


```
##CEE TEMPLATE
template(name="cee" type="list") {
    constant(value="<") property(name="pri") constant(value=">")
    property(name="timereported" dateFormat="rfc3339")
    constant(value=" ") property(name="$myhostname")
    constant(value=" ") property(name="programname")
    constant(value=" ")
    constant(value="@cee: {")
    #SYSLOG
    constant(value="\"using_cee_relp\":\"yes\", ")
    property(name="$myhostname" format="jsonf" outname="host") constant(value=", ")
    property(name="syslogtag" format="jsonf" outname="tag") constant(value=", ")
    property(name="programname" format="jsonf" outname="prog") constant(value=", ")
    property(name="syslogfacility-text" format="jsonf" outname="facility") constant(value=", ")
    property(name="syslogpriority-text" format="jsonf" outname="priority") constant(value=", ")
    property(name="timegenerated" dateFormat="rfc3339" format="jsonf" outname="syslog_timestamp") constant(value=", ")
    ##ES TIMESTAMP
    constant(value="\"es_timestamp\":\"")
    property(name="timereported" dateFormat="unixtimestamp")
    constant(value="000\", ")
    #REST
    property(name="$!all-json" position.from="2")
}
```

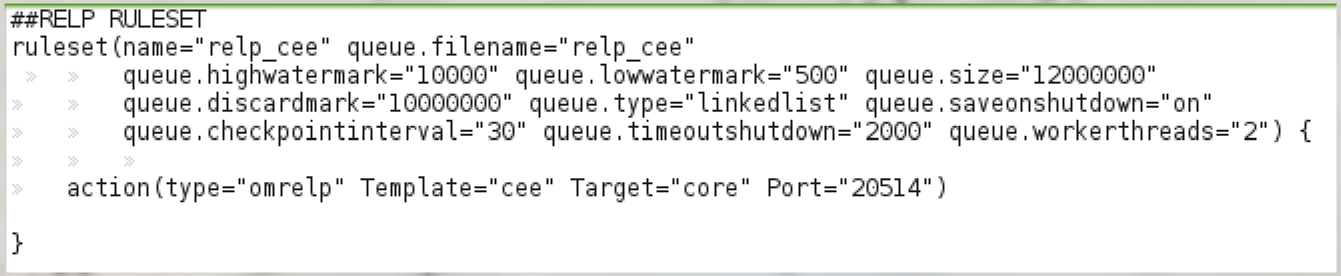
- CEE (LumberJack) JSON messages
- “timestamp” field in ES format (us)

Rsyslog event transport

Rulesets & actions



```
if $hostname == $$myhostname and $programname == 'kernel' and $msg contains 'SFW2' then {
    action(type="mmnormalize" useRawMsg="on" ruleBase="/etc/rsyslog.d/_rules/kernel-firewall")

    if ( strlen($!unparsed-data) <1) then {
        set $!msg_class ="net";
        set $!msg_view = "firewall";

        call roger & stop
    }
}
```



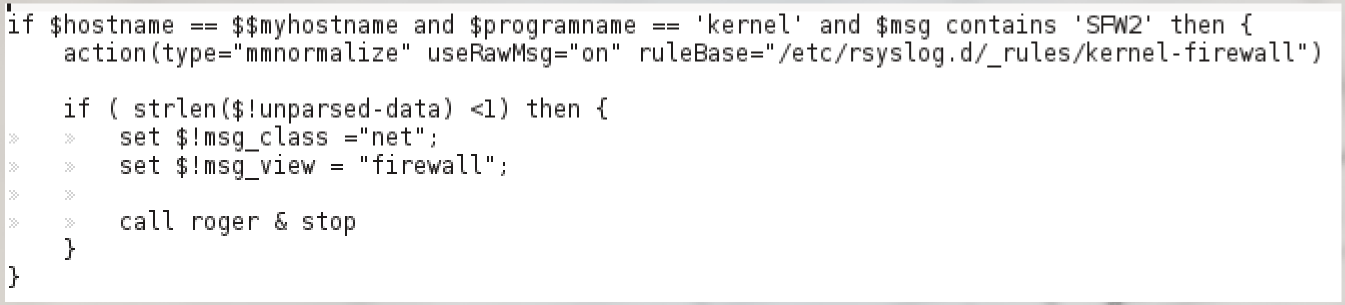
```
##RELP RULESET
ruleset(name="relp_cee" queue.filename="relp_cee"
        queue.highwatermark="10000" queue.lowwatermark="500" queue.size="12000000"
        queue.discardmark="10000000" queue.type="linkedlist" queue.saveonshutdown="on"
        queue.checkpointinterval="30" queue.timeoutshutdown="2000" queue.workerthreads="2") {

    action(type="omrelp" Template="cee" Target="core" Port="20514")

}
```

All logs must been tokenized:

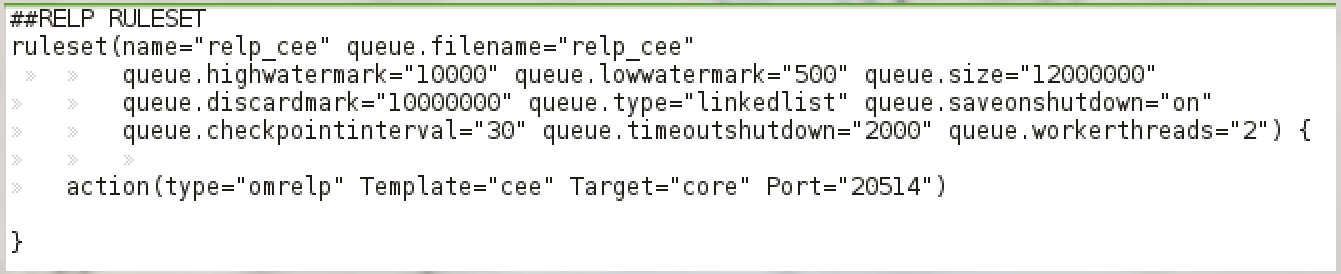
- Before Rsyslog (in application)
- Using Rsyslog (mmnormalize)

Rsyslog event transport

Rulesets & actions



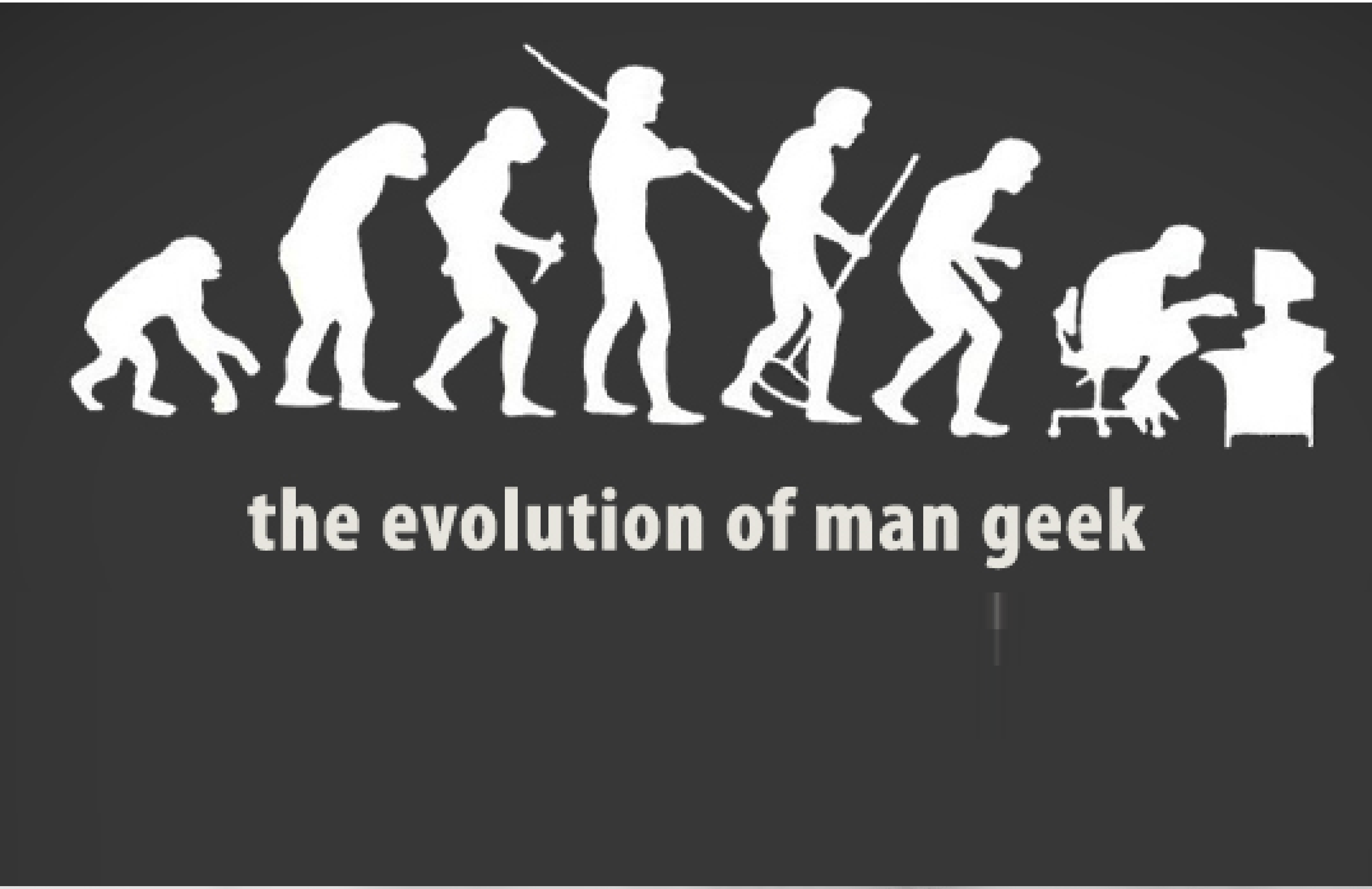
```
if $hostname == $$myhostname and $programname == 'kernel' and $msg contains 'SFW2' then {
    action(type="mmnormalize" useRawMsg="on" ruleBase="/etc/rsyslog.d/_rules/kernel-firewall")

    if ( strlen($!unparsed-data) <1) then {
»   »   set $!msg_class ="net";
»   »   set $!msg_view = "firewall";
»   »
»   »   call roger & stop
    }
}
```



```
##RELP RULESET
ruleset(name="relp_cee" queue.filename="relp_cee"
 »  »   queue.highwatermark="10000" queue.lowwatermark="500" queue.size="12000000"
»   »   queue.discardmark="10000000" queue.type="linkedlist" queue.saveonshutdown="on"
»   »   queue.checkpointinterval="30" queue.timeoutshutdown="2000" queue.workerthreads="2") {
»   »   »
»   action(type="omrelp" Template="cee" Target="core" Port="20514")

}
```

- Every ruleset have own queue
- Queues are disk-backed (watermark-based)
- Shutdowns and restarts are safe

“Talk is cheap. Show me the code.”



TOC

Metrics in monitoring and logging

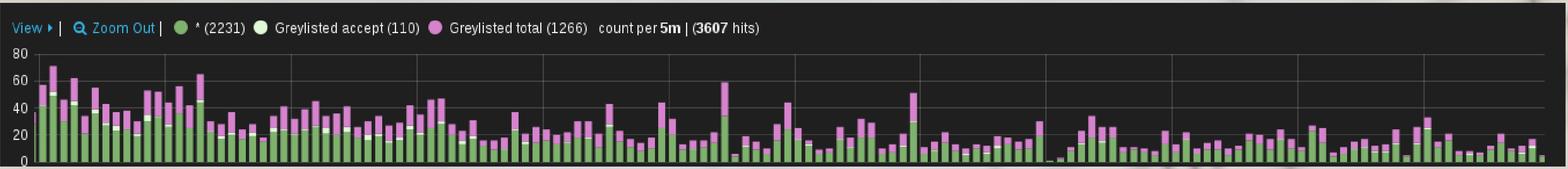
By log-driven monitoring – to dataflow -driven services.

Rsyslog event transport

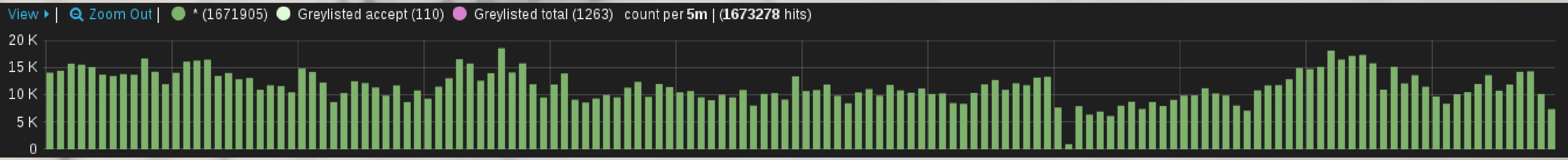
Let's try. Live test case

Let's try. Live test case

<ins>Application</ins> – MTA + spamfilter, scope-12h



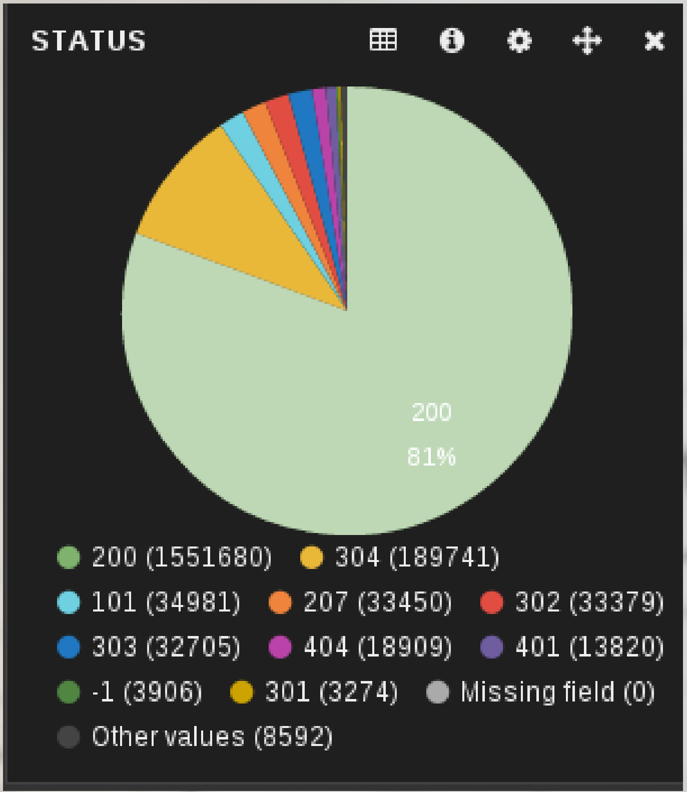
Show accepted mails, 2.2Km, time to retrieve – 92 ms



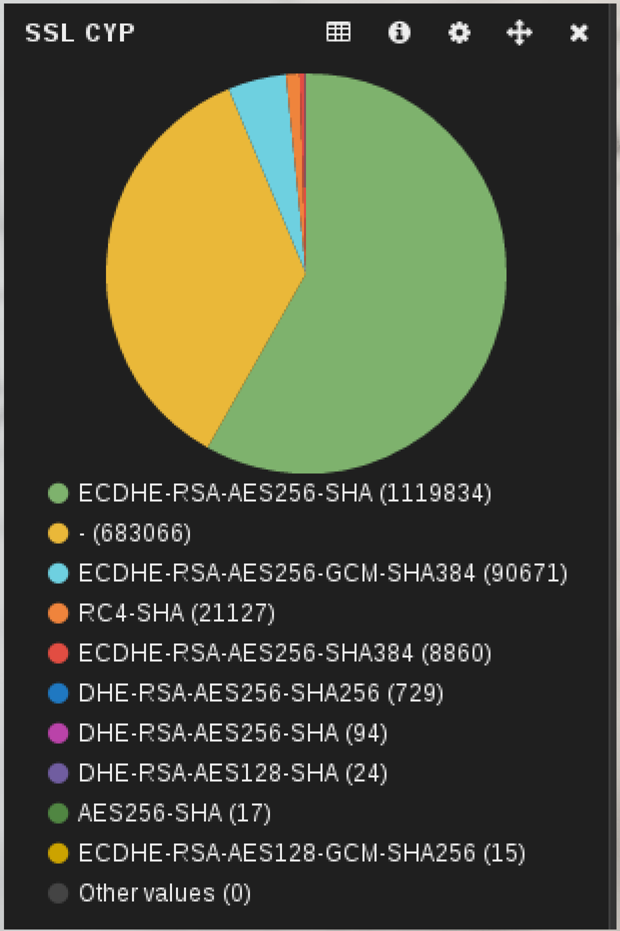
Show all msg, ~1.7Mm, time to retrieve – 400 ms

Let's try. Live test case

Application – HTTP(S) gate, scope-12h (08:00-18:00)



● 200 (1551680) ● 304 (189741)
● 101 (34981) ● 207 (33450) ● 302 (33379)
● 303 (32705) ● 404 (18909) ● 401 (13820)
● -1 (3906) ● 301 (3274) ● Missing field (0)
● Other values (8592)



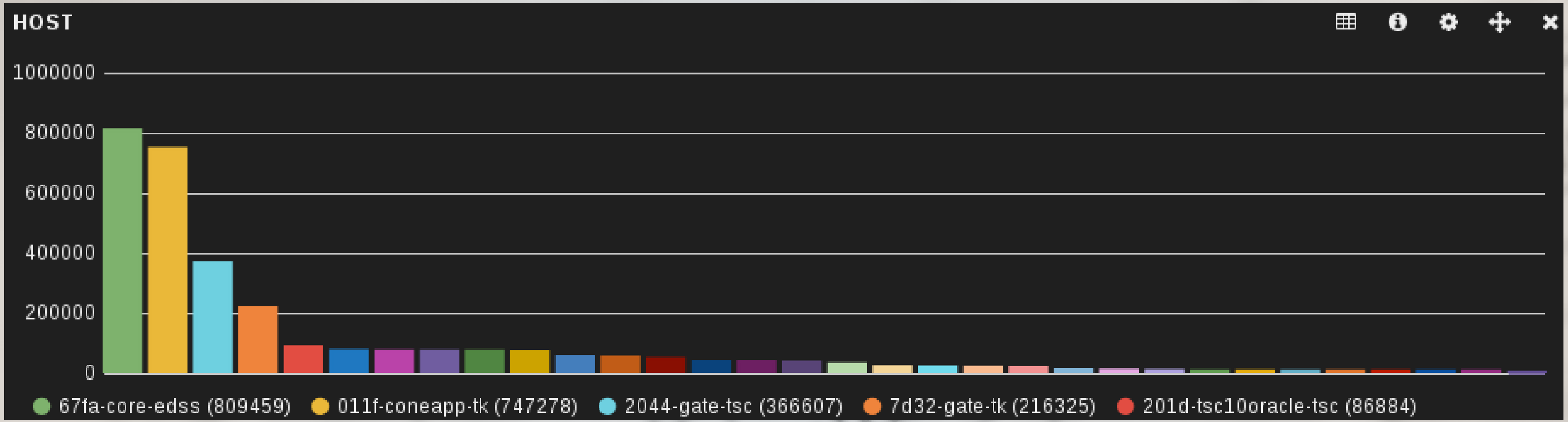
● ECDHE-RSA-AES256-SHA (1119834)
● - (683066)
● ECDHE-RSA-AES256-GCM-SHA384 (90671)
● RC4-SHA (21127)
● ECDHE-RSA-AES256-SHA384 (8860)
● DHE-RSA-AES256-SHA256 (729)
● DHE-RSA-AES256-SHA (94)
● DHE-RSA-AES128-SHA (24)
● AES256-SHA (17)
● ECDHE-RSA-AES128-GCM-SHA256 (15)
● Other values (0)

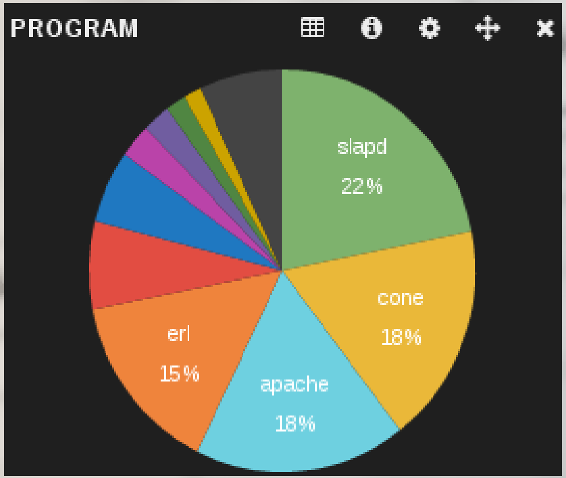
Show all HTTPS traffic per hour

- ~1.9Mm,
- time to retrieve – 210 ms

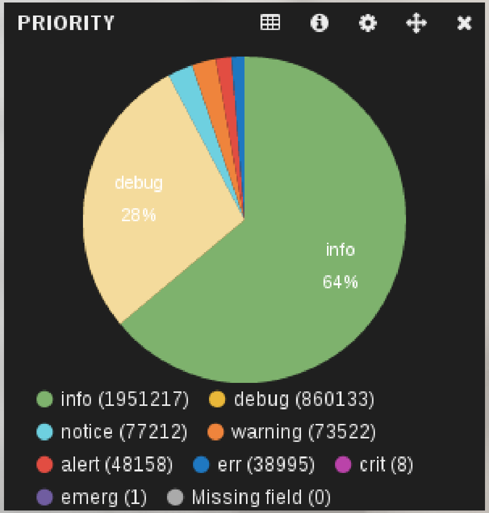
Let's try. Live test case

Application – All app-specific logs (no per-field tokenizing)





- ~4Mm,
- time to retrieve
  - 8 s



Thanks!

Mail your CV:

info@cone.ee

“Talk is cheap. Show me the code.” L.Torvalds

ZABBIX 2014 Conference

Eugene Istomin

IT Architect

e.istomin@edss.ee

Cone Center,Tallinn