Logfile monitoring

Lukasz Lipski
IT Infrastructure Specialist, Nordea IT Polska sp. z o.o.

NORDEA IT POLSKA

- IT support for our Polish, Latvian, Lithuanian and Estonian branches
- core banking, e-banking, backoffice, and in-house development
- large, complex IT infrastructure under constant monitoring

ZABBIX AT NORDEA

- 350 monitored hosts
- 45000 monitored items
- 18000 triggers

MONITORING COMPLEXITY

- ZABBIX
- SCOM
- DynaTrace
- Oracle EM
- many others...

LOGFILE MONITORING

THE POSSIBILITIES

- agent keeps track of the point where it stopped last time
- agent does not assume any particular log file rotation scheme
  (keeps track of file modification time)
- agent can filter entries of the log file by the content regexp
- agent can extract desired values from matched lines (2.2)

...CONTINUED

It's easy to underestimate the possibilities
that come out of the box.

It's good to look at the docs, once in a while:

`/2.4/manual/config/items/itemtypes/log_items`

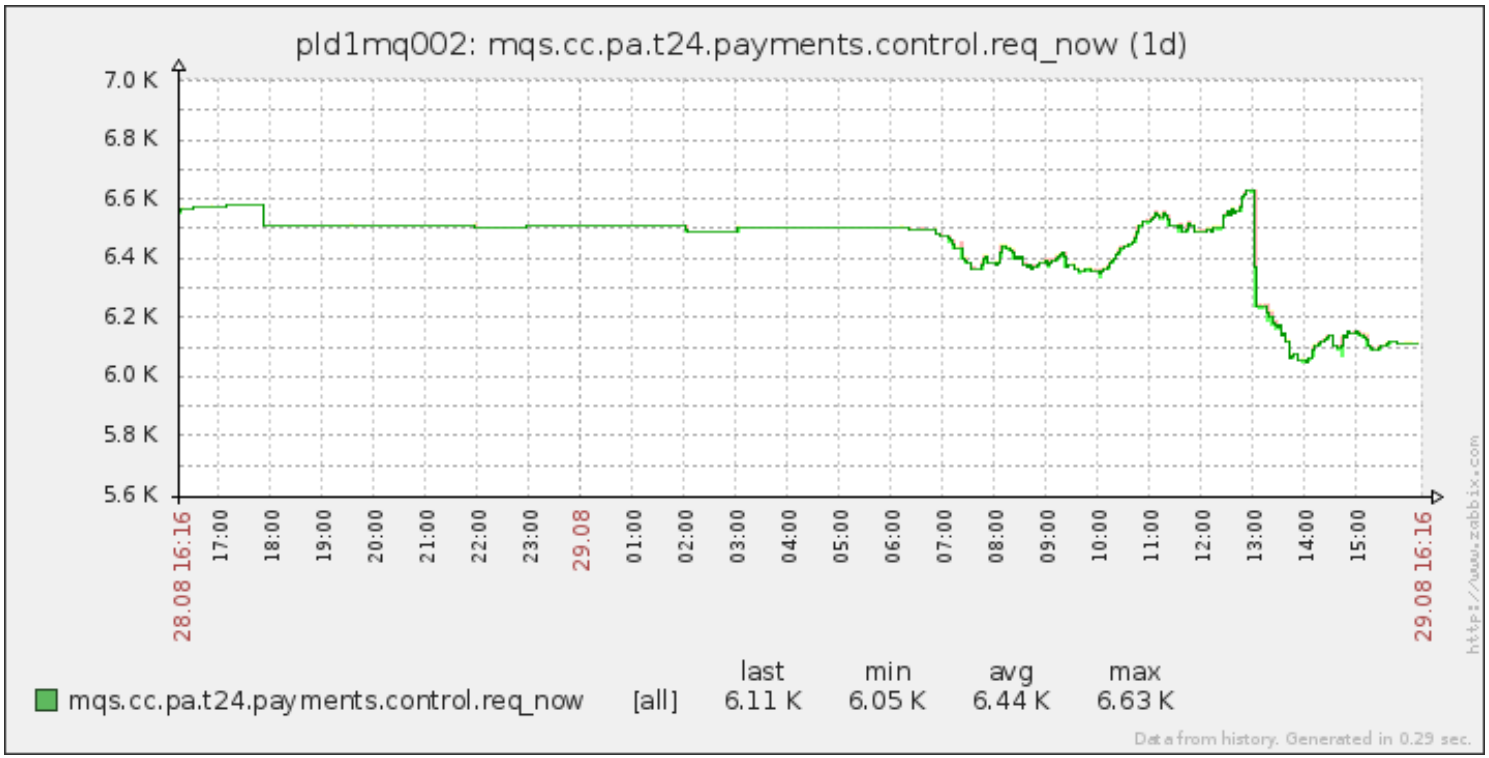
GRAPHING LOG VALUES

OVERVIEW

- since 2.2, you can grab a numeric value from a log line
- it still is a text value
- you want to graph it

SOLUTION

- create a calculated item based on the value from the log file
- now, it just works


pld1mq002: mqs.cc.pa.t24.payments.control.req_now (1d)
7.0 K
6.8 K
6.6 K
6.4 K
6.2 K
6.0 K
5.8 K
5.6 K
28.08 16:16
17:00
18:00
19:00
20:00
21:00
22:00
23:00
29.08
01:00
02:00
03:00
04:00
05:00
06:00
07:00
08:00
09:00
10:00
11:00
12:00
13:00
14:00
15:00
29.08 16:16
last
min
avg
max
mqs.cc.pa.t24.payments.control.req_now
[all]
6.11 K
6.05 K
6.44 K
6.63 K
Data from history. Generated in 0.29 sec.

CALCULATED ITEMS

It's not the only way in which calculated items can support logfile monitoring.

Another useful example would be counting occurences of a specific type within the logfile (like errors within a specified timeframe).

VIRTUAL LOGFILES

OVERVIEW

- a simple way to monitor existing script based solutions
- a single item per host, serving as a trap for sent messages
- basically, a virtual logfile within Zabbix

LOGGING SCRIPT – PART 1

```
log2zbx.pl --error --msg "[CR_3] Loading failed"
```

```
#!/usr/local/bin/perl
use warnings;
use strict;

use Getopt::Long qw(:config no_auto_abbrev);

sub get_hostname {
  # return hostname gathered from /etc/zabbix/zabbix_agentd.conf
}

sub send_message {
  # send a text value to a given Zabbix host / item
  # via Zabbix API
  # use Zabbix::API, write your own, or wrap zabbix sender
}
```

LOGGING SCRIPT – PART 2

```
my $zbx_server =  '127.0.0.1';
my $log_item_key = 'host_log';

my %opt;
GetOptions(
    'error|err|e!'      => \$opt{'error'},
    'warning|warn|w!'   => \$opt{'warning'},
    'info|i!'           => \$opt{'info'},
    'message|msg|m=s'   => \$opt{'msg'},
) or pod2usage() && exit;

pod2usage(-message => "No message specified.") && exit
    unless defined $opt{'msg'};

my $hostname = get_hostname();

my $message = '[INFO] '.$opt{'msg'}; # default level

if (defined $opt{'warning'}) { $message = '[WARN] '.$opt{'msg'}; }
if (defined $opt{'error'})   { $message = '[ERROR] '.$opt{'msg'};}

log_message($zbx_server, $hostname, $log_item_key, $message);
```

KEY BENEFITS

- lightweight approach to add zabbix monitoring to existing solutions
- works as a drop-in replacement for „send mail to admin” lines in many shell scripts
- default actions on the virtual log item can be put in place, so no further work is needed

Any questions?

Thank you!