Elastic Platform Technical Deep-Dive

May 27, 2015

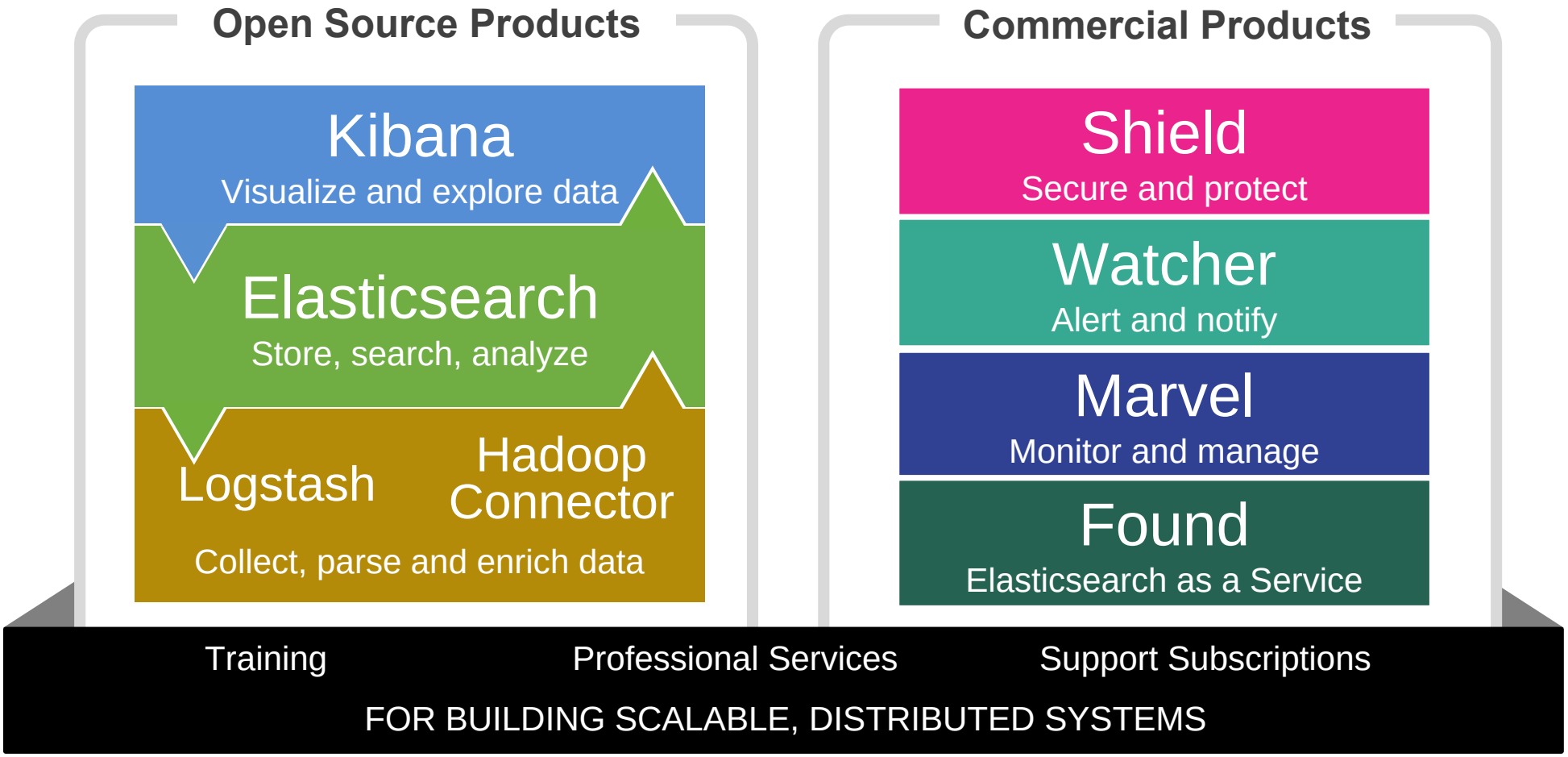
Alan Hardy
Solutions Architect

Pere Urbon-Bayes
Software Engineer

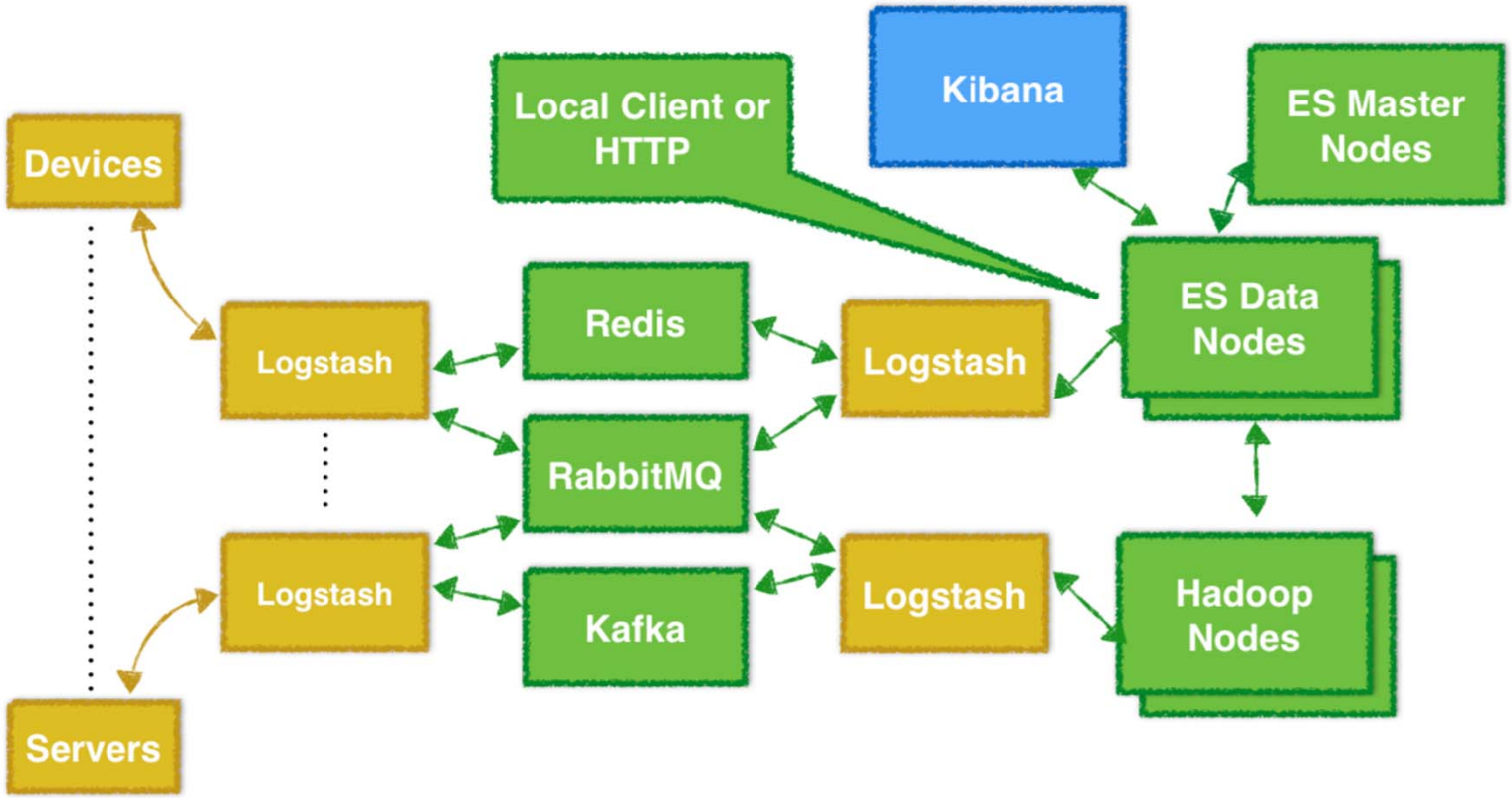
Agenda

- Elastic Platform
- Deployment Architecture
- Logstash Deep-Dive
- Elasticsearch Deep-Dive
- Kibana Deep-Dive & Demo
- Real-World Use Cases
- Q&A

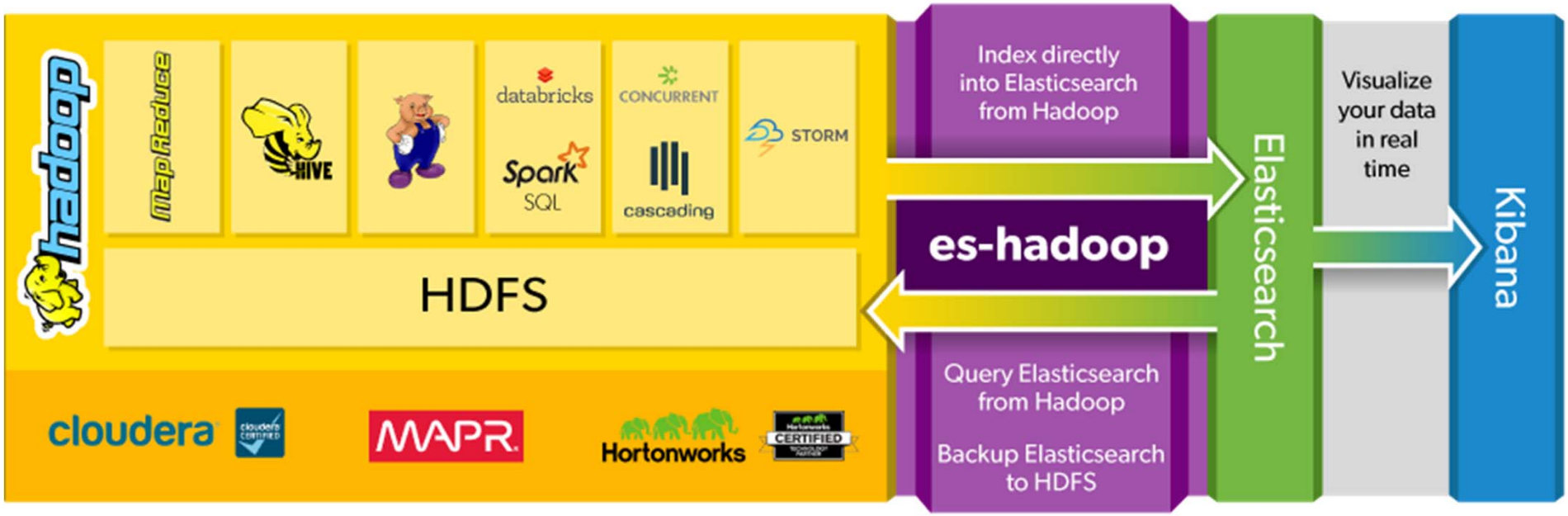
The Elastic Platform



Architecture: Logging



Architecture: Elasticsearch Hadoop ecosystem



Logstash Deep-Dive

Pere Urbon-Bayes

Software Engineer

Logstash - The shipper with a moustache

Being on call

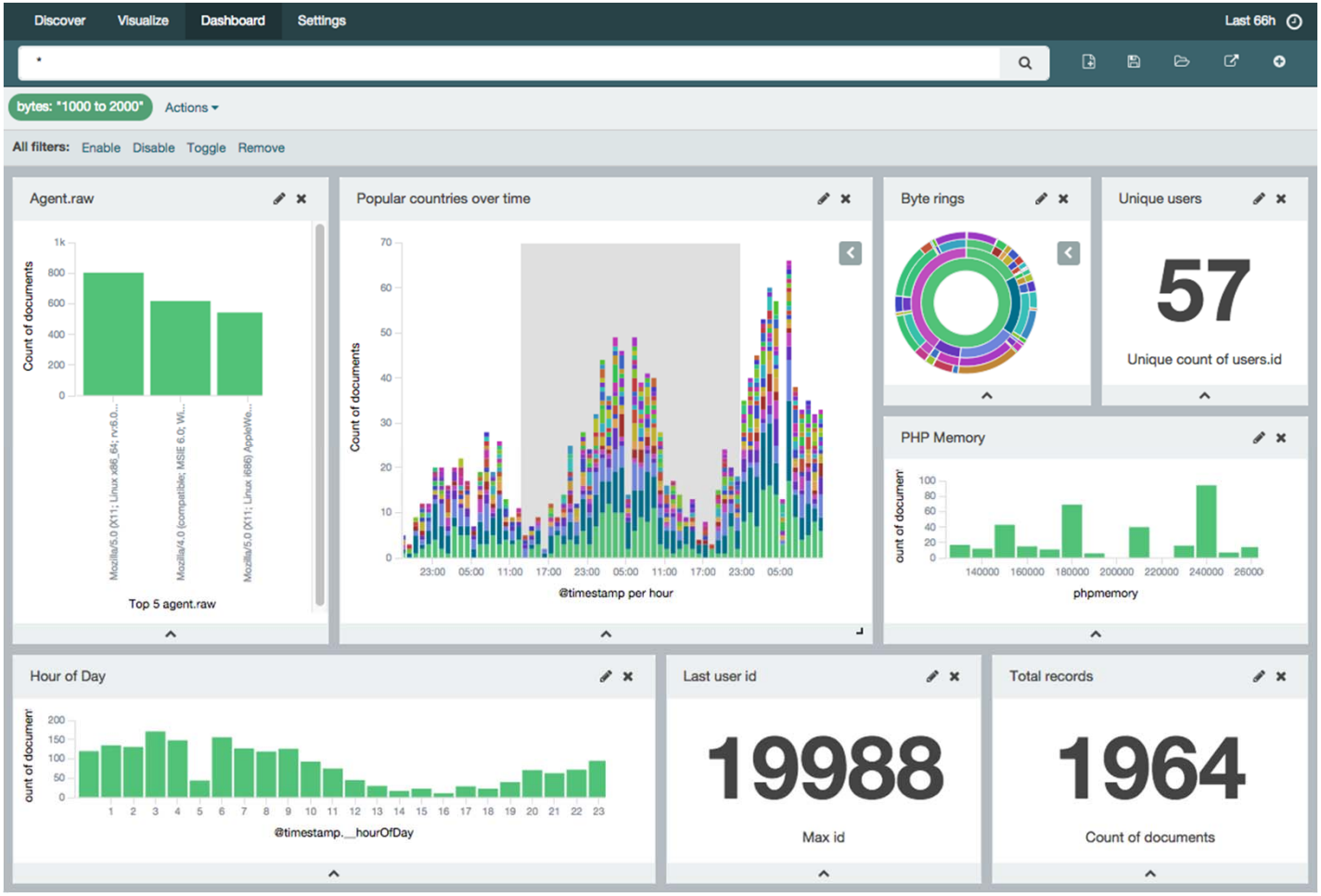
Debugging logs

```
50.180.79.170 - - [09/Nov/2014:23:31:37 +0000] "GET /favicon.ico HTTP/1.1" 200 3638 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.5; rv:16.0) Gecko/20100101 Firefox/16.0"
208.115.111.72 - - [09/Nov/2014:23:31:37 +0000] "GET /blog/tags/subversion HTTP/1.1" 200 12557 "-" "Mozilla/5.0 (compatible; Ezooms/1.0; help@moz.com)"
208.115.111.72 - - [09/Nov/2014:23:31:38 +0000] "GET /blog/web/194.html HTTP/1.1" 200 8251 "-" "Mozilla/5.0 (compatible; Ezooms/1.0; help@moz.com)"
208.115.111.72 - - [09/Nov/2014:23:31:40 +0000] "GET /files/blogposts/20070901/?C=D;O=A HTTP/1.1" 200 980 "-" "Mozilla/5.0 (compatible; Ezooms/1.0; help@moz.com)"
208.115.111.72 - - [09/Nov/2014:23:31:41 +0000] "GET /files/blogposts/20080109/boost_xpressive_test.cpp HTTP/1.1" 200 1533 "-" "Mozilla/5.0 (compatible; Ezooms/1.0; help@moz.com)"
208.115.111.72 - - [09/Nov/2014:23:31:46 +0000] "GET /files/blogposts/20090520/ HTTP/1.1" 200 966 "-" "Mozilla/5.0 (compatible; Ezooms/1.0; help@moz.com)"
208.115.111.72 - - [09/Nov/2014:23:31:46 +0000] "GET /files/fastsplit/?C=M;O=D HTTP/1.1" 200 958 "-" "Mozilla/5.0 (compatible; Ezooms/1.0; help@moz.com)"
208.115.111.72 - - [09/Nov/2014:23:31:47 +0000] "GET /files/xdotool/docs/man/?C=M;O=D HTTP/1.1" 200 959 "-" "Mozilla/5.0 (compatible; Ezooms/1.0; help@moz.com)"
208.115.111.72 - - [09/Nov/2014:23:31:57 +0000] "GET /scripts/python/wrap/?C=N;O=D HTTP/1.1" 200 2631 "-" "Mozilla/5.0 (compatible; Ezooms/1.0; help@moz.com)"
208.115.111.72 - - [09/Nov/2014:23:32:00 +0000] "GET /files/images/?C=S;O=D HTTP/1.1" 200 944 "-" "Mozilla/5.0 (compatible; Ezooms/1.0; help@moz.com)"
208.115.111.72 - - [09/Nov/2014:23:32:01 +0000] "GET /files/blogposts/20080611/ HTTP/1.1" 200 1175 "-" "Mozilla/5.0 (compatible; Ezooms/1.0; help@moz.com)"
208.115.111.72 - - [09/Nov/2014:23:32:01 +0000] "GET /files/logstash/?C=D;O=D HTTP/1.1" 200 13316 "-" "Mozilla/5.0 (compatible; Ezooms/1.0; help@moz.com)"
208.115.111.72 - - [09/Nov/2014:23:32:04 +0000] "GET /presentations/hackday06/ HTTP/1.1" 200 6719 "-" "Mozilla/5.0 (compatible; Ezooms/1.0; help@moz.com)"
208.115.111.72 - - [09/Nov/2014:23:32:05 +0000] "GET /scripts/grok-py-test/ HTTP/1.1" 200 2362 "-" "Mozilla/5.0 (compatible; Ezooms/1.0; help@moz.com)"
208.115.111.72 - - [09/Nov/2014:23:32:06 +0000] "GET /?N=A&page=21 HTTP/1.1" 200 33514 "-" "Mozilla/5.0 (compatible; Ezooms/1.0; help@moz.com)"
208.115.111.72 - - [09/Nov/2014:23:32:09 +0000] "GET /blog/geekery/oniguruma-named-capture-example.html?commentlimit=0 HTTP/1.1" 200 9208 "-" "Mozilla/5.0 (compatible; Ezooms/1.0; help@moz.com)"
208.115.111.72 - - [09/Nov/2014:23:32:11 +0000] "GET /blog/geekery/ssh-key-invalid-hack.html?commentlimit=0 HTTP/1.1" 200 9335 "-" "Mozilla/5.0 (compatible; Ezooms/1.0; help@moz.com)"
208.115.111.72 - - [09/Nov/2014:23:32:12 +0000] "GET /blog/geekery/server-side-javascript.html HTTP/1.1" 200 8587 "-" "Mozilla/5.0 (compatible; Ezooms/1.0; help@moz.com)"
208.115.111.72 - - [09/Nov/2014:23:32:23 +0000] "GET /blog/geekery/yahoo-hackday-08.html HTTP/1.1" 200 9882 "-" "Mozilla/5.0 (compatible; Ezooms/1.0; help@moz.com)"
105.235.130.196 - - [09/Nov/2014:23:32:32 +0000] "GET /images/googledotcom.png HTTP/1.1" 200 65748 "-" "Dalvik/1.6.0 (Linux; U; Android 4.1.2; GT-S5282 Build/JZO54K)"
174.37.205.76 - - [09/Nov/2014:23:32:37 +0000] "GET /blog HTTP/1.1" 200 37936 "-" "Mozilla/5.0 (X11; U; Linux x86_64; en-US; rv:1.9.0.19; aggregator:Spinn3r (Spinn3r 3.1); http://spinn3r.com/robot) Gecko/2010040121 Firefox/3.0.19"
54.255.13.204 - - [09/Nov/2014:23:33:11 +0000] "GET /articles/ssh-security/ HTTP/1.1" 200 16543 "http://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&sqi=2&ved=0CCQQFjAA&url=http%3A%2F%2Fwww.semicomplete.com%2Farticles%2Fssh-security%2F&ei=vdMAU8LgLcPorQfR9oHwDQ&usg=AFQjCNHWyA_svkWgk70ovEbZidQhlAC84w&bvm=bv.61535280,d.bmk&cad=rja" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.8; rv:27.0) Gecko/20100101 Firefox/27.0"
105.235.130.196 - - [09/Nov/2014:23:33:09 +0000] "GET /blog/tags/X11 HTTP/1.1" 200 32742 "-" "Mozilla/5.0 (Linux; Android 4.1.2; GT-S5282 Build/JZO54K) AppleWebKit/537.31 (KHTML, like Gecko) Chrome/26.0.1410.58 Mobile Safari/537.31"
54.255.13.204 - - [09/Nov/2014:23:33:12 +0000] "GET /reset.css HTTP/1.1" 200 1015 "http://www.semicomplete.com/articles/ssh-security/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.8; rv:27.0) Gecko/20100101 Firefox/27.0"
54.255.13.204 - - [09/Nov/2014:23:33:12 +0000] "GET /style2.css HTTP/1.1" 200 4877 "http://www.semicomplete.com/articles/ssh-security/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.8; rv:27.0) Gecko/20100101 Firefox/27.0"
54.255.13.204 - - [09/Nov/2014:23:33:12 +0000] "GET /favicon.ico HTTP/1.1" 200 3638 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.8; rv:27.0) Gecko/20100101 Firefox/27.0"
105.235.130.196 - - [09/Nov/2014:23:33:13 +0000] "GET /reset.css HTTP/1.1" 200 1015 "http://www.semicomplete.com/blog/tags/X11" "Mozilla/5.0 (Linux; Android 4.1.2; GT-S5282 Build/JZO54K) AppleWebKit/537.31 (KHTML, like Gecko) Chrome/26.0.1410.58 Mobile Safari/537.31"
54.255.13.204 - - [09/Nov/2014:23:33:13 +0000] "GET /images/jordan-80.png HTTP/1.1" 200 6146 "http://www.semicomplete.com/articles/ssh-security/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.8; rv:27.0) Gecko/20100101 Firefox/27.0"
54.255.13.204 - - [09/Nov/2014:23:33:13 +0000] "GET /images/web/2009/banner.png HTTP/1.1" 200 52315 "http://www.semicomplete.com/style2.css" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.8; rv:27.0) Gecko/20100101 Firefox/27.0"
105.235.130.196 - - [09/Nov/2014:23:33:15 +0000] "GET /style2.css HTTP/1.1" 200 4877 "http://www.semicomplete.com/blog/tags/X11" "Mozilla/5.0 (Linux; Android 4.1.2; GT-S5282 Build/JZO54K) AppleWebKit/537.31 (KHTML, like Gecko) Chrome/26.0.1410.58 Mobile Safari/537.31"
105.235.130.196 - - [09/Nov/2014:23:33:15 +0000] "GET /images/jordan-80.png HTTP/1.1" 200 6146 "http://www.semicomplete.com/blog/tags/X11" "Mozilla/5.0 (Linux; Android 4.1.2; GT-S5282 Build/JZO54K) AppleWebKit/537.31 (KHTML, like Gecko) Chrome/26.0.1410.58 Mobile Safari/537.31"
105.235.130.196 - - [09/Nov/2014:23:33:19 +0000] "GET /images/web/2009/banner.png HTTP/1.1" 200 52315 "http://www.semicomplete.com/blog/tags/X11" "Mozilla/5.0 (Linux; Android 4.1.2; GT-S5282 Build/JZO54K) AppleWebKit/537.31 (KHTML, like Gecko) Chrome/26.0.1410.58 Mobile Safari/537.31"
134.76.249.10 - - [09/Nov/2014:23:33:24 +0000] "GET /projects/xdotool/ HTTP/1.1" 200 12292 "http://www.google.de/url?sa=t&rct=j&q=&esrc=s&source=web&cd=3&ved=0CDwQFjAC&url=http%3A%2F%2Fwww.semicomplete.com%2Fprojects%2Fxdotool%2F&ei=zNMAU5qaEcantAbD3YHIAQ&usg=AFQjCNE3V_aCf3-gfNcbS924S6jZ6FqffA&bvm=bv.61535280,d.Yms&cad=rja" "Mozilla/5.0 (X11; Linux x86_64; rv:26.0) Gecko/20100101 Firefox/26.0"
134.76.249.10 - - [09/Nov/2014:23:33:24 +0000] "GET /reset.css HTTP/1.1" 200 1015 "http://www.semicomplete.com/projects/xdotool/" "Mozilla/5.0 (X11; Linux x86_64; rv:26.0) Gecko/20100101 Firefox/26.0"
134.76.249.10 - - [09/Nov/2014:23:33:25 +0000] "GET /style2.css HTTP/1.1" 200 4877 "http://www.semicomplete.com/projects/xdotool/" "Mozilla/5.0 (X11; Linux x86_64; rv:26.0) Gecko/20100101 Firefox/26.0"
134.76.249.10 - - [09/Nov/2014:23:33:25 +0000] "GET /favicon.ico HTTP/1.1" 200 3638 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:26.0) Gecko/20100101 Firefox/26.0"
134.76.249.10 - - [09/Nov/2014:23:33:25 +0000] "GET /images/jordan-80.png HTTP/1.1" 200 6146 "http://www.semicomplete.com/projects/xdotool/" "Mozilla/5.0 (X11; Linux x86_64; rv:26.0) Gecko/20100101 Firefox/26.0"
134.76.249.10 - - [09/Nov/2014:23:33:25 +0000] "GET /images/web/2009/banner.png HTTP/1.1" 200 52315 "http://www.semicomplete.com/style2.css" "Mozilla/5.0 (X11; Linux x86_64; rv:26.0) Gecko/20100101 Firefox/26.0"
134.76.249.10 - - [09/Nov/2014:23:33:50 +0000] "GET /projects/xdotool HTTP/1.1" 301 339 "http://tuxradar.com/content/xdotool-script-your-mouse" "Mozilla/5.0 (X11; Linux x86_64; rv:26.0) Gecko/20100101 Firefox/26.0"
134.76.249.10 - - [09/Nov/2014:23:33:51 +0000] "GET /projects/xdotool/ HTTP/1.1" 200 12292 "http://tuxradar.com/content/xdotool-script-your-mouse" "Mozilla/5.0 (X11; Linux x86_64; rv:26.0) Gecko/20100101 Firefox/26.0"
66.249.73.135 - - [09/Nov/2014:23:34:12 +0000] "GET /?flav=atom HTTP/1.1" 200 32352 "-" "Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)"
207.241.237.220 - - [09/Nov/2014:23:34:34 +0000] "GET /blog/tags/C?page=2 HTTP/1.0" 200 16311 "http://www.semicomplete.com/blog/tags/C" "Mozilla/5.0 (compatible; archive.org_bot +http://www.archive.org/details/archive.org_bot)"
68.184.202.186 - - [09/Nov/2014:23:34:43 +0000] "GET /projects/xpathtool/ HTTP/1.1" 200 10745 "https://www.google.com/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_8_5) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.107 Safari/537.36"
68.184.202.186 - - [09/Nov/2014:23:34:44 +0000] "GET /reset.css HTTP/1.1" 200 1015 "http://www.semicomplete.com/projects/xpathtool/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_8_5) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.107 Safari/537.36"
68.184.202.186 - - [09/Nov/2014:23:34:44 +0000] "GET /images/jordan-80.png HTTP/1.1" 200 6146 "http://www.semicomplete.com/projects/xpathtool/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_8_5) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.107 Safari/537.36"
68.184.202.186 - - [09/Nov/2014:23:34:44 +0000] "GET /style2.css HTTP/1.1" 200 4877 "http://www.semicomplete.com/projects/xpathtool/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_8_5) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.107 Safari/537.36"
68.184.202.186 - - [09/Nov/2014:23:34:44 +0000] "GET /images/web/2009/banner.png HTTP/1.1" 200 52315 "http://www.semicomplete.com/projects/xpathtool/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_8_5) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.107 Safari/537.36"
68.184.202.186 - - [09/Nov/2014:23:34:44 +0000] "GET /favicon.ico HTTP/1.1" 200 3638 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_8_5) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.107 Safari/537.36"
46.105.14.53 - - [09/Nov/2014:23:36:19 +0000] "GET /blog/tags/puppet?flav=rss20 HTTP/1.1" 200 14872 "-" "UniversalFeedParser/4.2-pre-314-svn +http://feedparser.org/"
66.249.73.135 - - [09/Nov/2014:23:36:23 +0000] "GET /?flav=rss20 HTTP/1.1" 200 29941 "-" "Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)"
24.233.162.179 - - [09/Nov/2014:23:36:31 +0000] "GET /favicon.ico HTTP/1.1" 200 3638 "-" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:25.0) Gecko/20100101 Firefox/25.0"
123.125.71.117 - - [09/Nov/2014:23:37:37 +0000] "GET / HTTP/1.1" 200 36824 "-" "Mozilla/5.0 (compatible; Baiduspider/2.0; +http://www.baidu.com/search/spider.html)"
220.181.108.153 - - [09/Nov/2014:23:38:18 +0000] "GET / HTTP/1.1" 200 36824 "-" "Mozilla/5.0 (compatible; Baiduspider/2.0; +http://www.baidu.com/search/spider.html)"
65.19.138.34 - - [09/Nov/2014:23:39:56 +0000] "GET / HTTP/1.1" 200 37932 "-" "Feedly/1.0 (+http://www.feedly.com/fetcher.html; like FeedFetcher-Google)"
66.249.73.135 - - [09/Nov/2014:23:40:09 +0000] "GET /blog/geekery/rhapsody-on-linux.html HTTP/1.1" 200 9109 "-" "Mozilla/5.0 (iPhone; CPU iPhone OS 6_0 like Mac OS X) AppleWebKit/536.26 (KHTML, like Gecko) Version/6.0 Mobile/10A5376e Safari/8536.25 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)"
97.116.185.190 - - [09/Nov/2014:23:40:50 +0000] "GET /articles/dynamic-dns-with-dhcp/ HTTP/1.1" 200 18848 "http://ubuntuforums.org/showthread.php?t=2003644" "Mozilla/5.0 (Windows NT 5.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.107 Safari/537.36"
97.116.185.190 - - [09/Nov/2014:23:40:50 +0000] "GET /reset.css HTTP/1.1" 200 1015 "http://www.semicomplete.com/articles/dynamic-dns-with-dhcp/" "Mozilla/5.0 (Windows NT 5.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.107 Safari/537.36"
97.116.185.190 - - [09/Nov/2014:23:40:50 +0000] "GET /style2.css HTTP/1.1" 200 4877 "http://www.semicomplete.com/articles/dynamic-dns-with-dhcp/" "Mozilla/5.0 (Windows NT 5.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.107 Safari/537.36"
97.116.185.190 - - [09/Nov/2014:23:40:50 +0000] "GET /images/jordan-80.png HTTP/1.1" 200 6146 "http://www.semicomplete.com/articles/dynamic-dns-with-dhcp/" "Mozilla/5.0 (Windows NT 5.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.107 Safari/537.36"
97.116.185.190 - - [09/Nov/2014:23:40:51 +0000] "GET /images/web/2009/banner.png HTTP/1.1" 200 52315 "http://www.semicomplete.com/articles/dynamic-dns-with-dhcp/" "Mozilla/5.0 (Windows NT 5.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.107 Safari/537.36"
97.116.185.190 - - [09/Nov/2014:23:40:52 +0000] "GET /favicon.ico HTTP/1.1" 200 3638 "-" "Mozilla/5.0 (Windows NT 5.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.107 Safari/537.36"
5.255.72.168 - - [09/Nov/2014:23:41:14 +0000] "GET / HTTP/1.0" 200 37932 "http://www.semicomplete.com/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.7; rv:21.0) Gecko/20100101 Firefox/21.0"
5.255.72.168 - - [09/Nov/2014:23:41:15 +0000] "GET /blog/geekery/installing-windows-8-consumer-preview.html HTTP/1.0" 200 8948 "http://www.semicomplete.com/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.7; rv:21.0) Gecko/20100101 Firefox/21.0"
46.105.14.53 - - [09/Nov/2014:23:41:20 +0000] "GET /blog/tags/puppet?flav=rss20 HTTP/1.1" 200 14872 "-" "UniversalFeedParser/4.2-pre-314-svn +http://feedparser.org/"
5.102.173.71 - - [09/Nov/2014:23:42:00 +0000] "GET /robots.txt HTTP/1.1" 200 - "-" "Mozilla/5.0 (compatible; MojeekBot/0.6; http://www.mojeek.com/bot.html)"
5.102.173.71 - - [09/Nov/2014:23:42:01 +0000] "GET /projects/xdotool/ HTTP/1.1" 200 12292 "-" "Mozilla/5.0 (compatible; MojeekBot/0.6; http://www.mojeek.com/bot.html)"
208.91.156.11 - - [09/Nov/2014:23:42:10 +0000] "GET /files/logstash/logstash-1.3.2-monolithic.jar HTTP/1.1" 404 324 "-" "Chef Client/10.18.2 (ruby-1.9.3-p327; ohai-6.16.0; x86_64-linux; +http://opscode.com)"
66.249.73.185 - - [09/Nov/2014:23:42:13 +0000] "GET /presentations/logstash-1/ HTTP/1.1" 304 - "-" "Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)"
74.125.176.81 - - [09/Nov/2014:23:44:14 +0000] "GET /?flav=rss20 HTTP/1.1" 200 29941 "-" "FeedBurner/1.0 (http://www.FeedBurner.com)"
66.249.73.135 - - [09/Nov/2014:23:45:15 +0000] "GET /blog/geekery/xdotool-2.20110530.html HTTP/1.1" 200 11936 "-" "Mozilla/5.0 (iPhone; CPU iPhone OS 6_0 like Mac OS X) AppleWebKit/536.26 (KHTML, like Gecko) Version/6.0 Mobile/10A5376e Safari/8536.25 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)"
187.45.193.158 - - [09/Nov/2014:23:45:33 +0000] "GET /presentations/logstash-1/file/about-me/tequila-face.jpg HTTP/1.1" 200 196054 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; SV1; .NET CLR 2.0.50727; InfoPath.1)"
90.220.199.149 - - [09/Nov/2014:23:45:40 +0000] "GET /blog/geekery/puppet-manage-homedirectory-contents.html HTTP/1.1" 200 10001 "https://www.google.co.uk/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.107 Safari/537.36"
90.220.199.149 - - [09/Nov/2014:23:45:40 +0000] "GET /reset.css HTTP/1.1" 200 1015 "http://www.semicomplete.com/blog/geekery/puppet-manage-homedirectory-contents.html" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.107 Safari/537.36"
90.220.199.149 - - [09/Nov/2014:23:45:40 +0000] "GET /style2.css HTTP/1.1" 200 4877 "http://www.semicomplete.com/blog/geekery/puppet-manage-homedirectory-contents.html" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.107 Safari/537.36"
90.220.199.149 - - [09/Nov/2014:23:45:40 +0000] "GET /images/jordan-80.png HTTP/1.1" 200 6146 "http://www.semicomplete.com/blog/geekery/puppet-manage-homedirectory-contents.html" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.107 Safari/537.36"
90.220.199.149 - - [09/Nov/2014:23:45:40 +0000] "GET /images/web/2009/banner.png HTTP/1.1" 200 52315 "http://www.semicomplete.com/blog/geekery/puppet-manage-homedirectory-contents.html" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.107 Safari/537.36"
90.220.199.149 - - [09/Nov/2014:23:45:41 +0000] "GET /favicon.ico HTTP/1.1" 200 3638 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.107 Safari/537.36"
36.38.8.174 - - [09/Nov/2014:23:45:50 +0000] "GET /blog/geekery/ssl-latency.html HTTP/1.1" 200 17147 "https://www.google.co.kr/" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.107 Safari/537.36"
36.38.8.174 - - [09/Nov/2014:23:45:51 +0000] "GET /reset.css HTTP/1.1" 200 1015 "http://www.semicomplete.com/blog/geekery/ssl-latency.html" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.107 Safari/537.36"
36.38.8.174 - - [09/Nov/2014:23:45:51 +0000] "GET /style2.css HTTP/1.1" 200 4877 "http://www.semicomplete.com/blog/geekery/ssl-latency.html" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.107 Safari/537.36"
36.38.8.174 - - [09/Nov/2014:23:45:51 +0000] "GET /images/jordan-80.png HTTP/1.1" 200 6146 "http://www.semicomplete.com/blog/geekery/ssl-latency.html" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.107 Safari/537.36"
36.38.8.174 - - [09/Nov/2014:23:45:53 +0000] "GET /images/web/2009/banner.png HTTP/1.1" 200 52315 "http://www.semicomplete.com/blog/geekery/ssl-latency.html" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.107 Safari/537.36"
36.38.8.174 - - [09/Nov/2014:23:45:56 +0000] "GET /favicon.ico HTTP/1.1" 200 3638 "-" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.107 Safari/537.36"
71.207.12.53 - - [09/Nov/2014:23:46:04 +0000] "GET /favicon.ico HTTP/1.0" 200 3638 "-" "Safari/9537.73.11 CFNetwork/673.0.3 Darwin/13.0.0 (x86_64) (MacBookPro8%2C1)"
220.241.45.142 - - [09/Nov/2014:23:46:05 +0000] "GET /robots.txt HTTP/1.0" 200 - "-" "Mozilla/5.0 (compatible; MJ12bot/v1.4.4; http://www.majestic12.co.uk/bot.php?+)"
220.241.45.142 - - [09/Nov/2014:23:46:06 +0000] "GET /projects/firefox-tabsearch/ HTTP/1.0" 200 9661 "-" "Mozilla/5.0 (compatible; MJ12bot/v1.4.4; http://www.majestic12.co.uk/bot.php?+)"
209.85.238.199 - - [09/Nov/2014:23:46:17 +0000] "GET /?flav=atom HTTP/1.1" 200 32352 "-" "Feedfetcher-Google; (+http://www.google.com/feedfetcher.html; 16 subscribers; feed-id=3389821348893992437)"
46.105.14.53 - - [09/Nov/2014:23:46:17 +0000] "GET /blog/tags/puppet?flav=rss20 HTTP/1.1" 200 14872 "-" "UniversalFeedParser/4.2-pre-314-svn +http://feedparser.org/"
66.249.73.135 - - [09/Nov/2014:23:46:32 +0000] "GET /blog/tags/noise HTTP/1.1" 200 8985 "-" "Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)"
```

Managing Logs

Logs need to be delivered and stored somewhere,
so we can analyse them easily.

Understanding logs

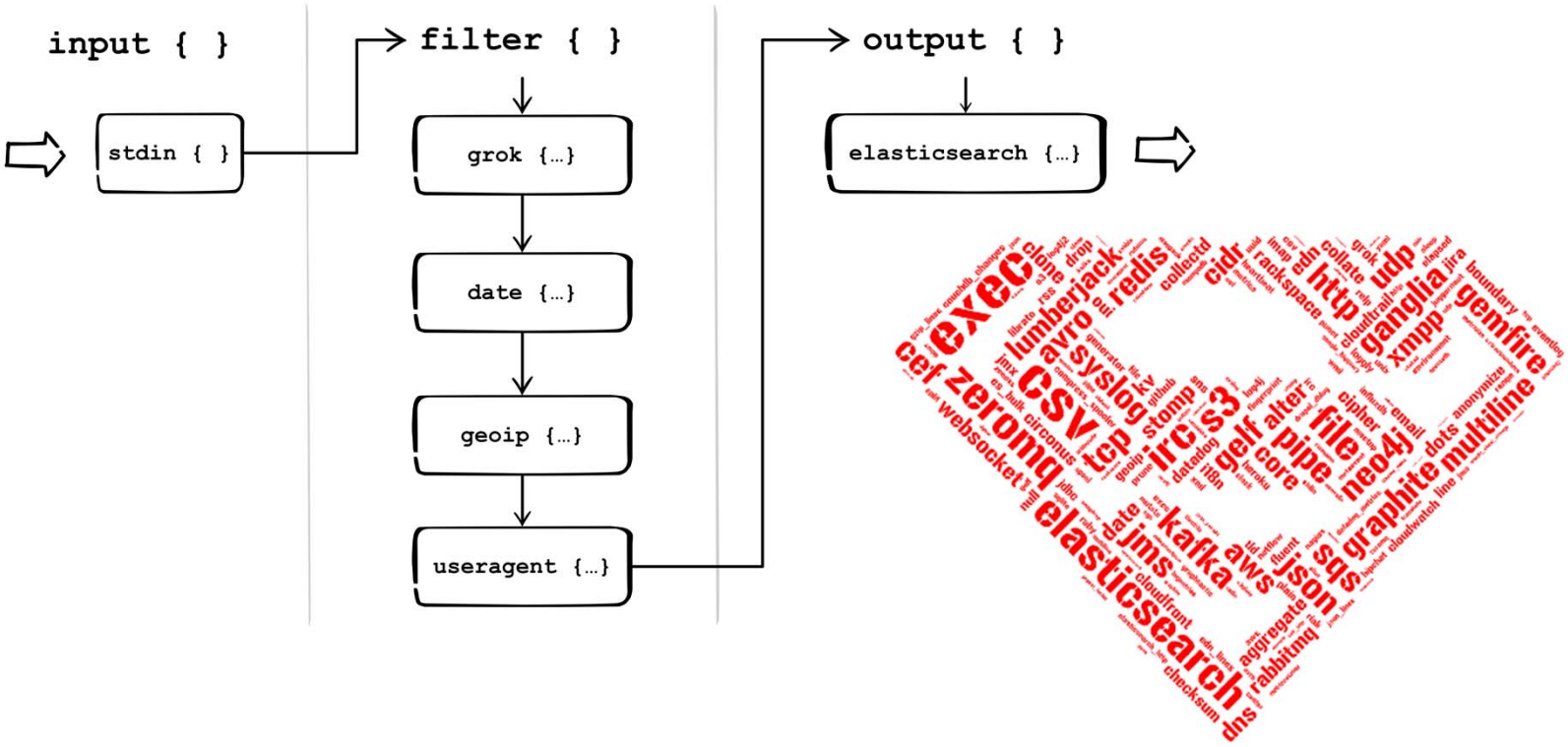


All about Logstash

What logstash can do for you….

- Receiving your events/log data
- Processing and normalising them
- Transporting them to a final destination

How Logstash works



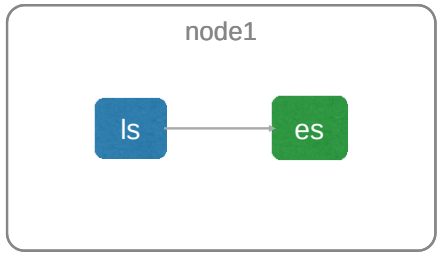
How to configure Logstash

```
input { stdin {} }

filter {
  grok {
    match => {
      "message" => "%{HTTPDATE:timestamp} %{IP:ip} <%{DATA:msg}>"
    }
  }
}

output {
  stdout {
    codec => rubydebug
  }
}
```

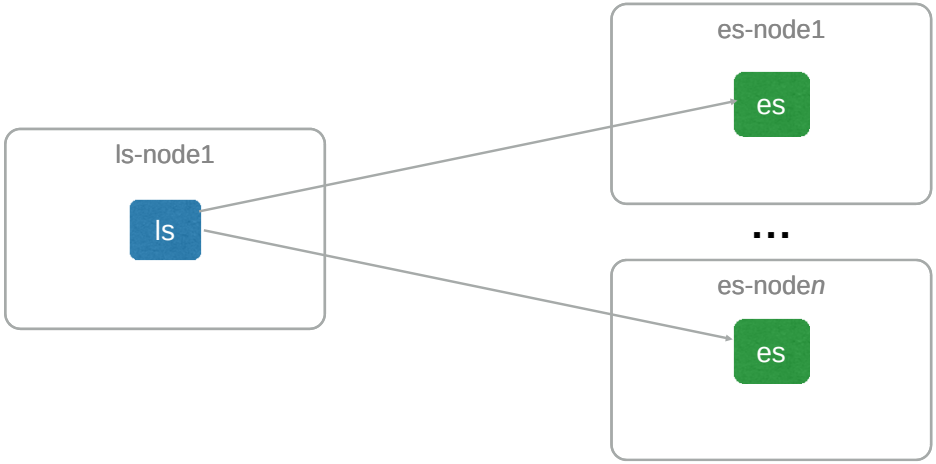
```
output {
  if [action] == “alert” {
    pagerdutty {}
  }
}
```

Logstash at scale

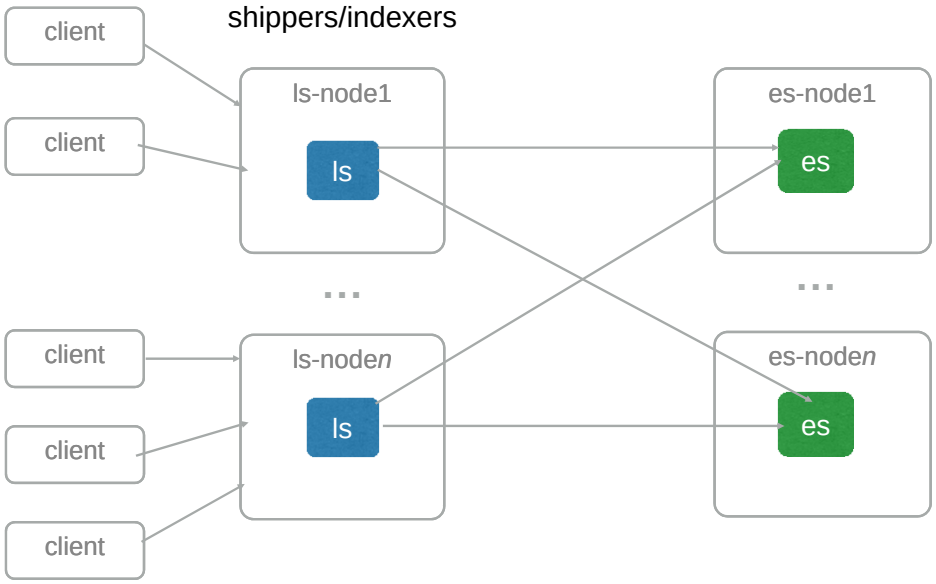
The one node experience



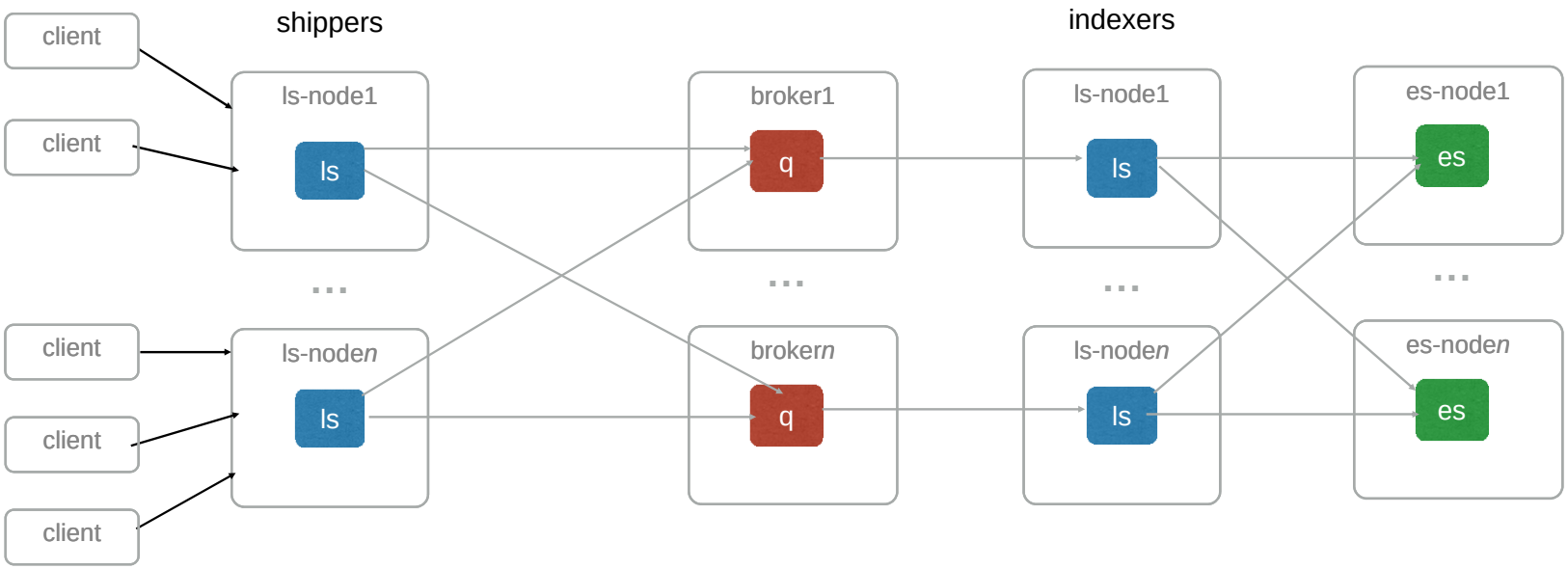
A single LS node



Multiple LS instances



Message Brokers



Baby steps on scaling

In Logstash land: *Redis*

```
input {
    redis {
        name => “default”
        host => “127.0.0.1”
        port => 6379
        db => 0
        timeout => 5
        password => “”
        queue => “”
        key => “”
        data_type => “["list", "channel", ”pattern_channel"]"
        batch_count => “”
    }
}
```

```
# The `name` configuration is used for logging
# The hostname of your Redis server
# The port to connect on.
# The Redis database number.
# Initial connection timeout in seconds.
# Password to authenticate with.
# The name of the Redis queue  (deprecated)
# The name of a Redis list or channel.
```

There is an output counterpart with similar configuration options

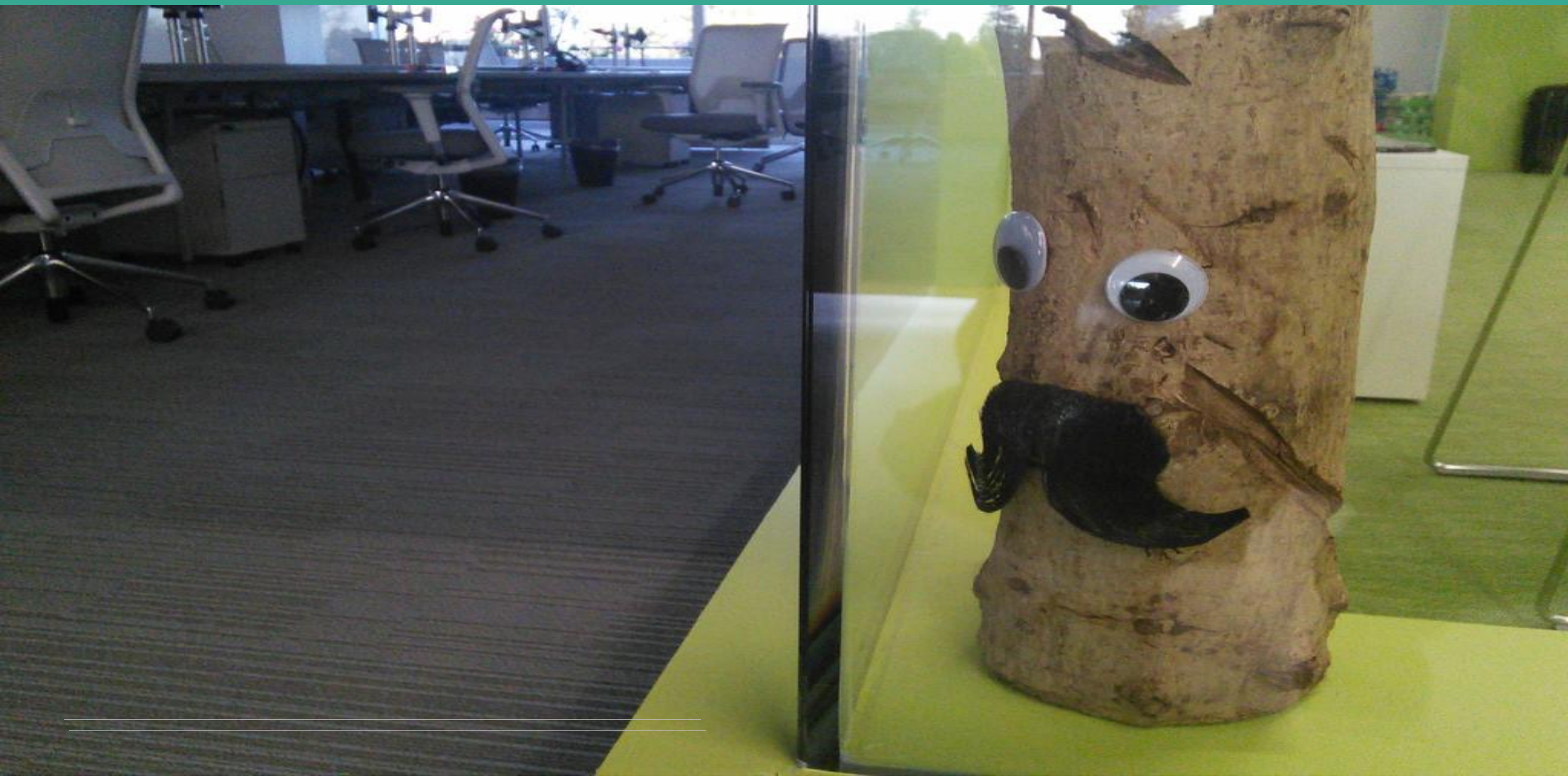
Viva la resistance: *A more resilience way of scaling*

In Logstash Land: *RabbitMQ*

```
input {
    rabbitmq {
        host => “”                  # RabbitMQ server address
        port => 5672                # RabbitMQ port to connect on
        user => “guest"             # RabbitMQ username
        password => “guest"         # RabbitMQ password
        vhost => “/”                # The vhost to use.
        ssl => false                # Enable or disable SSL
        verify_ssl => false         # Validate SSL certificate
        debug => false              # Enable or disable logging (deprecated)
    }
}
```

There is an output counterpart with similar configuration options

Logstash in the wild



Logstash vs Fluentd vs Flume

	Logstash	Fluentd	Flume
#plugins	180+	440+	25+
Predefined parsing formats	Yes	Yes	No
Variable Buffering	Not yet	Yes	Yes
Persistent queues	Not yet	Yes	Yes
Recipes	Yes	Yes	Not for NG
Configuration reloading	Not yet	Yes	Yes
Conditionals in config	Yes	No	No
Event enrichment	Yes	Yes	No

Logstash vs Fluentd vs Flume

	Logstash	Fluentd	Flume
Monitoring API	Not yet	Yes	No
JMX integration	Partially	No	Yes
Custom reporting	No	No	Yes
Hadoop integration	No	Partially	Yes
OOB Elasticsearch integration	Yes	No	No
RDBMS integration	Partially (Input)	Partially	Partially (Channel)
Lighweitght shipper	Yes	No (himself)	No (himself)

Elasticsearch Deep-Dive

Alan Hardy

Solutions Architect

Elasticsearch

Store, Search and Analyze

Distributed, scalable, and resilient

Designed for scale-out; high availability

Developer friendly

API-first; schemaless, native JSON, client libraries for any language

Real-time Search & Analytics

Real-time aggregations, geospatial, full-text search; query structured and unstructured data

Terminology

“node”

running instance of elasticsearch

≈ one server

Terminology

“shard”

holds just a a slice of the data

physical worker unit

lives on one node

(a full Lucene search engine)

Terminology

“index”

logical namespace

points to one or more shards

```
shard = hash(_id) % no_of_shards
```

Terminology

many segments → one shard

many shards → one index

scale out, not up

Create an Index

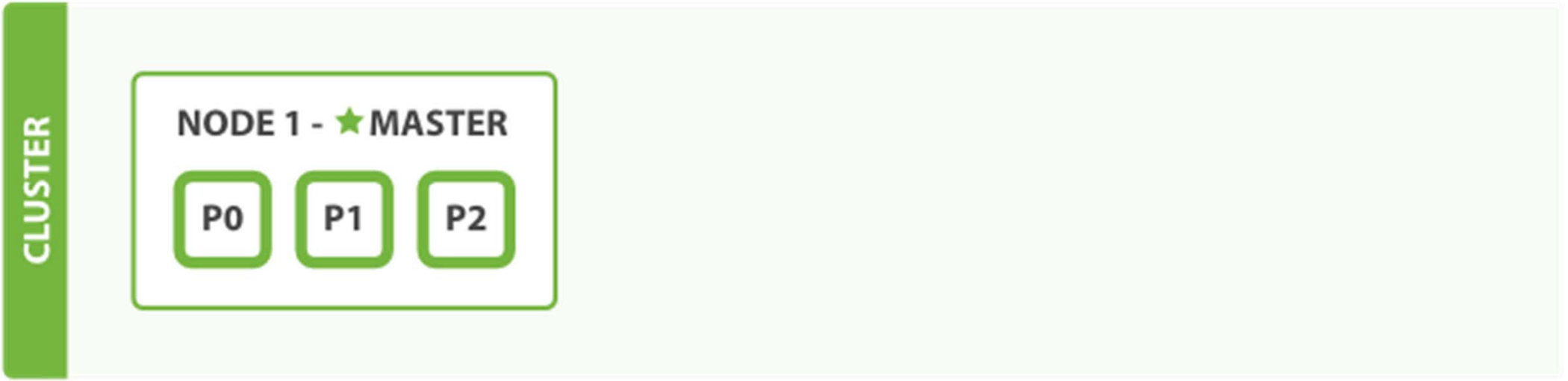
To add data we need an **index** (one or more shards)

A shard can be either a **primary** shard or a **replica** shard

A document belongs to a single **primary** shard

```
curl -XPUT 'http://localhost:9200/logs
{
  "settings" : {
    "number_of_shards" : 3,
    "number_of_replicas" : 1
  }
}
```

Single node cluster



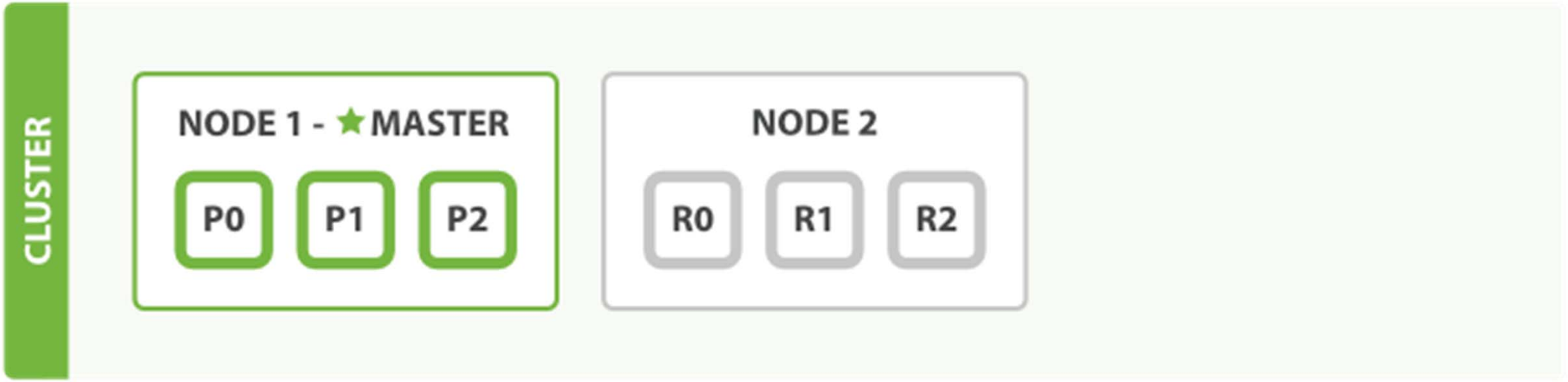
one **node** with three primary shards

creates a **cluster** of one node

node is elected to **master** role within the cluster

replica shards not allocated

Add Resiliency

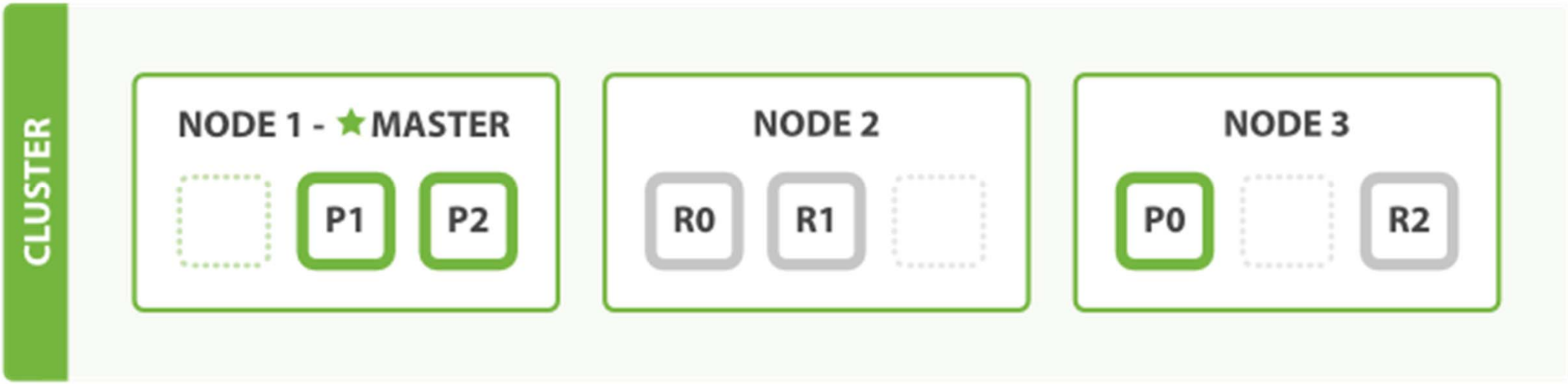


second **node** started with same **cluster.name**

node joins cluster (**discovery** unicast/multicast)

replica shards **automatically** allocated to second node

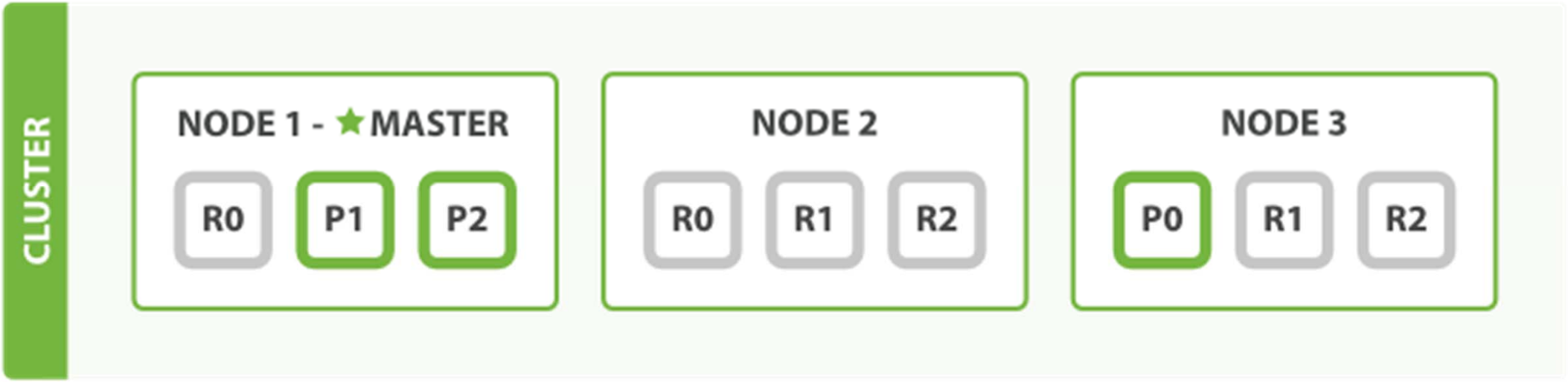
Scale Horizontally



add another node

elasticsearch **automatically** balances data

Scaling out more (number_of_replicas: n)

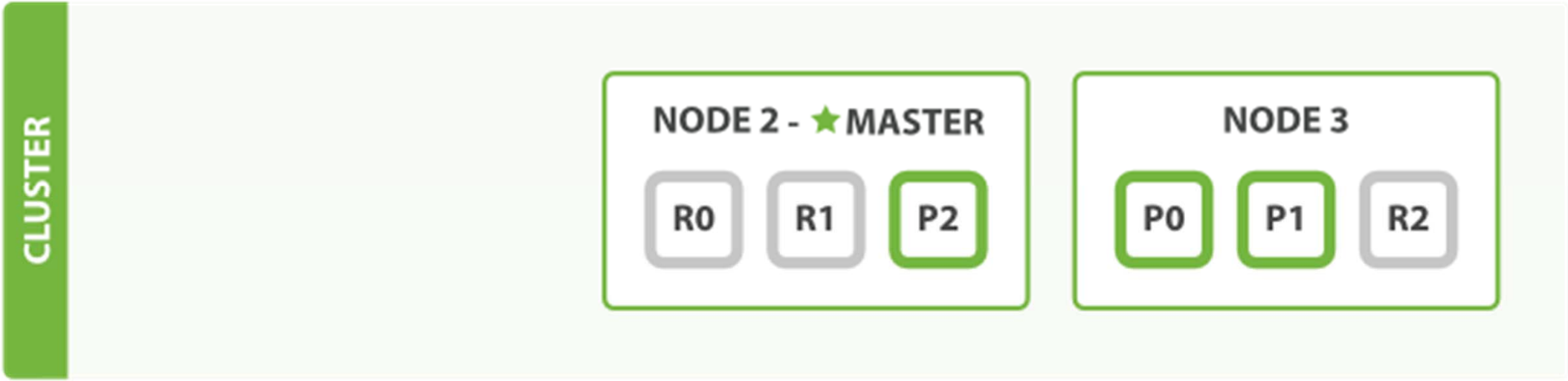


number of **primary** shard **fixed** at index creation

can **dynamically** increase the number of **replica** shards

more copies of you data means higher **read** throughput

Coping with failure



previous master node fails

triggers a new **master node election**

new master instantly **promotes** replicas to primary

Distributed

- **Replication**: Data duplication
  - read scalability
  - high-availability
- **Sharding**: Data partitioning
  - split logical data over several machines
  - write scalability
  - control data flow

Search

Search

query dsl

query dsl

flexible, powerful query language

query dsl

queries

- relevance
- full text
- not cached
- slower

filters

- boolean yes/no
- exact values
- cached
- faster

Filter first, then query remaining docs

query dsl: basic query

```
GET /_search
{
  "query": {...}
}
```

query dsl: basic query

```
GET /_search
{
  "query": { "match": { "title": "search" }}
}
```

query dsl: filtered query

```
GET /_search
{
  "query": {
    "filtered": {
      "query":  {...},
      "filter": {...}
    }
  }}
```

query dsl: filtered query

```
GET /_search
{
  "query": {
    "filtered": {
      "query":  { "match": { "title":  "search" }},
      "filter": { "term":  { "status": "active" }}
    }
  }}
```

other filter types

WHERE field CONTAINS "value"

term filter

```
"term":  {
   "title": "brown"
}
```

WHERE field IN ["val",…]

terms filter

```
"terms":  {
   "title": ["quick", "pets"]
}
```

other filter types

WHERE field >= x
AND field < y

range filter

```
"range": {
  "content":{
    "gte": 10,
    "lt": 80
  }
}
```

```
"range": {
  "date":{
    "gte": "2014-01-01",
    "lt": "2041-02-01"
  }
}
```

boolean filter types

```
"bool":  {
  "must":     [ <filters> ],
  "should":   [ <filters> ],
  "must_not": [ <filters> ]
}
```

AND

OR

NOT

query dsl: full example

```
{
  "filtered": {
    "query": { "match": { "title": "full text search" }},
    "filter": {
      "bool": {
        "must": { "range": { "created": { "gte": "now - 1d / d" }}},
        "should": [
          { "term": { "featured": true }},
          { "term": { "starred":  true }}
        ],
        "must_not": { "term": { "deleted": false }}
      }
    }
  }
}
```

query dsl: filter caching

```
{
  "filtered": {
    "query": { "match": { "title": "full text search" }},
    "filter": {
      "bool": {
        "must": { "range": { "created": { "gte": "now - 1d / d" }}},
        "should": [
          { "term": { "featured": true }},
          { "term": { "starred":  true }}
        ],
        "must_not": { "term": { "deleted": false }}
      }
    }
  }
}
```

analytics (aggregations dsl)

Types of Aggregations

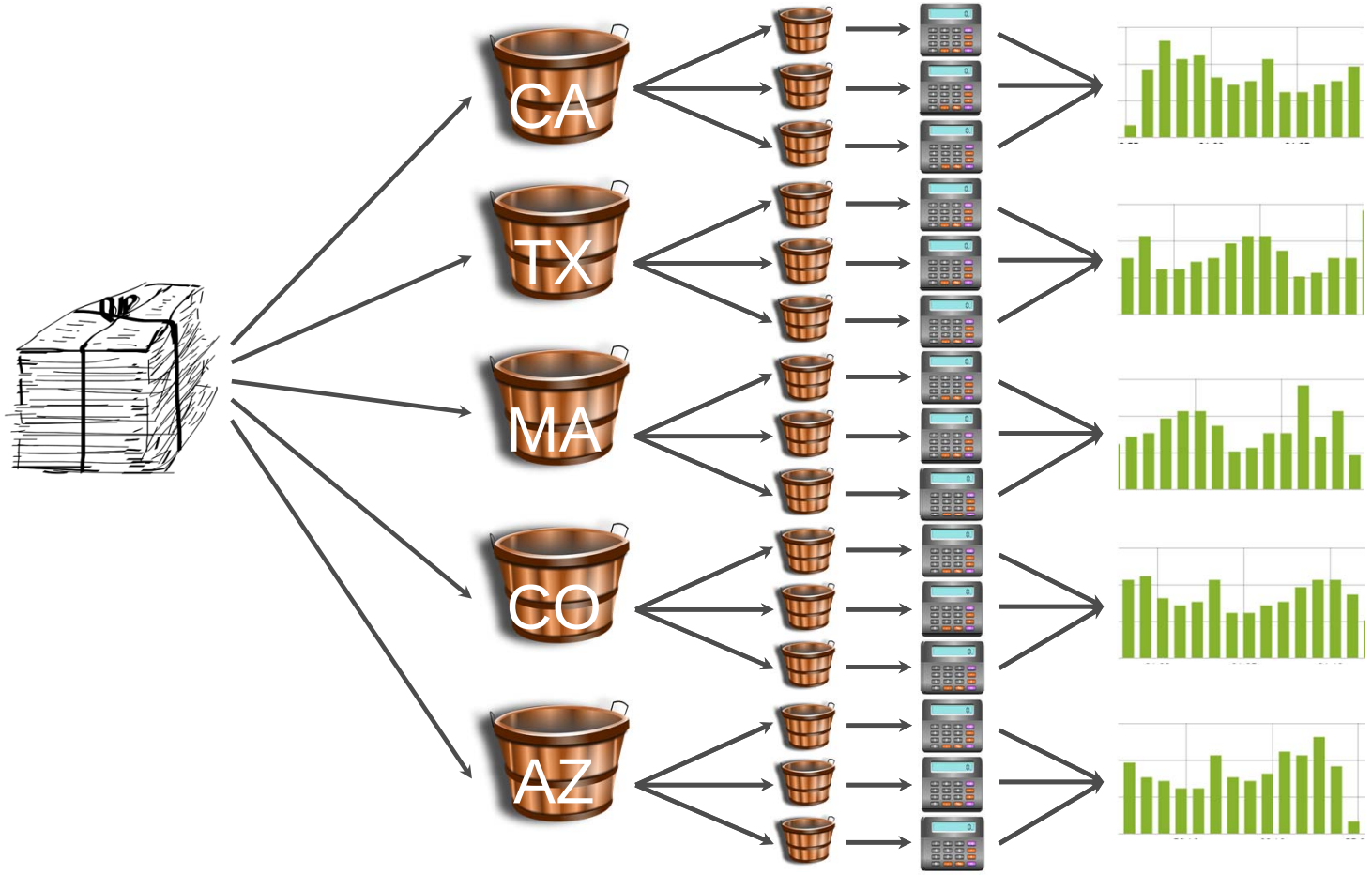
Buckets 

- Terms
- Date Histogram
- Filter
- Range
- Nested
- Children
- ….

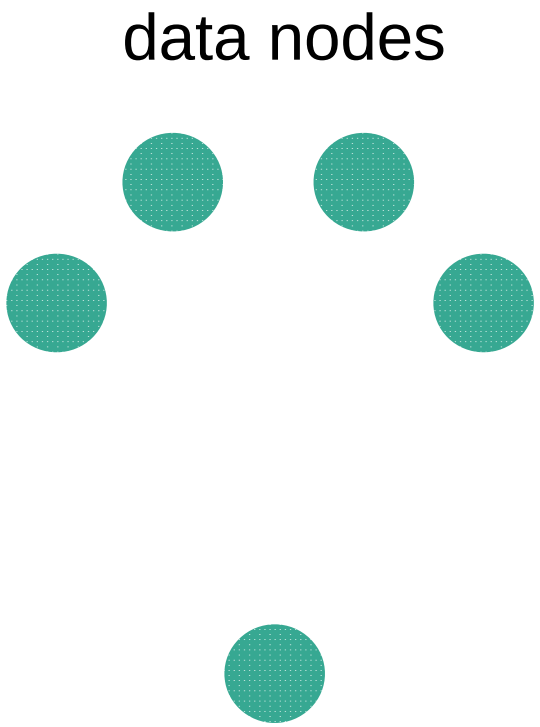
Metrics 

- Stats
- Percentile
- Cardinality
- Top hits
- Scripted
- Max | Min | Avg
- ….

aggs = buckets + calculated metric

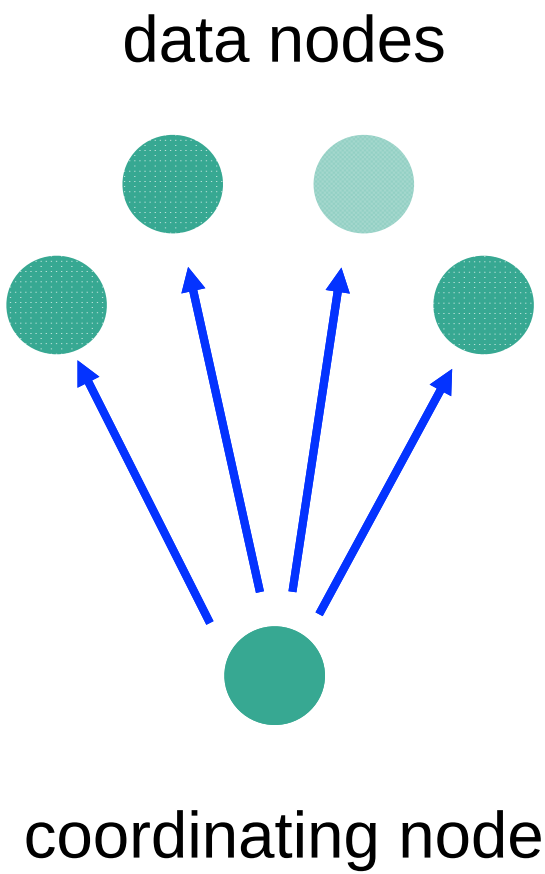


How do aggs work?



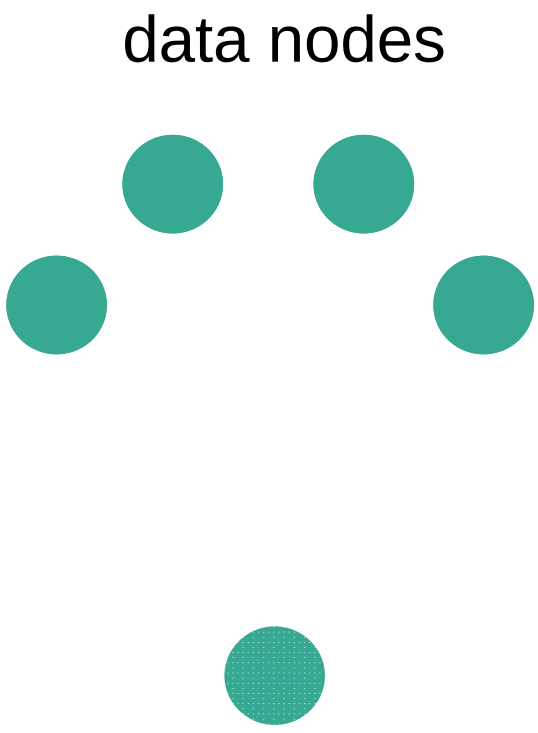
- ‘inline’ with search query
- execute in isolation on each shard
- 4 phases
  - parse
  - collect
  - combine
  - reduce

Phase 1 : Parse



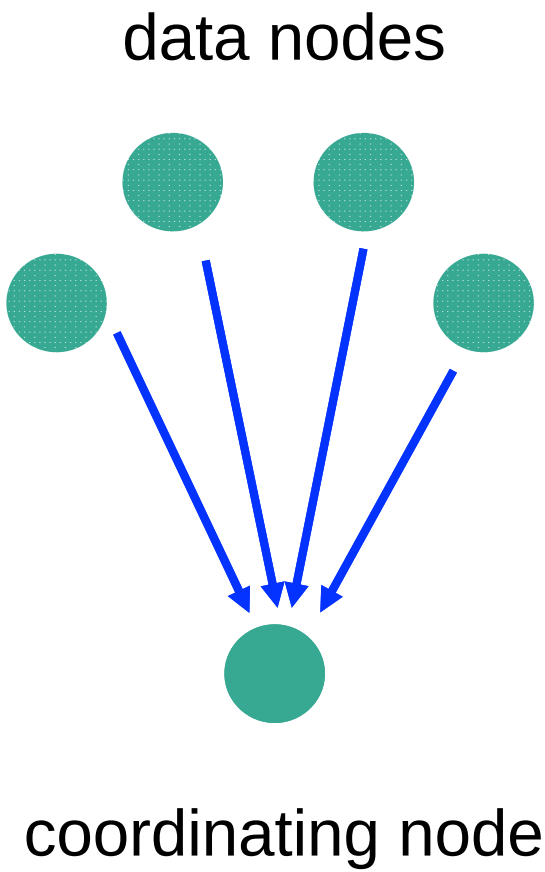
- Coordinating node splits the request into shard request
- shards parse aggregation and initialize data structures

Phase 2 + 3: Collect & Combine



- shards process all matching documents
- once done, they combine the aggregated data into an aggregation

Phase 4: Reduce



- shards sends their aggregation to the coordinating node
- coordinating node reduces them into a single aggregation

Designed for speed and scale

- Single network round-trip
- Single pass through the data on shards
- Aggregates are computed in-memory
- Trades accuracy for speed in some use cases
- Aggregations can be composed
- Near real-time response times

Aggregation DSL Example

Request

```
..
  “aggs”: {
    “by_date”: {
    “date_historgram”: {
       “field”: “timestamp”,
       “interval”: “day”
     },
     “aggs”: {
       “max_temperature”: {
         “max” : {
           “field”:”temperature”
         }
       }
    }
…
```

Response

```
..
  “aggregation”: {
    “by_date”: {
      “buckets”: [
       {
        “key”: “2015-01-01T00:00:00.000Z”,
        “doc_count”: 24,
        “max_temperature”: {
          “value” : 23
        }
       }]
    }
  }
…
```

Kibana Deep-Dive

Pere Urbon-Bayes

Software Engineer

DEMO

Real-World Use Cases

Alan Hardy

Solutions Architect

Verizon Business

Use Case: Large-Scale Log Analytics for Infrastructure and Application Monitoring

- Netflix Platform Engineering team deployed a centralized ELK stack as part of their real-time query service
- Billions of events ingested into a system called Suro using Kafka, representing infrastructure events, application logs, API calls
- Hadoop used for batch analytics, ES+Kibana for real-time interactive analytics

Scale & Environment

- Multiple clusters with varying sizes
- Indexing billions events daily
- Elastic{ON} 2015 video available talking about details

Verizon Business

Use Case: Large-Scale Log Analytics for Security

- The ELK stack is powering security analytics for Verizon's Data Breach Investigation Report (DBIR)
- Previous solution was based on Hadoop and while functional was not optimized to deliver real-time, interactive insights
- Indexed data from Hadoop to enable real-time interactive analytics

Scale & Environment

- One cluster with 128+ nodes
- 500+ billion documents
- 10B+ documents indexed daily
- Elastic{ON} 2015 video available talking about details

Q & A

elastic