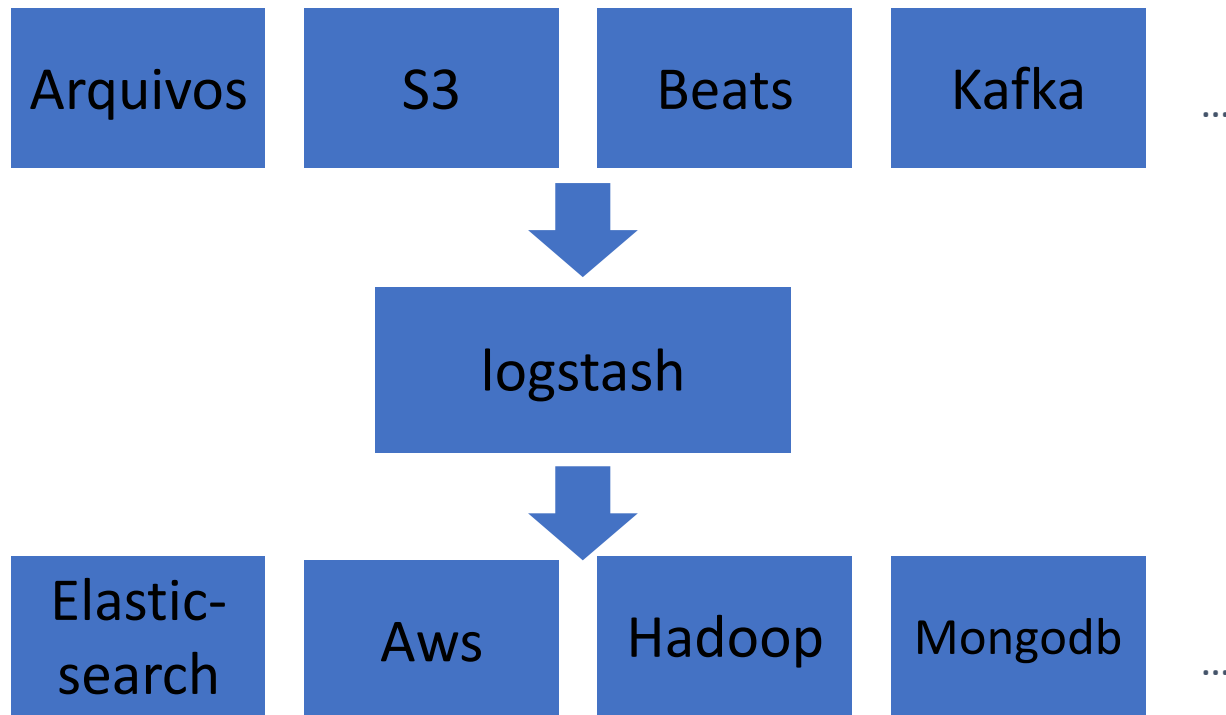


O que é Logstash



Mais do que importação

- Pode analisar, transformar e filtrar os dados no processo
- Pode produzir dados estruturados de dados não estruturados
- Pode anonimizar dados pessoais ou excluir completamente
- Pode fazer pesquisas em dados geoespaciais
- Pode escalar entre vários nós
- Garantia de pelo menos uma entrega "at-least-once delivery"
- Pode absorver dados em picos de cargas

Veja <https://www.elastic.co/guide/en/logstash/current/filter-plugins.html> um lista de plugins.

Grande variedade de fonte de entrada

elastic beats – cloudwatch – couchdb – drupal – elasticsearch – windows
event log – shell output – local files – ganglia – gelf – gemfire – random
generator – github – google pubsub – graphite – heartbeats – heroku –
http – imap – irc – jdbc – jmx – kafka – lumberjack – meetup – command
pipes – puppet – rabbitmq – rackspace cloud queue – redis – relp – rss –
s3 – salesforce – snmp – sqlite – sqs – stdin – stomp – syslog – tcp –
twitter – udp – unix sockets – varnish log – websocket – wmi – xmpp –
zenoss – zeromq

Grande variedade de destinos onde pode "juntar" os dados

boundary – circonus – cloudwatch – csv – datadoghq –
elasticsearch – email – exec – local file – ganglia – gelf – bigquery
– google cloud storage – graphite – graphtastic – hipchat – http –
influxdb – irc – jira – juggernaut – kafka – librato – loggly –
lumberjack – metriccatcher – mongodb – nagios – new relic
insights – opentsdb – pagerduty – pipe to stdin – rabbitmq –
rackspace cloud queue – redis – redmine – riak – riemann – s3 –
sns – solr – sqs – statsd – stdout – stomp – syslog – tcp – udp –
webhdfs – websocket – xmpp – zabbix – zeromq

Uso típico

