38 | 日志管理：如何借助工具快速发现和定位产品问题？

2019-05-28 宝玉 来自北京

《软件工程之美》

你好，我是宝玉。在开始学习之前我想先问你几个问题：

> 如果你的网站或者服务出现故障，是谁第一时间发现问题的？用户还是运维人员？
>
> 假设你的服务架构是由若干微服务组成的，其中一个微服务的异常导致了你的某个 API 请求异常，你是否能快速定位到是哪个微服务出了问题？
>
> 在部署系统后，你是否能观察出来系统的性能是上升了还是下降了？

如果你自己对这些问题的答案不是很满意，那么就可以来看看，如何借助监控和日志分析工具，或者说日志管理工具，第一时间发现线上问题，以及快速定位产品问题。

什么是日志管理？

要理解上面提到的这些问题，首先你要清楚，什么是日志管理。

日志就是操作系统和应用软件自动生成的事件说明或者消息记录，包含了时间、日志信息。举例来说，下面就是一个典型的 Web 请求日志：

> 10.0.1.22 – – [15/Oct/2018:13:46:46 -0700] “GET /favicon.ico HTTP/1.1” 404
> 10.0.1.22 – – [15/Oct/2018:13:46:58 -0700] “GET / HTTP/1.1” 200

从上面的日志中，可以看出来，日志包含两次 http 请求，它们发生的时间、请求的 URL、请求的 IP 地址、最后返回的状态码等信息。

在日志数量不多的时候，凭借肉眼或者借助文本编辑器，还能大概看出日志的内容，但是当日志数量一多，从日志里面查找需要的信息就变得很困难了。

现在的应用程序越来越复杂了，尤其是像微服务这样的架构，一个系统需要由若干微服务组成，每个微服务可能还会部署在若干容器上，那么意味着如果你要根据日志去排查故障的话，需要从几十、上百个地方去收集日志，再逐个去分析。

要解决这样的问题，就需要对日志进行统一管理。日志管理就是指对系统和应用程序产生的日志进行处理的方法，包括对日志进行统一收集，对日志数据进行筛选和解析，统一存储，还要让它们可以方便被检索。

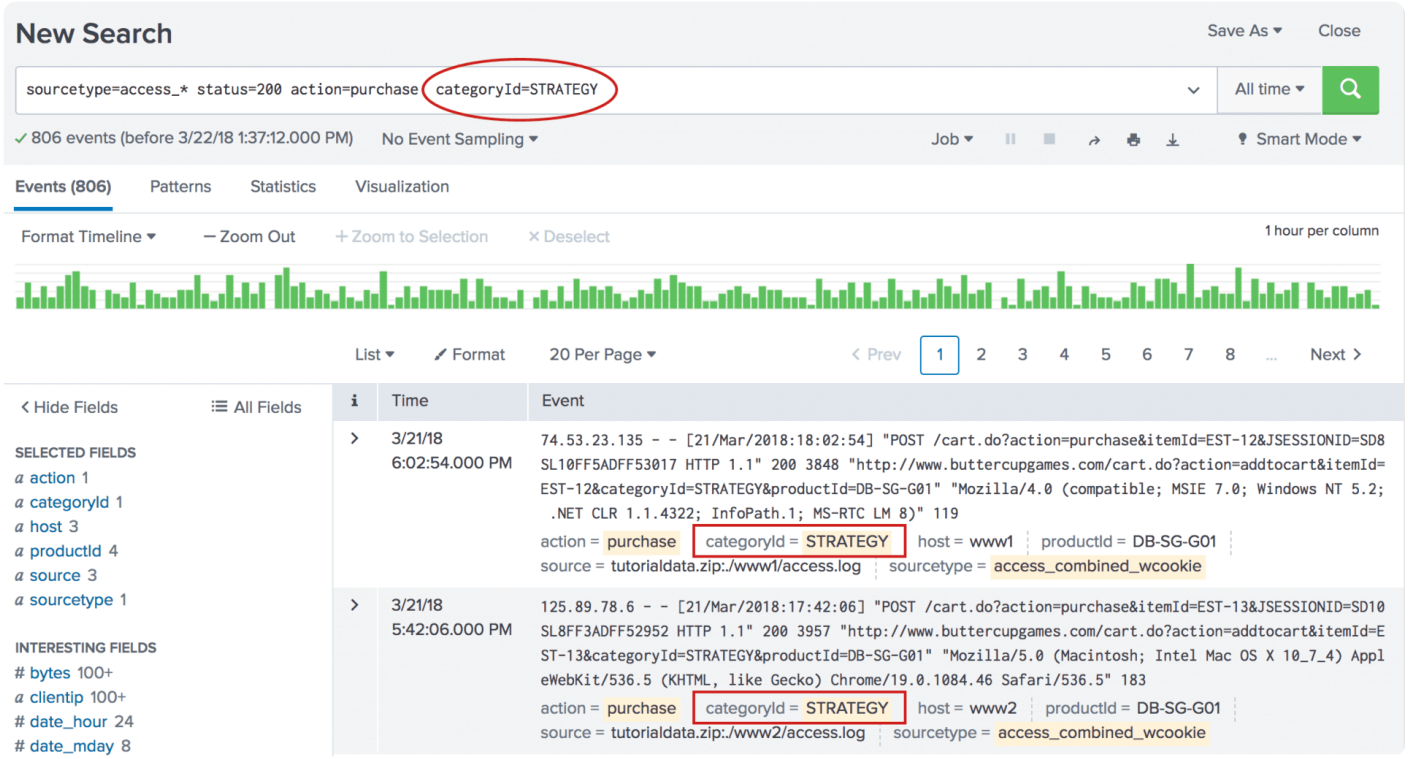
当然你不需要自己去从头实现这样的日志管理系统，现在已经有很多成熟的日志管理工具可以帮助你对日志进行管理，你只要去了解这些工具可以帮助你做什么，以及如何基于它们来搭建适合你项目的日志管理系统即可。

如何快速发现和定位问题?

也许你会问，为什么说搭建了日志管理系统，就可以帮助快速发现和定位问题呢?

首先，日志集中式管理后，就可以方便地对所有日志进行统一的检索。当所有日志都可以放在一起检索了，自然就能高效地定位到问题，而不再需要到各个应用程序的日志里面去分别检索。

同时在检索的方式上，可以用类似于 SQL 语句的方式来检索，高效地对结果进行查询和归类。



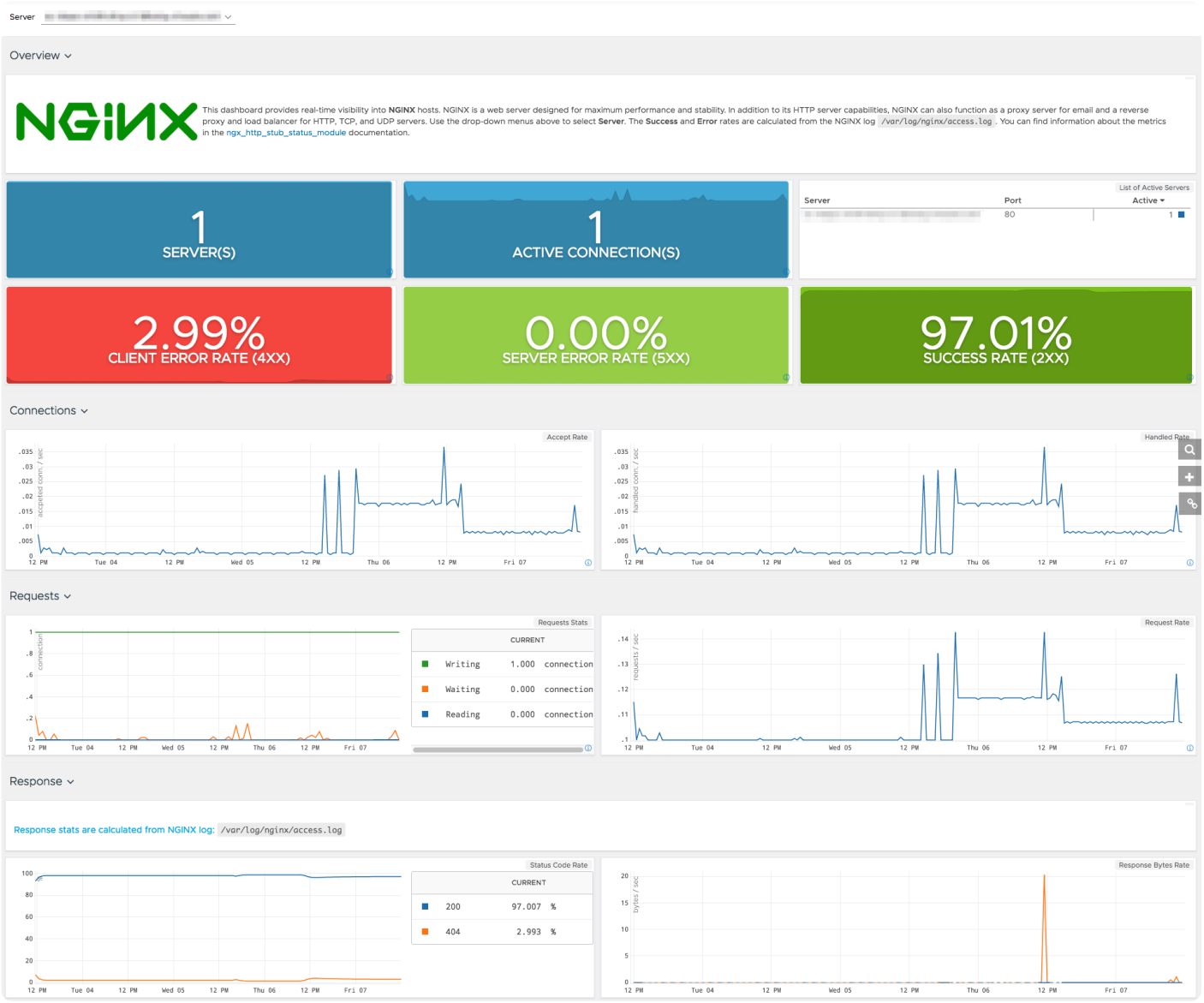
图片来源：Splunk

然后，对日志进行集中式管理后，可以通过图表直观的看到应用运行情况。当所有的应用实时将日志传输到一起，日志管理系统就可以根据应用日志中记录的信息，动态地生成图表，实时看到应用运行的情况。

举例来说，某一个 API 服务，日志信息记录了每一次 Http 请求的状态、耗费时间等信息。

> 127.0.0.1 [10/Oct/2018:13:55:36 -0700] "GET /api HTTP/1.1” 200 2326 0.038

那么把这些信息统一收集、实时统计的话，就可以随时看到单位时间内，这个 API 错误率有多少，平均耗时多久，从而可以根据这样的信息生成实时的图表，方便查看当前 API 服务的运行情况。



图片来源：WaveFront

最后，可以根据日志的数值设置规则自动报警。对于这些从日志中实时分析出来的数据结果，如果设置好相应的阈值，在超过阈值后，比如说 API 错误率超过 10%，或者 90% 的 API 请求时间超过 1 秒，就会自动触发报警，通知相关的开发人员进行维护。

所以你看，当你搭建好一整套日志管理系统后，不仅可以帮助你快速地对日志进行检索，你也可以根据图表看数据走势，还可以通过对日志分析结果的监控，设置自动报警的规则，第一时间了解系统故障。

大厂的日志管理系统的架构是什么样子？

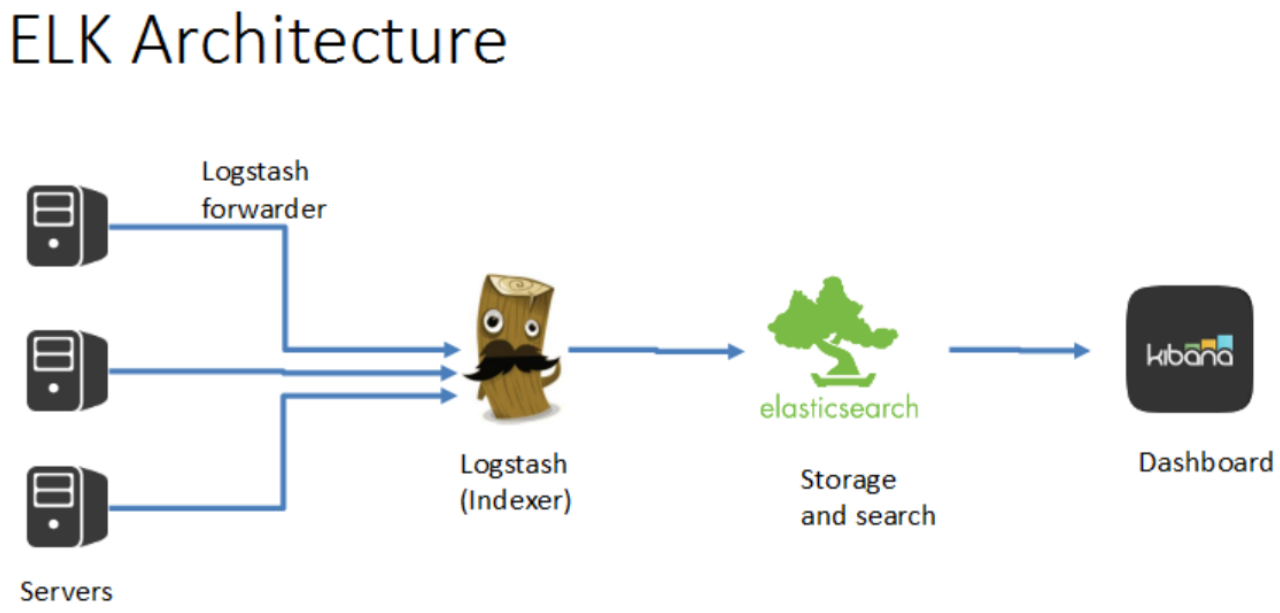
现在对于像阿里、新浪这样的大厂来说，对日志管理系统的应用已经是标配了，比如说阿里云：《基于 ELK 实时日志分析的最佳实践》、新浪：《ELK Stack 在新浪微博的最佳实践》、《新浪是如何分析处理 32 亿条实时日志的？》，七牛：《如何快速搭建智能化的统一日志管理系统》。

可以看得出，很多大厂是基于 ELK 搭建的自己的日志管理系统，而 ELK 的架构也是一套经典的日志管理的架构，所以这里我就以 ELK 为例来说明日志管理系统的基本架构。

先解释一下 ELK：

> ELK 是 Elasticsearch+Logstash+Kibana 的缩写。
> ElasticSearch 是一套搜索框架，提供了方便的接口，可以方便地做全文检索，可以用来对日志进行检索。
> Logstash 是一个数据收集工具，可以用来收集日志数据。
> Kibana 是一套可以和 ElasticSearch 交互的界面，通过 Kibana 可以方便的检索 ElasticSearch 内的所有数据，还可以用图形化的方式展示数据结果。

基于 ELK 搭建的日志管理系统基本架构是这样的：



这套架构有几个重要的模块：日志采集和解析、存储和搜索、结果可视化、监控和报警。

日志采集和解析

要想对日志进行统一管理，就必须要从各个应用系统收集日志。Logstash 就可以帮助实现对日志的采集。

如果日志文件只是一行行带时间戳的文本，那其实是无法有效检索的，必须将其解析成结构化的数据，才能方便地检索。

另外，一套系统可能由不同的应用类型组成，有的是 Java 写的，有的是 Go 写的，日志格式可能完全是不一样的，所以还有必要在对日志解析后，提取公共元素，比如时间、IP 地址、主机名、应用名称等。

Logstash 不仅可以对日志数据进行收集，还能对日志数据进行过滤和解析，解析完成后再将解析好的数据发送给 ElasticSearch。

存储和搜索

当所有的日志数据都被集中存储后，可以想象这个日志数据库是相当庞大的，直接查询效率是比较低下的，这就意味着还需要对日志数据进行索引和分析，从而让你可以快速地检索出来结果。

ElasticSearch 就是一套专业的全文检索和数据存储系统，同时还有一套类似于 SQL 的查询语句，这样你就可以基于它，方便对收集好的日志数据进行检索了。

但 ElasticSearch 本身类似于数据库，没有图形化界面。

结果可视化

可视化是日志管理的另一项重要功能。通过可视化的图表，可以直观地看到数据的走势，以及方便地和历史数据进行对比。

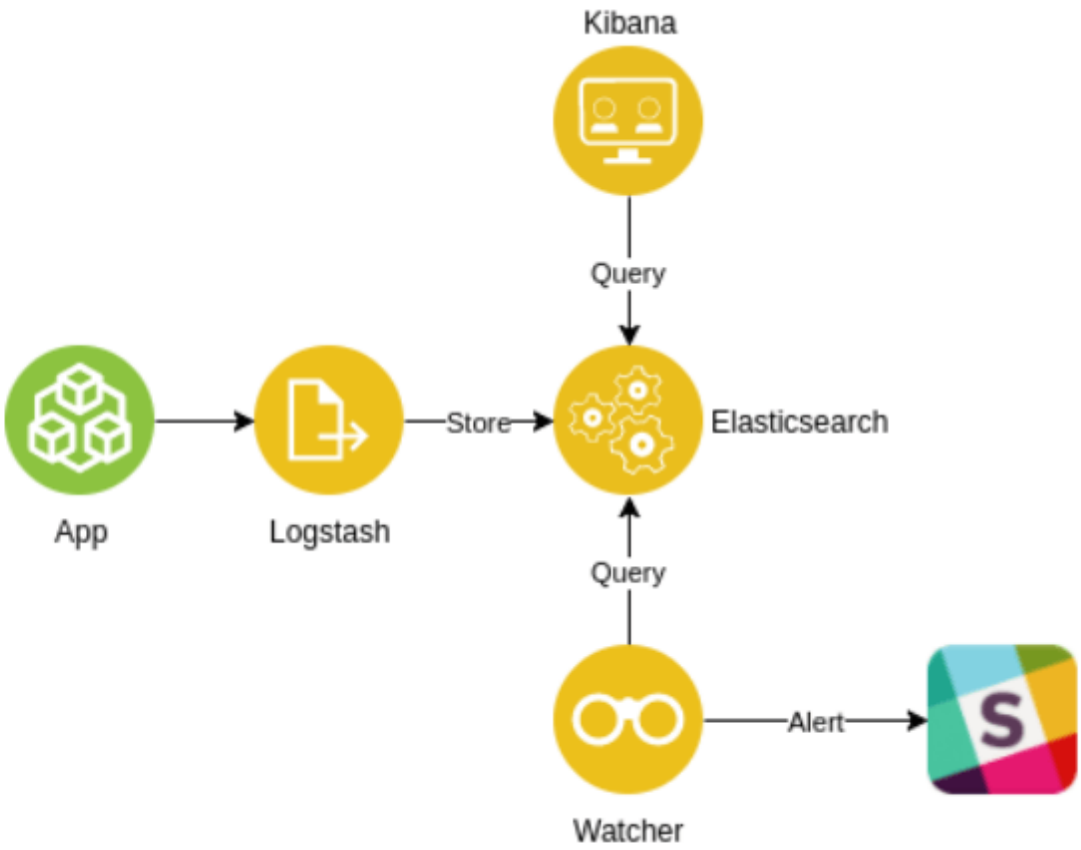
比如说通过观察交易数据的走势曲线，就能看出来这周的交易数据比上周是增长还是下降；根据 API 响应速度的走势，可以看得出新版本部署后，性能是提升了还是下降了。

像 Kibana 就是一套专门针对 ElasticSearch 的图形化操作工具，可以方便对 ElasticSearch 数据进行检索，也可以对结果用图表的方式展现。

监控和报警

ELK 本身只是提供了一套基础的日志管理框架，但是基于它之上还可以有很多扩展，比如说自动报警就是一个非常典型的场景，可以基于已经存储和索引好的日志数据，制定相应的自动报警规则，当线上服务发生异常时，可以自动地触发报警，通知相关值班人员及时处理。

ELK 可以通过插件的方式，安装像 ElastAlert 或Watcher这样的自动报警插件，实现自动报警功能。



图片来源：Build your own error monitoring tool

怎样搭建一套日志管理系统?

在了解了整个日志管理系统的基础架构后，再要去搭建这样一套日志管理系统，就可以做到心中有数了。你可以基于这套架构去寻找合适的工具，或者直接基于 ELK 去搭建一套日志管理系统。

关于 ELK 网上已经有很多安装使用教程，比如这一本电子教程《ELK 教程》就写的很详细。

ELK 本身是一套开源免费的工具，除了 ELK，还有一些类似的工具可以选择，可以和 ELK 配合使用。

Splunk

Splunk 是一套商业的日志管理系统，搜索功能非常强大，操作方便，就目前来说，要比 ELK 好用，但价钱很高。

Grafana

Grafana 是一套开源的数据监测和可视化工具，可以和 ELK 或 Splunk 配合使用，展示效果比 Kibana 要更好。同时可以支持自动报警功能。

Wavefront

Wavefront 是 VMware 旗下的一款商业的图形化监控和分析工具，可以从 ELK 或 Splunk 等数据源收集数据，在此基础上分析应用的性能瓶颈所在，排除故障。也支持自动报警。

PagerDuty

PagerDuty 是一套报警服务，不仅可以和手机、邮件、Slack 等方便地集成，还可以和企业的轮值安排结合，按照排班顺序呼叫当值人员。

以上就是一些常用日志管理系统以及配套系统工具，基本上可以很好地满足你对日志管理的需求，通过搜索引擎你也可以找到更多类似的服务。

总结

今天我带你一起学习了日志管理工具相关的内容。通过日志管理工具，可以集中的管理所有系统的日志，方便对日志进行检索，图形化的展示结果，还可以做到根据设置的规则进行自动报警。

如果你想搭建属于自己的日志管理系统，可以基于 ELK 或者 Splunk 这样的日志管理工具，配合一些插件，实现你自己的日志监控和分析工具。

在搭建好日志管理系统后，如果我们再回头看文章开头那几个问题，你会发现：

> 如果你的网站或者服务出现故障，可以通过你设置好的自动报警规则第一时间通知值班人员，及时解决；
>
> 假如你的某一个微服务出现异常，你可以从你的日志管理系统中直接对所有微服务的日志进行查询，快速定位到问题所在；
>
> 在部署系统后，通过对 API 响应时间等数据指标的图形化显示，你可以直观的看到性能是上升了还是下降了。

总的来说，借助日志管理工具，可以帮助你快速发现和定位产品问题。

课后思考

你的项目中是否有应用日志管理工具？你觉得这样的工具的应用，对你的日常项目可以带来哪些好处？如果还没有应用，主要阻力是什么？欢迎在留言区与我分享讨论。

感谢阅读，如果你觉得这篇文章对你有一些启发，也欢迎把它分享给你的朋友。

精选留言 (10)

yellowcloud

2019-05-28

宝玉老师您好，目前我们公司是做数据共享交换平台的，目前对接了大量的汇聚共享的数据，对接这些数据也使用了大量的服务，随着对接工作的日益庞大，目前也考虑搭建一套ELK对日志进行管理。但是目前在使用过程中，我们一直在思考服务实际运行或者对接链路中那些信息需要抛给日志管理系统，目前已有的日志记录信息是请求IP、访问路由、访问时间、内容字节、参数、响应时间、报文等等，总是感觉自己在某些方面考虑不周全，无法对可能发生错误的区域进行全覆盖，宝玉老师这里有关于日志具体记录那些细节的材料吗？

作者回复: 抱歉我没有材料来说明应该记录哪些日志。

不过我觉得你说的这些日志信息基本上涵盖了，如果要补充的话，我建议对于每一次用户的请求，在入口处生成一个唯一的请求编号，对于这次请求经过的所有服务，都统一带上这个唯一请求编号，以后定位问题是，根据请求编号，就可以快速的发现是在哪一个服务出现问题。这是我在实践中觉得特别有效的一个字段。

另外异常信息、错误堆栈非常有用，必须确保记录下来了。

其实具体要哪些信息，你可以站在故障排查和数据统计的角度思考，哪些信息是有帮助的，然后记录下来。

最重要是先搭建起来一套日志管理的体系，然后实际应用中逐步补充完善。

7

alva_xu
2019-05-29

我写过一遍关于ELK的博文《从Filebeat到Logstash再到Elasticsearch,如何搭建ELK 日志平台》https://blog.csdn.net/alva_xu/article/details/84578787，敬请指正。

作者回复: 感谢分享，已拜读。这一篇是关于如何搭建系统的，后续是不是还会有基于这个系统集成应用程序日志，以及对应用程序监控的文章？期待：）

4

峰
2019-06-01

宝玉老师，我们项目是.net做的，最近想用nlog 来采集日志到es中，但系统度量是另外的方案baidu 上都是appmetrices+influxdb+grafana,所以我想实现日志,应该放es好些，但如何同时满足度量的需求呢？因为度量本身也是基于日志

作者回复: 我觉得不必非要强行整合在一起，因为对于监控来说，理论上来说可以有多个数据源，我对Grafana不够熟悉，不太确认但我想应该可以同时获取展示来自InfluxDB和ES的数据。

你可以考虑以下方案（仅供参考，我没有验证过可行性）：nlog的数据还是放在es，系统度量用app metrices+influxdb+grafana，然后在grafana上集成其余的你想监控的从es查询的数据。

我有见过类似的架构：
wavefront（类似于grafana）获取metrices和ES查询的数据。

3

hua168
2019-05-30

大公司系统复杂，每天产生日子很大又多，单靠人工排查肯定不行。
是不是他们有很好的监控系统？尤其是业务监控，都做监控埋点？一般像一场马上就可以报警，有的会先自动化修复，不行的话就报警。

作者回复: 是的，基于日志有监控系统，可以直观从图表实时看到数据变化，会有自动报警。

数据量大不是问题，现在基于大数据的数据检索方案已经比较成熟了。

自动修复我不知道是不是有，目前应该还不成熟，也就是自动重启下服务，未来也许会有AI能直接处理线上故障吧：）

3

hua168
2019-05-29

像ELK收集到日志，还要做日志过滤的吧，怎么过滤，是收集的时候过滤，还是收集好再用大数据分析显示出自己需要的?
现在有点大的单有日志监控不行，都会链路跟踪系统去跟踪哪个环节出问题

作者回复: 拿ELK来说，是在Logstash那一层做过滤和解析，必须现过滤和解析检索才能高效。

是的，如果系统很多很复杂，必须要链路跟踪是哪个环节出的问题。

4

孤星可
2019-05-29

graylog 也不错 开源

作者回复: 谢谢分享👍

3

Charles
2019-05-28

我们目前用了云厂商的日志服务，尝试过自己搭和维护，实在太费劲了

问老师一个问题，目前只放了nginx日志到日志服务做一些简单的分析，还有其他什么日志是应该放到日志服务里的？有什么比较好的实践吗？谢谢

作者回复: 我觉得应用程序的日志也应该考虑放进去，对排查问题很有帮助。

应用程序的异常信息、错误堆栈非常有用，必须确保记录下来了。

举个例子来说，你的一个手机App，一些特定场景下，某个API请求出错，而这个API可能背后会连接多个服务或者数据库，这样的场景下，光靠nginx日志是不够的，必须要有应用程序的日志配合才好定位。

你可以参考上一篇我提到了一个requestId的实践。

3

峰
2019-05-29

请问可以通过什么系统设置响应阀值报警呢

作者回复: 你可以搜索一下关键字：“ELK ElastAlert 报警”应该可以找到不少记录，比如说：
https://blog.51cto.com/seekerwolf/2121070

https://segmentfault.com/a/1190000017553282

2

拉欧

2019-05-28

现在几乎所有的大厂都有一整套日志管理方案，大部分还不止一套

作者回复: 👍确实如此，因为这样的系统对于复杂应用的故障定位来说，太有用了太有必要了。

2

ifelse

2022-07-07

通过日志管理工具，可以集中的管理所有系统的日志，方便对日志进行检索，图形化的展示结果，还可以做到根据设置的规则进行自动报警。--记下来

2