

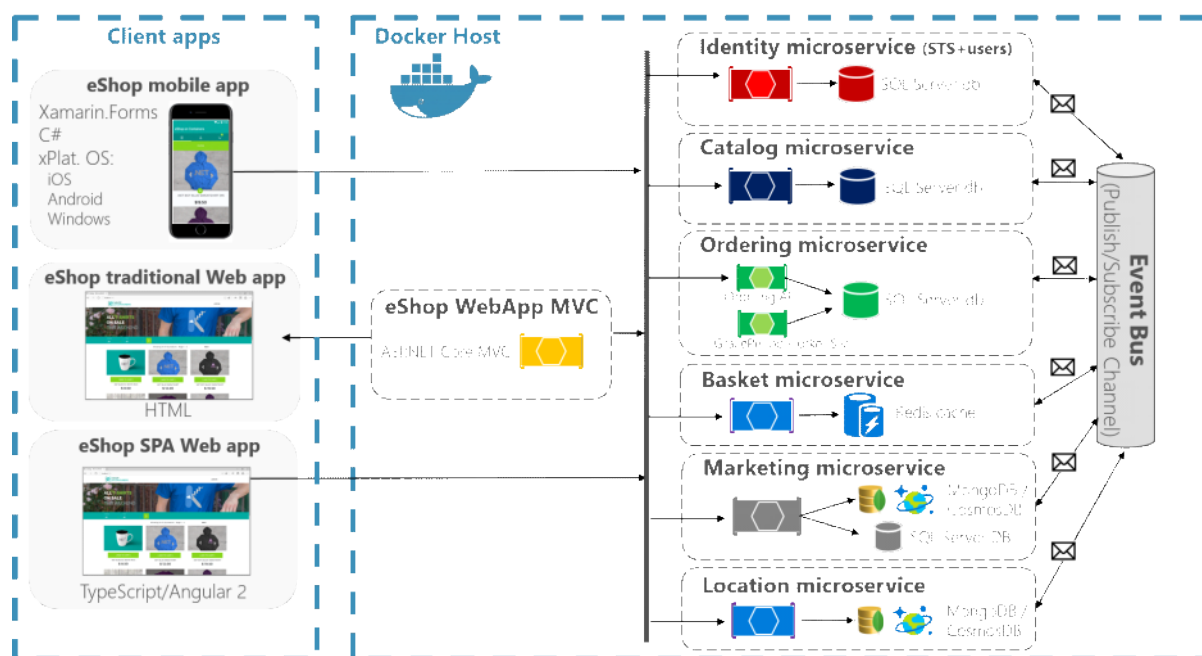
第33期-分布式结构化日志系统

2020年5月26日 13:11

日志主要包括系统日志、应用程序日志和安全日志。系统运维和开发人员可以通过日志了解服务器软硬件信息、检查配置过程中的错误及错误发生的原因。经常分析日志可以了解服务器的负荷，性能安全性，从而及时采取措施纠正错误。

通常，日志被分散的储存在不同的设备上。如果你管理数十上百台服务器，你还在使用依次登录每台机器的传统方法查阅日志。这样是不是感觉很繁琐和效率低下。当务之急我们使用集中化的日志管理，例如：开源的 seq，将所有服务器上的日志收集汇总。

eShopOnContainers Reference Application - Architecture



<https://github.com/serilog/serilog>

<https://github.com/nlog/NLog>

<https://datalust.co/seq>

开源实时日志分析ELK平台部署

使用requestId在分布式系统追踪请求

ELK 由 Elasticsearch、Logstash 和 Kibana 三个开源工具组成。

Elasticsearch是个开源分布式搜索引擎，它的特点有：分布式，零配置，自动发现，索引自动分片，索引副本机制，restful风格接口，多数据源，自动搜索负载等。

Logstash是一个完全开源的工具，他可以对你的日志进行收集、分析，并将其存储供以后使用（如，搜索）。

Kibana 也是一个开源和免费的工具，他Kibana可以为 Logstash 和 ElasticSearch 提供的日志分析友好的 Web 界面，可以帮助您汇总、分析和搜索重要数据日志。

