

36 | 微服务架构最佳实践 - 基础设施篇

2018-07-19 李运华

从0开始学架构

[进入课程 >](#)



讲述：黄洲君

时长 12:32 大小 5.74M



每项微服务基础设施都是一个平台、一个系统、一个解决方案，如果要自己实现，其过程和做业务系统类似，都需要经过需求分析、架构设计、开发、测试、部署上线等步骤，专栏里我来简单介绍一下每个基础设施的主要作用，更多详细设计你可以参考 Spring Cloud 的相关资料 (<https://projects.spring.io/spring-cloud/>)。

下面进入今天的内容，**微服务架构最佳实践的基础设施篇**。

自动化测试

微服务将原本大一统的系统拆分为多个独立运行的“微”服务，微服务之间的接口数量大大增加，并且微服务提倡快速交付，版本周期短，版本更新频繁。如果每次更新都靠人工回归

整个系统，则工作量大，效率低下，达不到“快速交付”的目的，因此必须通过自动化测试系统来完成绝大部分测试回归的工作。

自动化测试涵盖的范围包括代码级的单元测试、单个系统级的集成测试、系统间的接口测试，理想情况是每类测试都自动化。如果因为团队规模和人力的原因无法全面覆盖，至少要做到接口测试自动化。

自动化部署

相比大一统的系统，微服务需要部署的节点增加了几倍甚至十几倍，微服务部署的频率也会大幅提升（例如，我们的业务系统 70% 的工作日都有部署操作），综合计算下来，微服务部署的次数是大一统系统部署次数的几十倍。这么大量的部署操作，如果继续采用人工手工处理，需要投入大量的人力，且容易出错，因此需要自动化部署的系统来完成部署操作。

自动化部署系统包括版本管理、资源管理（例如，机器管理、虚拟机管理）、部署操作、回退操作等功能。

配置中心

微服务的节点数量非常多，通过人工登录每台机器手工修改，效率低，容易出错。特别是在部署或者排障时，需要快速增删改查配置，人工操作的方式显然是不行的。除此以外，有的运行期配置需要动态修改并且所有节点即时生效，人工操作是无法做到的。综合上面的分析，微服务需要一个统一的配置中心来管理所有微服务节点的配置。

配置中心包括配置版本管理（例如，同样的微服务，有 10 个节点是给移动用户服务的，有 20 个节点给联通用户服务的，配置项都一样，配置值不一样）、增删改查配置、节点管理、配置同步、配置推送等功能。

接口框架

微服务提倡轻量级的通信方式，一般采用 HTTP/REST 或者 RPC 方式统一接口协议。但在实践过程中，光统一接口协议还不够，还需要统一接口传递的数据格式。例如，我们需要指定接口协议为 HTTP/REST，但这还不够，还需要指定 HTTP/REST 的数据格式采用 JSON，并且 JSON 的数据都遵循如下规范。

```
{  
    "requestId": 10086,  
    "time": "2017-01-01 00:00:00",  
    "caller": "tencent",  
    "api": "get_money",  
    "param": {  
        "userId": 13800138  
    },  
    "sign": "098f6bcd4621d373cade4e832627b4f6"  
}
```

如果我们只是简单指定了 HTTP/REST 协议，而不指定 JSON 和 JSON 的数据规范，那么就会出现这样混乱的情况：有的微服务采用 XML，有的采用 JSON，有的采用键值对；即使同样都是 JSON，JSON 数据格式也不一样。这样每个微服务都要适配几套甚至几十套接口协议，相当于把曾经由 ESB 做的事情转交给微服务自己做了，这样做的效率显然是无法接受的，因此需要统一接口框架。

接口框架不是一个可运行的系统，一般以库或者包的形式提供给所有微服务调用。例如，针对上面的 JSON 样例，可以由某个基础技术团队提供多种不同语言的解析包（Java 包、Python 包、C 库等）。

API 网关

系统拆分为微服务后，内部的微服务之间是互联互通的，相互之间的访问都是点对点的。如果外部系统想调用系统的某个功能，也采取点对点的方式，则外部系统会非常“头大”。因为在外部系统看来，它不需要也没办法理解这么多微服务的职责分工和边界，它只会关注它需要的能力，而不会关注这个能力应该由哪个微服务提供。

除此以外，外部系统访问系统还涉及安全和权限相关的限制，如果外部系统直接访问某个微服务，则意味着每个微服务都要自己实现安全和权限的功能，这样做不但工作量大，而且都是重复工作。

综合上面的分析，微服务需要一个统一的 API 网关，负责外部系统的访问操作。

API 网关是外部系统访问的接口，所有的外部系统接入系统都需要通过 API 网关，主要包括接入鉴权（是否允许接入）、权限控制（可以访问哪些功能）、传输加密、请求路由、流量控制等功能。

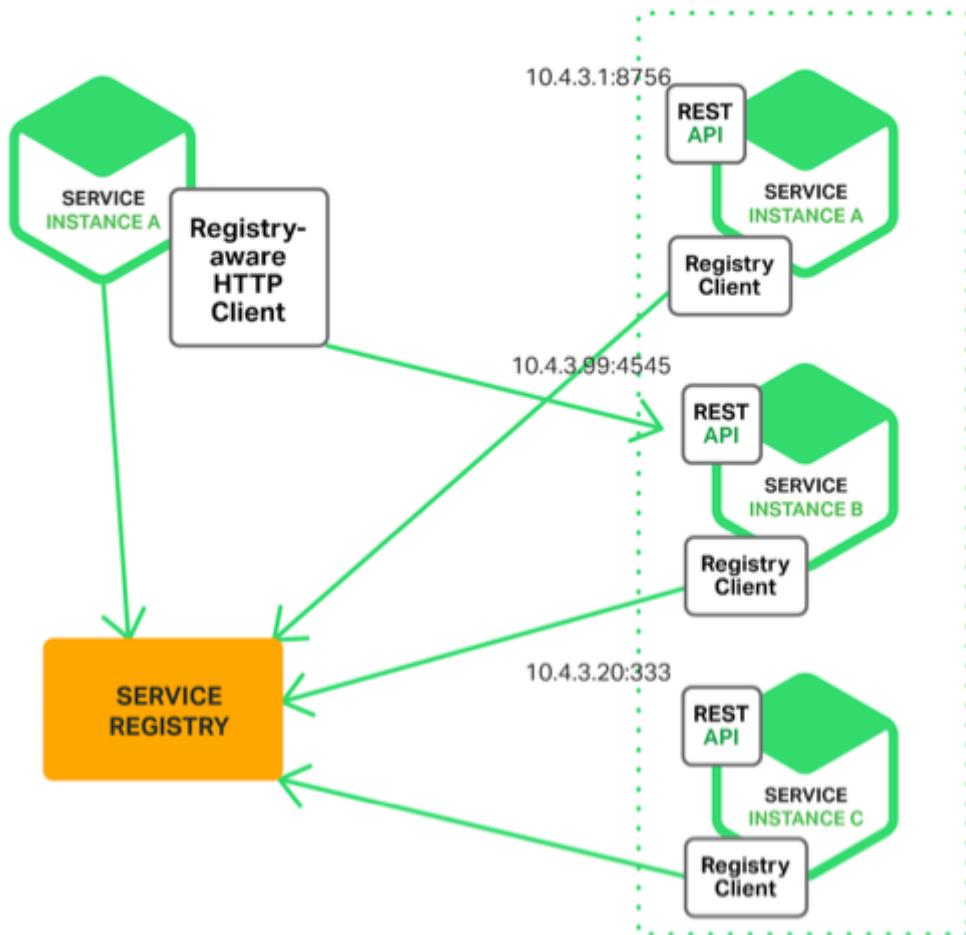
服务发现

微服务种类和数量很多，如果这些信息全部通过手工配置的方式写入各个微服务节点，首先配置工作量很大，配置文件可能要配几百上千行，几十个节点加起来后配置项就是几万几十万行了，人工维护这么大量配置项是一项灾难；其次是微服务节点经常变化，可能是由于扩容导致节点增加，也可能是故障处理时隔离掉一部分节点，还可能是采用灰度升级，先将一部分节点升级到新版本，然后让新老版本同时运行。不管哪种情况，我们都希望节点的变化能够及时同步到所有其他依赖的微服务。如果采用手工配置，是不可能做到实时更改生效的。因此，需要一套服务发现的系统来支撑微服务的自动注册和发现。

服务发现主要有两种实现方式：自理式和代理式。

1. 自理式

自理式结构如下：



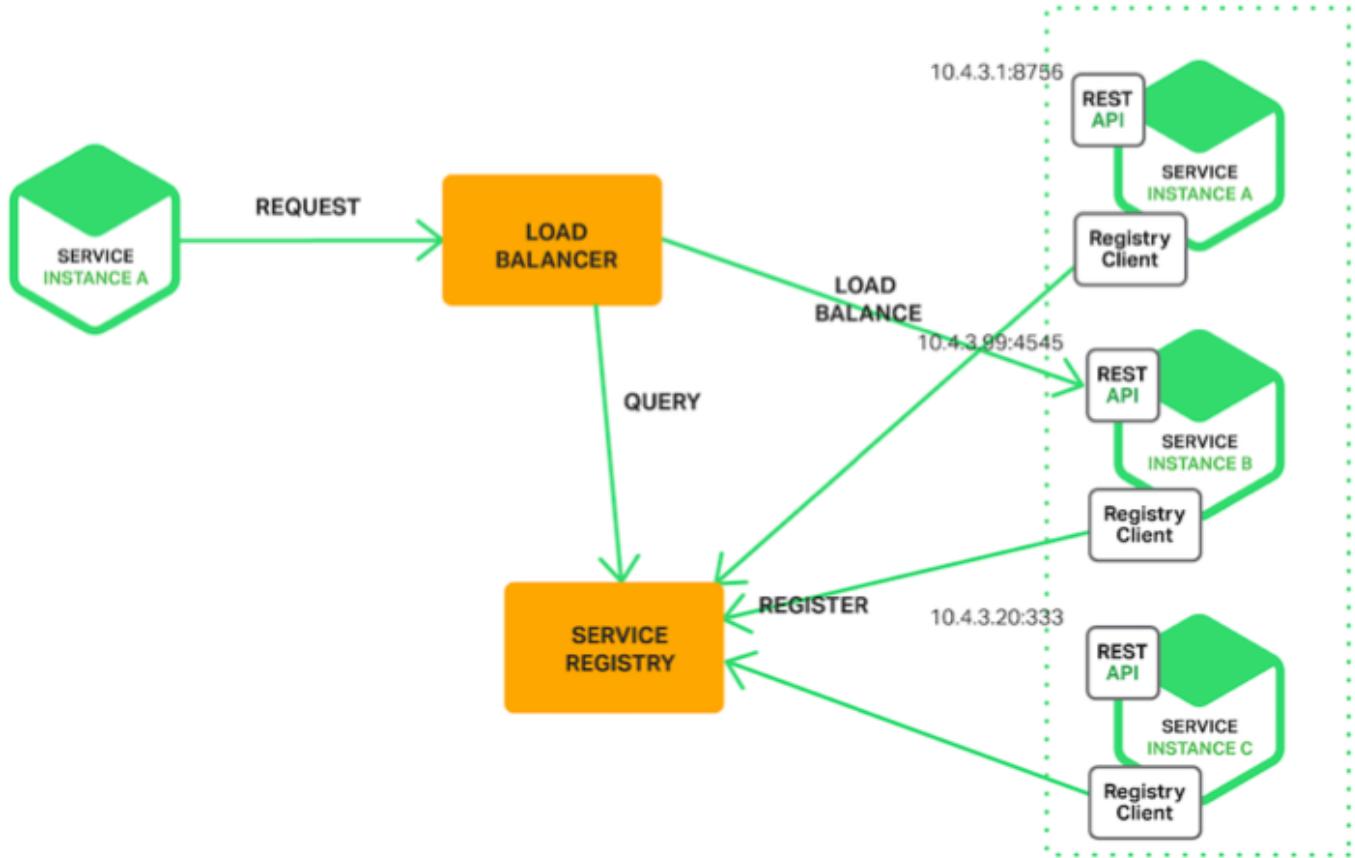
(https://cdn-1.wp.nginx.com/wp-content/uploads/2016/04/Richardson-microservices-part4-2_client-side-pattern.png)

自理式结构就是指每个微服务自己完成服务发现。例如，图中 SERVICE INSTANCE A 访问 SERVICE REGISTRY 获取服务注册信息，然后直接访问 SERVICE INSTANCE B。

自理式服务发现实现比较简单，因为这部分的功能一般通过统一的程序库或者程序包提供给各个微服务调用，而不会每个微服务都自己来重复实现一遍；并且由于每个微服务都承担了服务发现的功能，访问压力分散到了各个微服务节点，性能和可用性上不存在明显的压力和风险。

2. 代理式

代理式结构如下：



(https://cdn-1.wp.nginx.com/wp-content/uploads/2016/04/Richardson-microservices-part4-3_server-side-pattern.png)

代理式结构就是指微服务之间有一个负载均衡系统（图中的 LOAD BALANCER 节点），由负载均衡系统来完成微服务之间的服务发现。

代理式的方式看起来更加清晰，微服务本身的实现也简单了很多，但实际上这个方案风险较大。第一个风险是可用性风险，一旦 LOAD BALANCER 系统故障，就会影响所有微服务之间的调用；第二个风险是性能风险，所有的微服务之间的调用流量都要经过 LOAD BALANCER 系统，性能压力会随着微服务数量和流量增加而不断增加，最后成为性能瓶

颈。因此 LOAD BALANCER 系统需要设计成集群的模式，但 LOAD BALANCER 集群的实现本身又增加了复杂性。

不管是自理式还是代理式，服务发现的核心功能就是服务注册表，注册表记录了所有的服务节点的配置和状态，每个微服务启动后都需要将自己的信息注册到服务注册表，然后由微服务或者 LOAD BALANCER 系统到服务注册表查询可用服务。

服务路由

有了服务发现后，微服务之间能够方便地获取相关配置信息，但具体进行某次调用请求时，我们还需要从所有符合条件的可用微服务节点中挑选出一个具体的节点发起请求，这就是服务路由需要完成的功能。

服务路由和服务发现紧密相关，服务路由一般不会设计成一个独立运行的系统，通常情况下是和服务发现放在一起实现的。对于自理式服务发现，服务路由是微服务内部实现的；对于代理式服务发现，服务路由是由 LOAD BALANCER 系统实现的。无论放在哪里实现，服务路由核心的功能就是路由算法。常见的路由算法有：随机路由、轮询路由、最小压力路由、最小连接数路由等。

服务容错

系统拆分为微服务后，单个微服务故障的概率变小，故障影响范围也减少，但是微服务的节点数量大大增加。从整体上来看，系统中某个微服务出故障的概率会大大增加。[专栏第 34 期](#)我在分析微服务陷阱时提到微服务具有故障扩散的特点，如果不及时处理故障，故障扩散开来就会导致看起来系统中很多服务节点都故障了，因此需要微服务能够自动应对这种出错场景，及时进行处理。否则，如果节点一故障就需要人工处理，投入人力大，处理速度慢；而一旦处理速度慢，则故障就很快扩散，所以我们需要服务容错的能力。

常见的服务容错包括请求重试、流控和服务隔离。通常情况下，服务容错会集成在服务发现和服务路由系统中。

服务监控

系统拆分为微服务后，节点数量大大增加，导致需要监控的机器、网络、进程、接口调用数等监控对象的数量大大增加；同时，一旦发生故障，我们需要快速根据各类信息来定位故障。这两个目标如果靠人力去完成是不现实的。举个简单例子：我们收到用户投诉说业务有

问题，如果此时采取人工的方式去搜集、分析信息，可能把几十个节点的日志打开一遍就需要十几分钟了，因此需要服务监控系统来完成微服务节点的监控。

服务监控的主要作用有：

实时搜集信息并进行分析，避免故障后再来分析，减少了处理时间。

服务监控可以在实时分析的基础上进行预警，在问题萌芽的阶段发觉并预警，降低了问题影响的范围和时间。

通常情况下，服务监控需要搜集并分析大量的数据，因此建议做成独立的系统，而不要集成到服务发现、API 网关等系统中。

服务跟踪

服务监控可以做到微服务节点级的监控和信息收集，但如果我们要跟踪某一个请求在微服务中的完整路径，服务监控是难以实现的。因为如果每个服务的完整请求链信息都实时发送给服务监控系统，数据量会大到无法处理。

服务监控和服务跟踪的区别可以简单概括为宏观和微观的区别。例如，A 服务通过 HTTP 协议请求 B 服务 10 次，B 通过 HTTP 返回 JSON 对象，服务监控会记录请求次数、响应时间平均值、响应时间最高值、错误码分布这些信息；而服务跟踪会记录其中某次请求的发起时间、响应时间、响应错误码、请求参数、返回的 JSON 对象等信息。

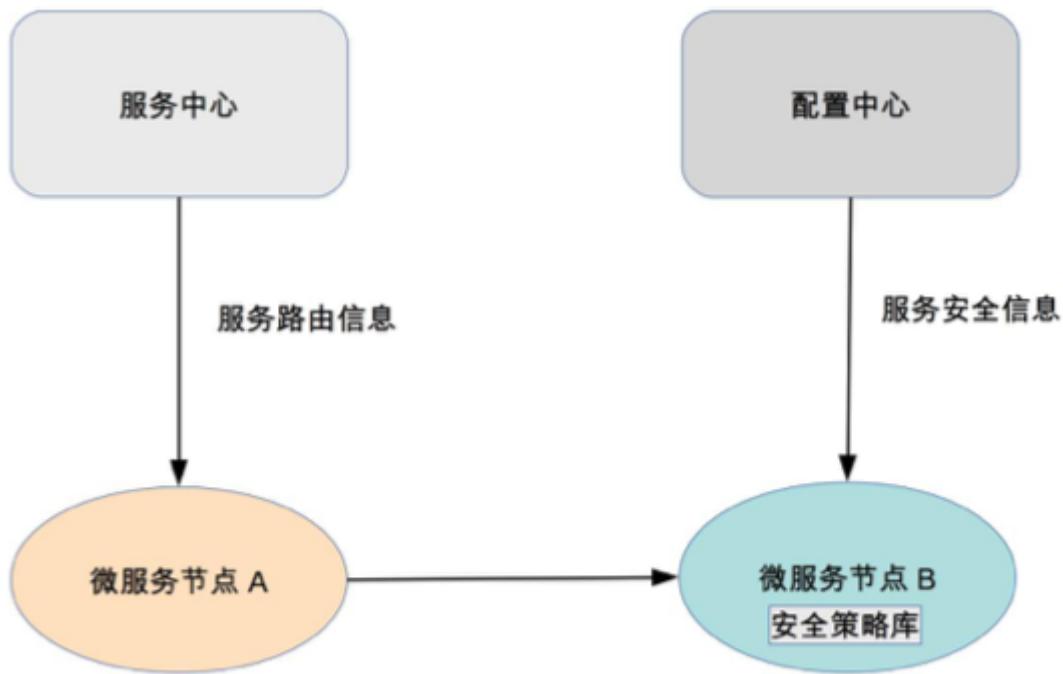
目前无论是分布式跟踪还是微服务的服务跟踪，绝大部分请求跟踪的实现技术都基于 Google 的 Dapper 论文《Dapper, a Large-Scale Distributed Systems Tracing Infrastructure》。

服务安全

系统拆分为微服务后，数据分散在各个微服务节点上。从系统连接的角度来说，任意微服务都可以访问所有其他微服务节点；但从业务的角度来说，部分敏感数据或者操作，只能部分微服务可以访问，而不是所有的微服务都可以访问，因此需要设计服务安全机制来保证业务和数据的安全性。

服务安全主要分为三部分：接入安全、数据安全、传输安全。通常情况下，服务安全可以集成到配置中心系统中进行实现，即配置中心配置微服务的接入安全策略和数据安全策略，微

服务节点从配置中心获取这些配置信息，然后在处理具体的微服务调用请求时根据安全策略进行处理。由于这些策略是通用的，一般会把策略封装成通用的库提供给各个微服务调用。基本架构如下：



小结

今天我为你讲了微服务架构相关的基础设施的概要介绍和关键设计点，希望对你有所帮助。

这就是今天的全部内容，这一期的思考题很特别，给你一个由 10 位 Java 高级软件工程师组成的开发团队，采用自研的方式，完成所有的微服务基础设施开发，你预测需要多长时间？理由是什么呢？

欢迎你把答案写到留言区，和我一起讨论。相信经过深度思考的回答，也会让你对知识的理解更加深刻。（编辑乱入：精彩的留言有机会获得丰厚福利哦！）



从0开始学架构

资深技术专家的
实战架构心法

李运华 资深技术专家



新版升级：点击「 请朋友读」，10位好友免费读，邀请订阅更有**现金奖励**。

© 版权归极客邦科技所有，未经许可不得传播售卖。 页面已增加防盗追踪，如有侵权极客邦将依法追究其法律责任。

上一篇 35 | 微服务架构最佳实践 - 方法篇

下一篇 37 | 微内核架构详解

精选留言 (32)

写留言



孙振超

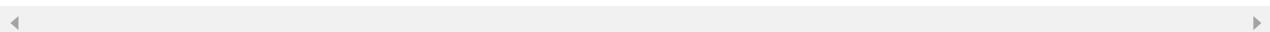
2018-09-18

35

文章中一共列了11个部分，但只有10个人，很明显是不可能同时开工的，即使能够同时开工也是需要经过几轮迭代才能达到一个比较完善的状态。

依据简单原则和演化原则以及“三个火枪手”的人员分配原则，首先可以做API网关、配置中心、服务发现、服务路由这4部分，经过一个月的开发+半个月的联调的先让基础框...
[展开](#)

作者回复: 你是第一个认真分析且抓住重点的同学凸凸





Coder4

2018-07-19

8

看怎么定义自研了，今年花了1个月，每天半小时代码。半开源，半代码，已经实现了服务发现，追踪，自动部署，以及后端服务数据库，消息队列，缓存，内存数据库的对接，真正熟悉了，花不了太多时间，另外得合理利用轮子。

展开 ▼

作者回复: 你这个太牛了，惊为天人啊😊



无痕

2018-07-20

3

老师，很多人把oauth2的鉴权放到了网关，这个你怎么看

作者回复: 不符合网关的定位，因为有的业务要鉴权有的不要，放在网关就相当于网关要和业务耦合了



程启

2018-08-12

2

华仔老师，

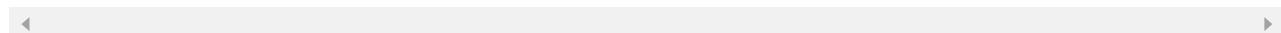
之前看您留言提到过service mesh不成熟，中小公司不建议使用。请问看起来最近gcp云平台，主推的k8s加上Istio/envoy实现服务治理，您认为未来方向如何，这个是试用中小型团队的方案吗？感谢解答！

展开 ▼

作者回复: 我没有service mesh具体实践经验，主要信息来源于网上资料，意见供参考。

1. Istio刚发布1.0版本，spring cloud成熟很多
2. service mesh中文为服务网格，很形象，说明了更加适合非常多的服务节点，简单来说，如果你只有一两个服务没必要用微服务架构，你只有几十个微服务节点可能也不需要service mesh
3. service mesh对程序无侵入，这点非常好，但随着spring cloud之类的方案成熟，侵入问题其实不是主要问题

因此，我认为大部分中小公司目前不需要service mesh，能把微服务做好已经很不错了。





成功

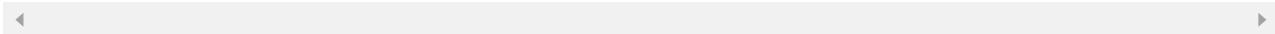
2018-07-27

▲ 2

30天左右

展开 ▼

作者回复: 太乐观，30天就算用spring全家桶，都不可能上线的



空档滑行

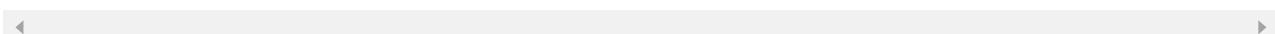
2018-07-19

▲ 2

工作量需要看这一套框架要应对的服务规模和流量。以100个微服务，接口平均qps100以下做了简单测算，不考虑同城和异地多活，达到基本可用的话配置中心，包括配置项管理和推送，和微服务一起打包的客户端接口框架，使用http和Json的话，只需要一种语言的解析包Api网关，后端服务对接和接入层实现...

展开 ▼

作者回复: 半年只能出最简单的版本，不完善



kyll

2018-07-19

▲ 2

按照我们公司的情况来说，1.5个人，spring全家桶，花费6个月，才让系统上线。要是完全自研，10个高程在，也信心不大。

展开 ▼



每天学英语...

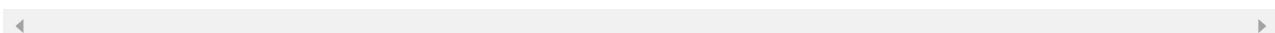
2019-01-09

▲ 1

微服务这两章讲的非常好，解决了长久以来的困惑

展开 ▼

作者回复: 都是实战经验总结





易燃易爆炸

2018-11-29

1

自己写的话肯定坑太多，也没有经过太多实践上的检验。感觉真正稳定下来需要趟过很多坑才行，当然成长也是成倍的，最终苦了公司，系统天天挂。

展开 ▼



文竹

2018-08-25

1

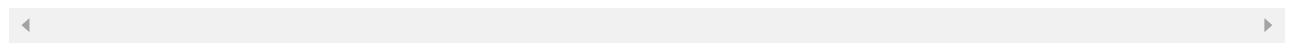
自动化测试：主要支持接口测试，可以使用robot framework，无需额外人天。

自动化部署：使用开源jenkins进行构建，无需人天。

配置中心：需要支持的功能有服务节点管理，节点配置管理，配置版本管理，配置变更...

展开 ▼

作者回复: 你还是太乐观了 😄



mayer

2018-07-19

1

这10个人分别有相关经验的话，不考虑复杂的业务逻辑实现调试，整个框架搭起来可应用，应该在3个月左右可以完成，条件是高级工程师真的高级，哈哈 😊

展开 ▼

作者回复: 太乐观了 😊



凡凡

2018-07-19

1

按照以往了解的基础架构部的开发速度来看，而且文中涉及的基础设施都有开源实现可以借鉴，一个基础设施从调研（开源系统代码review），到设计，再到开发，再到小流量接入，全公司推广，一个基础设施3个人大概5到6个月时间，如果去掉小流量和推广阶段，估计也需要3到4个月。

...

展开 ▼

作者回复: 这类微服务做出基本功能9个月可以，做完善需要耗时更长



Kyle

2018-07-19

1

Dubbo弄了这么久，配套的基础设施都还没有。高级的水平也有高有低。总觉得怎么也要个一年半载吧。

作者回复: 一年可以，半载不行😊



小智e

2019-04-11

1

老师讲到很好，不过由于自己还是在校生，没经历过，只能得到感性的认识，谢谢老师



aduan

2019-03-02

1

用了网关后，如何避免服务调用不会绕过网关直接调用接口？

作者回复: 封装SDK给业务用



依乐祝

2019-01-03

1

看了这么久第一次留言，老师你好，刚看你说网关层不建议做鉴权！但是如果这样的话，那内部微服务之间如何进行通信呢？我的理解是网关做与url有关的权限处理！而具体的业务服务里面做与数据相关的权限鉴别！这样职责分开！然后内部进行通信的话就可以采用rpc进行高效的交互，而且都是可信的！不知道我的理解是否有误，还请老师指正下哈

展开 ▼

作者回复: 这样是可以的，网关鉴权仅限于和用户相关的登录态，登录环境等，业务权限还是要业务做



乘风

2018-12-13



上面一共提到11个功能，每个功能按照业务职责去分可以分成11个服务，但按照三个火枪手原则来拆分服务大概是4个服务，拆分如下：

按照业务拆分：分为三类：

- 1.构建微服务的内部依赖：接口框架、服务路由、服务容错、服务安全
- 2.构建微服务的外部依赖：配置中心、api网关、服务发现、...

展开 ▼



模式

2018-11-10



我司就在往Spring cloud迁移，期间还要开发新需求，目前6个后台，都不是高程，领导让年底之前完成，以后会不会累成狗。

展开 ▼



AmosWooo

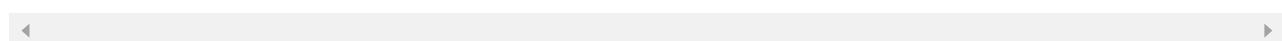
2018-10-29



接上一问题，微服务提倡无状态，那就必须有一个认证授权服务存在，我的理解是在APIGateway下层，存在一个同级服务来提供验证授权，或者说结合API网关提供全面安全机制，这样既可以在APIGateway层过滤部分非法请求，又在下层提供更细粒度安全控制，整体来说压到服务节点的流量被有效降低了，不知道这样子理解正确否

展开 ▼

作者回复: 可以这样做，网关依赖安全服务



AmosWooo

2018-10-29



李老师，请教个问题：API网关提供认证授权功能，那请求穿透API网关这一层之后，后续的业务流程依然会涉及在多个子服务之间交互，此时如何授权呢？难道需要反向去API网关查询吗？谢谢回答

作者回复: 网关是针对外部系统的认证授权，内部系统如果要做权限控制，一般放在配置中心做，因为独立做内部的认证系统代价比较高

