涂鸦科技：支撑从零暴增数十亿数据的背后，竟无专职运维！

原创：场景研读 云栖社区 2016-03-28

3月23日云栖社区在线实时分享顺利结束，本次由涂鸦科技技术总监柯都敏分享了涂鸦科技云上架构设计和借助阿里云实现轻运维高可用性监控的实战经验，同时也介绍了网络安全、权限控制等特定场景下如何利用阿里云产品解决特定的问题题。本次视频直播的整理文章完毕，如下内容。

直播预告
3月29日直播：《有货：基于混合云架构的高可用实践》

随着有货电商业务的高速发展，为了应对电商平台流量爆发式增长，由此对系统进行大规模重构，开始微服务加混合云的探索，从传统的单 IDC演变为“IDC+公共云”混合云架构，从单一的全站应用演变为微服务架构，通过多级缓存、分流与限流、自动监控及故障恢复、弹性伸缩、服务降级等一 系列措施，多维度提升系统性能与可用性。

分享者：李健，有货CTO

分享时间：3月29日，10:00–11:00

扫一扫，快速报名

架构演变历程

初创公司的团队刚起步时一般规模都不是很大，并且成员能力各异，而且为了公司的长远发展，初始的架构需要设计的尽可能优秀。因此在设计时需要考虑到架构性能、扩展、代码安全、测试等等问题。

图一 第一代轻架构

在涂鸦科技设计第一代架构时，业务量并不是很大。在设计之初，对整个架构进行了简单的拆分，基础服务层内存放的是公共的资源，为以后的其他业务作支撑；为了保障网络接

口的安全性，同时为了缩短开发周期，在架构上封装了Atop网关层，在网关层内完成接口配置、接口的访问控制、数据转换、统一日志等操作。

开发人员只需要将精力集中于业务层开发，业务层向上提供服务。网关层通过配置化来调用业务接口。当接受到外部请求时，通过网关层进行协议转换、数据转换，再通过配置中心来对业务接口进行调度，业务层返回的数据再通过网关层转换，返回给原请求者。第一代架构仅仅使用一个库和一台主机，并且该架构是分布式架构，但在最初时整合到一个工程使用本地调用。

第一代架构实现了前后端的完全分离，使得前端的效率大大提升；同时业务通过网关暴露，后端的效率也随着提升；此外公共的技术模型的统一封装，降低了上手成本；在安全风险方面，通过网关的统一授权和用户模型特征验证，降低了安全风险；接口配置化部署实现上午提需求，下午就可以联调，满足产品的要求。

图二 第二代平行架构

第一代轻架构几乎没有做性能评估，也没有对数据库做分表。随着业务量的增加，数据库压力逐渐增大。第二代架构中，同样进行了拆分分层，相对于第一代架构，网关层几乎不存在改动，实现风险可控。中间层进行模块化拆分，服务化治理方面采用阿里的Dubbo，同时也进行了一些对应的改进，使其更加适应用于网关层，通过配置中心动态配置生效。

同时使用Dubbo monitor对服务进行监控，同时自行开发了服务化治理的调用依赖等。目前，涂鸦科技内部服务已经有十几种之多。数据库方面，通过涂鸦科技自行开发数据库中间件，实现路由、分库分表、主从备份等操作。

通过对架构的优化，第二代架构对业务有了更好的支撑。数据方面，目前可以处理日峰值30T数据上传；可以运行几十亿用户核心数据；支持实时日志搜索和分析报警以及支持离线和实时数据处理。

模块化方面，对业务服务模块化拆分，做到可独立发布部署；同时服务治理工具可分析服务调用情况按需扩容；通过性能和可用性监控，及时发现技术瓶颈，同时支持服务热发布。

网关方面，通过网关隔离内外数据；同时采用网关服务组装业务场景，使得模块颗粒更细化；除此之外，网关提供了多种安全机制支持多业务场景；网关可以进行平行扩展，并且没有性能瓶颈；网关作为统一的数据出入口，可以方便进行日志分析跟踪。

中间件方面，通过自主开发数据组件支持分库分表、主从读写等操作；同时对Mq等中间服务封装，便于架构选型；此外架构中尽量多的使用阿里云来减少维护成本。同时通过配置中心，满足了网关接口的实时更新的需求。

涂鸦在云上

图三 涂鸦科技云上架构

上图是涂鸦科技在云上的架构场景。从图上可看，该架构几乎采用了所有的阿里云产品。前端通过SLB将流量引入，根据业务不同对SLB进行拆分，根据业务流量不同，调用不同的SLB，尽可能使得不同的业务各自可进行扩容。

同时，流量入口可动态配置，当一个SLB无法承受流量压力时，后续的流量会转移到其他SLB上，做到动态扩展。通过ECS搭建的网关集群和业务集群可实现平行扩展和热扩展。

在整个架构的高可用方面，流量入口通过SLB实现高可用；网关层通过对多组机器的SLB监控和自主监控，当有业务发布时，通过SLB对脚本的监控，对一些机器做下线操作，当服务上线再将流量导通到这些机器上，做到流量热迁移；业务层通过服务模块化，当业务量压力增加时，可以采用动态加机做到高可用性。

数据库容灾备份方面，核心数据库采用主从配置，无需将大流量的数据放在主库上，主库上主要处理写操作，备份主要采用阿里云的RDS的默认定时备份机制，同时在数据量方面做了大量的异步处理，通过Cache和队列将数据进行异步化处理。

图四 云产品使用场景

上图是阿里云产品在涂鸦科技的一个使用场景。由于业务数据增加较快，单RDS接近瓶颈，同时IOPS高数据库IO高，峰值突然出现服务慢，必须进行数据迁移。当时的选择可以使自行开发进行迁移，但时间成本较高，至少需要一个人一周才能完成。当时恰逢阿里云数据迁移服务DTS对外公测，如果仅对数据进行读写操作时，风险很小，通过DTS对数据的迁移，增加了数据存储空间，同时IOPS也急速下降，平稳度过了风险。

图五 云产品使用经验

涂鸦科技通过使用阿里云服务，有很多的收获经验。首先在RAM权限，从最初使用阿里云时的五个具有全部权限的超级Key到现在不同的客户端使用不同的Key，隐藏超级Key，采用RAM自定义权限细化到每个用户，通过对业务拆分减少了安全风险。

其次在云监控技巧，通过对ECS、RDS、OCS等常规监控，如何出现报警时，可以做到及时的修改。通过自定义监控服务的存活情况，由于自定义监控的信息量有限，后期又开发了自主监控，监控信息内加上日志分析出来的链接地址，如果有报警情况出现时，可用过该链接地址准确找到问题所在。通过SLB进行内部服务管理，首先SLB内网免费使用，十分灵活。前端Nodejs服务器调用后端API时，通过SLB搭建内网，避免内网服务器更换、下线时带来的不可用性。

此外，还通过SLB管理ZooKeeper集群，无需对代码进行变更，避免了风险。OSS方面，通过OSS的图片服务降低了成本，还可以通过OSS管理内部的运维小工具，通过OSS的Python的Client自主化运维一些服务器。

经验分享

图六 基于ECS安全组的权限控制

涂鸦科技不仅在架构中使用阿里云服务，同时在很多的项目中也使用了阿里云服务。例如基于ECS安全组的权限控制，在ECS安全组没有上市前，采用的是在每台机器上部署防火墙方式，在不同的服务器上部署的防火墙规则也不同，当需要修改防火墙时，需要上机处理，十分繁琐，通过ECS安全组，将相应的防火墙规则进行梳理，比如可以将所有的日志分析服务器添加到日志分析服务安全组内，十分灵活。另外安全组内可进行内网通信，阿里云自带的安全组和自定义的安全组之间也进行了打通。

图七 基于ECS API的主机管理和高可用监控

上图是基于ECS API的主机管理和高可用监控流程图，目前RAM权限还是比较广，很多服务还不支持。涂鸦科技基于ECS API自行开发一套工具。这套工具可以获取机器列表和信息（RAM权限），然后通过主机Tag管理给每台机器打上Tag，不同的开发人员只能接触与之对应的机器。通过Tag标记，可以使得主机按需管理，批量运维，同时还可以根据Tag类型做对应的可用性监控。

通过对所有数据的实时分析，利用Tag的标记来明确服务的类型，基于服务类型来调用分析结果。比如可以分析出网关在一定时间内的错误量，以及网络的响应时间等信息。如果错误量或响应时间超过一定的阀值，可以进行自动化报警，无需人工，开发人员通过报警提供的URL地址快速定位问题的所在。

相对于亚马逊，阿里云在网络访问时间、稳定性、使用成本、技术支持更有优势。

QA问答环节

1. 作为技术人员，可以分享下这几年的创业经验吗?

> 创业这一段时间感触颇大，在公司时更专注于做自己的事情，对其他知识了解不多，比较安分。创业时，不仅要着重提高自己的技术，同时还需要关注团队的发展，将整个链路连接起来，成长很大。

2. 一个完美的架构应该经历哪些发展过程的?

> 个人认为没有最完美的架构，最适合业务的架构就是最好的，比如说刚开始处于一台机器上的架构，成本最低，对当时来说，就是最完美的架构。

3. 目前你的团队内有多少运维人员?

> 目前团队中没有专职运维人员，运维是我自己在兼职做。

关于分享者

柯都敏，涂鸦科技技术总监。近10年互联网从业经历，曾任职阿里巴巴，2014年9月加入涂鸦科技，5个月完成涂鸦科技第一二代技术架构，平稳支撑涂鸦一年从零到几十亿数据快速发展。

涂鸦科技，一家专业的智能硬件解决方案提供商，以云平台为核心、软硬件结合的方式提供智能生活服务，安全快速稳定地推进中国制造业转型升级，促进传统产业“互联网+”有效深入的融合，“中国制造”转型“中国智造”。基于涂鸦智能的一站式硬件智能化解决方案，厂商只需要专注于自己最擅长的领域，最大化提升硬件品质，让产品更具竞争力，给用户更好的体验。目前涂鸦科技旗下拥有涂鸦智能硬件平台和自有软硬件产品。2015年获得了NEA千万美元A轮投资。

阅读原文