阿里云
通用解决方案

游戏行业解决方案

文档版本：20181211

法律声明

阿里云提醒您在阅读或使用本文档之前仔细阅读、充分理解本法律声明各条款的内容。如果您阅读或使用本文档，您的阅读或使用行为将被视为对本声明全部内容的认可。

1. 您应当通过阿里云网站或阿里云提供的其他授权通道下载、获取本文档，且仅能用于自身的合法合规的业务活动。本文档的内容视为阿里云的保密信息，您应当严格遵守保密义务；未经阿里云事先书面同意，您不得向任何第三方披露本手册内容或提供给任何第三方使用。
2. 未经阿里云事先书面许可，任何单位、公司或个人不得擅自摘抄、翻译、复制本文档内容的部分或全部，不得以任何方式或途径进行传播和宣传。
3. 由于产品版本升级、调整或其他原因，本文档内容有可能变更。阿里云保留在没有任何通知或者提示下对本文档的内容进行修改的权利，并在阿里云授权通道中不时发布更新后的用户文档。您应当实时关注用户文档的版本变更并通过阿里云授权渠道下载、获取最新版的用户文档。
4. 本文档仅作为用户使用阿里云产品及服务的参考性指引，阿里云以产品及服务的”现状“、“有缺陷”和“当前功能”的状态提供本文档。阿里云在现有技术的基础上尽最大努力提供相应的介绍及操作指引，但阿里云在此明确声明对本文档内容的准确性、完整性、适用性、可靠性等不作任何明示或暗示的保证。任何单位、公司或个人因为下载、使用或信赖本文档而发生任何差错或经济损失的，阿里云不承担任何法律责任。在任何情况下，阿里云均不对任何间接性、后果性、惩戒性、偶然性、特殊性或刑罚性的损害，包括用户使用或信赖本文档而遭受的利润损失，承担责任（即使阿里云已被告知该等损失的可能性）。
5. 阿里云网站上所有内容，包括但不限于著作、产品、图片、档案、资讯、资料、网站架构、网站画面的安排、网页设计，均由阿里云和/或其关联公司依法拥有其知识产权，包括但不限于商标权、专利权、著作权、商业秘密等。非经阿里云和/或其关联公司书面同意，任何人不得擅自使用、修改、复制、公开传播、改变、散布、发行或公开发表阿里云网站、产品程序或内容。此外，未经阿里云事先书面同意，任何人不得为了任何营销、广告、促销或其他目的使用、公布或复制阿里云的名称（包括但不限于单独为或以组合形式包含”阿里云”、Aliyun”、“万网”等阿里云和/或其关联公司品牌，上述品牌的附属标志及图案或任何类似公司名称、商号、商标、产品或服务名称、域名、图案标示、标志、标识或通过特定描述使第三方能够识别阿里云和/或其关联公司）。
6. 如若发现本文档存在任何错误，请与阿里云取得直接联系。

通用约定

格式	说明	样例
	该类警示信息将导致系统重大变更甚至故障，或者导致人身伤害等结果。	 **禁止：** 重置操作将丢失用户配置数据。
	该类警示信息可能导致系统重大变更甚至故障，或者导致人身伤害等结果。	 **警告：** 重启操作将导致业务中断，恢复业务所需时间约10分钟。
	用于补充说明、最佳实践、窍门等，不是用户必须了解的内容。	 **说明：** 您也可以通过按**Ctrl** + **A**选中全部文件。
>	多级菜单递进。	设置 > 网络 > 设置网络类型
粗体	表示按键、菜单、页面名称等UI元素。	单击 **确定**。
`courier` 字体	命令。	执行 `cd /d C:/windows` 命令，进入Windows系统文件夹。
斜体	表示参数、变量。	`bae log list --instanceid` *`Instance_ID`*
[]或者[a|b]	表示可选项，至多选择一个。	`ipconfig` *`[-all|-t]`*
{}或者{a|b}	表示必选项，至多选择一个。	`swich` *`{stand | slave}`*

目录

1 游戏行业防DDoS攻击解决方案

1.1 行业综述

根据全球游戏和全球移动互联网行业第三方分析机构Newzoo的数据显示：2017年上半年，中国以275亿美元的游戏市场收入超过美国和日本，成为全球榜首。

游戏行业的快速发展、高额的攻击利润、日趋激烈的行业竞争，让中国游戏行业的进军者们，每天都面临业务和安全的双重挑战。

游戏行业一直是竞争、攻击最为复杂的一个江湖。 曾经多少充满激情的创业团队、玩法极具特色的游戏产品，被互联网攻击的问题扼杀在摇篮里；又有多少运营出色的游戏产品，因为遭受DDoS攻击，而一蹶不振。

DDoS攻击的危害

阿里云安全发布的2017年上半年的游戏行业DDoS攻击态势报告中指出：2017年1月至2017年6月，游戏行业大于300G以上的攻击超过1800次，攻击最大峰值为608G；游戏公司每月平均被攻击次数高达800余次。

目前，游戏行业因DDoS攻击引发的危害主要集中在以下几点：

- 90%的游戏业务在被攻击后的2-3天内会彻底下线。
- 攻击超过2-3天以上，玩家数量一般会从几万人下降至几百人。
- 遭受DDoS攻击后，游戏公司日损失可达数百万元。

为什么游戏行业是DDoS攻击的重灾区？

据统计表明，超过50%的DDoS和CC攻击，都在针对游戏行业。游戏行业成为攻击的重灾区，主要有以下几点原因：

- 游戏行业的攻击成本低，几乎是防护成本的1/N，攻防两端极度不平衡。

  随着攻击方的手法日趋复杂、攻击点的日趋增多，静态防护策略已无法达到较好的效果，从而加剧了这种不平衡。
- 游戏行业生命周期短。

  一款游戏从出生到消亡，大多只有半年的时间，如果抗不过一次大的攻击，很可能就死在半路上。黑客也是瞄中了这一点，认定只要发起攻击，游戏公司一定会给保护费。
- 游戏行业对连续性的要求很高，需要7×24小时在线。

因此如果受到DDoS攻击，很容易会造成大量的玩家流失。在被攻击的2-3天后，玩家数量从几万人掉到几百人的事例屡见不鲜。

- 游戏公司之间的恶性竞争，也加剧了针对行业的DDoS攻击。

游戏行业的DDoS攻击类型

- 空连接

  攻击者与服务器频繁建立TCP连接，占用服务端的连接资源，有的会断开、有的则一直保持。空连接攻击就好比您开了一家饭馆，黑帮势力总是去排队，但是并不消费，而此时正常的客人也会无法进去消费。

- 流量型攻击

  攻击者采用UDP报文攻击服务器的游戏端口，影响正常玩家的速度。用饭馆的例子，即流量型攻击相当于黑帮势力直接把饭馆的门给堵了。

- CC攻击

  攻击者攻击服务器的认证页面、登录页面、游戏论坛等。还是用饭馆的例子，CC攻击相当于，坏人霸占收银台结账、霸占服务员点菜，导致正常的客人无法享受到服务。

- 假人攻击

  模拟游戏登录和创建角色过程，造成服务器人满为患，影响正常玩家。

- 对玩家的DDoS攻击

  针对对战类游戏，攻击对方玩家的网络使其游戏掉线或者速度慢。

- 对网关DDoS攻击

  攻击游戏服务器的网关，导致游戏运行缓慢。

- 连接攻击

  频繁的攻击服务器，发送垃圾报文，造成服务器忙于解码垃圾数据。

1.2 游戏安全痛点

- 业务投入大，生命周期短

  一旦出现若干天的业务中断，将直接导致前期的投入化为乌有。

- 缺少为安全而准备的资源

游戏行业玩家多、数据库和带宽消耗大、基础设施资源准备时间长，而安全需求往往没有被游戏公司优先考虑。

- 可被攻击的薄弱点多

  网关、带宽、数据库、计费系统都可能成为游戏行业攻击的突破口，相关的存储系统、域名DNS系统、CDN系统等也会遭受攻击。

- 涉及的协议种类多

  难以使用同一套防御模型去识别攻击并加以防护，许多游戏服务器多用加密私有协议，难以用通用的挑战机制进行验证。

- 实时性要求高，需要7×24小时在线

  业务不能中断，成为DDoS攻击容易奏效的理由。

- 行业恶性竞争现象猖獗

  DDoS攻击成为打倒竞争对手的工具。

1.3 如何判断已遭受DDoS攻击

假定已排除线路和硬件故障的情况下，突然发现连接服务器困难、正在游戏的用户掉线等现象，则说明您很有可能是遭受了DDoS攻击。

目前，游戏行业的IT基础设施一般有 2 种部署模式：一种是采用云计算或者托管IDC模式，另外一种是自行部署网络专线。无论是前者还是后者接入，正常情况下，游戏用户都可以自由流畅地进入服务器并进行游戏娱乐。因此，如果突然出现以下几种现象，可以基本判断是被攻击状态：

- 主机的IN/OUT流量较平时有显著的增长。
- 主机的CPU或者内存利用率出现无预期的暴涨。
- 通过查看当前主机的连接状态，发现有很多半开连接；或者是很多外部IP地址，都与本机的服务端口建立几十个以上的ESTABLISHED状态的连接，则说明遭到了TCP多连接攻击。
- 游戏客户端连接游戏服务器失败或者登录过程非常缓慢。
- 正在进行游戏的用户突然无法操作、或者非常缓慢、或者总是断线。

1.4 为什么选择阿里云

- 资源统一管理

  面对快速发展的游戏业务，需要高效进行游戏运维和资源管理。

- 阿里云超大规模数据中心遍布全球。
- 统一账号进行游戏运维和资源管理。
- 全球统一的售前售后服务体系加本地化服务。

- 稳定的国际网络连通

  稳定、低延时的网络是让分布于全球不同国家/地区的玩家能顺畅地体验游戏、并进行公平PK的关键。

  - 高速通道打通阿里云全球数据中心，形成全球一张网。
  - 网络质量SLA保障、超低延时。

- 完善的产品支撑

  游戏行业的安全防护需要设计合理的逻辑架构和物理部署方案以满足业务的安全需求，需要有成熟的安全产品体系支撑。

  - 全套的游戏行业安全参考架构和部署方案。
  - 完整的安全产品体系帮助解决游戏行业各种类型的DDoS攻击问题。

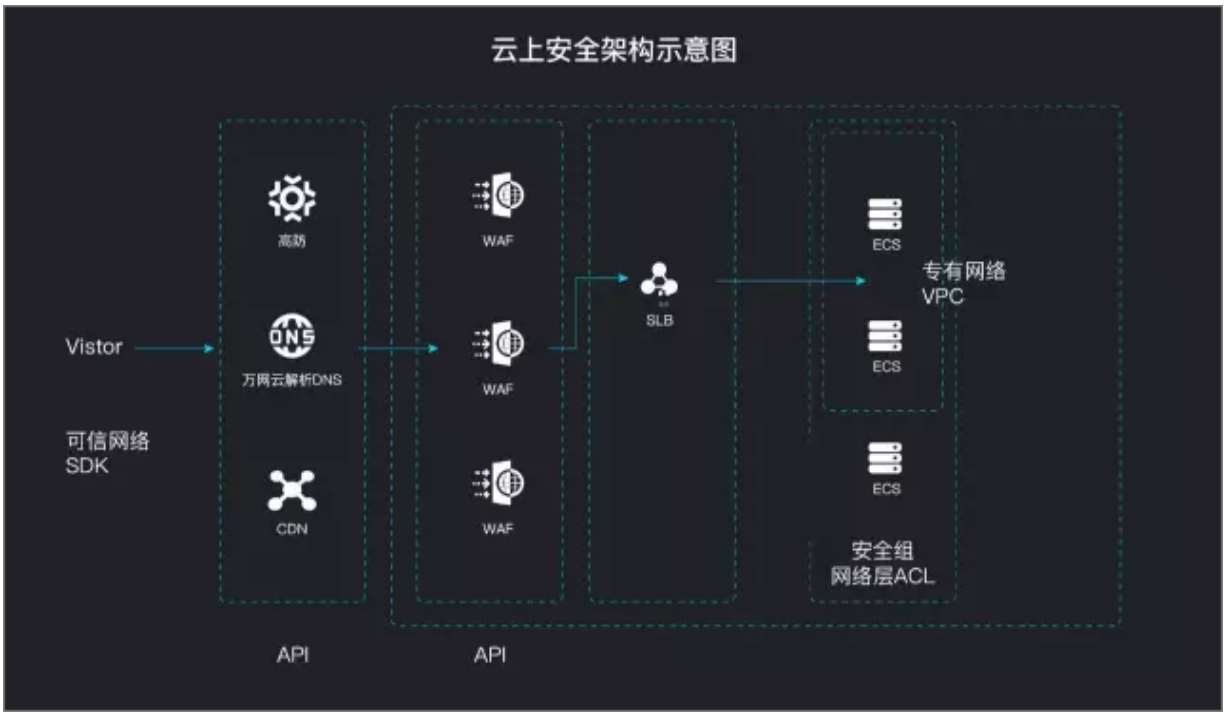
1.5 DDoS攻击缓解最佳实践

目前，有效缓解DDoS攻击的方法可分为 3 大类：

- 架构优化
- 服务器加固
- 商用的DDoS防护服务

架构优化

在预算有限的情况下，建议您优先从自身架构的优化和服务器加固上下功夫，减缓DDoS攻击造成的影响。



- 部署**DNS**智能解析

  通过智能解析的方式优化DNS解析，有效避免DNS流量攻击产生的风险。同时，建议您托管多家DNS服务商。

  - 屏蔽未经请求发送的DNS响应信息

    典型的DNS交换信息是由请求信息组成的。DNS解析器会将用户的请求信息发送至DNS服务器中，在DNS服务器对查询请求进行处理之后，服务器会将响应信息返回给DNS解析器。

    但值得注意的是，响应信息是不会主动发送的。服务器在没有接收到查询请求之前，就已经生成了对应的响应信息，这些回应就应被丢弃。

  - 丢弃快速重传数据包

    即便是在数据包丢失的情况下，任何合法的DNS客户端都不会在较短的时间间隔内向同一DNS服务器发送相同的DNS查询请求。如果从相同IP地址发送至同一目标地址的相同查询请求发送频率过高，这些请求数据包可被丢弃。

  - 启用TTL

    如果DNS服务器已经将响应信息成功发送了，应该禁止服务器在较短的时间间隔内对相同的查询请求信息进行响应。

对于一个合法的DNS客户端，如果已经接收到了响应信息，就不会再次发送相同的查询请求。每一个响应信息都应进行缓存处理直到TTL过期。当DNS服务器遭遇大量查询请求时，可以屏蔽掉不需要的数据包。

- 丢弃未知来源的DNS查询请求和响应数据

  通常情况下，攻击者会利用脚本对目标进行分布式拒绝服务攻击（DDoS攻击），而且这些脚本通常是有漏洞的。因此，在服务器中部署简单的匿名检测机制，在某种程度上可以限制传入服务器的数据包数量。

- 丢弃未经请求或突发的DNS请求

  这类请求信息很可能是由伪造的代理服务器所发送的，或是由于客户端配置错误或者是攻击流量。无论是哪一种情况，都应该直接丢弃这类数据包。

  非泛洪攻击 (non-flood) 时段，可以创建一个白名单，添加允许服务器处理的合法请求信息。白名单可以屏蔽掉非法的查询请求信息以及此前从未见过的数据包。

  这种方法能够有效地保护服务器不受泛洪攻击的威胁，也能保证合法的域名服务器只对合法的DNS查询请求进行处理和响应。

- 启动DNS客户端验证

  伪造是DNS攻击中常用的一种技术。如果设备可以启动客户端验证信任状，便可以用于从伪造泛洪数据中筛选出非泛洪数据包。

- 对响应信息进行缓存处理

  如果某一查询请求对应的响应信息已经存在于服务器的DNS缓存之中，缓存可以直接对请求进行处理。这样可以有效地防止服务器因过载而发生宕机。

- 使用ACL的权限

  很多请求中包含了服务器不具有或不支持的信息，可以进行简单的阻断设置。例如，外部IP地址请求区域转换或碎片化数据包，直接将这类请求数据包丢弃。

- 利用ACL，BCP38及IP信誉功能

  托管DNS服务器的任何企业都有用户轨迹的限制，当攻击数据包被伪造，伪造请求来自世界各地的源地址。设置一个简单的过滤器可阻断不需要的地理位置的IP地址请求或只允许在地理位置白名单内的IP请求。

  同时，也存在某些伪造的数据包可能来自与内部网络地址的情况，可以利用BCP38通过硬件过滤清除异常来源地址的请求。

- **部署负载均衡**

  通过部署负载均衡（SLB）服务器有效减缓CC攻击的影响。通过在SLB后端负载多台服务器的方式，对DDoS攻击中的CC攻击进行防护。

  部署负载均衡方案后，不仅具有CC攻击防护的作用，也能将访问用户均衡分配到各个服务器上，减少单台服务器的负担，加快访问速度。

- **使用专有网络**

  通过网络内部逻辑隔离，防止来自内网肉鸡的攻击。

- **提供余量带宽**

  通过服务器性能测试，评估正常业务环境下能承受的带宽和请求数，确保流量通道不止是日常的量，有一定的带宽余量可以有利于处理大规模攻击。

服务器加固

在服务器上进行安全加固，减少可被攻击的点，增大攻击方的攻击成本：

- 确保服务器的系统文件是最新的版本，并及时更新系统补丁。
- 对所有服务器主机进行检查，清楚访问者的来源。
- 过滤不必要的服务和端口。例如，**WWW**服务器，只开放80端口，将其他所有端口关闭，或在防火墙上做阻止策略。
- 限制同时打开的SYN半连接数目，缩短SYN半连接的timeout时间，限制SYN/ICMP流量。
- 仔细检查网络设备和服务器系统的日志。一旦出现漏洞或是时间变更，则说明服务器可能遭到了攻击。
- 限制在防火墙外与网络文件共享。降低黑客截取系统文件的机会，若黑客以特洛伊木马替换它，文件传输功能无疑会陷入瘫痪。
- 充分利用网络设备保护网络资源。在配置路由器时应考虑以下策略的配置：流控、包过滤、半连接超时、垃圾包丢弃，来源伪造的数据包丢弃，SYN 阀值，禁用ICMP和UDP广播。
- 通过iptable之类的软件防火墙限制疑似恶意IP的TCP新建连接，限制疑似恶意IP的连接、传输速率。
- 识别游戏特征，自动将不符合游戏特征的连接断开。
- 防止空连接和假人攻击，将空连接的IP地址直接加入黑名单。

- 配置学习机制，保护游戏在线玩家不掉线。例如，通过服务器搜集正常玩家的信息，当面对攻击时，将正常玩家导入预先准备的服务器，并暂时放弃新进玩家的接入，以保障在线玩家的游戏体验。

商用的DDoS防护服务

针对超大流量的攻击或者复杂的游戏CC攻击，可以考虑采用专业的DDoS解决方案。目前，通用的游戏行业安全解决方案做法是在IDC机房前端部署防火墙或者流量清洗的一些设备，或者采用大带宽的高防机房来清洗攻击。

当宽带资源充足时，此技术模式的确是防御游戏行业DDoS攻击的有效方式。不过带宽资源有时也会成为瓶颈：例如单点的IDC很容易被打满，对游戏公司本身的成本要求也比较高。

您可根据自己的预算和遭受攻击的严重程度，来决定采用哪些安全措施。

1.6 DDoS攻击解决方案——游戏盾

游戏盾是阿里云针对游戏行业面对的DDoS、CC攻击推出的具有针对性的网络安全解决方案，相较与高防IP，除了能针对大型DDoS攻击（T级别）进行有效防御外，还具备彻底解决游戏行业特有的TCP协议的CC攻击问题能力，防护成本更低，效果更好！

2017年3月29日，阿里云云盾在深圳云栖大会发布了游戏行业安全风控新模式：游戏盾。游戏盾在风险治理方式、算法技术上全面革新，帮助游戏行业用户用更低的成本缓解超大流量攻击和CC攻击，解决以往的攻防框架中资源不对等的问题。

与传统单点防御DDoS防御方案相比，游戏盾用数据和算法来实现智能调度，将正常玩家流量和黑客攻击流量快速分流至不同的节点，最大限度缓解大流量攻击；通过端到端加密，让模拟用户行为的小流量攻击也无法到达客户端。

同时，在传统防御中，黑客很容易锁定攻击目标IP，在攻击过程中受损非常小。而游戏盾的智能调度和识别，可让用户隐形，让黑客显形 —— 每一次攻击都会让黑客受损一次，攻击设备和肉鸡不再重复可用。颠覆以往DDoS攻防资源不对等的状况。

游戏盾的前世今生

游戏盾从诞生之初到现在，经历了3次重大的技术变革。从初代的云层，到现在的游戏盾，无论是从技术架构还是从功能实现上，都发生了翻天覆地的变化。

而驱动这些变化的浅层因素，是攻防资源的不对等问题；深层因素则是对现有网络本身的路由规则和基础设施的深度思索。

简单来说，游戏盾通过风控模式调度流量来撬动攻防天平；而从本质来说，游戏盾更像是一个除了路由和DNS之外，能够再次改变流量走向的存在。

- 云层：第一次实验

  游戏盾的前身是云层项目。它诞生在2015年初的一次营救实验。

  一家公司遭受黑客的反复攻击，传统的DDoS防御方法已全部败下阵来。在紧急情况下，公司向阿里云安全团队寻求合作，并提出可以尝试一种**通过快速流量调度，来躲避黑客攻击**的新方法。

  当时，这种方法并没有在任何实战场景中被验证过。阿里云DDoS防护安全技术团队在**摸着石头过河**的情况下，与用户的技术团队一起合作，将这种新的防护方法付诸于实践，成功扛下了一次次攻击。

  云层时代也就此开始。

  当时，黑客的攻击手法相对来说比较单一，找到目标IP地址，通过一波大流量（10~50GBps）攻击将IP打进黑洞。而黑客发动下一波攻击的准备时间大约需要10~15分钟。而云层通过秒级分布式IP的快速调度，压制了黑客的分钟级攻击跟随，赢得了这场竞赛的阶段性胜利。

  接下来，云层模式在其它几场攻防实战中屡立战功。但与此同时，新形态的攻击方式也在不断地进化，云层尽管实现了秒级的IP调度速度，但要跟上黑客的嗅探和跟随，其算法和效率仍然需要进化。在这种背景下，游戏盾的时代来了！

- 游戏盾：正式踏入战场

  一直以来，国内超过50%的DDoS和CC攻击，都是针对游戏行业。因此，游戏成了DDoS攻防最好的战场，也是调度算法的最佳训练场。

  于是，阿里云安全团队决定将云层时代积累下来的技术经验，应用在游戏行业中，成为所有用户能够用得上、并且管用的风控模式。

  在游戏盾诞生之前的很长一段时间，阿里云安全团队对游戏行业的攻防对抗模式反复分析，深入了解了游戏业务的注册特点、登录特点、玩家特点，并在此基础上重构了游戏盾的智能调度算法。

  游戏盾继承了云层快速调度的能力，又通过对端信息的采集、和对网络通信等行为进行归一化的处理分析。基于云上的资源和特性，游戏盾得以对海量的端数据进行计算、处理和存储。相比线下环境，借助云计算平台在计算和数据处理上的优势，阿里云取得了实质性的突破——完成对每一个终端设备的画像，并最终沉淀为**端威胁值**这一新的调度因子。

游戏盾所有数据处理的核心是空中流量调度系统（AirTraffic Control ，ATC），它以深度机器学习（DL）和神经网络（LSTM）为认知基础，将恶意用户快速隔离在调度体系之外。

在游戏行业炮火重重的前线上，游戏盾完成了涅槃重生，并在最猛烈的攻击之下不断进行自我升级。同时，威胁识别和影响面控制代替调度成为了新的技术关键词。

- 精细化和分层而治：领先一小步

  当然，这仍只是一个开始。攻击方也在逐步加重自己的兵力投入。想要领先黑客一小步，光靠数据和算法还不够，需要真正了解对方的攻击趋势和攻击手法。

  在实战的磨砺中，游戏盾正式踏入精细化攻防对抗这一领域：NetGuard应运而生。借助前2个阶段所积累的AI建模分析能力，游戏盾向针对业务层的攻击发起挑战。

  游戏盾通过串行学习特定业务数据特征，快速识别畸形和突发的异常流量，并在干路上进行阻截。与此同时，阿里云安全团队提出了由用户层、网络层、接入层和业务层4级联动的立体防护体系，让游戏盾帮助用户搭建最适合自己的安全架构。

  游戏盾的立体防护体系的核心，在于分层而治。首先，大流量攻击依托网络层去解决；而技巧型CC攻击通过接入层去解决。立体防护体系可以达到突破带宽限制，控制攻击影响范围和时间，精准识别用户行为的目标。

- 倾斜的天平

  从2015到2017，经过2年的攻防实战和技术打磨让游戏盾将一种新的安全风控模式，应用到攻防战场中，帮助游戏行业的用户去解决实质性的问题。

  然而，从云层到游戏盾，只是阿里云安全团队撬动DDoS攻防天平的第一步。真正前进的方向，是构筑一张安全、可信、承载着“干净流量”的网络，并将这张网络延展到更广的边界。

方案简介

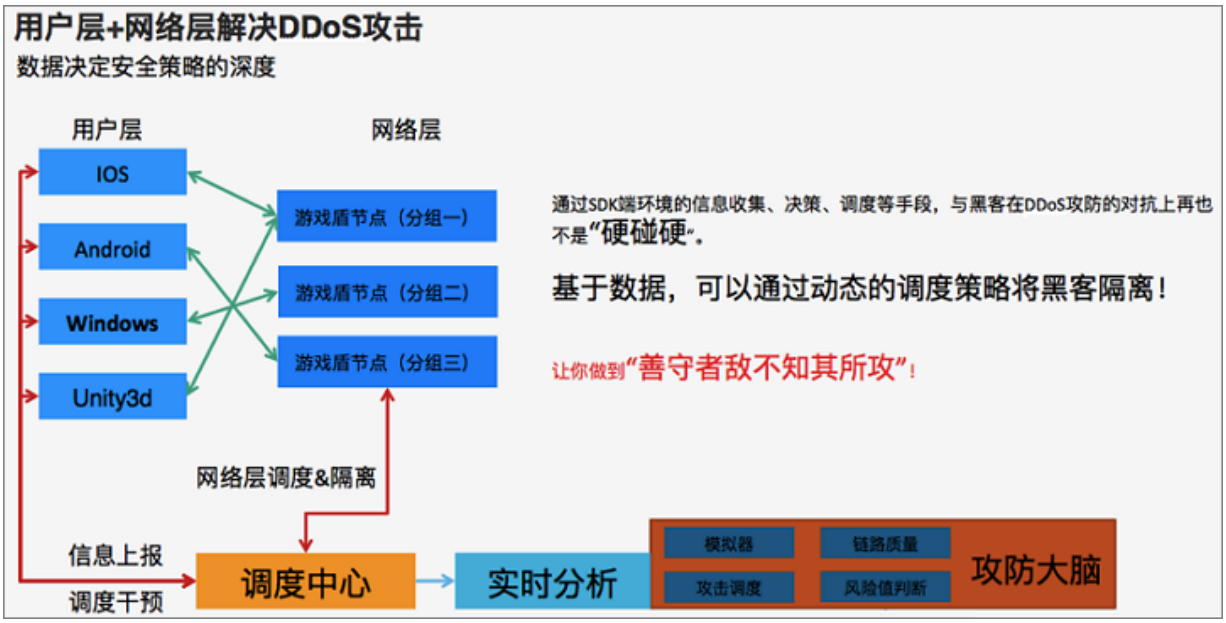
游戏盾是阿里云DDoS高防IP产品系列中针对游戏行业的安全解决方案。游戏盾专为游戏行业定制，针对性解决游戏行业中复杂的DDoS攻击、游戏CC攻击等问题。

游戏盾由 2 大模块组成：

- 分布式抗D节点：通过分布式的抗D节点，游戏盾可以做到防御600G以上的攻击。
- 游戏安全网关：通过针对私有协议的解码，支持防御游戏行业特有的CC攻击。

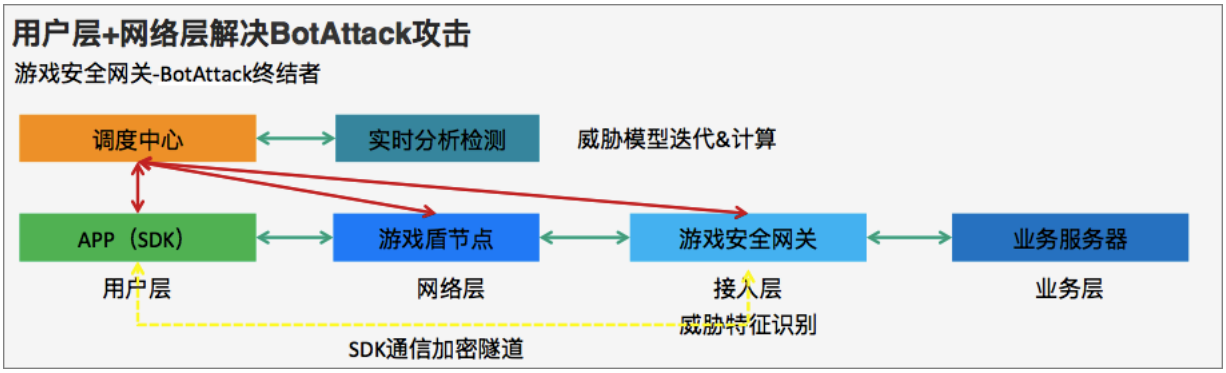
游戏盾如何防御DDoS攻击？

与普通的DDoS高防机房不同，游戏盾并不是通过海量的带宽硬抗攻击，而是通过分布式的抗D节点，将黑客的攻击进行有效的拆分和调度，使得攻击无法集中到某一个点上。同时基于SDK端数据、流量数据，可以通过动态的调度策略将黑客隔离！



游戏盾如何防御CC攻击？

一般来说，游戏行业的CC攻击跟网站的CC攻击不同。网站类的CC攻击主要是基于HTTP或者HTTPS协议，协议比较规范，相对容易进行数据分析和协议分析。但是游戏行业的协议大部分是私有的或者不常见的协议，因此对于CC攻击的防御，阿里云推出了专业的云上防御游戏安全网关（原称NetGuard、简称NG）。



- 游戏安全网关通过在用户业务和攻击者之间建立起一道游戏业务的防火墙，根据攻击者的TCP连接行为、游戏连接后的动态信息、全流量数据，准确分辨出真正的玩家和黑客。
- 游戏安全网关支持大数据分析，根据真实用户业务的特点分析出正常的玩家行为，从而直接拦截异常的客户端。且可以随时针对全国省份、海外的流量进行精确封禁，支持百万级的黑白名单。

- 游戏安全网关可以同SDK建立加密通信隧道，全面接管客户端和服务端的网络通信，仅放行经过SDK和游戏安全网关鉴权的流量。彻底解决TCP协议层的CC攻击。（需SDK版本在5.1.7以上）

方案特点

- **技术革新——智能调度算法拆分流量**

  DDoS攻防的本质，是资源的对抗。从网络、CDN、服务器到数据库，只要存在资源差的地方，就可以有DDoS攻击在发生。

资源类别	用户	黑客
带宽资源	G级别有限的带宽和峰值触发方式的黑洞机制	T级别压倒性带宽资源
肉鸡资源	有限的服务器资源	大数量级领先的肉鸡资源
技术资源	需要防护完整的一个面	只需要击破一个点
资金资源	有限的预算+高昂的防护成本	几乎无成本

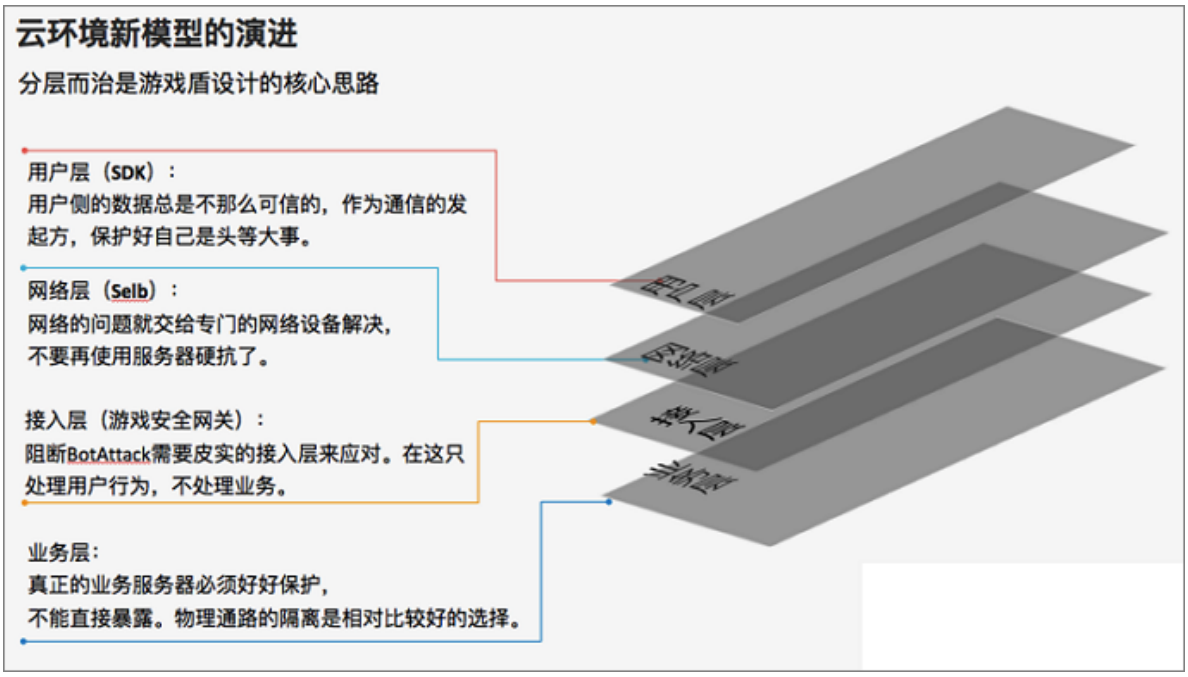
  从云层、弹性安全网络到现在的游戏盾，阿里云安全团队在与游戏行业用户并肩作战几年后，用数据和算法来改变了大流量攻击防御的模式。

  今天，游戏盾在应对黑客攻击的时候，不仅是被动在防御，也具备主动的反击能力。有效识别哪个客户端是黑客、哪个客户端是好的用户，通过更加灵活的调度算法，让用户的正常流量和黑客的攻击流量不往一处走，扛住一次次超大型的DDoS攻击。

- **风控模式革新——从单点防御到分层治理**

  在游戏盾的演进过程中，阿里云安全团队成功平衡了 4 大资源不对等的难题：

  - 如何对抗黑客T级压倒性带宽资源。
  - 如何攻破黑客的肉鸡资源。
  - 如何填补黑客只需要攻点、用户需要防面的鸿沟。
  - 如何解决资金成本的问题。



分层而治，是解决这些问题的基础。所有资源的不对等，都是因为攻击方太容易找到目标，而防御方太容易成为目标。分层而治中的分，代表流量的拆分、业务的拆分和目标的拆分；让攻击者的成本和门槛增大，把用户成本控制到最低；层代表一种漏斗模型。

- 用户层：用户层的数据总是不那么可信的，作为通信的发起方，保护好自己是头等大事。
- 网络层：网络的问题就交给专门的网络设备解决，不要再使用服务器硬扛了。
- 接入层：接入层是为了应对CC攻击而准备的。在这一层，只处理用户行为，不处理业务。
- 业务层：真正的业务服务器必须好好保护，不能直接暴露，物理通路的隔离是相对比较好的选择。

游戏盾改变了DDoS攻防只是拼带宽的传统概念，成为针对游戏行业用户的整体风控方案。在游戏盾的风控理论下，只要您解决好用户端的问题，就可以解决无限大的DDoS攻击，从而达到攻防成本的平衡。

与传统DDoS攻击解决方案对比

对比项	游戏盾	传统DDoS流量清洗机房
游戏行业超大DDoS攻击	摆脱DDoS攻防军备竞赛，专业防御游戏行业超大DDoS攻击。分布式抗D节点优质BGP接入，针对游戏提供高可用的网络环境。	仅能靠一个本地机房，带宽无法扩展，无法防御更大的DDoS攻击。

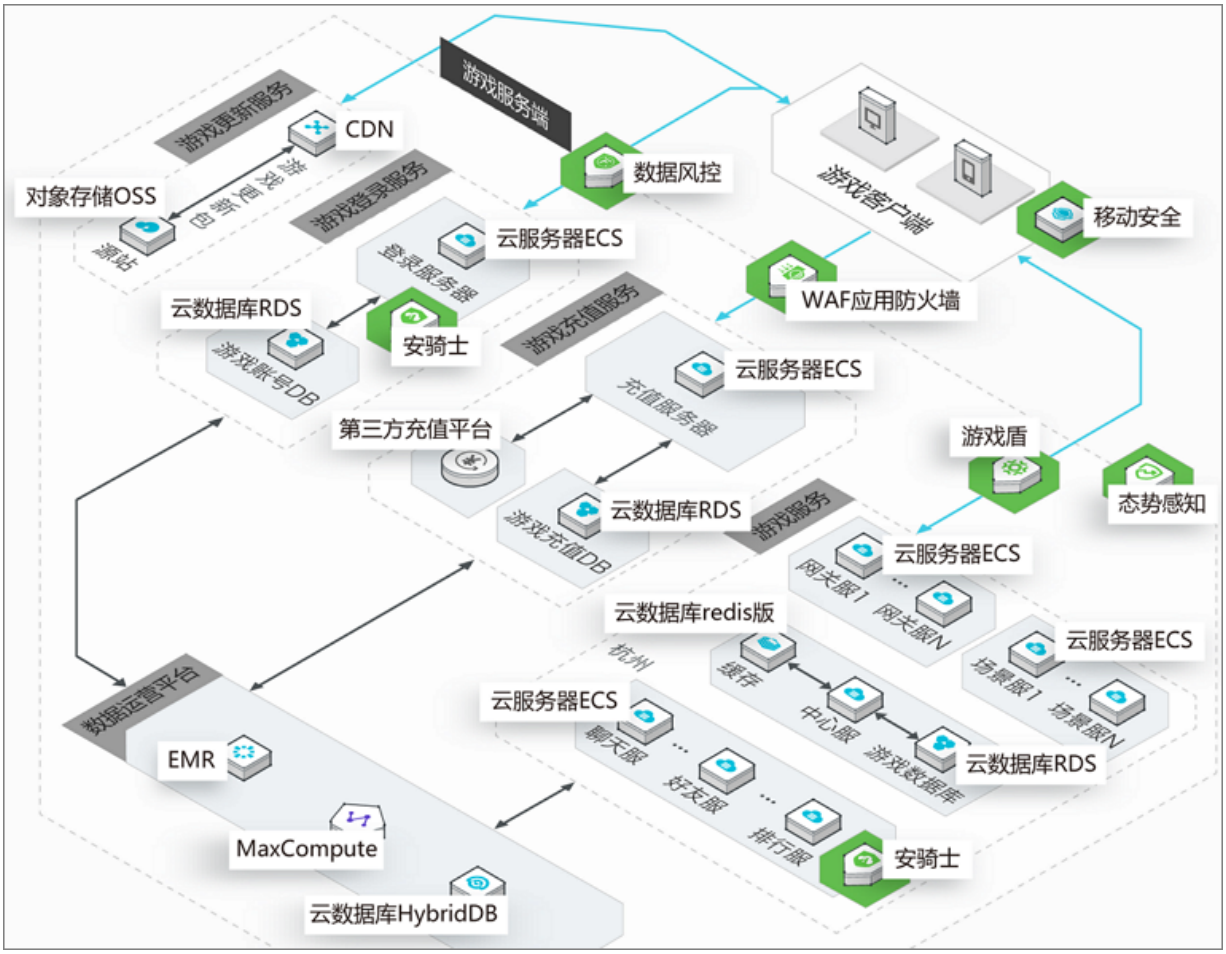
对比项	游戏盾	传统DDoS流量清洗机房
指纹加密、链路加密	支持TCP/UDP/HTTP/HTTPS，适合手游、端游等各类业务场景。支持DDoS，CC，支持云内/云外客户集成游戏SDK，数据报文全链路加密，防黑客破解。端到端的加密，游戏安全接入。支持防护针对模拟游戏协议的攻击。	传统清洗机房仅靠硬件设备来识别，无法解码游戏私有协议。
支持解码游戏私有协议	防护算法实时调整 128 位加密算法。	传统清洗机房仅靠硬件设备来识别，无法解码游戏私有协议。
定制游戏防护算法	防御游戏空连接、慢连接、恶意踢人攻击。防御针对游戏私有协议的CC攻击。全球僵尸网络库、神盾局攻击溯源。	传统机房大多采购防火墙设备或者硬件设备，防御算法更新慢，自身没有调整防御算法的能力。

游戏盾接入说明

- 关于游戏盾SDK接入指南，请点击这里。
- 更多关于游戏盾接入操作的指导视频，参考如下：
  - 如何5分钟配置出游戏安全超强黑科技#
  - 游戏盾的Android-SDK接入
  - 游戏盾的ios-SDK接入
  - 游戏盾的Windows-SDK接入

1.7 全套安全解决方案

阿里云深度分析游戏安全问题，基于阿里巴巴集团海量攻防实战积累，为游戏运营量身打造最全面、最可信的阿里云游戏安全完整解决方案。



该解决方案具有以下特点：

- 全方位安全防护
- 超强防护、实时响应
- 针对游戏、智能调节
- 行业最强安全大数据

本方案能够全面解决游戏行业安全风险，涉及的云产品具体如下：

- 游戏盾：抵御大流量攻击和CC攻击、保障核心用户体验。
- 数据风控&移动安全：人机识别，App加固，预防恶意注册、流量作弊、撞库盗号。
- Web应用防火墙：保障游戏主站及支付服务安全，全面支持HTTPS。
- 安骑士：预防暴力破解、服务器漏洞修复。

- 堡垒机：资源分级授权管理，运维更安全。
- 态势感知：利用机器学习还原已发生的攻击，预测未发生的攻击，扩大安全可见性。
- 先知：加入先知平台的安全众测服务，帮助游戏公司全面发现业务漏洞及风险。

1.8 云安全产品介绍

数据风控

除DDoS攻击之外，游戏行业另一大安全威胁就是欺诈作弊，包括：

- 垃圾注册：玩家大量注册小号，获取新号奖励和刷金币。
- 流量作弊：渠道商利用模拟器等手段批量挂机，进行流量作弊，获取非正常利益。
- 游戏盗号：攻击者利用自动化工具，通过扫库撞库等方式进行盗号。

然而，这些安全威胁会直接导致游戏公司耗费大量心血设计的游戏平衡遭到破坏，从而大大降低玩家体验、导致用户流失。因此，在游戏安全解决方案中，数据风控是必不可少的安全产品之一。

Web应用防火墙

游戏公司的官方网站页面是游戏的门户，也是游戏公司推出活动的宣传窗口，同时大多游戏公司也会在网站中提供社区功能供玩家进行交流。因此，对于游戏官方网站的安全防护也必不可少。另外，部分游戏直接以网页的形式（页游）供玩家进行游玩，对于这种情况，Web应用的防护更是重中之重。

移动安全

游戏行业另一大安全威胁是破解、外挂，包括客户端破解和伪造数据包等风险。

- 游戏破解

  破解客户端游戏程序，免费获得游戏内购，改变游戏设定。

- 内挂

  通过破解游戏和数据包结构，逆向出或直接调用发包函数，改变正常游戏数据，实现超出正常玩家的水平和能力。

- 脱机挂

  完全脱离游戏客户端程序，但可以与游戏服务器自由通讯的外挂程序。此类外挂对游戏的危害最大，严重破坏游戏平衡，缩短游戏运营周期。无论是手游还是端游在被破解之后都可以做外挂，还能够通过破解协议报文模拟数据并发送到服务器上去，消耗游戏的资源使得正常玩家也无法进行游戏。

这类安全威胁，对游戏公司整体的安全架构的各方面来说都是巨大的挑战。首先对于游戏客户端程序，需要具有明确的安全代码开发规范，保障客户端程序安全的健壮性。同时，数据包在客户端与游戏服务器之间的传输过程中必须采用加密传输；并且在服务器端也需要部署完善的安全措施和安全能力。

首先针对客户端，手游客户端的安全问题随着移动游戏行业的大热，已经成为游戏公司不得不重视的关键点。

安骑士

加固移动客户端的安全之后，您更需要全面加固服务器端的安全能力，保障游戏业务的安全稳定。服务器经常面临着各类漏洞、木马后门、异常登录等威胁，而任何一项风险事件被恶意攻击者利用都意味着用户信息、账号数据、游戏数据等可能泄露或被恶意篡改。

堡垒机

随着游戏的内容更新、新版本的发布，承载着游戏运行的这些服务器上经常会进行各类操作。
同时，游戏服务器的运维也需要大批人员进行操作，一旦某个操作出现失误，往往带来巨大的损失，比如紧急停服维护在各类游戏运营过程中都司空见惯。因此，对于游戏服务器上的操作需要慎之又慎，并且需要完善的服务器审计进行监控和记录，便于第一时间发现误操作，并对经常出现的失败操作进行分析改进。

态势感知

游戏行业遭受的恶意攻击往往错综复杂，在被动采取各种安全防护措施之后，如何能够主动发现、预知攻击，才是更为领先的防御理念。不再仅仅是头痛医头脚痛医脚的传统安全解决思路，而将整个安全数据进行整体分析，从更全面的角度看待自己当前面临的安全威胁，并预知可能发生的安全攻击。

安全管家

不同的游戏环境、不同的游戏运营方式可能存在着不同的漏洞，借助专家群众的力量去发现自身全链路的安全问题，才是互联网思路的解决方式。

1.9 客户案例

案例一

游戏公司 A，其主要游戏业务是地方棋牌游戏，刚开始时发展非常迅速，但是却在2016年5月和6月份时被DDoS攻击打击得非常惨烈，使得其业务基本上无法开展并且接近倒闭边缘。

这时，阿里云向该游戏公司提供了游戏行业安全解决方案，并且将安全解决方案应用到了其整个游戏攻防体系中去。在4月份到11月份期间，经历了 2 次大型的攻击对抗。

第一次对抗发生在安全解决方案部署完成之后，黑客很快发现仅靠大流量攻击完全打不下来，于是黑客开始破解游戏客户端，将游戏客户端破解之后就发现了游戏客户端中对于流量调度的原理，这样就能够把所有的 IP 防护节点全部找出来，之后对于找出的节点进行逐个打死。阿里云在第一轮对抗中做的就是将应用进行加密，并将逻辑进行混淆，这样就使得黑客难以在同一时间发现更多的节点的IP地址，而最多一次只能获取一个节点的IP。

在第二轮攻防中，黑客发现使用大流量攻击无法打下来，但是使用CC攻击却非常有效，于是他们使用CC攻击的手法去攻击登录服务，当登录服务受到攻击时就发现防御能力急剧下降，即便其他的游戏节点都正常也是无济于事，不能起到任何作用，所以阿里云此时推出了游戏安全网关的CC防护能力，使用游戏安全网关的CC防护之后即便是 500 万QPS也能够轻松防御。

案例二

2016年2月，游戏公司B在一个月的时间内连续被攻击了多次，并且攻击流量超过了 400 G，而这个流量在2016年初时是非常高的，公司B同样也快被打挂了，此时阿里云帮助其启用了高防+游戏盾的安全解决方案，同时帮助该公司实现了态势感知和溯源，也帮其找到了在背后进行攻击的黑客并通过游戏公司报警，阿里云提供证据最后将犯罪嫌疑人捉拿归案，这也是反击能力的体现。

很多游戏公司被攻击之后往往是打不还手的，其实并不是因为游戏公司脾气好，而是往往通常情况下游戏公司并不知道到底谁在发起攻击，所以如果客户拥有了溯源的能力就可以找到在背后对自己发起攻击的那个人并将其绳之以法，同时也将会为自己的业务赢得一定时间的安全发展时机。

1.10 总结与展望

本文档从行业背景、DDoS攻击分析、常用缓解DDoS攻击方法、阿里云游戏盾DDoS攻击解决方案以及阿里云游戏安全整体解决方案等多个方面进行了阐述，旨在为游戏行业的客户提供全面的安全解决方案。

阿里云游戏行业DDoS攻击解决方案——游戏盾，是阿里云的人工智能技术与调度算法在安全行业中的成功实践。

随着攻防进程的推进，网络层和接入层逐步壮大，游戏盾的风控模式，会逐步延展到各个行业中，建立起一张安全、可信的网络。在这张网络中，传输着干净的流量，而攻击被前置到网络的边缘处。所有的端，在接入这张网络时，都会经过风险控制的识别，同时网内的风控系统，也让恶意攻击者无法访问到他锁定的资源。

未来，以资源为基础的DDoS防护时代终将被打破，推出对DDoS真正免疫的风控架构，而这不仅仅局限于游戏行业。

1.11 售前咨询

- **7×8** 小时售前咨询电话：**95187-1**。
- 专业的售前团队已经做好准备，随时为您提供全面的售前服务支持。
- 您还可以进入游戏安全解决方案在线官网进行全方位的咨询和了解。
- 阿里云专业的售前咨询团队为您提供全方位的购买咨询/配置推荐/价格方案等1对1的贴心服务。

2 MMO类游戏解决方案

行业综述

随着游戏行业市场的发展，休闲类、卡牌类游戏已经无法满足玩家对高品质游戏的追求，同时移动终端硬件配置也在飞速提升，满足了MMO RPG（Massively Multiplayer Online Role Playing Game）、MOBA（Multiplayer Online Battle Arena）等中重度游戏运行对硬件的要求，越来越多的MMO类型产品随之诞生。

MMO类型端游产品也同步向手游产品领域进军，这也标志着云服务未来要承载越来越多此类游戏后端服务器的支撑工作，合理的平台架构是系统稳定运行和业务保障的基础。

目前，游戏产品同质化现象严重，游戏厂商已经从爆发式增长时代逐步回归理性，未来将走精品化路线、走全球化路线，一线大厂以及部分有实力的新晋厂商将在这一轮严峻的洗牌中存活下来，未来MMO类游戏在精品化游戏中将持续扮演非常重要的角色。

技术难题

- 大带宽高包量

  由于MMO类型游戏一般都希望可以尽量做大视野，且其核心玩法基础是移动和战斗，要求同屏间玩家互相实时可见，大量的移动包和战斗包都是需要在视野内进行广播。

  该玩法背景下，若MMO游戏服务器拥有较多的玩家同时在线时，会产生大量的通信包，这就要求MMO游戏服务器的接入层需要具备充足的网络带宽和较高的网络包吞吐能力。

- 资源弹性伸缩

  MMO类手游、页游具有轻游戏和时间碎片化的特点，这种短平快的行业特性，需要最大化地节约和利用游戏服务器资源，高效地完成MMO游戏服务器开服、合服，尤其是在页游场景尤为明显地情况下。

- 高计算能力

  对于MMO类型的网游，游戏策划们希望通过玩家之间的强交互来吸引更多的玩家，所以需要尽可能地提高单区玩家的同时在线数。单区最高玩家同时在线数一般要求能够达到数千，所以MMO类型的网游属于强交互强校验类型，对游戏服务器的计算能力有比较高的要求。

- 就近接入

  MMO类型游戏往往会采用分区、分服和跨地域多中心等就近部署的模式，让游戏玩家通过就近接入方式连接游戏服务器，保证游戏流畅性，提升游戏体验。

为什么选择阿里云？

- 顶级基础设施
  - 自建5A机房，全球16大IDC中心，BGP独享带宽，千G光纤接入，全球1200+CDN节点。
  - 借助阿里云遍布全球的自有数据中心和高速通道服务，轻松实现全球同服，形成全球一张网，单控制台秒级部署国内海外资源。
- 完善的产品支撑
  - 完整的产品线体系，满足各类业务场景的需求。
  - 丰富的实例类型，满足各类技术场景对实例规格及性能指标的需求。
- 支持高主频实例

  提供多种主频类型实例，满足各类场景对CPU计算能力的差异化需求。
  - 满足复杂游戏逻辑对计算时效性的要求。
  - 满足老端游架构对单核处理速度的要求。
- 高网络吞吐能力

  提供高网络吞吐类型ECS实例，100W以上pps吞吐能力，满足各类高包量场景的需求。
  - 满足多人同屏消息广播场景对pps能力的要求。
  - 满足公共数据读取时对内网带宽吞吐能力的要求。
- 稳定的计算能力保障

  提供独享型实例，保障持续稳定的计算能力输出。
  - 满足高负载场景对CPU计算能力稳定性的要求。
  - 满足密集型计算场景对计算时效性保障的要求。
- 全球就近接入

  遍布全球的数据中心，满足全球同服基础架构要求，实现玩家就近接入。
  - 保障全球同服玩家访问体验。
  - 解决玩家LastMale问题。
- 优质BGP网络

  多线BGP网络，保障玩家拥有高质量的网络访问体验，解决终端玩家跨运营商网络问题。
- 专业安全防护能力

阿里云集阿里集团十余年的安全攻防经验于一身，提供从客户端、网络层、应用层到基础资源层全链路的安全防护方案。

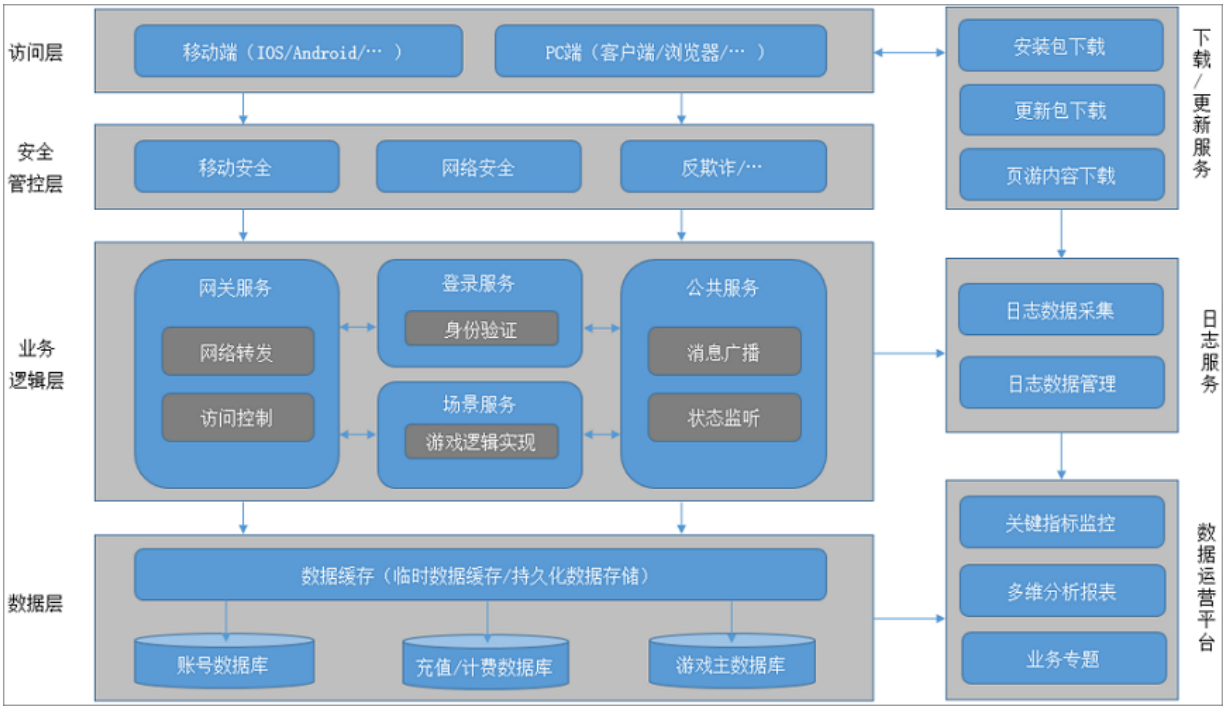
- 解决DDoS、CC等各种类型网络攻击防护问题。
- 解决登录、支付等核心业务平台应用层攻击及渗透问题。
- 通过大数据分析实现安全风险预测。

  阿里云DDoS高防IP构建业内最强游戏安全防护体系，轻松防御百G级别DDoS攻击和各种应用层攻击。

- 高效的运维支撑体系
  - 丰富的产品API大大提升客户运维灵活度及效率。
  - 完善的监控预警体系有效降低运维监控难度。
- 优质的服务体验
  - 全球统一售前售后服务体系加本地化服务支持。
  - 专业的技术服务支持保障响应速度及问题处理效率。

业务功能架构

关于MMO类游戏整体业务的流程和具体业务模块，可参考下图：

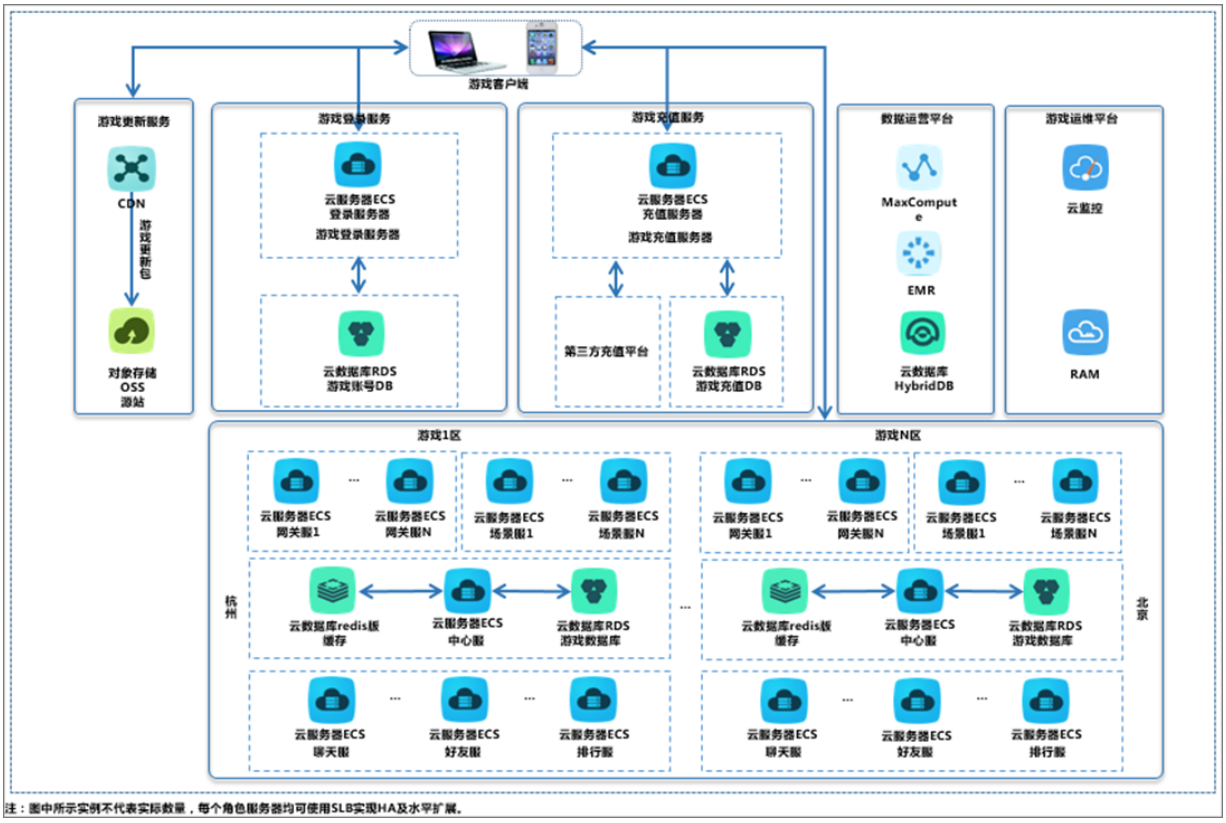


产品架构

MMO通用参考架构方案

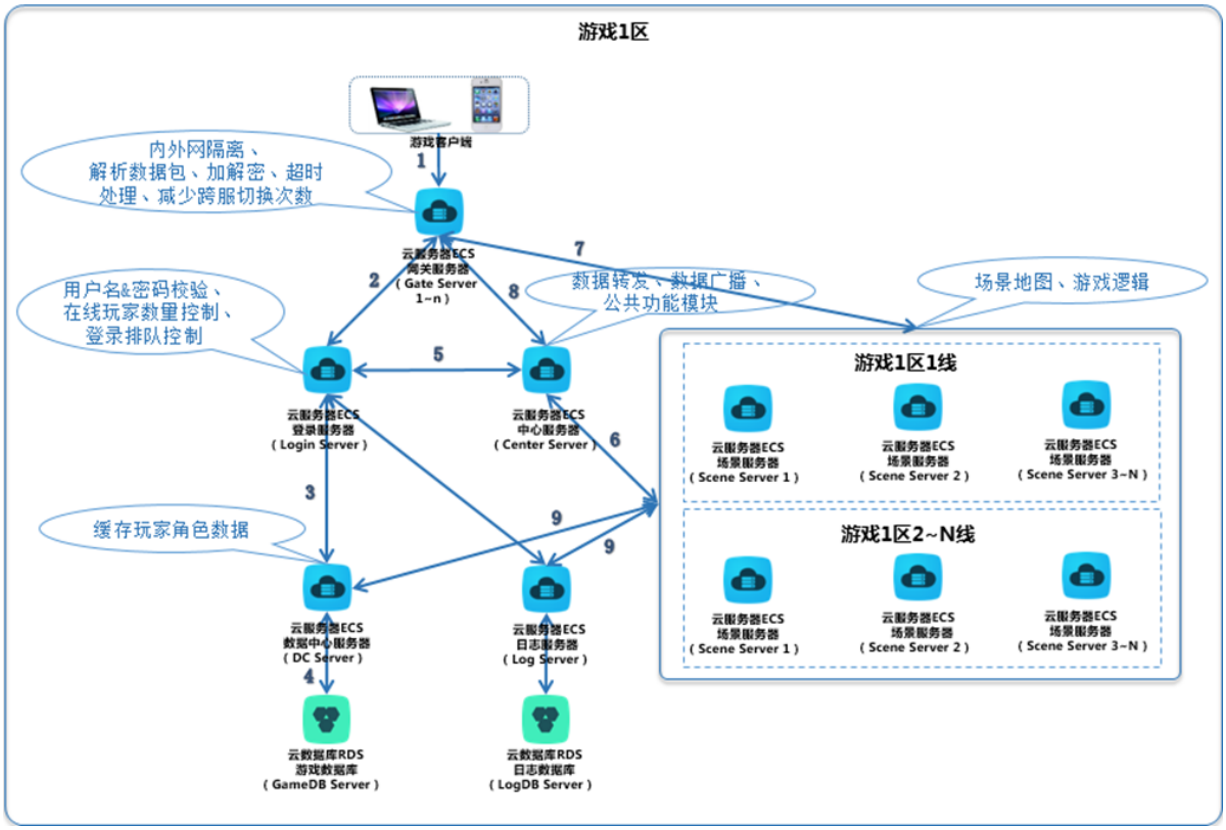
阿里云完整的产品线体系提供了从游戏下载&更新、游戏业务服务器、游戏逻辑服务器、游戏DB服务器、游戏数据运营平台到游戏运维监控平台的全场景解决方案。

通过合理的服务组合及资源配置可以有效提升运维效率，提高业务体验，降低综合运营成本。



MMO类游戏架构—端游

通过阿里云的不同产品来实现整体/某个特定的业务流程，MMO类的端游游戏架构如下所示：



数据交互过程

参见MMO类游戏架构—端游中所示图片，以下将列出图中各编号所代表的具体数据交互意义：

1. 客户端连接Gate Server发起登录请求。
2. Gate Server将登录请求转发给Login Server。
3. Login Server向DC Server发起身份数据验证查询。
4. DC Server访问GameDB Server完成数据查询并返回结果。
5. Login Server若通过身份校验，则继续查询并返回账号状态数据（角色、等级、属性、上次登录所在场景服务器及坐标等信息），登录状态及信息会同步到Center Server。
6. Center Server负责将信息下发给对应场景服务器，同时将玩家上线通知广播给该玩家好友及玩家在线状态监听（控制断线重连及断线超时）。
7. Gate Server收到认证信息后与对应场景服务器建立连接，玩家成功登录到场景服务器。
8. 如果玩家有公共信息需要广播会发请求给Center Server，由Center Server完成消息数据包的广播工作。
9. 场景服务器开始向日志中写入所有客户行为日志，同时将玩家相关数据存储或查询请求发给DC Server。

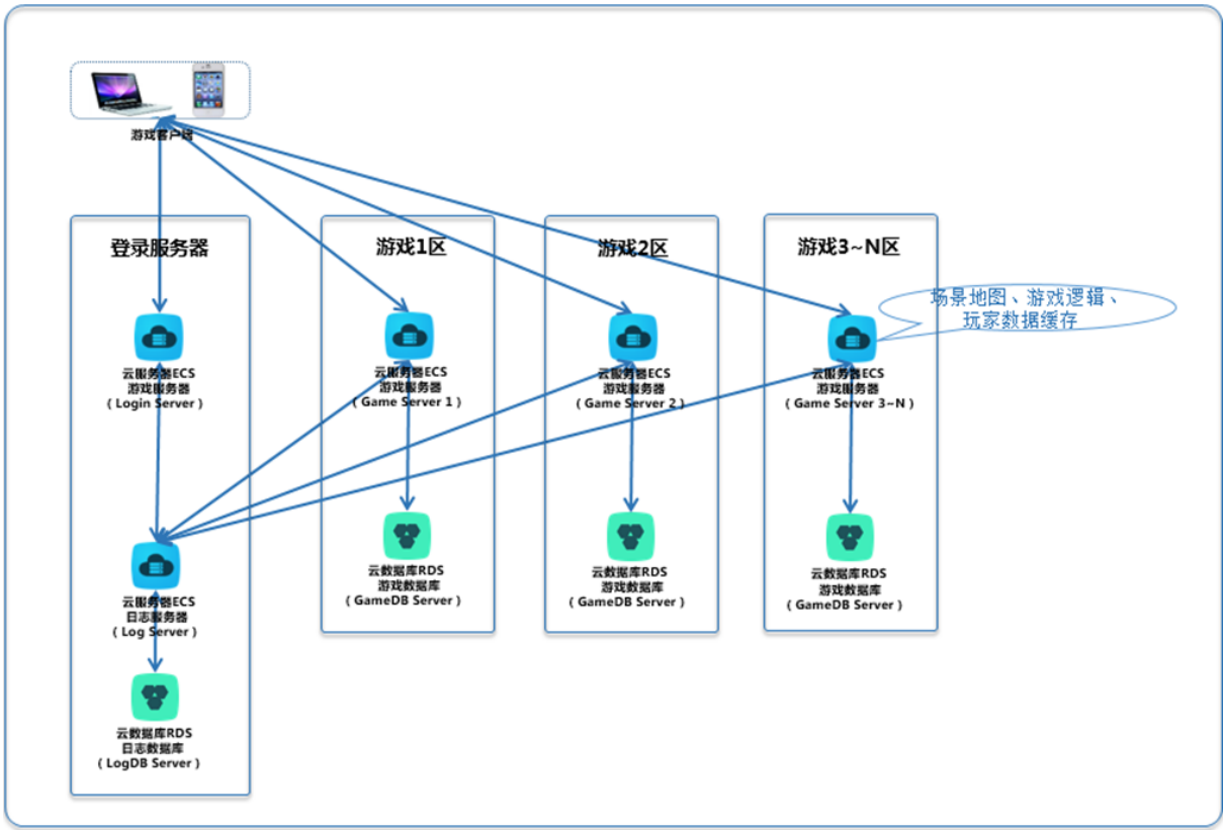
架构特点

MMO类端游游戏的架构特点主要如下所示：

- 网关服务器负责所有网络数据包的转发，通常是网络负载较集中的点，对于网络吞吐能力要求较高。
- 场景服务器包含游戏逻辑，相对依赖CPU处理能力以及一定的网络包转发能力。
- 单个游戏区承载玩家数量过万，逻辑服务器通常按照场景地图来划分，规模再大会通过分线的方式实现。
- 数据中心服务器负责缓存玩家数据并异步入库，保障玩家客户快速获取和写入数据，对于可用性要求较高，需要配合应用层实现数据容错机制。
- 日志服务器承载了大区所有业务行为的日志收集及处理的压力，对磁盘写入性能要求较高，通常采用多台分组方式实现。

MMO类游戏架构—手游

通过阿里云的不同产品来实现整体/某个特定的业务流程，MMO类的手游游戏架构如下所示:



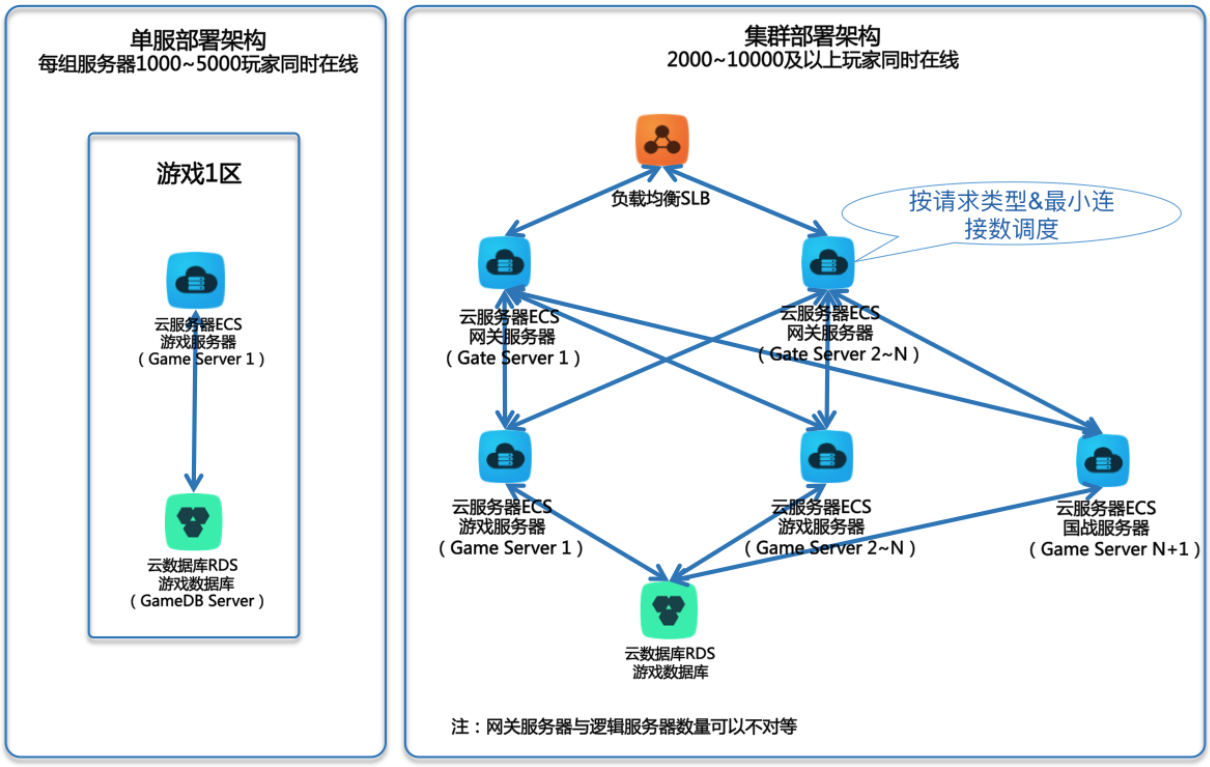
架构特点

MMO类手游游戏的架构特点主要如下所示：

- 手游项目相对端游玩法复杂度较低，生命周期相对较短，结合运营策略及资源经济模型通常采用相对简单的部署架构，少部分大型MMO类手游也会沿用端游部署架构。
- 客户端通常采用与游戏服务器直连的方式，少部分项目在游戏服务器前端设置网关或采用网关与游戏服务器同机部署的方式，相对依赖单台服务器的CPU处理能力以及网络包的转发能力，单个游戏区通常承载1000~5000玩家在线。
- 游戏数据库服务器可以采用与游戏服务器1:1的配比关系，也可以采用多区共用的部署方式。

MMO手游衍生架构

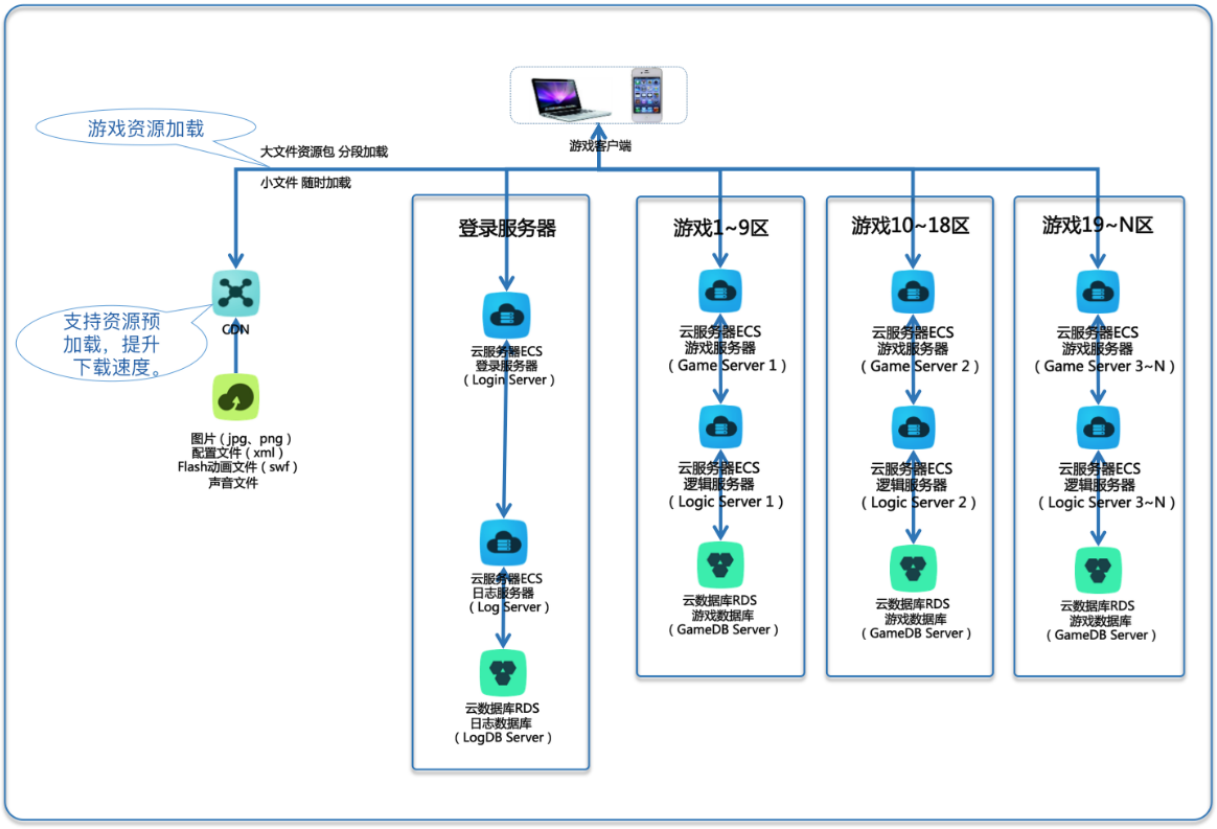
关于MMO的手游衍生架构图具体如下所示：



- 在MMO手游衍生架构中，通过负载均衡及网关服务器将原多台逻辑服务器组建成大服，同服可以承载更多玩家在线，有助于打造玩家生态。
- 通过网关服务器实现玩家请求调度及连接状态监测。
- 国战服务器（或PVP战场服务器）计算性能及负载能力相对要求更高，可以采用高配置实例或独享型实例构建，并由网关服务器统一调度管理。

MMO页游集中部署架构

逻辑服务器层和游戏数据库层采用集中部署方式时，具体架构如下所示：



- 页游整个游戏过程的内容加载依赖CDN，对CDN的稳定性和下载速度有一定的要求。资源加载通常采用大文件资源包分段加载和小文件随时加载2种方式。
- 页游通常采用快速开服、合服的运营策略，短时间内可能开通上千个游戏区，并随着每个区的活跃玩家降低而陆续的合服，通过自定义镜像加自动开服脚本可以实现快速的创建游戏大区及逻辑服务器。
- 页游计算复杂度相对端游、手游较轻，单个游戏区对服务器的计算能力和网络吞吐能力没有特殊要求，通常会采用一机多开的方式，会依据计算负载来决定每台服务器开服的数量。

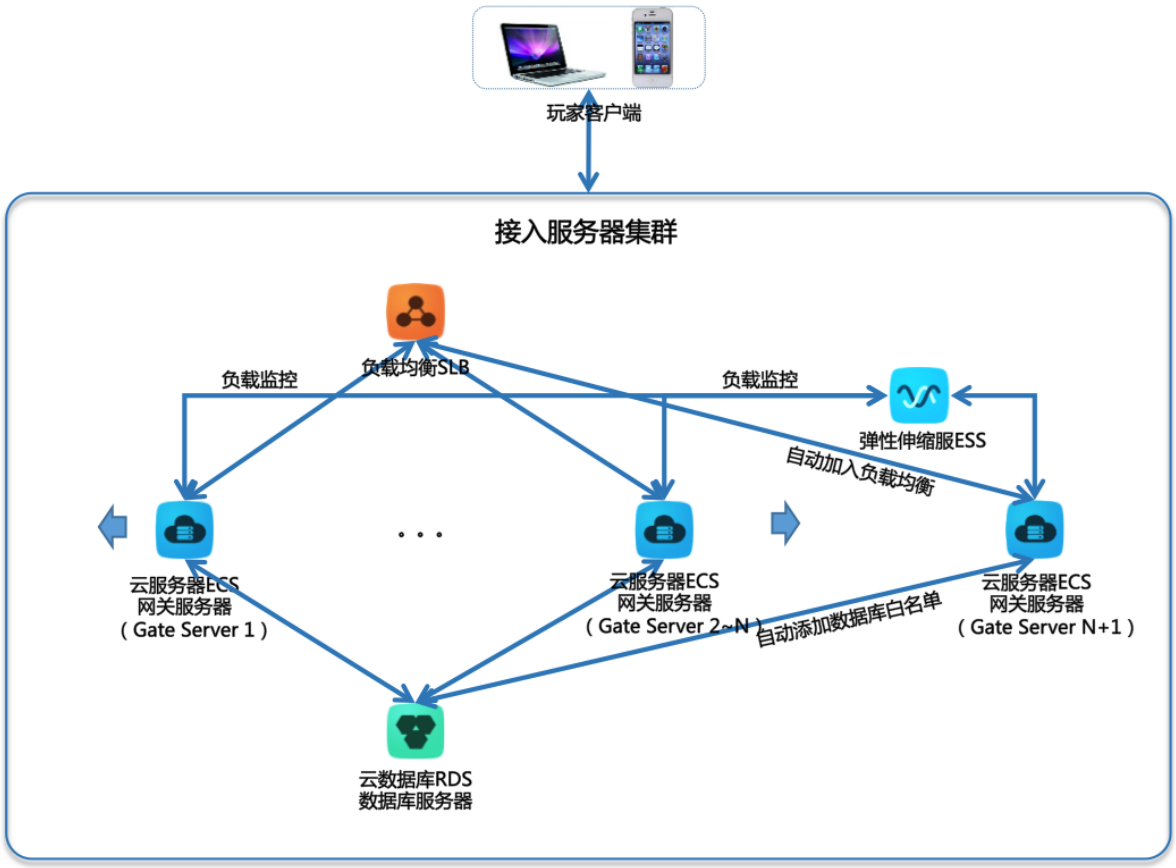
MMO页游分区部署架构

逻辑服务器层和游戏数据库层采用分区部署方式时，具体架构如下所示：

MMO游戏通用技术解决方案

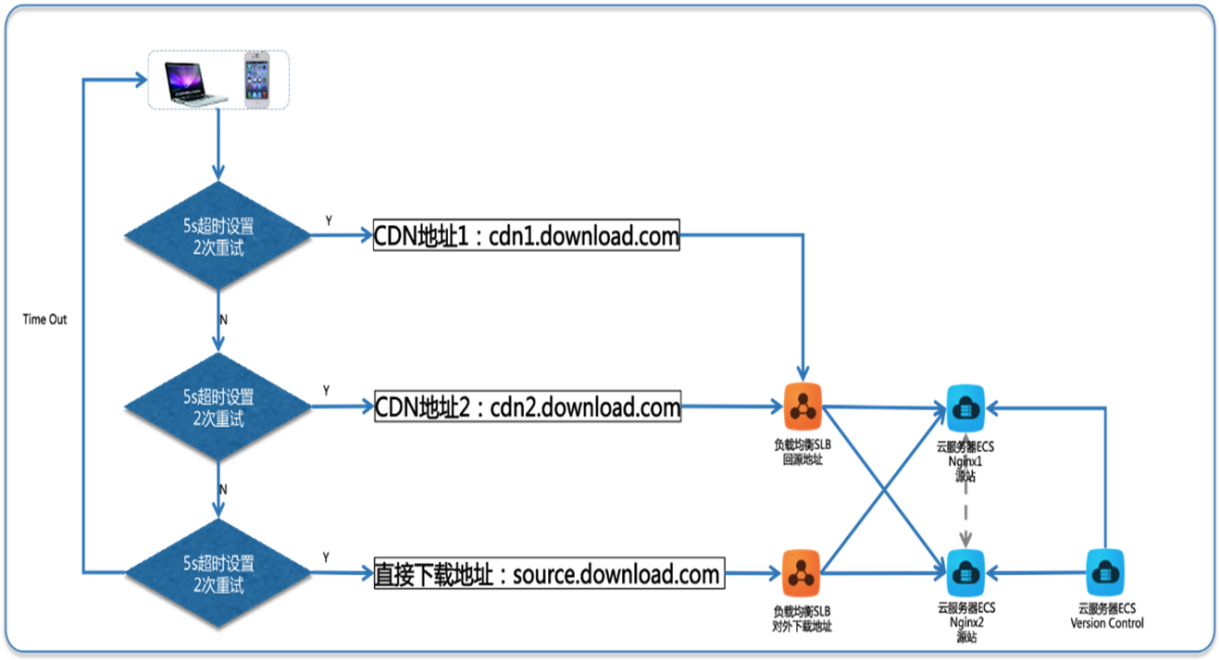
接入层服务器集群弹性扩容&缩容实现

- 接入层服务器集群借助ESS实现自动扩容及缩容，能够有效的应对开机风暴、国战活动高峰等场景，保障服务器集群资源的负载能力。
- 登录服务器或有弹性伸缩需求的服务器同样适用此方案。



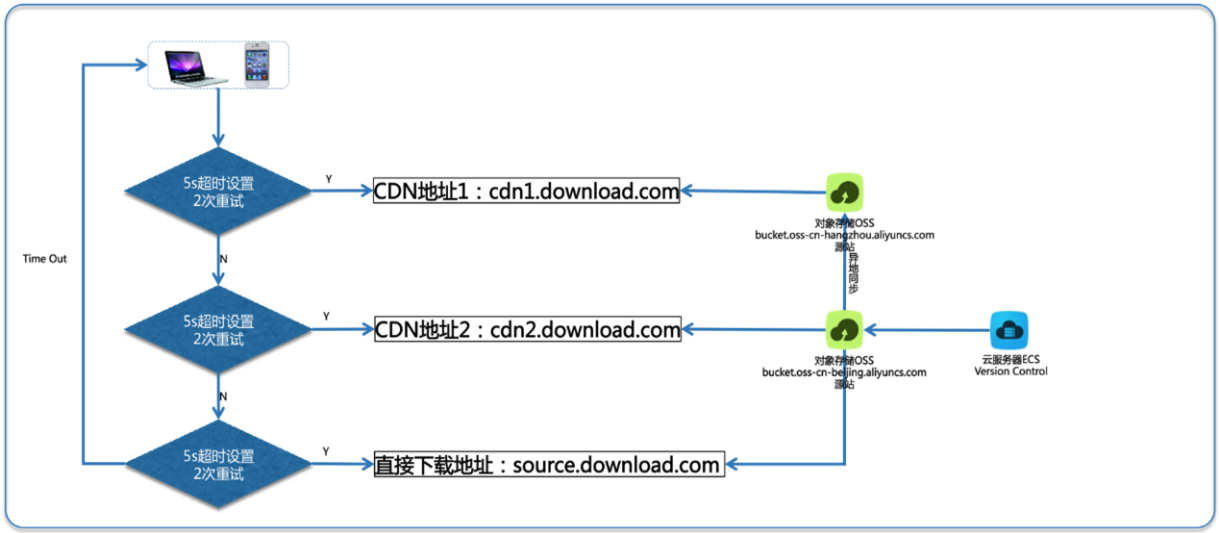
游戏下载&更新高可用实现—ECS自建源站

- 通过多级下载重试，保障下载及更新高可用，降低在此环节的玩家流失比例。
- 通过回源地址与直接对外下载地址分离，规避可能存在的地址暴露安全隐患及SLB不可用情况。
- 多个源站服务器之间的文件实时同步可以使用rsync+inotify实现。



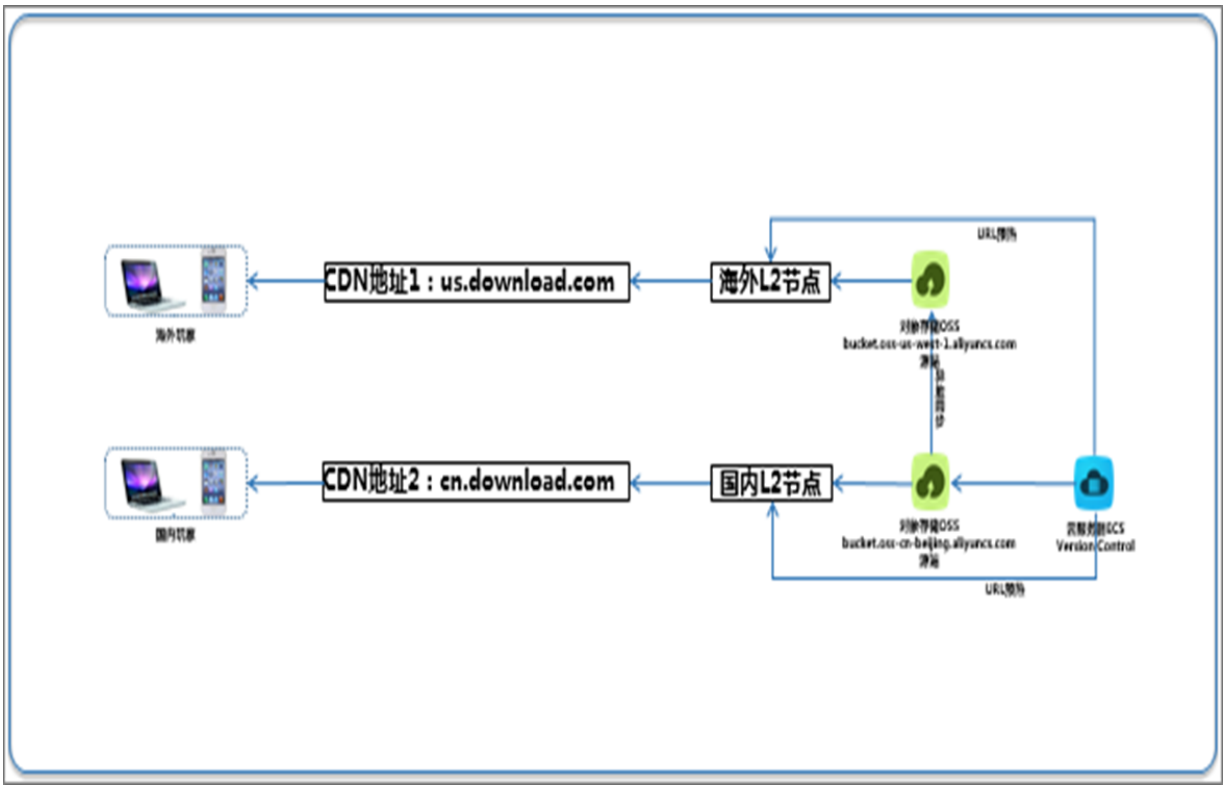
游戏下载&更新高可用实现—OSS源站

- 通过多级下载重试，保障下载及更新高可用，降低在此环节的玩家流失比例。
- 通过回源地址与直接对外下载地址分离，规避可能存在的地址暴露安全隐患。
- 通过设置OSS作为CDN源站，借助OSS异地自动复制功能，进一步提升源站可用性及吞吐能力。



游戏大文件下载&海外回源实现—OSS源站

- 通过在国内和海外分别部署源站，保障回源速度和稳定性。
- 通过OSS跨地域复制实现源站文件自动同步。
- 通过URL预热功能将大文件预热到L2节点，提高首次下载速度同时降低回源次数。



云产品介绍

ECS产品介绍

云服务器 Elastic Compute Service（ECS）是阿里云提供的一种基础云计算服务。您无需提前采购硬件设备，而是根据业务需要，随时创建所需数量的云服务器实例。使用过程中，随着业务的扩展，您可以对云服务器进行扩容磁盘、增加带宽。如果不需要了，您还可以释放资源，节省费用。

云服务器 ECS 实例是一个虚拟的计算环境，包含了 CPU、内存、操作系统、磁盘、带宽等最基础的服务器组件，是 ECS 提供给每个用户的操作实体。

更多参考云服务器*ECS*。

RDS产品介绍

阿里云关系型数据库（Relational Database Service，简称 RDS）是一种稳定可靠、可弹性伸缩的在线数据库服务。

基于阿里云分布式文件系统和高性能存储，RDS支持MySQL、SQL Server、PostgreSQL 和 PPAS（Postgre Plus Advanced Server，一种高度兼容 Oracle 的数据库）引擎，并且提供了容灾、备份、恢复、监控、迁移等方面的全套解决方案。

更多参考阿里云关系型数据库。

Redis产品介绍

云数据库 Redis 版（ApsaraDB for Redis）是兼容开源 Redis 协议标准的、提供持久化的内存数据库服务，基于高可靠双机热备架构及可无缝扩展的集群架构，满足高读写性能场景及容量需弹性变配的业务需求。

通过内存+硬盘的存储方式，云数据库 Redis 版在提供高速数据读写能力的同时满足数据持久化需求。

更多参考云数据库 *Redis*。

大数据计算服务

大数据计算服务(MaxCompute，原名ODPS)是一种快速、完全托管的TB/PB级数据仓库解决方案。MaxCompute向用户提供了完善的数据导入方案以及多种经典的分布式计算模型，能够更快速地解决用户海量数据计算问题，有效降低企业成本，并保障数据安全。

MaxCompute 主要服务于批量结构化数据的存储和计算，可以提供海量数据仓库的解决方案以及针对大数据的分析建模服务。

MaxCompute 的目的是为您提供一种便捷的分析处理海量数据的手段，您可以不必关心分布式计算细节，便可达到分析大数据的目的。

MaxCompute 已经在阿里巴巴集团内部得到大规模应用，例如：大型互联网企业的数据仓库和 BI 分析、网站的日志分析、电子商务网站的交易分析、用户特征和兴趣挖掘等。

更多参考大数据计算服务。

云监控介绍

云监控（CloudMonitor）是一项针对阿里云资源和互联网应用进行监控的服务。云监控服务可用于收集获取阿里云资源的监控指标，探测互联网服务可用性，以及针对指标设置警报。

更多参考云监控。

客户案例

《曙光之战》是由掌游天下自研的一款大型魔幻题材MMORPG手游，以欧式神话作为故事背景，游戏内容的设定十分厚重，坐骑、换装等特色系统基于3D设置，360度自由视角转换。

该游戏通过阿里云提供的上云解决方案形成一套可以有效避免单点故障、支持平滑扩容和支持灵活部署方式的游戏服务器架构。高性能的云服务器（ECS）解决重游戏逻辑对计算能力有较高要求的问题，云数据库（RDS）的只读实例特性有效满足了MMO类型游戏读写分离需求。

总结与展望

MMO类游戏一直是倍受行业关注的游戏产品类型，从原IDC物理机时代到今天的云平台，从原MMO端游发展到后期的手游、页游，众多的技术挑战及创新有待发掘。

本文从MMO类游戏的通用参考架构、MMO端游游戏架构、MMO手游游戏架构以及MMO页游部署架构等多个方面进行了产品架构介绍。同时，针对MMO游戏的通用技术解决方案进行了部分的说明。针对方案中涉及的云产品也进行了简要的阐述。本文虽未能完全涉猎各个场景和细节，希望已有内容能够给客户带来一定的启示。

随着行业和技术的进步，阿里云也在不断打磨各类基础服务、网络服务、安全服务以及大数据服务，持续为客户提供更完整、更稳定、更易用的解决方案。

售前咨询

- **7×8小时售前咨询电话：95187-1**
- 专业的售前团队已经做好准备，随时为您提供全面的售前服务支持。
- 您还可以进入阿里云直播问答解决方案进行全方位的咨询和了解。
- 阿里云专业的售前咨询团队为您提供全方位的购买咨询/配置推荐/价格方案等1对1的贴心服务。