**1、棋牌游戏是安防重灾区，请简列棋牌游戏解决方案中常用的安全防护产品（至少三种）。简要说明为何要选用该产品，以及所选产品的核心功能及优势。**

游戏盾：

选用理由：游戏行业最容易出现DDoS攻击，一旦被DDoS，游戏无法登陆，用户很快就会流失掉。

核心功能：智能调度算法拆分流量；分层而治

优势：防御游戏行业超大DDoS攻击、指纹加密/链路加密、支持解码游戏私有协议、定制游戏防护算法。

云安全中心：

选用理由：游戏服务器容易被黑客攻击，挂马、挖矿等，因此选用云安全中心进行防护。

核心功能：安全告警、漏洞管理、基线配置检查、攻击分析、AK泄密检测、云平台配置检查、日志分析、资产指纹调查等。

优势：安全事件告警和检索；漏洞和基线配置检测；安全风险量化和预测；安全可视化界面；原始日志存储和检索；全量日志分析漏洞扫描：

漏洞扫描：

选用理由：游戏会有各种各样的漏洞，使用漏洞扫描在游戏上线前提前发现漏洞，修补漏洞。

核心功能：全面发现关联资产、深度专业的漏洞扫描、敏感违规违法内容检测、篡改挂马检测、直观的风险扫描报告、辅助风险严重和修复指导。

优势：风险覆盖全、检测准确高、响应速度快、随时随地查

**2、阿里云视频监控-OSS方案，可以给客户带来哪些价值？解答要求：请认真阅读题目，给出至少4点业务价值，并详述理由。**

1.成本较低：智能监控类业务，大多是需要做视频存储和点播的，而且对直播延时要求不苛刻，因此从成本角度考虑建议用0SS存储再播放的方式。

2.可靠性高：采用0SS做视频存储，高可靠，并且可暴增视频业务alwayswriteable。

3.分级存储：采用低频存储IA做冷视频存储，与0SS相结合，形成热、冷二级存储架构，降低存储成本。

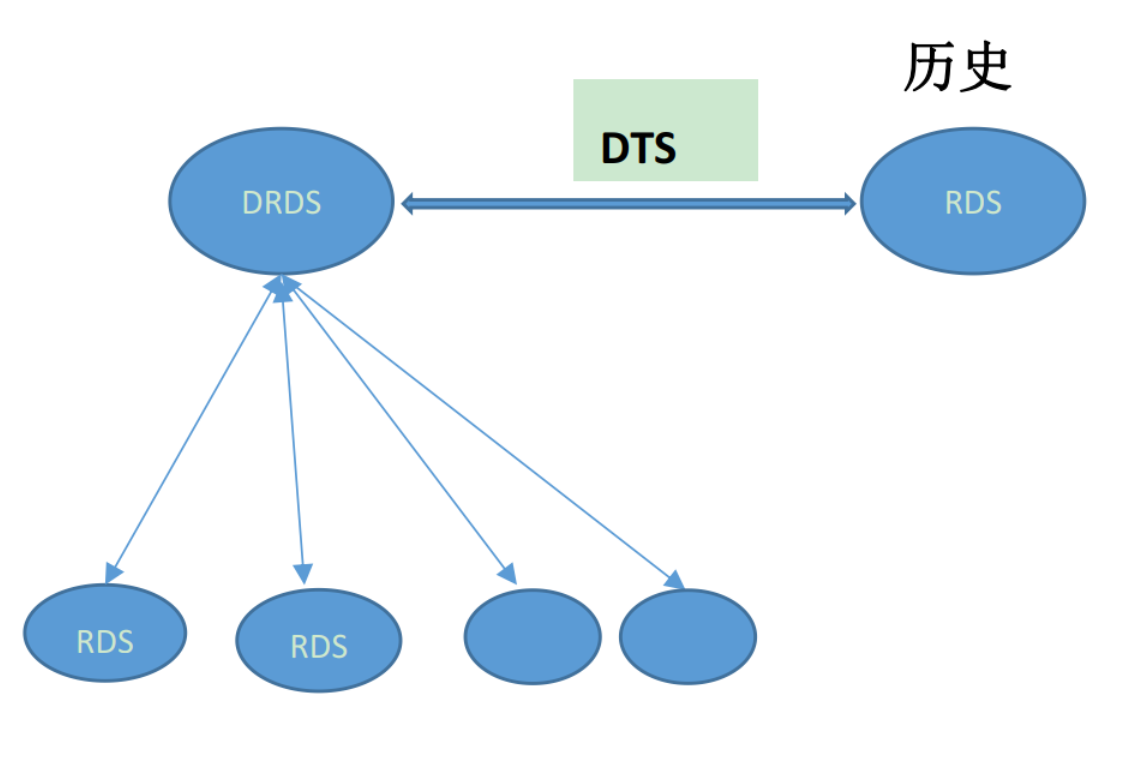
4.节省视频接收服务器：摄像头内嵌OSS的直存SDK，实现监控视频直接推送到云存储0SS中，省掉大量视频接收服务器。

**3、用户需要在每月的月末清理历史数据，但业务允许的清理时间仅有1个小时，如果1小时内不能完成，需要立即回滚以保障业务正常运行；请从架构和schema设计方面提供保障清理任务及时完成、业务能够及时恢复的措施。**

1.使用DRDS+RDS对数据库进行分库分表，使清理任务的压力下发到每个RDS上面，分散单库的压力。

2.对每个RDS的表按照分区键（月份）进行分区，在清理时直接删除相应月份的表分区，加快清理过程。

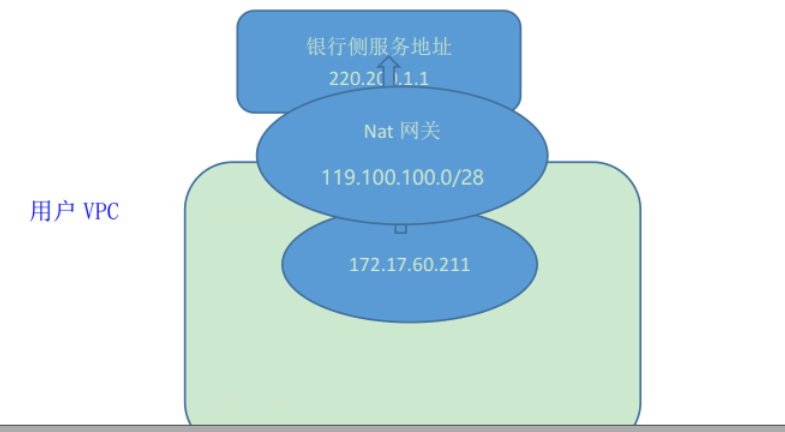
3.建立历史库（RDS），利用数据传输工具（DTS）定期将生产库的数据同步到历史库。如果出现意外情况，可从历史数据库将数据恢复至生产库。



**4、对于典型WEB服务，通常有负载均衡、流量接入层、业务逻辑层、缓存、数据库、存储等组成、在迁移过程当中，一般采取什么样的迁移步骤，保证业务平滑迁移？**

为了保证业务不中断，首先在云上部署一套新的平台，接着把web应用部署到云端，再把数据库、存储迁移上云，云端web应用和原有系统同时运行，一方面保证业务的正常运行，一方面测试云端WEB应用。待云端业务运行稳定之后，再把原WEB应用的数据变化同步到云端平台，保证云端平台业务环境和数据都是最新的。最后把域名解析到云端平台的负载均衡上，启用新平台，停用老平台。

图：云上部署一套新平台—云端部署WEB应用—DTS迁移数据库存储迁移到云上—云端负载均衡接入—测试云上web应用系统—如云端web应用业务正常—选择一个晚上或节假日业务低估-DTS同步测试期间的数据变化—域名解析到云端负载均衡—原WEB应用系统停止服务，新平台启用。



**5、如果某用户的IDC在和阿里云VPC打通混合云时，用户的IDC存在公网私用的情况，例如：当某客户在阿里云向银行方向连接专线时，银行出于安全目的，会要求客户访问银行的数据包的源ip地址是银行指定的地址。且类地址一般是公网私用。例如：客户的VPC地址是172.17.48.0/20，其中的一台ECS：172.17.60.221 要访问119.100.100.0/28 该如何处理？**

公网私用的应用场景可以用nat网关来解决。

1、创建一个nat网关，并把公网地址119.100.100.0/28地址段绑定到nat网关

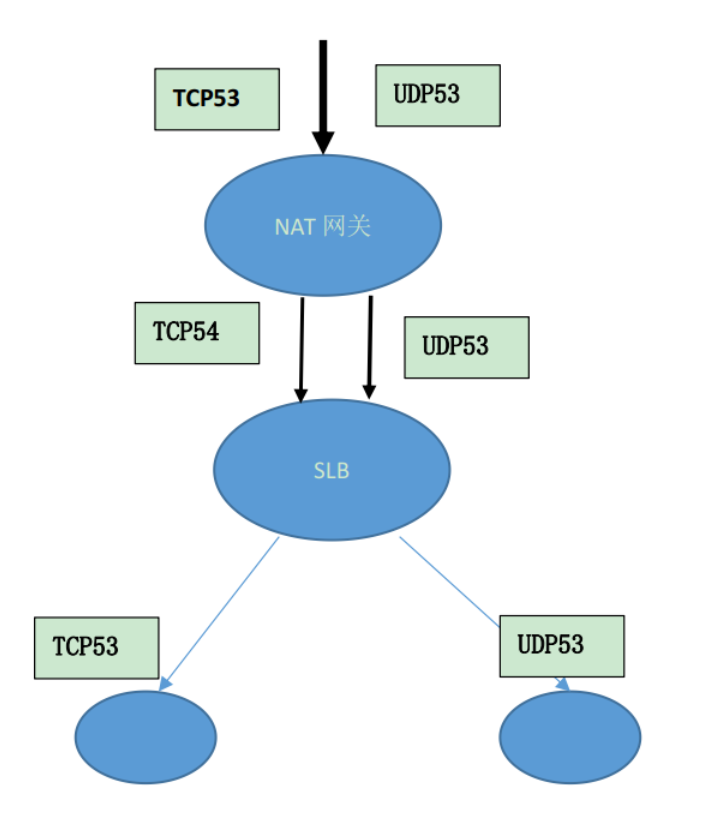
2、把VPC中的ECS172.17.60.211业务端口通过DNAT表映射到nat网关上；

3、ECS 172.17.60.211访问银行侧业务通过nat网关绑定的公网地址池119.100.100.0/28访问。

**6、某企业的DNS服务器计划迁移到阿里云上，做域名的权威解析，能使用阿里云的SLB作负载均衡保证高可用，需要SLB同时代理UDP和TCP的53端口，但是SLB目前不支持同时代理两种协议，请使用阿里云的云服务设计一套解决方案解决这个问题。**

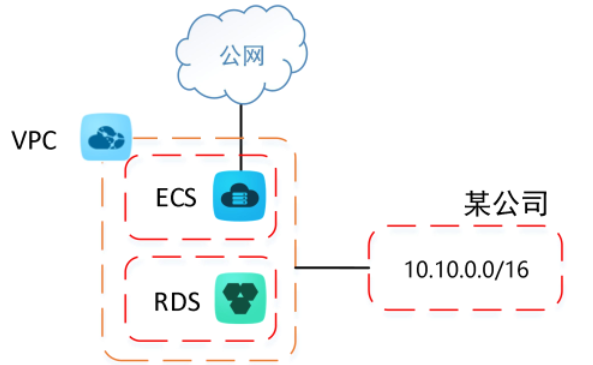
1.利用NAT网关，将入口处的TCP53映射为TCP54，UDP53保持不变。

2.在SLB层面，进行53端口转发（SLB前端端口不可重复，后端可重复）



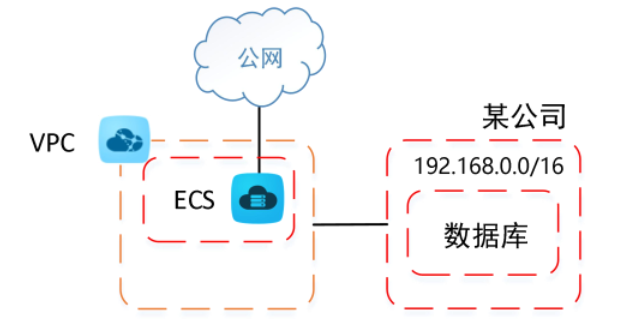
**7、由于网络规划原因，某公司网段：10.10.0.0/16，可以通过VPN访问ECS（公网：172.168.3.10，内网：10.192.16.8），但是无法直接访问到RDS（数据库）：10.192.200.9，ECS到RDS网络可达，现在，该公司在测试代码阶段，希望办公网可以连通RDS的3306端口，网络限制不可取消，具体措施是？**

该公司通过建立VPC并将ECS、RDS实例划分至该VPC域内，将公网IP映射至ECS主机，访问ECS时，仍通过VPN访问ECS服务器，为了测试代码阶段能够从内网访问RDS的3306端口，通过VPC内的访问控制规则指定仅对RDS所在网断的地址及3306端口开放，实现相应功能。



**8、某公司只有内网，没有公网出口也不可能开通公网访问，内网ip段为192.168.0.0/16，现在公司想通过购买阿里云主机提供对外的页面或者其他服务，但是所有后端数据必须放在公司内网中。请结合阿里云相关产品，设计一套方案来满足上述需求，要求阐述网络架构方案、数据流向、DNS等解决方案。**

使用VPC及专线将该公司与阿里云打通，后端数据及数据库服务在该公司内，前端数据存储于阿里云，外部访问通过阿里云ECS对外提供服务，数据流向为用户-阿里云-专线-该公司。



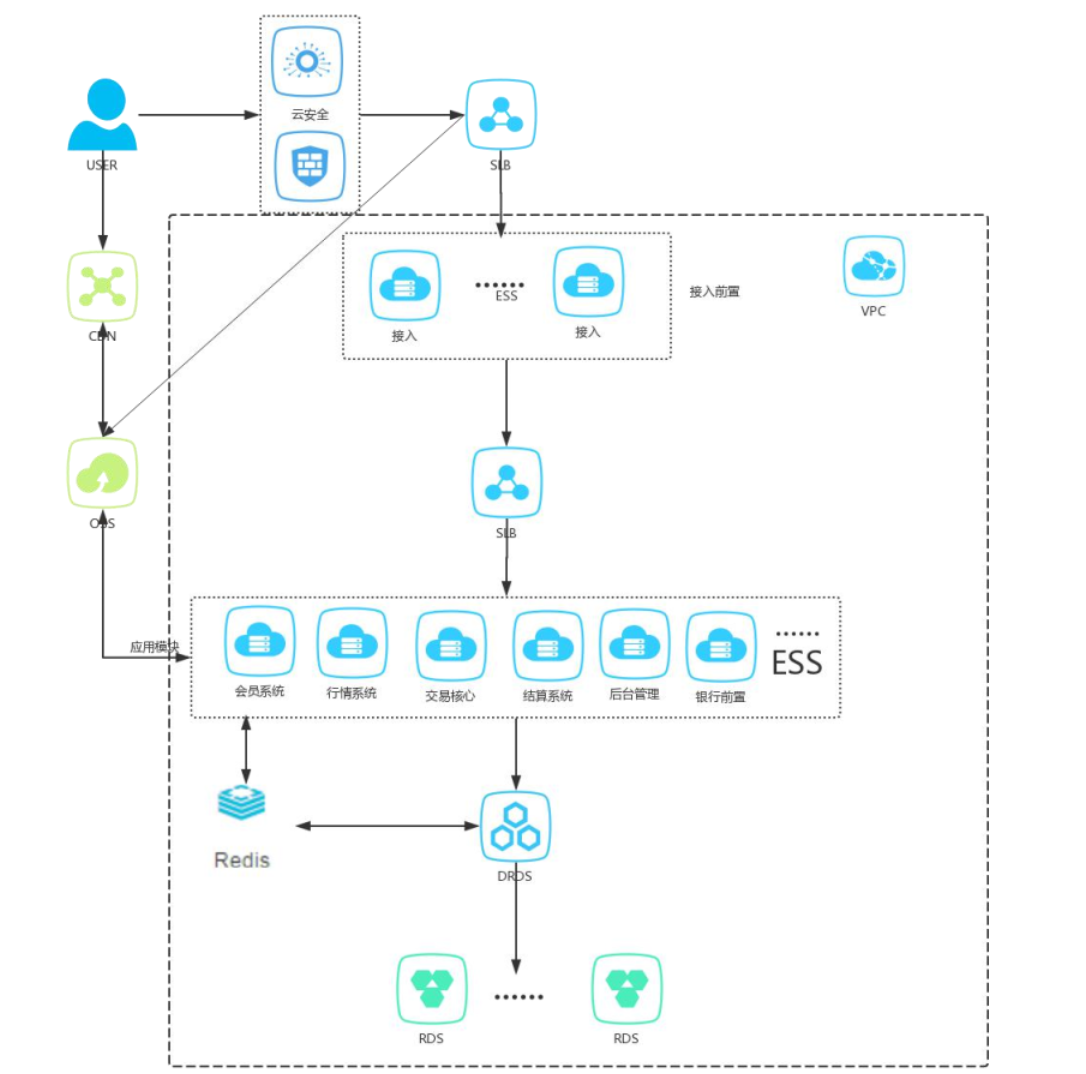
**9、结合阿里云相关云产品或者业界通用技术，设计一套以java为主要开发语言的交易系统，要求此系统可以承受高并发的考验；并且要涵盖整个交易链路中数据流的逻辑走向、各个应用间角色说明、业务逻辑、运维指标、应急方案等描述，侧重点在说清楚系统架构逻辑；系统要具备快速扩容、容灾、多区域访问加速等能力。（通用技术架构）**

答：系统设计时有以下理念：多级缓存，静态化，任务切分（MR），多线程并行执行（MPP），读写分离，业务拆分，模块无状态，负载均衡，异地容灾，异地备份。

数据流走向如图：用户访问时通过对CDN内的缓存读取加载静态资源，如资源有更新则从0SS读取后再加载，静态资源加载完成后访问数据通过负载均衡设备进入各个子服务模块，在服务模块通过缓存、DRDS与RDS进行数据交互后，将数据用户请求数据返回。

为了承受高并发的考验，做以下设计：在应用前端部分做动静分离，减轻前端服务器压力；在应用部分以业务角色及功能拆分任务为多个模块，使用弹性伸缩对各个子模块承载的主机做快速扩容，所有服务模块无状态，以期达到通过快速扩展节点数量增加吞吐量的目的；在数据库部分，通过使用Redis、Memcache等实现数据库高速缓存，配合DRDS增强数据库的访问承载能力。

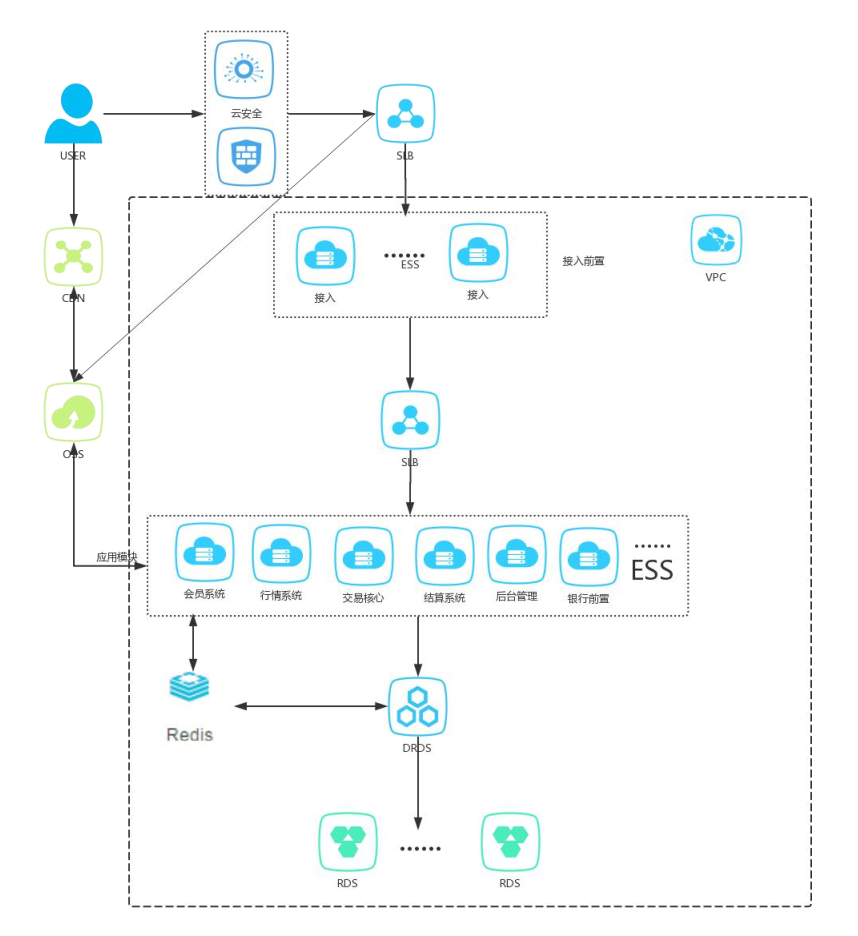
针对容灾和多区域访问加速的需求，使用CDN及不同可用区、异地多备份实现，正常情况下分区域主备使用，使用DTS进行数据同步传输，保证主备节点的数据同步，主可用区或主区域发生异常情况时，通过CDN将域名切换至其他可用服务节点，保证访问的正常。



**10、某公司有一套业务系统，主要针对国内和美国的用户提供服务，属于计算密集型系统，涉及到的有cms、app、财务系统等，目前服务器主要都在国内IDC托管，由于该公司业务量越来越大，所以希望将除了财务系统以外的系统全部上云，并且想通过阿里云的产品能提升用户的体验，请根据阿里云相关产品，帮该公司设计一套云上解决方案，要求综合考虑成本、用户体验以及财务系统对接等问题。**

答：该系统方案为境内外多区域混合云方案。分别在美西和华北3部署两套业务系统对外提供服务，用户通过云解析访问最近路由的系统，两套业务系统都有弹性伸缩性能。华北3VPC和美西VPC通过高速通道连接，把两地的数据同步延时降到最低，两套业务系统的RDS数据库通过最新的DTS双向实时同步功能进行数据同步。财务服务器依然在本地IDC数据中心，IDC通过合作伙伴的VPN通道与华北3VPC连通，降低通讯成本。

系统架构如下图：



数据流走向如图：用户访问时通过对CDN内的缓存读取加载静态资源，如资源有更新则从0SS读取后再加载，静态资源加载完成后访问数据通过负载均衡设备进入各个子服务模块，在服务模块通过缓存、DRDS与RDS进行数据交互后，将数据用户请求数据返回。

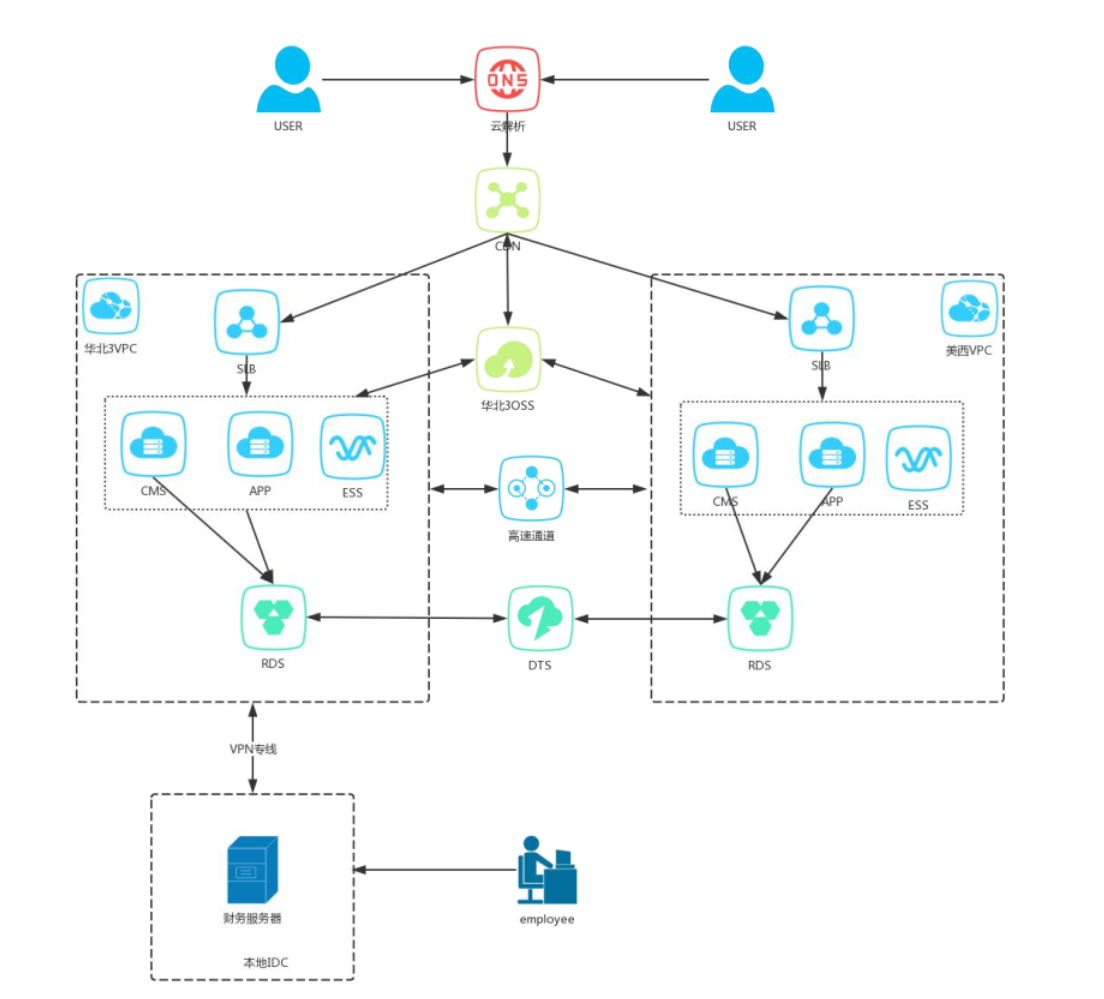
为了承受高并发的考验，做以下设计：在应用前端部分做动静分离，减轻前端服务器压力；在应用部分以业务角色及功能拆分任务为多个模块，使用弹性伸缩对各个子模块承载的主机做快速扩容，所有服务模块无状态，以期达到通过快速扩展节点数量增加吞吐量的目的；在数据库部分，通过使用Redis、Memcache等实现数据库高速缓存，配合DRDS增强数据库的访问承载能力。

针对容灾和多区域访问加速的需求，使用CDN及不同可用区、异地多备份实现，正常情况下分区域主备使用，使用DTS进行数据同步传输，保证主备节点的数据同步，主可用区或主区域发生异常情况时，通过CDN将域名切换至其他可用服务节点，保证访问的正常。

**11、某公司有一套业务系统，主要针对国内和美国的用户提供服务，属于计算密集型系统，涉及到的有cms、app、财务系统等，目前服务器主要都在国内IDC托管，由于该公司业务量越来越大，所以希望将除了财务系统以外的系统全部上云，并且想通过阿里云的产品能提升用户的体验，请根据阿里云相关产品，帮该公司设计一套云上解决方案，要求综合考虑成本、用户体验以及财务系统对接等问题。**

答：该系统方案为境内外多区域混合云方案。分别在美西和华北3部署两套业务系统对外提供服务，用户通过云解析访问最近路由的系统，两套业务系统都有弹性伸缩性能。华北3VPC和美西VPC通过高速通道连接，把两地的数据同步延时降到最低，两套业务系统的RDS数据库通过最新的DTS双向实时同步功能进行数据同步。财务服务器依然在本地IDC数据中心，IDC通过合作伙伴的VPN通道与华北3VPC连通，降低通讯成本。

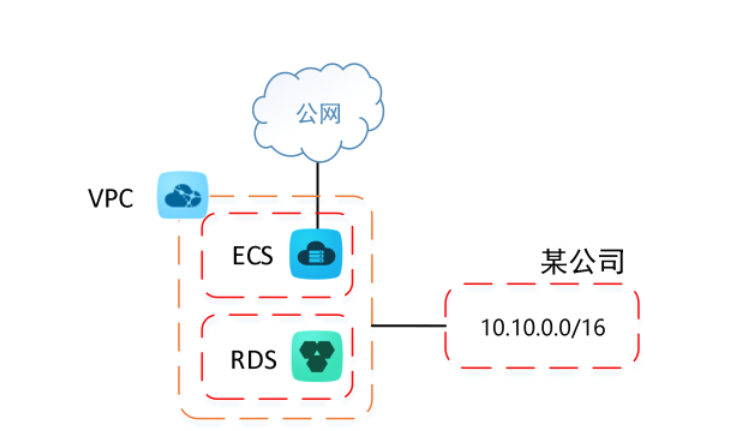
系统架构如下图：



数据量走向如图：国内外用户通过云解析选择最佳路径CDN节点请求静态资源，并如资源有更新则从0SS读取后再加载，静态资源加载完成后访问数据通过最近负载均衡设备进入相应业务系统，CMS和APP通过内网访问各自VPC内的数据库。两地的数据库通过高速通道双向同步数据。本地员工可通过互联网专线访问IDC财务服务器，并通过IDC到华北3VPC的VPN专线和云上资源进行数据交互。

**12、由于网络规划原因，某公司网段：10.10.0.0/16，可以通过VPN访问ECS（公网：172.168.3.10，内网：10.192.16.8），但是无法直接访问到RDS（数据库）：10.192.200.9，ECS到RDS网络可达，现在，该公司在测试代码阶段，希望办公网可以连通RDS的3306端口，网络限制不可取消，具体措施是？**

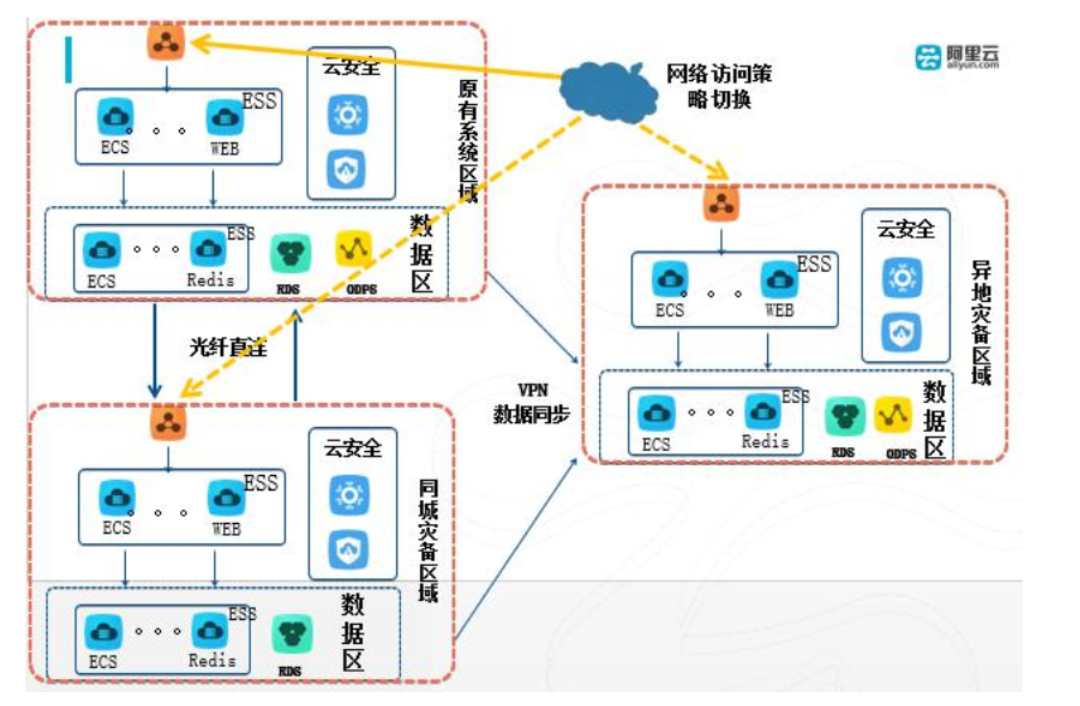
方案一：该公司通过建立VPC并将ECS、RDS实例划分至该VPC域内，将公网IP映射至ECS主机，访问ECS时，仍通过VPN访问ECS服务器，为了测试代码阶段能够从内网访问RDS的3306端口，通过VPC内的访问控制规则指定仅对RDS所在网断的地址及3306端口开放，实现相应功能。



方案二：在上述结构下，ECS内对RDS做端口映射，使得从该公司私网访问ECS时使用ECS的指定端口访问RDS的3306端口。

**13、实时交易系统**

**一个实时交易系统，整体架构是：一组7层负载均衡集群中的一个VIP（220.223.8.10，对应域名：shishijiaoyi.com)下挂了50台Web服务器，web服务器对接（一组8台的redis服务器+一台mysq1数据库）。现在，公司业务要求，运维团队需要进行同城容灾和异地容灾方案评估，请拿出一份可行性方案出来供财务部门、技术部门、开发部门进行选择。（请列出重要评估点，具体方案，取舍依据）**

****

实时交易系统，服务的高可用和数据的安全是核心保障要求，所以高可用方面在同城灾备和异地灾备均搭建了完全的系统，细节说明如下：

1、考虑在线交易系统的高可靠性要求，本地、同城容灾、异地容灾均搭建完整的实时交易系统，确保在任何情况下，均可以完整的提供对外服务。服务100%可用即为最大的效益；

2、利用ess、云安全技术，提高对突发系统压力的应对能力以及安全防护能力

3、通过云安全功能，避免系统被攻击或者渗透，造成数据被篡改、窃取等，确保数据安全。

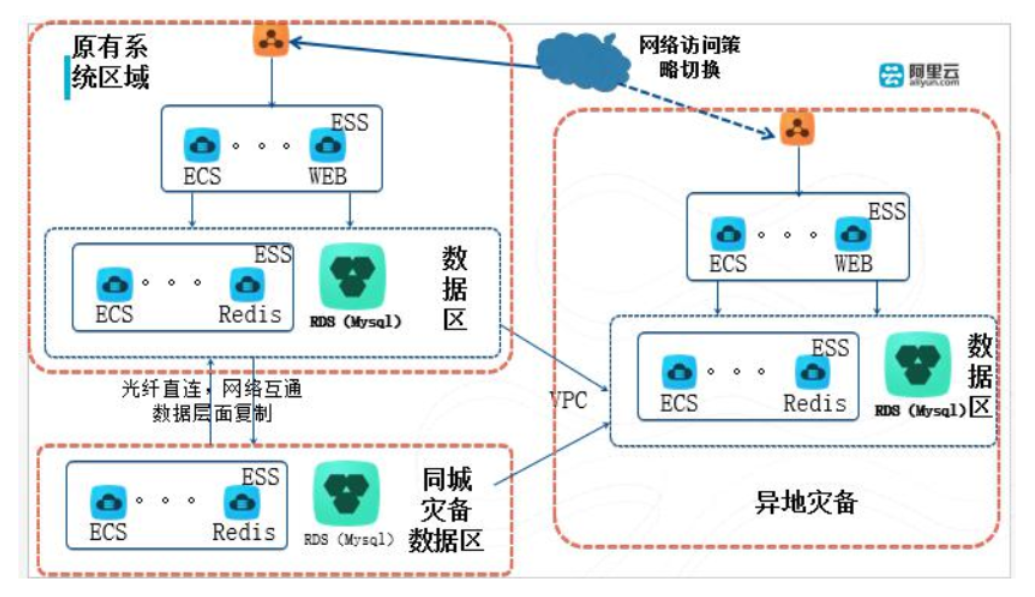
4、在本地和异地容灾部署odpsbi分析，对交易进行分析审计，考虑到投资，在同城容灾未部署odps bi分析，一般同城容灾启用并且可用的情况，一般不是出现如重大地质灾害等的情况，一般可以在较短的时间在恢复本地机房，BI类业务停止的时间可以忍受，并且BI类的服务可以通过异地容灾机房实现，且实时性要求较低；

5、同城和异地容灾的ecs服务器，均按照最低要求配置，降低能源消耗，通过部署ess，实现在必要的时候自动扩充服务能力；

6、同城两机房采用光纤直连，以QOS保证为重点，保证两机房切换时间最小；异地与本地之间采用vpn连接，以安全可靠的数据同步为重

**14、在线论坛**

**一个在线论坛系统，整体架构是：一组7层负载均衡集群中的一个VIP（220.223.8.10，对应域名：shishijiaoyi.com)下挂了50台Web服务器，web服务器对接（一组8台的redis 服务器+一台mysq1数据库）。现在，公司业务要求，运维团队需要进行同城容灾和异地容灾方案评估，请拿出一份可行性方案出来供财务部门、技术部门、开发部门进行选择。（请列出重要评估点，具体方案，取舍依据）**

****

1、在线论坛核心是数据的安全性，其次是业务的高可用，所以同城容灾中重点进行了数据级的容灾考虑；

2、考虑财务成本等因素，同城容灾只做了数据级容灾，避免数据的损失。同城与现有机房通过光纤直连，保证了网络QOS，主要用于防备数据级的重大问题；

3、异地容灾做了应用及数据级的容灾，通过访问策略，确保在同城容灾无法保证正常服务的情况下，可以顺利接手服务，防备现有机房及同城机房彻底失效的重大问题；

4、设计考虑了ess弹性伸缩，容灾中的ecs服务器最保持最低的应急运行需求，以降低资源消耗，又可在需要的时候实时自动扩充服务能力，同时现有机房服务器采用ess改造，可以避免用户集中上线业务高峰期，处理能力无法及时提升的问题。又可以在业务平稳期快速释放资源，降低消耗。

**15、CDN行业解决方案设计**

**有2个客户，分别从事电商和视频行业，想对自己的网站进行CDN加速，请分别推荐技术方案，并阐述需要关注点和异同点。**

电商行业在内容分发时面对的主要关注点有：

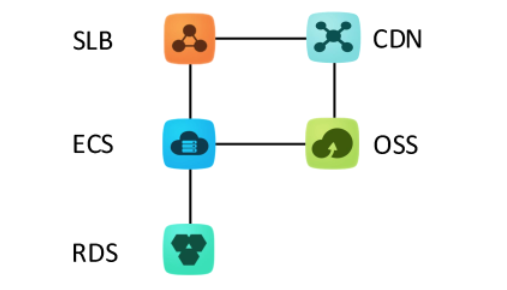
1.静态图片资源多、请求多；2.突发流量；3.访问稳定性、安全性；。

视频行业在内容分发时面对的主要关注点有：

1.视频文件存储量大、多样性强；2.突发访问量大时，服务器和带宽压力大；3.直播业务需求高网络质量。

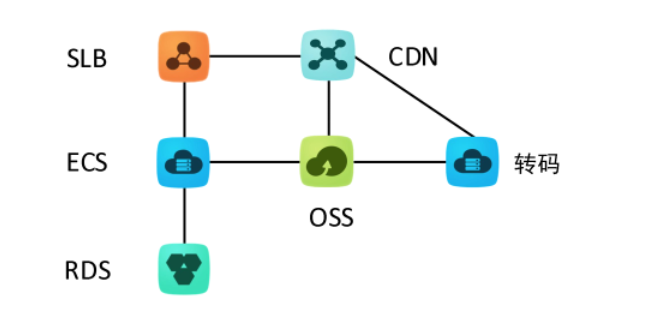
上述典型电商与视频行业的关注点中，相似的是用户的非集中性、突发访问以及非结构化资源访问多，带宽压力大；不同点在于，电商部分更关注于访问稳定性与安全性，视频行业更关注于带宽问题。

针对电商行业，使用CDN加速的方案如下：



在用户经由CDN访问站点时，对网站的静态资源如html，css，等在CDN内进行存储，针对访问量较多的图片等资源，0SS作为CDN的源站，通过CDN加速分发，用户通过CDN节点就近获得文件。

针对视频行业，使用CDN加速的方案如下：



在用户经由CDN访问站点时，对网站的静态资源如html，css，等在CDN内进行存储，视频流最终通过CDN服务完成视频分发；针对热点内容，通过CDN主动推流的方式将视频流加载到CDN边缘节点；若存在需要转码等处理的视频流，则由CDN直接请求进行转码存储于OSS并进行分发