规划设计类

介绍一下容灾图景

灾备，是企业中一项重要的技术应用，对于企业数据安全起到了很大的作用。 一般来说，灾备的级别可以分为数据级、应用级和业务级三个级别。

- **数据级灾备**：主要关注的就是数据，就是在灾难发生之后，可以确保数据不受到损坏。比如早期的通过备份到磁带转移到异地或者基于网络实现灾备中心与生产中心的异步\同步的数据传输。
- **应用级灾备**：建立在数据级灾备的基础上，对应用系统进行复制，也就是在异地灾备中心再构建一套应用支撑系统，可提供应用接管能力。支撑系统包括数据备份系统、备用应用系统、以及备用网络等。
- **业务级灾备**：也是最高级别的灾备系统，包括超过IT系统的部分，比如业务用户的办公场所以及业务工作人员备份等。

我们这里主要讲述IT系统的灾备。常见的灾备架构有以下几种：

集群部署

通过将应用和数据集群化部署在同一数据中心的多台服务器上，使用多线网络接入、多路电力供应、应用的负载均衡、多主机集群、数据库集群、日志同步等技术来满足对可用性和可靠性的要求。

同城双活

同城双活是在相距20公里以上的同城或者相邻区域镜像部署两个独立的集群，数据单点写到主机房，然后实时同步到从机房，从而避免单个IDC机房可能发生的风险。这个方案的优点在于方案简单、通信条件好，缺点在于对于城市级电力、网络故障或者地震、洪水、山火等大范围自然灾害的抗风险能力不足。同时该方案存在数据或者存储的单点故障，当某个机房停止服务或者性能不足时，整体性能下降严重或者数据丢失。该方案主要涉及的技术难点有服务的路由和数据的双活。

两地三中心

所谓两地三中心是指同城双中心+异地灾备中心，异地灾备中心是指在相隔1000公里以上的城市建立一个备份的灾备中心用于双活中心的数据备份。数据和服务平时都是冷数据和冷服务，只有当双中心所在区域出现访问异常时，异地灾备中心可用备份数据进行业务恢复。该方案相对同城双活复杂度增加不多，有效解决了异地数据灾备问题，但依然存在主机房依赖，不能完全解决同城双活的痛点。

此外，类似的概念还有“同城双活、异地多活”、“同城灾备，异地容灾”、“三写两同步”等方案。其中，三写两同步是不再同步数据库数据，而是应用层同步向同城的三个数据中心进行读写操作，只要两个数据中心返回成功即可，这样保证三个数据中心随机停止一个服务，不影响高可用架构的运行。

异地多活

异地多活也称为三地五中心，是将在分布在异地的多个站点同时对外提供服务，与传统灾备的区别在于多活，即所有站点同时对外提供服务。这个架构面临的主要挑战在于“解决异地高延时和随之带来的数据同步。主要的方案是通过把能完成所有业务操作的服务和数据作为一个单元作为系统部署的基本单位，在全站所有机房部署数个单元，每个机房单元数目补丁，任意单元包含系统所需所有应用，每个服务上下层调用仅使用本单元节点。对于无法单元化业务，延时不敏感但一致性要求高的业务仍然使用两地三中心部署、跨地区调用；延时敏感而一致性要求不高的业务的则每个机房部署全量数据，机房之间增量同步。为保证用户请求能够正确进入目标单元，每个机房部署流量入口网关集群，由流量网关感知全局流量分片情况，自动计算和转发到对应单元。同时，使用RPC、MQ等中间件提供服务路由能力，将跨单元请求正确路由到对应单元。

异地多活方案容灾能力大幅提高，实现了服务异地多活、数据异地多活，有效减少机房和地区级别的故障影响范围，理论上服务可以水平扩展，没有性能的局限。缺点在于架构非常复杂，部署和运维成本很高。

混合云容灾

混合云容灾服务（Hybrid Disaster Recovery， 简称 HDR）是一个为数据中心提供企业级应用的本地备份与云上容灾一体化的服务，免去了灾备中心的建设，通过云上部署和公网环境将数据实时复制到阿里云。部署在阿里云ECS上的应用通过HDR的CDP技术，实现跨可用区或跨地域的实时复制，实现秒级RPO，分钟级RTO的高性能应用级容灾。更有容灾编排能力，可以预制多节点复杂应用云上一键恢复流程。实现方式有两种：

1. 云盘的异步复制：适用于规模较大、操作系统多样、数据量大的情况
    1. 资源规划
    2. 创建容灾站点对
    3. 设置网络安全
    4. 创建保护组
    5. 添加保护实例
    6. 启动复制
2. CDR(连续数据复制)：适用于小规模环境，成本高、需要安装客户端
    1. 搭建云上专有网络
    2. 创建容灾站点对
    3. 部署CDR网关
    4. 安装阿里云复制服务
    5. 应用容灾
    6. 容灾回切

解释一下RTP和RPO

RTO和RPO是Service Level Agreement (SLA)的两个重要的衡量指标。

1. Recovery Point Objective (RPO)，指的是最多可能丢失的数据的时长。提升RPO的常用技术有：磁带备份、定期数据复制、异步数据复制、同步数据复制等。
2. Recovery Time Objective (RTO)，指的是从灾难发生到整个系统恢复正常所需要的最大时长。提升RTO的常用技术有：磁带恢复、人工迁移、应用系统远程切换、负载均衡等。

简单而言就是RTO是指多久修好，RPO是指丢了多久的数据。

如何考虑业务流程层的灾备设计

1. 多活数据中心：建立多个分布于不同地域的活动数据中心，确保业务能够在单一数据中心发生故障时能够无缝迁移到其他数据中心
2. 冗余网络架构：采用冗余的网络设计，确保网络的可用性和容错能力。可以配置多个路由路径使用多个网络提供商来实现
3. 负载均衡：使用负载均衡将流量分发到多个服务器或者数据中心上
4. 数据备份和复制：定期对业务数据进行备份，并实时或者异步同步到其他数据中心或者存储设备中
5. 弹性扩展：根据业务流量的变化自动调整服务器或者资源的数量，以满足业务需求和应对突发情况

6. 合理的容灾测试：定期进行容灾测试，验证灾备方案的可靠性和有效性，及时发现和修复潜在问题

具体的实施过程中，可以根据业务需求和资源限制进行灵活的设计和选择。同时，也需要考虑成本和收益的平衡，确保灾备方案的可行性和可持续性。

如何进行上云迁移

混合云的部署方式

1. 基于VPC+专线的混合云架构
2. RDS自建主从同步实施混合云
3. RabbitMQ+SLB的混合云实践
4. 云端自建DNS实践

混合云的优势

1. 减少自建数据中心的设备及维护人员资金投入成本；
2. 云上资源按量付费、降低运维难度、减少人员投入；
3. 缩短业务部署开发上线周期，从以周为单位部署到以小时为单位计算；
4. 提升容灾能力，

上云的收益

1. 更快的访问基础设施
2. 更高的伸缩性
3. 便捷的实现高可用
4. 快速部署、快速上线
5. 保障业务的连续性
6. 更大地域的覆盖
7. 能够廉价的实现高性能部署
8. 转移资本支出到运营成本
9. 节约整体成本
10. 更高效的的IT技术人员

云迁移之前的准备工作有那些

1. 前期资产大致评估，由售前和销售执行
    1. 了解运维团队规模和水平测试
    2. 计算资源规模、技术选型和架构拓扑
    3. 了解迁移限制：时间、运维文档、业务状况
    4. 评估迁云成本，调研阿里云资源
    5. 确立相关业务合同
2. 项目启动，由项目交付组长确认：
    1. 识别干系人、指定通讯录，指定关键联络人，召开项目立项会议
    2. 确定项目实施计划和实施周期
    3. 明确项目范围、项目进度、项目风险和验收标准

    4. 根据实际情况设立里程碑和创建WBS
    5. 对口头承诺以及招标内容与实际不符项进行摸底
3. 系统架构的梳理和评估
    1. 离线采集IDC资源，包括操作系统和网络资源，输出资源清单
    2. 对数据资产软件和系统架构进行盘点和建立拓扑
4. 确定迁移方案
    1. 输出现网架构、业务运行情况文档、软件系统架构文档
    2. 输出迁移方案、实施配置方案文档
    3. 使用资源计划创建资源
5. 迁移实施
    1. 域名备案要先行
    2. 定制系统镜像
    3. 自动化运维工具的应用
6. 迁移测试
7. 上线切割
8. Nginx反向代理将老用户请求引流到阿里云（302转向）
9. 项目交付及后期监控运维
    1. 主要内容为文档的编写总结
    2. 包括系统软件架构、系统架构、迁移方案、运维实施配置文档、运维维护手册、故障处理手册

迁移过程中用到那些迁移工具

1. 服务器SMC实现，制成镜像式实现迁移
2. 块存储可以使用闪电立方(mini版、3U机架式、6U机架式)、rsync、ftp、scp实现全量或者增量迁移
3. OSS通过OSSimport、FTP、NAS方式迁移，还可以使用部署代理进行迁移
4. OSS还可以通过在线迁移和离线迁移的方式进行不同主机环境和云间迁移
5. 数据库传输服务DTS，是阿里云提供的实时数据流服务，支持关系型数据、非关系型数据库和数据多维分析OLAP等的数据源间数据交互，支持MySQL、PostgreSQL、Redis、MongoDB
6. 异构数据库迁移ADAM提供数据库平滑迁移方案，支持将Oracle、Teradata、DB2转化为MySQL、PolarDB O引擎
7. 云迁移中心CMH 是阿里云自研的一站式迁移平台可以实现多源迁移、自助完成迁云成本评估、可视化业务分析、应用拓扑展示和内置迁移计划模板降低了云迁移门槛、提高了迁移效率。
    1. 创建SMC迁移任务实现服务器的迁移
    2. 创建DTS迁移数据库实例

阿里云交付流程

1. 需求确认：通过与客户的充分沟通和需求明确，摸底用户的技术要求和业务需求
2. 架构设计：根据客户需求进行架构设计，包括配置选型、容量规划、网络拓扑等，以满足用户性能、成本、可用性等要求
3. 环境搭建：根据架构设计方案，部署云上要求资源

4. 应用部署：将客户的应用程序部署都阿里云环境中，包括安装、配置和测试应用程序等相关组件
5. 数据迁移：包括数据库、文件存储等数据的备份、导入和同步
6. 安全设置：根据用户安全要求，进行相关安全配置，确保用户数据安全和业务安全
7. 性能优化：对客户的应用和数据库进行性能优化，包括调整系统参数、资源调度、负载均衡等，以满足可用性、可靠性的要求
8. 监控和运维：配置监控系统，实时监测客户的应用程序和系统性能，及时发现和处理故障。同时建立适配的运维机制，定期维护和更新系统环境
9. 交付验收：与客户一起进行系统交付验收，确保交付的系统满足用户期望和需求
10. 培训和支持：为客户提供系统的培训和技术支持，使客户能够熟练维护相关环境，解决常见问题

以上时阿里云交付流程设计的一般步骤，具体流程要参考具体客户和落地实践来进行调整和优化。

如何理解CDN

C：分发内容-Content
D：分发策略-Delivery
N：分发网络-Network

CDN可以实现对静态资源和动态内容的网络分发和访问预热，从而提高网络服务访问体验。

CDN工作机制

1. 内容注入
    1. 源站push相关内容到CDN网络
    2. CDN网络从源站pull相关内容
2. 用户请求调度
    1. 用户发起请求
    2. CDN授权DNS服务器(全局负载均衡GLSB)将节点设备IP返回用户或者将l另一个GSLB设备的IP返回用户
    3. 用户向GLSB设备发起内容访问请求
    4. 根据用户IP地址以及访问URL，选择用户所属地域负载均衡设备(SLB)，并让用户向该SLB发起访问
    5. SLB设备通过决策为用户选择最佳服务器，用户向服务器发起访问请求
    6. 若服务器内容未命中，则该服务器向上级节点请求内容，然后由该服务器提供服务
3. 内容分发
4. 内容服务

CDN预热

预热式指提交URL预热请求之后，源站将主动push对应资源到CDN节点，当用户首次请求时，就能直接从CDN节点中获取到最新的请求资源，无需再回源站拉取，从而提高了缓存的命中率。

游戏业务大促措施

在游戏业务大促期间，可以采取以下措施来确保系统的稳定性和安全性

1. 限流：实施请求限制，控制同时访问游戏服务器的用户数量，通过限制每个用户的请求频率或者同时连接数，避免服务器过载和性能下降

2. 智能解析：通过使用DNS根据链路和IP将用户流量导流到不同地域的应用服务器
3. 负载均衡：通过使用SLB或者Ngingx等负载均衡技术，将流量分散到不同的应用服务器上，以平衡单点负载，提高可用性和系统容量
4. 弹性扩缩容：根据需求自动后者手动增加服务器数量，以适应峰值负载，应对突发高流量情况
5. 缓存优化：利用浏览器cookie缓存、静态资源本地磁盘缓存、Nginx的proxy_cache等缓存技术以及CDN，将频繁访问的数据存储在最接近用户的位置，减轻服务器压力并提高响应速度
6. 安全监测和防护：加强对网络流量和用户行为的监测，及时发现异常活动，并采取相应的安全防护措施，保护系统免受攻击
7. 预案和灾备：事前建立访问流量预测，进行详细和完善的压测并进行相应的优化措施。同时，开发、运维等协同跨部门进行对应的故障、攻击、系统崩溃的事件演习。事中对网络、主机、数据库进行密切的监测。事后认真复盘，总结经验教训，将相关文档和报告归档。

如何解决全球系统访问慢的问题

1. 在全球建立多个站点，通过DNS解析不同线路的为不同地域用户返回最近的主机
2. 使用全球加速GA的CDN服务提供全球的访问能力加速
3. 部署边缘计算节点，在靠近用户的IDC建立边缘计算服务器
4. 使用VPN通过高速专线网络连接多个节点
5. 通过高速节点来实现代理访问
6. 前端优化，优化网页和应用程序的前端性能，包括合并压缩js和css文件、减少HTTP请求数量、为不同类型文件使用不同的子域名等，提高页面加载速度
7. 带宽优化，增加带宽，避免拥堵
8. 缓存和预加载
9. 流量管理和负载均衡
10. 通过合并请求、懒加载和优化数据传输方式，减少网络往返
11. 监测和优化，定期监测全球访问性能，并根据实际情况进行调整和优化
12. 使用超高IO的ESSD云盘、ECS挂载多个ESSD云盘使用LVM组建高速磁盘、将多个ECS挂载的ESSD云盘组建分布式文件系统
13. 使用更高性能的PolarDB来替换自建MySQL和普通RDS数据库

综合考虑以上内容，可以采取适当内容来改善全球系统访问慢的问题，以切实改善用户体验。

安全保护类

谈谈你对等保三级的理解

等保测评是一种评估信息系统安全性的方法。《网络安全法》和《信息安全等级保护管理办法》要求信息系统运营单位应当选择符合国家要求的测评机构，依据《信息安全技术网络安全等级保护基本要求》等技术标准，定期对信息系统开展测评工作。信息安全等级保护有五个等级，从等保一级到等保五级，等级越高，要求越高。等保三级适用于“地级市以上的国家机关、企业、事业单位的内部重要信息系统。等保四级适用于国家重要领域、涉及国家安全、国计民生的核心系统，比如中国人民银行就是目前唯一四级等保的中国央行门户集群。等保五级是目前我国最高级别，一般应用于国家的机密部门。等保测评流程是一个五阶段的过程，包括：定级、备案、建设整改、等级测评、监督检查。等保的实施是法律要求的，明确规定信应履行安全保护义务，如果拒不履行，将会受到相应处罚。

等保需要用到那些产品

等级保护主要涉及到网络安全、主机安全、应用安全、数据安全、业务安全、安全管理和规章制度这几个部分。阿里云所涉及的产品主要有：

1. 操作审计ActionTrail
2. 访问控制RAM：集中管理阿里云服务和资源，可以创建对应用户和组来实现细颗粒度的管理
3. 日志服务(原来的SLS)LOG：实现实时数据采集、消费、投递和查询分析功能
4. WEB应用防火墙，针对恶意流量进行特征识别和防护
5. SSL证书：实现网站访问加密，同时提供统一生命周期管理、简化部署
6. 云防火墙：集中管理公网IP访问策略，内置IPS，支持失陷主机检测、主动外联行为阻断，留存6个月网络流量日志
7. 堡垒机：集中管理资产权限、全程记录操作数据
8. 数据库审计：智能解析数据库流量、细粒度审计数据库访问呢行为
9. 云安全中心：实时识别、分析、预警安全威胁的统一安全管理系统。

等保落地如何实施

WEB主机防护一般采用DNS解析——CDN网络——高防IP——web应用防火墙WAF——云防火墙/安全组——SLB——部署弹性伸缩和冗余服务来实现主动防御。同时结合SSL安全证书体系，结合日志服务和数据库安全审计仿制SQL注入和网络攻击。对于非结构化数据则采用内容安全审核，避免文字、视频的违规风险。在主机运维层面则使用堡垒机来实现对资产的权限管理和操作审计。

你知道GDPR么?

一般数据保护条例（General Data Protection Regulation）是一项全面的法律，赋予了欧盟居民对个人数据的更多控制权，并试图澄清在线服务商在收集、利用欧洲用户个人数据的规则和责任。该规定扩大了公司必须考虑到的个人数据范围，并要求他们密切跟踪他们存储的欧盟居民的数据。如果欧盟的某个人想要一个公司删除他或她的数据，发送数据副本，或者更正数据中的错误，该公司必须遵守。GDPR甚至比这还要更进一步。欧盟居民现在可以反对公司使用他们数据的具体方式。GDPR要求那些对客户data失去控制的公司，或者已经被黑客入侵的公司，在72小时内通知用户。这是最高刑罚的规则之一

GDPR适用于任何收集、处理、管理或存储欧洲公民数据的组织。包括大多数主要的在线服务和收集、处理、管理或存储数据的企业。正因为如此，GDPR本质上是为数据保护设置了一个新的全球标准。

海外合规要求

1. 数据隐私和保护：不同地区有不同的数据隐私法律和规定，比如GDPR、CCPA等
2. 电子商务规范
3. 支付合规
4. 知识产权保护
5. 电子通信合规
6. 就业合规

不同国家和地区的合规要求不同，具体的合规要求应根据具体目标市场的法律法规进行详细调研

怎样考虑游戏系统的安全防护

需要解决那些问题

1. 服务器和网络安全：确保游戏服务器和网络受到适当的保护，以防止未经授权的访问、黑客攻击或者数据泄露
2. 用户账户安全：采取措施来保护用户账户信息，例如要求使用强密码、双因素身份验证等
3. 游戏内部作弊和外挂：实施反作弊措施，检测和阻止玩家使用非法软件或者外挂程序来获得不公平优势
4. 数据传输加密：通过使用加密协议和技术，保护游戏中传输用户登陆凭据、支付信息不被窃听和泄露；
5. 游戏内容过滤，通过人工和AI审核机制检测和过滤不当、冒犯性或者违法违规内容，维护社区环境秩序和健康环境

可能遇到的安全问题

1. 黑客攻击，包括DDoS攻击、SQL注入、XSS跨站脚本等攻击，意图破坏游戏服务器的可用性或者盗窃用户信息
2. 账号盗窃，黑客通过钓鱼网站、鱼叉攻击、水坑攻击等方式获取用户账户信息，从而盗窃游戏道具、虚拟货币和个人资料
3. 外挂和作弊：玩家使用外部软件或者修改游戏文件以获得不公平的优势，破坏游戏平衡性和公平性
4. 社会工程攻击：黑客通过欺骗、诱导或者胁迫玩家来获取敏感信息，如密码、支付信息等
5. 未经授权的访问和泄露：未经授权的第三方访问游戏数据库或服务器，进行拖库等违法操作，获取用户信息和登陆凭据

为了解决这些安全问题，您可以采用综合的安全措施，包括加密通信、多重身份验证、防火墙和入侵监测、反作弊技术、定期安全审核和更新的方法。

阿里云那些产品提供了数据加密功能

1. 密钥管理服务(KMS): 提供安全可靠的密钥管理，包括生成、存储、使用和轮转密钥，以及加密算法和密钥策略管理。
2. 对象存储(OSS):支持数据的加密传输和服务端加密，可以使用KMS进行自定义密钥加密
3. 数据库加密服务(DESS):为云数据库实例提供透明数据加密功能，确保数据的存储和传输安全
4. 虚拟专网(VPC)：提供安全隔离的私有网络环境，用户可以使用配置网络ACL隔离和安全组规则来保护云上数据安全，同时可以使用SSL VPN等方式实现远程访问的加密。
5. 容器服务(ACK)：支持容器镜像加密、容器与容器之间的网络隔离

VPC网络中的的安全产品有那些

VPC是一种虚拟网络环境，可以让用户在阿里云上创建一个隔离的、安全的网络环境，类似传统物理网络的概念。其上相关的安全产品有：

1. 安全组：安全组是一种虚拟防火墙，能够控制ECS实例的出入站流量
2. 负载均衡白名单：为负载u南横监听设置仅允许那些IP访问
3. 云数据库RDS白名单：用户可以自定义允许访问RDS的IP地址
4. NAT/SNAT:实现内外部访问的单独配置

系统压测

需要关注的指标

1. 响应时间：衡量系统处理请求所需的时间
2. 吞吐量：表示系统在单位时间内能够处理的请求数量
3. 并发用户数：指同时访问系统的用户数量
4. CPU使用率: 了解系统在承受压力时的资源消耗情况
5. 内存使用率：监控系统的内存利用率，确保系统在高负债下不会出现OOM
6. 网络延迟：测量请求从客户端到服务器的传输延迟时间。
7. 错误率：错误数量和总请求梳理之比
8. 数据库性能指标：数据库响应时间、并发连接数、事务处理速度

在进行系统压测时，业务层需要关注那些

在进行系统压测时，除了底层的系统指标外，还要关注业务层的指标，以确保系统在实际业务场景下的性能和可用性。

1. 业务响应时间：衡量系统处理完整业务流程所需要时间
2. 业务吞吐量：表示系统在单位时间内能够处理的完整业务流程数量
3. 业务成功率：记录业务请求中成功完成的比例
4. 关键业务路径：确定业务中最重要、最频繁使用的功能或流程，并对其进行压力测试和性能评估
5. 并发用户行为模式：在压测中模拟真实用户的行为模式，比如登陆、搜索、下单等操作，以更准确的评估系统在实际使用情况下的性能
6. 业务数据准确性：在压测过程中，需要验证系统处理业务请求后产生的数据是否正确和准确。
7. 业务故障恢复时间：衡量系统从故障状态中恢复正常运行所需要的时间。

以上指标将帮助评估系统在业务层面的性能和可用性。根据具体的业务请求，还可以关注其他特定的业务指标来确保系统满足预期的业务要求。

多Agzin多VPC如何进行数据回传

1. CEN云企业网：用户实现不同地域或者不同VPC之间的网络通信和互联，CEN使用阿里云全球骨干网络，提供安全可靠的专线级别互联
2. VPC互联：通过VPC peering，实现国内VPC互联，实现两个VPC之间直接通信
3. VPN网关：通过公网进行数据同步和回传，配置IPsec VPN连接，通过VPN进行数据传输，确保数据安全性和完整性
4. 边界路由器
5. 弹性公网IP：如果只需要简单的数据回传，可以为ECS实例分配EIP，然后使用公网进行数据传输。

运维实施类

云监控

Arms、Grafana分别用到什么地方

1. Arms时阿里云提供的应用实时监控服务，主要用于监控云上应用的性能、稳定性和可用性。它可以收集和分析应用程序的关键指标，提供实时的性能监控、异常诊断和报警功能。
2. Grafana是一款开源的数据可视化监控平台，通过接入各种数据源进行图表化展示和分析。在阿里云中，arms可以和grafana进行集成，将arms收集的应用监控指标展示在grafana中，从而方便用户进行灵活和自定义的监控数据分析和展示。
3. 将arms和grfana的结合可以提供全面的应用实时监控和数据可视化解决方案，帮助用户更好地了解和管理云上应用。

云监控地优势和不足

云监控是一种通过云服务提供商提供地工具和服务来实时监测、管理和分析云环境中资源和应用程序地性能和状态

优势：

1. 实时监控和反应快速：云监控可以实时监测资源和应用程序地性能指标
2. 自动化和集中管理：云监控可以自动化监测和管理多个云资源，简化了管理的复杂性
3. 可扩展性和弹性：云监控可以根据实际需求扩展和自动缩放，适应不同规模和负载的环境
4. 提供可视化和报表功能：云监控通常提供友好的用户界面和报表功能，帮助用户更加直观的了解系统的性能状况

劣势：

1. 依赖云服务提供商：如果云服务上监控出现故障或者限制，可能影响监控的有效性和可用性
2. 数据安全性和隐私问题：云监控收集和处理的大量监控数据设计数据隐私和安全问题
3. 云监控不能满足更加个性化和更多维度的用户自定义需求

云监控改进方向

1. 多样化的监控工具选择：用户根据自身需求和情况选择最合适的监控工具
2. 多层次的监控设计：采用多层级的监控架构，将监控数据收集、处理和展示分层进行，降低对单一监控系统的依赖
3. 安全与隐私保护：加强对监控数据的安全保护，包括加密传输、权限控制、数据脱敏等手段，以确保数据的安全与隐私

云监控在实时性、自动化和扩展性等方面具有优势，但也要考虑依赖性、数据安全和隐私等问题。通过选择合适的监控工具、设计合理的监控架构以及加强安全与隐私保护措施，可以弥补云监控的不足，提高监控系统的可靠性和有效性。

云原生和K8S

云原生就是cloud native，云原生技术的目标在于帮助组织基于公有云、私有云和混合云等动态环境来构建和运行可弹性扩展的应用。

云原生的主要技术

1. 微服务
2. 服务网格
3. 不可变基础设施
4. 容器和容器编排
5. 声明式API
6. DveOps

容器的特点是什么

容器技术是一种内核轻量级的操作系统层虚拟化技术，使用Namespace进行资源隔离，使用cgroup进行资源的管理，有效的将单个操作系统管理的资源划分到孤立的组中。不同于传统虚拟化是基于硬件的抽象，容器技术是基于操作系统的抽象，只对必要的系统接口、配置文件进行虚拟化，极大的增加了配置效率。

其特点有如下：

1. 极其轻量
2. 秒级部署
3. 易于移植
4. 安全隔离
5. 弹性伸缩
6. 版本控制

解决的问题

1. 实现应用的快速构建、发布和部署，实现底层硬件和操作系统的解耦，满足用户在扩展性、可用性、可移植性等要求
2. 通过极致的弹性伸缩能力、高效的故障自愈能力、应用开放的高速迭代能力，实现业务短期迭代、产品更新、应用弹性伸缩，释放了云计算的效能
3. 通过与人员、流程和工具更好的结合，降低了企业信息系统维护成本，提升了信息系统的稳定性和安全性

Kubernetes的架构以及系统组件

物理架构：master/node模式

Master节点是控制节点，负责整个集群的管理和控制，主节点主要用于暴露API、调度部署和节点的管理。工作节点主要运行容器。

kubectl：k8s管理命令行工具

etcd：高可用kv键值数据库，存储k8s资源状态信息和网络信息

apiserver：整个系统的对外接口，是资源操作的唯一入口，提供了k8s各类资源对象的增删改查，是整个系统的数据总线和数据中心，提供认证、授权、API注册和发现机制

scheduler：负责pod的调度

controller-manager：与apiserver交互，实时监控和维护k8s集群控制器的监控状况，对有故障的进行处理和恢复

kubelet：node节点上kubelet定期调用apiserver的reset接口报告自身状态

kube-proxy：提供网络代理和负载均衡

阿里云容器服务ACK和原生K8S的区别

ack专有版、托管版、serverless版K8S的区别

1. Master节点的管理权限
2. 收费模式

如何做灰度发布

灰度发布时一种在生产环境中逐渐将新版本应用程序或功能部署给一部分用户的策略。

1. 制订计划：确定灰度发布的目标、时间计划和发布策略
2. 准备环境：确保目标环境已经准备就绪
3. 选择目标用户：根据一定规则或者随机选择一部分用户作为灰度发布目标用户
4. 发布新版本：将新版本的应用程序或功能部署到选定目标用户
5. 监控和收集反馈：对已发布用户进行监控，收集用户反馈和指标数据
6. 分析和评估：根据收集的数据和用户反馈，分析新版本实际使用情况，评估是否可以全面发布
7. 扩大范围：新版本通过评估之后，逐步扩大用户范围、降低发布风险
8. 完成发布：当新版本完成较大范围的验证之后，就可以全面发布新版本，替换旧版本

灰度发布需要慎重进行，确保发布过程中及时监控和回滚。同时，也要充分考虑用户体验和反馈，及时修复和改进新版本。

什么是蓝绿发布

1. 蓝绿部署是不停老版本，部署新版本然后进行测试，确认OK，将流量切到新版本，然后老版本同时也升级到新版本。
2. 灰度是选择部分部署新版本，将部分流量引入到新版本，新老版本同时提供服务。等待灰度的版本OK，可全量覆盖老版本。

灰度是不同版本共存，蓝绿是新旧版本切换，2种模式的出发点不一样。

什么是serverless架构

根据CNCF的定义，ServerLess是指构建和运行不需要服务器管理的应用程序。Serverless并不是不再需要服务器，而是无需管理服务器的架构方式，借助云产品提供的函数计算和事件触发功能，按需运行代码逻辑。在架构设计中可以将业务逻辑拆分为多个小的函数，并通过事件触发来调用函数，这样研发专注于业务逻辑的编写，运维转向SRE负责技术SLA的制订和保障，就可以以实现高效的资源利用和成本优化。

当前的serverless架构主要包含两个方面：提供计算资源的函数服务平台FaaS和提供托管云云服务的BaaS。

1. FaaS：负责代码部署和定义业务逻辑，是无需配置和管理，运行在无状态的容器中，按量计费。
2. BaaS：涵盖数据库、身份验证、云存储、推送通知、消息队列等，开发人员通过API和SDK来调用后端应用，而无需管理虚拟机或者容器。

serverless架构主流的应用代表有阿里云的函数计算和Amazon的Lambda以及开源的Knative和apache openwhisk。

什么是全链路跟踪

全链路跟踪是一种用于分析和调式分布式系统性能的技术，它可以追踪请求在系统中的传递过程，并记录每个组件的处理时间、调用关系等信息，从而帮助开发人员定位性能瓶颈或故障点。

1. 注入标识：在系统请求入口，会为请求生成一个唯一的标识，并将该标识传递到请求的各个组件中
2. 传递标识：当请求经过分布式系统的不同组件时，每个组件在处理请求时，记录下当前请求的标识
3. 记录信息：每个组件在处理请求时，记录开始时间、结束时间、调用关系等，这些信息通常倍发送专门的分布式追踪系统中。
4. 聚合追踪信息：将各个组件记录的信息进行聚合和分析，还原请求咋整个系统中的传递过程，并计算出各个组件的处理时间、调用链路等关键指标。

架构设计怎么和云产品结合

将架构设计与云产品结合可以带来包括弹性扩展、高可用、灵活性和改善成本效益。

1. 弹性扩展：云产品可以根据负载需求自动调整计算资源。在架构设计中，可以利用云产品的弹性扩展功能，根据负载情况自动增减计算实例，从而提高系统吞吐量和性能。
2. 高可用：云产品提供有多个可用区和多个数据中心的部署选项，可以通过在不同区域数据中心间进行负载均衡和容灾备份，增加系统可用性。在架构设计中，可以分布式部署应用程序和数据，利用云产品的负载均衡、容错机制和自动备份功能，保证系统的持续可用性
3. 异地容灾：云产品提供了跨地域的部署选项，可以在不同地理区域进行数据备份和容灾。在架构设计中，可以将关键数据进行异地备份。
4. 云原生架构：云原生架构设计是一种将应用程序设计为适应云环境的方式，借助云厂商提供的容器化、微服务、自动化管理的特性，可以实现可伸缩、可扩展、高度解耦的架构，以实现快速交付和部署的优势。
5. serverless架构：serverless架构是一种无需管理服务器的架构方式，借助云产品提供的函数计算和事件触发功能，按需运行代码实现业务逻辑，并按量计费。在架构设计中，可以将业务逻辑拆解为多个小的函数，并通过事件来触发调用函数，以其实现高效资源利用和成本优化。
6. 数据存储和分析：云产品提供各种数据存储和分析服务。在架构设计中，可以选择合适的云产品来存储和处理数据，以满足业务需求。

总之，结合云产品进行架构设计可以提供更好的弹性、可扩展性、高可用性和费效比。在设计过程中，需要根据业务和程序的需求结合云产品特性，选择合适的云产品，并遵循最佳实践进行架构设计和实施。

谈谈你对SLB的理解

SLB是一种用于分发网络流量和负载均衡的技术，用于提高系统的可用性、可扩展性和性能。部署和设计SLB时，需要考虑如下几个方面：

1. 选择合适的负载均衡算法：常见的算法包括:轮询、加权轮询、最小连接数、加权最小连接数等，需要根据业务需求和服务器资源不同选择合适负载均衡算法
2. 网络拓扑设计：常见的架构包括单层式、双层式和多层式架构。在设计过程中，根据系统的规模和需求，考虑SLB设备与服务器以及其他网络设备之间的连接方式和带宽需求，来选择合理的网络拓扑。

3. 高可用设计：为了保证SLB设备的高可用性，可以采用主备结构或集群模式，通过配置冗余设备或者多个SLB节点来保证系统的连续性
4. 健康检测与故障切换：配置健康检查机制，定期监测后端服务器的可用性。当服务器异常或者不可用时，SLB设备自动切换流量到其他健康服务器上，避免将流量分发到故障节点。
5. 动态负载均衡：根据实时的流量情况和服务器负载情况，动态调整负载均衡策略和流量分发策略。以调整权重、设置阈值等方式，实现流量均衡分配和性能优化。
6. 安全性设计：配置访问策略，限制只有授权的客户端可以访问SLB设备。此外，还可以采用SSL终端端到端加密来保护流量的安全。
7. 日志和监控：配置日志记录和监控系统，实时监控SLB设备和后端服务器的性能、流量情况和异常状态，并及时发现和解决问题。

在设计SLB时，需要根据具体的业务需求、系统规模以及资源限制综合考虑。同时，也需要定期进行性能评估和优化，确保SLB系统的稳定性和可扩展性。