1.云上业务系统高并发场景下，如何评估系统性能，如何评估性能瓶颈？

在云上业务系统面临高并发场景时，评估系统性能和识别性能瓶颈是确保系统稳定性和用户体验的关键步骤。以下是一些评估和优化策略：

### 评估系统性能

**1).响应时间测试**：

使用工具如Apache JMeter、LoadRunner或Gatling等，模拟用户行为，发送请求到服务器并记录响应时间。确保在不同负载条件下测试，以观察系统表现。

**2).负载测试**：

渐进式增加并发用户数或请求速率，监测系统在接近预期峰值负载及超出设计容量时的表现。这有助于确定系统处理能力和崩溃点。

**3).压力测试**：

目的是找到系统的最大承受能力，通过极端负载条件迫使系统达到其性能极限，识别系统何时开始出现错误或响应时间急剧上升。

**4).稳定性测试**：

在长时间内持续施加高负载，检查系统是否能维持稳定性能，包括资源使用情况、错误率等。

**5).监控与日志分析**：

利用云平台提供的监控工具（如AWS CloudWatch、Azure Monitor、Google Cloud Monitoring等）实时跟踪CPU、内存、网络IO、磁盘I/O等关键指标，结合日志分析工具定位问题。

### 评估性能瓶颈

**1).资源利用率监控**：

监控CPU、内存、磁盘I/O和网络带宽的使用情况，识别资源饱和点。高利用率并不总是坏事，但长期接近饱和可能意味着瓶颈。

**2).应用性能管理(APM)**：

使用APM工具（如New Relic、Dynatrace或Pinpoint）深入代码级别，分析事务追踪、慢SQL查询、线程阻塞等，精确定位问题代码或服务。

**3).分布式追踪**：

对于微服务架构，使用Distributed Tracing（如Jaeger、Zipkin）来跟踪跨服务调用，理解服务间的依赖关系和延迟。

**4).数据库性能分析**：

分析数据库查询性能，识别慢查询和索引缺失。使用数据库自带的性能分析工具或第三方工具进行优化。

**5).缓存策略评估**：

检查缓存命中率，合理设置缓存策略减少数据库负载。评估是否可以通过增加缓存层来减轻后端压力。

**6).网络延迟与带宽**：

测试云服务之间的通信延迟，优化网络配置，比如使用VPC内网通信、CDN加速等技术减少延迟。

### 综合分析与优化

根据测试结果，综合分析性能瓶颈所在，可能是硬件资源不足、代码效率低下、数据库设计不合理、网络配置不当等因素。

实施优化措施后，重复测试以验证优化效果，形成迭代优化的过程。

通过上述方法，可以全面评估云上业务系统的性能，并针对性地解决高并发场景下的性能瓶颈，保障业务的稳定运行。

2.高并发场景下，在不去大规模扩容比如ECS或容器等资源的前提下，如何提升用户访问体验，缓解高并发对系统的压力，提升系统性能？

1).**优化缓存策略**：

增强和优化缓存机制，如使用Redis、Memcached或本地缓存，减少对数据库的直接访问，特别是对于热点数据和频繁读取的内容。

**2).负载均衡**：

利用负载均衡器（如Nginx、HAProxy或云服务商提供的负载均衡服务）分散请求，确保请求均匀分配到各个服务器，避免单点过载。

**3).异步处理**：

将耗时的操作（如大文件上传、邮件发送、数据分析等）改为异步处理，释放主线程快速响应用户请求，提高系统吞吐量。

**4).数据库优化**：

优化数据库查询，使用索引、分表分库、读写分离等策略减少数据库访问延迟。考虑使用缓存数据库减少直接查询次数。

**5).资源预热**：

预先加载或预计算可能的高访问资源，确保在高峰到来前，相关数据和服务已经准备好，减少即时处理负担。

**6).动态内容静态化**：

尽可能将动态内容转化为静态或半静态内容，减少服务器动态渲染的压力，利用CDN分发。

**7).限流与降级**：

实施流量控制策略，如漏桶算法、令牌桶算法等，对超过阈值的请求进行限流或拒绝。同时，为非核心功能设置降级策略，在系统负载过高时暂时禁用或简化处理。

**8).微服务拆分与优化**：

对复杂系统进行微服务化改造，使得各服务间解耦，独立可扩展。优化服务间通讯，减少不必要的交互和数据传输。

**9).利用云服务弹性伸缩**：

即使不进行大规模手动扩容，也可以设置云服务的自动弹性伸缩策略，根据预设的指标自动增加或减少资源。

通过上述策略的综合运用，可以在不大幅增加基础资源的情况下，有效提升系统在高并发场景下的处理能力，改善用户体验。这些策略侧重于软件层面的优化，是成本效益较高的解决方案。

3.限流、熔断、降级对于高并发场景有作用吗，分别是什么作用？

**1).限流**：

**作用**：主要是为了控制系统的并发请求量，确保系统不会因为请求过多而崩溃。通过设置阈值，当请求量达到或超过这个阈值时，系统会拒绝超出部分的请求或者延迟处理，以此来保护系统资源不被耗尽。限流有助于实现系统的负载均衡，避免瞬间高峰流量对系统造成冲击，同时可以通过分配请求优先级，保证关键服务或接口的正常运行。

**2).熔断**：

**作用**：灵感来源于电路中的保险丝，当检测到某个服务的错误率超过设定阈值时，自动“熔断”该服务的调用，转而执行降级逻辑或者直接返回一个友好的错误提示给用户，而不是持续尝试可能会失败的操作，这样可以防止整个系统被某个不稳定服务拖垮。熔断机制通常会伴随有自我恢复功能，即在一段时间后自动尝试恢复服务调用，判断是否恢复正常。

**3).降级**：

**作用**：在系统面临压力或某些依赖服务不可用时，采取的一种应对措施，通过提供一种简化的服务版本或者默认的处理逻辑，来保证系统核心功能的可用性。例如，对于非核心业务，可能暂时关闭或者返回静态数据，而对于核心业务，则尽可能维持最基本的功能。降级策略可以确保在极端情况下，系统仍能提供有限但稳定的服务，避免完全不可用。

综上所述，这三种策略共同作用，可以有效提升高并发系统在面对突发流量或依赖服务故障时的韧性，确保系统的稳定性和用户体验。

4.如何防护DDoS攻击？

防护DDoS（分布式拒绝服务）攻击是一个多层面的过程，涉及预防、检测和响应策略。以下是一些有效的防护措施：

**1).保持系统更新**：确保所有系统和应用程序都是最新版本，并及时安装安全补丁，以减少利用已知漏洞的机会。

**2).配置防火墙和安全组**：设置防火墙规则，过滤掉明显恶意的流量，如来自已知恶意IP的流量或不符合标准协议的流量。在云服务器上，合理配置安全组，只开放必要的端口和服务。

**3).使用入侵检测与预防系统**（IDPS）：这些系统可以识别潜在的DDoS攻击模式，并在攻击造成损害之前采取行动。

**4).限制速率和连接数**：通过设置合理的连接限制和速率限制，可以减少攻击者利用大量连接淹没服务器的能力。

**5).采用DDoS防护服务**：很多云服务提供商和第三方安全公司提供DDoS防护服务，可以自动检测并缓解攻击流量，比如高防IP和流量清洗服务。

**6).分散流量**：使用CDN（内容分发网络）和负载均衡器可以分散流量，使得攻击者难以集中攻击单一点。

**7).准备应急响应计划**：提前制定应对DDoS攻击的应急预案，包括联系列表、流程文档和回滚策略，以便在攻击发生时迅速响应。

**8).监控和警报**：实施实时网络监控和流量分析，设置警报系统，在流量异常时立即通知运维团队。

**9).使用高带宽和冗余**：增加服务器的带宽容量，确保即使在遭受攻击时，仍有足够的带宽处理合法流量。

**10).教育和培训**：提高团队对DDoS攻击的认识，包括如何识别攻击迹象和遵循安全最佳实践。

记住，完全防止DDoS攻击是不可能的，但通过上述措施可以显著降低其影响，并提高系统的整体韧性。

5.假设攻击或者高并发访问流量过大，已经进去了云内，这时候该如何紧急处理应对？

启动自动或手动DDoS防护：

如果您正在使用华为云或其他具有内置DDoS防护功能的云服务提供商，如阿里云、腾讯云或AWS，立即启用相应级别的DDoS防护策略，确保云服务商的清洗中心能够开始过滤恶意流量。

调整云资源：

针对高并发访问，如果云服务器配置不足，可以通过弹性伸缩功能迅速增加实例数量，分散负载。对于DDoS攻击，联系云服务商升级您的带宽或购买临时的DDoS防护套餐，以应对超大流量攻击。

流量调度和隔离：

使用负载均衡服务，将流量分发至多个后端服务器，减轻单个服务器压力。

如果攻击目标明确，考虑暂时禁用非关键服务或API接口，减少受攻击面。

分析与监控：

迅速开启详细日志记录和性能监控，识别攻击来源和特征，以便进一步采取针对性措施。

利用云平台提供的实时告警和分析工具，了解攻击动态，指导应急响应。

更换IP地址或域名解析：

在极端情况下，可能需要临时更改受影响服务器的公网IP地址，并通过DNS重新解析到新的IP，切断攻击者与原服务器之间的连接。

寻求专业服务支持：

如果内部团队处理能力有限，及时联系云服务商的专业安全团队或第三方安全公司协助抵御攻击。

事后改进：

攻击过后，要复盘整个事件，优化安全策略，比如加强身份验证、限制非法访问、优化架构设计等，以预防类似情况再次发生。

请注意，实际操作中应结合具体云服务提供商的功能和服务特点来执行上述建议。在实际场景下，务必遵循云服务商官方文档中

的最佳实践和应急预案流程。

6.云防火墙用到了哪些底层技术？

云防火墙利用了一系列底层技术来确保云环境中的网络安全，以下是一些关键的技术组件：

**1).虚拟化技术**：云防火墙运行在虚拟化环境中，能够为每台弹性云服务器提供直接防护。这依赖于虚拟化技术，如hypervisors，来创建和管理虚拟网络环境和安全资源。

**2).分布式架构**：为了实现细粒度的微隔离和大规模部署，云防火墙采用分布式架构，使其能分散部署在各个云服务器或服务前端，提供低延迟和高可用性的防护。

**3).深度包检测（DPI, Deep Packet Inspection）**：这是一种数据包处理技术，允许云防火墙深入分析网络流量的内容，不仅仅是基于IP地址和端口，还能识别应用层协议、用户行为、内容类型等，以实施更精确的访问控制策略。

**4).流量可视化与分析**：结合大数据分析和机器学习技术，云防火墙能够实时分析网络流量模式，识别异常行为和潜在威胁，为安全策略的制定提供数据支持。

**5).威胁情报集成**：云防火墙通常集成了全球威胁情报源，这些情报包括最新的恶意软件签名、攻击模式、IP黑名单等，以便即时阻止已知威胁。

**6).策略引擎与规则管理**：基于策略的引擎负责执行预定义的安全规则和策略，这些规则可以高度定制，支持多维度的访问控制，比如基于用户身份、应用、时间、地理位置等。

**7).自动化与编排**：自动化工具和API接口使得云防火墙策略能够随着云环境的变化动态调整，支持DevOps流程，确保安全策略与基础设施配置同步更新。

**8).加密技术**：云防火墙支持传输层安全(TLS)、SSL卸载等功能，以保护敏感数据传输并执行安全策略，同时也能对加密流量进行必要的检查。

**9).微服务与容器安全**：随着云原生技术的发展，云防火墙也需适应微服务架构和容器环境，提供容器级别的网络策略实施和隔离。

**10).云原生集成**：云防火墙紧密集成到云平台的服务中，如VPC（虚拟私有云）、负载均衡器等，确保安全策略能够无缝应用于云上资源。

这些技术共同作用，使得云防火墙能够在复杂多变的云环境中提供高效、灵活且全面的安全防护。

7.NFV里具体用到了哪些技术？

网络功能虚拟化（NFV）作为一种将传统网络功能以软件形式运行在标准化的通用硬件上的技术，融合了多种关键技术来实现其目标。

具体而言，NFV涉及以下核心技术：

1).虚拟化技术：这是NFV的核心，它允许将单一的物理服务器分割成多个虚拟机（VMs），每个虚拟机可以运行不同的网络功能软件。虚拟化技术包括硬件虚拟化（如使用Hypervisor来管理CPU、内存等硬件资源的分配）和操作系统级虚拟化（如容器技术），这些技

术使得网络功能能够独立于底层硬件运行。

2).软件定义网络（SDN）：虽然SDN与NFV是两个不同的概念，但它们常常协同工作。SDN通过将网络控制平面与数据转发平面分离，实现了网络流量的灵活控制和管理。SDN控制器可以动态配置网络资源，为NFV环境中运行的虚拟网络功能（VNFs）提供所需的网络连接。

3).云计算技术：NFV利用云计算的资源池化、弹性扩展和自动化管理能力，将网络功能作为云服务提供。这包括使用云操作系统

（如OpenStack）来管理计算、存储和网络资源，以及利用云平台的API进行资源调配和生命周期管理。

4).网络编排与管理：为了高效部署和管理VNFs，NFV架构中采用了网络编排工具（如ETSI的MANO架构中的NFVO、VNFM和VIM组件）。

这些工具负责VNF的自动部署、配置、监控、故障恢复以及资源优化，确保网络服务的高可用性和灵活性。

5).存储虚拟化：为了支持VNFs的状态保存和数据持久化，存储虚拟化技术被用来创建一个统一的、易于管理和扩展的存储资源池。这包括块存储、对象存储和文件存储等多种存储类型，可以根据VNF的需求动态分配和调整。

6).高性能计算与加速技术：由于某些网络功能（如加密/解密、深度包检测）对计算性能要求较高，NFV环境中可能会采用GPU、FPGA或ASIC等硬件加速技术来提升处理效率。

7).容器技术：容器作为一种轻量级的虚拟化方式，可以更高效地部署和运行VNFs，相比传统VMs具有更快的启动速度和更高的资源利用率。Docker、Kubernetes等容器技术和编排平台在NFV领域逐渐获得应用。

这些技术的综合运用，使得NFV能够以更灵活、成本效益更高的方式提供网络服务，同时提高了网络的可编程性和响应速度。

8.解释一下，云防火墙和普通的硬件物理防火墙，还有用户自己在云上用ECS搭建的虚拟防火墙，有什么区别？

硬件物理防火墙：

物理实体设备：部署在企业的数据中心或网络边缘，作为网络入口或出口点，保护内部网络不受外部威胁。

固定位置：由于是实体设备，其位置固定且不能轻易迁移，适用于本地数据中心环境。

性能：通常具有高性能处理能力，尤其适合大型企业网络或要求严格的场景，如高吞吐量、低延迟的数据中心。

维护与升级：由企业自行管理和维护，包括硬件更新、软件升级和策略配置等。

云防火墙 (Cloud Firewall)：

虚拟化服务：云防火墙作为一种服务运行在云端，通常由云服务提供商提供并托管在云环境中。

弹性扩展：可根据业务需求进行动态扩容和缩容，无需关注底层硬件资源。

管理便捷：可通过云平台界面统一管理，简化了防火墙规则配置和维护工作，同时云服务提供商可能会提供持续的安全更新和维护。

多租户与隔离：在云环境中，云防火墙可以为不同客户提供隔离的网络安全保障，每个客户可以独立配置安全策略。

高度集成：与云服务紧密结合，例如与云负载均衡器、云服务器等服务无缝配合，实现全云环境下的安全防护。

基于ECS搭建的虚拟防火墙：

自主可控：用户可以在自己的云服务器（Elastic Compute Service，ECS）上部署虚拟防火墙软件，构建出定制化的防火墙环境。

灵活性：同样具备虚拟化特性，可以根据需求调整资源配置，但需用户自行负责系统的安装、配置、优化以及日常运维。

成本：相比于云防火墙服务，可能需要更高的技术投入和运维成本，但也提供了更大的灵活性和定制化程度。

整合与兼容性：可能需要更多地考虑与其他云服务的整合以及兼容性问题。

总结来说，硬件物理防火墙适合于传统的本地数据中心环境，强调高性能和稳定性；云防火墙更加便捷、灵活，

适应云环境的弹性需求；而基于ECS的虚拟防火墙更侧重于用户的个性化定制和深度集成，但同时也增加了用户自身的运维复杂度。

9.如果用户自己用ECS搭建虚拟防火墙，和云上防火墙有区别吗？

用户自己使用ECS（弹性云服务器）搭建虚拟防火墙与使用云服务商提供的云上防火墙之间存在一些显著的区别，主要体现在以下几个方面：

**1).管理复杂度**：

自建虚拟防火墙：用户需要自行安装、配置和维护防火墙软件（如iptables、firewalld或其他第三方防火墙软件），这涉及到操作系统层面的配置，可能较为复杂，需要具备一定的技术知识。

云上防火墙：云服务商通常提供图形化的管理界面或者API，让用户能够更加直观和简便地配置防火墙规则，减少了管理难度和时间成本。

**2).功能与特性**：

自建虚拟防火墙：功能和特性取决于所选软件，可能需要额外配置以支持高级功能，如深度包检测（DPI）、应用层过滤等。

云上防火墙：通常集成了更多高级安全功能，如自动化的威胁防护、集成的威胁情报、灵活的策略管理、以及与云平台其他安全服务（如WAF、DDoS防护）的紧密集成。

**3).可扩展性和性能**：

自建虚拟防火墙：受限于ECS实例的性能和规模，扩展性较差。若防火墙成为瓶颈，需要手动升级ECS实例或部署复杂的集群方案。

云上防火墙：设计为自动扩展，能够随着流量需求的增长而动态调整资源，确保高性能和稳定性，无需用户干预。

**4).维护与更新**：

自建虚拟防火墙：用户需要自行监控系统更新和安全补丁，以保持防火墙软件的最新状态，防止潜在的安全风险。

云上防火墙：由云服务商负责维护和更新，确保防火墙软件总是最新的，减轻了用户的维护负担。

**5).成本**：

自建虚拟防火墙：虽然ECS实例本身可能已有成本，但自行搭建可能不直接增加额外费用，除非考虑人工维护和潜在的性能升级成本。

云上防火墙：通常是按使用情况计费，虽然提供了便利性，但也意味着需要为此支付额外的服务费用。

**6).可靠性与合规性**：

自建虚拟防火墙：可靠性依赖于用户自身的架构设计和维护水平，可能需要额外工作来满足特定的合规要求。

云上防火墙：云服务商通常会提供SLA（服务等级协议），保证服务的高可用性，并且通常符合多种行业安全标准和合规要求。

综上所述，用户自建虚拟防火墙提供了更高的定制自由度，但伴随而来的是更高的管理复杂度和责任；而云上防火墙则提供了更为便捷、可扩展且通常更为安全的解决方案，尽管可能涉及额外成本。选择哪种方式取决于用户的特定需求、技术能力以及预算。

1. 云上VPN产品有哪些，用到哪些VPN技术？

云上VPN产品主要指的是云计算服务提供商（如华为云、阿里云、AWS、Azure等）提供的虚拟专用网络服务，旨在帮助用户安全地连接本地数据中心、分支办公室或远程员工与云端资源。云上VPN产品通常利用以下几种常见的VPN技术：

**1).IPSec (Internet Protocol Security)**：这是一种成熟的安全协议，用于在IP网络中提供安全服务，包括认证、加密和封装技术，以确保数据在公共互联网上传输时的安全性。云上的IPSec VPN通常用于建立本地网络与云VPC之间的安全隧道。

**2).SSL/TLS (Secure Sockets Layer/Transport Layer Security)**：SSL/TLS VPN允许用户通过浏览器安全地访问内部网络资源，无需安装专用客户端软件，仅需浏览器支持。它适用于远程办公场景，可以对单个应用或服务进行细粒度的访问控制。

**3).L2TP/IPSec (Layer 2 Tunneling Protocol with IPSec)**：结合了L2TP的数据封装技术和IPSec的安全保障，提供了一种安全的远程访问方式，常见于移动设备或需要点到点连接的场景。

**4).GRE (Generic Routing Encapsulation)**：虽然GRE本身不提供加密，但它经常与IPSec一起使用，以创建一个能够封装多种协议数据包的隧道，适合于需要跨不同网络传输多种协议数据的情况。

**5).VXLAN (Virtual eXtensible LAN)**：主要用于数据中心网络虚拟化，它在UDP之上封装以太网帧，实现了二层网络在三层网络上的扩展，虽然不是严格意义上的VPN技术，但在云环境中常被用来构建大型的虚拟网络隔离。

以华为云为例，其虚拟专用网络（VPN）产品就采用了上述技术中的IPSec，以确保数据传输的安全性和稳定性。同时，IP VPN产品则采用了多协议标记交换（MPLS）技术，为客户提供私有数据通道服务。这些云上VPN产品都强调了即开即用、高安全、高可靠以及易于管理的特性，旨在满足企业对云上业务安全互联的需求。

11.ipsecvpn有哪些加密算法？

IPSec VPN支持多种加密算法以确保数据的安全传输，这些算法主要包括对称加密算法和非对称加密算法，以及用于数据完整性和认证的哈希算法。以下是常用的几种加密算法：

### 对称加密算法：

**1).AES (Advanced Encryption Standard)**：这是目前最常用的对称加密算法，支持128、192和256位密钥长度，提供高效且安全的数据加密。

**2).3DES (Triple Data Encryption Standard)**：作为一种老式但仍然可用的算法，3DES通过三次DES加密来提高安全性，提供168位的有效密钥长度。

### 非对称加密算法：

主要用于密钥交换过程，确保对称密钥的安全传输。

**1).RSA**：广泛应用于身份验证和密钥交换的公钥加密算法。

**2).Diffie-Hellman (DH)**：一种密钥协议，允许双方在不安全的通道上生成共享的密钥，常用于IKE (Internet Key Exchange) 协议中。

**3).ECDH (Elliptic Curve Diffie-Hellman)**：基于椭圆曲线密码学的密钥交换协议，相较于传统DH，提供相同安全级别的同时所需密钥长度更短。

### 哈希算法：

用于数据完整性校验和认证。

**1).SHA (Secure Hash Algorithm)**：家族包括SHA-1、SHA-256、SHA-384、SHA-512等，其中SHA-256及以上版本因其更强的安全性被推荐使用。

**2).MD5 (Message-Digest Algorithm 5)**：尽管曾经常用，但现在因其安全性问题而不建议用于安全认证。

在IPSec协议栈中，这些加密算法会被用于封装安全载荷(ESP)和认证头(AH)，其中ESP负责数据的加密和可选的认证，而AH主要负责数据的完整性和来源验证。具体使用哪些算法取决于实际部署时的安全策略和合规要求。

12.混合云场景，涉及到专线，包括专网及互联网，如何保证或提高专线的高可用性？

答：拉多根专线，相关线下物理网络设备也要多台，做高可用。对于多根专线，做BFD或NQA监测，监测搭配路由，如果监测失败就自动切换到备用路由。包括专线搭配VPN去做主备。

13.BFD监测的时间，多久能切换过去？

答：通常是300ms发一个监测包，连续3次失败，900ms就切换，可以做到秒级。

14.关于阿里云的云上安全，如果用户的某台ECS因为安全漏洞被黑客植入了木马webshell，如何结合阿里云的相关产品去排查，处理，应急，溯源呢？

1. .排查阶段：  
   云安全中心：  
     
   登录阿里云云安全中心，查看告警信息和安全报告，确认是否存在Webshell相关的安全风险提示。  
   利用云安全中心的“漏洞扫描”功能，检查ECS实例上的操作系统、应用程序和其他组件是否存在未修复的安全漏洞。  
   态势感知：  
     
   利用态势感知服务，查看异常登录、恶意进程、网络流量异常等情况，确定是否有异常活动。文件完整性检查：  
     
   使用云安全中心或ECS自带的文件系统审计功能，对比文件变更历史，找出被篡改的文件和Webshell的确切位置。

2).处理阶段：

隔离感染实例：  
  
将疑似感染的ECS实例从生产环境剥离，避免木马进一步传播或造成数据泄露。  
清除木马：  
  
根据云安全中心提供的信息，删除或隔离发现的Webshell文件。  
执行病毒查杀，阿里云提供了云查杀服务，可以针对服务器进行全面扫描和清理。  
修复漏洞：  
  
对于导致木马植入的安全漏洞，尽快应用补丁或更新软件版本，防止再次被利用。  
应急响应：

备份重要数据：  
  
在清除木马之前，备份可能被影响的重要数据，以防误删或潜在的数据丢失。

调整安全策略：  
  
根据实际情况，强化ECS实例的访问控制策略，例如设置更为严格的防火墙规则、关闭不必要的端口、加固SSH登录安全等。  
启用WAF和DDoS防护：  
  
启用阿里云Web应用防火墙(WAF)以防止后续Web层面的攻击，同时开启DDoS防护服务，防止流量型攻击。

1. .溯源阶段：  
   日志分析：  
     
   查看ECS实例的操作系统日志、Web服务器日志、数据库日志等，通过阿里云的日志服务(SLS)或云审计服务(CAS)，收集并分析攻击轨迹。  
   攻击源追踪：  
     
   利用态势感知的IP信誉功能，追溯攻击源IP及其相关联的信息，判断是否涉及已知的僵尸网络或攻击组织。
2. 事件复盘：  
     
   分析黑客入侵途径，查明是通过哪个应用漏洞或弱口令被利用，然后修复这些薄弱环节，提高整体安全水平。最后，根据阿里云的服务协议和支持体系，及时提交工单或联系技术支持团队，获得专业的安全应急响应指导和帮助。同时，应根据这次事件的经验教训，定期对系统进行安全评估和加固，建立和完善长期的安全运营机制。

15.一个全球企业，在阿里云上北京和法兰克福地域都都部署了业务系统，对于企业内部员工，和对外业务，如何进行访问的优化，

加速，应该使用哪些阿里云的产品？

答：比如CEN、VPC对等连接、高速通道、VPN网关等。

16.你提到的主要还是企业内网专线互联，那互联网的呢？

答：如果针对全球企业的对外互联网业务，可以通过CDN、DCDN、GA等手段进行访问优化和网络加速，还可以比如在香港等区

域搭建中转节点提高访问速度。

17.你们专有云用到哪些云原生产品了？

答：用到的不是太多，比如ACK、EDAS这些，主要是ACK。

18.你说ACK，主要是哪些业务去使用？为什么考虑使用ACK？

答：主要是考虑到利用ACK，或者说K8S、容器的高弹性、更快伸缩、即开即用的特性，相比ECS更加灵活。我们有些大数据分析业务

用到了。

19.K8S有哪些组成部分？

答：master和worker，master包括api-server、kube-ctl、controller-manager、etcd、kube-scheduler，worker包括kubelet、

kube-proxy、容器等。worker是运营NODE、POD、容器环境的。然后介绍了下刚才提到的各个组件的作用。

20.你刚才提到大数据，阿里云上有哪些大数据产品？

答：比如DataWorks、EMR、MaxCompute。

21.EMR和MaxCompute有什么区别？

答：这个没答出来。其实主要是EMR是提供一些开箱即用的开源大数据PaaS平台，比如Hadoop、Spark、Hive、Flink、Mapreduce等功能，

需要一定大数据技术能力。MaxCompute主要是阿里自研大数据产品，提供一站式的大数据处理计算展示功能的SaaS产品，更加的便捷，

技术门槛更低，开箱即用，用户只需关注业务层面需求。