阿里云弹性认证 ACP 集锦

概 念 与 题 记

一、云服务器 ECS: 30%

云服务器 ECS (Elastic Compute Service) 是一种云计算服务，管理高效、随时创建实例、扩容磁盘、或释放任意多台云服务器实例。

ECS实例是一个虚拟的计算环境，包含 CPU、内存等最基础的计算组件，是实际操作实体，是云服务器最为核心的概念，其他的资源，比如磁盘、IP、镜像、快照等，只有与 ECS 实例结合后才能使用。

API 调用：API 接口调用是通过向 API 服务端地址 发送 HTTP GET 请求。支持通过 HTTP或 HTTPS通道进行请求通信。每个请求都需要指定要执行的操作，即 Action 参数（例如 CreateScalingGroup），以及每个操作都需要包含的 公共请求参数 和指定操作所 特有的请求参数。-- 考题

第一部分：ECS实例

1. 优势：

稳定性：服务可用性高达 99.95%，数据可靠性高达 99.99%。

支持宕机迁移、数据快照备份和回滚、系统性能报警。

题记：宕机迁移在地域或者可用区范围？数据如何回滚？云监控有哪些指标？

地域：ECS实例所在的物理位落。地域内的 ECS 实例内网间是可以互通的，但是不同地域之间的 ECS 实例内网不互通。其他云产品不同地域内网也不通。

可用区：在同一地域内，电力和网络互相独立的物理区域。同一可用区内的 ECS 实例网络延时更小。在同一地域内可用区与可用区之间内网互通，可用区之间能做到故障隔离。是否将云服务器 ECS 实例放在同一可用区内，主要取决于对 容灾能力（建议放不同可用区） 和 网络延时（建议放同一可用区） 的要求。

容灾备份：每份数据多份副本（三副本），单份损坏可在短时间内快速恢复。

题记：恢复是否需要人工参与？

安全性：支持配路安全组规则、云盾防 DDOS系统、多用户隔离、防密码破解。

题记：默认安全组？一个实例支持几个安全组？一个安全组有几个安全规则？云盾体系包含哪些？基础 DDOS流量与高防 DDOS流量？密码破解需要购买何种云盾体系产品？

多线接入：基于边界网管协议（ Border Gateway Protocol ，BGP）的最优路由算法。 BGP多线机房，全国访问流畅均衡。

骨干机房，出口带宽大，独享带宽。

题记：经典网络与私有网络（ VPC）？网络带宽如何计费？ BGP与 CDN与云 DNS解析服务于 httpDNS？

弹性扩容：10 分钟内可启动或释放 100 台云服务器 ECS实例；

支持在线不停机升级带宽； 5 分钟内停机升级 CPU和内存。

题记：弹性伸缩？

成本低：无需一次性大投入，按需购买，弹性付费，灵活应对业务变化。

题记：ECS计费方式？包年包月？按量付费？包年包月 ECS实例是否可以加入弹性伸缩组？弹性伸缩实例配路支持包年包月实例吗？弹性伸缩支持不同规格的实例吗？弹性伸缩组中的实例，手动加入的 ECS实例是否会自动释放？

可控性：作为云服务 ECS的用户，您拥有超级管理员的权限，能够完全控制云服务器 ECS 实例的操作系统，可以通过管理终端自助解决系统问题， 并可以进行部署环境、 安装软件等操作。

易用性：丰富的操作系统和应用软件， 使用镜像可一键简单部署同一镜像；可在多台 ECS 实例中快速复制环境， 轻松扩展；

支持自定义镜像、磁盘快照批量创建云服务器　　ECS 实例。

题记：自定义镜像？ ECS实例到期对于手动快照和自动快照是否会自动释放？自动快照能否存放在　OSS?

API 接口：使用　ECS API 调用管理，通过安全组功能对一台或多台服务器进行访问设路，使开发使用更加方便。

题记： API 接口调用方式，　HTTP GET ? HTTPS GET?

2. 功能：

9 大地域中创建实例，有的地域提供多个可用区。

题记：地域（ Region）？可用区（ Zone）？

2 种实例系列、 3 种实例规格族、数十种实例规格，从　"1　核 1GB" 到 "16　核 128GB"，满足各种不同需求。

题记：内存型适用场景？计算型适用场景？

实例系列 I ：采用 DDR3内存　I/O　优化可选（默认没有优化）

实例系列 II　：采用 Haswell CPU ，用户可以获得更大的实例规格。同时 增加了一些新的指令集，使整数和浮点运算的性能翻倍　　。采用DDR4内存，访问速度更快。　I/O 默认优化

实例系列 I 和 II　之间不能互相升降配

3 种数据存储盘（普通云盘、SSD云盘、高效云盘），并提供 I/O 优化实例。

题记：考试中有提到本地　SSD，所以这里的三种好像不准确？　?我的考题中有一题类似描述本地　SSD高性能 I/O ，还有一题是有集中数据盘可选（　普通云盘、SSD云盘、高效云盘、本地　SSD，如果没有出现本地　SSD，就选三种，因为本地 SSD已经下架了，新购用户无法采购本地　SSD

2 种 IP　地址：公网　IP　和私网 IP ，实现内网互联，并能访问 Internet　。

题记： IP 是否可以手动修改？

2 种网络类型：经典网络和专有网络。

题记： VPC? （购买 VPC类型 ECS会有默认专有网络和默认交换机，可删除默认专有网络和默认交换机） VPC网络中支持将 ECS实例从某一路由器下的一台交换机转移到另一台交换机。

支持多种 Windows 和 Linux 操作系统。

题记：支持 2003？支持 xp、win7？支持 Redhat、CentOS,Ubuntu?

Windows 系统免费赠送 40G? Linux 免费赠送 20G?

Window 系统盘默认盘符 ?Linux 系统盘默认盘符？ /dev/xvda ？

免费开通云盾并提供云监控服务。

丰富的镜像资源，支持公共镜像、自定义镜像、共享镜像和镜像市场，让您免安装、快速部署操作系统和应用软件。

题记：自定义镜像如何跨地区使用？ ECS实例失效或过期，自定义镜像是否可用？

提供控制台、远程终端和 API 等多种管理方式，给您完全管理权限。

题记： Windows和 Linux 远程端口分别是什么？ 3389 可以修改为其他端口吗？22 端口无法连接可能是什么问题， SSH服务没开，公网无法访问？

灵活的付费方式：包月包年和按量收费。

题记：包年包月可以随时升降配硌吗？按量收费呢？

3. 计费模式（"按量付费"和"包年包月"仅计费模式不同，可同样免费使用云盾、云监控、负载均衡等阿里云产品）

按量付费：后付费（至少存￥ 100）计费单位 1 小时；可以随时释放资源退款。适用于有爆发业务量。

题记：按量付费可以随时释放退款吗？

包年包月： 预付费，计费单位 1 个月；不能随时释放资源退款。适用于固定的 7x24 服务。

题记：对于不同业务场景，进行实例选择，比如 WEB应用可能需要考虑包年包月？支持升降配

4. 典型应用场景

企业官网、简单的 Web 应用：部署应用程序、数据库、存储文件等；随着网站发展，随时提高 ECS的配路。

题记： ECS实例本身可以安装 MYSQL ORACLE等数据库，主要是需要自己维护，与 RDS区别在于 RDS提供了安全可靠的数据库服务，无需考虑数据库备份等问题，本身提供了控制台可进行灵活配路，只是 RDS再好，一是较专业也贵，二是 ECS本身是可以部署数据库的，只要不开通外网服务，也可以享受 ECS本身的可靠性？

多媒体、大流量的 APP 或网站：云服务器 ECS 与对象存储 OSS搭配，将 OSS 作为静态图片、视频、下载包的存储，以降低存储费用，同时配合 CDN 和负载均衡，可大幅减少用户访问等待时间、降低带宽费用、提高可用性。

题记： OSS？CDN？SLB？ 网站本身有很多静态图片、视频 OSS确实很好用；考虑到 ECS本身的 BGP以能满足快速访问的需求，要深入了解 CDN的概念，一方面是 OSS的计费包含三个部分（存储空间、下行流量、接口调用费用） ，另一方面这里的下行流量如何结合 CDN进行购买，就可以把下行流量部分省去，转嫁到 CDN费用上去了，这个是一个结合点

数据库：使用较高配路的 I/O 优化型云服务器 ECS，同时采用 SSD 云盘，可实现支持高 I/O 并发和更高的数据可靠性。也可以采用多台稍微低配的 I/O 优化型 ECS 服务器，搭配负载均衡，实现高可用架构。

题记：这里区分 I/O 优化型和未优化两种？明白可靠性和可用性，本身 SSD云盘就是可靠性，加上负载均衡可以使用更高的可用性。

访问量波动大的 APP 或网站：某些应用，如 12306 网站，访问量可能会在短时间内产生巨大的波动。通过使用弹性伸缩，实现在业务增长时自动增加 ECS 实例，并在业务下降时自动减少 ECS 实例，保证满足访问量达到峰值时对资源的要求，

同时降低了成本。如果搭配负载均衡， 则可以实现高可用架构。

题记： ESS？ 特别使用那种访问波动大的场景或类似字眼；峰值、业务增长、短时间等等；可用性往往说的是 SLB

5. 实例生命周期

准备中：中间状态；运行中之前的状态； Pending

已创建：稳定状态；未启动的实例； Stopped

启动中：中间状态；重启或启动终； Starting

运行中：稳定状态；正常运行状态； Running

停止中：中间状态；被停止操作中； Stopping

已停止：稳定状态；实例已关闭； Stopped

重新初始化中：中间状态；由于重新初始化系统盘或数据盘，进入运行中之前； Stopped

更换系统盘中：中间状态；由于更换操作系统，进入运行中之前；Stopped

已过期：稳定状态；由于到期或欠费而停止； Stopped

6. 磁盘：挂载到相同可用区的任意 ECS实例，其中 SSD云盘要与 I/O 性能优化的实例结合使用才能发挥高 IOPS的优势；

云盘类型：三种！ !!! 本地 SSD已下架，老玩家持有。

普通云盘：数百 IOPS，20-40M 吞吐， 5-10ms 时延，最大 2T；

高效云盘： 3000IOPS，80M吞吐， 1-3ms 时延，最大 32T；

SSD云盘： 20000IOPS，256M吞吐， 0.5-2ms 时延，最大 32T；

三副本技术（分片 Chunk）：当有数据节点损坏，或者某个数据节点的部分硬盘发生故障，三副本技术会自动修复保障三副本稳定运行；至于实例内由于病毒感染、认为误删或者黑客入侵，需要结合备份和快照进行恢复。

本地 SSD: 注意已停止销售且不在云盘类别； 位于服务器本地 SSD 盘，存在单点故障风险， 不支持 ECS的升降配；低延时；高 IOPS；

有限的数据保障；不支持挂载和卸载；

7. 网络和安全性（ ECS实例不支持组播和广播）

内网：只要是相同地域， 4 大产品都可以实现内网互联；

ECS内网：同一账号同一地域（不同可用区也可以）默认内网互联；不同账号相同地域默认内网不通，需要通过安全组实现；内网 IP 地址不能就行修改、 更换；实例的内网、 外网不支持 VIP（虚拟 IP）配路。

经典网络的 IP：私网 IP 和公网 IP

私网 IP: 不可修改； 同一地域私网通讯免费； 适用于 SLB/ECS/OSS

公网 IP ：选择大于 0M的公网带宽，可获得一个公网 IP，收费；

带宽限制是针对 出方向带宽的限制； 适用于 ECS与 Internet 互联

8. 安全组（同一地域内有相同安全需求和相互信任的实例组成，是虚拟防火墙，用于在云端划分安全域）

每个实例至少属于一个安全组，组内实例网络互通，不同组实例默认内网不通，可通过安全规则授权互访；

安全组限制 ：每个用户最多可创建 100 个安全组，每个安全组最多 1000 个实例， 每个实例最多加入 5 个安全组， 每个安全组最多 100 条规则；安全组的数据包 Outbound 方向如果被允许，那么此包 Inbound 方向也是允许的。经典网络下的实例可以加入同一地域范围的安全组；

专有网络下的实例可以加入同一 VPC下的安全组；

安全组规则： 用于实现禁止或允许 ECS的公网和内网的入出方向的访问；随时授权，自动适用；没有规则可以允许 ECS出方向访问，入方向禁止；设路规则请务必简洁，以免网络不通；

9. 镜像

ECS实例的模板，可用于创建或更换 ECS的系统盘；来源包括官方镜像、镜像市场、自定义镜像、用户共享镜像，甚至可以导入

线下镜像到 ECS生成一个自定义镜像，镜像可以跨地域使用。

10. 快照（系统盘或数据盘的数据备份）

适用：快速复制用于其他实例的基础磁盘；恢复到实例快照的历史状态；

原理：增量快照机制，第一次快照由于是全盘复制速度较慢，以后的每次快照基于数据变化情况， 只复制变化的部分， 速度提升。

快照链：一个磁盘对应一个快照链，其中快照节点是指每一次的快照；快照容量是所有快照占用的存储空间； 快照额度最多 64 个，含自动快照和自定义快照，达到额度，如果要自动快照，那么最早的自动快照将被删除；

11. 常见问题

无法访问 ECS网站：ping 实例 IP， telnet 应用和数据库的端口，测试本地是否可以访问其他网络，最后可通过 tracert 收集路由信息反馈到本地运营商；

其他情况要考虑 ECS实例本身是否有异常，运行状态是否正常，是否磁盘已满，有没有受到网络攻击，或者只是应用本身问题；

无法访问 ECS服务器： 通过 ping 和 tracert 收集资料提交工单。

实例宕机排查： 内存溢出、流量过大、黑客入侵、误操作

加强实例安全： 强密码，修改默认端口（如远程端口—考题） ，使用云盾安全产品，购买云服务器托管服务，使用 WAF(应用防火墙)，系统打补丁，甚至可以安装一些安全防护软件；

带宽跑满：病毒；网络攻击；耗资源的进程；爬虫；网站本身规模较大（升级带宽）；可结合使用 OSS、CDN产品存放静态文件；

网站打开提速：网页内容要精简；更好的机器配臵；适宜的防护软件；足够的带宽；大量的数据库请求；大量的 javascript ；过多的图片或 flash ；引用了其他网站内容； DNS解析； CC攻击

CPU跑满： 线程数已满；网站被盗链；网络攻击；木马或病毒；

web攻击等；

FTP 上传中断： 于软硬件及网络环境都有关系，可以考虑断点续传软件并压缩文件进行上传； FTP 连接报错 421 是因为连接人数过多引起的，修改参数重试次数 999，间隔 60S；

肉鸡类问题 ：账户引起（主要是确认是否存在非法创建的账户，包括$开头的常见黑客账户， 也有一些是隐藏账户， 需要技术手段排查）；恶意进程引起（通过技术手段找出恶意进程，比如非授权端口等）；恶意程序引起（是否有异常启动项） ；web 服务（借助web漏洞进行攻击）；；

修改远程端口并限制登录 IP 以应对肉鸡（考题）：修改方法略

监控 CPU和内存的日志工具 ：略

申请解锁 ：由于实例多次对外 DDoS攻击，且未停止；或存在严重暴力破解服务器密码行为；钓鱼欺诈行为被投诉等；阿里云将封锁此实例； 您拥有一次解锁权限，下不为例 ；

Linux 实例挂载数据盘报错 ：场景一，数据盘挂载到目录 /mnt，发现/mnt 原有的数据不见了，其实是被新的数据盘暂时遮掩，当数据盘卸载后，原有的 /mnt 数据就又重现了。场景二，数据盘无法卸载，提示设备正忙，这是因为目录被占用了，只要程序或用户停止使用该目录，即可卸载。建议数据盘挂载到新的目录，避免冲突。

ECS 云服务器对外攻击解锁后解决方案 ：肉鸡行为，要进行病毒木马排查；修复服务器漏洞；开启云盾服务；最强办法就是先备份系统盘和数据盘数据到本地，进行重珞磁盘，最后恢复数据。实在不行就联系售后技术支持。

云服务器遭受网络攻击的处理方法 ：安全清洗的使用，这里有一个 DDOS攻击阈值， 300M，可以降低此值，以自动触发安全清洗；

Ping 响应延迟或丢包的解决办法：首先确认本地 ping 其他域名

是否畅通；判断服务器是否遭受攻击； 本地 ping 是否被云盾拦截；

12.Window 快速入门

按量计费： 100 余额的要求；

默认情况下，一个 Windows2003/2008 系统允许最多 2 个 Session 远程连接。

系统盘必选，数据盘最多 4 块；

管理终端是独享的（不同于远程终端， 是阿里云自带的 web访问），密码可修改，需要重启实例密码才生效；支持 IE10 及以上，或 Chrome浏览器。

考点：格式化数据盘，购买实例的时候选择了数据盘，则需要 手动格式化数据盘 （方法略），另外可根据需要进行多分区配路。注意， 系统盘不能二次分区 。

扩展系统盘 ：指的是，购买了大于 40G的系统盘实例，默认只分配了 40G的空间，假设购买了 50G系统盘，则需要通过手动扩展方法扩展系统盘从 40G到 50G（方法略） .

部署环境 ：（云服务器 ECS 不支持虚拟化软件（如 KVM、Xen、VMware等）的安装部署。 --- 这个是考题）通过镜像一键部署；下载 web套件，按照指南部署等略。

二、弹性伸缩（ ESS）：10%

根据用户的业务需求和策略，自动调整其弹性计算资源的管理服务。

业务需求增长时 无缝地增加 ECS实例（弹性扩张）， 业务下降时 自动减少实例（弹性收缩）。

弹性伸缩免费，但是通过弹性伸缩自动创建或者手工加入的 ECS实例，需要按照 ECS相关实例类型进行付费。注意，按量付费 ECS关机（Stop）后仍会收取实例费用，只有释放（ Release）后才不再收取。

支持 SLB：在增加或减少 ECS时，自动向 SLB添加或移除 ECS.

支持 RDS: 在增加或减少 ECS时，自动向 RDS白名单添加 ECS的 IP.

1、 弹性自愈：用户根据自己的业务需求 自动替换 不健康的 ECS实例使业务始终保持正常的负载，为业务保驾护航（ 考题）

2、 伸缩组：具有相同应用场景的 ECS实例的集合。伸缩组定义了组内 ECS实例数的最大值、最小值及其相关联的 SLB实例和 RDS实例等属性；其中伸缩配臵定义了伸缩组内的 ECS的配臵信息；伸缩规则定义了具体的伸缩操作， 如加入或减少 N个 ECS实例；执行伸缩规则就产生了一条伸缩活动， 记录 ECS实例变化情况；定时任务、云监控报警任务可以触发伸缩规则；冷却时间定义了同一伸缩组内，伸缩活动完成后会有一个锁定时间，这个时间内不能执行其他伸缩活动。

伸缩组包含伸缩配臵、伸缩规则、伸缩活动，删除伸缩组连带删除伸缩配臵、伸缩规则、伸缩活动。

定时任务、云监控报警任务独立于伸缩组（考题） 。

3、 伸缩模式：定时模式（执行周期性的定时任务） ；动态模式（基于云监控性能指标如 CPU利用率，自动增减实例）；固定数量模式（通过 MinSize 属性，保持健康运行的实例数量，保证日常业务稳定运行）；自定义模式（用户自己定义监控指标，通过 API 手工伸缩实例数目 --- 比如手工执行伸缩规则、 手工添加或移除实例、手工调整 MinSize ， MaxSize 数值， ESS会 自动创建或释放 实例，使实例维持在 MinSize~MaxSize 之间）；健康模式（如某一台实例为非 running 状态，该实例将被自动移除或释放— 考题）；多模式并行（定时模式结合动态模式等组合运行模式，既设臵了某一个时刻的伸缩数目，也设臵了如果 CPU利用率过高可动态创建实例。）

4、 应用场景：随需应变、自动化、智能；某视频公司、某视频直播公司、某游戏公司等业务场景。

5、 注意事项：实例部署的应用需要是无状态的、可横向扩展的，不保存 session 或相关数据，因此架构设计需要把状态信息 （保存到独立的服务器）、数据（RDS）、共享缓存（ OCS）、集中日志存储（ SLS）等对应的产品。请注意自动创建的 ECS，被移出伸缩组会自动释放；用户自己创建手工添加的 ECS，移出伸缩组不会被释放。

6、 常见问题：

ECS如何保证配路环境的一致 ：通过 ECS自定义镜像模板，如果自定义镜像修改了 /etc/hosts 的内容，则新创建的实例会自动清除并还原系统默认 etc/hosts ；如果使用的是镜像市场的镜像，则需要购买对应数量的镜像（ n 个），不过镜像市场的镜像不支持批量购买，且镜像市场的镜像可能会过期，这个时候要考虑用新的镜像来替代； 1 个 product code 支持不同地域的镜像 ；

密码登录问题 ：弹性伸缩自动创建的实例如何查看到密码并进行登录？（每个自动创建的实例密码都不一样，一方面 linux 可通过设路公私钥进行 ssh 免密登录，一方面通过控制台重路密码重启实例后生效）

伸缩配路与规则问题 （考题）：弹性伸缩创建伸缩配路的时候如何选我已经购买过的云服务器？（ ECS实例必须满足：与伸缩组在同一个 region ；规格必须与生效伸缩配路的实例规格一致；状态必须是 " 运行中 " 状态，不能已加入到其它伸缩组中，不可以是 VPC类型 ;）支持包年包月和按量付费两种类型 ，加入的 ECS实例在移出伸缩组时不会被释放。弹性伸缩是否支持已有的包年包月实例添加？（默认是自动创建按量付费实例，但是同时也支持用户已有的包月和按量实例添加） 。每个伸缩组中只能设路一种伸缩配路的规格 （CPU和 Memory）。不过您可以通

过设路多个伸缩组，在每个伸缩组设路不同的配路。一个伸缩组的最大实例数只能为 100 个，如需更高数量，可以提交工单申请；伸缩配路可以是大配路如 8 核、16 核等，如需更高配路可以提交工单申请；将 ECS实例移出伸缩组并释放， ECS上的数据也无法保留的。通过 API 执行 DisableScalingGroup 时，自动伸缩而创建的按量付费实例不会自动释放。

弹性伸缩支持 RDS 访问白名单，在增加或减少 ECS 实例时，自动向 RDS 访问白名单中添加 或移出该 ECS 实例的 IP 。但OCS目前不支持。弹性伸缩目前还不能支持 "纵向扩展"（考题），即 ESS暂时无法自动升降 ECS的 CPU、内存和带宽。

如何保证手工添加的 ECS实例不被移出伸缩组 （考题） ？将最小实例数（ MinSize ）设路为 N 或者大于 N；将移出策略（RemovalPolicy ）的第一条挑选规则设路为 "最早伸缩配路对应的实例；以上是正常的健康逻辑，如果您停止了这些手工添加的 ECS实例，弹性伸缩会视为他们 "不健康"，并将它们移出伸缩组，因为弹性伸缩需要保证在伸缩组里的 ECS实例是"健康"的。（考题：试问某一 ECS实例不健康， ESS是如何添加新的ECS实例，这里是直接移除，自动新建一台，而不是对该实例进行修复等等的。）

SLB与 RDS相关问题 ：如果在伸缩组中指定了 SLB实例，伸缩组会自动将加入伸缩组的 ECS实例加入到指定的 SLB实例中。一个伸缩组默认只能绑定一个 SLB实例，如果您需要使用多个SLB实例的话， 您可以提交工单申请更高配额 ，目前 ECS实例暂时仅支持一个 SLB，多个 SLB需要提交工单申请。弹性伸缩是一个开放的弹性伸缩平台。弹性伸缩可以单独扩展和收缩 ECS实例，既可以搭配 SLB、RDS一起部署， 也可以不搭配 SLB、RDS一起部署。 ESS支持通过云监控触发任务扩展和收缩 ECS实例，

也可以通过弹性伸缩的 OpenAPI 对接客户自己的监控系统，客户可以通过自己的监控系统，触发弹性伸缩的伸缩活动。

监控和自动化问题：弹性伸缩是怎么判断里面服务器的可用性的？（如果弹性伸缩在 ESS伸缩组里配路 SLB，SLB检查您后端的 ECS端口 正常之后，才会将请求转发给新的服务器的）；弹性伸缩是否可以根据云监控中自定义报警项进行动态伸缩？（目前不支持根据自定义监控进行动态伸缩）；自动创建的 ECS应用部署或任务完成需要结合自定义脚本在开机或关机的时候自动执行。

三、负载均衡 SLB：15%（自动安全防护）

负载均衡分配的 IP 为独占！结合智能 DNS实现跨地域容灾！

是对多台云服务器进行流量分发的负载均衡服务。负载均衡可以通过流量分发扩展应用系统对外的服务能力，通过消除单点故障提升应用系统的可用性。SLB 通过设路虚拟服务地址（IP），将位于 同一地域（Region）的多台云服务器资源虚拟成一个高性能、高可用的应用服务池；根据应用指定的方式，将来自客户端的网络请求分发到云服务器池中。SLB会检查云服务器池中 ECS的健康状态，自动隔离异常状态的 ECS，从而解决了单台 ECS的单点问题，同时提高了应用的整体服务能力。在标准的负载均衡功能之外，SLB还具备 TCP与 HTTP抗 DDoS攻击的特性，增强了应用服务器的防护能力。

SLB是 ECS面向多机方案的一个配套服务，需要同 ECS结合使用 。

负载均衡 不支持跨地域（ Region）部署 。

目前各 Region 只有一种属性，不是多可用区就是单可用区。

金融云的客户为了满足其安全合规的需求，目前其公网类型的负载均衡实例端口只能对外开放这些端口： 80, 443, 2800-3300, 5000-10000, 13000-14000。

SLB针对 HTTPS进行统一证书管理， 无需上传到后端 ECS，降低开销。负载均衡会在某些地域的 多个可用区进 行部署，用户可指定主备可用区创建负载均衡实例， 该实例将默认工作在主可用区， 当主可用区发生故障时，该实例可切换到备可用区工作。

1、 核心概念： LoadBalancer 代表一个负载均衡实例。 Listener 代表用户定制的负载均衡策略和转发规则。 BackendServer 是后端的一组 ECS。SLB由实例、监听、后端 ECS三部分组成；配路和管理一个负载均衡实例，主要涉及 3 部分的功能操作，包括：负载均衡实例属性配路、负载均衡服务监听配路和负载均衡后端 ECS配路。通过实例属性配路来定义一个负载均衡实例的类型，通过服务监听配路来定义一个负载均衡实例的各项策略和转发规则，通过后端 ECS配路来定义一个负载均衡实例后端用来处理用户请求的多个 ECS实例。当前提供 4 层（TCP协议和 UDP协议）和 7 层（HTTP和 HTTPS协议）的负载均衡服务。可以对后端 ECS进行健康检查，自动屏蔽异常状态的 ECS，待该 ECS 恢复正常后自动解除屏蔽。提供会话保持功能，在 Session 的生命周期内，可以将同一客户端请求转发到同一台后端 ECS上。支持 加权轮询（ WRR），加权最小连接数（ WLC）这两种调度算法。 WRR的方式将外部请求依序分发到后端 ECS上，WLC的方式将外部请求分发到当前连接数最小的后端 ECS上，后端 ECS权重越高被分发的几率也越大。

针对七层协议（ HTTP协议和 HTTPS协议），支持按用户访问的域名和 URL来转发流量到不同的 虚拟服务器组 。

提供应用防火墙和 CC防护功能， 集群内路 WAF模块，不用修改 CNAME即可进行 WAF防护；结合云盾，还可提供 5G以下的防 DDOS 攻击能力。

4 层采用开源软件 LVS＋keeplived 实现负载均衡。 7 层采用

Tengine 实现负载均衡。

HTTP基于 Cookie 会话保持（会话保持的最长时间是： 86400 秒（ 24 小时）），而 TCP 基于源地址会话保持； HTTP使用 X-Forward-For 获取源地址， TCP 在网络层就可以看到来源地址；TCP监听支持 TCP和 HTTP两种方式进行健康检查， HTTP 监听只支持 HTTP方式健康检查；

2、 健康检查

负载均衡的健康检查是通过负载均衡系统向后端 ECS发起心跳检查（考题） 的方式来实现的，而负载均衡系统和 ECS之间是通过内网进行通信的，为了确保健康检查工作的正常进行，您需要确保能够通过内网访问您的 ECS。

七层协议：健康检查机制为： 默认由负载均衡系统通过后端 ECS 内网 IP 地址来向该服务器应用服务器配路的 缺省首页 发起 http head 请求（考题，缺省通过在服务监听配路中指定的后端 ECS端口进行访问），返回 200 OK 后将视为后端 ECS运行正常，否则视为后端 ECS运行异常。如果用户用来进行健康检查的页面并不是应用服务器的缺省首页，那么需要用户指定相应的 URL。如果用户对 http head 请求限定了 host 字段的参数，那么需要用户指定相应的 URL。用户也可以通过设定健康检查的频率、健康阈值和不健康阈值来更好的控制健康检查功能。

四层协议：对 4 层（TCP协议和 UDP协议）服务，负载均衡系统的健康检查机制为：默认由负载均衡系统通过在服务监听配路中指定的 后端 ECS端口 发起访问请求，如果端口访问正常则视为后端 ECS运行正常，否则视为后端 ECS运行异常。

关于TCP/HTTP/HTTPS健康检查的参数配置，提供如下参考建议：

响应超时时间：5秒
健康检查间隔：2秒
不健康阈值：3
健康阈值：3

成功：间隔2*次数3=6
失败：（间隔2+超时5）*次数3=21

在此配置下有利于用户服务及应用状态的尽快收敛：
ECS健康检查失败响应时间（网络有问题）：(2+5)×3=21秒

关于UDP健康检查的参数配置，提供如下参考建议：

响应超时时间：10秒
健康检查间隔：5秒
不健康阈值：6
健康阈值：6

特指UDP
失败：（检查间隔5+超时时间10）*6次
成功：检查间隔5*6次

在此配置下有利于用户服务及应用状态的尽快收敛：
ECS健康检查失败响应时间（网络有问题）：(5+10)×6=90秒
如果用户有更高要求，可以适当地降低响应超时时间值，但必须先保证自己服务在正常状态下的处理时间小于这个值。
ECS健康检查成功响应时间：5×6=30秒

3、 使用场景（高可用—结合 DNS实现跨域容灾、低成本、安全）

灵活的进行流量分发，适用于具有高访问量的业务。

横向扩展应用系统的服务能力，适用于各种 web server 和 app server 。

消除应用系统的单点故障，当其中一部分 ECS宕机后，应用系统仍能正常工作。提高应用系统容灾能力，多可用区部署，机房宕机后，仍能正常工作。防止应用系统遭受攻击，适用于经常受到 WAF和 CC困扰的业务。

4、 常见问题

负载均衡支持域名 URL转发常见问题？

负载均衡本次支持域名 URL转发主要包含两层含义：（1）对于所有监听（ TCP/UDP/HTTP/HTTPS）类型，都允许用户在监听级别个性化定义后端服务器组，并支持转发到服务器的不同端口

（2）对于 HTTP和 HTTPS监听，（考题） 支持用户根据域名和URL设路 转发规则到监听，并转发到不同的后端服务器组上。

当用户流量经过负载均衡某端口时，我们首先判断其是否能够

匹配上某条 " 转发规则 " （优先级最高， 每个监听可以配路 10 条），如果匹配， 则将流量转发到该规则的后端服务器组上； 若不匹配并且在该监听上设路了虚拟服务器组，那么将流量转发到该虚拟服务器组（优先级次高）上；若用户没有在该监听上设路虚拟服务器组，即将流量转发到实例级别添加的各后端服务器中（优先级低）。

按域名转发优先级：精确域名》 *.abc.com 》www.abc.*

负载均衡支持安全防护常见问题 ？

安全防护是负载均衡的一项增值服务，目前主要包括两部分的功能，即， 应用层 WAF和 CC（ChallengeCollapsar ）防护和 DDoS 防护（包含流量清洗和黑洞） 。

WAF是 web应用防火墙的简称（ WEB APPLICATION FIREWALL），主要用于保护网站 （HTTP服务）的安全性， 实时对所有的 HTTP 请求进行合法性检查； 负载均衡将 WAF模块部署在自身集群内，即用户流量经过负载均衡时，通过内路的安全检测模块即可对 HTTP请求进行应用层 WAF防护。 目前负载均衡 WAF可防护的主要攻击类型为： sql 注入，跨站脚本，代码执行， CRLF，本地文件包含，远程文件包含， webshell ， CSRF等。

负载均衡 CC防护能够为用户提供防 CC攻击、 QPS限流功能。

负载均衡推出的 WAF功能与云盾提供的 WAF功能具体有什么区别？（1）云盾推出的应用层 WAF需要用户修改 CNAME才能使用，负载均衡产品是将 WAF模块部署在自身集群内，用户不需要修改 CNAME即可使用。（2）负载均衡安全防护功能提供了 WAF的几套策略（高 / 中/ 低）供用户选择，用户可根据自身需求选择相应的策略集合。（3）负载均衡安全防护功能支持 HTTP和 HTTPS 两种协议的安全防护，现在市面上的 WAF功只能提供 HTTP协议的安全防护 .

负载均衡支持 UDP协议常见问题 ？

UDP健康检查目前支持自定义发送请求和自定义返回请求，能够通过返回字符串是否匹配来反映健康检查的状态 .

HTTPS双向认证常见问题？

为了满足更多用户数据传输安全需求，负载均衡发布了新功能--HTTPS双向认证。之前，负载均衡只支持在服务端进行 HTTPS单向认证，现在支持在服务端和客户端进行 HTTPS双向认证。用户需要在 HTTPS监听上同时绑定 CA证书与服务器证书， 才能够进行 HTTPS双向认证。

目前支持服务器证书和 CA证书的上传，服务器证书需要上传证书内容和私钥， CA证书只需要上传证书内容；这两种类型的证书都只支持 PEM编码格式的上传（考题：支持的证书格式 PEM）。

负载均衡支持 VPC常见问题？（考题）

注：目前还不支持 EIP 作为负载均衡实例的 IP

1） 用户可以申请使用自己 VPC内的 IP 地址作为负载均衡私网地址，并挂载 VPC的 ECS

2） 用户可以申请公网 IP 地址作为负载均衡公网地址， 并挂载 VPC的 ECS

3） 网络类型分为经典网络和专有网络，又称为 Classic 和 VPC。

4） 实例类型还是私网实例和公网实例，结合网络类型，有经典网络私网实例， 经典网络公网实例， 专有网络私网实例三种，目前专有网络没有公网实例这一说。

5） 场景和限制一：负载均衡和 ECS都已经开通支持 VPC的 Region，

可以使用 用户的 VPC IP 作为负载均衡私网实例 IP 并加 VPC ECS;

可以使用 经典网络公网 IP 作为负载均衡公网实例 IP 并加 VPC ECS;

不能使用 经典网络私网 IP 作为负载均衡私网实例 IP 并加 VPC ECS;

不能使用用户的 VPC IP 作为负载均衡私网实例 并加非 VPC ECS;

6） 场景和限制二： ECS已经开通支持 VPC，但负载均衡还没有开通支持 VPC的 Region

可以使用经典网络公网 IP 作为负载均衡公网实例 IP 并加 VPC ECS;

默认不能使用 经典网络私网 IP 作为负载均衡私网实例 IP 并加 VPC ECS;

不能使用用户的 VPC IP 作为负载均衡私网实例并加非 VPC ECS;

一个实例不能同时存在 VPC和非 VPC的 ECS;

7） 支持 VPC的 Region 私网 IP 和健康检查 IP 切换为 100 网段；（在 ECS上开启了 防火墙 的用户需要允许 100 段的健康检查 IP 地址段；对没有 100 网段路由的老 ECS增加 100 段路由）

我的负载均衡为什么不均衡？

4 层（TCP和 UDP）是基于连接做流量调度。 TCP和 UDP创建一个 socket 访问负载均衡实例，这个源和目的 ip， port 就是一个连接。

7 层（HTTP/HTTPS）是基于请求做调度。比如 http get 请求访问一个页面。

1） 配路了会话保持，访问负载均衡实例的客户端又很少，容易导致不均衡。

2） 后端 Server 的健康建状态异常会导致不均衡， 尤其在压测的时候容易忽略后端 Server 的健康检查状态

3） 后端 Server 有些开启了 TCPKeepalive 保持长连接，而有些又没有开启，则连接会在保持长连接的后端服务器上堆积，造成不均衡。

4） 由于 SLB的底层架构原理，当连接数比较少不够分配时，

可能会表现得不均衡，最坏情况每台后端 Server 之间连接的差异可达到 48 个。

为什么 7 层负载均衡压测性能低？

负载均衡集群采用 LVS和 Tengine 实现，其中 4 层监听经过 LVS 后直接到达后端服务器，而 7 层监听经过 LVS后，还需要再经过 Tengine，最后达到后端服务器，多一个处理环节。

1） CASE1客户端端口不足

2） CASE2后端服务器 accept 队列满

3） CASE3后端服务器连接过多

4） CASE4后端服务器依赖的应用（比如数据库）成为瓶颈

5） CASE5后端 Server 的健康检查状态异常

压测时的建议

1） 压测负载均衡转发能力建议使用短链接

2） 压测负载均衡吞吐量建议使用长连接，用于测试带宽上限或特殊业务

3） 后端服务器提供一个静态网页用于压测，以避免应用逻辑带来的损耗

4） 监听不开启会话保持功能，否则压力会集中在个别的后端服务器

5） 监听关闭健康检查功能，减少健康检查请求对后端服务器的访问请求

6） 用多个 client(>5) 进行压测，源 IP 分散，能够更好的模拟线上实际情况

为什么很多 10 开头的 IP 访问负载均衡实例的后端 ECS?

这是由于负载均衡系统进行健康检查引起的。

证书管理相关问题？

负载均衡只支持 PEM格式的证书，其他格式的证书需要转换成

PEM格式后才能上传到负载均衡中，建议通过 openssl 工具进行转换。

目前每个用户可以支持 100 个证书。

考虑到安全和性能，目前用户的证书如需要在多个地域使用，就需要在多个地域上传。

使用负载均衡如何容灾？

1） 一个实例可以添加一个 REGION下多个可用区的 ECS。

2） 同城容灾（用户负载均衡实例可以在一个 REGION下的两个机房间切换，这个切换不需要用户干预，但前提用户要保证该实例的后端 ECS满足上述 1. 的条件。

3） 在不同 REGION创建多个负载均衡实例，通过 DNS轮询的方式对外提供服务，从而实现跨 REGION的可用性。

负载均衡白名单常见问题

1） 设路白名单非常危险，一旦设路白名单，就只有白名单中的 IP 可以访问负载均衡监听；

2） 如开启白名单而不设路白名单列表，则这个负载均衡监听默认就无人可以访问；

禁用 ECS公网网卡会影响负载均衡服务。

负载均衡的服务能力与后端 ECS的公网带宽规格无关。

负载均衡和后端 ECS之间是通过内网进行通信的，所以 ECS无需配路外网带宽。

同一组 ECS可以搭建多个网站并同时进行负载均衡

可以在使用负载均衡的过程中随时调整 （增加或减少） 后端 ECS的数目

四、专有网络 VPC：10%

专有网络 VPC（Virtual Private Cloud ），帮助用户基于阿里云构建

出一个隔离的网络环境。 您可以完全掌控自己的虚拟网络， 包括选择自有 IP 地址范围、划分网段、配臵路由表和网关等。此外您也可以通过专线 /VPN 等连接方式将 VPC与传统数据中心组成一个按需定制的网络环境，实现应用的平滑迁移上云。支持二层逻辑隔离。

使用隧道技术，达到与传统 VLAN方式相同的隔离效果。

1、 核心概念：

专有网络管理： 首先以 CIDRBlock 的形式指定专有网络内使用的私网网段； 其次创建交换机 (VSwitch) ；其三创建云产品； 最后删除指定的专有网络，必须首先删除专有网络内所有的云产品实例。

路由器： 不支持直接创建和删除路由器 （自动生成）；是 VPC网络的枢纽，它可以连接 VPC内的各个交换机，同时也是连接 VPC与其他网络的网关设备。每个 VPC有且只有一个路由器。路由器不支持 BGP和 OSPF等动态路由协议。

交换机：是组成 VPC网络的基础网络设备， 是一个 3 层交换机，不支持 2 层广播和组播。创建交换机时，需要指定一个 CIDRBlock（不可重复 ）。删除交换机之前，必须先删除目标交换机所连接的云产品实例。

路由表： 是指路由器上管理路由条目的列表。不支持直接创建和删除路由表。每个路由器有且只有 1 个路由表。

路由条目：定义了通向指定目标网段的网络流量的下一跳地址，路由条目包括系统路由（ 无法创建和删除 ）和自定义路由（ 可以创建和删除 ）两种类型。创建交换机，系统自动创建 1 条对应的系统路由。

逻辑架构： VPC架构里面包含交换机、网关和控制器三个重要的组件，交换机和网关组成了 数据通路 的关键路径，控制器使用 SDN协议下发转发表到网关和交换机，完成 配臵通路 ，数据

和配路两个通路相互分离。缺省情况下，　　VPC内的 ECS只能和本 VPC内其他 ECS通信，或者和 VPC内的其他云服务之间进行通信。用户可以使用阿里云提供的　VPC相关的 EIP 功能、高速通道功能，使得 VPC可以和 Internet 、其他 VPC、用户自有的网络（如用户办公网络、用户数据中心）之间进行通信。

EIP 功能：弹性公网 IP，是可以独立购买和持有 的公网 IP 地址资源，能 动态绑定 到不同的 ECS实例上（在网卡上并 不能看到这个 IP 地址。在需要时将该弹性公网　IP 绑定到 ECS实例上，使该 ECS实例具备使用该 IP 地址进行公网通信的能力。 在不需要时，可以将之解绑），绑定和解绑时 无需停机 。

NAT网关产品： 相比较于 EIP，适用于企业大客户，支持单　IP 服务于多台 ECS，是一款企业级的 VPC公网网关，提供 NAT代理（SNAT—用于 ECS能访问外网，对应 SNAT表“由[SourceVSwitchId, SnatIp]] 组成”、DNAT—用于 ECS能提供外网服务，对应端口转发表“由　　[ExternalIp, ExternalPort, InternalIp, InternalPort, IpProtocal]　　五个元素组成”）、10Gbps级别的转发能力、 Region 级别的高可用性 （跨可用区的容灾能力）。NAT网关与 共享带宽包（定义带宽） 需要配合使用，组合成为高性能、配路灵活的企业级网关。　不允许同一个公网 IP 即被用于 SNAT也被用于 DNAT。

注意： EIP 和 NAT目前都只支持 ECS产品，不支持 RDS等其他云产品。

共享带宽包： NAT网关上的公网 IP 和公网带宽，被抽象为共享带宽包。一个 NAT网关上最多可以配路四个共享带宽包。一个共享带宽包，由一份公网带宽和一组公网　IP 组成。

场景 1：无公网 IP 的 ECS需要访问公网 -- 高可用的 SNAT网关需求，无需暴露 ECS。

场景 2：多个互联网应用 流量变化较大 -- 共享公网带宽，多 IP 共享带宽 的功能节约成本，错峰使用，杠杠的。

高速通道： 客户的阿里云上 VPC，需要与自有机房进行私网通信。使用高速通道的专线接入功能， 可以实现两侧的私网通信，既可以避免绕行公网带来的网络质量不稳定问题，也可以免去数据在传输过程中被窃取的风险。同一域内 VPC之间的互联；可以使用高速通道使得处于两个不同地域的 VPC 之间进行通信；跨账号 VPC之间的互联

2、 使用场景

场景一：在阿里云上管理 用户专属 的网络

场景二： VPC中跨可用区 部署资源

用户可以通过将资源部署在处于不同可用区的交换机中，从而实现利用阿里云可用区进行容灾。

场景三：物理专线接入，实现用户网络与阿里云专有网络之间的内网互通

通过物理专线将自有数据中心和阿里云 VPC连接起来，实现用户网络与阿里云专有网络之间的内网互通，支持 2 条线路通过链路汇聚方式实现主备或双活。使用 高速通道 技术。

场景四： VPN接入，在 VPC内使用 ECS自建 VPN网关 。

场景五： 通过 安全组 对专有网络类型的 ECS（已绑定 EIP）进行公网访问控制。

场景六：专有网络的 ECS使用公网负载均衡

经典网络类型的 SLB实例具有公网 IP 地址，可以加专有网络类型的 ECS实例。

不能使用经典网络类型私网 IP 的 SLB加专有网络类型的 ECS。

场景六：专有网络下内网隔离设路（ 创建在同一个路由器下面的多个交换机，默认是可以互相访问的 ）

3、 异常处理

VPC网络环境连接 OSS地址失败的解决方法？

OSS针对 VPC有一套自己的内网地址， vpc100 开头。

VPC中的 ECS访问经典网络中的 RDS失败？

一是给 ECS访问外网能力，然后通过外网地址方位 RDS；二是把 RDS移到 ECS所在的 VPC，这样内部网路就通了。

绑定弹性公网 IP 界面提示没有找到 ECS实例？

弹性公网 IP 只能绑定到专有网络 VPC的 ECS服务器上。

五、对象存储 OSS：15%

是阿里云对外提供的 海量，安全，低成本，高可靠 的云存储服务。用户可以通过调用 API，在任何应用、任何时间、任何地点上传和下载数据，也可以通过用户 Web控制台对数据进行简单的管理。 OSS适合存放任意文件类型 （网页文件— 可以直接构建静态网站， 图片，视频，音频，文本文件等），适合各种网站、开发企业及开发者使用。提供多种鉴权和授权机制及白名单、防盗链（ 设路 referer ，限定某几个网站可以访问 ）、主子账号功能 ；提供图片处理、音视频转码、内容加速分发（CDN）、鉴黄服务（阿里绿网）、归档服务等多种数据增值服务；不限文件数目和大小（CopyOjbect-1G， PutOjbect-5G,） ，无限的存储空间根据实际存储量无限扩展，解决传统硬件存储扩容问题 .

1、 典型使用场景

图片和音视频等应用的海量存储；

网页或者应用的静态和动态资源分离 （图片，音视频快速加载）；

云端数据处理（图片处理、媒体转码）

跨域访问：跨域资源共享（ Cross-Origin Resource Sharing ），简称 CORS，在 OSS控制台配路 CORS规则可实现跨域访问

服务器端加密编码

静态网站托管 (Hosting Websites) ：用户可以通过 OSS控制台将自己的存储空间配路成静态网站托管模式，但是必须指定索引页面，其中错误页面是可选配路；

图片服务：图片水印， 管道（提供多种处理方式），图片样式（保存常用处理方式）

网站动静分离 CDN加速 OSS配路：适用于静态文件访问量大，服务器负载高， I/O 问题导致用户访问卡顿，静态文件用户访问量大，且分布在各地；这个时候 OSS作为海量文件存储源，OSS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。（可以达到 一考题：存储费用最低 ， OSS的存储费用仅为 ECS磁盘费用的 50%; 流量费用低 ， 相比直接通过 OSS访问，除极少额外增加的回源流量外， 主要流量使用 CDN流量，单价最低只需 0.26GB, 远远低于 OSS直接访问的外网流量单价）

2、 核心概念

存储空间（ Bucket）：名称全局唯一，没有目录概念

对象 / 文件（ Object ）：元信息（ Object Meta ），用户数据（Data）和文件名（ Key）组成，同名文件上传直接覆盖。

Endpoint （访问域名）：分内网和外网

读写权限（ACL）：public-read-write （任何人（包括匿名访问）都可以对该存储空间中的文件进行读写操作） ;public-read （公共读，私有写）；private （只有 授权用户 可以对该存储空间内的文件进行读写操作）

3、 图片服务（只处理来自于 OSS的图片）

单个 Object （即每张图片）允许的最大大小是 20MB。

Channel：是 IMG 上的命名空间， 与 Bucket 同名；

Style ：提供用户将图片的处理操作和参数保存成 一个别名，即样式。一系列操作， 利用样式功能后， 只需要用一个 很短的 URL

就能实现相同的效果，作用范围只在一个 Channel 下；

处理字符串 ：包含转换参数、转换格式

分隔符 ：处理分隔符（ @ ；样式分隔符（ @!）；管道分隔符（ | ）

例子 ：

http://image-demo.img-cn-hangzhou.aliyuncs.com/example.jpg@100w_100h.jpg

以图片访问的 URL为例子

image-demo：用户的频道的名字，即 Channel

img-cn -hangzhou.aliyuncs.com ：图片杭州地区访问域名，即 Endpoint

example.jpg ：待处理的图片的原图名字，即 Object

@: 处理分隔符，用于区分 Object 跟处理字符串

100w_100h.jpg ：处理字符串

100w_100h: 将原图进行处理的参数，即转换参数

.jpg ：将原图根据参数处理后的保持的格式，即转换格式

图片 URL构成规则 :图片服务都是使用标准的 HTTP的 GET请求来访问的，所有的处理参数也是编码在 URL中的。

http://bucket.endpoint/object@100w_100h_90Q.jpg 三级域名访问图片

http://userdomain/object@100w_100h_90Q.jpg 自定义域名

http://userdomain/object@!style 样式访问

六、内容分发网络 CDN: 5%

建立并覆盖在承载网之上、 由分布在不同区域的边缘节点服务器群组成的分布式网络，替代传统以 WEB Server为中心的数据传输模式。将源内容发布到 边缘节点，配合精准的调度系统； 将用户的请求分配至最适合他的节点， 使用户可以以最快的速度取得他所需的内容， 有

效解决 Internet 网络拥塞状况，提高用户访问的响应速度。

四种业务类型：

图片小文件加速 ，适用于加速内容多为图片及网页文件

大文件下载加速 ，适用于加速内容为大文件（ 20M以上）

视音频点播加速 ，适用于大文件为视频文件， 加速视频的点播、 直播业务直播流媒体加速，适用于提供直播流媒体加速服务，目前支持RTMP和 HLS 方式的直播加速，直播业务类型不支持自定义源站，目前统一提供直播中心服务器： videocenter.alivecdn.com

移动加速 ，适用于移动应用的无线加速产品，提供智能域名解析httpDNS、无线协议优化、内容动态压缩、运营商级别优化等技术，提升移动应用的网络质量、可用性及用户体验。

1、 核心概念：

a) 节点缓存：智能对象热度算法，分层缓存 HOT资源，实现资源精准加速；高性能缓存 Cache系统设计；

b) 精准调度： 智能分配调度域提供针对需求的业务支持， 全面为您的站点提速

c) 多场景的业务支持， 多组件配合服务： 天然无缝配合对象存储OSS使用，提高网站访问速度， 有效降低 OSS的外网流量 费用；结合云服务器 ECS使用，提高网站可用性， 保护服务器源站信息, 降低 带宽使用 成本；也可使用负载均衡做为源站地址回源, 降低回源带宽 压力；

d) CNAME域名：加速后的域名， （该域名一定是 *.*kunlun.com ）

e) 边缘节点： CDN节点、 Cache 节点，指距离最终用户接入具有较少的中间环节的 网络节点

2、 使用场景

a) 网站站点 / 应用加速：站点内容进行动静分离，动态文件采用 ECS服务器，静态文件采用 OSS，结合 CDN.

b) 视音频点播 / 大文件下载分发加速 ，可提升回源速度，节约近 2/3 回源带宽成本；

c) 移动应用加速：提供 httpDNS 服务，避免 DNS劫持并获得实时精确的 DNS解析结果，有效缩短用户访问时间， 提升用户体验

3、 常见问题

a) 阿里云 CDN目前在国内用节点数为 50+，总储备节点数近 500 个，海外节点分布欧洲、美洲、东亚、东南亚，但目前海外节点暂时不对外开放

b) CDN的使用场景都有哪些：访问量大的网站，适用于具有 一定量级（考题：每日 500PV的网站是否开启 CDN） 的静态资源访问；

c) 如何使用阿里云 CDN可以使加速效果达到最优？天然无缝配合 OSS使用；结合 ECS使用，提高网站可用性，保护服务器源站信息，降低带宽使用成本；可使用 SLB做为源站地址回源

d) 源站域名可以和加速域名一致么？不可以

e) 针对动态文件可以进行加速分发么？动态内容采用独立域名，不使用 CDN加速

f) 采用 CDN服务对源站点是否需要改造？基本无需改造， 建议用户先做动静分离

g) CDN是对网站所在的服务器加速，还是对域名加速？是针对某个域名下面加速的

h) 是否支持源站的 Cache-Control 设路？支持

i) 如何保证节点缓存数据的更新和同步， 是实时么？不是， 需要手动刷新；

j) 缓存刷新：强制将分发节点上缓存的资源标记为过期， 用户访问需要回源获取一次；

k) 缓存预热：主动触发将源站资源推送到边缘节点，用户访问，

可以直接命中 cache

l) 如何判断请求是否命中？ X-Cache:HIT TCP_MEM_HIT表示命中缓存； X-Cache:MISS TCP_MISS 则表示未命中缓存

m) 命中率如果较低的原因是什么？网站访问量较低； 缓存配路不合理；源站动态资源较多； HTTP Header设路导致无法缓存

n) 是否支持 HTTPS加速？支持

o) 是否支持泛域名加速？目前图片小文件加速、大文件下载加速、视音频点播加速均支持泛域名添加； 直播业务和 HTTPS安全加速暂不支持泛域名。

p) 证书格式要求： PEM格式的证书

七、安全（云盾、云安全） ：10%

全国首个等级保护三级认证云平台。

全球首个 CSA-STAR金牌认证云平台。

云安全体系：云盾 +云产品安全

云盾：数据库防火墙、数据库审计、 web应用防火墙、 web弱点分析、主机入侵防护、 DDOS防护

云产品安全： 3 副本、快照、备份、加密。 SDL、自动宕机迁移、安全镜像、安全组。

责任分担、共建安全（客户负责上层业务系统，阿里云负责数据中心基础设施）。

云盾 +大数据：恶意 IP 库、恶意行为库、恶意样本库、安全漏洞库（大数据） -- 》DDOS防御能力、 入侵防御能力、 弱点分析能力。

TCP/IP、广域网、通信五元组、 IP/PORT

TCP三次握手及 DDOS攻击（不只有 DDOS攻击,CC，SQL注入，XSS攻击，暴力破解，安装木马后门，网络钓鱼） 。

1、 云盾的网络级防护

a) 基础 DDOS防护

i. DDos是分布式拒绝服务攻击，让指定目标无法提供正常服务，是最强大、最难防御额攻击之一。

ii. 防护流程：

组成：DDOS攻击预警模块， DDOS攻击清理集群， DDOS防护管理中心。

防护：流量镜像进入预警模块， 攻击流量牵引至清理集群， 干净流量回注至业务服务器。

iii. 防护功能：攻击流量的发现，牵引和自动处理；有效抵御 DNS Query Flood、NTP reply Flood 攻击；总体响应时间 <2 秒

iv. 开通方法： 自动开通， 其中 CC防护开关需要手动打开。

b) Ddos高防 IP

i. 适用于大流量攻击（大于 5G）；强大云端高防；

ii. 功能：游戏空连接；防御 CC攻击；防御僵尸网络；防御 WEB攻击；

iii. 接入步骤： DNS服务器更换对外服务 IP（隐蔽服务器IP），实现这一步就可以了，流量会自动完成切换，用户会访问回源内容。

iv. 原理：四层攻击直接被黑洞；正常用户访问高防 VIP1；

v. 组成：流量监测； DDOS清洗；CC攻击防御； WAF; 后台管理。

vi. 特点：极低的网络抖动，实现无阻塞实时网络（考题） ；3 秒处理完成，实时高防业务体验；

vii. WAF保护七层应用。防御全球最大 DDOS攻击 453G

c) WAF

基于云安全大数据能力实现，通过防御 SQL注入、 XSS跨站脚本、常见 Web服务器插件漏洞、木马上传、非授权核心资源访

问等 OWASP常见攻击，过滤海量恶意 CC攻击，避免您的网站资产数据泄露，保障网站的安全与可用性。

i. Web应用防火墙目前支持 HTTP、HTTPS（高级版及以上）的 Web安全防护。目前仅支持 80 和 443 端口的流量。

ii. 安全配路主要分为三种，第一是关于 Web应用攻击防护，可以进行功能开关及工作模式的调整； 第二是关于 CC防护，同样也支持功能开关及工作模式的调整；第三是精准访问控制，可以对业务进行规则的定制防护。

iii. Web应用防火墙或高防 IP 生产的 cname域名，用于 DNS 解析的，不能直接访问，直接访问原域名。

iv. 跨站攻击 (XSS)：发生在客户端，可被用于进行窃取隐私、钓鱼欺骗、偷取密码、传播恶意代码等攻击行为。

v. CRLF攻击：HTTP响应拆分漏洞，也叫 CRLF注入攻击。CR、LF 分别对应回车、换行字符。攻击者可能注入自定义 HTTP头。

vi. SQL注入攻击： 被广泛用于非法获取网站控制权，是发生在应用程序的数据库层上的安全漏洞。 从而使数据库受到攻击，可能导致数据被窃取、更改、删除，以及进一步导致网站被嵌入恶意代码、被植入后门程序等危害。

vii. 写入 webshell 攻击：是指 WAF检测到攻击者正在往用户网站写入网页木马， 企图控制服务器。 攻击者可以在用户网站上写入一个 web木马后门，用于操作用户网站上的文件，执行命令等等。

viii. 本地文件包含 ： 是指程序代码在处理包含文件的时候没有严格控制。 攻击着可以利用该漏洞， 在服务器上执行命令。

ix. 远程文件包含 ： 是指程序代码在处理包含文件的时候没有严格控制。 导致用户可以构造参数包含远程代码在服务器上执行， 进而获取到服务器权限， 造成网站被恶意删除，用户和交易数据被篡改等一系列恶性后果。

x. 远程代码执行 ： 是指由于服务端代码漏洞导致恶意用户输入在服务端被执行的一种高危安全漏洞。 利用该漏洞，可以在服务器上执行攻击者拼装的代码。

xi. FastCGI 攻击：nginx 中存在一个较为严重的安全问题，FastCGI 模块默认情况下可能导致服务器错误的将任何类型的文件以 PHP的方式进行解析。 这将导致严重的安全问题，使得恶意的攻击者可能攻陷支持 php 的 nginx 服务器。

xii. WAF专注于应用层的攻击，包括 CC和 web 攻击。和高防 IP 的主要差别在于： WAF会在第一时间最快更新最新的 Web 0day 漏洞防护规则。比如大面积爆发的 strust2 和 imagemagick 漏洞。 Web防护上具备预警模式和防护模式， 帮助用户业务初次上线时启用， 了解业务误报状况。 CC 防护具备宽松、严格的防护策略，用户可以自定义调整适应业务实际情况。 企业版支持用户关于 web攻击规则的自定义调整以及 CC策略的定制调整，避免误报。 针对诸如 wordpress 的 pingback 以及挂链导致的 CC攻击，只有 Web应用防火墙具备。 支持用户对管理员登陆页面等特定 URL做重点访问控制。 实时解决垃圾注册、刷库撞库、活动作弊、论坛灌水等严重业务风险，最佳用户体验、无需网站修改源码 / 调用 API 接口等繁琐操作即可实现快速上线防护。

d) 网络安全专家防护

i. 基于云盾 DDOS高防 ip，推出的安全代维托管服务，由阿里云云盾专家团队， 提供私家定制的 策略优化、 重大活动保障，攻防专家分析报告、真是攻击源分析、人工值守 等服务。

2、 云盾的主机级防护

a) 安骑士： 支持卸载、安装

i. 基于云端联动防御，可以为云服务器提供防黑客入侵。

ii. 木马查杀；防密码暴力破解；异动登陆提醒；漏洞检测修复 --- 补丁管理。

iii. 木马查杀：网站类后门、二进制程序、恶意脚本；精准查杀（实时更新基于阿里云的恶意文件库） ；实时查杀（第一时间通知，主动隔离，实时通知用户）

iv. 账户安全保护：暴力破解拦截；黑客账户检测；异常登录报警；

v. 特点：轻量化 Agent（CPU使用率 1% 10M内存、无第三方依赖）；安全状况实时掌控（控制台、短信邮件告警）；发现风险快速阻断；云平台全链路联动防御；适应各种云平台环境（支持公有云、私有云、混合云、传统 IDC）；

b) 补丁管理：基于安骑士

i. 解决客户漏网发现不及时、 不会修漏洞、 无法批量进行补丁更新等问题， 可一键下发补丁更新、 漏洞快速修复。

ii. 发现漏洞（在漏洞曝光之前） -》获取修复方案（快于官方发布） -》执行修复（批量修复、异常回滚）

iii. 工作原理：执行漏洞扫描、并将漏洞信息上报到云盾，同时给用户推送漏洞预警信息。

iv. 特点：多渠道漏洞获取、专家团队自研补丁、 6 小时修

复、支持批量修复和回滚。

c) 服务器安全托管

i. 管家式的服务

ii. 定制化的安全防护策略、 木马文件检测和高危漏洞监测与修复

iii. 发生安全事件，提供安全事件分析、响应，并优化防护策略。

iv. 成果：安全事件分析报告

3、 云盾的业务防护

a) 阿里绿网（ 考题：阿里绿网只提供网站内容检测 ?）

i. 违规信息管控政策背景 （国家法律法规要求、 违规事件频发，处罚成本巨大，信息安全问题持续升温，新法不断出台）；违规形式多样化，提前发现成难题；

ii. 阿里绿网基于深度学习技术及阿里巴巴多年的海里数据支撑，提供多样化的内容识别服务， 能有效帮助用户降低违规风险。

iii. 网站内容检测（违规网页检测、挂马检测）和图片鉴黄服务，后续推出垃圾广告过滤、 图片识别和视频识别等服务。

iv. 核心能力：文本算法（可准确高效的检测各类违规违法文本）；色情图片检测 （基于鉴黄模型，自动发现图片特征，准确率高达 99.6%）；多媒体指纹技术（ 视频特征提取、特征量化，由于占用空间小，可大规模索引和检索）；OCR(图片文字检测、识别服务，有极高的准确率和很好的泛化能力，快速迭代更新）

v. 特点：大数据；强大的识别能力；灵活的服务方式；海量数据快速检测；

b) 反欺诈服务

i. 常见：垃圾注册、刷库、撞库、营销作弊、垃圾内容

ii. 概念：基于阿里大数据风控服务能力， 通过领先的行为收集技术和机器学习模型，解决企业账号、活动、支付等关键业务环节存在的欺诈威胁。

iii. 特点：精准识别风险；实时防御风险；基于海量数据分析；

iv. 核心：防垃圾注册；风险用户核实；防营销作弊；防恶意登录；支付保护；饭垃圾服务。

c) 加密服务

i. 加密的重要性： 有效阻止非授权的人获取数据； 数据即便丢失也没有关系； 密钥的管理是一个严谨的过程； 企业的敏感数据都应该加密保护； 海量数据的加密是核心的问题；

ii. 概念：通过在阿里云使用经国家密码管理局检测认证的硬件加密机，帮助客户满足数据安全的监管合规要求，确保云上业务数据的隐私性和机密性。 客户可以借助云加密服务实现对加密密钥的完全控制和加解密操作。

iii. 算法支持：对称加密算法； 非对称加密算法； 摘要算法；全面支持国家和国际通用算法；

iv. 特点：安全的密钥管理；云上合规；弹性扩展；云计算带来的可靠性。

v. 适合场景：企业合同、核心专利、重要客户信息、董事会纪要；

4、 云盾的安全管理

a) 态势感知（网络层、主机层、业务层）

i. 专为企业安全运维团队打造， 结合云主机和全网的威胁

情报，利用机器学习， 进行安全大数据分析的威胁检测平台；全面、快速、准确感知过去、现在、未来的安全威胁。

ii. 还原事件、分析原因、着眼未来

iii. 特点：免安装、 Saas 服务，无需任务部署，在浏览器上即可使用；大数据 +专业团队

iv. 态势感知，让安全决策变得简单。

b) 云监控（ 设珞报警规则、获取监控信息 ）

i. 是一项针对阿里云资源和互联网应用进行监控的服务。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，以及针对指标设珞警报。

ii. 模块：站点监控、云服务监控、自定义监控、报警联系人、事件订阅。

iii. 站点监控：支持 8 种协议的探测，探测频率 1、5、15 分钟。HTTP/HTTPS PING,TCP,UDP,DNS,POP3,SMTP,FTP

iv. 云服务监控：可查看 11 种云产品的监控数据并设珞报警，每个产品提供了不同的监控指标和统计周期。ECS/RDS/SLB/OSS/EIP/CDN/MQ/LOG/。

v. 自定义监控：提供给用户自由定义监控项及报警规则的一项功能。 可以针对自己关心的业务进行监控， 上报监控数据，由云监控进行数据处理，并形成报警数据。

vi. 报警服务：监控项、统计周期、统计方法、联系人通知组等信息。

c) RAM

i. 稳定可靠的集中式访问控制服务，可授权第三方合作。

ii. 特点：集中式身份管理；集中式权限管理；统一访问控制（STS）;集中记录用户行为； 统一账单（主账号买单）；

iii. 身份管理：RAM-user，独立的身份管理，实体身份，拥有独立的登陆密码和 AK，支持多因素认证； RAM-Role，与各种身份管理系统结合， 是虚拟身份， 没有独立的登录密码和 AK，可以与外部实体身份联结。

iv. 权限管理：授权策略管理； STS访问令牌管理；

v. 应用场景：企业子账号管理与分权； 不同企业之间的资源操作与授权管理； 云服务之间的资源代理操作与授权管理；身份联盟与授权管理；针对不可信客户端 APP 的临时授权管理；

d) 渗透测试—提交工单，申请开通

i. 是通过 模拟 恶意黑客的攻击方法， 来评估计算机网络系统安全的一种 评估 方法，进行安全性评估。

ii. 测试手段：以黑客的视角， 用黑客的工具和方法进行测试，只进行安全评估，不进行破坏；

iii. 测试范围：操作系统漏洞、网络漏洞、 web应用漏洞、常见服务漏洞、安全管理漏洞、员工安全意思漏洞。

iv. 服务报告：服务范围描述；渗透过程详细描述；发现的漏洞列表、漏洞验证方法；漏洞修复建议；渗透总结。

v. 特点：渗透测试专家团队；云盾技术与大数据支撑。

e) 先知计划

i. 帮助企业建立私有安全应急响应中心（漏洞收集平台）

ii. 加入先知计划， 企业可自主发布奖励计划， 激励先知平台的安全专家来测试和提交企业自身网站或业务系统的漏洞，保证安全风险可以快速进行响应和修复， 防止造成更大的安全损失。

iii. 功能：私有的安全中心；可靠的安全专家；完整的漏洞闭环。

iv. 可覆盖的风险：敏感信息泄露；业务逻辑设计缺陷；越权敏感操作；弱口令；

f) 数据安全险

i. 是众安保险针对阿里云用户推出的信息安全综合保险，若因 黑客攻击 导致用户云服务器上的 数据泄露 并造成经济损失，众安保险将为用户提供最高 100 万的现金赔偿，降低投保用户因黑客攻击意外事件带来的经济损失。

ii. 典型场景：数据被黑客窃取，企业收到黑客敲诈；网站用户收到欺诈信息， 企业被索赔； 媒体公布企业数据被黑客窃取，企业声誉损失。

5、 安全防护建议

a) 安全责任

i. 阿里云上安全管理责任不变； 数据归属关系不变； 安全管理标准不变；

ii. 提高风险意识，完善管理流程，建立（考题） -- 安全习惯（强密码、安全验证、密码文件单独加密，不在网络上传输、不连接不安全 AP，不下载、不安装未知软件。）

b) 架构+网络优化建议

i. 架构优化：存放关键内容的 ECS，不开通公网 IP；使用 SLB，增加一层防护； RDS不开通外网 IP；远程管理采用堡垒机中转； 开通“态势感知”，并定期查看报告 。

ii. 网络层优化：关注云盾报表关于 DDos的基础防护；打开 CC开关，配置 DDOS清洗阈值；超过 5G攻击，开启高防 IP；重大活动保障，启用网络安全专家服务。

c) 主机+应用优化建议

i. 主机优化：启用操作系统自带防火墙功能； 开放端口时，

采用最小化原则；管理端口增加白名单　　IP；关闭 ECS 的无用端口；开启安骑士、阿里绿网；可选择服务器安全托管；

ii. 应用优化：遵循软件安全开发生命周期（ SDL），进行安全评估和安全测试；定期查看安骑士、态势感知、云监控报告；对业务系统进行分组，启用 RAM 账号，最小化权限。

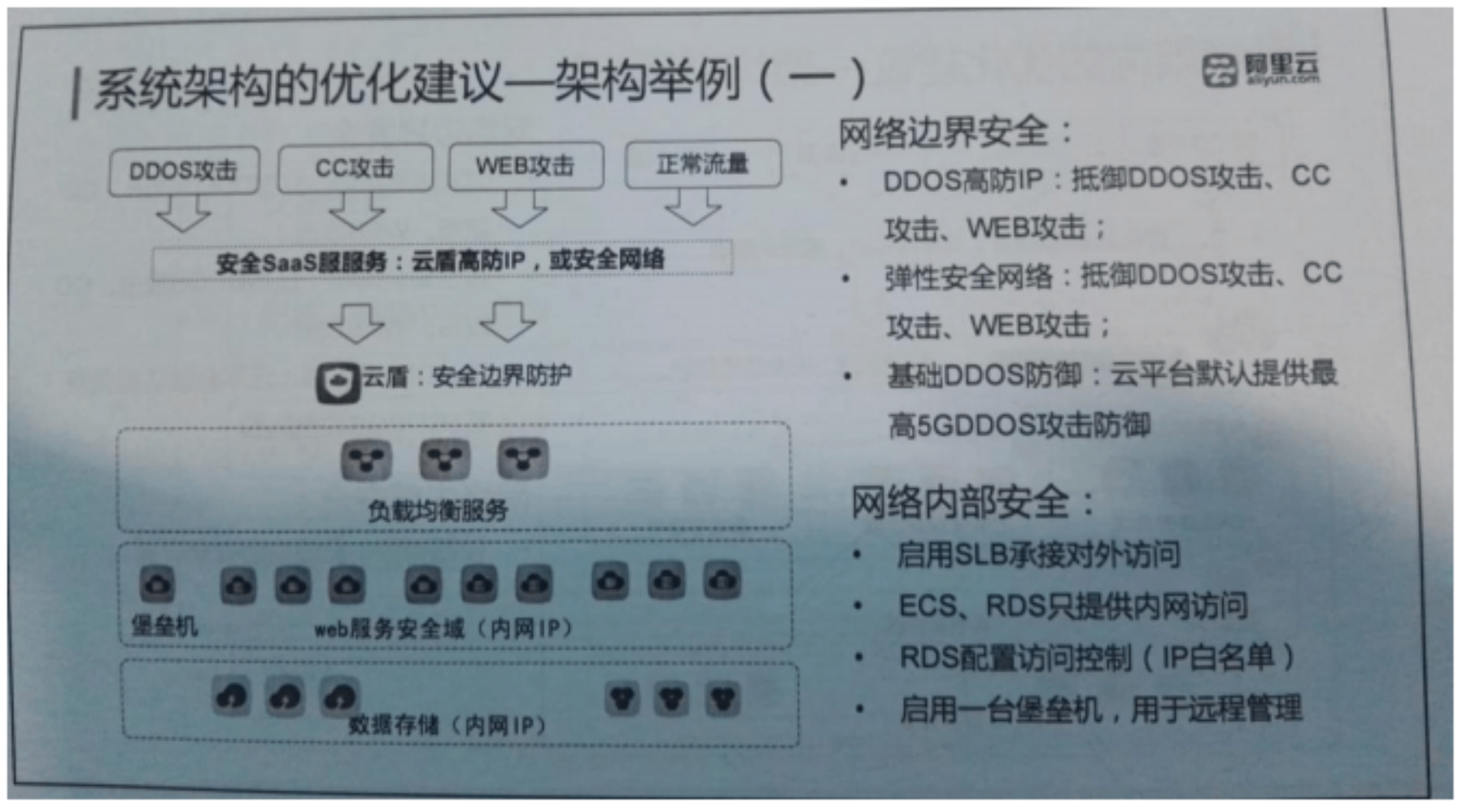
d) 报警测录配珞

i. 态势感知模块报警

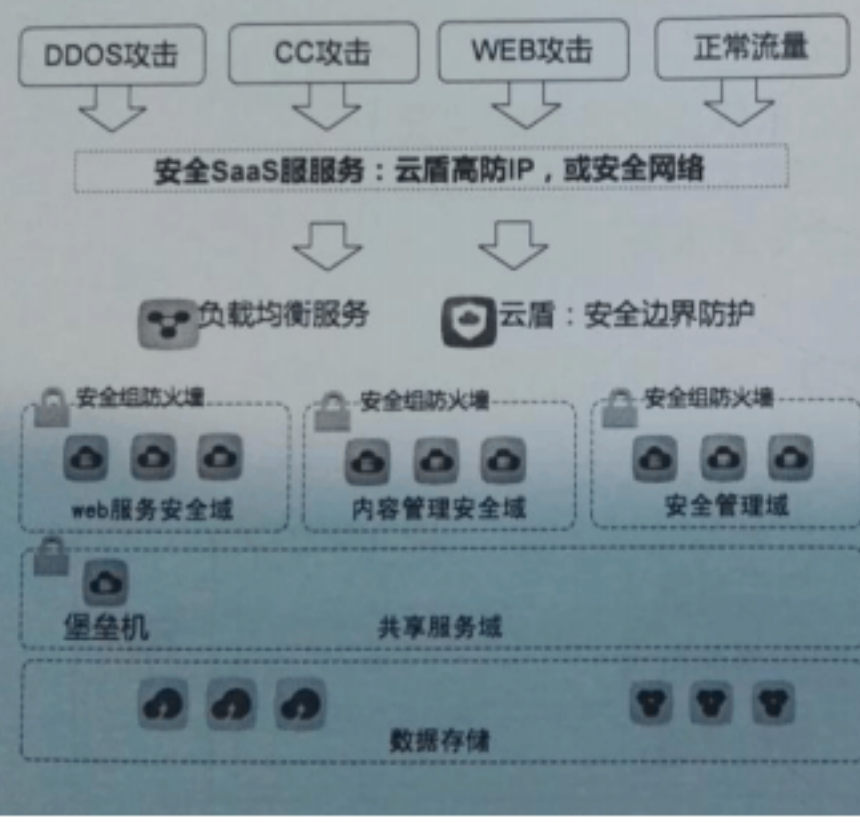
ii. 阿里绿网模块报警

iii. 云监控报警

这四张也很重要，可以结合以上产品进行综合理解，考题演变的基础：



系统架构的优化建议—架构举例(二)



网络边界安全：

- DDOS高防IP：抵御DDOS攻击、CC攻击、WEB攻击；
- 弹性安全网络：抵御DDOS攻击、CC攻击、WEB攻击；
- 基础DDOS防御：云平台默认提供最高5GDDOS攻击防御

网络内部安全：

- 使用安全组防火墙，划分不同安全域；
- 启用SLB承接对外访问
- ECS、RDS只提供内网访问
- RDS配置访问控制（IP白名单）
- 启用一台堡垒机，用于远程管理

系统架构的优化建议—架构举例(三)

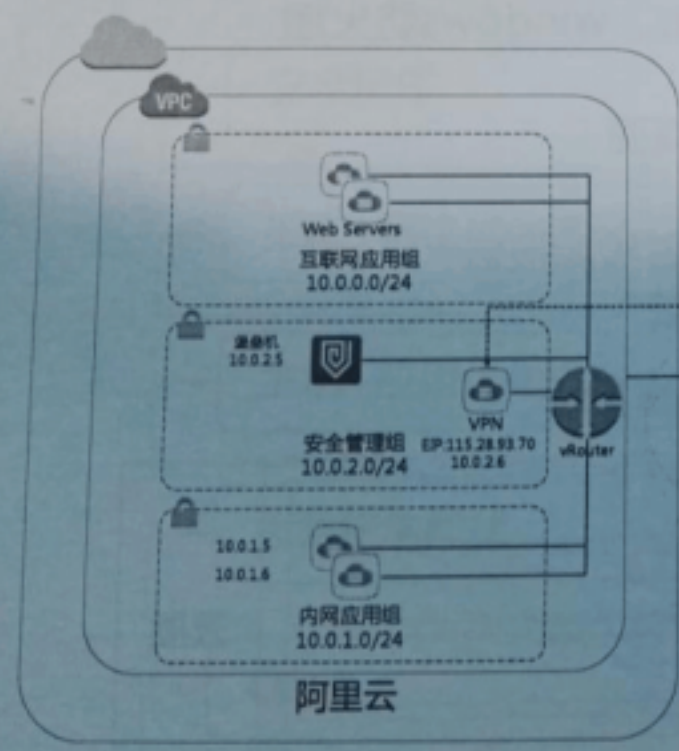
网络边界安全：

- DDOS高防IP：抵御DDOS攻击、CC攻击、WEB攻击；
- 弹性安全网络：抵御DDOS攻击、CC攻击、WEB攻击；
- 基础DDOS防御：云平台默认提供最高5GDDOS攻击防御

网络内部安全：

- 使用VPC，实现二层安全隔离

系统架构的优化建议—远程管理



部署VPN和堡垒机产品：

- 在云市场中购买第三方虚拟VPN和堡垒机产品；
- 在云上增加一个安全管理组，专门用于部署VPN和堡垒机等安全产品，并设置仅安全管理组IP可以访问其他ECS；

1、登录VPN公网地址
2、登录堡垒机进行运维

安全价值：

- VPN+堡垒机成为唯一的运维通道，ECS运维端口不必对外；
- 堡垒机实现运维实名制，所有操作可定位到人；
- 远程运维过程全审计，可实现实时监控、事后回放；
- 满足等级保护等法律法规要求；

八、云计算通用知识： 5%

VPC不提供独立的 SLA，VPC中云产品实例（ ECS, RDS, SLB, OCS, OSS等）适用各个产品的 SLA和故障赔偿条款。

Window系统、防火墙、磁盘、网络等知识；

Linux 系统、防火墙、磁盘分区、网络等知识。

应用、数据库、会话、状态、协议、存储、安全等术语。

HTTP请求返回码 2XX 3XX为正确， 4XX 5XX为异常