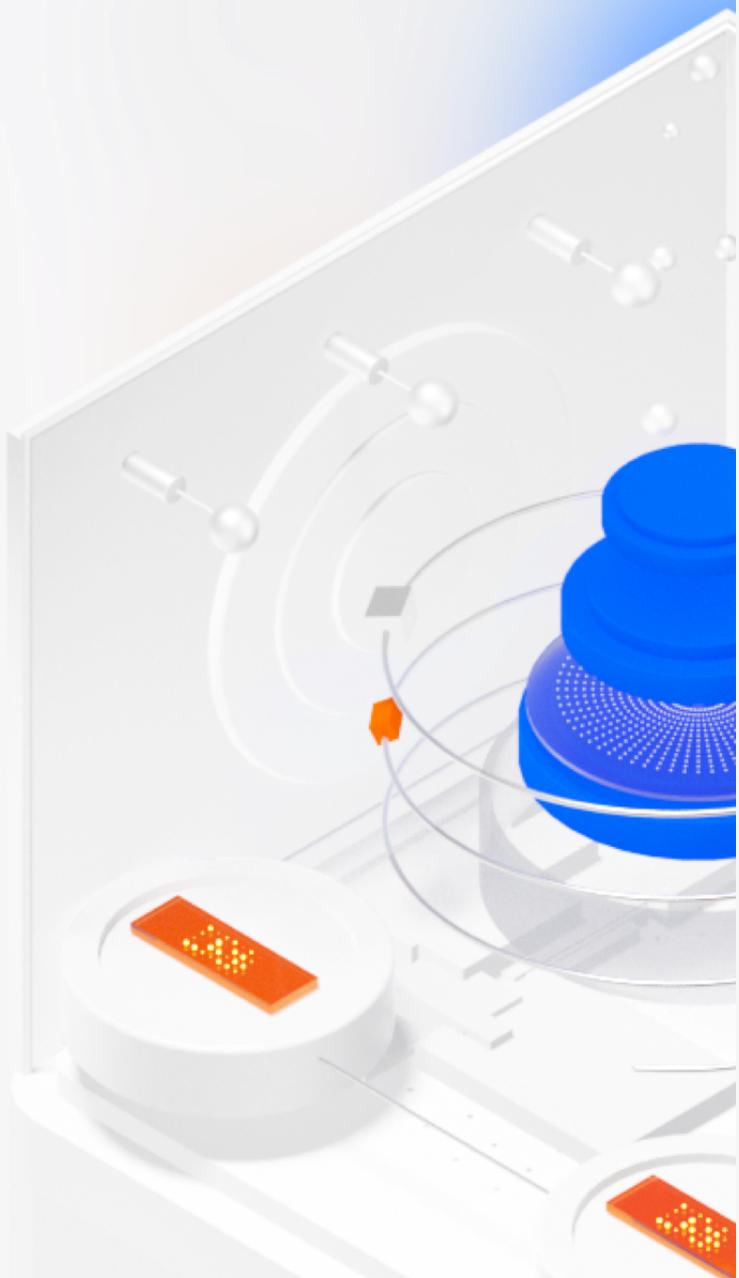


网络 稳定性 白皮书



目录

03 引言

04 云网络稳定性概述

- 云网络产品简介
- 云网络稳定性初心
- 云网络稳定性定义
- 云网络稳定性度量

07 云网络稳定性三大核心能力

- 平台能力
- 运营流程
- 最佳实践

引言

未来世界是数字化世界，云计算是数字化世界的基础设施。企业在数字化时代，“上云”是必经之路。企业“上云”，网络先行，云网络是用户使用云计算的第一步。云网络为企业修建“上云”的高速公路，建立万物互联的全球网络，助力企业连接数字世界。

云计算已经成为像水、电、煤一样的基础设施，千行百业的企业、个人上云后，都希望有一个绝对稳定的基础设施，尤其是云上网络。云网络是云计算时代的高速公路，需要为用户提供稳定可靠的万物连接，并且通过智能化可简化网络的运营和管理工作。这样，大家可以把自己更多的精力专注在业务创新上。

云计算的核心思想就是将资源、技术、能力以产品服务的形式提供给客户，大到跨国企业，小到个人开发者，都能简单地得到企业级的稳定性。

为了这个目的，阿里云洛神云网络持续创新，从 1.0 的云数据中心网络演进到 2.0 的广域网络，再到当下的云网络 3.0 的应用-云-边一体网络，不断延伸云网络产品的范围，增强产品能力，完善产品方案及最佳实践；同时，建设云网络各产品运维能力，提供用户自助服务；在上云后，用好云上网络。

我们希望通过本白皮书，读者可以系统性地了解到阿里云云网络的稳定性定义、能力及最佳实践。同时阿里云云网络产品做了哪些工作来保障和提升产品的稳定性。以及作为用户，应该怎样做才能充分利用阿里云云网络各产品提供的最佳实践及稳定性能力来支撑自己 IT 系统，更好地服务自身的业务。

云网络稳定性概述

云网络的稳定性是云网络提供产品及服务的基础，也会直接影响客户的业务连续性、操作流畅性以及账单准确性。因此，为了保障云网络的稳定性，阿里云自顶向下制定了云网络稳定性模型。基于这个模型，阿里云从平台建设 + 运营流程 + 最佳实践三个维度开展云网络的稳定性建设，打造了一套立体化的稳定性体系，帮助用户基于丰富灵活的云网络产品体系构建起稳定可靠的网络架构，支撑用户业务发展。

云网络产品简介

经过十多年的发展，阿里云云网络也服务了各行各业的千百万客户。洛神云网络从 1.0 的云数据中心网络演进到 2.0 的广域网络，再到当下的云网络 3.0 的应用-云-边一体的网络，云网络产品的范围也在不断延伸，产品体系愈加完善，包括 VPC、EIP、CLB、ALB、NAT、CEN、EC、TR、VPN、GA 等众多产品。阿里云云网络各产品仍将在稳定、安全、自助、弹性、易用等方面持续耕耘，更多了解可以参见[阿里云官网](#)。

云网络稳定性初心

阿里云云网络作为云计算的基础设施，是云计算核心 IaaS 服务之一，上面承载了千行百业的成千上万客户的 IT 系统，可以说甚至是用户的身家性命。阿里云深知客户将业务的应用、数据部署在阿里云上，通过云上网络进行互联互通，是源于对云网络的高度信任。云上网络资源实例的稳定性是云网络各产品的核心特性之一，就好比一架飞机，不管其性能有多优良、价格多实惠、技术有多先进、乘坐有多舒适，如果接二连三地发生故障，轻者会影响用户体验，重者甚至威胁到整个飞行的安全，用户就不会再选择乘坐。同样的道理如果云网络产品频繁发生故障，导致客户使用体验甚至业务受损，势必影响客户对阿里云云网络来之不易的信任，甚至是对整个阿里云的信任。所以稳定性是所有的前提，是云网络各产品的基石。因此，阿里云云网络把稳定性当作各产品立足之本，投入巨大资源支持稳定性能力建设，最终为客户提供稳如磐石的稳定性体验。

云网络稳定性定义

本白皮书讨论的云网络各产品稳定性是指云网络各产品实例运行状态及访问质量相关的稳定性，用来体现云网络各产品实例持续稳定提供云上网络访问服务的能力。各产品的实例状态、云上网络访问受损 / 不通等都是云网络各产品稳定性异常的表现。

云网络稳定性度量

稳定性度量方式

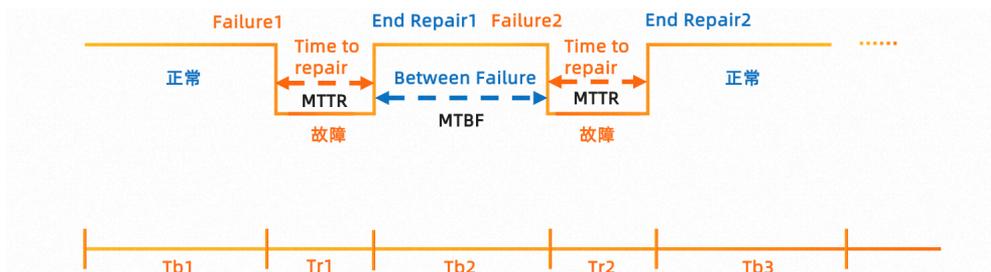
云网络产品稳定性主要体现在高可靠性、可用性上。所谓网络可用性，顾名思义，就是网络的可用程度，网络无故障运营的时间占总运营时间的百分比可以用来比较好的反映网络的可用性。其中 MTBF、MTTR 就是两个关键的指标：

MTBF (Mean Time Between Failures) :

平均无故障时间，即两次故障的平均时间，也就是指系统正常运行的平均时间。MTBF 越大，表明越不容易出故障，可用性自然高。MTBF 反映的是网络的可靠性 (Reliability)。

MTTR (Mean Time To Repair) :

平均修复时间，即出现故障后修复故障的平均时间，也就是故障发生到故障修复完成这段时间。MTTR 越小，表示故障时间越短，可用性也就越高。MTTR 反映的是网络的可用性 (Availability)。



稳定性指标的几种常用的计算方式如下：

$MTBF = (Tb1 + Tb2 + Tb3 + \dots + Tbn) / n$ ，平均无故障时间

$MTTR = (Tr1 + Tr2 + Tr3 + \dots + Trn) / n$ ，平均修复时间

$Availability = MTBF / (MTBF + MTTR)$ ，产品可用性

下表是可用性的几种常见的情况，包括可用率和中断服务时间，具体如下：

可用率	中断服务时间
99%	3.65天
99.9%	8.76小时
99.99%	52.56分钟
99.999%	5.256分钟

阿里云云网络产品采用业界通用的可用性指标来度量各产品的稳定性,这一指标能直观地反映产品的可用性,同时也符合客户使用体验的直觉。云网络各产品的可用性指标具体描述可能存在差异,但是整体都是产品实例正常状态提供服务的时长占实例生命周期的比例。基于可用性指标,阿里云云网络各产品提供了明确的可用性 SLA (Service Level Agreement, 服务等级协议), 规定了服务质量和赔偿条款。具体见阿里云帮助中心云网络各产品的服务等级协议文档。

云网络稳定性三大核心能力

平台能力

在业务发展初期，阿里云的网络运维也采用了传统的模式，在监控、告警、运维和可视化等方面，针对不同的业务场景进行定制化的开发。然而，随着业务规模的增长，这种一对一的模式逐渐暴露出弊端，如开发周期长、业务逻辑复杂和严重依赖人力资源等，使得云网络的运维能力很难跟上业务发展。随着 5G 时代的来临，数据将会迎来爆炸式的增长，传统的模式将无法适应运维需求。我们开始思考如何在有限的资源下，支撑日益增多的业务需求。

网络运维平台化需要将系统和业务的复杂包装起来。网络作为云基础设施，产品众多、业务复杂、集群庞大，要做好产品的运维，对运维人员甚至用户都提出了更高的要求。网络智能化是未来发展方向，网络运维平台化是网络智能化的基础。目前对于网络问题排查、恢复的手段，均依赖于人的经验。在智能化的情况下，网络异常检测、根因定位、故障逃逸和运维变更等，都将依赖智能系统实现，借助平台的力量，实现数据资源的整合和深度挖掘，为迈向智能化铺平了道路。

变更

变更在本质上是通过一系列的操作使得运维的产品走向预期的状态，在操作之前需要解决一些未知的问题，例如系统原来的状态是什么，目标的状态又是什么。在操作过程中，需要执行哪些指令，得到哪些输入，系统的表现怎么样，业务是否受损，在操作后，目标状态是否达到。变更的定义有狭义与广义之分。狭义定义：云网络产品和设备相关的版本发布、设备维护和配置修改等的线上操作。广义定义：所有会对线上设备、应用、软件、配置和文件等对象产生变化的操作。

云网络的变更从发展过程来看，经历了标准化 --> 自动化 --> 无人化的三个典型阶段。

1. 标准化。在云网络发展早期，受限于产品能力与系统建设，都是在黑屏上人工操作，对操作人员的素质要求非常高，所有变更的可靠性是依赖于 SOP(标准操作程序) 手册与高质量的人工实施保证的。
2. 在自动化阶段，变更的主要形态从 SOP 操作手册逐渐转化为对应的自动化工具。通过快速的运维工具开发与基础的变更步骤编排，将原来人工敲击执行命令的过程转化为执行变更工具，在变更运维代码中实现自动化执行原子变更任务。

3. 无人化变更系统是变更运维系统的理想终极目标,但是无人化的变更系统已经脱离了独立的变更系统概念。无人化变更系统的核心要素有:全自动化变更执行、异常发现、变更异常关联和变更快速止血。要满足这些要素,需要监控系统、告警系统、实时数据分析系统等联动实现。无人化阶段也是阿里云网络变更发展正在经历的阶段。

监控

传统的网络监控主要是针对网络设备的监控,比如交换机和路由器,监控设备是否宕机、端口上下线(端口 up/down)和丢包计数器等。

而在云网络的场景中,除了真实的网络设备,还有很多虚拟的服务于租户的网络设备,以及服务化的各种网络产品,比如专有 VPC、NAT 网关、负载均衡和云企业网等。这些虚拟的网络产品和租户的网络对象都需要监控起来,以此来衡量云网络产品的服务状态和 SLA。

另一方面,由于云网络是基于 SDN 思想设计的,将网络计算从传统的网络设备中剥离开来,下沉到了 x86 服务器中,可以摆脱网络设备可编程能力的限制,采集更多网络指标进行监控,如各种网络表项的上百种计数器的指标、各种查询队列的状态等。

云网络的监控主要分为三类:网络业务指标监控、网络设备或服务监控和租户实例监控。

1. 网络业务指标监控是指实际的网络产品服务的业务指标,如某个地域 VPC 公网流量或丢包指标,某个集群的 SLB 流量或丢包指标等。
2. 网络设备或服务监控是指云网络内部设备和服务的监控,比如 VPC 转发设备或管控服务、SLB 转发设备或管控服务的监控等。
3. 租户实例监控是指对虚拟出来的属于租户的网络实例进行监控,比如用户购买的 VPC 实例、SLB 实例。按照用户的具体实例进行单独的监控,满足不同用户、不同业务的监控诉求。

应急

一旦监控发现网络异常,则依赖故障应急来自动化处理,也就是网络自愈。

云网络全系列产品都是自主研发的,随着产品功能特性上线,监控指标项的精细化会让系统化发现异常的能力逐渐增强,此时人力响应告警的工作投入越来越大,自动化应急的必要性显得尤为必要,让机器自动运维机器,从而控制人工处理告警的投入成本,避免运维人力投入随着告警的精细化而线性增长。

应急系统的具体实现，整体是建立在监控告警平台和变更系统之上，监控负责发现问题，变更平台负责恢复时的执行操作，应急系统负责自愈过程中的分析决策。应急决策的发展，也经历从人工到系统化，从离散到中心，以及人工定义到自动决策演进。

人工到系统化应急。最初产品层线上需要运维的设备数量和对告警少，研发同学在负责开发的同时，基于偶尔的监控告警手动登入线上设备进行修复即可。但人工运维毕竟会占用研发同学的时间，同时当异常发生在半夜，人力的消耗更大，于是低效的人工应急自然会被系统化应急所替换。

离散到中心化应急。离散应急指的是基于最为基础的监控告警，在本地就可以完成自动修复，比如典型设备磁盘空间不足，基于系统的 crontab 定时任务，自动检测清理轮替后的历史日志。但对于需要基于跨设备层面的多个告警项做判断的异常，则需要中心化判断后才能做出决策，于是有了中心化应急系统。

人工定义到自动决策。最初的应急判断相对简单，只需要将运维工程师的经验通过系统的自定义进行沉淀，包括系统服务不可用时，可以基于健康检查和进程监控做综合决策，可以解决大部分的应急场景。对于更为复杂场景，人的经验无法具体描述，通过机器算法来决策的智能化运维成为主流，形成最终的决策大脑，让机器运维机器成为可能，这也是今天 AIGC 大模型的落地场景之一。

运营流程

云网络稳定性运维运营角色拆分为 7*24H 的 NOC 运营、轮值值班长，以及产研专家服务三级，通过组织梯队来实现全天候的运营护航服务。云网络 NOC 运营可以跟踪、处理、闭环云网络监控、故障、风险、变更、以及用户报障等运维工单，对接监控告警、故障应急、风险处理、变更处理以及用户报障应急运维进行记录、复盘和结果闭环。

工单服务

服务单是用户需求人工支持的标准流程，确保用户的每一个问题都能简单高效地解决，而不会因为找不到合适的人而产生困惑和痛苦。而服务单流程也是数据化服务体系的关键，服务单收集了真实发生的问题信息，通过服务单数据，可以快速分析出问题类型占比、发生频率、问题来源及服务质量。整个体系通过数据运维，对服务单的各项指标数据进行打分，通过大盘报表，不断复盘，驱使各个产品团队建设和改善服务外能力，提升人员服务意识。在服务单打造标准流程的同时，也让服务通过数据自运维起来，让我们知道服务到底做得如何。

服务单背后还有知识库和工具箱提供能力保障。知识库在服务体系中是非常重要的的一环，相当于一个集中的存储库存放知识和已知错误的修复方案。随着常见问题的不断沉淀，用户可以自助搜索问题的答案，不仅提升了用户的体验，还可以让用户低成本地学习很多有用的知识。借助智能机器人，还可实现机器人在

线答疑,减少服务人力的投入。对于技术问题,无法单纯地用知识库解答,此时工具必不可少。相比于传统网络中的 ping、tracert 等工具,云网络提供了更加丰富的工具体验,让有一定网络基础的用户及服务运维人员可以通过工具协助排查问题。工具箱将工具按照产品、功能分类,提供一站式接入方式,让网络专家快速地接入工具。工具箱与服务单流程联合在一起,当问题无法解决时,一键提交服务单并推送工具诊断结果。工具箱和知识库是服务沉淀的产物,这些知识和工具能快速地让用户找到问题的答案,使得云网络的每一位用户都变成了网络专家。

大客户重保

大客户作为云平台的核心服务对象,其业务的稳定性是衡量云平台稳定性的重要指标。由于客户业务类型、部署形态各有不同,每个客户业务对网络质量与容灾能力的敏感度与容忍度各不相同,云平台稳定性与客户业务稳定性之间存在一定的距离,因此大客户重保应运而生。

大客户重保的主要形式为客户业务常态化监控预警、客户重大活动护航、客户联合故障/容灾演练等。大客户重保作为提升客户体感满意度与客户业务稳定性提升的有效手段,不仅仅是云网络提供给客户的服务方式,对于云平台更有其深层次的业务价值:

1. 通过客户重保活动,更深入地理解客户业务,对不同的业务模型构建具备一定行业普适的网络监控模型与容灾架构模型,形成更有效更精准的监控与故障发现、故障逃逸方案。
2. 由于云平台上运行的虚拟实例数量是海量级别的,无法进行有效的实例监控;通过客户重保实例的常态化监控,在客户的协助下发掘海量实例中具备稳定监控价值的实例,变相实现了实例级别监控的采样覆盖,补足平台的在实例级别监控能力不足的短板。
3. 通过联合演练的方式,一方面协助客户优化业务架构,增强应用层容灾能力;另一方面打磨云网络自身人员、流程、工具与平台的应急作战能力;同时为云平台核心设备替换与升级提供了宝贵的业务可损窗口,实现部分有损变更的客户业务无损化。

最佳实践

举例:负载均衡高可用最佳实践

负载均衡高可用是从系统设计、产品配置等多个方面提供了可用性保障。此外,您可以根据业务需求,配合使用云解析 DNS 等产品实现跨地域容灾。以传统型负载均衡 CLB 为例,多可用区高可用指标设计为 99.99%,单可用区设计为 99.90%。

CLB 系统的高可用

负载均衡实例采用集群部署,可实现会话同步,以消除服务器单点故障,提升冗余,保证服务的稳定性。其中四层负载均衡通过 LVS (Linux Virtual Server) + keepalived 的方式实现,七层负载均衡通过 Tengine (淘宝网发起的 Web 服务器项目,在 Nginx 的基础上,针对有大访问量的网站需求进行了优化)实现。

来自公网的请求通过等价多路径路由 (ECMP) 到达 LVS 集群, LVS 集群内的每台 LVS 通过组播报文将会话同步到该集群内的其它 LVS 机器上,从而实现 LVS 集群内各台机器间的会话同步。同时, LVS 集群会对 Tengine 集群进行健康检查,将异常机器从 Tengine 集群移除,保证七层负载均衡的可用性。

最佳实践:

会话同步可以保证长连接不受集群内服务器故障的影响,但是对于短连接或连接未触发会话同步规则时(未完成三次握手)集群内的服务器故障仍可能会影响用户请求。为了防止集群中某台机器故障导致的会话中断,您可以在业务逻辑中加入重试机制,降低对用户访问造成的影响。

单 CLB 实例的高可用

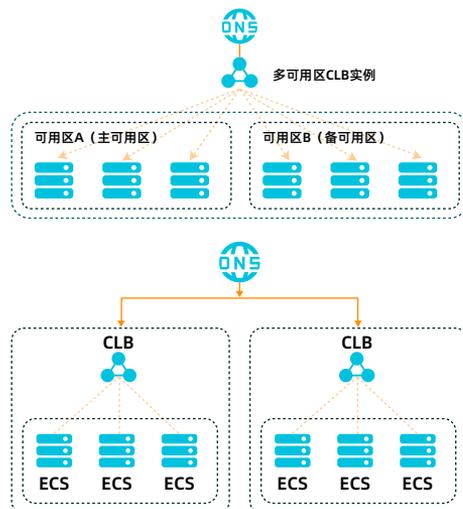
为了向广大用户提供更稳定可靠的负载均衡服务,阿里云负载均衡已在大部分地域部署了多可用区以实现同地域下的跨机房容灾。当主可用区出现故障或不可用时,负载均衡有能力在非常短的时间内(约 30 秒)切换到备可用区并恢复服务;当主可用区恢复时,负载均衡同样会自动切换到主可用区提供服务。

说明: 负载均衡的主备可用区是可用区级别的容灾。只有当主可用区整体不可用时,如机房整体断电或者机房出口光缆中断等,负载均衡才会切换到备可用区。而并非某个实例出现故障,就切换到备可用区。

最佳实践:

1. 为了更好的利用负载均衡的主备可用区机制,建议您在支持主备可用区的地域创建负载均衡实例,即在购买负载均衡实例时选择可用区类型为多可用区的地域。

2. 当您选择 CLB 的主备可用区时,可以根据 ECS 实例的可用区分布进行选择。大部分 ECS 实例位于哪个可用区,就将哪个可用区选择为 CLB 的主可用区,以获取最小的访问延迟。但是并不建议您将全部 ECS 实例都部署在一个可用区内,您也需要在 CLB 的备可用区部署少量 ECS 实例,以便在极端情况下(主可用区整体不可用时),切换到备可用区后仍旧可以正常处理负载均衡转发的请求。



多 CLB 实例的高可用

如果您对可用性的要求特别高，负载均衡实例自身的可用性保障机制可能无法满足您的需求。例如当网络攻击或配置错误等情况导致负载均衡实例不可用时，由于未出现可用区级故障，不会触发负载均衡实例的可用区切换。此时，您可以创建多个 CLB 实例，通过云解析 DNS 对访问进行调度，或通过全球负载均衡解决方案实现跨地域容灾备份。

最佳实践：

您可以在一个地域内的多个可用区或多个地域内部署负载均衡实例和后端 ECS 实例，然后使用云解析 DNS 对访问进行调度。

后端 ECS 实例的高可用

负载均衡通过健康检查来判断后端 ECS 实例的可用性。健康检查机制提高了前端业务整体可用性，避免了后端 ECS 异常对总体服务的影响。

开启健康检查功能后，当后端某个 ECS 实例健康检查出现异常时，负载均衡会自动将新的请求分发到其他健康检查正常的 ECS 实例上。而当该 ECS 实例恢复正常运行时，负载均衡会将其自动恢复到负载均衡服务中。关于健康检查的详细机制，请参见帮助文档[健康检查概述](#)。

最佳实践：

为了使健康检查功能正常运作，您需要开启并正确配置健康检查。具体的操作流程请参见帮助文档[配置健康检查](#)。

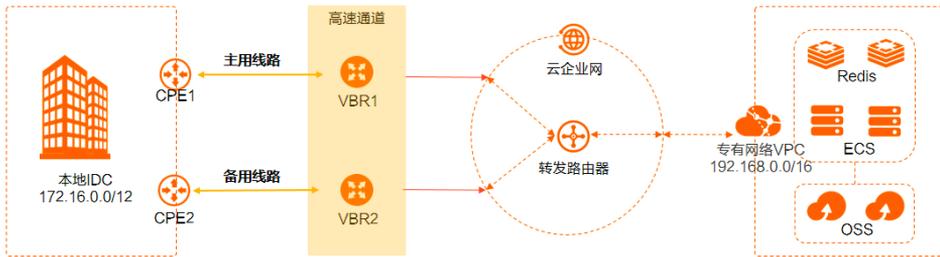
本地数据中心通过专线上云高可靠组网场景最佳实践

网络连接的可靠性对于企业来说至关重要，找到一个可靠性高的网络连接方式更是重中之重。企业专线就可以提供稳定的网络连接，确保关键业务系统和应用程序之间的数据交换不受公网异常情况影响，数据传输始终高速且安全。

企业专线能够为企业创建点到点的专用传输通道，并提供更好的网络性能，不受公共互联网波动的影响，可靠性更高。且区别于公网，不需要和其他用户共享网络，所以可以始终如一地为企业提供高可靠性的网络，让用户享用低延迟、大带宽的高品质网络环境，从而不受公网故障和拥塞的影响，这使企业能够高效处理核心业务，提高工作效率和客户满意度。

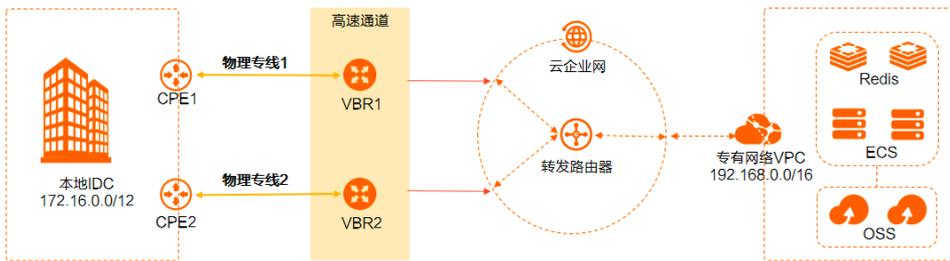
通过多线接入的组网方式可以最大限度保证业务的高可用性，可以通过如下方式组网保证上云网络的高可靠性。

1. 双线接入形成两条专线之间的主备组网, 使用两条物理专线以主备方式将本地数据中心 IDC (Internet Data Center) 接入阿里云。采用主备接入方式时, 正常情况下仅主用线路在进行流量转发。阿里云按照您配置的健康检查的发包时间间隔探测主用线路连通性, 当探测到主用线路故障时, 自动将流量切换至备用线路, 保证业务不受影响。



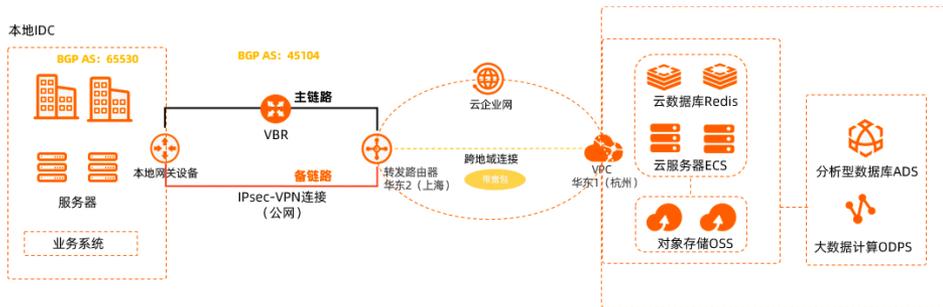
具体的配置步骤可参考帮助文档[主备冗余专线组网最佳实践](#)。

2. 双线接入形成两条专线之间的负载均衡组网, 使用两条物理专线通过负载冗余方式将本地数据中心 IDC (Internet Data Center) 接入阿里云。正常情况下, 两条物理专线同时转发流量。当阿里云检测到其中一条物理专线网络连接不通时, 该物理专线的流量将被切换至另一条物理专线进行传输, 保证业务不受影响。



具体的配置步骤可参考[负载均衡冗余专线组网最佳实践](#)。

3. 对成本敏感的用户, 无法承担多条专线的费用, 同时对上云接入存在高可靠性组网要求, 可以通过 IPsec-VPN 联合专线实现主备链路上云接入阿里云。正常情况下, 仅专线正常进行转发流量, VPN 链接作为专线发生故障时临时备份转发流量保证业务不会长时间中断, 等待专线链路恢复后流量重新 VPN 链接回到专线上。



具体的配置步骤可参考帮助文档[专线与IPsec-VPN主备组网最佳实践](#)。

大规模组网场景最佳实践

随着云上业务的发展，云上网络 VPC 之间、云上和云下的网络链接的规模将持续增大。在过去传统 IDC 中，复杂的组网通常对稳定性有三类挑战：

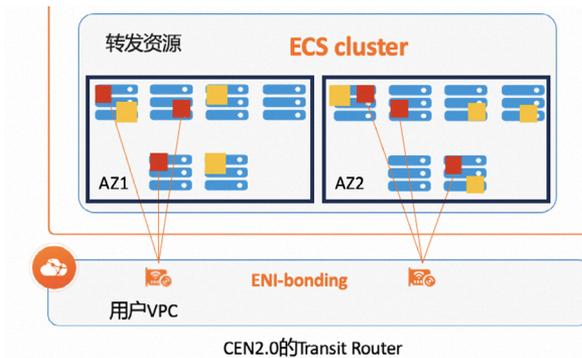
1. 网络设计复杂：为了业务稳定性，网络拓扑必须消除单点故障，需要在每一跳考虑故障情况下流量选路对稳定性的影响，复杂度高，安全隐患大。
2. 网络运维复杂：多个网络平面需要时刻保持配置一致，确保在故障情况下能够承载业务。
3. 变更影响严重：网络规模的增大势必带来网络设备的升级、替换，这些变更过程复杂，一旦出错对业务影响非常严重。

而云上网络环境中，通过云原生的高可用能力和弹性能力，能极大地简化客户组网拓扑、降低运维复杂度、自动弹性伸缩，极大地提升了网络稳定性。

云上的组网有两种方式：VPC peer 和 TR 转发路由器。VPC peer 是 VPC 之间两两链接，通常形成一种 mesh 结构。TR 转发路由器可以中心化的连接 VPC、VBR 和 VPN，形成 Hub-Spoke 的网络拓扑。关于跨 VPC 组网解决方案可参考帮助文档[跨 VPC 互联概述](#)。

在大规模组网实践中，推荐使用 TR 转发路由器形成 Hub-Spoke 的网络拓扑。使用 TR 进行大规模组网有如下好处：

1. TR 实例本身是多可用区分布式转发系统，具备 99.95% 的可用性 SLA。客户可以选择多个 TR 接入的可用区，单个可用区故障可自动进行容灾倒换。



2. 每个 TR 实例 支持最大 1000 个 VPC 互联, 20 张路由表, 每张路由表 2000 条路由。满足客户业务长期发展需要, 避免大范围变更网络架构带来的稳定性风险。

3. 所有边界网络 (VPC、VBR、VPN) 统一连接到 TR, 网络结构清晰, 易于维护。

异地多活网络组网方案

异地多活组网是客户在业务发展过程中, 出于性能、安全、容灾等角度演化出的一种高级组网诉求, 典型的需求场景包括:

多云架构:

由于地缘政治等多方面原因, 客户往往在采取多个云服务厂商的多云架构, 需要在多云之间构建异地多活网络架构。

异地容灾:

当一个地域遇到大型故障完全不可用时, 能够快速切换到其他地域, 业务不受影响。

在构建异地多活网路架构时, 需要多个层面:

弹性公网接入:

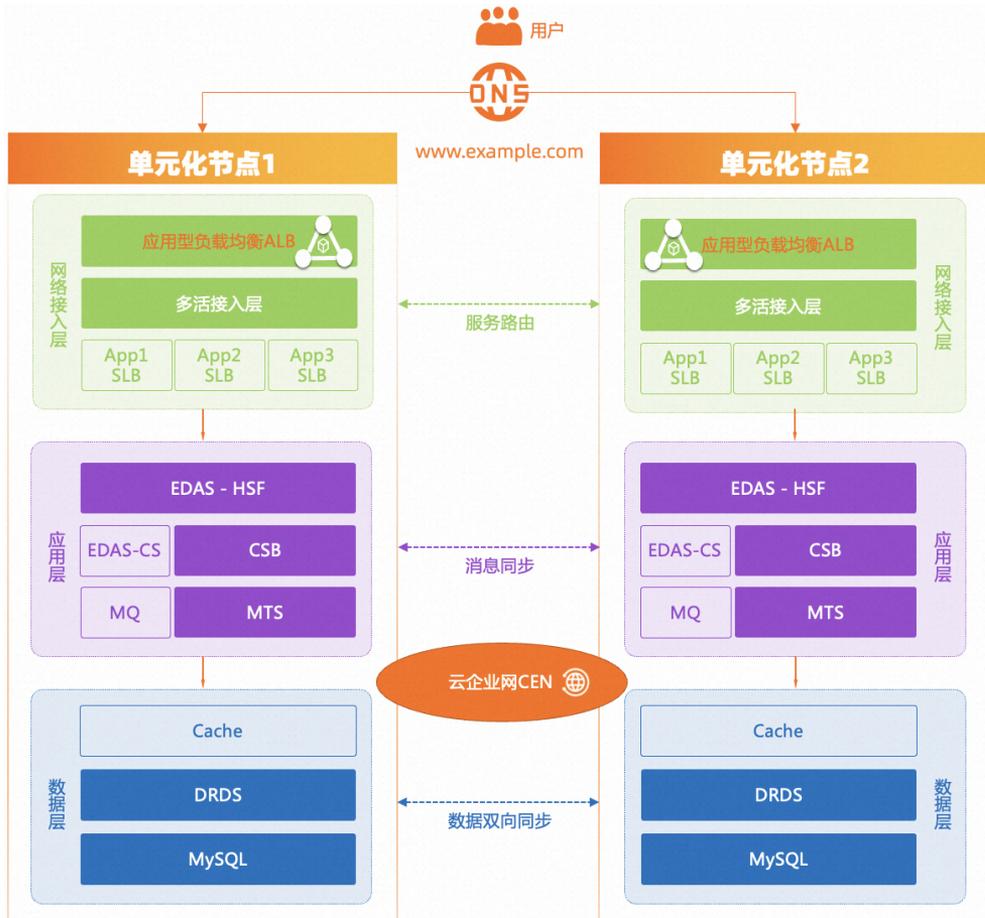
互联网应用如电商秒杀、交易、社交等场景往往需要很高的弹性, 需要弹性可靠的公网接入地域单元化模块。当一个地域无法提供服务时, 灾备地域有足够公网带宽承载业务流量。

多地域数据同步:

高并发、大流量的业务请求需要在多个地域之间实时 / 离线传输。需要稳定可靠、大带宽高性能的传输容量。在线同步业务、语音业务、离线数据同步业务等, 不同业务模型, 对网络需求也不尽相同, 需要对业务进行隔离, 避免离线业务的数据影响在线业务带宽。

调度能力:

用过 DNS 解析控制不同单元节点之间的流量分发, 当一个地域的单元节点不可用时, DNS 自动调整到其他健康的单元节点。



云上异地多活网络组网方案推荐使用:

全局流量管理 GTM

实现公网入口的流量调度

ALB / NLB

作为不同地域单元化节点的四层 / 七层流量入口, 提供超高性能, 超大弹性的流量分发能力

云企业网 CEN

连接各个地域实现大带宽、稳定可靠的跨地域数据同步能力