

深信服企业云aCloud 超融合灾备解决方案

目录

- 1 灾备建设意义与挑战
- 2 灾备设计方法论
- 3 企业云aCloud超融合灾备解决方案
- 4 价值与优势
- 5 案例实践

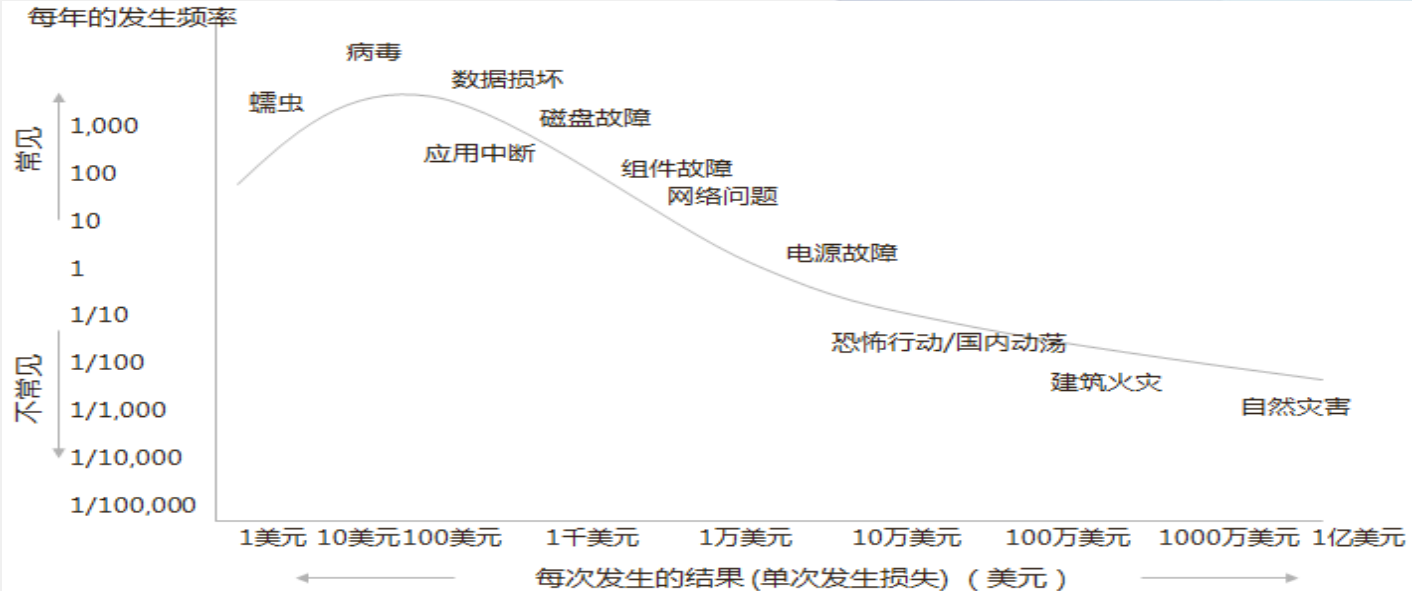
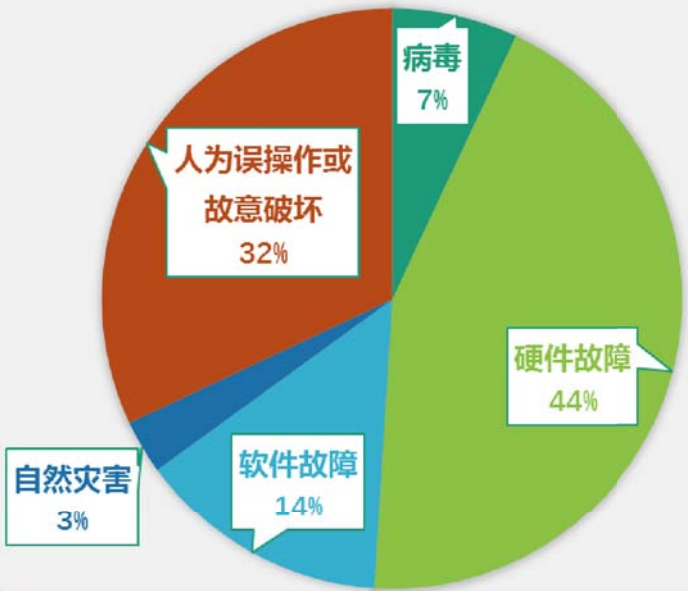
必要性：永远无法预测下一刻会发生什么

宏观统计：

- 据IDC统计，美国在2000年以前的10年间，发生过灾难的公司中，有55%当时倒闭，剩下的45%中，因为数据丢失，有29%也在两年之内倒闭，生存下来的仅占16%。
- 据Gartner Group的统计数据也表明，在经历大型灾难而导致系统停运的公司中有2/5再也没有恢复运营，剩下的公司中也有1/3在两年内破产。
- 2007年8月国务院办公厅印发的《国家综合减灾“十一五”规划》中指出，据估计我国近年来各类灾情综合直接损失已高达8%的GDP（大多数发达国家只是千分之几）。

微观分析

- 2002年7月5日，深交所因通信系统发生异常导致部分营业部无法正常交易；
- 2003年7月1日，上海市轨道交通4号线发生险情，临江花苑大厦内的劳动保障局和市财税局的重要信息系统被迫中断和搬迁；
- 2004年5月1日，黄金周第一天，北京市铁路局电脑售票系统出现临时性故障，致使全市各火车站的售票窗口、代售网点的售票工作全部处于瘫痪状态，时间长达一个多小时。
- 2008年5月12日，四川省汶川发生强地震，震区受地震波及的信息系统大部分完全瘫痪。
- 2017年9月8日，中国移动广西分公司系统割接，用户数据丢失，影响钦州、北海、防城港、桂林、梧州、贺州本地网部分用户，影响用户80万打电话与上网。
- 2018年7月20日，垂直行业媒体“前沿数控技术”硬盘数据近千万元级的平台数据全部丢失。



灾备无小事，轻者巨大经济损失，重者企业直接倒闭破产。

典型行业内灾备建设要求及趋势

银行：

2008年2月 中国人民银行正式发布和实施《银行业信息系统灾难恢复管理规范》(JR/T0044-2008)

2009年6月 银监会发布了新的《商业银行信息科技风险管理指引》

16年7月 银监印发《非银行支付机构信息科技风险管理指引》

保险：

2008年3月 保监会下发了《保险业信息系统灾难恢复管理指引》

证券：

2009年,中国证券业协会先后发布了《证券公司网上证券信息系统技术指引》、《期货公司信息技术管理指引》、《证券营业部信息技术指引》



金融



各地政府对相关电子政务建设，均把容灾中心的建设作为工作规划内容：

- 湖南省人民政府办公厅关于促进电子政务协调发展与深化应用的实施意见,湘政办发〔2016〕34号
- 四川省加快推进“互联网+政务服务”工作方案
- 江西省全面促进电子政务提质升级
- 山东省政务信息系统整合共享实施方案
- 安徽省人民政府办公厅关于印发安徽省推进“互联网+政务服务”工作规划的通知
- 海南省人民政府关于印发海南省政务信息整合共享专项行动实施方案的通知

.....

政府

《电子病历基本规范（试行）》第十六条第一项规定：“具备保障电子病历数据安全的制度和措施，有数据备份机制，有条件的医疗机构应当建立信息系统灾备体系。应当能够落实系统出现故障时的应急预案，确保电子病历业务的连续性。”

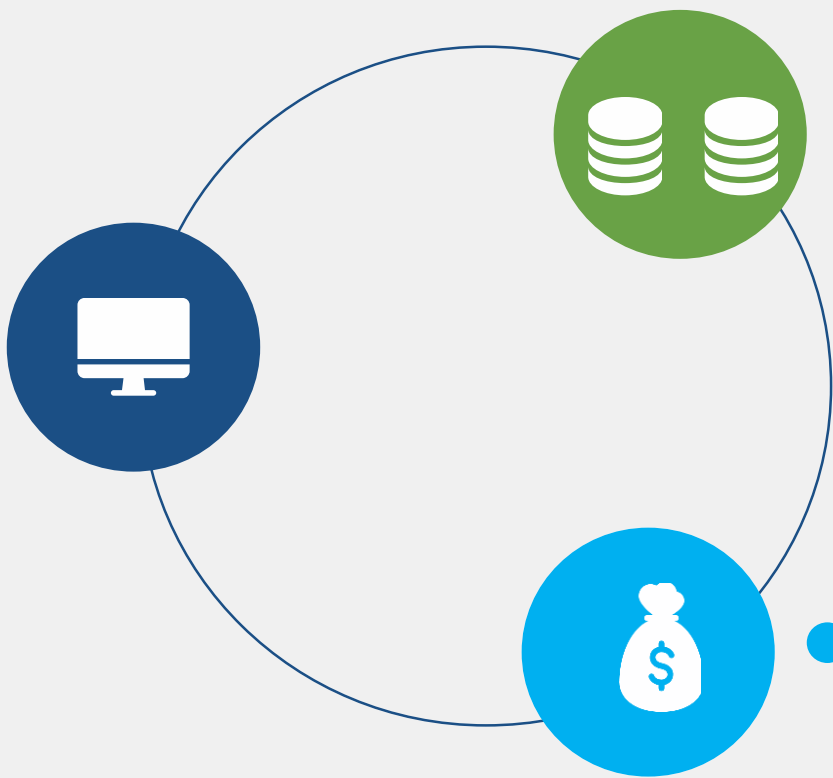


医疗

灾备建设面临的主要困难和挑战

● 灾备管理困难

灾备系统的建设涉及网络切换、应用切换、数据复制策略管理、容灾演练等多种技术知识，因此，对IT运维团队带来非常大的压力，一方面、一般用户的IT运维团队人力有限；另一方面，缺少相应的灾备专门技术人才。



● 数据同步困难

传统容灾在数据同步过程中，需要考虑主机层、数据库层、存储层的数据复制，由于数据格式复杂、数据量大，数据在传输过程中，网络受限于带宽的限制，无法满足RPO和RTO的要求。

● 灾备建设成本高

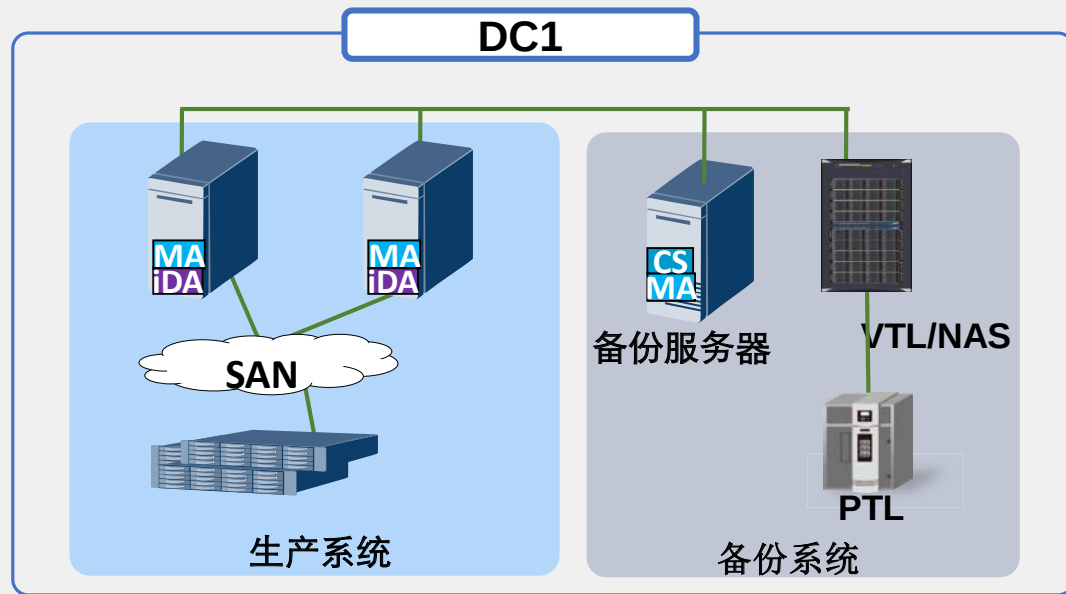
灾备中心也是成本中心，需要在满足业务系统要求的基础上，投入额外的预算来建设灾备中心，而灾备系统往往只有在IT系统发生故障或灾难时，才能体现其价值。

目录

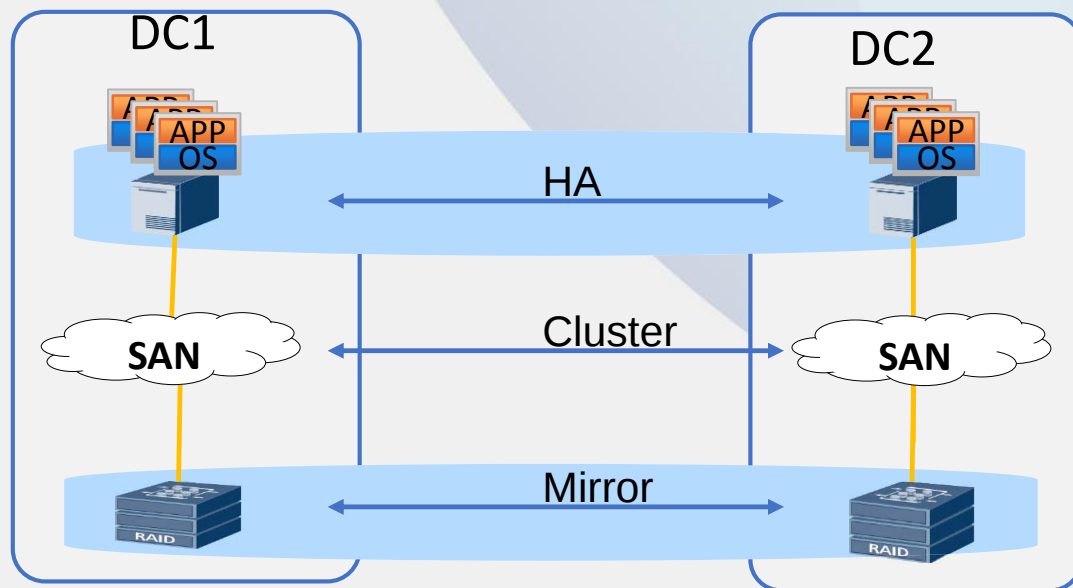
- 1 灾备建设意义与挑战**
- 2 灾备设计方法论**
- 3 企业云aCloud超融合灾备解决方案**
- 4 价值与优势**
- 5 案例实践**

灾备的定义：容灾, 备份

备份：备份是容灾的基础，通常指在数据中心内，将全部或部分数据集合从应用主机的硬盘或阵列复制到其它的存储介质的过程。



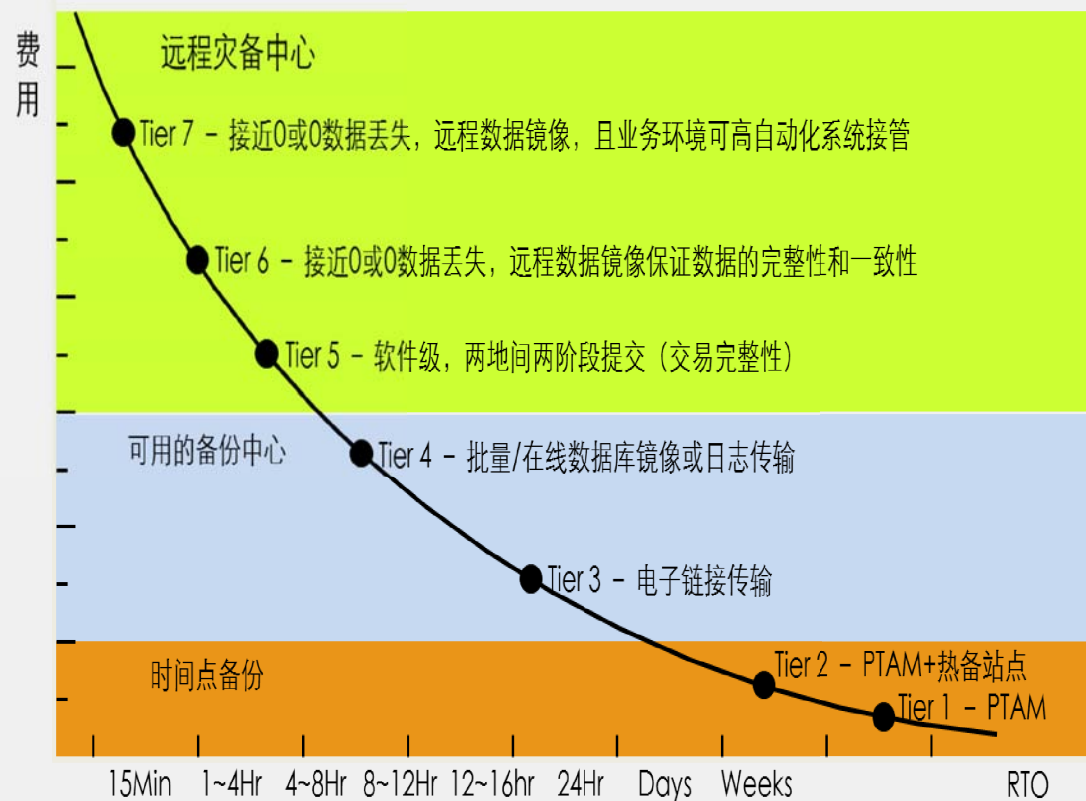
容灾：容灾系统是指在相隔较远的异地，建立两套或多套功能相同的IT系统，互相之间可以进行健康状态监视和功能切换，当一处系统因意外(如火灾、地震等)停止工作时，整个应用系统可以切换到另一处，使得该系统功能可以继续正常工作。



一般意义上，容灾指的是不在同一机房的数据或应用系统备份，备份指的是本地的数据或系统备份。通常说的灾备是将容灾与备份结合，即本地备份结合远程数据复制实现完善的数据保护。

灾备建设标准：国内标准、国际标准

根据SHARE 78国际组织提出的标准，可以将系统容灾的级别划分为如下7级。



本地备份——异地备份——主备容灾——双活容灾——两地三中心容灾
(GB/1-2级) (GB/3级) (GB/4-5级) (GB/6级)

根据《信息系统灾难恢复规范》国家标准GB/T 20988-2007,可以将系统容灾的级别分为如下6级。

6级	数据零丢失和远程集群支持	- 实现远程数据实时备份，实现零丢失 - 应用软件可以实现实时无缝切换 - 远程集群系统的实时监控和自动切换能力
5级	实时数据传输及完整设备支持	- 实现远程数据复制技术 - 备用网络也具备自动或集中切换能力
4级	电子传输及完整设备支持	- 配置所需要的全部数据和通讯线路及网络设备，并处于就绪状态 7*24 运行:更高的技术支持和运维管理
3级	电子传输和部分设备支持	- 配置部分数据、通信线路和网络设备 - 每天实现多次的数据电子传输 - 备用场地配置专职的运行管理人员
2级	备用场地支持	- 预定时间调配数据、通信线路和网络设备 - 备用场地管理制度 - 设备及网络紧急供货协议
1级	基本支持	- 每周至少做一次完全数据备份 - 制定介质存取、验证和转储的管理制度 - 完整测试和演练的灾难恢复计划

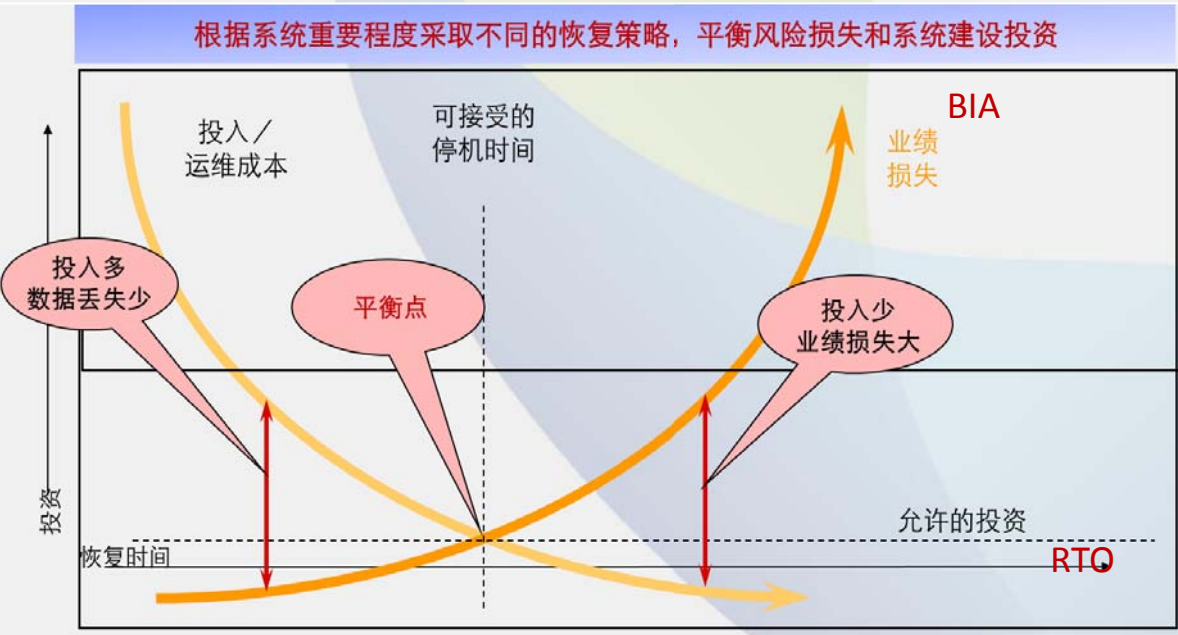
灾备的关键指标：RPO与RTO的平衡



- ◆ 数据恢复时间点(RPO)
- ◆ RPO (Recovery Point Objective):
 - ✧ 以数据为出发点
 - ✧ 能够容忍的数据丢失量
- ◆ 应用恢复时间 (RTO)
- ◆ RTO (Recovery Time Objective):
 - ✧ 以应用为出发点
 - ✧ 能够容忍的应用系统恢复时间段



RTO与RPO是衡量业务灾备系统可用性和可靠性的关键指标，应根据业务风险分析（RA）和业务影响分析（BIA）的综合评估制定合理的保护计划，以达到最佳的风险投资平衡点。



容灾等级 (GB)	RPO	RTO
1级	2天以上	1-7天
2级	24小时以上	1-7天
3级	12小时以上	数小时至1天
4级	数小时至2天	数小时至1天
5级	数分钟至2天	0到30分钟
6级	数分钟	0

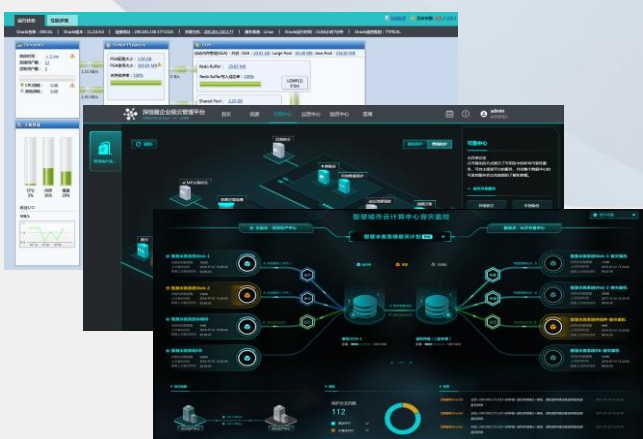
SANGFOR
深信服科技



容灾状态监控

异常切换

事后回迁



目录

- 1 灾备建设意义与挑战
- 2 灾备设计方法论
- 3 企业云aCloud超融合灾备解决方案
- 4 价值与优势
- 5 案例实践

深信服企业云aCloud超融合灾备解决方案架构

政府行业

金融行业

交通行业

能源行业

教育行业

医疗行业

大企业

.....

灾备管理

策略配置

网络IP配置

一键切换

一键回迁

状态监控

大屏展示

深信服云灾备解决方案架构

应用级容灾

链路全局负载

WEB高可用

中间件集群高可用

数据库高可用

云平台延伸集群

数据级容灾

CDP复制

存储延伸集群

跨中心多副本

数据库复制

第三方工具

备份（快照/CDP）

虚拟机备份

文件备份

数据库备份

操作系统备份

咨询服务

合作交付

容灾选型

链路设计

演练切换

服务交付

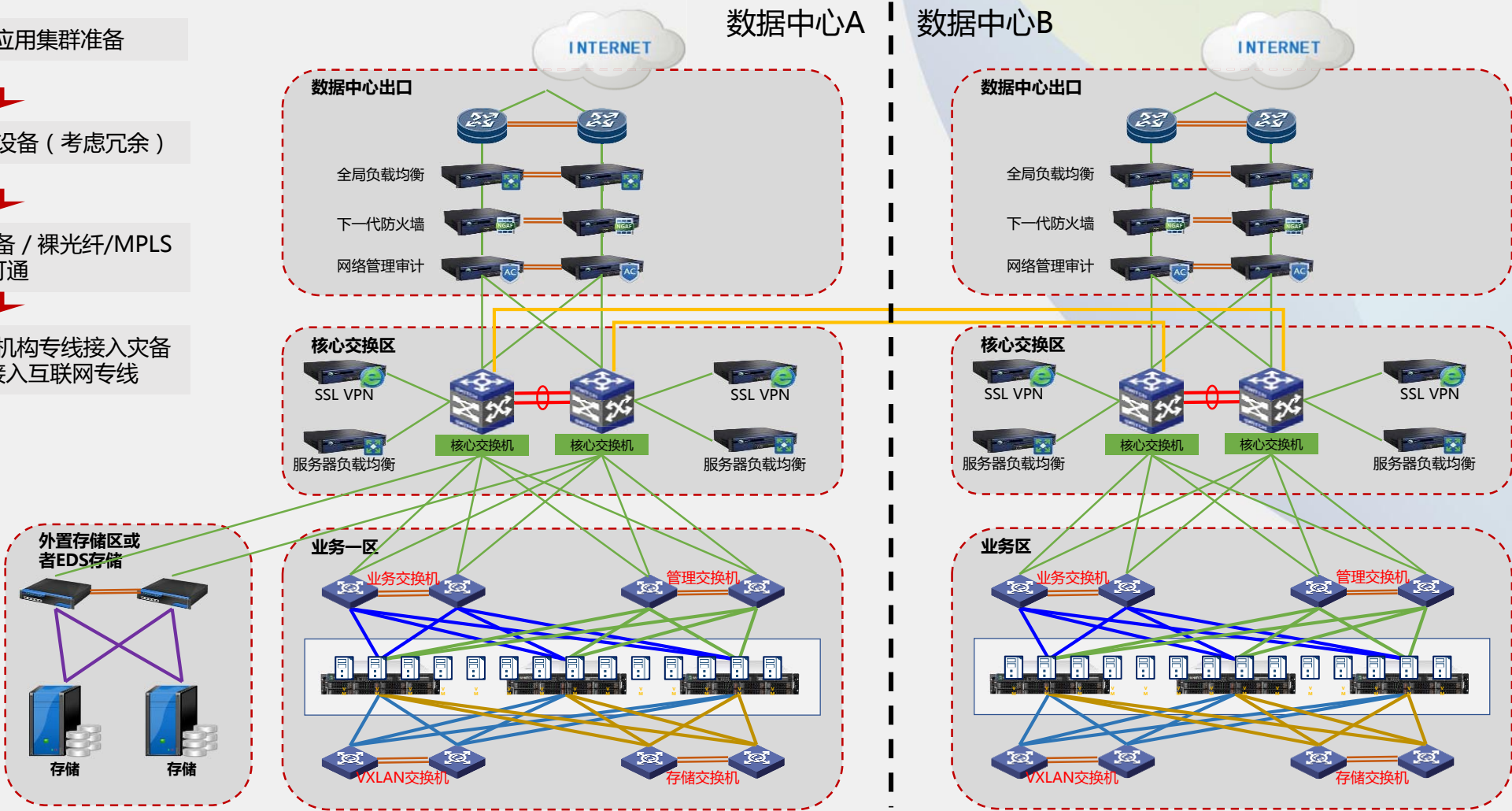
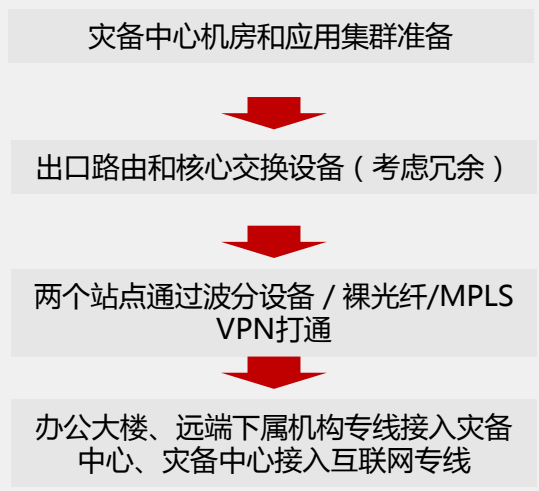
评估优化

企业云aCloud超融合数据中心A

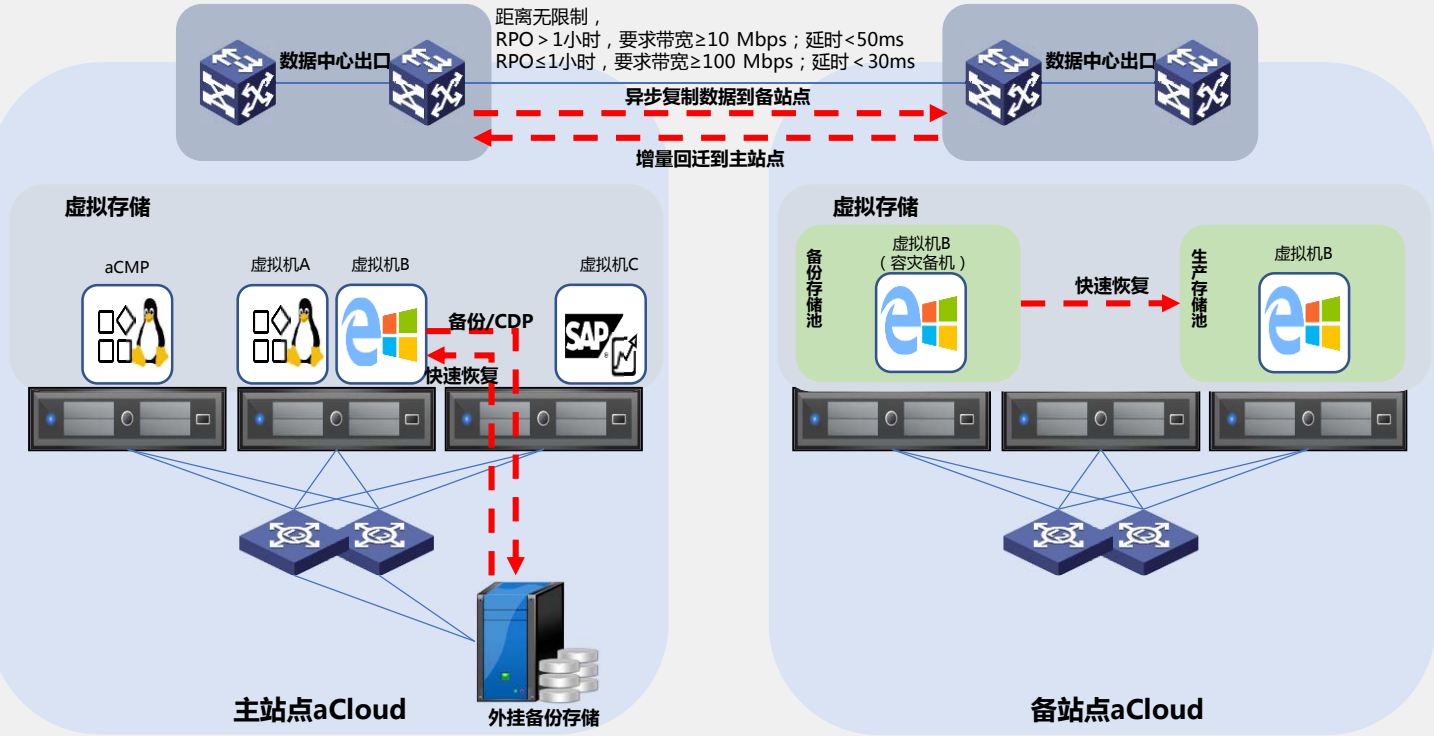
专线

企业云aCloud超融合数据中心B

容灾解决方案网络架构



超融合aCloud平台级主备容灾

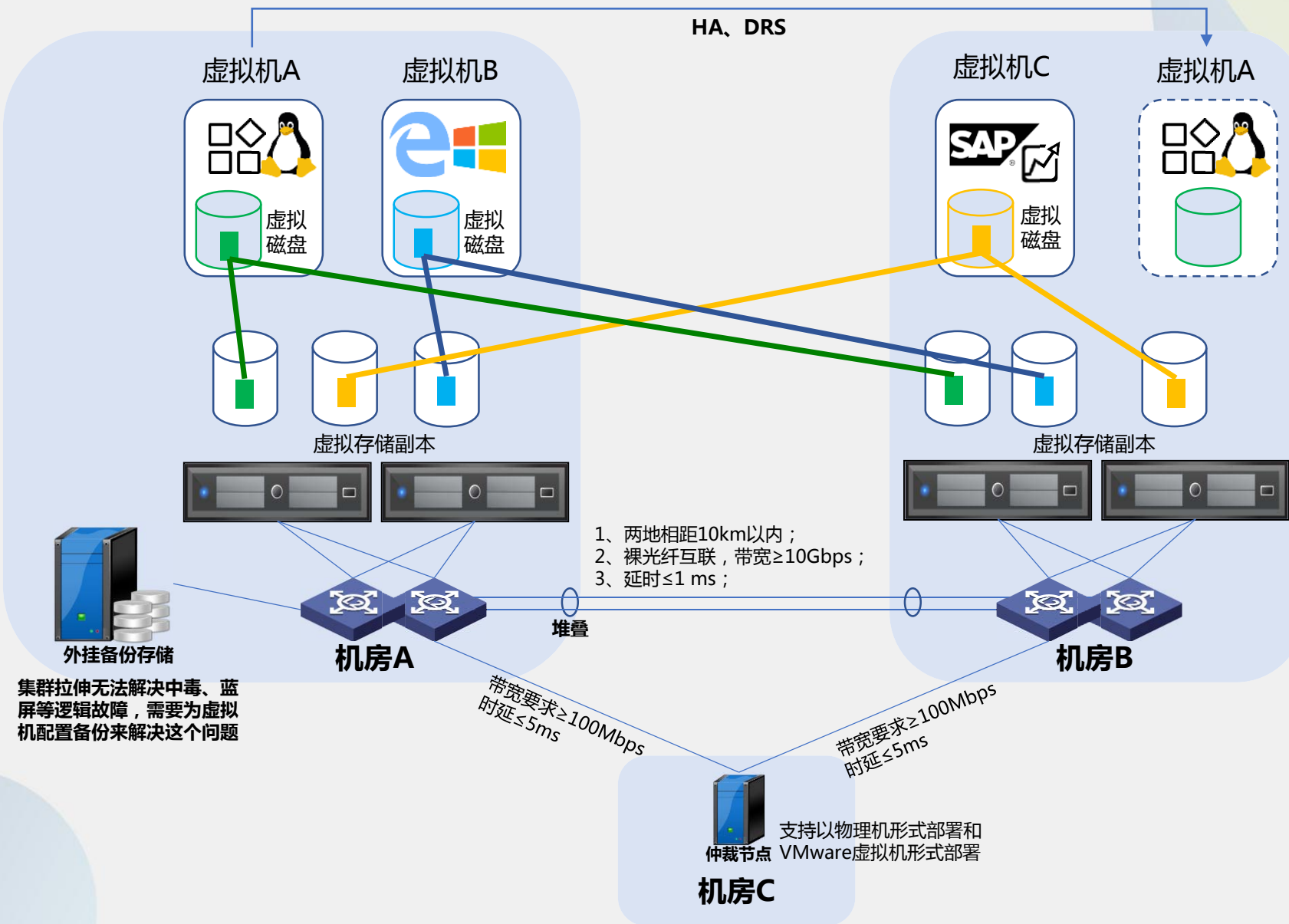


方案特点：

- 集成于平台中，融合交付，无须安装第三方软件和插件，一键获取容灾功能，是虚拟机级别的容灾方案
- 采用“**本地备份-异地容灾**”的方案，本地提供秒级的持续数据保护方案，当虚拟机出现故障时，可以快速从本地的保护数据中恢复整台虚拟机；异地提供**不同RPO**（1秒、10秒、10分钟、30分钟、1小时、2小时、4小时、8小时、12小时、1天、2天、一周）的虚拟机级容灾功能，主、备站点皆为深信服的企业云平台。
- 可根据RPO需求调整配置的带宽大小，提供**断点续传、压缩传输**功能，帮助用户节省带宽资源，节约成本
- 提供从备站点**一键恢复**的功能，可提前配置好恢复网络，RTO做到最小15分钟
- 提供从备站点**一键回迁**到主站点的功能，只回迁差异数据，降低虚拟机在备站点运行时间过长带来的风险（备站点往往环境不如主站点）
- 提供主、备aCMP管理平台，应对管理层的单点故障问题
- 提供**可视化的容灾监控中心大屏**页面，可以直观地看到当前容灾的配置关系、容灾的运行状态，可及时对可能出现影响RPO异常的告警进行处理
- 简单易用，无学习成本，帮助用户完成稳定可靠的IT创新

关键步骤	步骤说明
主站点备份/CDP	定期备份数据，确保数据在生产环境之外，有额外的数据副本；可以根据业务数据的重要程度，设置不同的备份周期（秒~天级）
快速恢复到主站点	当虚拟机发生系统性损坏，如蓝屏、黑屏、中毒，从主站点的备份中，选择最近可用的的备份点恢复整个虚拟机，恢复业务和数据。
异步复制数据到备站点	按照RPO，定期地将数据同步到备站点，确保在备站点上有额外的数据副本
从备站点快速恢复	主站点故障，在既定的RTO内，从备站点直接拉起虚机接管业务
增量回迁到主站点	主站点恢复正常后，将备站点上拉起的虚拟机回迁到主站点。（备站点机房条件往往比不上主站点）

超融合aCloud拉伸集群容灾方案



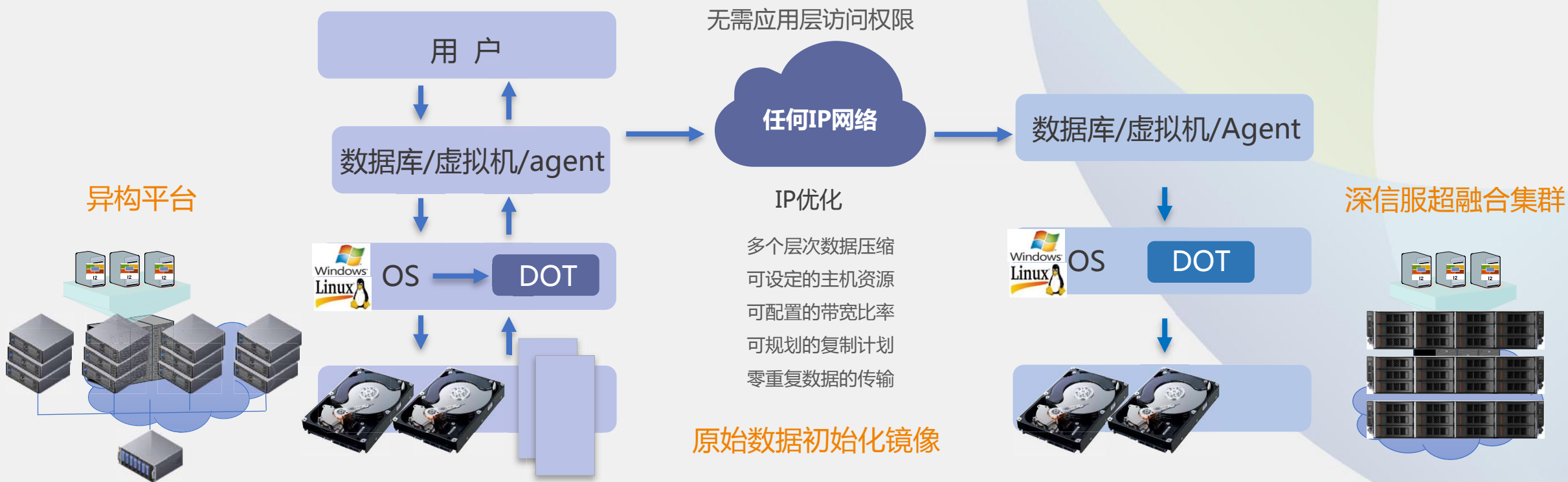
方案说明：

1. aCloud一个集群，集群内分成**两个故障域**，每个机房一个故障域，数据两副本分别落在两个故障域
2. 支持数据双活，即机房A和机房B的数据完全一致，RPO=0
3. 支持跨机房HA，即整个机房出现故障，虚拟机可以从另一个机房HA拉起，**RTO为3~5分钟**（虚拟机触发HA时间+重启时间）
4. 支持对分布式应用实现数据双活和业务双活，即RPO=0，RTO由应用自身的切换机制所需的时间决定，如**Oracle RAC 的RTO $\approx 30\text{s}$**
5. 仲裁节点故障或机房间的链路发生故障，虚拟机正常运行，不受影响

约束条件：

1. **最小交付节点为2+2**，一共4台，两地机房需要按照1：1配置主机节点
2. 两地机房之间需要**仲裁节点**，**建议部署在第三站点**，**带宽要求 $\geq 100\text{Mbps}$** ，**时延 $\leq 5\text{ms}$** （如果仲裁节点放在了机房A，机房A的节点和仲裁节点同时故障，虚拟机是无法从机房B拉起的）
3. 集群拉伸无法解决中毒、蓝屏等逻辑故障，需要**为虚拟机配置备份**来解决这个问题，使方案更完整。

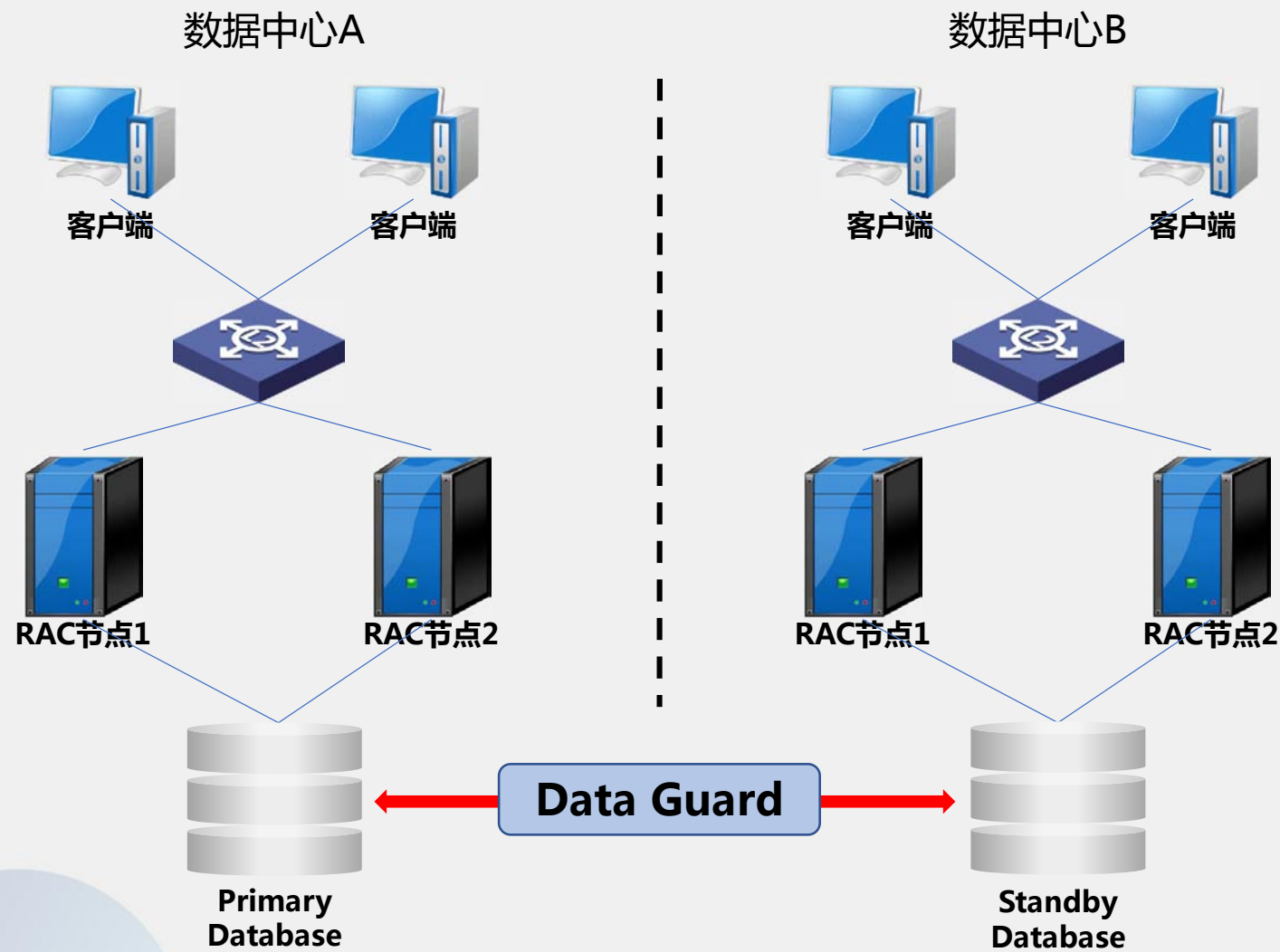
异构平台到超融合aCloud容灾



方案特点：

- **融合交付**，兼容主流操作系统，架构简单，交付快速
- **与平台无关**，支持物理服务器、VMware、华为、华三、Hyper-v、公有云主机等多种平台上的服务器灾备到灾备集群。
- 支持增量传输，以及多个层次的数据压缩能力，**带宽占用更小**
- 灾备集群提供池化的CPU、内存、存储资源，以及秒级、小时级、天级、周级的备份方案，解决业务层逻辑错误的担忧，**提供稳定可靠的备机运行环境**
- 提供从备站点**一键恢复**的能力，**RTO做到1分钟以内**
- 提供从备站点**一键回迁**到主站点的能力，只回迁差异数据
- 提供**可配置的带宽使用方案**，对带宽的使用更合理，利用率更高

Oracle数据库容灾设计



Oracle Data Guard (简称ODG) 确保企业Oracle数据库的高可用性，支持数据保护和灾难恢复功能，它提供了一整套服务，可以为生产Oracle创建、维护、管理和监视一个或多个备用数据库，并将这些备用数据库维护为生产数据库的事务一致性副本。

在某些情况下，业务数据是无论如何不能丢失的。而在有些情况下，某些应用程序需要最佳的数据库性能并能承担数据丢失风险。ODG **提供三种不同的数据保护模式**来满足这些不同需求

模式	特点	传输方式	应用场景
最大保护 Maximum protection	确保数据零丢失 可能会影响原数据库性能	同步	交易型业务，对数据安全极度敏感
最高可用 Maximum performance	不影响原数据库可用前提下，提供数据最高级别的数据保护	同步	优先保障业务连续运行
最大性能 Maximum availability	不影响原数据库性能 可能有少部分数据丢失	异步	并发访问极高的业务，允许少量数据丢失

同城或异地容灾用户访问切换机制

访问路径：

内网用户

①切换前：办公区 -> 核心交换机 -> 主DC接入 -> 服务器

②切换后：办公区 -> 核心交换机 -> vpn隧道 -> 备DC接入 -> 服务器

分支用户

①切换前：分支用户 -> vpn隧道 (woc_1) -> 核心交换机 -> 主DC接入 -> 服务器

②切换后：分支用户 -> vpn隧道 (woc_2) -> 备DC接入 -> 服务器

外部用户

①切换前：

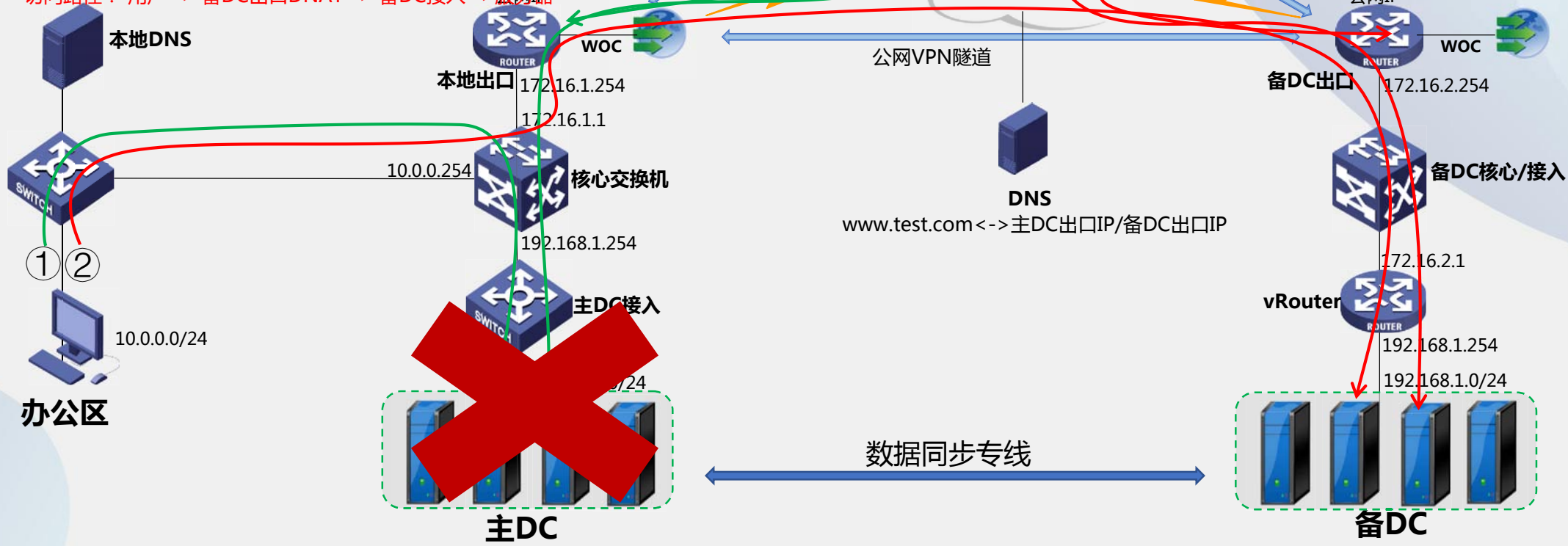
DNS A记录：www.test.com <---> 主DC出口公网IP

访问路径：用户 -> 主DC出口DNAT -> 主DC接入 -> 服务器

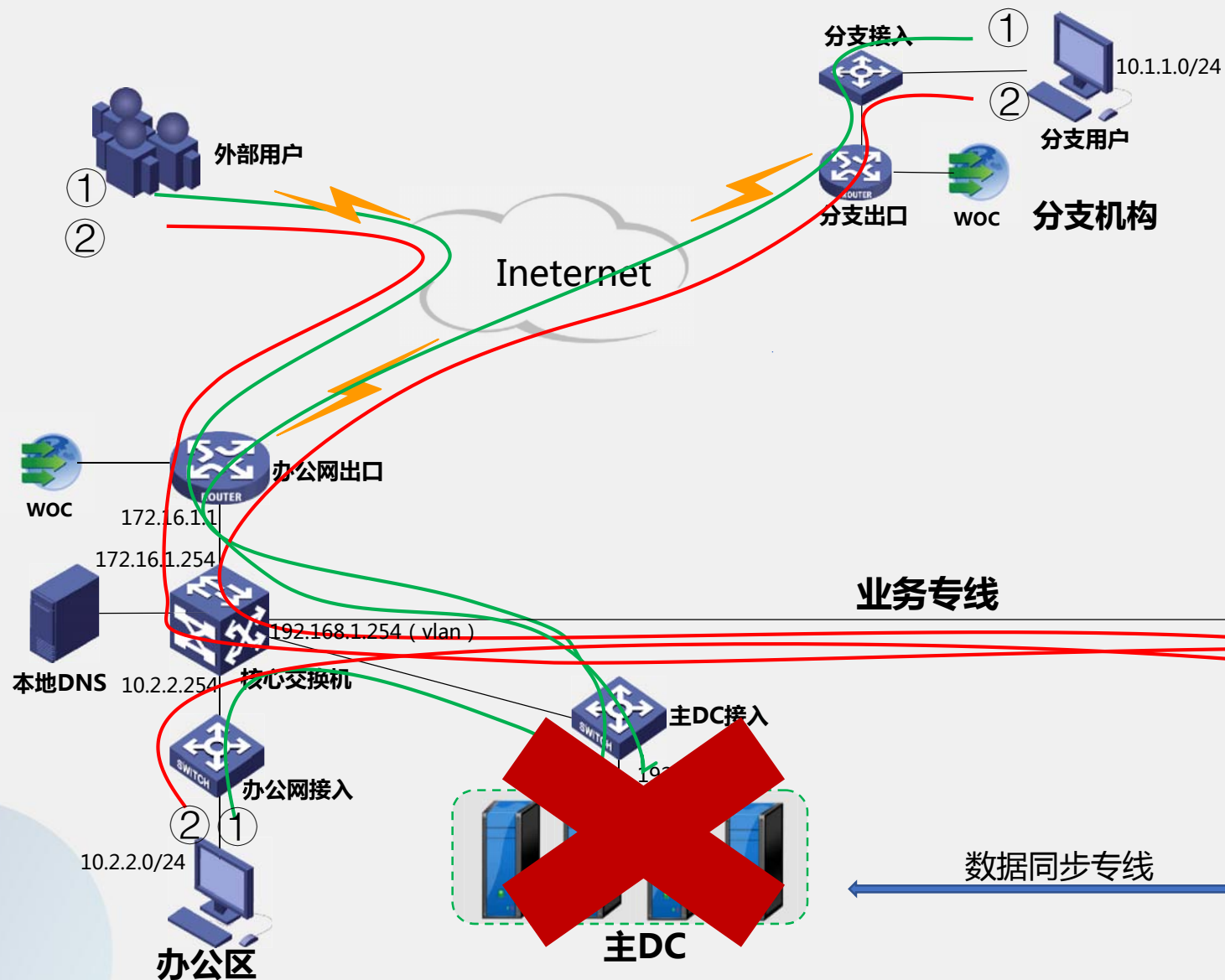
②切换后：

DNS A记录：www.test.com <---> 备DC出口公网IP

访问路径：用户 -> 备DC出口DNAT -> 备DC接入 -> 服务器



园区级容灾用户访问切换机制



互联网及内部用户访问路径 :②

①切换前

DNS A记录 : www.test.com <---> 192.168.1.1

访问路径 :

- ◆ 分支用户 -> 分支接入 -> 分支出口 -> woc隧道 -> 核心交换 -> 主DC接入 -> 服务器
- ◆ 内网用户 -> 办公接入 -> 核心交换 -> 主DC接入 -> 服务器
- ◆ 外部用户 -> 出口路由 -> 核心交换 -> 主DC接入 -> 服务器

②切换后

DNS A记录 : www.test.com <---> 192.168.1.1

访问路径 :

- ◆ 分支用户 -> 分支接入 -> 分支出口 -> woc隧道 -> 核心交换 -> 备DC接入 -> 服务器
- ◆ 内网用户 -> 办公接入 -> 核心交换 -> 备DC接入 -> 服务器
- ◆ 外部用户 -> 出口路由 -> 核心交换 -> 备DC接入 -> 服务器

容灾线路和带宽计算



RPO受数据更改速率与带宽的影响，在某个RPO时间段内的平均数据更改量，必须要在给定的带宽条件下，在该时段内传输完毕。下表为常用RPO与带宽关系一览：

RPO	数据变化类型	数据变化量	需要的带宽
1秒	IO吞吐	5MB/s	40 (Mbps)
		10MB/s	80 (Mbps)
		30MB/s	240 (Mbps)
2小时	每小时数据增量	1GB	3 (Mbps)
		5GB	15 (Mbps)
		10GB	25 (Mbps)
		20GB	50 (Mbps)
		50GB	160 (Mbps)
12小时	每6小时数据增量	50GB	20 (Mbps)
		100GB	45 (Mbps)
		150GB	70 (Mbps)
		200GB	100 (Mbps)
		300GB	160 (Mbps)
24小时	每12小时数据增量 43200	50GB	10 (Mbps)
		100GB	20 (Mbps)
		150GB	30 (Mbps)
		200GB	45 (Mbps)
		300GB	70 (Mbps)

专线模式：

DWDM+裸光纤：高性能，低时延(适合园区级双活延伸集群容灾场景)

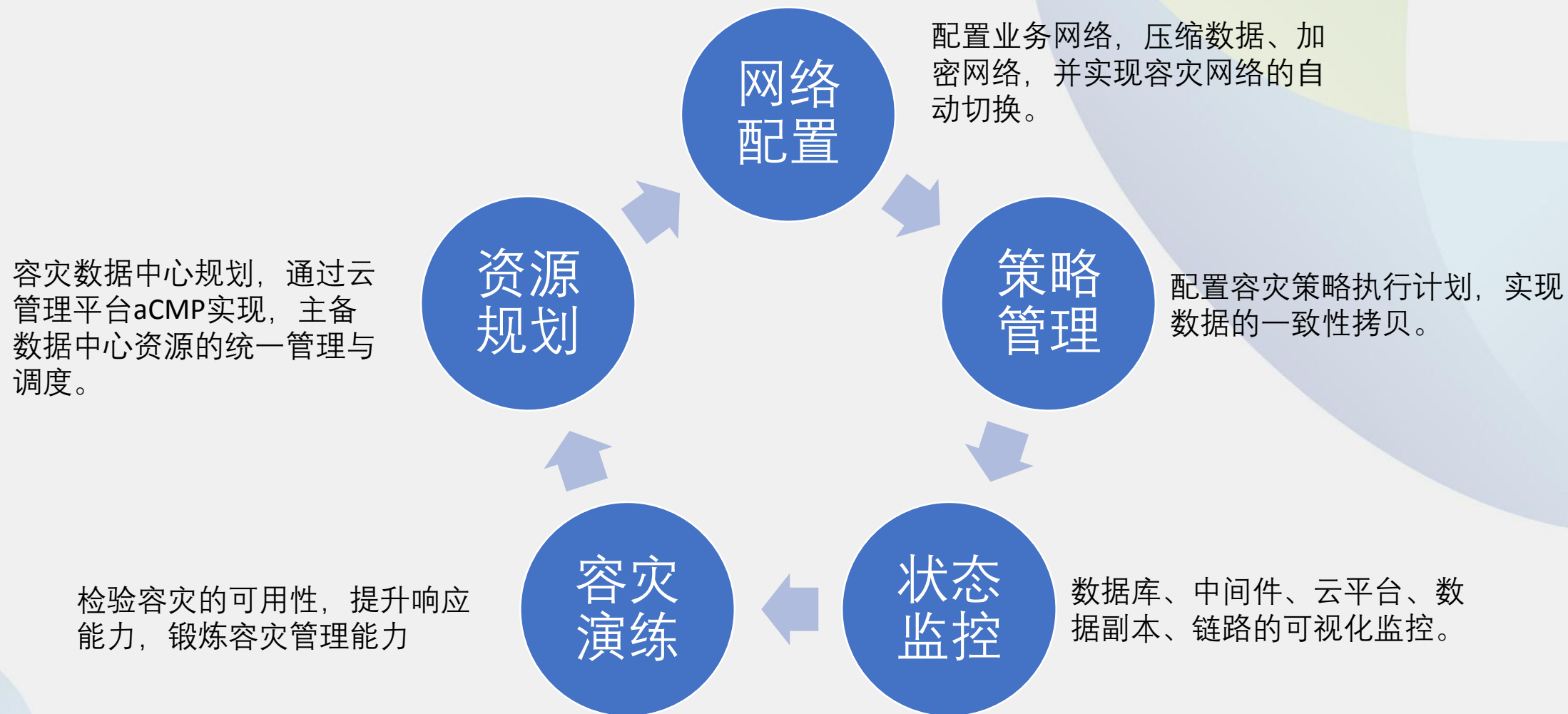
MPLS VPN专线：高性价比，配置简单（适合同城、跨城主备容灾场景）

aCloud-aCloud容灾带宽核算公式

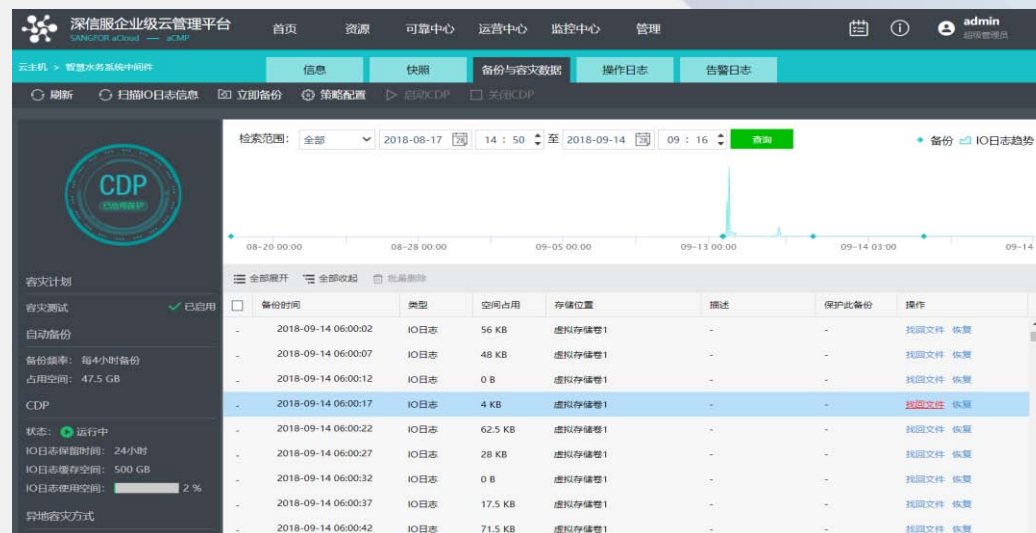
项目	RPO要求	同步数据间隔	间隔时间内的数据变化量	本地备份速率	需要的带宽
示例	1天	12小时	12小时内数据变化量：100GB	50MB/s（默认值）	$100\text{GB} * 1024 * 8 / (12 * 3600 - 100\text{GB} * 1024 / 50) \approx 20\text{Mbps}$
公式	R 秒	R/2 秒	R/2 秒内的数据变化量：N GB	T MB/s	$N * 1024 * 8 / (R/2 - N * 1024 / 50)$

说明：aCloud-aCloud的容灾，需要先将数据备份到本地备份存储中，才同步到异地，所以计算带宽时，要将本地备份的时间减掉。

容灾全生命周期管理



容灾策略配置与恢复演练



容灾状态监控



目录

- 1 灾备建设意义与挑战
- 2 灾备设计方法论
- 3 企业云aCloud超融合灾备解决方案
- 4 价值与优势
- 5 案例实践

深信服容灾解决方案价值与优势

以客户为中心，项目成功为导向，
从容灾的咨询、规划、设计、实施、
管理及培训提供端到端的服务

①端到端容灾服务

深信服容灾解决方案，从平台、数据、网络、
管理四个层面提供容灾保护机制，保障灾难
故障时，RPO、RTO实现分钟级业务恢复。

②四重容灾机制保障

价值与 优势

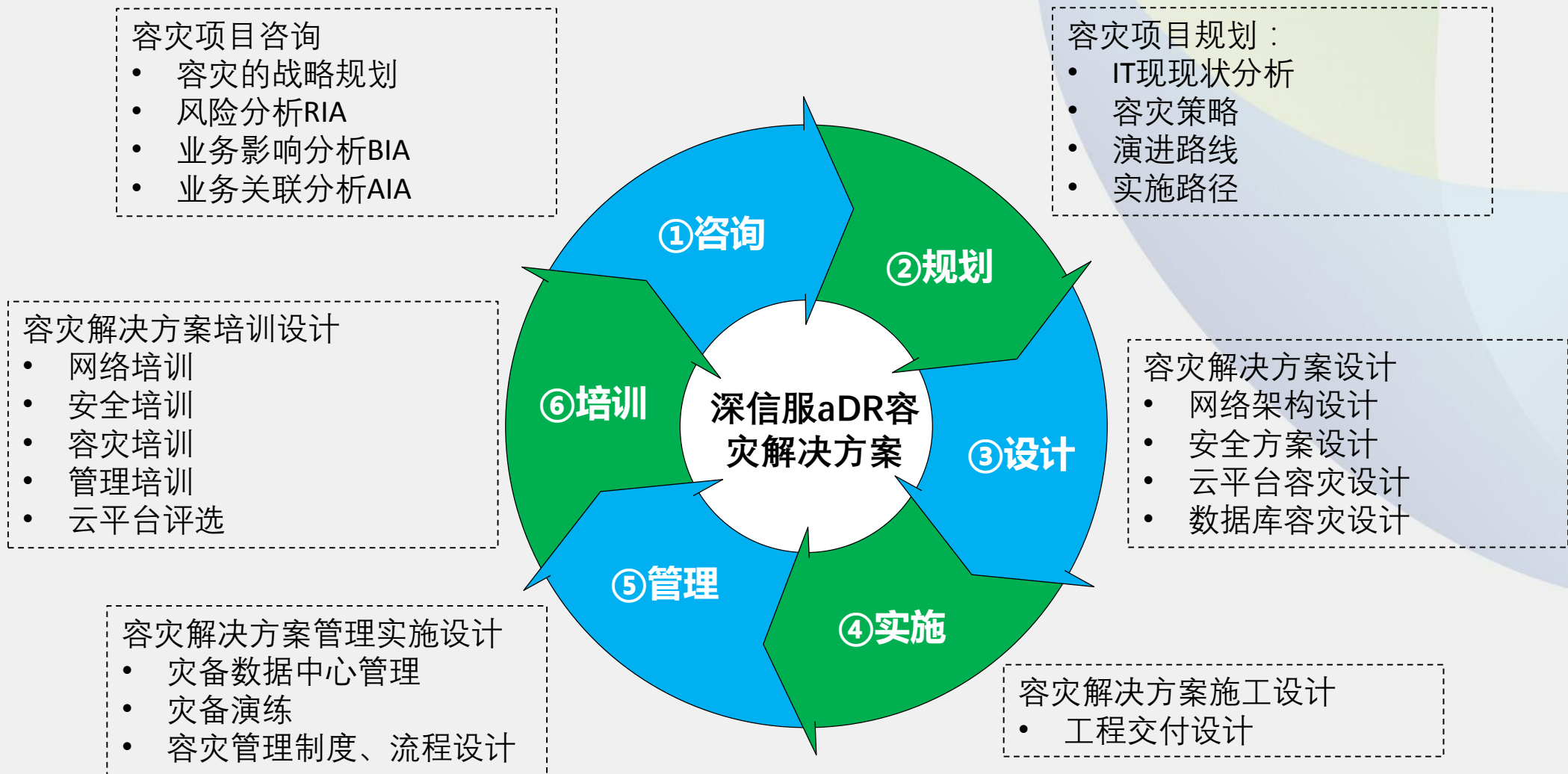
④最优性价比

深信服解决方案利用超融合平台，可实现
同构和异构平台的容灾，数据加密、
压缩等，降低平台和网络带宽成本。

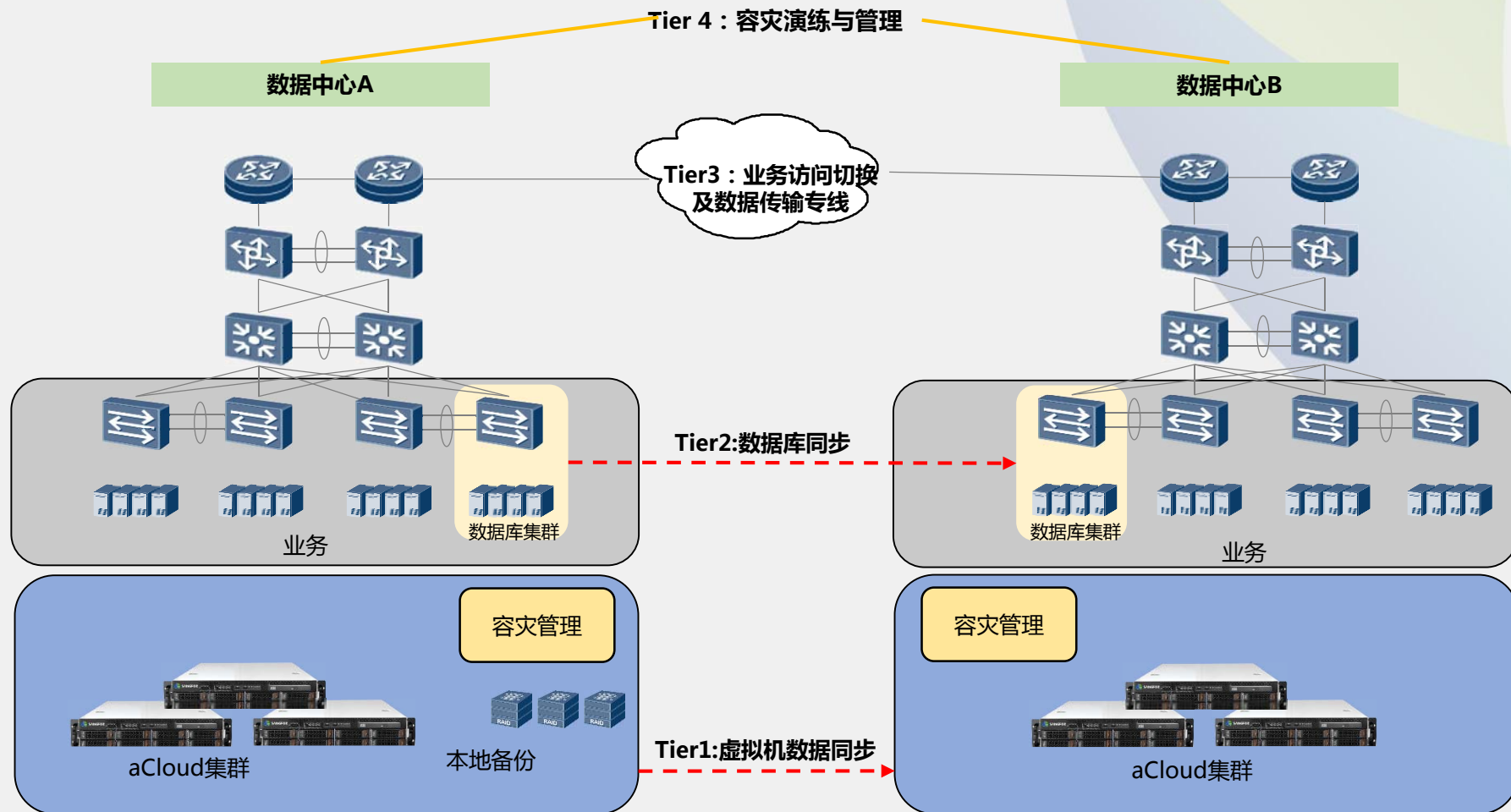
③可视化容灾管理

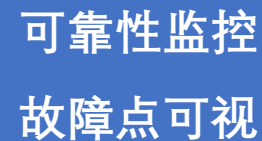
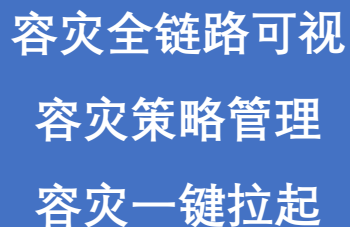
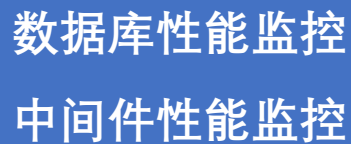
提供可视化容灾管理平台，可实现容灾
的策略管理、容灾演练功能，并提供容
灾全链路的可刷性能监控。

价值一：客户为中心，提供端到端容灾服务



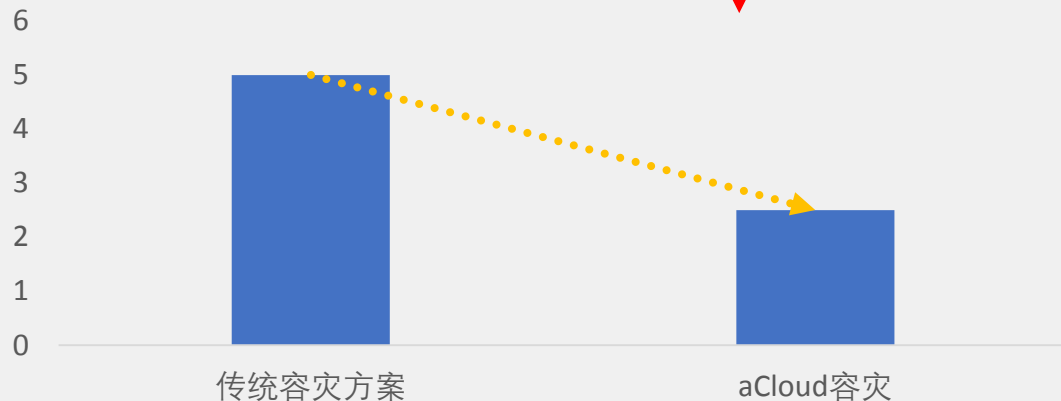
价值二：四重容灾保障机制，快速实现容灾业务切换



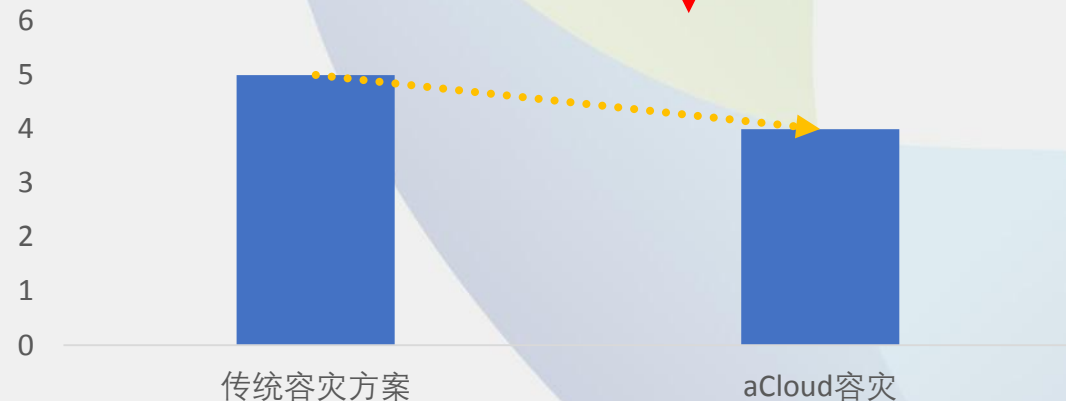


价值四：最优性价比，容灾不再是成本负担

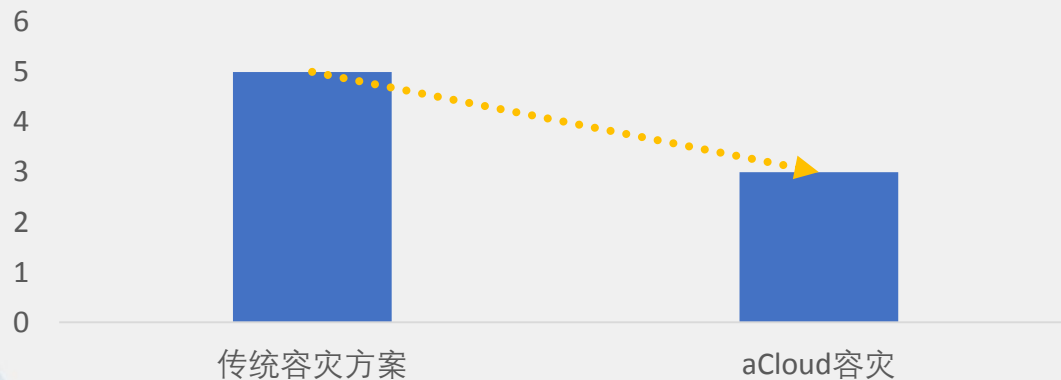
专线成本 50%



IT成本 20%



人力运维成本 40%

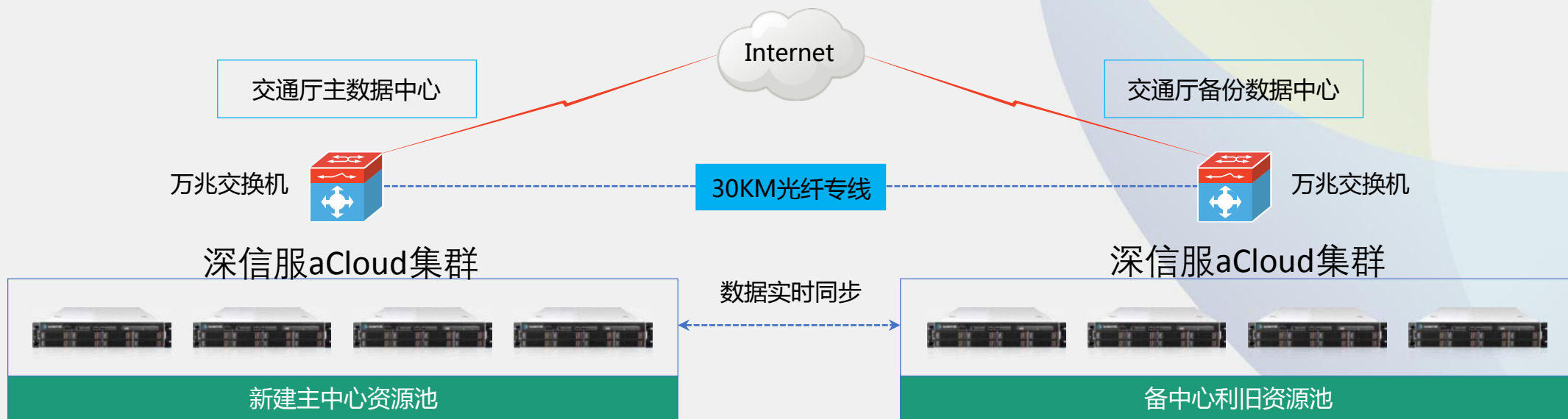


- 采用超融合架构作为载体，相对传统数据中心建设模式，可以节省20%的投资，
- 利用WOC对容灾数据进行压缩与加密，可以节省50%带宽
- 超融合平台运维简单、并集成容灾管理平台，降低人力运维成本40%；

目录

- 1 灾备建设意义与挑战
- 2 灾备设计方法论
- 3 企业云aCloud超融合灾备解决方案
- 4 价值与优势
- 5 案例实践

典型案例：广西省交通厅aCloud容灾方案



业务发展面临的挑战

- 随着电子政务发展，交通厅及下属公司业务数据量爆发性增长，数据丢失后果严重。
- 传统灾备方案架构高昂，实施复杂，预算有限情况下，难以落地。

深信服解决方案及价值

- 纯软件超融合建设方案，灾备数据中心服务器利旧，线性建设，降低灾备投资。
- 可视化灾备管理，轻松灾备切换。

THANK YOU