闪存化政务云统一灾备中心建设

（华为）

一、背景

构建基于云计算技术的政务云数据灾备平台，将各委办局的政务云业务系统进行集中数据保护。充分发挥云计算虚拟化、高可靠性、通用性、高可扩展性等优势，利用现有数据中心基础，建设完善政务云数据灾备服务职能，提升信息安全保障能力，保障政府信息系统安全可靠运行。

在本方案中，基于业务和数据安全优先考虑、平台运营的权责分离、应用系统安全可控、各业务子平台弹性扩展、云平台统一管理等原则，并充分利用闪存存储高性能、高可靠特点，建设一个闪存化的统一政务云数据灾备平台。

二、方案

（一）建设原则

根据国家和我省信息安全发展战略、规划和电子政务总体框架的要求，以“统筹规划、资源共享，平战结合”为原则，以灾备需求为引导，以现有资源为依托，以政务云业务数据灾备为主体，努力确保基础设施投入实际效益，坚决制止重复建设和投资浪费，按照统建共用、统一运维、集中投入、规范化、社会化、专业化和可持续发展的思路实施我省政务云灾备中心建设。

1.统筹规划：在项目建设过程中，要从实际出发，针对灾备系统的整体要求，统筹规划，分步实施。对于由财政投资建立和在建的政务云系统，要加强管理，数据保护统一纳入灾备中心，原则上不得自行再建。

2.资源共享：为保证信息系统的抗毁性和可用性，政务云灾备系统建设应是立体式的、多样的。在灾备系统建设过程中要充分利用云计算存储技术和已有基础，集中建设灾备系统，以实现资源共享。

3.平战结合：加强平战结合，充分利用和平时期的现有资源，服务于地方。在不影响容灾备份和恢复功能的前提下，充分利用容灾备份设施的各类资源，开展科学研究、培训人才、应急演练等工作，切实提高灾备中心的利用率。

政务云灾备中心的建设，主要是为了实现，当政务云业务数据发生错误或丢失时可以快速，准确的恢复数据，同时将关键业务的数据丢失风险降到最低。总体目标体现如

下：

关键业务应用系统 RTO 小于等于 2 小时；RPO 等于 0 小时；

非关键业务应用系统 RTO 小于等于 24 小时；RPO 小于等于 24 小时；

切换目标：能够实现整体切换和局部切换。

根据政务云对安全等保合规以及业务连续性的要求，统一规划“两地三中心”的备份容灾方案，分为政务云主数据中心、政务云同城灾备中心和政务云异地灾备中心。规划提供本地备份、异地备份、存储双活、同城应用双活和异地容灾等能力满足业务的备份和容灾需求。

根据灾备方案建设的进度，整体将分为 3 步：

第一步：建设本地数据备份，建立政务云主数据中心的数据灾备能力，当数据发生异常时能快速恢复，确保数据的可用性，使平台具备本地数据容灾能力，同时建设本地存储双活实现存储级的保护；

第二步：建设同城+异地数据备份，在政务云同城容灾机房和异地容灾机房建立远程备份系统，实现数据的同城或异地保存和恢复，具备数据的同城和异地容灾能力

第三步：建设同城应用双活，及异地容灾，实现完整的灾备能力。

（二）方案概述

灾备中心基础设施资源包括计算、存储、网络、备份和容灾等，建设总体按照基于 OpenStack 框架的 IaaS 云服务资源池架构，形成逻辑统一的虚拟资源池，为各单位提供计算资源服务、存储资源服务、网络资源服务等 IaaS 层服务。

政务云平台基础设施建设内容包括：基础设施资源池、备份、容灾建设等基础设施资源池。该方案规划建设三个数据中心——政务云主数据中心、政务云同城灾备中心和政务云异地灾备中心：

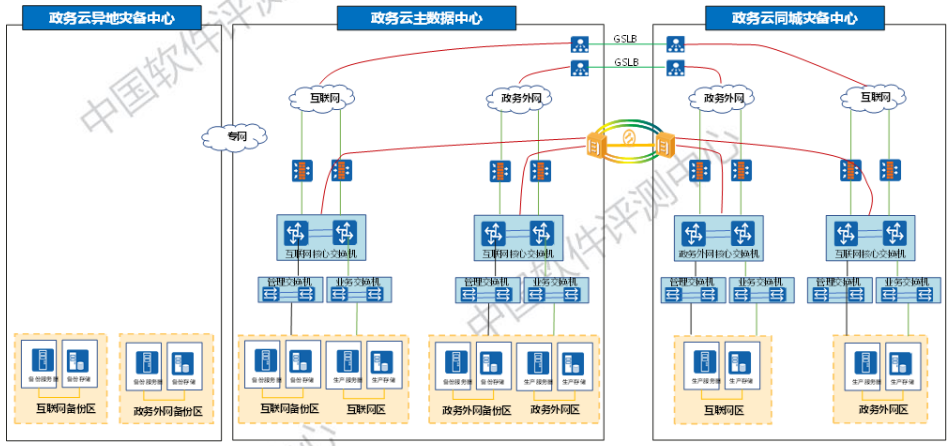
1.政务云主数据中心：提供云主机和核心应用的备份服务，核心业务（数据库）的高性能块存储高可用服务；

2.政务云同城灾备中心：提供主备容灾服务。当主中心出现异常无法对外提供服务时，可以通过同城灾备中心；

3.政务云异地灾备中心：提供异地远程备份服务，备份数据复制到异地灾备中心，提升业务安全性。

灾备架构图如下所示：

灾备方案的整体建设架构如下图所示：



本地备份分为云主机备份和应用备份，适配政务云所有业务，主要在政务云主数据中心部署，实现数据本地备份。

异地备份主要适配需符合安全等保三级及以上要求的业务，在异地灾备中心部署备份系统，与政务云主数据中心协同完成异地备份。

针对核心应用（数据库）部署的高性能存储，提供存储高可用服务，主要在政务云主数据中心部署。

在政务云主数据中心和同城灾备中心：在同城灾备中心部署核心应用（数据库）高性能块存储和重要业务的通用块存储，与主中心对应的存储复制实现同城容灾。

（三）方案详述

1. 备份方案

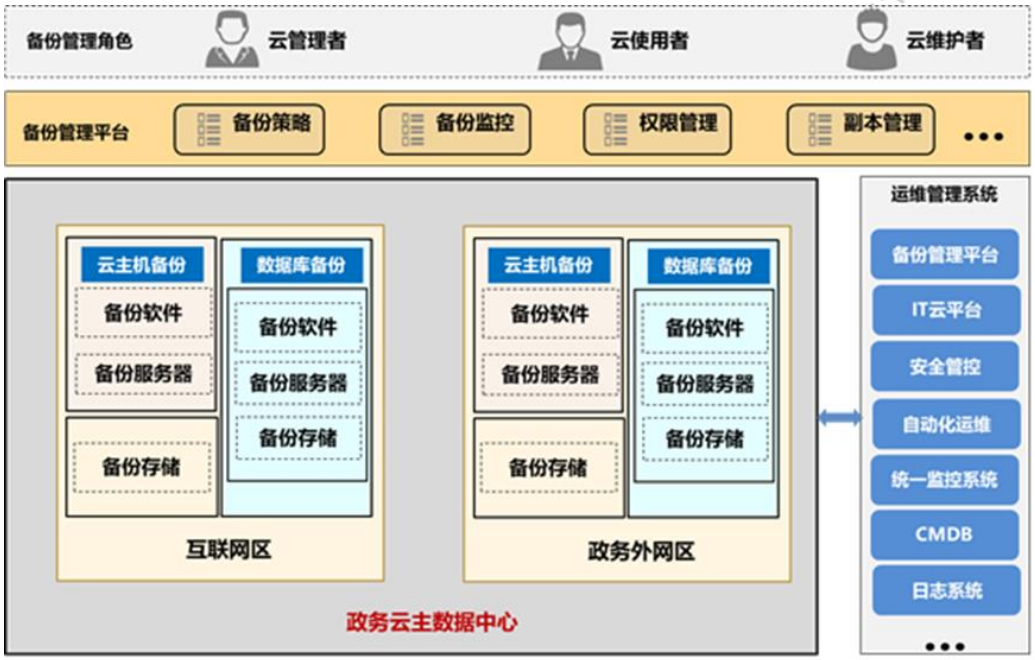
为建立一个统一、可靠、安全、可管理的统一数据备份服务，为各局委办的业务数据提供数据保护，有效控制数据安全风险，并降低数据安全管理成本。

本方案设计云备份服务能力，支持多租户的共享使用，提供基于虚拟机、数据库、文

件、视频和图片的在线数据保护。为委局办客户提供全方位的数据保护机制。当委局办在遭遇数据灾难时，能完整、准确、快速地还原数据，最大化降低数据丢失风险。

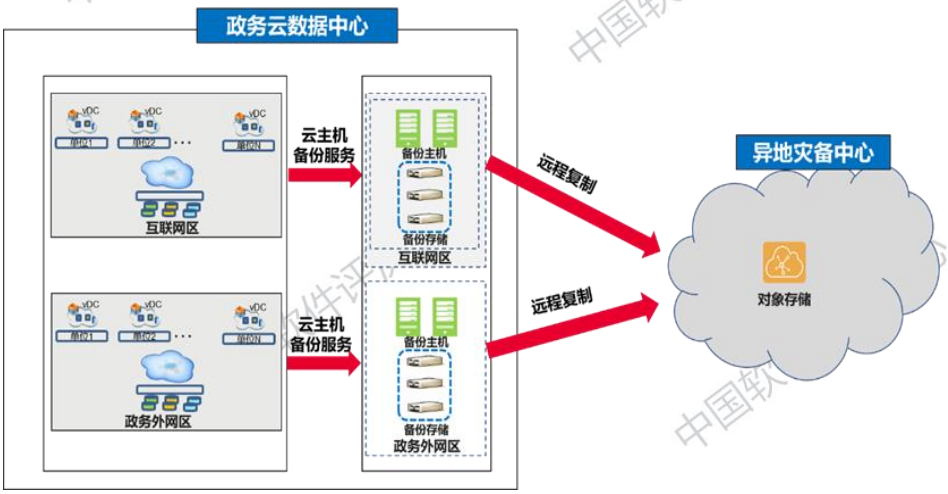
备份服务的开通是自助完成的，用户只需要指定备份对象、备份策略、复制策略（可选），系统将会自动创建备份服务实例，同时用户也可以根据需要调整备份服务实例。

针对数据中心的政务外网区和互联网区务采用分区独立的备份设计，备份链路和备份介质资源池分区间互相隔离，如下图所示。

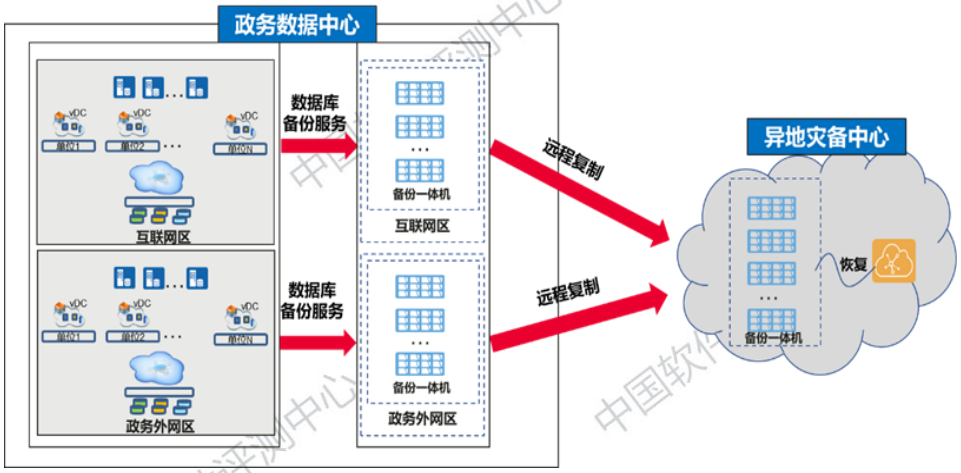


每个分区的备份架构相同，采用备份软件和分布式备份存储架构，单个分区备份详细组网如下所示。

云主机备份方案组网和备份数据流如下图所示：



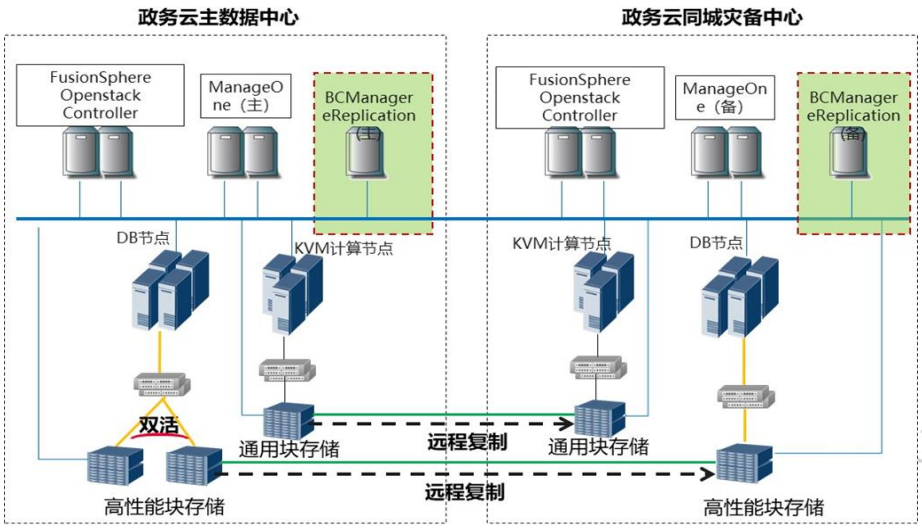
数据库备份组网和备份数据流如下图所示：



2.容灾方案

政务云需要 7*24 全天业务连续运营越来越成为优质核心业务的关键保障，对 RTO 和 RPO 的追求也越来越趋于极限 0，容灾成为政务云保障业务连续性的标配，正常情况下，业务运行于主数据中心，当出现突发情况，主数据中心不可用时，同城灾备中心可以快速恢复业务应用和数据，减轻灾难给委办局造成的损失。

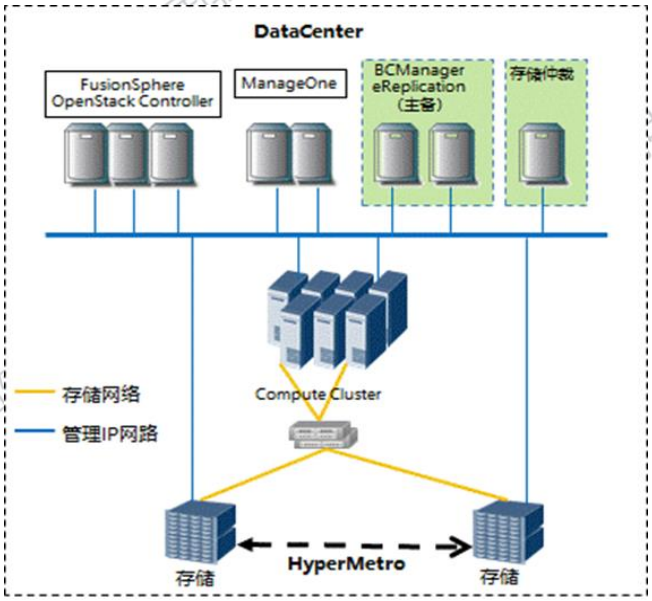
同城灾备中心可以为政务云提供容灾服务，当政务云出现意外情况，导致无法对外提供业务访问的情况下，可以快速切换到同城灾备中心快速恢复业务应用和数据。整体容灾架构如下图：



以上在政务云数据中心构建存储双活（VHA）、同城容灾（CSDR）服务，满足政务云业务和数据的容灾需求。

云硬盘高可用服务（Volume High Availability Service）简称 VHA，为 ECS/BMS 中

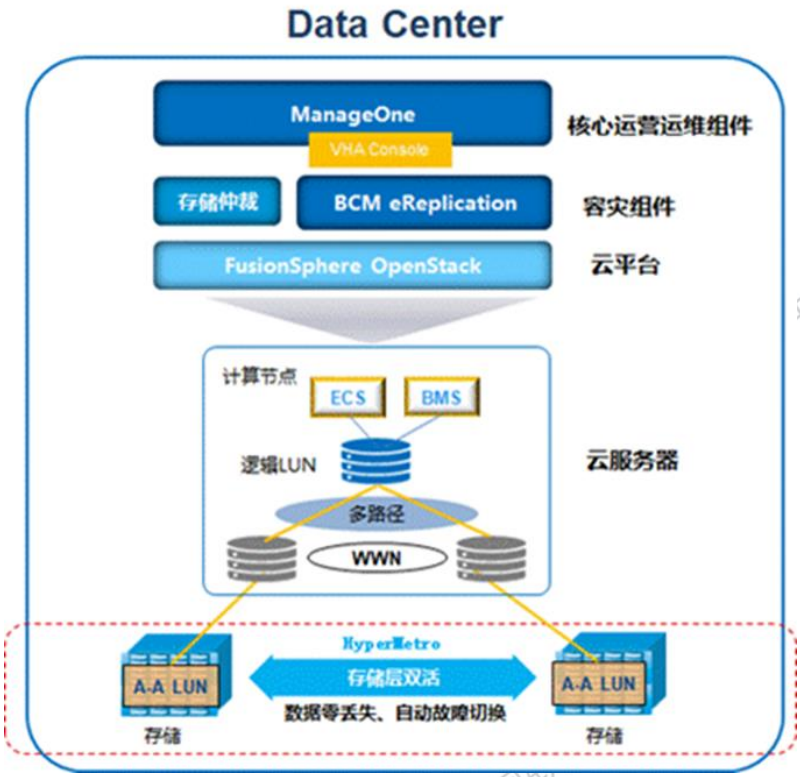
的云硬盘提供本地存储双活保护。当单套存储设备发生故障时，数据零丢失，业务不中断。该方案是基于 FusionSphere OpenStack 云操作系统平台的 IaaS 层容灾方案，通过云数据中心结合存储双活实现单 AZ 内的云硬盘容灾，避免存储单点故障，导致业务中断或数据丢失。



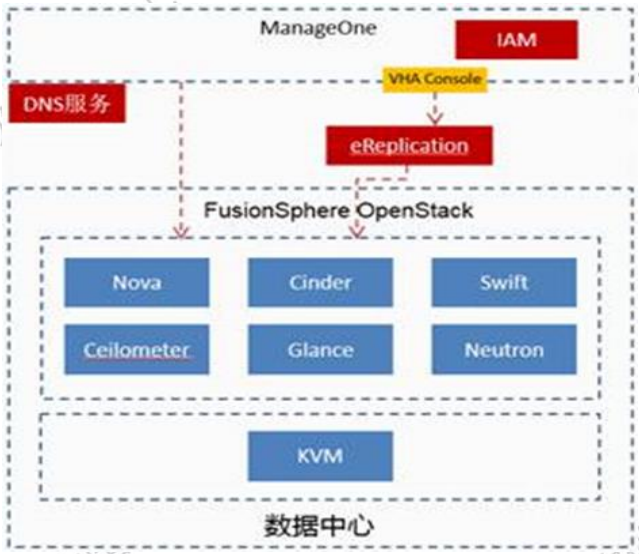
云硬盘高可用服务与网络是解耦的，原则上使用华为云的通用网络方案即可，仅要求在通用组网方案上预留存储网络端口，增加两套双活存储间的双活数据路径即可。

云硬盘高可用服务是针对 AZ 内实现存储双活，为实现该容灾功能，需要对基础设施进行如下部署：

- AZ 内存储双活：需要至少部署两套存储用于配置存储双活，建议配置存储双活的两套存储设备型号相同且版本相同，并采用全闪存存储提升性能。
- 部署存储仲裁：在管理节点上部署存储仲裁虚拟机。用于为双活存储提供仲裁，当一个存储故障时，通过仲裁机制确保另一个存储存活并正常对外提供服务。
- 部署 VHA 服务组件：在管理节点上部署 BCManager eReplication 虚拟机；VHA Console 已合并到 ManageOne 中，不需单独部署虚拟机。
- 配置存储双活：对 AZ 内两套存储配置双活集群，并对接存储仲裁，以实现一个存储故障时通过多路径自动切换而不影响业务。



在同一个 Region 内的单个站点内部署一套 FusionSphere OpenStack 云平台，实现 AZ 内的云硬盘高可用，为云硬盘提供本地存储双活保护，当数据中心内单套存储发生故障时，数据不丢失，云服务器业务不中断。

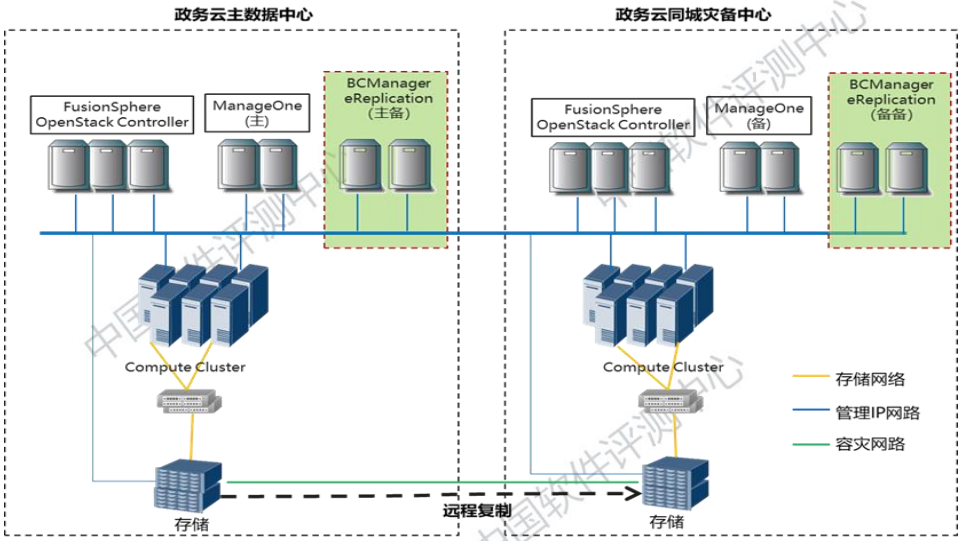


管理组件主要包括 FusionSphere OpenStack，ManageOne 和 BCManager eReplication。其中 BCManager eReplication 为容灾管理组件，通常会以主备或 HA 方式部署到生产中

心及灾备中心，用于容灾管理。

云服务器容灾服务（CSDR，Cloud Server Disaster Recovery），为云服务器提供跨 Region 异地容灾保护，当生产中心故障，可在异地容灾中心快速恢复云服务器。

此外，生产中心的云服务器还可叠加配置本地存储双活保护，形成本地存储双活+异地远程复制存储环形容灾，当生产中心单套存储设备发生故障时，数据零丢失，业务不中断。仅在生产中心发生整站点灾难时，才需要切换到异地容灾中心。



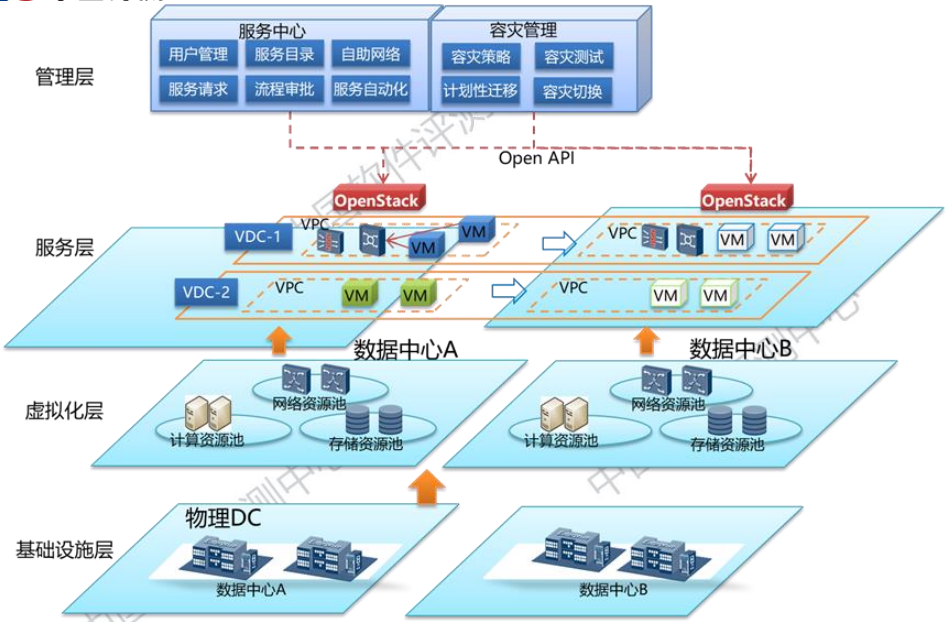
如上图所示，根据项目规划，建设政务云主数据中心和政务云同城灾备中心两个云数据中心，两个数据中心之间构建 IaaS 层的基础容灾能力。通过部署的 eReplication，实现两个数据中心容灾的保护和灾难恢复管理。相对于非容灾场景下的两 Region 部署，部署 CSDR 容灾服务需要增加：

1.BCManager eReplication 组件，采用虚拟机部署；CSDR Console 已合并到 ManageOne 中，不需单独部署虚拟机。

2.对于 Global 管理组件需部署跨 Region 主备容灾。

3.对于生产 Region 和容灾 Region 间的存储需配置远程复制。支持的存储类型包括：集中式存储、分布式块存储。

4.可以扩展环形容灾：数据中心内存储双活，单个存储故障，数据不丢失，业务不中断；数据中心间仅支持存储异步复制（最小复制周期为 5 分钟），不支持同步复制。复制过程不影响云服务器计算性能。



如图所示自下而上，云数据中心逻辑上分为多层，管理组件主要包括 ManageOne、云服务 Console、DNS 服务组件、BCManger eReplication、FusionSphere OpenStack，其组件用途及关系如下：

- ManageOne

负责租户门户和业务申请发放。负责租户及管理员的授权、云服务的授权管理，起用户登录、资源操作的鉴权作用。

- 云服务 Console

各云服务面向租户提供服务实例增删改查用户界面，并对用户输入的参数做校验，实现云服务的自助运营。安装注册于 ManageOne 中。

- BCManager eReplication

eReplication 容灾管理组件，在主 Region 和备 Region 主备部署一套，用于容灾管理，主 Region 发生灾难后，切换到备 Region。

- FusionSphere OpenStack

OpenStack 各个组件需要分别在生产中心和灾备中心部署，各自管理本地资源。

- 内部 DNS 服务组件

每个 Region 均独立部署一套，彼此间无复制关系。内部 DNS 仅用于组件间交互的 DNS 解析，不用于租户或对外提供 DNS 服务。主要用于 ManageOne 与云服务、云服务 Console 与云服务后端、数据库、云服务与 OpenStack 间交互的 DNS 解析。

每个 Region 的内部 DNS 组件的域名配置，应当按照华为云 Stack 多 Region 场景的部署要求配置，主备 Region 中的 DNS 组件包含各 Region 的全量域名信息，以确保每个 Region 的服务组件，均能够与 Global 层的 ManageOne、eReplication 等通信。当管理面

进行主备切换时，需刷新内部 DNS 的解析记录，完成组件间访问的主备切换。

三、设备选型

（一）存储设备选型

统一灾备中心存储选型应满足以下要求：

- 高可靠：存储应支持双活、同步复制、异步复制等能力，并具备应对复制链路质量抖动的能力。存储应具备平滑提升灾备等级的能力，以实现更灵活的灾备建设。
- 高性能：作为支撑政务能力一体化平台的存储设备，需要具备极高的性能，且在不同业务压力下表现平稳。
- 高集约度：由于承载大量数据和多样业务，存储应具备极高的集成能力，能够负载多种业务的数据访问。

本方案推荐采用华为 OceanStor Dorado 全闪存存储作为数据底座，它具有以下特点：

- 极致性能：OceanStor Dorado 存储专门面向全闪存设计，采用业界顶尖的全均衡架构，和面向闪存优化的 FlashLink 算法，最大化闪存潜力发挥，大幅提高了存储性能；率先支持端到端 NVMe 架构，大幅缩短存储访问时延，并在业务高峰期时延无明显波动。
- 极致可靠：OceanStor Dorado 存储采用业界领先的自研 SmartMatrix 全互联架构，是业界唯一容忍控制器八坏七业务不中断的存储；OceanStor Dorado 存储也是业界唯一支持 SAN&NAS 一体化 A-A 双活的存储，还率先支持了复制光纤劣化后的秒级倒换，大幅减少了单存储故障后的切换时间，提升了业务可靠性。
- 极致集约：OceanStor Dorado 存储单套存储支持 SAN、NAS、S3 等协议，文件共享和双活都无需网关，并且对虚拟化、容器和各类数据库提供良好的兼容性，一套存储即可满足几乎所有业务诉求。

（二）数据保护一体机设备选型

华为数据保护一体机是一款集备份软件、备份服务器、备份存储为一体的数据保护与数据管理产品。基于分布式架构设计，性能与容量线性增长，一套设备即可满足保护、构建、管理用户数据和应用，帮助用户提升数据保护效率、节省数据保护投资、简化数据管理流程，广泛适用于政府、金融、运营商、医疗、制造等行业。

- 全面保护

集中保护企业复杂的 IT 环境，全面保护 Windows、Linux 等主流操作系统；VMware、FusionCompute 等主流虚拟化平台；Oracle、SQL Server 等主流数据库；Hadoop 等大数据平台，实现虚拟、物理、云环境的统一保护和集中运维，降低管理复杂度和成本投入，

有效避免单点方案难管理、成本高等问题。CDM 致力于构建开放融合的生态体系，与多家主流厂商合作，实现互认证。

- 卓越性能

面对指数级、爆炸式增长的业务数据，CDM 软件提供多重数据保护技术，如：并行重删、永久增量备份、并发备份、CBT 变化数据块跟踪、多通道备份等，不断追求更高效的数据保护性能，帮助用户从容面对 PB 级数据保护。

- 弹性扩展

采用集群式架构，保障备份业务高可用，并消除单节点故障导致备份业务不可用的问题，确保备份业务连续性。同时，支持负载均衡，增强吞吐量、提升业务处理性能。采用 Scale-out 架构，根据业务发展规模，按需扩展集群节点，无需停止备份业务，灵活满足业务需求。

- 智能灾备运维

能够提供全生命周期的灾备保障，覆盖分析、评估、设计、实施、演练、运营多个环节。同时通过统一运营管理平台，可提供多样化报表服务，全方位概览灾备运行状态。基于全面的日志分析，合理调整优化灾备策略。

CDM 软件具有核心功能如下：

- 集中数据备份

用户自定义备份时间点和周期，使系统按照任务策略和计划，定期自动发起数据备份。用户无需购买多套单点方案，即可通过一个平台，保护所有应用，其保护对象全面覆盖文件系统、主流数据库、虚拟化平台、云平台等。当数据丢失或损坏时，根据不同的场景、不同应用类型，用户可以选择灵活高效的恢复方式。

- 副本数据管理

从主存储（生产存储）通过快照技术获取有应用一致性保证的数据，在 CDM 软件中创建活动的“黄金副本”（golden image），可通过“黄金副本”按需提供多个数据以原始磁盘格式组织的虚拟化副本，直接挂载出来给到诸如备份/恢复、容灾、开发/测试等场景使用。

- 持续数据保护

按照一定的时间频率，持续的纪录并备份数据变化，并持续复制到 CDM 中，在特定的情况下可以做到 RPO≈0，而且当灾难发生后，只需要简单的选择要恢复到的时间点即可实现数据快速恢复使用。

- 并行重删

通过重删，数据源中重复的数据在备份过程中均可以被识别并消除，适用于不同平台中的文件、数据库、虚拟机等不同应用类型的数据，可以大幅度减少需要传输的数据量，从而极大地节省数据传输带宽，节约备份数据所占用的存储空间。

并行重删，是指在集群环境中，重删计算由多个节点并行，提交去重效率，用户可根据硬件设备的配置来决定并行重删的计算的并行节点数。

- 永久增量备份

传统的周期性完全备份与增量备份模式，在大型数据应用备份场景下，将面临备份窗口大，存储空间占用多的挑战。而永久增量技术，首次执行完全备份，之后只对新增的数据进行增量备份，并自动合成完全副本。不仅大幅度缩减备份时间，还能节省大量存储空间。

- 异地数据容灾（远程复制）

现代企业进行数据保护，不仅希望能够实现本地数据保护，也能有灾备中心进行异地数据保护。如此，即便本地数据中心遭遇地震、火灾等重大自然灾害或人为操作失误等事故，导致本地备份数据或生产数据发生损坏或丢失时，能够通过异地数据灾备，确保数据可恢复性。CDM 支持通过远程复制功能，将数据同步到异地灾备中心，实现异地数据容灾。

- 自动化备份策略

提供备份计划等策略，便于系统自动触发备份、恢复管理方式，简化管理操作，提升灾备管理的运维效率。

- 完善的安全管理机制

采用基于四员体系的权限管理机制，数据加密算法等，实现数据管理安全。

（三）灾备管理软件选型

华为 OceanStor BCManager eReplication 是面向企业数据中心的容灾管理软件，实现主备、两地三中心、双活等容灾场景的统一管理，简单高效的完成对数据库应用、虚拟化环境以及云环境的容灾业务配置，清晰可视的掌控系统容灾业务的运行情况，快速方便的完成数据恢复和测试演练，该产品具有以下特性：

业务一体化

- 支持对虚拟化环境的应用一致性保护
- 支持对物理环境的应用一致性保护
- 支持对云环境的应用一致性保护
- 容灾备份一体化融合管理

管理自动化

- 应用自动识别
- 提供模板化的策略配置
- 支持可定制化的恢复流程
- 支持一键式容灾切换
- 支持一键式容灾测试

- 按时按需生成副本及副本自动挂载
- 支持分权分域的用户权限管理
- 支持 REST 北向接口，与客户其他管理系统集成

容灾可视化

- 提供可视化的容灾拓扑展示
- 提供可视化的容灾流程展示

华为 BCManager eBackup 是一款针对华为 FusionSphere 和 VMware vSphere 虚拟化及云平台的备份软件，基于虚拟机快照、存储快照和 CBT（change block tracking）技术，对虚拟机数据提供全面的保护。它是一个满足海量虚拟机备份场景、简单易用、性价比极高的数据保护方案。该产品具有以下特性：

高效备份

- 永久增量备份
- 无合成恢复技术，10 倍效率提升

海量虚拟机备份

- 分布式可扩展 64 节点，保护 10000 虚拟机
- 任务自动负载均衡，1 分钟内完成任务故障切换

租户级自动备份

- 1 分钟完成备份服务申请
- 备份、恢复自动执行，无需人工干预

简单易用

- 配置向导，4 步完成虚拟机保护
- 图形化界面直观监控备份系统运行状态