产品名称	密级
Distributed Cloud Data Center	
产品版本	
V100R001C10	

华为云数据中心解决方案技术白皮书

拟制 _____ 日期 _____

审核 _____ 日期 _____

批准 _____ 日期 _____

华为技术有限公司

修订记录

日期	修订版本	修改描述	作者

目 录

表目录

图目录

Key words 关键词：

分布式云数据中心，VDC，VPC，虚拟化，SDN，容灾，备份，安全，云管理，资源弹性

Abstract 摘要： 本文是分布式云数据中心解决方案 V100R001C10 技术白皮书。

术语和缩略语清单：

术语/缩略语	描述
DC^2	分布式云数据中心
VDC	虚拟数据中心
VPC	虚拟私有云
SDN	软件定义网络
IAAS	基础设施即服务
PAAS	平台即服务
SAAS	软件即服务
DRAAS	容灾即服务
RTO	恢复时间目标
RPO	恢复点目标
DC	数据中心
SLA	服务等级协议
VPN	虚拟专用网络
VFW	虚拟防火墙
EBS	弹性块存储服务
RD	虚拟机容灾软件（Replication Director）
EIP	弹性 IP
SNAT	源地址转换
DNAT	目的地址转换
SC	服务中心（Service Center）
OC	运维中心（Operation Center）
FM	云管理中心（FusionManager）
eSight	eSight 是华为公司 DC 基础设施监控平台，包括网络、服务器、存储设备的告警、性能、拓扑等监控能力
TCO	拥有总成本
ROI	投资回报率
OpenStack	开源云管理平台，对虚拟计算、存储、网络等服务提供管理框架与开放 API，支持多种虚拟化平台

1 技术背景

1.1 数据中心架构现状

传统的大型企业数据中心是一个物理分层的架构。随着公司规模的增长以及跨地域众多分支机构的建立，企业全局应用集中部署来实现跨地域跨组织的共享，在每个地域中建立地域级数据中心满足地域内各分支机构的应用集中部署和数据共享。而营业/办公网点则一般采用模块化或者集装箱方式建设微数据中心，主要是解决网络安全接入的问题。

以华为自身的数据中心建设为例，可以很容易理解大型企业的数据中心物理分层架构。华为企业级的数据中心部署在深圳和南京，主要负责全球业务的应用集中部署，同时通过深圳和南京的异地容灾解决数据中心的安全可靠性问题。在俄罗斯、英国和南非等 7 个地方建立区域级别的数据中心，建立全球应用的镜像同时集中共享区域应用和数据，每个区域级数据中心覆盖数个到数十个国家的业务，通过部署区域级别数据中心，可以保证网络响应时间在 100ms 内。在每个区域，仍然存在对于服务质量要求更高的应用，如研发仿真等，这样在 100 多个地区又建立了服务器机房。对于遍布全球的分支机构，主要是建设网络机房解决纯网络接入问题。

1.2 数据中心架构的挑战

目前数据中心架构采用按应用烟囱式构建基础架构的方式，存在以下挑战：

✧ **建设与运营成本高**。数据中心建设成本高昂，按应用垂直构建运营系统，当需要支持新建业务或扩展已有业务能力时，需要不断对现有数据中心扩容。大量构建的小规模DC或分支机构DC的建设和维护成本更高。

✧ **资源利用率低**。目前的数据中心的资源使用理念为应用间隔离，资源容量按照应用的最大预期负荷来设计。同时，资源为应用静态分配，大部分时间数据中心的计算、存储和网络资源利用率低下。一般情况下，数据中心服务器资源利用率常年低于15%。资源利用率低也带来能效比低的问题，数据中心的能耗成为企业心头之痛。

✧ **服务SLA保证困难**。数据中心层次过多时，使用者访问应用时必然会造成较大时延，尤其是对于处于分层架构顶端的应用，所需经过的数据中心站点网络环节和层级过多，这就加大了网络连接故障或流量拥塞发生的概率；同时由于数据中心基础设施设备均按照应用最大峰值流量需求进行容量和部署规划，缺少对企业用户漫游及业务热点变化的感知能力，因此面向企业最终客户接入的业务体验优化将更加困难。

✧ **管理复杂**。由于数据中心承载的业务多种多样，而不同业务对软硬件系统的要求以及容灾备份策略各不相同，因此按应用纵向构建基础设施的方式造成了协同管理非常困难。如何全局管理的效率，降低物理资源和应用的耦合度，使得业务能实现快速部署上线，实现对业务的扩容、升级等全生命周期管理都对数据中心管理提出了极大的挑战。

1.3 数据中心的发展趋势

新一代数据中心的目标应是建设高效节能与运营成本合理的数据中心，支持企业或机构业务的持续发展，满足对业务的全生命周期管理需求。高利用率、自动化、低功耗、管理自动化等成为了新一代数据中心建设的关注点。

✧ **数据中心的分布化建设和集中化管理成为方向**

- 数据中心向基础设施的分布式建设和管理的集中化方向发展

- 数据的集中化管理和数据中心的整合是当前信息化发展的方向
- 行业需求推动的技术发展趋势将支撑数据中心的分布式建设

✧ **数据中心日益提供整合的网络、存储和计算能力，管理工具的重构和发展将成为核心的控制点**

- 可编程的虚拟网络交换方式将带来更多挑战和机会
- 数据中心竞争将由单个设备竞争变化为提供整个网络架构的竞争
- 数据中心基础设施管理系统将成为未来数据中心的核心控制点

✧ **数据中心向全方位服务化方向发展**

IT成本分析、桌面帮助、IT服务管理和数据中心基础设施监控—只有极少数的系统管理软件工具不能作为一个服务处理。通过IaaS/PaaS/SaaS等不同层级的服务，为企业用户提供方便灵活的业务选择。数据中心成为服务中心，是多种服务的承载容器，这是数据中心发展的必然趋势。

✧ **向基于云计算技术的软件定义数据中心发展的趋势**

- 资源全面池化：计算虚拟化向存储虚拟化和网络虚拟化发展，基于 SDN 技术为实现基于业务需求的可编程、高度弹性和动态、大规模的虚拟化网络提供了技术支撑，数据中心存储资源的统一虚拟化后构成统一的资源池，包括服务器内存储资源、直连存储阵列、异构的各类存储系统，如 NAS、SAN 和统一存储等。
- 资源按需分配：包括计算、存储、网络和安全等所需资源、基于 SLA 的虚拟数据中心（VDC）服务，VDC 部署时间下降到分钟级，资源按需快速发放。
- 混合云：多数企业将探索私人和公共的云技术的混合，我们称之为混合云。未来几年，以 IT 服务交付为服务重点中心的私有云服务企业将会出现。企业应该评估哪些是商品服务，并将它们转移到公共云。

✧ **安全与可靠性成为未来数据中心的基础能力**

安全性并不单指防火墙、IPS/IDS、入侵检测以及防病毒等安全防范措施。实际上，火灾、飓风和其他灾害能在任何时候袭击数据中心。在数据中心建设的初始阶段就应该构建可靠的容灾方案，或建立异地的灾难备份中心。通过多种技术手段保障业务的连续性和数据的安全性。

2 分布式云数据中心解决方案架构

2.1 分布式云数据中心解决方案架构目标

为了应对数据中心面对的挑战并顺应技术发展趋势，华为提出了分布式云数据中心（DC^2）的理念。分布式云数据中心是物理分散，逻辑统一，业务驱动，云管协同，业务感知的数据中心。

分布式云数据中心以融合架构（计算、存储、网络融合）作为资源池的基础单元，构建SDN业务感知网络，通过自动化管理和虚拟化平台来支撑IT服务精细化运营。分布式云数据中心的核心理念在于：物理分布、逻辑统一。它可以将企业分布于全球的数据中心整合起来，使其像一个统一的数据中心一样提供服务，通过多数据中心融合来提升企业IT效率。去地域化、软件定义数据中心、自动化是这个阶段的主要特征。逻辑统一有两方面的含义：所有数据中心及其资源统一管理、调度和运维支持，分权分域管理，这些能力需要分布式云数据中心提供统一的运维管理支撑平台；当分布式云数据中心要对外提供服务时，提供统一的服务呈现界面、统一的支撑流程，这需要分布式云数据中心提供统一的服务平台。

分布式云数据中心不再仅限于解决单个数据中心的效率和用户体验，而是将多个数据中心看成一个有机整体，围绕跨数据中心管理、资源调度和灾备设计，包括实现跨数据中心云资源迁移的云平台、多数据中心统一资源管理和调度的运营运维管理系统、大二层的超宽带网络和软件定义数据中心能力。分布式云数据中心将为客户带来前所未有的价值和全新的使用体验，其价值是：

降低TCO，提高ROI： 分布式云数据中心采用虚拟化技术，消除了软件对运行软件的硬件的依赖性，使IT主管可以将利用率不足的基础结构转变成富有弹性、自动化和安全的计算资源池，供应程序按需使用。华为分布式云数据中心通过资源整合和自动化帮助企业降低运营成本，通过分布式技术实现多个数据中心的资源的逻辑统一和高效利用，降低对基础架构的投资。 分布式云数据中心通过灾备服务和基于资源负载均衡的跨数据中心应用迁移来提升应用的可用性和资源利用率，可用性的提高和宕机时间的缩短使企业在无形成本方面节省了大量资金。虚拟机可以通过诸如虚拟机迁移之类的服务来提供更高的可用性。此外，虚拟机和虚拟磁盘的封装属性以及获取虚拟机状态的能力，还使虚拟机进行备份和恢复的速度得到提高。

提高业务敏捷性，加快上线速度，提高用户的满意度： 分布式云数据中心在虚拟化技术之上，提供了资源的按需服务能力，分布式云数据中心提供全方位的管理、业务自动化的能力。通过自助式服务，用户可以按需自助申请所需的计算、存储、网络的资源。提供业务的快速发放和部署、动态负载均衡的能力，能够基于模板快速进行应用的部署和创建。通过服务模版中的服务建模功能使得应用程序的所有者可以反复并快速地创建、配置，以及部署应用程序服务到云端。让应用服务的部署过程更形象，并可跨越私有和公共云进行重新配置。从而可以将用户业务上线的时间从天级缩短到分钟级。分布式云数据中心根据用户不同的应用需求提供不同的SLA水平的资源池服务。同时分布式云数据中心具有灵活的弹性伸缩能力，根据用户配置的灵活的调度策略，实现自动的水平（Scale-Out）、垂直（Scale-Up）弹性伸缩的能力，从而保证IT能够快速响应业务变化，使得数据中心从成本中心变为价值中心。

减少IT管理和维护资源，提高IT治理能力： 分布式云数据中心提供自助的服务能力，而用户可以根据需要自己申请业务，降低对IT运营部门的依赖。通过为事件管理、问题管理、变更管理，以及发布管理等标准化流程创建自动化的工作流，让IT的管理更加有效。 集中的运营与运维，主动式的管理，利用简化和标准化的工作流将业务要求与 IT 流程连接起来，帮助消除代价高昂的错误并降低对手动任务的依赖，从而使得多个多数据中心的运营与运维效率大大提升。

从能力来讲，分布式云数据中心要提供以下关键能力:

采用虚拟数据中心方式为租户提供数据中心即服务（DCaaS）

虚拟数据中心(VDC)为租户提供DCaaS服务，是软件定义数据中心(SDDC)的一种具体实现。VDC的资源可以来自于多个物理数据中心的不同资源池，资源类型分为虚拟化的计算、存储和网络资源以及Bare-metal物理机资源等。VDC的资源容量在创建时由VDC管理员申请或domain管理员指定，在申请审批后提供给VDC用户使用。

VDC用户使用VDC内的资源需要提交申请由VDC管理员审批。VDC管理员的管理范围包括服务审批、服务模板、服务管理、资源配置、资源发放、自助运维等。VDC管理员对VDC内提供的服务进行全生命周期的管理，可以定义服务并发布到服务目录供用户申请，可以审批用户申请，也可以取消发布的服务。VDC内的资源支持访问权限控制。VDC的网络可以由管理员自助定义，将VDC划分为多个VPC，VPC包括多个子网，并通过VFW、VRouter等部件进行安全、网络管理。VDC内支持IaaS层的多种计算、存储、网络和应用服务。其中VAPP服务支持对软件应用的灵活定义和弹性伸缩。

VDC服务提供部分自助运维能力，包括查看VDC告警、性能、容量、拓扑信息。VDC提供VDC级别的资源使用计量信息，方便租户计算计费信息。

针对多种应用场景优化的云基础设施

在不同的应用场景下，对云数据中心的基础设施需求会有差异。分布式云数据中心解决方案针对不同应用场景提供了不同的基础设施，以满足上层应用的差异化需求，提高基础设施效率和快速交付能力。目前主要针对四大场景：标准虚拟化场景，提供对普通应用虚拟化以及桌面云等虚拟化方案的基础设施；高吞吐场景，主要针对OLAP分析型应用的支持，在存储和网络方面提供了优化，支持InfiniBand等高性能网络连接；高扩展场景，对于需要快速水平扩展的应用，采用计算存储一体机方案提供快速扩展能力；高性能场景，主要对于OLTP应用，X86服务器替代小机等场景，在服务器提供了多种RAS技术增强可靠性，存储支持百万级IOPS，服务器微秒级稳定响应能力等。

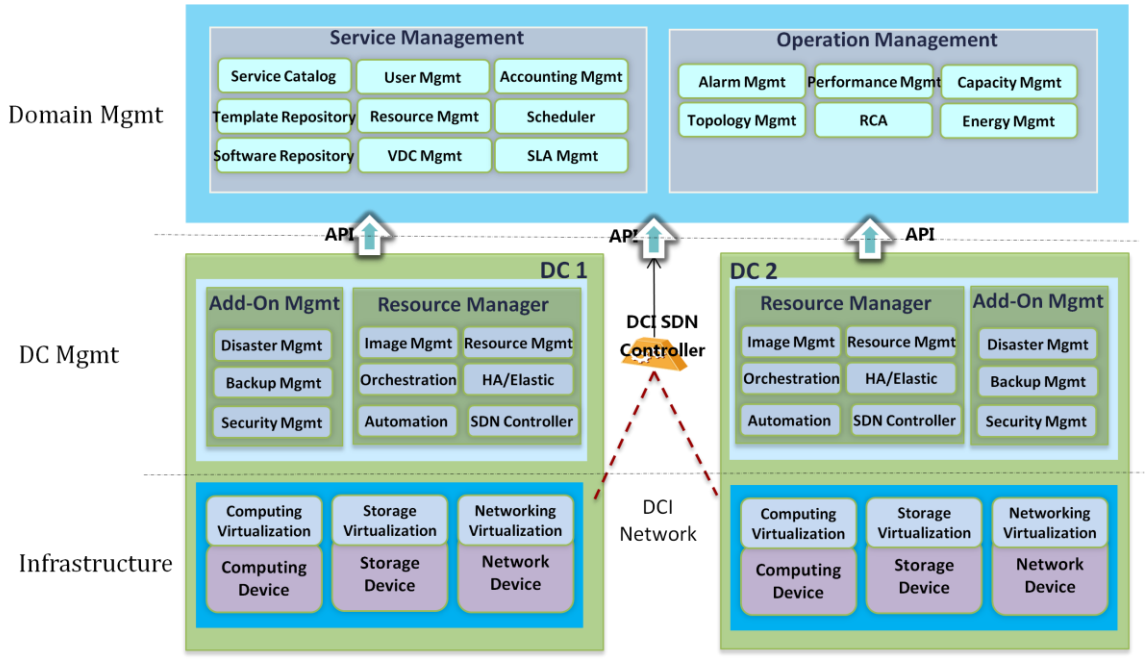
基于SDN网络虚拟化技术的网络自动化和多租户

云数据中心的网络构建基于SDN虚拟化网络技术，提供业务感知的自助网络管理能力。SDN技术提升了网络的自动化管理能力。SDN控制器可以对接物理、虚拟的网络设备，通过调用其接口进行统一管理，同时提供接口给管理系统调用。这种能力在多租户云数据中心场景下带来的直接价值就是每个租户可以自助定义自己的网络并自动化实施。利用SDN网络管理的能力，VDC管理员可以定义VDC的安全区，创建虚拟防火墙并配置ACL、NAT策略等，然后快速的实现这些策略。这种灵活度极大的提升了网络对业务的支持，使业务网络变得灵活。SDN管理的VxLAN技术也突破了传统VLAN的约束，给跨数据中心的虚拟机迁移等提供了可能。

统一灵活的云数据中心管理能力

分布式云数据中心的资源来自于多个物理数据中心，资源类型多样，管理需求复杂。针对这种情况，分布式云数据中心（DC^2）提出了统一管理,包括：多数据中心统一管理，支持对多个数据中心资源的资源统一的接入和管理；物理虚拟统一管理，物理服务器、存储、网络资源和上面虚拟化出来的资源提供一致性的管理，提供拓扑对应关系，在同一个管理界面上呈现；多种虚拟化平台统一管理，现有虚拟化技术多种多样，既有VMware的商业化产品，也包括XEN,KVM等开源平台，需要提供统一的能力。

2.2 分布式云数据中心总体架构



图表 1分布式云数据中心逻辑架构

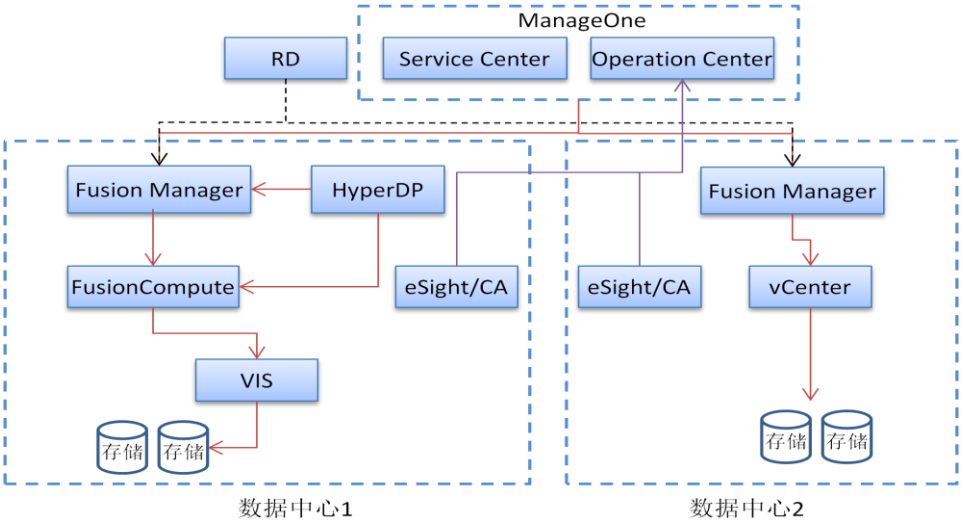
分布式云数据中心总体架构如上图所示，由基础设施层、虚拟化层和服务层组成。各层都分别向上层提供接口供上层调用或对接。

表3 分布式云数据中心各层介绍

功能分层	说明
基础设施层	基础设施层提供构建数据中心计算、存储和网络的资源池能力。分布式云数据中心提供针对多种场景的POD配置方案。基于物理资源构建了虚拟计算、虚拟存储、虚拟网络资源池。
数据中心管理层	数据中心管理层提供对虚拟计算、存储、网络的资源管理能力。分布式云数据中心1.1提供基于OpenStack和FusionSphere的云平台管理，支持镜像、服务管理、资源调度等方面能力，也提供SDN的网络虚拟化管理能力。
域管理层	提供对多个云数据中心的统一管理调度能力，提供以VDC为核心的DCaaS，VDC内提供多种云服务能力。该层也提供对虚拟物理资源的统一运维能力。

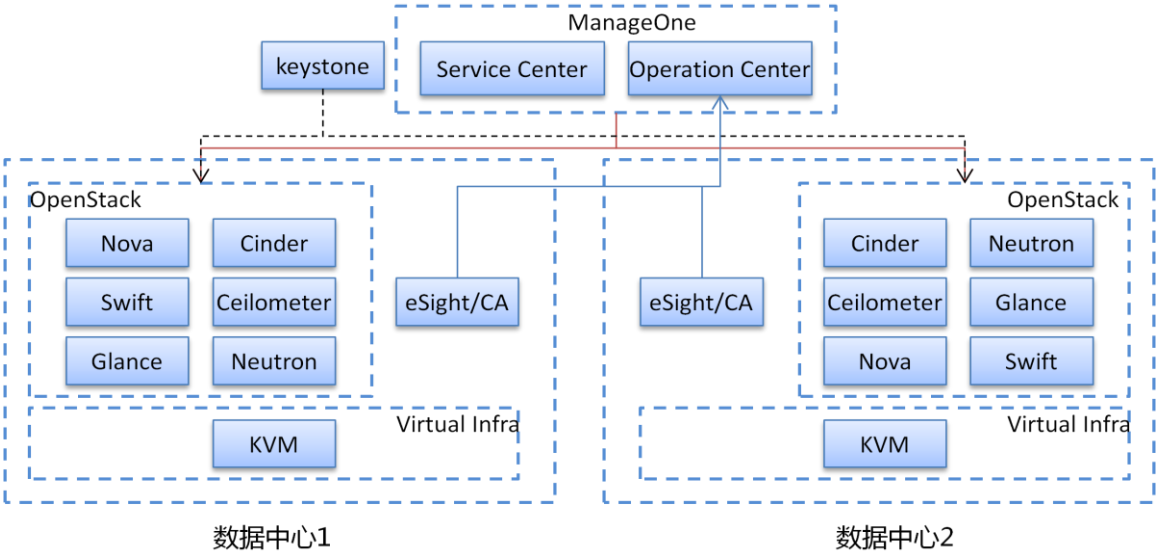
2.3 分布式云数据中心逻辑部署图

分布式云数据中心在OpenStack架构和Fusion Manager架构下部署方式和部件会有不同。下图是FusionManager架构下的各部件关系。



图表 2分布式云数据中心传统架构逻辑部署图

上图描述的是传统FusionSphere部署架构，云管理采用FusionManager，可管理VMware和华为UVP虚拟化平台。RD支持跨数据中心的容灾管理，同时对接异地数据中心的FusionManager。



图表 3OpenStack架构下部件部署图

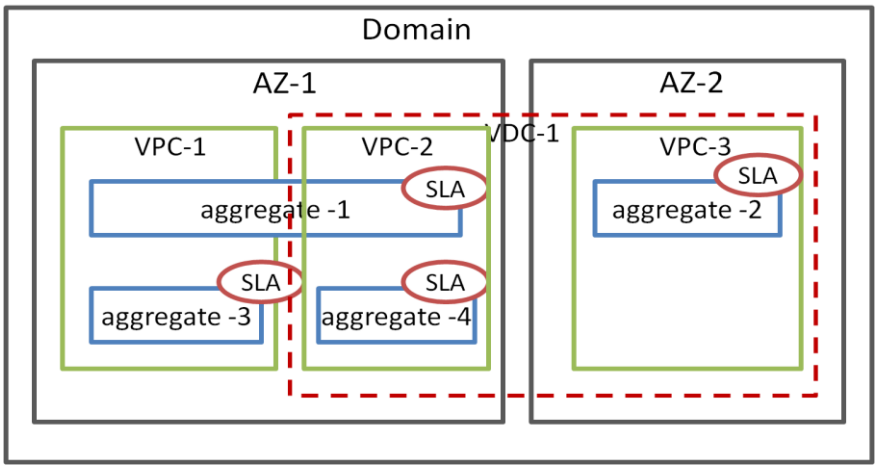
上图是在OpenStack架构下各部件的部署及连接关系，其中keystone部署在domain域，实现对多个OpenStack实例的统一认证管理。OpenStack平台原生提供了适配异构虚拟化平台能力，当前仅支持KVM平台，未来进行产品化后可支持多种虚拟化平台。

下表描述了分布式云数据中心的部件及功能：

部件	功能描述
ManageOne	提供分布式云数据中心服务中心（SC）和运维中心（OC）： SC:服务中心基于资源池提供的云和非云资源统一编排和自动化管理能力，包括可定制的异构和多资源池策略和编排，可定制的企业

	服务集成，可通过集成第三方系统补足资源池管理能力，特别是异构的传统资源自动化发放能力。 OC:运维中心面向数据中心业务，进行场景化运维操作和可视化的状态/风险/效率分析，基于分析能力提供主动和可预见的运维中心。
FusionManager	FusionManager的定位是集成多个虚拟化软件和物理设备，提供统一硬件资源管理和虚拟化资源管理。
FusionCompute	提供网络，存储，计算资源的虚拟化，从而实现资源的池化。
RD (Replication Director)	提供分布式云数据中心的虚拟机容灾能力，支持主机复制方式将主虚拟机数据映射到容灾虚拟机，支持容灾切换。
HyperDP	提供分布式云数据中心的虚拟机备份能力
VIS	提供存储虚拟化功能，配合系统提供双活容灾能力
OpenStack	OpenStack是开源云管理系统，由多个部件构成，采用REST接口和消息队列实现部件解耦，支持对异构虚拟化平台管理（KVM, VMware, XEN等）。主要部件包括： Nova:虚拟计算,Glance:镜像,cinder:虚拟磁盘,neutron:虚拟网络,swift: S3存储, keystone:认证,Ceilometer:监控等

2.4 分布式云数据中心数据关系图



图表 4服务式云数据中心概念关系

分布式云数据中心中逻辑概念的关系是：

- Domain：代表数据中心管理系统管理的总范围，对分布式云数据中心来说包括多个物理数据中心及包含的物理虚拟资源。
- Available Zone（AZ）：AZ是对用户可见的，用户在资源申请时首先需要选择AZ。在同一个AZ区域内，存储是可达的，因此虚拟机在同一个AZ内可以迁移。AZ在同一个汇聚/核心交换机下。

- VDC：虚拟数据中心，可以跨多个AZ，包括多个VPC。
- VPC：VPC是一个AZ内为保证网络安全而划分的区域，各VPC网络间采用多种网络隔离技术。一个VPC仅属于一个AZ。
- Host Aggregate：该概念来自OpenStack的定义，同一个Aggregate是具有相同属性的资源集群，属性通过元数据描述。资源分发时通过Scheduler部件来根据用户需求选择合适的Aggregate分配资源。一个Aggregate属于一个AZ。

3 分布式云数据中心解决方案关键特性

3.1 虚拟数据中心

3.1.1 适用场景

虚拟数据中心(VDC)主要适用于如下场景：

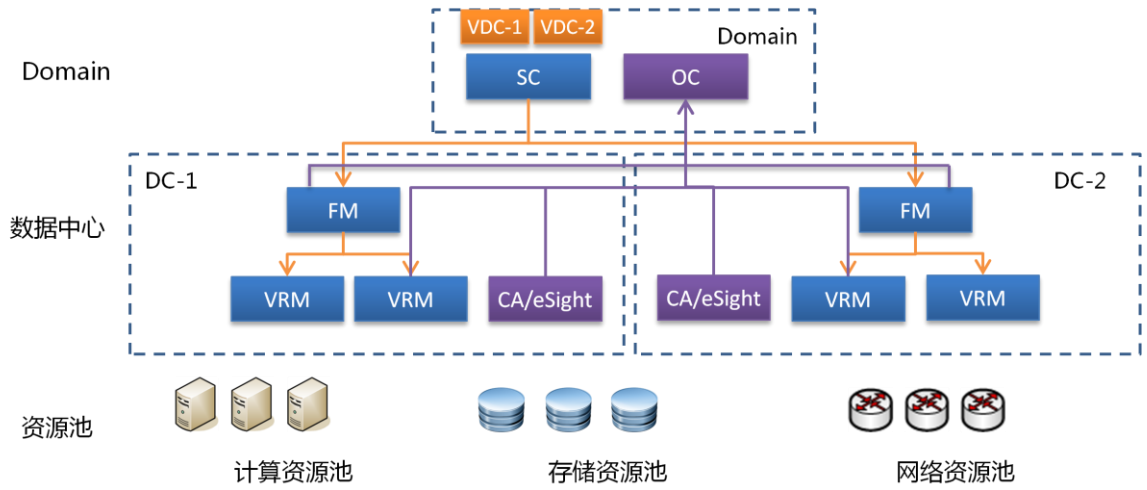
企业私有云中，有独立管理租用资源并实现网络隔离需求的场景。每个VDC是一个具有自运营和自运维能力的独立管理实体。在企业中，VDC的划分方式可以灵活多样，可以按照场景要求灵活划分。

a) 可以按部门划分，每个部门可以独立管理本部门资源。

b) 可以按使用领域划分，例如：开发VDC，测试VDC等。

注：VDC可以支持一个或多个物理数据中心的资源。VDC对客户的价值点在于租户的自助运营、运维能力和资源隔离管理。

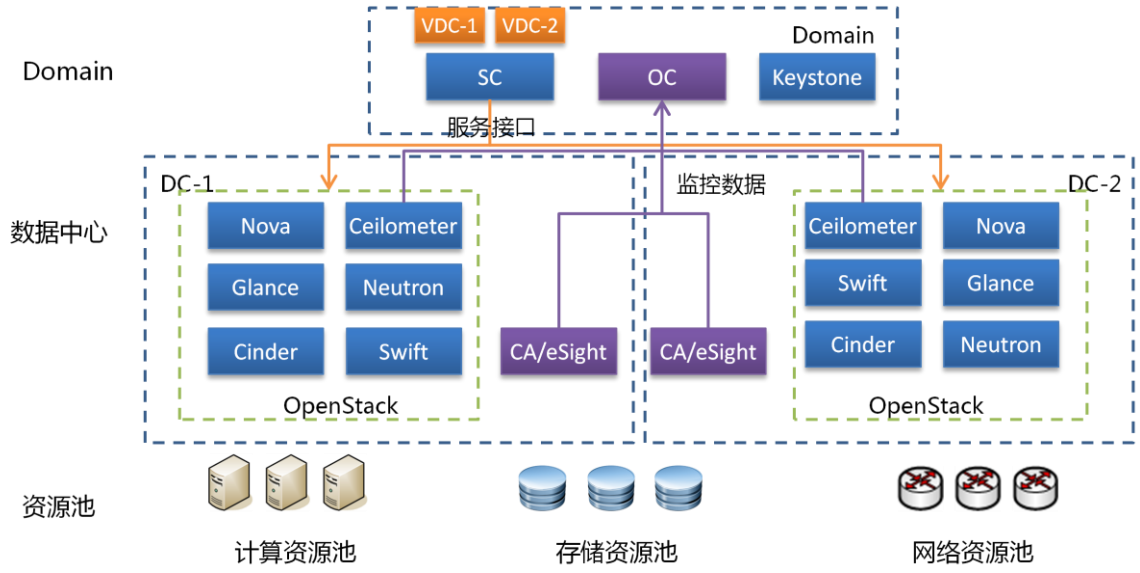
3.1.2 部署架构



图表 5FM + SC方式部署

在SC加FM的部署方式中， FM提供云管理能力和虚拟化平台的访问接口；SC提供VDC服务和VDC内包含服务的管理能力。

- 在服务管理方面， SC是VDC的服务提供方。VDC管理员和用户可以登录SC门户，VDC管理员可以自助管理VDC内的服务、网络和自助运维等。
- 在运维层面，VDC相关的信息可以从eSight或合作厂商的部件获取性能、告警信息，然后统一在OC上呈现。运维管理员可以在OC上对运维信息进行统一处理。



图表 6SC + OpenStack方式部署

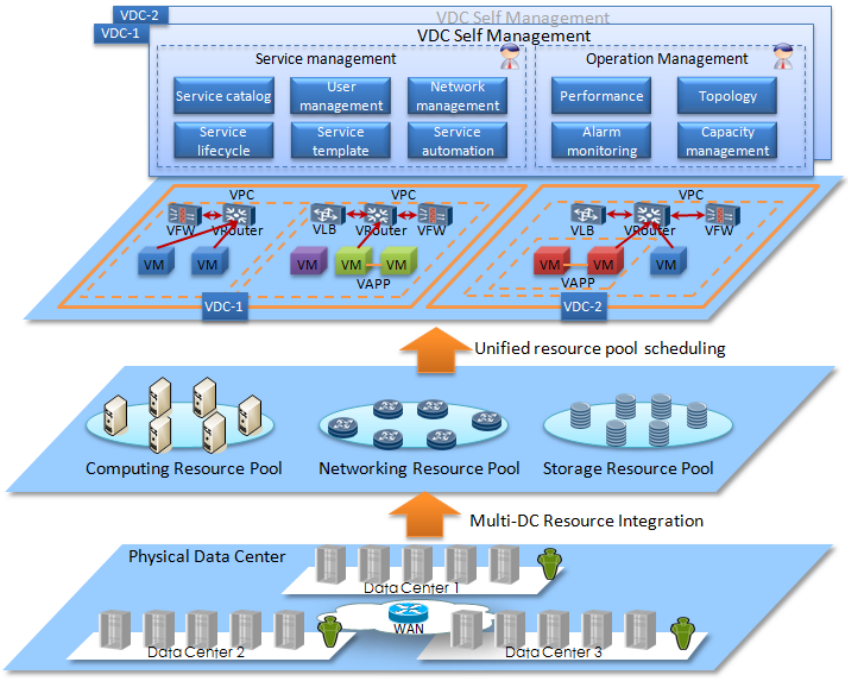
SC加OpenStack部署方式采用OpenStack提供的服务作为基础云管理平台，SC提供VDC服务。SC和OpenStack利用OpenStack提供的REST API对接起来。

3.1.3 VDC 角色

VDC相关的角色描述见下表：

角色	职责	层次	部件
Domain Admin	负责 DC^2 总体的资源管理和运维管理，例如：可以查看 VDC 资源、告警、性能数据，VDC 物理和虚拟拓扑等	Domain	OC
Domain Service Manager	负责 DC^2 总体的业务运营管理，例如：VDC 的创建、全局服务管理等	Domain	SC
VDC Service Manager	VDC 的管理员，能够对 VDC 内的资源和用户进行管理，管理 VDC 内的服务，可以查看 VDC 的运维统计信息	VDC	SC
Service User	VDC 最终用户	APP/Host	SC

3.1.4 关键特性



图表 7VDC功能概述

1. 多数据中心资源统一管理

VDC可以从多个物理数据中心的资源池中获取资源。数据中心采用Available Zone（AZ）方式提供资源池，选择不同的AZ也就选择了不同数据中心的资源池。在VDC创建时，管理员会根据需求从AZ列表中选择需要的AZ，后续VDC用户申请资源时将根据用户需求从这些AZ中获取资源。

每个AZ内部划分为不同的Host Aggregate，不同Aggregate具备不同的SLA特性。例如：有的Aggregate的服务器包含SSD盘,可以定义为高性能Aggregate。Aggregate完全由管理员根据SLA特性自主划分。Aggregate对用户是不可见的，但当用户申请资源时可提出SLA需求，系统调度器将根据SLA需求在满足要求的Aggregate中选择资源。

2. VDC间的隔离

VDC之间提供管理、网络和资源隔离能力。

- 管理隔离：VDC有管理员和用户等角色。用户登录VDC后，可以申请VDC提供的服务，由VDC管理员审批后使用。每个VDC内部有独立的用户管理、服务管理、模板管理、服务目录、容量管理、运维管理和审批流程等管理能力。不同VDC之间的这些管理能力是互相独立的。每个VDC的管理员负责本VDC的管理职责，互不干扰，从而保证VDC管理上的隔离。
- 网络隔离：VDC内部的网络拓扑可以自主定义，包含多个安全区。每个安全区采用VLAN / VxLAN等方式互相隔离。虚拟资源（如虚拟机等）包含在这些安全区内。安全外部用户访问安全区内的资源需要经过VFW。VFW上设置的ACL,ASPF,NAT等规则可以保证访问的安全控制。不同安全区之间互通通过IPSec VPN，保证网络数据的安全性。
- 资源隔离：每个VDC都独立管理自己的资源（例如：VM,VFW属于某VDC），不存在VDC

共享资源情况。针对某资源的查看及操作（例如：开机、关机、扩容），仅能由资源拥有用户在VDC内完成。其他VDC是无法查看和操作该资源的。资源包括虚拟化资源（比如虚拟机，虚拟磁盘），服务模板，软件库等被管理的资源。

3. 配额管理

VDC支持对使用的资源进行配额控制。配额的数量可以在创建VDC时由申请者指定，然后domain管理员审批通过，也可以由domain管理员创建VDC时直接指定。配额种类包括：VCPU个数，内存大小，VLAN个数，VPC个数，子网个数，VM个数，网络带宽等。对于超过VDC配额后的资源申请，VDC将自动拒绝。VDC可以显示当前配额使用的数量，方便管理员控制容量。

4. 用户管理

每个VDC支持独立的用户管理能力。VDC管理员可以授权某用户访问VDC的权限。在获得授权后，用户可以登录该VDC并申请该VDC的服务。一个用户可以获得多个VDC的授权，从而成为多个VDC的用户。

5. 服务管理

VDC管理员可以对服务目录和服务生命周期进行管理。VDC管理员可以定义服务目录，服务目录包含当前已经发布并可以订购的服务列表。VDC管理员首先需要定义服务，包括服务名称、描述和规格属性等，然后可以发布到服务目录中。然后，VDC用户就可以浏览服务目录并订购其中的服务。对于不再提供的服务，管理员也可以对服务取消发布。取消发布的服务不再呈现在服务目录中，用户也就无法订购了。

6. 模板管理

VDC内支持多种服务模板，服务模板可以帮助快速定义新服务。服务模板中可以定义服务的配置规格项和缺省值等。VDC支持的服务模板包括：VM模板，VAPP模板。这些模板可以帮助管理员实现服务快速创建部署。支持全局模板和局部模板，全局模板所有VDC可见，局部模板仅本VDC可见。

7. 服务自动化

服务自动化为系统提供服务自动化发放上线能力。当用户在服务目录上申请服务并审批完成后，服务自动化引擎将根据订购的服务来调用相应的服务实施流程。服务流程的实施由内置的BPM执行引擎执行，执行引擎自动调用虚拟化系统REST接口并保证执行的顺序和结果。系统内置了缺省支持的服务流程，包括虚拟机、虚拟磁盘、虚拟网络设备等。管理员可以自定义新的服务发放流程来满足新业务需求。

8. 自助网络管理

VDC的自助网络管理利用了底层SDN提供的基础能力，主要包括的功能有：

- VPC：在VDC内部可以定义VPC，每个VPC内部包括多个子网，VPC内可以定义一个VRouter，作为进入VPC的入口点。此外根据网络拓扑要求还可以定义VFW和VLB等虚拟网络部件。在VFW上通过安全策略控制可以控制对VPC内资源的访问。
- 子网：安全区内部可以划分为多个子网，每个子网通过VLAN机制实现子网间的二层网络隔离。对于子网内的IP地址提供管理能力。
- VDC虚拟网络拓扑：可以查看VDC的网络拓扑，网络拓扑展示了VDC内部的安全区及连接管理，每个安全区内部包括的网络资源和子网信息，以及每个子网内部的VAPP和VM资源

情况。虚拟网络拓扑可以展示虚拟资源和物理资源的映射管理，例如VFW和FW间的关联关系等。

9. 自助运维管理

- 容量管理

VDC管理员可以查看VDC当前的资源使用情况和容量占用率，占用指标包括：CPU，内存，磁盘，带宽等。VDC管理员可以设置容量阈值告警，当系统资源使用率超过阈值时，系统将发出告警信息。

- 拓扑管理

VDC管理员可以查看VDC的虚拟网络拓扑，包括VDC内包括的VPC,VPC连接关系，VPC子网，VPC内虚拟机，VPC内包括的虚拟网络设施VFW, VLB, VRouter的连接关系等。当用户修改虚拟网络拓扑后，比如增加了VFW或增加了子网，能够自动看到网络拓扑的改变。VDC管理员可以在SC上查看到VDC的虚拟拓扑，物理和虚拟拓扑的对应关系在OC上查看。

- 性能管理

VDC管理员能够查看到VDC的性能列表，包括topN的CPU,内存,磁盘IO等性能指标的性能列表。管理员可以设置阈值报警，当性能指标不能达到性能阈值时，系统将自动产生性能告警通知管理员。

- 告警管理

VDC管理员在OC可以查看VDC的告警列表，然后对告警信息进行相应的处理，包括屏蔽告警、转工单、告警降级等多种方式，帮助VDC管理员处理系统的告警。

10. 支持服务列表

用户登录VDC自助服务门户，可以在服务目录中看到多种预置的云服务，服务包括：

- 云主机服务

虚拟云主机服务提供云托管业务，让用户能够象使用本地物理机一样使用虚拟机云主机。用户登录服务门户来申请云主机服务，选择相应的虚拟机模板，并指定规格（存储大小，内存大小等）并提交申请，申请批准后，用户就可以用虚拟机IP登录这台云主机。用户可以对云主机开机、关机、休眠、唤醒、扩容、减容等操作。

- 物理服务器服务

用户可以线上申请物理服务器服务。用户在申请时可查看服务器的可选规格，操作系统类型来申请物理服务器服务。该申请审批成功后，实施服务器服务需要线下操作。然后用户根据分配给物理服务器的IP地址登录到物理服务器，进行相关的业务操作。

- EBS服务

Elastic Block Store (EBS，弹性块存储) 可以为虚拟机动态提供块级存储服务。弹性块存储为虚拟机提供可按需扩展存储空间的块级别存储服务，虚拟机以卷设备的方式访问块存储空间。EBS服务支持对块存储扩容、减容操作。

- VFW服务

虚拟防火墙（VFW）用于保护用户在数据中心的资源，不同用户的虚拟防火墙之间有独立的策略配置、独立的吞吐量限制、独立的会话数限制、独立的带宽保障，能够保证不同用户之间的业务互不影响。

1) 弹性IP

弹性公网IP也称为弹性IP业务，是指给用户申请的虚拟机或物理服务器配置私网IP与公网IP的一对一地址映射，使用户通过公网地址访问数据中心内部的虚拟机或物理服务器。

用户在使用弹性IP业务时，在自助服务系统上需要先申请一个弹性IP，选择该弹性IP的带宽大小。在提交业务请求后，系统会从公网地址池中选择一个公网IP地址分配给用户。用户将弹性IP和合法的私网IP（这里可以是虚拟机IP地址，也可以是物理服务器IP地址）进行绑定。系统在VFW上通过NAT配置实现业务自动化发放。

2) SNAT/DNAT

SNAT功能称为源地址转换，提供租户的多台虚拟机从数据中心内部主动发起访问到外网，对用户虚拟机的私网IP做多对一的源地址转换。使多台虚拟机可以同时通过一个公网地址访问外网。用户在使用SNAT功能时，可直接对申请的私网网段开启或者关闭SNAT功能。

DNAT功能称为目的地址转换，提供租户从外网访问虚拟机，使用一个公网地址通过端口区分数据中心租户的多台虚拟机或者物理服务器做一对多的地址映射。用户在使用DNAT功能时，需要选择一个已经申请的公网IP地址（这个公网IP地址不能是已经被用于弹性IP业务的），然后输入公网IP地址的端口、私网IP地址以及端口；提交业务请求之后系统会记录该条NAT策略，同时在底层设备上实现NAT配置完成业务发放

3) ASPF

ASPF功能是针对应用层的包过滤，即基于状态的报文过滤，以便于实施内部网络的安全策略。ASPF能够检测试图通过Eudemon的应用层协议会话信息，阻止不符合规则的数据报文穿过。并提供对有害Java Applets、有害ActiveX的阻断。用户可以自定义选择针对某些协议开启ASPF功能。用户在使用ASPF功能时，需要先选择申请的虚拟防火墙，然后选择需要检查的协议类型进行开启或者关闭。

4) ACL

ACL（Access Control List）是针对用户的业务做访问权限的控制，用于控制用户南北向流量的业务访问，解决方案中的ACL功能是基于虚拟防火墙提供的，根据用户的虚拟机或者物理服务器的IP地址来配置有限的ACL规则。用户在使用ACL功能时，这些规则受到以下条件的约束：

- ✓ 如果是IN方向的ACL规则，那么目标地址必须是用户申请的虚拟机的地址段，如果设定为其他地址段，则系统会报错，返回不允许配置的信息。
- ✓ 如果是OUT方向的ACL规则，那么源地址必须是用户申请的虚拟机的地址段，如果设定为其他地址段，则系统将报错，返回不允许配置的信息。

5) IPSec VPN

IPSec VPN即指采用IPSec协议来实现远程接入的一种VPN技术，用以提供公用和专用网络的端对端加密和验证服务。

用户可以申请多个IPSec VPN业务，用于用户租用的数据中心资源与用户企业侧不同数据中心

的资源在公网上实现加密传输，同时提供私网地址访问能力。用户在使用IPSec VPN业务时，需要申请一个公网IP地址用户IPSec VPN对接，然后在配置IPSec VPN页面中自定义IKE策略以及IPSec策略，提交业务请求之后系统会自动化下发配置，同时用户还需要在企业侧的IPSec VPN设备进行策略配置，需要与数据中心侧的IPSec VPN策略匹配才能建立成功。

- VLB服务

弹性负载均衡(VLB)属于增值业务，主要向用户提供负载均衡服务。用户可以申请负载均衡器，将业务主机关联到负载均衡器中。负载均衡器可以根据用户设定的负载均衡策略，将业务请求均匀分发到相互关联的主机上，使得每个业务主机的负载保持均衡，保证业务运行的稳定性和可靠性。

负载均衡器能够检查服务池中云服务器的健康状态，自动隔离异常状态的云服务器，从而解决单台服务器在处理性能、扩展性、稳定性方面的问题，同时负载均衡器还能起到增强服务器池抗攻击的能力。用户需要先申请VLB服务，选择VLB的最大吞吐量、最大会话数、最大的负载服务数量，提交请求之后开通VLB服务。服务开通之后，用户可以根据业务需求自定义配置负载均衡策略。

- VAPP服务

VAPP服务包括如下子特性：

✧ VAPP快速部署

对于一些常用的应用系统、中间件，（如LAMP、WebSphere、Hadoop等），可以将其制作成应用模板，从而方便业务用户快速的创建、部署应用。分布式云数据中心提供了便捷的应用模板制作功能和应用快速部署服务,管理员或应用开发者通过自助门户，根据应用需求，制作虚拟机模板、上传应用软件包，通过基于图形化拖拽方式设计应用模板，最后发布应用模板。

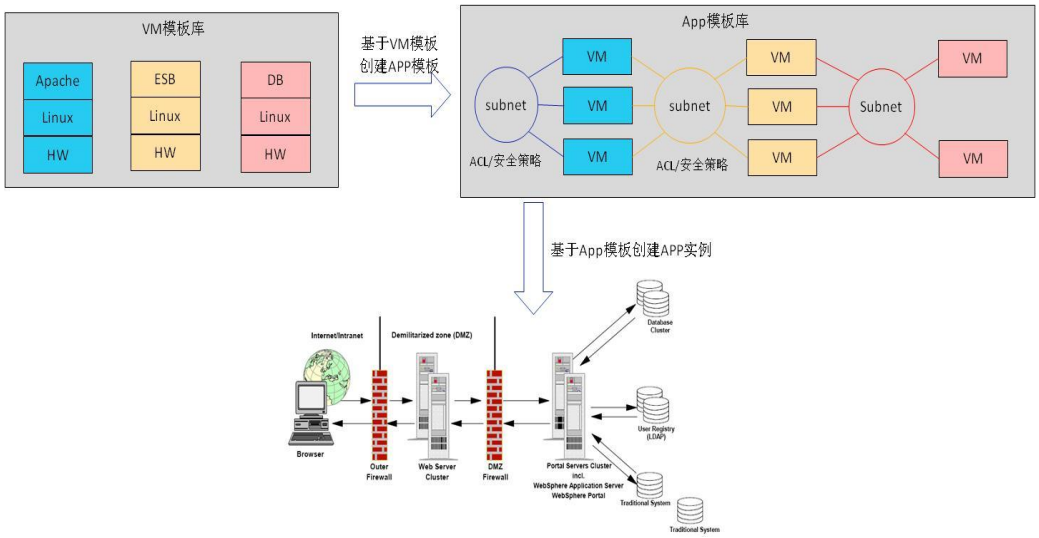
分布式云数据中心通过虚拟机模板、应用模板，以及用户自定义编排等能力，提供用户应用快速、自动化部署的能力。

用户可以自行创建自己的虚拟机模板，并通过系统提供的图形化编排工具，通过拖拽、画图等可视化手段，自行创建应用模板，模板可以包括计算、存储、网络及弹性策略等关键因素，从而用户可以方便的根据模板自动化、快速的进行应用的部署。

用户可以通过已发布的模板进行应用的自动部署，用户通过图形化拖拽的方式，按照简单的系统提示可以非常方便的部署自己的应用。系统接受到用户应用部署请求后，会根据应用模板中各个资源的定义，自动的创建虚拟机，自动的给虚拟机/物理机上安装应用软件，自动的建立应用软件间的依赖关系和网络，采用基于VXLAN的SDN技术，灵活的定义网络，从而快速建立应用的之间的拓扑，灵活定义网络，并且实现不同租户之间的隔离。

同时用户可以指定自己的应用弹性伸缩策略，系统可根据用户自定义的监控条件，自动触发弹性伸缩组的扩容、减容。管理弹性伸缩组内部的资源调整，保证应用的健康运行。

注：OpenStack场景不支持采用软件包方式部署应用，仅支持采用镜像方式部署应用。



图表 8基于模板的业务快速部署

在应用模板发布后，业务用户可以在服务目录中选择相应模板，填写应用基本信息，配置应用网络及应用参数，通过向导式应用创建流程创建应用。分布式云数据中的管理系统根据用户的设置，自动化的分配云资源、安装应用软件、配置网络，从而快速的为业务用于生成一个可用的应用环境。

业务用户也可以不使用模板，直接基于图形化界面，直观的拖放画布快速创建完整的部署蓝本（可视部署拓扑），并可轻松部署到混合云环境中，并提供完整的应用生命周期管理，用于简化包括治理、开发和维护在内的应用部署流程，该服务基于强大的流程编排引擎，实现应用拓扑的建模，应资源的分发，软件的安装，网络配置，实现完全的服务自动化。

✧ VAPP弹性伸缩

对于每小时、每天或每周使用率都不同的应用系统，分布式云数据中心提供了应用弹性伸缩服务，可以根据用户预先设定的策略自动调整应用占用的资源，可以确保占用的资源数量与业务需求保持同步，以最大程度降低成本。

用户可以在应用中创建弹性伸缩组，并针对弹性伸缩组设置弹性伸缩策略。弹性伸缩组是一组适用于相同伸缩策略的虚拟机的集合。系统会根据自定义的弹性伸缩策略，通过对虚拟机的CPU、内存占用率等指标监控，实现弹性伸缩组的伸缩控制。伸就是对虚拟机进行创建，启动，唤醒等操作，缩就是对虚拟机进行删除，关机，休眠等操作。其实际目的就是通过对虚拟机的资源的控制，达到对伸缩组所使用资源的控制，进而到达对应用所占资源的控制。

用户不仅可以对单个应用设置弹性伸缩策略，也可对多个应用设置应用间资源共享策略。

组间策略是指不同应用弹性伸缩组间的组间资源共享策略。管理一个资源池内，各个弹性伸缩组之间的的资源分配及抢占。保证整个资源池的健康运行。对于无伸缩组、不参与抢占的应用，不在管理范围之内，不会对业务做任何操作。组间资源共享策略可以和弹性伸缩组的自动伸缩策略合并使用，满足多应用间的资源的弹性设置需求。用户通过设置组间共享策略，设置此组间共享策略所在资源池的资源预留值，同时需要设置对不同应用的弹性伸缩组的资源使用，当系统检测到资源池的资源少于资源预留值的时候，就会从优先级低的应用的伸缩组开始回收资源，以保证高优先级的应用申请资源的时候，资源池内有足够的资源进行分配。

组间策略的另外一种使用方式，是结合计划任务使用。应用在不同的时间点重要性和资源的需求上限是不同的。用户可以通过定义计划任务，调整伸缩组在不同时间段的资源使用上限、优先级，达到资源分时复用的目的。

3.2 SDN 网络

3.2.1 适用场景

SDN（Software Define Network）是一种新的网络框架，其本质是网络的可编程，SDN框架给用户提供最大的控制网络灵活度；随着移动互联、大数据等技术的发展，越来越多的IT业务迁移到数据中心，而在云数据中心Naas(Network As a Service)已经成为一种基本的IT服务，租户可以灵活的申请所需的虚拟网络资源来满足自己的IT业务。在云数据中心，SDN框架的网络可以使用于如下场景：

- 网络自动化

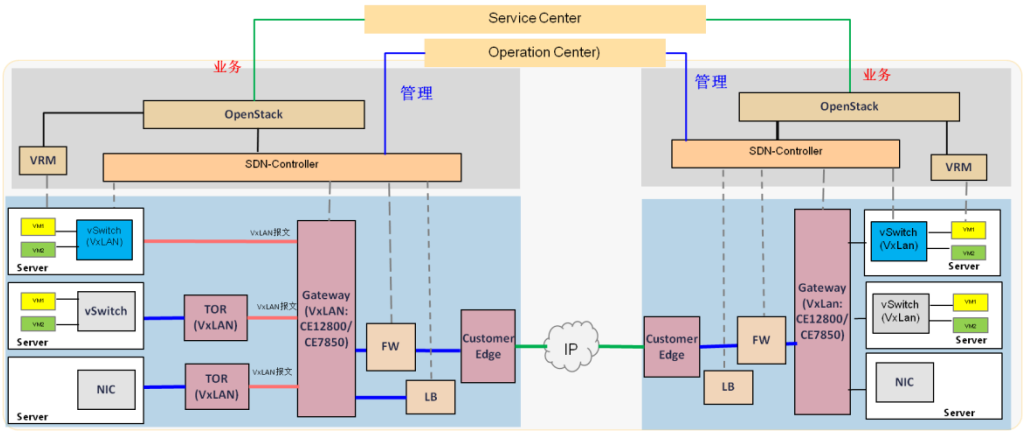
通过提供北向API，由上层管理软件通过调用API接口，实现网络自动化，提供即时的网络服务。为业务快速上线部署提供网络环境。

- 灵活的业务网络

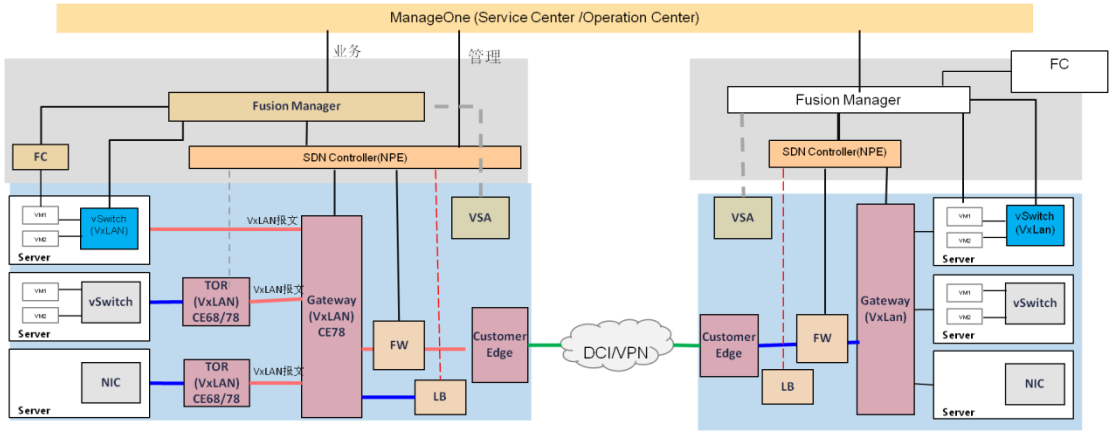
基于SDN网络架构，将物理网络虚拟化，提供不同的业务网络，实现业务网络的灵活部署。并提供多租户隔离，用户可自定义网络策略实现保护数据中心内部的资源安全访问。

3.2.2 部署架构

分布式云数据中心网络子系统采用SDN框架的网络设计，框架图如下：

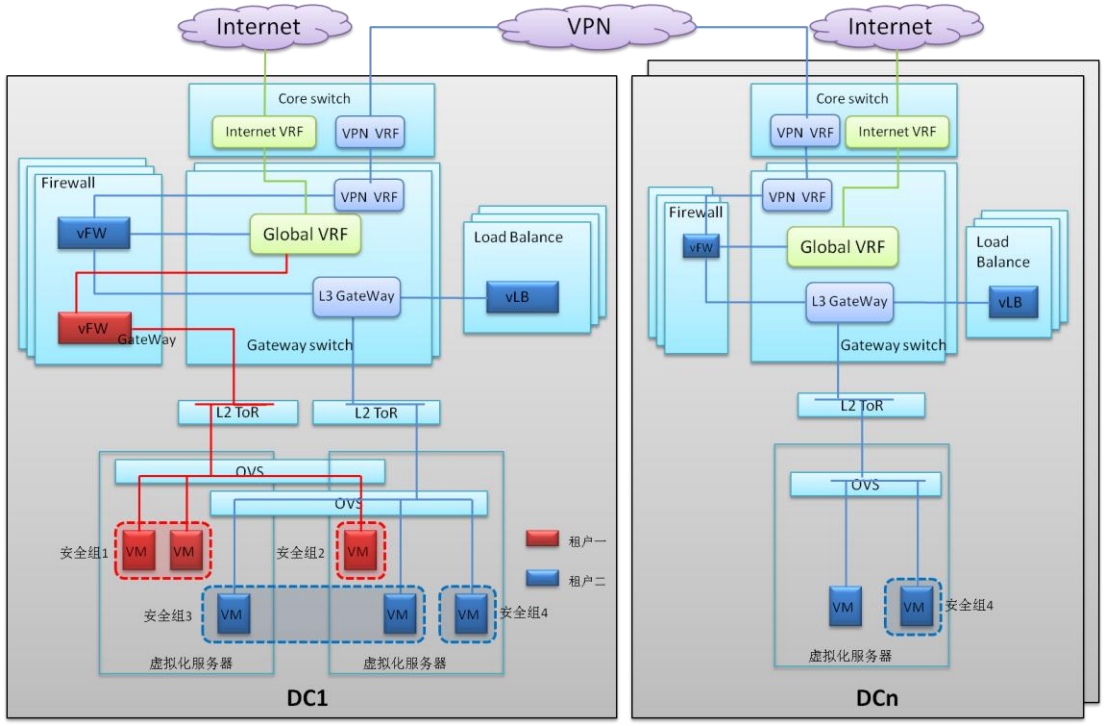


图表 9 DC2 SDN网络框架图(openstack)



图表 10DC2 SDN网络框架图(FM)

通过上述的SDN框架实现将网络虚拟化，自动为每个租户提供所需虚拟网络环境，如下图所示：



图表 11DC2网络子系统架构图

从上图可以看出，核心交换机上配置VPN VRF和Internet VRF，VPN VRF与汇聚交换机上的VPN VRF对接，internet VRF与汇聚交换机的Global VRF对接，用户将租户之间的网络逻辑隔离。

汇聚交换机上配置一个Global VRF，每个租户的虚拟防火墙都对接到Global VRF中实现对公网访问。

汇聚交换机上配置多个VRF，用于为每个租户提供虚拟路由器，提供租户的业务网关路由功能，在VRF下配置三层网关用于提供业务网关，每个VRF将与租户的虚拟防火墙对接；实现对租户业务的

保护。租户如果租用了虚拟负载均衡将对接到虚拟路由器上，提供服务器的负载均衡功能，同时受虚拟防火墙的规则保护。

虚拟交换机逻辑上接入到TOR交换机端口，每个租户有自己独立的虚拟交换机。虚拟交换机上有不同的端口组，不同的端口组有不同的网络属性。虚拟机网卡可任意加入不同端口组，用户不同租户之间的隔离。

同时租户可以创建多个安全组，一台虚拟机（通过不同的虚网口）可以划到不同的安全组内，不同的安全组有不同的安全访问策略保证租户内的虚拟机隔离。

3.2.3 特性设计

- 多租户网络设计

数据中心支持多租户管理，能够在以较低成本合理利用资源，优化资源利用率。数据中心必须具备不同租户资源的隔离设计，确保端到端的隔离以及满足租户的安全要求。

为了支持多租户，分布式云计算数据中心采用虚拟化技术，在逻辑上划分成多个（每个租户）虚拟网络环境，每个虚拟网络拥有独立的路由表、地址空间、安全服务、配置管理。这些依赖于设备虚拟化，包括以下方面：

- DC内网络设计
  - 三层网络设计

在核心层或者汇聚层使用VRF技术提供网络层（L3）之间隔离设计，保证每个租户有独立的路由转发表，不同VRF之间的数据流交互默认情况下将被不允许，能够支持不同租户的地址重叠场景。每个VRF中可以绑定多个三层网关，承载多个子网，为虚拟机或者物理服务器提供网关功能。同一个VRF下的不同网关之间默认可以互相访问。

  - 二层网络设计

支持VLAN ID或者VXLAN两种不同二层的隔离域，一个租户内不同的二层网络之间转发需要通过网关设备才可以进行互通，不同的租户默认是无法互通的。

  - 网络服务设计

将防火墙和负载均衡虚拟化，为每个租户提供虚拟防火墙、虚拟负载均衡功能。

    - 虚拟防火墙

将一个物理防火墙逻辑的虚拟出多个防火墙或者在虚拟机上跑的软件虚拟防火墙，每个虚拟防火墙有独立的路由转发表、安全服务策略、配置管理。租户在修改所属虚拟防火墙的配置时不影响其他虚拟防火墙的运行。同时对虚拟防火墙做吞吐量和会话数限制，确保虚拟防火墙的资源利用不占有其他虚拟防火墙资源。

    - 虚拟负载均衡

将一个物理负载均衡逻辑的虚拟出多个负载均衡或者在虚拟机上跑的软件虚拟负载均衡，每个虚拟负载均衡有独立的路由转发表、负载均衡策略、配置管理。租户在修改所属虚拟负载均衡的配置时不影响其他虚拟负载均衡的运行。同时对虚拟负载均衡做吞吐量和会话数限制，确保虚拟负载均衡的资源利用不占有其他虚拟负载均衡资源。

- DC间网络设计
  - Internet

    数据中心之间互联支持internet互联，所有租户之间的业务访问通过公网IP访问,可以支持跨数据中心的资源调度，由于Internet网络质量相对较差，根据物理距离原因延迟会大一些。

  - VPN 或者专线

    数据中心之间，特别是不同企业的异地数据中心可以通过租用运营商的VPN或者专线资源实现物理DC之间的互通， VPN或者专线链路质量相对稳定，是优先推荐的互联方式。

3.2.4 关键特性

- 多租户隔离

保证每个租户之间的网络资源互相隔离，拥有独立的网络控制平面、独立的数据转发平面以及独立的策略配置管理；不同租户之间的资源运行互不影响。

- 网络即服务

网络资源做为一种基础服务提供给最终用户，如subnet、虚拟防火墙、虚拟负载均衡、VPN服务。

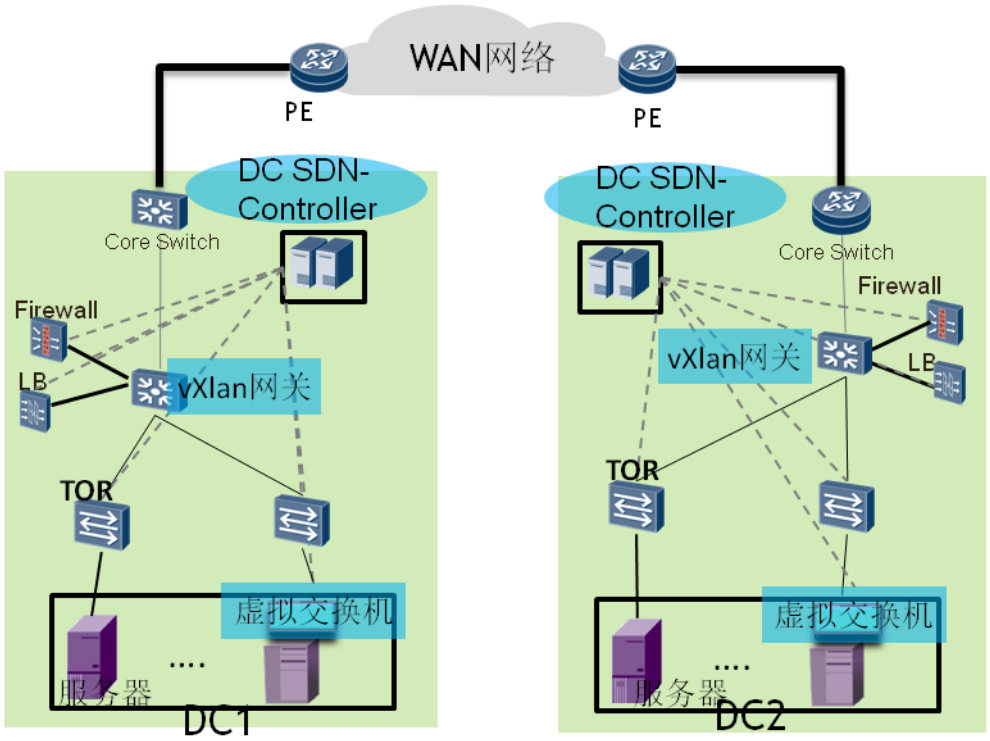
- 网络自动化

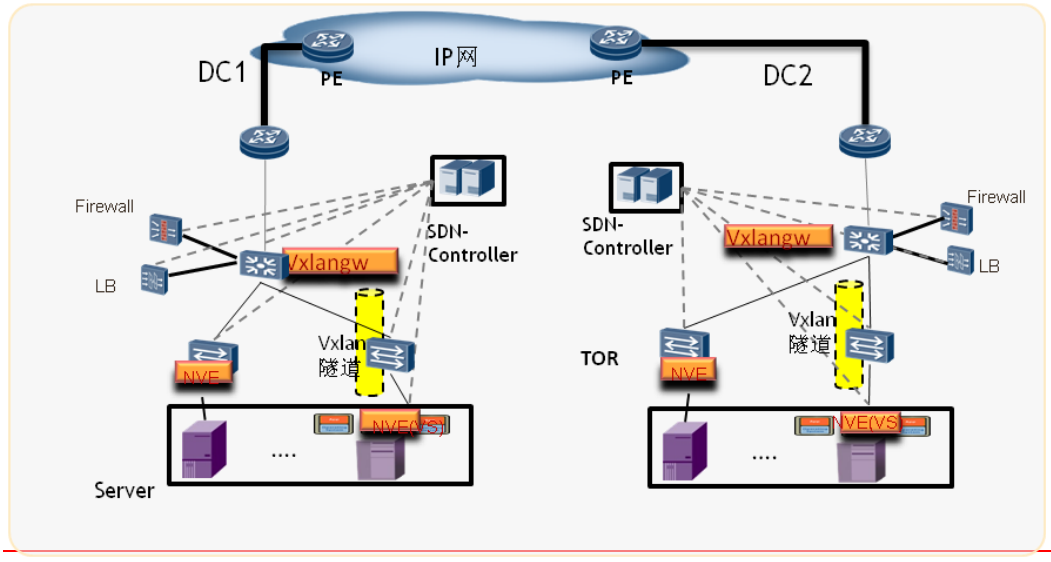
基于网络设备功能的抽象，设计可编排的最小单元作为网络服务单元（网络对象），通过业务需求的编排组合出不同的网络模型。为业务快速部署提供基础的网络环境。减少管理员的配置操作，网络配置更简单。

- VXLAN的虚拟网络

VXLAN技术是一种大二层的虚拟网络技术，主要的技术原理就是引入一个UDP格式的外层隧道，作为数据的链路层，而原有数据报文内容作为隧道净荷来传输。由于外层采用了UDP作为传输手段，就可以让净荷数据轻而易举的在二三层网络中传送。

VXLAN解决在部署了VM、多租户环境下数据中心网络的二层和三层需求。VXLAN运行在现有网络架构上，提供了一种方法“延展”二层网络。简言之，VXLAN是一种基于L3网络的L2叠加机制。位于相同VXLAN网段的VM之间彼此可以通信。每个VXLAN网段通过一个24bit上午网段ID标识，称为VNI(VXLAN Network Identifier)。这就允许多达16M的VXLAN网段可以在相同的管理域内共存。通过了SDN控制器的部署实现了VXLAN的技术部署，如下：





图表 12 SDN控制器实现VXLAN的部署框图

3.2.5 SDN 控制器设备配套

运营商控制器配套关系:

NetMatrix 控制器和网络设备配套关系	设备形态	版本
网络协同	NetMatrix	V100R001C20
网络控制器	SNC	V100R001C30
VXLAN GW /出口路由器	NE40E-X8/X16	V800R006C30
		V800R007C00
VXLAN GW/NVE	CE128/CE78	V100R003C10
	CE128/CE78/CE6850HI	V100R005C00
交换机（非VXLAN）	CE128/CE6850EI/CE58	V100R003C00
		V100R002C00
FW	E8000E-X	V200R001C01
		V300R001
	E1000E-X	V300R001C10
	E1000E-N	V100R001
LB（集成F5）	F5-BIG-LB-8900	BIG-IP 10.2

企业网配套关系(目前仅用于测试)

AC/CC控制器和网络设备配套关系	设备形态	对接版本
	AC/CC(仅用于测试)	
汇聚交换机	CE12800 系列	V1R3C10
接入交换机	CE5800 系列	V1R3C10
	CE6800 系列	V1R3C10
	CE7800 系列	V1R3C10
防火墙	USG 9500 系列	V3R1C01
负载均衡 :LTM系列		BIG-IP 10.2

3.3 统一管理

3.3.1 适用场景

统一管理主要针对的场景描述如下：

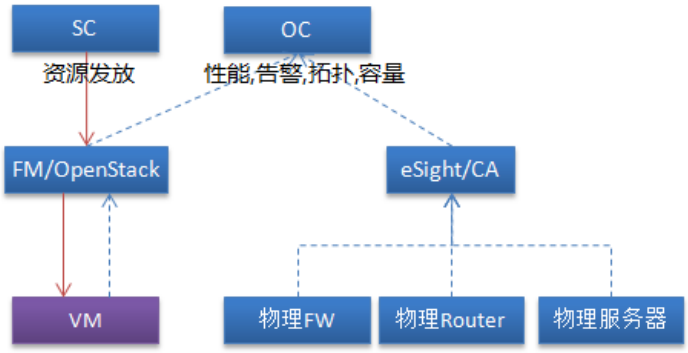
1. 多数据中心统一管理：存在多个物理数据中心需要进行统一管理的场景
2. 物理、虚拟统一管理：数据中心中存在虚拟资源和物理资源需要统一管理的，例如：支持对虚拟资源和物理资源的统一监控，拓扑管理等运维管理能力。
3. 异构资源池统一管理：数据中心有异构的虚拟化平台需要统一管理的，例如：同时有vSphere

虚拟化和KVM虚拟化平台需要统一管理。

只要存在上述场景就可以使用分布式云数据中心的统一管理能力。

3.3.2 部署架构

1. 云和非云统一管理

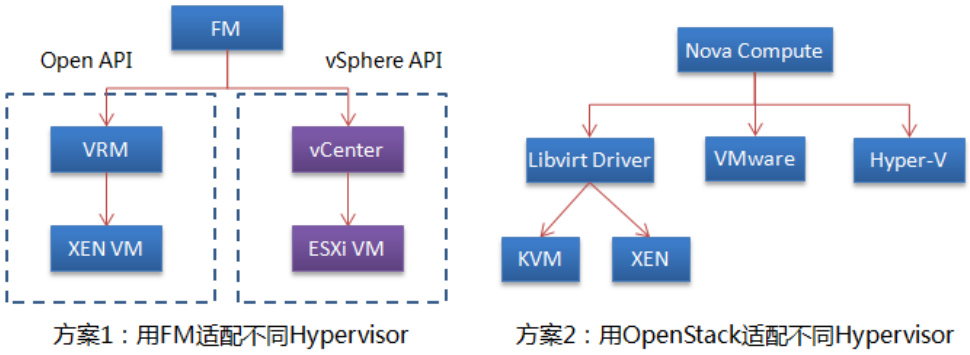


图表 13物理、虚拟资源统一管理

提供云资源和非云资源的统一管理能力：

- 非云资源管理：管理物理资源的性能、告警和拓扑。
- 云资源管理：管理云资源的自动化部署、操作能力；云资源的性能、拓扑、容量管理；云资源和非云资源拓扑映射关系。

2. 异构虚拟化统一管理



图表 14异构虚拟化管理

针对不同的方案采用不同的异构虚拟化方式：

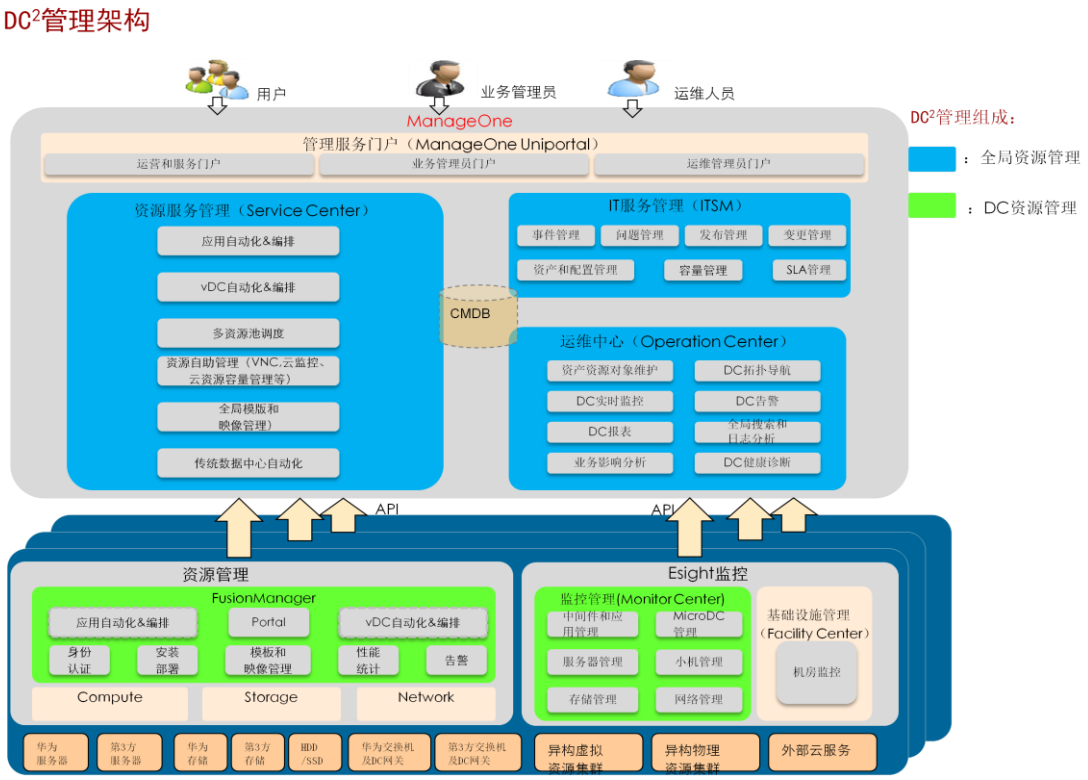
方案1：在采用FM作为云资源池管理节点的场景下，FM提供了对异构Hypervisor的适配能力主要包括华为FusionSphere平台和VMware的vCenter。FM对异构平台的适配采用接口调用方式，FM提供了适配VRM和vCenter北向接口的。

方案2：采用OpenStack对多Hypervisor的适配能力来解决，目前支持KVM。

注：OpenStack原生支持VMware、XEN、Hyper-V、KVM，目前除KVM外其它尚不能商用，商用需要对各厂商对各自插件的服务支持。

OpenStack在Nova组件的子目录nova/virt/下为Hypervisor提供了对应的compute driver，VMware, Hyperver-V提供特定的driver和OpenStack对接。对于KVM, XEN, LXC等通过Libvirt库提供的标准接口实现。

3.3.3 关键特性



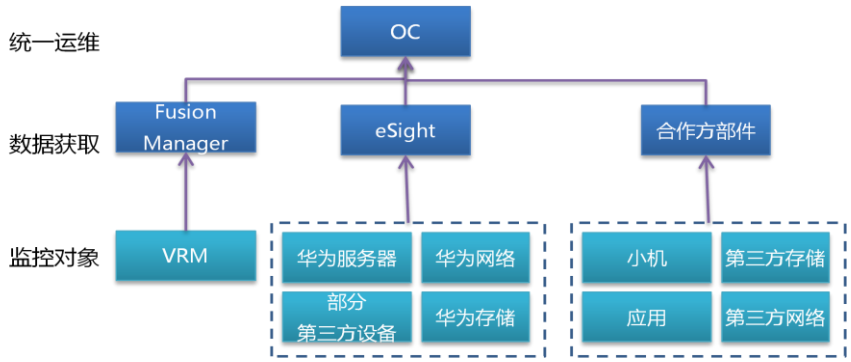
图表 15DC²管理子系统总体架构

1. 云资源和非云资源统一监控能力

对云资源和非云资源的统一监控体现在对虚拟平台和物理资源的告警监控能力上。支持对物理资源，例如：服务器、存储和网络设备的告警监控能力；同时支持和VMware的vCenter以及华为FusionManager云管理平台对接，获取虚拟化平台的告警数据。详细的监控设备列表请参考对应的软件监控对象列表。

根据不同的运维场景可选择不同的监控软件：

- 云资源池： FusionManager
- 华为基础设施：OC + eSight，支持部分异构化能力
- 异构化基础设施：OC+合作部件，支持小机，第三方存储设备等



图表 16DC²管理系统部件组合

云资源与非云资源统一管理包括的能力有：

- 虚拟机和裸机管理统一管理平台，支持业界主流的虚拟化产品和操作系统，可以兼容客户现有IT资源。
- 设备自动发现，资源快速发放，缩短业务上线时间。
- 提供对传统设备，包括服务器、网络设备、存储，以及虚拟化设备如VMware、华为FusionCompute、华为云存储OceanStor、华为桌面云的统一监控，包括自动发现上述传统设备和虚拟化设备，提供统一的资源发放，提供集中的告警呈现和处理界面，以及提供设备性能监控和报表功能。
- 支持对告警的处理，在OC上可以对告警进行相应处理，包括告警展示、告警屏蔽、告警确认、告警转工单等多种处理方式。

2. 云资源和非云资源的性能管理能力

管理云资源和非云资源的性能管理，包括获取性能数据和性能阈值告警处理等。

- 虚拟机性能：支持和FusionManager以及vCenter对接，监控虚拟化平台上VM的性能指标，包括CPU利用率，内存利用率，网络带宽，磁盘IO等。
- 物理资源性能：物理资源性能依赖于eSight或CA监控部件的指标获取。主要的对象有物理服务器，网络设备（交换机、路由器、防火墙等），存储设备的性能监控。监控指标主要包括CPU利用率，内存利用率，网络带宽等。根据设备类型不同而略有不同。监控采集层软件将监控结果上报给OC，由OC进行统一展现。OC可以展示topN性能排序，对服务器、存储、网络设备的性能进行排序。
- 阈值告警：管理员可以定义性能阈值告警，在监控的资源性能指标超过了定义的阈值时，系统将自动产生告警，提醒管理员对相应的性能风险进行处理。

3. 云资源和非云资源的拓扑管理能力

云资源和非云资源的拓扑管理能力，

- 物理拓扑管理：对物理资源的自动发现，物理资源连接关系的自动发现。拓扑数据的自动化发现由CA部件提供，OC集成CA的拓扑数据并统一展现。
- 虚拟拓扑管理：提供VDC内部不同虚拟化部件拓扑关系的展现，由于虚拟部件和连接关系都可以由管理员自主定义，因此虚拟拓扑是根据创建的结果来定义的。

- 拓扑关系映射：虚拟网络是叠加在物理网络上的，因此存在虚拟网络设备和物理网络设备间的映射关系。例如：VFW是在哪个物理FW上创建，VLB 是在哪个物理LB上创建等。这些关系是动态变化的，由于管理员可以个性化修改VDC的网络拓扑，因此这种映射关系应该能实时反映当前的映射关系。

4. 云资源的容量管理能力

云资源的容量管理是通过OC从FusionManager获取云平台资源数据来实现的。OC将统一展现当前云系统资源的使用情况，主要包括：VCPU，内存，磁盘容量，带宽等资源的使用情况。容量的展示方式可以基于物理DC和VDC两种不同的场景来分别展示。

注：缺乏对物理资源的容量管理能力，包括物理空间、存储空间、网络带宽的容量管理能力。

5. 异构虚拟化平台管理能力

在异构虚拟化平台管理能力上，针对FusionSphere和OpenStack两种部署场景提供异构虚拟化平台的支持：

- FusionSphere：采用FusionManager来屏蔽异构虚拟化平台。提供对华为Fusion云平台的支持，通过和VRM对接调用相应的Open API接口；提供对VMware平台的支持，通过和vCenter平台对接实现对ESX平台的管理，包括虚拟资源部署和操作，以及监控信息的获取。
- OpenStack：OpenStack架构天然支持多种虚拟化平台，包括KVM,XEN,VMware,LXC等。华为目前支持和KVM，XEN的对接，对接方式是通过LibVirt实现。

3.4 POD

3.4.1 POD 概念

POD即Point of delivery，做为数据中心的建设单元，代表了成熟的模块化设计理念和方法。具有按需部署、分步投资、可灵活扩展、维护方便的优点，可有效提高初始阶段设备利用率（IT设备提高50%～60%、机房设备提高25%～30%），并缩短部署周期70%以上。

POD具备的特点：

1. 模块化，粒度适中
2. 具有可复用性，可快速部署与施工
3. 可适应业务类型、层次、服务器类型的分类
4. 具有配套基础设施
5. 具有标准化网络部署方案

3.4.2 标准 POD

- 适用场景

  通用场景：支持大多数虚拟化场景（包括公有云、私有云、混合云等）和普通应用系统（包括云主机、统一通信、办公自动化等），此场景要求系统架构成熟，可靠性高；

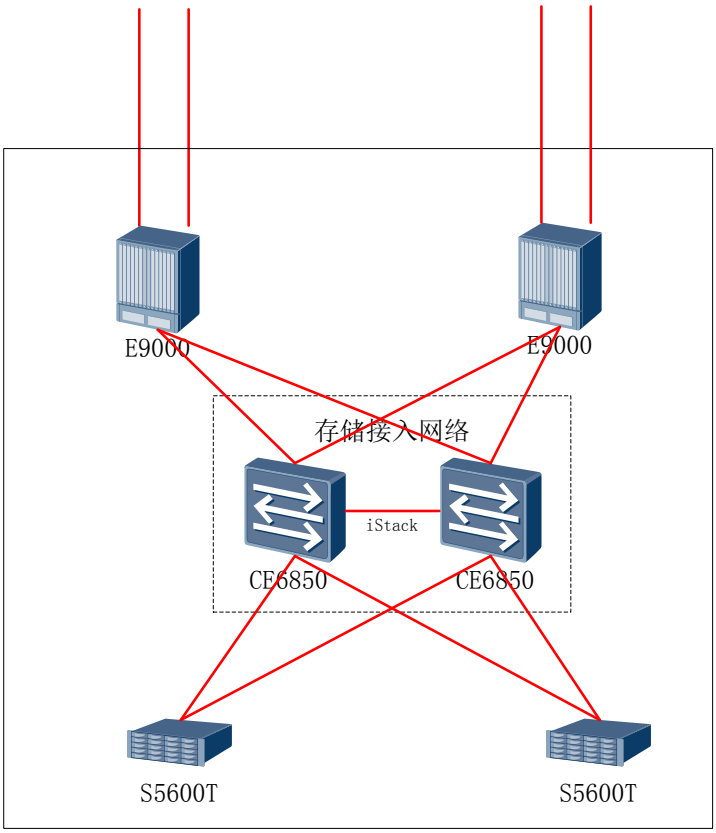
- 部署架构

标准PoD提供两种部署架构：

1. E9000+IP SAN

初始1柜配置，含1个E9000插框。

最大2柜配置，含2个E9000插框。



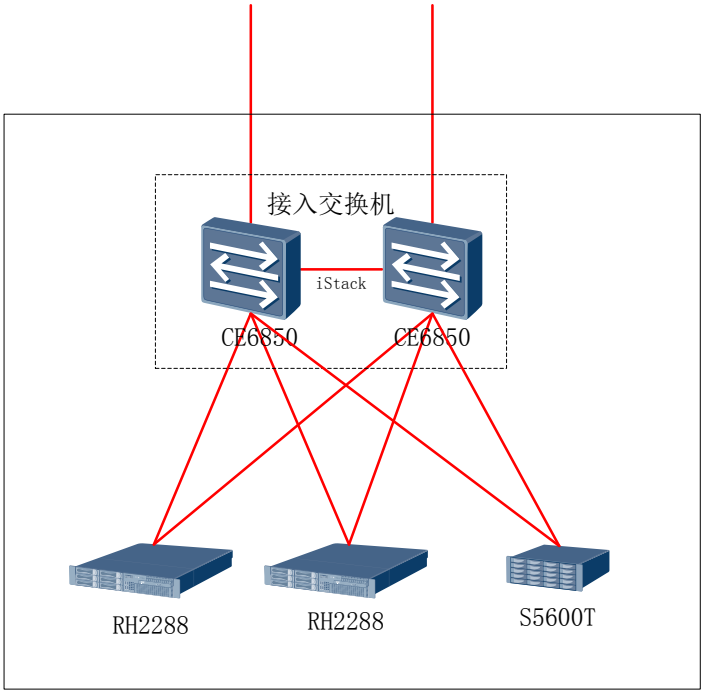
部署架构一：E9000+IP SAN

2. RH2288+IP SAN

初始1柜配置，含12个RH2288。

按半柜粒度扩容，含4个RH2288。

最大配置32台RH2288。



部署架构二：RH2288+IP SAN

- 关键特性

1. 10GE互连、提升东西流量处理能力，简化网络模型，支持网络平滑演进；
2. 计算密度高，最大64个处理器；
3. 单服务器支持1.5T内存、轻松支持应用需求；

另外配置VIS可支持双活容灾，支持基于阵列的容灾方案；

3.4.3 高扩展 POD

- 适用场景

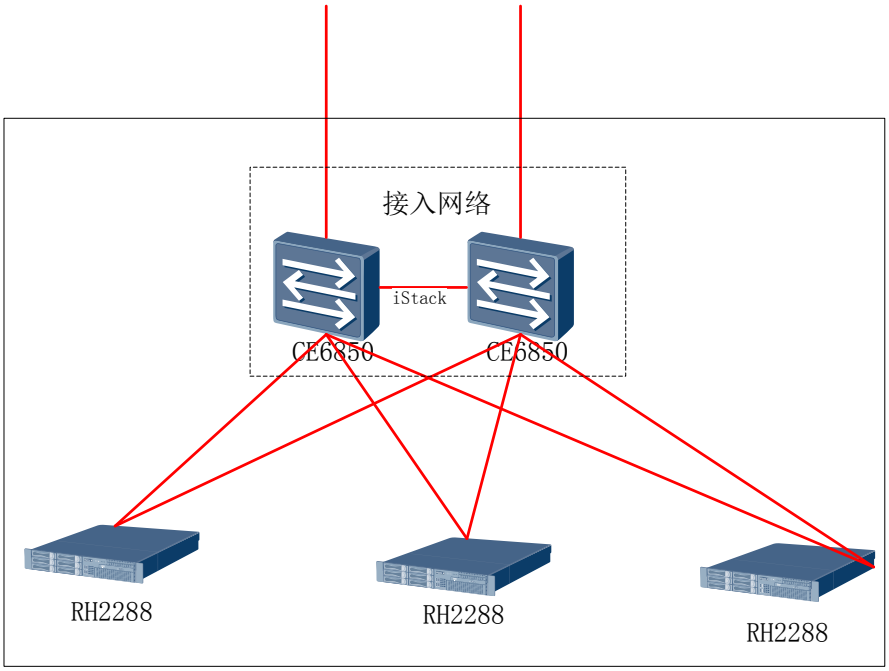
非大数据量的核心应用，支持大多数虚拟化场景（包括公有云、私有云、混合云等）和普通应用系统（包括云主机、统一通信、办公自动化等）

- 部署架构

由RH2288和CE6850组成，及FusionStroage本地存储。

初始半柜配置，包含6台RH2288。

按半柜（6台RH2288）粒度扩容，最大配置128台RH2288。



- 关键特性

1. 计算存储融合，无需外置SAN，扁平架构，简化维护；
2. SATA分布式存储+PCI-E SSD，降低成本同时提升业务处理性能；
3. 10GE互连、提升东西流量处理能力，简化网络模型，支持SDN演进；
4. 支持半柜方式平滑扩容，应对业务增长，高扩展，低成本；

3.4.4 高性能 POD

- 适用场景

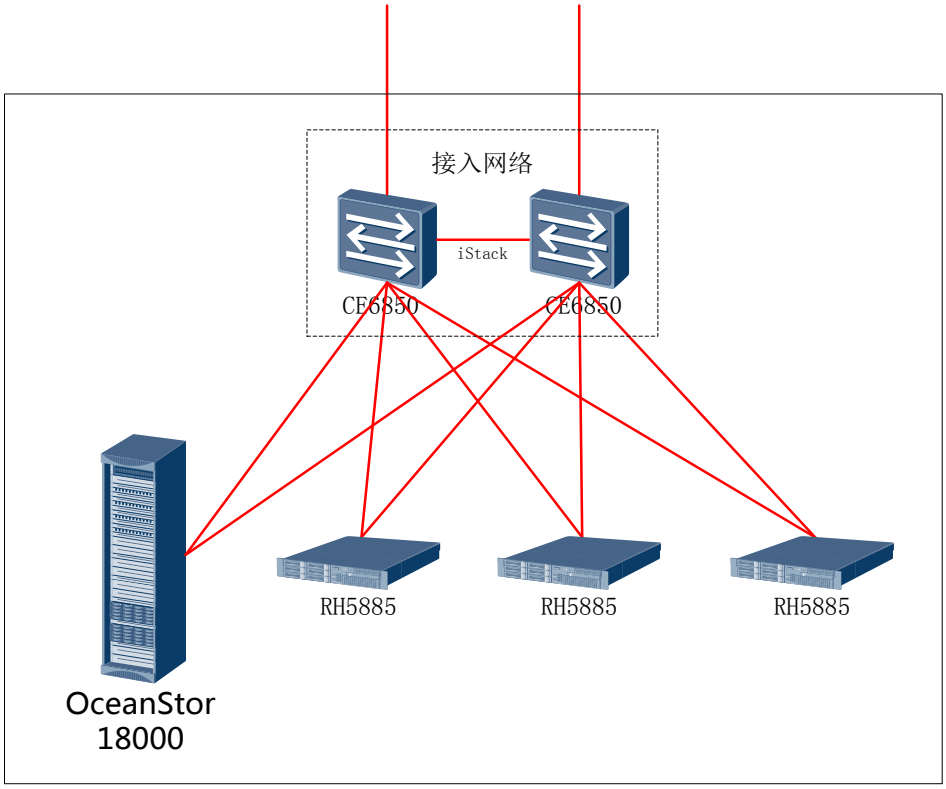
  适用于大数据量、大并发、高IO的核心虚拟化应用

- 部署架构

  由RH5885 8路服务器和OceanStor 18000组成。

  初始1柜配置，包含2台RH5885 8路服务器。

  按半柜（1台RH5885）粒度扩容，最大配置32台。



- 关键特性

1. 计算：

1)60项RAS特性媲美小型机，采用完善容错设计确保系统稳定无忧

2)单服务器8路处理器，计算性能强劲，SPEC整型计算和浮点计算性能测试世界第一

2. 存储：

1）高性能：百万级IOPS，业界平均2倍规格与性能

2) 高效率：微秒级稳定响应，业务响应速度提升10倍

3) 高可靠：20倍数据恢复速度，99.9999%可用性

3.5 备份业务

3.5.1 适用场景

用户在部署和使用虚拟机或者应用时，为应对文件、数据丢失或损坏等可能出现的意外情况，往往需要对现有的数据进行备份。分布式云数据中心解决方案针对备份业务提供了虚拟机备份框架和应用备份框架，其关键价值点有：提供基于虚拟机的备份，无需专用的备份系统，用户可以在服务Portal上自助完成虚拟机备份；提供基于代理的应用备份能力，用户可以按照应用或者文件粒度进行应用备份；

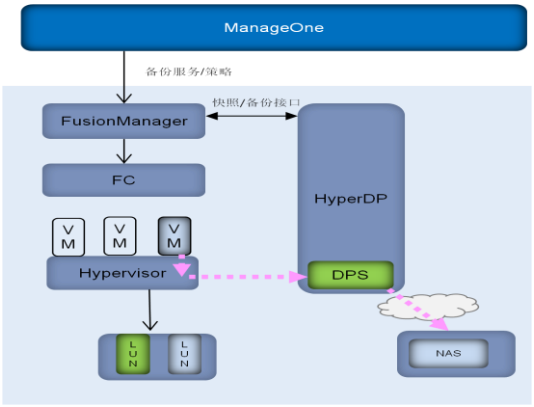
3.5.2 部署架构

分布式云数据中心的备份子系统，主要承载分布式云数据中心数据保护的功能，其架构目标如下：

- 虚拟机备份系统采用无代理备份方式、以虚拟机为单元进行备份；
- 应用备份系统采用有代理备份，用户可以在系统内安装代理，实现应用数据的备份和恢复；
- 用户可以定义备份策略；
- 用户可以通过业务Portal实现虚拟机和应用的备份；

3.5.2.1 虚拟机备份子系统

虚拟机备份子系统的框架如下图所示：



图表 17虚拟机备份架构

虚拟机的备份子系统由ManageOne、HyperDP备份服务器、虚拟化平台、备份存储构成；

（1） ManageOne 管理平台：提供虚拟机备份自服务 Portal，用户可以通过 Portal 对虚拟机进行备份的自助操作；

（2） 虚拟化平台：FusionSphere 平台，提供虚拟机快照功能，和 HyperDP 备份服务器配合提供虚拟机备份业务；

（3） HyperDP 备份服务器：部署在虚拟机内，虚拟机规格为：4U4G 及 30GB 系统盘，每个 HyperDP 备份服务器可备份 200 个虚拟机，最多可部署 10 个备份服务器组成一个备份域。FusionManager 目前只对接一个备份域。

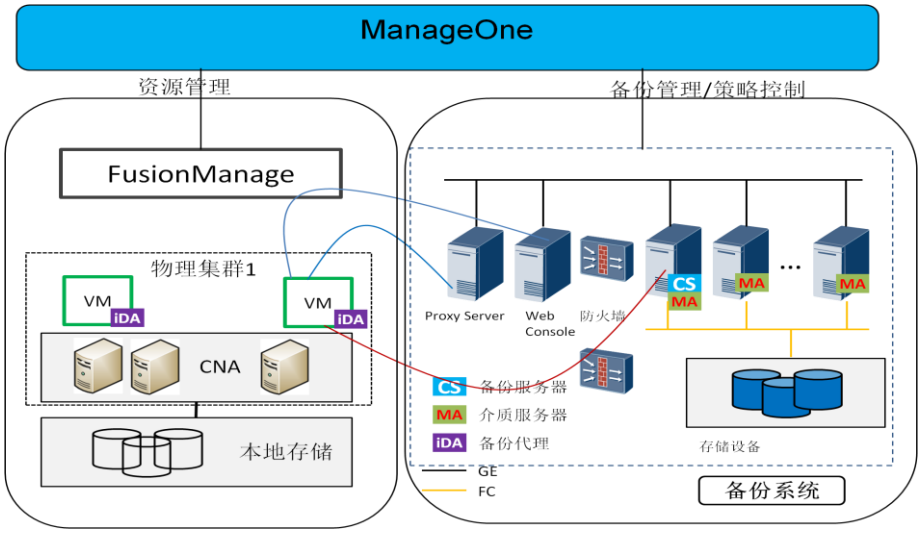
（4） 备份存储：可备份 HyperDP 虚拟机挂载的虚拟磁盘，或备份到 NFS/CIFS 共享文件系统中。推荐采用华为 N8500 集群 NAS 系统。备份存储所需容量大小与需要备份数据量大小及备份策略相关。

用户通过ManageOne下发备份策略到FusionManager，由FusionManager下发到HyperDP，HyperDP根据备份策略和虚拟机化平台配合，针对虚拟机完成备份。

约束：当前HyperDP只支持FusionSPhere虚拟机的备份；

3.5.2.2 应用备份子系统

应用备份子系统的框架如下图所示：



图表 18应用备份架构

应用备份子系统由ManageOne、备份系统、备份代理组成；其中备份系统采用simpana备份框架，包含备份服务器、介质服务器、代理服务器、web 控制台；其中，备份服务器用于控制和管理备份业务、备份用户信息；介质服务器用于控制备份任务和备份数据存储；代理服务器用于代理软件服务；web 控制台用于用于的web网页操作；各部分组件的具体功能描述如下：

逻辑划分	组件名称	功能
管理平台	ManageOne	提供应用备份自服务发放Portal，用户可以通过Portal对申请应用备份服务；
备份系统	Simpana CommServe	协调和管理Simpana其他组件，发起数据保护、管理和恢复操作。
	Simpana MediaAgent	在备份客户端与存储介质之间传送数据。
	Simpana Proxy (Simpana Windows FileSystem iDataAgent)	用于备份客户端与CommServe、MediaAgent间的通信转发。 用于管理节点与CommServe通信，实现备份业务的开通、注销，各种报告的获取等。
	Simpana CommCell Console	用户通过Simpana控制台，实现执行备份、查看备份历史、浏览和恢复数据等操作。

	Simpana客户端安装包	定制化的Simpana客户端代理程序安装包（各种平台和应用的iDataAgent组件），供用户下载安装到需要备份的主机上。
	下载Portal	提供Web页面供用户选择下载所需的Simpana客户端安装包。
备份客户端	Simpana FS iDataAgent	用于备份和恢复主机的文件系统。
	Simpana xx iDataAgent	用于备份和恢复主机上的某种应用，比如Oracle、Exchange等，一种应用对应一种代理组件。

3.5.3 关键特性

3.5.3.1 虚拟机备份方案

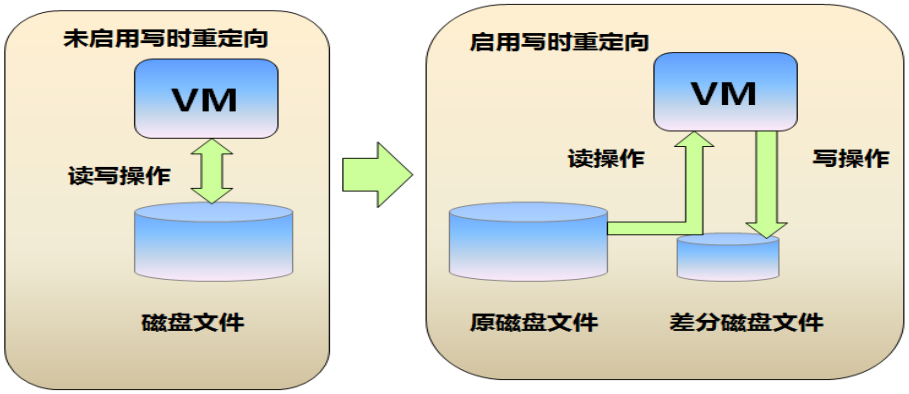
分布式云数据中心解决方案提供以下虚拟机无代理备份能力和服务：

- 云主机用户可以根据业务需要自助申请云主机备份服务，云主机备份为无代理备份，用户无需额外安装代理软件；用户可对云主机做整机备份；
- 用户可以自己定义备份策略；
- 支持虚拟机整机恢复，当用户选择整机恢复时，系统将为用户创建一个新的虚拟机，并将用户的所有数据恢复到新的虚拟机上。
- 适用于服务器虚拟化、数据中心、一体机、桌面云场景下用户虚拟机的备份。
- 支持生产存储为虚拟存储（基于SAN、NAS或本地磁盘）及FusionStorage下的虚拟机备份

虚拟机的备份采用无代理的备份，依赖虚拟化平台提供的虚拟机快照技术实现；虚拟机备份是周期性进行的，每次备份备份服务器都会通过虚拟化平台提供的北向接口创建一个新的虚拟机快照，完成数据增量计算后和数据下载后，删除上一次备份的虚拟机快照，其关键技术是：

- 虚拟机快照

虚拟机快照利用FusionSphere的写时重定向技术（Redirect on Write）实现。写时重定向技术能够在虚拟机磁盘文件被修改时，可以不修改原磁盘文件，而是将修改区域记录在另一个差分磁盘中，将差分磁盘的父磁盘指向原磁盘文件，使得虚拟机在从差分磁盘文件中读取数据时，能够自动从原磁盘文件中获得需要的数据。



图表 19虚拟机快照

当对虚拟机生成快照时，虚拟机将当前状态保存在快照文件中，包括磁盘内容、内存和寄存器数据。用户可以通过恢复快照多次回到这一状态，虚拟机用户在执行一些重大、高危操作前，例如系统补丁，升级，破坏性测试前执行快照，可以用于故障时的快速还原。其功能特点如下：

- 无代理备份，不需要在要备份的虚拟机内安装备份代理软件。
- 支持虚拟机在线备份，不管虚拟机是开机还是关机都可进行备份。
- 支持对多种生产存储上的虚拟机进行备份和恢复，包括FusionStorage与存储虚拟化。
- 支持备份到多种备份存储，包括备份服务器所在虚拟机挂载的虚拟磁盘（可位于SAN、NAS或本地硬盘上）和外接的NFS/CIFS共享文件系统存储设备（如NAS）。
- 支持Windows VSS（Volume Shadow Copy Service，卷影复制服务）应用一致性，保证备份数据可恢复。
- 支持多种备份类型，包括完全备份、增量备份和差量备份，并可批量备份，其特点如下：
  - 完全备份支持有效数据备份。对于“普通延迟置零”或“精简”模式磁盘只备份有效数据（如 100GB 磁盘有效数据 20GB，则只需要备份 20GB 数据），对于“普通”模式磁盘需要备份所有数据（如 100GB 磁盘需要备份 100GB 数据）；对需要备份的虚拟机建议其磁盘类型设置为“普通延迟置零”或“精简”，以减少备份空间。
  - 增量备份和差量备份功能只需备份变化数据块，减少备份数据量，降低了备份虚拟机的成本，并最大限度地缩短了备份窗口。
- 支持多种恢复类型，包括恢复到新虚拟机（整机恢复）、恢复到原虚拟机和恢复到指定虚拟机（磁盘恢复），并可批量恢复。
- 支持多种恢复方式，包括虚拟机镜像恢复和虚拟机差量恢复。
  - 虚拟机镜像恢复时，恢复的数据量与完全备份相同。
  - 虚拟机差量恢复仅针对存储虚拟化，恢复到原虚拟机时，利用更改数据块跟踪(CBT，Changed Block Tracking)功能只需恢复从备份点到当前变化的数据块，从而实现快速恢复。
- 支持灵活备份策略，管理员可以通过HyperDP设置策略。
  - 支持针对不同虚拟机或虚拟机组设置不同备份策略，最多支持 200 个备份策略。
  - 支持对全备份与增量备份或差量备份分别设置不同备份周期、备份时间窗口；如

支持设置每周进行一次全备、每天进行一次增备，也可只进行一次全备，后续一直进行增备

- 支持设置备份数据保留时间以自动清除过期备份数据。
- 支持设置备份策略优先级。

◆ 支持并发备份与恢复，最多支持8个虚拟机的并发备份与恢复。

◆ 支持跨FusionCompute站点的虚拟机磁盘的备份和恢复。

◆ 采用备份管理服务器与备份处理服务器结合的分布式备份架构，一个备份管理服务器可最多管理10个备份处理服务器（由某个备份处理服务器兼做备份管理服务器功能，不需单独部署备份管理服务器），并可通过浏览器统一管理。每个备份处理服务器支持200个虚拟机的备份。

◆ 支持备份服务器自身管理数据的备份与灾难恢复。

◆ 易管理和维护

- 备份服务器通过虚拟机模板安装，简化备份软件安装部署操作，缩短部署时间。
- 提供基于图形的管理工具 HyperDP Management Console 和基于命令行的 CLI（Command-Line Interface），进行集中的备份恢复业务和系统管理，为用户提供简单直观的操作维护方式。

从完成的数据备份与恢复的过程来看，备份过程与恢复过程的特点如下：

■ 数据备份过程

◆ VM内不需要安装备份代理软件，由虚拟化层通过业务网络与HyperDP备份服务器通信，将虚拟机快照数据备份到备份存储上。

◆ VM的数据备份策略可以在HyperDP服务器上灵活设置。建议在业务空闲时进行备份，避免数据备份影响业务。备份策略可以根据业务需要进行调整，存储容量和带宽也需要进行相应的调整。

■ 数据恢复过程

◆ 当某个虚拟机数据故障需要恢复时，可以通过HyperDP备份服务器将需要恢复的虚拟机或指定卷恢复到原虚拟机中。

◆ 若某个虚拟机被意外删除时，可以通过HyperDP备份服务器恢复到新虚拟机，或用户创建一个新虚拟机后通过HyperDP备份服务器恢复到该指定的新虚拟机中。

■ 约束

虚拟机无代理备份该版本只支持FusionSphere的虚拟机备份，在Openstack架构下不支持该能力；

3.5.3.2 应用备份方案

分布式云数据中心解决方案提供以下应用备份能力：

◆ 应用备份以数据中心管理员手工操作为主；用户可以根据业务需要线下向管理员申请应用备份服务；管理员在备份系统上增加相关权限和业务配置后，通知用户下载备份代理并进行相关的备份业务.

- 用户可以在备份平台上自己定义备份策略；
- 用户可以根据需要备份的应用，下载不同的备份代理软件，系统可以支持应用备份和文件粒度的备份；
- 支持基于SAN、NAS或VTL作为备份存储；
- 兼容多种应用和操作系统

应用兼容性	描述
浏览器	支持 IE8 及以上版本浏览器
文件系统备份	支持 Windows 32/64、Linux 32/64、AIX、HP-UX、Solaris 平台
Active Directory 备份	支持 Windows 32/64 平台
Exchange 备份	支持 Windows 32/64 平台
MySQL 备份	支持 Windows 32/64、Linux 32/64、HP-UX、Solaris 平台
DB2 备份	支持 Windows 32/64、Linux 32/64、AIX、HP-UX、Solaris 平台
Oracle 备份	支持 Windows 32/64、Linux 32/64、AIX、HP-UX、Solaris 平台
SharePoint 备份	支持 Windows 32/64 平台
Sybase 备份	支持 Windows 32/64、Linux 32/64、AIX、HP-UX、Solaris 平台
SQL Server 备份	支持 Windows 32/64 平台
Lotus Notes 备份	支持 Windows 32/64、Linux 32/64、AIX、Solaris 平台
Informix 备份	支持 Windows 32/64、Linux 32/64、AIX、HP-UX、Solaris 平台
PostgreSQL 备份	支持 Windows 32/64、Linux 32/64 平台
SAP 备份	支持 Windows 32/64、Linux 32/64、AIX、HP-UX、Solaris 平台
虚拟机备份	支持备份企业用户侧 Vmware、Hyper-V 虚拟机

- 支持备份重删除和压缩功能；

■ Commvault备份申请过程

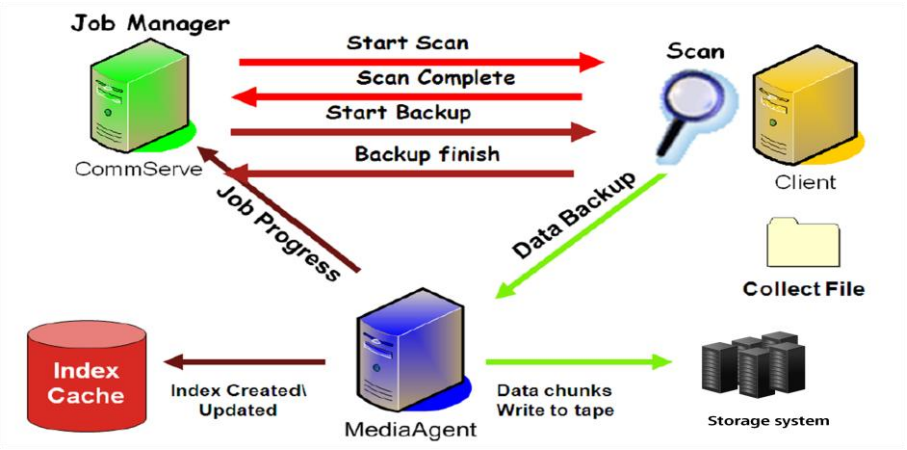
当用户由业务平台申请备份服务时，系统或管理员会在commvault simpana上创建用户信息和注册用户主机信息，并根据用户申请的备份空间提供存储空间，然后通知用户下载代理软件；

用户根据业务的要求，选择安装合适的代理软件，然后通过web控制台操作，完成备份策略、备份任务创建操作，在备份过程中，用户可以通过web控制台查看备份任务状态，当需要做数据恢复时，用户可以通过web控制台进行备份恢复操作。

■ Commvault备份过程

commserve服务器开始扫描待备份的客户主机，获取待备份的索引，然后通知客户主机启动备份； 客户主机将备份数据发送到MediaAgent，由MeidaAgnet完成备份数据写入存储，并建立索引；

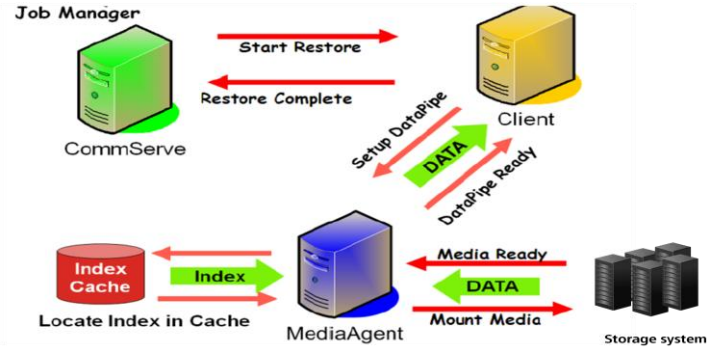
备份作业完成后，由客户主机通知commserve备份完成。



图表 20备份过程示意图

- Commvault备份恢复的过程

commserve服务器下发指令通知客户主机进行数据恢复，客户主机向MediaAgent发起数据通道建立请求，MediaAgent根据内部索引关系建立好数据映射后，通知主机数据通道建立成功，主机开始进行数据恢复，恢复后，通知commserve恢复完成。



图表 21备份恢复示意图

3.6 容灾业务

3.6.1 适用场景

为了保证企业的业务连续性，企业除了对业务数据做备份外，通常还需要建立容灾系统。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系统，系统之间可以相互进行健康状态监视和功能切换，当一处系统因意外(如火灾、洪水、地震、人为蓄意破坏等)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。容灾系统需要具备较为完善的数据保护与灾难恢复功能，保证生产中心不能正常工作时数据的完整性及业务的连续性，并在最短时间内由灾备中心接替，恢复业务系统的正常运行，将损失降到最小。

针对企业部署的虚拟化平台，分布式云数据中心提供基于IaaS层的容灾方案，支持主备容灾和双活容灾场景；基于物理部署的应用容灾，不在这个文档的描述范围内，请参考《华为点

对点容灾解决方案 V100R001C00 技术白皮书》。

业务连续性保证是分布式云数据中心的一个重要特性，分布式数据中心提供以下容灾能力：

- 支持FusionSphere容灾管理、灾备业务可视化管理、灾备自动化配置，流程编排、支持容灾切换定制；
- 支持应用级容灾管理；
- 提供双活容灾解决方案，FusionSphere云平台双活容灾方案适用于满足下列条件的客户：
  - 客户生产中心的业务系统有应用级容灾需求，生产中心部分或全部设备（网络、存储、主机）故障时需要尽快恢复业务。对 RPO 和 RTO 要求较高，如 RPO 为 0，RTO 为分钟级。
  - 生产中心和容灾中心要求配置为双活模式，需要实现跨数据中心业务负荷分担。
  - 生产中心和容灾中心距离较近，小于 100KM。
  - 生产中心与容灾中心之间具有高速、低时延和高可靠性的光纤互联网络。
- 提供主备容灾解决方案，支持存储阵列复制技术和主机层复制技术；

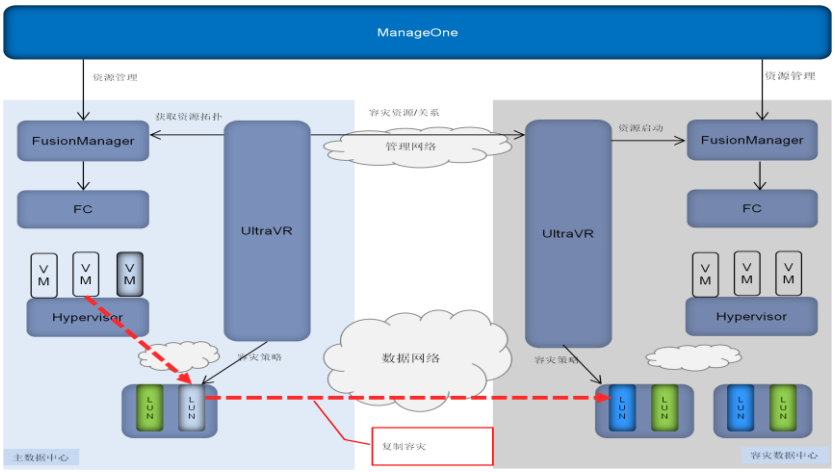
3.6.2 部署架构

分布式云数据中心容灾子系统，提供基于IaaS层的容灾方案，包含：

- 基于存储阵列复制的云平台主备容灾框架；
- 基于主机复制的云平台主备容灾框架；
- 基于VIS的云平台双活容灾部署框架；

3.6.2.1 基于存储阵列复制的云平台主备容灾部署架构

分布式云数据中心基于IaaS层的容灾方案中，基于存储阵列复制的容灾业务部署如下图所示：



图表 22 阵列容灾部署框架

基于阵列复制的虚拟机容灾子系统由FusionSphere、UltraVR 容灾管理服务器、虚拟化平台、

容灾阵列构成；

（1） 虚拟化平台：FusionSphere 平台，和 UltraVR 配合完成虚拟机的容灾业务；FusionSphere 在主备节点各部署一套；

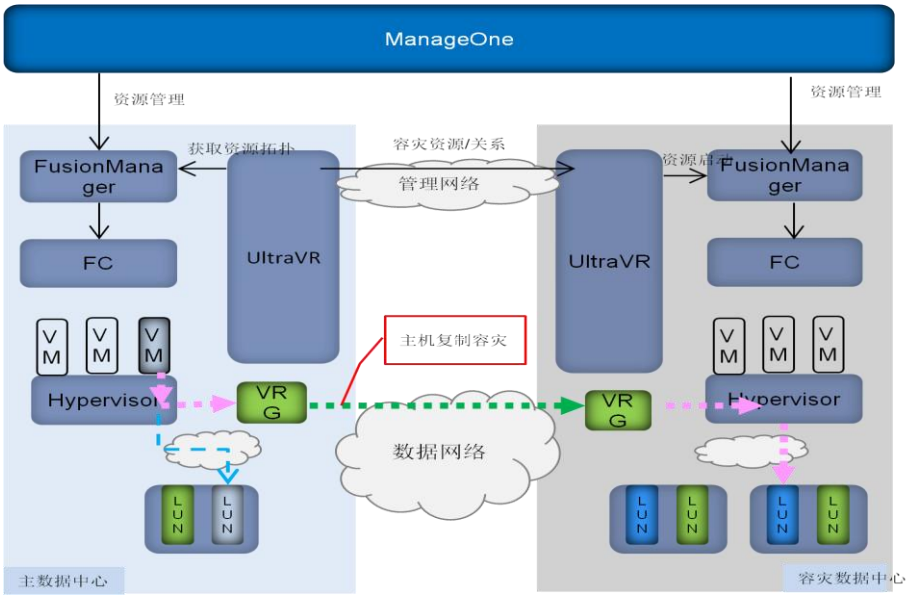
（2） UltraVR 容灾管理服务器：部署在虚拟机内，主备站点各部署一套。虚拟机规格至少为：4CPU*1.6GHz、8GB 内存、50GB ，每个 UltraVR 服务器可管理 3000 个虚拟机容灾。

（3） 容灾阵列：用于做生产侧 SAN 阵列的容灾，阵列上配置 HyperMirror license，用于阵列的数据复制。要求和生产中心的存储同构；

UltraVR根据管理员定义的容灾策略，主备资源关系，通过数据网络实现从主用生产中心到容灾中心的数据容灾；通过管理网络实现从主用生产中心到容灾中心的虚拟机，存储、网络、资源池等的信息同步；当灾难发生时，UltraVR可以根据预先定义好的容灾恢复计划，实现容灾站点的业务切换，快速恢复业务；

3.6.2.2 基于主机层复制的云平台主备容灾部署架构

分布式云数据中心基于IaaS层的容灾方案中，基于主机层复制的容灾业务部署如下图所示：



图表 23 主机层复制容灾部署框架

基于主机复制的虚拟机容灾子系统由FusionSphere、UltraVR 容灾管理服务器、虚拟化平台、容灾阵列构成；

（1） 虚拟化平台：FusionSphere 平台，和 UltraVR 配合完成虚拟机的容灾业务；FusionSphere 在主备节点各部署一套；

（2） UltraVR 容灾管理服务器：部署在虚拟机内，主备站点各部署一套。虚拟机规格至少为：4CPU*1.6GHz、8GB 内存、50GB ，每个 UltraVR 服务器可管理 3000 个虚拟机

容灾。

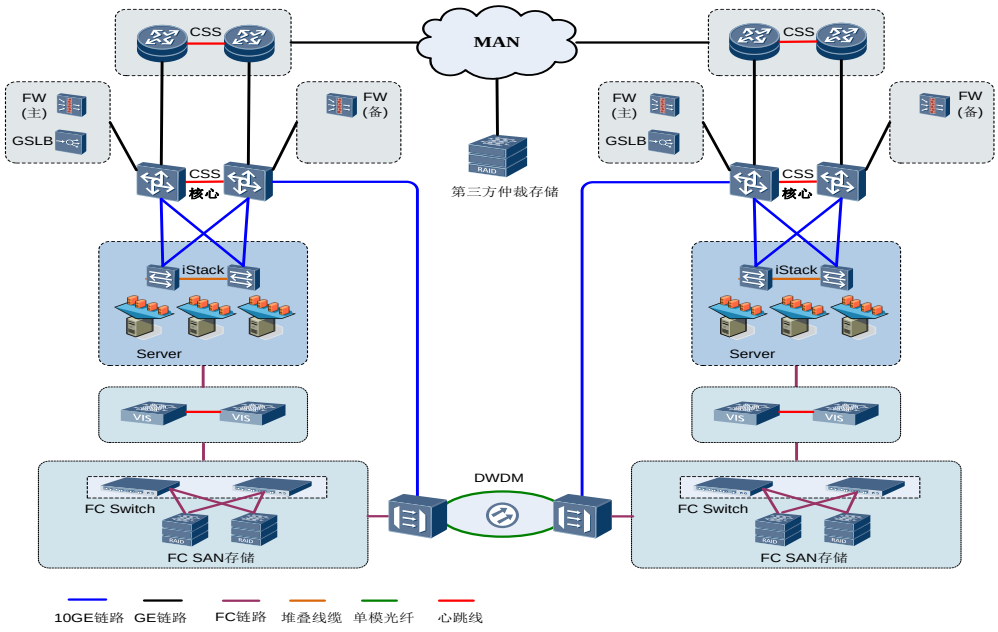
（3） VRG 复制网关：用于将虚拟机的数据复制到容灾中心，采用虚拟机部署，单个 VRG 网关可以支持 150 个虚拟机的复制（IO 轻载的场景，平均 IOPS <= 7，所有 VM 卷总数不超过 300）；

（4） 容灾阵列：支持容灾中心和生产中心的存储异构；

UltraVR根据管理员定义的容灾策略，主备资源关系，通过数据网络实现从主用生产中心到容灾中心的数据容灾；通过管理网络实现从主用生产中心到容灾中心的虚拟机，存储、网络、资源池等的信息同步；当灾难发生时，UltraVR可以根据预先定义好的容灾恢复计划，实现容灾站点的业务切换，快速恢复业务；

3.6.2.3 基于VIS的云平台双活容灾部署架构

分布式云数据中心基于IaaS层的容灾方案中，基于VIS的云平台双活容灾的业务部署如下图所示：



图表 24FusionSphere云平台双活容灾方案网络拓扑

基于VIS的云平台双活容灾是结合VIS集群技术和云平台Active-Active模式部署技术实现的双活容灾方案。通过在云平台与存储阵列之间部署VIS集群，多个VIS节点按照Active-Active模式分布在本地和远端，并结合VIS的镜像技术，可以支持本地和远端同时访问共享存储；实现容灾倒换后存储业务的无缝切换；同时云平台同一个集群内的主机按照Active-Active模式分布在本地和远端，利用虚拟机的HA功能实现容灾自动倒换功能。

基于VIS的云平台双活容灾的业务框架由FusionSphere、UltraVR容灾管理服务器、VIS6600T虚拟机化网关构成；

（1） 虚拟化平台：FusionSphere 平台，和 UltraVR 配合完成虚拟机的容灾业务；FusionSphere 在两站点配置成；

（2） UltraVR 容灾管理服务器：部署在虚拟机内，主备站点各部署一套。

（3） VIS6600T 虚拟机化存储网关：在云平台与存储阵列之间部署 VIS6600T 集群，多个 VIS 节点按照 Active-Active 模式分布在本地和远端，并结合 VIS 的镜像技术，支持本地和远端同时访问共享存储；本地和远端的 FC 交互机通过 DWDM 实现光纤直连；

（4） 第三方仲裁存储：在部署双活容灾时，需要在第三地部署第三方仲裁存储，用于在网络故障时仲裁主用 VIS 节点，避免出现脑裂。

（5） 云平台的大二层网络：为了支持集群中主机在物理上拉远后仍能实现 HA、热迁移等功能，管理/业务/VIS 心跳平面需要提供大二层组网。考虑到对网络时延的要求，目前推荐 L1 专线(以太口)方式在核心交换机二层互联（也可以通过波分设备+裸光纤连接），要求至少两条 L1 专线冗余以保证可靠性。

（6） 全局负载均衡 GSLB：在本地和远端各部署一个 GSLB，在多个可提供相同服务的站点之间，根据相应的分配策略将用户请求“路由”到合适的站点上。

3.6.3 关键特性

3.6.3.1 基于存储阵列复制的云主机容灾

基于阵列复制容灾，通过存储系统的远程复制功能实现生产中心到容灾中心之间虚拟主机或应用的数据保护；根据业务的RPO要求以及生产中心与容灾中心的网络状况，可以选择同步复制或者异步复制。

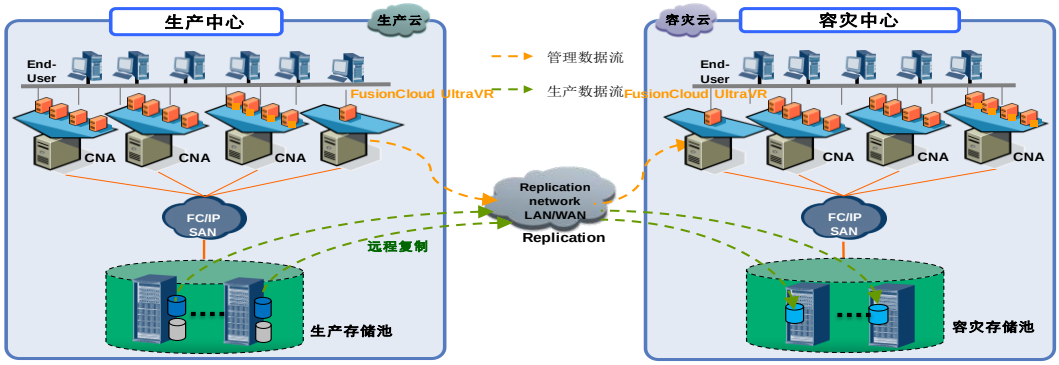
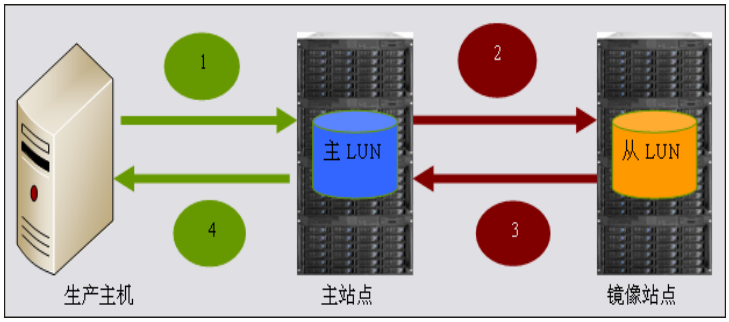


图 14 基于阵列复制的云平台数据级容灾拓扑图

- 同步复制

同步复制利用日志原理实现主、从LUN的数据一致性，同步复制实现原理如下**错误！未找到引**

用源。所示。



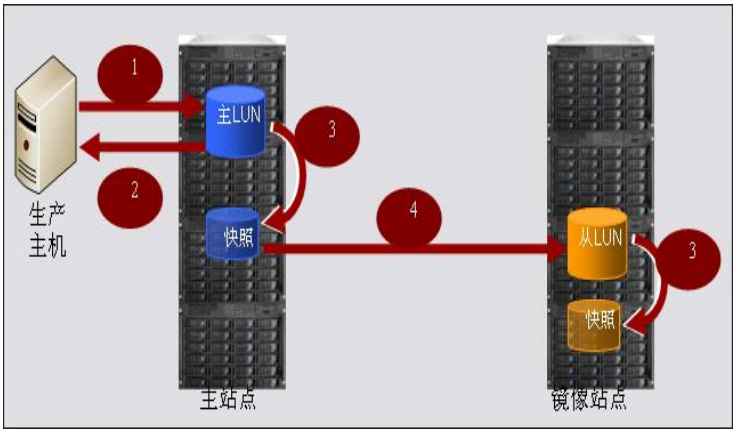
图表 25同步复制I/O处理原理图

同步复制实现过程如下：

1. 首先为主站点的主 LUN 和远端复制站点的从 LUN 建立同步复制关系，并启动数据初始同步，将主 LUN 数据全量拷贝到从 LUN。
2. 如果在初始同步时主 LUN 收到生产主机写请求，需要检查同步进度：若要写入位置的数据块尚未拷贝到从 LUN，只需要写主 LUN 即可返回主机成功，稍后利用同步任务将整个数据块同步到从 LUN；若要写入位置的数据块已经拷贝，需要分别写入主 LUN 和从 LUN；若要写入位置的数据块正在拷贝，需要等待该数据块拷贝完成后分别写入主 LUN 和从 LUN。
3. 初始同步完成以后，主、从 LUN 数据完全一致，如果此时主 LUN 收到生产主机写请求，按照下面的流程进行 I/O 处理。
4. 主 LUN 接收生产主机写请求，记录这个 I/O 对应数据块的差异日志值为“有差异”；
5. 同时把写请求的数据写入主 LUN 和从 LUN，写从 LUN 时需要利用配置好的链路将数据发送到远端复制站点；
6. 判断写主 LUN 和写从 LUN 的执行结果，如果都成功，则将差异日志改为“无差异”，否则保留“有差异”，在下一次启动同步时重新拷贝这一个数据块；
7. 主 LUN 返回生产主机写请求完成。

- 异步复制

  异步复制I/O处理的原理如下图所示：



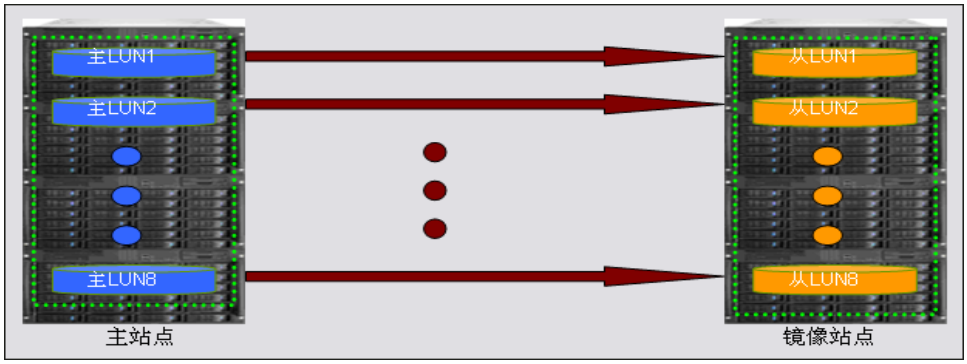
图表 26异步复制I/O处理原理图

1. 首先为主站点的主 LUN 和复制站点的从 LUN 建立异步复制关系，并启动初始数据同步，将主 LUN 数据全量拷贝到从 LUN。
2. 如果在初始同步时主 LUN 收到生产主机写请求，只会将数据写入主 LUN。
3. 初始同步完成后，从 LUN 数据状态变为已同步或一致（在整个初始同步过程中都没有主机写请求下发时，从 LUN 数据状态为已同步，否则为一致），然后开始按照下面的流程进行 I/O 处理。
4. 主 LUN 接收生产主机的写请求；
5. 写请求数据写入主 LUN 后，立即响应主机写完成；
6. 每当间隔一个同步周期（由用户设定，范围为 1-1440 分钟）以后，会自动启动一个将主 LUN 数据增量同步到从 LUN 的同步过程（如果同步类型为手动，则需要用户来触发同步）。在同步开始以前，先对主 LUN 和从 LUN 分别生成快照：主 LUN 的快照可以保证同步过程中读取到的主 LUN 数据是具备一致性的；从 LUN 的快照用于备份从 LUN 在同步开始前的数据，避免同步过程发生异常导致从 LUN 的数据不可用；
7. 主 LUN 向从 LUN 同步数据时，读取主 LUN 快照的数据，复制到从 LUN；
8. 主 LUN 向从 LUN 同步数据完成后，分别取消主 LUN 和从 LUN 的快照，然后等待下一个同步的到来。

■ 一致性组

通常业务系统中会包含多个LUN，并且这些LUN的数据存在相互关联性；为了保证多LUN在数据复制时的数据一致性，业务复制还需要用到存储提供的一致性组功能；

一致性组可以添加多个复制对，如下图。当对一致性组进行分裂、同步和主从切换等操作时，一致性组的所有成员复制对同时进行分裂、同步、主从切换和强行主从切换。此外，当遇到故障时，一致性组的所有复制对都会一起进入断开状态。



图表 27复制一致性组示意图

3.6.3.2 基于主机层复制的云主机容灾方案

虚拟机的主机层复制容灾，主要是通过虚拟化平台的Hypervisor层进行IO捕获与复制，实现虚拟主机数据的远程复制；此外，结合云数据中心的容灾管理平台，容灾管理员可以实现容灾保护策略制定、容灾计划制定、容灾切换、容灾回切及有计划性的虚拟机迁移。

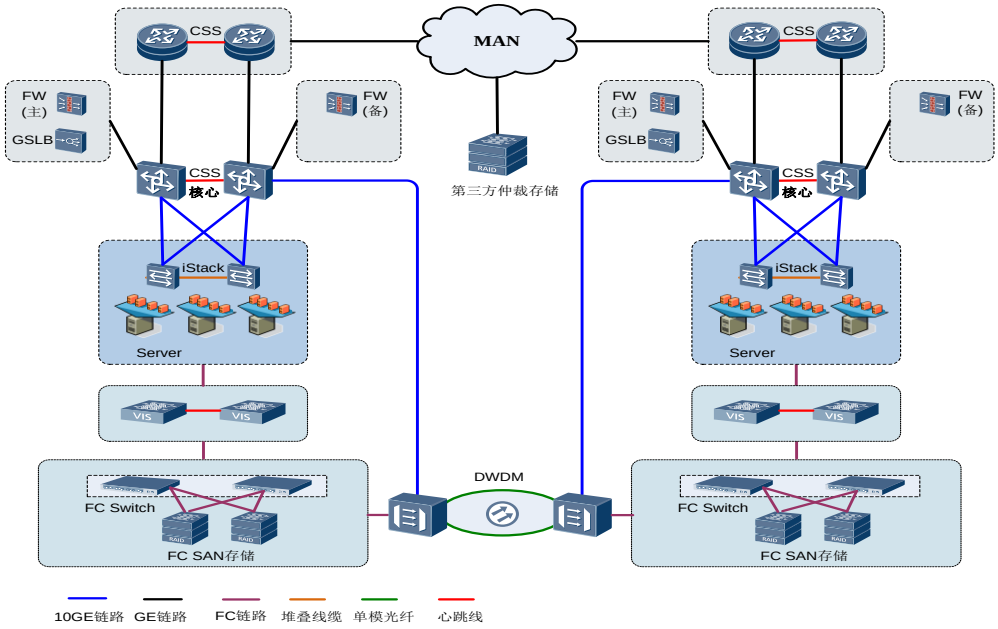
基于主机层的复制容灾技术，有以下特点：

- 实时IO分流复制：实时IO分流复制技术是基于华为自研虚拟化平台开发的复制技术，通过HypserVisor层的IO分流，实现基于虚拟机的整机复制。支持Windows系统**的数据一致性，通过**VSS功能实现系统级别的一致性；**支持**Linux系统**的数据一致性，通过**部署特定的插件支持文件系统，特定应用（Oracle、DB2）的数据一致性；支持更低的RPO需求（最低10S），单VM RTO<=3mins。
- 复制网关： 通过在生产站点和容灾站点部署复制网关，可以将多个虚拟机数据复制到异地进行保护；复制网关支持传输压缩、加密，队列缓存；支持虚拟化部署；
- 可扩展：支持按照虚拟机粒度进行容灾，容灾规模可水平扩展，复制网关可以通过水平扩展，支持大规模的虚拟机实例复制，架构上无规模限制，同等规模下资源/成本使用更低，业界最优；
- 存储无关：支持生产站点与容灾站点采用不同存储阵列，和阵列解耦；

3.6.3.3 基于VIS的云平台双活容灾方案

基于VIS的云平台双活容灾是结合VIS集群技术和云平台Active-Active模式部署技术实现的双活容灾方案。通过在云平台与存储阵列之间部署VIS集群，多个VIS节点按照Active-Active模式分布在本地和远端，并结合VIS的镜像技术，可以支持本地和远端同时访问共享存储；实现容灾倒换后存储业务的无缝切换；同时云平台同一个集群内的主机按照Active-Active模式分布在本地和远端，利用虚拟机的HA功能实现容灾自动倒换功能。

基于VIS的容灾方案能够实现RPO、RTO接近于0的自动容灾切换方案，在生产侧站点故障之后能够自动地容灾倒换到另一侧站点。

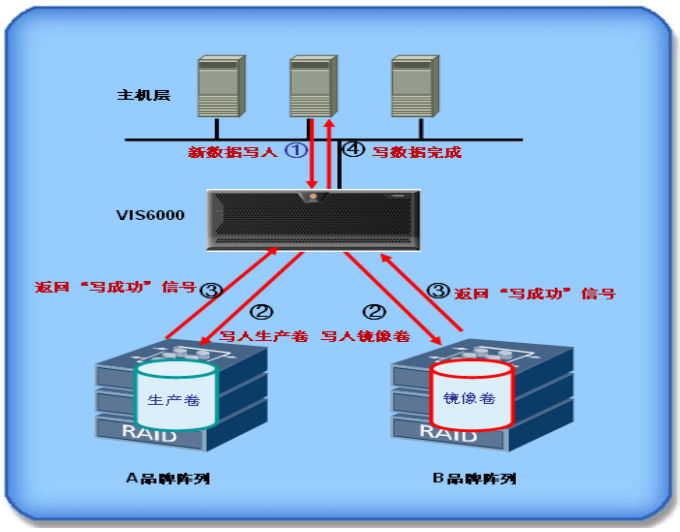


图表 28FusionSphere云平台双活容灾方案网络拓扑

FusionSphere云平台双活容灾方案采用下面关键技术：

- 跨阵列镜像技术

存储虚拟化设备支持跨异构阵列配置镜像，以华为VIS6600T为例，其实现原理如下图所示：



图表 29华为VIS6600T跨阵列镜像技术原理图

其工作流程如下：

- 主机写入新数据到VIS6600T；
- VIS6600T同时将数据写入到生产卷跟镜像卷；
- 生产卷写入成功，并且镜像卷也写入成功，都给VIS6600T返回“写成功”的信号；

- VIS6600T返回“写完成”信号给主机。

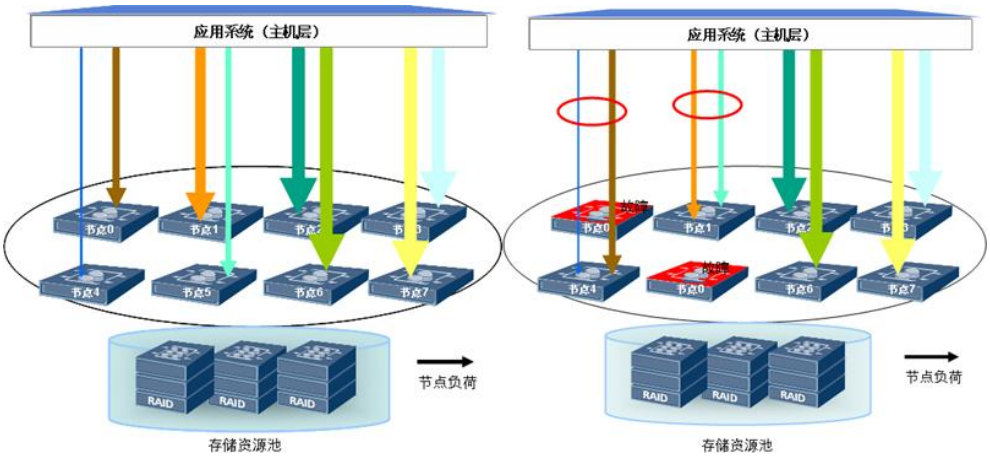
在镜像方式下，镜像卷与生产卷的数据严格保持一致。镜像既可以在本地进行部署，也可以在远端进行部署。相比较于其他备份技术，镜像技术数据保护程度最高，效果最好。

■ 集群技术

VIS6600T集群采用Active-Active存储架构，正常情况下各节点同时工作，并发处理主机的业务请求。各节点互为备份，当其中一个或多个节点发生故障的时候，剩余节点会快速地自动接管其业务，保证业务运行的连续性。

VIS6600T集群可以将业务均衡到多个节点上处理。这种均衡的分担业务的方式，叫做负载均衡。能更有效的利用资源，提高系统的工作效率和性能，用户可以从集群系统的投资中获得最大的价值。

华为VIS6600T虚拟化设备故障切换如下图所示：



图表 30VIS6600T故障切换原理图

VIS6600T集群支持在线动态扩容节点，不影响现网业务的运行。VIS6600T集群支持最多8个节点，扩容时只需在阵列上把LUN映射给新增节点，并将新增节点接入集群的私有通信网络中。新增节点上电后，原有集群会自动检测到新增节点的加入，自动同步相关的配置信息并添加新增节点到集群中，便捷地完成集群的节点扩容。

当前VIS6600T集群不能满足日益增长的业务需求时，用户可以购买新的节点，对现有集群进行扩展。

■ 全局负载均衡（GSLB）技术

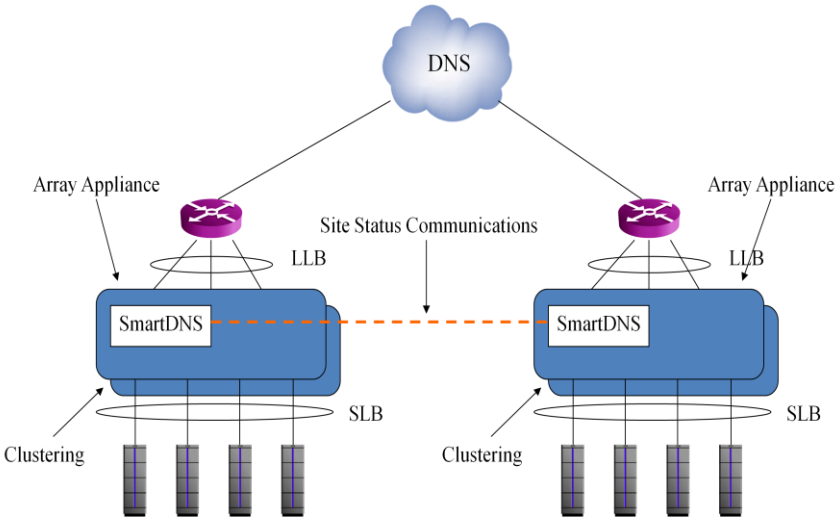
全局负载均衡（GSLB）在多个可提供相同服务的站点之间，根据相应的分配策略将用户请求“路由”到合适的站点上。Array GSLB的目的是在多个可提供相同服务的站点之间，根据相应的分配策略将用户请求分配到合适的站点上。Array TM（流量管理）提供高性能的GSLB功能Smart DNS。Smart DNS通过其内置的IP地址或网络对应表来实现用户的就近访问策略，当位于不同位置的Local DNS请求到达时，Smart DNS根据对用户的Local DNS策略判断用户所处的位置，可以返回距离用户最近的镜像站点的IP地址。

SmartDNS通过智能状态检测功能实现对链路、服务器健康状态的检测。检测的策略可以为Ping、TCP端口检测和内容检测，真正地检测服务器和链路的健康状态。对于因故障或检修而停止服务的服务器和链路从负载均衡组中去除，并继续检测链路和服务器的状态，一旦该链路或服务器恢复健

康，则将其再次加入负载均衡组。

在SmartDNS的内部，采用矩阵算法对服务器健康状态、网络健康状态、用户IP地理位置等参数进行综合计算，判断返回给用户的最佳镜像站点IP地址，使用户始终能得到最佳的网络服务。

对GSLB而言，最重要的一点是每一个Array TM需要知道其他TM所了解的服务、链路和系统状态信息，这一点是通过Array的SICP(状态信息通信协议)来完成的。SICP是Array公司的私有协议，主要完成GSLB服务器组中状态信息的交换，需要利用SLB、LLB的健康检查和状态监测功能。处在GSLB中的TM每隔几秒即可互相交换健康状态信息，还可以互相交换本地服务器负载、链路负载、网络状况等信息。这些状态信息主要包括链路可用性、服务可用性以及集群状态等。

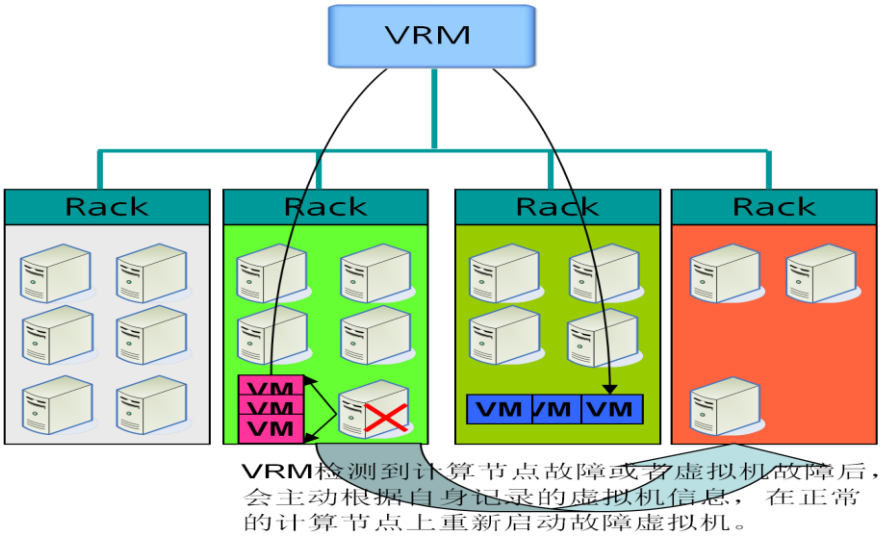


图表 31GSLB结构图

- FusionSphere HA技术

当CNA物理服务器宕机或者重启，系统可以将具有HA属性的虚拟机故障迁移到其他计算服务器，保证虚拟机能够快速恢复。

当计算服务器宕机后，由于单个集群内可以运行上千个虚拟机，为避免大量虚拟机迁移造成网络拥塞和目的服务器过载，系统会根据网络流量、目的服务器负荷选择将虚拟机迁移到不同的目的服务器。



图表 32虚拟机HA特性示意图

当VRM与CNA的心跳中断超过30秒则会触发虚拟机HA，当一个虚拟机有运行状态突然异常消失也会触发HA在其他正常的计算节点上快速恢复业务。在HA技术中，涉及以下关键技术：

- 防止脑裂：通过存储层面的锁机制防止同一个虚拟机实例在多个CNA上同时启动。
- CNA节点的掉电恢复：CNA节点掉电恢复后，业务进程开机自启动恢复，其上之前运行的虚拟机全部故障迁移至其他计算节点。

3.7 安全管理

3.7.1 适用场景

随着信息技术的发展，如Web2.0、SOA和云计算技术的涌现，以及移动设备、远程设备连接、浏览器以及各种应用程序的插件程序、智能终端、云主机的出现，为信息安全带来了新的挑战。网络外部与内部的攻击，以及系统漏洞仍然为信息安全最大威胁。攻击永远围绕最有价值的信息资产展开，作为信息最核心的节点，数据中心首当其冲。

随着云计算、以及数据中心的分布式部署，数据中心的组成元素也发生了一些变化，例如虚拟化、边界延伸。因此，一个体系化的分布式云数据中心安全解决方案必然应该覆盖所有组成元素，且安全元素支持逻辑隔离，而不能单用传统的技术手段、物理边界实现其全部的安全保障。

分布式云数据中心安全子系统根据业界最佳社会实践，结合自身多年来的项目积累，提取经验中的精华进行设计的。安全子系统架构目标如下：

■ **模块化**

从物理层安全、网络安全、主机安全、应用安全、虚拟化安全、用户安全、安全管理、安全服务八大块内容进行设计。安全架构可以根据客户实际的需求，可以快组合，形成满足用户实际需求的安全体系，更具针对性。

■ **端到端安全**

实现用户从接入、使用、完成退出的端到端的安全防护。通过提供基于双因素的认证技术、特权用户权限控制技术、vpn技术、应用防护技术、事件审计技术等，实现了用户对IT资源的安全访问控制，数据通信安全，应用安全访问，操作可以进行安全审核等，端到端地实现了安全保障。

- **低耦合**

涉及到数据、网络、应用等各个层面的安全防护，因此，涉及各种安全技术、安全产品，以及安全管理策略。但整个安全架构体系具备低耦合性的特点，各种安全技术之间不存在强关联性，各种安全产品不局限于特定的安全厂家和特定型号规格的产品，安全管理策略制定原则不依赖于具体安全的产品等。

- **逻辑隔离**

网络安全技术，如防火墙、Anti-DDoS、IDS、IPS、网络防病毒、WEB安全网关等支持1虚多，满足分布式云数据中心无清晰的物理边界的特点，构建安全的逻辑边界，全面保护虚拟数据中心（VDC）的安全。

- **易扩展**

为满足用户的安全需求而提出的一个指导性框架。用户可以根据该指导性框架结合其不同时期的安全需求进行相应的安全建设，在满足用户安全需求的同时，又保护了用户的投资价值。

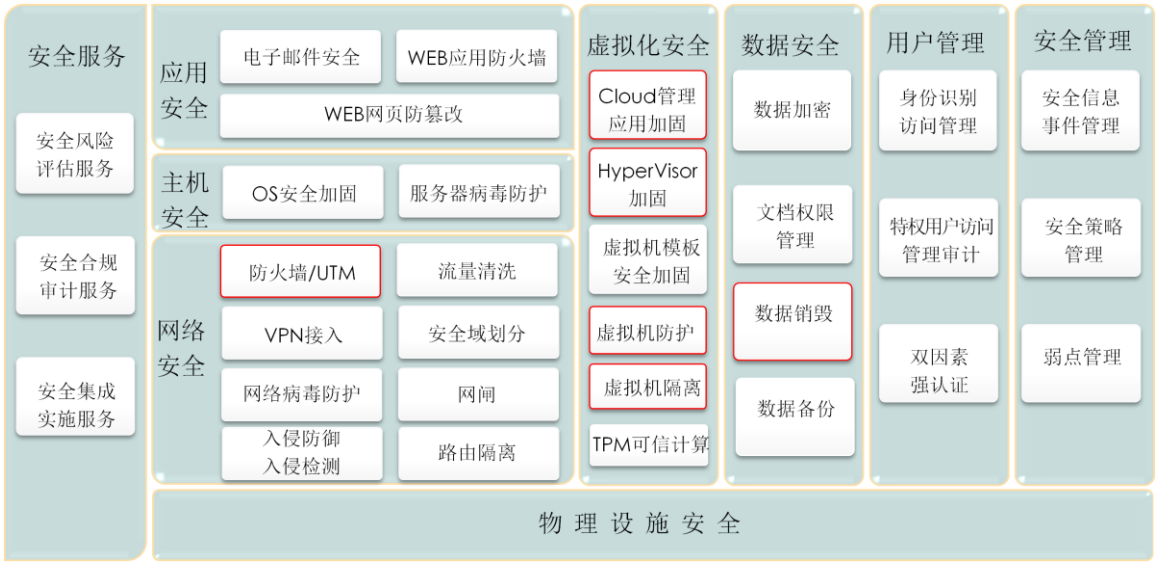
- **合规性**

分布式云数据中心安全方案从物理层、网络层、主机层、应用层、数据安全、用户管理、安全管理等方面进行了详实的设计，是建设高安全等级数据中心的最佳指导框架。同时，结合云计算的特点，补齐了虚拟化部分的安全设计，真正实现全面满足合规要求。

分布式云数据中心安全方案全面满足电子政务等级保护三级要求。

3.7.2 部署架构

分布式云数据中心从分层、纵深防御思想出发，根据层次分为物理设施安全、网络安全、主机安全、应用安全、虚拟化安全、数据保护、用户管理、安全管理等几个层面，全面满足用户的各种安全需求，安全子系统架构如下图所示，图中红框安全模块为分布式云数据中心基础安全模块：



图表 33安全子系统架构图

该架构中包含以下安全层面的能力：

- 物理设施安全：通过门禁系统、视频监控、环境监控等实现数据中心环境、物理访问控制等确保物理设施层面的安全；
- 网络安全：从防火墙、IPS、SSL VPN、Anti-DDoS、IDS/IPS、网闸等技术手段确保VDC边界和VDC内部系统、数据和通信的隔离和安全，不因偶然的或者恶意的原因而遭受到破坏、更改、泄露，系统连续可靠正常地运行，网络服务不中断。
- 主机安全：保护主机层操作系统的安全，通过主机加固、防病毒软件、主机IPS、主机补丁管理等技术手段确保主机免受攻击。
- 虚拟化安全：从虚拟层加固、Cloud管理应用加固和虚拟机隔离等技术手段确保虚拟化的安全。
- 应用安全：从电子邮件防护、Web应用防护等技术手段对应用层面的数据进行保护，保障用户的应用数据能够不受破坏、更改、泄漏、篡改。
- 数据安全：从数据加密、剩余数据防护、数据备份等技术手段保障数据安全。
- 用户管理：从特权用户访问审计等加强用户管理。
- 安全管理：从安全信息与事件管理等技术手段加强。
- 安全服务：从安全集成到安全评估、再到安全优化，阶段性的专业服务，为用户建立更安全的IT信息系统。

3.7.3 关键特性

1. 网络安全防护

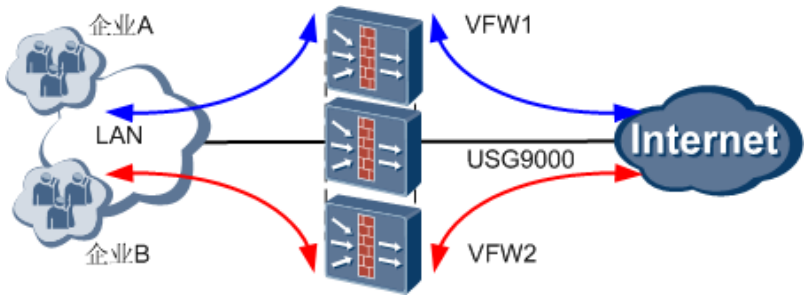
通过防火墙、IDS、IPS、VPN、Anti-DDoS攻击、网络防病毒网关、数据摆渡等技术手段，实现对网络系统中的系统和通信数据进行保护，不因偶然的或者恶意的原因而遭受到破坏、更改、泄露，系

统连续可靠正常地运行，网络服务不中断。

传统的物理边界的防护已经不能适应分布式云数据中心以VDC为主体的应用场景。为适应云技术的发展，网络安全产品已经逐渐演化为支持虚拟化，支持设备1虚多，提供网络安全逻辑隔离。目前应用最广泛的是虚拟防火墙技术。同时，基于云技术实现软件边界防火墙、安全组等网络安全特性，提供全面的网络安全防护。

1) 虚拟防火墙

虚拟防火墙是将一台防火墙划分多个为逻辑防火墙，每个逻辑防火墙能够独立为一个企业服务，提供私有网络，实现独立的安全保障，进而实现防火墙资源使用率的最大化。虚拟防火墙可以由物理防火墙或软件防火墙提供。



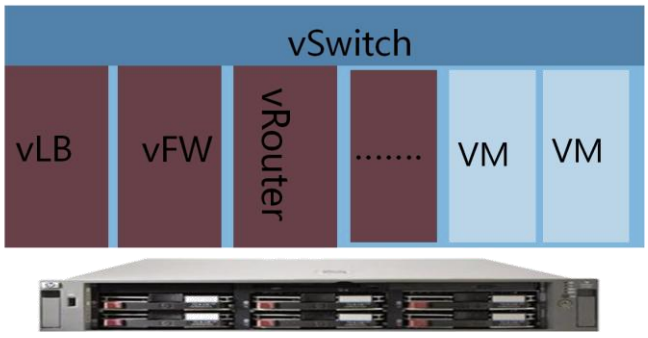
图表 34虚拟防火墙示意图

每台虚拟防火墙能够为用户提供私有的路由转发服务、安全服务和配置管理服务。

2) 软件虚拟防火墙VSA Virtual Service Appliance

华为虚拟化服务应用系统是软件的虚拟化网络边界网关，VSA部署在VM上。VSA提供以下功能：

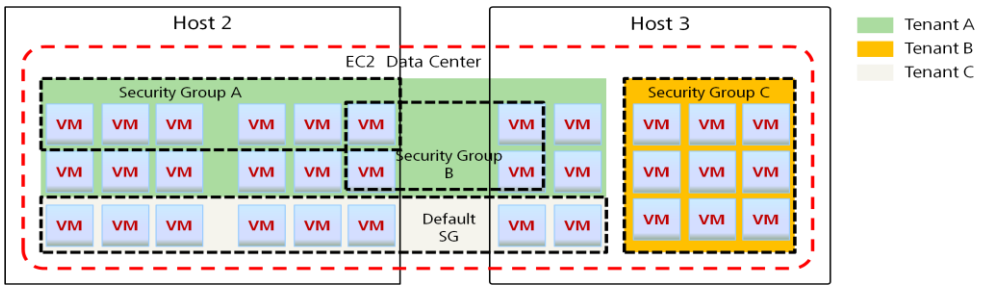
- VRouter/VFW，提供 L3 路由转发、OSPF/BGP、ACL、NAT、IPSec/GRE VPN。
- VLB，提供 TCP、HTTP、HTTPS 负载均衡，VLB 可以根据需要部署多个。



图表 35软件虚拟防火墙

3) 安全组

用户根据虚拟机安全需求创建安全组，每个安全组可以设定一组访问规则。当虚拟机加入安全组后，即受到该访问规则组的保护。用户通过在创建虚拟机时选定要加入的安全组来对自身的虚拟机进行安全隔离和访问控制。



图表 36安全组示意图

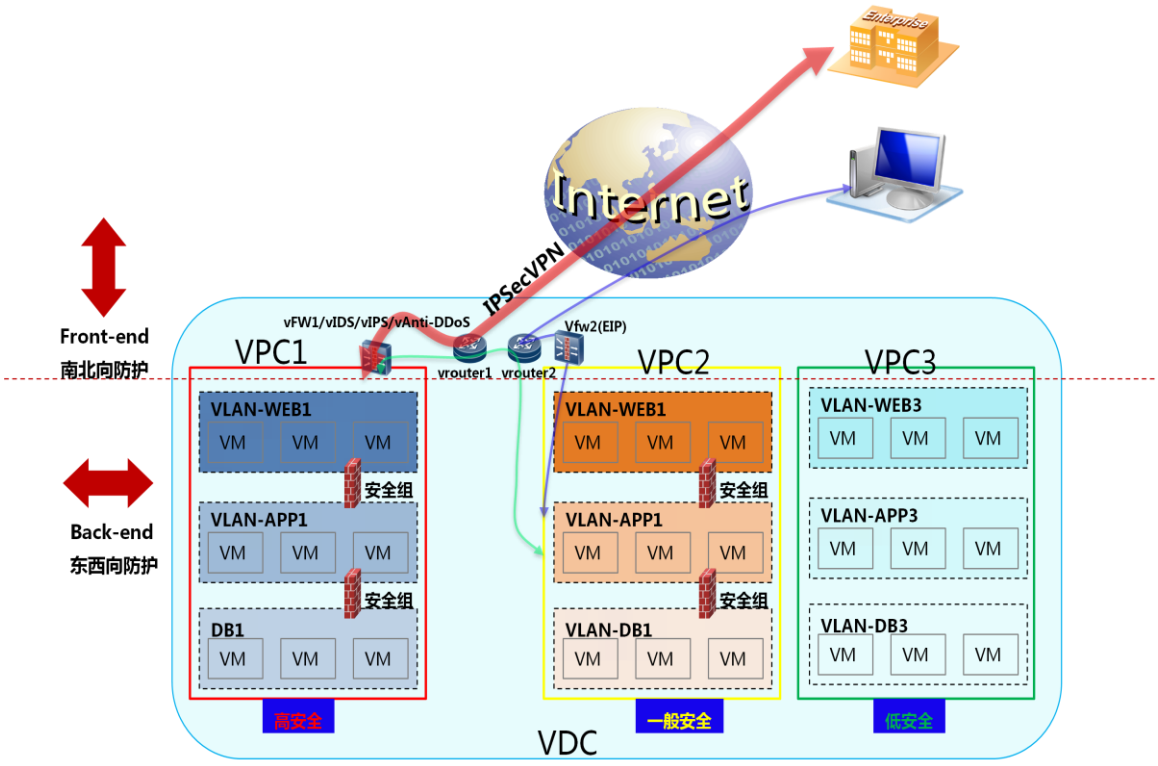
同一个安全组中的虚拟机可能分布在多个物理位置分散的物理机上，一个安全组内的虚拟机之间是可以相互通信，而不同的安全组之间的虚拟机默认是不允许进行通信的，可配置为允许通信。

4) 下一代防火墙统一威胁防护

华为下一代防火墙NGFW支持防火墙、VPN、IDS、IPS、Anti-DDoS、防病毒网关、垃圾邮件防护、WEB防护，并支持以上所有安全防护功能虚拟化。

5) VDC网络安全防护框架

VDC的边界部署VFW（可以是硬件防火墙一虚多，也可是软件VSA）和vIDS、vIPS、vAnti-DDoS等网络安全防护功能，防护VDC的南北向流量；VDC内部，VPC边界通过VFW，防护VPC之间的东西向流量；VPC内部，使用安全组，防护应用之间的东西向流量。



图表 37VDC安全防护框架

6) 防IP及MAC仿冒

通过IP和MAC绑定方式实现：防止虚拟机用户通过修改虚拟网卡的IP、MAC地址发起IP、MAC仿冒攻击，增强用户虚拟机的网络安全。具体技术能力包括通过DHCP snooping生成IP-MAC的绑定关系，然后通过IP源侧防护(IP Source Guard)与动态ARP检测（DAI）对非绑定关系的报文进行过滤。

7) DHCP隔离

支持对虚拟机的DHCP隔离，禁止用户虚拟机启动DHCP Server服务，防止用户无意识或恶意启动DHCP Server服务，影响正常的虚拟机IP地址分配过程。

8) 广播报文抑制

在服务器整合、桌面云等企业应用场景，如果发生网络攻击或病毒发作等引起的广播报文攻击，可能造成网络通信异常，此时可以开启虚拟交换机的广播报文抑制功能。

虚拟交换机提供虚拟机虚端口发送方向ARP广播报文和IP广播报文的抑制开关，以及抑制阈值设置功能。可以通过开启虚拟机网卡所在端口组的广播包抑制开关设置阈值，减少过量广播报文对二层网络带宽的消耗。

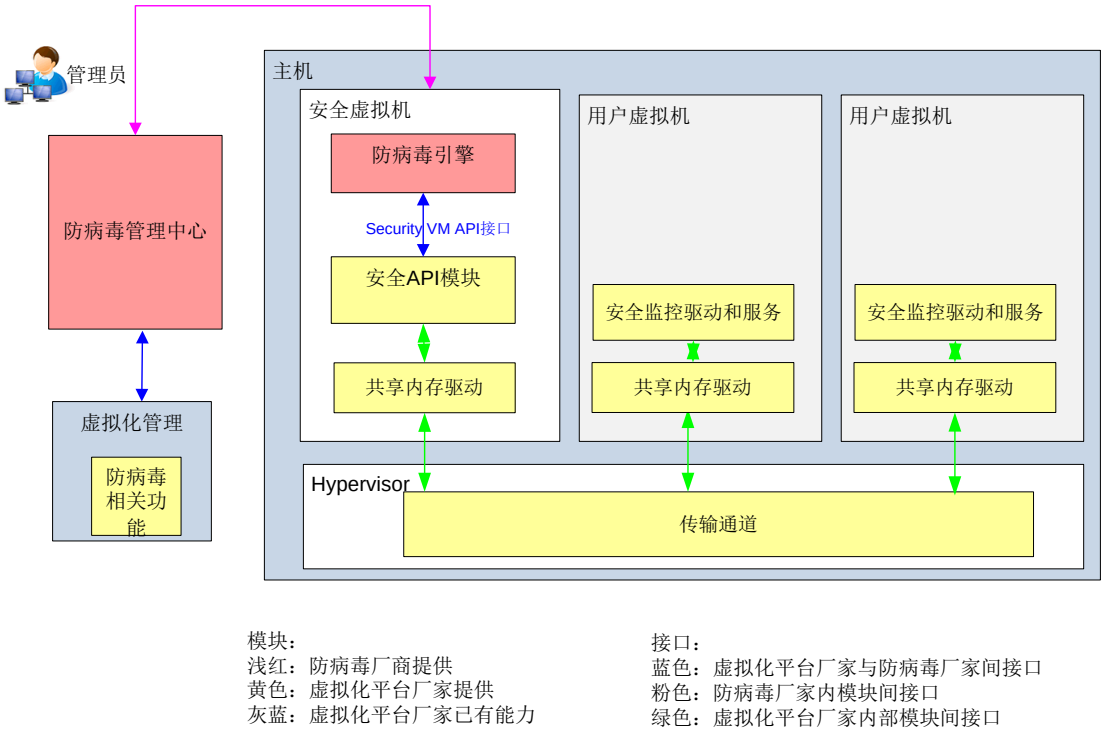
管理员可以通过系统Portal，基于虚拟交换机端口组对象，配置广播报文抑制开关、ARP广播报文抑制阈值、IP广播报文抑制阈值。

2. 虚拟化无代理防病毒

华为虚拟化平台（基于XEN虚拟化平台）提供了防病毒所需API，防病毒厂家可基于API进行二次开发，形成虚拟化防病毒解决方案，做到仅需在一台特殊的安全虚拟机中部署防病毒引擎，在用户虚拟机本地安装轻量级驱动即可完成杀毒。已经与瑞星、趋势科技、卡巴斯基虚拟化防病毒软件集成验证，支持windows云主机的无代理防病毒。

无代理防病毒有以下两个优势：

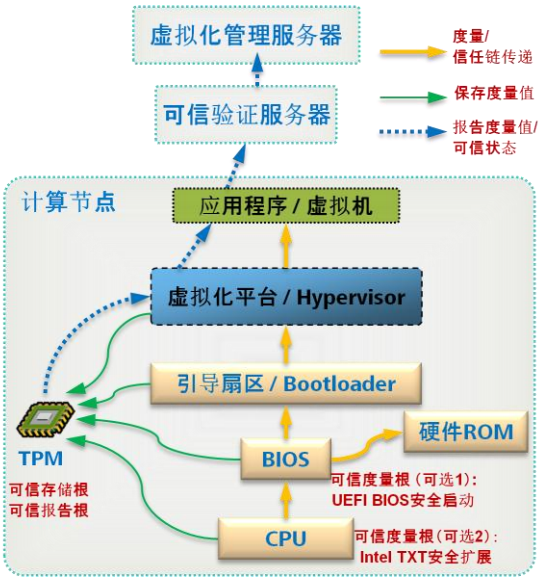
- 病毒库管理上的优势，即无需对每台虚拟机的病毒库安装、更新等进行管理，而是仅需对安全虚拟机进行管理；
- 病毒扫描结果在整个主机中所有虚拟机范围内共享，而不是如传统防病毒仅一台虚拟机内部共享，提升扫描效率。



图表 38虚拟化防病毒架构图

3. TPM完整性保护

云操作系统的裁剪加固和安全设置可以有效提升安全性，但不能完全杜绝编码的安全漏洞等带来的安全风险，因此，需要提供云操作系统完整性保护方案，以避免安全漏洞被利用。华为云平台（基于XEN虚拟化平台）支持基于硬件TPM芯片的完整性校验，保证主机和虚拟机的完整性不被破坏，以及破坏之后能够及时发现，采取一定的处理措施，从而更好的保护使用虚拟机的用户的数据。完整性保护方案确保虚拟化平台始终运行的是未经篡改的软件和正确的配置，TPM提供计算节点的信任根，从虚拟化OS启动、运行到主机OS的启动和运行，均基于可信根，通过可信信任链的一级一级传递进行完整性度量，提供可信虚拟机服务。



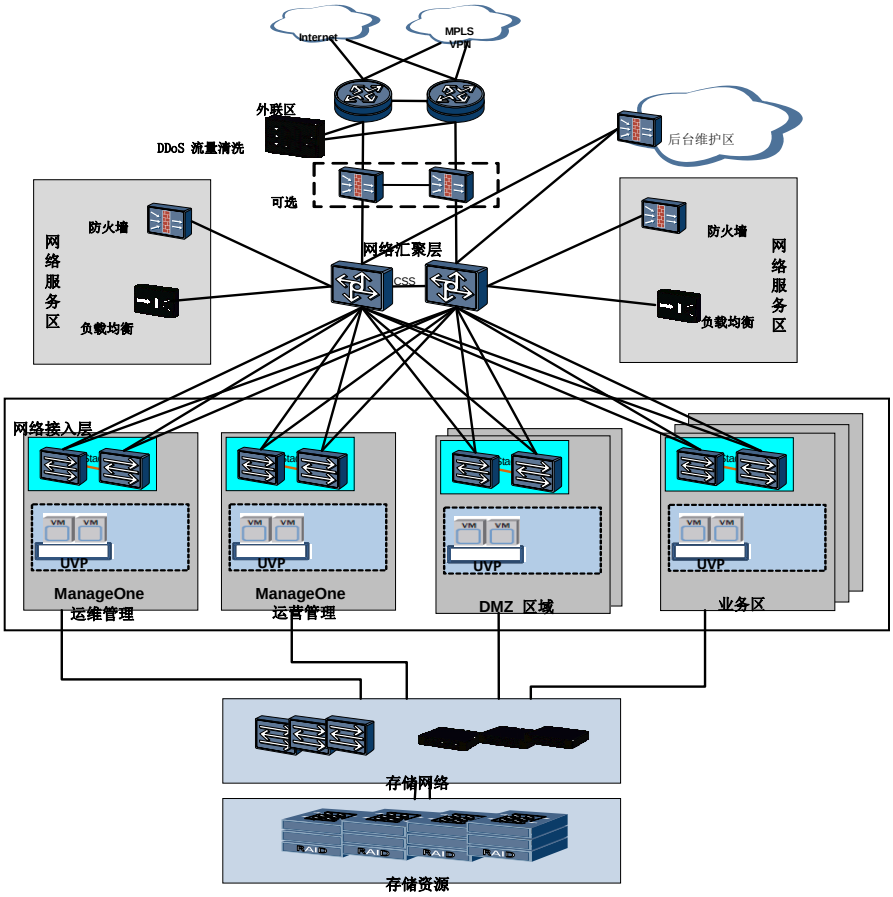
图表 39TPM可信计算架构图

4 典型部署场景

4.1 单 DC 部署

4.1.1 物理架构

扁平两级架构的物理部署如下所示：



图表 40 扁平两级架构物理部署图

4.1.2 架构概述

- IDC数据中心采用“扁平化”两级架构设计，内部交换结构简单明了，主要分层汇聚层和接入层。
- IDC数据中心根据组网逻辑功能划分为四大区域，包括外联区、核心区、网络服务区、接入区，其中外联区主要功能是对接Internet线路和接入网络；汇聚区是整个数据中心交换核心，由高性能交换机组成；网络服务区提供防火墙、负载均衡、VPN等IDC增值服务；接入区主要为数据中心服务器节点设备的接入。
- 汇聚层使用机框式交换机做集群，使用“多虚一”的技术，将多台交换机逻辑上虚拟成一台交换机，提高设备冗余。只需要一个管理IP即可对设备进行管理。
- 采用“CSS+istack+eth-trunk”提供可靠性、扁平两级网络无环、低收敛比的设计。

- 在汇聚层上使用VRF技术将各个网络区以及业务区域进行三层网络的逻辑隔离。
- 网络虚拟化功能提供虚拟防火墙、虚拟负载均衡功能、网络虚拟交换机，满足不同用户对虚拟化隔离的需求。
- 在接入层采用VLAN或者VXLAN技术实现二层网络隔离。
- 服务器接入可采用刀片服务器或者机架服务器，如果是刀片服务器则通过交换背板连接到核心交换机上；如果是机架服务器则需要通过接入交换机连接到核心交换机上。
- 存储采用FC SAN通过光纤交换机连接至服务器的存储平面端口，也可用IP SAN通过IP接入交换机连接至服务器的存储平面端口；所有服务器共享存储。形成统一存储资源池。

4.1.3 组件部署规格建议

表 2 单 DC 扁平两级网络部署配置表

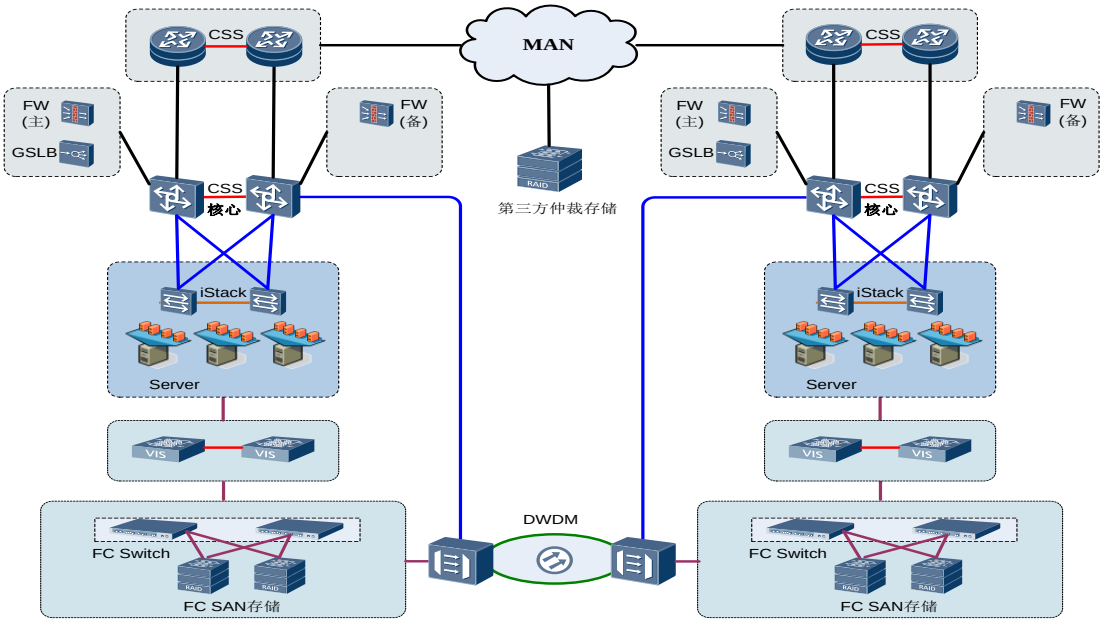
数据中心区域	设备类型	设备型号（运营商）	设备型号(企业网)	数量	组件重要性
汇聚区	交换机	CE12800	CE12800	2台	必选
	防火墙(选择一款即可)	E8000E-X	USG9500	2台	必选
		E1000E-X	USG5500	2台	必选
		E1000E-N	USG5500	2台	必选
	负载均衡器（F5）	BIGIP3900	BIGIP3900	2台	可选
		BIGIP6900	BIGIP6900	2台	可选
		BIGIP8900	BIGIP8900	2台	可选
接入区	接入交换机	CE6800、CE5800以及CE7800系列	CE6800、CE5800以及CE7800系列	按需	可选
服务器	刀片服务器	E6000、E9000（华为）		按需	可选
	机架服务器	RH2288、RH5885（华为）		按需	可选
存储网络区	FC交换机	SNS2000、SNS5000系列（华为）		按需	可选
	IP交换机	S5300、S6300、S6700、CE6800（华为）		按需	可选
存储资源区	SAN存储	OceanStor系列（华为）：		按需	可选

		S2600T、S5500T、S5600T、S5800T、S6800T、18000			
	NAS存储	OceanStor 9000系列（华为）		按需	可选
虚拟化软件	虚拟化平台	Vsphere5.0以上（VMware）		1套	可选
		FusionSphere3.1以上		1套	可选
数据中心管理软件	分布式数据中心管理软件	ManageOne2.1以上		1套	必选

4.2 双活容灾部署

4.2.1 物理架构

双活容灾物理结构如下：



图表 41双活容灾的物理部署

4.2.2 架构概述

- 生产、容灾站点之间通过L1专线(基于光纤直连的FC/以太端口二层直连)连接；
- 第三地仲裁盘推荐采用IPSAN，与生产、容灾站点间租用三层专网连接，有条件的客户也可以采用FCSAN并租用FC链路与生产、容灾站点相连；
- 管理网关（FusionSphere管理VLAN、VIS心跳VLAN、仲裁VLAN）、业务网关配置在汇聚交换机上；

- 异地三层网关之间（两对汇聚交换机，组成VRRP），业务归属地网关配置为VRRP主，VRRP的地址为虚拟机业务Subnet的网关地址；管理网关按照规划配置某地为VRRP主；
- 通过核心交换机与承载网的互联成二层，汇聚交换机与核心交换机机间通过二层连通，为了避免环路，多条站点间以太链路在核心交换机上捆绑配置成Trunk；
- 汇聚与核心交换机基于容灾VLAN，通过核心交换机与承载网二层连通；
- 汇聚交换机间，VLAN若重叠，需要在核心交换机上配置基于端口的VLAN映射；
- 数据中心对外的三层业务接入，需要在汇聚交换机上配置到核心交换机的三层互联（VLAN IF），然后以VLAN为单位在主网关侧的核心交换机发布精细路由，备网关侧核心交换机发布VLAN粗略路由，通过子网掩码控制精细度；
- 如果数据中心通过防火墙NAT/NAPT提供公有IP业务，需要防火墙对外发布公有IP地址路由。为保证按照网段路由方式进行路由优先级发布，要求提供的公有IP地址是标准的网段，同时生产、容灾两地提供相同公有IP地址段。

4.2.3 组件部署建议

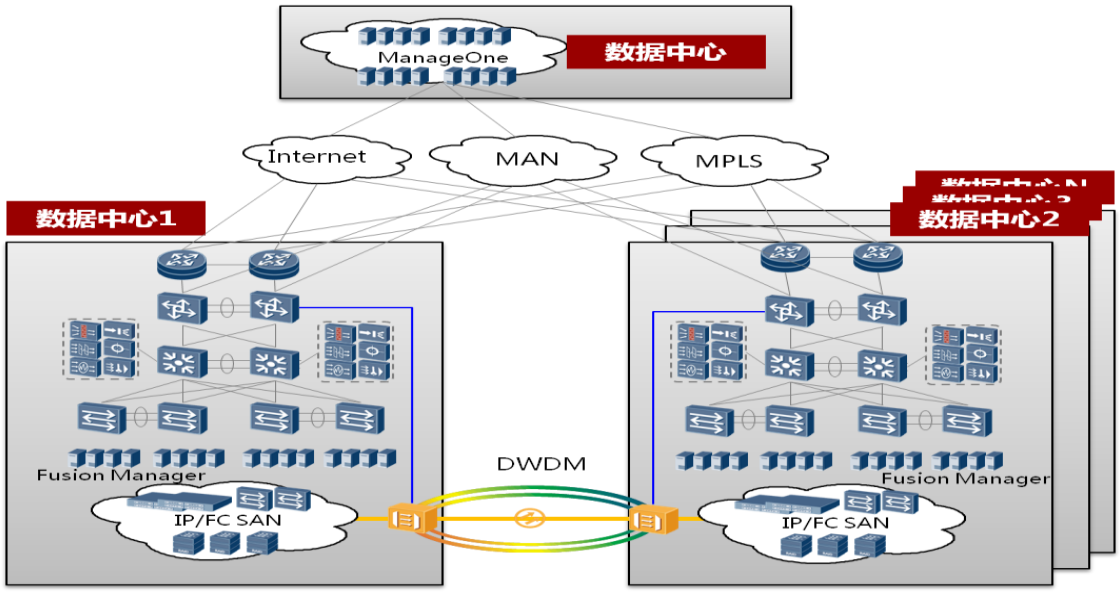
容灾数据中心场景下增加UltraVR容灾管理软件，同时需要增加存储远程复制License及快照License。双活数据中心场景下增加了VIS6000系列设备，使多个存储资源池形成一个统一的资源池，同时可异构其他厂商存储产品。管理软件使用1套，2个数据中心2套虚拟化平台。通过管理软件对数据中心资源进行统一管理和调度。

其他的组件部署参考单DC组件部署建议。

4.3 多 DC 分布式部署

4.3.1 物理架构

多数据中心的物理部署架构如下图所示：



图表 42多DC物理部署图

4.3.2 架构概述

- 管理部署

分布式云数据中心管理软件（ManageOne）放在第三地或者放在运营数据中心，通过专线方式管理其他数据中心，进行资源的统一分配和调度。

虚拟化管理软件（FusionManager）每个数据中心部署一套，由ManageOne统一管理。

管理软件下发业务过程中的数据流保证机密性、可靠性、低延迟。

- 数据中心间互联构架
  - 两个数据中心之间的互联可以通过Internet网络、MPLS网络、城域网、或者裸光纤互联。
  - 采用Internet和城域网互联时，采用三层路由互联。
  - 采用MPLS网络互联时，边界路由器需要做MCE，构建三层网络互联。

采用裸光纤互联时，通过核心交换机二层互联

4.3.3 组件部署规格建议

分布式云数据中心的管理软件使用1套，多个数据中心多套虚拟化平台。通过管理软件对数据中心资源进行统一管理和调度。其他的组件部署参考单DC组件部署建议以及双活容灾组件部署建议。