CloudFabric 云数据中心网解决方案

设计指南（云网一体化）

目 录

1 云网一体化场景概述

1.1 云网一体化的由来

传统数据中心的挑战

传统数据中心遇到了以下几个困境：

- 困境一：业务部署效率低。新业务上线时，需要大量规划、配置、测试、老业务影响评估等，部署时长无法满足新业务要求。
- 困境二：资源利用率低。很多系统独立占用资源池，形成烟囱式资源利用形态，当一个系统资源使用率低时，其他系统无法使用此资源池中多余的资源。
- 困境三：运维管理复杂。数据中心中多样化业务叠加运行，当某一业务故障时，很难快速发现并隔离故障。

SDN 和云计算可以来解决传统数据中心的上述困境。云化数据中心具有业务自动化、弹性资源池、精细化运维三个典型特征。

SDN 是用来支撑 ICT 实现云计算的关键技术。目前软件定义计算（虚拟服务器）、软件定义存储（分布式存储）已经具备，因此呼唤网络层面也必须实现软件定义网络，从而实现敏捷网络的目标。

云计算的分类

云主要分为私有云、公有云、混合云三类：

- 私有云是单个企业的一种专用云基础架构，其基础设施的定制化程度较高，突显了企业自身的业务特点。
- 很多中小型企业无法自己建设具有一定规模的云，因此转而向云服务提供商租用相关的基础设施和资源，从而迅速构建自己的虚拟数据中心，这就是公有云。

- 企业的一部分基础设施在公有云上，另一部分在私有云上，这两种云通过某种形式互通，实现应用可移植、数据可迁移等，这就是混合云。

表 1-1 中总结了公有云和私有云之间的区别。

表1-1 公有云和私有云的简要对比

云分类	关键区别	安全/合规	资源使用	基础设施	服务器规模	使用者
私有云	企业自建自用	严格	较粗放、以不计费居多	灵活、可定制	100~3K	大型企业
公有云	服务于公众	较弱	按使用量计费	标准化	一般大于10K	中小型企业

云数据中心的行业诉求

当企业的网络部门和 IT 部门已经有机结合，并具备一定技术实力，则可以考虑部署云网一体化方式的云化数据中心。

表 1-2 中总结了三个典型行业对云数据中心的诉求和业务场景。

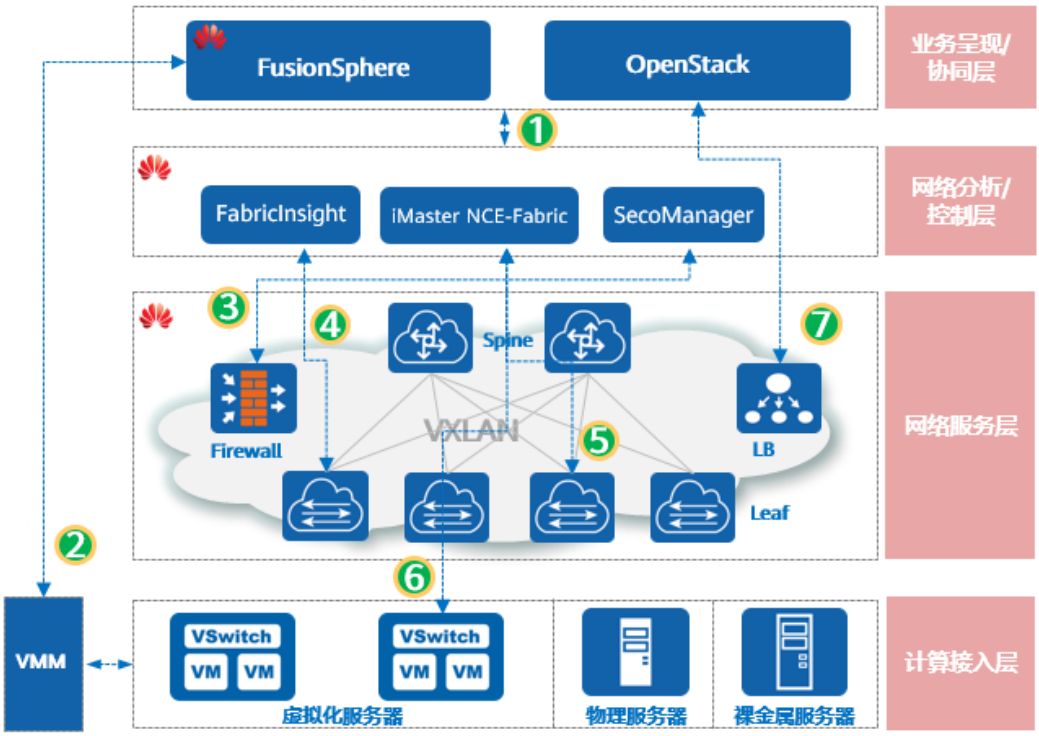
表1-2 典型行业对云数据中心的诉求

项目	政企/金融	运营商	互联网
业务场景	IT 计算池化、EDC 云化	机架出租、IDC 云化、NFVI 电信云	物理机/虚拟机/VPC 出租、提供 IaaS/PaaS 业务
网络核心诉求	1. 提升新业务 TTM 2. 部署复杂业务，降低 CAPEX 3. 业务可靠性保障，多活数据中心部署	1. 利用率：多数据中心网络资源整合 2. 标准化：多厂商 Fabric 互通、多厂商 VAS 兼容 3. 网络质量： 跨广域质量保证	1. 大规模服务器部署（10万+） 2. SLA 服务：租户级粒度、实时网络质量感知、主动运维 3. 新业务快速部署、网络支持业务弹性扩展

1.2 云网一体化简介

华为 CloudFabric 云数据中心网解决方案中的云网一体化方案，其逻辑分层架构如下图所示。

图1-1 云网一体化逻辑分层架构示意图



逻辑分层

层次	说明
业务呈现/协同层	支持对接社区或第三方商业 OpenStack 云平台+第三方云管理平台。支持对接华为 FusionSphere 云平台+华为 ManageOne 云管理平台。用户的操作界面一般在云管理平台上。
网络控制层	控制器北向与 OpenStack Neutron 对接，实现云平台业务模型参数向控制器的下发。控制器南向支持 OpenFlow/OVSDB/Netconf/SNMP 等接口，统一管理控制物理和虚拟网络，完成网络配置的自动化下发。 SecoManager 纳管华为防火墙，提供 L4~L7 策略业务发放。 FabricInsight 提供流量数据采集、网络故障分析功能。
网络服务层	由物理设备组成的 Spine-Leaf 基础物理组网（常见的有华为 CloudEngine 系列交换机、NGFW、vNGFW、LB 等），用以承载 VXLAN Overlay 网络，并由物理或虚拟设备提供 VAS 服务。
计算接入层	• 虚拟化服务器：虚拟机的上线信息由云平台通知给控制器。 • 物理服务器：通过 L2BR 接入到 VXLAN 网络，通过控制器界面来发放接入配置，云平台不感知。 • 裸金属服务器：一般形成一个裸金属服务器池；由云平台触发裸金属服务器的端到端上线过程。

交互接口

图中序号	接口两端	接口说明
1	控制器<->云平台	控制器提供插件部署在云平台上，从而完成云平台与控制器提的对接。控制器提通过 RESTful（控制器北向开放的接口）和 RESTConf 接口（控制器调用的接口）与云平台对接，接收云平台下发的网络业务指令。
2	云平台<->VMM	云平台与 VMM 间接口，控制流不经过控制器提传递。
3	SecoManager<->防火墙	• SNMP：用于 SecoManager 发现和获取防火墙的信息。 • NETCONF：用于 SecoManager 向防火墙下发配置。
4	FabricInsight<->物理交换机	• SNMP：用于 FabricInsight 发现和获取物理交换机的信息。 • NETCONF：用于 FabricInsight 与物理交换机进行流镜像同步。 • gRPC：FabricInsight 获取交换机 CPU、RAM 利用率。 • Netstream：交换机通过 Netstream 上送指定流 分析结果。
5	控制器提<->物理交换机	• SNMP：用于控制器提发现和获取物理交换机的信息。 • NETCONF：用于控制器提向物理交换机下发配置。 • OpenFlow：主要在运维层面提供路径探测等功能。
7	LB<->云平台	LB 提供补丁部署在云平台上，同时本身部署相应的插件，两者通过 RESTFul 接口对接，从而使云平台纳管 LB 设备，并向 LB 设备下发配置。 控制器提在云平台上的插件和 LB 在云平台上的插件会交互信息，由控制器提告诉 LB 流量应该携带哪一个 VLAN 标签进入到 Fabric 网络中。

1.3 Overlay 网络类型和对比

在 VXLAN 网络中，根据承担 Overlay 边缘设备（VXLAN NVE）属性的不同，又可以分为 Network Overlay、Host Overlay、Hybrid Overlay 三种网络类型。CloudFabric 解决方案推荐使用 Network Overlay 类型的 VXLAN 网络。

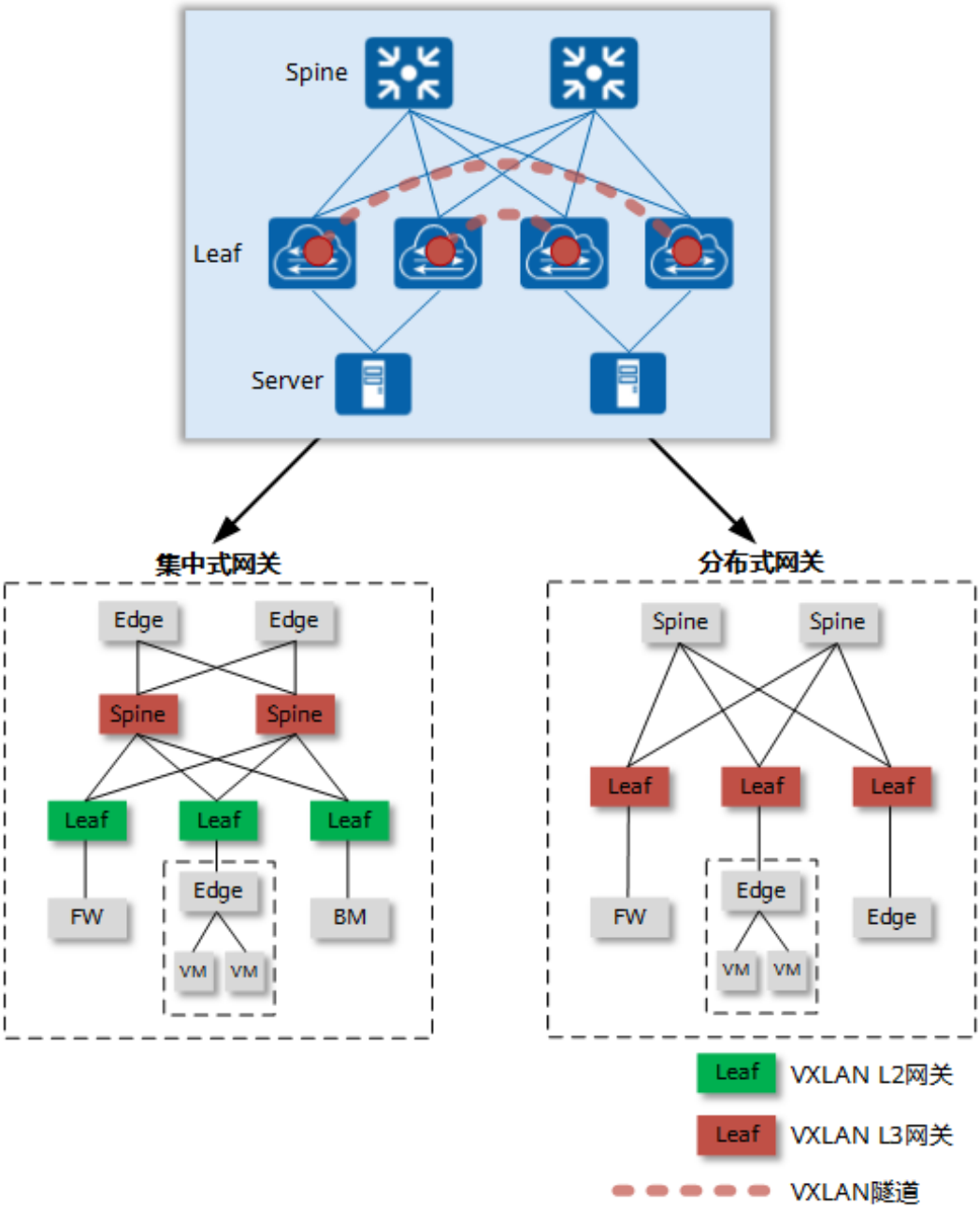
- Network Overlay：所有 NVE 全部由物理交换机承担。
- Host Overlay：所有 NVE 全部由 vSwitch 承担。
- Hybrid Overlay：NVE 一部分部署在物理交换机上，另一部分部署在 vSwitch 上。

Network Overlay

Network Overlay 的特点是 VXLAN 隧道的两个端点全部是物理交换机。其中，Network Overlay 有分为集中式和分布式两类，如图 1-2 所示。

- 集中式 Network Overlay 中，Leaf 作为 VXLAN 的 L2 网关、Spine 或 Border Leaf 作为 VXLAN 的 L3 网关。
- 分布式 Network Overlay 中，Leaf 同时作为 VXLAN 的 L2 和 L3 网关，Spine 仅作为 IP 流量高速转发节点，不处理 VXLAN 报文。

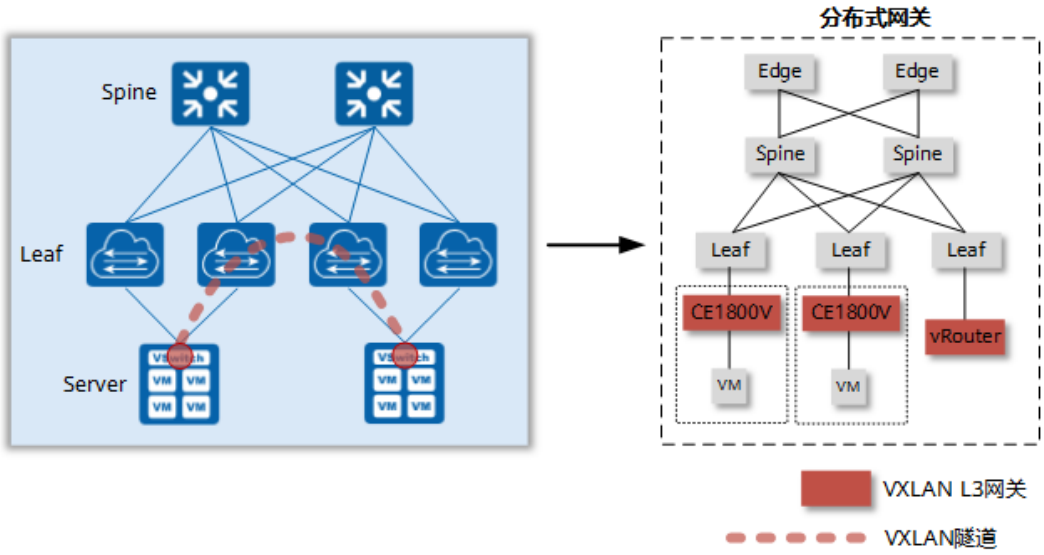
图1-2 Network Overlay 及其集中式和分布式示意图



Host Overlay

Host Overlay 的特点是 VXLAN 隧道的两个端点全部是虚拟交换机，而虚拟交换机部署在服务器上，如图 1-3 所示。数据中心内部的东西向流量在虚拟交换机之间通过 VXLAN 隧道转发；南北向流量在虚拟交换机与虚拟路由器之间转发，作为 Leaf 和 Spine 的物理交换机仅作 IP 报文的高速转发，不处理 VXLAN 报文。

图1-3 Host Overlay 示意图

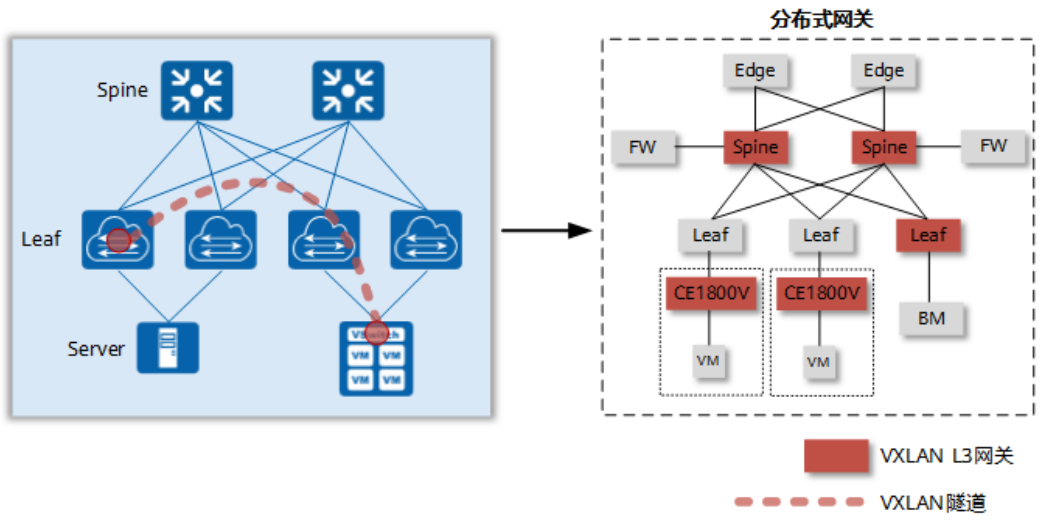


Hybrid Overlay

Hybrid Overlay 的特点是 VXLAN 隧道的端点既可以是虚拟交换机也可以是物理交换机，因此也称为混合 Overlay，如图 1-4 所示，混合 Overlay 常见的是分布式的。

数据中心内部的东西向流量在虚拟交换机和物理 Leaf 交换机之间通过 VXLAN 隧道转发；南北向流量在虚拟交换机/Leaf 物理交换机与 Spine/Edge 之间通过 VXLAN 隧道转发。

图1-4 Hybrid Overlay 示意图



网络类型对比

表 1-3 中对 Network Overlay、Host Overlay 和 Hybrid Overlay 三种类型的网络特点进行了对比。

表1-3 Network Overlay、Host Overlay 和 Hybrid Overlay 对比说明

对比项	Network Overlay	Host Overlay	Hybrid Overlay
NVE	硬件交换机	vSwitch	• 硬件交换机 • vSwitch
VXLAN L3 GW	硬件交换机（分布式部署，根据 VM 上线位置相应的部署）	vSwitch（分布式部署，根据 VM 上线位置相应的部署）	• 硬件交换机 • 和 vSwitch（分布式部署，根据 VM 上线位置相应的部署）
接入服务器类型	虚拟化服务器、物理服务器	虚拟化服务器	虚拟化服务器、物理服务器
接入 L4~L7 类型	• 硬件 L4~L7 • 软件 L4~L7（X86 物理服务器） • 软件 L4~L7（SRIOV 接入）	软件 L4~L7（vSwitch 接入）	• 硬件 L4~L7 • X86 物理服务器软件 L4~L7 • SRIOV 虚拟化软件 L4~L7 • 软件 L4~L7（vSwitch 接入）
控制面	• 设备 L2/L3 自学习 • 设备间 L2 通过头端复制广播自学习 • 可支持控制面上收控制器（特指 ARP/ND 及路由。当前未合入主线，可 POC 测试） • 可支持设备间通过 BGP-EVPN 同步	• vSwitch 通过 openflow 将 ARP/ND 上报控制器， • 控制器 L2/L3 学习 • vSwitch 间通过控制器下发流表同步	• 硬件设备 L2/L3 本地自学习， • 硬件设备间通过 BGP-EVPN 同步 • vSwitch 通过 OpenFlow 将 ARP/ND 上报控制器，控制器 L2/L3 学习，vSwitch 间通过控制器下发流表同步 • 硬件 NVE 和 vSwitch NVE 之间通过控制器的 BGP-EVPN 同步
转发性能	不占用服务器 CPU 资源，硬件设备转发性能高	VXLAN 处理占用服务器 CPU 资源，性能受 CPU 影响大	硬件部分不占用服务器 CPU 资源，软件部分 VXLAN 处理占用服务器资源
虚拟机规格	• VPC 数量受限于 TOR VRF 和路由规格 • 同一 VPC 虚机数量受	• 仅受限于控制器的能力 • 海量 VPC，海量虚机	• 海量 VPC，海量虚机 • 同一 VPC 虚机数量受

对比项	Network Overlay	Host Overlay	Hybrid Overlay
			限于 TOR 表项规格

	限于 TOR 表项规格		
适用场景	• 适用于对转发性能、运维、安全等有很高要求的私有云用户 • 适用于虚拟化服务器/物理服务器同时接入 • SDN 网络与传统网络互联互通	• 适用于仅虚拟化服务器接入 • 适用于租户规模超大的用户 • 网络内有多个厂商网络设备，需要 VXLAN 与硬件网络设备解耦	• 适用于虚拟化服务器/物理服务器同时接入 • SDN 网络与传统网络互联互通 • 对硬件成本敏感，强调网络利旧，需要 VXLAN 与硬件网络设备解耦

2 设计云网一体化类型的数据数据中心

2.1 业务模型与概念

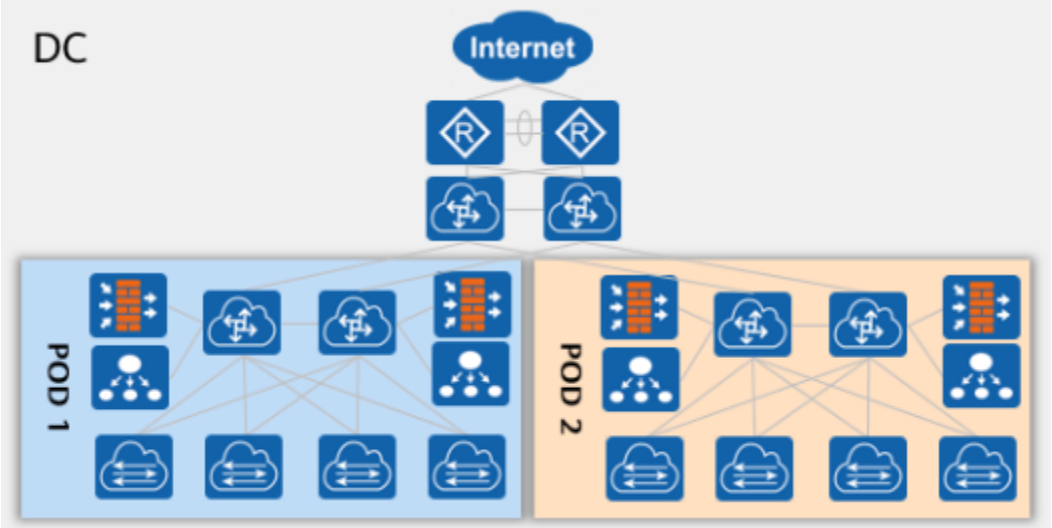
2.1.1 常见概念解释

DC、POD 和 AZ

DC：Data Center，数据中心。DC 是物理概念，是指在一个物理空间（比如机房）内实现信息的集中处理、存储、传输、交换和管理。服务器、存储和网络设备是 DC 的关键设备，供电、制冷、消防、监控等基础设施是 DC 的关键配套。

POD：Point of Delivery，分发点。为了便于 DC 的资源池化操作，可将一个 DC 划分为一或多个物理分区，每个物理分区就称为一个 POD，如图 2-1 所示。由此可见，POD 也是物理概念，是 DC 的基本部署单元，一台物理设备只能属于一个 POD。

图2-1 DC 和 POD 示意图



AZ：Availability Zone，可用区域。AZ 是一个计算侧的逻辑概念，代表了一个故障隔离区域。比如一些主机共用了一套电源和网络设施，当这套设施出现故障时，这部分资源就全部不可用了。在规划时，AZ 与 DC 可按实际部署情况灵活映射。例如在大规模公有云中，一个 AZ 可包含多个 DC；在中小规模私有云中，一个 DC 内可设置多套独立的 AZ；也可将一个 DC 规划为一个 AZ，这时 DC 与 AZ 是等同的。

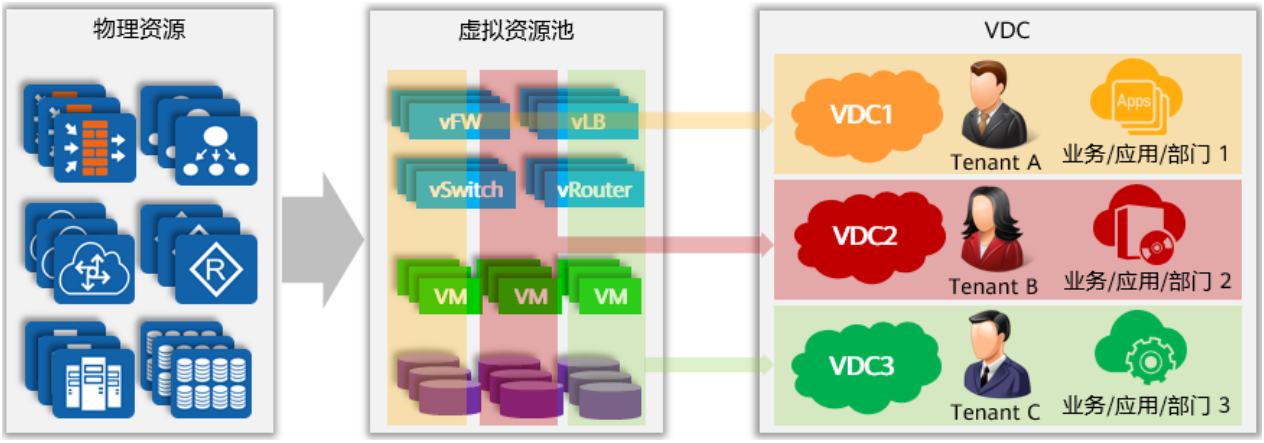
VDC 和 Tenant

VDC：Virtual Data Center，虚拟数据中心。VDC 是一个组织可使用资源的集合，一般包括计算、存储和网络资源。

Tenant：租户，由系统管理员创建和分配。租户是一个 VDC 的实际拥有者和管理者，不同 VDC 对应不同的租户，如图 2-2 所示。

- 在公有云场景，系统管理员可以定义 VDC 并为 VDC 分配管理员，只有该 VDC 的管理员才可管理该 VDC 下的资源。
- 在私有云场景，VDC 可以灵活定义，分配给一个业务/应用/部门。系统管理员可以通过 VDC 对企业内的不同业务/应用/部门进行不同等级的资源配额管理。

图2-2 VDC 和 Tenant 示意图

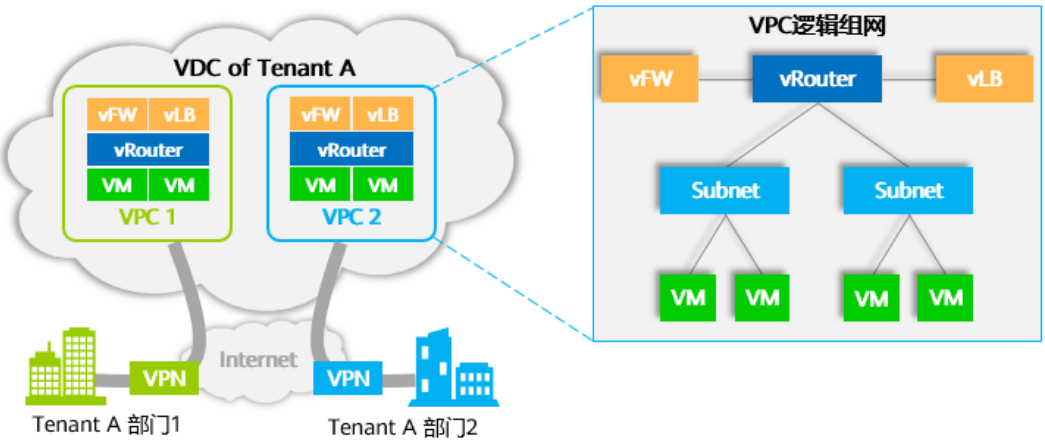


VPC

VPC：Virtual Private Cloud，虚拟私有云。基于物理网络中抽象出来的逻辑网元，并根据业务的实际情况，编排这些逻辑网元，从而形成一个虚拟的网络。不同 VPC 之间是逻辑上隔离的，但是都共用一套物理网络，从而实现了物理网络资源资源池化以后的共享问题。

可以将 VPC 理解为一种“容器”，VPC 中提供了 vRouter、Subnet、vFW、vLB 等逻辑元素，租户可以根据自己的需要，在一定的规则下灵活组合这些元素，例如需要几个网段，每个网段中接入多少台 VM，VM 流量需要配置什么样的安全策略和负载策略等，典型部署方式如图 2-3 所示。

图2-3 VPC 和 VPC 内部逻辑元素示意图



VPC 有以下特点：

- VPC 使用 VDC 中的资源，一个 VPC 只能属于一个 VDC，而一个 VDC 可包含多个 VPC。每个 VPC 为一个安全域，对应于一个业务/应用/部门。

- VPC 提供隔离的虚拟机和网络环境，满足不同业务/部门的网络隔离要求。

- 每个 VPC 可提供丰富的独立业务，例如 vFW、vLB、安全组、EIP、IPsec VPN、NAT 等。
- VPC 可提供直联网络、路由网络和内部网络等多种组网模式。

VPC 中常见的元素有以下几种：

- vRouter：作为业务子网的网关，用于子网间的三层互通。一个 VPC 只能有一个 vRouter
- Network：定义为一个二层网络，通常只含一个 Subnet，在 Share 模式下可包含多个 Subnet。（Share 模式映射到交换机上为一个接口下启用多个从 IP，用于划分不同网段，例如多个小型租户共用一个 VLAN 的场景）

  注：FusionSphere 模型不支持 Share 模式，开源的 OpenStack 模型中是呈现此元素的。
- Subnet：用于二层广播域的隔离，对应于一个子网网段。同一 VPC 内不同 Subnet 的三层网关，都在同一个 vRouter 上。同一 Subnet 内默认互通；不同 Subnet 间默认互通，也可通过配置安全组进行隔离
- vFW：作为 VPC 的边界，除了可提供外部访问 VPC 内的安全访问控制，还可提供外部访问 VPC 内的接入服务，可提供的特性有：FW、EIP、SNAT、IPsec VPN 等。
- vLB：用于对外提供内部服务器间的负载均衡能力，一个 vLB 可以带多个监听器，用户可给不同业务申请不同的监听器。

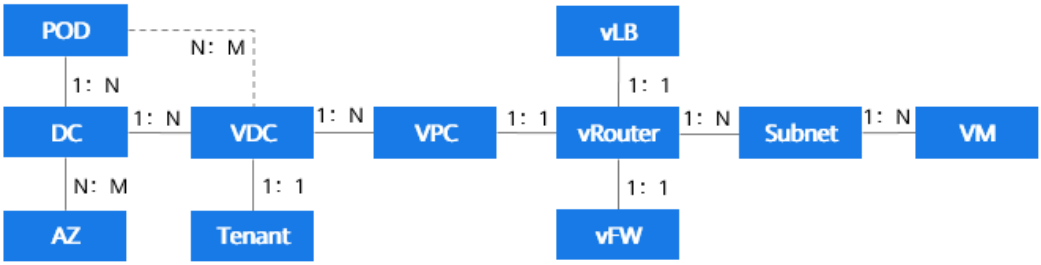
2.1.2 FusionSphere 和开源 OpenStack 业务模型简介

FusionSphere 业务模型简介

FusionSphere 是华为公司的云平台，基于开源 OpenStack 来开发，并在此基础上进行了商业加强，因此很多基本概念与开源 OpenStack 是类似的。

FusionSphere 业务模型的内部映射关系如图 2-4 所示。

图2-4 FusionSphere 业务模型的内部映射关系



POD 是物理单元，比如可将一个 Fabric 网络视为一个 POD，作为承载业务的基本部署单元，一套资源可部署在一个或多个 POD 内，而一个 POD 也可承载多套资源。

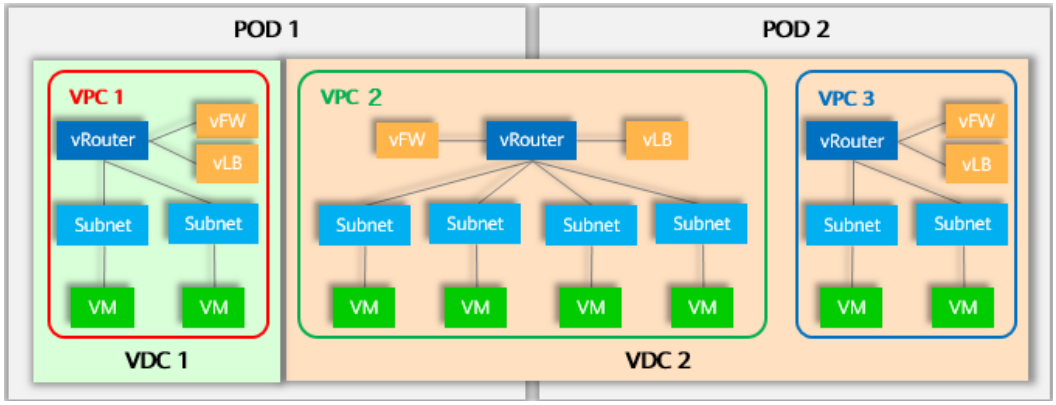
VDC 是资源单元，于租户对应。VDC 支持跨 POD 部署，租户以 VDC 为粒度进行资源租用。一个 VDC 中可以有多个 VPC。

VPC 是业务单元，VPC 支持跨 POD 部署，同一租户的不同 VPC 也可部署在不同 POD 内。一个 VPC 对应一个 vRouter，一个 vRouter 在交换机上就表现为一个 VRF。

vRouter 是 VPC 中的一个逻辑单元，与 vLB、vFW 之间是 1:1 的关系；一个 vRouter 可以连接多个 Subnet，一个 Subnet 可连接多台 VM。

上述业务模型之间的典型部署关系如图 2-5 所示。

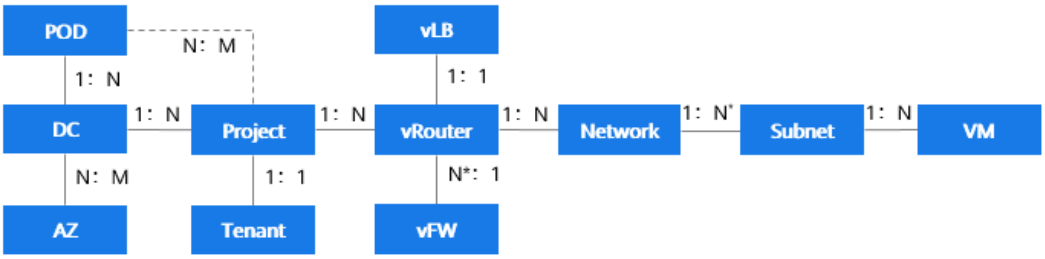
图2-5 FusionSphere 业务模型部署关系



开源 OpenStack 业务模型简介

OpenStack 的业务模型和 FusionSphere 的业务关系有少量的不同，开源 OpenStack 业务模型的内部映射关系如图 2-6 所示。OpenStack 内部的业务模型和部署关系中，重点介绍一下 POD 和 Project。

图2-6 开源 OpenStack 业务模型的内部映射关系



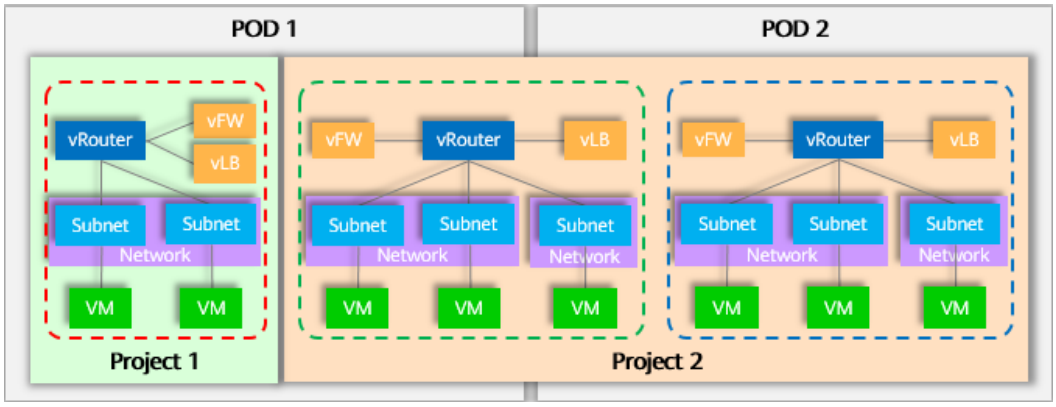
POD 是物理单元，比如可将一个 Fabric 网络视为一个 POD。作为承载业务的基本部署单元，一套资源可部署在一或多个 POD 内，而一个 POD 也可承载多套资源。

Project 是资源单元，对应于租户。Project 支持跨 POD 部署，租户以 Project 为粒度进行资源租用。在 Project 中，以 vRouter 为核心部署不同的业务单元。业务单元可跨 POD 部署，同一租户的不同业务单元也可部署在不同 POD 内。

一个 Project 中可以包含多个 vRoute，一个 vRouter 可以连接多个 Network，一个 Network 可以连接多个 Subnet（类似于一个 VLAN 三层接口可以配置 Secondary IP 地址），一个 Subnet 可连接多台 VM。

上述业务模型之间的典型部署关系如图 2-7 所示。

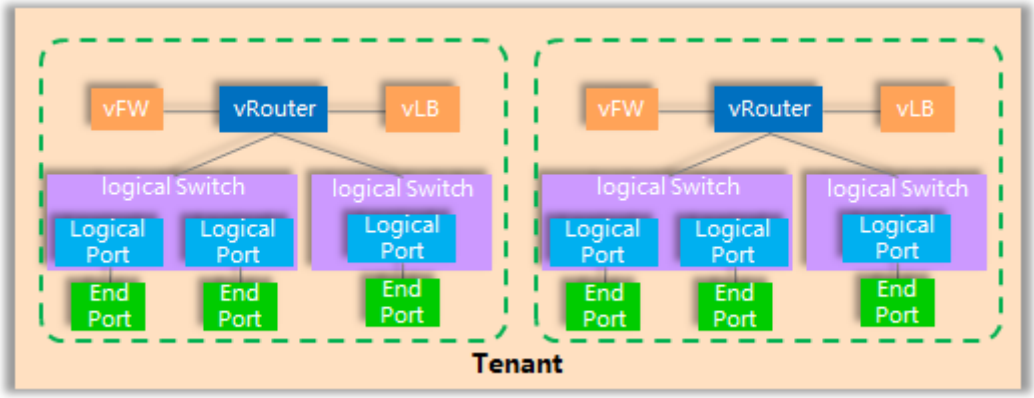
图2-7 OpenStack 业务模型部署关系



2.1.3 控制器业务模型简介

如图 2-8 所示，控制器的基本业务模型中包含了 Tenant、VPC、Logic Router、Logic Switch、Logic FW 和 Logic LB。

图2-8 控制器的业务模型示意图



在控制器中，管理员可以将一定数量的 VPC 授权给 Tenant（租户）使用，并授权 Logic Router、Logic Switch、Logic FW 和 Logic LB 的使用限额。其中，Logic Router、Logic Switch、Logic FW 和 Logic LB 就提供了 FaaS（Fabric As a Service），即将网络抽象成了多种服务。

控制器中定义的 Logic Router 对应云平台的 vRouter；Logic Switch 对应云平台的 Network/Subnet；Logic FW 和 Logic LB 分别对应云平台的 vFW 和 vLB。控制器中定义 logical port 标识物理机交换机上的逻辑接口；End Port 是用来模拟链接到 Logic Switch 上的逻辑接入点，可以是 VM，也可以是物理服务器或第三方设备，可以配置 EndPort 的接入信息。

表 2-1 中针对 FusionSphere、开源 OpenStack 和控制器的业务模型，从资源管理层、逻辑组织层、网络实体层、计算实体层进行对比。

- 资源管理层：本层将数据中心资源以租户粒度进行分配，并指定相应的租户管理员，是基本的资源单元。
- 逻辑组织层：本层是网络和计算实体的逻辑组织，是基本的业务单元，各业务单元之间的网络是安全隔离的。
- 网络实体层：一个业务单元中包含的各种网络实体在本层予以呈现。
- 计算实体层：一个业务单元中包含的所有计算实体在本层予以呈现。

表2-1 FusionSphere、开源 OpenStack 和控制器之间业务模型的对比信息

项目	资源管理层	逻辑组织层	网络实体层	计算实体层
OpenStack	Project/Tenant	无	External Network vRouter Network/Subnet vFW/vLB	VM
FusionSphere	VDC/Tenant	VPC	External Network vRouter Subnet vFW/vLB	VM
控制器	Tenant	VPC	External Network Logic Router Logic Switch Logic FW/Logic LB	End Port

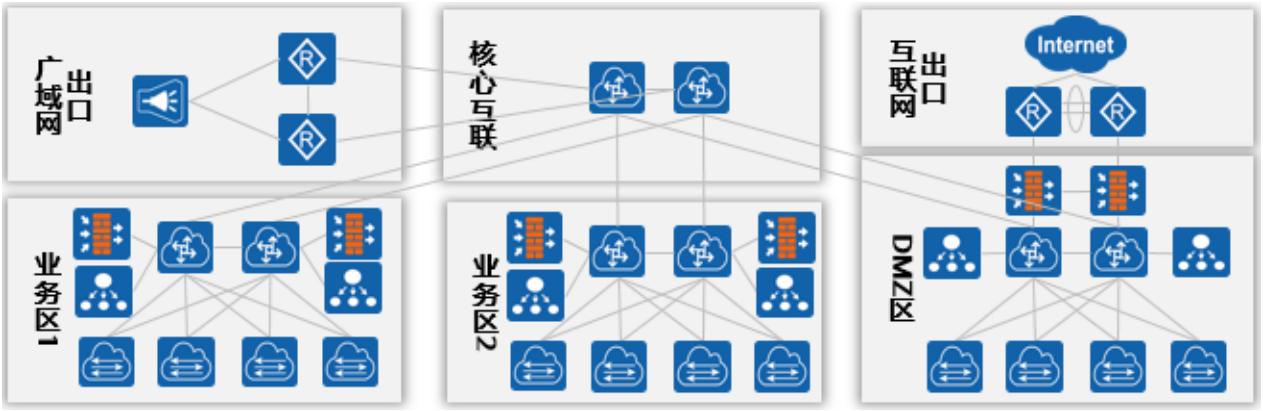
2.2 业务规划设计流程和原则

业务规划的一般流程

1. 网络管理员先基于业务特点，划分物理网络的分区，并进行分区内物理网络的设计。典型的网络分区划分如图 2-9 所示，分为业务区、核心互联区、DMZ 区、出口区等。

   注：在 CloudFabric 解决方案中，物理网络的分区设计一般建议与控制器中的 Fabric 相对应，控制器编排界面中的 Fabric 是指一组位于同一 VXLAN 路由域内的网络设备，组网上通常采用 Spine-Leaf 架构，Fabric 内所有业务可共用相同的出口网络资源和 L4-L7 网络资源；基于以上原则，建议网络分区的按控制器中的 Fabric 定义范畴进行设计，也支持将多个 Fabric 属性相同的分区划分为一个 Fabric。

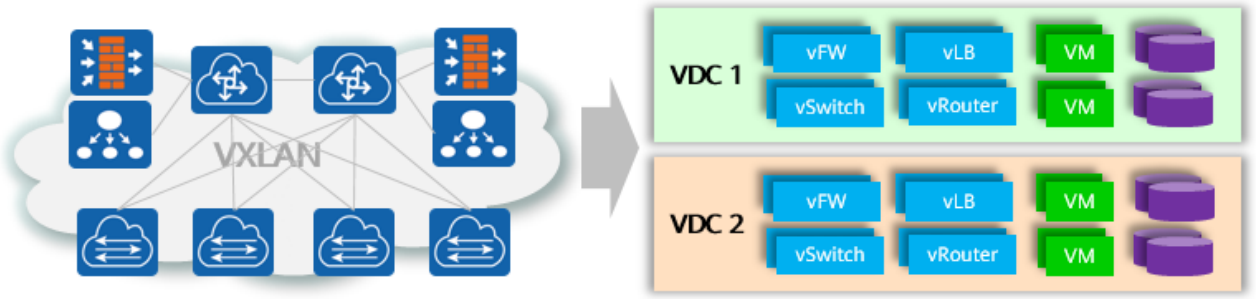
图2-9 典型的物理网络分区设计



被控制器纳管的网络分区推荐采用各种 Leaf 角色相互解耦的组网方式，并部署分布式 VXLAN 网关。

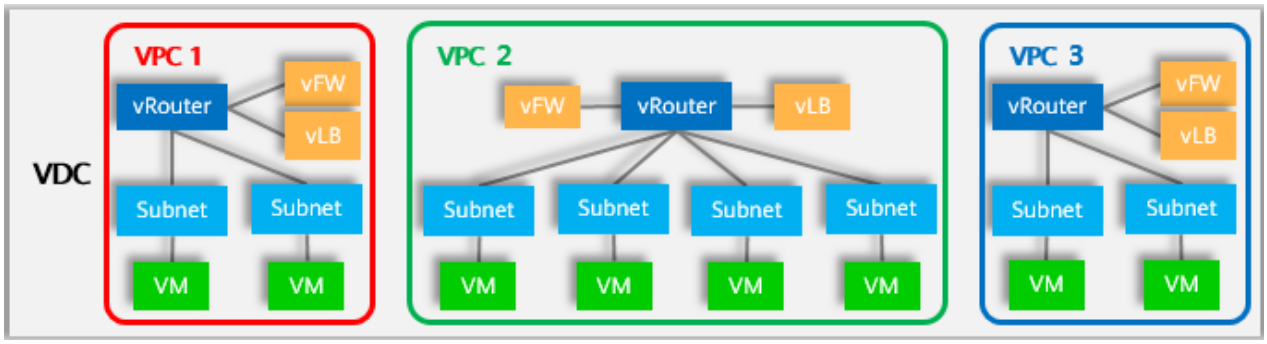
1. 系统管理员进行 VDC 的规划设计，这个阶段主要是基于业务的种类和需求来规划。对企业私有云来说，首先区分网络中需要部署多少种业务，对应于多少个逻辑相互隔离的网络。有业务相关性的网络放到同一个 VDC 中，没有相关性的放到不同的 VDC 中，如图 2-10 所示。系统管理员再创建具体的租户管理员账号，并分配资源给该租户。

图2-10 VDC 设计规划示意图



2. 租户管理员根据被分配到的资源进行自己 VPC 网络的设计和配置，可以根据业务需求对 VPC 中提供的逻辑元素进行组合、编排，如图 2-11 所示。

图2-11 租户管理员设计 VPC 网络示意图

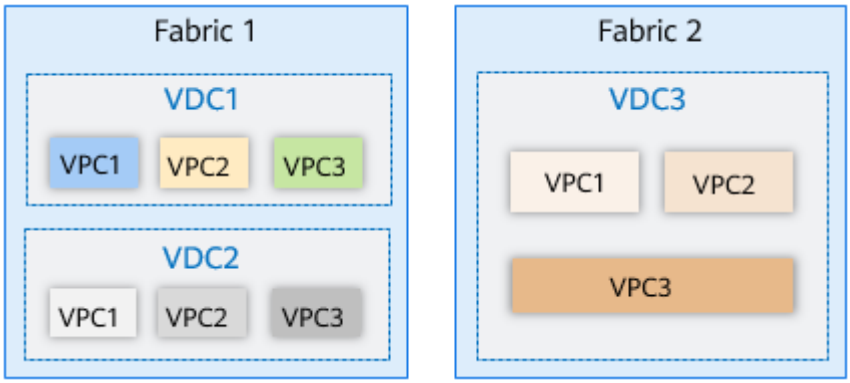


VDC 和 VPC 的规划原则

公有云场景中，VDC 和 VPC 的规划原则如下。

- VDC 规划要求：
  - 一个 Fabric 可部署多个 VDC，单个 VDC 不能跨 Fabric 部署。
  - 单个 VDC 的网络资源必须被分配在一个 Fabric 内，相应的计算和存储资源需要被分配到一个 AZ 内。
- VPC 规划要求：
  - 组建 VPC 的资源范畴只能是 VDC 的子集，因此 VPC 在多租户场景下也只能部署在一个 Fabric 内，不能跨 Fabric 部署。
  - 租户内部网络自行规划，租户间 IP 地址可重叠。

图2-12 公有云 VDC 和 VPC 划分示意图

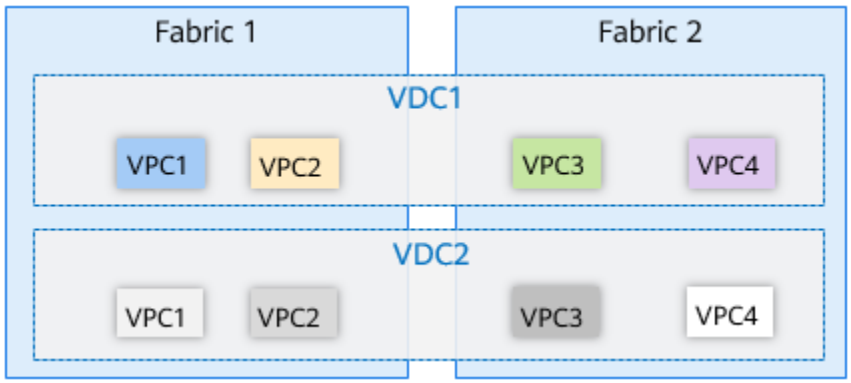


私有云场景中，VDC 和 VPC 的规划原则如下。

- VDC 规划要求：
  - 一个 Fabric 可部署多个 VDC，单个 VDC 可以跨 Fabric 部署。
  - 在选择 VDC 资源部署时可以包含多个 AZ。
- VPC 规划要求：

- 同一个 VPC 的所有计算和网络资源需要发放到同一个 Fabric 中，但同一个 VDC 中的不同 VPC 可以属于不同的 Fabric。
- 全网 IP 地址统一规划，所有 VDC 内 IP 地址无重叠。

图2-13 私有云 VDC 和 VPC 划分示意图



在公有云和私有云中，对 VDC 和 VPC 的规划设计原则有所区别，参见表 2-2。

表2-2 公有云和私有云中的 VDC 和 VPC 规划原则说明

场景	VDC 规划指导		VPC 规划指导		
	Fabric 划分原则	**VDC 划分原则**	**业务要求**		**VPC 部署原则**
公有云	按性能等级 按增值服务能力 按资源容量	每租户一个 VDC	业务内部互访无须安全控制		每业务一个 VPC VPC 内部子网间默认互通
			业务内部互访需要安全控制，但要求较低		每业务一个 VPC VPC 内部子网间默认互通 VPC 内部子网互访通过安全组隔离
			业务分层部署，内部互访有较高安全控制要求		每业务多个 VPC VPC 之间互访通过防火墙控制
私有云	按安全等级 按部门 按业务类别	每部门一个 VDC 规模大、部署复杂的业务单独划分为一个 VDC	多业务混合部署的 Fabric	业务要求请参考公有云	VPC 部署原则请参考公有云
			单个业务或业务某一层体量较大，需要占用独立的 Fabric	业务与外部的东西向流量大，默认无须安全控制 业务与外部的南北向流量需要安全控制	每个业务或业务某一层（如 APP 或 DB），一个 VPC 占用一个 Fabric 东西向流量默认互

					通，可按需配置安全组进行隔离 南北向流量须通过防火墙控制
				业务与外部的东西、南北向流量均需要安全控制	每个业务或业务某一层（如 Web），一个 VPC 占用一个 Fabric 东西/南北向流量均须通过防火墙控制

2.3 云网一体化方案说明

本章介绍云网一体化方案方案组件架构，组件功能及关键业务流程。

2.3.1 云网一体化方案架构

如 **Error! Reference source not found.**所示，云网一体化方案：

- 支持对接开源 OpenStack、Redhat OpenSack 10、和华为 FusionCloud（**不支持 ACGBP Plugin Driver**）。
- 对接开源/Redhat OpenStack 支持 Network overlay 和 Hybrid overlay 组网。
- 对接 FusionCloud 私有云场景支持 Network Overlay 组网。NFVI 电信云场景支持 Hybrid Overlay 组网。