



基于 OpenStack 的异构混合云解决方案

陈 天, 陈 楠, 黄志兰, 樊勇兵, 赖培源

(中国电信股份有限公司广州研究院 广州 510630)

摘 要: 对混合云产业发展现状、主流产品和解决方案进行了梳理, 对混合云适用场景和部署方式进行了分析, 并基于电信运营商云资源特点和混合云业务需求, 提出了基于 OpenStack 开源实现的异构混合云系统和解决方案, 对该系统相关的系统框架、混合云统一管理、异构资源池统一管理、混合云网络互通、混合云安全等关键问题进行了阐述。

关键词: 混合云; OpenStack; 电信运营商; 异构网络

doi: 10.11959/j.issn.1000-0801.2015169

OpenStack-Based Heterogeneous Hybrid Cloud Solution

Chen Tian, Chen Nan, Huang Zhilan, Fan Yongbing, Lai Peiyuan

(Guangzhou Research Institute of China Telecom Co., Ltd., Guangzhou 510630, China)

Abstract: The status of hybrid cloud industry, mainstream products and solutions of hybrid cloud were studied. The applicable scenarios and deployment options were analyzed. Based on the characteristics of cloud resource and the hybrid cloud business needs of telecom operators, heterogeneous hybrid cloud system and technical solutions were proposed. The system framework and key technologies of hybrid cloud unified management, heterogeneous resource pools unified management, hybrid cloud network connectivity, and hybrid cloud security were described.

Key words: hybrid cloud, OpenStack, telecom operator, heterogeneous network

1 引言

混合云^[1]是私有云、公有云、社区云等两种或多种云计算部署模式的结合体, 支持应用在云间的数据共享、自动部署、灵活迁移和按需扩展。一般而言, 混合云等于“私有云+公有云”, 兼具公有云可扩展、节约成本和私有云安全可控的优势, 但存在安全、认证、管理、数据私密性等潜在风险。

混合云近年来成为行业热点, 也是中国云计算市场未来几年的主要增长点之一。业界调查表明, 中国企业客户对私有云/混合云的接受度远高于公有云, 但由于各种内外部因素, 尚未成功构建混合云/IT 环境。

对电信运营商而言, 混合云直面用户需求, 解决了云的互通和竖井问题, 实现了 IT 应用的混合交付和“没有围墙”的云数据中心, 将衍生出更多的商业价值。然而, 鉴于商业因素和技术成熟度等因素, 现有主流的混合云业务和

收稿日期: 2014-05-20; 修回日期: 2015-07-08

论文引用格式: 陈天, 陈楠, 黄志兰等. 基于 OpenStack 的异构混合云解决方案. 电信科学, 2015169

Chen T, Chen N, Huang Z L, et al. OpenStack-based heterogeneous hybrid cloud solution. Telecommunications Science, 2015169

方案,大多将客户限定于特定的技术和服务,仅能实现特定云互通,尚未达到真正的“开放”和“混合”。开源云操作系统,特别是 OpenStack,为电信运营商提供了一个好的机遇和选择。OpenStack 虽是开源新军,但凭借先进的技术架构、有效运作的开放社区,打造了欣欣向荣的产业生态圈,引领了云计算领域开放式创新的潮流,已成为行业主流。

本文对混合云产业现状进行了梳理,对混合云场景进行了分析,并从电信运营商角度出发,提出了基于 OpenStack 的异构混合云解决方案。

2 混合云产业发展现状

混合云整体发展迅速,产业巨头纷纷赶赴混合云盛宴。当前业界主流的混合云业务和方案见表 1。

鉴于商业和技术成熟度等因素,现有主流的混合云业务和方案,大多将客户限定于特定的技术和服务,仅能实现特定云互通,尚未达到真正的“开放”和“混合”,兼容性、中立性、标准性、可互操作性等有待提升。如何构建开放的混合云平台,尽可能地融入丰富的混合云场景,最大化拓展和拉动公有云业务,利用自身网络优势形成差异化竞争能力,成为电信运营商需要重点解决的问题。

3 混合云适用场景和部署方式

电信运营商拥有庞大的 IDC 基础设施资源和网络管道资源,兼具规模化和专业化运营基础,通常是全云服务

提供商。电信运营商提供混合云业务,不仅可实现各种云的混合与互通,还可借此打造丰富多样的云生态系统,聚合产业力量,打通服务链条,加强产业渗透。

混合云主要适用场景包括^[9]以下几个方面。

- 研发测试环境的按需部署与迁移:企业将开发测试环境部署在公有云,生产环境部署在私有云,并按需在私有云与公有云之间迁移。
- 区分关键应用与一般应用的资源统筹规划和按需部署:企业通常选择将简单的、非关键的协同软件迁移至公有云,将关键业务和高价值应用系统部署在私有云,并按需迁移。
- 同一应用分层部署实现混合架构:传统的三层(多层)应用,可按需将其应用服务器或数据服务器等不同层次迁移至公有云,充分利用公有云按需弹性等特点。
- 同一应用跨云弹性伸缩(云爆发):为应对季节性或突发性业务流量,将私有云中所部署应用的一部分扩展至公有云,并按需回迁和释放公有云资源,在满足资源需求的同时最大化节约成本。
- 应用与数据的备份与恢复等:企业应用系统和数据备份在云端,遇到突发情况时,数据不会丢失,应用系统能够在云端启用,从而有效节省企业自建灾备环境所带来的额外成本和管理投入。

由于目前混合云技术和业务发展成熟度限制,各种混合云场景的实现程度不一。目前业界大多数实现的是简单

表 1 主流混合云业务和方案

云产业角色	混合云目标	代表厂商及当前具体实现
全能型云平台商	既拥有服务器虚拟化、虚拟化管理软件到云操作系统等全套产品体系,也提供公有云服务,其混合云方案的主要对象是其私有云客户	VMware ^[2] :实现 vSphere/vCloud 私有云与 vCloud Air 公有云的互通; Microsoft ^[3] :实现 System Center 私有云与 Azure 公有云的互通
纯公有云提供商	专注于公有云,并基于此为用户提供混合云能力	Amazon ^[4] :基于 VPC 等公有云业务实现用户 IT 环境到公有云的扩展,构建混合 IT 架构,满足简单的混合云场景需求
私有云解决方案提供商	以合作的方式靠拢公有云事实标准	Eucalyptus ^[5] :提供开源的与 AWS API 完全兼容的私有云平台,其用户可无缝使用 Amazon 公有云,借力实现混合云架构,但暂未考虑对其他异构云的兼容
云解决方案提供商	以异构云互通为目标,实现对 VMware、Microsoft、OpenStack、CloudStack 等异构云的互通和管理,但目前管理程度和功能实现不一,异构云间相对独立	RedHat ^[6] :主要实现对上述异构云的烟囱式的统一管理; Cisco ^[7] :主要提供异构云间互通的网络解决方案
电信运营商	基于自身的基础设施和网络基础,主要实现“托管私有云+公有云”场景,并基于自身网络基础实现与用户数据中心的连通	Rackspace ^[8] :主要实现同一数据中心内用户的托管专属物理服务器与 Rackspace 公有云服务的互通及云爆发等场景,并提供与用户数据中心间的 IPSec VPN 连接; NTT:基于统一网络控制器自动化实现用户数据中心、NTT 托管私有云及 NTT 企业云(公有云)之间的混合云网络连接

上述混合云场景可基于不同的部署方式实现,主要有以下两种方式。

- 电信运营商一般是全云业务提供商,“托管私有云+公有云”的混合云部署方式有利于充分利用既有 IDC 资源和公有云业务,打造包括公有云、私有云及网络的“一揽子”解决方案,同时便于实现统一的混合云管理、提供丰富的混合云高级业务能力,体现与其他云提供商的差异性。具体实施时,可依据用户需求,综合考虑多种业务场景和部

4 基于 OpenStack 的异构混合云技术方案

- 开源的开放式创新和可定制化有利于满足混合云对异构、可移植、可互操作及差异化的需求。OpenStack 已成为 IaaS 开源领域行业主流，为电信运营商提供了一个好的机遇和选择。
- 电信运营商的云包括多个异构的云资源池，如何整合异构资源池，融入丰富的混合云场景，带动公有云/托管私有云业务销售，并充分利用自身网络优势形成差异化竞争能力，是需要重点解决的问题。
- 在用户需求方面，VMware/ESXi 商业平台与 OpenStack/KVM (Linux kernel-based virtual machine，基于 Linux 内核的服务器虚拟化) 开源的整合一直是强劲需求，对 AWS/EC2 的中介代理、统一管理也是一个普遍需求，更是一大趋势。

因此,为了便于说明,本方案重点解决 VMware/ESXi 与 OpenStack/KVM 的互通整合及对 AWS/EC2 的云代理,并基于此提供多种混合云业务场景,阐述如下。

4.1 系统框架

基于 OpenStack 的异构混合云框架如图 1 所示, 主要包括如下组件。

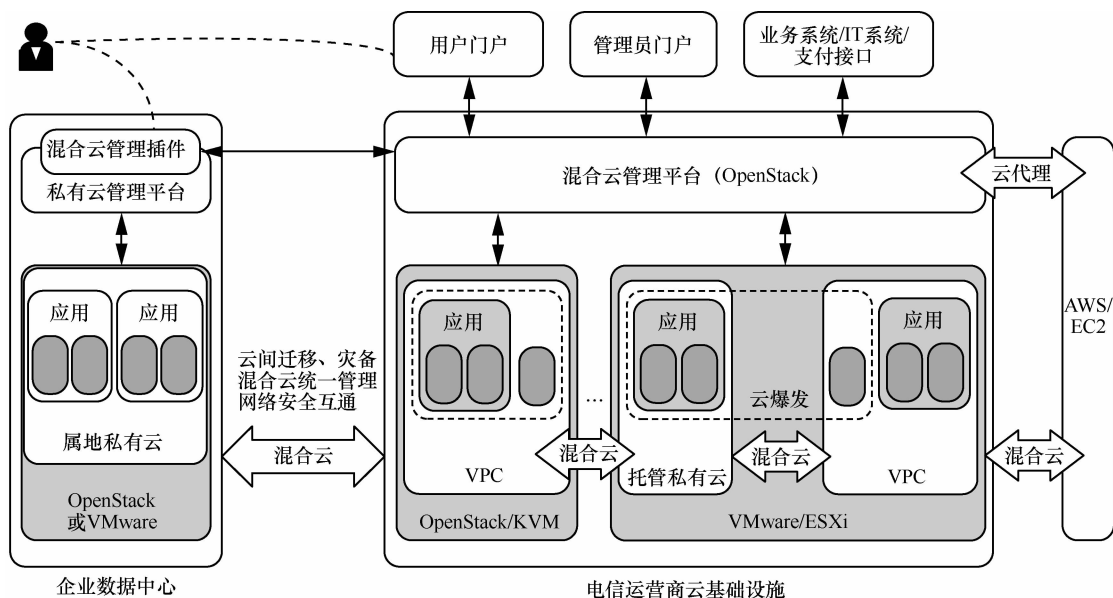


图 1 基于 OpenStack 的异构混合云系统框架

(1)混合云管理平台

位于运营商侧,基于 OpenStack 构建,是整个混合云系统的核心,实现对异构云资源池的统一管理,提供 IaaS 公有云/混合云业务功能,开放用户/管理员门户及 API,兼具对第三方公有云(AWS)的云代理能力,北向与相关业务/IT/支付等系统对接,实现开户、计费、支付等能力。

(2)混合云管理插件

位于用户侧,基于 OpenStack 实现,可与企业私有云管理平台(如 OpenStack、VMware 等)集成,可将运营商侧环境的管理拉至用户侧,实现两侧混合云环境的“烟囱式”统一纳管。

(3)电信运营商云基础设施

包括多个云资源池,单个云资源池一般基于单一服务器虚拟化技术构建,不同的云资源池可能位于不同的云数据中心,异构云资源池之间网络大二层互通。

该混合云系统可兼顾多种混合云场景和部署方式,并可混搭使用,具体介绍如下。

- 属地私有云+公有云:可提供混合云网络互通、应用的离线迁移、应用与数据灾备等混合云场景,并可通过分别接入两侧管理平台或安装混合云管理插件的方式实现混合云统一管理。
- 托管私有云+公有云:可提供应用云间热迁移、应用跨云弹性伸缩(云爆发)以及全局负载均衡等高级网络业务等,用户可通过运营商侧的管理平台实现混合云统一管理。

- 云代理/云互联:基于 OpenStack 的混合云管理平台实现对第三方公有云(如 AWS 等)的单点接入和统一管理,具体业务能力视第三方云平台开放接口能力而定。

4.2 混合云统一管理

如图 2 所示,混合云统一管理主要包括混合云管理平台与混合云管理插件两大组件。

(1)混合云管理平台

位于电信运营商侧,基于 OpenStack 架构优化实现,主要包括如下功能模块。

- 接口适配:统一纳管 VMware/ESXi、OpenStack/KVM 异构云资源池。
- 资源部署调度:混合云业务的跨云资源部署、多云镜像管理、云间迁移管理等。
- 网络统一管理:云间网络互通管理、云间网络业务管理(如全局负载均衡)、用户跨云网络管理。
- 业务编排重组:多云服务目录同步、重组、编排和统一呈现,混合云业务生命周期管理。
- 业务统一分发:混合云业务统一订购和分发部署。
- 统一认证管理:多云用户账户和角色权限管理、多云鉴权管理。
- 策略配置管理:负载部署位置、云间资源调度、资源跨云弹性伸缩等相关策略配置管理。
- 统一监控告警:多云 SLA、QoS 的统一监控、告警及处理。

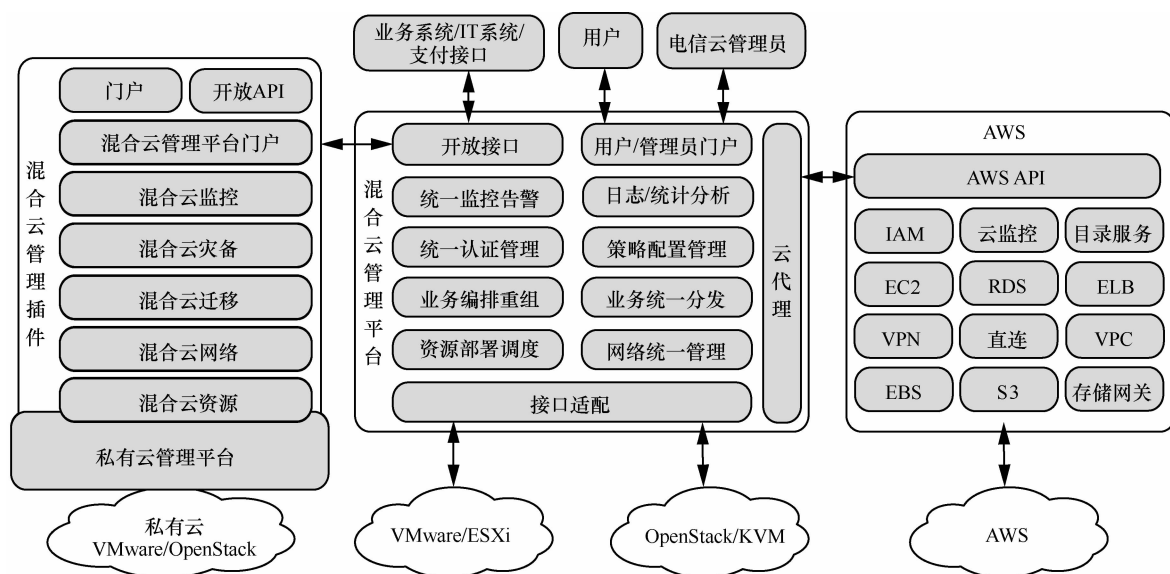


图2 混合云统一管理整体逻辑功能架构



- 日志/统计分析:多云系统日志和操作日志的同步、呈现和管理,定制化多云统计分析报告。
- 用户/管理员门户:混合云管理界面。
- 开放接口:北向开放 OpenStack RESTful API,供其他业务/IT/支付等系统集成和调用。
- 云代理:调用 AWS API 实现对 AWS 公有云业务资源的统一纳管。

(2)混合云管理插件

位于企业用户侧,作为混合云管理平台的客户端延伸,是混合云管理平台的功能子集,将运营商侧提供的混合云资源、网络、云间迁移、灾备、监控等功能引入用户私有云侧,提供到混合云管理平台门户的快捷接入,统一认证等功能仍保留在运营商侧。

4.3 异构资源池统一管理

如图 3 所示,OpenStack 可通过 vCenter API 或 ESXi API 管理 ESXi 虚拟化环境,其中,vCenter API 可提供更多高级功能。与 KVM 不同的是,在 OpenStack Nova 计算节点(compute node)上部署的是 VMware vCenter 服务器等虚拟化管理服务器端,而 KVM 虚拟机则可直接部署在 Nova 计算节点上。因此,在 OpenStack 的 Horizon 等模块中,需额外开发以打开 VMware 环境的更多功能。

OpenStack 对不同 Hyper-V 的支持程度和功能实现不同。Libvirt 驱动用于管理 KVM/QEMU,是目前 OpenStack 部署中应用最多的服务器虚拟化技术,社区支持及功能实现程度最高;VMware ESXi 与 Hyper-V、XenServer 同属第 2 个档次,支持程度次之,虽然各厂商都提供免费 License 版本,但相对于商业版本而言功能受限;此外还有第 3 类驱动,如 Baremetal、Docker 及 Libvirt(Xen)等,支持程度较弱,有待于进一步完善。

4.4 混合云网络互通

混合云网络互通主要包括如下两方面。

- 属地私有云与公有云之间、运营商公有云与第三方公有云之间:大多采用专线或 VPN(如 IPSec VPN)来实现混合云网络互通与安全接入。其中,VPN 网关可作为虚拟应用部署在 VPC 网络环境中,企业侧可按需采用各种软硬件 VPN 方案,同时,对端传输加密以增强安全性。
- 托管私有云与公有云 VPC 之间、异构云资源池之间:运营商统管,可按需部署基于 overlay 的 SDN 解决方案,满足大规模、多租户环境部署需求,提供大二层互通功能,实现同一网段在混合云之间的扩展,为虚拟机带 IP 地址迁移创造条件。

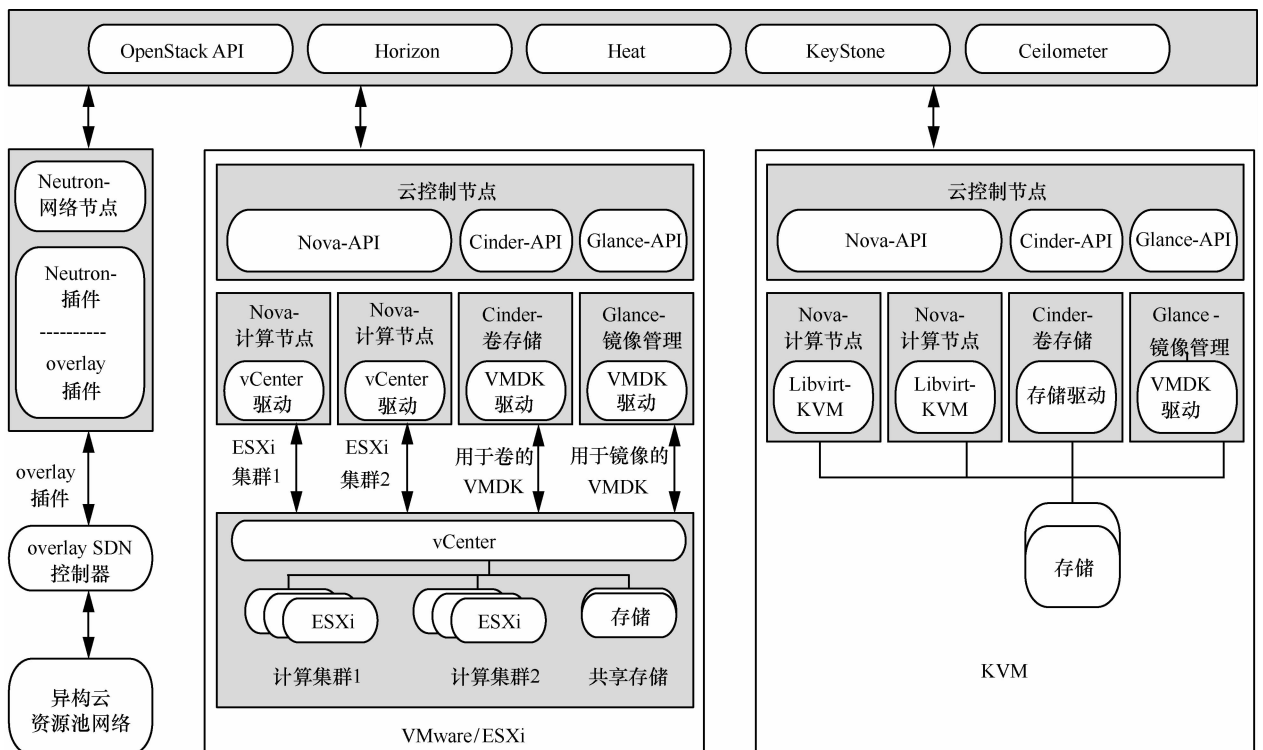


图 3 基于 OpenStack 的 VMware/ESXi、OpenStack/KVM 统一管理逻辑参考架构

OpenStack Neutron 组件提供了丰富的网络功能,支持两种类型的后端插件:核心插件和业务插件。核心插件完成二层网络隔离的相关配置和实现互通性的虚拟机报文转发;业务插件主要实现三层网络功能及三层以上的业务应用功能。这些插件有开源与商业版本之分,商业版本在使用时可能存在许可证等诸多限制,可按需选择使用。其中,overlay SDN 相关插件属于核心插件,支持 VxLAN、NVGRE 等 overlay 技术;VPNaaS 是 Neutron 提供的高级网络功能,目前在混合云网络互通方面一般采用 IPSec VPN 技术方案,当前 Neutron 支持的 IPSec 插件主要有 Openswan 和 CiscoCsrIPSec。如图 4 所示,实际部署中,可通过集中式的 overlay SDN 控制器控制管理网络节点和计算节点上的所有 OVS 虚拟交换机,配置 overlay 隧道接口;网络边缘虚拟路由器同时承担 VPN 网关、L3 路由、overlay 网关、NAT 等业务功能。

4.5 混合云安全考虑

混合云安全是混合云用户重点关注的问题,混合云用户在从私有云扩展到混合云时,有对安全的一致性需求,有必要在混合云架构的各个层面都进行安全要素集成。重点考虑以下几方面。

- 云间网络安全:通过防火墙、网关等各种措施提供安全的专线或 VPN 连接,保证用户跨云网络安全策略的一致性。
- 云间负载安全:提供数据加密、传输加密、API 加密等各种措施,建立端到端的数据传输安全机制,保

证企业数据在多云平台上的存储安全以及多云平台之间的安全迁移。

- 多云统一认证鉴权:提供统一的用户账户管理,实现不同云平台间用户账户的关联,并提供统一的密钥和鉴权管理。目前 OpenStack 正在推进统一认证项目,未来或可成为一种可选方案。

4.6 其他

该异构混合云系统中还需考虑的其他一些关键问题主要有以下两个方面。

(1) 云间迁移

综合考虑业务需求和技术成熟度,在属地私有云和公有云之间提供简单的虚拟机镜像和数据迁移,在运营商异构资源池之间可提供虚拟机带 IP 地址迁移,在托管私有云和公有云之间可提供虚拟机在线迁移。

除了通常所说的网络时延、迁移流程等问题之外,混合云间迁移的一大问题是虚拟机格式问题。异构云间迁移通常采用的格式转换和迁移流程是:卸载虚拟机中的虚拟化工具;关闭虚拟机;虚拟机格式转换;虚拟机位置迁移;虚拟机开机;为虚拟机安装虚拟化工具。

(2) 云爆发

该混合云系统中,云爆发应用场景主要基于同一资源池内的托管私有云和公有云实现。可考虑如下的云爆发技术方案^[10]:用户的云应用采用分层、模块化设计,较易产生突发流量的前端会话层由无状态组件构成,通过全局负载均衡统一进行流量管理;当峰值来临时,根据

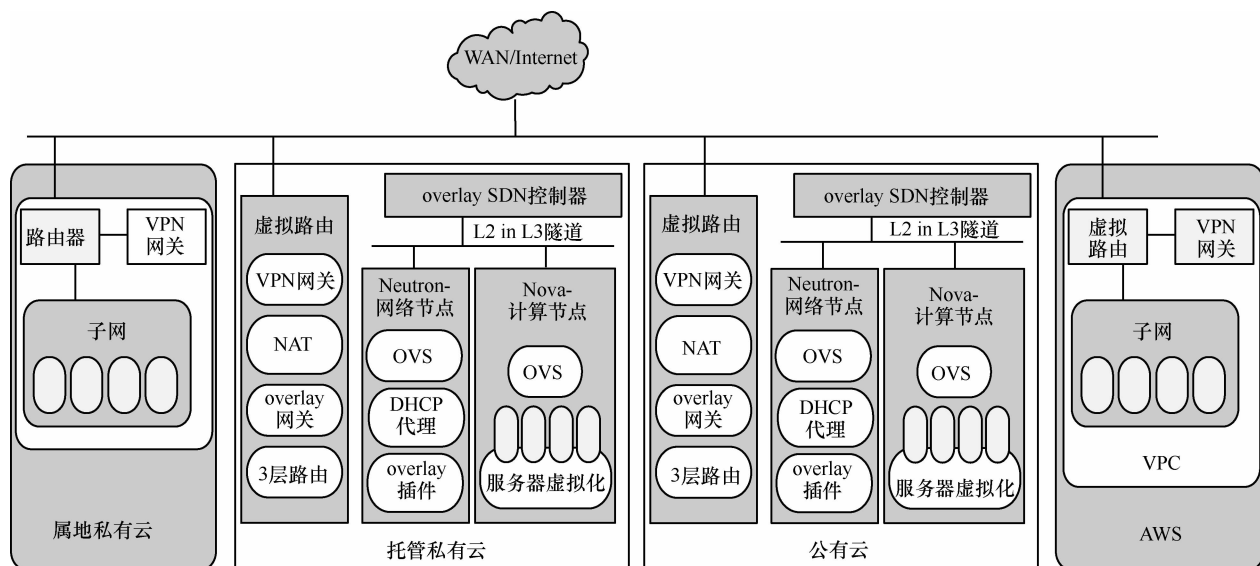


图4 混合云网络互通



既定策略在公有云中启动和部署附加环境,部署完成后通过全局负载均衡器进行用户流量重定向;当峰值流量过去之后,再根据既定策略按需释放公有云中的资源。

5 结束语

混合云是行业一大热点,也是中国云计算市场未来几年的主要增长点之一。当前,云计算客户已经从纠结于公有云和私有云的选择,转向混合云部署架构。2014年是混合云解决方案商和服务商闭关修炼、用户观望的一年;2014年底主流厂商混合云战略/方案的密集发布,彻底引爆了混合云市场;2015年将成为用户开始接受、采用混合云的一年,也将是混合云落地元年。

混合云是私有云与公有云等多种云计算部署模式的结合体,随着云计算业务的发展,还将不可避免地融入云代理、云互联、混合IT等多个概念,未来混合云业务场景将愈加复杂,混合云网络、云间迁移、混合云灾备、云爆发、全局负载均衡、基于策略的动态执行等都是下一步研究重点。此外,OpenStack虽然为混合云提供了一个较好的框架,但由于技术和业务发展成熟度限制,如何提升混合云系统的标准性、兼容性、可操作性等,都将是持续的挑战。

参考文献

- 1 NIST. Special Publication 800-145. The NIST Definition of Cloud Computing, 2011
- 2 VMware. VMware-Hybrid-Cloud-Brochure, 2014
- 3 Microsoft. Microsoft System Center 2012 R2 Technical Overview, 2014
- 4 孙素梅. 基于AWS云服务的企业混合IT架构和网络实现. AWS技术峰会, 北京, 中国, 2014
Sun S M. Enterprise hybrid IT architecture and network implementation based on AWS cloud services. Proceedings of AWS Summit, Beijing, China, 2014
- 5 Eucalyptus. Eucalyptus 4.0 Reference Architecture, 2014
- 6 RedHat. RedHat Upgrades Hybrid Cloud Management Platform, Releases RedHat CloudForms 3.1, 2014
- 7 Cisco. Cisco InterCloud: Enable a Hybrid Cloud, 2014
- 8 Rackspace. Hybrid Cloud: The Evolved Enterprise Cloud of the Future, 2015
- 9 陈天,樊勇兵,赖培源等. 混合云技术架构及应用研究. 电信科学, 2014, 30(Z2)

Chen T, Fan Y B, Lai P Y, *et al.* Research on hybrid cloud technology architecture and application. Telecommunications Science, 2014, 30(Z2)

- 10 Drake J, Jacob A, Simpson N, *et al.* Open Data Center Alliancesm Developing Cloud-Capable Applications White Paper Rev. 1.1, 2013

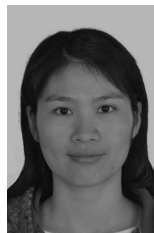
[作者简介]



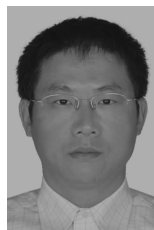
陈天,女,现就职于中国电信股份有限公司广州研究院,主要研究方向为互联网、云计算、IDC。



陈楠,男,博士,现就职于中国电信股份有限公司广州研究院,主要研究方向为互联网、云计算、IDC。



黄志兰,女,现就职于中国电信股份有限公司广州研究院,主要研究方向为互联网、云计算、IDC。



樊勇兵,男,博士,中国电信股份有限公司广州研究院高经工程师,中国通信学会高级会员,全球云网 OpenCircus 中国电信节点负责人、中国电信重点实验室——数据多媒体实验室负责人、中国电信数据网支撑中心主要成员,主要研究方向为互联网、云计算、IDC等。



赖培源,男,现就职于中国电信股份有限公司广州研究院,主要研究方向为互联网、云计算、定制化服务器、IDC。