一、 案例概述

1. 案例背景

去年 7 月，中国信息通信研究院发布的《金融云行业趋势研究报告》指出，金融云已经进入 3.0 时代。相比 1.0 阶段以行业应用软件开发为核心，2.0 阶段以云计算为支撑发展符合分布式架构的金融行业云。金融云到了 3.0 阶段，以“公有云+专有云+混合云”的混合数字基础设施模式则是未来金融云整体架构的基础。

作为依托运营商主业优势和资源禀赋，拓展科技金融新领域的某金融科技公司来说，随着支付、特色电商和互联网金融业务的不断发展，容器、微服务、服务网格等云原生技术在业务系统中被更多的应用。数据中心网络团队不得不面对 OpenStack、VMware、Bare-metal、容器等多种类型的资源池资源，和多厂商网络交换矩阵共存的复杂网络环境。传统的网络架构设计和网络编排管理的效率已经无法满足业务跨资源池互访、弹性扩展、双活灾备、合规审计等的需求，那么为业务提供稳定、高效且安全的组网模型，让网络更加自动化地为业务提供服务成为客户所关注的焦点。

2. 需求与痛点

2.1 业务隔离

原生 K8S 缺省 POD 网络全通，安全性较差；如实现安全策略配置，策略数量庞大，会造成转发效率低下且诊断复杂。业务层面要求进行不同业务间的逻辑区隔，与此同时也要有按需互访策略开通的能力，提升安全性的同时不降低网络转发效率且不额外提高计算资源池的负载。

2.2 弹性扩展

原生 K8S 网络通过在所有计算节点间组建 Overlay 网络实现业务间通信，网络间的连通完全依靠计算节点的 CPU 计算实现。物理网络对于原生 K8S 来说是纯粹的 Underlay 网络，仅对计算节点间提供三层互联能力。原生 K8S 也无法与物理网络联动，较难实现集群扩展、DCI 扩展及与其他资源池互访。

金融云平台支撑的业务系统间对计算资源类型的需求较为丰富，且需提供高可靠异地支援的容灾支持，这对组网提出了更高要求。具体来说容器资源池要支持容器集群规模可按需扩展；虚拟化资源池可接入 KVM 资源，同时在虚拟机之间提供逻辑隔离；裸机资源池也提出了对大数据计算能力的接入需求。在实现各类资源池接入的基础上，还需实现不同资源类型之间的互访能力和安全管控能力。

2.3 地址管理

对于经典 K8S 网络插件如 Flannel、Calico 等，POD 地址范围受限于各 Node 节点分配地址的范围，无法完全按照业务进行全资源池环境内的地址规划及部署，亦无法实现特殊业务对固定 POD IP 地址的需求。

2.4 服务访问

原生容器 SDN 组网方案多采用 Server Overlay 方式，所有 Overlay 的流量均需通过计算节点的 CPU 参与运算，性能消耗会随着资源池量级的提升而增大，转发效率也会逐步降低，限制整体资源池规模；Netfilter 规则增加时东西向流量通信性能差。

解除资源池量级与转发性能间的耦合关系，保持转发性能的基础上实现对大体量资源池的支持。最大化利用现有网络设备资源提升转发效率并将计算能力最大化归还给计算资源池的业务。

二、 解决方案

客户的容器资源池由 x86 服务器和锐捷交换机构成，将原生 K8S 的经典网络插件更换为 NSP 的 CNI plugin 容器网络插件，并通过与 NSP-Controller 控制器的联动，实现了跨资源池扩容、跨异构资源池组网以及跨数据中心互联等网络能力。数据转发方面，通过集群内部的 OVS 与网络交换机硬件的联动，将数据转发工作彻底从 Server Overlay 转换成了更加稳定高效的 Network Overlay。通过将网络数据转发与计算资源相剥离的做法，实现了对大体量集群的支持而不消耗计算资源的数据转发能力。

同时，NSP 的 CNI plugin 插件带来了能够在 Namespace 间更加稳定高效实现双向安全组的能力，将安全管控能力落入到 VPC 内部。

1. 解决方案概述

云杉网络 NSP 针对 Kubernetes 提供的统一网络编排和服务管理解决方案。通过 NSP 的 CNI plugin 插件实现了对 Kubernetes 的 Pod 网络、东西向和南北向服务网络统一纳管，同时支持 Kubernetes 的资源弹性扩容和跨资源池互联，并满足高性能网络的需求。

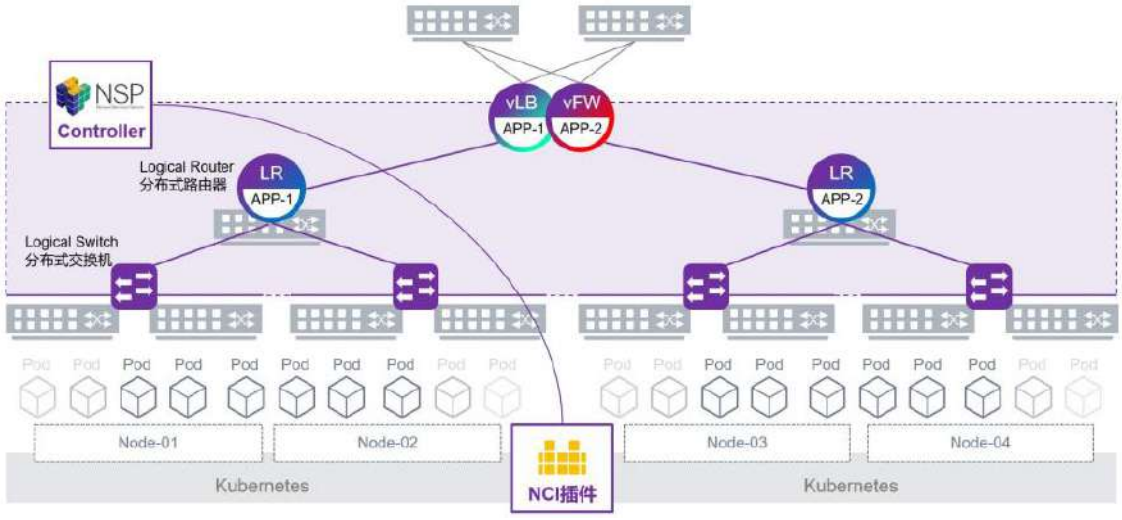

图 1 NCI 插件

如图所示，NSP 基于 Logical Switch（LS）和 Logical Router（LR）来实现同 Fabric 网络下多资源池的组网互联，通过 Virtual Routing Bridge（VRB）来实现边界服务接入以及跨 Fabric 网络或者跨数据中心的组网互联。

而 NSP 在结合了 CNI plugin 之后，进一步实现了对 Kubernetes 资源池的统一纳管支持，即 Kubernetes 资源池的网络虚拟化，Kubernetes 资源池自身扩容以及同其他异构资源池以及混合云互通，还有边界服务。

2. 解决方案技术特点和优势

2.1 基于 VPC 的业务隔离

在 NSP NCI 容器网络方案的设计实现中，一个 VPC 下可以关联多个 Kubernetes 集群中的 Namespace，默认 Namespace 属于 default VPC，隶属于同一个 VPC 下的 POD 是可以互通的，而不同 VPC 的 POD 之间默认是隔离的。相应地，一个 VPC 中的 POD 通过组网编排，最终可以对外提供完整的业务。

2.2 提供弹性扩容机制

- 资源扩容

NSP NCI 容器网络方案按照 VPC 的逻辑为 Namespace 提供了隔离，在 EVPN 配置的 Fabric 网络中将不会出现所有 POD 的 IP 地址表项都在 Leaf 交换机上聚集的情况，因此基于 EVPN 的 LS 和 LR 为数据中心内部资源池提供规模能够达到 Kubernetes 集群理论上限 5000 台的 Node 要求。

- 服务扩容

NSP 控制器通过对多厂商交换机（包括业界主流交换机如华为、H3C、锐捷、思科、Arista、盛科等）进行组网编排，依靠其性能在对外服务提供上可以支持更大的业务规模，在秒杀等场景下只需要在资源池内或者跨资源池扩展后端的业务 POD 数量就能实现弹性扩容。

- 跨地域扩容

NSP 通过 Multi-Fabric 以及 Multi-Site（按需）方式，可支持数据中心之间的二层、三层互联，从而可实现 Kubernetes 集群在异地多数据中心的弹性扩展。

2.3 基于子网地址的管理机制

NSP NCI 容器网络方案实现了基于 Subnet 来为 POD 分配地址的逻辑。一个 Namespace 中允许创建多个 Subnet，不同的 Subnet 对应不同网段，这样可以让不同类型应用的 POD 加到不同的 Subnet 中，从而同类型应用的 POD 可以二层互通，而不同类型应用的 POD 则通过三层互通，带来的好处是可以更清晰地为不同类型应用的 POD 创建对应的服务。

2.4 双层网络设计逻辑

在 Node 上，POD 均是接入到 OvS 网桥 br-int 上，通过 VLAN 广播域进行隔离。一个 Node 上接入同一 Subnet 的 POD 分配同样的 VLAN Tag，这些 POD 可以直接通过 OvS 网桥实现二层互通。对于同一 Subnet 中跨 Node 或者跨机柜的 POD，则通过 Leaf 交换机上创建的 Logical Switch（对应图中的 MAC-VRF）实现大二层互通。对于同一 Namespace 不同 Subnet 中的 POD，无论是否在同一个 Node 或者同一个机柜，均通过 Leaf 交换机上创建的分布式 Logical Router（对应图中的 IP-VRF）实现三层互通。

三、 商业价值

1. 商用部署规模和实际效果

客户的网络架构是典型的两地三中心设计，每数据中心内部建设多个 Region（安全域）。

NSP-Controller（网络控制器）已完成对双数据中心所有现网网络设备的全量纳管，完成包括网络交换机、防火墙、负载均衡设备以及 DNS 等多种设备类型。目前纳管总服务器数量上千台，容器节点纳管数百台。通过部署三台 NSP-Orchestrator（网络编排器）用于热备，当两地管理网络中断时，可切换至本地网络编排器进行本地管理，保持组网及管理能力的安全可控。

本案例 SDN 网络技术架构采用 NSP NCI 容器网络方案，是结合控制面的 MP-BGP+EVPN 协议，数据面的 Vxlan 协议，基于硬件 SDN 交换机实现的 Network Overlay 能力。方案充分利用交换机的高性能和可靠性并为容器网络提供 VPC 网络模型，并提供实现了业务隔离、地址管理、安全组等功能。

2. 用户价值

基于 SDN 控制器实现了多类型资源池多安全域的两地三中心架构，完成了对多类型资源池的纳管及组网。实现了高效低消耗的安全隔离方案，最大化将计算资源归还于计算资源池的同时还实现了充分利用网络硬件的数据处理转发能力。借由基于本 SDN 网络架构的计算资源池，支撑起了总用户数近 10 亿，峰值日交易量超千万笔的电商业务，达成了高效稳定服务用户的目标。

- 提高运维效率

基于 SDN 技术，实现网络资源的配置模板化，可以避免由于人工配置可能带来的错误。当环境出现问题的时候也可通过 SDN 控制器快速定位问题并进行排障。未来随着骨干网扩容，可以通过 SDN 控制器进行割接、业务迁移等操作。

- 降低运维成本

SDN 控制器提供了多种灵活的实时告警接口，提供相比传统监控系统更加及时的平台动态。运维人员可以在任意地点登录到 SDN 控制器页面进行网络配置以及运维服务，大大的节省了运维成本。

- 提升管理及创新能力

通过 SDN 关键技术研究和运用可以加快公司科技创新的步伐，提升公司信息系统运维的科技水平和管理水平，提高公司的信息服务水平。帮助公司树立起敢于在新技术领域创新实践的先锋模范形象。

了解更多信息

专业的售前技术支持及商务合作，协助您选择最合适的解决方案

详询：400-9696-121

网址：www.yunshan.net

北京云杉世纪网络科技有限公司

北京市海淀区成府路 28 号优盛大厦 A 座 1209