JUNIPER NETWORKS | Engineering Simplicity

白皮书

网络和云架构的多云技术指南

如何跨多个云连接和保护工作负载并像它们在一个云中一样操作

©2018，Juniper Networks, Inc.

目录

简介：什么是多云？ 4

为何采用多云？ 4

多云挑战 5

- 多域连接 5
- 多供应商编排 5
- 端到端可见性 6
- 全面的安全性 6
- 复杂性 6

端到端和自上而下 7

多云架构概述 8

基础资源 9

- 交换矩阵 9
- IP 交换矩阵 10
- 基于意图的交换矩阵操作 12
- 统一数据中心和园区交换矩阵 12

工作负载管理 13

- 特定于实例的应用环境 13
- 工作负载抽象化 13
- 叠加控制 15
- 统一底层和叠加管理 15

服务消费 15

- 应用程序开发生命周期 16
- 服务感知网络 16
- 服务感知结构 18

总结 19

关于瞻博网络 19

©2018，Juniper Networks, Inc.

图片列表

图 1：端到端和自上而下多云设计 8
图 2：多云架构概述 8
图 3：多云通用交换矩阵 9
图 4：EVPN-VXLAN 架构 10
图 5：统一多云管理 11
图 6：联合交换矩阵 12
图 7：Contrail 架构 14
图 8：策略和控制 15
图 9：简化的策略实施 16
图 10：高级分析 17
图 11：跨层可见性和分析 18
图 12：服务感知结构 18

©2018，Juniper Networks, Inc.

执行摘要

组织不断寻求跨多个云端到端连接和保护工作负载的方法，期望像它们在一个云中一样简单，这一愿景推动着从云过渡到多云。这种转变代表着重大的运营转型，进行这种转变需要经过深思熟虑。整个行业都在全面讨论构成这一过渡的要点，并从中受益。

本白皮书讨论如何在组织从云过渡到多云时构思网络设计，包括安全和运营。先阐明转变的原因，再界定问题领域，然后讨论关键架构决策点。着重讨论满足今天和未来的技术需求，应对复杂性，打造卓越运营，保留选择，以及支持架构师作为业务技术主管的角色。

简介：什么是多云?

多云是将不同的基础架构域以一组融合资源的形式进行管理，不管这些资源在哪里，从而使用户能够从任何位置在任何环境中使用这些资源。在这一点上，尽管多云与底层传输有关，但它更主要是围绕更高层的功能构建的。从根本上说，多云更多地是一种操作条件，而不是对核心基础架构的描述。

由于多云需要统一管理方法，因此“多个云”和“多云”之间存在针对性的区别。只是按照基础架构和运营的有界域将 IT 环境分为特定于云的碎片，不会实现多云承诺。多云的真正优势在于其与众不同的特性，即跨私有云和公有云、在内部和外部、作为单个实体进行运营的能力。

为何采用多云?

要了解对多云的需求，务必首先讨论企业为何要先采用云技术。从传统基础架构迁移到云（公有云或私有云）的需求通常由成本或敏捷性推动。

一些公司发现维护传统基础架构昂贵得令人望而却步，因此通过专为该目的而生的提供商来满足技术需求的想法对他们极具吸引力，因为假定成本较低，使企业能够专注于推动有意义价值的核心能力。

然而，对成本的主要关注会导致忽略云的主要优势。企业与其说是外包基础架构，不如说是利用云操作的敏捷性。如果企业能够更快地部署软件和服务，他们就能够更好地应对周遭的变化速度。而正是这种宏观变化趋势对企业业务构成了真正的威胁。

虽然大多数公司最初并没抱多大的雄心壮志，但仍有很多公司，即便是那些中型企业，最终都迁移到了多云。不论是追求双供应商策略，还是需要支持差异化能力，甚至是实现新旧技术必须和平共存（至少暂时共存），大多数企业都会发现自己正在支持一个包含多个私有云和公有云的混合环境。

为了全面实现云承诺，即使企业今天进行的是较小规模的云迁移，都必须谨记其最终目标。表 1 详述了今天的云部署为何最终会发展成多云。

©2018，Juniper Networks, Inc.

表 1：为何云会发展成多云

原因	为何采用多云?
经济性	在不同的云提供商之间进行选择创造了经济杠杆作用。而且，云之旅现象日益增长，在这种现象中，尝试采用云的企业受到普遍不协调的部署和/或持久应用程序引起的高成本的强烈冲击，导致他们重新审视私有基础架构和公有基础架构之间的平衡。
功能性	随着企业开发不同的需求，他们可能会发现云产品的不同之处。例如，Amazon AWS 竞争服务产品的广度和灵活性，Microsoft Azure 竞争企业应用程序，Google Cloud 竞争机器学习，Oracle 竞争 ERP 软件。
可用性	分布式应用程序为应对云服务故障提供更大的可用性和弹性。尽管这种多样化发生在云端，但由于企业使用多个云帐户、地区和可用性区域，因而也不可避免地发生在单个提供商领域内。
数据隐私	对数据来源进行监控的需求（特别是对全球企业而言）将有利于不同的本地云提供商，这样一来，工作负载就可与其提供的数据一起使用。
相近性	在性能很重要的地方，组织可以选择在不同的云中运行工作负载。例如，本地云将提供更短的流量往返时间，而多接入边缘计算 (MEC) 的兴起可能会导致云实例在内部或分布式电信云中运行。
过渡	采用多云的决策可能受到完成从私有云到公有云过渡的需求推动，在这种情况下，企业将不得不将这两种架构连接起来，而这一过程的时间无法确定。

多云挑战

迁移至多云的企业面临着一系列多云采用受阻的挑战。本节将重点讨论这些障碍，帮助架构师认识到潜在的问题领域，并了解在设计多云未来时，他们必须在哪些约束条件下工作，以便规划他们的前进之路。

多域连接

诚然，多云主要是操作问题的解决方案，但仍然存在着无缝连接和保护资源孤岛的潜在需求。由于多云还涉及控制端到端基础架构，因此这种连接还至少必须跨越数据中心、公有云以及园区和分支机构网关，并以实现完全园区和分支机构集成作为更长远的目标。

跨越如此广泛的网络位置，无论是在内部还是在云中，都需要一系列物理和虚拟形式的因素和功能。通过高容量 WAN 管理流量通常需要定制芯片，而数据中心交换机利用普通商用芯片，分支机构盒使用 x86 CPU。

通用交换矩阵管理平台还将通过跨域无缝连接来简化网络虚拟化。虚拟叠加网络必须跨越不同类型的服务器以及虚拟/物理网络和安全设备，以便工作负载或用户不会暴露在不同的域中。不管外形如何，这些设备必须不断地与诸如编排、可见性和安全性等北向软件层通信，从而对底层连接元素提出架构要求，特别是围绕可编程性和遥测。

多供应商编排

由于多云部署对外形和功能有着一系列要求，因此往往采用多供应商的形式，这对寻求统一基础架构的企业构成了挑战。历史证明，在异构底层之上提供公共编排层是很困难的；例如，多供应商元素管理系统 (EMS) 就有着糟糕的记录。

简言之，今天的主流运营模式依赖于精确控制和逐设备手动管理，因此无法在向多云迁移的过程中存活下来。在多云环境中，应用程序版本和运行应用程序工作负载的位置可能会随着时间的变化而变化，这就需要一个同样快速适应的网络。同时，多云更多的是以月份来衡量变化，因此与当今的运营模式有显著不同。架构师必须做好充分准备，围绕支持数字业务的应用程序的新操作实践展开设计。

©2018，Juniper Networks, Inc.

端到端可见性

如果多云是基于将基础架构组合作为一个单一实体来处理的，那么可见性就不能局限于单个域。对许多现有部署来说，统一可见性是一个重大的技术障碍。

使过渡更加复杂的是，多云将高度自动化。由于自动化的基本前提是看到什么做什么，这就强调了集中化监控和可见性，以及以一致的方式扩展可以观察并采取行动的事物的表面。在多云环境中，目标应该是减少用户发现问题的需求，并减轻运营团队为了确定问题发生的根本原因而跨域边界执行繁琐、耗时任务的需要。

当环境处于隔离状态时，很难跨域边界将事件关联在一起，这极大地缩小了所有运营控制的范围。如果遥测在不同的云上是不同的，那么它必须经过标准化和转换，才能用于多云目的。实时分析和用于标记问题的基于意图的监控和告警，以及了解哪里的资源需要启动或关闭的数据驱动型容量规划，必须是任何多云设计的基本要求。

全面的安全性

虽然网络在历史上一直把安全视为一个边界问题，但今天它显然已经突破了这个边界。要管理网络内部发生的攻击，安全性必须考虑不同网络子集内部和之间的流量。仅仅在网段之间设置防火墙过滤器和 ACL 是不够的；我们必须能够将流量隔离在这些网段内，这种做法通常称为微分段。

要使多云以一致的方式运行，必须在整个基础架构中应用一致的保护方案，从而提高园区内、分支机构间、云之间和数据中心内部的通信的安全性。

租户和应用级别都必须存在策略和控制，并且必须以统一的方式进行管理，这样分发和更新安全策略的操作负担不会影响解决方案的操作力度。这就需要单点管理和单点端到端验证，以确保遵守法规。

复杂性

也许操作多云最大的挑战在于复杂性。在今天的环境中，复杂性已经如此普遍，令人头痛，网络极其脆弱，无法忍受变革；如果没有良好的基础设计，跨多个云运行的网络将增加这一复杂性，使问题更加严重。

遗憾的是，复杂性不可避免地取决于设备、用户、应用程序、工具等的数量—这是给定生态系统无法完全消除的情况。然而，好的设计和自动化可以应对日常操作任务中的大部分复杂情况。

为此，生态系统的所有方面在设计时都必须考虑到简单性。实现这一目的的一种方法是移除碎片、抽象化功能和自动化工作流（请参见表 2）。一致的拓扑和通用策略，以及确保主动管理和方便故障排除的自动化，都是必不可少的。这种方法可以跨整个多云环境获得可靠、简化的解决方案。

试用 Contrail 和 AppFormix

您可以在安全的云托管环境中免费测试 Contrail 企业多云（云自动化平台）和 AppFormix（云操作优化工具）。访问 http://juniper.net/try。

©2018，Juniper Networks, Inc.

表 2：应对复杂性

操作	如何开始
移除	云公司通过明智的设计减少网络元素的总数量，从而在运营方面进行了创新。例如，他们： 1. 通过在可灵活扩展和适应增长的基础架构上采用单个架构，消除了不同架构的复杂性。 2. 尽可能使用通用构建块来简化培训、维护和更换。 3. 从他们的设备中删除了许多协议，保留少数几个（不到 10 个）由软件自动化和控制驱动的协议。 4. 标准化连接选项和协议，以便跨环境和工作负载进行一致的部署过程。 5. 更频繁地更新网络设备，而不是一用多年，使一切保持最新并创建操作一致性。 这些设计方法将帮助企业简化多云设计和运营。
抽象化	要使今天的网络正常工作，操作人员必须拥有跨多个设备的专业知识。如果网络涵盖多个供应商，则操作人员必须了解每个供应商的精确语言、语法和细微差别。 虽然这一方法在过去几十年中得到了改进，并有逐步的改变和发展，但它最终导致网络复杂、脆弱且不可预测，在需要改变时实行严格控制就证明了这一点。 抽象化控制的理念允许操作人员将整个网络作为单个实体来管理，而不是一次管理一个设备或交换矩阵。抽象化使操作人员能够在一个位置执行工作流、获取信息、处理集成和插入策略。 在多云设计中考虑抽象化时，架构师应将重点放在： 1. 识别抽象点，以及这些抽象点将如何对网络解释和传达意图。 2. 使操作人员和开发人员能够以对其角色直观的语言与点进行交互。 3. 将控制点转换成所有代表的设备和命令。 考虑到多云的范围意味着异构环境，架构师如何规划抽象化是总体设计的一个重要部分。
自动化	IT 运营商应该考虑自动化是如何提高敏捷性和效率的，又是如何提高可靠性的。指望不会发生网络中断是不现实的；最好的策略是通过实现网络操作自动化来积极规划中断，确保服务始终可用。 架构师可以重新构建自动化对话，以获取好设计决策中的全部优势： 1. 许多团队并不知道他们要实现什么自动化。自动化的主要目标不应该是消除击键操作，而是改进事物的运作方式。延迟和故障发生在事物的边界上：人员、系统、组织。正是在这些由人员和流程定义的工作流切换中，自动化对其产生的影响最大。 2. 自动化的关键在于将数据从一个实体移至另一个实体。这意味着自动化传输的是数据。自动化设计必须考虑如何交换数据并确保对数据达成共识。 3. 确定高价值工作流和数据交换方法后，组织必须确定如何设置并使用自动化工具。无论意图高度如何，以及系统中是否存在自主传感器、逻辑和执行器，都将由人来推动变化，并提供对系统状态的洞察力以实现数据驱动决策和服务级可观测性。

端到端和自上而下

讨论多云时，架构师必须小心不要缩小设计范围并冒险加剧上述挑战。

由于用户和应用程序都可以在任何位置，因此真正的多云设计必须包括适应完全通信的完整的端到端角度。例如，用户可以从园区、远程分支机构、家庭办公室或公共场所访问应用程序，而应用程序可以部署在内部数据中心、各种公有云中，或者动态地移动到边缘计算和无服务器环境，在这些环境中，它们只能存留很短的时间。由于应用程序必须对所有用户都可用，无论用户在哪个位置，多云架构均应触及网络中的所有位置。

架构师必须考虑的还不仅仅是用户和应用程序之间的连接。仅允许数据包流动是不够的；多云还需要从上到下扩展网络功能，以保护一切、监控性能和编排策略。集中管理多云环境需要端到端编排来实施策略和启用自动化，需要端到端的可见性来了解资源、用户和应用程序所在的位置。还需要端到端安全来保护用户、应用程序和数据。图 1 描述了完整的端到端、从上而下的多云设计。

©2018，Juniper Networks, Inc.

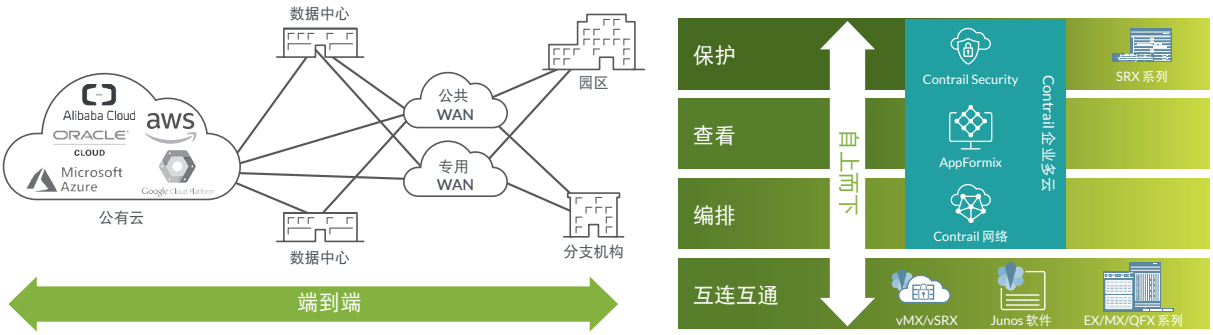


图 1：端到端和自上而下多云设计

多云架构概述

考虑到多云设计的范围和潜在挑战，多云的主要构建块可分为三层（请参阅图 2：）

- **基础资源：** 构成任何工作负载基础架构的底层计算、存储、网络和安全要素。
- **工作负载管理：** 工作负载结构，如虚拟机 (VM)、容器和无服务器架构，以及更广泛的工作负载生命周期管理框架，如 OpenStack、Kubernetesc、OpenShift 和各种公有云。
- **服务消费：** 最终，用户通常通过应用程序使用服务。该层通过透明地将基础管理层和工作负载管理层抽象化为每个应用程序的一组服务来分离基础架构和服务。

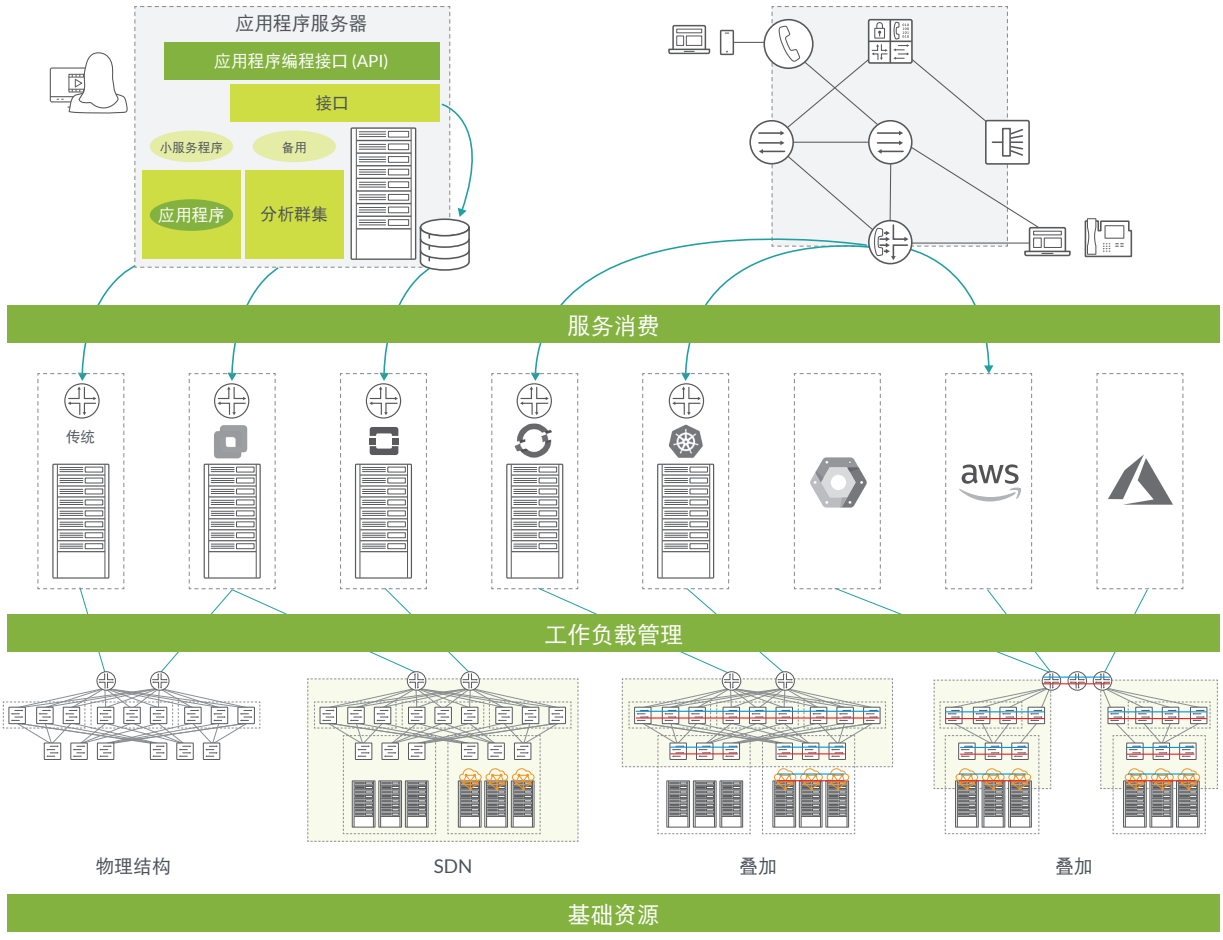


图 2：多云架构概述

基础资源

从网络角度来看，基础资源主要负责传输。租户、用户和应用程序跨共享底层基础架构获取逻辑叠加连接。该层还包括全权管理它的主要管理结构，如 SDN 控制器（包括叠加管理器）。

由于底层网络必须跨越数据中心、云以及应用程序和用户驻留的任何位置，因此它包括在内部和公有云上部署的物理和虚拟设备组合。对通用编排层的需求要求底层设备具有基于标准的可编程接口；组合使用封闭的专用系统只会导致复杂性提高。

交换矩阵

多云致力于将底层、叠加和公有云统一为单个通用交换矩阵，该交换矩阵跨越整个基础架构利用统一运营框架（请参阅图 3）。此联合交换矩阵使用一组通用协议创建，以便组合不同的基础架构，并使硬件和软件（包括虚拟设备和云原生基础架构）无缝共存。

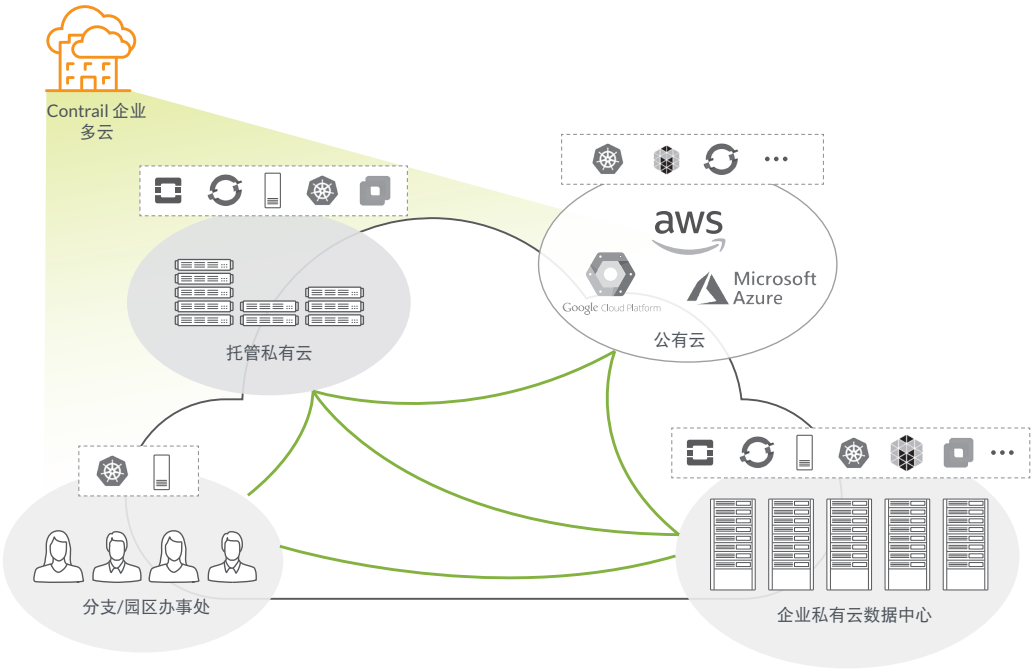


图 3：多云通用交换矩阵

过去几年来，数据中心网络在脊叶式架构上实现了标准化。此 Clos 网络类型将交换基础架构层连接在非阻塞模式中，为东西流量简化网络和减少延迟。

网络团队使用此架构构建两种类型的交换矩阵：在 2 层运营的以太网交换矩阵，以及在 3 层运营的 IP 交换矩阵。随着越来越多的应用程序设计为在 L3 运行，许多组织选择将其底层网络作为 IP 交换矩阵运行。将网络设计为兼具简单 IP 交换矩阵底层和精心编排的叠加，为对更动态网络日益增长的需求提供支持，以便跟上新应用程序需求所引发的频繁变化。

为了实现这些优势，超大规模用户（AWS、Azure、Google 云等）将其网络构建为一个具有逻辑叠加的 IP 交换矩阵，并且许多企业现在也采用此设计。此外，该方法允许使用标准协议构建网络，从而允许在网络中保留多个供应商，既可作为首选供应商，又可进行多次供应商过渡，从而减少供应商锁定。

©2018，Juniper Networks, Inc.

IP 交换矩阵

将网络作为 IP 交换矩阵来操作，提供了与应用程序的直接 L3 连接，以及更大的规模和弹性的优势。需要 L2 时，以太网 VPN 虚拟可扩展 LAN (EVPN-VXLAN) 转换 IP 交换矩阵以支持端到端以太网连接。IP 交换矩阵上的以太网连接标准是 EVPN-VXLAN（请参阅图 4），它允许网络团队在不依赖专有协议的情况下构建交换矩阵。这也使得部署多供应商网络成为可能，反过来使企业能够在不必搁置现有资产的情况下发展。

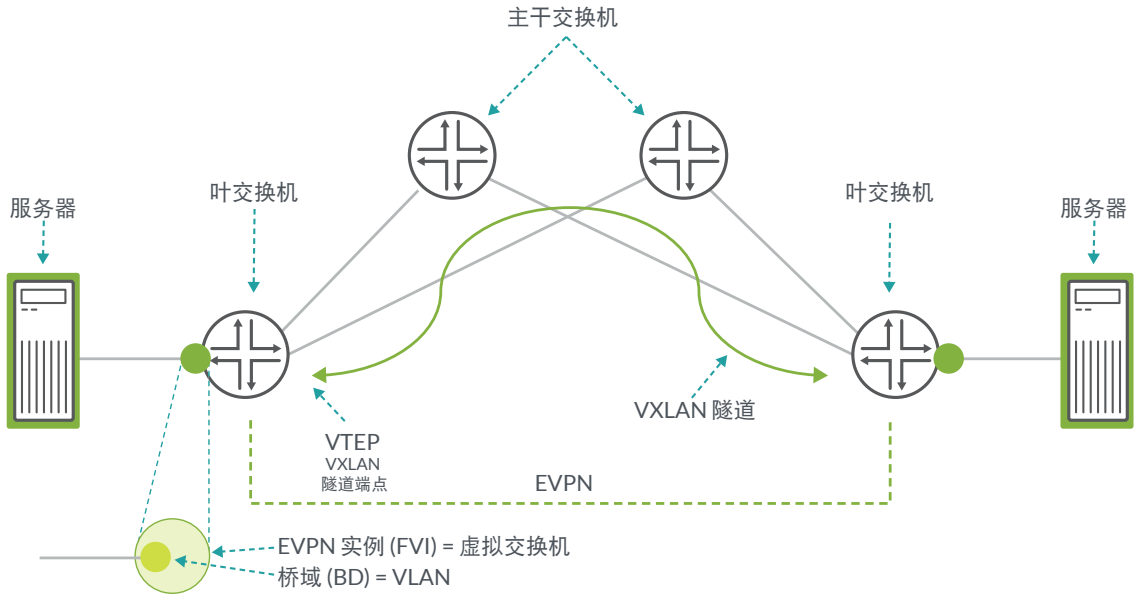


图 4：EVPN-VXLAN 架构

由于 EVPN 在 L3 IP 交换矩阵上运行，它通过减少对生成树等脆弱的 L2 结构的依赖，简化了网络。尽管大多数刚起步的架构师会选择 L3 而不是 L2，但他们的数据中心实际存在传统应用程序和设备。对于应用程序依赖于 L2 连接的企业，EVPN-VXLAN 通过封装（隧道）以太网帧来跨路由接口扩展 L2 域。L2 和 L3 共存使 EVPN-VXLAN 成为加速从传统环境过渡到现代多云环境的理想技术。

此外，该技术可在服务器节点和硬件网络设备上发起/终止 EVPN-VXLAN 叠加，使同一叠加能够跨越物理和虚拟元素并创建单个无缝交换矩阵。

EVPN-VXLAN 可通过 CLI 使用 Ansible 等自动化工具配置。它还可以通过瞻博网络® Contrail® 企业多云等多云编排器的统一托管界面 Contrail 命令（请参阅图 5）来编排底层和叠加设置。

试用瞻博网络 vQFX 和 EVPN-VXLAN

下载具有预建 EVPN-VXLAN 网络的免费瞻博网络 vQFX 虚拟化数据中心交换机软件，并在笔记本电脑或台式机上构建虚拟网络。访问 https://www.juniper.net/vqfx，试用软件功能以了解有关 QFX 系列数据中心交换机以及如何构建 EVPN-VXLAN 交换矩阵的更多信息。

©2018，Juniper Networks, Inc.

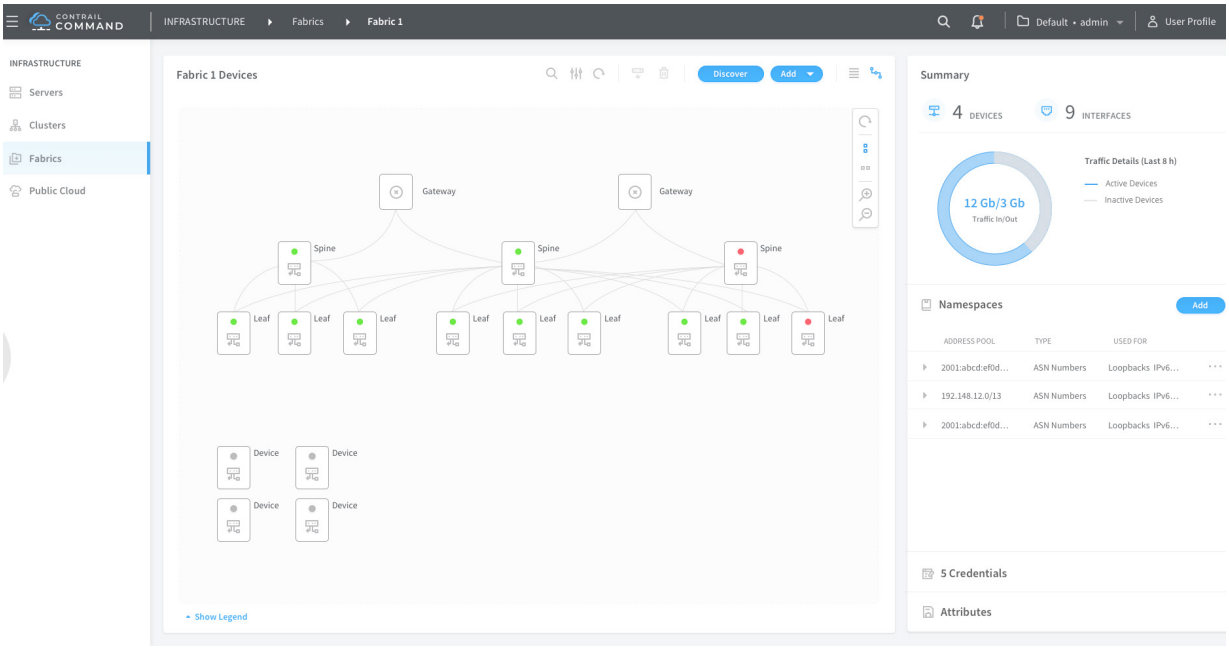


图 5：统一多云管理

多云交换矩阵由三个主要元素组成，如表 3 中概述。

表 3：交换矩阵元素

元素	功能	描述
控制平面	如何在端点间交换信息	实施通用交换矩阵的一个重要方面是设备使用其自己的本地控制平面，使它们能够使用 EVPN 作为交换控制情报的机制进行连接。作为 BGP 的扩展，EVPN 部署因其固有特性而享有无限规模和高可靠性。 与互联网一样，每个 BGP-EVPN 支持的设备在通过控制平面学习和推出本地发现的终端系统（或其他设备）时都独立运行。 BGP-EVPN 的其中一个优势是能够组合多个交换矩阵（请参阅图 6）。由于控制平面通过 BGP-EVPN 分发，相关的任何信息都可与其他设备共享，用于管理交换矩阵的新工具也可实现其操作自动化。
数据平面	如何传输流量	交换矩阵内的传输机制是 IP，因其广泛采用而能够创建简单开放的底层和叠加。 对于叠加，封装技术实施端到端连接。要保持供应商选择的灵活性，以便在新合同中发挥经济杠杆作用，应考虑 VXLAN（或 UDP/GRE 和 IPsec 上的 MPLS）等基于标准且广泛采用的封装协议。 专有数据平面机制会产生集成问题，导致交换矩阵不兼容。因此，利用 IP 作为数据平面协议至关重要。
管理平面	如何结合一切实现扩展和联合	管理平面的作用在于统一一切，在整个多云环境中实现自动化运营、可见性和系统集成。 为此，所有设备都必须是交换矩阵的组成部分，使得数据中心和私有云环境能够扩展到公有云并跨不同的域创建统一架构。这就创建了一个同质管理环境，在这个环境中，不管资源位于哪里，都可以相同方式使用。

©2018，Juniper Networks, Inc.

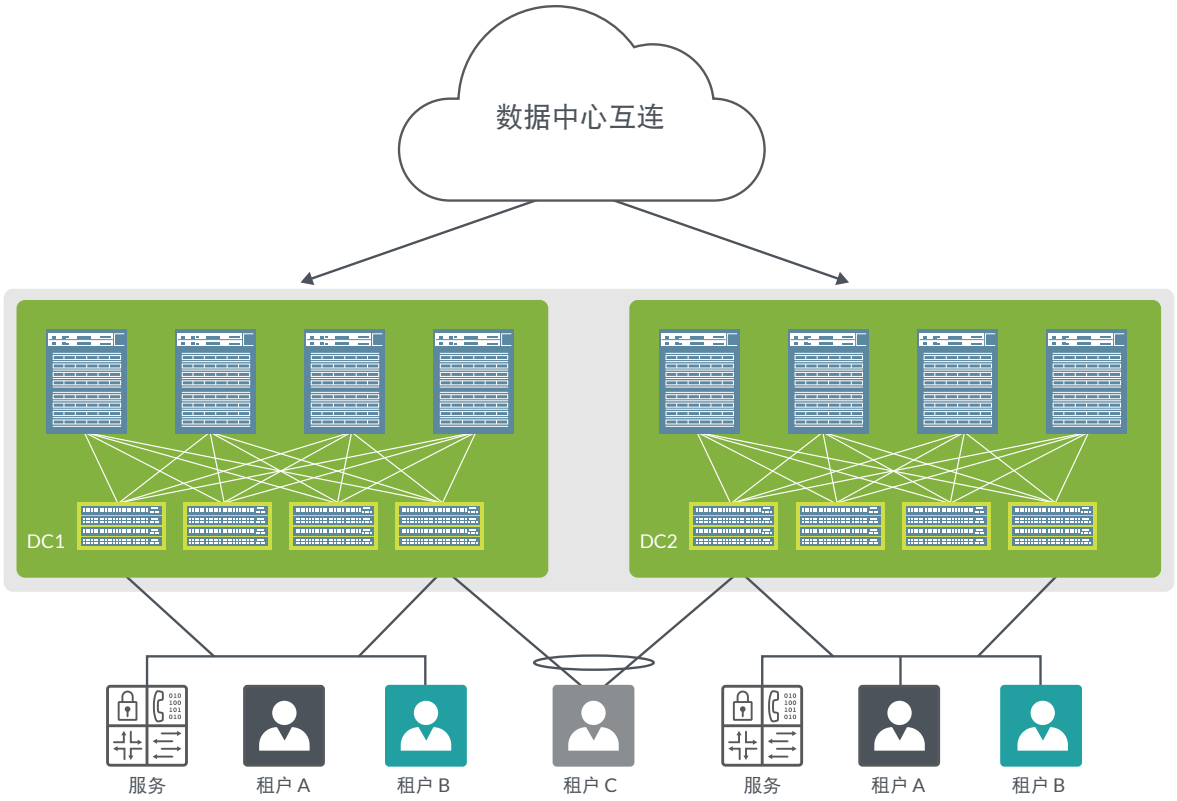


图 6：联合交换矩阵

基于意图的交换矩阵操作

交换矩阵操作通常集中在运行网络所需的工作流上 — 设置、扩展、维护、保证等。例如，部署新服务可能需要跨一组设备修改边缘策略。操作人员可以使用 Contrail 企业多云等中的交换矩阵自动化功能集中执行工作流，并跨网络将新策略推送至所有需要的设备，而无需在每个设备上更改策略配置。

在内部或云端集中部署的 Contrail 企业多云控制器可用作底层和叠加的主要控制点。Contrail 企业多云传输通过 GUI 中的模板工作流提交的用户意图，然后转换它以使用 JavaScript 对象标记法 (JSON) 或网络配置协议 (NETCONF) 等标准输出直接管理设备。这样，平台就能够从单个中央位置管理包含多供应商设备的异构网络并实现其自动化，显著简化交换矩阵操作。此类平台不会取代元素管理系统 (EMS)；EMS 将根据需要继续支持非常具体的请求的点配置。

统一数据中心和园区交换矩阵

如果简化操作对于成功部署多云至关重要，那么尽可能推动通用架构也同样重要。否则，管理员别无选择，只能解释并手动遍历存在操作唯一性的不同环境。

瞻博网络的解决方案允许企业跨园区和数据中心利用同一架构。在短期内，这些域可能以独立的孤岛形式存在。但是，随着企业向多云发展，就创造了机会来管理具有通用框架的园区和数据中心，以及借助 Contrail 企业多云支持过顶策略和控制。此外，旗舰式瞻博网络 Junos® 操作系统的通用 EVPN-VXLAN 实施在瞻博网络 QFX 系列数据中心交换机、EX 系列以太网交换机和 MX 系列 5G 通用路由平台及其虚拟同等平台内部运行。

©2018，Juniper Networks, Inc.

工作负载管理

编排提供了满足动态应用需求的抽象化网络，通常无需重新配置底层网络。因此，网络编排必须与自动化操作相结合，才能启动和处理新工作负载实例。

如今迁移到多云的企业使用三个基本工作负载管理策略和一项应急技术。大多数企业可能使用裸机服务器（有时是平台即服务产品的一部分）、虚拟机（通常由 VMware 或 OpenStack 产品托管）和容器（通常是由 Kubernetes 和 OpenShift 托管的 Docker 运行时）的组合。这些技术既在内部提供，也在公有云产品中提供。企业还可以采用新兴的无服务器方法，在这种方法中，应用程序的碎片可以在不同的云服务器上按需执行，而不是作为一个单点或几个层运行。

挑战在于，即使在中等大小的环境中，应用程序架构也可能使用这些技术的组合。随着引入的虚拟化和云计算技术及服务数量不断增加，网络和网络安全必须改变它们支持工作负载的方式。

特定于实例的应用程序环境

由于应用程序与网络相关，因此在很大程度上依赖于边缘设计和策略。也就是说，应用程序体验、安全和拓扑都依赖于 VLAN、服务质量 (QoS) 和防火墙过滤器（或 ACL）等策略结构以及加密。

多年来，网络一直是一门相当静态的学科。因此，要跟上由现代应用程序实践支持的工作负载开发和管理方面的快速变化，对一些人来说尤其困难。

虽然在一个环境中生成一个新虚拟机或容器的机制并不特别强大，但将多个环境视为可替换资源并在任何这些环境上启动各种计算工具的前景令人望而生畏。如今向新环境提供连接性和应用一致的策略通常是手动过程。配置连接需要指定边缘策略，而在每个环境中处理边缘策略的方式都不同。例如，在内部或私有云中配置与在 AWS 或 Azure 中配置不同；为虚拟机配置与为容器配置也不同。

此外，将传统安全模型应用到云或容器（以及应用到仅存在几秒钟就会再次出现在别处的边缘计算或无服务器进程）时，外围、执行点、关联等安全结构将需要由过去执行的操作进行演变。考虑到位置的概念，如在“我的数据中心”与“公共提供商”中，攻击面突然变得更广、更多样化，且入口点也比至今为止 IT 必须保护的全部都要多。

随着威胁性质的不断变化和演变，从工作负载启动直至停止的各个环节都必须迅速部署和维护安全。工作负载生命周期管理活动和适当安全策略的应用程序之间不允许有延迟。不管是访问控制、身份验证和加密、入侵检测服务/入侵防御系统 (IDS/IPS)，还是一些其他安全服务，都必须始终启用并更新策略。

复杂性也可能影响安全。如果管理在运营上很复杂，也可能影响安全效力。企业不能长时间依赖由操作人员手工执行的繁重工作流。如果要为企业提供足够的保护，解决方案必须是简单的、多域的和动态管理的。

在设计支持工作负载管理的网络和安全时，架构师需要考虑三个方面：工作负载抽象化、叠加控制以及统一底层和叠加管理。

工作负载抽象化

工作负载抽象化是实现网络中工作负载管理自动化的第一步。多云编排工具必须能够以与底层基础架构无关的方式表达策略（应用程序体验和安全两方面）。

抽象策略的基本功能是将需求表达为意图。瞻博网络 Contrail 企业多云通过其控制器提供工作负载抽象化，从而使用其底层工作流引擎将意图转换为设备或系统特定的命令。用户与工作流模板（此处为策略定义）交互，控制器将表达的意图转换为对每个系统、EMS 和设备类型支持的基础架构的南向调用，包括物理及虚拟设备；无论位于内部还是云端。定义一次意图，转换好意图，可使操作人员通过一个平台在整个网络上一致应用策略。

Contrail 企业多云通过将其虚拟路由器 (vRouter) 用作每个特定工作负载（不论位于哪里）的策略实施点，在虚拟化环境中完成此操作。对于在裸机服务器上运行的应用程序，控制器管理架顶式交换机端口以设置并应用策略。

虽然 vRouter 和其主机操作系统一起本地安装在服务器内核上（图 7），它也可部署在虚拟机中，部署为虚拟私有云 (VPC) 网关，或部署在公有云实例中。vRouter 评估资源（如果是 VPC 则评估资源池）中的入口流量，并实施定义的策略。这为在分布式防火墙模型中实现应用程序体验控制和应用程序安全性提供了一个位置。该方法支持微分段，这是为个别工作负载定义深入策略和保护的功能。

©2018，Juniper Networks, Inc.

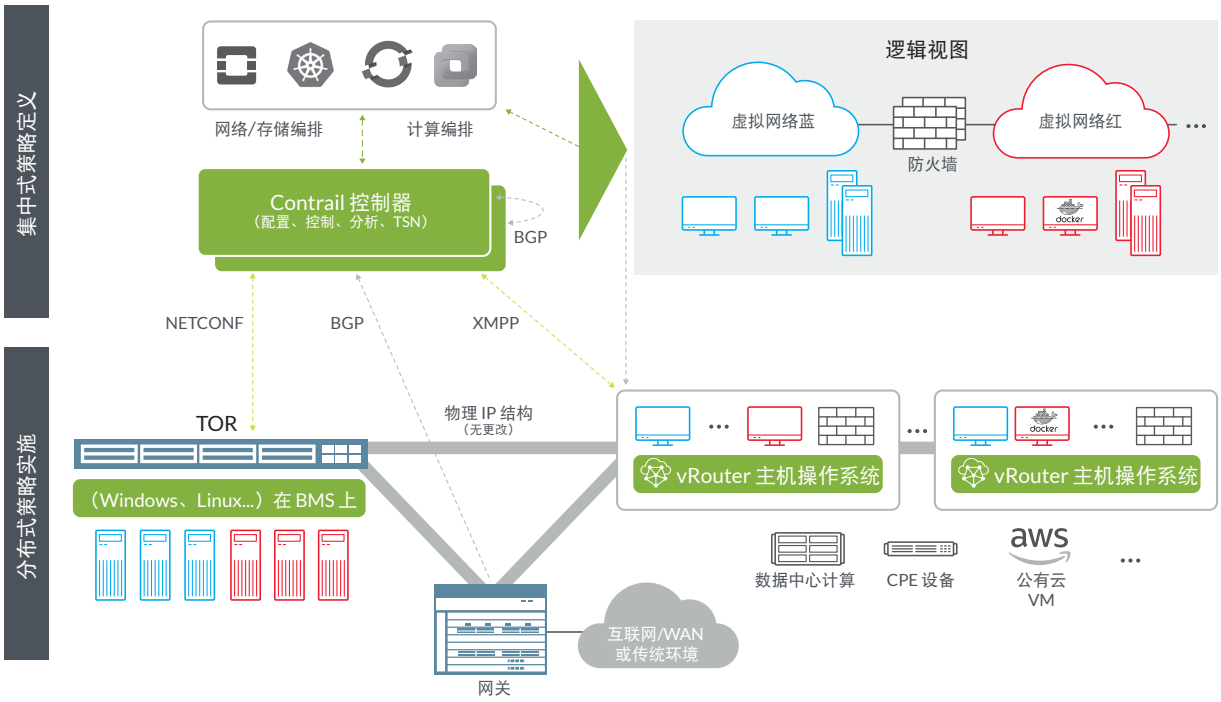


图 7：Contrail 架构

Contrail 企业多云可让操作人员从单个中央位置跨所有可能执行应用程序的环境统一编排和管理策略。该解决方案支持在内部、私有云或公有云（AWS、Azure、Google 云等）中的虚拟机或容器中运行的工作负载。Contrail 企业多云提供包含一致且高细粒度服务（路由、防火墙、NAT、负载平衡器等）的虚拟网络，全部都扩展至工作负载级别。其中包括以下虚拟化环境，实现现代多云所需的动态控制水平（请参阅图 8）：

- 运行 VMware ESXi/vCenter 环境的私有云虚拟机
- 运行 OpenStack 的私有云虚拟机
- 私有云 Docker 容器
- 公有云虚拟机或容器

©2018，Juniper Networks, Inc.

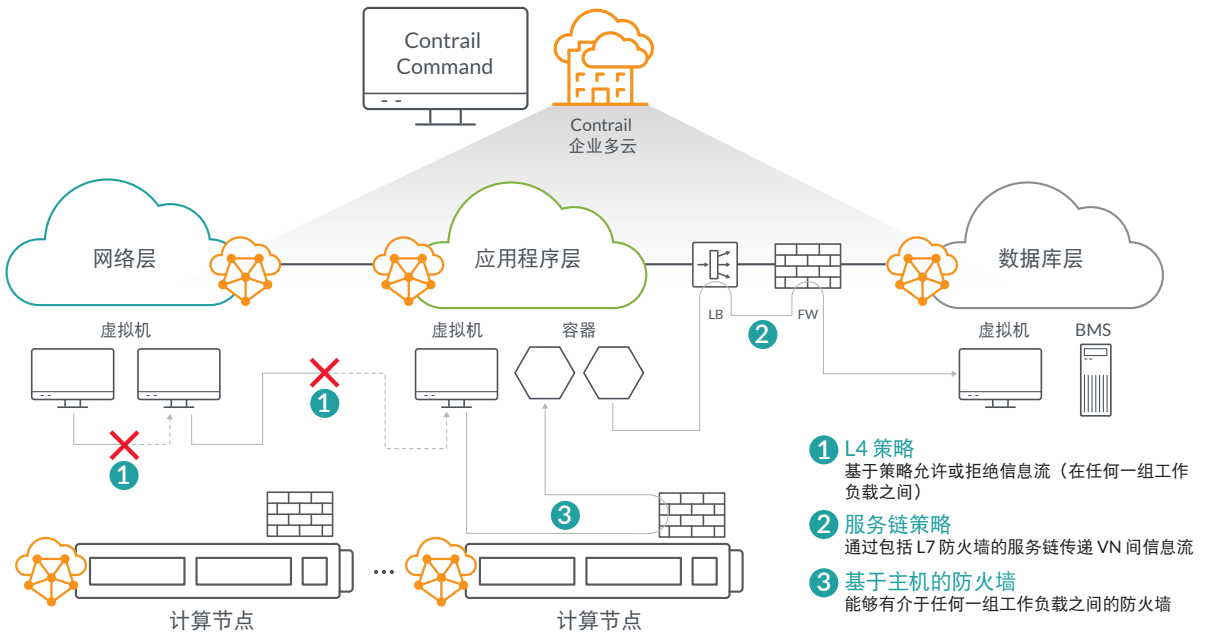


图 8：策略和控制

叠加控制

多云中的工作负载管理的第二大需求是随处使用既定 EVPN-VXLAN 交换矩阵的叠加控制。如果根据需求跨多云启动和停止应用程序实例，网络必须能够为这些应用程序动态设置新安全路径。

叠加网络是允许应用程序以这种方式运行的关键。了解工作负载、数据和用户所在的位置，以及相关的基于角色的权限，就可以让应用程序运行。为此，必须根据应用程序的安全连接要求自动配置叠加。

通过使用叠加，将边缘策略应用到叠加端点，包括与工作负载关联的 vRouter（请参阅图 8）。管理这些连接和安全策略是叠加控制器的责任。通过使用基于意图的工作流，Contrail 企业多云可跨任意数量的端点（不管所处位置在哪里）配置这些策略，从而为操作人员提供一个统一多云方法。

设计还允许在叠加端点即接近工作负载的地方加密流量，对来源进行加密。安全叠加环境意味着流量以完全加密的形式发送至底层 — 使用由第三方云提供商所有的公有云基础架构时尤其重要。

统一底层和叠加管理

最后，要简化日常运营，架构师应考虑结合了底层和叠加管理与关联的单个平台，如 Contrail 企业多云。Contrail 企业多云支持交换矩阵管理和异构计算环境，包括裸机服务器、虚拟机、容器和网络设备；私有云和公有云；以及网络和安全策略编排，包括微分段，从而满足一系列广泛的多云管理需求。

服务消费

衡量任何多云部署是否成功的最终指标是底层基础架构是否对用户透明。多云的目标是允许根据成本等业务和职能需求在任何位置部署工作负载。不应使用户察觉到工作负载是从私有云还是公有云提供。

要做到这一点，网络必须最终集成到应用程序层，包括连接性和安全性，以及如何部署和使用新的应用程序和服务。多云架构的这个顶层通过透明地将较低层抽象化到每个应用程序所需的服务集中，将基础架构和服务分离。

通过将服务与底层基础架构分离，设计建立了安全多租户，将服务彼此隔离。隔离机制只允许服务基于操作人员指定的意图进行通信，同时执行连接和安全策略。

下面的部分描述了在应用程序开发过程中，如何紧密集成多云网络和应用程序，以响应实时情况并作为服务感知结构的一部分。

©2018，Juniper Networks, Inc.

应用程序开发生命周期

大多数现代应用程序遵循开发-分阶段-生产生命周期。应用程序运行的位置，及其网络和安全需求，将随每个应用程序通过其生命周期的各个阶段的不同而发生变化。

Contrail 企业多云通过使用标签来单独处理这些阶段，每个阶段都有自己的网络和安全环境，以及不同应用程序阶段的独立策略。因为策略可以绑定到这些阶段中的每一个阶段，所以它建立了一个强大的多云结构，开发人员可以在其中使用特定的安全策略为某个网络设置创建和验证应用程序，然后将该环境部署为连续集成和连续交付 (CI/CD) 应用程序管道的一部分（请参阅图 9）。标签还允许进行更高层次的抽象，从而导致与位置无关。通过标记对象，操作人员现在可以在任何阶段任何地方使用特定的策略关联。

1. 降低复杂性（较少的策略数量）
2. 简化管理（更改控制等，使其更加简便）
3. 改进可扩展性
4. 定义/审查/立即批准 -> 在任意位置使用

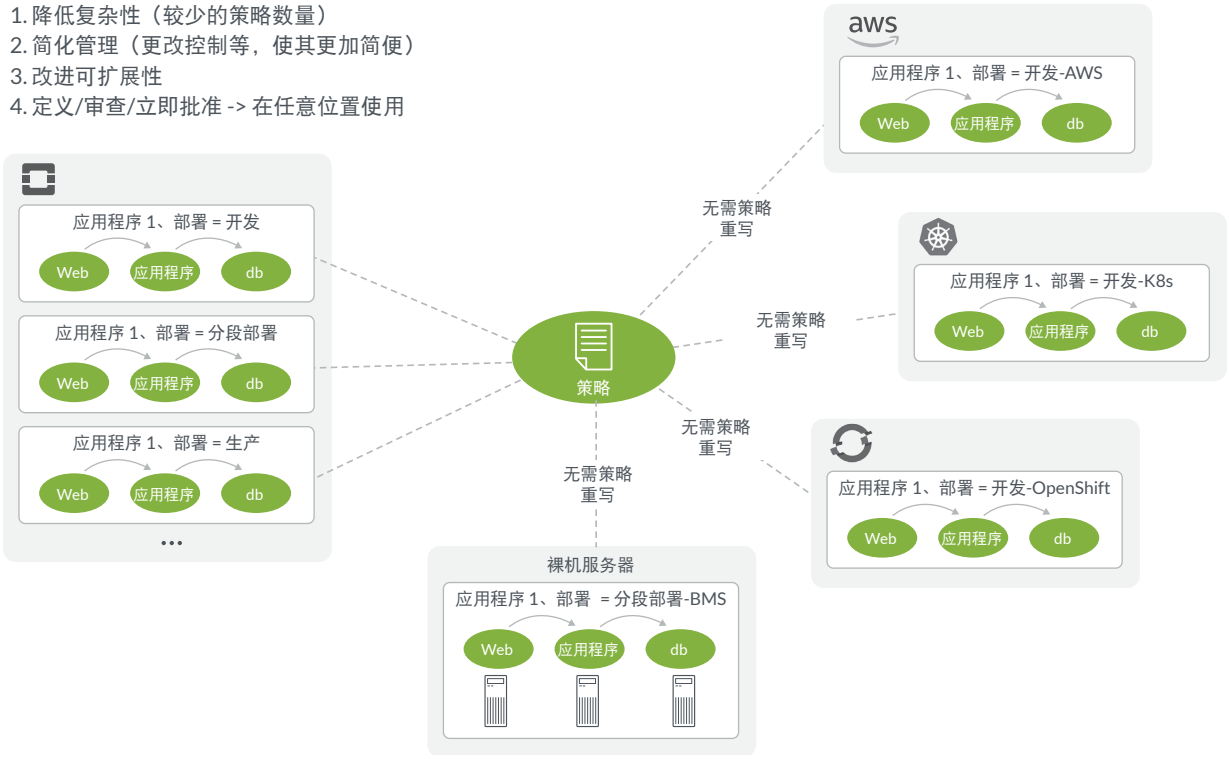


图 9：简化的策略实施

通过将网络和安全集成到应用程序环境中，瞻博网络打破了应用程序工作流与网络团队之间的传统分离，形成一个更加无缝的过程，该过程可提高速度，并支持更广泛的企业敏捷性目标。

服务感知网络

在确定网络和应用程序如何协同工作时，架构师必须考虑如何根据基础架构的实时条件满足动态应用程序需求。传统上，网络和提供服务的应用程序是独立处理的。应用程序通常假定网络提供零损失、低延迟连接，而网络大多不知道应用程序在做什么。

软件定义 WAN (SD-WAN) 等技术的兴起提供了一个动态调整策略的机会，以便为特定应用程序和用户需求优化网络性能。例如，在关键或带宽密集型活动（如灾难恢复）期间卸载流量是最大程度地减少对宝贵 WAN 资源的影响的有效方式。或者，异常网络事件可能会触发关键资源的隔离和特定工作负载的隔离。这两种情况的关键都在于从基础架构向控制实体提供实时遥测，以便进行事件关联和动态补救或警报。

在架构上，这些用例需要一些收集和分发数据的方法。现代分布式架构将消息总线与侦听器（如能够执行实时分析的收集器）配合使用，这对基础架构中事件和状态信息的实时传送非常重要（请参阅图 10）。

©2018，Juniper Networks, Inc.

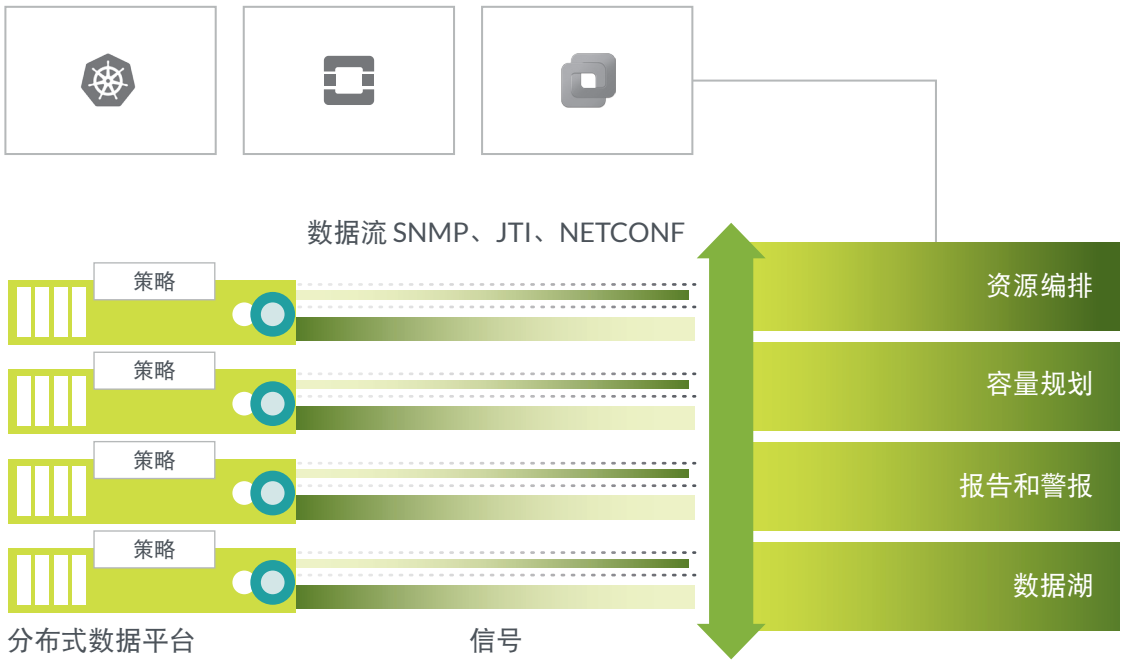


图 10：高级分析

在底层，设备可能使用类似 Google 的开源 gRPC 等技术，这是瞻博网络产品组合中的常见功能。在较高层元素中，基础架构性能监视 (IPM) 和应用程序性能监视 (APM) 工具跨关键物理和虚拟资源提供对性能和利用率等方面的洞察力。确定有效性的关键是可用数据的丰富性，及其实时可用性的程度。像 SNMP 这样的传统协议在可用状态的广度和轮询性能方面都存在差距。无论采用什么流机制，数据通常都是通过消息总线分发的，消息总线向侦听器提供要执行的操作的相关信息。

将收集拓扑、寻址、位置、流量类型、速率、会话、命名空间等内容，然后分发到分析应用程序中，为做出有关路径选择或安全操作的明智决策提供必要的上下文。瞻博网络 AppFormix® 软件提供对环境的全面实时可见性，以及基于意图的分析。AppFormix 实时进行自动预防性补救，覆盖各种基础架构类型上的堆栈和操作层（请参阅图 11）。

©2018，Juniper Networks, Inc.

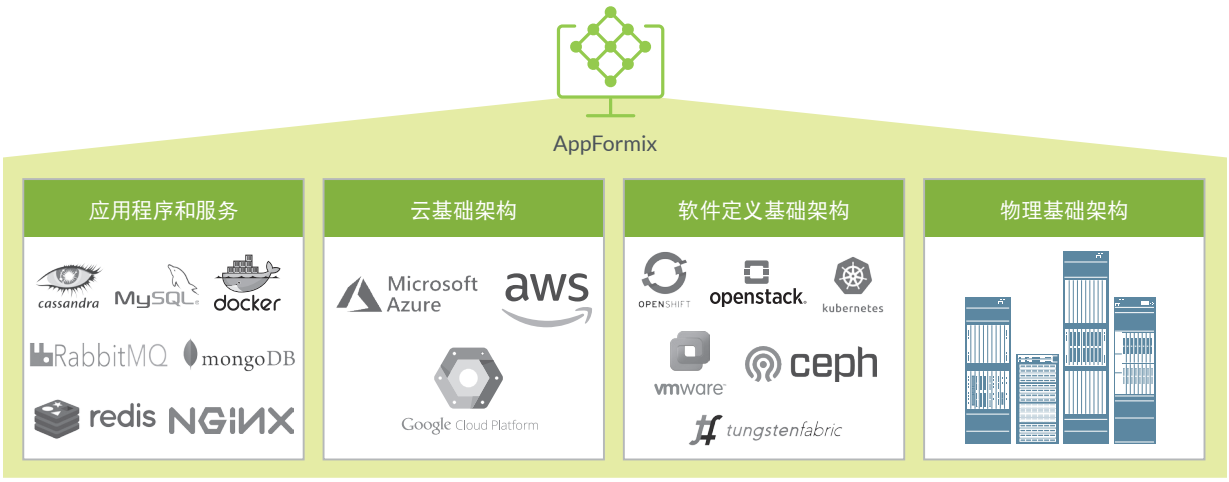


图 11：跨层可见性和分析

服务感知结构

随着时间的推移，多云部署将具有服务感知结构，跨当前和未来的所有技术孤岛提供一致的网络服务（请参阅图 12）。这些结构指定了从根本上与底层基础架构分离的服务详情，允许它们通过由多云控制器动态管理的策略转换进行应用。

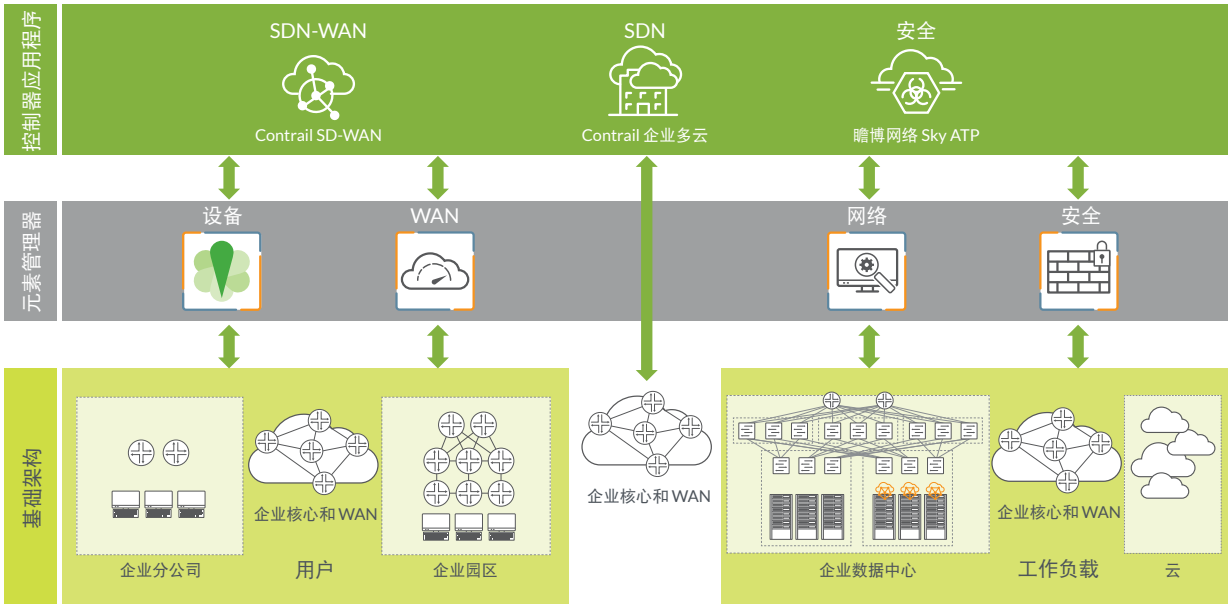


图 12：服务感知结构

经过身份验证的用户获得网络授权后，只要具备基于角色和用户的必要权限，应能够访问其域内存在的任何应用程序。提出请求时，多云控制器通过预定义服务感知结构了解用户的需求，然后服务感知结构定义在用户和应用程序之间建立最优连接所需的特定网络服务。这包括路径设置以及实施合适的应用程序体验（如网关的 QoE）和安全性（包括加密的传输或防火墙规则）的策略。

由于该结构不与基础架构绑定，如果工作负载移到其他资源池中，或在其他资源池中实例化，则该结构将跟随它到新资源。

©2018，Juniper Networks, Inc.

总结

应用程序创新正在助力今天的数字业务。应用程序开发和更新过程的加速，再加上工作负载可以在哪里运行的灵活性，给网络带来了相当大的复杂性，特别是运营复杂性。当组织开始将其应用程序工作负载从云迁移到多云，以及向更多虚拟化技术迁移时，就会出现挑战。网络不仅必须支持这些新的运营环境，还必须安全地支持与现有应用程序和数据的通信。

随着应用环境和需求的迅速发展，企业对网络设计、安全和运营提出了新的要求。一个能够跨多个云端到端连接和保护应用程序的多云，就像它们是一个云一样，可以让组织将资源优化为单个融合基础架构，并在整个过程中进行一致的操作。

这意味着运营商可以全面地管理在虚拟机、容器或裸机服务器、内部和公有云中运行的工作负载的网络，同时管理叠加和底层。他们可以基于与其角色有关的意图驱动的方向，端到端配置、执行工作流以及监控一切。这种到多云的迁移不仅仅是技术上的迁移；它需要企业发展他们的架构、流程和人员。

瞻博网络的多云蓝图包含多域连接、多供应商编排、端到端可见性和普遍安全性。瞻博网络解决方案使用单一编排平台跨多供应商环境指导通用策略和操作，帮助您管理多云的复杂性，而多云框架则为您的多云转换提供了方法驱动的迁移映射。

瞻博网络独特的方法允许您保持控制权，同时为应用程序开发人员和用户提供参与竞争所必需的敏捷性。

关于瞻博网络

瞻博网络引领网络创新。从设备到数据中心，从消费者到云提供商，瞻博网络提供彻底转变网络体验和经济效益的软件、硬件和系统。瞻博网络竭诚为全球客户和合作伙伴服务。如需了解更多信息，请访问 www.juniper.net。

公司和销售总部
Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, CA 94089 USA
电话：888.JUNIPER (888.586.4737)
或 +1.408.745.2000
传真：+1.408.745.2100
www.juniper.net

APAC 和 EMEA 总部
Juniper Networks International B.V.
Boeing Avenue 240
1119 PZ Schiphol-Rijk
Amsterdam, The Netherlands
电话：+31.0.207.125.700
传真：+31.0.207.125.701

JUNIPER NETWORKS | Engineering Simplicity

版权所有 2018 Juniper Networks, Inc. 保留所有权利。瞻博网络、瞻博网络徽标、瞻博和 Junos 是 Juniper Networks, Inc. 在美国和其他国家/地区的注册商标。所有其他商标、服务标识、注册商标或注册服务标识均为其各自所有者的资产。瞻博网络对本文档中的任何不准确之处不承担任何责任。瞻博网络保留对本出版物进行变更、修改、转换或以其他方式修订的权利，恕不另行通知。