HashiCorp

解锁云运营模式

在现代多云数据中心中实现最快的价值实现途径

白皮书

解锁云运营模式

执行摘要

现在是云需要工作的时候了。为了在数字转型驱动的多云架构时代蓬勃发展，企业 IT 必须从基于 ITIL 的网关管理演进为支持共享自助服务流程，以实现卓越的开发运营。

对大多数企业来说，数字化转型意味着更快速、更大规模地提供新的业务和客户价值。对企业 IT 来说，这意味着从成本优化到速度优化的转变。云是这一转变不可避免的一部分，因为它提供了以无限规模快速部署按需服务的机会。

为了解锁最快实现云价值的途径，企业必须考虑如何在云的每一层上实现应用程序交付过程的工业化：接纳云运营模式，以及调整人员、流程和工具。

在本白皮书中，我们将介绍云运营模式的影响，并为 IT 团队提供解决方案，以便在基础架构、安全防护、网络和应用程序交付方面采用此模式。

过渡到多云数据中心

向云和多云环境的过渡是 IT 的代际过渡。这种过渡意味着从私有数据中心中的大量专用服务器，转变为按需提供的计算容量池。虽然大多数企业都是从一家云供应商开始的，但有充分的理由使用其他供应商提供的服务，而且大多数全球 2000 强组织将不可避免地通过设计或兼并和收购，与多家云供应商合作。

云为新的“参与型系统”（即为吸引客户和用户而构建的应用程序）提供了速度和规模优化的机会。这些新应用程序是客户参与业务的主要界面，非常适合在云中交付，因为它们往往：

- 具有动态使用特性，需要在短时间内按数量级上下扩展负载。
- 承受快速构建和迭代的压力。许多这些新系统本质上可能是临时的，在事件或活动中提供特定的用户体验。

然而，对于大多数企业而言，这些参与型系统必须连接到现有的“记录型系统”—— 核心业务数据库和内部应用程序，它们通常继续驻留在现有数据中心的基础架构上。因此，企业最终会得到一个混合体 —— 多种公共和私有云环境的混合。

因此，大多数企业面临的挑战是如何将这些应用程序以一致的方式交付到云端，同时确保尽可能减少不同开发团队之间的摩擦。

使这一挑战更加复杂的是，底层原语已经从在自给环境中操纵虚拟机转变为在共享环境中操纵云“资源”。 企业便拥有了有竞争力的运营模式来维护其现有资产，同时开发新的云基础架构。

为了让云计算发挥作用，需要有一致的工作流，并可跨多个云供应商大规模重用。这需要：

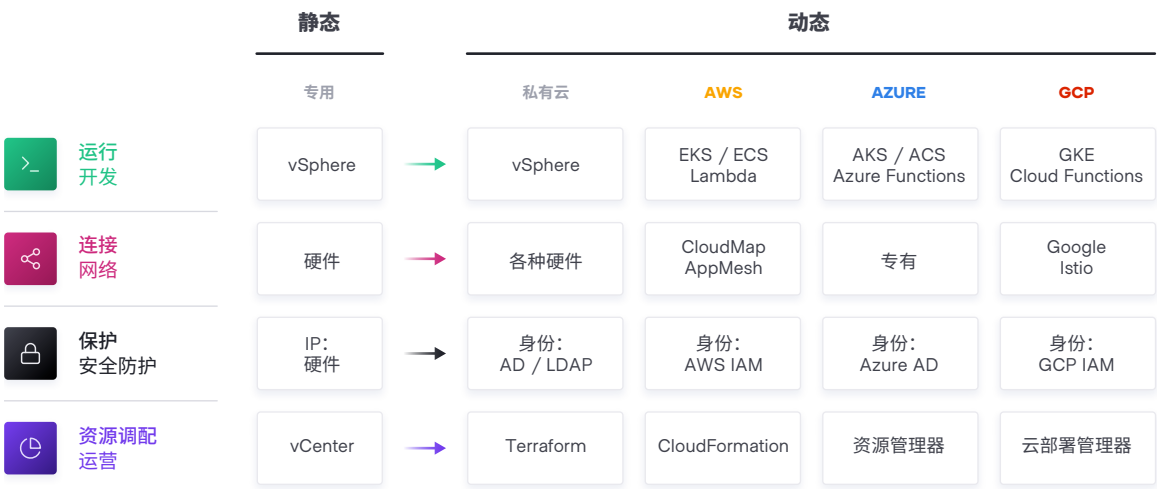
- 用于资源调配的一致指令集
- 用于安全防护和网络连接的身份
- 可以部署和运行的特权和权限

云运营模式的影响

向云过渡的本质影响是从“静态”基础架构向“动态”基架构础设施的转变：从关注静态 IT 资源群的配置和管理，到按需资源调配、保护、连接和运行动态资源。

分解这一影响，并处理堆栈，便能得到由方法衍生出的各种变化：

- **资源调配。**基础架构层从以有限的规模运行专用服务器过渡到动态环境，从而使组织能够通过启动数千台服务器并在不使用时缩小使用规模，来轻松适应不断增长的需求。随着体系结构和服务变得更加分散，计算节点的数量显著增加。
- **保护。**安全层从一个基本上“高信任”的世界过渡到一个没有清晰或静态周界的“低信任”或“零信任”的环境。因此，安全防护的基本假设从基于 IP 转变为使用基于身份的资源访问。这种转变对传统的安全模式具有极大的破坏性。
- **连接。**网络层从严重依赖于服务和应用程序的物理位置和 IP 地址过渡到使用**服务的动态注册表进行发现**、分段和组合。企业 IT 团队对网络或计算资源的物理位置的控制水平并不相同，必须考虑基于服务的连接性。
- **运行。**运行时层从将工件部署到静态应用程序服务器，转变为在按需供应的基础架构池上部署具有调度机构的应用程序。此外，新的应用程序已成为动态配置的服务集合，并以多种方式打包：从虚拟机到容器。



为了应对这些挑战，这些团队必须提出以下问题：

- **人。**我们如何使团队能够适应多云现实，无论目标环境如何，都确保技能得到一致的应用？
- **流程。**在保持合规和治理的同时，我们如何将中央 IT 服务定位为速度的自助服务促成者，而不是基于工单的控制把关者？
- **工具。**我们如何以最佳方式释放云供应商可用功能的价值，从而追求更高的客户和业务价值？

解锁云运营模式

由于云运营模式的影响会影响基础架构、安全防护、网络和应用程序的团队，我们看到企业反复采用一种模式，即建立中央共享服务（卓越中心），以在每一层交付所需的动态基础架构从而交付成功的应用程序。

随着团队为云运营模式交付每项共享服务，IT 速度也随之提高。一个组织的云成熟度越高，其速度就越快。

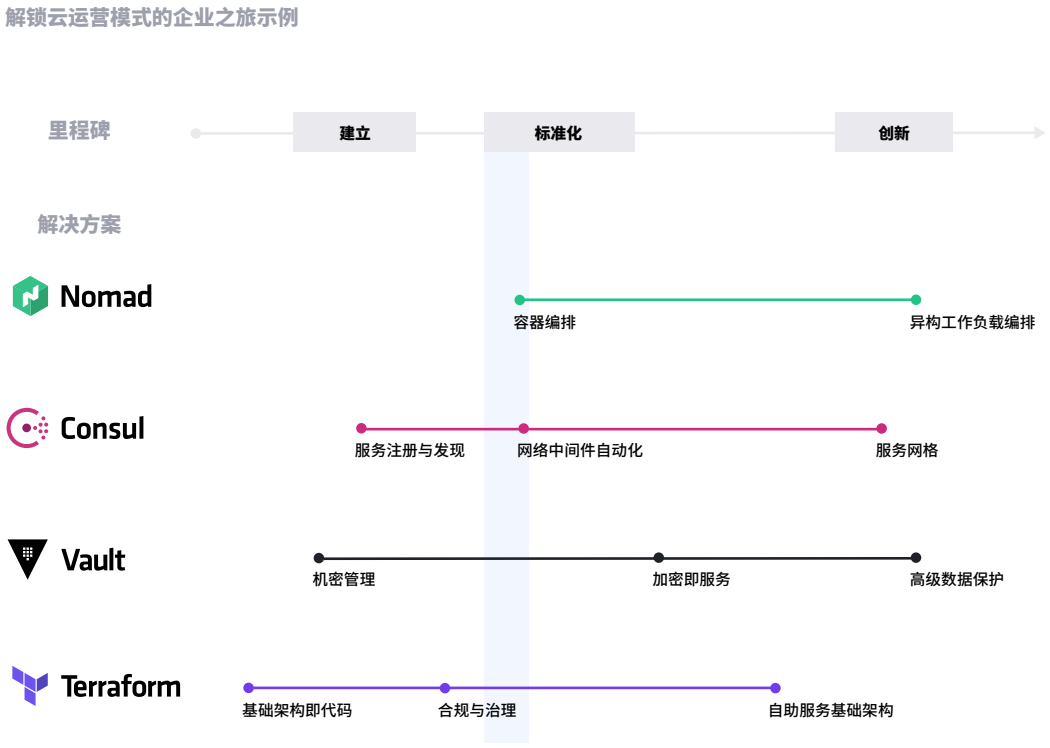
HASHICORP 堆栈的扩展使用，为我们的客户提高了成熟度和速度

我们看到客户在解锁云运营模式时所采用的典型流程，包括三个主要里程碑：

1. **建立云基础架构** - 在您开始云之旅时，最紧迫的要求是云基础架构资源调配，通常采用基础架构即代码，并通过机密管理解决方案确保其安全。这些都是最基本的必要元素，可以让您构建一个可扩展的、真正动态的、面向未来的云架构。

2. **在一组共享服务上实现标准化** - 随着云消费开始增加，您需要实施和标准化一组共享服务，以便充分利用云提供的功能。随着设置访问控制规则和跟踪需求变得越来越重要，这也带来了治理和合规性方面的挑战。

3. **使用通用逻辑体系结构进行创新** - 当您完全接纳云，并依赖云服务和应用程序作为主要参与系统时，将需要创建一个通用逻辑体系结构。这需要一个与扩展的云解决方案生态系统连接的控制平面，并固有地提供跨服务和多个云的高级安全防护和编排。



接下来，是我们见证的各组织成功采用的循序渐进的过程。

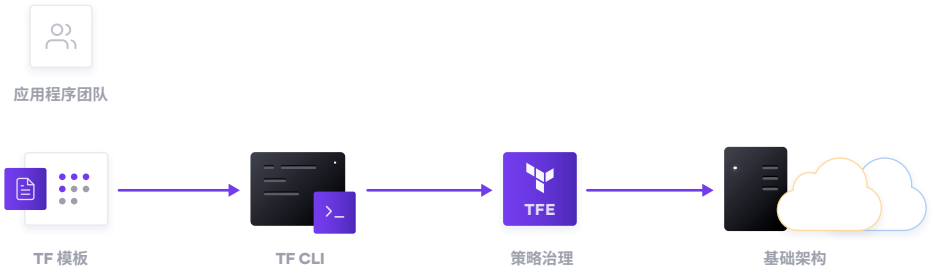
第一步：多云基础架构资源调配

采用云的基础是基础架构资源调配。HashiCorp Terraform 是世界上使用最广泛的云资源调配产品，可用于为任何目标平台使用一系列供应商的应用程序资源调配基础架构。

为了实现基础架构资源调配的共享服务，IT 团队应该从实现可复制的基础架构即代码实践开始，然后是分层合规审查和治理工作流，以确保适当的控制。

使用 TERRAFORM 前

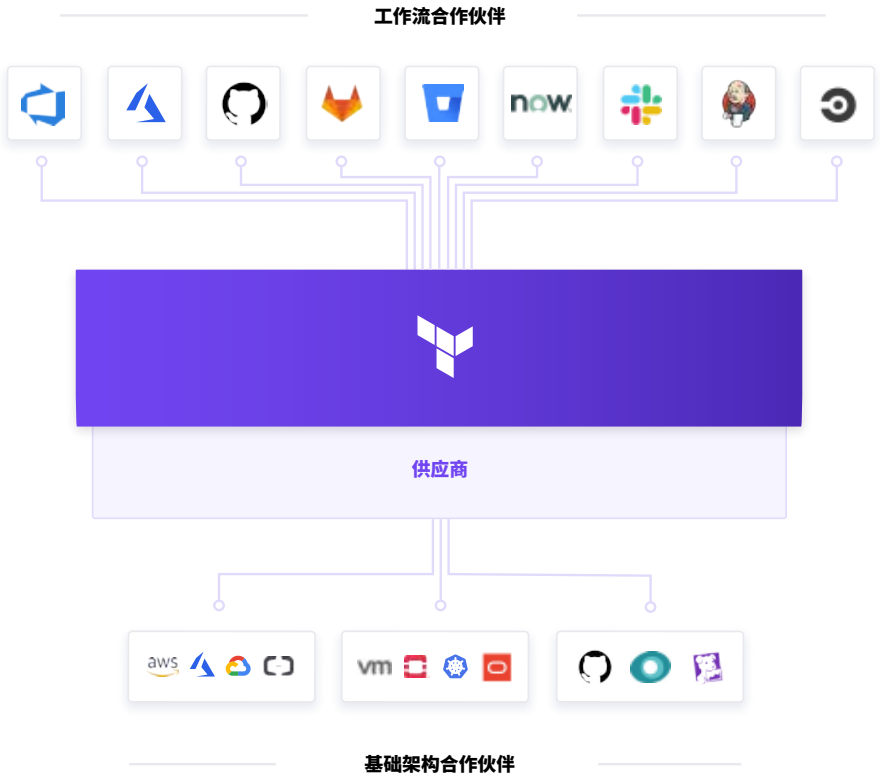
使用 TERRAFORM 后



可复制的基础架构即代码

基础架构资源调配共享服务的第一个目标是实现以代码形式交付可复制的基础架构，为开发运营团队提供一种在 CI/CD 工作流中，使用熟悉的工具规划和调配资源的方法。

开发运营团队可以创建表示一个或多个云平台服务配置的 Terraform 模板。Terraform 与所有主要配置管理工具集成，以允许在调配底层资源之后进行细粒度调配。最后，可以使用许多其他 ISV 供应商的服务扩展模板，以包括监控代理、应用程序性能监控 (APM) 系统、安全工具、DNS 和内容交付网络等。一旦定义了模板，就可以根据需要自动配置模板。在此基础上，Terraform 成为了跨公共和私有云调配资源的团队的*通用语言*和通用工作流。



对于自助式服务 IT，模板创建过程和资源调配过程的分离，大大缩短了任何应用程序上线所需的时间，因为只要开发人员使用预先批准的模板，就不再需要等待运营批准。

合规性和管理

对于大多数团队来说，还需要对所创建的基础架构类型、如何使用基础架构以及哪些团队可以使用基础架构实施策略。HashiCorp 的 Sentinel 策略即代码框架，提供了合规审查和治理，而不需要改变整个团队的工作流，并且也被定义为代码，从而支持对开发运营的协作和理解。

如果没有策略即代码，组织会求助于使用基于票证工单的审核流程来批准更改。这导致开发人员需等待数周或更长时间来配置基础架构，并成为一个瓶颈。策略即代码允许我们通过将策略的定义与策略的执行分离来解决这个问题。

集中化的团队编写策略，在所有云资源调配中实施安全防护、合规审查和运营的最佳实践。自动实施策略可确保更改符合法规要求，而不会造成手动审查瓶颈。

第二步：多云安全防护

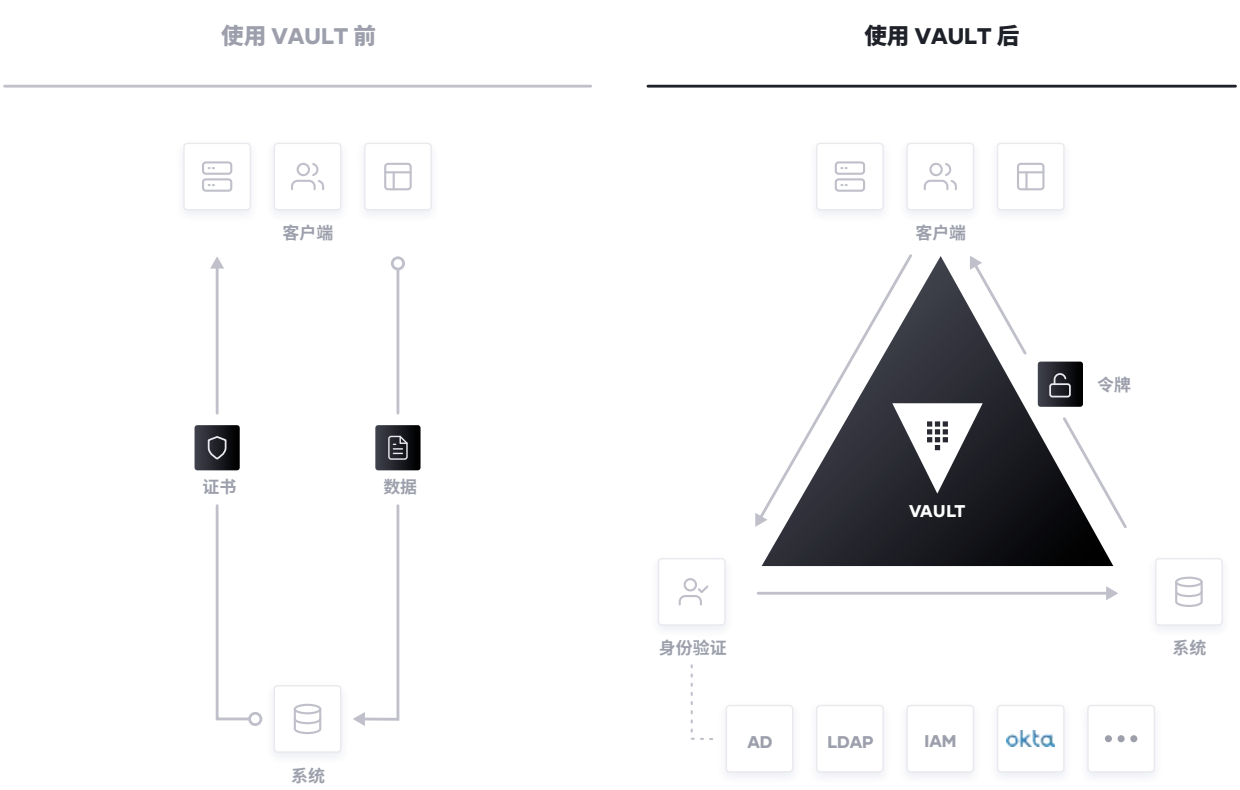
动态云基础架构意味着从基于主机的身份转变为基于应用程序的身份，跨越多云环境且没有清晰网络周界的低信任或零信任网络。

在传统的安全防护世界中，我们假设内部网络具有高信任度，这导致了外硬内软的局面。通过现代“零信任”方法，我们同时努力强化内部。这要求应用程序经过明确的身份验证，经授权获取机密和执行敏感操作，并通过严格的审核。

HashiCorp Vault 帮助团队安全地存储和严格控制对令牌、密码、证书和加密密钥的访问，以保护机器和应用程序。这提供了一个全面的机密管理解决方案。除此之外，Vault 还有助于保护静止的数据和传输中的数据。Vault 为开发人员提供了用于加密的高级 API，以确保敏感数据的安全，而无需公开加密密钥。Vault 还可以充当证书颁发机构，提供动态短期证书以保护通过 SSL/TLS 的通信。最后，Vault 支持在不同平台（如本地 Active Directory 和 AWS IAM）之间进行身份代理，以允许应用程序跨平台工作。

Vault 被广泛应用于证券交易所、大型金融组织、连锁酒店以及介于两者之间的一切，以在云运营模式中提供安全防护。

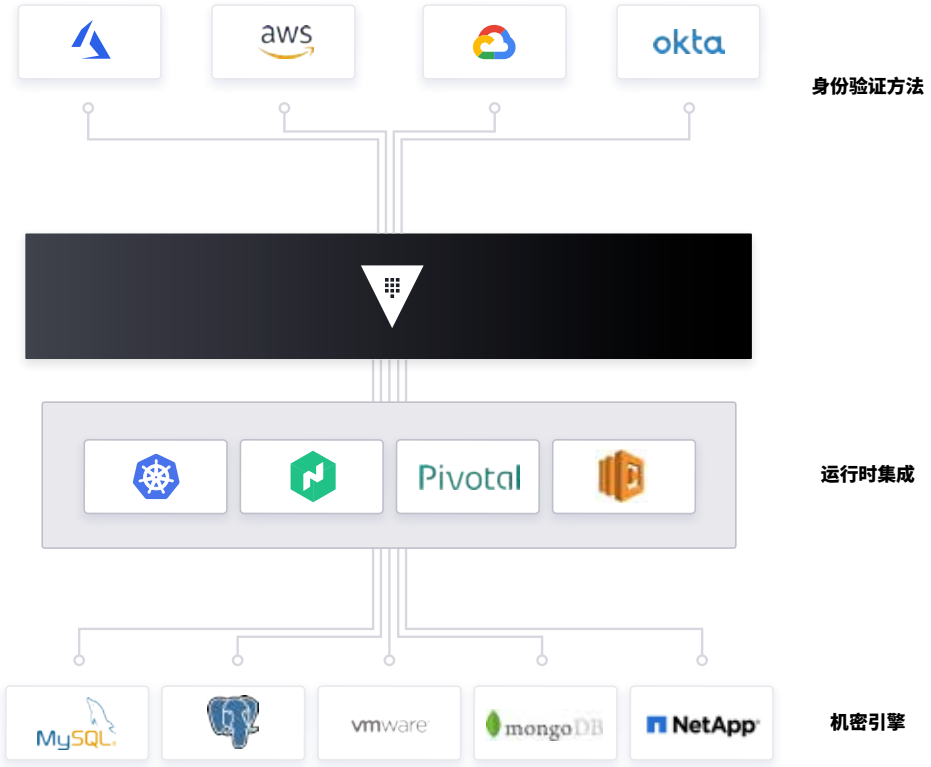
为了实现安全共享服务，IT 团队应该启用集中的机密管理服务，然后使用该服务提供更复杂的加密即服务用例，如证书和密钥轮换，以及传输和静止数据的加密。



机密管理

云安全防护的第一步通常是机密管理：中央存储、访问控制和动态机密的分发。与基于身份的访问系统（如 AWS IAM 和 Azure AAD）集成以进行身份验证和访问服务及资源，而不是依赖于静态 IP 地址，这一点至关重要。

Vault 使用策略来编码应用程序如何进行身份验证、授权使用哪些凭据以及应如何执行审核。它可以与一系列可信的身份提供者集成，如云身份和访问管理 (IAM) 平台、Kubernetes、Active Directory 和其他基于 SAML 的系统，以进行身份验证。然后，Vault 根据应用程序和用户身份的可信来源集中管理和强制访问机密和系统。



企业 IT 团队应该构建一个共享服务，通过一致、经审核且安全的工作流，为任何系统请求机密。

加密即服务

此外，企业需要加密静止和传输中的应用程序数据。Vault 可以提供加密即服务，为密钥管理和加密提供一致的 API。这允许开发人员执行单个集成，然后跨多个环境保护数据。

使用 Vault 作为加密即服务的基础，解决了安全团队面临的难题，如证书和密钥轮换。Vault 支持集中化密钥管理，以简化跨云和数据中心的传输及静止数据加密。这有助于降低昂贵的硬件安全模块 (HSM) 成本，并可通过组织内一致的安全工作流和加密标准提高生产效率。

虽然许多组织都要求开发人员对数据进行加密，但他们通常不提供方法，这让开发人员只能在没有充分了解加密技术的情况下构建自定义解决方案。Vault 为开发人员提供了易于使用的简单 API，同时为中央安全团队提供了他们需要的策略控制和生命周期管理 API。

高级数据保护

移动到云或跨混合环境的组织仍然维护和支持需要执行加密操作的内部部署服务和应用程序，例如静态存储的数据加密。这些服务不一定要想实施管理这些加密密钥的逻辑，因此寻求将密钥管理任务委托给外部提供者。高级数据保护允许组织在基础架构和 Vault 企业版之间安全地连接、控制和集成高级加密密钥、操作和管理，包括使用透明数据加密 (TDE) 自动保护 MySQL、MongoDB、PostgreSQL 和其他数据库中的数据。

对于对数据合规性（PCI=SS、HIPAA 等）、保护数据和以加密方式保护个人可识别信息（或 PII）匿名性有较高安全要求的组织，高级数据保护为组织提供了数据标记化功能，如数据屏蔽，以保护诸如信用卡、敏感个人信息、银行号码等敏感数据。

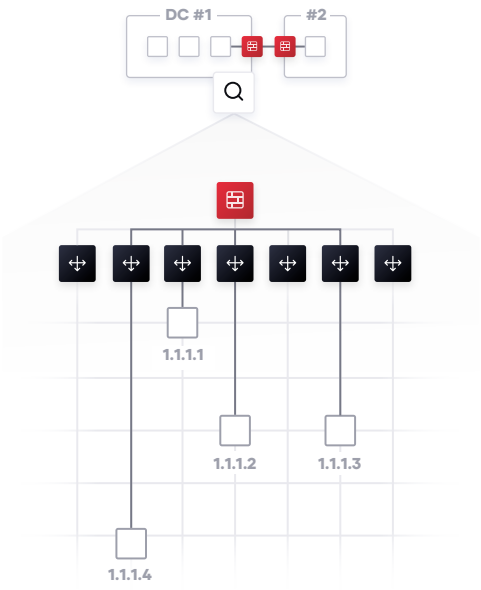
第三步：多云服务网络

云中网络的挑战通常是企业采用云运营模式最困难的方面之一。动态 IP 地址的组合、采用微服务模式时东西向流量的显著增长以及缺乏清晰的网络周界是一项巨大的挑战。

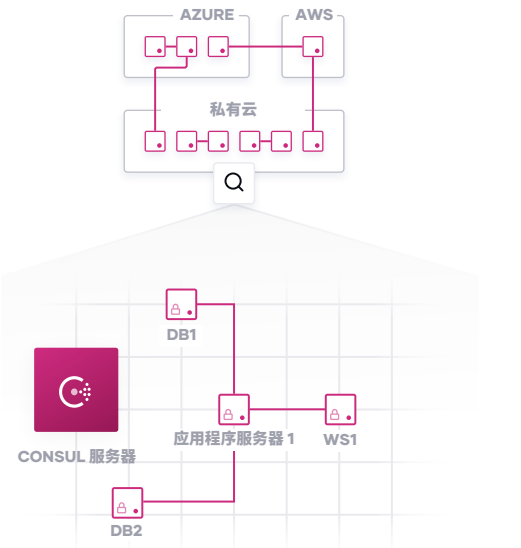
HashiCorp Consul 提供了一个多云服务网络层来连接和保护服务。Consul 是一种广泛部署的产品，大量客户在其环境中运行的节点数量远超 100000 个。

网络服务应集中提供，由 IT 团队提供服务注册和服务发现功能。拥有一个公共注册中心可以提供一张“地图”，显示哪些服务正在运行、所在位置以及当前的运行状况。可以通过编程方式查询注册表，以启用服务发现或驱动 API 网关、负载均衡器、防火墙和其他关键中间件组件的网络自动化。中间件组件可以通过使用服务网格方法移出网络，其中代理在边缘上运行，以提供同等功能。 服务网格方法允许简化网络拓扑，特别是对于多云和多数据中心拓扑。

使用 CONSUL 前



使用 CONSUL 后



服务发现

在云运营模式中，网络的起点通常是公共服务注册中心，它提供了一个实时目录，其中包含正在运行的服务、所在位置以及它们当前的运行状况。传统的网络方法依赖于负载均衡器和虚拟 IP 提供命名抽象，来表示具有静态 IP 的服务。跟踪服务网络位置的过程通常采用电子表格、负载均衡器仪表板或配置文件的形式，所有这些都是不连贯的手动过程，并不理想。

而 Consul，每个服务都以编程方式注册，并提供 DNS 和 API 接口，以使任何服务都能够被其他服务发现。集成运行状况检查将监控每个服务实例的运行状况，以便 IT 团队可以对每个实例的可用性进行分类，而 Consul 可以帮助防止将流量路由到不健康的服务实例。

Consul 可以与管理现有南北向流量的其他服务（如传统负载均衡器）和分布式应用程序平台（如 Kubernetes）集成，以跨多数据中心、云和平台环境提供一致的注册和发现服务。

网络中间件自动化

下一步是通过网络自动化使用现有的网络中间件降低操作复杂性。与每次服务网络位置或配置发生变化时，重新配置负载均衡器和防火墙的基于工单的手动过程不同，Consul 可以使这些网络操作自动化。这是通过使网络中间件设备能够从服务注表订阅服务更改来实现的，从而使高度动态的基础架构得以比基于静态的方法进行更高的扩展。

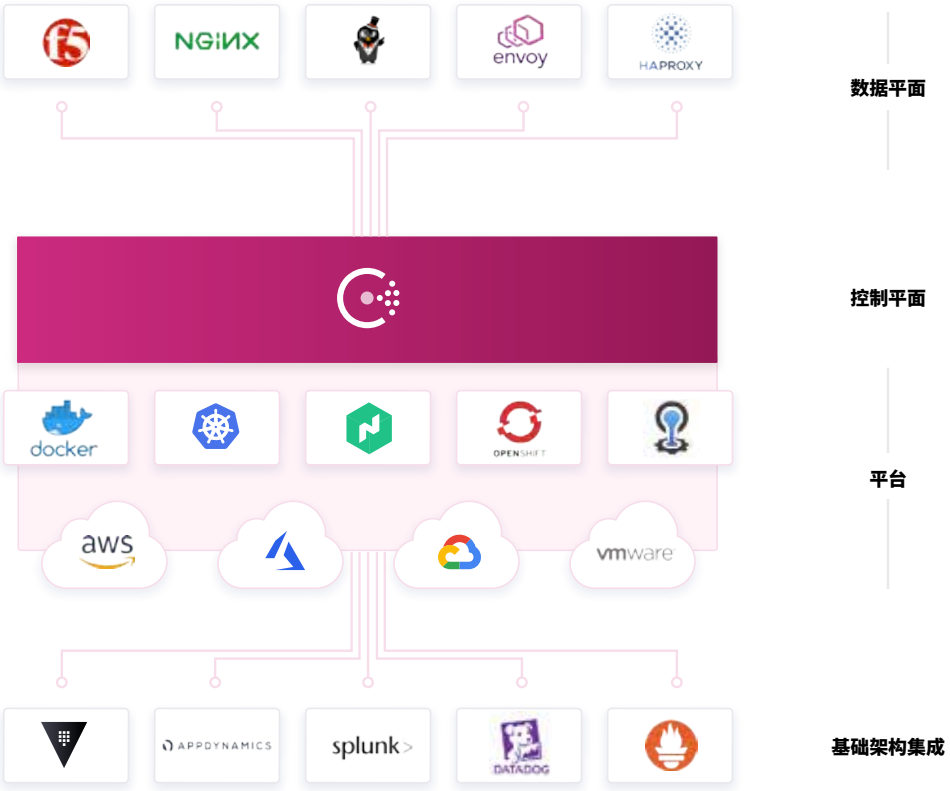
这将使团队之间的工作流程解耦，因为运营商可以独立部署应用程序并发布到 Consul，而网络运营团队可以订阅 Consul 以处理下游自动化。

使用服务网格的零信任网络

随着组织继续使用基于微服务的应用程序或云原生应用程序进行扩展，底层基础架构变得更大，并且随着东西向流量的激增而变得更具动态性。这导致具有单点故障的昂贵网络中间件激增，IT 团队也面临的巨大运营开销。

Consul 提供了一个分布式服务网格，它将路由、授权和其他网络功能推送到网络中的端点，而不是通过中间件强加它们。这使得网络拓扑更简单、更易于管理，消除了在东西向流量路径中使用昂贵中间件的需要，并使服务到服务的通信更加可靠和可扩展。

Consul 是一个 API 驱动的控制平面，它与每个服务实例旁边的 sidecar 代理（如 Envoy、HAProxy 和 NGINX 之类的代理）集成。这些代理提供分布式数据平面。这两个平面共同实现了一个零信任网络模型，该模型通过自动 TLS 加密和基于身份的授权，保护服务到服务的通信。网络运营和安全团队可以通过使用逻辑服务而不是 IP 地址来定义安全策略。

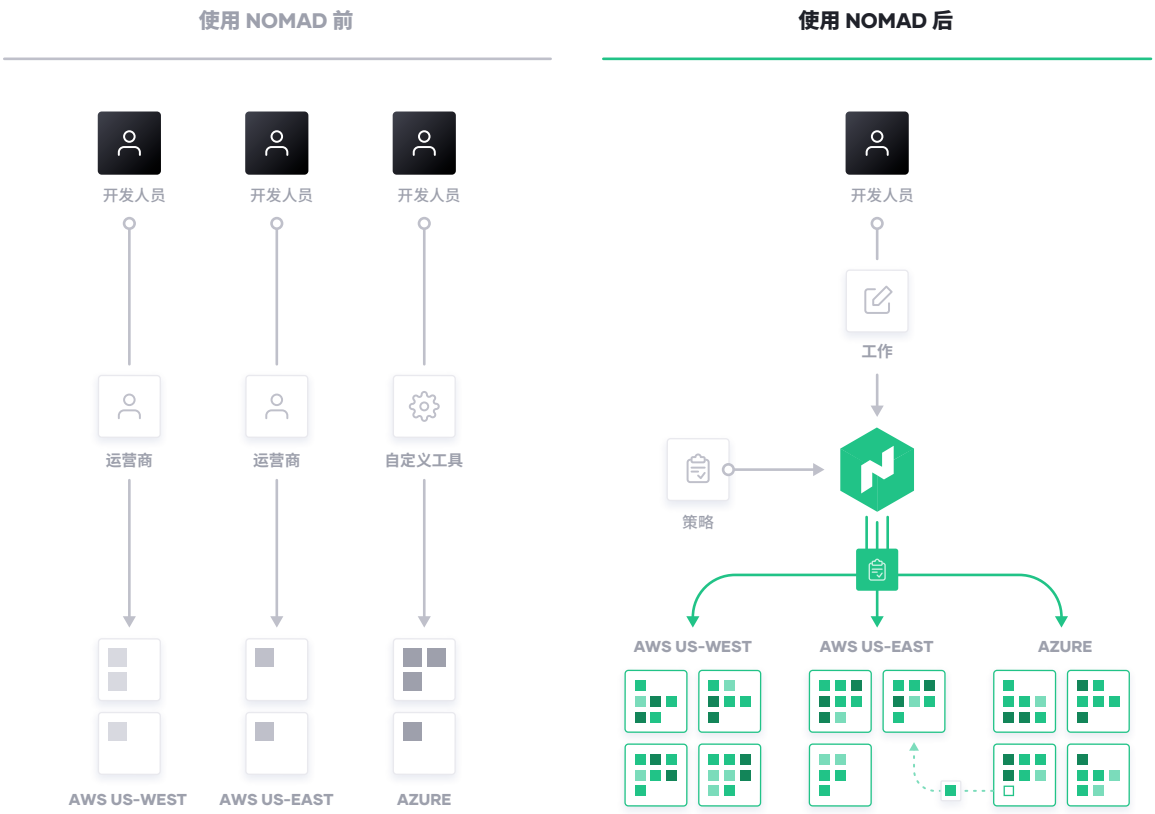


Consul 支持细粒度服务分段，以通过自动 TLS 加密和基于身份的授权，保护服务到服务的通信。Consul 可与 Vault 集成，用于集中的 PKI 和证书管理。服务配置是通过 API 驱动的 Key/Value 存储来实现的，该 Key/Value 存储可用于在任何环境中的运行时轻松配置服务。

第四步：多云应用程序交付

最后，在应用层，新的应用程序越来越多地分布，而传统应用程序也需要更灵活地管理。HashiCorp Nomad 提供了一个灵活的编排工具，用于部署和管理传统和现代应用程序，适用于所有类型的工作负载：从长时间运行的服务，到短期的批处理，再到系统代理。

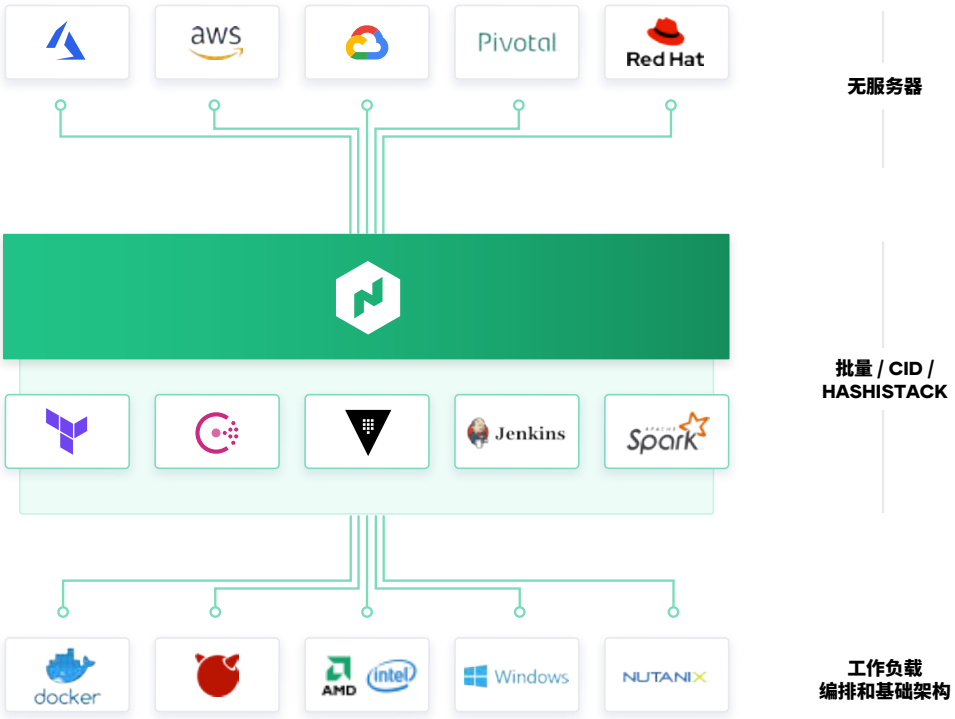
为了实现应用程序交付的共享服务，IT 团队应使用 Nomad 与 Terraform、Vault 和 Consul 协同工作，以实现云基础架构上应用程序的一致交付，包括必要的合规性、安全防护和网络要求，以及工作负载编排和调度。



混合工作负载协调

许多新的工作负载是通过容器打包开发的，目的是部署到 Kubernetes 或其他容器管理平台。但许多传统工作负载将不会移动到这些平台上，未来的无服务器应用程序 Nomad 也不会通过独立二进制文件和容器，提供从虚拟机部署所有工作负载的一致流程，并提供跨这些工作负载的核心编排优势，例如发布自动化，多种升级策略、装箱和恢复能力。

对于现代应用程序（通常内置于容器中），Nomad 在任何环境中都提供相同的大规模一致工作流。Nomad 专注于协调和调度的简单性和有效性，并避免了 Kubernetes 等平台的复杂性，这些平台需要专业技能来操作和解决容器工作负载。



Nomad 集成到现有 CI/CD 工作流中，为传统和现代工作负载提供快速、自动的应用程序部署。

高性能计算

Nomad 设计用于跨大规模集群低延迟调度应用程序。这对于具有大批量作业的客户至关重要，这些客户通常要求高性能计算 (HPC) 工作负载。在百万容器挑战中，Nomad 能够在不到 5 分钟的时间内，在三个数据中心的 5000 台机器上调度 100 万个 Redis 实例。一些大型 Nomad 部署的规模甚至更大。

Nomad 使高性能应用程序能够轻松使用 API 动态消耗容量，从而实现数据分析应用程序（如 Spark）的高效资源共享。低延迟调度可确保结果及时可用，并将浪费的空闲资源降至最低。

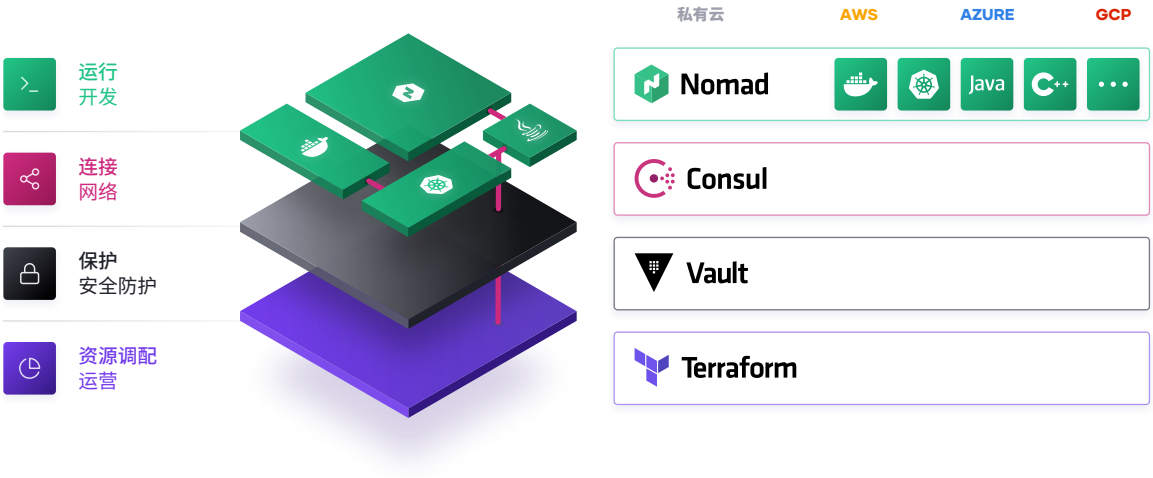
多数据中心工作负载编排

Nomad 是多区域和多云设计，具有一致的工作流来部署任何工作负载。 随着团队在多个数据中心或跨云边界推出全球应用程序，Nomad 为这些应用程序提供编排和调度，并由基础架构、安全防护和网络资源及策略提供支持，以确保成功部署应用程序。

第五步：工业化应用程序交付流程

最终，这些跨基础架构、安全防护、网络和应用程序运行时的共享服务，为应用程序交付提供了一个工业化的过程，同时充分利用了云每一层的动态特性。

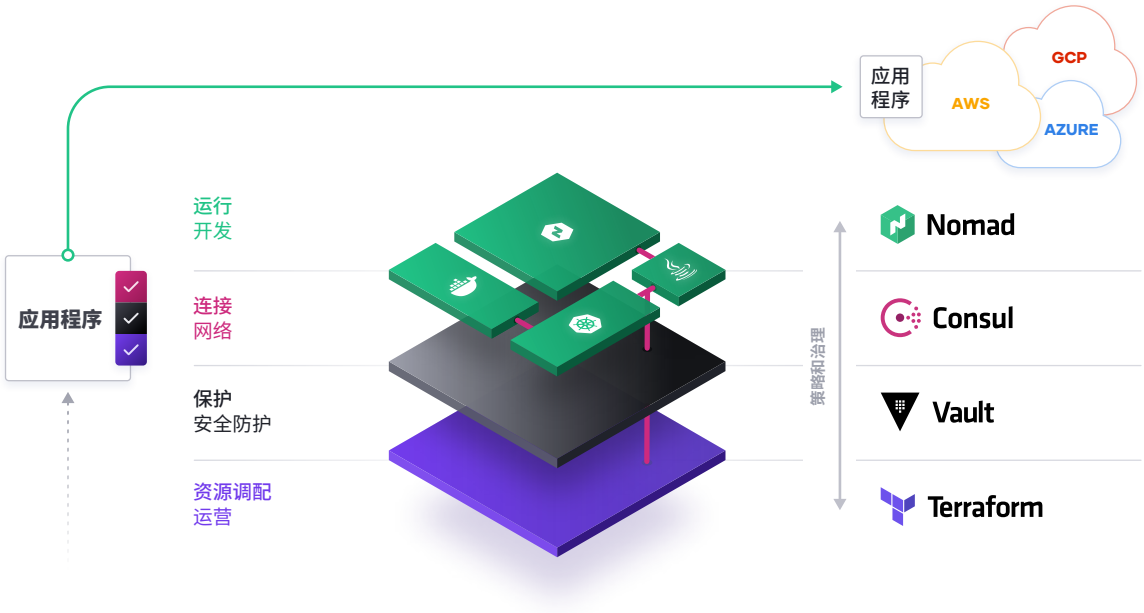
采用云运营模式可以实现完全兼容和受管理的自助服务 IT，使团队能够以更快的速度交付应用程序。



结论

通用云运营模式是企业最大程度实现数字化转型的必然转变。HashiCorp suite 工具套件旨在为云的每一层提供解决方案，使企业得以实现向云运营模式的转变。

企业 IT 需要从以成本优化为重点的基于 ITIL 的控制点，向以速度优化为重点的自助服务支持者转变。可以通过在云的每一层提供共享服务来实现这一点，这些服务旨在帮助团队快速交付新的业务并实现客户价值。



通过采用通用云运营模式，在现代多云数据中心中解锁实现价值的最快路径，意味着企业 IT 的特征发生了转变：

- **人：转向多云技术**
  - 重用来自内部数据中心管理和单一云供应商的技能，并在任何环境中一致地应用这些技能。
  - 采用 DevSecOps 和其他敏捷实践，持续交付生命周期越来越短的分布式系统。

- **流程：转向自助服务 IT**
  - 将中央 IT 定位为以应用程序交付速度为重点的支持共享服务：以最小的风险更快地交付软件。
  - 在云的每一层建立卓越中心，以提供自助服务能力。

- **工具：转向动态环境**
  - 使用支持基础架构和应用程序不断发展的短生命周期和分布性并支持关键工作流的工具，而不是与特定技术相关联的工具。
  - 提供策略和治理工具，使交付速度与合规性相匹配，以便在自助服务环境中管理风险。

关于 HashiCorp

HashiCorp 是多云基础架构自动化软件的领导者。HashiCorp 软件套件帮助企业采用一致的工作流来为任何应用程序进行资源调配、保护、连接和运行任何基础架构。HashiCorp 开源工具 Vagrant、Packer、Terraform、Vault、Consul 和 Nomad 每年的下载次数多达数千万次，并被全球 2000 强组织广泛采用。这些产品的企业版通过促进协作、运营、治理和多数据中心功能的特性，增强了开放源代码工具。公司总部位于旧金山，得到 Mayfield、GGV Capital、Redpoint Ventures、True Ventures、IVP 和 Bessemer Venture Partners 的支持。欲了解更多信息，请访问 www.hashicorp.com 或在 Twitter 上关注 HashiCorp @HashiCorp。


HashiCorp