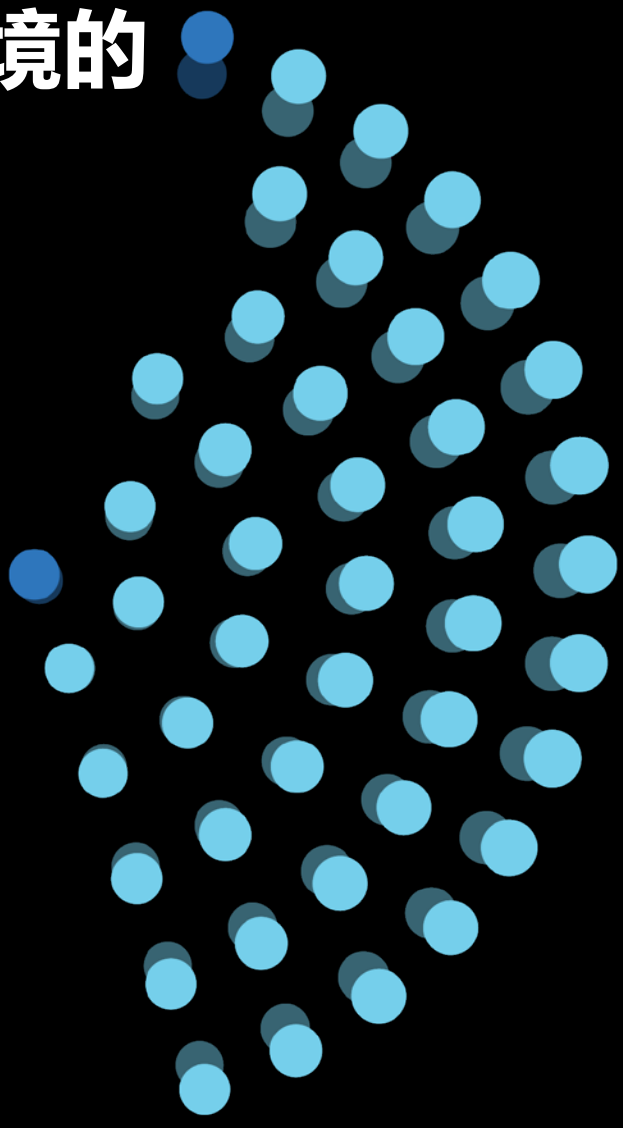
Azure 电子书系列

Microsoft Azure

无处不在的云：

适用于混合和多云环境的 Azure



Contents

01 /
引言

云是数字化转型的基础。战略性地利用混合云的公司可获得巨大的价值，这种价值体现在缩短上市时间以及管理成本和规模的灵活性方面，足以使其从竞争对手中脱颖而出。

如今，94% 的公司以某种方式使用云[1]，但每个公司都以不同的速度迁移到云，并且对于需要部署到云的内容有着不同的战略和优先级。有的公司将采用云计算来解决紧急的业务需求，而有的公司则将进行长期、有计划的云迁移。无论哪种方式，通过持续努力改进业务运营和创建敏捷开发流程，组织都能在跨越本地、多云和边缘基础结构的 IT 环境中开展工作。

虽然有些人可能认为混合云只是通往完全云业务的垫脚石，但许多公司认识到混合云战略不是过渡性的，而是基于各种考虑因素优化基础结构的一部分。混合云基础结构是信息技术的自然演变，通常以渐进的速度发生。很多公司将部分硬件和软件过渡到云服务和技术，从而创建了一个结合了本地、多云和边缘计算的计算环境，使用软件即服务 (SaaS)、平台即服务 (PaaS) 以及基础结构即服务 (IaaS)。一项研究显示，多达 85% 的企业 IT 经理将混合云作为最适合其业务的模式。[2]

但是，对于这些公司而言，一个关键的挑战是，为用户、开发人员和管理员提供跨环境的真正集成的解决方案。
为了帮助企业应对日益复杂的混合基础结构 (通常包含数十到数千个应用程序)，IT 经理需要管理和维护跨本地技术、多云服务和边缘设备的环境。这一挑战对于那些拥有传统 IT 资产的公司，或者具有复杂的监管要求或边缘计算需求的公司来说尤为艰巨，因为这些公司必须跟上创新的步伐。

作为集中 IT 团队，你需要想办法构建和维护平台，无论它在你的环境的什么位置运行。你还需要以能够最大限度提高工作效率和敏捷性的方式管理混合环境，而不会牺牲安全性和合规性等重要方面。

为了帮助 IT 团队响应在复杂环境中高效工作的需求，Azure 提供了服务，可帮助你治理和管理整个环境，构建应用并将其部署到任何位置，在 Kubernetes 群集上部署和管理 Azure 服务，以及在整个组织中提供安全性。Azure 混合云能够使用本地、多云或边缘技术来开发、部署、管理和保护应用程序基础结构，使

你的团队能够轻松地将各种技术集成到可扩展、可靠和高效的体系结构中。

本电子书将向你展示最佳实践，包括你应注意的事项以及任何公司为实现混合环境所需采取的基本步骤。本书还提供了一些关于混合云常见用例的见解，其中一些可能是即时相关的，而另一些则可能提出了有关如何在混合环境中工作的新想法。在简要介绍设置混合云环境的三个重要因素 (网络连接、身份管理和安全性) 后，本电子书介绍了六个不同的混合用例，使你能够探索与业务最相关的主题。

---

[1] RightScale。“2019 年云状态报告。” Flexera RightScale，2019 年 2 月，第 2 页。https://resources.flexera.com/web/media/documents/rightscale-2019-state-of-the-cloud-report-from-flexera.pdf。[PDF]

[2] Nutanix。“2019 年 Nutanix 企业云指数。” 调查报告。2019 年 11 月。https://www.nutanix.com/enterprise-cloud-index

02 /

混合基础结构基础知识

为了构建适合的混合云基础结构，企业需要创建可靠、高效且安全的基础。接下来的一节将介绍构建体系结构需要了解的三个基本方面：网络连接、身份和访问管理以及安全性。

如果你计划大规模迁移到云，可在适用于 Azure 的云采用框架中找到相关指导，此框架旨在帮助 IT 专业人员和云架构师制定云战略并迁移其本地工作负载。此框架侧重于评估当前基础结构，将应用程序和基础结构迁移到云，优化其体系结构以降低成本，以及更安全地管理其工作负载和数据。此外，通过帮助开发人员对其代码负责 (即所谓的 Shifting Left)，可以更快地更新、修补和保护生成的应用程序。

云采用框架侧重于将公司基础结构的异构组件整合在一起，并提供单一的管理、部署和管理平台。

对于本指南，我们不介绍云采用的所有方面，而是介绍对于当前在混合或多云环境中工作或迁移到这些环境的组织尤其重要的三个方面：网络连接、身份和访问管理以及安全性。

混合基础知识

01.网络连接

有许多方法可用来创建可靠但经济高效的网络，充当混合解决方案的主干。网络依赖于多个功能领域。在考虑云中的网络体系结构时，重点关注以下方面很重要:

- 连接和扩展: 企业需要连接现有资源，并使用 VPN、ExpressRoute 和虚拟 WAN 等技术扩展自己的网络。
- 保护: 任何连接都可以成为网络的入口点，因此贵公司应该可以使用最适合的工具来保护自己，比如 DDoS 保护、防火墙和 Web 应用程序防火墙。
- 交付: 要提供出色的客户体验，需要使用 Azure Front Door 和应用程序网关技术为应用程序交付构建一个网络。

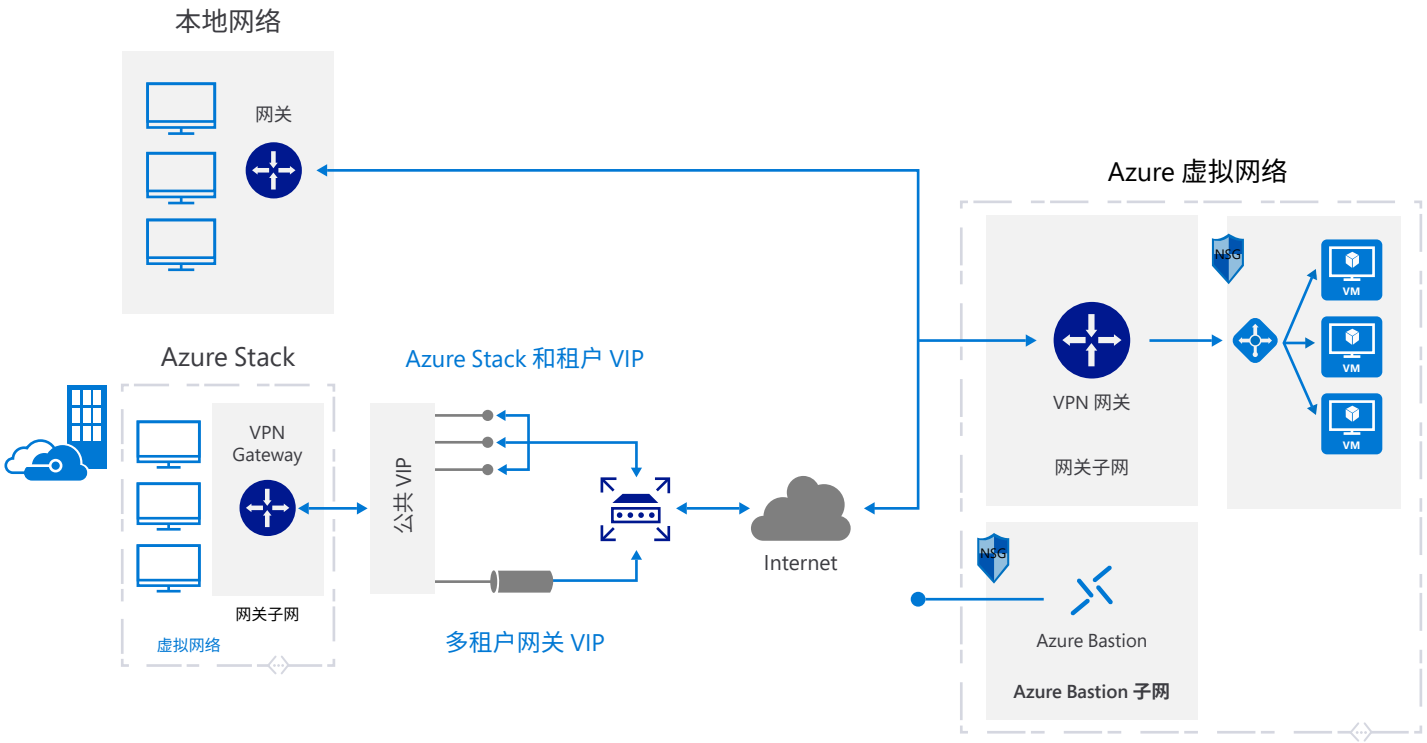
在本电子书中，我们仅关注最常见的连接和扩展现有网络的场景，以及用于应用程序交付的一项基本服务。有关 Azure 网络连接服务的更多详细信息，请访问此处的文档: https://docs.microsoft.com/azure/networking/networking-overview

连接和扩展

VPN 连接

虚拟网络网关使用公共 Internet 在 Azure 虚拟网络 (VNet) 和本地位置之间发送加密流量。此体系结构适用于混合应用程序, 在这些应用程序中, 本地硬件和云之间的流量可能很小, 或者你愿意以稍微延长的延迟来换取云的灵活性和处理能力。

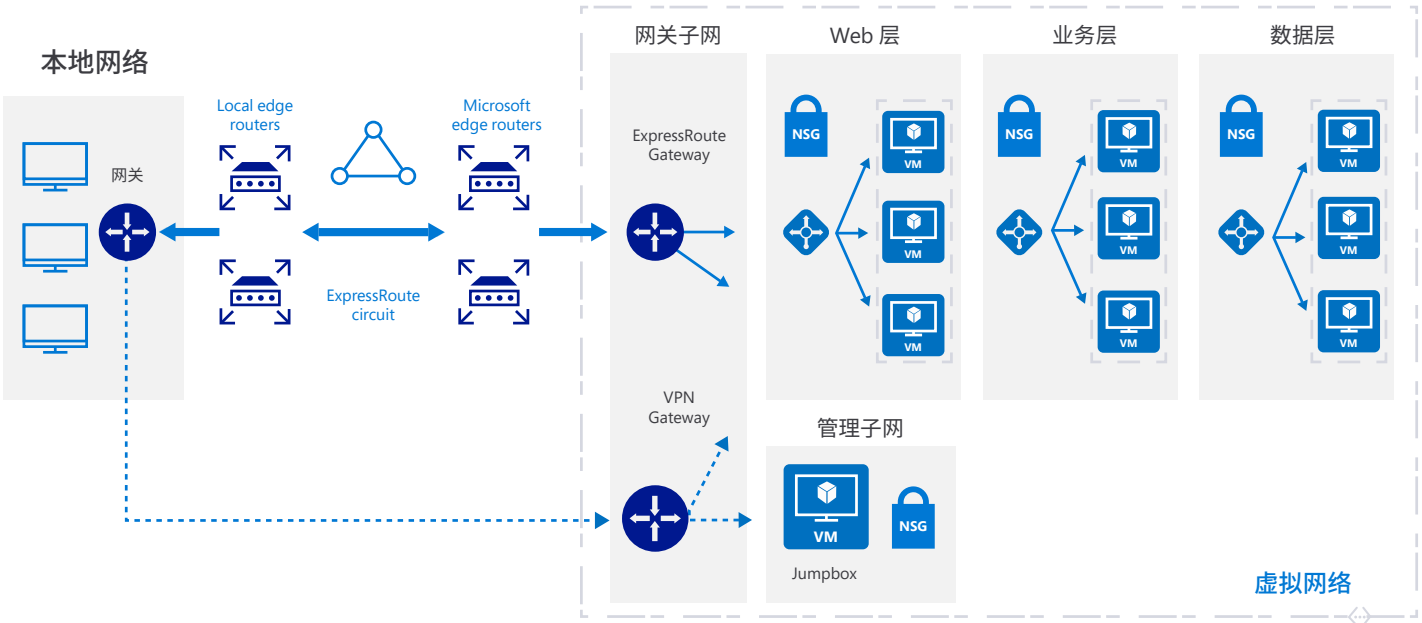
- 优势: 易于配置; 经济高效; 可用带宽大幅度提升 (高达 10 Gbps, 具体取决于服务) 。
- 挑战: 需要本地 VPN 设备; 可靠性 (Microsoft 保证每个 VPN 网关 99.9% 的可用性, 但网络连接可能不可靠) 。



ExpressRoute 兼 VPN 故障转移

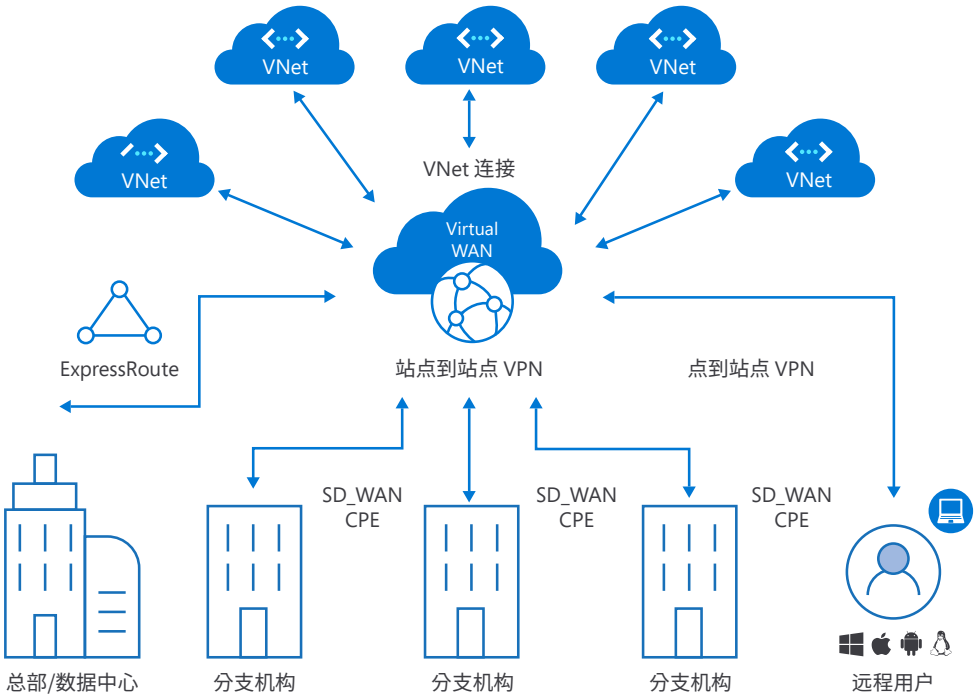
此选项将前两者结合在了一起，在正常情况下使用 ExpressRoute，但如果 ExpressRoute 线路中的连接丢失，则将故障转移到 VPN 连接。此体系结构适用于需要更高带宽的 ExpressRoute 的混合应用程序，并且还需要高度可用的网络连接。

- 优势：高可用性。
- 挑战：与 VPN 连接相比，配置更复杂，因为必须配置两个外部链接；需要冗余硬件和连接；成本更高。



虚拟 WAN

对于拥有分支机构的公司，Azure 虚拟 WAN 可以通过优化和自动化的网络连接将这些站点链接到 Azure 并连通 Azure。Azure 虚拟 WAN 将许多 Azure 云连接服务 (如站点到站点 VPN、用户 VPN (点到站点) 和 ExpressRoute) 整合到单个操作界面中，从而构建起一个基于经典的中心辐射型连接模式的全球传输网络体系结构。
在此处阅读有关虚拟 WAN 的更多信息： https://azure.microsoft.com/services/virtual-wan/

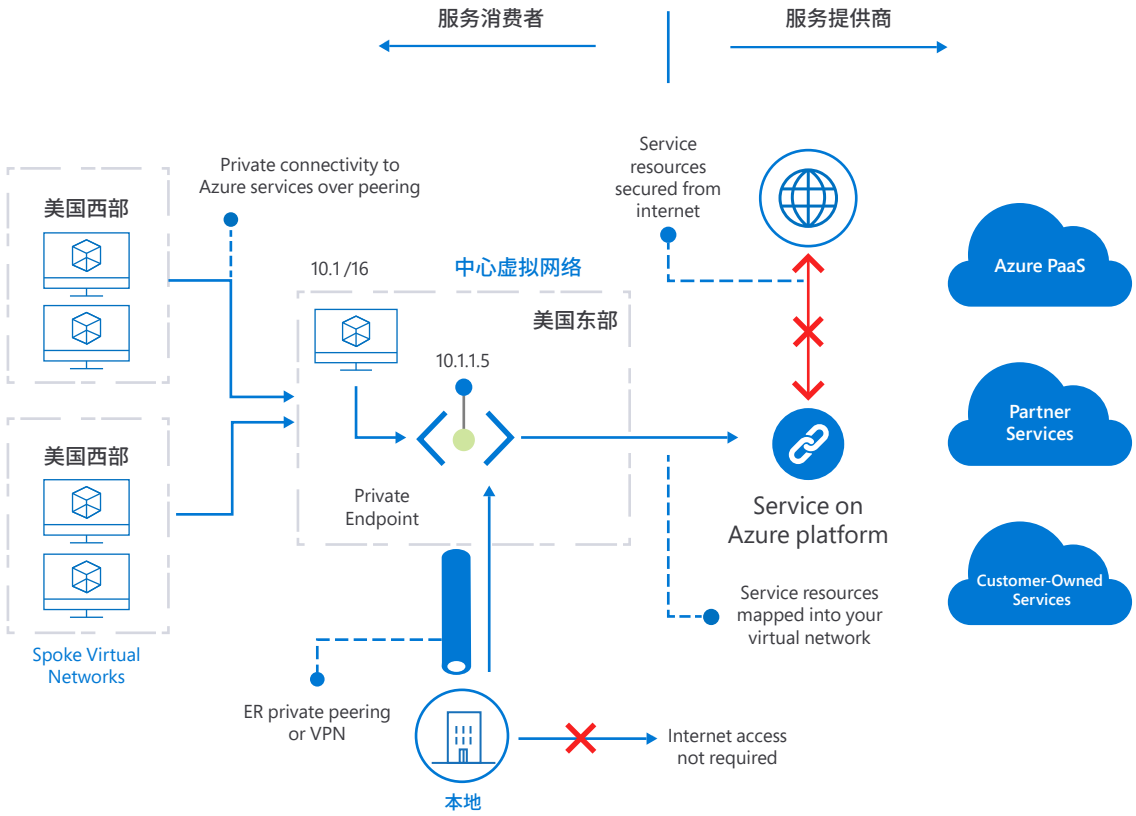


专用链接

Azure 专用链接使你能够通过虚拟网络中的专用终结点访问 Azure PaaS (例如 Azure 存储、Azure Cosmos DB 和 SQL 数据库) 以及 Azure 托管的客户或合作伙伴服务。虚拟网络和服务之间的流量通过 Microsoft 主干网络传输, 消除了公共 Internet 中的风险。

借助专用链接, 你的公司可以:

- 私下访问 Azure 平台上的服务,
- 通过 ExpressRoute 专用对等互连或 VPN 隧道, 从本地访问在 Azure 中运行的服务,
- 通过将资源映射到客户 PaaS 资源的特定实例, 获得针对数据泄露的有效防护,
- 私下连接到在其他区域运行的服务, 以及
- 通过将服务置于负载均衡器后面来启用专用链接, 扩展到你自己的服务。



交付

Azure Front Door

每个面向 Internet 的 Web 应用程序, 无论是为单个区域中的大量受众还是一小群用户提供服务, 默认情况下都是全局应用程序, 要求你最大限度地提高面向最终用户的性能, 并确保应用程序在发生故障和攻击时始终处于打开状态。Azure Front Door 是可扩展且安全的入口点, 可快速交付全局应用程序, 从而为公司提供应用程序和 API 加速、HTTP 流量的负载均衡、可扩展的 SSL 卸载以及位于边缘的 Web 应用程序防火墙。详细了解 Azure Front Door: https://azure.microsoft.com/services/frontdoor/

混合基础知识
02. 身份访问管理

如今, 很多公司正在使用更复杂的本地和云应用程序组合, 员工需要跨环境进行访问, 因此集成管理至关重要。身份解决方案应利用通用用户身份面向所有资源进行身份验证和授权, 无论其位于何处。我们称之为*混合身份*。

对于希望将应用程序迁移到云的组织来说, 选择正确的身份验证方法是
首要考虑的问题。
身份验证方法是组织云基础结构的关键组成部分; 它是 Azure Active Directory (AD) 中所有其他高级安全和用户体验功能的基础。身份是新的控制平面, 在用户、设备和各种互联终结点 (包括应用程序, 传感器和自动程序) 的混乱中提供业务控制权。

要选择身份验证方法, 你需要考虑实施所选解决方案的时间、现有基础结构、复杂性和成本。这些因素对于每个组织都是不同的, 并且可能会不断演变。

Azure AD 支持混合身份解决方案的以下身份验证方法:

- **云身份验证:** Azure AD 处理用户登录流程, 该流程与无缝单一登录相结合, 允许用户访问云和本地应用程序, 而无需重新输入其凭据。通过 Azure AD 密码哈希同步, 用户可以使用与在本地使用的相同的用户名和密码, 而无需部署任何其他基础结构, 从而获得密码不存储在云中的额外好处, 这有助于满足法规要求并防止停机。通过 Azure AD 直通身份验证, 服务器会直接使用本地 Active Directory 验证用户, 从而确保密码验证不会在云中进行, 这可能是行业或政府法规所要求的。

- **联合身份验证:** 对于由于法规要求而无法支持云中身份验证的公司, Azure AD 将身份验证流程移交单独的受信任身份验证系统 (如本地 Active Directory 联合身份验证服务) , 以验证用户的密码。虽然不建议使用此方法, 但身份验证系统可以提供其他高级身份验证, 如基于智能卡的身份验证或第三方多重身份验证, 这是对纯本地解决方案的改进。

通过将本地目录与 Azure AD 集成在一起, 可为访问云和本地资源提供通用身份, 从而提高用户的工作效率。该解决方案可同步本地身份与 Azure AD, 而 IT 则使本地 Active Directory 与任何现有治理解决方案一起运行, 作为身份认证的主要来源。Microsoft 的 Azure AD 混合身份解决方案跨越本地和云功能, 从而创建用于身份验证和授权的通用用户标识以访问所有资源, 无论这些资源位于何处。

混合身份也为应用程序管理提供支持。组织通常拥有数百个用户完成工作所需的应用程序, 用户会从许多设备和位置访问这些应用程序。有了如此多的应用程序和访问点, 使用基于云的解决方案来管理用户对所有应用程序的访问变得前所未有的重要。

混合基础知识
03. 安全性

随着运营和应用程序在本地、多云和边缘基础结构上扩展，安全性变得很复杂。在这个数据泄露频繁的时代，拥有一个可保护数据库和非结构化数据湖的云平台至关重要。Azure 为公司提供了两种从一个位置管理安全性的方法。

Azure 安全中心

Azure 安全中心允许企业通过单一门户管理其各个基础结构的安全状态，方法包括设置针对不同资源的策略，监视违规和异常，以及执行常见的安全任务，例如修补、合规性测试和配置管理。安全性是 Azure 结构的一部分，为公司提供特定应用程序或服务可能没有的功能。

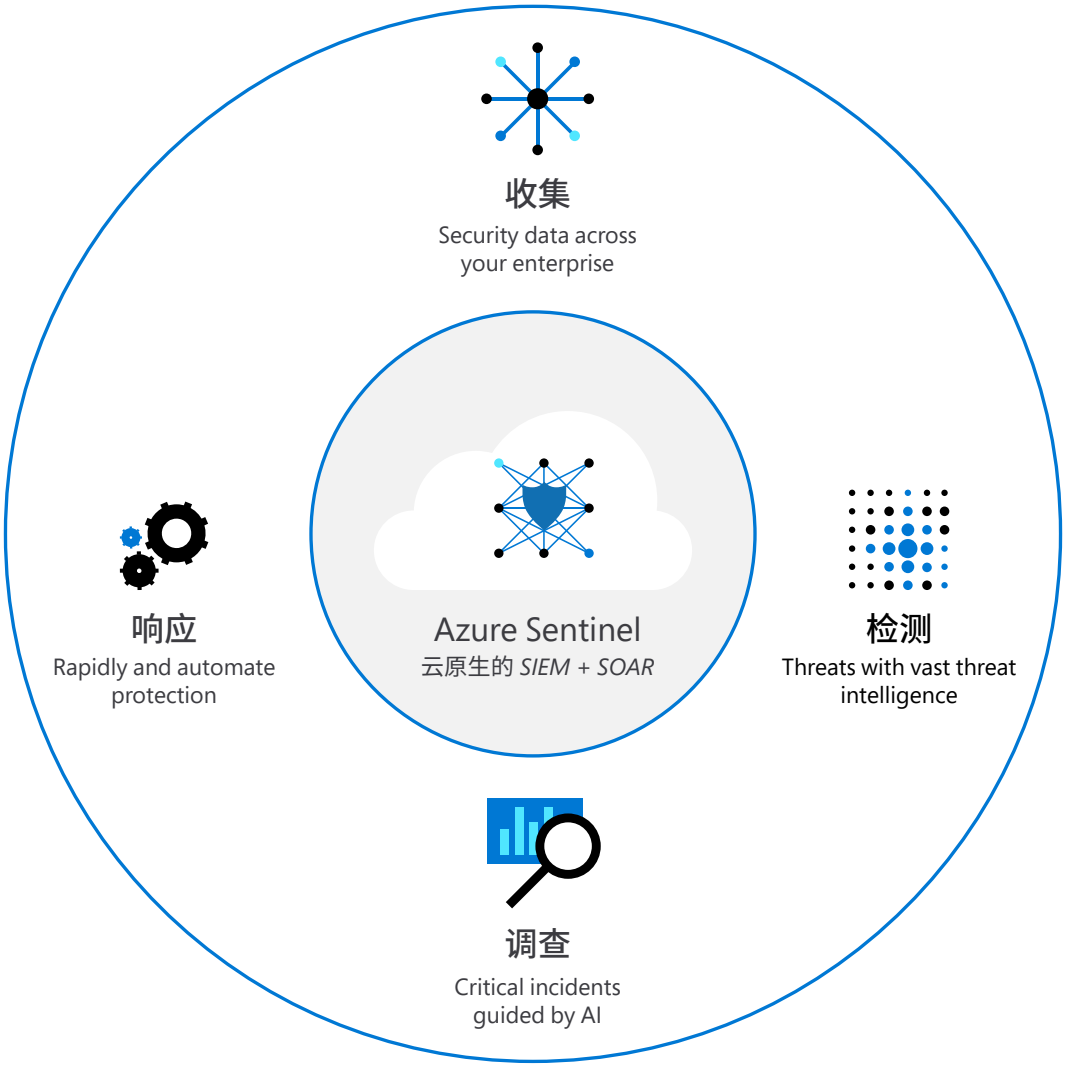
Azure Sentinel

Azure Sentinel 是一种可扩展的云原生安全信息和事件管理 (SIEM) 以及安全编排自动响应 (SOAR) 解决方案。通过此功能，IT 团队能够访问整个企业的实时安全分析和威胁情报，为警报检测、威胁可见性、主动搜索和威胁响应提供单一解决方案。

随着违规行为持续影响业务，快速发现和补救对于确保基础结构的安全性至关重要。Azure Sentinel 从混合云体系结构的所有部分以及其他云提供商处收集数据，从而支持多云战略。通过结合利用全球和行业威胁情报，该平台还可以检测复杂的攻击者并减少误报。Azure Sentinel 整合了人工智能 (AI)，可帮助公司更快地做出响应，并以正确的方式调查每种威胁。

Azure Sentinel 以所有现有 Azure 服务为基础，原生整合了很多经过验证的基础，例如 Log Analytics 和 Logic Apps。Azure Sentinel 借助 Microsoft 威胁情报流丰富了你的调查和检测，并通过添加 AI 和机器学习功能来帮助你获取自己的威胁情报。

Azure Sentinel 功能



03 /

常见混合用例

01. 跨环境组织和管理

基础结构存在于各种位置: 从传统的分支机构和数据中心到边缘位置 (如工厂车间) , 或云提供商的基础结构即服务产品。这些服务器和群集可能作为物理服务器或虚拟机运行 Windows Server、Linux 或 Kubernetes。跨位置、操作系统和外形规格管理这些不同的系统历来是困难且不一致的。

示例

一家保险公司的 IT 资产具有不同的监管要求。他们的一些工作负载位于 Azure 中, 一些位于公司数据中心, 最近则位于不同的公有云中。每个系统 (可能还有每个位置和外形规格) 都有自己的运作方式。添加的设备和位置越多, 控制技术蔓延就越困难。随着技术的扩展, 员工的技能和流程难以跟上变化的步伐。

解决方案

Microsoft 数据中心和世界各地的 200 多种不同类型的服务中有数百万种资源。Azure 资源管理器是 Microsoft 构建的技术, 用于以标准化的方式协调这些资源的生命周期和操作。它使客户能够清点、组织和控制其 Azure 资源。Azure Arc 将 Azure 资源管理器扩展到 Microsoft 数据中心之外的服务器和群集。Azure 资源管理器通过 Azure Arc 在几个主要领域提供功能, 例如:

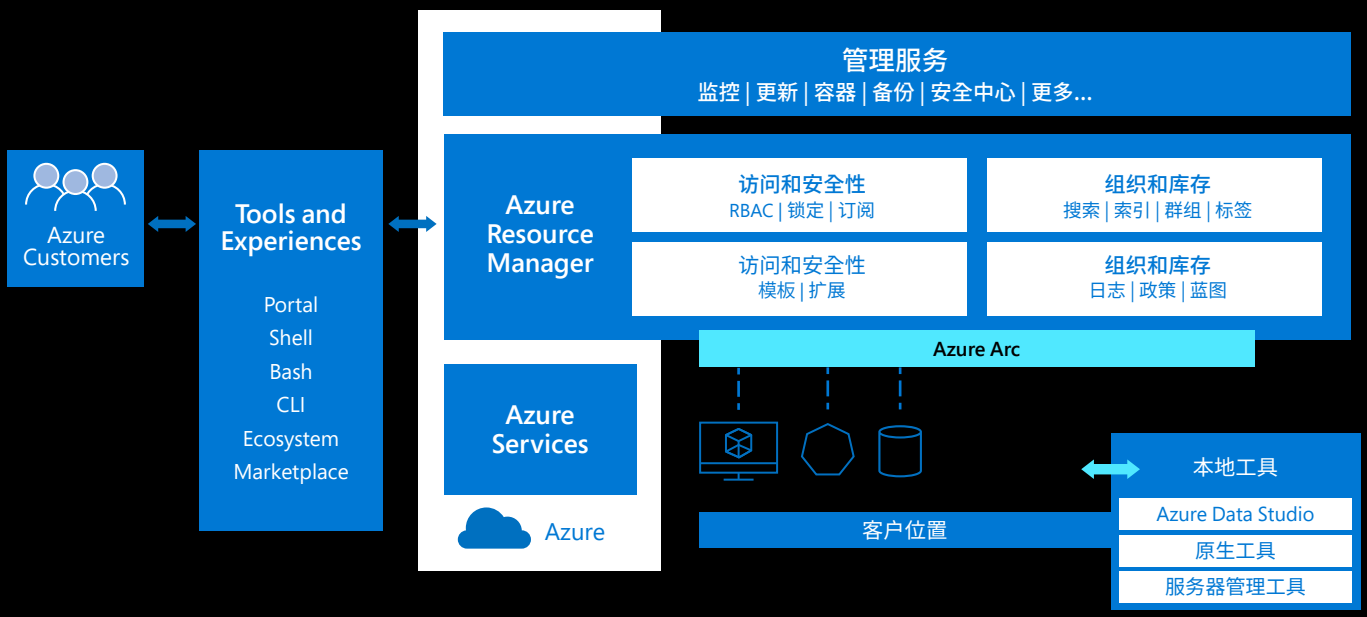
- 组织和库存: 资源组、标记、搜索和索引。例如, 启用 Azure Arc 的服务器可以标记为 “成本中心” 和 “位置” , 而 Azure 可用于搜索在 DC1 中运行的所有 HR 服务器。
- 治理和合规性: 日志、策略、蓝图。例如, 可以在启用了 Arc 的群集和服务器上使用 Azure 策略, 通过定义护栏来提供集中治理。

- 访问和安全性: 基于角色的访问控制、锁定和订阅。例如, 运营团队可以轻松地将资源的控制权委派给一部分管理员。这些管理员将能够访问资源并根据需要修复问题。
- 环境和自动化: Azure 模板和扩展。例如, 可以编写一个策略, 要求特定资源组中的所有资源都由 Azure 安全中心通过虚拟机扩展进行管理。

通过将资源和资产链接到 Azure 资源管理器, 你可以主动管理公司的环境, 即使这些资源位于其他云提供商的基础结构中也不例外。控制平面是不依赖于域的, 因此域控制器之间不需要信任, 并且你的团队可以继续使用其本地工具。

Azure 管理

适用于任何地方的资源的单一控制平面



接下来要了解的内容

Azure Arc
视频: 使用 Azure Arc 整理 Azure 之外的所有服务器

02. 大规模的 Kubernetes 应用程序管理

容器已被企业广泛采用, 并已成为部署业务应用程序的标准。许多新应用程序被编写为基于 Kubernetes 群集构建的微服务。即使是现有的软件, 也正在通过重建为容器来实现现代化。但是, 如何在不减慢公司创新和开发人员的速度的情况下大规模管理这些群集和应用程序呢? 为了进一步说明这一点, 让我们介绍一个假设的用例。

示例

一家拥有数百家商店的零售商希望将所有店内应用程序迁移到在 Kubernetes 群集上运行的容器。IT 团队面临着如何在多个位置统一部署、配置和管理其容器化应用程序的挑战。零售商
需要启动一家新商店, 使用一组
特定的应用程序开展完全运营, 同时强制执行必要的配置和部署实践。此外, IT 需要能够应用和监视所有商店中应用程序和配置的状态, 以及它们的合规性状态。

解决方案

使用 Azure Arc, 公司可以轻松地将新应用程序部署到多个位置, 使用单个策略来锁定网络端口, 并使用其他策略来处理常见的错误配置。Azure Kubernetes 服务 (AKS) 上托管的服务可处理很多关键任务, 例如运行状况监控和维护、装载存储卷以及并行处理启用 GPU 的节点。

此外, 应用程序策略可以链接到特定的 GitHub 存储库, 这样, 提交到应用程序主分支的内容将部署具有所有正确策略的软件。使用这种持续部署技术, 公司可以轻松地使应用程序保持最新状态并符合其策略。

最后, 分支机构位置的所有群集都将由 Azure Arc 和 Azure 策略管理, 从而为资产组织提供一个清单, 并在 Azure 门户中针对所有位置提供统一视图。可以使用基于 GitOps 的模型将配置作为代码部署, 根据订阅、资源组和标记来大规模地进行配置和部署。

接下来要了解的内容

Azure Arc
视频: 使用 Azure Arc 管理 Azure 之外的 K8 群集

03. 在任何位置运行云服务

公司面临着越来越多的数据蔓延，数据不仅收集自终结点，还来自本地数据库和基于云的数据存储桶。日益异构的数据存储给使用混合云基础结构的公司带来了重大问题。如果缺乏所有环境中数据资产的统一视图，公司将更难以利用其最宝贵的资产。

示例

一家能源公司的目标是在整个基础结构中利用人工智能实现高效且完全自动化的运营。客户经营着多个经营场地，并经营公用事业和服务，从提取到零售分销。该公司在边缘拥有大量数据，需要实时获取见解。该企业需要利用现有的 OEM 硬件和应用程序，并使 IT 系统实现大规模自动化。他们希望部署最新的创新，并在其数据基础结构中应用一致的安全性和治理。

解决方案

Azure Arc 解决了公司在混合云基础结构中的分发数据方面所面临的许多问题。由 Azure Arc 支持的 Azure 数据服务可为企业的数据基础结构提供云弹性。此功能使客户能够根据其基础结构的可用容量，与在 Azure 中相同的方式动态地向上或向下扩展数据库。此功能可以以亚秒级的响应时间满足具有不稳定需求的突发场景需求，包括需要实时接收和查询任何规模的数据的场景。

该能源公司可以将数据服务带到任何需要访问的位置。完全托管的数据库服务 (如 Azure SQL 数据库) 为将数据库迁移到 Azure 的客户消除了修补和升级的负担。Azure 数据库托管实例创建允许你选择要部署的位置。你不必部署到 Azure;可以部署到本地环境或其他云提供商。

借助 Azure Arc, 客户 (如该能源公司) 首次可以从 Azure 安全中心访问 Azure 独特的安全功能, 以处理其本地数据工作负载。他们可以像在 Azure 中一样, 通过高级威胁防护和漏洞评估等功能来保护数据库。

通过升级辅助系统并在足够的测试期后故障转移到系统, 可对更新进行处理。通过这些滚动升级, 公司可以将每个数据库提升到所需的兼容性级别。

高级数据安全性为你提供漏洞评估, 帮助你发现安全状况中的弱点。高级威胁防护可以帮助你识别可能表示特定威胁的规律。

接下来要了解的内容

[适用于数据服务的 Azure Arc, 包括 SQL 和 PostgreSQL (Microsoft Ignite)]

04. 监管、隔离和非互联工作负载

一些组织可能需要能够与公有云完全断开连接运行，或仅在公有云外部存储敏感数据。这些要求也可能是物理环境的结果，我们将在下面的用例中看到。

示例

满足隔离要求

金融和制造业等关键行业可能要求其系统和应用程序独立运行。政府机构通常希望关键信息只在机构的四面墙内存储和访问，绝对不连接到 Internet。这些要求通常是一种安全措施或遵守法规要求的方式。

边缘的非互联计算

我们经常看到这样的混合云场景：系统和流程由于间歇性连接而与 Internet 隔离。游轮是一个容易理解的示例 - 卫星连接既昂贵又有限，因此移动海量数据可能会导致成本过高且不可靠。如果你希望能够为任何地方的游轮乘客提供一流的体验，那么无论是在陆地上还是在海上，你都希望在游轮上拥有相同的应用。

数据隐私和合规性

数据隐私的新法规非常常见, 因为许多国家/地区正在更新其法律。这给全球运营的公司增加了真正的业务风险, 因为这可能导致特定区域的 服务关闭和/或需要投资来创建单独的应用程序, 以便在不同位置的单独系统上运行。

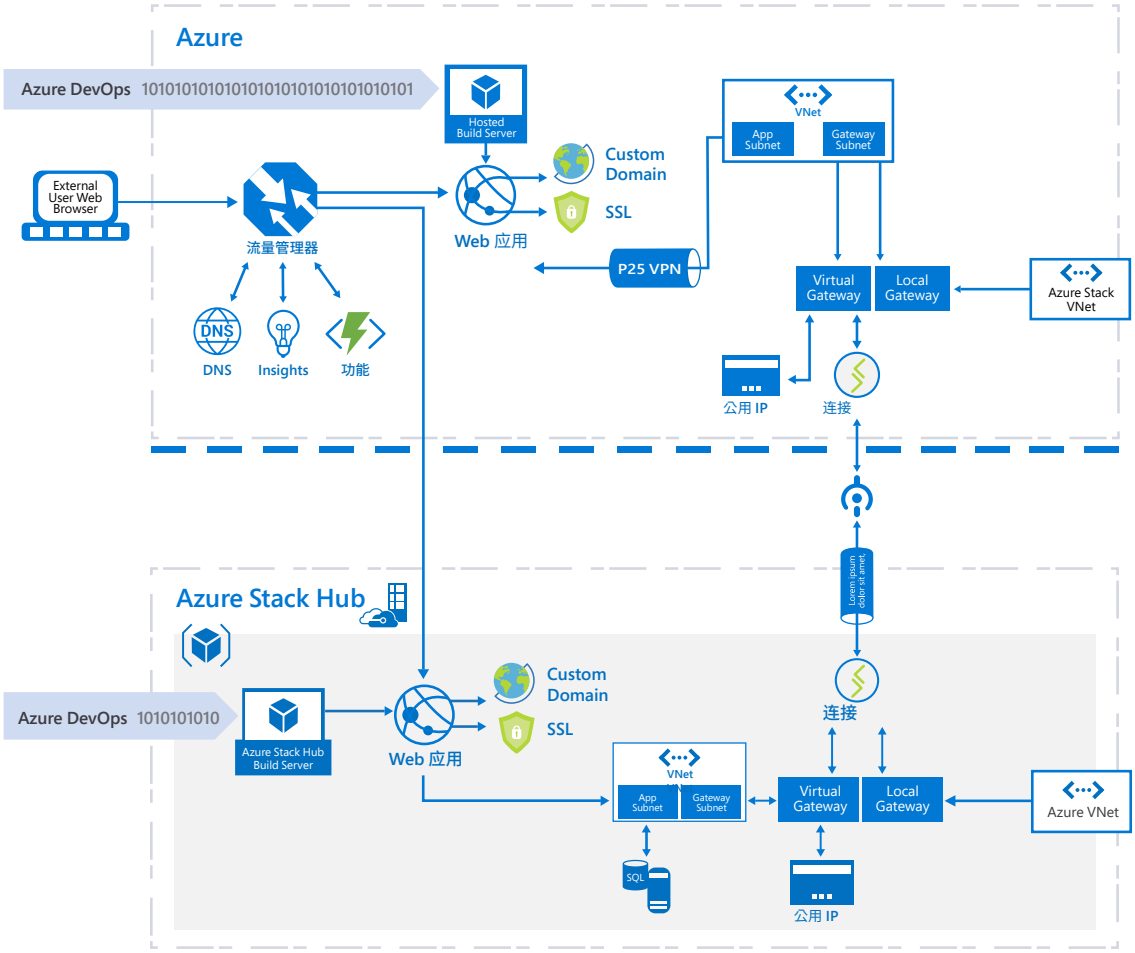
解决方案

Azure Stack Hub 是一个经过全面优化和专门构建的集成系统, 无论你连接到 Internet 还是以完全隔离的方式断开连接, 它都可以运行 Azure 服务。

使用该技术, 公司可以在 Azure 和本地环境中重用代码并一致地运行云原生应用程序, 同时继续利用 IaaS 并通过可选的云连接运行虚拟化工作负载。

借助 Azure Stack Hub, 公司可以将应用程序部署到隔离或非互联的环境中, 无论是需要满足法规要求的金融公司, 还是需要适应不可靠连接的运输公司。数据可以保留在云中或本地, 以满足数据驻留要求, 并且应用程序可以从云或本地运行, 以满足非互联工作负载的需求。

Azure Stack Hub



参考: https://docs.microsoft.com/azure-stack/hybrid/pattern-cross-cloud-scale-onprem-data

接下来要了解的内容

Azure 针对 Azure Stack Hub 集成系统的非互联部署规划决策

视频: 适用于混合计算和非互联场景的 Azure Stack

扩展 Azure Stack 产品组合, 跨云、数据中心和边缘

运行混合应用程序

Azure 混合模式和解决方案文档

Azure Stack Hub 概述

Azure Stack Hub 开发工具包

05. 远程分支机构

拥有分支机构的企业是部署混合基础结构的挑战。当多个位置没有专门的 IT 人员时，保持身份服务同步、备份数据和部署应用程序变得更加复杂。任何解决方案都必须能够快速、轻松地在远程分支机构部署应用程序和身份变更，同时允许中央 IT 部门监视异常和违规行为。

示例

企业通常需要数周或数月时间才能在多个分支机构和基础结构中部署应用程序更新。一家在全球拥有 300 个分支机构的全球性银行需要一年的时间来 更新全球的每个分支机构。此外，多个位置使其难以避免配置错误，例如开放端口。

向分支机构部署新的和更新的应用程序可能给拥有数十或数百个此类站点的公司带来问题。分支机构通常需要在本地服务器上运行一些应用程序，以防出现将公共 Internet 可用性问题，比如备份或延迟问题。

在许多远程分支机构中，可用的 IT 人员很少，这可能会使将应用程序部署到多个站点具有挑战性。

解决方案

Azure Stack HCI 提供采用行业标准 x86 服务器的超融合基础结构以及软件定义的计算、存储和网络。通过 Windows Admin Center 中内置的 Azure 集成，轻松开始使用云进行超融合基础结构管理。

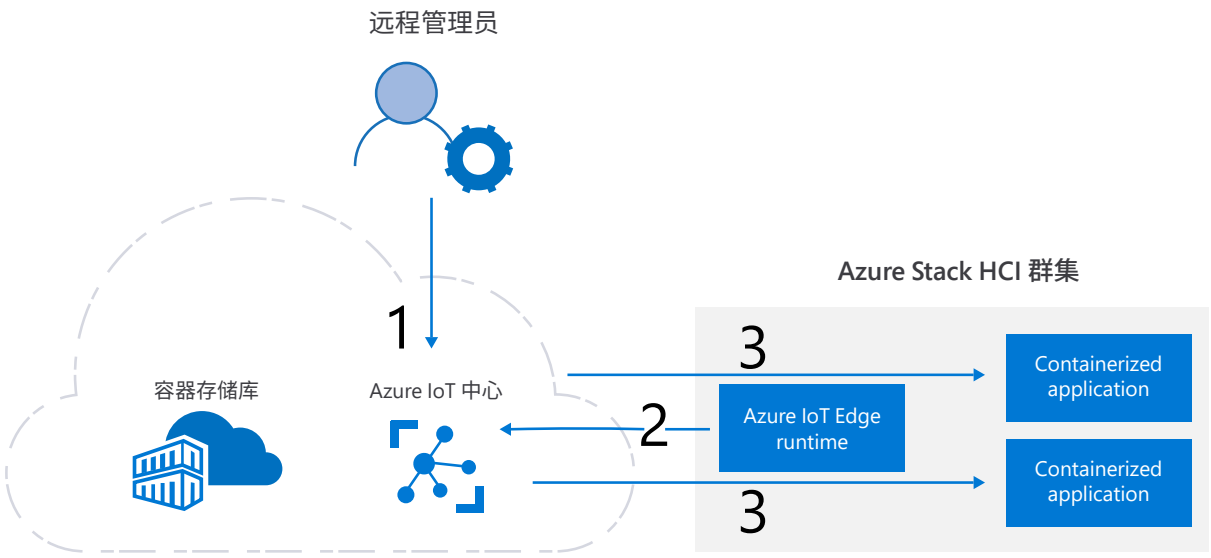
满足分支机构、零售商店和现场位置不断变化的 IT 需求。将你的容器构建的边缘工作负载和必要的业务应用程序部署到高度可用的虚拟机中，并使用 Azure Monitor 来全面 了解系统运行状况。

对于 IT 人员很少的分支机构，在全球任何地方工作的管理员的帮助下，Azure IoT Edge 可用于简化将容器化应用程序部署到 Azure Stack HCI 群集的过程。Azure IoT Edge 是一个引擎，可以安装在 Azure Stack HCI 中的虚拟机上，并为群集启用容器。Azure IoT Edge 还包含物联网 (IoT) 网关功能，使安装在上面的设备能够通过 Azure IoT 中心从云中进行远程管理。

对于技术人员很少的分支机构，可以在全球任何地方工作的管理员的帮助下，使用 Azure IoT Edge 来简化将容器化应用程序部署到 Azure Service HCI 群集的过程。

接下来要了解的内容

[分支机构考虑事项]
[使用 Azure 备份企业的两种强大方法]
[Azure Stack HCI 白皮书]



06. 在边缘部署计算和 AI

随着世界的数字化，组织在边缘生成越来越多的数据。数据来自许多来源，如摄像头、物联网传感器和工业自动化。组织可以从在数据生成的位置对数据进行分析、修改和筛选中受益，并且只需将所需的数据传输到云以进行进一步处理或存储。

示例

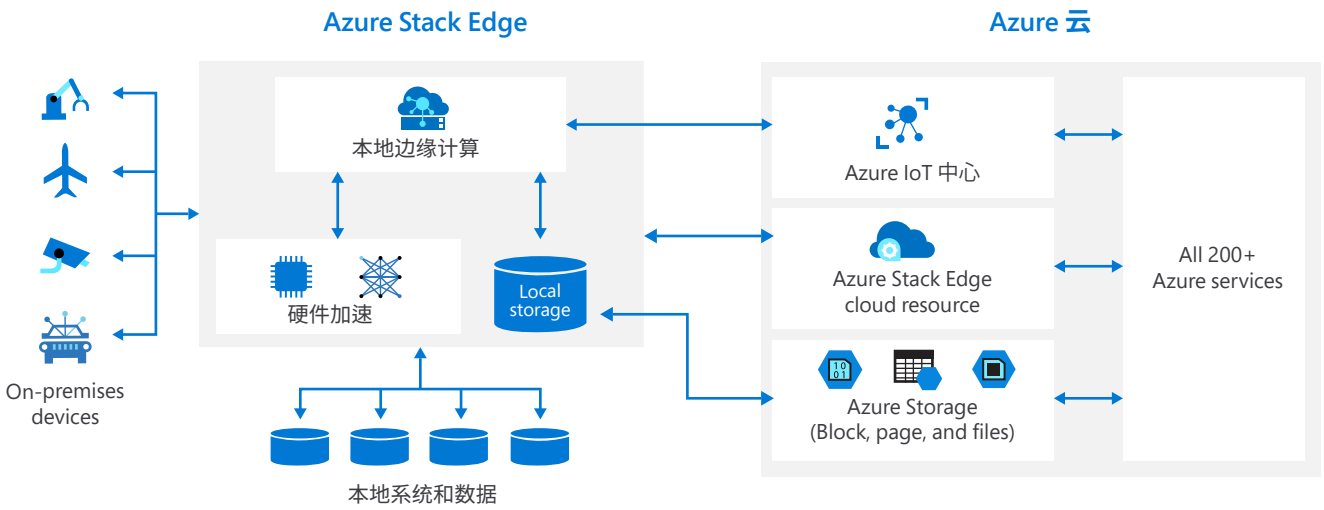
一个零售楼层在商店里有几十个摄像头。库存不足或缺失是一个影响很大的业务情况，会导致客户不满、收入损失，并且可能会耗费员工大量时间。

解决方案

使用商店中的 Azure Stack Edge 从店内摄像头收集货架的实时馈送，同时利用板载 FPGA 或 GPU 的 AI 功能，你可以运行在 Azure 上训练并在 Azure Stack Edge 上本地运行的机器学习代码，以对场景进行评分并就库存、客户需求和购物模式做出决策。

使用 Azure Stack Edge，你可以在接近数据来源的地方处理数据，而无需等待在云之间的往返，从而可以快速获取结果。在边缘分析、转换和筛选数据，仅将所需的数据发送到云以进行进一步处理或存储。使用云将容器化的应用程序推送到所有位置的 Azure Stack Edge 设备。

Azure Stack Edge 如何支持边缘计算和机器学习



Azure Stack Edge 在作为 Azure 服务交付的云托管边缘计算设备中结合使用了 IoT Edge 和加速 ML 推理

接下来要了解的内容

Azure Stack Edge
Azure IoT Edge
计算的未来: 智能云和智能边缘

07. 跨 VMware 环境迁移和管理应用程序

要想使混合方法成功，组织必须拥有一致的解决方案，以统一跨物理和虚拟环境的计算机管理，并快速扩展。运行 VMware 工作负载的客户现在可以使用一个共同的操作框架在 VMware 环境和 Microsoft Azure 中无缝地运行、管理和保护应用程序。

示例

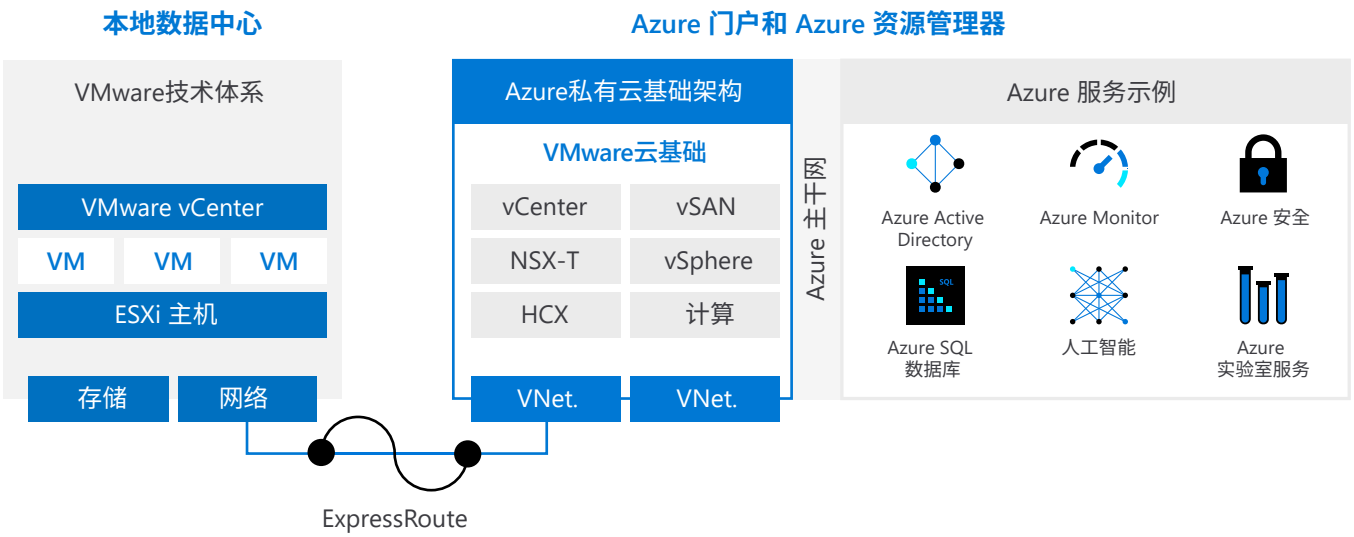
全球健康危机给
医院的运营骤然造成巨大的压力，而医院的应用程序都运行在 VMware 上。随着人员配置的增加，医院需要扩展其 IT 基础架构，以便测试其人力资源、患者管理和 EMR 系统，同时确保仍然符合 HIPAA 的要求并满足最近的预算削减要求。部署新技术基础架构的申请流程、审批和后勤可能需要 4 到 6 个月或更长时间。因此，为了在扩展和缩减其基于云的系统的同时
最大限度地利用时间和资源，医院将需要能够使用在 VMware 方面现有的 IT 技能、流程和经验来进行高效部署和增强。

解决方案

Azure VMware 解决方案具有基础结构弹性，无需花费资金即可进行扩展和缩减，同时保持员工和流程的连续性。除获得其他主要的行业标准认证外，该解决方案还完全符合 HIPAA 的要求，减少了采用的障碍，加快了向云端迁移的速度。

使用 Azure VMware 解决方案，医院可以快速扩展，以满足其 IT 系统的意外需求。通过使用 Azure VMware 解决方案将医院当前的 VMware 环境扩展到 Azure，医院利

用跨本地环境和 Azure 的一致管理体验最大限度地减少了中断。他们可以利用已在使用的工具和技能，使以前的投资最大限度地发挥其价值。此外，医院可以在此基础上发展，随着时间的推移实现无缝现代化，利用 Azure 进行资源的统一管理。



接下来要了解的内容

[Azure VMware 解决方案]
[Azure VMware 解决方案文档]
[AVS 演示]

04 /

结语

随着公司努力实现业务的数字化转型，混合计算发挥着重要作用。

成功将运营迁移到云并使用本地技术改善运营的企业将更好地控制应用程序，并降低部署和管理成本。这将使运营更加灵活，形成一系列标准化的共享工具和服务，并降低业务成本。

由于许多不同的原因，企业依赖于混合云方法。随着越来越多的业务运营和应用程序扩展到包括边缘设备和多个云，组织面临着这样的现实：拥有数百到数千个应用程序，跨广泛的基础结构运营，跨越本地数据中心、多云和边缘。

因此，你的混合云战略必须不断发展，以便随时随地实现创新，同时在所有分布式位置提供无缝的开发、部署和持续管理体验。专注于混合云基础结构的公司应：

- **以自己的方式构建**

  以极高的灵活性提供应用程序创新 - 构建任何应用程序，并始终部署到本地、多云和边缘中所需的任何位置。

- **无缝运营**

  运营本地、多云和边缘环境 (如单个环境) ，并使用 Azure 中的单个控制平面无缝管理所有资源。

- **保护企业**

  安心无忧地在整个组织中实施集成的 Azure 安全性 - 获取全面的安全管理，获得支持 AI 的威胁防护，并启用单一登录访问。

采取下一步行动

如有任何疑问，请联系 Microsoft 客户团队，
或使用下面的联系链接。

免费试用 Azure

联系我们