技术摘要

无缝 SD-WAN 编排

一个使用 Aruba Central 的简化模型

简介

SD-WAN天生可以解决大型分布式网络运维的许多配置难题。它可以根据基于用户角色和应用程序的策略，有效利用与底层传输网络无关的叠加隧道和中心化路由转发流量。只此一点，便可简化广域网的管理。

但是由于分布式网络可能需要处理来自很多不同站点的数以万计的用户和设备，为大量站点手动配置隧道和路由表仍会极其复杂。如果分支机构的网络包含各种独立的联网设备，配置起来将会更加复杂。

管理员需要一种简单且不容易出错的方式。为了满足这一需要，高度可扩展的云原生管理系统 Aruba Central 提供了 SD-WAN 编排功能。这个功能让 IT 能够根据业务策略快速且高效地建立跨越整个组织（分支机构、总部、企业数据中心，以及 Amazon Web Services (AWS)或 Microsoft Azure 等云服务商提供的虚拟私有云 (VPC)）的路由和隧道。

关于 ARUBA SD-WAN 编排工具

Aruba SD-WAN 编排工具基于能够随用户增加而平滑扩展的云原生多租户控制平面。而市场中其它竞争的编排工具都是基于虚拟机 (VM) 的控制平面元素，当需求增长并超过虚拟机的资源限制时，必须通过手动方式进行扩展。

Aruba SD-WAN 编排工具的优势在于可以自动发现广域网链路，并且能够根据业务和拓扑需求编排隧道，例如将数据中心映射到分支机构。编排工具仅会在有需要的站点之间创建隧道。同样地，路由也只在可以彼此到达的网关之间广播。

主要优势

- 节约分布式企业网络的主要管理成本
- 大幅简化广域网的管理
- 从星型到全网状的灵活拓扑选项
- 根据业务意图快速建立任意连接
- 在 SD-WAN 架构中随意组合上行链路类型
- 随客户增长情况扩展的云原生多租户控制平面
- 无需在站点之间手动设置 VPN 隧道或路由

客户不需要再为每一台设备创建单独的叠加隧道或配置独立的路由策略。图 1 提供了一个简单的示例。

在此示例中，分支机构网关具有多个上行链路，其中包括两个不同运营商的 MPLS 链路和一个互联网链路（通过有线或者 LTE）。不难想象，若有成百上千个分支机构，多个数据中心或一个或更多 VPC，路由的配置会变得极其复杂。例如，您将需要知道 IP 地址、接口名称、链路类型等。

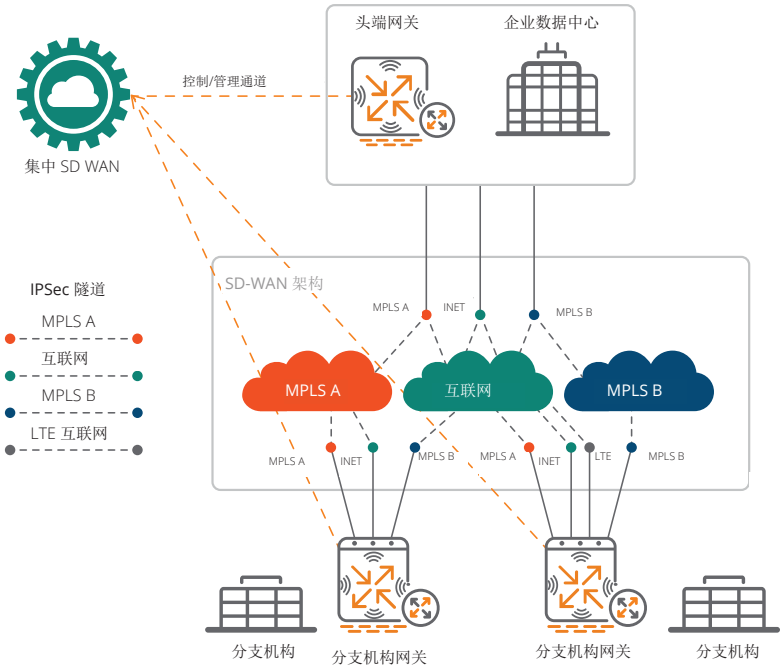

图 1：为分支机构和头端定义隧道和路由

拓扑选项

Aruba 款编排工具可以根据业务连接需要为SD-WAN叠加网络拓扑提供多个灵活选项。以下拓扑选项适用于网络中的所有节点：

- 星型互联：所有分支机构按优先顺序连接到其各自的中心
- 部分互联（中心）：网络中的特定节点可以被指定为中心（连接一组分支机构）或被选定以连接到网络内的其他节点
- 完全互联：每个节点建立全网状拓扑的隧道，所有站点均连接到所有其他站点
- 任意互联：可以选中网络中的特定节点进行连接。

可在 Aruba 编排工具中轻松选择这些选项（图 2）。

您也可以根据站点安全标准设置合理的平滑重启时间和隧道密钥更新计时器。

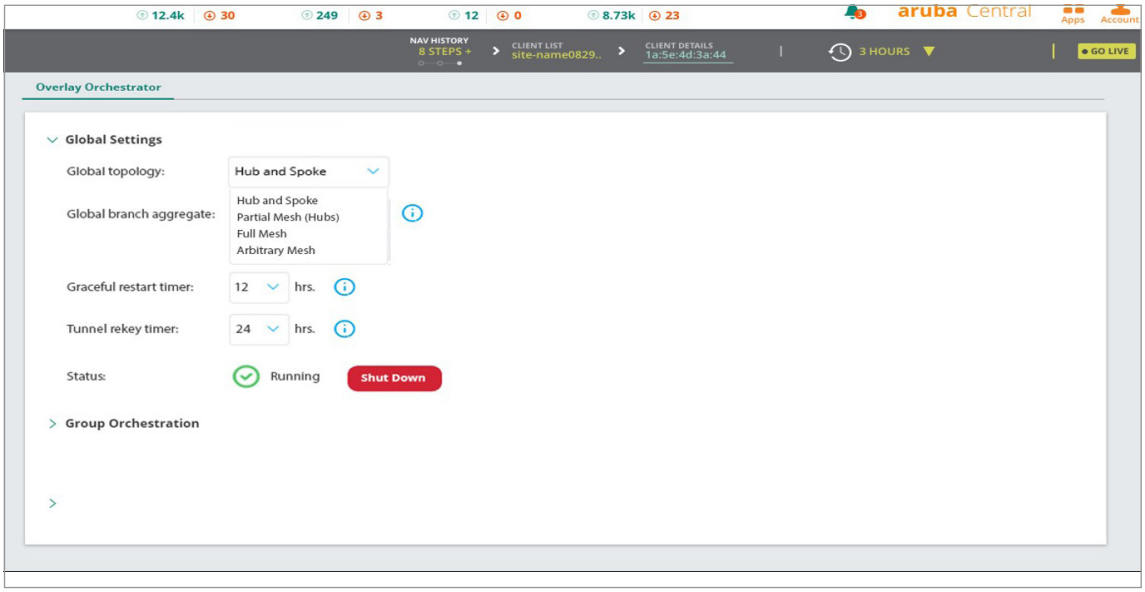

图 2：Overlay Orchestrator 下拉菜单

分组级别编排策略

针对大型部署，通常会根据区域将网络进行层次划分。利用分组级别策略，您将可以为不同区域设置不同拓扑。在这种情况下（图 3），可以在每个分组级别选择叠加网络的拓扑。

不同区域内的中心和分支机构组会与站点数量一同显示。每个区域均可根据连接需求拥有自己独有的拓扑。

路由、隧道和密钥交换的编排步骤

为大幅简化操作流程，SD-WAN 编排工具可以管理所有的广域网接口，包括其公共和私有 IP 地址。然后，SD-WAN 编排工具会自动创建隧道，例如在分支机构网关与头端设备的运营商 A 的 MPLS 接口之间。为优化流量，编排工具还会尝试尽可能把会话建立在同一运营商的互联网线路上。

分支机构网关 (BGW) 可以在互联网或其他不受信任的网络之上建立到其他站点网关的 Ipsec 隧道。为管理 VPN 隧道的密钥，Aruba Central 为隧道设置集中化的密钥管理，以便处理密钥交换和密钥轮换。IT 只需按偏好顺序提供叠加网络拓扑和中心列表即可。

该工具也会根据提供的叠加网络拓扑将路由策略集中化。该工具可以自动分布路由，及其相关偏好。

下面是编排流程中的自动化助手：

- 发现公共/私有 IP 地址
- 交换密钥
- 构建隧道
- 了解中心/分支机构站点的路由
- 以正确的 cost 值在广域网上广播路由，以及
- 以正确的 cost 值在 重分发局域网侧路由。

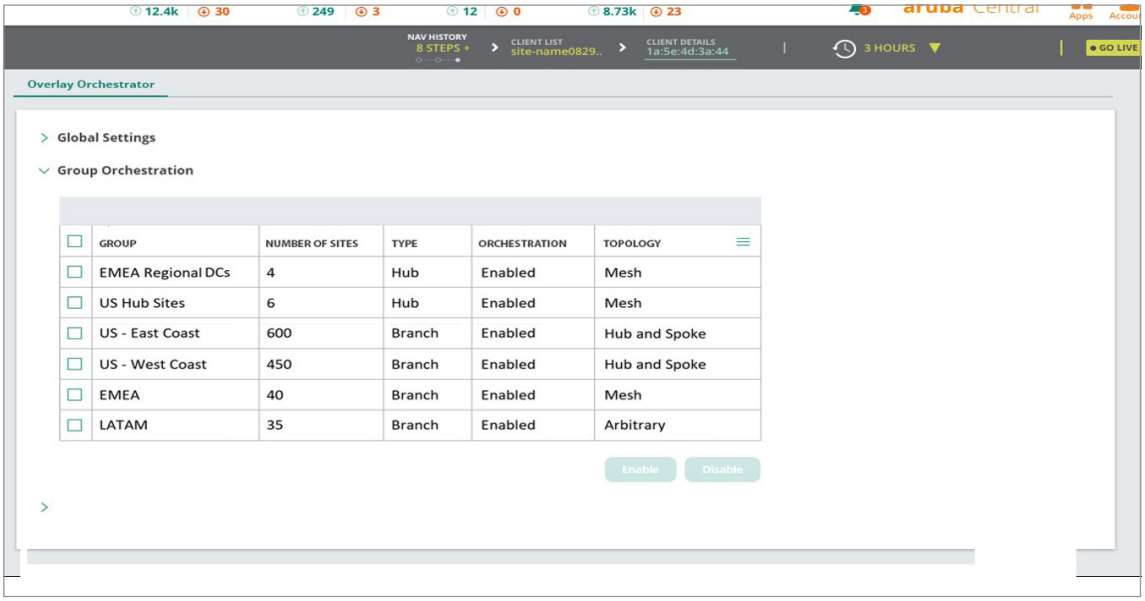

图 3：分组编排

示例：编排 SD-WAN 叠加网络

在此示例中（图 4），我们展示了一个具有单个分支机构（可能有多个，这是其中一个）的全球网络，此网络可能连接多个数据中心或云提供商端点。

此网络所需路径的编排十分简单。Aruba Central 可提供一个简化视图，展示与每个企业和云数据中心的连接和状态。在此视图中，您可以快速“双击”以更好地查看每个隧道、广域网链路、分支机构和 Aruba 头端及虚拟网关。

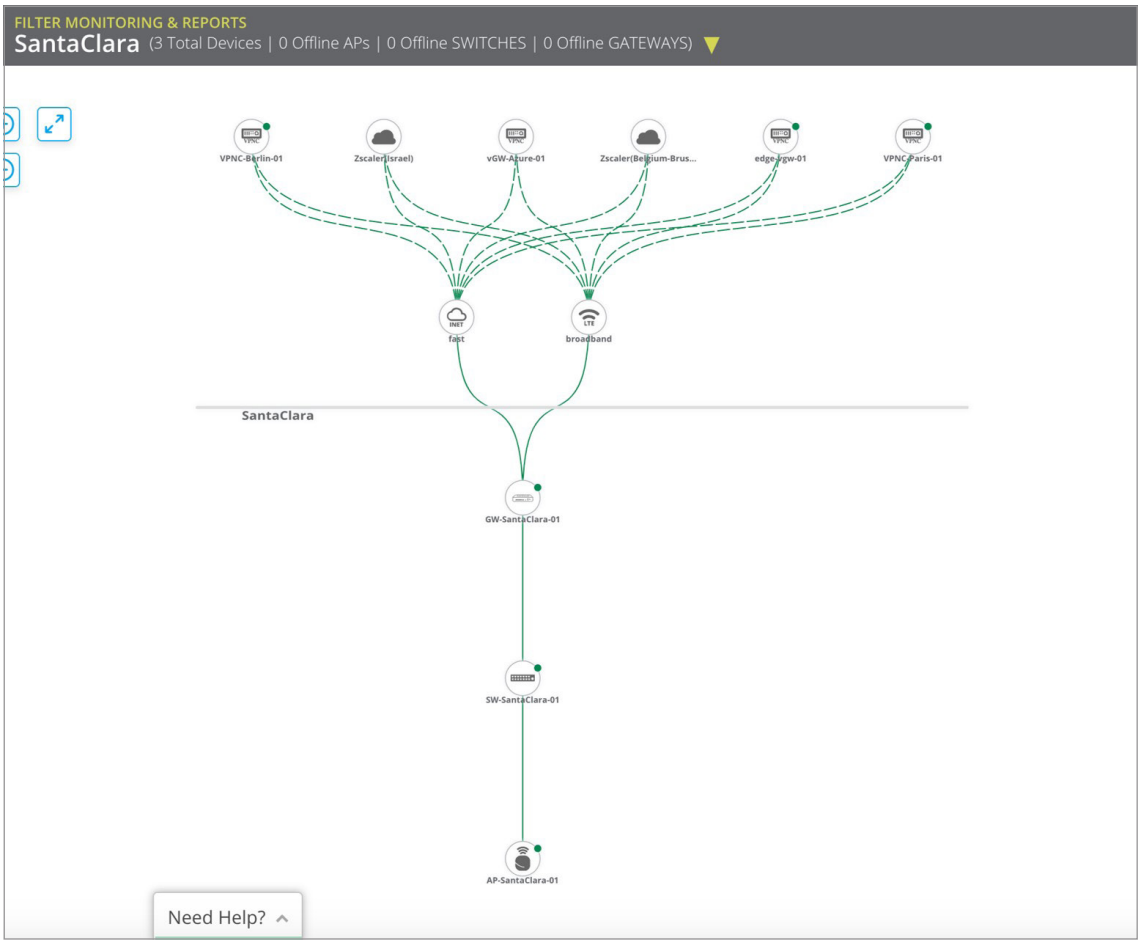

图 4：分支机构视图中的全局网络拓扑视图

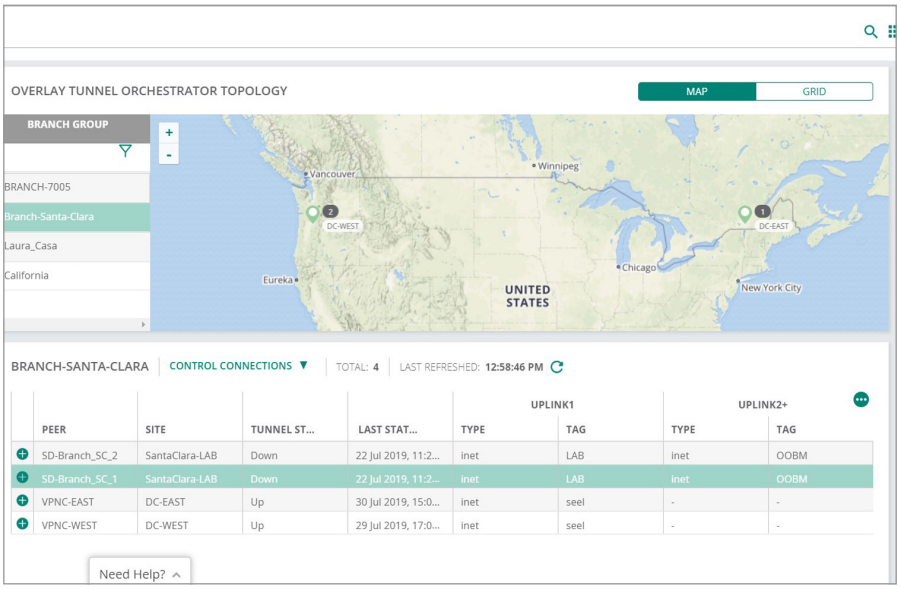

图 5：用于选定分支机构组的隧道编排工具的控制连接

隧道编排

作为管理员，您可以将网络分为多个组。这便于您根据需要更轻松地建立和查看网络的特定部分。当您选择一个分支机构组时，您可以查看分支机构可以连接到的具体头端网关（虚拟或物理）。在这里，您可以选择需要隧道连接的站点：这是有效的“基于意图的配置”，因为编排工具会完成建立隧道的工作。

通过逻辑分区方式将分支站点划分成组，您可以轻松地配置基于组的策略，以及在便于管理的抽象层面查看网络。例如，图 5 说明管理员如何查看分支机构网关与 SD-WAN 编排工具之间的连接。

如此一来，管理员便可以查看为北美组建立的所有隧道。

在下图中，图 6 显示为选定分支机构编排的所有 IPSec 隧道的列表。

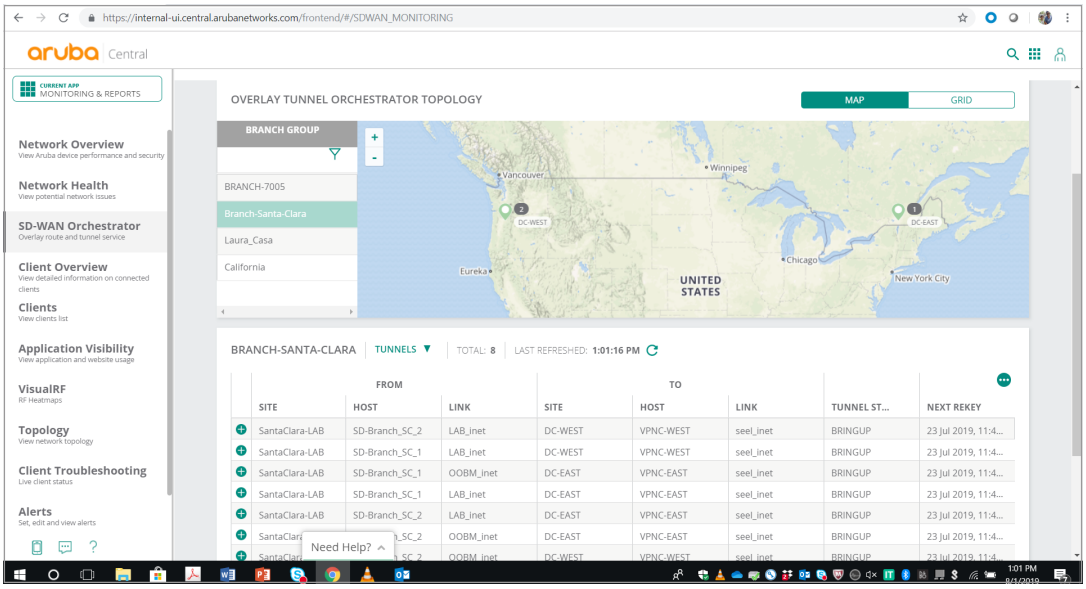

图 6：自动建立分支机构到头端的隧道

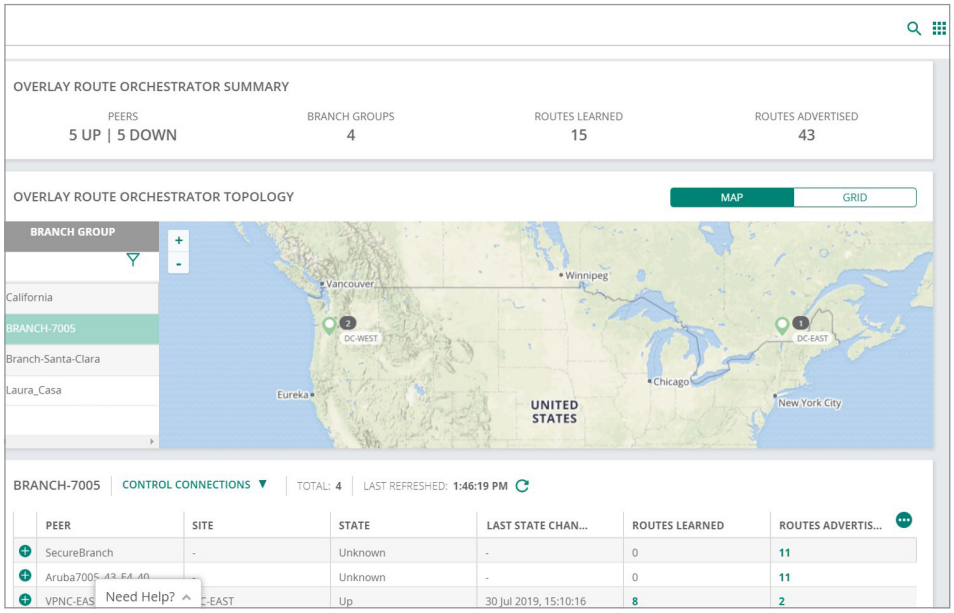

图 7：路由编排工具的控制连接

隧道会自动根据预先配置的策略建立。

路由编排

无论连接到多少头端位置或分支机构，您均可采用类似方式将路由编排自动化。SD-WAN 叠加网络上不再需要传统路由协议；您可以重新分类通过底层网络（如 BGP 或 OSPF）建立或通过其他方式（如静态路由）建立的路由。

图 7 显示的是路由编排工具。

路由编排工具会在通过不同端点学习多个路由时显示每个控制连接。分支机构网关会将已连接的路由广播给 SD-WAN 编排工具，反之，SD-WAN 编排工具也会根据预先配置的策略将路由广播给多个站点。如果您希望查看所有已学到或广播的路由（图 8），您可以在“控制连接”视图中单击这些值。

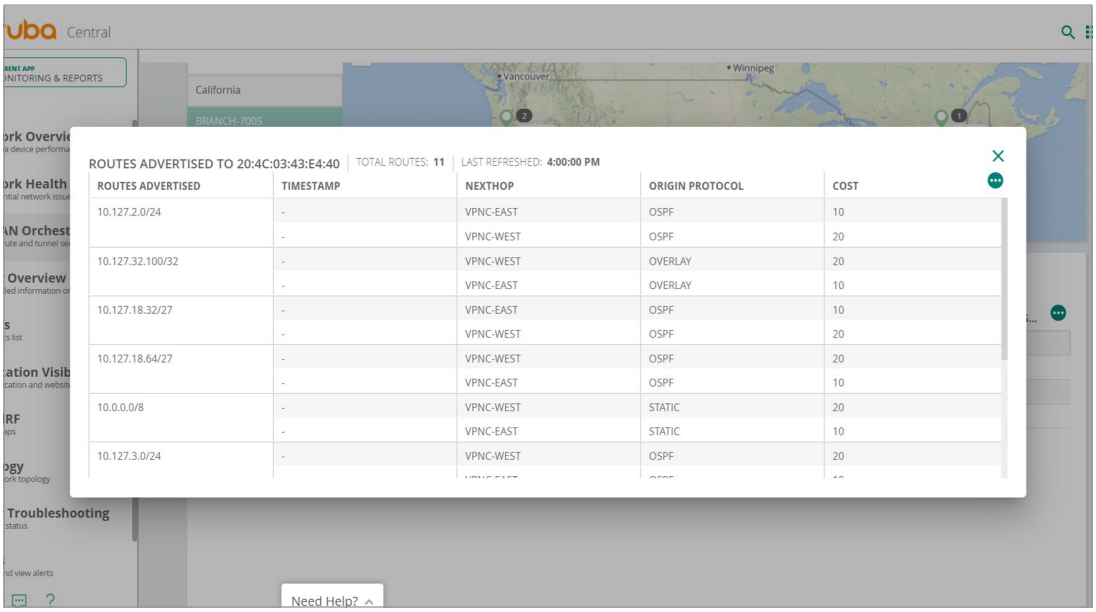

图 8：学习和广播的路由

在路由编排工具中创建并维护所有路由信息。对于每个端点和广播路由，路由编排工具会列出下一跳、原始协议和成本。

结论

SD-WAN 编排工具的价值主张在于整个 SD-WAN 部署的简化管理和优化的可达性。Aruba 解决方案和底层技术旨在简化全球最复杂分布式企业网络的 IT 体验。此外，此方法还可以改善用户体验：提高服务和应用程序性能，管理员同时获得迁移到 SD-WA N所带来的简单性。这会大幅提高企业的底线。

a Hewlett Packard Enterprise company

© 版权所有 2019 Hewlett Packard Enterprise Development LP.此处所含信息可能会在未经通知的情况下更改。对于 Hewlett Packard Enterprise 提供的产品和服务，仅在随产品和服务提供了明示担保声明时，Hewlett Packard Enterprise 方按照其中规定的条款提供担保，此处所述任何内容均不可理解为构成额外担保。对于此处所含的技术或编辑错误或疏漏，Hewlett Packard Enterprise 不承担任何责任。

TB_SeamlessSDWANOrchestration_082819