AWS 白皮书

部署的最佳实践 WorkSpaces

部署的最佳实践 WorkSpaces: AWS 白皮书

Table of Contents

部署 Amazon 的最佳实践 WorkSpaces

发布日期：2022 年 6 月 1 日 (文档修订)

摘要

本白皮书概述了一组部署的最佳实践。 WorkSpaces本白皮书涵盖了网络注意事项、目录服务和用户身份验证、安全性以及监控和日志记录。

本白皮书还允许快速访问相关信息，适用于网络工程师、目录工程师或安全工程师。

简介

Amazon WorkSpaces 是一项云端托管桌面计算服务。亚马逊 WorkSpaces 消除了采购或部署硬件或安装复杂软件的负担，只需点击几下、使用 Amazon Web Services (AWS) 命令行界面 (CLI) 或使用应用程序编程接口 (API)，即可提供桌面体验。AWS Management Console借助亚马逊 WorkSpaces，您可以在几分钟内启动微软 Windows 或 Amazon Linux 桌面，这使您能够从本地或外部网络安全、可靠、快速地连接和访问您的桌面软件。您可以：

- 使用目录服务：Active Directory Connector（ AD Connec AWS t or ），利用现有的本地 Microsoft 活动目录 (AD Connector)
- 将您的目录扩展到 AWS 云端。
- 使用 Directory Service M icrosoft AD 或 Simple AD 构建托管AWS 目录，以管理用户和 WorkSpaces。
- 利用 AD Connector 利用您的本地或云托管的 RADIUS 服务器，为您的服务器提供多因素身份验证 (MFA)。 WorkSpaces

您可以使用 CLI 或 API 自动配置亚马逊 WorkSpaces ，这使您能够将亚马逊 WorkSpaces 集成到现有的配置工作流程中。

为了安全起见，除了 Amazon WorkSpaces 服务提供的集成网络加密外，您还可以为自己启用静态加密 WorkSpaces。请参阅本文档的加密 WorkSpaces部分。

你可以使用现有的本地工具，例如微软系统中心配置管理器 (SCCM)、Puppet Enterprise 或 Ansible，将应用程序部署到你的。 WorkSpaces

以下各节提供有关Amazon的详细信息 WorkSpaces，解释该服务的工作原理，描述启动该服务所需的内容，并告诉您有哪些选项和功能可供您使用。

WorkSpaces 要求

Amazon WorkSpaces 服务需要三个组件才能成功部署：

- WorkSpaces 客户端应用程序 — Amazon WorkSpaces 支持的客户端设备。请参阅 “您的入门” WorkSpace。

  您也可以使用基于互联网协议的个人计算机 (PCoIP) Zero Clients 进行连接。 WorkSpaces有关可用设备的列表，请参阅亚马逊 PCoIP 零客户端。 WorkSpaces
- 一项目录服务，用于对用户进行身份验证并提供访问权限，亚马逊 WorkSpaces 目前与AWS 目录服务和微软广告合作。 WorkSpace您可以将本地 AD 服务器与 AWS Directory Service 配合使用，以支持您现有的亚马逊企业用户证书 WorkSpaces。
- 运行您的亚马逊的亚马逊虚拟私有云（Amazon VPC） WorkSpaces— 亚马逊部署至少需要两个子网，因为在多可用区 WorkSpaces部署中，每个 AWS 目录服务结构都需要两个子网。

网络注意事项

它们 WorkSpace 都与您用来创建它的特定 Amazon VPC 和 AWS Directory Service 结构相关联。所有 AWS 目录服务结构（Simple AD、AD Connector 和 Microsoft AD）都需要两个子网才能运行，每个子网位于不同的可用区 (AZ)。子网与 Directory Service 结构永久关联，创建后无法对其进行修改。因此，在创建目录服务结构之前，必须确定正确的子网大小。在创建子网之前，请仔细考虑以下几点：

- 随着时间的推 WorkSpaces 移，你需要多少？
- 预期增长是多少？
- 您需要容纳哪些类型的用户？
- 您将连接多少个 AD 域名？
- 您的企业账户在哪里？

Amazon 建议根据您在规划过程中所需的访问类型和用户身份验证来定义用户组或角色。当您需要限制对某些应用程序或资源的访问时，这些问题的答案会很有帮助。定义的用户角色可以帮助您使用 AWS Directory Service、网络访问控制列表、路由表和 VPC 安全组来分段和限制访问。每个 AWS Directory Service 结构使用两个子网，并将相同的设置应用于从 WorkSpaces 该构造启动的所有子网。例如，您可以使用适用于连接到 AD Connector 的所有 WorkSpaces 人的安全组来指定是否需要 MFA，或者最终用户是否可以对其拥有本地管理员访问权限。 WorkSpace

> **Note**
>
> 每个 AD Connector 都连接到你现有的企业版 Microsoft AD。要利用此功能并指定组织单位 (OU)，您必须在构建 Directory Service 时将您的用户角色考虑在内。

VPC 设计

本节介绍调整您的 VPC 和子网的最佳实践、流量以及对目录服务设计的影响。

在为您的 Amazon 设计 VPC、子网、安全组、路由策略和网络访问控制列表 (ACL) 时，需要考虑以下几点， WorkSpaces 以便您可以构建可扩展、安全且易于管理的 WorkSpaces 环境：

- VPC — 我们建议使用专门用于 WorkSpaces 部署的单独的 VPC。使用单独的 VPC，您可以 WorkSpaces 通过创建流量分离来为自己指定必要的监管和安全护栏。
- 目录服务-每个 AWS Directory Service 结构都需要一对子网，这些子网提供在可用区之间分配的高可用性目录服务。
- 子网大小 — WorkSpaces 部署与目录结构相关联并驻留在与您选择的 VPC 相同的 VPC 中 AWS Directory Service，但它们可以位于不同的 VPC 子网中。一些注意事项：
  - 子网大小是永久性的，不能更改。你应该为未来的增长留出充足的空间。
  - 您可以为所选安全组指定默认安全组 AWS Directory Service。安全组适用于与特定 AWS Directory Service 构造关联的所有 WorkSpaces 组件。
  - 您可以让多个实例 AWS Directory Service 使用同一个子网。

在设计 VPC 时，请考虑未来的计划。例如，您可能需要添加管理组件，例如防病毒服务器、补丁管理服务器或 AD 或 RADIUS MFA 服务器。值得在您的 VPC 设计中规划更多可用 IP 地址以满足此类要求。

有关 VPC 设计和子网规模调整的深入指导和注意事项，请参阅 re: Invent 演示文稿 Amazon.com 如何迁移到亚马逊。 WorkSpaces

网络接口

每个 WorkSpaces 都有两个弹性网络接口 (ENI)、一个管理网络接口 (`eth0`) 和一个主网络接口 (`eth1`)。 AWS 使用管理网络接口来管理 WorkSpace — 这是您的客户端连接终止的接口。 AWS 为此接口使用私有 IP 地址范围。为了使网络路由正常运行，您不能在任何可以与您的 WorkSpaces VPC 通信的网络上使用此私有地址空间。

有关按地区使用的私有 IP 范围的列表，请参阅 Amazon WorkSpaces 详情。

> **Note**
>
> 亚马逊 WorkSpaces 及其关联的管理网络接口不在您的 VPC 中，您也无法查看管理网络接口或您的 Amazon Elastic Compute Cloud (Amazon EC2) 实例 ID（请参阅Figure 5Figure 6、Figure 7和）。 AWS Management Console 但是，您可以在控制台中查看和修改主网络接口 (`eth1`) 的安全组设置。每个 WorkSpace 接口的主网络接口都会计入您的 ENI Amazon EC2 资源配额。对于 Amazon 的大规模部署 WorkSpaces，您需要通过打开支持请求 AWS Management Console 以增加 ENI 配额。

流量流

您可以将 Amazon WorkSpaces 流量分为两个主要部分：

- 客户端设备和 Amazon WorkSpaces 服务之间的流量。
- Amazon WorkSpaces 服务与客户网络流量之间的流量。

下一节将讨论这两个组件。

客户端设备到 WorkSpace

无论位于何处（本地还是远程），运行 Amazon WorkSpaces 客户端的设备都使用相同的两个端口连接到 Amazon WorkSpaces 服务。客户端使用端口 443（HTTPS 端口）来传输所有身份验证和会话相关信息，使用端口 4172（PCoIP 端口），同时使用传输控制协议 (TCP) 和用户数据报协议 (UDP)，用于向给定和网络运行状况检查进行像素流式传输。 WorkSpace 两个端口上的流量都经过加密。端口 443 流量用于身份验证和会话信息，并使用 TLS 加密流量。像素流媒体流量使用 AES-256 位加密，通过流媒体网关在客户端与`eth0`客户端之间进行通信。 WorkSpace更多信息可以在本文档的安全性章节中找到。

我们按区域发布 PCoIP 流媒体网关和网络运行状况检查端点的 IP 范围。通过仅允许端口 4172 上的出站流量进入您使用 Amazon 的特定 AWS 区域，您可以限制端口 4172 从公司网络到 AWS 流媒体网关和网络运行状况检查终端节点的出站流量。 WorkSpaces有关 IP 范围和网络运行状况检查终端节点，请参阅 Amazon WorkSpaces PCoIP 网关 IP 范围。

Amazon WorkSpaces 客户端具有内置的网络状态检查功能。此实用程序通过应用程序右下角的状态指示器向用户显示其网络是否支持连接。下图显示了通过选择客户端右上角的 “网络” 可以访问的网络状态的更详细视图。

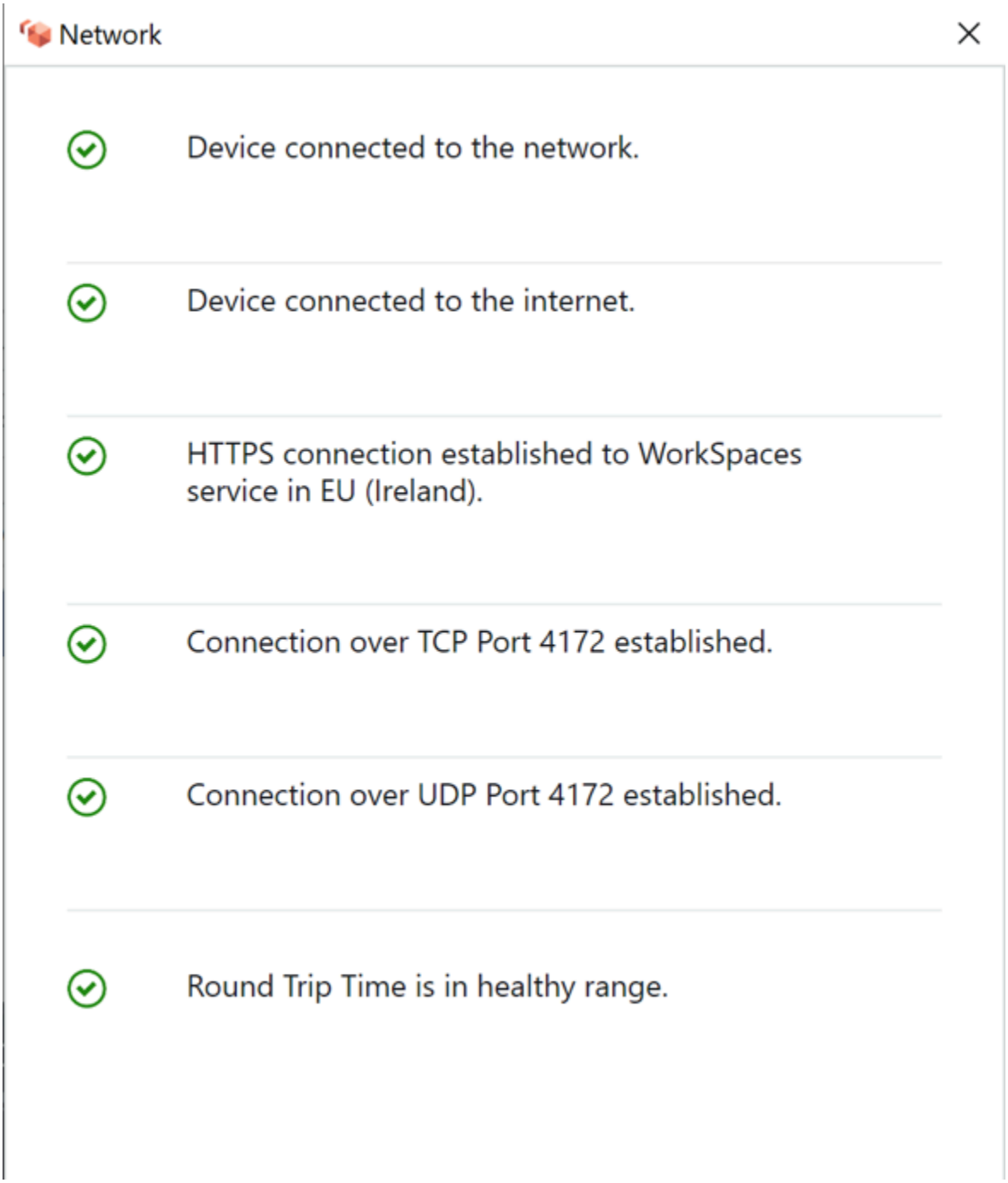

图 1： WorkSpaces 客户端：网络检查

用户通过提供目录 WorkSpaces 服务结构所使用的目录（通常是他们的公司目录）的登录信息，启动从其客户端到 Amazon 服务的连接。登录信息通过 HTTPS 发送到所在地区的 Amazon WorkSpaces 服务的身份验证网关。 WorkSpace 然后，Amazon WorkSpaces 服务的身份验证网关会将流量转发到与您 WorkSpace关联的特定 AWS Directory Service 结构。

例如，使用 AD Connector 时，AD 连接器会将身份验证请求直接转发到您的 AD 服务，该服务可能位于本地或 AWS VPC 中。有关更多信息，请参阅本文档的 AD DS 部署场景部分。AD Connector 不存储任何身份验证信息，它充当无状态代理。因此，AD Connector 必须连接到 AD 服务器。AD 连接器使用您在创建 AD 连接器时定义的 DNS 服务器来确定要连接到哪个 AD 服务器。

如果您使用的是 AD Connector，并且在目录上启用了 MFA，则在目录服务身份验证之前会检查 MFA 令牌。如果 MFA 验证失败，则不会将用户的登录信息转发到您的 Di AWS rectory Service。

用户通过身份验证后，流式传输流量将使用端口 4172（PCoIP 端口）通过 AWS 流媒体网关开始流式传输。 WorkSpace在整个会话过程中，仍通过 HTTPS 交换与会话相关的信息。流式传输流量使用 WorkSpace （ `eth0`上 WorkSpace ）上未连接到您的 VPC 的第一个 ENI。从流媒体网关到 ENI 的网络连接由管理 AWS。如果从流媒体网关到流媒体网卡的连接出现故障，则 CloudWatch 会生成一个事件。 WorkSpaces 有关更多信息，请参阅本文档的 “使用 Amazon 进行监控或记录 CloudWatch” 部分。

Amazon WorkSpaces 服务和客户端之间发送的数据量取决于像素活动级别。为确保用户获得最佳体验，我们建议 WorkSpaces 客户与您所在 AWS 地区之间的往返时间 (RTT) 小 WorkSpaces 于 100 毫秒 (ms)。通常，这意味着您的 WorkSpaces 客户距离托管区域不到两千英里。 WorkSpace C onnection Health Check 网页可以帮助您确定连接亚马逊 WorkSpaces 服务的最佳 AWS 区域。

到 VPC 的亚马逊 WorkSpaces 服务

在对从客户端到的连接进行身份验证 WorkSpace 并启动流式传输流量后，您的 WorkSpaces 客户端将显示连接到您的虚拟私有云 (VPC WorkSpace) 的 Windows 或 Linux 桌面（您的 Amazon），并且您的网络应显示您已建立该连接。 WorkSpace的主弹性网络接口 (ENI)（标识为`eth1`）将从您的 VPC 提供的动态主机配置协议 (DHCP) 服务中为其分配一个 IP 地址，该服务通常来自与您的 Di AWS rectory Service 相同的子网。IP 地址在 WorkSpace生命周期内一直保留 WorkSpace。您的 VPC 中的 ENI 可以访问 VPC 中的任何资源以及您已连接到 VPC 的任何网络（通过 VPC 对等互连、 AWS Direct Connect 连接或 VPN 连接）。

ENI 对您的网络资源的访问取决于子网的路由表和您的 AWS Directory Service 为每个子网配置的默认安全组 WorkSpace，以及您分配给 ENI 的任何其他安全组。您可以使用 AWS Management Console 或随时向面向您的 VPC 的 ENI 添加安全组 AWS CLI。（有关安全组的更多信息，请参阅您的安全组 WorkSpaces。）除安全组外，您还可以在给定对象上使用首选的主机防火墙 WorkSpace 来限制对 VPC 内资源的网络访问。

建议使用特定于您的环境的 Active Directory 的 DNS 服务器 IP 和完全限定域名创建 DHCP 选项集，然后将这些自定义创建的 DHCP 选项集分配给亚马逊使用的亚马逊 VPC WorkSpaces。默认情况

下，亚马逊虚拟私有云（亚马逊 VPC）使用 AWS DNS 而不是您的目录服务 DNS。使用 DHCP 选项集可以确保正确的 DNS 名称解析和内部 DNS 域名服务器的配置一致 WorkSpaces，这不仅适用于您的，而且适用于您可能为部署计划的任何支持工作负载或实例。

在应用 DHCP 选项时，与传统 EC2 实例的应用 WorkSpaces 方式相比，它们的应用方式有两个重要区别：

- 第一个区别是 DHCP 选项 DNS 后缀的应用方式。每个都为其网络适配器配置 WorkSpace 了 DNS 设置，启用了 “追加主后缀和连接特定 DNS 后缀” 和 “追加主 DNS 后缀的父后缀” 选项。配置将使用在您注册并默认关联的 DNS AWS 目录服务中配置的 DNS 后缀进行更新。 WorkSpace 此外，如果在使用的 DHCP 选项集中配置的 DNS 后缀不同，则会将其添加并应用于任何关联 WorkSpaces的 DNS 后缀。
- 第二个区别是，由于 Amazon WorkSpaces 服务优先考虑已配置目录的域控制器 IP 地址，WorkSpace 因此配置的 DHCP 选项 DNS IP 不会应用于。

或者，您可以配置 Route 53 私有托管区域以支持混合或拆分 DNS 环境，并为您的 Amazon WorkSpaces 环境获取正确的 DNS 解析。有关更多信息，请参阅 VPC 的混合云 DNS 选项和带有 Active Directory 的AWS 混合 DNS。

> **Note**
>
> 在 VPC 上应用新的或不同的 DHCP 选项集时，每个人都 WorkSpace 必须刷新 IP 表。要进行刷新，您可以运行 ipconfig /renew 或重启使用更新后的 DHCP 选项集配置的 VPC 中的任何 WorkSpace一个。如果您使用的是 AD Connector，并更新已连接的 IP 地址/域控制器的 IP 地址，则必须更新自己的 Skylight `DomainJoinDNS` 注册表项。 WorkSpaces建议通过 GPO 执行此操作。此注册表项的路径是`HKLM:\SOFTWARE\Amazon\Skylight`。如果修改 AD 连接器`REG_SZ`的 DNS 设置，则该值不会更新，而且 VPC DHCP 选项集也不会更新此密钥。

本白皮书 “AD DS 部署场景” 部分中的图显示了所描述的流量。

如前所述，Amazon WorkSpaces 服务会优先考虑已配置目录的域控制器 IP 地址以进行 DNS 解析，并忽略在 DHCP 选项集中配置的 DNS 服务器。如果您需要更精细地控制亚马逊的 DNS 服务器设置 WorkSpaces，可以使用《亚马逊 WorkSpaces 管理指南》的《更新亚马逊的 DNS 服务器 WorkSpaces》指南 WorkSpaces 中的说明更新亚马逊的 DNS 服务器。

因此，如果您 WorkSpaces 需要解析中的其他服务 AWS，并且使用在 VPC 中设置的默认 DHCP 选项，则必须将此 VPC 中的域控制器 DNS 服务配置为使用 DNS 转发，指向 Amazon DNS 服务器，IP

地址位于您的 VPC CIDR 底部加两个；也就是说，如果您的 VPC CIDR 是 10.0.0.0/24，则您将 DNS 转发配置为使用标准 Route 53 DNS 解析器 10.0.0.2。

如果您 WorkSpaces 需要对本地网络上的资源进行 DNS 解析，则可以使用 R oute 53 解析器出站终端节点，创建 Route 53 转发规则，并将此规则与需要此 DNS 解析的 VPC 关联起来。如果您已按照上一段所述在域控制器 DNS 服务上将转发配置为 VPC 的默认 Route 53 DNS 解析器，则可以在《Amazon Route 53 开发者指南》的《解决 VPC 之间的 DNS 查询》和您的网络指南中找到 DNS 解析流程。

如果您使用的是默认 DHCP 选项集，并且要求您的 VPC 中不属于您的 Active Directory 域的其他主机能够解析 Active Directory 命名空间中的主机名，则可以使用此 Route 53 解析器出站端点，并添加另一条 Route 53 转发规则，将活动目录域的 DNS 查询转发到 Active Directory DNS 服务器。此 Route 53 转发规则必须与能够访问您的 Active Directory DNS 服务的路由 53 解析器出站终端节点以及您想要启用的所有 VPC 关联以解析 Act WorkSpaces ive Directory 域中的 DNS 记录。

同样，R oute 53 解析器入站终端节点可用于允许对本地网络中的 Act WorkSpaces ive Directory 域的 DNS 记录进行 DNS 解析。

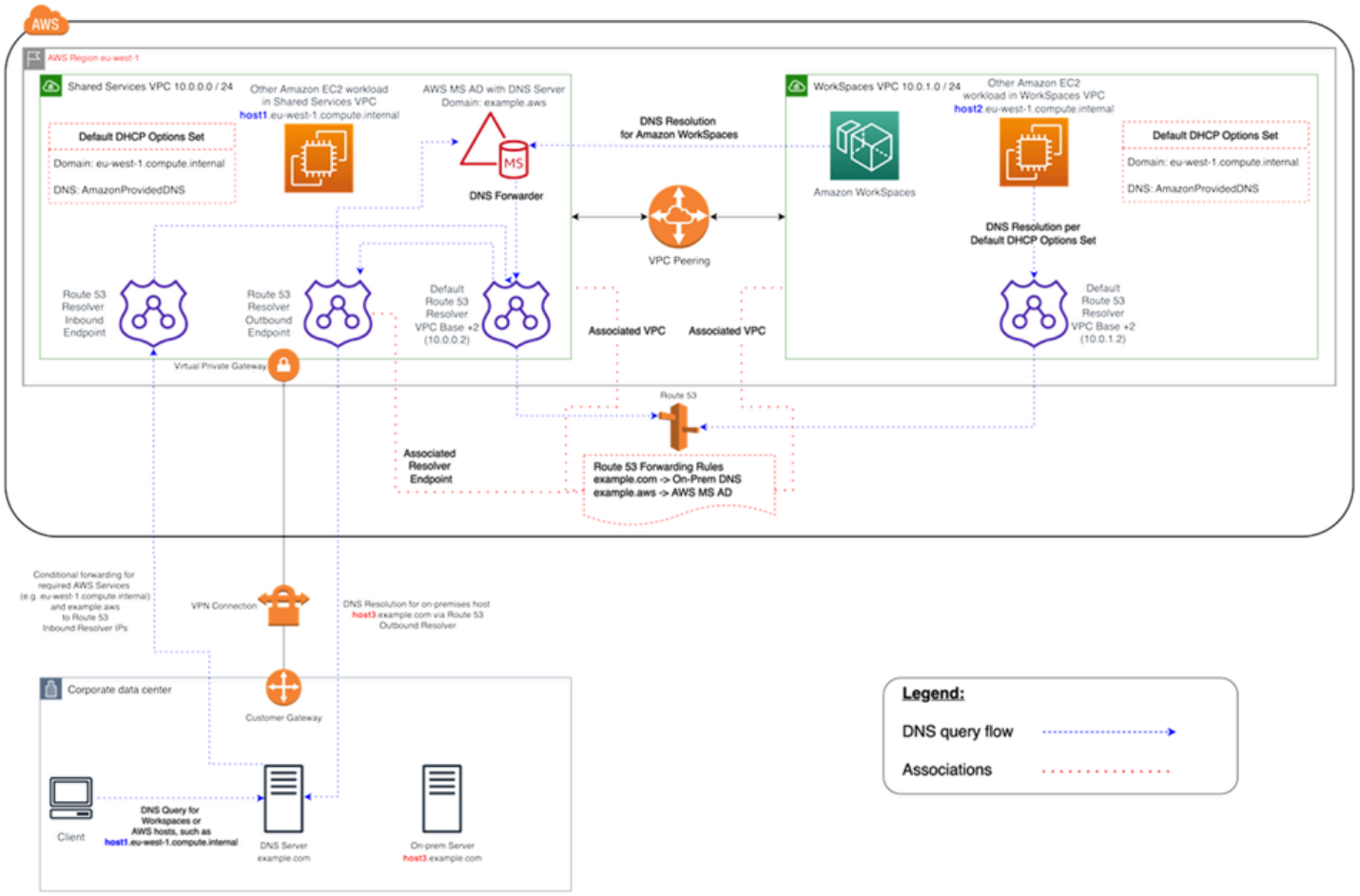

图 2：带有 Route 53 端点的 WorkSpaces DNS 解析示例

- 您的亚马逊 WorkSpaces 将使用 AWS Directory Service for Microsoft Active Directory (AWS Managed Microsoft AD) DNS 服务进行 DNS 解析。 AWS Managed Microsoft AD DNS 服务解析`example.aws`域，并将所有其他 DNS 查询转发到 VPC CIDR 基本 IP 地址 +2 处的默认 Route 53 DNS 解析器以启用 DNS 解析

  共享服务 VPC 包含一个 Route 53 出站解析器终端节点，该终端节点与两个 Route 53 转发规则相关联。其中一条规则将`example.com`域名的 DNS 查询转发到本地 DNS 服务器。第二条规则将您的 AWS Managed Microsoft AD 域名的 DNS 查询转发`example.aws`到共享服务 VPC 中的 Active Directory DNS 服务。

  使用此架构，您的 Amazon WorkSpaces 将能够解析以下内容的 DNS 查询：

  - 您的 AWS Managed Microsoft AD 域名`example.aws`。
  - 使用默认 DHCP 选项集配置的域中的 EC2 实例（例如`host1.eu-west-1.compute.internal`）以及其他 AWS 服务或终端节点。
  - 本地域中的主机和服务，例如`host3.example.com`。
- • 只要 Route 53 转发规则与两个 VP WorkSpaces C 关联即可，共享服务 VPC (`host1.eu-west-1.compute.internalhost2.eu-west-1.compute.internal`) 和 VPC () 中的其他 EC2 工作负载可以执行与您 WorkSpaces相同的 DNS 解析。在这种情况下，`example.aws`域的 DNS 解析将通过 VPC CIDR 基本 IP 地址 +2 的默认 Route 53 DNS 解析器进行，根据配置和关联的 Route 53 转发规则，该解析器将通过 Route 53 解析器出站端点将其转发到 Act WorkSpaces ive Directory DNS 服务。
- • 最后，本地客户端也可以执行相同的 DNS 解析，因为本地 DNS 服务器配置了`example.aws`和`eu-west-1.compute.internal`域的条件转发器，将这些域的 DNS 查询转发到 Route 53 解析器入站端点 IP 地址。

典型配置示例

让我们考虑一个场景，即你有两种类型的用户，而你的 AWS 目录服务使用集中式 AD 进行用户身份验证：

- 需要从任何地方获得完全访问权限的员工（例如全职员工）— 这些用户将拥有对互联网和内部网络的完全访问权限，并且他们将通过防火墙从 VPC 进入本地网络。
- 只能从公司网络内部进行限制访问的员工（例如承包商和顾问）— 这些用户通过代理服务器限制对 VPC 中特定网站的互联网访问，并且在 VPC 和本地网络中的网络访问权限将受到限制。

您想让全职员工能够拥有本地管理员访问权限 WorkSpace 以安装软件，并且您想使用 MFA 强制执行双重身份验证。您还希望允许全职员工不受其限制地访问互联网 WorkSpace。

对于承包商，您希望阻止本地管理员的访问权限，以便他们只能使用特定的预安装应用程序。您想使用安全组对其应用限制性网络访问控制 WorkSpaces。您只需要向特定的内部网站开放端口 80 和 443，并且您想完全阻止他们访问互联网。

在这种情况下，有两种完全不同的用户角色，它们对网络和桌面访问的要求不同。最佳做法是以 WorkSpaces 不同的方式管理和配置它们。您需要创建两个 AD 连接器，每个用户角色一个。每个 AD Connector 需要两个具有足够可用的 IP 地址的子网，以满足您的 WorkSpaces使用增长预期。

> **Note**
>
> 出于管理目的，每个 AWS VPC 子网消耗五个 IP 地址（前四个，最后一个 IP 地址），每个 AD Connector 在每个子网中占用一个 IP 地址。

此场景的进一步考虑因素如下：

- AWS VPC 子网应该是私有子网，这样流量就可以通过网络地址转换 (NAT) 网关、云中的代理 NAT 服务器或通过本地流量管理系统路由回来控制，例如互联网接入。
- 所有发往本地网络的 VPC 流量均已设置防火墙。
- Microsoft AD 服务器和 MFA RADIUS 服务器要么位于本地（请参阅本文档中的场景 1：使用 AD Connector 对本地 AD DS 进行代理身份验证），要么是 AWS 云实施的一部分（请参阅本文档中的场景 2 和方案 3，AD DS 部署场景）。

鉴于所有人 WorkSpaces 都有某种形式的互联网访问权限，并且它们托管在私有子网中，因此您还必须创建可以通过互联网网关访问互联网的公有子网。您需要为全职员工提供一个 NAT 网关，允许他们访问互联网，还需要一个供顾问和承包商使用的代理 NAT 服务器，以限制他们访问特定的内部网站。要做好故障规划、设计高可用性并限制跨可用区的流量费用，在多可用区部署中，您应该在两个不同的子网中安装两个 NAT 网关和 NAT 或代理服务器。在拥有两个以上区域的区域中，您选择作为公有子网的两个可用区将与您用于 WorkSpaces 子网的两个可用区相匹配。您可以将每个 WorkSpaces 可用区的所有流量路由到相应的公有子网，以限制跨可用区的流量费用并简化管理。下图显示了 VPC 的配置。

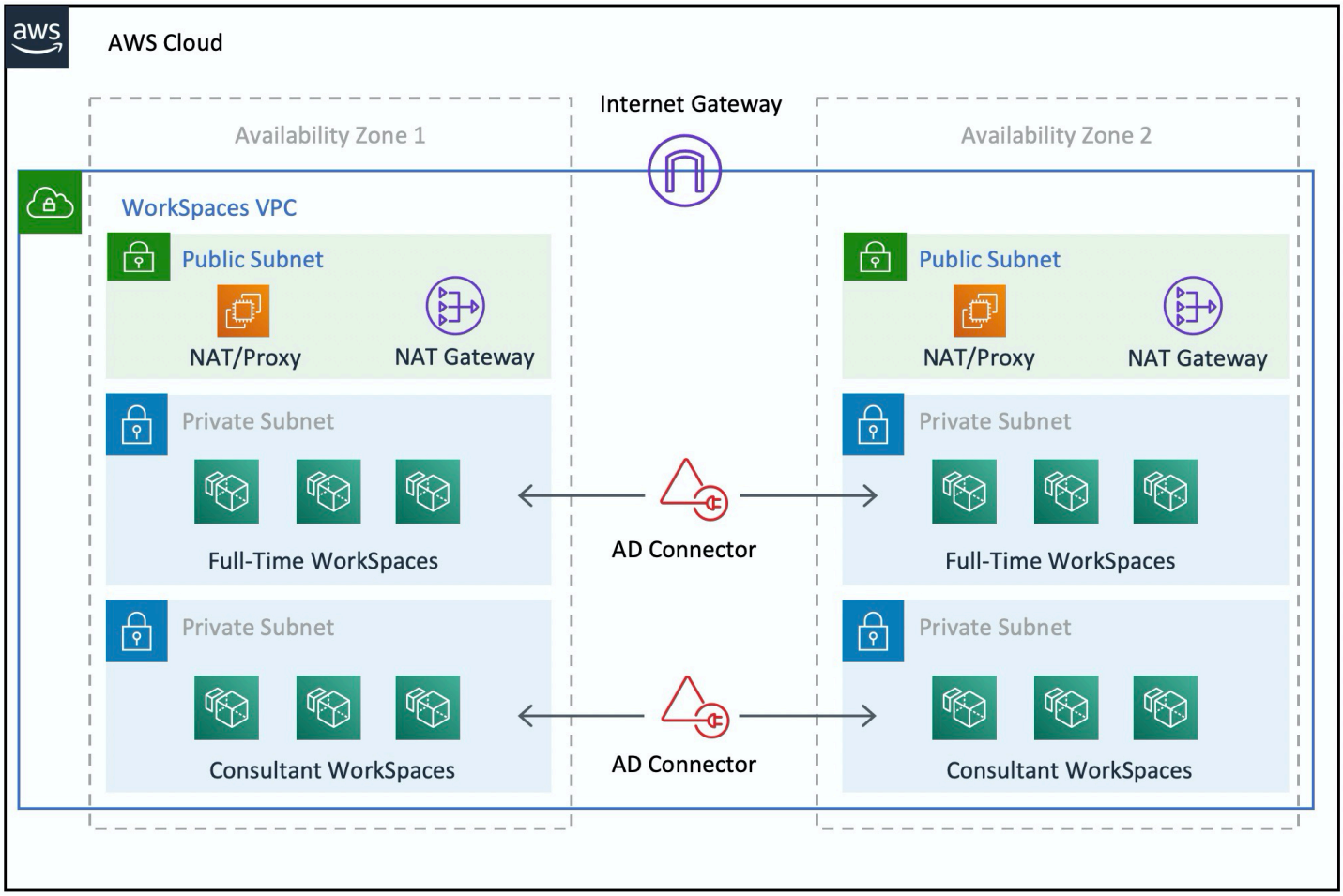

图 3：高级 VPC 设计

以下信息描述了如何配置这两种不同的 WorkSpaces 类型：

要为全职员工 WorkSpaces 进行配置，请执行以下操作：

1. 在 Amazon WorkSpaces 管理控制台中，选择菜单栏上的 “目录” 选项。
2. 选择接待全职员工的名录。
3. 选择 “本地管理员设置”。

启用此选项后，任何新创建的都 WorkSpace 将具有本地管理员权限。要授予互联网访问权限，请将 NAT 配置为从您的 VPC 进行出站互联网访问。要启用 MFA，您需要指定 RADIUS 服务器、服务器 IP、端口和预共享密钥。

对于全职员工 WorkSpaces， WorkSpace 可通过 AD Connector 设置应用默认安全组，将入站流量限制为来自帮助台子网的远程桌面协议 (RDP)。

要 WorkSpaces 为承包商和顾问进行配置，请执行以下操作：

1. 在 Amazon WorkSpaces 管理控制台中，禁用 Internet 访问和本地管理员设置。
2. 在 “安全组设置” 部分下添加一个安全组，以便为在该目录下 WorkSpaces创建的所有新用户强制使用安全组。

对于顾问 WorkSpaces，可通过 AD Connector 设置将默认安全组应用于与 AD Connector WorkSpaces 关联的所有人，从而限制出站和入站流量。 WorkSpaces 该安全组可防止从 HTTP 和 HTTPS 流量 WorkSpaces 以外的任何内容进行出站访问，以及本地网络中从 Helpdesk 子网到 RDP 的入站流量。

> **Note**
>
> 安全组仅适用于 VPC（`eth1`上 WorkSpace）中的 ENI，并且不会因为安全组而限制 WorkSpace 从 WorkSpaces 客户端访问该弹性网卡。下图显示了最终的 WorkSpaces VPC 设计。

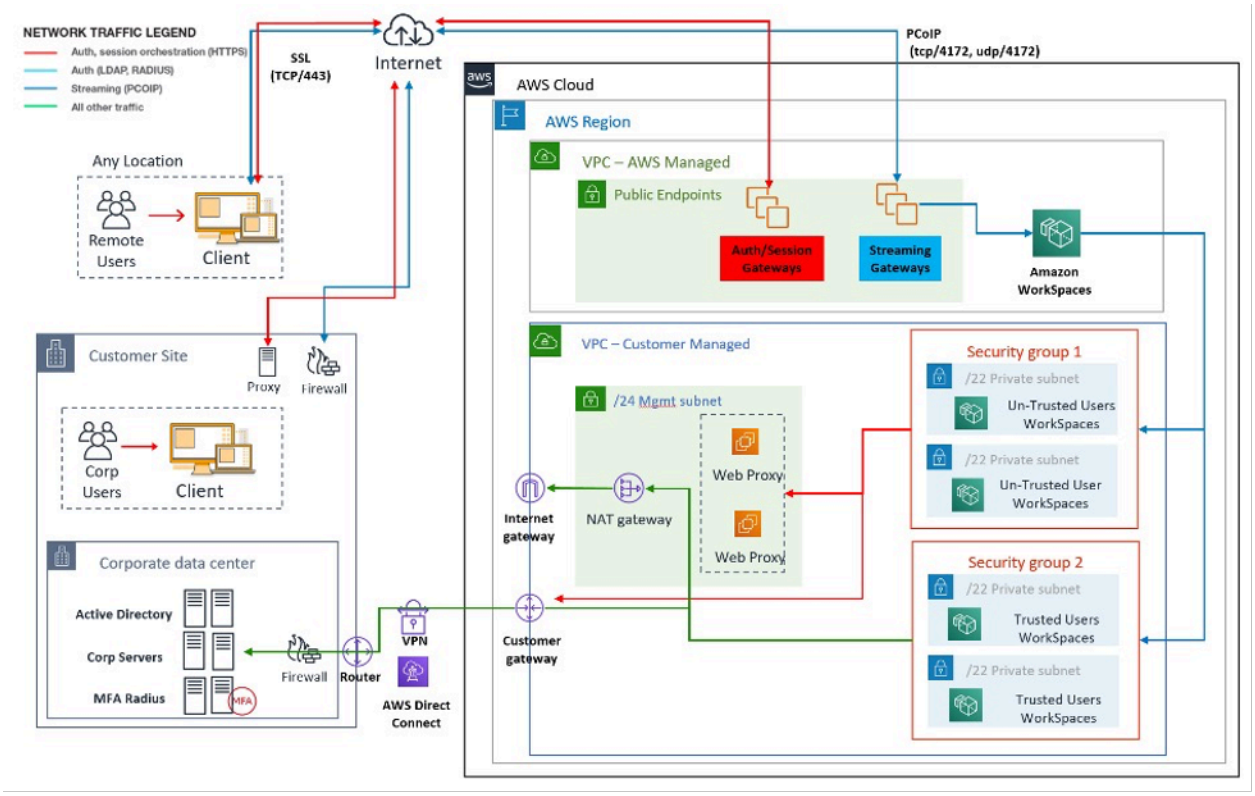

图 4：使用用户角色进行 WorkSpaces 设计

AWS Directory Ser

如导言中所述， AWS Directory Service 是亚马逊的核心组件 WorkSpaces。使用 AWS Directory Service，您可以在亚马逊上创建三种类型的目录 WorkSpaces：

- AWS M@@ anaged Microso ft AD 是一款托管的微软 AD，由 Windows Server 2012 R2 提供支持。 AWS 托管 Microsoft AD 有标准版或企业版两种版本。
- S@@ imple AD 是一款独立的、与 Microsoft AD 兼容的托管目录服务，由 Samba 4 提供支持。
- AD Con nector 是一个目录代理，用于将身份验证请求和用户或组查询重定向到你现有的本地 Microsoft AD。

以下部分介绍亚马逊 WorkSpaces 经纪服务与 AWS 目录服务之间身份验证的通信流程、 WorkSpaces 使用 AWS 目录服务实施的最佳实践以及高级概念，例如 MFA。它还讨论了亚马逊 WorkSpaces 大规模基础设施架构概念、Amazon VPC 要求和 AWS 目录服务，包括与本地微软 AD 域服务 (AD DS) 的集成。

AD DS 部署方案

支持 Amazon WorkSpaces 的是 AWS 目录服务，正确设计和部署目录服务至关重要。以下六个场景以 AWS 快速入门指南中的 A ctive Directory 域服务为基础，描述了与 Amazon 一起使用时 AD DS 的最佳实践部署选项 WorkSpaces。本文档的设计注意事项部分详细介绍了使用 AD Connector 的具体要求和最佳实践 WorkSpaces，这是整体 WorkSpaces设计概念不可或缺的一部分。

- 场景 1：使用 AD Connector 代理对本地 AD DS 的身份验证 — 在这种情况下，客户已建立网络连接（VPN/Direct Connect），所有身份验证都通过 AWS 目录服务（AD Connector）代理到客户的本地 AD DS。
- 场景 2：将本地 AD DS 扩展到 AWS （副本）— 此场景与场景 1 类似，但此处将客户 AD DS 的副本与 AD Connector 结合部署，从而减少了向 AD DS 和 AD DS 全局目录发送身份验证/查询请求的延迟。 AWS
- 场景 3：使用 AWS 云端的 AWS Directory Service 进行独立隔离部署 — 这是一个孤立的场景，不包括与客户进行身份验证的连接。这种方法使用 AWS 目录服务（微软 AD）和 AD Connector。尽管这种情况不依赖于与客户的连接进行身份验证，但它确实在需要时通过VPN或Direct Connect为应用程序流量提供了预配置。
- 场景 4： AWS Microsoft AD 和到本地的双向传递信任 — 此场景包括 AWS 托管微软 AD 服务 (MAD)，该服务与本地 Microsoft AD Forest 具有双向传递信任。
- 场景 5：使用共享服务 VPC 的 AWS Micro soft AD — 此场景使用共享服务 VPC 中的 AWS 托管 Microsoft AD 用作多个 AWS 服务（亚马逊 EC2 WorkSpaces、Amazon 等）的身份域，同时使用 AD Connector 将轻型目录访问协议 (LDAP) 用户身份验证请求代理到 AD 域控制器。
- 场景 6： AWS Microsoft AD、共享服务 VPC 和对本地 AD 的单向信任 — 此场景与场景 5 类似，但它包括使用对本地的单向信任的不同身份和资源域。

在选择 Active Directory 域服务 (ADDS) 的部署方案时，您需要考虑几个因素。本节介绍了 AD Connector 在 Amazon 中的作用 WorkSpaces，并介绍了选择 ADDS 部署方案时的一些重要注意事项。有关 ADDS 设计和规划的更多指导 AWS，请查阅 A ctive Directory 域服务 AWS 设计和规划指南。

AWS AD Connector 在亚马逊的角色 WorkSpaces

AWS AD Connec tor 是一种 AWS 目录服务，充当 Active Directory 的代理服务。它不存储或缓存任何用户凭据，而是将身份验证或查找请求转发到您的 Active Directory（本地或本地）。 AWS除非您正在

使用 AWS Managed Microsoft AD，否则它也是注册您的 Active Directory（本地或扩展到 AWS）以便在 Amazon WorkSpaces (WorkSpaces) 中使用的唯一方法。

AD Connector 可以指向您的本地 Active Directory、扩展到 AWS （Amazon EC2 上的 AD 域控制器）的活动目录，或者指向 AWS Managed Microsoft AD。

AD Connector 在以下各节中介绍的大多数部署场景中起着重要作用。将 AD Connec WorkSpaces tor 与配合使用具有许多好处：

- 当指向您的公司 Active Directory 时，它允许您的用户使用他们现有的公司凭证登录 WorkSpaces 和其他服务，例如亚马逊 WorkDocs。
- 无论您的用户访问的是本地基础设施中的资源还是诸如中的资源，您都可以始终如 WorkSpaces一地应用现有的安全策略（密码过期 AWS Cloud、帐户锁定等）。
- AD Connector 可与您现有的基于 RADIUS 的 MFA 基础设施轻松集成，从而提供额外的安全保护。
- 它可以隔离您的用户。例如，它允许为每个业务部门或角色配置多个 WorkSpaces 选项，因为多个 AD 连接器可以指向 Active Directory 的相同域控制器（DNS 服务器）进行用户身份验证：
  - 目标域或组织单位，用于有针对性地应用 Active Directory 组策略对象 (GPO)
  - 使用不同的安全组来控制往返流量 WorkSpaces
  - 不同的访问控制选项（允许的客户端设备）和 IP 访问控制组（限制对 IP 范围的访问）
  - 选择性启用本地管理员权限
  - 不同的自助服务权限
  - 选择性地强制执行多因素身份验证 (MFA) Authentication
  - 将您的 WorkSpaces 弹性网络接口 (ENI) 放置到不同的 VPC 或子网中进行隔离

如果您达到单个小型或大型 AD 连接器的性能极限，则多个 AD 连接器还允许支持更多用户。有关更多详细信息，请参阅该的大小 AWS Managed Microsoft AD部分。

只要小型 AD Connec WorkSpaces tor 中至少有一个活跃 WorkSpaces 用户，大型 AD Connector 中至少有 100 个活跃 WorkSpaces 用户，就可以免费使用 AD Connector。有关更多信息，请参阅AWS 目录服务定价页面。

网络 AWS 与本地 Active Directory 关联的重要性

WorkSpaces 依赖于与您的活动目录的连接。因此，指向 Active Directory 的网络链接的可用性至关重要。例如，如果场景 1 中的网络链接已关闭，则您的用户将无法进行身份验证，因此也将无法使用他们的 WorkSpaces。

如果要将本地 Active Directory 用作场景的一部分，则需要考虑网络链接的弹性、延迟和流量成本。AWS在多区域 WorkSpaces 部署中，这可能涉及不同 AWS 区域的多个网络链接，或者在它们之间建立对等连接的多个 AWS Transit Gateway网络链接，将您的 AD 流量路由到与本地 AD 相连的 VPC。这些网络链接注意事项适用于以下各节中概述的大多数场景，但对于那些来自 AD Connectors 的广告流量 WorkSpaces 需要穿过网络链接才能到达本地 Active Directory 的场景尤其重要。 场景 1 重点介绍了一些注意事项。

将多因素身份验证与 WorkSpaces

如果您计划将多因素身份验证 (MFA) Authentication WorkSpaces 与一起使用，则必须使用 AD Conn AWS ector 或 AWS Managed Microsoft AD，因为只有这些服务允许注册目录以与 RADIUS 一起使用 WorkSpaces 和配置。对于您的 RADIUS 服务器的放置，本网络 AWS 与本地 Active Directory 关联的重要性节中介绍的网络链路注意事项适用。

将账户和资源域分开

出于安全原因或为了提高可管理性，可能需要将账户域与资源域分开。例如，将 WorkSpaces 计算机对象放在单独的资源域中，而用户则是帐户域的一部分。这样的实现可用于允许合作伙伴组织在资源域中 WorkSpaces使用 AD 组策略进行管理，同时不放弃对账户域的控制权或授予访问权限。这可以通过使用两个带有已配置活动目录信任的活动目录来实现。以下各节对此进行了更详细的介绍：

- 场景 4： AWS Microsoft AD 和到本地的双向传递信任
- 场景 6： AWS Microsoft AD、共享服务 VPC 和对本地的单向信任

大型活动目录部署

您必须确保相应地配置 Active Directory 网站和服务。如果您的 Active Directory 由位于不同地理位置的大量域控制器组成，则这一点尤其重要。你的 Windows WorkSpaces 使用标准的 Microsoft 机制来发现他们被分配到的 Active Directory 站点的域控制器。此 DC 定位器流程依赖于 DNS，如果在 DC Locator 流程的早期阶段返回一长串优先级和权重不明确的域控制器，则可能会显著延长。更重要的是，如果您 WorkSpaces 被 “固定” 到次优域控制器，则在穿越广域网链路时，与该域控制器的所有后续通信都可能会增加网络延迟并降低带宽。这将减慢与域控制器的任何通信，包括处理可能大量的组策略对象 (GPO)，以及从域控制器传输文件。根据网络拓扑的不同，它还可能增加您的网络成本，因为 WorkSpaces 和域控制器之间交换的数据可能会不必要地通过更昂贵的网络路径。有关您的 VPC 设计 VPC 设计的 DHCP 和 DNS 以及 Active Directory 网站和服务的指导，请参阅和设计注意事项部分。

将 Microsoft Azure 活动目录或活动目录域服务与 WorkSpaces

如果你打算将 Microsoft Azure 活动目录与一起使用 WorkSpaces，你可以使用 Azure AD Connect 将你的身份与本地活动目录或开启的活动目录同步 AWS （亚马逊 EC2 上的域控制器或 AWS Managed Microsoft AD）。但是，这将不允许你加 WorkSpaces 入 Azure 活动目录。有关更多信息，请参阅微软 Azure 文档中的微软混合身份文档。

如果你想加入 Azure Active Directory，你需要部署微软 Azure Active Directory 域服务 (Azure AD DS)，在 AWS 和 Azure 之间建立连接，然后使用指向 Azure A AWS D DS 域控制器的 AD Connector。 WorkSpaces 有关如何设置的更多信息，请参阅使用 Azure Active Directory 域服务将你的添加 WorkSpaces 到 Azure AD 博客文章。

将 AWS Directory Service s 与 s 配合使用时 WorkSpaces，必须考虑 WorkSpaces部署规模及其预期增长，才能 AWS Directory Service 适当地调整部署规模。本节提供有关调整大小以 AWS Directory Service 供使用的指导 WorkSpaces。我们还建议您查看 AD Connector 的最佳做法和《AWS Directory Service 管理指南》中 AWS Managed Microsoft AD各节的最佳实践。

AD Connector 的大小调整为 WorkSpaces

Active Directory 连接器（AD Connector）有两种尺寸可供选择，小号和大号。虽然没有强制性的用户或连接限制，但我们建议对最多 500 个授权用户使用小型 AD Connector，为最多 5000 个 WorkSpaces 授权用户使用大型 AD Connector。 WorkSpaces 您可以将应用程序负载分布在多个 AD Connector 上，以根据您的性能需求进行扩展。例如，如果您需要支持 1500 个 WorkSpaces 用户，则可以 WorkSpaces 平均分配到三个小型 AD Connector，每个都支持 500 个用户。如果您的所有用户都居住在同一个域中，则 AD Connector 可以全部指向同一组 DNS 服务器来解析您的 Active Directory 域。

请注意，如果您从小型 AD Connector 开始，并且 WorkSpaces 部署会随着时间的推移而增长，则可以提出支持请求，将 AD Connector 的大小从小改为大，以便处理更多的 WorkSpaces 授权用户。

的大小 AWS Managed Microsoft AD

AWS Managed Microsoft AD允许你将 Microsoft 活动目录作为托管服务运行。启动服务时，您可以在标准版和企业版之间进行选择。标准版建议用户数不超过 5,000 的中小型企业使用，并且最多支持大约 30,000 个目录对象，例如用户、群组和计算机。企业版旨在支持多达 500,000 个目录对象，还提供一项附加功能，例如多区域复制。

如果你需要支持超过 500,000 个目录对象，可以考虑在 Amazon EC2 上部署 Microsoft Active Directory 域控制器。有关这些域控制器的大小，请参阅微软的 Act ive Directory 域服务容量规划文档。

场景 1：使用 AD 连接器对本地 Active Directory Service 进行代理身份验证

此场景适用于不想将其本地 AD 服务扩展到 AWS内部 AD 服务或无法选择新部署 AD DS 的客户。下图概述了每个组件和用户身份验证流程。

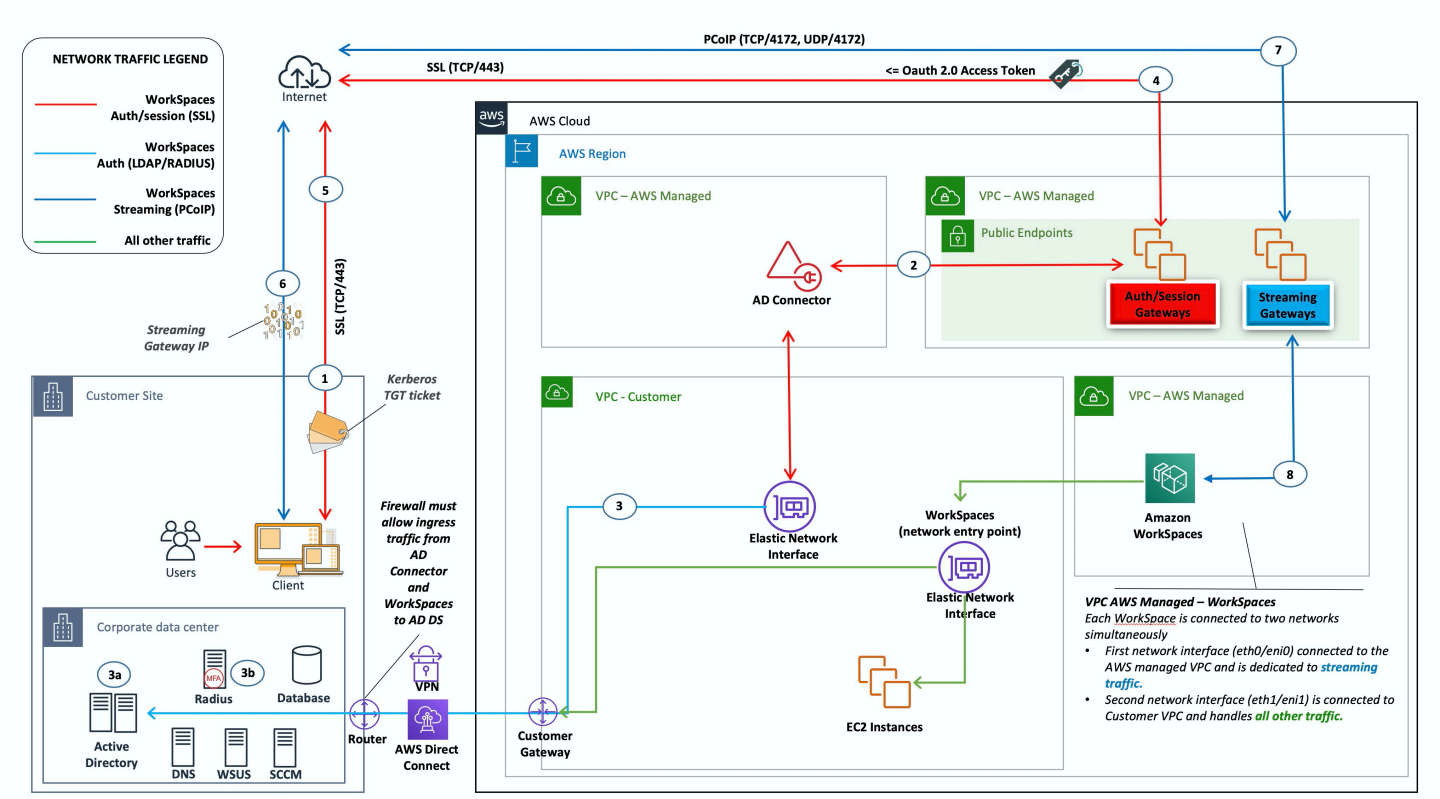

图 5：连接到本地活动目录的 AD Connector

在这种情况下，AWS 目录服务（AD Connector）用于通过 AD 连接器代理到客户本地 AD DS 的所有用户或 MFA 身份验证（详见下图）。有关用于身份验证过程的协议或加密的详细信息，请参阅本文档的安全性部分。

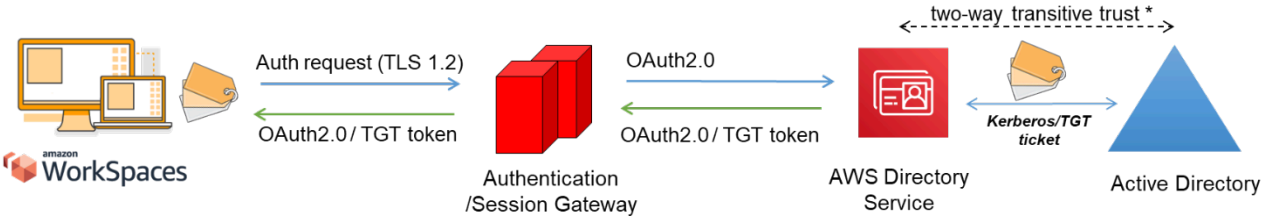

图 6：通过身份验证网关进行用户身份验证

场景 1 显示了一种混合架构，在该架构中 AWS，客户可能已经拥有资源，而本地数据中心中也有可以通过 Amazon 访问的资源 WorkSpaces。客户可以利用其现有的本地 AD DS 和 RADIUS 服务器进行用户和 MFA 身份验证。

此架构使用以下组件或结构：

AWS

- Amazon VPC — 创建跨两个可用区至少有两个私有子网的亚马逊 VPC。
- DHCP 选项集 — 创建亚马逊 VPC DHCP 选项集。这允许定义客户指定的域名和域名服务器 (DNS)（本地服务）。有关更多信息，请参阅 DHCP 选项集。
- Amazon 虚拟专用网关-允许通过 IPsec VPN 隧道或 AWS Direct Connect 连接与您自己的网络进行通信。
- AWS Directory Service — AD Connector 部署到一对 Amazon VPC 私有子网中。
- 亚马逊 WorkSpaces — 部署 WorkSpaces 在与 AD Connector 相同的私有子网中。有关更多信息，请参阅本文档的 “活动目录：网站和服务” 部分。

客户

- 网络连接-企业 VPN 或 Direct Connect 端点。
- 广告 DS — 公司广告 DS。
- MFA（可选）-企业 RADIUS 服务器。
- 最终用户设备 — 用于访问亚马逊服务的企业或自带许可 (BYOL) 的最终用户设备（例如 Windows、Mac、iPad、安卓平板电脑、零客户端和 Chromebook）。 WorkSpaces 有关支持的设备和 Web 浏览器，请参阅此客户端应用程序列表。

尽管此解决方案非常适合不想将 AD DS 部署到云端的客户，但它确实有一些注意事项：

- 依赖连接 — 如果与数据中心的连接中断，用户将无法登录各自 WorkSpaces的数据中心，并且现有连接将在 Kerberos/Ticket-Agranting Ticket Ticket (TGT) 的生命周期内保持活动状态。

- 延迟 — 如果通过连接存在延迟（VPN 比 Direct Connect 更是如此），则 WorkSpaces 身份验证和任何与 AD DS 相关的活动（例如组策略 (GPO) 强制执行）将花费更多时间。
- 流量成本-所有身份验证都必须通过 VPN 或 Direct Connect 链路，因此这取决于连接类型。这要么是从 Amazon EC2 向互联网传输数据，要么是数据传出（Direct Connect）。

> **Note**
>
> AD Connector 是一种代理服务。它不存储或缓存用户凭据。相反，所有身份验证、查询和管理请求都由您的 AD 处理。您的目录服务中需要一个具有委托权限的帐户，该帐户具有读取所有用户信息以及将计算机加入域的权限。

通常，WorkSpaces 体验在很大程度上取决于上图所示的 Active Directory 身份验证过程。在这种情况下，WorkSpaces 身份验证体验在很大程度上取决于客户 AD 和 WorkSpaces VPC 之间的网络链接。客户应确保链接高度可用。

场景 2：将本地 AD DS 扩展到 AWS （副本）

此场景与场景 1 类似。但是，在这种情况下，将客户 AD DS 的副本与 AD Connec AWS tor 结合部署。这减少了向在亚马逊弹性计算云 (Amazon EC2) 上运行的 AD DS 发出的身份验证或查询请求的延迟。下图显示了每个组件和用户身份验证流程的高级视图。

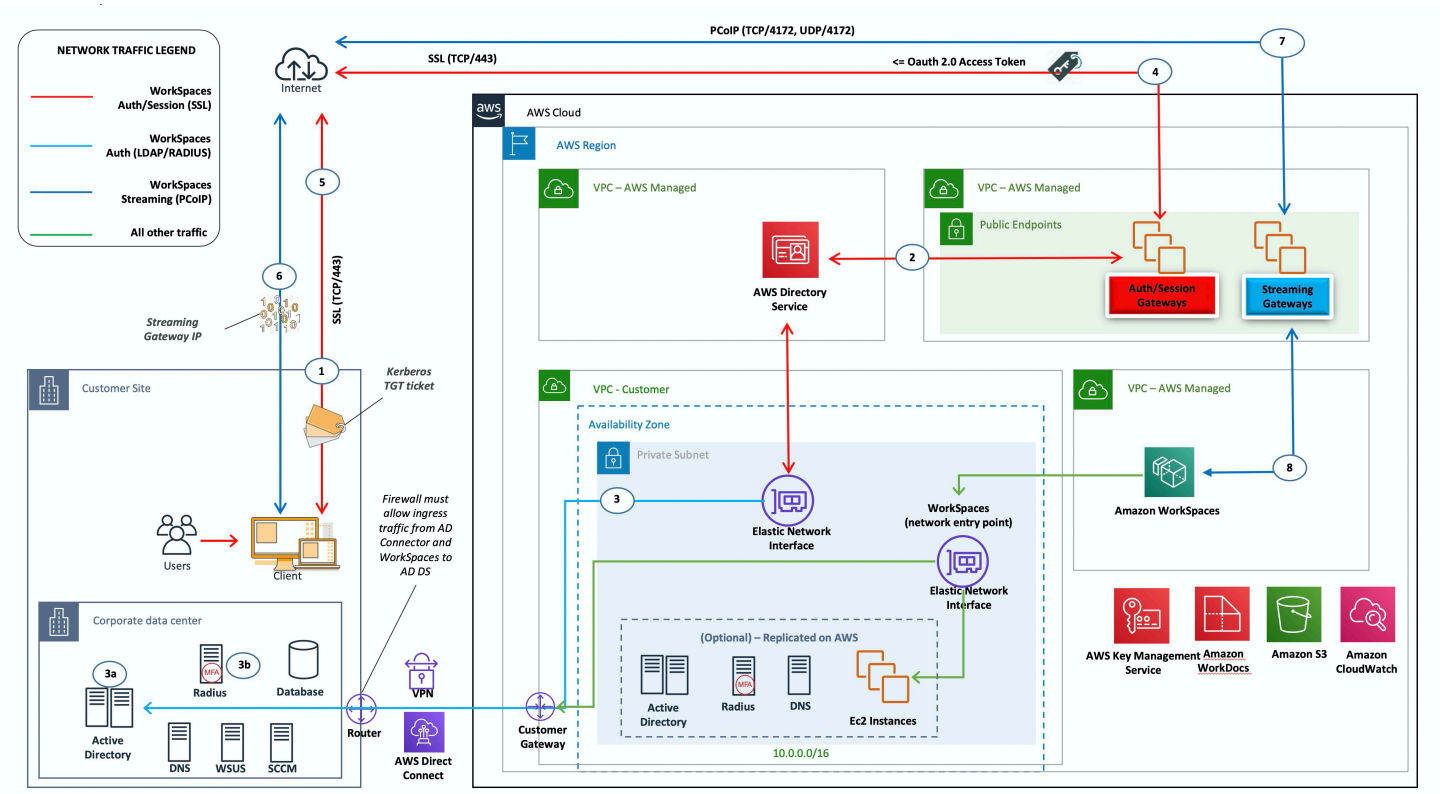

图 7：将客户 Active Directory 域扩展到云端

与场景 1 一样，AD Connector 用于所有用户或 MFA 身份验证，这反过来又被代理给客户 AD DS（参见上图）。在这种情况下，客户 AD DS 跨可用区部署在 Amazon EC2 实例上，这些实例被提升为客

户本地 A D 林中的域控制器，在 AWS 云中运行。每个域控制器都部署到 VPC 私有子网中，以使 AD DS 在 AWS 云中具有高可用性。有关在上部署 AD DS 的最佳实践 AWS，请参阅本文档的设计注意事项部分。

部署 WorkSpaces 实例后，它们可以访问基于云的域控制器，以获得安全、低延迟的目录服务和 DNS。所有网络流量，包括 AD DS 通信、身份验证请求和 AD 复制，均在私有子网内或通过客户 VPN 隧道或 Direct Connect 进行保护。

此架构使用以下组件或结构：

AWS

- 亚马逊 VPC — 创建一个亚马逊 VPC，在两个可用区中至少有四个私有子网，两个用于客户 AD DS，两个用于 AD Connector 或亚马逊。 WorkSpaces
- DHCP 选项集 — 创建亚马逊 VPC DHCP 选项集。这允许客户定义指定的域名和 DNS（本地 AD DS）。有关更多信息，请参阅 DHCP 选项集。
- Amazon 虚拟专用网关-允许通过 IPsec VPN 隧道或 AWS Direct Connect 连接与客户拥有的网络进行通信。
- Amazon EC2
  - 客户企业 AD DS 域控制器部署在 Amazon EC2 实例上的专用私有 VPC 子网中。
  - 用于专用私有 VPC 子网中的 Amazon EC2 实例上的 MFA 的客户（可选）RADIUS 服务器。
- AWS 目录服务 — AD Connector 部署到一对 Amazon VPC 私有子网中。
- 亚马逊 WorkSpaces — 部署 WorkSpaces 在与 AD Connector 相同的私有子网中。有关更多信息，请参阅本文档的 “活动目录：网站和服务” 部分。

客户

- 网络连接-企业 VPN 或 AWS Direct Connect 端点。
- AD DS — 企业 AD DS（复制所必需的）。
- MFA（可选）-企业 RADIUS 服务器。
- 最终用户设备 — 用于访问亚马逊服务的企业或自带终端用户设备（例如 Windows、Mac、iPad、安卓平板电脑、零客户端和 Chromebook）。 WorkSpaces 请参阅支持的设备和 Web 浏览器的客户端

应用程序列表。此解决方案与场景 1 没有相同的注意事项。Amazon WorkSpaces 和 AWS Directory Service 不依赖现有的连接。

- 对@@ 连接的依赖 — 如果与客户数据中心的连接中断，最终用户可以继续工作，因为身份验证和可选的 MFA 是在本地处理的。
- 延迟-除复制流量外，所有身份验证均为本地身份验证且延迟较低。请参阅本文档的 “活动目录：网站和服务” 部分。
- 流量成本 — 在这种情况下，身份验证是本地的，只有 AD DS 复制必须通过 VPN 或 Direct Connect 链路，从而减少了数据传输。

总的来说， WorkSpaces 体验会得到增强，并且不会高度依赖与本地域控制器的连接，如上图所示。当客户想要扩展 WorkSpaces 到数千台台式机时，情况也是如此，尤其是在与 AD DS 全球目录查询相关的情况下，因为这种流量仍然是 WorkSpaces 环境本地的。

场景 3：使用 AWS 云端的 AWS Directory Service 进行独立隔离部署

如下图所示，该场景将 AD DS 部署在 AWS 云端的独立隔离环境中。 AWS Directory Service 仅用于这种情况。客户无需完全管理 AD DS，而是可以依靠 Directory Servic AWS e 来完成诸如构建高可用性目录拓扑、监控域控制器以及配置备份和快照之类的任务。

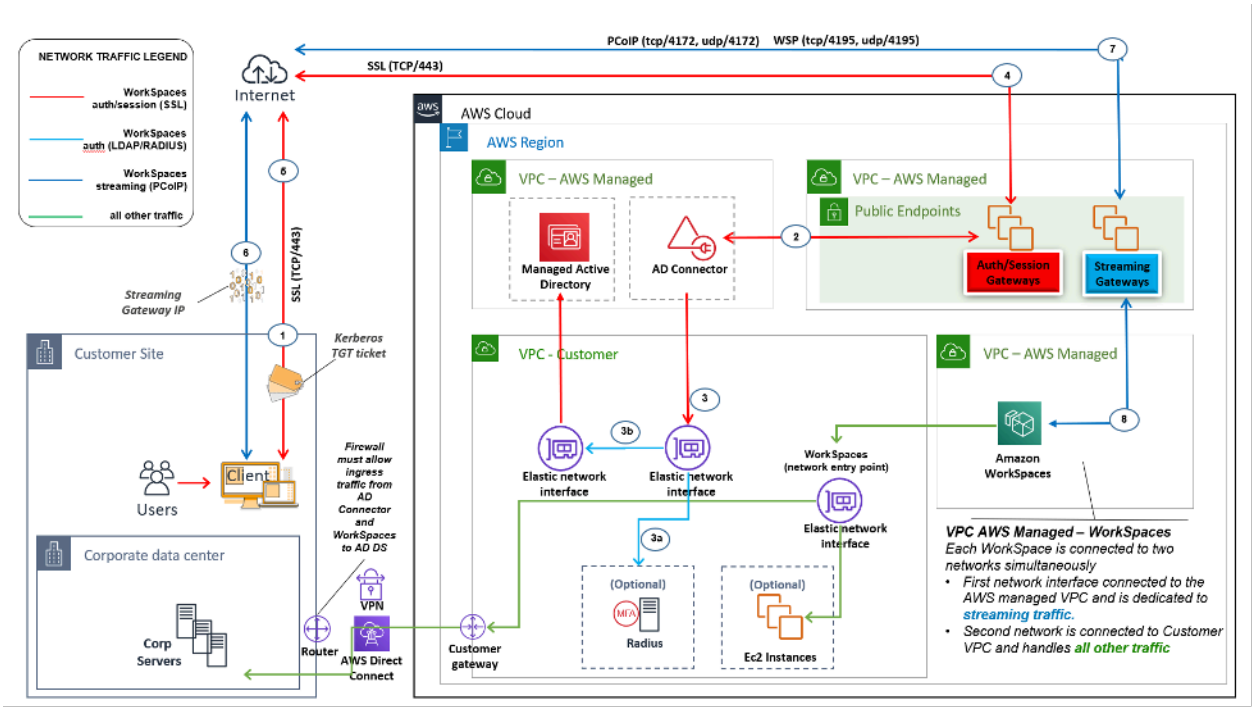

图 8：仅限云端： AWS 目录服务（Microsoft AD）

与场景 2 一样，AD DS（Microsoft AD）部署到跨越两个可用区的专用子网中，这使得 AD DS 在云中具有很高的可用性。 AWS 除了 Microsoft AD 之外，还部署了 AD Connector（在所有三个场景中），用于 WorkSpaces 身份验证或 MFA。这可确保在 Amazon VPC 内实现角色或职能的分离，这是一种标准的最佳实践。有关更多信息，请参阅本文档的设计注意事项部分。

场景 3 是一种标准的全方位配置，非常适合想要 AWS 管理 Di AWS rectory Service 的部署、修补、高可用性和监控的客户。由于其隔离模式，该场景还适用于概念验证、实验室和生产环境。

除了 AWS Directory Service 的位置外，此图还显示了从用户到工作空间的流量以及工作空间与 AD 服务器和 MFA 服务器的交互方式。

此架构使用以下组件或结构。

AWS

- 亚马逊 VPC — 创建一个亚马逊 VPC，在两个可用区中至少有四个私有子网——两个用于 AD DS M icrosoft AD，两个用于 AD Connector 或。 WorkSpaces
- DHCP 选项集 — 创建亚马逊 VPC DHCP 选项集。这允许客户定义指定的域名和 DNS（Microsoft AD）。有关更多信息，请参阅 DHCP 选项集。
- 可选：Amazon 虚拟专用网关-允许通过 IPsec VPN 隧道 (VPN) 或 AWS Direct Connect 连接与客户拥有的网络进行通信。用于访问本地后端系统。
- AWS Directory Ser vice — 部署到一对专用 VPC 子网中的 Microsoft AD（AD DS 托管服务）。
- 亚马逊 EC2 — 适用于 MFA 的客户 “可选” RADIUS 服务器。
- AWS 目录服务 — AD Connector 部署到一对 Amazon VPC 私有子网中。
- 亚马逊 WorkSpaces — 部署 WorkSpaces 在与 AD Connector 相同的私有子网中。有关更多信息，请参阅本文档的 “活动目录：网站和服务” 部分。

客户

- 可选：网络连接-企业 VPN 或 AWS Direct Connect 终端。
- 最终用户设备 — 用于访问亚马逊服务的企业或自带终端用户设备（例如 Windows、Mac、iPad、安卓平板电脑、零客户端和 Chromebook）。 WorkSpaces 有关支持的设备和 Web 浏览器，请参阅此客户端应用程序列表。

与场景 2 一样，此场景在依赖客户本地数据中心的连接、延迟或数据输出传输成本（VPC WorkSpaces 内启用互联网访问的除外）方面没有问题，因为从设计上讲，这是一个隔离或仅限云的场景。

场景 4： AWS Microsoft AD 和到本地的双向传递信任

如下图所示，该场景将 AWS 托管 AD 部署在云中， AWS 云端与客户的本地 AD 具有双向传递信任。用户和 WorkSpaces 是在托管 AD 中创建的，AD 信任允许在本地环境中访问资源。

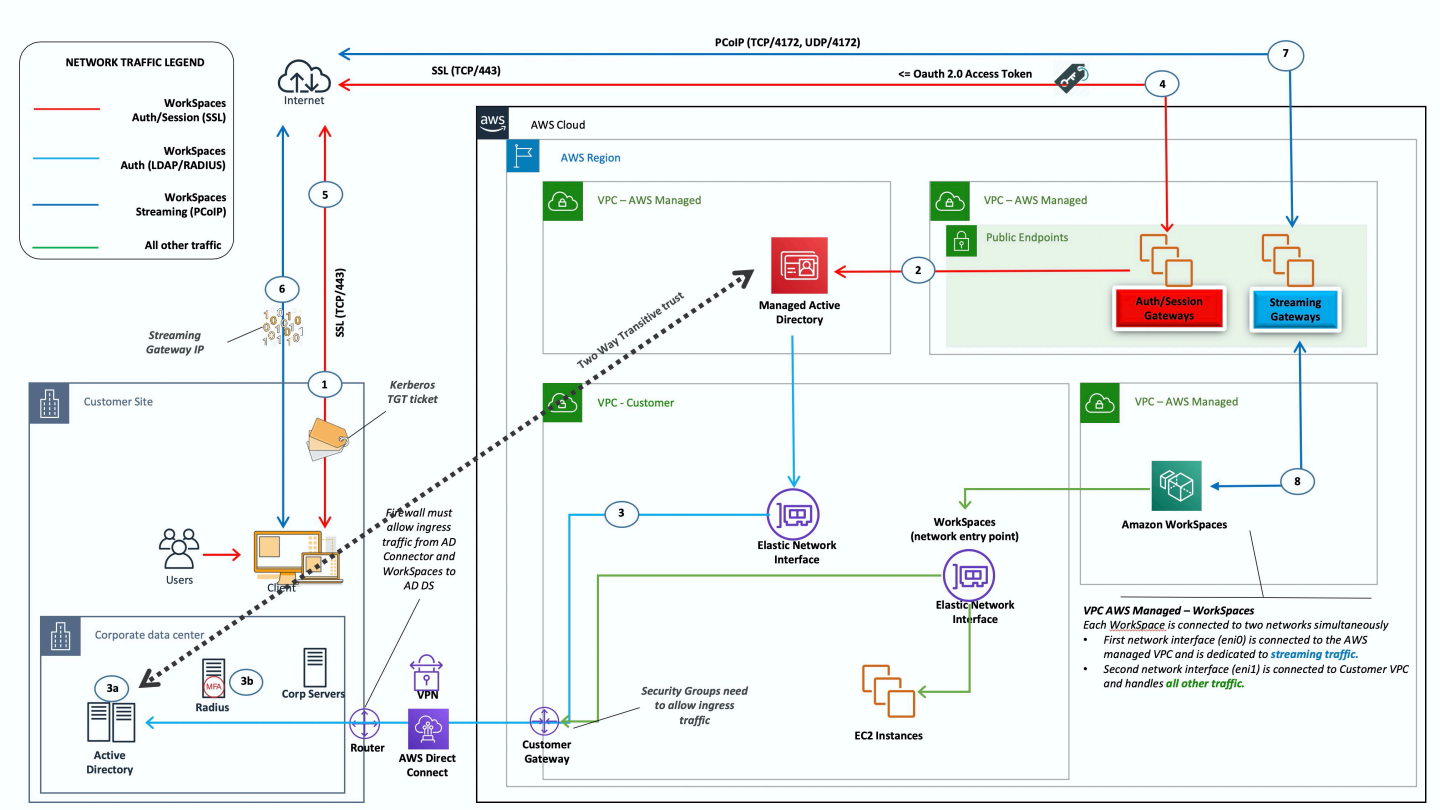

图 9： AWS Microsoft AD 和到本地的双向传递信任

与场景 3 一样，AD DS（Microsoft AD）部署到跨越两个可用区的专用子网中，这使得 AD DS 在云中具有很高的可用性。 AWS

此方案非常适合想要拥有完全托管的 AWS Directory Service（包括部署、修补、高可用性和 AWS 云监控）的客户。此场景还允许 WorkSpaces 用户在其现有网络上访问已加入广告的资源。这种情况需要建立域信任。安全组和防火墙规则需要允许两个活动目录之间的通信。

除了 AWS Directory Service 的位置外，上图还概述了从用户到工作空间的流量以及工作空间与 AD 服务器和 MFA 服务器的交互方式。

此架构使用以下组件或结构。

AWS

- 亚马逊 VPC — 创建一个亚马逊 VPC，在两个可用区中至少有四个私有子网——两个用于 AD DS M icrosoft AD，两个用于 AD Connector 或。 WorkSpaces
- DHCP 选项集 — 创建亚马逊 VPC DHCP 选项集。这使客户能够定义指定的域名和 DNS（Microsoft AD）。有关更多信息，请参阅 DHCP 选项集。
- 可选：Amazon 虚拟专用网关-允许通过 IPsec VPN 隧道 (VPN) 或 AWS Direct Connect 连接与客户拥有的网络进行通信。用于访问本地后端系统。
- AWS Directory Ser vice — 部署到一对专用 VPC 子网中的 Microsoft AD（AD DS 托管服务）。

- 亚马逊 EC2 — 客户可选 RADIUS 服务器，适用于 MFA。
- 亚马逊 WorkSpaces — 部署 WorkSpaces 在与 AD Connector 相同的私有子网中。有关更多信息，请参阅本文档的 “活动目录：网站和服务” 部分。

客户

- 网络连接-企业 VPN 或 AWS Direct Connect 端点。
- 最终用户设备 — 用于访问亚马逊服务的企业或自带终端用户设备（例如 Windows、Mac、iPad、安卓平板电脑、零客户端和 Chromebook）。 WorkSpaces 请参阅支持的设备和 Web 浏览器的客户端应用程序列表。

此解决方案需要连接到客户的本地数据中心，才能使信任流程正常运行。如果 WorkSpaces用户使用本地网络上的资源，则需要考虑延迟和出站数据传输成本。

场景 5： AWS 微软 AD 使用共享服务虚拟私有云 (VPC) Private Cloud

如下图所示，该场景在 AWS 云中部署了 AWS 托管 AD，为已经托管在更广泛的迁移中 AWS 或计划作为更广泛迁移的一部分的工作负载提供身份验证服务。最佳实践建议是将 Amazon 置 WorkSpaces 于专用 VPC 中。客户还应创建特定的 AD OU 来整理 WorkSpaces 计算机对象。

要 WorkSpaces 使用托管托管 AD 的共享服务 VPC 进行部署，请使用在托管 AD 中创建的 ADC 服务账户部署 AD Connector (ADC)。服务帐户需要权限才能在共享服务 Managed AD 的 WorkSpaces指定 OU 中创建计算机对象。

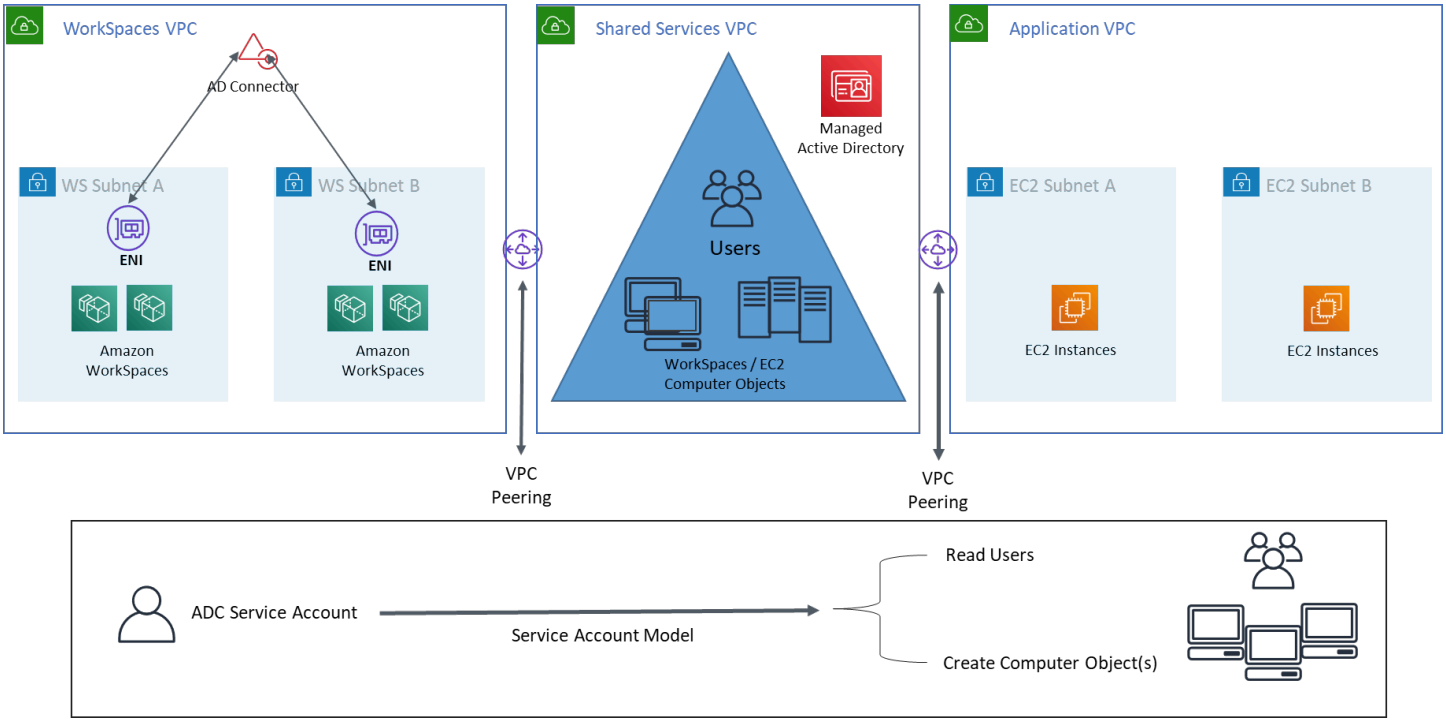

图 10：使用共享服务 VPC 的 AWS 微软 AD

此架构使用以下组件或结构。

AWS

- 亚马逊 VPC — 创建在两个可用区中至少有两个私有子网的亚马逊 VPC（两个用于 AD Connector 和 WorkSpaces）。
- DHCP 选项集 — 创建亚马逊 VPC DHCP 选项集。这允许客户定义指定的域名和 DNS（Microsoft AD）。有关更多信息，请参阅 DHCP 选项集。
- 可选：Amazon 虚拟专用网关-允许通过 IPsec VPN 隧道 (VPN) 或 AWS Direct Connect 连接与客户拥有的网络进行通信。用于访问本地后端系统。
- AWS Directory Ser vice — 部署到一对专用的 VPC 子网（AD DS 托管服务）、AD Connector 中的微软 AD
- AWS Transit Gateway/VPC 对等互连 — 启用工作空间 VPC 和共享服务 VPC 之间的连接
- 亚马逊 EC2 — 客户可选 RADIUS 服务器，适用于 MFA。

- 亚马逊 WorkSpaces — 部署 WorkSpaces 在与 AD Connector 相同的私有子网中。有关更多信息，请参阅本文档的 “活动目录：网站和服务” 部分。

客户

- 网络连接-企业 VPN 或 AWS Direct Connect 端点。
- 最终用户设备 — 用于访问亚马逊服务的企业或自带终端用户设备（例如 Windows、Mac、iPad、安卓平板电脑、零客户端和 Chromebook）。 WorkSpaces 请参阅支持的设备和 Web 浏览器的客户端应用程序列表。

场景 6： AWS Microsoft AD、共享服务 VPC 和对本地的单向信任

如下图所示，此场景使用现有的本地 Active Directory 供用户使用，并在 AWS 云中引入了一个单独的托管 Active Directory 来托管与关联的计算机对象 WorkSpaces。此方案允许计算机对象和 Active Directory 组策略独立于公司 Active Directory 进行管理。

当第三方想要代表客户管理 Windows WorkSpaces 时，此场景非常有用，因为它允许第三方定义和控制与其关联的 WorkSpaces 和策略，而无需向第三方授予对客户 AD 的访问权限。在这种情况下，将创建一个特定的 Active Directory 组织单位 (OU) 来组织共享服务 AD 中的 WorkSpaces 计算机对象。

> **Note**
>
> Amazon Linux WorkSpaces 需要建立双向信任才能创建它们。

要使用客户身份域中的用户在托管 Active Directory 的共享服务 VPC 中创建的计算机对象部署 Windows WorkSpaces ，请部署引用公司 AD 的 Active Directory 连接器 (ADC)。使用在企业 AD（身份域）中创建的 ADC 服务帐户，该帐户具有在共享服务托管 AD 中为 Windows 配置的组织单位 (OU) WorkSpaces 中创建计算机对象的委托权限，并且具有企业 Active Directory（身份域）的读取权限。

为确保域定位器功能能够对身份域所需 AD 站点中的 WorkSpaces 用户进行身份验证，请按照 Microsoft 的文档为两个域名的 Amazon WorkSpaces 子网的 Amazon Subnets 的广告站点命名。最佳做法是将身份域和共享服务域 AD 域控制器与 Amazon 位于同一 AWS 区域 WorkSpaces。

有关配置此场景的详细说明，请查看 WorkSpaces 使用 AWS 目录服务为 Amazon 设置单向信任的实施指南

在此场景中，我们在共享服务 VPC 和本 AWS Managed Microsoft AD 地 AD 之间建立单向传递信任。图 11 显示了信任和访问的方向，以及 AWS AD Connector 如何使用 AD Connector 服务帐户在资源域中创建计算机对象。

按照 Microsoft 的建议使用森林信任来确保尽可能使用 Kerberos 身份验证。您 WorkSpaces 将在中接收来自资源域的组策略对象 (GPO)。 AWS Managed Microsoft AD此外，您还可以使用您的身份域 WorkSpaces 执行 Kerberos 身份验证。为了使其可靠地运行，最佳做法是将您的身份域扩展到 AWS 如上所述。我们建议查看《WorkSpaces 使用单向信任资源域部署 Amazon AWS Directory Service》以及实施指南，了解更多详情。

AD Connector 和您的 WorkSpaces，都必须能够与您的身份域和资源域的域控制器通信。有关更多信息，请参阅《Amazon WorkSpaces 管理指南》 WorkSpaces中的 IP 地址和端口要求。

如果您使用多个 AD 连接器，则最好让每个 AD 连接器使用自己的 AD 连接器服务帐户。

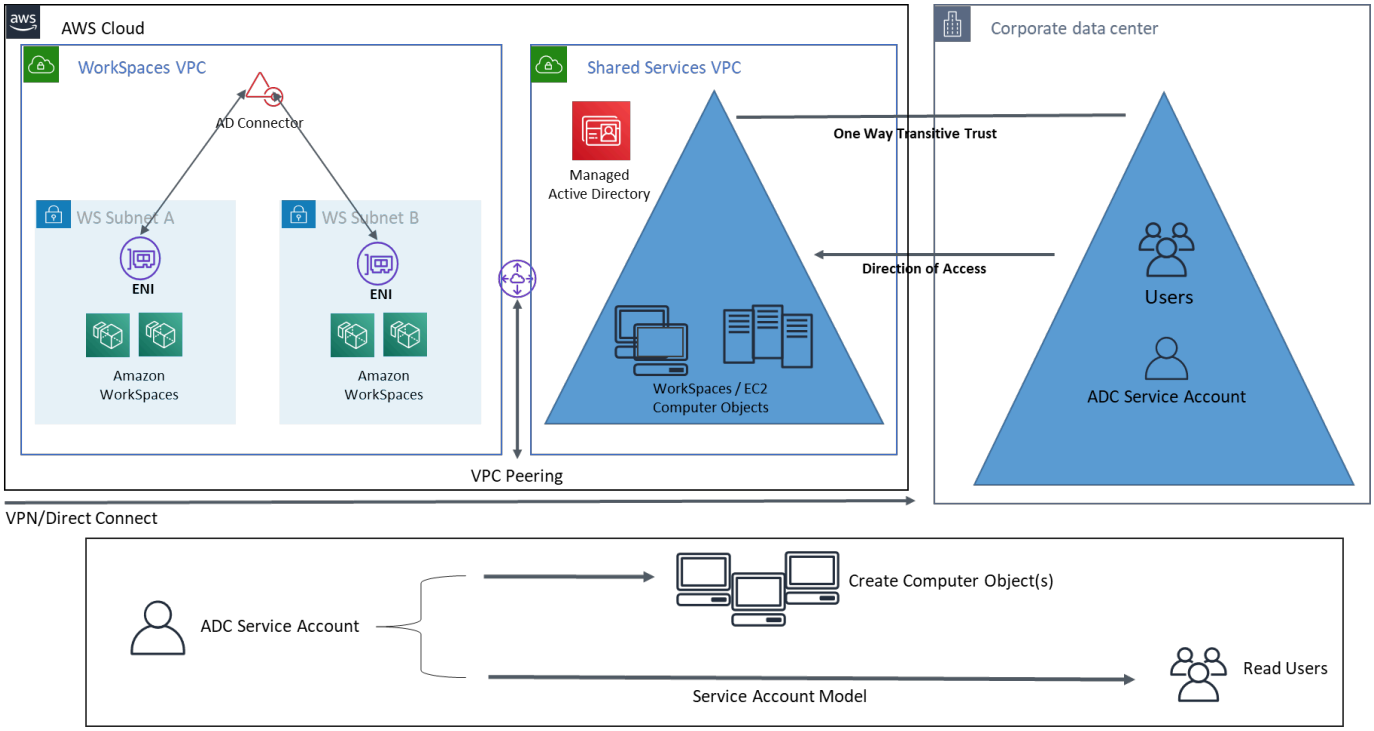

图 11： AWS 微软、共享服务 VPC 和对本地 AD 的单向信任

此架构使用以下组件或结构：

AWS

- 亚马逊 VPC — 创建一个亚马逊 VPC，其中至少有两个私有子网横跨两个可用区，其中两个用于 AD Connector 和。 WorkSpaces

- DHCP 选项集 — 创建亚马逊 VPC DHCP 选项集。这允许客户定义指定的域名和 DNS（Microsoft AD）。有关更多信息，请参阅 DHCP 选项集。
- 可选：Amazon 虚拟专用网关-允许通过 IPsec VPN 隧道 (VPN) 或 AWS Direct Connect 连接与客户拥有的网络进行通信。用于访问本地后端系统。
- AWS Directory Ser vice — 微软 AD 部署到一对专用的 VPC 子网（AD DS 托管服务），即 AD Connector。
- 传输网关/VPC 对等互连 — 启用工作空间 VPC 和共享服务 VPC 之间的连接。
- 亚马逊 EC2 — 适用于 MFA 的客户 “可选” RADIUS 服务器。
- 亚马逊 WorkSpaces — 部署 WorkSpaces 在与 AD Connector 相同的私有子网中。有关更多信息，请参阅本文档的 “活动目录：网站和服务” 部分。

客户

- 网络连接-企业 VPN 或 AWS Direct Connect 端点。
- 最终用户设备 — 用于访问亚马逊服务的企业或自带终端用户设备（例如 Windows、Mac、iPad、安卓平板电脑、零客户端和 Chromebook）。 WorkSpaces 有关支持的设备和 Web 浏览器，请参阅此客户端应用程序列表。

在 Amazon 上使用多区域 AWS 托管活动目录 WorkSpaces

AWS 微软目录服务 Active Directory (MAD) 是一个完全托管的微软 Active Directory (AD)，可以与亚马逊配对 WorkSpaces。客户之所以选择 AWS 托管 Microsoft AD，是因为它具有内置的高可用性、监控和备份功能。 AWS Microsoft AD Enterprise 托管版增加了配置多区域复制的功能。此功能可自动配置区域间网络连接、部署域控制器并在多个区域之间复制所有 Active Directory 数据，从而确保驻留在这些区域的 Windows 和 Linux 工作负载能够以低延迟和高性能连接和使用 AWS MAD。无法直接向注册复制的 MAD 区域 WorkSpaces，但是可以通过将 AD Connector (ADC) 配置为指向复制的域控制器来注册复制的 MAD 目录。 WorkSpaces

使用 MAD 部署 AD 连接器的最佳做法是为 WorkSpaces 环境中的每个业务部门创建一个 AD 连接器。这将允许您将每个业务部门与 Active Directory 中的特定组织单位保持一致。然后，您可以在组织单位级别分配与相关业务部门直接对应的 AD 组策略对象。

架构

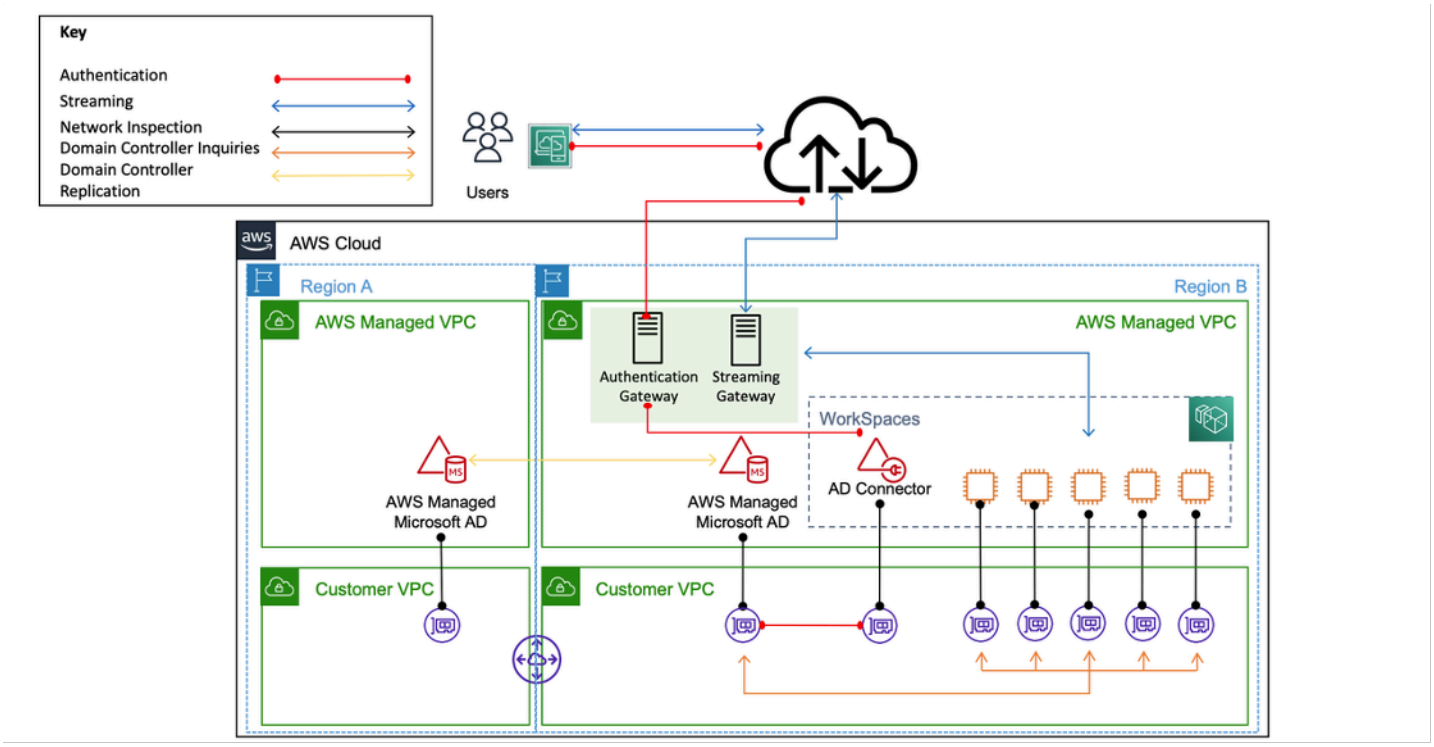

图 12：将复制的 MAD 区域注册到的示例架构 WorkSpace

实施

要将复制的 MAD 区域注册到 WorkSpaces，你需要创建一个指向你的 MAD 域控制器 IP 的 AD Connector。您可以前往 Directory S ervic AWS e 控制台导航窗格，选择“目录”，然后选择正确的目录 ID，找到您的 MAD 域控制器 IP 地址。要创建这些 AD 连接器，请遵循本指南。创建它们后，您可以注册它们 WorkSpaces。在新区域部署 WorkSpaces 之前，请确保已更新您的 VPC DHCP 选项集。

设计注意事项

在 AWS 云端部署功能性的 AD DS 需要充分了解 Active Directory 的概念和特定 AWS 服务。本节讨论部署适用于 Amazon 的 AD DS 时的关键设计注意事项 WorkSpaces、 AWS 目录服务的 VPC 最佳实践、DHCP 和 DNS 要求、AD Connector 细节以及 AD 站点和服务。

VPC 设计

正如先前在本文档的 “网络注意事项” 部分所讨论以及前面针对场景 2 和 3 所记录的那样，客户应将 AD DS 部署到一对专用的私有子网中，跨两个可用区，并与 AD AWS Connector 或 WorkSpaces 多个子网分开。这种结构提供了对 AD DS 服务的高可用性、低延迟访问 WorkSpaces，同时保持了 Amazon VPC 内角色或职能分离的标准最佳实践。

下图显示了 AD DS 和 AD Connector 分成专用私有子网的情况（方案 3）。在此示例中，所有服务都位于同一 Amazon VPC 中。

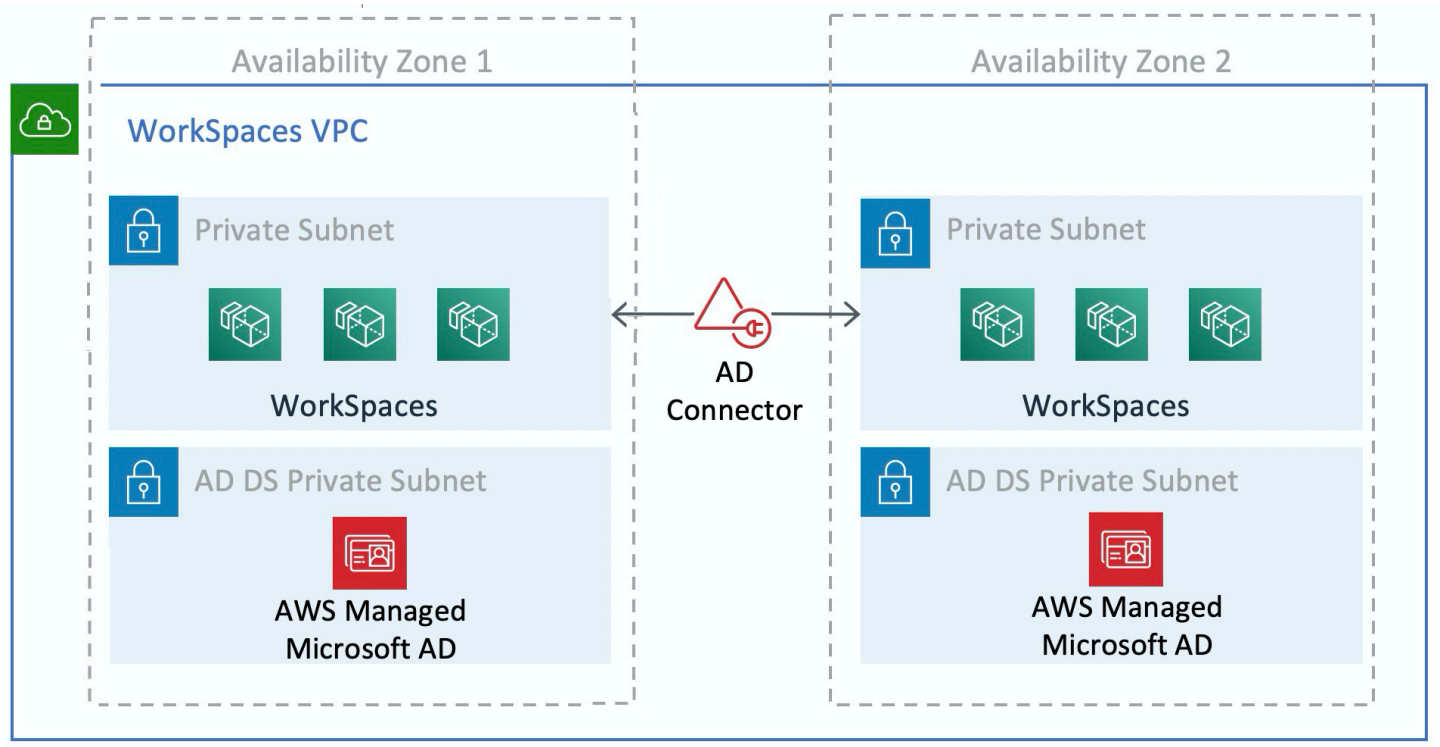

图 13：AD DS 网络分离

下图显示了与场景 1 相似的设计；但是，在这种情况下，本地部分位于专用 Amazon VPC 中。

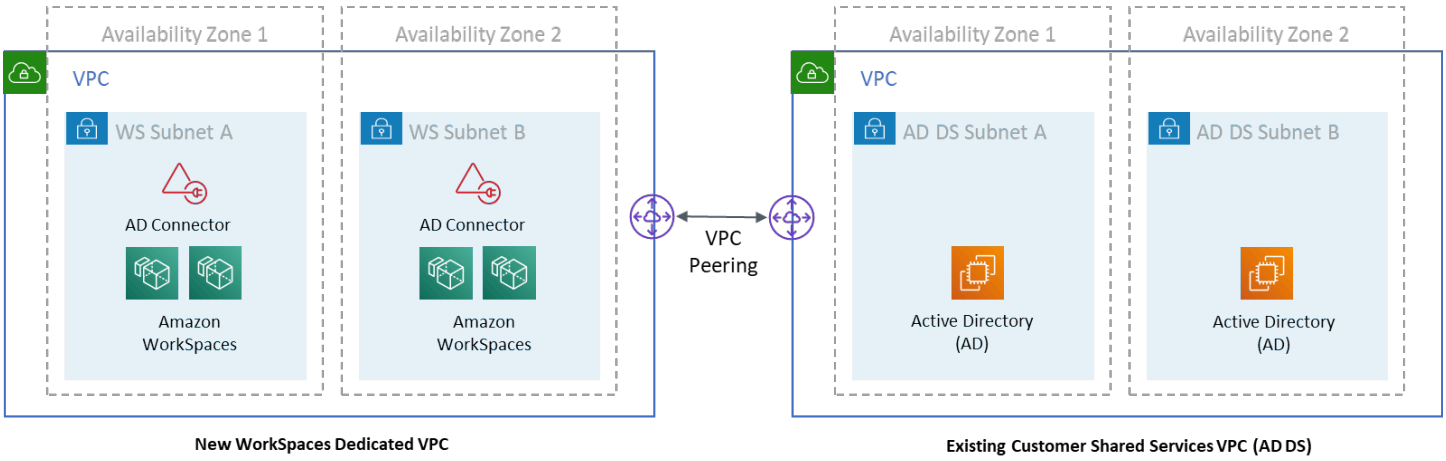

图 14：专用 WorkSpaces VPC

> **Note**
>
> 对于现有 AWS 部署中使用 AD DS 的客户，建议他们将其放置在专用 VPC WorkSpaces 中，并使用 VPC 对等连接进行 AD DS 通信。

除了为 AD DS 创建专用的私有子网外，域控制器和成员服务器还需要多个安全组规则来允许服务流量，例如 AD DS 复制、用户身份验证、Windows Time 服务和分布式文件系统 (DFS)。

> **Note**
>
> 最佳实践是将所需的安全组规则限制在 WorkSpaces私有子网上，在场景 2 中，允许在本地与 AWS 云之间进行双向 AD DS 通信，如下表所示。

表 1 — 往返云端的双向 AD DS 通信 AWS

协议	端口	使用	目标位置
TCP	53、88、135、139、389， 445、464、636	身份验证（主要）	活动目录（私有数据中心或 Amazon EC2）*

协议	端口	使用	目标位置
TCP	49152 — 65535	RPC 高端口	活动目录（私有数据中心或 Amazon EC2）**
TCP	3268-3269	信托	活动目录（私有数据中心或 Amazon EC2）*
TCP	9389	远程微软 Windows PowerShell （可选）	活动目录（私有数据中心或 Amazon EC2）*
UDP	53、88、123、137、138，389、445、464	身份验证（主要）	活动目录（私有数据中心或 Amazon EC2）*
UDP	1812	身份验证 (MFA)（可选）	RADIUS（私有数据中心或 Amazon EC2）*

有关更多信息，请参阅 Windows 的 A ctive Directory 和 Active Directory 域服务端口要求和服务概述以及网络端口要求

有关实施规则的 step-by-step 指南，请参阅 Amazon 弹性计算云用户指南中的向安全组添加规则。

VPC 设计：DHCP 和 DNS

在 Amazon VPC 中，默认情况下会为您的实例提供动态主机配置协议 (DHCP) 服务。默认情况下，每个 VPC 都提供一个内部域名系统 (DNS) 服务器，该服务器可通过无类域间路由 (CIDR) +2 地址空间进行访问，并通过默认 DHCP 选项集分配给所有实例。

在 Amazon VPC 中使用 DHCP 选项集来定义范围选项，例如应通过 DHCP 交给客户实例的域名或域名服务器。客户 VPC 中 Windows 服务的正确功能取决于此 DHCP 范围选项。在前面定义的每种场景中，客户都会创建和分配自己的作用域来定义域名和名称服务器。这样可以确保已加入域的 Windows 实例或配置 WorkSpaces 为使用 AD DNS。

下表是一组自定义 DHCP 范围选项的示例，必须创建这些选项才能让 Amazon WorkSpaces 和 AWS 目录服务正常运行。

表 2-自定义 DHCP 作用域选项集

参数	值
名称标签	创建一个 key = name 且值设置为特定字符串的标签 示例：example.com
域名	example.com
域名服务器	DNS 服务器地址，用逗号分隔 示例：192.0.2.10、192.0.2.21
NTP 服务器	将此字段留空
NetBIOS 名称服务器	输入与域名服务器相同的逗号分隔的 IP 示例：192.0.2.10、192.0.2.21
NetBIOS 节点类型	2

有关创建自定义 DHCP 选项集并将其与亚马逊 VPC 关联的详细信息，请参阅《亚马逊虚拟私有云用户指南》中的 “使用 DHCP 选项集”。

在场景 1 中，DHCP 范围将是本地 DNS 或 AD DS。但是，在方案 2 或 3 中，这将是本地部署的目录服务（亚马逊 EC2 上的 AD DS 或 AWS 目录服务：Microsoft AD）。建议将驻留在 AWS 云中的每个域控制器都设置为全局目录和集成目录的 DNS 服务器。

活动目录：网站和服务

对于场景 2，站点和服务是 AD DS 正常运行的关键组件。站点拓扑控制同一站点内域控制器之间以及跨站点边界的 AD 复制。在场景 2 中，至少存在两个站点：本地站点和云端的 Amazon WorkSpaces 站点。

定义正确的站点拓扑可确保客户端的亲和性，这意味着客户端（在本例中为 WorkSpaces）使用其首选的本地域控制器。

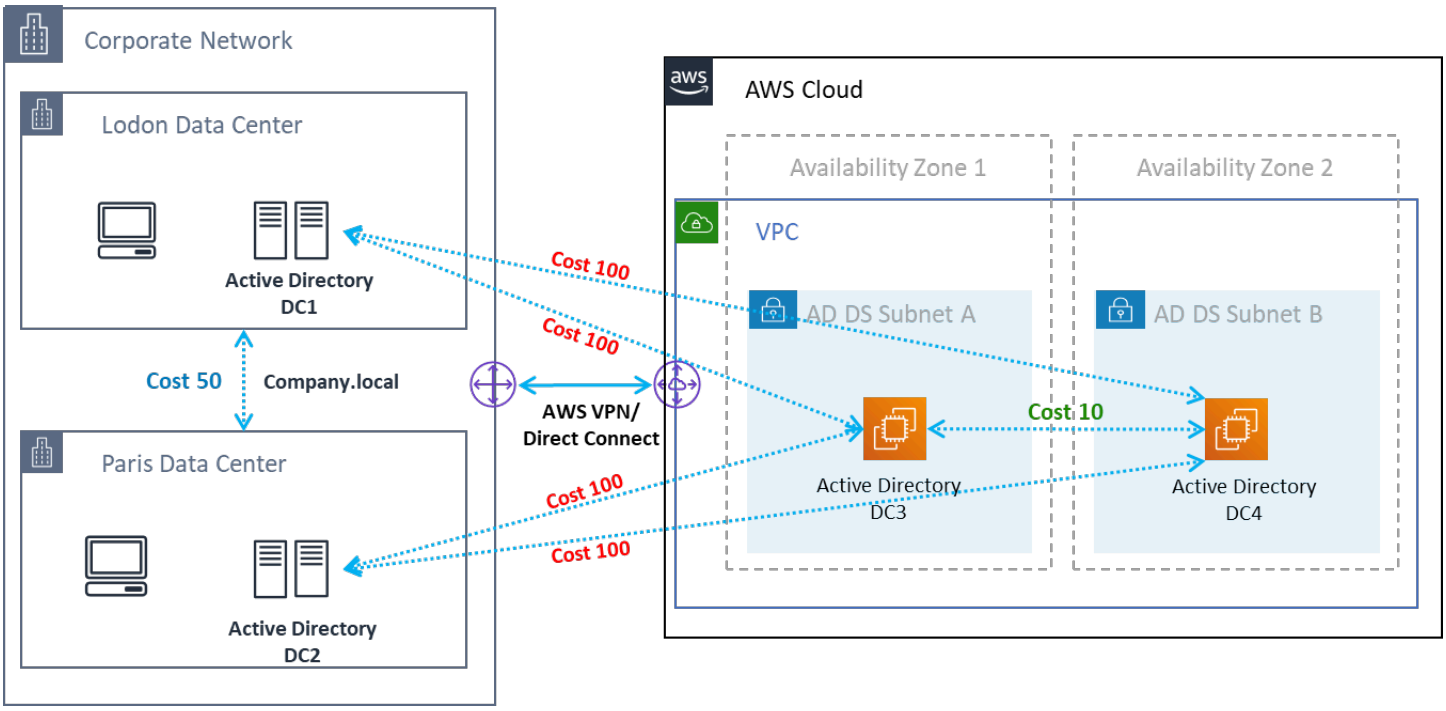

图 15：Active Directory 网站和服务：客户端亲和力

最佳实践：为本地 AD DS 和 AWS 云之间的站点链接定义高昂的成本。下图举例说明了为确保独立于站点的客户亲和力而分配给站点链接的成本（成本 100）。

这些关联有助于确保流量（例如 AD DS 复制和客户端身份验证）使用通往域控制器的最有效路径。对于场景 2 和 3，这有助于确保更低的延迟和交叉链接流量。

协议

Amazon WorkSpaces Streaming Protocol (WSP) 是一种云原生流媒体协议，可在全球距离和不可靠的网络上提供一致的用户体验。WSP WorkSpaces 通过卸载指标分析、编码、编解码器使用和选择来解耦协议。WSP 使用端口 TCP/UDP 4195。在决定是否使用 WSP 协议时，应在部署之前回答几个关键问题。请参阅下面的决策矩阵：

问题	WSP	PCoIP
已识别的 WorkSpaces 用户是否需要双向音频/视频？	•	

问题	WSP	PCoIP
是否会将零个客户端用作远程端点（本地设备）？		•
远程端点会使用 Windows 还是 macOS 吗？	•	•
Ubuntu 18.04 会用于远程端点吗？		•
用户是否会 WorkSpaces 通过网络访问亚马逊？		•
是否需要会前或会话期间的智能卡支持 (PIC/CAC)？	•	
WorkSpaces 将在中国（宁夏）区域使用吗？		•
是否需要智能卡预身份验证或会话中支持？	•	
最终用户使用的是不可靠、高延迟还是低带宽连接？	•	

前面的问题对于确定应使用的协议至关重要。有关推荐协议用例的更多信息，可在此处查看。以后也可以使用 Amazon M WorkSpaces igrate 功能更改所使用的协议。有关使用此功能的更多信息，请点击此处查看。

WorkSpaces 使用 WSP 部署时，应将 WSP 网关添加到允许列表中，以确保与服务的连接。此外，连接 WorkSpaces 使用 WSP 的用户，为了获得最佳性能，往返时间 (RTT) 应低于 250 毫秒。RTT 在 250 毫秒到 400 毫秒之间的连接将降级。如果用户的连接持续降级，建议尽可能 WorkSpaces 在离最终用户最近的服务支持区域部署 Amazon。

Multi-Factor Authentication (MFA)

实施MFA需要将Active Directory连接器（A WorkSpaces D Connector）或托管微 AWS 软 AD（MAD）配置为其目录服务，并具有目录服务可通过网络访问的RADIUS服务器。简单活动目录不支持 MFA。

请参阅上一节，其中涵盖了 AD 的 Active Directory 和目录服务部署注意事项，以及每种场景中的 RADIUS 设计选项。

MFA — 双因素身份验证

启用 MFA 后，用户需要向 WorkSpaces 客户端提供其用户名、密码和 MFA 代码，以便在各自的桌面上进行身份验证。 WorkSpaces

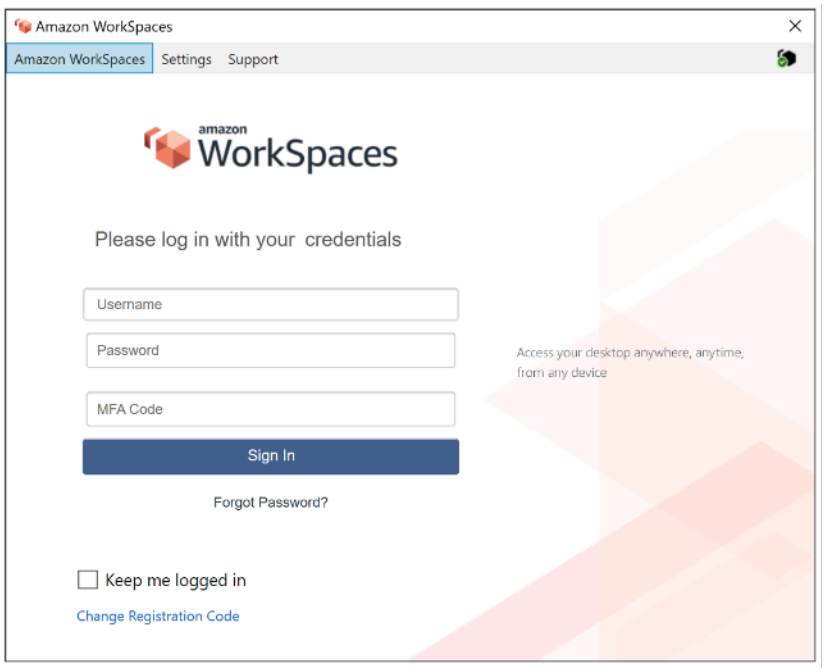

图 16：启用了 MFA 的 WorkSpaces 客户端

> **Note**
>
> Directory Servic AWS e 不支持按用户选择或上下文 MFA：这是每个目录的全局设置。如果需要选择性的 “每用户” MFA，则必须用 AD Connector 将用户隔开，该连接器可以指向同一个源 Active Directory。

WorkSpaces MFA 需要一台或多台 RADIUS 服务器。通常，这些是您可能已经部署的现有解决方案，例如 RSA 或 Gemalto。或者，可以在您的 VPC 内的 EC2 实例上部署 RADIUS 服务器（有关架构选项，请参阅本文档的 AD DS 部署场景部分）。如果你正在部署新的 RADIUS 解决方案，则有几种实现方案，例如 FreeRadius，还有 SaaS 产品，例如 Duo Secur ity 或 Okta MFA。

最佳做法是利用多台 RADIUS 服务器来确保您的解决方案能够抵御故障。在为 MFA 配置 Directory Service 时，你可以用逗号分隔多个 IP 地址（例如 192.0.0.0,192.0.0.12），从而输入多个 IP 地址。目录服务 MFA 功能将尝试使用指定的第一个 IP 地址，如果无法与第一个 IP 地址建立网络连接，则该功能将移至第二个 IP 地址。高可用架构的 RADIUS 配置对于每个解决方案集都是独一无二的，但总体建议是将 RADIUS 功能的底层实例放在不同的可用区域中。一个配置示例是 Duo Secur ity，对于 Okta MFA，你可以用相同的方式部署多个 Okta RADIUS 服务器代理。

有关启用 MFA AWS 目录服务的详细步骤，请参阅 AD Conn ector 和托管 M AWS icrosoft AD。

灾难恢复/业务连续性

WorkSpaces 跨区域重定向

Amazon WorkSpaces 是一项区域性服务，可为客户提供远程桌面访问权限。根据业务连续性和灾难恢复要求 (BC/DR)，一些客户需要无缝故障转移到另一个 WorkSpaces 提供服务的区域。这个 BC/DR 要求可以使用 WorkSpaces 跨区域重定向选项来实现。它允许客户使用完全限定的域名 (FQDN) 作为 WorkSpaces 注册码。

一个重要的考虑因素是确定应在何时重定向到故障转移区域。此决策的标准应基于贵公司的政策，但应包括恢复时间目标 (RTO) 和恢复点目标 (RPO)。Well-Architect WorkSpaces ed 架构设计应包括可能出现的服务故障。正常业务运营恢复的时间容忍度也将影响决策。

当您的最终用户使用 FQDN 作为 WorkSpaces 注册码登录时，将解析一个 DNS TXT 记录，其中包含用于确定用户将定向到的注册目录的连接标识符。 WorkSpaces 然后，将根据与返回的连接标识符关联的注册目录显示 WorkSpaces 客户端的登录登录页面。这允许管理员根据您的 FQDN 的 DNS 策略将其最终用户定向到不同的 WorkSpaces目录。假设私有区域可以从客户端计算机解析，则此选项可用于公共或私有 DNS 区域。跨区域重定向可以是手动的，也可以是自动的。这两种故障转移都可以通过将包含连接标识符的 TXT 记录更改为指向所需目录来实现。

在制定 BC/DR 策略时，务必考虑用户数据，因为 WorkSpaces 跨区域重定向选项不会同步任何用户数据，也不会同步您的图像。 WorkSpaces 您在不同 AWS 区域的 WorkSpaces 部署是独立的实体。因此，您必须采取其他措施来确保您的 WorkSpaces 用户在重定向到次要区域时可以访问他们的数据。有许多选项可用于用户数据复制 WorkSpaces，例如 Windows FSx（DFS 共享）或用于在区域之间同

步数据卷的第三方实用程序。同样，您必须确保您的次要区域可以访问所需的 WorkSpaces 图像，例如，通过跨区域复制图像。有关更多信息，请参阅《亚马逊 WorkSpaces 管理指南》 WorkSpaces中的 Amazon 跨区域重定向以及图表中的示例。

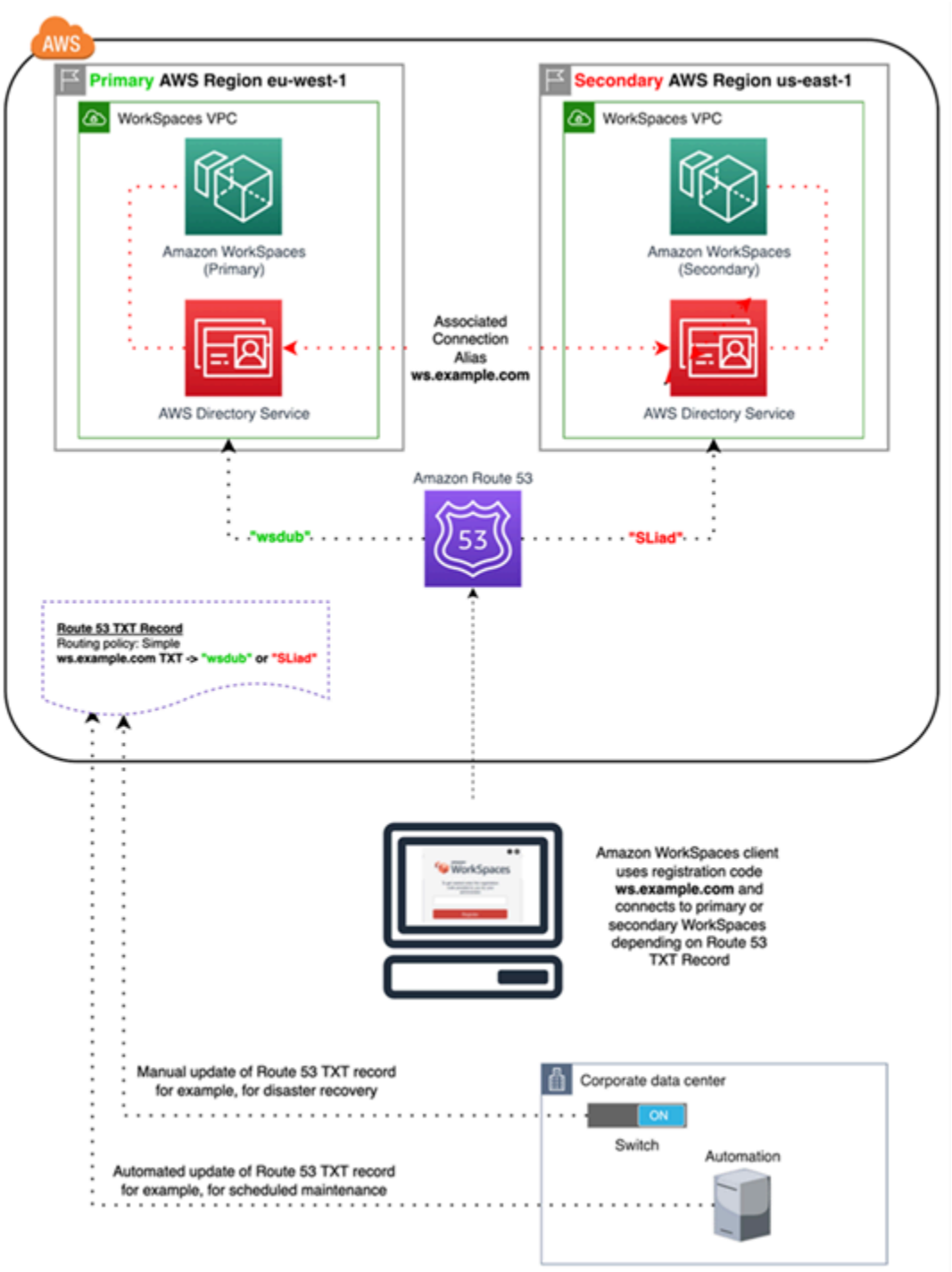

图 17：使用 Amazon Route 53 的 WorkSpaces 跨区域重定向示例

WorkSpaces 接口 VPC 终端节点 (AWS PrivateLink) — API 调用

支持@@ 亚马逊 WorkSpaces 公共 API AWS PrivateLink。 AWS PrivateLink 通过减少公共互联网上的数据暴露，提高与基于云的应用程序共享的数据的安全性。 WorkSpaces 可以使用接口终端节点保护 VPC 内的 API 流量，接口终端节点是一个弹性网络接口，其私有 IP 地址来自您的子网 IP 地址范围，可用作发往受支持服务的流量的入口点。这使您能够使用私有 IP 地址私密访问 WorkSpaces API 服务。

PrivateLink 与 WorkSpaces 公共 API 配合使用还使您能够安全地将 REST API 仅向您的 VPC 内的资源公开，或者通过安全地向与您的数据中心相连的资源公开 REST API AWS Direct Connect。

您可以限制对选定的 Amazon VPC 和 VPC 终端节点的访问，并使用特定于资源的策略启用跨账户访问。

确保与终端节点网络接口关联的安全组允许终端节点网络接口与您的 VPC 中与服务通信的资源之间进行通信。如果安全组限制来自 VPC 中资源的入站 HTTPS 流量（端口 443），则您可能无法通过终端节点网络接口发送流量。接口终端节点仅支持 TCP 流量。

- 终端节点仅支持 IPv4 流量。
- 在创建终端节点时，您可为其连接终端节点策略来控制对连接到的服务的访问。
- 您可以为每个 VPC 创建的终端节点的数量有配额。
- 仅在同一区域内支持终端节点。您无法在 VPC 与其他区域的服务之间创建终端节点。

创建通知以接收有关接口终端节点事件的警报-您可以创建通知以接收接口终端节点上发生的特定事件的警报。要创建通知，您必须将 Amazon SNS 主题与通知关联。您可以订阅 SNS 主题以在终端节点事件发生时收到电子邮件通知。

为亚马逊创建 VPC 终端节点策略 WorkSpaces — 您可以为亚马逊的 Amazon VPC 终端节点创建策略 WorkSpaces 以指定以下内容：

- 可执行操作的主体。
- 可执行的操作。
- 可对其执行操作的资源。

将您的私有网络连接到您的 VPC — 要通过您的 VPC 调用 Amazon WorkSpaces API，您必须从 VPC 内的实例进行连接，或者使用亚马逊虚拟专用网络 (VPN) 将您的私有网络连接到您的 VPC 或 AWS

Direct Connect。有关亚马逊 VPN 的信息，请参阅《亚马逊虚拟私有云用户指南》中的 VPN 连接。有关信息 AWS Direct Connect，请参阅《AWS Direct Connect 用户指南》中的创建连接。

有关通过 VPC 接口终端节点使用 Amazon WorkSpaces API 的更多信息，请参阅亚马逊的基础设施安全 WorkSpaces。

智能卡支持

微软 Windows 和亚马逊 Linux 均支持智能卡 WorkSpaces。通过通用访问卡 (CAC) 和个人身份验证 (PIV) 提供的智能卡支持只能通过亚马逊 WorkSpaces 使用 WorkSpaces 流媒体协议 (WSP) 获得。WSP 上的智能卡支持 WorkSpaces 提供了更高的安全性，可以对组织批准的连接端点上的用户进行身份验证，这些终端以智能卡读卡器为形式的特定硬件。首先要熟悉智能卡可用的支持范围，并确定智能卡在现有和未来的 WorkSpaces 部署中将如何发挥作用，这一点很重要。

最佳做法是确定需要哪种类型的智能卡支持，即会话前身份验证还是会话中身份验证。会前身份验证仅在撰写本文时提供 AWS GovCloud （美国西部）、美国东部（弗吉尼亚北部）、美国西部（俄勒冈）、欧洲（爱尔兰）、亚太地区（东京）和亚太地区（悉尼）。会话中智能卡身份验证通常需要考虑一些注意事项，例如：

- 您的组织是否拥有与 Windows Active Directory 集成的智能卡基础架构？
- 您的在线证书状态协议 (OCSP) 响应器是否可以访问公共互联网？
- 用户证书的使用者备用名称 (SAN) 字段中是否带有用户主体名称 (UPN)？
- 会期和会前部分详细介绍了更多注意事项。

智能卡支持是通过组策略启用的。最佳做法是将 WSP 的亚马逊 WorkSpaces 组策略管理模板添加到亚马逊 WorkSpaces 目录使用的活动目录域的中央存储区。 WorkSpaces 将此策略应用于现有的 Amazon WorkSpaces 部署时，所有人都需要更新组策略并重启才能使更改对所有用户生效，因为这是一项基于计算机的策略。

根 CA

由于亚马逊 WorkSpaces 客户端和用户的可移植性，需要将第三方根 CA 证书远程传送到用户用来连接其亚马逊的每台设备的受信任根证书存储区。 WorkSpacesAD 域控制器和带有智能卡的用户设备必须信任根 CA。有关确切要求的更多信息，请查看 Microsoft 提供的启用第三方 CA 的指南。

在已加入 AD 域的环境中，这些设备通过分发根 CA 证书的组策略来满足此要求。在 non-domain-joined 设备上使用 Amazon C WorkSpaces lient 的场景中，必须确定第三方根 CA 的替代交付方式，例如 Intune。

会话中

会话内身份验证可简化并保护 Amazon WorkSpaces 用户会话启动后的应用程序身份验证。如前所述，Amazon 的默认行为 WorkSpaces 会禁用智能卡，并且必须通过组策略启用。从 Amazon WorkSpaces 管理的角度来看，通过身份验证的应用程序（例如 Web 浏览器）特别需要进行配置。无需对 AD 连接器和目录进行任何更改。

大多数需要会话内身份验证支持的常见应用程序是通过网络浏览器，例如Mozilla Firefox和Google Chrome浏览器。Mozilla Firefox 需要有限的配置才能支持会话中的智能卡。亚马逊 Linux WSP WorkSpaces 需要额外的配置才能支持 Mozilla Firefox 和谷歌浏览器的会话中智能卡。

由于 Amazon C WorkSpaces lient 可能没有访问本地计算机的权限，因此在进行故障排除之前，最好确保根 CA 已加载到用户的个人证书存储中。此外，在对任何可疑的智能卡会话中身份验证问题进行故障排除时，请使用 OpenSC 识别智能卡设备。最后，建议使用在线证书状态协议 (OCSP) 响应器，通过证书吊销检查来改善应用程序身份验证的安全状况。

会前

支持会话前身份验证需要 Windows WorkSpaces Client 版本 3.1.1 及更高版本，或 macOS WorkSpaces 客户端版本 3.1.5 及更高版本。使用智能卡进行的会话前身份验证与标准身份验证有根本的不同，标准身份验证要求用户通过插入智能卡和输入 PIN 码的组合进行身份验证。使用这种身份验证类型，用户会话的持续时间受 Kerberos 票证的生命周期限制。完整的安装指南可以在这里找到。

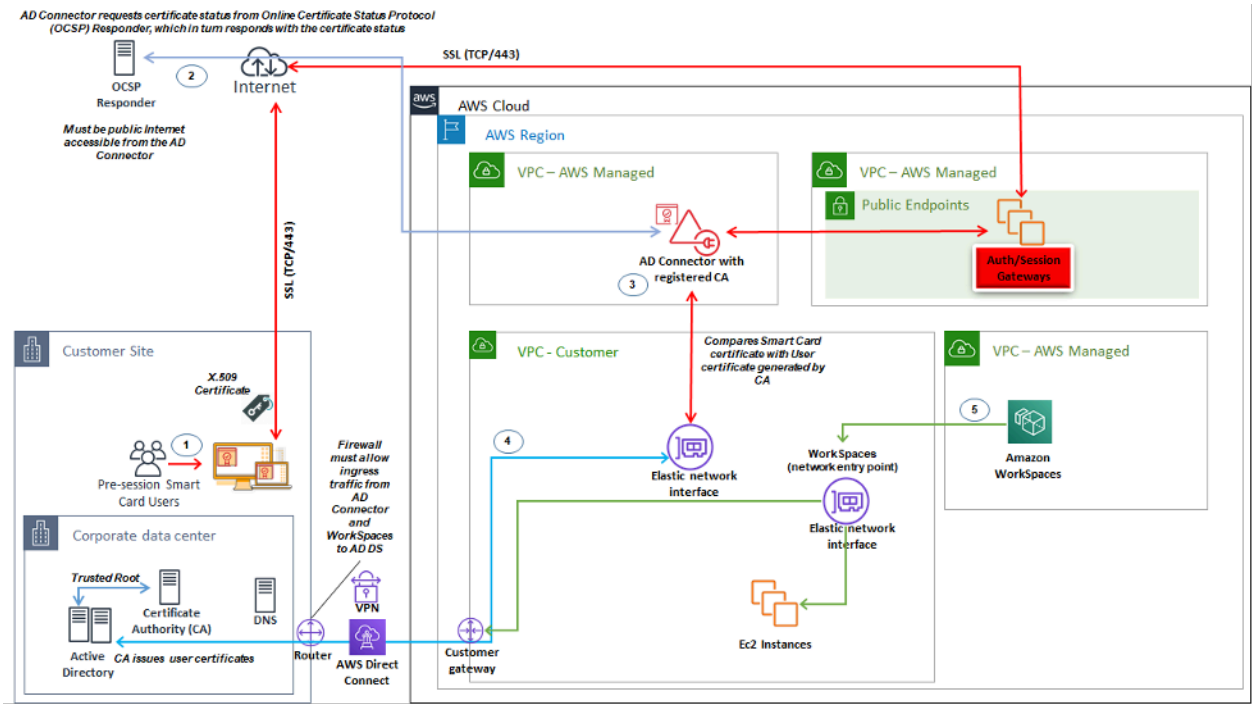

图 18：会话前身份验证概述

1. 用户打开 Amazon WorkSpaces 客户端，插入智能卡，然后输入其 PIN。Amazon C WorkSpaces lient 使用 PIN 来解密 X.509 证书，该证书是通过身份验证网关连接到 AD Connector 的代理。
2. AD Connector 会根据目录设置中指定的可公开访问的 OCSP 响应器 URL 验证 X.509 证书，以确保该证书未被吊销。
3. 如果证书有效，Amazon C WorkSpaces lient 会通过提示用户再次输入 PIN 来解密 X.509 证书和代理到 AD Connector，然后在 AD Connector 中将其与 AD Connector 的根证书和中间证书进行匹配以进行验证，从而继续身份验证过程。
4. 成功匹配证书验证后，AD Connector 将使用 Active Directory 对用户进行身份验证，并创建 Kerberos 票证。
5. Kerberos 票证将传递给用户的 Amazon WorkSpace 以进行身份验证并开始 WSP 会话。

OCSP Responder 必须可公开访问，因为连接是通过 AWS 托管网络而不是客户管理的网络进行的，因此此步骤中没有指向专用网络的路由。

不需要输入用户名，因为向 AD Connector 提供的用户证书在证书的 userPrincipalName (SAN) 字段中包含用户的 subjectAltName (UPN)。最佳做法是让所有需要使用智能卡进行会话前身份验证的用户自动更新其 AD 用户对象，以使用证书中的预期 UPN 进行身份验证 PowerShell，而不是在 Microsoft 管理控制台中单独执行此操作。

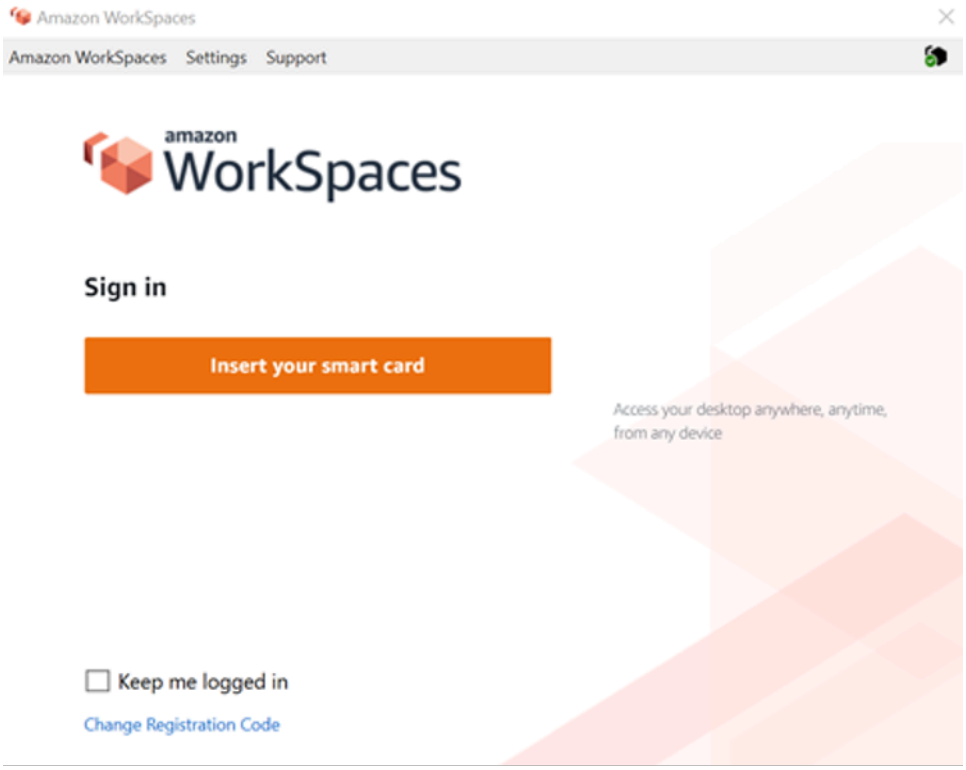

图 19： WorkSpaces 登录控制台

客户端部署

Amazon WorkSpaces Client（版本 3.X+）使用标准化配置文件，管理员可以利用这些文件来预配置其用户的客户端。 WorkSpaces 两个主要配置文件的路径可在以下网址找到：

OS	配置文件路径
Windows	C:\Users\USERNAME\\ LocalAppData\ Amazon Web Services\ Amazon WorkSpaces
macOS	/users/用户名/Library/应用程序支持/亚马逊网络服务/亚马逊 WorkSpaces
Linux (Ubuntu 18.04)	/HOME/ubuntu/.local/share/亚马逊网络服务/亚马逊/ WorkSpaces

在这些路径中，您将找到两个配置文件。第一个配置文件是 UserSettings .json，它将设置诸如当前注册、代理配置、日志级别和保存注册列表的功能之类的内容。第二个配置文件是 RegistrationList .json。此文件将包含所有 WorkSpaces 目录信息，供客户端用来映射到正确的 WorkSpaces 目录。预配置 RegistrationList .json 将在客户端中为用户填充所有注册码。

> **Note**
>
> 如果您的用户运行的是 WorkSpaces 客户端版本 2.5.11，则 proxy.cfg 将用于客户端代理设置，client_settings.ini 将设置日志级别以及保存注册列表的功能。默认代理设置将使用操作系统中设置的内容。

由于这些文件是标准化的，因此管理员可以下载WorkSpaces 客户端，设置所有适用的设置，然后将相同的配置文件推送给所有最终用户。要使设置生效，必须在设置新配置后启动客户端。如果在客户端运行时更改配置，则不会在客户端内设置任何更改。

可以为 WorkSpaces 用户设置的最后一个设置是 Windows 客户端自动更新。这不是通过配置文件控制的，而是通过Windows注册表来控制的。当客户端出现新版本时，您可以创建一个注册表项来跳过该版本。这可以通过在以下路径中创建一个字符串注册表项名称 SkipThisVersion 来设置，

其值为完整版本号：计算机\ HKEY_CURRENT_USER\ Software\ Amazon Web Services。LLC WorkSpaces\ Amazon\ WinSparkle 此选项也适用于 macOS；但是，配置位于需要特殊软件才能编辑的 plist 文件中。如果您仍然想执行此操作，可以通过在 com.amazon.workspaces 域中添加一个 SU SkippedVersion 条目来完成，该域名位于：/users/username/Library/Preferences

亚马逊 WorkSpaces 终端节点选择

为您选择终端节点 WorkSpaces

亚马逊 WorkSpaces 为多种终端设备提供支持，从 Windows 台式机到 iPad 和 Chromebook。您可以从 Amazon Workspaces 网站下载可用的亚马逊 WorkSpaces 客户端。为用户选择正确的端点是一个重要的决定。如果您的用户需要使用双向音频/视频，并且将使用 WorkSpaces流媒体协议，则他们必须使用 Windows 或 macOS 客户端。对于所有客户端，请确保 WorkSpaces已明确配置 Amazon 的 IP 地址和端口要求中列出的 IP 地址和端口，以确保客户端可以连接到服务。以下是一些其他注意事项，可帮助您选择终端设备：

- Windows — 要使用 Windows 亚马逊 WorkSpaces 客户端，4.x 客户端必须运行所需的 64 位微软 Windows 8.1、Windows 10 桌面。用户可以仅为其用户配置文件安装客户端，而无需在本地计算机上拥有管理权限。系统管理员可以使用组策略、Microsoft Endpoint Manager 配置管理器 (MEMCM) 或环境中使用的其他应用程序部署工具将客户端部署到托管端点。Windows 客户端最多支持四台显示器，最大分辨率为 3840x2160。
- macOS — 要部署最新的 macOS 亚马逊客户端 WorkSpaces ，macOS 设备必须运行 macOS 10.12（Sierra）或更高版本。如果终端运行的是 OSX 10.8.1 或更高版本， WorkSpaces 则可以部署较旧版本的 WorkSpaces 客户端来连接到 PCoIP。macOS 客户端最多支持两台 4K 分辨率的显示器或四台 WUXGA (1920 x 1200) 分辨率的显示器。
- Linux — 亚马逊 WorkSpaces Linux 客户端需要 64 位 Ubuntu 18.04 (AMD64) 才能运行。如果您的 Linux 终端节点不运行此操作系统版本，则不支持 Linux 客户端。在部署 Linux 客户机或向用户提供其注册码之前，请确保在 WorkSpaces 目录级别启用 Linux 客户端访问权限，因为默认情况下，该功能处于禁用状态，用户在启用 Linux 客户端之前将无法从 Linux 客户端进行连接。Linux 客户端最多支持两台 4K 分辨率的显示器或四台 WUXGA（1920 x 1200）分辨率的显示器。
- iPad — 亚马逊 WorkSpaces iPad 客户端应用程序支持 PCoIP WorkSpaces。支持的 iPad 是搭载 iOS 8.0 或更高版本的 iPad2 或更高版本、搭载 iOS 8.0 及更高版本的 iPad Retina、搭载 iOS 8.0 及更高版本的 iPad Mini 以及搭载 iOS 9.0 及更高版本的 iPad Pro。确保用户连接的设备符合这些标准。iPad 客户端应用程序支持许多不同的手势。（请参阅支持的手势的完整列表。）亚马逊 WorkSpaces iPad 客户端应用程序还支持 Swiftpoint GT 和 ProPoint鼠标。 PadPoint 不支持 Swiftpoint TRACPOINT PenPoint 和 GoPoint 鼠标。

- Android/Chromebook — 在考虑部署安卓设备或 Chromebook 作为最终用户的终端节点时，必须考虑一些注意事项。确保将要连接 WorkSpaces 的用户是 PCoIP WorkSpaces，因为此客户端仅支持 PCoIP。 WorkSpaces此客户端仅支持单个显示器。如果用户需要多显示器支持，请使用其他端点。如果您要部署 Chromebook，请确保您部署的机型支持安装安卓应用程序。只有安卓客户端支持全部功能，而旧版 Chromebook 客户端不支持。对于2019年之前生产的Chromebook，这通常只是一个考虑因素。只要安卓运行操作系统 4.4 及更高版本，平板电脑和手机都支持安卓。但是，建议安卓设备运行操作系统 9 或更高版本才能使用最新的 WorkSpace Android 客户端。如果您的 Chromebook 运行的是 WorkSpaces 客户端版本 3.0.1 或更高版本，那么您的用户现在可以利用自助服务功能。WorkSpaces 此外，作为管理员，您可以利用可信设备证书限制对具有有效证书的可信设备的 WorkSpaces 访问。
- 网络访问-用户可以使用网络浏览器 WorkSpaces 从任何位置访问其Windows。对于必须使用锁定设备或限制性网络的用户，这是一种理想选择。除了使用传统的远程访问解决方案和安装相应的客户端应用程序，用户还可以访问此网站来访问其工作资源。用户可以利用 WorkSpaces Web Acces non-graphics-based s 连接到 WorkSpaces 运行 Windows 10 的 Windows PCoIP 或带有桌面体验的 Windows Server 2016。用户必须使用 Chrome 53 或更高版本或 Firefox 49 或更高版本进行连接。对于基于 WSP WorkSpaces，用户可以利用 WorkSpaces Web Access 连接到基于 Windows 的非显卡。 WorkSpaces这些用户必须使用微软 Edge 91 或更高版本或谷歌 Chrome 91 或更高版本进行连接。支持的最低屏幕分辨率为 960 x 720，支持的最大分辨率为 2560 x 1600。不支持多个显示器。为了获得最佳用户体验，建议用户尽可能使用操作系统版本的客户端。
- PCoIP 零客户端 — 您可以将 PCoIP 零客户机部署给已分配或将要分配 PC WorkSpaces oIP 的最终用户。Tera2 零客户端的固件版本必须为 6.0.0 或更高版本才能直接连接到。 WorkSpace要在亚马逊上使用多重身份验证 WorkSpaces，Tera2 零客户端设备必须运行固件版本 6.0.0 或更高版本。零客户机硬件的 Support 和故障排除应与制造商联系。
- IGEL OS — WorkSpaces 只要固件版本为 11.04.280 或更高版本，你就可以在端点设备上使用 IGEL 操作系统连接到基于 PCoIP 的设备。支持的功能与当今现有 Linux 客户端的功能相匹配。在部署 IGEL OS 客户端或向用户提供注册码之前，请确保在 WorkSpaces 目录级别启用 Linux 客户端访问权限，因为默认情况下，该功能处于禁用状态，并且在启用 IGEL OS 客户端之前，用户将无法从 IGEL OS 客户端进行连接。LGel OS 客户端最多支持两台 4K 分辨率的显示器或四台 WUXGA (1920x1200) 分辨率的显示器。

Web 访问客户端

Web Access 客户端专为锁定设备而设计， WorkSpaces 无需部署客户端软件即可访问亚马逊。仅在亚马逊是 Windows 操作系统 (OS) WorkSpaces 且用于有限用户工作流程（例如自助服务终端环境）的环境中才建议使用 Web Access 客户端。大多数用例都受益于 Amazon WorkSpaces 客户端提供的功能集。仅在设备和网络限制需要其他连接方法的特定用例中才建议使用 Web Access 客户端。

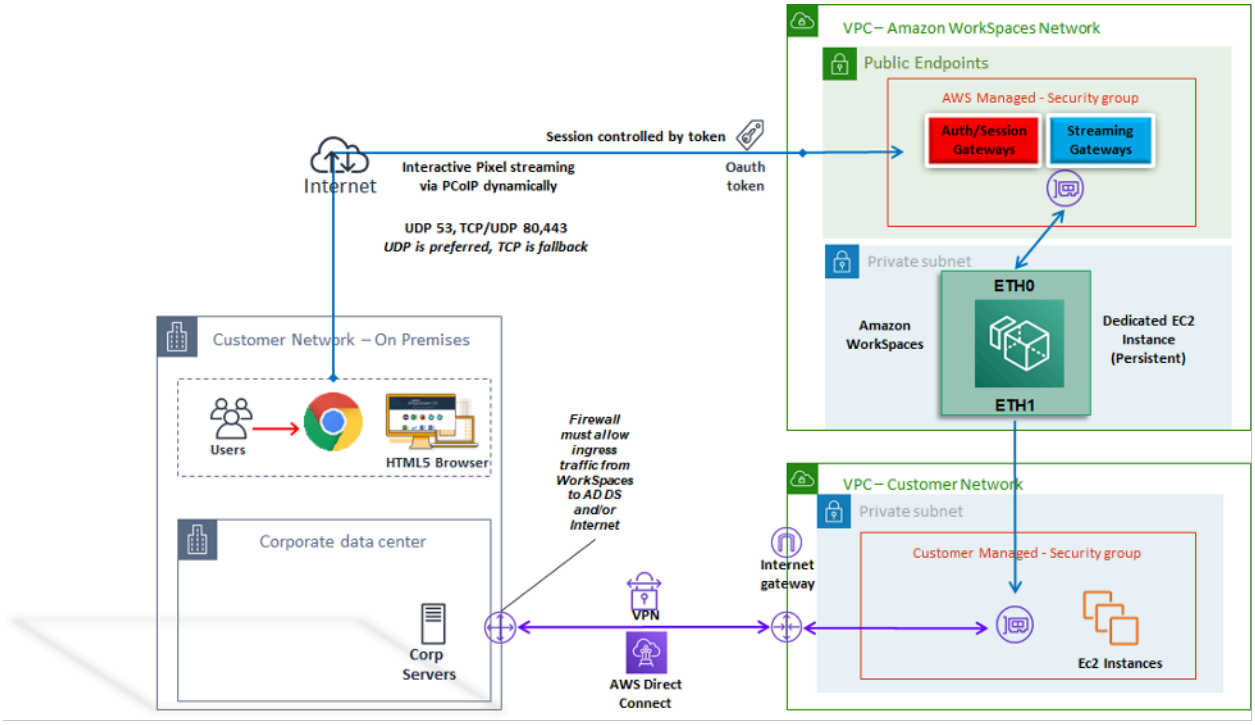

图 20：Web 访问客户端架构

如图所示，Web Access 客户端在将会话流式传输给用户时具有不同的网络要求。使用 PCoIP 或 WSP 协议的 Windows 可以 WorkSpaces 使用 Web Access。在网关上进行身份验证和注册需要使用 DNS 和 HTTP/HTTPS。 WorkSpaces 要 WorkSpaces 使用 WSP 协议，需要打开 UDP/TCP 4195 与 WSP 网关 IP 地址范围的直接连接。流媒体流量不会像完整版 Amazon WorkSpaces 客户端那样分配到固定端口；而是动态分配。UDP 更适合流式传输流量；但是，当 UDP 受到限制时，Web 浏览器将回退到 TCP。在 TCP/UDP 端口 4172 被屏蔽且由于组织限制而无法解除封锁的环境中，Web Access 客户端为用户提供了另一种连接方法。

默认情况下，Web Access 客户端在目录级别处于禁用状态。要使用户能够 WorkSpaces 通过网络浏览器访问他们的 Amazon，请使用更新目录设置，或者以编程方式使用 WorkspaceAccessProperties API 修改 DeviceTypeWeb 为 “允许”。 AWS Management Console 此外，管理员必须确保组策略设置不与登录要求冲突。

亚马逊 WorkSpaces 标签

```
Tags enable you to associate metadata with AWS resources. Tags can be used with Amazon
 WorkSpaces to registered directories,
  bundles, IP Access Control Groups, or images. Tags assist with cost allocation to
 internal cost centers. Before using tags with Amazon WorkSpaces,
  refer to the Tagging Best Practices whitepaper.
```

```
Tag restrictions
```

- 每个资源的标签数上限 – 50
- 最大密钥长度 - 127 个 Unicode 字符
- 最大值长度 - 255 个 Unicode 字符
- 标签键和值区分大小写。允许使用的字符包括可用 UTF-8 格式表示的字母、空格和数字，以及以下特殊字符： + - = 。_ : / @。请不要使用前导空格或尾随空格。
- 请勿在标签名称或值中使用 aws: 或 aws: workspaces: 前缀，因为它们已保留供使用。 AWS 您无法编辑或删除带这些前缀的标签名称或值。

你可以标记的资源

- 您可以在创建以下资源时为其添加标签： WorkSpaces、导入的映像和 IP 访问控制组。
- 您可以为以下类型的现有资源添加标签： WorkSpaces、注册目录、自定义捆绑包、映像和 IP 访问控制组。

使用成本分配标签

要在 Cost Explorer 中查看您的 WorkSpaces WorkSpaces资源标签，请按照 AWS Billing and Cost Management 和成本管理用户指南中激活用户定义的成本分配标签中的说明激活已应用于资源的标签。

尽管标签会在激活 24 小时后出现，但与这些标签关联的值可能需要四到五天才能显示在 Cost Explorer 中，要在 Cost Explorer 中显示并提供成本数据，已标记的 WorkSpaces 资源必须在这段时间内产生费用。Cost Explorer 仅显示从标签激活之时起的成本数据。目前没有可用的历史数据。

管理标签

要使用更新现有资源的标签，请使用 create-tags 和 delet e-tags 命令。 AWS CLI为了实现批量更新和在大量 WorkSpaces 资源上自动执行任务，Amazon WorkSpaces 增加了对 AWS Resource Groups 标签编辑器的支持。 AWS Resource Groups 标签编辑器使您能够在自己的 WorkSpaces AWS 资源和其他资源中添加、编辑或删除 AWS 标签。

亚马逊 WorkSpaces 服务配额

Service Quotas 可以轻松查找特定配额（也称为限制）的值。您还可以查看特定服务的所有配额。

要查看您的配额 WorkSpaces

1. 导航到 S ervice Quotas 控制台。
2. 在左侧导航窗格中，选择AWS 服务。
3. WorkSpaces从列表中选择亚马逊，或在预先输入的搜索字段 WorkSpaces中输入亚马逊。
4. 要查看有关配额的其他信息，例如其描述和 Amazon 资源名称 (ARN)，请选择配额名称。

Amazon WorkSpaces 提供不同资源，供您在给定区域的账户中使用，包括图像 WorkSpaces、捆绑包、目录、连接别名和 IP 控制组。在您创建 Amazon Web Services 账户时，系统会对您可以创建的资源数量设置默认配额（也称为限制）。

您可以使用 S ervice Quotas 控制台查看默认的服务配额或请求增加可调整配额的配额。

有关更多信息，请参阅 Service Quot as 用户指南中的查看服务配额和请求增加配额。

自动部署亚马逊 WorkSpaces

借助亚马逊 WorkSpaces，您可以在几分钟内启动微软 Windows 或 Amazon Linux 桌面，并安全、可靠、快速地从本地或外部网络连接和访问您的桌面软件。您可以自动配置 Amazon WorkSpaces ，以便将亚马逊 WorkSpaces集成到您现有的配置工作流程中。

常见的 WorkSpaces 自动化方法

客户可以使用多种工具来实现Amazon的快速 WorkSpaces 部署。这些工具可用于简化管理 WorkSpaces、降低成本并实现可快速扩展和移动的敏捷环境。

AWS CLI 和 API

您可以使用 Amazon WorkSpaces API 操作来安全、大规模地与服务进行交互。所有公共 API 都适用于的 AWS CLI SDK 和工具 PowerShell，而私有 API（例如图像创建）只能通过使用 AWS Management Console。在考虑 Amazon 的运营管理和业务自助服务时 WorkSpaces，请考虑 WorkSpaces API 确实需要技术专业知识和安全权限才能使用。

可以使用AWS 软件开发工具包进行 API 调用。AWS 适用于 Windows 的 AWS 工具 PowerShell和适用于 PowerShell Core 的工具是基于适用于.NET 的 AWS SDK 公开的功能构建的 PowerShell 模块。这些模块使您能够通过 PowerShell 命令行编写 AWS 资源操作脚本，并与现有工具和服务集成。例

如，API 调用可以让您自动管理 WorkSpaces 生命周期，方法是与 AD 集成， WorkSpaces 根据用户的 AD 组成员资格进行配置和停用。

AWS CloudFormation

AWS CloudFormation 使您能够在文本文件中对整个基础架构进行建模。此模板将成为您的基础架构的单一事实来源。这可以帮助您标准化组织中使用的基础架构组件，从而实现配置合规性并更快地进行故障排除。

AWS CloudFormation 以安全、可重复的方式配置资源，使您能够构建和重建基础架构和应用程序。你可以使用 CloudFormation 来调试和停用环境，当你有多个账户需要以可重复的方式建立和停用时，这很有用。在考虑亚马逊的运营管理和业务自助服务时 WorkSpaces，请考虑这AWS CloudFormation确实需要技术专业知识和安全权限才能使用。

自助服务 WorkSpaces 门户

客户可以使用基于 WorkSpaces API 命令和其他 AWS 服务来创建 WorkSpaces 自助服务门户。这可以帮助客户简化大规模部署和回收 WorkSpaces 的流程。使用 WorkSpaces 门户，您可以让员工使用集成的审批工作流程来配置自己的 WorkSpaces 工作流程，该工作流程不需要 IT 部门对每个请求进行干预。这可以降低 IT 运营成本，同时帮助最终用户 WorkSpaces 更快地开始工作。额外的内置审批工作流程简化了企业的桌面审批流程。专用门户可以提供用于配置 Windows 或 Linux 云桌面的自动工具，使用户能够重建、重启或迁移其云桌面 WorkSpace，还可以提供密码重置工具。

本文档的 “进一步阅读” 部分提到了创建自助服务 WorkSpaces 门户的指导示例。 AWS 合作伙伴通过提供预配置的 WorkSpaces 管理门户。AWS Marketplace

与企业 IT 服务管理集成

随着企业大规模采用 Amazon WorkSpaces 作为其虚拟桌面解决方案，需要实施 IT 服务管理 (ITSM) 系统或与之集成。ITSM 集成允许提供用于配置和运营的自助服务。S ervice Catalog 使您能够集中管理常用部署的 AWS 服务和预配置的软件产品。该服务可帮助您的组织实现一致的治理和合规性要求，同时允许用户仅部署他们需要的经批准的 AWS 服务。Service Catalog 可用于通过 IT 服务管理工具（例如）为亚马逊 WorkSpaces 启用自助生命周期管理服务。ServiceNow

WorkSpaces 部署自动化最佳实践

在选择和设计 WorkSpaces 部署自动化时，您应该考虑 Well Architected 原则。

- 自动化设计 — 设计时尽可能减少流程中的手动干预，以实现可重复性和可扩展性。

- 成本优化设计 — 通过自动创建和回收 WorkSpaces，您可以减少提供资源所需的管理工作，并消除闲置或未使用的资源产生不必要的成本。
- 效率设计-最大限度地减少创建和终止所需的资源 WorkSpaces。在可能的情况下，为企业提供第 0 层自助服务功能以提高效率。
- 灵活性设计-创建一致的部署机制，该机制可以处理多种场景，并且可以使用相同的机制（使用标记的用例和配置文件标识符进行自定义）进行扩展。
- 为生产力而设计 — 设计您的 WorkSpaces 运营以允许正确的授权和验证来添加或删除资源。
- 可扩展性设计 — Amazon WorkSpaces 采用的 pay-as-you go 模式可以根据需要创建资源，并在不再需要时将其移除，从而节省成本。
- 为安全而设计-设计您的 WorkSpaces 操作以允许使用正确的授权和验证来添加或删除资源。
- 为可支持性而设计 — 设计您的 WorkSpaces 运营以允许非侵入性支持和恢复机制和流程。

Amazon WorkSpaces 修补和就地升级

在亚马逊 WorkSpaces，您可以使用现有的第三方工具（例如微软系统中心配置管理器 (SCCM)、Puppet Enterprise 或 Ansible）来管理修补和更新。就地部署安全补丁通常会保持每月的补丁周期，还有额外的升级或快速部署流程。但是，在操作系统就地升级或功能更新时，通常需要特别注意事项。

WorkSpace 维护

亚马逊 WorkSpaces 有一个默认的维护时段，在此期间 WorkSpace 会安装亚马逊 WorkSpaces 代理更新和任何可用的操作系统更新。 WorkSpaces 在计划维护时段内，用户连接将不可用。

- AlwaysOn WorkSpaces 默认维护时段为每个星期日上午的 00h00 到 04h00，按时区划 WorkSpace 分。

- 默认情况下，时区重定向处于启用状态，并且可以覆盖默认窗口以匹配用户的本地时区。
- 你可以 WorkSpaces使用组策略禁用 Windows 的时区重定向。你可以使用 PCoIP Agent conf 禁用 Linux WorkSpaces 的时区重定向。

- AutoStop WorkSpaces 每月自动启动一次，用于安装重要更新。从每月的第三个星期一开始，最长为两周，维护窗口的开放时间为每天大约 00:00 到 05h00，与该地区的时区相同。 AWS WorkSpace WorkSpace 可以在维护窗口中的任何一天进行维护。

- 尽管您无法修改用于维护的时区 AutoStop WorkSpaces，但您可以为自己禁用维护时段 AutoStop WorkSpaces。

- 手动维护时段可以根据您的首选计划进行设置，方法是将的状态设置为 ADMIN _MAINTA WorkSpace NTINE。

- 该 AWS CLI 命令modify-workspace-state可用于将 WorkSpace 状态修改为 ADMIN_MAINTANTINE。

亚马逊 Linux WorkSpaces

有关在 Amazon Linux WorkSpaces 自定义映像上管理更新和补丁的注意事项、先决条件和建议模式，请参阅白皮书《 WorkSpaces 为亚马逊提供 Linux 镜像做好准备的最佳实践》。

Linux 修补的先决条件和注意事项

- Amazon Linux 存储库托管在亚马逊简单存储服务 (Amazon S3) Service 存储桶中，可通过可访问互联网的公共终端节点或私有终端节点进行访问。如果您的 Amazon Linux WorkSpaces 无法访问互联网，请参阅此过程以访问更新：如何在运行 Amazon Linux 1 或 Amazon Linux 2 的 EC2 实例上更新 yum 或在没有互联网访问的情况下安装软件包？
- 您无法为 Linux 配置默认维护时段 WorkSpaces。如果需要自定义此窗口，则可以使用手动维护流程。

亚马逊 Windows 补丁

默认情况下，您 WorkSpaces 的 Windows 配置为接收来自 Windows 更新的更新，这些更新需要从您的 WorkSpaces VPC 访问互联网。要为 Windows 配置自己的自动更新机制，请参阅 Window s 服务器更新服务 (WSUS) 和配置管理器的文档。

亚马逊 Windows 就地升级

- 如果您计划从 Windows 10 创建映像 WorkSpace，请注意，从先前版本升级（Windows 功能/版本升级）的 Windows 10 系统不支持创建映像。但是， WorkSpaces 映像创建和捕获过程支持 Windows 累积更新或安全更新。

- 自定义 Windows 10 自带许可证 (BYOL) 映像应以虚拟机上最新支持的 Windows 版本开头，作为 BYOL 导入过程的来源：有关更多详细信息，请参阅 BYOL 导入文档。

Windows 就地升级先决条件

- 如果你使用 Active Directory 组策略或 SCCM 推迟或暂停 Windows 10 升级，请为 Windows 10 启用操作系统升级。 WorkSpaces
- 如果 WorkSpace 是 AutoStop WorkSpace，请将 AutoStop 时间更改为至少三小时以适应升级时段。
- 就地升级过程通过复制 “默认用户” (C:\Users\Default) 来重新创建用户配置文件。请勿使用默认用户配置文件进行自定义。建议改为通过组策略对象 (GPO) 对用户配置文件进行任何自定义。通过 GPO 进行的自定义可以很容易地修改或回滚，而且不易出错。
- 就地升级过程只能备份和重新创建一个用户配置文件。如果您在驱动器 D 上有多个用户配置文件，请删除除所需配置文件之外的所有用户配置文件。

Windows 就地升级注意事项

- 就地升级过程使用两个注册表脚本（enable-inplace-upgrade.ps1 和 update-pvdrivers.ps1）对您的进行必要的更改并启用 Windows 更新进程运行。 WorkSpaces 这些更改涉及在驱动器 C 而不是驱动器 D 上创建临时用户配置文件。如果驱动器 D 上已存在用户配置文件，则该原始用户配置文件中的数据仍保留在驱动器 D 上。
- 部署就地升级后，必须将用户配置文件还原到 D 盘，以确保可以重建或迁移您的 D 盘 WorkSpaces，并避免用户 shell 文件夹重定向出现任何潜在问题。您可以使用 PostUpgradeRestoreProfileOnD 注册表项执行此操作，如 BYOL 升级参考页面中所述。

Amazon WorkSpaces 语言包

提供 Windows 10 桌面体验的 Amazon WorkSpaces 套装支持英语（美国）、法语（加拿大）、韩语和日语。但是，您可以为西班牙语、意大利语、葡萄牙语以及更多语言选项添加其他语言包。有关更多信息，请参阅如何使用英语以外的客户端语言创建新 Windows WorkSpace 映像？ 。

亚马逊 WorkSpaces 个人资料管理

亚马逊通过 WorkSpaces 将所有个人资料写入重定向到单独的亚马逊弹性区块存储 (Ama zon EBS) 卷，将用户配置文件与基本操作系统 (OS) 分开。在微软 Windows 中，用户配置文件存储在 D:\Users

\username 中。在 Amazon Linux 中，用户配置文件存储在 /home 中。EBS 卷每 12 小时自动拍摄一次快照。快照会自动存储在 AWS 托管 S3 存储桶中，以便在重建或恢复 WorkSpace Amazon 时使用。

对于大多数组织而言，每 12 小时创建一次自动快照要优于现有的桌面部署（不为用户配置文件进行备份）。但是，客户可能需要对用户配置文件进行更精细的控制；例如，从桌面迁移到新的操作系统/AWS 区域，支持灾难恢复等。 WorkSpacesAmazon 还有其他管理个人资料的方法 WorkSpaces。

文件夹重定向

虽然文件夹重定向是虚拟桌面基础架构 (VDI) 架构中常见的设计考虑因素，但它不是最佳实践，甚至不是亚马逊 WorkSpaces 设计中的常见要求。其原因是 Amazon WorkSpaces 是一种永久性的桌面即服务 (DaaS) 解决方案，应用程序和用户数据开箱即用。

在某些特定情况下，需要对用户 Shell 文件夹进行文件夹重定向（例如，D:\Users\username\Desktop 重定向到\\ Server\ RedirectionShare $\ username\ Desktop），例如灾难恢复 (DR) 环境中用户配置文件数据的即时恢复点目标 (RPO)。

最佳实践

为实现强大的文件夹重定向，列出了以下最佳实践：

- 将 Windows 文件服务器托管在亚马逊 WorkSpaces 启动的同一 AWS 地区和可用区。
- 确保 AD 安全组入站规则包含 Windows 文件服务器安全组或私有 IP 地址；否则，请确保本地防火墙允许相同的基于 TCP 和 UDP 端口的流量。
- 确保 Windows 文件服务器安全组入站规则包括适用于所有亚马逊 WorkSpaces 安全组的 TCP 445 (SMB)。
- 为亚马逊 WorkSpaces 用户创建一个 AD 安全组，以授权用户访问 Windows 文件共享。
- 使用 DFS 命名空间 (DFS-N) 和 DFS 复制 (DFS-R) 来确保你的 Windows 文件共享非常灵活，不会绑定到任何一个特定的 Windows 文件服务器，并且所有用户数据都会在 Windows 文件服务器之间自动复制。
- 在 Windows 资源管理器中浏览网络共享时，在共享名称的末尾添加 “$” 以隐藏共享托管用户数据。
- 按照 Microsoft 关于重定向文件夹的指导创建文件共享：使用离线文件部署文件夹重定向。严格遵循安全权限和 GPO 配置指南。
- 如果您的 Amazon WorkSpaces 部署是 “自带许可 (BYOL)”，则还必须按照 Microsoft 的指导指定禁用离线文件：禁用单个重定向文件夹中的离线文件。

- 如果您的 Windows 文件服务器是 Windows Server 2016 或更高版本，请安装并运行重复数据删除（通常称为“重复数据删除”），以减少存储消耗并优化成本。请参阅安装并启用重复数据删除和运行重复数据删除。
- 使用现有的组织备份解决方案备份您的 Windows 文件服务器文件共享。

要避免的事情

- 请勿使用只能通过广域网 (WAN) 连接访问的 Windows 文件服务器，因为 SMB 协议不是为此目的而设计的。
- 请勿使用与主目录相同的 Windows 文件共享，以减少用户意外删除其用户外壳文件夹的机会。
- 虽然为了便于文件恢复，建议启用卷影复制服务 (VSS)，但仅此一项并不能取消备份 Windows 文件服务器文件共享的要求。

其他考虑因素

- 适用于 Windows File Server 的 Amazon FSx 为 Windows 文件共享提供托管服务，并简化了文件夹重定向（包括自动备份）的操作开销。
- 如果没有现有的组织备份解决方案，请使用 AWS Storage Gateway SMB File Share 来备份您的文件共享。

个人资料设置

群组策略

企业 Microsoft Windows 部署中常见的最佳做法是通过组策略对象 (GPO) 和组策略首选项 (GPP) 设置来定义用户环境设置。快捷方式、驱动器映射、注册表项和打印机等设置是通过组策略管理控制台定义的。通过 GPO 定义用户环境的好处包括但不限于：

- 集中式配置管理
- 用户配置文件由 AD 安全组成员资格或 OU 位置定义
- 防止删除设置
- 首次登录时自动创建个人资料并进行个性化设置
- easy of future 更新

> **Note**
>
> 遵循 Microsoft 优化组策略性能的最佳实践。

不得使用交互式登录横幅群组政策，因为亚马逊 WorkSpaces不支持这些政策。横幅是通过 AWS 支持请求在 Amazon WorkSpaces 客户端上展示的。此外，不得通过组策略阻止可移动设备，因为它们是 Amazon 所必需的 WorkSpaces。

GPO 可以用来管理 Windows WorkSpaces。有关更多信息，请参阅管理您的 Windows WorkSpaces。

Amazon WorkSpaces 交易量

每个 Amazon WorkSpaces 实例包含两个卷：一个操作系统卷和一个用户卷。

- Amazon Windows WorkSpaces — C:\ 驱动器用于操作系统 (OS)，D:\ drive 用于用户音量。用户配置文件位于用户卷上（“文档” AppData、“图片”、“下载” 等）。
- 亚马逊 Linux WorkSpaces — 在亚马逊 Linux 中 WorkSpace，系统卷 (/dev/xvda1) 将作为根文件夹挂载。用户卷用于存放用户数据和应用程序；/dev/xvdf1 挂载为 /home。

对于操作系统卷，您可以为该驱动器选择 80 GB 或 175 GB 的起始大小。对于用户卷，您可以选择 10 GB、50 GB 或 100 GB 的起始大小。两个卷的大小都可以根据需要增加到 2TB；但是，要将用户容量增加到 100 GB 以上，操作系统容量必须为 175 GB。每个卷每六小时只能更改音量一次。有关修改 WorkSpaces 卷大小的更多信息，请参阅《管理指南》的 “修改 WorkSpace” 部分。

WorkSpaces 卷最佳实践

在规划 Amazon WorkSpaces 部署时，建议考虑操作系统安装、就地升级以及将添加到操作系统卷映像中的其他核心应用程序的最低要求。对于用户卷，建议从较小的磁盘分配开始，然后根据需要逐渐增加用户卷的大小。最小化磁盘卷的大小可以降低运行的成本 WorkSpace。

> **Note**
>
> 虽然可以增加卷大小，但不能减小。

Amazon WorkSpaces 日志

在 Amazon WorkSpaces 环境中，可以捕获许多日志源来解决问题并监控整体 WorkSpaces 性能。

Amazon C WorkSpaces lient 3.x 在每个亚马逊 WorkSpaces 客户端上，客户端日志都位于以下目录中：

- Windows — %LOCALAPPDATA%\ Amazon Web Services\ Amazon\ logs WorkSpaces
- macOS — ~/Library/ “Application Support”/“亚马逊网络服务”/“亚马逊” /logs WorkSpaces
- Linux（Ubuntu 18.04 或更高版本）— /opt/workspacesclient/workspacesclient

在许多情况下，可能需要从客户端获取 WorkSpaces 会话的诊断或调试详细信息。也可以通过在工作区可执行文件中添加 “-l3” 来启用高级客户机日志。例如：

```
"C:\Program Files (x86)\Amazon Web Services, Inc\Amazon WorkSpaces"
workspaces.exe -l3
```

亚马逊 WorkSpaces 服务

亚马逊 WorkSpaces 服务与亚马逊 CloudWatch 指标、 CloudWatch 事件和 CloudTrail。这种集成允许将性能数据和 API 调用记录到中央 AWS 服务中。

在管理 Amazon WorkSpaces 环境时，持续监控某些 CloudWatch 指标以确定整体环境运行状况非常重要。指标

虽然 Amazon 还有其他可用 CloudWatch 指标 WorkSpaces（请参阅监控您的 WorkSpaces 使用 CloudWatch 指标），但以下三个指标将有助于保持 WorkSpace实例的可用性：

- Un healthy — 返回 WorkSpaces 不健康状态的数字。
- SessionLaunchTime— 启动 WorkSpaces 会话所花费的时间。
- InSessionLatency— WorkSpaces 客户端与之间的往返时间。 WorkSpace

有关 WorkSpaces 日志选项的更多信息，请参阅使用记录 Amazon WorkSpaces API 调用 CloudTrail。其他 CloudWatch 事件将有助于捕获用户会话的客户端 IP、用户何时连接到 WorkSpaces 会话以及连接期间使用了什么端点。所有这些详细信息都有助于隔离或查明用户在故障排除会话期间报告的问题。

> **Note**
>
> 某些 CloudWatch 指标仅适用于 AWS 托管 AD。

亚马逊上适用于 Linux 的容器和 Windows 子系统 WorkSpaces

容器和亚马逊 WorkSpaces

希望通过 Amazon 为容器工作负载提供服务的客户通常会使用最终用户计算 WorkSpaces。尽管有可能，但这不是首选或推荐的解决方案。强烈建议希望通过容器实现潜在成本和运营节约的客户评估亚马逊弹性容器服务 (Amazon ECS) 和/或亚马逊弹性 Kubernetes Service（亚马逊 EKS）。

如果客户要求必须启用使用 Amazon 的容器 WorkSpaces，则已经发布了支持使用 Docker 的技术操作方法。应告知客户，这需要其他跟踪服务，而且与分离的原生容器服务相比，成本和复杂性都会增加。

适用于 Linux 的 Windows 子系统

随着Windows Server 2019作为亚马逊底层操作系统的推出 WorkSpaces，客户一直渴望实施适用于Linux的Windows子系统（WSL），特别是WSL2。由于 WSL2 调用虚拟机 (Hyper-V) 来执行其功能，因此它无法在由虚拟机管理程序管理的 Ama WorkSpaces zon 上运行。 AWS 出于这个原因，客户应该知道只有 WSL1 可用，并理解 WSL1 和 WSL2 之间的区别。

亚马逊 WorkSpaces 迁移

借助 Amazon WorkSpaces 迁移功能，您可以将用户卷数据带到新的捆绑包中。您可以使用此功能来：

- 将你 WorkSpaces 从 Windows 7 体验迁移到 Windows 10 桌面体验。
- 从 PCoIP 迁移 WorkSpace 到 WorkSpaces 流式传输协议 (WSP)。 WorkSpace
- WorkSpaces 从一个公共或自定义捆绑包迁移到另一个捆绑包。例如，您可以从支持 GPU 的（图形和 GraphicsPro）捆绑包迁移到不支持 GPU 的捆绑包，反之亦然。

迁移过程

使用 m WorkSpaces igrate，您可以指定目标 WorkSpaces 捆绑包。迁移过程 WorkSpace使用目标包映像中的新根卷和最新的原始用户卷快照重新创建用户卷。为了提高兼容性，迁移期间会生成新的用户配置文件。旧用户配置文件中无法移动到新配置文件的数据存储在.notMigrated 文件夹中。

在迁移过程中，用户卷（驱动器 D）上的数据会保留，但根卷（C:\ drive）上的所有数据都将丢失。这意味着不会保留已安装的应用程序、设置和对注册表的更改。将旧的用户配置文件文件夹重命名为。NotMigrated suffix，然后创建了一个新的用户配置文件。

每次迁移过程最多需要一个小时 WorkSpace。此外，如果迁移工作流程未能完成该过程，该服务将在迁移前自动将其回滚 WorkSpace 到其原始状态，从而最大限度地降低任何数据丢失的风险。

在迁移过程中，分配给原始标签的所有标签 WorkSpace 都将被保留。的运行模式将 WorkSpace 保留。迁移后的计算机 WorkSpace 有了新的 WorkSpace ID、计算机名称和 IP 地址。迁移程序

您可以 WorkSpaces 通过亚马逊 WorkSpaces 控制台、 AWS CLI 使用迁移工作空间命令或亚马 WorkSpaces 逊 API 进行迁移。所有迁移请求都会排队，如果迁移请求过多，该服务将自动限制迁移请求的总数。迁移限制

- 您不能迁移到公有或自定义 Windows 7 桌面体验捆绑包。
- 你无法迁移到 BYOL Windows 7 捆绑包。
- 您 WorkSpaces 只能将 BYOL 迁移到其他 BYOL 捆绑包。
- 您无法将从公共或自定义捆绑包中 WorkSpace 创建的分发包迁移到 BYOL 捆绑包。
- WorkSpaces 目前不支持迁移 Linux。
- 在支持多种语言的 AWS 区域中，您可以在语言包 WorkSpaces 之间迁移。

- 源捆绑包和目标捆绑包必须不同。（但是，在支持多种语言的区域，只要语言不同，您就可以迁移到相同的 Windows 10 软件包。）如果您想 WorkSpace 使用相同的捆绑包刷新，请 WorkSpace改为重新构建。
- 您无法 WorkSpaces 跨区域迁移。
- WorkSpaces 当它们处于管理员维护模式时无法迁移。

成本

在迁移发生的当月，您需要为新迁移和原始 WorkSpaces迁移按比例支付费用。例如，如果您在 5 月 10 日将 WorkSpace A 迁移到 WorkSpace B，则将在 5 月 1 日至 5 月 10 日期间支付 WorkSpace A 费用，并在 5 月 11 日至 5 月 30 日期间支付 WorkSpace B 费用。

WorkSpaces 迁移最佳实践

在迁移之前 WorkSpace，请执行以下操作：

- 将驱动器 C 上的任何重要数据备份到另一个位置。在迁移过程中，将擦除驱动器 C 上的所有数据。
- 请确保 WorkSpace 正在迁移的已有至少 12 小时的时间，以确保已创建用户卷的快照。在 Amazon WorkSpaces 控制台的 M igrat e WorkSpaces 页面上，您可以参考上次拍摄快照的时间。在迁移过程中，上一个快照之后创建的所有数据将丢失。
- 为避免潜在的数据丢失，请确保您的用户注销其用户 WorkSpaces，并且在迁移过程完成之前不要重新登录。
- 确保 WorkSpaces 要迁移的状态为 “可用”、“已停止” 或 “错误”。
- 请确保您有足够的 IP 地址供 WorkSpaces要迁移的。在迁移期间，将为分配新的 IP 地址 WorkSpaces。
- 如果您使用脚本进行迁移 WorkSpaces，请分批迁移它们，一次不超过 25 WorkSpaces 个。

架构完善的框架

AWS Wel l-Architected 帮助云架构师为其应用程序和工作负载构建安全、高性能、弹性和高效的基础架构。它描述了在云中设计和运行工作负载的关键概念、设计原则和架构最佳实践。它基于五个关键支柱：

- 卓越运营
- 安全性
- 可靠性
- 性能效率
- 成本优化

在构建 Amazon WorkSpaces 环境时，重要的是要评估这些关键支柱以确定成熟度部署级别，并发现可与 Amazon WorkSpaces 一起使用的其他功能。虽然 Well-A AWS rchitect Fram ework 有总体指导，但以下内容提供了一些关键问题，这些问题可以包含在 WorkSpaces 部署的规划阶段，以确保五个支柱中的每一个都得到考虑。

一般性问题

- 这个项目的业务驱动因素是什么？

卓越运营

- 如何隔离用户和不同管理员组之间的访问控制？

安全性

1. 运营时需要考虑哪些安全与合规性要求？ WorkSpaces
2. 路由到外部 IP 地址是否有任何限制？
3. 所需的 WorkSpaces 端口是否允许通过公司防火墙？
4. 此部署是否或将使用多因素身份验证？
5. 你今天有多少用户身份和授权请求？

可靠性

1. 台式机的数据保留政策是什么？
2. 最终用户数据的恢复点目标 (RPO) 是什么？
3. 最终用户数据的恢复时间目标 (RTO) 是多少？

成本优化

1. WorkSpaces 捆绑包的大小是否适合用户案例和应用程序？
2. 用户每月消耗的时间会 WorkSpaces 超过 82 小时吗？

虽然上述问题并不构成应考虑的项目的详尽清单，但它们提供了一些总体指导，可帮助您部署 Well-Architected Amazon WorkSpaces。

安全性

本节介绍在使用 Amazon WorkSpaces 服务时如何使用加密来保护数据。它描述了传输中的加密和静态加密，以及使用安全组来保护对网络的访问 WorkSpaces。本节还提供有关如何使用可信设备和 IP 访问控制组 WorkSpaces 来控制对终端设备的访问的信息。

有关Di AWS rectory Service中身份验证（包括MFA支持）的其他信息可以在本节中找到。

传输中加密

Amazon WorkSpaces 使用加密技术来保护不同通信阶段（传输中）的机密性，并保护静态数据（加密 WorkSpaces）。以下各节介绍了 Amazon WorkSpaces 在传输过程中使用的每个加密阶段的流程。

有关静态加密的信息，请参阅本文档的加密 WorkSpaces部分。

注册和更新

桌面客户端应用程序使用 HTTPS 与 Amazon 通信以获取更新和注册。

身份验证阶段

桌面客户端通过向身份验证网关发送凭据来启动身份验证。桌面客户端和身份验证网关之间的通信使用 HTTPS。在此阶段结束时，如果身份验证成功，则身份验证网关将通过相同的 HTTPS 连接向桌面客户端返回 OAuth 2.0 令牌。

> **Note**
>
> 桌面客户端应用程序支持使用代理服务器处理端口 443 (HTTPS) 流量、更新、注册和身份验证。

收到来自客户端的凭据后，身份验证网关会向 AWS Directory Service 发送身份验证请求。从身份验证网关到 AWS Directory Service 的通信通过 HTTPS 进行，因此不会以明文形式传输任何用户凭证。

身份验证-活动目录连接器 (ADC)

AD Connecto r 使用 Kerberos 与本地 AD 建立经过身份验证的通信，因此它可以绑定到 LDAP 并执行后续的 LDAP 查询。ADC 中的客户端 LDAPS 支持也可用于对 Microsoft AD 和应用程序之间的查询进行加密。 AWS 在实现客户端 LDAPS 功能之前，请查看客户端 LDAPS 的先决条件。

AWS 目录服务还支持带有 TLS 的 LDAP。任何时候都不会以纯文本形式传输用户凭证。为了提高安全性，可以使用 VPN 连接将 WorkSpaces VPC 与本地网络（AD 所在地）连接起来。使用 AWS 硬件 VPN 连接时，客户可以使用带有 AES-128 或 AES-256 对称加密密钥的标准 IPSEC（互联网密钥交换 (IKE) 和 IPSEC SA）、完整性哈希的 SHA-1 或 SHA-256 以及 DH 组（第 1 阶段为 2,14-18、22、23 和 24；第 2 阶段为 1,2,5、14-18、22、23 和 24）来设置传输中的加密。

经纪人阶段

在收到 OAuth 2.0 令牌（如果身份验证成功，则来自身份验证网关）后，桌面客户端将使用 HTTPS 查询亚马逊 WorkSpaces 服务（代理连接管理器）。桌面客户端通过发送 OAuth 2.0 令牌进行身份验证，因此，客户端会收到流媒体网关的 WorkSpaces 端点信息。

直播阶段

桌面客户端请求打开与流媒体网关的 PCoIP 会话（使用 OAuth 2.0 令牌）。此会话采用 AES-256 加密，使用 PCoIP 端口进行通信控制 (4172/TCP)。

流媒体网关使用 OAuth2.0 令牌，通过 HTTPS 向亚马逊 WorkSpaces服务请求用户特定的 WorkSpaces 信息。

流媒体网关还接收来自客户端的 TGT（使用客户端用户的密码进行加密），通过使用 Kerberos TGT 直通，网关使用用户检索到的 Kerberos TGT 在上启动 Windows 登录。 WorkSpace

WorkSpace 然后，使用标准的 Kerberos 身份验证向已配置的 AWS Directory Service 发起身份验证请求。

成功登录后，PCoIP 直播开始。 WorkSpace 连接由客户端在端口 TCP 4172 上启动，返回流量通过端口 UDP 4172 发起。此外，流媒体网关和 WorkSpaces 桌面之间通过管理接口的初始连接是通过 UDP 55002 进行的。（请参阅文档，了解 A mazon 的 IP 地址和端口要求 WorkSpaces。 初始出站 UDP 端口为 55002。）使用端口 4172（TCP 和 UDP）的流媒体连接使用 AES 128 位和 256 位密码进行加密，但默认为 128 位。客户可以主动将其更改为 256 位，方法是使用适用于 Windows WorkSpaces 的 PCoip 特定的 AD 组策略设置，也可以使用亚马逊 Linux 的 pcoip-agent.conf 文件。 WorkSpaces有关 Amazon 组策略管理的更多信息 WorkSpaces，请参阅文档。

网络接口

每个 Amazon WorkSpace 都有两个网络接口，分别称为主网络接口和管理网络接口。

主网络接口提供与客户 VPC 内部资源的连接，例如访问 AWS Directory Service、互联网和客户公司网络。可以将安全组附加到该主网络接口。从概念上讲，根据部署范围对附加到此 ENI 的安全组进行区分： WorkSpaces 安全组和 ENI 安全组。

管理网络接口

无法通过安全组控制管理网络接口；但是，客户可以使用基于主机的防火墙 WorkSpaces 来屏蔽端口或控制访问。我们不建议对管理网络接口施加限制。如果客户决定添加基于主机的防火墙规则来管理此接口，则应打开几个端口，以便 Amazon WorkSpaces 服务可以管理该接口的运行状况和可访问性。WorkSpace有关更多信息，请参阅《Amazon Workspaces 管理指南》中的网络接口。

WorkSpaces 安全组

默认安全组是按照 Directory Servic AWS e 创建的，该安全组会自动附加到属于 WorkSpaces 该特定目录的所有安全组。

与许多其他 AWS 服务一样 WorkSpaces，Amazon也使用安全组。当您向该 WorkSpaces 服务注册目录时，Amazon WorkSpaces 会创建两个 AWS 安全组。一个用于目录控制器 directoryID_Controllers，另一个用于目录 directoryID_workspacesMembers WorkSpaces 中。请勿删除其中任何一个安全组，否则您的安全组 WorkSpaces 将受到损害。默认情况下， WorkSpaces 成员安全组的出口开放至 0.0.0.0/0。您可以将默认 WorkSpaces安全组添加到目录中。将新的安全组与 WorkSpaces 目录关联后 WorkSpaces ，您启动的新安全组或重建 WorkSpaces 的现有安全组将拥有新的安全组。您也可以将这个新的默认安全组添加到现有安全组中， WorkSpaces 而无需对其进行重建。当您将多个安全组与一个 WorkSpaces 目录关联时，请将每个安全组中的规则 WorkSpaces聚合为一组规则。建议尽可能精简您的安全组规则。有关安全组的更多信息，请参阅 Amazon VPC 用户指南中的您的 VPC 的安全组。

有关向 WorkSpaces 目录中添加安全组或现有安全组的更多信息 WorkSpace，请参阅WorkSpaces 管理员指南。

一些客户希望限制 WorkSpaces 流量可以输出的端口和目的地。要限制来自的出站流量 WorkSpaces，必须确保保留服务通信所需的特定端口；否则，您的用户将无法登录其 WorkSpaces端口。

WorkSpaces 在 WorkSpace 登录期间，使用客户 VPC 中的弹性网络接口 (ENI) 与域控制器通信。要允许您的用户 WorkSpaces 成功登录，您必须允许以下端口访问您的域控制器或 CIDR 范围，包括您的域控制器在 _workspacesMembers 安全组中。

- TCP/UDP 53 - DNS

- TCP/UDP 88 - Kerberos 身份验证
- TCP/UDP 389 — LDAP
- TCP/UDP 445 - SMB
- TCP 3268-3269 – 全局目录
- TCP/UDP 464-Kerberos 密码更改
- TCP 139 - Netlogon
- UDP 137-138 - Netlogon
- UDP 123 - NTP
- TCP/UDP 49152-65535 RPC 的临时端口

如果您 WorkSpaces 需要访问其他应用程序、互联网或其他位置，则需要在 _workspacesMembers 安全组中以 CIDR 表示法允许这些端口和目的地。如果您不添加这些端口和目的地，则除了上面列出的端口之外， WorkSpaces 将无法到达其他任何地方。最后一个考虑因素是，默认情况下，新的安全组没有入站规则。因此，在您向安全组添加入站规则之前，不允许来自另一台主机的入站流量传输到您的实例。只有当您想要限制来自的出站流量 WorkSpaces或将入口规则锁定为仅应有权访问它们的资源或 CIDR 范围时，才需要执行上述步骤。

> **Note**
>
> 新关联的安全组将仅附加到修改后 WorkSpaces 创建或重建的安全组。

ENI 安全组

由于主网络接口是常规 ENI，因此可以使用不同的 AWS 管理工具对其进行管理。有关更多信息，请参阅弹性网络接口。导航到 WorkSpace IP 地址（在亚马逊 WorkSpaces 控制台的 WorkSpaces 页面中），然后使用该 IP 地址作为筛选条件来查找相应的 ENI（在 Amazon EC2 控制台的 “网络接口” 部分中）。

找到弹性网卡后，即可由安全组直接对其进行管理。手动为主网络接口分配安全组时，请考虑 Amazon 的端口要求 WorkSpaces。有关更多信息，请参阅《Amazon Workspaces 管理指南》中的网络接口。

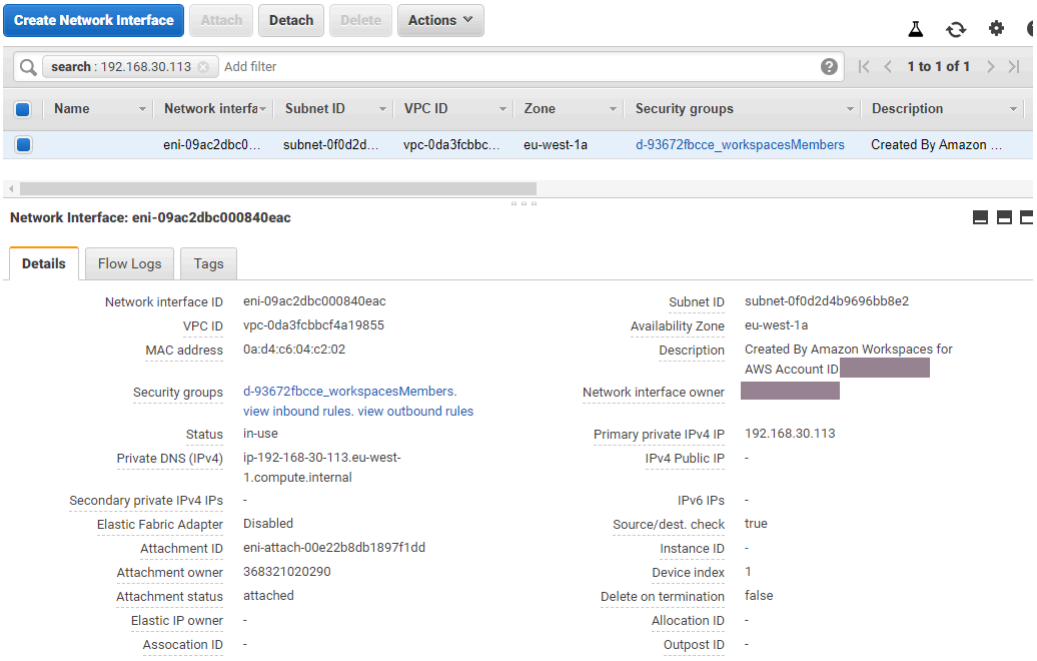

图 21：启用了 MFA 的 WorkSpaces 客户端

网络访问控制列表 (ACL)

由于管理另一个防火墙会增加复杂性，网络 ACL 通常用于非常复杂的部署，通常不用作最佳实践。由于网络 ACL 连接到 VPC 中的子网，因此其功能集中在 OSI 模型的第 3 层（网络）。由于 Amazon WorkSpaces 是基于目录服务设计的，因此必须定义两个子网。网络 ACL 与目录服务分开管理，因此网络 ACL 很可能只能分配给一个 “已分配 WorkSpaces” 子网。

当需要无状态防火墙时，网络 ACL 是确保安全的最佳实践。作为最佳实践，确保对网络 ACL 所做的任何超出默认设置的更改均按子网进行验证。如果网络 ACL 的性能未达到预期，请考虑使用 VPC 流日志来分析流量。

AWS 网络防火墙

AWS Network Fi@@ rewall 提供的功能超出了原生安全组和网络 ACL 所提供的功能，但要付出一定的代价。当客户要求能够提高网络连接的安全性（例如基于 HTTPS 的网站的服务器名称检查 (SNI)、入侵检测和预防，以及域名的允许和拒绝列表）时，他们只能在上面寻找替代防火墙。 AWS Marketplace部署这些防火墙的复杂性带来了超出标准 EUC 管理员所擅长的难题。 AWS Network Firewall 提供原生 AWS 体验，同时启用第 3 层到第 7 层保护。当组织没有任何其他手段（可以转移到云端的第三方防火墙的现有本地许可或管理防火墙的独立团队除外）来涵盖所有 EUC AWS 网络保

护时，将 Network Firewall 与 NAT Gateway 结合使用是最佳实践。使用 Network Firewall 时，NAT AWS 网关也是免费的。

Network Fire AWS wall 的部署是围绕现有的 EUC 设计设计而设计的。单个 VPC 设计可以实现简化的架构，其子网用于防火墙端点和单独的 Internet 出口路由注意事项，而多个 VPC 设计可以从带有防火墙和传输网关端点的整合检查 VPC 中受益匪浅。

设计场景

场景 1：基本实例锁定

默认 WorkSpaces 安全组不允许任何入站流量，因为默认情况下，安全组会被拒绝，并且是有状态的。这意味着无需配置其他配置即可进一步保护 WorkSpaces 实例本身。考虑允许所有流量的出站规则，以及是否符合用例。例如，最好拒绝所有发往端口 443 的出站流量到任何地址，以及适合端口用例的特定 IP 范围，例如 LDAP 的 389、LDAPS 的 636、SMB 的 445 等；但请注意，环境的复杂性可能需要多条规则，因此可以通过网络 ACL 或防火墙设备更好地提供服务。

场景 2：入库异常

虽然这不是一个固定的要求，但有时网络流量可能会被发起入站 WorkSpaces。例如，在 WorkSpaces 客户端无法连接时对实例进行分类需要其他远程连接。在这些情况下，最好暂时启用客户 ENI 安全组的入站 TCP 3389。 WorkSpace

另一种情况是组织脚本，它执行由集中式实例启动的清单或自动化功能的命令。可以永久配置该端口上来自入站上那些特定集中式实例的流量，但是，最佳做法是在附加到目录配置的其他安全组上执行此操作，因为它可以应用于 AWS 账户中的多个部署。

最后，有些网络流量不是基于状态的，需要在入站例外中指定临时端口。如果查询和脚本失败，则在确定连接失败的根本原因时，最好允许临时端口，至少是暂时允许使用临时端口。

场景 3：单个 VPC 检查

简化的部署 WorkSpaces （例如没有扩展计划的单个 VPC）不需要单独的 VPC 进行检查，因此可以通过 VPC 对等互连来简化与其他 VPC 的连接。但是，必须为防火墙端点创建单独的子网，为这些端点配置路由以及 Internet Gateway (IGW) 出口路由，否则无需配置。如果所有子网都使用整个 VPC CIDR 块，则现有部署可能没有可用的 IP 空间。在这些情况下，方案 4 可能效果更好，因为部署已经超出了其初始设计。

场景 4：集中检查

在一个 AWS 区域的多个 EUC 部署中通常是首选，它简化了 AWS 网络防火墙有状态和无状态规则的管理。现有的 VPC 对等体将被传输网关所取代，因为这种设计需要使用 Transit Gateway 附件以及只能通过这些附件配置的检查路由。此外，还可以对这种配置进行更大程度的控制，从而实现超出默认 WorkSpaces 体验的安全性。

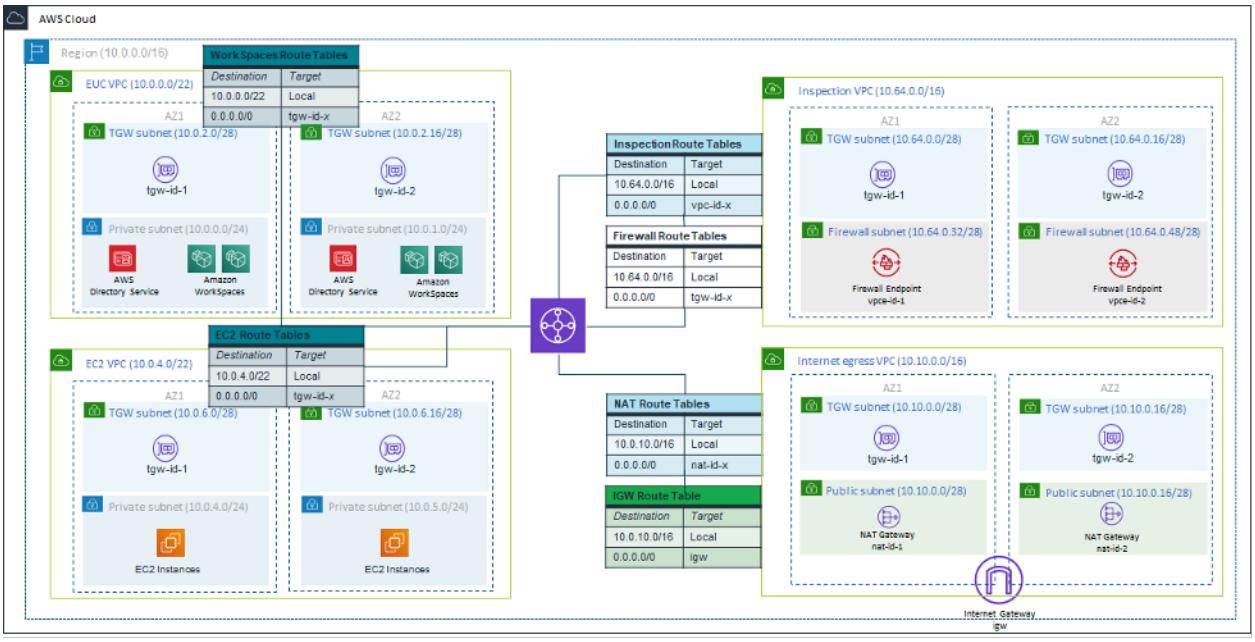

图 22：使用 Transit Gateway 附件的示例架构

已加密 WorkSpaces

每个亚马逊 WorkSpace 都配置了一个根卷（Windows 版 C：驱动器 WorkSpaces，亚马逊 Linux 为根盘 WorkSpaces）和一个用户卷（D：Windows 驱动器 WorkSpaces，/home 用于亚马逊 Linux WorkSpaces）。加密 WorkSpaces 功能允许对一个或两个卷进行加密。

什么是加密？

静态存储的数据、卷的磁盘输入/输出 (I/O) 以及从加密卷创建的快照都经过加密。

什么时候会加密？

在启动（创建）时 WorkSpace 应指定对的加密 WorkSpace。 WorkSpaces 只能在启动时对卷进行加密：启动后，无法更改卷加密状态。下图显示了在新版本发布期间用于选择加密的 Amazon WorkSpaces 控制台页面 WorkSpace。

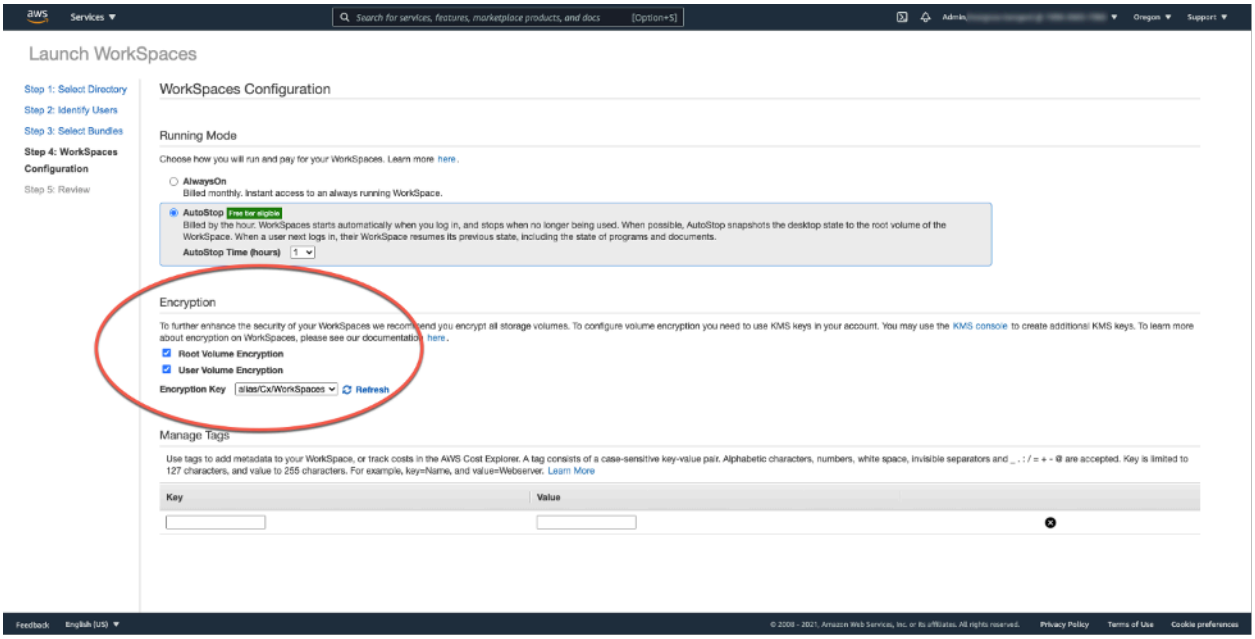

图 23：加密 WorkSpace 根卷

新版是如何 WorkSpace 加密的？

客户可以从亚马逊 WorkSpaces 控制台或 AWS CLI在客户启动新产品时使用亚马逊 WorkSpaces API 选择 “加密” WorkSpaces 选项 WorkSpace。

为了加密卷，Amazon WorkSpaces 使用 AWS Key Management Service (AWS KMS) 中的 CMK。在区域中首次启动时会创建默认 AWS KMS CMK。 WorkSpace （ CMK 具有区域范围。 ）

客户还可以创建客户托管的 CMK 以与加密一起使用。 WorkSpacesCMK 用于加密 Amazon WorkSpaces 服务用于加密每个 WorkSpace 卷的数据密钥。（严格来说，Amazon EBS 将对卷进行加密）。有关当前的 CMK 限制，请参阅AWS KMS 资源配额。

> **Note**
>
> 不支持使用加密 WorkSpace 镜像创建自定义镜像。此外，在启用根卷加密的情况下 WorkSpaces启动最多可能需要一个小时才能进行配置。

有关 WorkSpaces 加密过程的详细说明，请参阅 Amazon 的 WorkSpaces 使用方式 AWS KMS。考虑如何监控 CMK 的使用，以确保加密请求得到 WorkSpace 正确处理。有关 AWS KMS 密钥和数据密钥的更多信息，请参阅AWS KMS 页面。

访问控制选项和可信设备

Amazon WorkSpaces 为客户提供了管理哪些客户端设备可以访问的选项 WorkSpaces。客户只能限制对可信设备的 WorkSpaces 访问。允许 WorkSpaces 使用数字证书从 macOS 和微软 Windows 电脑上进行访问。它还可以允许或阻止 iOS、Android、Chrome 操作系统、Linux 和零客户端以及 WorkSpaces Web Access 客户端的访问。借助这些功能，它可以进一步改善安全状况。

新部署启用了访问控制选项，允许用户 WorkSpaces 从 Windows、macOS、iOS、安卓、ChromeOS 和 Zero Client 上的客户端访问他们的客户端。默认情况下，新 WorkSpaces 部署不启用使用 Web Access 或 Linux WorkSpaces 客户端进行访问，需要启用。

如果对来自可信设备（也称为托管设备）的企业数据访问有限制，则可以将 WorkSpaces 访问权限限制为具有有效证书的可信设备。启用此功能后，Amazon 将 WorkSpaces 使用基于证书的身份验证来确定设备是否可信。如果 WorkSpaces 客户端应用程序无法验证设备是否可信，则会阻止尝试登录或从该设备重新连接的尝试。

可信设备支持适用于以下客户端：

- Google Play 上的亚马逊 WorkSpaces 安卓客户端应用程序，可在兼容安卓和安卓的 Chrome 操作系统设备上运行
- 在 WorkSpaces macOS 设备上运行的亚马逊 macOS 客户端应用程序
- WorkSpaces 在 Windows 设备上运行的亚马逊 Windows 客户端应用程序

有关控制哪些设备可以访问的更多信息 WorkSpaces，请参阅限制对可信设备的 WorkSpaces 访问。

> **Note**
>
> 可信设备的证书仅适用于亚马逊 WorkSpaces Windows、macOS 和安卓客户端。此功能不适用于 Amazon WorkSpaces Web Access 客户端或任何第三方客户端，包括但不限于 Teradici PCoIP 软件和移动客户端、Teradici PCoIP 零客户端、RDP 客户端和远程桌面应用程序。

IP 访问控制组

使用基于 IP 地址的控制组，客户可以定义和管理可信 IP 地址组，并允许用户 WorkSpaces 仅在连接到可信网络时才能访问这些地址。此功能可帮助客户更好地控制自己的安全状况。

可以在 WorkSpaces 目录级别添加 IP 访问控制组。有两种方法可以开始使用 IP 访问控制组。

- IP 访问控制页面-通过 WorkSpaces 管理控制台，可以在 IP 访问控制页面上创建 IP 访问控制组。通过输入可以访问的 IP 地址或 IP 范围， WorkSpaces 可以将规则添加到这些组中。然后，可以将这些组添加到更新详细信息页面上的目录中。
- Workspace WorkSpaces AP I — API 可用于创建、删除和查看群组；创建或删除访问规则；或在目录中添加和删除群组。

有关在 Amazon WorkSpaces 加密过程中使用 IP 访问控制组的详细说明，请参阅[您的 IP 访问控制组 WorkSpaces]。

使用 Amazon 进行监控或记录 CloudWatch

监控网络、服务器和日志是任何基础架构不可或缺的一部分。部署 Amazon 的客户 WorkSpaces 需要监控其部署，特别是个人的整体运行状况和连接状态 WorkSpaces。

以下各项的亚马逊 CloudWatch 指标 WorkSpaces

CloudWatch 的指标旨在 WorkSpaces 为管理员提供对个人整体运行状况和连接状态的更多见解 WorkSpaces。在给定目录中 WorkSpace，可以按组织 WorkSpaces 中的每个组织提供或汇总指标。

与所有指标一样，这些 CloudWatch 指标可以在中查看 AWS Management Console （如下图所示），通过 CloudWatch API 进行访问，也可以通过 CloudWatch 警报和第三方工具进行监控。

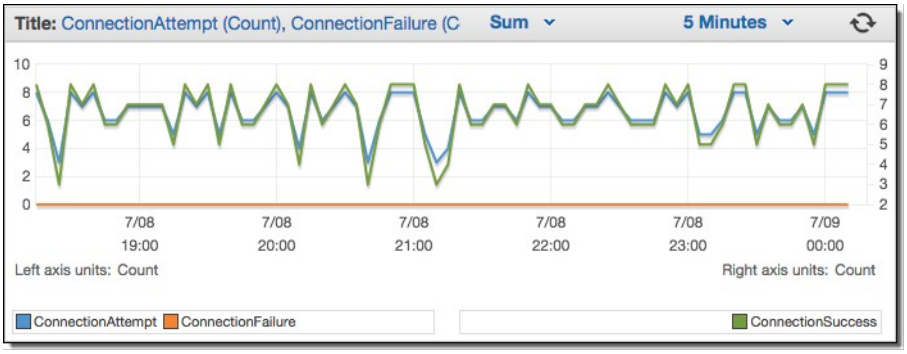

图 24： CloudWatch 指标： ConnectionAttempt / ConnectionFailure

默认情况下，以下指标处于启用状态，且无需支付额外费用即可使用：

- 可用 — WorkSpaces 对状态检查的响应计入此指标。
- 不健康 — 未 WorkSpaces对相同状态检查做出响应的计入此指标。

- ConnectionAttempt— 尝试连接的次数 WorkSpace。
- ConnectionSuccess— 成功连接尝试的次数。
- ConnectionFailure— 连接尝试失败的次数。
- SessionLaunchTime— 启动会话所花费的时间，由 WorkSpaces 客户端测量。
- InSessionLatency— 客户与 WorkSpaces 客户测量和 WorkSpaces报告的往返时间。
- SessionDisconnect— 用户发起和自动关闭的会话数。

此外，还可以创建警报，如下图所示。

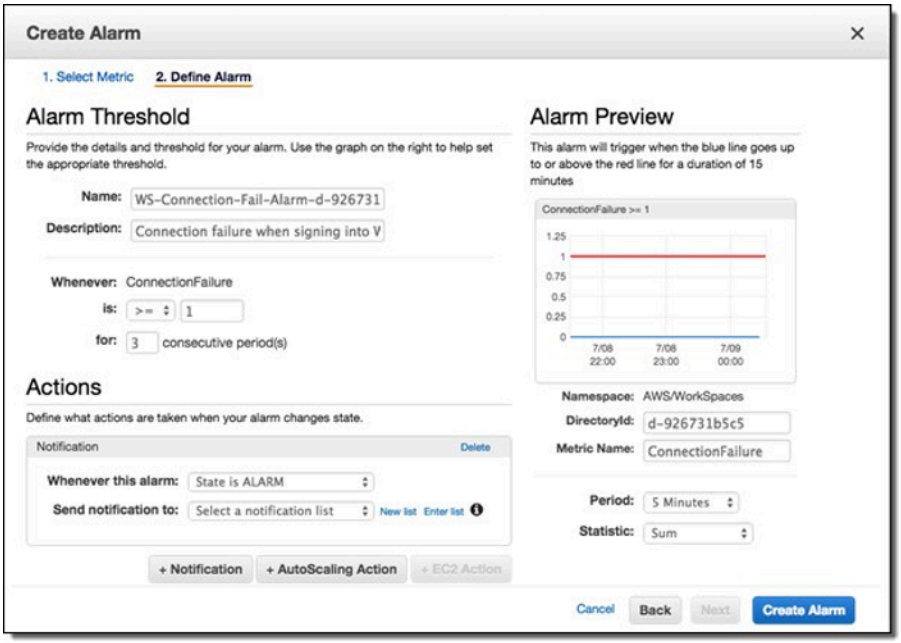

图 25：为 WorkSpaces 连接错误创建 CloudWatch 警报

适用于 Amazon CloudWatch 的活动 WorkSpaces

来自 Amazon Events CloudWatch 的事件可用于查看、搜索、下载、存档、分析和响应成功登录。WorkSpaces该服务可以监控用户登录的客户端 WAN IP 地址、操作系统、ID 和目录 ID 信息。WorkSpaces WorkSpaces例如，它可以将事件用于以下目的：

- 将 WorkSpaces 登录事件存储或存档为日志，以备将来参考，分析日志以寻找模式，然后根据这些模式采取行动。
- 使用 WAN IP 地址确定用户从何处登录，然后使用策略仅允许用户访问 WorkSpaces 符合访问 CloudWatch 事件类型中找到的访问标准的文件或数据。WorkSpaces
- 使用策略控制阻止未经授权的 IP 地址访问文件和应用程序。

有关如何使用 CloudWatch 事件的更多信息，请参阅 Amazon CloudWatch Events 用户指南。要了解有关 CloudWatch 事件的更多信息 WorkSpaces，请参阅 WorkSpaces 使用 Cloudwatch 事件监控您的。

YubiKey 对 Amazon 的支持 WorkSpaces

为了增加额外的安全层，客户通常会选择使用多因素身份验证来保护工具和网站。有些客户选择使用 Yubic YubiKey o 来执行此操作。亚马逊同时 WorkSpaces 支持一次性密码 (OTP) 和 FIDO U2F 身份验证协议。 YubiKeys

Amazon WorkSpaces 目前支持 OTP 模式，管理员或最终用户无需执行任何其他步骤即可 YubiKey 使用 OTP。用户可以将其 YubiKey 连接到计算机，确保键盘聚焦在计算机上 WorkSpace （特别是在需要输入 OTP 的字段中），然后触摸计算机上的金色触点。YubiKey YubiKey 将自动在所选字段中输入 OTP。

要使用带有 YubiKey 和的 FIDO U2F 模式 WorkSpaces，需要执行其他步骤。确保您的用户获得以下支持的 YubiKey 模型之一，以便通过以下方式使用 U2F 重定向： WorkSpaces

- YubiKey 4
- YubiKey 5 NFC
- YubiKey 5 Nano
- YubiKey 5C
- YubiKey 5C Nano
- YubiKey 5 NFC

为 U2F 启用 USB 重定 YubiKey 向

默认情况下，PCoIP 的 USB 重定向处于禁用状态 WorkSpaces；要使用 U2F 模式 YubiKeys，必须将其启用。

1. 确保已安装最新的 PCoIP WorkSpaces组策略管理模板（32 位）或 PCoIP（64 位）的WorkSpaces组策略管理模板（64 位）。
2. 在目录管理 WorkSpace 或已加入 WorkSpaces 目录的 Amazon EC2 实例上，打开组策略管理工具 (gpmc.msc) 并导航到 PC oIP 会话变量。
3. 要允许用户覆盖您的设置，请选择可覆盖的管理员默认值。否则，请选择 “管理员默认值不可覆盖”。
4. 打开启用/禁用 PCoIP 会话的 USB 设置。

5. 选择启用，然后选择确定。
6. 打开配置 PCoIP USB 允许和不允许的设备规则设置。
7. 选择启用，然后在输入 USB 授权表（最多十条规则）下，配置您的 USB 设备允许列表规则。
   a. 授权规则 - 110500407。此值是供应商 ID (VID) 和产品 ID (PID) 的组合。VID/PID 组合的格式为`1xxxxyyyy`，其中是十六进制格式的 VID，`xxxx`是十六进制格式`yyyy`的 PID。在本例中，1050 是 VID，0407 是 PID。如需了解更多 YubiKey USB 值，请参阅 YubiKeyUSB ID 值。
8. 在“输入 USB 授权表（最多十条规则）”下，配置您的 USB 设备黑名单规则。
   a. 对于取消授权规则，设置一个空字符串。这意味着仅允许授权列表中的 USB 设备。

> **Note**
>
> 您最多可以定义 10 条 USB 授权规则和最多 10 条 USB 取消授权规则。使用竖线 (|) 字符分隔多个规则。有关授权/取消授权规则的详细信息，请参阅 Terad ici PCoIP Windows 标准代理

9. 选择确定。
10. 组策略设置更改将在的下一次组策略更新之后 WorkSpace 以及会 WorkSpace 话重新启动后生效。要应用组策略更改，请执行下列操作之一：
    a. 重启 WorkSpace（在 Amazon WorkSpaces 控制台中，选择 WorkSpace，然后选择操作，重启 WorkSpaces）。
    b. 在管理命令提示符下，输入 gpupdate /force。
11. 设置生效后，除非通过 USB 设备规则设置配置了限制， WorkSpaces 否则所有支持的 USB 设备都可以重定向到。

为 U2F 启用 USB 重定向后，你就可以在 YubiKey Fido U2F 模式下使用你的 YubiKey USB 重定向。

成本优化

自助 WorkSpace 管理功能

在 Amazon 中 WorkSpaces，可以为用户启用自助 WorkSpace 管理功能，让他们能够更好地控制自己的体验。允许用户使用自助服务功能可以减少您的 IT 支持人员在 Amazon 上的工作量 WorkSpaces。启用自助服务功能后，它允许用户直接从适用于亚马逊的 Windows、macOS 或 Linux 客户端执行以下一项或多项任务： WorkSpaces

- 将其凭证缓存在其客户端上。这样，用户 WorkSpace 无需重新输入凭据即可重新连接到他们的。
- 重启他们 WorkSpace的。
- 在其上增加根卷和用户卷的大小 WorkSpace。
- 更改它们的计算类型（捆绑包） WorkSpace。
- 切换他们的运行模式 WorkSpace。
- 重建他们 WorkSpace的。

允许用户使用 “重新启动” 和 “重建” 选项不会持续产生任何成本影响 WorkSpaces。用户应注意，在重建过程进行时，他们 WorkSpace WorkSpace将会在长达一个小时的时间内无法使用。

增加卷大小、更改计算类型和切换运行模式的选项可能会产生额外费用 WorkSpaces。最佳做法是启用自助服务以减少支持团队的工作量。在确保已获得额外收费授权的工作流程中，应允许对额外费用项目进行自助服务。这可以通过专门的自助服务门户来实现 WorkSpaces，也可以通过与现有的信息技术服务管理 (ITSM) 服务集成，例如ServiceNow。

有关更多详细信息，请参阅为用户启用自助服务 WorkSpace 管理功能。有关如何为用户自助服务启用结构化门户的示例，请参阅使用自助服务门户自动化 WorkSpaces Amazon。

Amazon WorkSpaces 成本优化器

Amazon WorkSpaces 成本优化器解决方案会分析您的所有亚马逊 WorkSpaces 使用数据。根据您的使用情况，它会自动 WorkSpace 转换为最具成本效益的计费选项（按小时或按月）。该解决方案可帮助您监控 WorkSpace 使用情况并优化成本，并用于 AWS CloudFormation 自动配置和配置必要的 AWS 服务，以便每 24 小时分析一次使用情况并进行个人转换 WorkSpaces。最新版本 2.4 允许客户灵活地在现有 VPC 中部署解决方案，为区域和终止配置为可选。它还提高了计费工时计算的准确性，WorkSpaces 并增强了报告元数据。如果您之前部署了此解决方案的早期版本（v2.2.1 或更低版本），

请按照更新堆栈文档更新 Ama WorkSpaces zon Cost Optimizer CloudFormation 堆栈以获取该解决方案框架的最新版本。

的运行模式 WorkSpace 决定了它的即时可用性和计费。以下是当前的 WorkSpaces 运行模式：

AlwaysOn— 在支付固定的月费以无限使用时使用 WorkSpaces。此模式最适合将自己的桌面 WorkSpace 用作主桌面并需要随时访问正在运行 WorkSpace 的用户。

AutoStop— WorkSpaces 按小时付费时使用。使用此模式，在指定的非活动时间后 WorkSpaces 停止，并保存应用程序和数据的状态。要设置自动停止时间，请使用 AutoStop 时间（小时）。此模式最适合只需要兼职访问权限的用户 WorkSpaces。

最佳做法是监控使用情况，并使用诸如Amazon成本优化器 WorkSpaces之类的解决方案将亚马逊的运行模式设置为最具 WorkSpaces 成本效益的模式。此解决方案部署了 Amazon CloudWatch 事件规则，该规则每 24 小时调用一次AWS Lambda函数。

该解决方案可以在达到阈值后的任何一天将个人 WorkSpaces 从按小时计费模式转换为按月计费模式。如果解决方案将按小时计费转换为按月计费，则该解决方案要等 WorkSpace 到下个月初才会将按小时计费转换为按小时计费，并且前提是使用量低于阈值。 WorkSpace 但是，您可以随时使用 AWS Management Console 或 Amazon WorkSpaces API 手动更改账单模式。该解决方案的 AWS CloudFormation 模板包含用于运行这些转换的参数，并允许在试运行模式下运行解决方案以提供建议报告。

使用标签选择退出

为防止解决方案在计费模式 WorkSpace 之间进行转换，请 WorkSpace 使用标签密钥 Skip_Convert 和任何标签值将资源标签应用于计费模式。此解决方案将记录已标记 WorkSpaces，但不会转换已标记的内容 WorkSpaces。可以随时移除该标签以恢复自动转换 WorkSpace。有关更多详情，请参阅 Amazon WorkSpaces 成本优化器。

选择区域

默认情况下，此解决方案将通过扫描 WorkSpaces 在同一 AWS 账户中 WorkSpaces 在 Amazon 注册的目录来监控所有可用 AWS 区域。您可以在 “区域列表” 输入参数中提供要监控的 AWS 区域的 AWS 逗号分隔列表，以限制要监控的区域。

在现有 VPC 中部署

此解决方案需要 VPC 才能运行 ECS 任务。默认情况下，该解决方案将创建一个新的 VPC，但您可以通过在输入参数中提供子网 ID 和安全组 ID 来在现有 VPC 中进行部署。您当前的子网有一条通往互联网的路由，可让 ECS 任务提取托管在公共 Amazon ECR 存储库中的 Docker 镜像。

终止未使用的 WorkSpaces

此解决方案允许您在满足所有标准的当月最后一天终止未使用状态 WorkSpaces 。您可以通过将TerminateUnusedWorkSpaces输入参数更改为 CloudFormation 模板来选择使用此功能。最佳做法是在试运行模式下运行此功能几个月，然后查看月度报告以查看 WorkSpaces 标记为终止的内容。

针对亚马逊的 Amazon Connect 优化 WorkSpaces

联络中心客服的最终用户体验必须是重中之重，因为如果他们的音频质量下降，就会给他们所服务的客户带来糟糕的通话体验。在远程桌面中运行联络中心解决方案时，当语音流量不优先于网络连接时，音频性能将始终受到一定程度的影响。这种影响是由于音频从音频端点流向虚拟会话，然后通过流媒体协议进行压缩，然后传送给最终用户。这种额外的路由会导致音频因网络瓶颈而降低性能。

避免这种行为的一种方法是将音频从会话中分离出来，这意味着联络中心座席的所有资源都保留在会话中，而音频流则不在会话中。这种拆分允许音频从音频端点直接流向最终用户，而所有其他呼叫资源，包括代理正在查看的 PII，则保持在安全的会话中。这种音频优化被认为是一种最佳实践，因为它可以确保客户的通话体验尽可能好。

Amazon Connect 提供了 Streams API，允许管理员自定义其联系人控制面板 (CCP) 以满足其业务需求。管理员的选项之一是控制自定义 CCP 是否可以接收呼叫的音频。这些设置允许我们配置拆分 CCP；为会话外配置纯音频 CCP，为会话中配置无媒体 CCP。一旦管理员配置了这些自定义 CCP，他们就可以利用 Amazon Connect 音频优化来实现。 WorkSpaces由于 CCP 是在浏览器中传送的，因此此设置允许管理员向目录提供纯音频的 CCP URL。 WorkSpaces配置完成后，当 WorkSpaces Connect 联络中心座席成功向其进行身份验证时 WorkSpaces， WorkSpaces 客户端将在代理的本地默认浏览器中自动打开提供的纯音频的 CCP URL。此操作允许音频直接流到代理的本地计算机，而无媒体 CCP 则处理安全 WorkSpaces 会话中的其他所有内容。

架构示意图

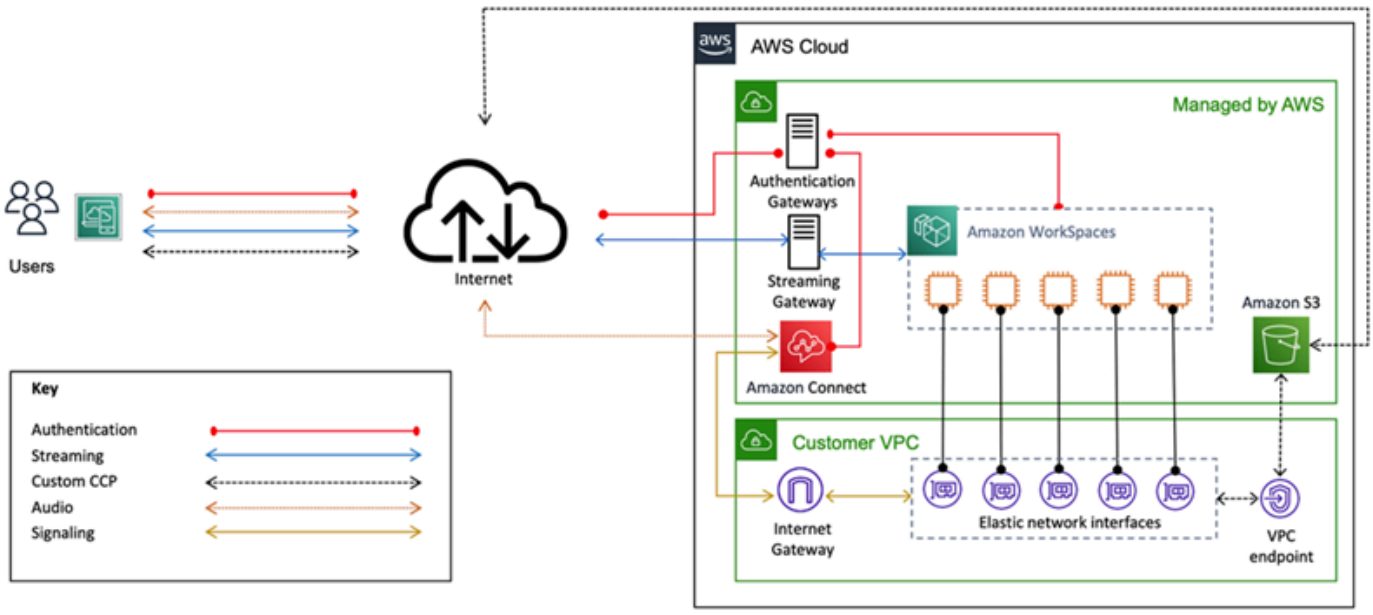

图 26 — Amazon Connect 和 WorkSpaces 架构图

故障排除

常见的管理和客户端问题，例如您的设备无法连接到 WorkSpaces 注册服务或无法 WorkSpace 使用交互式登录横幅连接等错误消息，可在《 Amazon WorkSpaces 管理指南》的 “客户端” 和 “管理员疑难解答” 页面上找到。

主题

- AD Connector 无法连接到活动目录
- 疑难解答 WorkSpace 自定义镜像创建错误
- 对 WorkSpace 标记为运行状况不佳的 Windows 进行故障排除
- 收集用于调试的 WorkSpaces 支持日志包
- 如何检查距离最近 AWS 区域的延迟

AD Connector 无法连接到活动目录

为了让 AD Connector 连接到本地目录，本地网络的防火墙必须为 VPC 中的两个子网的 CIDR 开放某些端口。请参阅场景 1：使用 AD Connector 对本地 Active Directory Service 进行代理身份验证。要测试是否满足这些条件，请执行以下步骤。

要测试连接，请执行以下操作：

1. 在 VPC 中启动一个 Windows 实例并通过 RDP 连接它。在 VPC 实例上执行剩余步骤。
2. 下载并解压缩DirectoryServicePortTest测试应用程序。如果需要，还包括源代码和 Microsoft Visual Studio 项目文件，用于修改测试应用程序。
3. 在 Windows 命令提示符下，使用以下选项运行 DirectoryServicePortTest 测试应用程序：

```
DirectoryServicePortTest.exe -d <domain_name>
-ip <server_IP_address> -tcp "53,88,135,139,389,445,464,636,49152" -udp
 "53,88,123,137,138,389,445,464" <domain_name>
```

<domain_name>— 完全限定的域名，用于测试林和域的功能级别。如果排除域名，则不会测试功能级别。

< server_IP_Address>-本地域中域控制器的 IP 地址。针对此 IP 地址对端口进行了测试。如果排除该 IP 地址，则不会测试端口。

此测试可确定从 VPC 到域的必要端口是否已打开。此外，该测试应用还验证最小的林和域功能级别。

疑难解答 WorkSpace 自定义镜像创建错误

如果 WorkSpace 已经启动并自定义了 Windows 或 Amazon Linux，则可以从中创建自定义映像 WorkSpace。自定义映像包含操作系统、应用程序软件和设置 WorkSpace。

查看创建 Windows 自定义映像的要求或创建 Amazon Linux 自定义映像的要求。映像创建需要满足所有先决条件才能开始创建映像。

要确认 Windows 是否 WorkSpace 满足创建映像的要求，我们建议运行图像检查器。Image Checker 会对图像的创建时间进行一系列测试，并就如何解决发现的任何问题提供指导。 WorkSpace 有关详细信息，请参阅安装和配置图像检查器。

WorkSpace 通过所有测试后，将出现 “验证成功” 消息。现在，您可以创建自定义捆绑包。否则，请解决导致测试失败和警告的所有问题，然后重复运行图像检查器的过程，直到 WorkSpace 通过所有测试。必须先解决所有故障和警告，然后才能创建映像。

有关更多信息，请按照提示解决图像检查器检测到的问题。

对 WorkSpace 标记为运行状况不佳的 Windows 进行故障排除

Amazon WorkSpaces 服务 WorkSpace 通过向其发送状态请求来定期检查其运行状况。如果未及时收到来自的回复，则会将其标记为 “ WorkSpace 不健康”。 WorkSpace 导致此问题的常见原因包括：

- 上的应用程序 WorkSpace 正在阻止 Amazon WorkSpaces 服务与之间的网络连接 WorkSpace。
- 上的 CPU 利用率很高 WorkSpace。
- 的计算机名称 WorkSpace 已更改。
- 响应 Amazon WorkSpaces 服务的代理或服务未处于运行状态。

以下故障排除步骤可以 WorkSpace 使恢复正常状态：

- 首先， WorkSpace从 Amazon WorkSpaces 控制台重启。如果重新启动 WorkSpace 无法解决问题，请使用 RDP，或者使用 SSH 连接到 A mazon Linux WorkSpace 。
- WorkSpace 如果无法通过其他协议访问，请 WorkSpace从 Amazon WorkSpaces 控制台重新构建。
- 如果无法建立 WorkSpaces 连接，请验证以下内容：

验证 CPU 利用率

使用 “打开任务管理器” WorkSpace 来确定 CPU 使用率是否较高。如果是，请尝试以下任一故障排除步骤来解决问题：

1. 停止任何消耗大量 CPU 的服务。
2. 将调整 WorkSpace 为比当前使用的计算类型更大的计算类型。
3. 重新启动 WorkSpace。

> **Note**
>
> 要诊断 CPU 使用率过高，以及如果上述步骤无法解决 CPU 使用率过高的问题，请参阅如何诊断 EC2 Windows 实例上的 CPU 使用率过高，如果我的 CPU 未受到限制，如何诊断 EC2 Windows 实例上的 CPU 使用率过高？

验证计算机的名称 WorkSpace

如果工作区的计算机名称已更改，请将其更改回原始名称：

1. 打开 Amazon WorkSpaces 控制台，然后展开 Unhealth WorkSpace y 以显示详细信息。
2. 复制计算机名称。
3. WorkSpace 使用 RDP 连接到。
4. 打开命令提示符，然后输入主机名以查看当前计算机名称。
   a. 如果名称与步骤 2 中的计算机名称匹配，请跳至下一个疑难解答部分。
   b. 如果名称不匹配，请输入 sysdm.cpl 打开系统属性，然后按照本节的其余步骤进行操作。
5. 选择 “更改”，然后粘贴步骤 2 中的 “计算机名称”。
6. 如果出现提示，请输入域用户凭证。
7. 确认SkyLightWorkspaceConfigService处于 “正在运行” 状态
   a. 在服务中，验证 WorkSpace服务是否SkyLightWorkspaceConfigService处于运行状态。如果不是，请启动该服务。

验证防火墙规则

确认 Windows 防火墙和任何正在运行的第三方防火墙都有允许使用以下端口的规则：

- 端口 4172 上的入站 TCP：建立直播连接。
- 端口 4172 上的入站 UDP：直播用户输入。
- 端口 8200 上的入站 TCP：管理和配置。 WorkSpace
- 端口 55002 上的出站 UDP：PCoIP 直播。

如果防火墙使用无状态筛选，则打开临时端口 49152-65535 以允许返回通信。

如果防火墙使用状态过滤，则临时端口 55002 已打开。

收集用于调试的 WorkSpaces 支持日志包

在对 WorkSpaces 问题进行故障排除时，必须从受影响的服务器 WorkSpace 和安装 WorkSpaces 客户端的主机处收集日志包。日志有两种基本类别：

- 服务器端日志：在这种情况下 WorkSpace 是服务器，所以这些日志是独立存在的 WorkSpace 。
- 客户端日志：最终用户用于连接的设备上的日志。 WorkSpace

- 只有 Windows 和 macOS 客户端在本地写入日志。
- 零客户端，iOS 客户端不登录。
- Android 日志在本地存储上进行加密，并自动上传到 WorkSpaces 客户工程团队。只有该团队才能查看 Android 设备的日志。

WSP 服务器端日志

所有 WSP 组件都将其日志文件写入以下两个文件夹之一：

- 主要位置：`C:\ProgramData\Amazon\WSP\`和 `C:\ProgramData\NICE\dcv\log\`
- 存档位置：`C:\ProgramData\Amazon\WSP\TRANSMITTED\`

在 Windows 上更改日志文件的详细程度

您可以通过配置日志详细级别组策略设置来大规模配置 WSP Windows WorkSpaces 的日志文件详细级别。

要更改个人日志文件的详细程度 WorkSpaces，请使用 Windows 注册表编辑器配置`h_log_verbosity_options`密钥：

1. 以管理员身份打开 Windows 注册表编辑器。
2. 导航到 \HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Amazon。
3. 如果WSP密钥不存在，请右键单击并选择 “新建” > “密钥” 并命名它WSP。
4. 导航到 \HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Amazon\WSP。
5. 如果该h_log_verbosity_options值不存在，请右键单击并选择 “新建” > “DWORD”，然后将其h_log_verbosity_options命名。
6. 单击新的 h_log_verbosity_options DWORD 并将值更改为以下数字之一，具体取决于所需的详细程度：
   - 0 — 错误
   - 1 — 警告
   - 2 — 信息
   - 3 — 调试
7. 选择确定，并关闭 Windows 注册表编辑器。
8. 重新启动 WorkSpace。

PCoIP 服务器端日志

所有 PCoIP 组件都将其日志文件写入以下两个文件夹之一：

- 主要位置：C:\ProgramData\Teradici\PCoIPAgent\logs
- 存档位置：C:\ProgramData\Teradici\logs

有时， AWS Support 在处理复杂问题时，需要将 PCoIP Server 代理置于详细日志模式。要启用它，请执行以下操作：

1. 打开以下注册表项：HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Teradici\PCoIP \pcoip_admin_defaults
2. 在pcoip_admin_defaults密钥中，创建以下 32 位 DWORD：pcoip.event_filter_mode
3. 将的值设置pcoip.event_filter_mode为 “3”（十进制或十六进制）。

作为参考，这些是可以在此 DWORD 中定义的日志阈值。

- 0 —（严重）

- 1 —（错误）
- 2 —（信息）
- 3 —（调试）

如果 pcoip_admin_default DWORD 不存在，则2默认情况下为日志级别。建议在 DWORD 不再需要冗余日志后将其恢复2为的值，因为这些日志要大得多，并且会不必要地消耗磁盘空间。

WebAccess 服务器端日志

对于 PCoIP 和 WSP（版本 1.0+）WorkSpaces， WorkSpaces Web Access 客户端使用 STXHD 服务。 WorkSpaces Web 访问的日志存储在C:\ProgramData\Amazon\Stxhd\Logs。

对于 WSP（版本 2.0+）WorkSpaces， WorkSpaces Web 访问的日志存储在。C:\ProgramData\Amazon\WSP\

客户端日志

这些日志来自用户连接的 WorkSpaces 客户端，因此日志位于最终用户的计算机上。Windows 和 Mac 的日志文件位置为：

- Windows："%LOCALAPPDATA%\Amazon Web Services\Amazon WorkSpaces\Logs"
- macOS：~/Library/"Application Support"/"Amazon Web Services"/"Amazon WorkSpaces"/logs
- Linux：~/.local/share/Amazon Web Services/Amazon WorkSpaces/logs

要帮助解决用户可能遇到的问题，请启用可在任何 Amazon WorkSpaces 客户端上使用的高级日志记录。在禁用之前，将为每个后续客户端会话启用高级日志记录。

1. 在连接到之前 WorkSpace，最终用户应为其 WorkSpaces 客户端启用高级日志记录。
2. 然后，最终用户应照常连接，使用他们的 WorkSpace，并尝试重现问题。
3. 高级日志记录将生成包含诊断信息和调试级别详细信息（包括详细的性能数据）的日志文件。

在明确关闭之前，此设置一直有效。用户成功重现详细登录问题后，应禁用此设置，因为它会生成较大的日志文件。

适用于 Windows 的自动服务器端日志包收集

该Get-WorkSpaceLogs.ps1脚本有助于快速收集服务器端日志包。 AWS Support可以通过在支持案例中请求脚本 AWS Support 来请求脚本：

1. 使用客户端或 WorkSpace 使用远程桌面协议 (RDP) 连接到。
2. 启动管理命令提示符（以管理员身份运行）。
3. 使用以下命令从命令提示符启动脚本：

```
powershell.exe -NoLogo -ExecutionPolicy RemoteSigned -NoProfile -File "C:\Program
 Files\Amazon\WorkSpacesConfig\Scripts\Get-WorkSpaceLogs.ps1"
```

4. 该脚本在用户的桌面上创建日志包。

   该脚本创建一个包含以下文件夹的 zip 文件：

   - C — 包含程序文件、程序文件 (x86) 和 Windows 中与 Skylight ProgramData、ec2Config、Teradici、事件查看器和 Windows 日志（Panther 等）相关的文件。
   - cliXML — 包含可用于交互式筛选的 XML 文件，这些文件可以导入 Powershell 中。Import-CliXML请参阅 Import -Clixml。
   - Config-所执行的每项检查的详细日志
   - ScriptLogs— 有关脚本执行的日志（与调查无关，但对于调试脚本的作用很有用）。
   - tmp —临时文件夹（应为空）。
   - 跟踪-在日志收集期间完成的数据包捕获。

如何检查距离最近 AWS 区域的延迟

C onnection Health Check 网站会快速检查是否 WorkSpaces 可以访问使用亚马逊的所有必需服务。它还会对每个有Amazon WorkSpaces 服务的 AWS 地区进行绩效检查，并让用户知道哪个区域最快。

结论

随着各组织努力提高灵活性、更好地保护数据并帮助员工提高工作效率，终端用户计算发生了战略转变。云计算已经实现的许多好处也适用于最终用户计算。通过使用 Amazon 将 Windows 或 Linux 桌面迁移到 AWS 云端 WorkSpaces，组织可以随着员工的增加而快速扩展，通过将数据拒之门外来改善安全状况，并为员工提供便携式桌面，使用他们选择的设备随时随地进行访问。

Amazon WorkSpaces 旨在集成到现有 IT 系统和流程中，本白皮书描述了这样做的最佳实践。遵循本白皮书中的指导方针的结果是实现了经济实惠的云桌面部署，该部署可以在 AWS 全球基础架构上随着您的业务而安全扩展。

贡献者

本文档的贡献者包括：

- 安德鲁·摩根，EUC 解决方案架构师，亚马逊 Web Services
- Don Scott，Amazon Web Services 高级欧洲委员会专业顾问
- Klaus Becker，Amazon Web Services 高级欧洲委员会专家解决方案架构师
- Naviero Magee，Amazon Web Services 首席解决方案架构师
- Robert Fountain，EUC 专业顾问，亚马逊 Web Services
- Stephen Stetler，Amazon Web Services 高级欧盟解决方案架构师

延伸阅读

如需了解其他信息，请参阅：

- 《亚马逊 WorkSpaces 管理指南》
- 《亚马逊 WorkSpaces 开发者指南》
- 亚马逊 WorkSpaces 客户
- WorkSpaces 使用 AWS OpsWorks Puppet Enterprise 管理亚马逊 Linux 2 亚马逊
- 自定义 Amazon Linux WorkSpace
- 如何使用客户端 LDAPS 提高 D AWS irectory Service 中的 LDAP 安全性
- 将 Amazon E CloudWatch vents WorkSpaces 与亚马逊搭配使用 AWS Lambda ，提高车队知名度
- 亚马逊如何 WorkSpaces 使用 AWS KMS
- AWS CLI 命令参考 — WorkSpaces
- 监控 Amazon WorkSpaces 指标
- MATE 桌面环境
- 解决 AWS Directory Service 管理问题
- 对亚马逊 WorkSpaces 管理问题进行故障排除
- Amazon WorkSpaces 客户机问题疑难解答
- 使用自助服务门户实现亚马逊 WorkSpaces 自动化

文档修订

如需获取有关该白皮书更新的通知，请订阅 RSS 源。

变更	说明	日期
次要更新	更新了 AD 目录服务、灾难恢复/业务连续性和跨区域重定向的内容。添加了 Amazon WorkSpaces Connect 音频优化。对格式进行了次要更新。	2022 年 5 月 26 日
次要更新	修复非包容性语言。	2022 年 4 月 6 日
已更新白皮书	更新的内容	2022 年 3 月 24 日
已更新白皮书	更新了 AWS Network Firewall、MAD 复制目录、YubiKey 支持、容器、WSL v1、智能卡支持、 WorkSpaces 服务配额和可信设备的内容。	2021 年 12 月 20 日
已更新白皮书	更新了 WorkSpaces 流媒体协议、智能卡身份验证、图表、客户端部署、终端设备选择和 Web 访问的内容	2021 年 4 月 28 日
已更新白皮书	更新的内容	2020 年 12 月 1 日
已更新白皮书	自首次发布以来更新了内容并添加了新的图表。	2020 年 5 月 1 日
初次发布	首次出版。	2016年7月1日

版权声明

客户有责任对本文档中的信息进行单独评测。本文件：(a) 仅供参考，(b) 代表当前 AWS 的产品供应和做法，如有更改，恕不另行通知，以及 (c) 不产生其关联公司、供应商或许可方的任何承诺或保证。AWS AWS 产品或服务 “按原样” 提供，不附带任何形式的担保、陈述或条件，无论是明示还是暗示。对客户的责任和责任由 AWS 协议控制，本文档不属于其客户之间的任何协议，也不会对其 AWS 进行修改。 AWS

AWS 词汇表

有关最新 AWS 术语，请参阅《AWS 词汇表 参考资料》中的AWS 词汇表。

本文属于机器翻译版本。若本译文内容与英语原文存在差异，则一律以英文原文为准。