部署 Amazon WorkSpaces 的最佳实践

网络访问、目录服务和安全性

2016 年 7 月

声明

本文档仅用于参考。本文档代表截至其发行之日的 AWS 的最新产品服务和实践，如有变更，恕不另行通知。客户负责对此文件的信息以及对 AWS 的产品或服务的任何使用进行自我独立的评估，每项产品或服务均按“原样”提供，且不提供任何类型的保证，不管是明示还是暗示。本文档不形成 AWS、其附属公司、供应商或许可方的任何保证、表示、合同承诺、条件或担保。AWS 对其客户承担的责任和义务受 AWS 协议制约，本文档不是 AWS 与客户之间的协议的一部分，也不构成对该协议的修改。

目录

摘要

本白皮书概述了部署 Amazon WorkSpaces 的一系列最佳实践。本文涵盖了网络方面的考量、目录服务和用户身份验证、安全性以及监控和记录。

本文件分为四个类别，以便您快速查阅相关信息。本文件的目标受众是网络工程师、目录工程师或安全工程师。

介绍

Amazon WorkSpaces 是云中的托管桌面计算服务。Amazon WorkSpaces 消除了采购/部署硬件或安装复杂软件的负担，并提供了便捷的桌面体验：您可以利用 AWS 管理控制台中方便的点击操作、使用 AWS 命令行界面 (CLI) 或使用 API 完成任务。借助 Amazon WorkSpaces，您可在数分钟内启动一个桌面，并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：

- 通过使用 AWS Directory Service：AD Connector 充分发挥现有的本地 Microsoft Active Directory (AD) 优势。
- 将您的目录拓展到 AWS 云。
- 借助 AWS Directory Service — Microsoft AD 或 Simple AD — 构建托管目录，以管理您的用户和 WorkSpaces。

此外，您还可以利用本地部署或云托管 RADIUS 服务器及 AD Connector 为您的 WorkSpaces 提供多重身份验证 (MFA) 功能。

您可以使用 CLI 或 API 将 Amazon WorkSpaces 集成到现有的预配置工作流程中，实现 Amazon WorkSpaces 的自动预配置。

出于安全考虑，除了 WorkSpaces 服务提供的集成网络加密功能外，您还可以为自己的 WorkSpaces 启用静态加密（请参阅安全章节中的加密的 WorkSpaces）。

您可以使用现有的本地部署工具（如 Microsoft System Center Configuration Manager (SCCM)）或借助 Amazon WorkSpaces Application Manager (Amazon WAM) 将应用程序部署到自己的 WorkSpaces 上。

下面的章节将详细介绍 Amazon WorkSpaces，讲解该服务的工作原理，说明启动该服务前的准备工作，并列出您可以使用的选项和功能。

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**。支持 Amazon WorkSpaces 的客户端设备。完整列表见：支持的平台和设备。

  此外，您还可以使用 Personal Computer over Internet Protocol (PCoIP) 零客户端连接 WorkSpaces。有关可用设备的列表，请参阅适用于 Amazon WorkSpaces 的 PCoIP 零客户端。

- **对用户进行身份验证并提供到其 WorkSpace 的访问的目录服务**。目前，Amazon WorkSpaces 可与 AWS Directory Service 和 Active Directory 同时使用。您可以使用装有 AWS Directory Service 的本地部署 Active Directory 服务器来为现有的企业用户凭证提供 WorkSpaces 支持。

- **用于运行 Amazon WorkSpaces 的 Amazon Virtual Private Cloud (Amazon VPC)**。要部署 WorkSpaces，您需要配置至少两个子网，因为在多可用区部署中，每个 AWS Directory Service 构造都需要两个子网。

网络方面的考量

每个 WorkSpace 都与某个特定的 Amazon VPC 及您用来创建它的 AWS Directory Service 构造相关联。所有 AWS Directory Service 构造（Simple AD、AD Connector 和 Microsoft AD）都需要两个子网才能正常工作，每个子网都位于不同的可用区中。子网永久附属于某个 Directory Service 构造，且在 AWS Directory Service 创建后无法修改。因此，在创建 Directory Services 构造之前，您首先要确定适当的子网大小。在创建子网前，请仔细考虑以下事项：

- 您日后会用到多少个 WorkSpaces？预计其增长性如何？
- 您需要适应哪些类型的用户？
- 您将连接多少个 Active Directory 域？
- 您的企业用户账户在何处？

Amazon 建议您在规划流程时根据访问类型和用户身份验证需求定义用户组或角色。当您需要限制针对特定应用程序或资源的访问时，这些答案非常有用。定义的用户角色可帮助您利用 AWS Directory Service、网络访问控制列表、路由表和 VPC 安全组来分段或限制访问。每个 AWS Directory Service 构造使用两个子网，并将相同的设置应用到从该构造启动的所有 WorkSpaces。例如，您可以使用应用于挂载到某个 AD Connector 的所有 WorkSpaces 的安全组来指定是否需要 MFA 身份验证功能，或最终用户能否拥有其 WorkSpace 的本地管理员访问权限。

> **注意** 每个 AD Connector 都连接到一个 Microsoft Active Directory 组织单位 (OU)。您必须构造自己的 Directory Service，以认真考虑用户角色，从而充分发挥该功能的优势。

本章节介绍有关调整 VPC 及子网、流量大小的最佳实践，以及目录服务设计的影响。

VPC 设计

在为您的 Amazon WorkSpaces 设计 VPC、子网、安全组、路由策略和网络 ACL 时，您需要仔细考虑以下事项，以便构建可扩展、安全且易于管理的 WorkSpaces 环境：

- **VPC**。我们建议为您的 WorkSpaces 部署使用专用的 VPC。利用专用的 VPC，您可以进行流量分离，从而为 WorkSpaces 指定必要的管理和安全“护栏”。
- **目录服务**。每个 AWS Directory Service 构造都需要一对子网来提供在 Amazon 可用区之间分离的高可用目录服务。
- **子网大小**。WorkSpaces 部署与目录构造绑定在一起，并与您选择的 AWS Directory Service 位于相同的 VPC 子网上。请考虑以下事项：
  - 子网大小是永久的，不可更改；您应预留充足的空间，以适应未来增长。
  - 您可以为自己选择的 AWS Directory Service 指定默认安全组；安全组应用于与特定 AWS Directory Service 构造关联的所有 WorkSpaces。
  - 您可以让多个 AWS Directory Services 使用同一个子网。

设计 VPC 时，请考虑到未来的规划。例如，您可能想要增加防病毒服务器、补丁管理服务器或 Active Directory、RADIUS MFA 服务器等管理组件。在 VPC 设计中多预留一些 IP 地址以适应此类需求是非常有益的。

有关 VPC 设计和子网大小调整的深入指导和注意事项，请参阅 **re:Invent** 演讲：Amazon.com 如何移至 Amazon WorkSpaces。

网络接口

每个 WorkSpace 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 使用管理网络接口管理 WorkSpace；您的客户端连接终止于该接口。AWS 为该接口使用私有 IP 地址范围。为使网络路由正常工作，您不能在可与 WorkSpaces VPC 通信的任何网络上使用该私有地址空间。

有关我们在各个区域使用的私有 IP 范围的列表，请参阅 Amazon WorkSpaces 详细信息。

注意 Amazon WorkSpaces 及其关联的管理网络接口不在您的 VPC 中，您无法在 AWS 管理控制台中查看该管理网络接口或 Amazon Elastic Compute Cloud (Amazon EC2) 实例 ID（请参阅图 4、图 5 和图 6）。但是，您可以在 AWS 管理控制台中查看和修改主网络接口 (eth1) 的安全组设置。此外，每个 WorkSpace 的主网络接口不计入您的 ENI Amazon EC2 资源限制。对于大型 WorkSpaces 部署，您需要通过 AWS 管理控制台提交支持服务单，以提高 ENI 限制。

流量

您可以将 Amazon WorkSpaces 流量分为以下两个主要部分：

- 客户端设备与 Amazon WorkSpace 服务之间的流量
- Amazon WorkSpace 服务与客户网络流量之间的流量

我们将在下一章节中对这些内容进行讨论。

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来连接 WorkSpaces 服务。客户端使用 https 端口 443 来进行所有身份验证及会话相关信息的通信，并使用端口 4172（PCoIP 端口）通过 TCP 和 UDP 通信方式来将像素流式传输到给定的 WorkSpace 以及进行网络运行状况检查。这两个端口上的流量都是加密的。端口 443 的流量用于身份验证和会话信息，并借助 TLS 对流量进行加密。像素流式传输流量通过流式处理网关对客户端与 WorkSpace 的 eth0 之间的通信进行 AES 256 位加密。有关更多信息，请参阅本文稍后的安全性章节。

我们公布了 PCoIP 流式处理网关和网络运行状况检查终端节点的 IP 范围（按区域划分）。您可以在端口 4172 上只开放目标为您使用的 Amazon WorkSpaces 所在的 AWS 区域的出站流量，从而对端口 4172 上从公司网络到 AWS 流式处理网关和网络运行状况检查终端节点的出站流量进行限制。有关 IP 范围和网络运行状况检查终端节点的信息，请参阅 Amazon WorkSpaces PCoIP 网关 IP 范围。

Amazon WorkSpaces 客户端内置了网络状态检查工具。该实用程序通过位于应用程序右下角处的状态指示灯来告知用户其网络能否支持连接。选择客户端右下角处的 **Network** 可以打开更详细的网络状态视图，如图 1 所示。

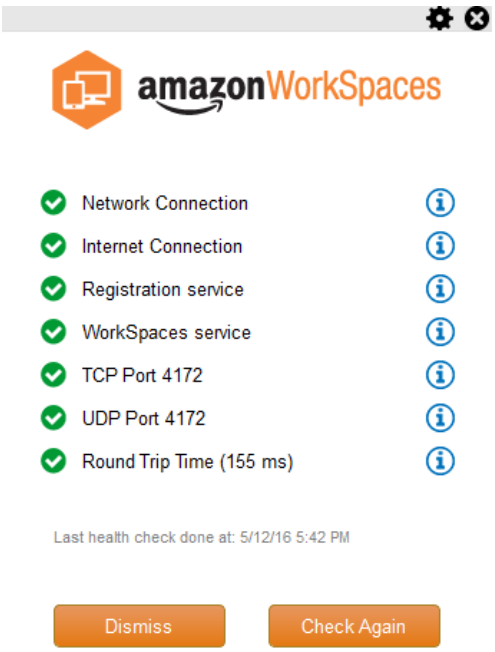

图 1：WorkSpaces 客户端 - 网络检查

用户通过提供 Directory Service 构造使用的目录的登录信息（通常为公司目录）来发起从客户端到 WorkSpaces 服务的连接。登录信息通过 https 发送到 WorkSpace 所在区域的 Amazon WorkSpaces 服务的身份验证网关。然后，Amazon WorkSpaces 服务的身份验证网关将该流量转发到与您的 WorkSpace 关联的特定 AWS Directory Service 服务构造。例如，使用 AD Connector 时，AD Connector 将身份验证请求直接转发到您的 Active Directory 服务；后者可以部署在本地，也可以位于 AWS VPC 中（请参阅 AD DS 部署方案）。AD Connector 不存储任何身份验证信息，其充当的是无状态代理的角色。因此，首先需要为 AD Connector 配置到 Active Directory 服务器的连接。AD Connector 使用您在创建它时定义的 DNS 服务器，这决定了其能够连接的 Active Directory 服务器。

如果您使用的是 AD Connector 并在目录上启用了 MFA，则在对目录服务进行身份验证之前，系统需要先检查 MFA 令牌。如果 MFA 验证失败，则系统不会将用户的登录信息转发到 AWS Directory Service。

如果用户通过身份验证，则系统利用端口 4172（PCoIP 端口）经由 AWS 流式处理网关向 WorkSpace 发送流式传输流量。在整个会话期间，会话相关信息仍通过 https 进行交换。流式传输流量将使用 WorkSpace 上未连接到您的 VPC 的第一个 ENI（WorkSpace 上的 eth0）。AWS 会对从流式传输网关到 ENI 的网络连接进行管理。一旦从流式传输网关到 WorkSpaces 流式传输 ENI 的连接出现故障，系统将生成一个 CloudWatch 事件（请参阅本白皮书的使用 Amazon CloudWatch 进行监控或记录日志章节）。

在 Amazon WorkSpaces 服务与客户端之间发送的数据量取决于像素活动的级别。为确保用户获得最佳的体验，我们建议使 WorkSpaces 客户端与 WorkSpaces 所在的 AWS 区域之间的往返时间 (RTT) 低于 100 ms。通常，这意味着您的 WorkSpaces 客户端应位于距托管 WorkSpace 的区域不到 2000 英里的地方。我们提供了一个连接运行状况检查网页，以供您确定最适合 Amazon WorkSpaces 服务连接的 AWS 区域。

Amazon WorkSpaces 服务到 VPC

当从客户端到 WorkSpace 的连接通过身份验证且已发起流式传输流量后，WorkSpaces 客户端会显示连接到您的 VPC 的 Windows 桌面 (WorkSpace)，您的网络应会显示已建立连接。您的 VPC 提供的动态主机配置协议 (DHCP) 服务会为 WorkSpace 的主 ENI（以 eth1 标识）分配一个 IP 地址，通常与您的 AWS Directory Service 处于相同的子网中。在 WorkSpace 的生命周期内，该 IP 地址一直为该 WorkSpace 所有。您的 VPC 中的 ENI 有权访问该 VPC 中的任何资源，以及已连接到您的 VPC 的任何网络（通过 VPC 对等连接、AWS Direct Connect 连接或 VPN 连接）。

对您的网络资源的 ENI 访问由您的 AWS Directory Service 为每个 WorkSpace 配置的默认安全组（点击此处可了解有关安全组的更多信息）及您为该 ENI 分配的任何其他安全组决定。您可以通过 AWS 管理控制台或 CLI 向面向您的 VPC 的 ENI 随意添加安全组。除安全组外，您还可以在给定的 WorkSpace 上使用您偏好的基于主机的防火墙，以限制对 VPC 中资源的网络访问。

AD DS 部署方案（本白皮书中稍后的章节）中的图 4 显示了之前讲述的流量。

典型配置示例

我们来考虑这样一个场景：您有两类用户，AWS Directory Service 使用集中式 Active Directory 来进行用户身份验证：

- **需要在任意位置进行完全访问的工作人员**（例如：全职员工）。这些用户拥有对 Internet 和内部网络的完全访问权限，他们能够从 VPC 穿过防火墙连接到本地网络。
- **只能从公司网络内部进行有限访问的工作人员**（例如：合同工及顾问）。这些用户能在 VPC 中通过代理服务器对特定的网站进行有限的 Internet 访问，且只能在 VPC 和本地网络中进行有限的网络访问。

您需要全职员工在其 WorkSpace 上拥有本地管理员访问权限（以便安装软件），并打算通过 MFA 强制实施双重身份验证。此外，您还需要全职员工能够从其 WorkSpace 自由地访问 Internet。

对于合同工，您需要阻止本地管理员访问权限，使其只能使用特定的预装应用程序。您需要通过安全组为这些 WorkSpaces 应用限制性非常高的网络访问控制。您需要只针对特定的内部网站开放端口 80 和 443，并阻止他们访问 Internet。

在该场景中，有两种完全不同的用户角色类型，它们具有不同的网络和桌面访问需求。最佳实践是分别对其 WorkSpaces 进行管理和配置。为此，您需要创建两个 AD Connector，并将它们分别用于不同的用户角色。每个 AD Connector 都需要拥有两个子网，子网必须包含充足的 IP 地址，以满足您的 WorkSpaces 使用率增长预期。

> **注意** 每个 AWS VPC 子网都需要五个 IP 地址（前四个及最后一个 IP 地址）来进行管理，每个 AD Connector 在其所在的每个子网中占用一个 IP 地址。

对于该场景，您还需要考虑以下事项：

- AWS VPC 子网应为私有子网，以便能够通过 NAT 网关、云中的代理-NAT 服务器对流量（如 Internet 访问）进行控制，或通过本地部署的流量管理系统路由流量。

- 为本地网络的所有 VPC 流量设置一个防火墙。
- Microsoft Active Directory 服务器和 MFA RADIUS 服务器为本地部署（请参阅方案 1：使用 AD Connector 代理到本地部署 AD DS 的身份验证）或 AWS 云实施的一部分（请参阅方案 2 和 3，AD DS 部署方案）。

考虑到所有 WorkSpaces 都会被授予某种形式的 Internet 访问权限且它们将托管在私有子网中，您还需要创建可通过 Internet 网关访问 Internet 的公有子网。您需要为全职员工配置一个 NAT 网关，以便他们能够访问 Internet，并为合同工和顾问配置一个代理-NAT 服务器，以使他们只能访问特定的内部网站。为实现故障恢复、高可用性并限制跨可用区的流量费用，您应在多可用区部署中的两个不同子网中配置两个 NAT 网关和 NAT 或代理服务器。您选择用作公有子网的两个可用区将与您在具有多个可用区的区域中为 WorkSpaces 子网使用的两个可用区匹配。您可以将来自每个 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。图 2 显示了该 VPC 的配置。

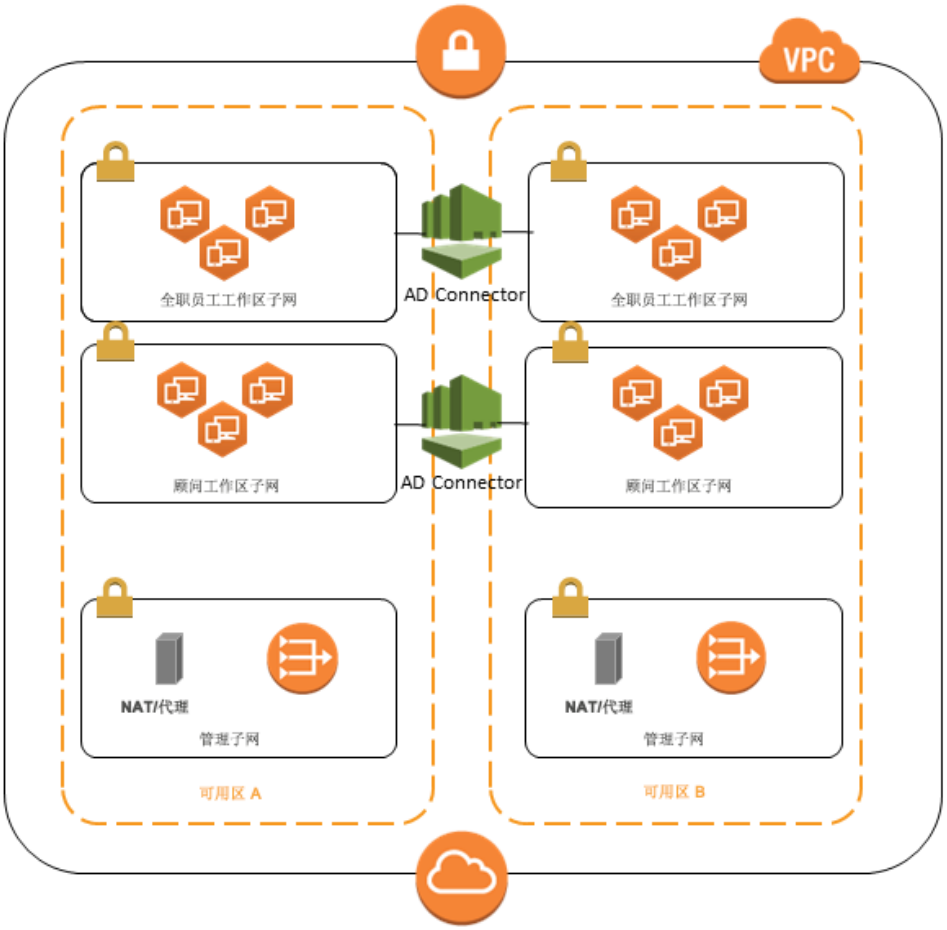

图 2：高层次的 VPC 设计

下述信息介绍如何配置早前提到的两种不同的 WorkSpaces 类型。

- **全职员工：**在 Amazon WorkSpaces 管理控制台中，选择菜单栏上的 **Directories** 选项，选择托管全职员工的目录，然后选中 **Local Administrator Setting**。启用该选项后，任何新创建的 WorkSpace 都将具有本地管理员权限。要授予 Internet 访问权限，您应为来自您的 VPC 的出站 Internet 访问配置网络地址转换 (NAT)。要启用 MFA，您需要指定 RADIUS 服务器、服务器 IP、端口及预共享密钥。

  对于全职员工的 WorkSpaces，到该 WorkSpace 的入站流量将限制为来自 Helpdesk 子网的远程桌面协议 (RDP)（通过 AD Connector 设置应用默认安全组来达到这一目的）。

- **合同工和顾问：**在 Amazon WorkSpaces 管理控制台中，禁用 **Internet Access** 和 **Local Administrator Setting**。然后，在 **Security Group** 设置部分下方添加安全组，以将安全组应用到在该目录下创建的所有新 WorkSpaces。

  对于顾问的 WorkSpaces，通过 AD Connector 设置将默认的安全组应用到与该 AD Connector 关联的所有 WorkSpaces，以限制该 WorkSpaces 的出站和入站流量。该安全组会阻止该 WorkSpaces 对除 HTTP 和 HTTPS 流量以外的任何资源进行出站访问，以及从本地网络的 Helpdesk 子网到 RDP 的入站流量。

注意 该安全组只对位于 VPC 中的 ENI（WorkSpace 上的 eth1）有效，安全组无法限制从 WorkSpaces 客户端到 WorkSpace 的访问。图 3 显示了早前介绍的 WorkSpaces VPC 的最终设计。

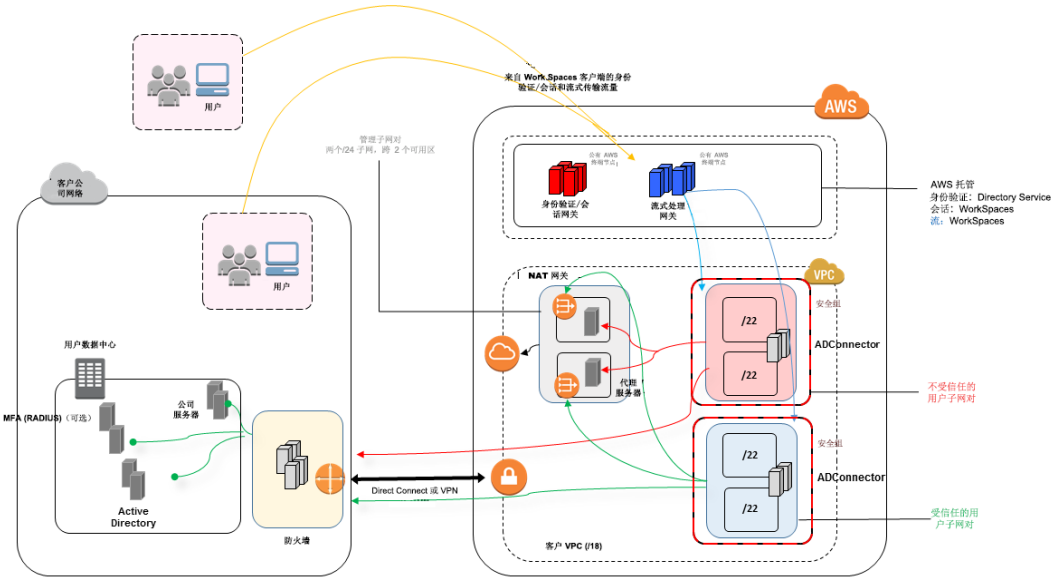

图 3：具有用户角色的 WorkSpaces 设计

AWS Directory Service

如“介绍”部分所述，AWS Directory Service 是 Amazon WorkSpaces 的基础。利用 AWS Directory Service，您可以创建三种类型的目录。前两种位于 AWS 云中：

- 用于 Microsoft Active Directory 企业版（即 **Microsoft AD**）的 AWS Directory Service，由 Microsoft Active Directory 管理并由 Windows Server 2012 R2 提供支持。
- **Simple AD**，是一种独立的、兼容 Microsoft Active Directory 的托管目录服务，由 Samba 4 提供支持。

第三种是 **AD Connector** — 一种目录网关，让您能够代理身份验证请求，并对现有的本地部署 Microsoft Active Directory 执行用户或组查找。

下一个章节介绍 Amazon WorkSpaces 代理服务与 AWS Directory Service 之间的身份验证的通信流程，利用 AWS Directory Service 实现 WorkSpaces 的最佳实践，以及 MFA 等高级概念。此外，我们还将讨论大规模 Amazon WorkSpaces 的基础设施架构概念，对于 Amazon VPC 的要求，以及 AWS Directory Service，包括与本地部署 Microsoft Active Directory Domain Services (AD DS) 的集成。

AD DS 部署方案

AWS Directory Service 是 Amazon WorkSpaces 的基础，因此，合理地设计和部署目录服务至关重要。以下三种方案基于 *Microsoft Active Directory Domain Services* 快速入门指南构建，它详细介绍了有关 AD DS 部署选项的最佳实践，特别是与 WorkSpaces 的集成。本章的 *设计注意事项* 小节介绍了将 AD Connector 用于 WorkSpaces 时的具体要求和最佳实践，这是整个 WorkSpaces 设计概念的一部分。

- **方案 1：使用 AD Connector 代理到本地部署 AD DS 的身份验证。**在此方案中，客户处将部署网络连接 (VPN/Direct Connect (DX))，并通过 AWS Directory Service (AD Connector) 代理到客户本地部署 AD DS 的所有身份验证。
- **方案 2：将本地部署 AD DS 扩展到 AWS（副本）。**此方案类似于方案 1，但其在 AWS 上部署了客户 AD DS 的副本并配合 AD Connector 使用，从而减少了到 AD DS 和 AD DS 全局目录的身份验证/查询请求的延迟。

- **方案 3：使用 AWS Directory Service 在 AWS 云中进行独立的隔离部署。**这是一种隔离方案，不包含反过来连接客户进行身份验证的过程。这种方法需要用到 AWS Directory Service (Microsoft AD) 和 AD Connector。虽然此方案不依赖于连接客户来进行身份验证，却为需要 VPN 或 DX 的应用程序流量提供了配置。

方案 1：使用 AD Connector 代理到本地部署 AD DS 的身份验证

此方案适用于不想将本地部署 AD DS 扩展到 AWS 或无法部署新 AD DS 的客户。图 4：AD Connector 到本地部署 Active Directory 概述了每个组件并展示了用户的身份验证流程。

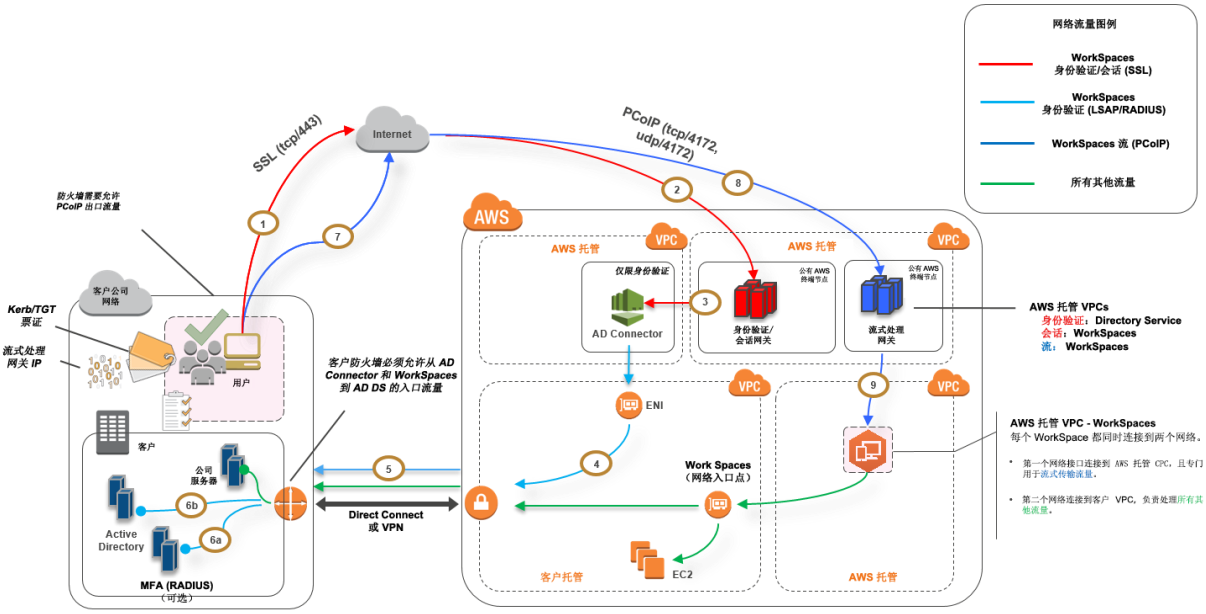

图 4：AD Connector 到本地部署 Active Directory

在此方案中，AWS Directory Service (AD Connector) 将用于通过 AD Connector 代理到客户本地部署 AD DS (图 5) 的所有用户或 MFA 身份验证。有关用于身份验证流程的协议或加密的详细信息，请参阅本白皮书的安全性章节。

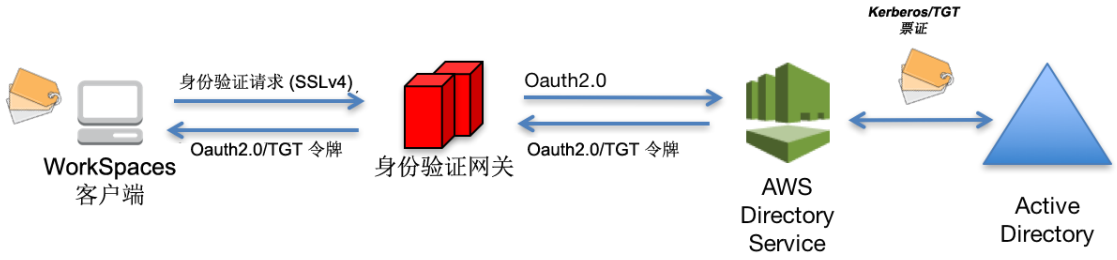

图 5：通过身份验证网关进行用户身份验证

方案 1 展示了一种混合架构，即客户可能已在 AWS 中拥有资源，并且在本地部署数据中心也拥有可通过 WorkSpaces 访问的资源。客户可以借助其现有的本地部署 AD DS 和 RADIUS 服务器进行用户和 MFA 身份验证。

该架构使用以下组件或构造。

Amazon Web Services：

- **Amazon VPC：**创建一个具有至少两个私有子网（跨两个可用区）的 Amazon VPC。
- **DHCP 选项集：**创建一个 Amazon VPC DHCP 选项集。这允许定义客户指定的域名和域名服务器 (DNS)（本地部署服务）。（有关更多信息，请参阅 DHCP 选项集。）
- **Amazon 虚拟专用网关：**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：**将 AD Connector 部署到一对 Amazon VPC 私有子网中。
- **Amazon WorkSpaces：**将 WorkSpaces 部署到 AD Connector 所在的私有子网中（请参阅设计注意事项，AD Connector）。

客户：

- **网络连接：**公司 VPN 或 Direct Connect 终端节点。
- **AD DS：**公司 AD DS。
- **MFA（可选）：**公司 RADIUS 服务器。

- **最终用户设备：**公司或 BYOL 最终用户设备（如 Windows、Mac、iPad 或 Android 平板电脑、零客户端、Chromebook），用于访问 Amazon WorkSpaces 服务（请参阅支持的平台和设备）。

虽然该解决方案非常适合不想将 AD DS 部署到云中的客户，但它有一些缺陷。

- **依赖于连接：**如果与数据中心的连接丢失，则所有用户都将无法登录其各自的 WorkSpaces，现有连接会保持活动状态并持续 Kerberos/TGT 的有效时间。
- **延迟：**如果连接存在延迟（VPN 比 DX 更易出现这种情况），则 WorkSpaces 身份验证及任意 AD DS 相关活动（如组策略 (GPO) 实施）都将花费更长的时间。
- **流量成本：**所有身份验证都必须遍历 VPN 或 DX 链接，因此，它依赖于连接的类型。这将归入从 Amazon EC2 到 Internet 的“数据传出”或“数据传出 (DX)”。

> **注意** AD Connector 是一种代理服务。它不存储也不缓存用户凭证。所有的身份验证、查找、管理请求都由您的 Active Directory 进行处理。您的目录服务中需要存在具有委派权限的账户，且其拥有读取所有用户信息和将计算机加入域的权限。

有关如何在您的目录中为 AD Connector 配置用户的详细信息，请参阅委派连接权限。

一般说来，WorkSpaces 体验高度依赖于图 4 中所示的项目 5。

方案 2：将本地部署 AD DS 扩展到 AWS（副本）

此方案类似于方案 1，但方案 2 会在 AWS 上部署客户 AD DS 的副本并配合 AD Connector 使用。这减少了到 AD DS 的身份验证或查询请求的延迟。图 6 展示了各个组件及用户身份验证流程的高层次视图。

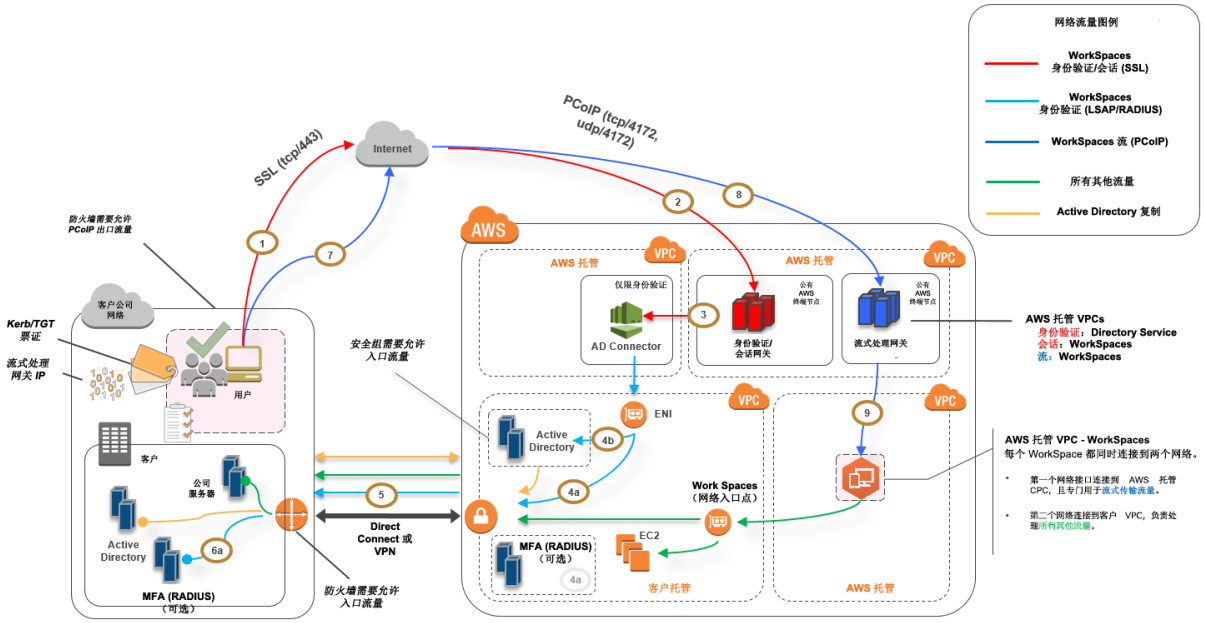

图 6：将客户 Active Directory 域扩展到云

与方案 1 一样，AD Connector 用于所有用户或 MFA 身份验证，其又通过代理连接到客户 AD DS（图 5）。在方案 2 中，客户 AD DS 跨 Amazon EC2 实例上的可用区进行部署 — 此处的 Amazon EC2 实例是指被提升为客户本地部署 Active Directory 林中的域控制器并在 AWS 云中运行的实例。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 AWS 云中部署 AD DS 的最佳实践，请参阅本白皮书中稍后的设计注意事项章节。

待 WorkSpaces 实例部署完成后，其将能够访问该基于云的域控制器，从而实现安全、低延迟的目录服务和 DNS。不管在私有子网中，还是跨客户 VPN 隧道或 DX，所有网络流量（包括 AD DS 通信、身份验证请求、Active Directory 复制）都是安全的。

该架构使用以下组件或构造。

Amazon Web Services：

- **Amazon VPC：**创建一个具有至少四个私有子网（跨两个可用区）的 Amazon VPC（两个子网用于客户 AD DS，另两个用于 AD Connector 或 WorkSpaces）。
- **DHCP 选项集：**创建一个 Amazon VPC DHCP 选项集。这让您能够定义客户指定的域名和 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：**通过 IPsec VPN 隧道或 AWS Direct Connect 连接与您自己的网络进行通信。
- **Amazon EC2：**
  - 在专用私有 VPC 子网中的 Amazon EC2 实例上部署的客户公司 AD DS 域控制器。
  - 用于 MFA 的客户“可选”RADIUS 服务器。
- **AWS Directory Services：**将 AD Connector 部署到一对 Amazon VPC 私有子网中。
- **Amazon WorkSpaces：**将 WorkSpaces 部署到 AD Connector 所在的私有子网中（请参阅设计注意事项，AD Connector）。

客户：

- **网络连接：**公司 VPN 或 AWS Direct Connect 终端节点。
- **AD DS：**公司 AD DS（复制时必需）。
- **MFA“可选”：**公司 RADIUS 服务器。
- **最终用户设备：**公司或 BYOL 最终用户设备（如 Windows、Mac、iPad 或 Android 平板电脑、零客户端、Chromebook），用于访问 Amazon WorkSpaces 服务（请参阅支持的平台和设备）。

此解决方案没有方案 1 的缺陷。因此，WorkSpaces 和 AWS Directory Service 不依赖于连接到位。

- **对连接的依赖：**如果与客户数据中心的连接丢失，最终用户可继续工作，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（请参阅 *设计注意事项：*AD DS 站点和服务），所有身份验证都在本地进行，延迟极低。
- **流量成本：**在此方案中，身份验证在本地处理，只有 AD DS 复制操作必须遍历 VPN 或 DX 链接，从而减少了数据传输。

一般说来，WorkSpaces 体验更好，且不过度依赖图 6 中所示的项目 5。当您需要将 WorkSpaces 扩展到成千上万的桌面时，特别是在关系到 AD DS 全局目录查询时，由于该流量局限在 WorkSpaces 本地环境中，这一点会更加明显。

方案 3：使用 AWS Directory Service 在 AWS 云中进行独立的隔离部署

此方案（如图 7 所示）将 AD DS 部署在 AWS 云中的独立隔离环境中。此方案只使用 AWS Directory Service。您不需要全面管理 AD DS，而是依赖于 AWS Directory Service 来完成此类任务，例如：构建高度可用的目录拓扑、监测域控制器、配置备份和快照等。

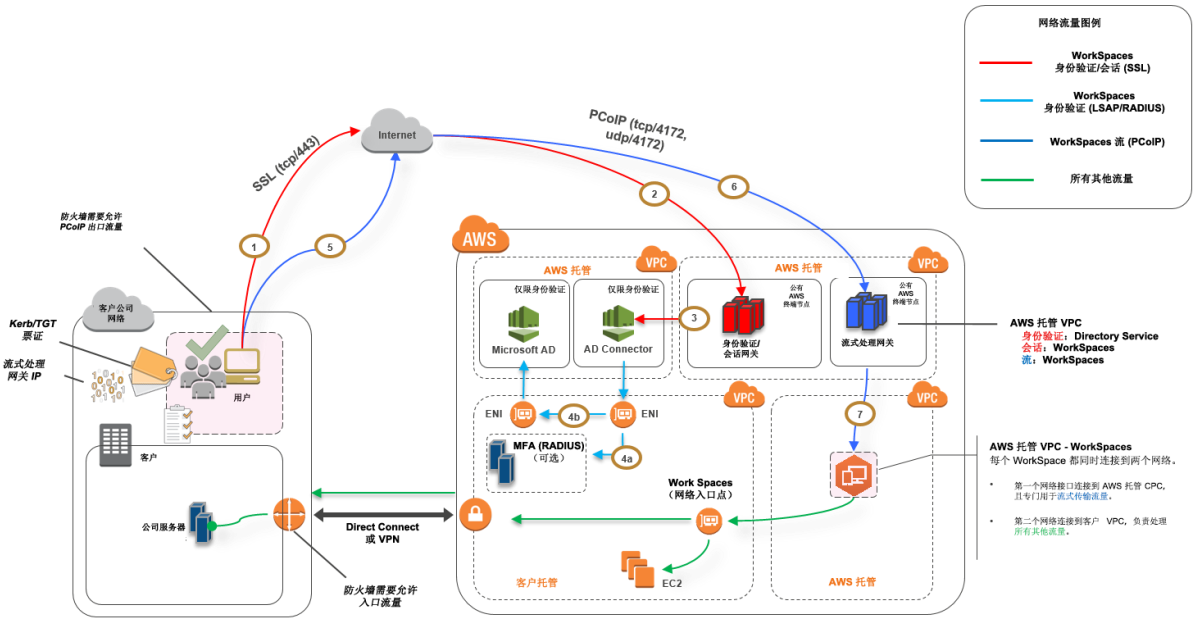

图 7：仅使用云 - AWS Directory Services (Microsoft AD)

与方案 2 一样，AD DS (Microsoft AD) 部署在跨两个可用区的专用子网中，使得 AD DS 在 AWS 云中高度可用。除 Microsoft AD 外，所有三种方案都部署了 AD Connector，以便进行 WorkSpaces 身份验证或 MFA。这确保了 Amazon VPC 中角色或功能的分离，也是标准的最佳实践（请参阅 *设计注意事项*：网络分区章节）。

方案 3 是一种标准的统包型配置，它非常适合想要让 AWS 管理 AWS Directory Service 部署、修补、高可用性和监控任务的客户。由于采用了隔离模式，该方案不仅适用于生产环境，还适合进行概念验证和用于实验室环境。

除 AWS Directory Service 的位置外，图 7 还显示了流量从用户到工作区的流动，以及该工作区如何与 AD 服务器和 MFA 服务器交互。

该架构使用以下组件或构造。

Amazon Web Services：

- **Amazon VPC：**创建一个具有至少四个私有子网（跨两个可用区）的 Amazon VPC（两个子网用于 AD DS *Microsoft AD*，另两个用于 AD Connector 或 WorkSpaces）。*“角色分离。”*
- **DHCP 选项集：**创建一个 Amazon VPC DHCP 选项集。这让您能够定义客户指定的域名和 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：**通过 IPsec VPN 隧道 (VPN) 或 AWS Direct Connect 连接与您的网络进行通信。用于访问本地部署的后端系统。
- **AWS Directory Service：**将 Microsoft AD 部署到一对专用的 VPC 子网中（AD DS 托管服务）。
- **Amazon EC2：**用于 MFA 的客户“可选”RADIUS 服务器。
- **AWS Directory Services：**将 AD Connector 部署到一对 Amazon VPC 私有子网中。
- **Amazon WorkSpaces：**将 WorkSpaces 部署到 AD Connector 所在的私有子网中（请参阅设计注意事项，AD Connector）。

客户：

- **可选：网络连接：**公司 VPN 或 AWS Direct Connect 终端节点。
- **最终用户设备：**公司或 BYOL 最终用户设备（如 Windows、Mac、iPad 或 Android 平板电脑、零客户端、Chromebook），用于访问 Amazon WorkSpaces 服务（请参阅支持的平台和设备）。

此解决方案从设计上来说是一个隔离的或仅使用云的方案，因此其与方案 2 一样不存在以下问题：依赖到客户本地部署数据中心的连接、延迟或数据传出成本（为 VPC 中的 WorkSpaces 启用了 Internet 访问时除外）。

设计注意事项

要在 AWS 云中成功部署 AD DS，您必须对 Active Directory 概念及具体的 AWS 服务有较为深入的了解。在本章节中，我们将讨论为 WorkSpaces 部署 AD DS 时的关键设计注意事项、针对 AWS Directory Service 的 VPC 最佳实践、DHCP 和 DNS 要求、AD Connector 细节信息以及 Active Directory 站点和服务。

VPC 设计

正如我们在本文档的网络方面的考量章节中的讨论和早前对于方案 2 和 3 的论述那样，您应该将 AWS 云中的 AD DS 部署到跨两个可用区的一对专用私有子网中，并与 AD Connector 或 WorkSpaces 子网隔离开。该构造可提供高可用性并对 AD DS 服务进行低延迟的 WorkSpaces 访问，同时遵循分离 Amazon VPC 中角色或功能的标准最佳实践。

图 8 显示了将 AD DS 和 AD Connector 隔离到专用私有子网中的情况（方案 3）。在该示例中，所有服务都位于同一个 Amazon VPC 中。

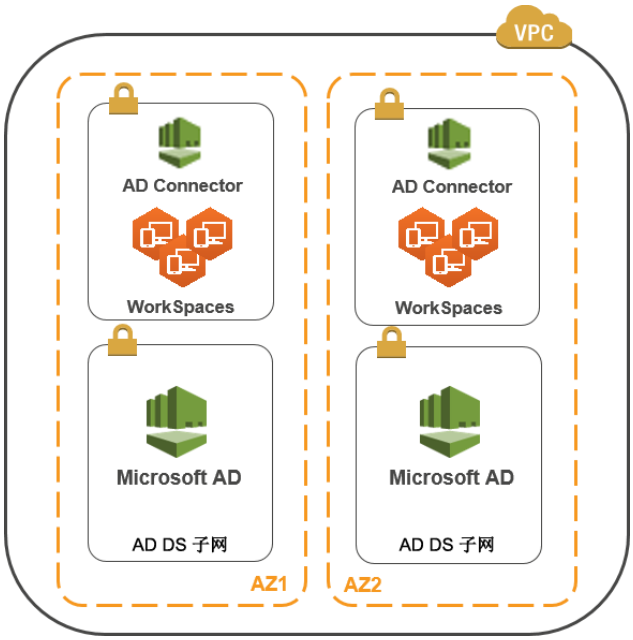

图 8：AD DS 网络隔离

图 9 显示了类似于方案 1 的设计，但在该方案中，本地部署部分位于专用的 Amazon VPC 中。

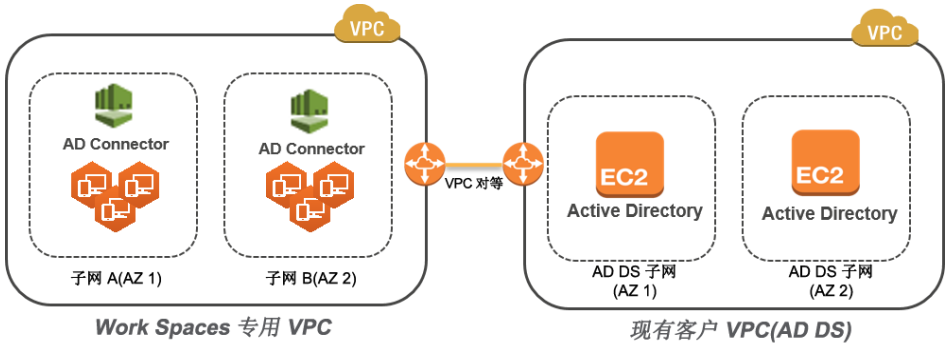

图 9：专用的 WorkSpaces VPC

注意 对于已有 AWS 部署并使用了 AD DS 的客户，我们建议您将 WorkSpaces 放置在专用的 VPC 中，并使用 VPC 对等连接进行 AD DS 通信。

除了为 AD DS 创建专用私有子网以外，域控制器和成员服务器还需要多条安全组规则，以允许 AD DS 复制、用户身份验证、Windows 时间服务、分布式文件系统 (DFS) 等服务的流量。

注意 最佳实践是将必要的安全组规则限制到 WorkSpaces 私有子网，且对于方案 2，允许本地部署与 AWS 云之间的双向 AD DS 通信，如下表所示。

协议	端口	使用	目标
tcp	53, 88, 135, 139, 389, 445, 464, 636	身份验证（主）	Active Directory（私有数据中心或 EC2）*
tcp	49152 – 65535	RPC 高端口	Active Directory（私有数据中心或 EC2）**
tcp	3268-3269	信任	Active Directory（私有数据中心或 EC2）*
tcp	9389	远程 Microsoft Windows PowerShell（可选）	Active Directory（私有数据中心或 EC2）*
udp	53, 88, 123, 137, 138, 389, 445, 464	身份验证（主）	Active Directory（私有数据中心或 EC2）*
udp	1812	身份验证 (MFA)（可选）	RADIUS（私有数据中心或 EC2）*

* 请参阅 Active Directory 和 Active Directory 域服务端口要求

** 请参阅 Windows 服务概述和网络端口要求

有关实施规则的分步指南，请参阅 *Amazon Elastic Compute Cloud 用户指南* 中的向安全组添加规则。

VPC 设计：DHCP 和 DNS

默认情况下，Amazon VPC 会为您的实例提供 DHCP 服务。每个 VPC 都提供一个可通过无类别域间路由 (CIDR) +2 地址空间访问的内部 DNS 服务器，并通过默认的 DHCP 选项集分配到所有实例。

DHCP 选项集在 Amazon VPC 内用于定义范围选项，例如：应通过 DHCP 提交给您的实例的域名或名称服务器。为使 VPC 中的 Windows 服务能够正常工作，该 DHCP 范围选项至关重要，您必须正确地设置它。在早前定义的各个方案中，您需要创建并分配自己的范围（定义域名和名称服务器）。这可确保加入域的 Windows 实例或 WorkSpaces 被配置为使用该 Active Directory DNS。为使 WorkSpaces 和 AWS Directory Services 正常工作，您必须创建一组 DHCP 范围选项。下表是一组自定义 DHCP 范围选项的示例。

参数	值
名称标签	创建一个键 = **名称**且**值**设置为特定字符串的标签 示例：exampleco.com
域名	exampleco.com
域名服务器	DNS 服务器地址，以逗号分隔 示例：10.0.0.10, 10.0.1.10
NTP 服务器	将此字段留空
NetBIOS 名称服务器	按照域名服务器输入相同的逗号分隔 IP 示例：10.0.0.10, 10.0.1.10
NetBIOS 节点类型	2

有关创建自定义 DHCP 选项集并将其关联到 Amazon VPC 的详细信息，请参阅 *Amazon Virtual Private Cloud 用户指南* 中的使用 DHCP 选项集。

在方案 1 中，DHCP 范围为本地 DNS 或 AD DS。但在方案 2 或 3 中，此为本地部署的目录服务（Amazon EC2 上的 AD DS 或 AWS Directory Services：Microsoft AD）。我们建议您使位于 AWS 云中的每个域控制器成为全局目录和 Directory 集成 DNS 服务器。

Active Directory：站点和服务

对于方案 2，要使 AD DS 正常工作，站点和服务至关重要。站点拓扑负责控制同一站点内和跨站点边界的域控制器之间的 Active Directory 复制。在方案 2 中，本地有至少两个站点且 AWS WorkSpaces 位于云中。定义适当的站点拓扑可确保客户端的相关性，也就是说，这些客户端（本例中为 WorkSpaces）会使用其首选的本地域控制器。

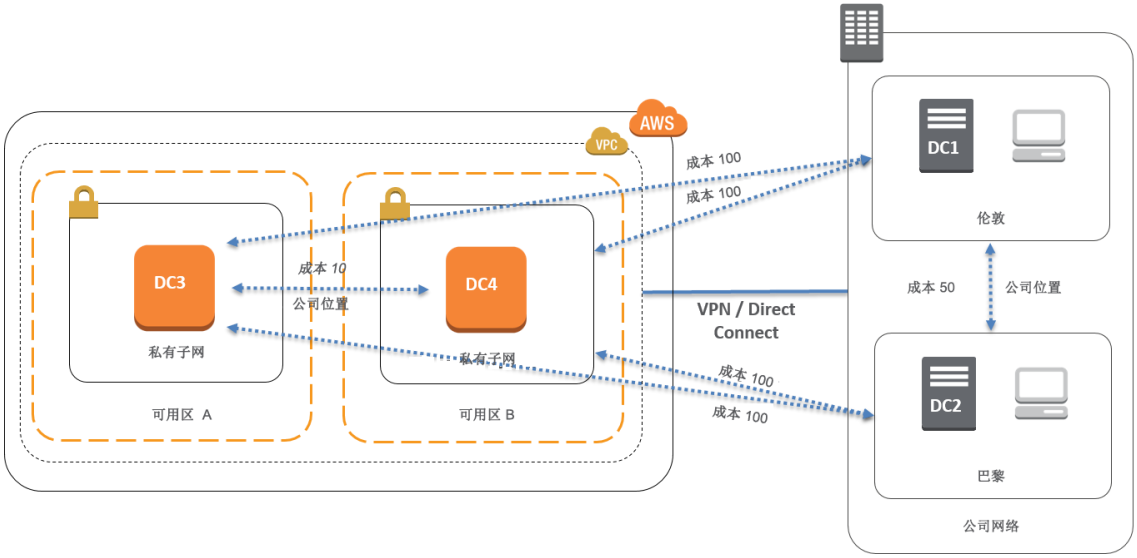

图 10：Active Directory 站点和服务：客户端相关性

最佳实践 为本地部署 AD DS 与 AWS 云之间的站点链接定义高成本。图 10 是一个示例，它为站点链接分配成本 100，以确保实现不依赖站点的客户端相关性。

这些关联可帮助确保 AD DS 复制、客户端身份验证之类的流量使用最高效的路径前往域控制器。在方案 2 和 3 中，这有助于确保较低的延迟和交叉链接流量。

多重身份验证 (MFA)

要实施 MFA，WorkSpaces 基础设施必须使用 AD Connector 作为其 AWS Directory Service 并拥有 RADIUS 服务器。虽然本文档不讨论 RADIUS 服务器的部署，但上一章节“AD DS 部署方案”详细介绍了 RADIUS 在每种方案中的部署情况。

MFA — 双重身份验证

Amazon WorkSpaces 通过 AWS Directory Service、AD Connector 及*客户所拥有的* RADIUS 服务器来支持 MFA。一经启用，用户必须向 WorkSpaces 客户端提供**用户名**、**密码**及 **MFA 代码**进行身份验证，然后才能访问其各自的 WorkSpaces 桌面。

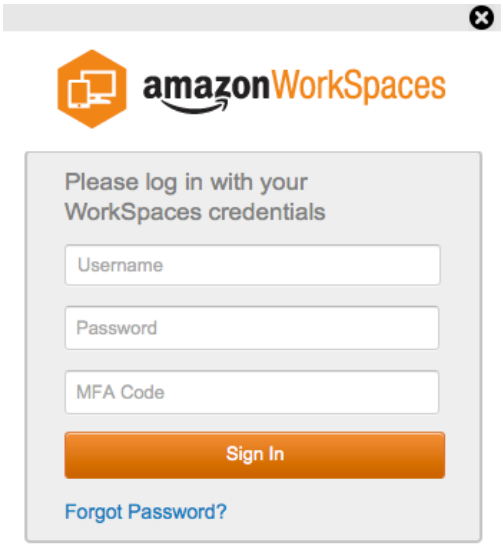

图 11：启用了 MFA 的 WorkSpaces 客户端

硬性规定 要实施 MFA 身份验证，您必须使用 AD Connector。AD Connector 不支持选择“每用户”MFA，因为这是一项每 AD Connector 的全局设置。如果您需要选择“每用户”MFA，则必须通过 AD Connector 分离用户。

WorkSpaces MFA 需要一台或多台 RADIUS 服务器。通常存在现成的解决方案（例如 RSA）。此外，您也可以将服务器部署到 VPC 中（请参阅 AD DS 部署方案）。如果您打算部署新的 RADIUS 解决方案，可以参考当今业界已存在的若干实施方案，例如：FreeRADIUS 或 Duo Security 之类的云服务。

有关针对 Amazon WorkSpaces 实施 MFA 的先决条件列表，请参阅 *Amazon WorkSpaces 管理指南*：为 AD Connector 目录准备您的网络。有关配置 AD Connector 以实现 MFA 的流程，请参阅 *Amazon WorkSpaces 管理指南* 中的“管理 AD Connector 目录：多重身份验证”。

安全性

本章节介绍在使用 Amazon WorkSpaces 服务时如何通过加密来保护数据。我们将介绍传输中和静态加密，以及如何借助安全组来保护对 WorkSpaces 的网络访问。有关身份验证（包括 MFA 支持）的更多信息，请参阅“AWS Directory Service”章节。

传输中加密

Amazon WorkSpaces 使用密码术来保护通信的各个阶段（传输中）的机密性，同时保护静态数据（加密的 WorkSpaces）的安全。后续的几个章节将介绍 Amazon WorkSpaces 在传输的各个加密阶段中采用的流程。有关静态加密的信息，请参阅本白皮书稍后的“加密的 WorkSpaces”章节。

注册和更新

桌面客户端应用程序使用 HTTPS 与 Amazon 交换更新和注册信息。

身份验证阶段

桌面客户端通过向身份验证网关发送凭证来发起身份验证。桌面客户端与身份验证网关之间的通信使用 HTTPS。在该阶段结束时，如果身份验证成功，身份验证网关通过同一个 HTTPS 连接向桌面客户端返回 OAuth 2.0 令牌。

> **注意** 桌面客户端应用程序支持使用代理服务器进行端口 443 (HTTPS) 流量、更新、注册和身份验证等操作。

收到来自客户端的凭证后，身份验证网关向 AWS Directory Service 发送一条身份验证请求。从身份验证网关到 AWS Directory Service 的通信使用 HTTPS 进行，因此，用户凭证不会以明文形式传输。

身份验证 — AD Connector

AD Connector 使用 Kerberos 与本地部署 AD 建立已认证的通信，因此，它能够绑定到 LDAP 并执行后续 LDAP 查询。此时，AWS Directory Service 不支持使用 TLS 的 LDAP (LDAPs)。但在任何时候，用户凭证都不会以明文形式传输。为了提高安全性，您可以使用 VPN 连接来连接 WorkSpaces VPC 与您的本地网络（AD 所在位置）。使用 AWS 硬件 VPN 连接时，您将使用标准 IPSEC（IKE 和 IPSEC SA）及 AES-128 或 AES-256 对称加密密钥、用于完整性哈希的 SHA-1 或 SHA-256 以及使用 PFS 的 DH 组（阶段 1 为 2、14-18、22、23 和 24；阶段 2 为 1、2、5、14-18、22、23 和 24）来设置传输中加密。

代理阶段

如果身份验证成功并收到来自身份验证网关的 OAuth 2.0 令牌，桌面客户端会使用 HTTPS 查询 Amazon WorkSpaces 服务（代理连接管理器）。桌面客户端通过发送 OAuth 2.0 令牌对自身进行身份验证，结果是，该客户端将收到 WorkSpaces 流式处理网关的终端节点信息。

流式处理阶段

桌面客户端请求与流式处理网关打开一个 PCoIP 会话（使用 OAuth 2.0 令牌）。该会话通过 aes256 进行加密，并使用 PCoIP 端口进行通信控制（即 4172/tcp）。

借助 OAuth2.0 令牌，流式处理网关请求 WorkSpaces 服务通过 HTTPS 发送特定于用户的 WorkSpaces 信息。

此外，流式处理网关还接收来自该客户端（已使用客户端用户密码加密）的 TGT，借助 Kerberos TGT 通过模式，网关使用用户检索到的 Kerberos TGT 在 WorkSpace 上发起 Windows 登录操作。

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

WorkSpace 成功登录后，PCoIP 开始进行流式传输。客户端在 tcp 端口 4172 上发起连接，并在 udp 端口 4172 上接收返回流量。此外，流式处理网关与 WorkSpaces 桌面通过管理接口上的 UDP 55002 建立初始连接（请参阅 Amazon Workspaces 文档 Amazon WorkSpaces 详细信息。初始出站 UDP 端口为 55002。）使用端口 4172（tcp 及 udp）的流式传输连接通过 AES 128 位和 256 位密码（默认为 128 位）进行加密。您可以通过特定于 PCoIP 的 Active Directory GPO (pcoip.adm) 将其主动更改为 256 位加密。

网络接口

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

主网络接口用于连接 VPC 内的资源，例如：访问 AWS Directory Service、Internet 及您的公司网络。您可以为该主网络接口挂载安全组（就像您对任何 ENI 所做的那样）。从概念上讲，我们根据部署范围来区分挂载到该 ENI 的安全组：WorkSpaces 安全组和 ENI 安全组。

管理网络接口

您无法通过安全组控制管理网络接口，但您可以借助位于 WorkSpace 上的基于主机的防火墙来阻止端口或控制访问。我们不建议对管理网络接口施加限制。如果您决定添加基于主机的防火墙规则来管理该接口，则您需要开放一些端口来让 WorkSpaces 服务管理 WorkSpace 的运行状况及可访问性，如 Amazon WorkSpaces 管理指南中定义的那样。

WorkSpaces 安全组

默认安全组是按 AWS Directory Service 创建的，且自动挂载到属于该特定目录的所有 WorkSpaces。

与任何其他安全组一样，您可以修改 WorkSpaces 安全组的规则。更改在应用后立即生效。

此外，您也可以通过更改 WorkSpaces 安全组关联来更改挂载到 AWS Directory Service 的默认 WorkSpaces 安全组。

> **注意** 新关联的安全组将只挂载到在修改后创建或重建的 WorkSpaces。

ENI 安全组

主网络接口是普通的 ENI，因此，您可以借助不同的 AWS 管理工具（请参阅弹性网络接口 (ENI)）来管理其配置。具体说来，您可以查找 WorkSpace IP（在 Amazon WorkSpaces 控制台的 WorkSpaces 页面中），然后使用该 IP 地址作为筛选条件来找到相应的 ENI（在 Amazon EC2 控制台的“Network Interfaces”部分中）。

找到 ENI 以后，您可以在这里直接管理安全组。在向主网络接口手动分配安全组时，请考虑 Amazon WorkSpaces 的端口要求（请参阅 Amazon WorkSpaces 详细信息）。

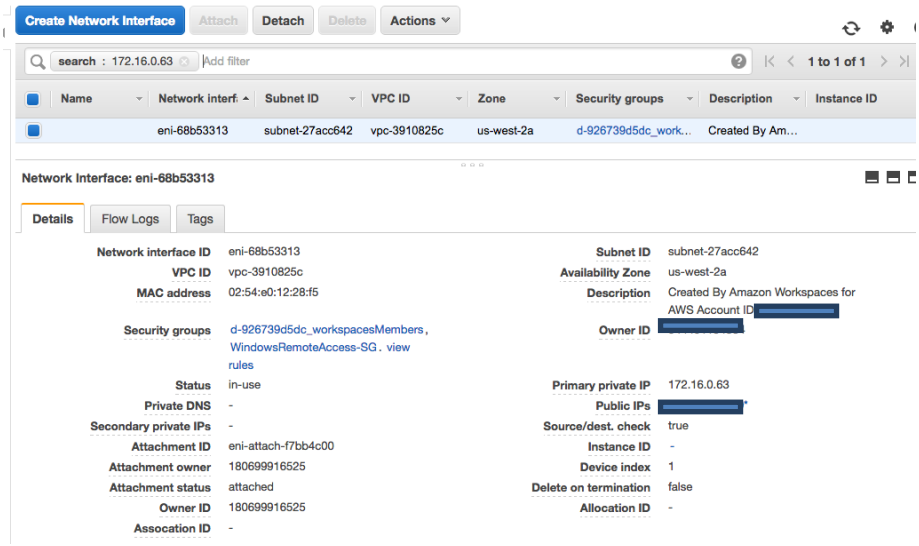

图 12：管理安全组关联

加密的 WorkSpaces

系统为每个 Amazon WorkSpace 都配置了一个根卷（C: 驱动器）和一个用户卷（D: 驱动器）。WorkSpaces 加密功能让您能够对一个或全部两个卷进行加密。

都会加密哪些内容？

静态存储的数据、卷的磁盘 I/O 及从加密卷创建的快照都会被加密。

何时进行加密？

您应在启动（创建）WorkSpace 时为其指定加密。WorkSpaces 卷只能在启动时加密：启动后，您将无法更改卷的加密状态。图 13 显示了启动新的 WorkSpace 时用于选择加密的 Amazon WorkSpaces 控制台页面。

图 13：加密 WorkSpaces 卷

新的 WorkSpace 是如何加密的？

您可以从 Amazon WorkSpaces 控制台或 AWS CLI 选择“Encrypted WorkSpaces”选项，或在启动新的 WorkSpace 时使用 Amazon WorkSpaces API 选择加密。

Amazon WorkSpaces 使用来自 AWS Key Management Service (KMS) 的客户主密钥 (CMK) 来加密卷。在某个区域首次启动 WorkSpace 时将会创建默认的 AWS KMS CMK（CMK 具有区域局限性）。您也可以创建由客户管理的 CMK 以用于加密的 WorkSpaces。CMK 用于加密数据密钥，后者被 Amazon WorkSpaces 服务用来加密卷（从严格意义上讲，Amazon Elastic Block Store (Amazon EBS) 服务负责对卷进行加密）。每个 CMK 可用来为多达 30 个 WorkSpaces 的密钥进行加密。

> **注意** 当前不支持从加密的 WorkSpace 创建自定义映像。此外，对于在启动时启用了根卷加密的 WorkSpaces，可能需要多达一个小时的时间才能完成配置。

有关 WorkSpaces 加密流程的详细说明，请参阅使用 AWS KMS 进行 Amazon WorkSpaces 加密概述。有关 AWS KMS 客户主密钥和数据密钥的更多信息，请参阅 AWS Key Management Service 概念。

使用 Amazon CloudWatch 进行监控或记录日志

不管是网络、服务器还是日志，监控都是任何基础设施不可或缺的一部分。部署 Amazon WorkSpaces 的客户需要监控其部署，特别是各个 WorkSpaces 的总体运行状况和连接状态。

有关 WorkSpaces 的 Amazon CloudWatch 指标

有关 WorkSpaces 的 CloudWatch 指标旨在使管理员更深入地了解各个 WorkSpaces 的总体运行状况和连接状态。您可以查看每个 WorkSpace 的指标，也可以查看给定目录（*AD Connector，请参阅“身份”*）中某个组织的所有 WorkSpaces 的汇总指标。

与所有 CloudWatch 指标一样，您可以在 AWS 管理控制台（图 13）中查看、通过 CloudWatch API 访问及通过 CloudWatch 警报和第三方工具监控这些指标。

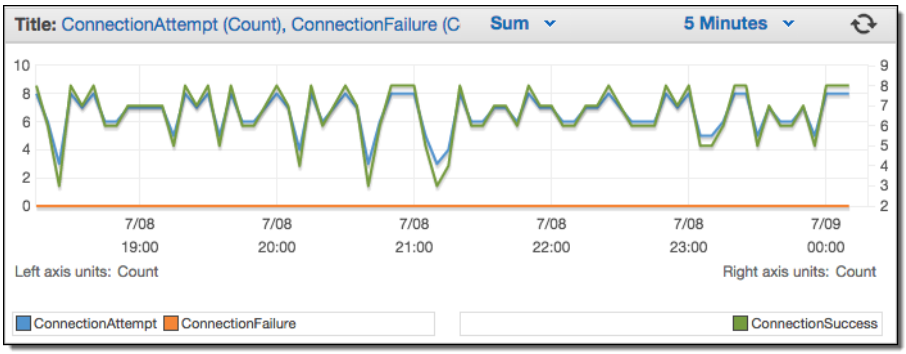

图 14：CloudWatch 指标 - ConnectionAttempt/ConnectionFailure

默认情况下，系统启用并提供以下指标（无额外费用）：

- **Available**：该指标统计响应状态检查的 WorkSpaces 的数量。
- **Unhealthy**：该指标统计不响应同一次状态检查的 WorkSpaces 的数量。
- **ConnectionAttempt**：尝试连接 WorkSpace 的次数。
- **ConnectionSuccess**：尝试连接成功的次数。
- **ConnectionFailure**：尝试连接失败的次数。

- **SessionLaunchTime**：WorkSpaces 客户端测量的发起会话所花费的时长。
- **InSessionLatency**：客户端测量并报告的 WorkSpaces 客户端与 WorkSpaces 之间的往返时间。
- **SessionDisconnect**：用户发起并自动关闭的会话的数量。

此外，您还可以创建警报，如图 15 所示。

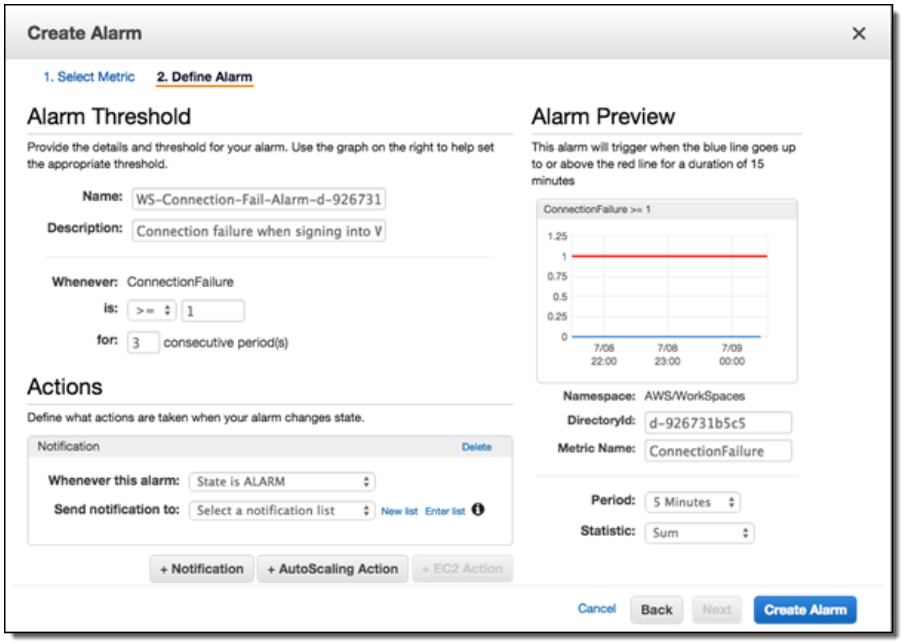

图 15：为 WorkSpaces 连接错误创建 CloudWatch 警报

疑难解答

有关常见的管理和客户端问题，如“我看到下面的错误消息：‘Your device is not able to connect to the WorkSpaces Registration service’ 或 ‘Can't connect to a WorkSpace with an interactive logon banner’”，请参阅 *Amazon WorkSpaces 管理指南* 中的客户端和管理疑难解答页面。

AD Connector 无法连接 Active Directory

为使 AD Connector 能够连接您的本地目录，您本地网络的防火墙必须向 VPC 中的两个子网的 CIDR 开放特定的端口（请参阅 AD Connector）。要测试这些条件是否得到满足，请执行以下步骤。

验证连接

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。其中包含源代码及 Visual Studio 项目文件，您可以根据需要修改该测试应用程序。
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*>

完全限定域名，用于测试林和域功能级别。如果不指定域名，则不测试功能级别。

<*server_IP_address*>

本地域中域控制器的 IP 地址。将针对该 IP 地址来测试端口。如果不指定 IP 地址，则不测试端口。

这可确定从 VPC 到您的域的必要端口是否打开。此外，该测试应用还验证最小的林和域功能级别。

如何检查到最近 AWS 区域的延迟

2015 年 10 月，Amazon WorkSpaces 推出了连接运行状况检查网站。该网站可快速检查您能否获得使用 WorkSpaces 所需的全部服务。此外，它还可对运行 WorkSpaces 的每个 AWS 区域进行性能检查，并告诉用户其访问哪个 AWS 区域最快。

总结

如今，各家组织纷纷寻求提高自身灵活性、更好地保护自己的数据并帮助员工提升工作效率的方法，在这样的背景下，我们发现最终用户计算领域正在发生战略转变。云计算已实现的许多优势同样适用于最终用户计算。通过使用 Amazon WorkSpaces 将桌面迁移到 AWS 云，组织可通过增加人手来迅速扩张，通过将数据存放在设备以外的位置来提高安全状况，并可为员工提供能够从其选择的设备随时随地进行访问的便携式桌面。

Amazon WorkSpaces 的设计可集成到现有的 IT 系统和流程中，而本白皮书讲解了实现这一目的的最佳实践。只要您按照本白皮书中的准则进行部署，就一定能实现托管在 AWS 全球基础设施中的可随您的业务一起扩展的、经济高效的云桌面。

撰稿人

本文的撰稿人包括：

- Justin Bradley（Amazon Web Services 解决方案架构师）
- Mahdi Sajjadpour（AWS 专业服务高级顾问）
- Mauricio Munoz（Amazon Web Services 解决方案架构师）

延伸阅读

如需其他帮助，请查阅以下资源：

- AWS Directory Service 管理问题排查
- Amazon WorkSpaces 管理问题排查
- Amazon WorkSpaces 客户端问题排查
- Amazon WorkSpaces 管理指南
- Amazon WorkSpaces 开发人员指南
- 支持的平台和设备
- Amazon WorkSpaces 如何使用 AWS KMS
- AWS CLI 命令参考 - workspaces
- 监控 Amazon WorkSpaces 指标