



架构图

安全的远程办公环境



安全的远程办公环境: 架构图

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon 的商标和商业外观不得用于任何非 Amazon 的商品或服务，也不得以任何可能引起客户混淆、贬低或诋毁 Amazon 的方式使用。所有非 Amazon 拥有的其他商标均为各自所有者的财产，这些所有者可能附属于 Amazon、与 Amazon 有关联或由 Amazon 赞助，也可能不是如此。

Table of Contents

安全的远程工作者 i

 安全的远程办公环境 1

 延伸阅读 2

 图表历史 2

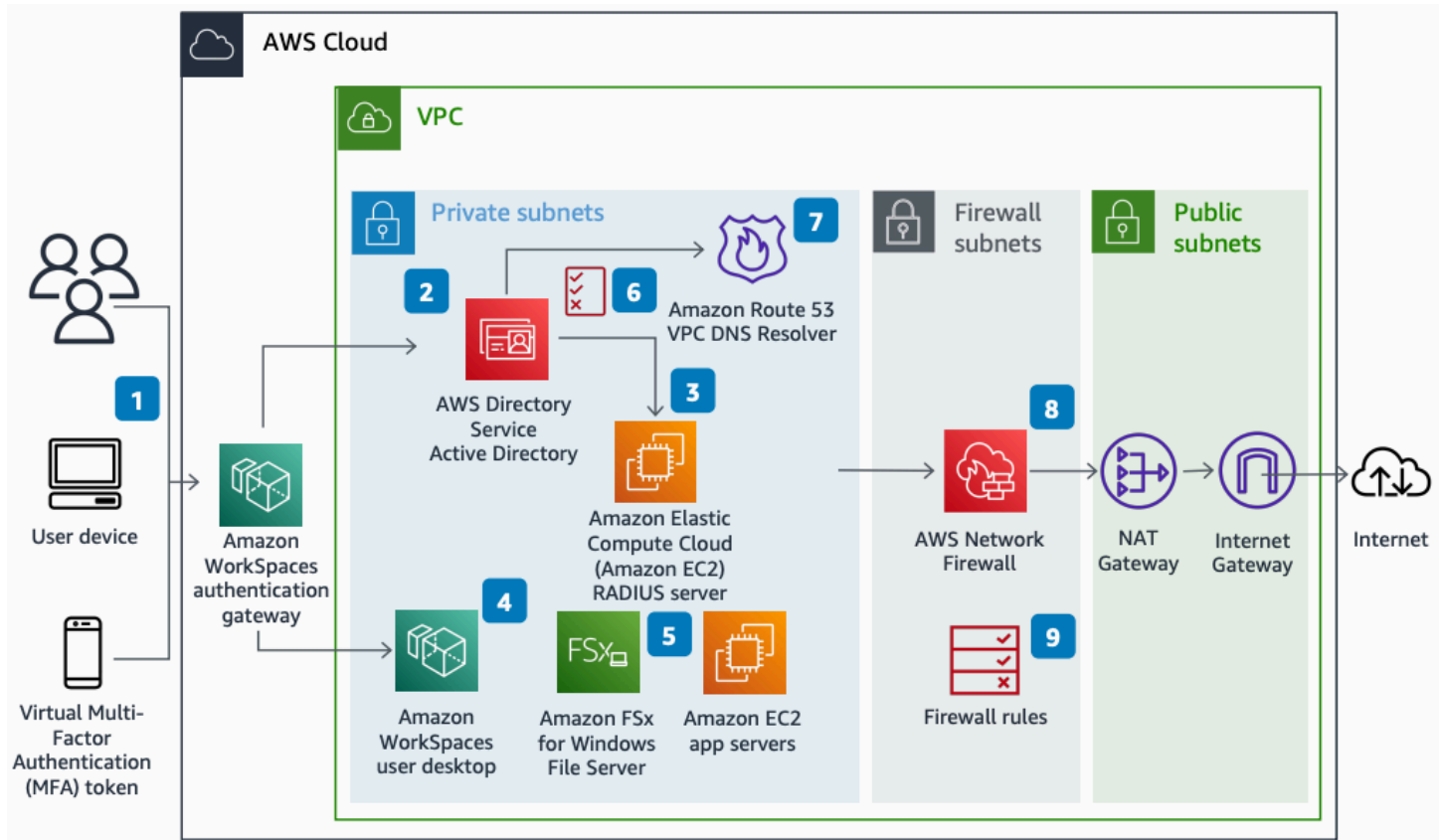
..... iii

安全的远程办公环境

发布日期：2022年 1月31日 ([图表历史](#))

该架构展示了如何为远程工作人员构建安全的桌面环境。员工可以访问关键的业务线应用程序和数据。

安全的远程办公环境



1. 用户使用带有用户名、密码和 MFA 代码的[亚马逊 WorkSpaces](#)应用程序连接到他们的桌面。
2. 亚马逊 WorkSpaces 身份验证网关针对[亚马逊 DynamoDB Streams](#) 进行身份验证。
3. MFA 代码针对 MFA 服务的 RADIUS 服务器进行身份验证（例如，[OneLogin](#)）。
4. 用户通过亚马逊连接到他们的桌面 WorkSpaces。
5. 用户访问[亚马逊弹性计算云和亚马逊 FSx](#) 上托管的核心系统和文件。
6. Active Directory 中的群组策略可防止不必要的活动，例如从亚马逊向本地打印机打印 WorkSpaces。
7. 域控制器 DNS 使用应用的路由 53 解析器 DNS 防火墙规则转发到 Route 53 VPC DNS 解析器。

8. [AWS Network Firewall](#) 过滤出站互联网流量，然后通过 NAT 网关和互联网网关将其路由到公共互联网。
9. 防火墙规则阻止流向有害站点（例如文件共享平台）的出站流量，以防止数据泄漏。

延伸阅读

有关其他信息，请参阅

- [AWS 架构图标](#)
- [AWS 建筑中心](#)
- [AWS Well-Architected](#)
- [亚马逊 WorkSpaces 产品页面](#)

图表历史

要获得有关此参考架构图更新的通知，请订阅 RSS 提要。

变更	说明	日期
初次发布	参考架构图首次发布。	2022 年 1 月 31 日

Note

要订阅 RSS 更新，必须为正在使用的浏览器启用 RSS 插件。

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。