



架構圖表

安全遠端工作者環境



安全遠端工作者環境: 架構圖表

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

Amazon 的商標和商業外觀不得用於任何非 Amazon 的產品或服務，也不能以任何可能造成客戶混淆、任何貶低或使 Amazon 名譽受損的方式使用 Amazon 的商標和商業外觀。所有其他非 Amazon 擁有的商標均為其各自擁有者的財產，這些擁有者可能附屬於 Amazon，或與 Amazon 有合作關係，亦或受到 Amazon 贊助。

Table of Contents

安全遠端工作者 i

 安全遠端工作者環境 1

 深入閱讀 2

 圖表歷史記錄 2

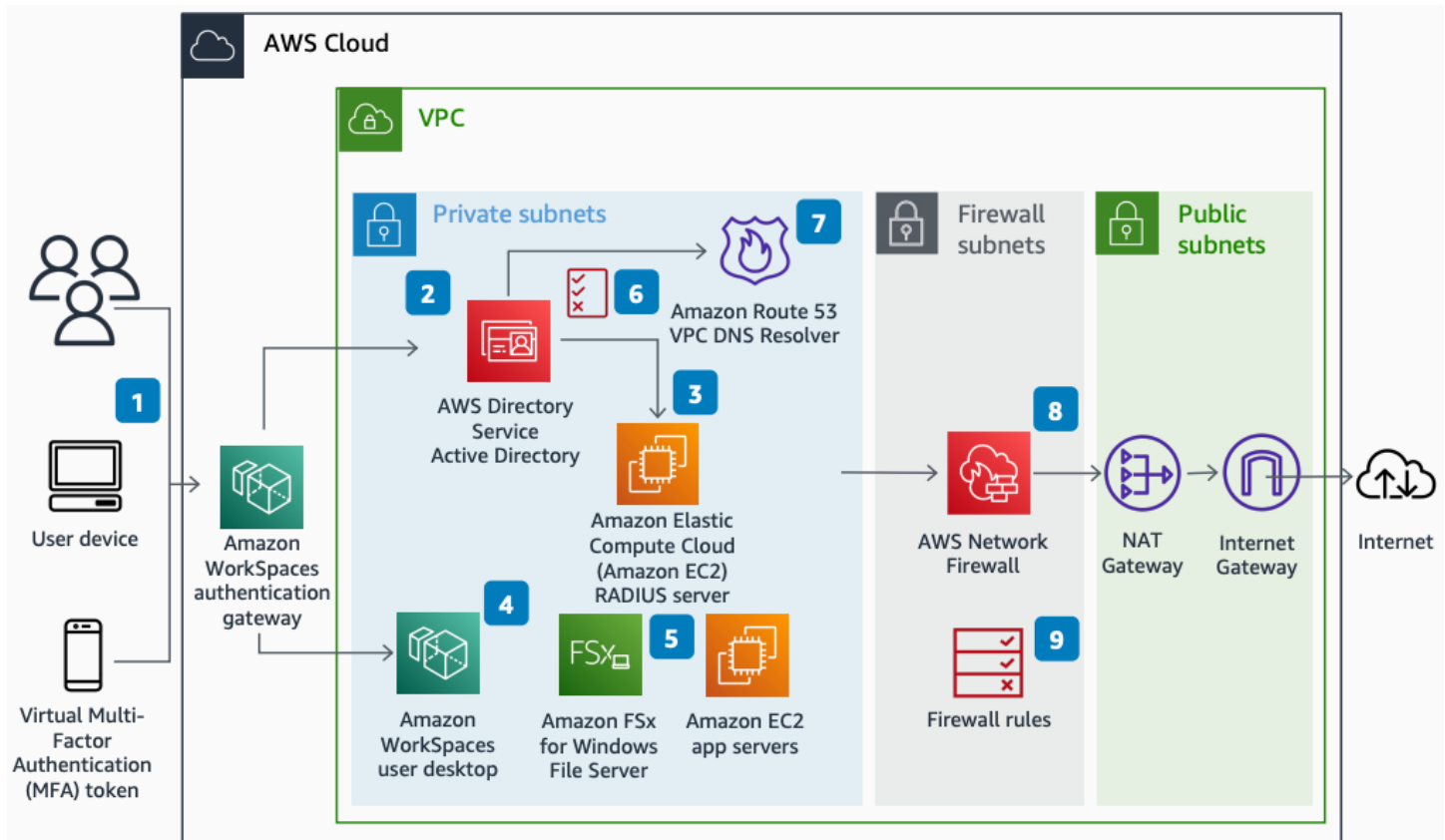
..... iii

安全遠端工作者環境

發佈日期：2022 年 1 月 31 日 ([圖表歷史記錄](#))

此架構說明如何為遠端工作者建置安全的桌面環境。工作者可以存取關鍵line-of-business應用程式和資料。

安全遠端工作者環境



1. 使用者使用 [Amazon WorkSpaces](#) 應用程式搭配使用者名稱、密碼和 MFA 代碼來連線至其桌面。
2. Amazon WorkSpaces 身分驗證閘道會對 [Amazon DynamoDB Streams](#) 進行身分驗證。
3. MFA 程式碼會根據 MFA 服務的 RADIUS 伺服器進行驗證（例如 OneLogin）。
4. 使用者透過 Amazon WorkSpaces 連線到其桌面。
5. 使用者存取 [Amazon Elastic Compute Cloud](#) 和 [Amazon FSx](#) 上託管的核心系統和檔案。
6. Active Directory 中的群組政策可防止不必要的活動，例如從 Amazon WorkSpaces 列印到本機印表機。

7. 網域控制器 DNS 會使用套用的 Route 53 Resolver DNS 防火牆規則轉送至 Route 53 VPC DNS 解析程式。
8. [AWS Network Firewall](#) 會篩選傳出網際網路流量，然後將其透過 NAT 閘道和網際網路閘道路由至公有網際網路。
9. 防火牆規則會封鎖對不需要的網站（例如檔案共用平台）的傳出流量，以防止資料洩漏。

深入閱讀

如需詳細資訊，請參閱

- [AWS 架構圖示](#)
- [AWS 架構中心](#)
- [AWS Well-Architected](#)
- [Amazon WorkSpaces 產品頁面](#)

圖表歷史記錄

若要收到此參考架構圖的更新通知，請訂閱 RSS 摘要。

變更	描述	日期
初次出版	首先發佈參考架構圖。	2022 年 1 月 31 日

Note

若要訂閱 RSS 更新，您必須為正在使用的瀏覽器啟用 RSS 外掛程式。

本文為英文版的機器翻譯版本，如內容有任何歧義或不一致之處，概以英文版為準。