



アーキテクチャ図

リモートワーカー環境を保護する



リモートワーカー環境を保護する: アーキテクチャ図

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

Amazon の商標およびトレードドレスは Amazon 以外の製品およびサービスに使用することはできません。また、お客様に誤解を与える可能性がある形式で、または Amazon の信用を損なう形式で使用することもできません。Amazon が所有していないその他のすべての商標は Amazon との提携、関連、支援関係の有無にかかわらず、それら該当する所有者の資産です。

Table of Contents

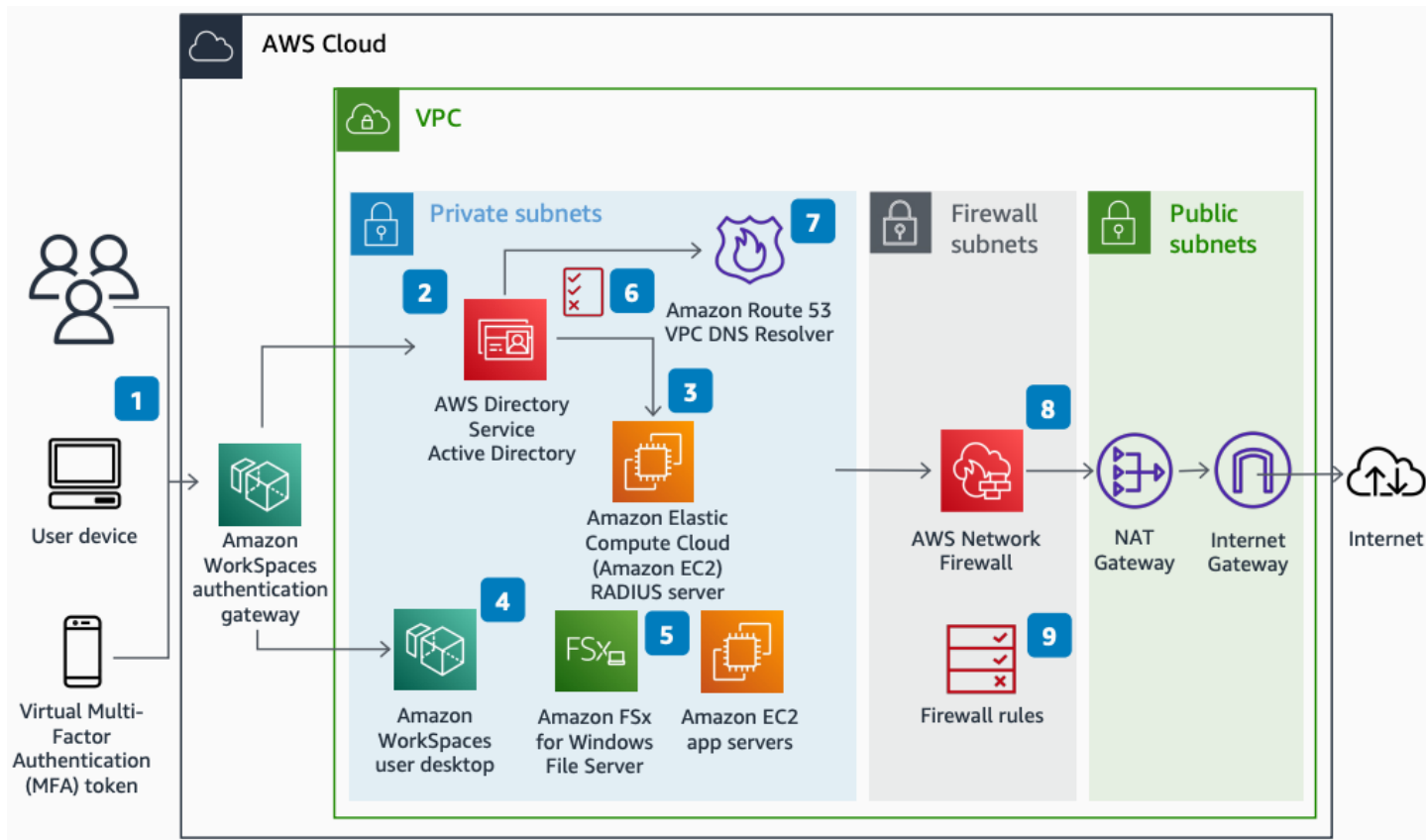
リモートワーカーの保護	i
リモートワーカー環境を保護する	1
詳細情報	2
図の履歴	2
.....	iii

リモートワーカー環境を保護する

公開日: 2022 年 1 月 31 日 ([図の履歴](#))

このアーキテクチャは、リモートワーカー向けの安全なデスクトップ環境を構築する方法を示しています。ワーカーは主要なline-of-businessアプリケーションとデータにアクセスできます。

リモートワーカー環境を保護する



1. ユーザーは、ユーザー名、パスワード、MFA コードを使用して [Amazon WorkSpaces](#) アプリケーションを使用してデスクトップに接続します。
2. Amazon WorkSpaces 認証ゲートウェイは [Amazon DynamoDB Streams](#) に対して認証します。
3. MFA コードは、MFA サービスの RADIUS サーバー (など) に対して認証しますOneLogin。
4. ユーザーは Amazon WorkSpaces を介してデスクトップに接続します。
5. ユーザーは、 [Amazon Elastic Compute Cloud](#) と [Amazon FSx](#) でホストされているコアシステムとファイルにアクセスします。

6. Active Directory のグループポリシーは、Amazon WorkSpaces からローカルプリンターへの印刷など、不要なアクティビティを防止します。
7. ドメインコントローラー DNS は、Route 53 Resolver DNS Firewall ルールを適用して Route 53 VPC DNS リゾルバーに転送します。
8. [AWS Network Firewall](#) はアウトバウンドインターネットトラフィックをフィルタリングし、NAT ゲートウェイとインターネットゲートウェイを介してパブリックインターネットにルーティングします。
9. ファイアウォールルールは、データ漏洩を防ぐために、不要なサイト (ファイル共有プラットフォームなど) へのアウトバウンドトラフィックをブロックします。

詳細情報

詳細については、「」を参照してください。

- [AWS アーキテクチャアイコン](#)
- [AWS アーキテクチャセンター](#)
- [AWS Well-Architected](#)
- [Amazon WorkSpaces 製品ページ](#)

図の履歴

このリファレンスアーキテクチャ図の更新について通知を受け取るには、RSS フィードにサブスクライブします。

変更	説明	日付
初版発行	リファレンスアーキテクチャ図が最初に公開されました。	2022 年 1 月 31 日

Note

RSS 更新をサブスクライブするには、使用しているブラウザで RSS プラグインが有効になっている必要があります。

翻訳は機械翻訳により提供されています。提供された翻訳内容と英語版の間で齟齬、不一致または矛盾がある場合、英語版が優先します。