



Diagrammi di architettura

Ambiente sicuro per i lavoratori remoti



Ambiente sicuro per i lavoratori remoti: Diagrammi di architettura

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

I marchi e l'immagine commerciale di Amazon non possono essere utilizzati in relazione a prodotti o servizi che non siano di Amazon, in una qualsiasi modalità che possa causare confusione tra i clienti o in una qualsiasi modalità che denigri o discrediti Amazon. Tutti gli altri marchi non di proprietà di Amazon sono di proprietà dei rispettivi proprietari, che possono o meno essere affiliati, collegati o sponsorizzati da Amazon.

Table of Contents

Lavoratore remoto sicuro i

 Ambiente sicuro per i lavoratori remoti 1

 Approfondimenti 2

 Storia del diagramma 2

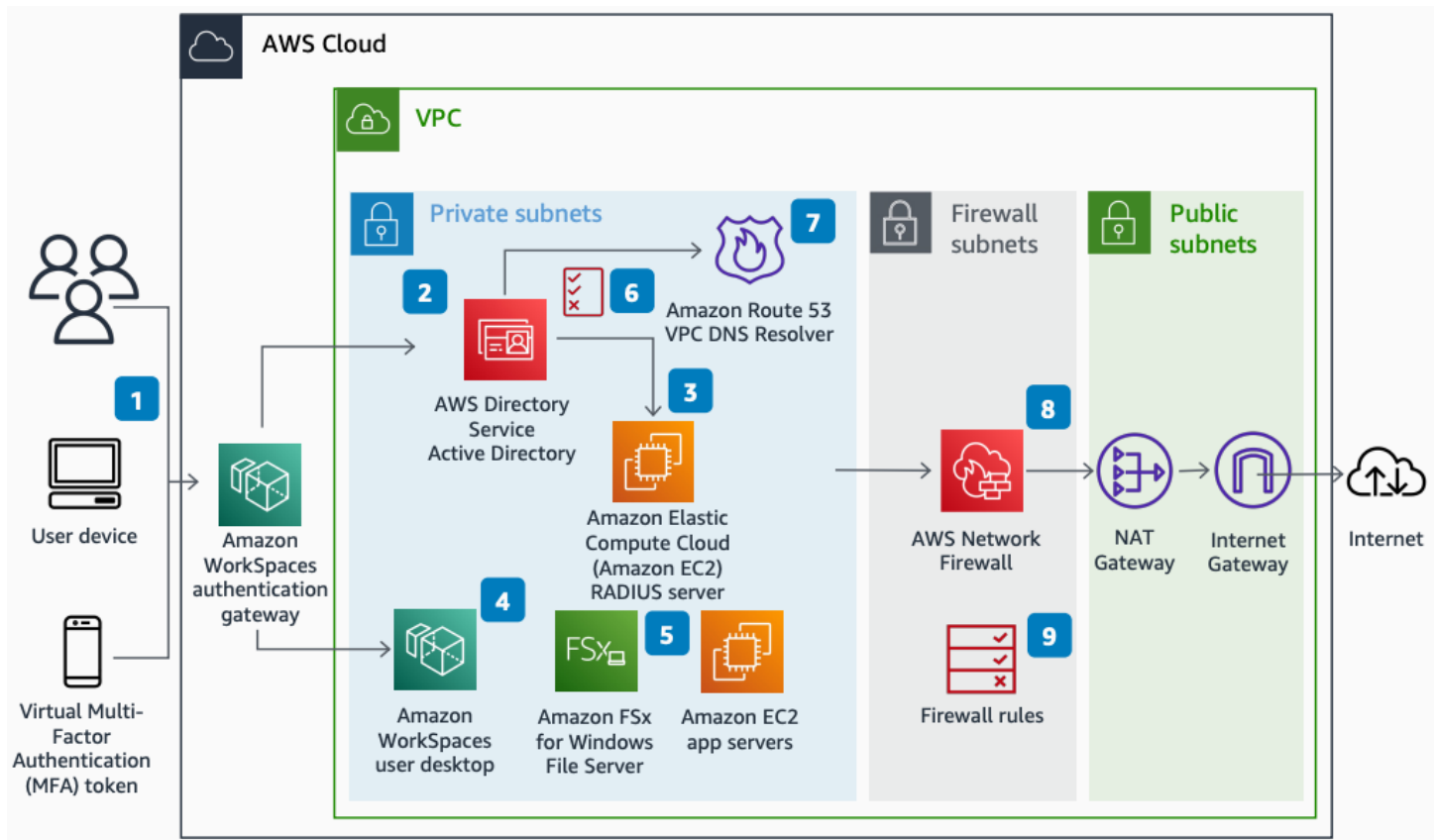
..... iii

Ambiente sicuro per i lavoratori remoti

Data di pubblicazione: 31 gennaio 2022 () [Storia del diagramma](#)

Questa architettura mostra come creare un ambiente desktop sicuro per i lavoratori remoti. I lavoratori possono accedere alle principali applicazioni e dati aziendali.

Ambiente sicuro per i lavoratori remoti



1. Gli utenti si connettono al proprio desktop utilizzando l' [WorkSpaces applicazione](#) Amazon con nome utente, password e codice MFA.
2. Il gateway di WorkSpaces autenticazione Amazon si autentica con [Amazon DynamoDB Streams](#).
3. Il codice MFA si autentica con il server RADIUS del servizio MFA (ad esempio,). OneLogin
4. Gli utenti si connettono al proprio desktop tramite Amazon. WorkSpaces
5. Gli utenti accedono ai sistemi e ai file principali ospitati su [Amazon Elastic Compute Cloud](#) e [Amazon FSx](#).

6. La politica di gruppo in Active Directory impedisce attività indesiderate, come la stampa su stampanti locali di Amazon. WorkSpaces
7. Il DNS del controller di dominio inoltra al resolver DNS Route 53 VPC con le regole del firewall DNS Route 53 Resolver applicate.
8. [AWS Network Firewall](#) filtra il traffico Internet in uscita, quindi lo indirizza attraverso un gateway NAT e un gateway Internet verso la rete Internet pubblica.
9. Le regole del firewall bloccano il traffico in uscita verso siti indesiderati (come le piattaforme di condivisione di file) per prevenire fughe di dati.

Approfondimenti

Per ulteriori informazioni, consulta

- [AWS Icone di architettura](#)
- [AWS Centro di architettura](#)
- [AWS Well-Architected](#)
- [Pagina WorkSpaces del prodotto Amazon](#)

Storia del diagramma

Per ricevere notifiche sugli aggiornamenti di questo diagramma di architettura di riferimento, iscriviti al feed RSS.

Modifica	Descrizione	Data
Pubblicazione iniziale	Diagramma dell'architettura di riferimento pubblicato per la prima volta.	31 gennaio 2022

Note

Per iscriverti agli aggiornamenti RSS, devi avere un plugin RSS abilitato per il browser che stai utilizzando.

Le traduzioni sono generate tramite traduzione automatica. In caso di conflitto tra il contenuto di una traduzione e la versione originale in Inglese, quest'ultima prevarrà.