



Architektur-Diagramme

Sichere Umgebung für Remote-Mitarbeiter



Sichere Umgebung für Remote-Mitarbeiter: Architektur-Diagramme

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

Die Handelsmarken und die Handelsaufmachung von Amazon dürfen nicht in einer Weise in Verbindung mit nicht von Amazon stammenden Produkten oder Services verwendet werden, durch die Kunden irregeführt werden könnten oder Amazon in schlechtem Licht dargestellt oder diskreditiert werden könnte. Alle anderen Handelsmarken, die nicht Eigentum von Amazon sind, gehören den jeweiligen Besitzern, die möglicherweise zu Amazon gehören oder nicht, mit Amazon verbunden sind oder von Amazon gesponsert werden.

Table of Contents

Sicherer Mitarbeiter im Homeoffice i

Sichere Umgebung für Mitarbeiter im Home-Office 1

Weitere Informationen 2

Verlauf des Diagramms 2

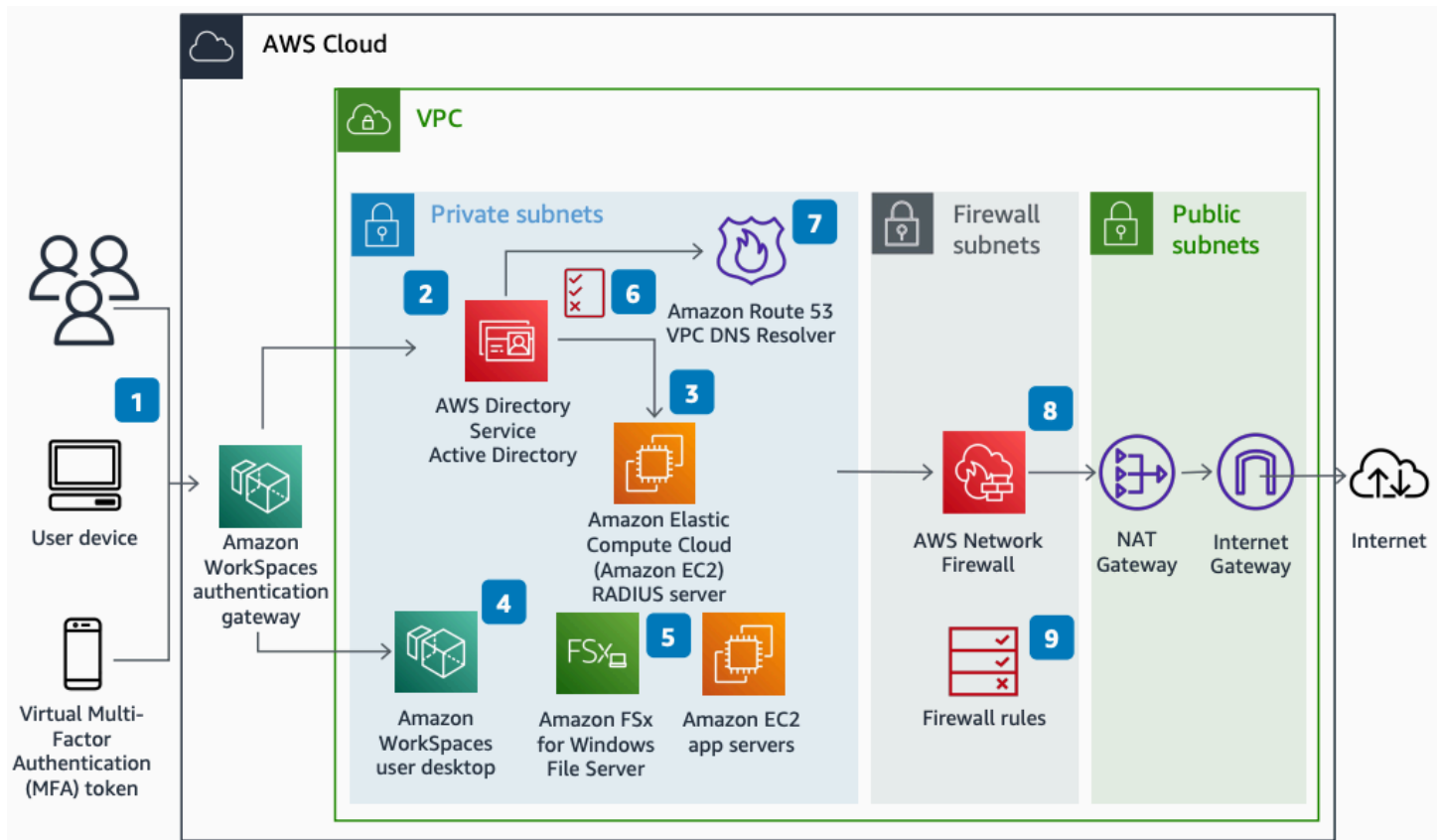
..... iv

Sichere Umgebung für Remote-Mitarbeiter

Veröffentlichungsdatum: 31. Januar 2022 () [Verlauf des Diagramms](#)

Diese Architektur zeigt, wie eine sichere Desktop-Umgebung für Mitarbeiter im Homeoffice eingerichtet werden kann. Mitarbeiter können auf wichtige Geschäftsanwendungen und Daten zugreifen.

Sichere Umgebung für Mitarbeiter im Home-Office



1. Benutzer stellen eine Verbindung zu ihrem Desktop her, indem sie die [WorkSpaces](#) Amazon-Anwendung mit einem Benutzernamen, einem Passwort und einem MFA-Code verwenden.
2. Das WorkSpaces Amazon-Authentifizierungsgateway authentifiziert sich gegenüber [Amazon DynamoDB Streams](#).
3. Der MFA-Code authentifiziert sich gegenüber dem RADIUS-Server des MFA-Dienstes (z. B.). OneLogin
4. Benutzer stellen über Amazon eine Verbindung zu ihrem Desktop her. WorkSpaces

5. Benutzer greifen auf Kernsysteme und Dateien zu, die auf [Amazon Elastic Compute Cloud](#) und [Amazon FSx](#) gehostet werden.
6. Gruppenrichtlinien in Active Directory verhindern unerwünschte Aktivitäten wie das Drucken auf lokalen Druckern von Amazon WorkSpaces aus.
7. Der Domänencontroller-DNS leitet an den Route 53-VPC-DNS-Resolver weiter, wobei die Route 53 Resolver-DNS-Firewallregeln angewendet werden.
8. [AWS Network Firewall](#) filtert ausgehenden Internetverkehr und leitet ihn dann über ein NAT-Gateway und ein Internet-Gateway an das öffentliche Internet weiter.
9. Firewallregeln blockieren ausgehenden Datenverkehr zu unerwünschten Websites (wie Filesharing-Plattformen), um Datenlecks zu verhindern.

Weitere Informationen

Weitere Informationen finden Sie unter

- [AWS Architektur-Symbole](#)
- [AWS Zentrum für Architektur](#)
- [AWS Well-Architected](#)
- [WorkSpaces Amazon-Produktseite](#)

Verlauf des Diagramms

Abonnieren Sie den RSS-Feed, um über Aktualisierungen dieses Referenzarchitekturdiagramms informiert zu werden.

Änderung	Beschreibung	Datum
Erste Veröffentlichung	Das Referenzarchitekturdiagramm wurde zuerst veröffentlicht.	31. Januar 2022

 Note

Um RSS-Updates zu abonnieren, muss ein RSS-Plugin für den von Ihnen verwendeten Browser aktiviert sein.

Die vorliegende Übersetzung wurde maschinell erstellt. Im Falle eines Konflikts oder eines Widerspruchs zwischen dieser übersetzten Fassung und der englischen Fassung (einschließlich infolge von Verzögerungen bei der Übersetzung) ist die englische Fassung maßgeblich.