



Schémas d'architecture

Environnement de télétravail sécurisé



Environnement de télétravail sécurisé: Schémas d'architecture

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

Les marques et la présentation commerciale d'Amazon ne peuvent être utilisées en relation avec un produit ou un service qui n'est pas d'Amazon, d'une manière susceptible de créer une confusion parmi les clients, ou d'une manière qui dénigre ou discrédite Amazon. Toutes les autres marques commerciales qui ne sont pas la propriété d'Amazon appartiennent à leurs propriétaires respectifs, qui peuvent ou non être affiliés ou connectés à Amazon, ou sponsorisés par Amazon.

Table of Contents

Travailleur à distance sécurisé i

 Environnement sécurisé pour les télétravailleurs 1

 Suggestions de lecture 2

 Historique du diagramme 2

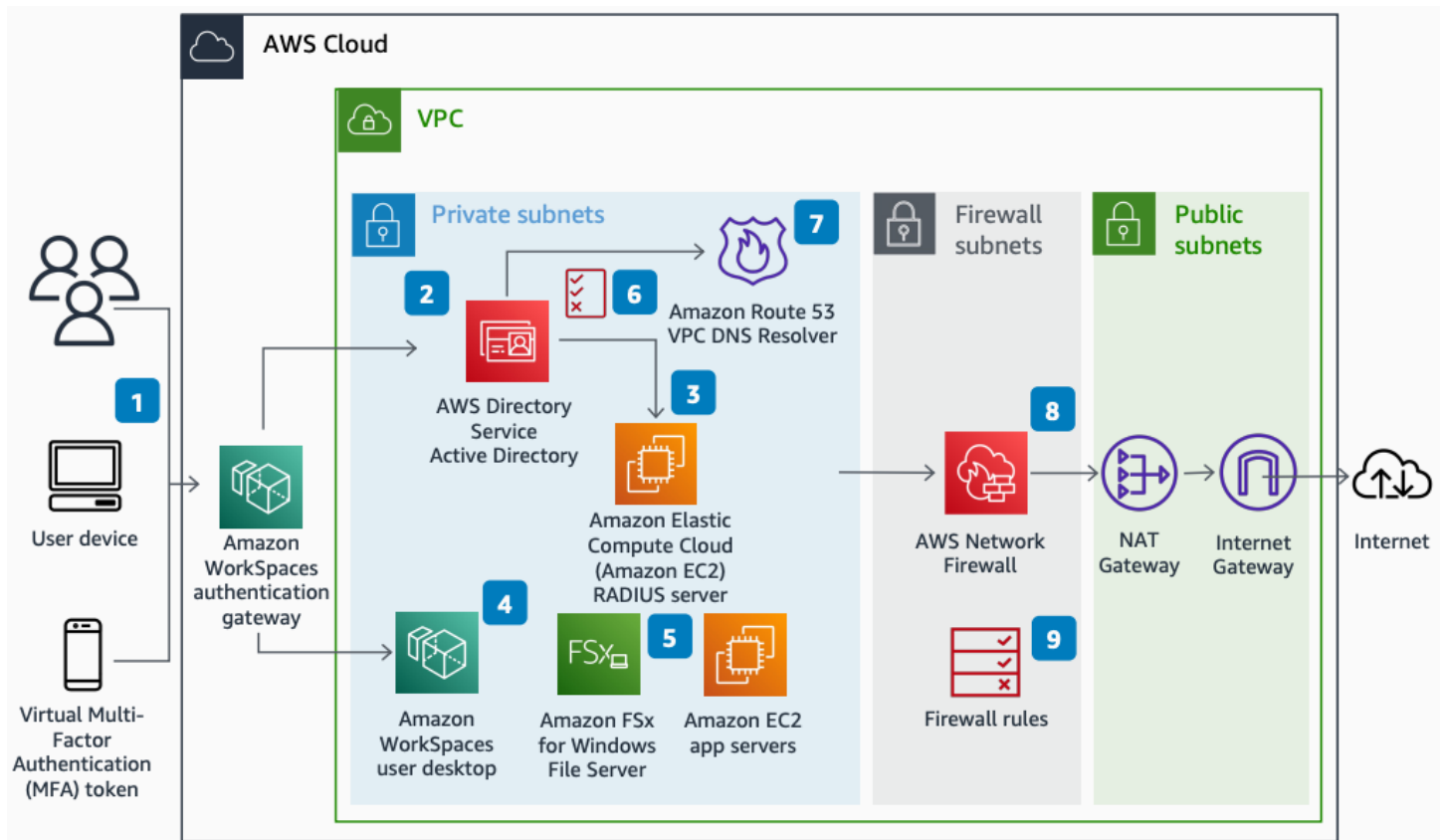
..... iv

Environnement de télétravail sécurisé

Date de publication : 31 janvier 2022 ([Historique du diagramme](#))

Cette architecture montre comment créer un environnement de bureau sécurisé pour les télétravailleurs. Les employés peuvent accéder à des applications et à des données clés du secteur d'activité.

Environnement sécurisé pour les télétravailleurs



1. Les utilisateurs se connectent à leur poste de travail à l'aide de l' [WorkSpaces application](#) Amazon avec un nom d'utilisateur, un mot de passe et un code MFA.
2. La passerelle WorkSpaces d'authentification Amazon s'authentifie auprès de [Amazon DynamoDB Streams](#).
3. Le code MFA s'authentifie auprès du serveur RADIUS du service MFA (par exemple,). OneLogin
4. Les utilisateurs se connectent à leur poste de travail via Amazon WorkSpaces.

5. Les utilisateurs accèdent aux principaux systèmes et fichiers hébergés sur [Amazon Elastic Compute Cloud](#) et [Amazon FSx](#).
6. La stratégie de groupe dans Active Directory empêche les activités indésirables, telles que l'impression sur des imprimantes locales depuis Amazon WorkSpaces.
7. Le DNS du contrôleur de domaine est transféré au résolveur DNS VPC Route 53 avec les règles de pare-feu DNS du résolveur Route 53 appliquées.
8. [AWS Network Firewall](#) filtre le trafic Internet sortant, puis l'achemine via une passerelle NAT et une passerelle Internet vers l'Internet public.
9. Les règles de pare-feu bloquent le trafic sortant vers des sites indésirables (tels que les plateformes de partage de fichiers) afin d'empêcher les fuites de données.

Suggestions de lecture

Pour plus d'informations, reportez-vous à

- [AWS Icônes de l'architecture](#)
- [AWS Centre d'architecture](#)
- [AWS Well-Architected](#)
- [Page WorkSpaces produit Amazon](#)

Historique du diagramme

Pour être informé des mises à jour de ce schéma d'architecture de référence, abonnez-vous au fil RSS.

Modification	Description	Date
Publication initiale	Schéma d'architecture de référence publié pour la première fois.	31 janvier 2022

 Note

Pour vous abonner aux mises à jour RSS, un plug-in RSS doit être activé pour le navigateur que vous utilisez.

Les traductions sont fournies par des outils de traduction automatique. En cas de conflit entre le contenu d'une traduction et celui de la version originale en anglais, la version anglaise prévaudra.