



Diagramas de arquitectura

Entorno seguro de trabajo remoto



Entorno seguro de trabajo remoto: Diagramas de arquitectura

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

Las marcas comerciales y la imagen comercial de Amazon no se pueden utilizar en relación con ningún producto o servicio que no sea de Amazon, de ninguna manera que pueda causar confusión entre los clientes y que menosprecie o desacredite a Amazon. Todas las demás marcas registradas que no son propiedad de Amazon son propiedad de sus respectivos propietarios, que pueden o no estar afiliados, conectados o patrocinados por Amazon.

Table of Contents

Trabajador remoto seguro i

Entorno seguro de trabajo remoto 1

Documentación adicional 2

Historial del diagrama 2

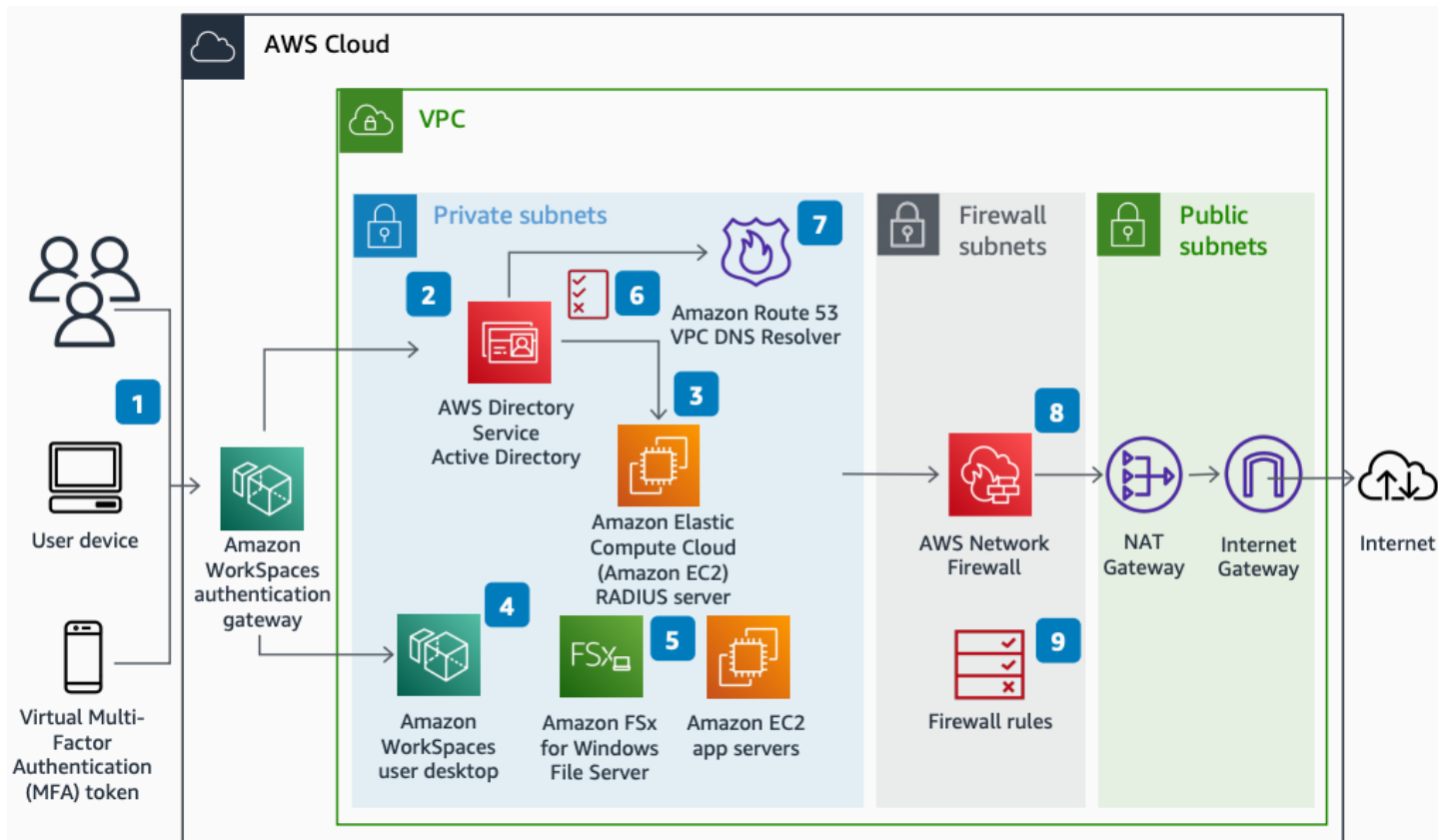
..... iii

Entorno seguro de trabajo remoto

Fecha de publicación: 31 de enero de 2022 () [Historial del diagrama](#)

Esta arquitectura muestra cómo crear un entorno de escritorio seguro para los trabajadores remotos. Los trabajadores pueden acceder a las aplicaciones y los datos clave de las líneas de negocio.

Entorno seguro de trabajo remoto



1. Los usuarios se conectan a su escritorio mediante la WorkSpaces [aplicación](#) Amazon con un nombre de usuario, una contraseña y un código MFA.
2. La pasarela de WorkSpaces autenticación de Amazon se autentica con [Amazon DynamoDB Streams](#).
3. El código MFA se autentica en el servidor RADIUS del servicio MFA (por ejemplo,). OneLogin
4. Los usuarios se conectan a su escritorio a través de Amazon. WorkSpaces
5. Los usuarios acceden a los sistemas y archivos principales alojados en [Amazon Elastic Compute Cloud](#) y [Amazon FSx](#).

6. La política de grupo de Active Directory evita actividades no deseadas, como imprimir en impresoras locales desde Amazon WorkSpaces.
7. El DNS del controlador de dominio se reenvía al solucionador de DNS de VPC de Route 53 con las reglas del firewall DNS de Route 53 Resolver aplicadas.
8. [AWS Network Firewall](#) filtra el tráfico de Internet saliente y, a continuación, lo dirige a través de una puerta de enlace NAT y una puerta de enlace de Internet a la Internet pública.
9. Las reglas de firewall bloquean el tráfico saliente a sitios no deseados (como las plataformas de intercambio de archivos) para evitar la filtración de datos.

Documentación adicional

Para obtener información adicional, consulte

- [AWS Iconos de arquitectura](#)
- [AWS Centro de arquitectura](#)
- [AWS Well-Architected](#)
- [Página de WorkSpaces producto de Amazon](#)

Historial del diagrama

Para recibir notificaciones sobre las actualizaciones de este diagrama de arquitectura de referencia, suscríbase a la fuente RSS.

Cambio	Descripción	Fecha
Publicación inicial	El diagrama de arquitectura de referencia se publicó por primera vez.	31 de enero de 2022

Note

Para suscribirse a las actualizaciones de RSS, debe tener un complemento de RSS habilitado para el navegador que esté utilizando.

Las traducciones son generadas a través de traducción automática. En caso de conflicto entre la traducción y la version original de inglés, prevalecerá la version en inglés.