Amazon WorkDocs

Guía de administración

Amazon WorkDocs: Guía de administración

Table of Contents

¿Qué es Amazon WorkDocs?

Amazon WorkDocs es un servicio empresarial seguro de almacenamiento y uso compartido completamente administrado con controles administrativos estrictos y funciones de comentarios que mejoran la productividad de los usuarios. Los archivos se almacenan en la nube de forma segura. Los archivos de sus usuarios solo están visibles para ellos y los colaboradores y espectadores designados. Otros miembros de la organización no tienen acceso a ningún otro archivo de usuario, salvo que se les haya concedido acceso específicamente.

Los usuarios pueden compartir sus archivos con otros miembros de su organización para colaboraciones o revisiones. Las aplicaciones cliente de Amazon WorkDocs se pueden utilizar para ver muchos tipos de archivos diferentes, que dependen del tipo de medios de Internet del archivo. Amazon WorkDocs admite todos los formatos de imagen y documentos más comunes y constantemente se van agregando más tipos de medios.

Para obtener más información, consulteAmazon WorkDocs.

Acceso a Amazon WorkDocs

Los administradores utilizan elConsola de Amazon WorkDocspara crear y desactivar los sitios de Amazon WorkDocs. Con el panel de control del administrador, pueden administrar la configuración de los usuarios, del almacenamiento y de la seguridad. Para obtener más información, consulte Administrar Amazon WorkDocs desde el panel de control del administrador del sitio (p. 27) y Invitar y gestionar WorkDocs usuarios de Amazon (p. 34).

Los usuarios no administrativos utilizan las aplicaciones cliente para obtener acceso a sus archivos. Nunca utilizan la consola de Amazon WorkDocs ni el panel de administración. Amazon WorkDocs ofrece diferentes aplicaciones cliente y utilidades:

- Una aplicación web que se utiliza para la administración y revisión de documentos.
- Aplicaciones nativas para dispositivos móviles que se utilizan para la revisión de documentos.
- Amazon WorkDocs Drive, una aplicación que sincroniza una carpeta del escritorio de macOS o de Windows con los archivos de Amazon WorkDocs.

Para obtener más información sobre cómo los usuarios pueden descargar clientes de Amazon WorkDocs y editar sus archivos y conocer los tipos de archivos admitidos, consulte:

- Introducción a Amazon WorkDocs
- Edición de archivos
- Tipos de archivo admitidos

Precios

Con Amazon WorkDocs, no hay cuotas de pago iniciales ni compromisos. Solo se paga por las cuentas de usuario activas y por el almacenamiento que se utiliza. Para obtener más información, consultePrecios.

Cómo empezar

Para comenzar a utilizar Amazon WorkDocs, consulteCrear un WorkDocs sitio de Amazon (p. 20).

requisitos previos de Amazon WorkDocs

Para configurar nuevos WorkDocs sitios de Amazon o administrar los sitios existentes, debe realizar las siguientes tareas.

Registro en una Cuenta de AWS

Si no dispone de una Cuenta de AWS, siga los pasos que figuran a continuación para crear una.

Para registrarse en Cuenta de AWS

1. Abra https://portal.aws.amazon.com/billing/signup.
2. Siga las instrucciones en línea.

   Parte del procedimiento de inscripción consiste en recibir una llamada telefónica e indicar un código de verificación en el teclado del teléfono.

   Al registrase en una Cuenta de AWS, se crea un Usuario raíz de la cuenta de AWS. El usuario raíz tiene acceso a todos los recursos y Servicios de AWS de esa cuenta. Como práctica recomendada de seguridad, asigne acceso administrativo a un usuario administrativo y utilice únicamente el usuario raíz para realizar la ejecución tareas que requieren acceso de usuario raíz.

AWS le enviará un email de confirmación luego de completar el proceso de registro. Puede ver la actividad de la cuenta y administrar la cuenta en cualquier momento entrando en https://aws.amazon.com/ y seleccionando My Account (Mi cuenta).

Crear un usuario administrativo

Después de registrarse para obtener una Cuenta de AWS, cree un usuario administrativo para que no utilice el usuario raíz en las tareas cotidianas.

Proteger su Usuario raíz de la cuenta de AWS

1. Inicie sesión en AWS Management Console como propietario de cuenta eligiendo Usuario raíz e ingrese el email de su Cuenta de AWS. En la siguiente página, escriba su contraseña.

   Para obtener ayuda para iniciar sesión con el usuario raíz, consulte Signing in as the root user (Iniciar sesión como usuario raíz) en la Guía del usuario de AWS Sign-In.
2. Active la autenticación multifactor (MFA) para el usuario raíz.

   Para obtener instrucciones, consulte Habilitar un dispositivo MFA virtual para el usuario raíz Cuenta de AWS (consola) en la Guía del usuario de IAM.

Crear un usuario administrativo

- Para las tareas administrativas diarias, conceda acceso administrativo a un usuario administrativo en AWS IAM Identity Center (successor to AWS Single Sign-On).

Para obtener instrucciones, consulte Introducción en la Guía del usuario de AWS IAM Identity Center (successor to AWS Single Sign-On).

Iniciar sesión como usuario administrativo

- Para iniciar sesión con el usuario del Centro de identidades de IAM, utilice la URL de inicio de sesión que se envió a la dirección de correo electrónico cuando creó el usuario del Centro de identidades de IAM.

  Para obtener ayuda para iniciar sesión con un usuario del Centro de identidades de IAM, consulte Iniciar sesión en el portal de acceso de AWS en la Guía del usuario de AWS Sign-In.

Seguridad en Amazon WorkDocs

La seguridad en la nube de AWS es la mayor prioridad. Como cliente de AWS, se beneficia de una arquitectura de red y un centro de datos que se han diseñado para satisfacer los requisitos de seguridad de las organizaciones más exigentes.

La seguridad es una responsabilidad compartida entre AWS y usted. El modelo de responsabilidad compartida la describe como seguridad de la nube y seguridad en la nube:

- Seguridad de la nube: AWS es responsable de proteger la infraestructura que ejecuta los servicios de AWS en la nube de AWS. AWS también proporciona servicios que puede utilizar de forma segura. Auditores externos prueban y verifican periódicamente la eficacia de nuestra seguridad en el marco de los programas de conformidad de AWS. Para obtener más información sobre los programas de cumplimiento que se aplican a AmazonWorkDocs, consulte AWSServices in Scope by Compliance Program.
- Seguridad en la nube: el AWS servicio que utiliza determina su responsabilidad. También es responsable de otros factores, incluida la confidencialidad de los datos, los requisitos de la empresa y la legislación y los reglamentos aplicables. Los temas de esta sección le ayudan a entender cómo aplicar el modelo de responsabilidad compartida al utilizar AmazonWorkDocs.

> **Note**
>
> Los usuarios de una WorkDocs organización determinada pueden colaborar con usuarios ajenos a esa organización enviando un enlace o una invitación a un archivo. Revisa la configuración de enlaces compartidos (p. 36) de tu sitio y selecciona la opción que mejor se adapte a los requisitos de tu empresa.

En los siguientes temas se muestra cómo configurar Amazon WorkDocs para cumplir sus objetivos de seguridad y cumplimiento. También aprenderás a utilizar otros AWS servicios que te ayudan a supervisar y proteger tus WorkDocs recursos de Amazon.

Temas

Gestión de identidades y accesos para Amazon WorkDocs

AWS Identity and Access Management (IAM) es un Servicio de AWS que ayuda a los administradores a controlar de forma segura el acceso a los recursos de AWS. Los administradores de IAM controlan quién puede autenticarse (iniciar sesión) y autorizar (tener permisos) para usar los recursos de AmazonWorkDocs. IAM es un Servicio de AWS que se puede utilizar sin cargo adicional.

Temas

Público

La forma de utilizar AWS Identity and Access Management (IAM) varía según el trabajo que realices en AmazonWorkDocs.

Usuario del servicio: si utilizas el WorkDocs servicio de Amazon para realizar tu trabajo, el administrador te proporcionará las credenciales y los permisos que necesitas. A medida que utilices más WorkDocs funciones de Amazon para realizar tu trabajo, es posible que necesites permisos adicionales. Entender cómo se administra el acceso puede ayudarlo a solicitar los permisos correctos a su administrador. Si no puedes acceder a una función de AmazonWorkDocs, consultaSolución de problemas de WorkDocs identidad y acceso a Amazon (p. 14).

Administrador de servicios: si estás a cargo de WorkDocs los recursos de Amazon en tu empresa, es probable que tengas acceso completo a AmazonWorkDocs. Es su trabajo determinar a qué WorkDocs funciones y recursos de Amazon deben acceder los usuarios de su servicio. Luego, debe enviar solicitudes a su administrador de IAM para cambiar los permisos de los usuarios de su servicio. Revise la información de esta página para conocer los conceptos básicos de IAM. Para obtener más información sobre cómo su empresa puede utilizar IAM con AmazonWorkDocs, consulteCómo WorkDocs trabaja Amazon con IAM (p. 9).

Administrador de IAM: si es administrador de IAM, puede que desee obtener detalles sobre cómo puede redactar políticas para gestionar el acceso a Amazon. WorkDocs Para ver ejemplos de políticas WorkDocs basadas en identidades de Amazon que puede usar en IAM, consulte. Ejemplos de políticas WorkDocs basadas en identidades de Amazon (p. 11)

Autenticación con identidades

La autenticación es la manera de iniciar sesión en AWS mediante credenciales de identidad. Debe estar autenticado (haber iniciado sesión en AWS) como el Usuario raíz de la cuenta de AWS, como un usuario de IAM o asumiendo un rol de IAM.

Puede iniciar sesión en AWS como una identidad federada mediante las credenciales proporcionadas a través de una fuente de identidad. AWS IAM Identity Center (successor to AWS Single Sign-On) Los usuarios (IAM Identity Center), la autenticación de inicio de sesión único de su empresa y sus credenciales de Google o Facebook son ejemplos de identidades federadas. Al iniciar sesión como identidad federada, su administrador habrá configurado previamente la federación de identidades mediante roles de IAM. Cuando accede a AWS mediante la federación, está asumiendo un rol de forma indirecta.

Según el tipo de usuario que sea, puede iniciar sesión en la AWS Management Console o en el portal de acceso AWS. Para obtener más información sobre el inicio de sesión en AWS, consulte Cómo iniciar sesión en su Cuenta de AWS en la Guía del usuario de AWS Sign-In.

Si accede AWS mediante programación, AWS proporciona un kit de desarrollo de software (SDK) y una interfaz de línea de comandos (CLI) para firmar criptográficamente sus solicitudes mediante sus credenciales. Si no usa las herramientas de AWS, debe firmar usted mismo las solicitudes. Para obtener más información sobre cómo utilizar el método recomendado para firmar las solicitudes usted mismo, consulte Firmar las solicitudes de AWS API en la Guía del usuario de IAM.

Independientemente del método de autenticación que use, es posible que deba proporcionar información de seguridad adicional. Por ejemplo, AWS le recomienda el uso de la autenticación multifactor (MFA) para aumentar la seguridad de su cuenta. Para obtener más información, consulte Autenticación multifactor en la Guía del usuario de AWS IAM Identity Center (successor to AWS Single Sign-On) y Uso de la autenticación multifactor (MFA) en AWS en la Guía del usuario de IAM.

Usuarios y grupos de IAM

Un usuario de IAM es una identidad de la Cuenta de AWS que dispone de permisos específicos para una sola persona o aplicación. Siempre que sea posible, recomendamos emplear credenciales temporales, en lugar de crear usuarios de IAM que tengan credenciales de larga duración como contraseñas y claves de acceso. No obstante, si tiene casos de uso específicos que requieran credenciales de larga duración con usuarios de IAM, recomendamos rotar las claves de acceso. Para obtener más información, consulte Rotar las claves de acceso periódicamente para casos de uso que requieran credenciales de larga duración en la Guía del usuario de IAM.

Un grupo de IAM es una identidad que especifica un conjunto de usuarios de IAM. No puede iniciar sesión como grupo. Puede usar los grupos para especificar permisos para varios usuarios a la vez. Los grupos facilitan la administración de los permisos de grandes conjuntos de usuarios. Por ejemplo, podría tener un grupo cuyo nombre fuese IAMAdmins y conceder permisos a dicho grupo para administrar los recursos de IAM.

Los usuarios son diferentes de los roles. Un usuario se asocia exclusivamente a una persona o aplicación, pero la intención es que cualquier usuario pueda asumir un rol que necesite. Los usuarios tienen credenciales permanentes a largo plazo y los roles proporcionan credenciales temporales. Para obtener más información, consulte Cuándo crear un usuario de IAM (en lugar de un rol) en la Guía del usuario de IAM.

IAM roles

Un rol de IAM es una identidad de la Cuenta de AWS que dispone de permisos específicos. Es similar a un usuario de IAM, pero no está asociado a una determinada persona. Puede asumir temporalmente un rol de IAM en la AWS Management Consolecambiando de roles. Puede asumir un rol llamando a una operación de la AWS CLI o de la API de AWS, o utilizando una URL personalizada. Para obtener más información acerca de los métodos para el uso de roles, consulte Uso de roles de IAM en la Guía del usuario de IAM.

Los roles de IAM con credenciales temporales son útiles en las siguientes situaciones:

- Acceso de usuario federado: para asignar permisos a una identidad federada, puede crear un rol y definir permisos para este. Cuando se autentica una identidad federada, se asocia la identidad al rol y se le conceden los permisos que están definidos en este. Para obtener información acerca de roles para federación, consulte Creación de un rol para un proveedor de identidades de terceros en la Guía del usuario de IAM. Si utiliza el Centro de identidades de IAM, debe configurar un conjunto de permisos. El Centro de identidades de IAM correlaciona el conjunto de permisos con un rol en IAM para controlar a qué pueden acceder las identidades después de autenticarse. Para obtener información acerca de los conjuntos de permisos, consulte Conjuntos de permisos en la Guía del usuario de AWS IAM Identity Center (successor to AWS Single Sign-On).
- Permisos de usuario de IAM temporales: un usuario de IAM puede asumir un rol de IAM para recibir temporalmente permisos distintos que le permitan realizar una tarea concreta.
- Acceso entre cuentas: puede utilizar un rol de IAM para permitir que alguien (una entidad principal de confianza) de otra cuenta acceda a los recursos de la cuenta. Los roles son la forma principal de conceder acceso entre cuentas. No obstante, con algunos Servicios de AWS se puede adjuntar una política directamente a un recurso (en lugar de utilizar un rol como representante). Para obtener información acerca de la diferencia entre los roles y las políticas basadas en recursos para el acceso entre cuentas, consulte Cómo los roles de IAM difieren de las políticas basadas en recursos en la Guía del usuario de IAM.
- Acceso entre servicios: algunos Servicios de AWS utilizan características de otros Servicios de AWS. Por ejemplo, cuando realiza una llamada en un servicio, es común que ese servicio ejecute aplicaciones en Amazon EC2 o almacene objetos en Amazon S3. Es posible que un servicio haga esto usando los permisos de la entidad principal, usando un rol de servicio o usando un rol vinculado a servicios.
  - Permisos principales: cuando utiliza un usuario o un rol de IAM para llevar a cabo acciones en AWS, se lo considera una entidad principal. Las políticas conceden permisos a una entidad principal. Cuando utiliza algunos servicios, es posible que realice una acción que desencadene otra acción en

un servicio diferente. En este caso, debe tener permisos para realizar ambas acciones. Para ver si una acción requiere acciones dependientes adicionales en una política, consulte la Referencia de autorizaciones de servicio.

- Rol de servicio: un rol de servicio es un rol de IAM que adopta un servicio para realizar acciones en su nombre. Un administrador de IAM puede crear, modificar y eliminar un rol de servicio desde IAM. Para obtener más información, consulte Creación de un rol para delegar permisos a un Servicio de AWS en la Guía del usuario de IAM.
- Rol vinculado a servicio: un rol vinculado a servicio es un tipo de rol de servicio que está vinculado a un Servicio de AWS. El servicio puede asumir el rol para realizar una acción en su nombre. Los roles vinculados a servicios aparecen en la Cuenta de AWS y son propiedad del servicio. Un administrador de IAM puede ver, pero no editar, los permisos de los roles vinculados a servicios.

- Aplicaciones que se ejecutan en Amazon EC2: puede utilizar un rol de IAM que le permita administrar credenciales temporales para las aplicaciones que se ejecutan en una instancia de EC2 y realizan solicitudes a la AWS CLI o a la API de AWS. Es preferible hacerlo de este modo a almacenar claves de acceso en la instancia de EC2. Para asignar un rol de AWS a una instancia de EC2 y ponerla a disposición de todas las aplicaciones, cree un perfil de instancia adjuntado a la instancia. Un perfil de instancia contiene el rol y permite a los programas que se ejecutan en la instancia de EC2 obtener credenciales temporales. Para obtener más información, consulte Uso de un rol de IAM para conceder permisos a aplicaciones que se ejecutan en instancias Amazon EC2 en la Guía del usuario de IAM.

Para obtener información sobre el uso de los roles de IAM, consulte Cuándo crear un rol de IAM (en lugar de un usuario) en la Guía del usuario de IAM.

Administración de acceso mediante políticas

Para controlar el acceso en AWS, se crean políticas y se asocian a identidades o recursos de AWS. Una política es un objeto de AWS que, cuando se asocia a una identidad o un recurso, define sus permisos. AWS evalúa estas políticas cuando una entidad principal (sesión de rol, usuario o usuario raíz) realiza una solicitud. Los permisos en las políticas determinan si la solicitud se permite o se deniega. Las mayoría de las políticas se almacenan en AWS como documentos JSON. Para obtener más información sobre la estructura y el contenido de los documentos de política JSON, consulte Información general de políticas JSON en la Guía del usuario de IAM.

Los administradores pueden utilizar las políticas JSON de AWS para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y bajo qué condiciones.

De forma predeterminada, los usuarios y los roles no tienen permisos. Un administrador de IAM puede crear políticas de IAM para conceder permisos a los usuarios para realizar acciones en los recursos que necesitan. A continuación, el administrador puede agregar las políticas de IAM a los roles y los usuarios pueden asumirlos.

Las políticas de IAM definen permisos para una acción independientemente del método que se utilice para realizar la operación. Por ejemplo, suponga que dispone de una política que permite la acción `iam:GetRole`. Un usuario con dicha política puede obtener información del usuario de la AWS Management Console, la AWS CLI o la API de AWS.

Políticas basadas en identidad

Las políticas basadas en identidad son documentos de políticas de permisos JSON que puede adjuntar a una identidad, como un usuario de IAM, un grupo de usuarios o un rol. Estas políticas controlan qué acciones pueden realizar los usuarios y los roles, en qué recursos y bajo qué condiciones. Para obtener más información sobre cómo crear una política basada en identidad, consulte Creación de políticas de IAM en la Guía del usuario de IAM.

Las políticas basadas en identidad pueden clasificarse además como políticas insertadas o políticas administradas. Las políticas insertadas se integran directamente en un único usuario, grupo o rol. Las

políticas administradas son políticas independientes que puede adjuntar a varios usuarios, grupos y roles de su Cuenta de AWS. Las políticas administradas incluyen las políticas administradas por AWS y las políticas administradas por el cliente. Para obtener más información acerca de cómo elegir una política administrada o una política insertada, consulte Elegir entre políticas administradas y políticas insertadas en la Guía del usuario de IAM.

Políticas basadas en recursos

Las políticas basadas en recursos son documentos de política JSON que se adjuntan a un recurso. Ejemplos de políticas basadas en recursos son las políticas de confianza de roles de IAM y las políticas de bucket de Amazon S3. En los servicios que admiten políticas basadas en recursos, los administradores de servicios pueden utilizarlos para controlar el acceso a un recurso específico. Para el recurso al que se adjunta la política, la política define qué acciones puede realizar una entidad principal especificada en ese recurso y en qué condiciones. Debe especificar una entidad principal en una política basada en recursos. Las entidades principales pueden incluir cuentas, usuarios, roles, usuarios federados o Servicios de AWS.

Las políticas basadas en recursos son políticas insertadas que se encuentran en ese servicio. No se puede utilizar políticas de IAM administradas por AWS en una política basada en recursos.

Listas de control de acceso

Las listas de control de acceso (ACL) controlan qué entidades principales (miembros de cuentas, usuarios o roles) tienen permisos para acceder a un recurso. Las ACL son similares a las políticas basadas en recursos, aunque no utilizan el formato de documento de política JSON.

Amazon S3, AWS WAF y Amazon VPC son ejemplos de servicios que admiten las ACL. Para obtener más información sobre las ACL, consulte Información general de Lista de control de acceso (ACL) en la Guía para desarrolladores de Amazon Simple Storage Service.

Otros tipos de políticas

AWS admite otros tipos de políticas adicionales menos frecuentes. Estos tipos de políticas pueden establecer el máximo de permisos que los tipos de políticas más frecuentes le otorgan.

- Límites de permisos: un límite de permisos es una característica avanzada que le permite establecer los permisos máximos que una política basada en identidad puede conceder a una entidad de IAM (usuario o rol de IAM). Puede establecer un límite de permisos para una identidad. Los permisos resultantes son la intersección de las políticas basadas en identidad de la entidad y los límites de permisos. Las políticas basadas en recursos que especifiquen el usuario o rol en el campo `Principal` no estarán restringidas por el límite de permisos. Una denegación explícita en cualquiera de estas políticas anulará el permiso. Para obtener más información sobre los límites de los permisos, consulte Límites de permisos para las entidades de IAM en la Guía del usuario de IAM.
- Políticas de control de servicio (SCP): las SCP son políticas de JSON que especifican los permisos máximos de una organización o una unidad organizativa en AWS Organizations. AWS Organizations es un servicio que le permite agrupar y administrar de manera centralizada varias Cuentas de AWS que posea su empresa. Si habilita todas las características en una organización, entonces podrá aplicar políticas de control de servicio (SCP) a una o todas sus cuentas. Una SCP limita los permisos para las entidades de las cuentas de miembros, incluido cada Usuario raíz de la cuenta de AWS. Para obtener más información acerca de Organizations y las SCP, consulte Funcionamiento de las SCP en la Guía del usuario de AWS Organizations.
- Políticas de sesión: las políticas de sesión son políticas avanzadas que se pasan como parámetro cuando se crea una sesión temporal mediante programación para un rol o un usuario federado. Los permisos de la sesión resultantes son la intersección de las políticas basadas en identidad del rol y las políticas de la sesión. Los permisos también pueden proceder de una política basada en recursos. Una denegación explícita en cualquiera de estas políticas anulará el permiso. Para obtener más información, consulte Políticas de sesión en la Guía del usuario de IAM.

Note

Amazon WorkDocs no admite políticas de control de servicios para organizaciones de Slack.

Varios tipos de políticas

Cuando se aplican varios tipos de políticas a una solicitud, los permisos resultantes son más complicados de entender. Para obtener información acerca de cómo AWS decide si permitir o no una solicitud cuando hay varios tipos de políticas implicados, consulte Lógica de evaluación de políticas en la Guía del usuario de IAM.

Cómo WorkDocs trabaja Amazon con IAM

Antes de utilizar IAM para gestionar el acceso a AmazonWorkDocs, debe comprender qué funciones de IAM están disponibles para su uso con Amazon. WorkDocs Para obtener una visión general de cómo Amazon WorkDocs y otros AWS servicios funcionan con IAM, consulte AWSlos servicios que funcionan con IAM en la Guía del usuario de IAM.

Temas

Políticas basadas en WorkDocs identidades de Amazon

Con las políticas basadas en identidad de IAM, puede especificar acciones permitidas o denegadas. Amazon WorkDocs admite acciones específicas. Para obtener más información acerca de los elementos que utiliza en una política de JSON, consulte Referencia de los elementos de las políticas de JSON de IAM en la Guía del usuario de IAM.

Acciones

Los administradores pueden utilizar las políticas JSON de AWS para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y bajo qué condiciones.

El elemento `Action` de una política JSON describe las acciones que puede utilizar para permitir o denegar el acceso en una política. Las acciones de la política generalmente tienen el mismo nombre que la operación de API de AWS asociada. Hay algunas excepciones, como acciones de solo permiso que no tienen una operación de API coincidente. También hay algunas operaciones que requieren varias acciones en una política. Estas acciones adicionales se denominan acciones dependientes.

Incluya acciones en una política para conceder permisos y así llevar a cabo la operación asociada.

Las acciones políticas en Amazon WorkDocs utilizan el siguiente prefijo antes de la acción:`workdocs:`. Por ejemplo, para conceder permiso a alguien para ejecutar la operación de la WorkDocs `DescribeUsers` API de Amazon, debes incluir la `workdocs:DescribeUsers` acción en su política. Las instrucciones de la política deben incluir un elemento `Action` o un elemento `NotAction`. Amazon WorkDocs define su propio conjunto de acciones que describen las tareas que puede realizar con este servicio.

Para especificar varias acciones en una única instrucción, sepárelas con comas del siguiente modo:

```
"Action": [
      "workdocs:DescribeUsers",
      "workdocs:CreateUser"
```

Puede utilizar caracteres comodín para especificar varias acciones (*). Por ejemplo, para especificar todas las acciones que comiencen con la palabra `Describe`, incluya la siguiente acción:

```
"Action": "workdocs:Describe*"
```

Note

Para garantizar la compatibilidad con versiones anteriores, incluya la `zocalo` acción. Por ejemplo:

```
"Action": [
"zocalo:*",
"workdocs:*"
],
```

Para ver una lista de WorkDocs las acciones de Amazon, consulte Acciones definidas por Amazon WorkDocs en la Guía del usuario de IAM.

Recursos

Amazon WorkDocs no admite la especificación de ARN de recursos en una política.

Claves de condición

Amazon WorkDocs no proporciona ninguna clave de condición específica del servicio, pero sí admite el uso de algunas claves de condición globales. Para ver todas las claves de condición globales de AWS, consulte Claves de contexto de condición globales de AWS en la Guía del usuario de IAM.

Ejemplos

Para ver ejemplos de políticas WorkDocs basadas en la identidad de Amazon, consulte. Ejemplos de políticas WorkDocs basadas en identidades de Amazon (p. 11)

Políticas basadas en WorkDocs recursos de Amazon

Amazon WorkDocs no admite políticas basadas en recursos.

Autorización basada en WorkDocs etiquetas de Amazon

Amazon WorkDocs no admite el etiquetado de recursos ni el control del acceso en función de etiquetas.

Funciones de Amazon WorkDocs IAM

Un rol de IAM es una entidad de la cuenta de AWS que dispone de permisos específicos.

Uso de credenciales temporales con Amazon WorkDocs

Recomendamos encarecidamente utilizar credenciales temporales para iniciar sesión en la federación, asumir una función de IAM o asumir una función de varias cuentas. Las credenciales de seguridad temporales se obtienen al llamar a operaciones de la AWS STS API como AssumeRoleo GetFederationToken.

Amazon WorkDocs admite el uso de credenciales temporales.

Roles vinculados a servicios

Los roles vinculados a servicios permiten a los servicios de AWS obtener acceso a los recursos de otros servicios para completar una acción en su nombre. Los roles vinculados a servicios aparecen en la cuenta

de IAM y son propiedad del servicio. Un administrador de IAM puede ver, pero no editar, los permisos de los roles vinculados a servicios.

Amazon WorkDocs no admite funciones vinculadas a servicios.

Roles de servicio

Esta característica permite que un servicio asuma un rol de servicio en su nombre. Este rol permite que el servicio obtenga acceso a los recursos de otros servicios para completar una acción en su nombre. Los roles de servicio aparecen en su cuenta de IAM y son propiedad de la cuenta. Esto significa que un administrador de IAM puede cambiar los permisos de este rol. Sin embargo, hacerlo podría deteriorar la funcionalidad del servicio.

Amazon WorkDocs no admite funciones de servicio.

Ejemplos de políticas WorkDocs basadas en identidades de Amazon

> **Note**
>
> Para mayor seguridad, cree usuarios federados en lugar de usuarios de IAM siempre que sea posible.

De forma predeterminada, los usuarios y roles de IAM no tienen permiso para crear o modificar WorkDocs recursos de Amazon. Tampoco pueden realizar tareas mediante la AWS Management Console, la AWS CLI, o la API de AWS. Un administrador de IAM debe crear políticas de IAM que concedan permisos a los usuarios y a los roles para realizar operaciones de la API concretas en los recursos especificados que necesiten. El administrador debe adjuntar esas políticas a los usuarios o grupos de IAM que necesiten esos permisos.

> **Note**
>
> Para garantizar la compatibilidad con versiones anteriores, incluya la `zocalo` acción en sus políticas. Por ejemplo:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Deny",
            "Action": [
            "zocalo:*",
            "workdocs:*"
            ],
            "Resource": "*"
        }
    ]
}
```

Para obtener más información acerca de cómo crear una política basada en identidad de IAM con estos documentos de políticas de JSON de ejemplo, consulte Creación de políticas en la pestaña JSON en la Guía del usuario de IAM.

Temas

- Prácticas recomendadas relativas a políticas (p. 12)
- Uso de la WorkDocs consola de Amazon (p. 12)
- Permitir a los usuarios consultar sus propios permisos (p. 13)
- Permitir a los usuarios el acceso de solo lectura a los recursos de Amazon WorkDocs (p. 13)

- Más ejemplos de políticas WorkDocs basadas en identidades de Amazon (p. 14)

Prácticas recomendadas relativas a políticas

Las políticas basadas en la identidad determinan si alguien puede crear, acceder o eliminar WorkDocs recursos de Amazon en tu cuenta. Estas acciones pueden generar costos adicionales para su Cuenta de AWS. Siga estas directrices y recomendaciones al crear o editar políticas basadas en identidad:

- Comience con las políticas administradas por AWS y continúe con los permisos de privilegio mínimo: a fin de comenzar a conceder permisos a los usuarios y las cargas de trabajo, utilice las políticas administradas por AWS, que conceden permisos para muchos casos de uso comunes. Están disponibles en la Cuenta de AWS. Se recomienda definir políticas administradas por el cliente de AWS específicas para sus casos de uso a fin de reducir aún más los permisos. Con el fin de obtener más información, consulte las políticas administradas por AWS o las políticas administradas por AWS para funciones de trabajo en la Guía de usuario de IAM.
- Aplique permisos de privilegio mínimo: cuando establezca permisos con políticas de IAM, conceda solo los permisos necesarios para realizar una tarea. Para ello, debe definir las acciones que se pueden llevar a cabo en determinados recursos en condiciones específicas, también conocidos como permisos de privilegios mínimos. Con el fin de obtener más información sobre el uso de IAM para aplicar permisos, consulte Políticas y permisos en IAM en la Guía de usuario de IAM.
- Use condiciones en las políticas de IAM para restringir aún más el acceso: puede agregar una condición a sus políticas para limitar el acceso a las acciones y los recursos. Por ejemplo, puede escribir una condición de política para especificar que todas las solicitudes deben enviarse utilizando SSL. También puede usar condiciones para conceder acceso a acciones de servicios si se emplean a través de un Servicio de AWS determinado, como por ejemplo AWS CloudFormation. Para obtener más información, consulte Elementos de la política JSON de IAM: condición en la Guía del usuario de IAM.
- Use el Analizador de acceso de IAM para validar las políticas de IAM con el fin de garantizar la seguridad y funcionalidad de los permisos: el Analizador de acceso de IAM valida políticas nuevas y existentes para que respeten el lenguaje (JSON) de las políticas de IAM y las prácticas recomendadas de IAM. IAM Access Analyzer proporciona más de 100 verificaciones de políticas y recomendaciones procesables para ayudar a crear políticas seguras y funcionales. Para obtener más información, consulte la política de validación del Analizador de acceso de IAM en la Guía de usuario de IAM.
- Solicite la autenticación multifactor (MFA): si se encuentra en una situación en la que necesita usuarios raíz o de IAM en su Cuenta de AWS, active la MFA para mayor seguridad. Para solicitar la MFA cuando se invocan las operaciones de la API, agregue las condiciones de MFA a sus políticas. Para obtener más información, consulte Configuración de acceso a una API protegida por MFA en la Guía de usuario de IAM.

Para obtener más información sobre las prácticas recomendadas de IAM, consulte las Prácticas recomendadas de seguridad en IAM en la Guía de usuario de IAM.

Uso de la WorkDocs consola de Amazon

Para acceder a la WorkDocs consola de Amazon, debes tener un conjunto mínimo de permisos. Estos permisos deben permitirle enumerar y ver los detalles de los WorkDocs recursos de Amazon en su AWS cuenta. Si creas una política basada en identidades que sea más restrictiva que los permisos mínimos requeridos, la consola no funcionará según lo previsto para las entidades de usuario o rol de IAM.

Para garantizar que esas entidades puedan utilizar la WorkDocs consola de Amazon, adjunte también las siguientes políticas AWS gestionadas a las entidades. Para obtener más información sobre cómo adjuntar políticas, consulte Agregar permisos a un usuario en la Guía del usuario de IAM.

- AmazonWorkDocsFullAccess
- AWSDirectoryServiceFullAccess

- Amazon EC2 FullAccess

Estas políticas otorgan al usuario acceso total a WorkDocs los recursos de Amazon, a las operaciones del Servicio de AWS directorio y a las operaciones de Amazon EC2 que Amazon WorkDocs necesita para funcionar correctamente.

No es necesario que conceda permisos mínimos para la consola a los usuarios que solo realizan llamadas a la AWS CLI o a la API de AWS. En su lugar, permite acceso únicamente a las acciones que coincidan con la operación de API que intenta realizar.

Permitir a los usuarios consultar sus propios permisos

En este ejemplo, se muestra cómo podría crear una política que permita a los usuarios de IAM ver las políticas administradas e insertadas que se adjuntan a la identidad de sus usuarios. Esta política incluye permisos para llevar a cabo esta acción en la consola o mediante programación con la AWS CLI o la API de AWS.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

Permitir a los usuarios el acceso de solo lectura a los recursos de Amazon WorkDocs

La siguiente AmazonWorkDocsReadOnlyAccesspolítica AWS gestionada otorga a los usuarios de IAM acceso de solo lectura a los recursos de Amazon. WorkDocs La política da al usuario acceso a todas las WorkDocs `Describe` operaciones de Amazon. El acceso a las dos operaciones de Amazon EC2 es necesario para que Amazon WorkDocs pueda obtener una lista de sus VPC y subredes. El acceso a la operación AWS Directory Service de `DescribeDirectories` es necesario para obtener información sobre los directorios de AWS Directory Service.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "workdocs:Describe*",
                "ds:DescribeDirectories",
                "ec2:DescribeVpcs",
                "ec2:DescribeSubnets"
            ],
            "Resource": "*"
        }
    ]
}
```

Más ejemplos de políticas WorkDocs basadas en identidades de Amazon

Los administradores de IAM pueden crear políticas adicionales para permitir que un rol o usuario de IAM acceda a la API de AmazonWorkDocs. Para obtener más información, consulte Autenticación y control de acceso para aplicaciones administrativas en la Guía para WorkDocs desarrolladores de Amazon.

Solución de problemas de WorkDocs identidad y acceso a Amazon

Utilice la siguiente información para diagnosticar y solucionar problemas comunes que puedan surgir al trabajar con Amazon WorkDocs e IAM.

Temas

No estoy autorizado a realizar ninguna acción en Amazon WorkDocs

Si la AWS Management Console le indica que no está autorizado para llevar a cabo una acción, debe ponerse en contacto con su administrador para recibir ayuda. Su administrador es la persona que le facilitó su nombre de usuario y contraseña.

No estoy autorizado a realizar iam: PassRole

Si recibes un error que indica que no estás autorizado a realizar la `iam:PassRole` acción, debes actualizar tus políticas para que puedas transferir un rol a AmazonWorkDocs.

Algunos servicios de Servicios de AWS le permiten transferir un rol existente a dicho servicio en lugar de crear un nuevo rol de servicio o uno vinculado al servicio. Para ello, debe tener permisos para transferir el rol al servicio.

El siguiente ejemplo de error se produce cuando un usuario de IAM llamado `marymajor` intenta utilizar la consola para realizar una acción en AmazonWorkDocs. Sin embargo, la acción requiere que el servicio cuente con permisos que otorga un rol de servicio. Mary no tiene permisos para transferir el rol al servicio.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform: iam:PassRole
```

En este caso, las políticas de Mary se deben actualizar para permitirle realizar la acción `iam:PassRole`.

Si necesita ayuda, póngase en contacto con su administrador de AWS. El administrador es la persona que le proporcionó las credenciales de inicio de sesión.

Quiero permitir que personas ajenas a mi AWS cuenta accedan a mis WorkDocs recursos de Amazon

Puede crear un rol que los usuarios de otras cuentas o las personas externas a la organización puedan utilizar para acceder a sus recursos. Puede especificar una persona de confianza para que asuma el rol. En el caso de los servicios que admitan las políticas basadas en recursos o las listas de control de acceso (ACL), puede utilizar dichas políticas para conceder a las personas acceso a sus recursos.

Para obtener más información, consulte lo siguiente:

- Para saber si Amazon WorkDocs admite estas funciones, consulteCómo WorkDocs trabaja Amazon con IAM (p. 9).
- Para obtener información acerca de cómo proporcionar acceso a los recursos de las Cuentas de AWS de su propiedad, consulte Proporcionar acceso a un usuario de IAM a otra Cuenta de AWS de la que es propietario en la Guía del usuario de IAM.
- Para obtener información acerca de cómo proporcionar acceso a los recursos a Cuentas de AWS de terceros, consulte Proporcionar acceso a Cuentas de AWS que son propiedad de terceros en la Guía del usuario de IAM.
- Para obtener información sobre cómo proporcionar acceso mediante una identidad federada, consulte Proporcionar acceso a usuarios autenticados externamente (identidad federada) en la Guía del usuario de IAM.
- Para obtener información sobre la diferencia entre los roles y las políticas basadas en recursos para el acceso entre cuentas, consulte Cómo los roles de IAM difieren de las políticas basadas en recursos en la Guía del usuario de IAM.

Registro y monitorización en Amazon WorkDocs

Los administradores WorkDocs del sitio de Amazon pueden ver y exportar el feed de actividades de todo un sitio. También se pueden utilizar AWS CloudTrail para capturar eventos desde la WorkDocs consola de Amazon.

Temas

Exportación del feed de actividades de todo el sitio

Los administradores pueden ver y exportar la fuente de actividades de un sitio completo. Para utilizar esta función, primero debe instalar Amazon WorkDocs Companion. Para instalar Amazon WorkDocs Companion, consulta Aplicaciones e integraciones para Amazon WorkDocs.

Para ver y exportar la fuente de actividades de un sitio completo

1. En la aplicación web, seleccione Actividad.

2. Selecciona Filtrar y, a continuación, mueve el control deslizante de actividad de todo el sitio para activar el filtro.
3. Seleccione los filtros Tipo de actividad, elija una opción en Fecha de modificación y después elija Aplicar.
4. Cuando aparezcan los resultados de la fuente de actividades filtrada, busque por archivo, carpeta o nombre de usuario para acotar los resultados. También puede añadir o eliminar filtros según sea necesario.
5. Elija Exportar para exportar la fuente de actividades a archivos `.csv` y `.json` en su escritorio. El sistema exporta los archivos a una de las siguientes ubicaciones:

   - Windows: WorkDocsDownloadscarpeta en la carpeta de descargas de su PC
   - macOS: `/users/`**`username`**`/WorkDocsDownloads/folder`

   El archivo exportado refleja los filtros que aplique.

   > **Note**
   >
   > Los usuarios que no sean administradores solo pueden ver y exportar la fuente de actividades de su propio contenido. Para obtener más información, consulte Visualización del feed de actividades en la Guía del WorkDocs usuario de Amazon.

Se usa AWS CloudTrail para registrar llamadas a WorkDocs la API de Amazon

Puede utilizarAWS CloudTrail; para registrar las llamadas a la WorkDocs API de Amazon. CloudTrailproporciona un registro de las acciones realizadas por un usuario, rol o AWS servicio en AmazonWorkDocs. CloudTrailcaptura todas las llamadas a la API de Amazon WorkDocs como eventos, incluidas las llamadas desde la WorkDocs consola de Amazon y las llamadas de código a las WorkDocs API de Amazon.

Si crea una ruta, puede habilitar la entrega continua de CloudTrail eventos a un bucket de Amazon S3, incluidos los eventos de AmazonWorkDocs. Si no configura un registro de seguimiento, podrá ver los eventos más recientes en la consola de CloudTrail, en Event history (Historial de eventos).

La información recopilada por CloudTrail incluye las solicitudes, las direcciones IP desde las que se realizaron las solicitudes, los usuarios que las realizaron y las fechas de las solicitudes.

Para obtener más información sobre CloudTrail, consulte la AWS CloudTrailGuía del usuario de .

WorkDocsInformación de Amazon en CloudTrail

CloudTrail se habilita en una cuenta de AWS al crearla. Cuando se produce una actividad en AmazonWorkDocs, esa actividad se registra en un CloudTrail evento junto con otros eventos del AWS servicio en el historial de eventos. Puede ver, buscar y descargar los últimos eventos de la cuenta de AWS. Para obtener más información, consulte Visualización de eventos con el historial de eventos de CloudTrail.

Para obtener un registro continuo de los eventos de tu AWS cuenta, incluidos los eventos de AmazonWorkDocs, crea una ruta. Una ruta permite CloudTrail entregar archivos de registro a un bucket de Amazon S3. De forma predeterminada, cuando se crea un registro de seguimiento en la consola, el registro de seguimiento se aplica a todas las regiones. El registro de seguimiento registra los eventos de todas las regiones de la partición de AWS y envía los archivos de registro al bucket de Amazon S3 especificado. También puede configurar otros servicios de AWS para analizar y actuar en función de los datos de eventos recopilados en los registros de CloudTrail. Para obtener más información, consulte:

- Introducción a la creación de registros de seguimiento

- Servicios e integraciones compatibles con CloudTrail
- Configuración de notificaciones de Amazon SNS para CloudTrail
- Recepción de archivos de registros de CloudTrail desde varias regiones y Recepción de archivos de registro de CloudTrail de varias cuentas

Todas WorkDocs las acciones de Amazon se registran CloudTrail y documentan en la referencia de la WorkDocs API de Amazon. Por ejemplo, las llamadas a las secciones `CreateFolder`, `DeactivateUser` y `UpdateDocument` generan entradas en los archivos de registro de CloudTrail.

Cada entrada de registro o evento contiene información sobre quién generó la solicitud. La información de identidad del usuario le ayuda a determinar lo siguiente:

- Si la solicitud se realizó con las credenciales raíz o del usuario de IAM de .
- Si la solicitud se realizó con credenciales de seguridad temporales de un rol o fue un usuario federado.
- Si la solicitud la realizó otro servicio de AWS.

Para obtener más información, consulte el elemento userIdentity de CloudTrail.

Descripción de las entradas de los archivos de WorkDocs registro de Amazon

Un registro de seguimiento es una configuración que permite la entrega de eventos como archivos de registros en un bucket de Amazon S3 que especifique. Los archivos de registro de CloudTrail contienen una o varias entradas de registro. Un evento representa una solicitud específica realizada desde un origen y contiene información sobre la acción solicitada, la fecha y la hora de la acción, los parámetros de la solicitud, etc. Los archivos de registro de CloudTrail no son un rastro de la pila ordenada de las llamadas a la API públicas, por lo que no aparecen en ningún orden específico.

Amazon WorkDocs genera diferentes tipos de CloudTrail entradas, las del plano de control y las del plano de datos. La diferencia importante entre ambos es que la identidad de usuario para las entradas del plano de control es un usuario de IAM. La identidad de usuario para las entradas del plano de datos es el usuario del WorkDocs directorio de Amazon.

> **Note**
>
> Para mayor seguridad, cree usuarios federados en lugar de usuarios de IAM siempre que sea posible.

La información confidencial, como contraseñas, tokens de autenticación, comentarios de archivos y contenido de archivos aparecen en las entradas de log. Aparecen como HIDDEN_DUE_TO_SECURITY_REASONS en los registros. CloudTrail Aparecen como HIDDEN_DUE_TO_SECURITY_REASONS en los registros. CloudTrail

El siguiente ejemplo muestra dos entradas de CloudTrail registro de AmazonWorkDocs: el primer registro corresponde a una acción del plano de control y el segundo a una acción del plano de datos.

```
{
  Records : [
    {
      "eventVersion" : "1.01",
      "userIdentity" :
      {
        "type" : "IAMUser",
        "principalId" : "user_id",
        "arn" : "user_arn",
        "accountId" : "account_id",
```

```
        "accessKeyId" : "access_key_id",
        "userName" : "user_name"
      },
      "eventTime" : "event_time",
      "eventSource" : "workdocs.amazonaws.com",
      "eventName" : "RemoveUserFromGroup",
      "awsRegion" : "region",
      "sourceIPAddress" : "ip_address",
      "userAgent" : "user_agent",
      "requestParameters" :
      {
        "directoryId" : "directory_id",
        "userSid" : "user_sid",
        "group" : "group"
      },
      "responseElements" : null,
      "requestID" : "request_id",
      "eventID" : "event_id"
    },
    {
      "eventVersion" : "1.01",
      "userIdentity" :
      {
        "type" : "Unknown",
        "principalId" : "user_id",
        "accountId" : "account_id",
        "userName" : "user_name"
      },
      "eventTime" : "event_time",
      "eventSource" : "workdocs.amazonaws.com",
      "awsRegion" : "region",
      "sourceIPAddress" : "ip_address",
      "userAgent" : "user_agent",
      "requestParameters" :
      {
        "AuthenticationToken" : "**-redacted-**"
      },
      "responseElements" : null,
      "requestID" : "request_id",
      "eventID" : "event_id"
    }
  ]
}
```


Validación de conformidad para Amazon WorkDocs

Para saber si un Servicio de AWS está incluido en el ámbito de programas de conformidad específicos, consulte Servicios de AWS en el ámbito del programa de conformidad y escoja el programa de conformidad que le interese. Para obtener información general, consulte Programas de conformidad de AWS.

Puede descargar los informes de auditoría de terceros utilizando AWS Artifact. Para obtener más información, consulte Descarga de informes en AWS Artifact.

Su responsabilidad de conformidad al utilizar Servicios de AWS se determina en función de la sensibilidad de los datos, los objetivos de cumplimiento de su empresa y la legislación y los reglamentos correspondientes. AWS proporciona los siguientes recursos para ayudar con la conformidad:

- Guías de inicio rápido de seguridad y conformidad: estas guías de implementación tratan consideraciones sobre arquitectura y ofrecen pasos para implementar los entornos de referencia centrados en la seguridad y la conformidad en AWS.

- Architecting for HIPAA Security and Compliance on Amazon Web Services (Arquitectura para la seguridad y el cumplimiento de la HIPAA en Amazon Web Services): en este documento técnico, se describe cómo las empresas pueden utilizar AWS para crear aplicaciones aptas para HIPAA.

  Note

  No todos los Servicios de AWS son aptos para HIPAA. Para obtener más información, consulte la Referencia de servicios aptos para HIPAA.
- Recursos de conformidad de AWS: este conjunto de manuales y guías podría aplicarse a su sector y ubicación.
- Evaluación de recursos con reglas en la Guía para desarrolladores de AWS Config: el servicio AWS Config evalúa en qué medida las configuraciones de sus recursos cumplen las prácticas internas, las directrices del sector y las normativas.
- AWS Security Hub: este Servicio de AWS proporciona una visión completa de su estado de seguridad en AWS. Security Hub utiliza controles de seguridad para evaluar sus recursos de AWS y comprobar su cumplimiento con los estándares y las prácticas recomendadas del sector de la seguridad. Para obtener una lista de los servicios y controles compatibles, consulte la referencia de controles de Security Hub.
- AWS Audit Manager: este servicio de Servicio de AWS lo ayuda a auditar continuamente el uso de AWS con el fin de simplificar la forma en que administra el riesgo y la conformidad con las normativas y los estándares del sector.

Resiliencia en Amazon WorkDocs

La infraestructura global de AWS se compone de regiones y zonas de disponibilidad de AWS. AWS Las regiones proporcionan varias zonas de disponibilidad físicamente independientes y aisladas que se encuentran conectadas mediante redes con un alto nivel de rendimiento y redundancia, además de baja latencia. Con las zonas de disponibilidad, puede diseñar y utilizar aplicaciones y bases de datos que realizan una conmutación por error automática entre zonas de disponibilidad sin interrupciones. Las zonas de disponibilidad tienen una mayor disponibilidad, tolerancia a errores y escalabilidad que las infraestructuras tradicionales de centros de datos únicos o múltiples.

Para obtener más información sobre las regiones y zonas de disponibilidad de AWS, consulte Infraestructura global de AWS.

Seguridad de la infraestructura en Amazon WorkDocs

Como servicio gestionado, Amazon WorkDocs está protegido por los procedimientos de seguridad de la red AWS global. Para obtener más información, consulte la seguridad de la infraestructura en AWS Identity and Access Management en la Guía del usuario de IAM y las prácticas recomendadas para la seguridad, la identidad y el cumplimiento en el Centro de AWS arquitectura.

Utiliza las llamadas a la API AWS publicadas para acceder a Amazon WorkDocs a través de la red. Los clientes deben admitir Transport Layer Security (TLS) 1.2 y se recomienda utilizar TLS 1.3. Los clientes también deben admitir suites de cifrado con un secreto directo perfecto, como Ephemeral Diffie-Hellman o Elliptic Curve Ephemeral Diffie-Hellman. La mayoría de los sistemas modernos como Java 7 y posteriores son compatibles con estos modos.

Además, las solicitudes deben estar firmadas mediante un ID de clave de acceso y una clave de acceso secreta que esté asociada a una entidad de seguridad de IAM. También puede utilizar AWS Security Token Service (AWS STS) para generar credenciales de seguridad temporales para firmar solicitudes.

Introducción a Amazon WorkDocs

Amazon WorkDocs usa un directorio para almacenar y administrar la información de la organización para sus usuarios y sus documentos. A su vez, usted adjunta un directorio a un sitio cuando aprovisiona ese sitio. Cuando lo haces, una WorkDocs función de Amazon llamada Activación automática añade a los usuarios del directorio al sitio como usuarios gestionados, lo que significa que no necesitan credenciales independientes para iniciar sesión en tu sitio y pueden compartir archivos y colaborar en ellos. Cada usuario tiene 1 TB de almacenamiento a menos que compre más.

Ya no es necesario añadir y activar usuarios manualmente, aunque aún puede hacerlo. También puede cambiar las funciones y los permisos de los usuarios siempre que lo necesite. Para obtener más información sobre cómo hacerloInvitar y gestionar WorkDocs usuarios de Amazon (p. 34), consulte más adelante en esta guía.

Si necesita crear directorios, puede:

- Cree un directorio de AD sencillo.
- Cree un AD Connector para conectarse a su directorio en las instalaciones.
- Permita WorkDocs que Amazon trabaje con unAWS directorio existente.
- Haga que Amazon WorkDocs cree un directorio para usted.

Asimismo, puede crear una relación de confianza entre su directorio de AD y un directorio de AWS Managed Microsoft AD.

> Note
>
> Si pertenece a un programa de cumplimiento, como PCI, FedRAMP o DoD, debe configurar unAWS Managed Microsoft AD directorio para cumplir con los requisitos de cumplimiento. En los pasos de esta sección se explica cómo utilizar un directorio de Microsoft AD existente. Para obtener información sobre la creación de un directorio de Microsoft AD, consulte Microsoft AD administrado por AWS en la Guía de administración delAWS Directory Service.

Contenido

Crear un WorkDocs sitio de Amazon

En las siguientes secciones se explica cómo se configura un nuevo WorkDocs sitio de Amazon.

Tareas

Antes de empezar

Debe tener los siguientes elementos antes de crear un WorkDocs sitio de Amazon.

- UnaAWS cuenta para crear y administrar WorkDocs sitios de Amazon. Sin embargo, los usuarios no necesitan unaAWS cuenta para conectarse y utilizar Amazon WorkDocs. Para obtener más información, consulte requisitos previos de Amazon WorkDocs (p. 2).
- Si tiene previsto utilizar Simple AD, debe cumplir los requisitos previos identificados en los requisitos previos Simple AD de la Guía deAWS Directory Service administración.
- UnAWS Managed Microsoft AD directorio si pertenece a un programa de cumplimiento, como PCI, FedRAMP o DoD. En los pasos de esta sección se explica cómo utilizar un directorio de Microsoft AD existente. Para obtener información sobre la creación de un directorio de Microsoft AD, consulte Microsoft AD administrado por AWS en la Guía de administración delAWS Directory Service.
- Información del perfil del administrador, incluidos el nombre y apellidos y una dirección de correo electrónico.

Crear un WorkDocs sitio de Amazon

Sigue estos pasos para crear un WorkDocs sitio de Amazon en cuestión de minutos.

Para crear el WorkDocs sitio de Amazon

1. Abre la WorkDocs consola de Amazon en https://console.aws.amazon.com/zocalo/.
2. En la página principal de la consola, en Crear un WorkDocs sitio, selecciona Comenzar ahora.

   -O BIEN-

   En el panel de navegación, elija Mis sitios y, en la página Administrar sus WorkDocs sitios, elija Crear un WorkDocs sitio.

   Lo que ocurre a continuación depende de si dispone de un directorio.

   - Si tiene un directorio, aparece la página Seleccione un directorio, que le permite elegir un directorio existente o crear un directorio.
   - Si no tiene un directorio, aparece la página Configurar un tipo de directorio, que le permite crear un directorio de Simple AD o AD Connector.

   En los siguientes pasos se explica cómo realizar ambas tareas.

   #### Para usar un directorio existente

   1. Abra la lista de directorios disponibles y elija el directorio que desee usar.
   2. Elija Habilitar directorio.

   #### Para crear un directorio

   1. Repita los pasos 1 y 2 anteriores.

      En este momento, lo que haga dependerá de si desea utilizar Simple AD o crear un AD Connector.

      #### Para usar Simple AD

      a. Elige Simple AD y, a continuación, selecciona Siguiente.

         Aparece la página Crear un sitio de Simple AD.

      b. En Punto de acceso, en el cuadro URL del sitio, introduzca la URL del sitio.

c. En Establecer WorkDocs administrador, introduce la dirección de correo electrónico, el nombre y los apellidos del administrador.
d. Si es necesario, complete las opciones en Detalles del directorio y configuración de VPC.
e. Elige Crear un sitio de Simple AD.

Para crear un directorio de AD Connector

a. Elige AD Connector y, a continuación, selecciona Siguiente.

   Aparece la página del sitio Create AD Connector.
b. Complete todos los campos de la sección Detalles del directorio.
c. En Punto de acceso, en el cuadro URL del sitio, introduce la URL de tu sitio.
d. Si lo desea, complete los campos opcionales de la configuración de VPC.
e. Elija Crear sitio de AD Connector.

Amazon WorkDocs hace lo siguiente:

- Si has elegido Configurar una VPC en mi nombre en el paso 4 anterior, Amazon WorkDocs creará una VPC para ti. Un directorio de la VPC almacena la información del usuario y WorkDocs del sitio de Amazon.
- Si utilizaste Simple AD, Amazon WorkDocs crea un usuario de directorio y lo establece como WorkDocs administrador de Amazon. Si ha creado un directorio de AD Connector, Amazon WorkDocs establece el usuario de directorio existente que proporcionó como WorkDocs administrador.
- Si has utilizado un directorio existente, Amazon te WorkDocs pedirá que introduzcas el nombre de usuario del WorkDocs administrador de Amazon. El usuario debe ser un miembro del directorio.

Note

Amazon WorkDocs no notifica a los usuarios sobre el nuevo sitio. Debes comunicarles la URL y hacerles saber que no necesitan un inicio de sesión por separado para usar el sitio.

Habilitación del inicio de sesión único

AWS Directory Servicepermite a los usuarios acceder a Amazon WorkDocs desde un ordenador unido al mismo directorio en el que Amazon WorkDocs está registrado, sin introducir las credenciales por separado. WorkDocs Los administradores de Amazon pueden habilitar el inicio de sesión único mediante laAWS Directory Service consola. Para obtener más información, consulte Inicio de sesión único en la GuíaAWS Directory Service de administración.

Una vez que el WorkDocs administrador de Amazon habilite el inicio de sesión único, es posible que los usuarios WorkDocs del sitio de Amazon también tengan que modificar la configuración de su navegador web para permitir el inicio de sesión único. Para obtener más información, consulte Inicio de sesión único para IE y Chrome e Inicio de sesión único para Firefox en la Guía deAWS Directory Service administración.

Habilitar la autenticación multifactor

Utilice la consola de servicios deAWS directorio en https://console.aws.amazon.com/directoryservicev2/ para habilitar la autenticación multifactorial en su directorio de AD Connector. Para habilitar la MFA, debe tener una solución de MFA que sea un servidor de servicio de usuario con acceso telefónico (RADIUS) de autenticación remota o debe tener un complemento de MFA para un servidor RADIUS ya implementado en

su infraestructura local. La solución de MFA debería implementar claves de acceso de un solo uso (OTP) que los usuarios obtienen de un dispositivo de hardware o de un software que se ejecuta en un dispositivo como un teléfono móvil.

RADIUS es un protocolo cliente/servidor estándar del sector que proporciona autenticación, autorización y administración de cuentas para permitir a los usuarios conectarse a los servicios de red. Microsoft AD administrado por AWS incluye un cliente RADIUS que se conecta al servidor RADIUS en el que ha implementado su solución de MFA. El servidor RADIUS valida el nombre de usuario y el código de OTP. Si su servidor RADIUS valida correctamente al usuario, AWS Managed Microsoft AD autentica al usuario contra AD. Tras la autenticación de correcta en AD, los usuarios pueden obtener acceso a la aplicación de AWS. La comunicación entre el cliente RADIUS de Microsoft AD administrado por AWS y su servidor RADIUS requiere que configure grupos de seguridad de AWS que permitan la comunicación a través del puerto 1812.

Para obtener más información, consulte Habilitar la autenticación multifactor para AWS Managed Microsoft AD en la Guía de administración deAWS Directory Service Administration Guide.

> **Note**
>
> La autenticación multifactorial no está disponible para los directorios de Simple AD.

Promover un usuario a administrador

Usas la WorkDocs consola de Amazon para ascender a un usuario a administrador. Siga estos pasos.

Para promocionar un usuario a administrador

1. Abre la WorkDocs consola de Amazon en https://console.aws.amazon.com/zocalo/.
2. En el panel de navegación, seleccione Mis sitios.

   Aparece la página Administra tus WorkDocs sitios.
3. Seleccione el botón situado junto al sitio deseado, elija Acciones y, a continuación, elija Establecer un administrador.

   Aparece el cuadro de diálogo Establecer WorkDocs administrador.
4. En el cuadro Nombre de usuario, introduce el nombre de usuario de la persona a la que quieres ascender y, a continuación, selecciona Establecer administrador.

También puedes usar el panel de control del administrador WorkDocs del sitio de Amazon para degradar a un administrador. Para obtener más información, consulte Editar usuarios (p. 38).

Administrar Amazon WorkDocs desde laAWS consola

Utiliza estas herramientas para administrar sus WorkDocs sitios de Amazon:

- LaAWS consola en https://console.aws.amazon.com/zocalo/.
- El panel de control del administrador del sitio, disponible para los administradores de todos los WorkDocs sitios de Amazon.

Cada una de esas herramientas proporciona un conjunto diferente de acciones, y en los temas de esta sección se explican las acciones proporcionadas por laAWS consola. Para obtener información sobre el panel de control del administrador del sitio, consulteAdministrar Amazon WorkDocs desde el panel de control del administrador del sitio (p. 27).

Configuración de administradores del sitio

Si es administrador, puede dar a los usuarios acceso al panel de control del sitio y a las acciones que proporciona.

Para configurar un administrador

1. Abre la WorkDocs consola de Amazon en https://console.aws.amazon.com/zocalo/.
2. En el panel de navegación, seleccione Sites (Sitios).

   Aparece la página Administra tus WorkDocs sitios, que muestra una lista de tus sitios.
3. Elija el botón situado junto al sitio situado al lado del archivo cuyo contenido desea establecer un administrador.
4. Abra la lista de acciones y seleccione Establecer un administrador.

   Aparece el cuadro de diálogo Establecer WorkDocs administrador.
5. En el cuadro Nombre de usuario, introduce el nombre del nuevo administrador y, a continuación, selecciona Establecer administrador.

ReReReReReReReReReRe

ReReReReReReReReReReReReReReReReReReReReReReReReReReReReRe

Para reenviar el correo electrónico de invitación

1. Abre la WorkDocs consola de Amazon en https://console.aws.amazon.com/zocalo/.
2. En el panel de navegación, seleccione Sites (Sitios).

   Aparece la página Administra tus WorkDocs sitios, que muestra una lista de tus sitios.
3. Elija el botón situado al lado del sitio al que desea reenviar el correo electrónico.
4. Abre la lista de acciones y selecciona Reenviar el correo electrónico de invitación.

   En la parte superior de la página, aparece un mensaje de confirmación en un banner verde

Gestión de la autenticación multifactorial

Puedes habilitar la autenticación multifactorial después de crear un WorkDocs sitio de Amazon. Para obtener más información acerca de la autenticación, consulte Habilitar la autenticación multifactor (p. 22).

Configuración de las URL del sitio

> Note
>
> Si ha seguido el proceso de creación del sitio enIntroducción a Amazon WorkDocs (p. 20), ha introducido una URL del sitio. Como resultado, Amazon WorkDocs hace que el comando Establecer URL del sitio no esté disponible, ya que solo puede configurar una URL una vez. Solo debes seguir estos pasos si implementas Amazon WorkSpaces y lo integras con Amazon WorkDocs. El proceso de WorkSpaces integración de Amazon requiere que introduzcas un número de serie en lugar de la URL de un sitio, por lo que tendrás que introducir una URL una vez finalizada la integración. Para obtener más información sobre la integración de Amazon WorkSpaces y Amazon, WorkDocs consulte Integrar con WorkDocs en la Guía del WorkSpaces usuario de Amazon.

Para configurar la URL de un sitio

1. Abre la WorkDocs consola de Amazon en https://console.aws.amazon.com/zocalo/.
2. En el panel de navegación, seleccione Sites (Sitios).

   Aparece la página Administra tus WorkDocs sitios, que muestra una lista de tus sitios.
3. Selecciona el sitio que integraste con Amazon WorkSpaces. La URL contiene el identificador de directorio de tu WorkSpaces instancia de Amazon, como https://{directory_id}.awsapps.com.
4. Pulse el botón situado junto a esa URL, abra la lista de acciones y elija Establecer URL del sitio.

   Aparece el cuadro de diálogo Establecer URL del sitio.
5. En el cuadro URL del sitio, introduzca la URL del sitio y, a continuación, seleccione Establecer URL del sitio.
6. En la página Administra tus WorkDocs sitios, selecciona Actualizar para ver la nueva URL.

Administrar las notificaciones

> Note
>
> Para mayor seguridad, cree usuarios federados en lugar de usuarios de IAM siempre que sea posible.

Las notificaciones permiten a los usuarios o roles de IAM llamar a la CreateNotificationSubscriptionAPI, que puedes usar para configurar tu propio punto final para procesar los mensajes de SNS que se WorkDocs envían. Para obtener más información sobre las notificaciones, consulte Configuración de notificaciones para un usuario o rol de IAM en la Guía para WorkDocs desarrolladores de Amazon.

Puede crear y eliminar notificaciones, y en los pasos siguientes se explica cómo realizar ambas tareas.

Para crear una notificación

1. Abre la WorkDocs consola de Amazon en https://console.aws.amazon.com/zocalo/.
2. En el panel de navegación, seleccione Sites (Sitios).

Aparece la página Administra tus WorkDocs sitios, que muestra una lista de tus sitios.

3. Elija el botón situado junto al sitio situado al lado del sitio electrónico situado al lado del sitio electrónico
4. Abre la lista de acciones y selecciona Administrar notificaciones.

   Aparece el cuadro de diálogo Establecer WorkDocs administrador.
5. En el cuadro Nombre de usuario, introduce el nombre del nuevo administrador y, a continuación, selecciona Establecer administrador.

Para eliminar una notificación

1. Abre la WorkDocs consola de Amazon en https://console.aws.amazon.com/zocalo/.
2. En el panel de navegación, seleccione Sites (Sitios).

   Aparece la página Administra tus WorkDocs sitios, que muestra una lista de tus sitios.
3. Elija el botón situado junto al sitio situado al lado del archivo cuyo contenido desea establecer un administrador.
4. Abra la lista de acciones y seleccione Establecer un administrador.

   Aparece el cuadro de diálogo Establecer WorkDocs administrador.
5. En el cuadro Nombre de usuario, introduce el nombre del nuevo administrador y, a continuación, selecciona Establecer administrador.

Eliminación de un sitio

Usa la WorkDocs consola de Amazon para eliminar un sitio.

> Warning
>
> Se pierden todos los archivos cuando se elimina un sitio. Solo debe eliminar un sitio si está absolutamente seguro de que esta información ya no es necesaria.

Para eliminar un sitio

1. Abre la WorkDocs consola de Amazon en https://console.aws.amazon.com/zocalo/.
2. En la barra de navegación, seleccione Sites (Sitios).

   Aparece la página Administra tus WorkDocs sitios.
3. Elija el botón situado al lado del sitio electrónico que desea eliminar.

   Aparece el cuadro de diálogo Eliminar URL del sitio.
4. Si lo desea, elija Eliminar también el directorio de usuarios.

   > Important
   >
   > Si no proporcionas tu propio directorio para Amazon WorkDocs, crearemos uno para ti. Al eliminar el WorkDocs sitio de Amazon, se le cobrará por el directorio que creamos, a menos que lo elimine o lo utilice para otra aplicación de AWS. Para obtener información sobre precios, consulte Precios de AWS Directory Service.
5. En el cuadro URL del sitio, introduce la URL del sitio y, a continuación, selecciona Eliminar.

   El sitio se elimina inmediatamente y deja de estar disponible.

Administrar Amazon WorkDocs desde el panel de control del administrador del sitio

Utiliza estas herramientas para administrar sus WorkDocs sitios de Amazon:

- El panel de control del administrador del sitio, disponible para los administradores de todos los WorkDocs sitios de Amazon, que se describe en los siguientes temas.
- La AWS consola en https://console.aws.amazon.com/zocalo/.

Cada una de esas herramientas proporciona un conjunto diferente de acciones. Los temas de esta sección explican las acciones que proporciona el panel de control del panel de control del panel de administración del sitio. Para obtener información sobre las tareas disponibles en la consola, consulteAdministrar Amazon WorkDocs desde laAWS consola (p. 24).

Configuración de idioma preferido

Puede especificar el idioma de las notificaciones por correo electrónico.

Para cambiar la configuración de idioma

1. En Mi cuenta, elija Abrir panel de control del administrador.
2. En Configuración de idioma preferido, elija el idioma que prefiera.

Hancom Online Editing y Office Online

Habilite o deshabilite la configuración de Hancom Online Editing y Office Online desde el panel de control del administrador. Para obtener más información, consulte Habilitación de la edición en colaboración (p. 47).

Almacenamiento

Especifique la cantidad de almacenamiento que reciben los usuarios nuevos.

Para cambiar la configuración de almacenamiento

1. En Mi cuenta, elija Abrir panel de control del administrador.
2. En Almacenamiento, seleccione Cambiar.
3. En el cuadro de diálogo Límite de almacenamiento, elija si desea conceder a los usuarios nuevos almacenamiento ilimitado o limitado.
4. Elija Save changes (Guardar cambios).

El cambio de la configuración de almacenamiento afecta solo a los usuarios que se añaden después de cambiarla. No modifica la cantidad de almacenamiento asignada a los usuarios existentes. Para modificar el límite de almacenamiento de un usuario existente, consulte Editar usuarios (p. 38).

Lista de direcciones IP permitidas

Los administradores WorkDocs del sitio de Amazon pueden añadir la configuración de la lista de direcciones IP permitidas para restringir el acceso al sitio a un rango permitido de direcciones IP. Puede añadir hasta 32 opciones IP Allow List (Lista de direcciones IP permitidas) por sitio.

> Note
>
> La opción IP Allow List (Lista de direcciones IP permitidas) solo funciona actualmente para las direcciones IPv4. Actualmente no se admiten listas de denegación de direcciones IP.

Para añadir un intervalo de direcciones IP a la opción IP Allow List (Lista de direcciones IP permitidas)

1. En Mi cuenta, elija Abrir panel de control del administrador.
2. En IP Allow List (Lista de direcciones IP permitidas), elija Change (Cambiar).
3. Para Introducir el valor CIDR, introduzca el bloque de enrutamiento entre dominios sin clases (CIDR) para los rangos de direcciones IP y elija Agregar.
   - Para permitir el acceso a una sola dirección IP, especifique `/32` como el prefijo de CIDR.
4. Elija Save changes (Guardar cambios).
5. Se permitirá el acceso a los usuarios del sitio que se conecten a las direcciones IP que figuran en IP Allow List (Lista de direcciones IP permitidas). Los usuarios que intenten conectarse al sitio desde direcciones IP no autorizadas recibirán una respuesta de acceso no autorizado.

> Warning
>
> Si escribe un valor de CIDR que le impide utilizar su dirección IP actual para obtener acceso al sitio, aparecerá un mensaje de advertencia. Si decide continuar con el valor de CIDR actual, se bloqueará el acceso al sitio con su dirección IP actual. Solo es posible revertir esta opción poniéndose en contacto con AWS Support.

Seguridad: ActiveDirectory sitios simples

En este tema se explican las distintas configuraciones de seguridad de ActiveDirectory los sitios simples. Si administra sitios que usan un ActiveDirectory conector, consulte la siguiente sección.

Para usar la configuración de configuración de configuración:

1. Seleccione el icono de perfil de la esquina superior derecha del WorkDocs cliente.

2. En Administrador, selecciona Abrir panel de control de administración.
3. Desplázate hacia abajo hasta Seguridad y selecciona Cambiar.

   Aparecerá el cuadro de diálogo de configuración de la configuración de la configuración. En la siguiente tabla se muestran los::::::::::::ActiveDirectory:::

Configuración	Descripción
En Elige tu configuración para los enlaces compartibles, selecciona una de las siguientes opciones:	
No permita enlaces que se puedan compartir en todo el sitio o en público	Deshabilita el uso compartido de enlaces para todos los usuarios.
Permita a los usuarios crear enlaces compartibles en todo el sitio, pero no les permita crear enlaces públicos que se puedan compartir	Limita el intercambio de enlaces solo a los miembros del sitio. Los usuarios gestionados pueden crear este tipo de enlace.
Permiten a los usuarios crear enlaces compartibles en todo el sitio, pero solo los usuarios avanzados pueden crear enlaces públicos que se puedan compartir	Los usuarios gestionados pueden crear enlaces para todo el sitio, pero solo los usuarios avanzados pueden crear enlaces públicos. Los enlaces públicos permiten el acceso a cualquier usuario de Internet.
Todos los usuarios gestionados pueden crear enlaces públicos y para todo el sitio que se puedan compartir	Los usuarios gestionados pueden crear enlaces públicos.
En Activación automática, active o desactive la casilla de verificación.	
Permita que todos los usuarios de su directorio se activen automáticamente al iniciar sesión por primera vez en su WorkDocs sitio.	Activa automáticamente a los usuarios cuando inician sesión en tu sitio por primera vez.
En Quién se debe permitir invitar a nuevos usuarios a tu WorkDocs sitio, selecciona una de las siguientes opciones:	
Solo los administradores pueden invitar a nuevos usuarios.	Solo los administradores pueden invitar a nuevos usuarios.
Los usuarios pueden invitar a nuevos usuarios desde cualquier lugar compartiendo archivos o carpetas con ellos.	Permite a los usuarios invitar a nuevos usuarios compartiendo archivos o carpetas con esos usuarios.
Los usuarios pueden invitar a nuevos usuarios de algunos dominios específicos compartiendo archivos o carpetas con ellos.	Los usuarios pueden invitar a personas nuevas de los dominios especificados compartiendo archivos o carpetas con ellas.
En Configurar rol para nuevos usuarios, active o desactive la casilla de verificación.	
Los nuevos usuarios de su directorio serán usuarios gestionados (son usuarios invitados de forma predeterminada)	Convierte automáticamente los nuevos usuarios de su directorio en usuarios gestionados.

4. Cuando haya terminado, seleccione Guardar cambios.

Seguridad: sitios ActiveDirectory de conexión

En este tema se explican las distintas configuraciones de seguridad de los sitios de ActiveDirectory conectores. Si administra sitios que utilizan SimpleActiveDirectory, consulte la sección anterior.

Para usar la configuración de configuración de configuración:

1. Seleccione el icono de perfil de la esquina superior derecha del WorkDocs cliente.

2. En Administrador, selecciona Abrir panel de control de administración.
3. Desplázate hacia abajo hasta Seguridad y selecciona Cambiar.

   Aparecerá el cuadro de diálogo de configuración de la configuración de la configuración. En la siguiente tabla se muestran y describen la configuración de configuración de ActiveDirectory los::

Configuración	Descripción
En Elige tu configuración para los enlaces compartibles, selecciona una de las siguientes opciones:	
No permita enlaces que se puedan compartir en todo el sitio o en público	Cuando se selecciona, se deshabilita el uso compartido de enlaces para todos los usuarios.
Permita a los usuarios crear enlaces compartibles en todo el sitio, pero no les permita crear enlaces públicos que se puedan compartir	Limita el intercambio de enlaces solo a los miembros del sitio. Los usuarios gestionados pueden crear este tipo de enlace.
Permiten a los usuarios crear enlaces compartibles en todo el sitio, pero solo los usuarios avanzados pueden crear enlaces públicos que se puedan compartir	Los usuarios gestionados pueden crear enlaces para todo el sitio, pero solo los usuarios avanzados pueden crear enlaces públicos. Los enlaces públicos permiten el acceso a cualquier usuario de Internet.
Todos los usuarios gestionados pueden crear enlaces públicos y para todo el sitio que se puedan compartir	Los usuarios gestionados pueden crear enlaces públicos.
En Activación automática, active o desactive la casilla de verificación.	
Permita que todos los usuarios de su directorio se activen automáticamente al iniciar sesión por primera vez en su WorkDocs sitio.	Activa automáticamente a los usuarios cuando inician sesión en tu sitio por primera vez.
En ¿Quién debe estar autorizado a activar los usuarios del directorio en su WorkDocs sitio? , seleccione una de:	
Solo los administradores pueden activar nuevos usuarios de su directorio.	Solo permite a los administradores activar nuevos usuarios del directorio.
Los usuarios pueden activar nuevos usuarios de su directorio al compartir archivos o carpetas con ellos.	Permite a los usuarios activar los usuarios del directorio al compartir archivos o carpetas con los usuarios del directorio.
Los usuarios pueden activar nuevos usuarios de algunos dominios específicos al compartir archivos o carpetas con ellos.	Los usuarios solo pueden compartir archivos o carpetas de usuarios de dominios específicos. Al elegir esta opción, debe introducir los:::
En ¿Quién debería poder invitar a nuevos usuarios a tu WorkDocs sitio? , seleccione una de:	
Compartir con usuarios externos	Enables administrators and users to invite new external users to your Amazon WorkDocs site.

Configuración	Descripción
Note Las siguientes opciones solo aparecen después de seleccionar esta configuración.	
Solo los administradores pueden invitar a usuarios externos	Solo los administradores pueden invitar a usuarios externos.
Todos los usuarios gestionados pueden invitar a nuevos usuarios	Permite a los usuarios gestionados invitar a usuarios externos.
Solo los usuarios avanzados pueden invitar a nuevos usuarios externos.	Permite que solo los usuarios avanzados inviten a nuevos usuarios externos.
En Configurar rol para nuevos usuarios, seleccione una o ambas opciones.	
Los nuevos usuarios de su directorio serán usuarios gestionados (son usuarios invitados de forma predeterminada)	Convierte automáticamente los nuevos usuarios de su directorio en usuarios gestionados.
Los usuarios nuevos externos serán usuarios administrados (de manera predeterminada, son usuarios invitados)	Convierte automáticamente los nuevos usuarios externos en usuarios gestionados.

4. Cuando haya terminado, seleccione Guardar cambios.

Retención de la papelera de recuperación

Cuando un usuario elimina un archivo, Amazon lo WorkDocs almacena en la papelera de reciclaje del usuario durante 30 días. Posteriormente, Amazon WorkDocs mueve los archivos a una papelera de recuperación temporal durante 60 días y, a continuación, los elimina de forma permanente. Solo los administradores pueden ver la papelera de recuperación temporal. Al cambiar la política de retención de datos de todo el sitio, los administradores del sitio pueden cambiar el período de retención de la papelera de recuperación a un mínimo de cero días y un máximo de 365.

Para cambiar el periodo de retención de la papelera de recuperación

1. En Mi cuenta, elija Abrir panel de control del administrador.
2. Junto a Retención de la papelera de recuperación, elija Cambiar.
3. Introduzca el número de días para conservar los archivos en la papelera de recuperación y seleccione Guardar.

   Note

   El periodo de retención predeterminado es de 60 días. Puede utilizar un período de 0 a 365 días.

Los administradores pueden restaurar los archivos de los usuarios desde la papelera de recuperación antes de que Amazon WorkDocs los elimine permanentemente.

Para restaurar un archivo de un usuario

1. En Mi cuenta, elija Abrir panel de control del administrador.
2. En Administrar usuarios, elija el icono de la carpeta del usuario.

3. En Recovery bin (Papelera de recuperación), seleccione el archivo o archivos que desea restaurar y, a continuación, elija el icono Recover (Recuperar).
4. En Restore file (Restaurar archivo), elija la ubicación en la que desea restaurar el archivo y elija Restore (Restaurar).

Administrar la configuración del usuario

Puede administrar la configuración de los usuarios, incluida la modificación de las funciones de usuario y la invitación, habilitación y deshabilitación de usuarios. Para obtener más información, consulte Invitar y gestionar WorkDocs usuarios de Amazon (p. 34).

Implementación de Amazon WorkDocs Drive en varios equipos

Si tiene una flota de equipos unidos al dominio, puede utilizar objetos de política de grupo (GPO) o System Center Configuration Manager (SCCM) para instalar el cliente de Amazon WorkDocs Drive. Puede descargar el cliente desdehttps://amazonworkdocs.com/en/clients.

A medida que avanzas, recuerde que Amazon WorkDocs Drive requiere acceso HTTPS en el puerto 443 para todas las direcciones IP de AWS. También querrá confirmar que los sistemas de destino cumplen los requisitos de instalación de Amazon WorkDocs Drive. Para obtener más información, consulteInstalación de Amazon WorkDocs Driveen laGuía del usuario de Amazon WorkDocs.

> Note
>
> Como práctica recomendada al utilizar GPO o SCCM, instale el cliente de Amazon WorkDocs Drive después de que los usuarios inicien sesión.

El instalador de MSI para Amazon WorkDocs Drive es compatible con los siguientes parámetros de instalación opcionales:

- **`SITEID`**rellenar previamente la información del sitio de Amazon WorkDocs para los usuarios durante el registro. Por ejemplo,`SITEID=`*`nombre-sitio`*.
- **`DefaultDriveLetter`**rellenar previamente la letra de la unidad a utilizar para el montaje de Amazon WorkDocs Drive. Por ejemplo,`DefaultDriveLetter=`*`W`*. Recuerde que cada usuario debe tener una letra de unidad diferente. Además, los usuarios pueden cambiar el nombre de la unidad, pero no la letra de unidad, después de iniciar Amazon WorkDocs Drive por primera vez.

En el siguiente ejemplo se implementa Amazon WorkDocs Drive sin interfaces de usuario ni reinicios. Tenga en cuenta que utiliza el nombre predeterminado del archivo MSI:

```
msiexec /i "AWSWorkDocsDriveClient.msi" SITEID=Your_workdocs_site_ID
DefaultDriveLetter=tu_drive_letterREBOOT=REALLYSUPPRESS /norestart /qn
```

Invitar y gestionar WorkDocs usuarios de Amazon

De forma predeterminada, cuando se adjunta un directorio durante la creación del sitio, la función de activación automática de Amazon WorkDocs añade a todos los usuarios de ese directorio al nuevo sitio como usuarios gestionados.

En WorkDocs, los usuarios gestionados no necesitan iniciar sesión con credenciales independientes. Pueden compartir archivos y colaborar en ellos, y disponen automáticamente de 1 TB de almacenamiento. Sin embargo, puede desactivar la activación automática cuando solo desee añadir algunos de los usuarios de un directorio, y los pasos de las siguientes secciones explican cómo hacerlo.

Además, puede invitar, habilitar o deshabilitar usuarios y cambiar las funciones y la configuración de los usuarios. También puede promocionar un usuario a administrador. Para obtener más información acerca de la promoción de los usuarios, consultePromover un usuario a administrador (p. 23).

Estas tareas se realizan en el panel de control de administración del cliente WorkDocs web de Amazon, y en los pasos de las siguientes secciones se explica cómo hacerlo. Sin embargo, si eres nuevo en Amazon WorkDocs, tómate unos minutos para conocer las distintas funciones de usuario antes de dedicarte a las tareas administrativas.

Contenido

Información general sobre las funciones de usuario

Amazon WorkDocs define las siguientes funciones de usuario. Puede cambiar las funciones de los usuarios editando sus perfiles de usuario. Para obtener más información, consulte Editar usuarios (p. 38).

- Administrador: usuario de pago que tiene permisos administrativos para todo el sitio, incluida la administración de usuarios y la configuración del sitio. Para obtener más información sobre cómo promocionar un usuario a administrador, consulte Promover un usuario a administrador (p. 23).
- Usuario avanzado: usuario de pago que tiene un conjunto especial de permisos del administrador. Para obtener más información sobre cómo configurar los permisos para un usuario avanzado, consulteSeguridad: ActiveDirectory sitios simples (p. 28) ySeguridad: sitios ActiveDirectory de conexión (p. 29).

- Usuario: un usuario de pago que puede guardar archivos y colaborar con otros en un WorkDocs sitio de Amazon.
- Usuario invitado: usuario gratuito que solo puede ver archivos. Puede actualizar los usuarios invitados a las funciones de usuario, usuario avanzado o administrador.

  Note

  Cuando cambias el rol de un usuario invitado, realizas una acción única que no puedes revertir.

Amazon WorkDocs también define estos tipos de usuarios adicionales.

Usuario de WS

Un usuario con un asignado WorkSpaces WorkSpace.

- Acceso a todas las WorkDocs funciones de Amazon
- Almacenamiento predeterminado de 50 GB (se puede pagar para ampliarlo a 1 TB)
- Sin cargos mensuales

Usuario de WS actualizado

Un usuario con un almacenamiento asignado WorkSpaces WorkSpace y actualizado.

- Acceso a todas las WorkDocs funciones de Amazon
- Almacenamiento predeterminado de 1 TB (almacenamiento adicional disponible de pay-as-you-go forma opcional)
- Se aplican cargos mensuales

WorkDocs Usuario de Amazon

Un WorkDocs usuario activo de Amazon sin un asignado WorkSpaces WorkSpace.

- Acceso a todas las WorkDocs funciones de Amazon
- Almacenamiento predeterminado de 1 TB (almacenamiento adicional disponible de pay-as-you-go forma opcional)
- Se aplican cargos mensuales

Iniciar el panel de control de administración

Utiliza el panel de control administrativo del cliente WorkDocs web de Amazon para activar y desactivar la activación automática y cambiar las funciones y la configuración de los usuarios.

Para abrir el panel de control de administración

1. Seleccione el qué icono de la esquina superior derecha del WorkDocs cliente.

   

2. En Administrador, selecciona Abrir panel de control de administración.

Note

Algunas opciones del panel de control difieren entre los directorios en la nube y los directorios conectados.

Desactivación de la activación automática

La activación automática se desactiva cuando no desee añadir todos los usuarios de un directorio a un sitio nuevo y cuando desee establecer diferentes permisos y funciones para los usuarios a los que invite a un sitio nuevo. Al desactivar la activación automática, también puede decidir quién puede invitar a nuevos usuarios al sitio: usuarios actuales, usuarios avanzados o administradores. En estos pasos se explica cómo realizar ambas tareas.

Para desactivar la activación automática

1. Seleccione el qué icono de la esquina superior derecha del WorkDocs cliente.

2. En Administrador, selecciona Abrir panel de control de administración.
3. Desplázate hacia abajo hasta Seguridad y selecciona Cambiar.

   Aparecerá el cuadro de diálogo Configuración de la política.
4. En Activación automática, desactive la casilla de verificación situada junto a Permitir que todos los usuarios de su directorio se activen automáticamente al iniciar sesión por primera vez en su WorkDocs sitio.

   Las opciones cambian en Quién se debe permitir activar a los usuarios del directorio en tu WorkDocs sitio. Puede permitir que los usuarios actuales inviten a nuevos usuarios o puede dar esa posibilidad a los usuarios avanzados u otros administradores.
5. Selecciona una opción y, a continuación, selecciona Guardar cambios.

Repita los pasos 1 a 4 para volver a habilitar la activación automática.

Administrar el uso compartido de enlaces

En este tema se explica cómo administrar la compartición de enlaces. WorkDocs Los usuarios de Amazon pueden compartir sus archivos y carpetas compartiendo enlaces a ellos. Pueden compartir enlaces a archivos dentro y fuera de la organización, pero solo pueden compartir enlaces a carpetas internamente. Como administrador, puedes gestionar quién puede compartir enlaces.

Para habilitar el uso compartido de enlaces

1. Seleccione el qué icono de la esquina superior derecha del WorkDocs cliente.

2. En Administrador, selecciona Abrir panel de control de administración.
3. Desplázate hacia abajo hasta Seguridad y selecciona Cambiar.

   Aparecerá el cuadro de diálogo Configuración de la política.
4. En Elige tu configuración para los enlaces compartibles, selecciona una opción:

   - No permita que se compartan en todo el sitio o en público: deshabilita el uso compartido de enlaces para todos los usuarios.
   - Permita a los usuarios crear enlaces que se puedan compartir en todo el sitio, pero no permita que creen enlaces públicos que se puedan compartir: limita el intercambio de enlaces solo a los miembros del sitio. Los usuarios gestionados pueden crear este tipo de enlace.
   - Permite a los usuarios crear enlaces para compartir en todo el sitio, pero solo los usuarios avanzados pueden crear enlaces públicos para compartir. Los usuarios gestionados pueden crear enlaces para todo el sitio, pero solo los usuarios avanzados pueden crear enlaces públicos. Los enlaces públicos permiten el acceso a cualquier usuario de Internet.
   - Todos los usuarios gestionados pueden crear enlaces públicos y para todo el sitio; los usuarios gestionados pueden crear enlaces públicos.
5. Elija Save changes (Guardar cambios).

Controlar las invitaciones de usuario con la activación automática habilitada

Si habilitas la activación automática (recuerda que está activada de forma predeterminada), puedes ofrecer a los usuarios la posibilidad de invitar a otros usuarios. Puede conceder una de las siguientes opciones:

- Todos los usuarios
- Usuarios avanzados
- Administradores.

También puedes deshabilitar los permisos por completo, y en estos pasos se explica cómo hacerlo.

Para configurar los permisos de invitación

1. Seleccione el qué icono de la esquina superior derecha del WorkDocs cliente.

   
2. En Administrador, selecciona Abrir panel de control de administración.
3. Desplázate hacia abajo hasta Seguridad y selecciona Cambiar.

   Aparecerá el cuadro de diálogo Configuración de la política.
4. En Quién se debe permitir activar los usuarios del directorio de tu WorkDocs sitio, selecciona la casilla Compartir con usuarios externos, selecciona una de las opciones que se encuentran debajo de la casilla de verificación y, a continuación, selecciona Guardar cambios.

   -O BIEN-

   Desactive la casilla de verificación si no quiere que nadie invite a nuevos usuarios y, a continuación, seleccione Guardar cambios.

Invitar a usuarios nuevos

Puede invitar a nuevos usuarios a unirse a un directorio. También puede habilitar a los usuarios existentes para invitar a nuevos usuarios. Para obtener más información, consulteSeguridad: ActiveDirectory sitios simples (p. 28) la ySeguridad: sitios ActiveDirectory de conexión (p. 29) en esta guía.

Para invitar a usuarios nuevos

1. Seleccione el qué icono de la esquina superior derecha del WorkDocs cliente.

2. En Administrador, selecciona Abrir panel de control de administración.
3. En Manage users (Administrar usuarios), elija Invite users (Invitar usuarios).
4. En el cuadro de diálogo Invitar usuarios, en ¿A quién desea invitar? , introduce la dirección de correo electrónico del invitado y selecciona Enviar. Repita este paso para cada invitación.

Amazon WorkDocs envía un correo electrónico de invitación a cada destinatario. El correo contiene un enlace e instrucciones sobre cómo crear una WorkDocs cuenta de Amazon. El enlace de invitación tiene una caducidad de 30 días.

Editar usuarios

Puede cambiar la información y la configuración del usuario.

Para editar usuarios

1. Seleccione el qué icono de la esquina superior derecha del WorkDocs cliente.

2. En Administrador, selecciona Abrir panel de control de administración.
3. En Administrar usuarios, elija el icono del lápiz (✎) junto al nombre del usuario.
4. En el cuadro de diálogo Editar usuario, puede editar las opciones siguientes:

   Nombre (solo en el directorio de la nube)

   El nombre del usuario.

   Apellidos (solo en el directorio de la nube)

   Los apellidos del usuario.

   Estado

   Especifica si el usuario está activo o inactivo. Para obtener más información, consulte Deshabilitación de usuarios (p. 39).

Rol

Especifica si alguien es usuario o administrador. También puede subir o bajar de categoría a los usuarios que tengan un WorkSpaces WorkSpace asignado. Para obtener más información, consulte Información general sobre las funciones de usuario (p. 34).

Almacenamiento

Especifica el límite de almacenamiento de un usuario existente.

5. Elija Save changes (Guardar cambios).

Deshabilitación de usuarios

Para deshabilitar el acceso de un usuario, cambie su estado a Inactivo.

Para cambiar el estado del usuario a Inactivo

1. Seleccione el qué icono de la esquina superior derecha del WorkDocs cliente.

2. En Administrador, selecciona Abrir panel de control de administración.
3. En Administrar usuarios, elija el icono del lápiz (✎) junto al nombre del usuario.
4. Elija Inactivo y después Guardar cambios

El usuario desactivado no puede acceder a tu WorkDocs sitio de Amazon.

Note

Cambiar el estado de un usuario al estado Inactivo no elimina sus archivos, carpetas ni comentarios de tu WorkDocs sitio de Amazon. Sin embargo, puede transferir los archivos y carpetas de un usuario inactivo a un usuario activo. Para obtener más información, consulte Transferir la propiedad de los documentos (p. 39).

Eliminar usuarios pendientes

Puede eliminar los usuarios de Simple AD,AWS Managed Microsoft y AD Connector en estado pendiente. Para eliminar uno de esos usuarios, selecciona el icono de la papelera (🗑) situado junto al nombre del usuario.

Tu WorkDocs sitio de Amazon siempre debe tener al menos un usuario activo que no sea un usuario invitado. Si necesitas eliminar todos los usuarios, elimina todo el sitio (p. 26).

Le recomendamos que no elimine usuarios registrados, En su lugar, debes cambiar el estado de un usuario del estado Activo al Inactivo para evitar que acceda a tu WorkDocs sitio de Amazon.

Transferir la propiedad de los documentos

Puede transferir los archivos y carpetas de un usuario inactivo a un usuario activo. Para obtener más información acerca de cómo desactivar un usuario, consulteDeshabilitación de usuarios (p. 39).

Warning

Esta acción no se puede deshacer.

Para transferir la propiedad de los documentos

1. Seleccione el qué icono de la esquina superior derecha del WorkDocs cliente.

2. En Administrador, selecciona Abrir panel de control de administración.
3. En Administrar usuarios, busque el usuario inactivo.
4. Elija el icono de lápiz (✎) que aparece junto al nombre del usuario inactivo.
5. Selecciona Transferir propiedad del documento e introduce la dirección de correo electrónico del nuevo propietario.
6. Elija Save changes (Guardar cambios).

Descarga de listas de usuarios

Para descargar una lista de usuarios desde el panel de control del administrador, debe instalar Amazon WorkDocs Companion. Para instalar Amazon WorkDocs Companion, consulta Aplicaciones e integraciones para Amazon WorkDocs.

Para descargar una lista de usuarios

1. Seleccione el qué icono de la esquina superior derecha del WorkDocs cliente.

2. En Administrador, selecciona Abrir panel de control de administración.
3. En Administrar usuarios, seleccione Descargar usuario.
4. En Descargar usuario, elija una de las siguientes opciones para exportar una lista de usuarios como un archivo `.json` en su escritorio:
   - Todos los usuarios
   - Usuario invitado
   - Usuario de WS
   - Usuario
   - Usuario avanzado
   - Administrador
5. WorkDocs guarda el archivo en una de las siguientes ubicaciones:
   - Windows – `Downloads/WorkDocsDownloads`
   - macOS: *`hard drive`*`/users/`*`username`*`/WorkDocsDownloads/folder`

Note

Las descargas pueden tardar un tiempo. Además, los archivos descargados no llegan a `/~users` la carpeta.

Para obtener más información sobre estas funciones de usuario, consulte Información general sobre las funciones de usuario (p. 34).

Compartir y colaborar

Los usuarios pueden compartir contenido mediante el envío de un enlace o una invitación. Los usuarios también pueden colaborar con usuarios externos si habilitas el uso compartido externo.

Amazon WorkDocs controla el acceso a las carpetas y los archivos mediante el uso de permisos. El sistema aplica los permisos en función del rol del usuario.

Contenido

Compartir enlaces

Los usuarios pueden elegir Compartir un enlace para copiar y compartir rápidamente los hipervínculos del WorkDocs contenido de Amazon con compañeros de trabajo y usuarios externos, tanto de dentro como de fuera de la organización. Cuando los usuarios comparten un enlace, pueden configurarlo para admitir una de las siguientes opciones de acceso:

- Todos los miembros del WorkDocs sitio de Amazon pueden buscar, ver y comentar el archivo.
- Cualquier persona que tenga el enlace, incluso las personas que no sean miembros del WorkDocs sitio de Amazon, pueden ver el archivo. Esta opción de enlace restringe los permisos solo lectura.

Los destinatarios con permisos de consulta solo pueden ver los archivos. Los permisos de visualización permiten a los usuarios hacer comentarios y realizar operaciones de actualización o eliminación, como cargar un archivo nuevo o eliminar un archivo existente.

De forma predeterminada, todos los usuarios administrados pueden crear enlaces públicos. Para cambiar esta configuración, actualice la configuración de Security (Seguridad) desde el panel de control del administrador. Para obtener más información, consulte Administrar Amazon WorkDocs desde el panel de control del administrador del sitio (p. 27).

Compartir por invitación

Al habilitar el uso compartido por invitación, los usuarios del sitio pueden compartir archivos o carpetas con usuarios individuales y con grupos mediante el envío de correos electrónicos de invitación. Las invitaciones contienen enlaces al contenido compartido y los invitados pueden abrir los archivos o carpetas compartidos. Los invitados también pueden compartir esos archivos o carpetas con otros miembros del sitio y con usuarios externos.

Puede establecer niveles de permisos para cada usuario invitado. También puedes crear carpetas de equipo para compartirlas mediante invitaciones a los grupos de directorios que crees.

Note

Las invitaciones para compartir no incluyen a los miembros de grupos anidados. Para incluir a esos miembros, debes agregarlos a la lista Compartir por invitación.

Para obtener más información, consulte Administrar Amazon WorkDocs desde el panel de control del administrador del sitio (p. 27).

Uso compartido externo

El uso compartido externo permite a los usuarios gestionados de un WorkDocs sitio de Amazon compartir archivos y carpetas y colaborar con usuarios externos sin incurrir en costes adicionales. Los usuarios del sitio pueden compartir archivos y carpetas con usuarios externos sin necesidad de que los destinatarios sean usuarios de pago del WorkDocs sitio de Amazon. Al habilitar el uso compartido externo, los usuarios pueden introducir la dirección de correo electrónico del usuario externo con el que desean compartir y establecer los permisos de uso compartido de espectadores adecuados. Cuando se añaden usuarios externos, los permisos se limitan a los de los espectadores y no hay otros permisos disponibles. Los usuarios externos reciben una notificación por correo electrónico con un enlace al archivo o la carpeta que se ha compartido. Al elegir el enlace, los usuarios externos acceden al sitio, donde introducen sus credenciales para iniciar sesión en AmazonWorkDocs. Pueden ver el archivo o la carpeta que se ha compartido en la vista Compartido conmigo.

Los propietarios de los archivos pueden modificar los permisos de uso compartido o eliminar el acceso del usuario externo a un archivo o carpeta en cualquier momento. El administrador del sitio debe habilitar el uso compartido externo del sitio para que los usuarios administrados puedan compartir contenido con usuarios externos. Para que los usuarios invitados se conviertan en colaboradores o copropietarios, el administrador del sitio debe asignarles el nivel Usuario. Para obtener más información, consulte Información general sobre las funciones de usuario (p. 34).

De forma predeterminada, el uso compartido externo está activado, y todos los usuarios pueden invitar a usuarios externos. Para cambiar esta configuración, actualice la configuración de Security (Seguridad) desde el panel de control del administrador. Para obtener más información, consulte Administrar Amazon WorkDocs desde el panel de control del administrador del sitio (p. 27).

Permisos

AmazonWorkDocsusa permisos para controlar el acceso a carpetas y archivos. Los permisos se aplican en función de las funciones de los usuarios.

Contenido

Roles de usuario

Los roles de usuario controlan los permisos de carpetas y archivos. Puede aplicar las siguientes funciones de usuario a nivel de carpeta:

- Propietario de la carpeta— El propietario de una carpeta o archivo.

- Copropietario de la carpeta— Un usuario o grupo que el propietario designa como copropietario de una carpeta o archivo.
- Colaborador de carpetas— Alguien con acceso ilimitado a una carpeta.
- Visor de carpetas— Alguien con acceso limitado (permisos de solo lectura) a una carpeta.

Puede aplicar las siguientes funciones de usuario a nivel de archivo individual:

- Dueño— El propietario de un archivo.
- Copropietario— Un usuario o grupo que el propietario designa como copropietario del archivo.
- Colaborador— Alguien autorizado a dar su opinión sobre el archivo.
- Visor— Alguien con acceso limitado (permisos de solo lectura) al archivo.
- Visor anónimo— Un usuario no registrado ajeno a la organización que puede ver un archivo que se ha compartido mediante un enlace de visualización externo. Salvo que se indique de otro modo, un usuario anónimo tiene los mismos permisos que un usuario con permiso para ver.

Permisos para las carpetas compartidas

Los siguientes permisos se aplican a las funciones de usuario de las carpetas compartidas:

> Note
>
> Los permisos aplicados a una carpeta también se aplican a las subcarpetas y archivos de esa carpeta.

- Ver— Ver el contenido de una carpeta compartida.
- Ver subcarpetas— Ver una subcarpeta.
- Ver recursos compartidos— Ver los demás usuarios con los que se comparte una carpeta.
- Carpeta de descargas— Descarga una carpeta.
- Añadir subcarpeta— Añadir una subcarpeta.
- Compartir— Comparte la carpeta de nivel superior con otros usuarios.
- Revocar compartir— Revocar el uso compartido de la carpeta de nivel superior.
- Eliminar subcarpeta— Eliminar una subcarpeta.
- Eliminar carpeta de nivel superior— Eliminar la carpeta compartida de nivel superior.

	Vista	Ver subcarpetas	Ver recursos compartidos	Carpeta de descargas	Añadir subcarpeta	Share	Revocar compartir	Eliminar subcarpeta	Eliminar carpeta de nivel superior
Propietario de la carpeta	✓	✓	✓	✓	✓	✓	✓	✓	✓
Copropietario de la carpeta	✓	✓	✓	✓	✓	✓	✓	✓	✓
Colaborador de carpetas	✓	✓	✓	✓	✓				

	Vista	Ver subcarpetas	Ver recursos compartidos	Carpeta de descargas	Añadir subcarpeta	Share	Revocar compartir	Eliminar subcarpeta	Eliminar carpeta de nivel superior
Visor de carpetas	✓	✓	✓	✓					

Permisos para archivos de carpetas compartidas

Los siguientes permisos se aplican a las funciones de usuario de los archivos de una carpeta compartida:

- Anota— Añadir comentarios a un archivo.
- Borrar— Eliminar un archivo de una carpeta compartida.
- Cambiar nombre— Cambiar el nombre de los archivos.
- Subir— Sube nuevas versiones de un archivo.
- Descarga— Descarga un archivo. Este es el permiso predeterminado. Puede utilizar las propiedades del archivo para permitir o denegar la posibilidad de descargar archivos compartidos.
- Impedir la descarga— Impedir que se descargue un archivo.

  Note

  - Al seleccionar esta opción, los usuarios conVerlos permisos aún pueden descargar archivos. Para evitarlo, abre la carpeta compartida y borra laPermitir descargasconfiguración para cada uno de los archivos que no desea que esos usuarios descarguen.
  - Cuando el propietario o copropietario de un archivo MP4 no permite la descarga de ese archivo, los colaboradores y los espectadores no pueden reproducirlo en AmazonWorkDocscliente web.
- Compartir— Compartir un archivo con otros usuarios.
- Revocar el uso compartido— Revocar el uso compartido de un archivo.
- Ver— Ver un archivo en una carpeta compartida.
- Ver recursos compartidos— Ver los demás usuarios con los que se comparte un archivo.
- Ver anotaciones— Ver los comentarios de otros usuarios.
- Ver actividad— Ver el historial de actividades de un archivo.
- Ver versiones— Ver versiones anteriores de un archivo.
- Eliminar versiones— Eliminar una o más versiones de un archivo.
- Recuperar versiones— Recuperar una o más versiones eliminadas de un archivo.
- Ver todos los comentarios privados— El propietario/copropietario puede ver todos los comentarios privados de un documento, incluso si no son respuestas a su comentario.

	Anotar	Eliminar	Cambiar de nombre	Cargar	Descargar	Impedir la descarga	Share	Revocar compartir	Vista recursos compartidos	Ver anotaciones	Ver actividad	Vista de las versiones	Eliminar versiones	Recuperar versiones	Ver todos los comentarios privados**
Propietario del archivo*	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

	Anotar	Eliminar	Cambiar de nombre	Cargar	Descargar	Impedir la descarga	Share	Revocar compartir	Vista recurso compartido	Ver anotaciones	Ver actividad	Vista de las versiones	Eliminar versiones	Recuperar versiones	Ver todos los comentarios privados**
Propietario* de la carpeta	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Copropietario de la carpeta	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Colaborador de carpetas	✓			✓	✓				✓	✓	✓	✓	✓			
Visor de carpetas					✓				✓	✓						
Visor anónimo									✓	✓						

* El propietario del archivo, en este caso, es la persona que cargó la versión original de un archivo en una carpeta compartida. Los permisos de este rol solo se aplican al archivo del que se es propietario, no a todos los archivos de la carpeta compartida.

** El propietario y el copropietario del archivo pueden ver todos los comentarios privados. Los colaboradores solo pueden ver los comentarios privados en respuesta a sus comentarios.

Permisos para archivos que no estén en carpetas compartidas

Los siguientes permisos se aplican a las funciones de usuario de los archivos que no residen en una carpeta compartida:

- Anota— Añadir comentarios a un archivo.
- Borrar— Eliminar un archivo.
- Cambiar nombre— Cambiar el nombre de los archivos.
- Subir— Sube nuevas versiones de un archivo.
- Descarga— Descarga un archivo. Este es el permiso predeterminado. Puede utilizar las propiedades del archivo para permitir o denegar la posibilidad de descargar archivos compartidos.
- Impedir la descarga— Impedir que se descargue un archivo.

  Note

  Cuando el propietario o copropietario de un archivo MP4 no permite la descarga de ese archivo, los colaboradores y los espectadores no pueden reproducirlo en AmazonWorkDocscliente web.
- Compartir— Compartir un archivo con otros usuarios.
- Revocar compartir— Revocar el uso compartido de un archivo.

- Ver— Ver un archivo.
- Ver recursos compartidos— Ver los demás usuarios con los que se comparte un archivo.
- Ver anotaciones— Ver los comentarios de otros usuarios.
- Ver actividad— Ver el historial de actividades de un archivo.
- Ver versiones— Ver versiones anteriores de un archivo.
- Eliminar versiones— Eliminar una o más versiones de un archivo.
- Recuperar versiones— Recuperar una o más versiones eliminadas de un archivo.

	Annotate	Elimina	Cambio de nombre	Carga	Descarg	Impedir la descarg	Share	Revoca compart	Vista	Ver recurso compartic	Ver anotacio	Ver activida	Vista de versione las versione	Elimina	Recuperar versiones
Propietario	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Copropietario	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Colaborador	✓			✓	✓				✓	✓	✓	✓	✓		
Espectador					✓				✓	✓					
Visor anónimo									✓	✓					

Habilitación de la edición en colaboración

Utiliza la sección Configuración de edición en línea del panel de control de administración para habilitar las opciones de edición colaborativa.

Contenido

Habilitar Hancom ThinkFree

Puede habilitar Hancom en su WorkDocs sitio de Amazon ThinkFree para que los usuarios puedan crear y editar archivos de Microsoft Office de forma colaborativa desde la aplicación WorkDocs web de Amazon. Para obtener más información, consulte Edición con Hancom. ThinkFree

Hancom ThinkFree está disponible sin coste adicional para WorkDocs los usuarios de Amazon. No se necesitan licencias adicionales ni instalar software.

Para habilitar Hancom ThinkFree

Habilite la ThinkFree edición de Hancom desde el panel de control del administrador.

1. En Mi cuenta, elija Abrir panel de control del administrador.
2. En Hancom Online Editing, elija Cambiar.
3. Seleccione Habilitar la característica Edición online de Hancom, lea las condiciones de uso y después elija Guardar.

Para deshabilitar Hancom ThinkFree

Desactive la ThinkFree edición de Hancom desde el panel de control del administrador.

1. En Mi cuenta, elija Abrir panel de control del administrador.
2. En Hancom Online Editing, elija Cambiar.
3. Desactive la casilla Habilitar la característica Edición online de Hancom y después elija Guardar.

Habilitación de Open with Office Online

Habilite Abrir con Office Online en su WorkDocs sitio de Amazon para que los usuarios puedan editar archivos de Microsoft Office de forma colaborativa desde la aplicación WorkDocs web de Amazon.

Abrir con Office Online está disponible sin coste adicional para WorkDocs los usuarios de Amazon que también tengan una cuenta profesional o educativa de Microsoft Office 365 con licencia para editar en Office Online. Para obtener más información, consulte Open with Office Online.

Para habilitar Open with Office Online

Habilite Open with Office Online desde el Panel de control del administrador.

1. En Mi cuenta, elija Abrir panel de control del administrador.
2. En Office Online, elija Cambiar.
3. Seleccione Habilitar Office Online y, a continuación, elija Guardar.

Para deshabilitar Open with Office Online

Deshabilite Open with Office Online desde el Panel de control del administrador.

1. En Mi cuenta, elija Abrir panel de control del administrador.
2. En Office Online, elija Cambiar.
3. Desactive la casilla Habilitar Office Online y después elija Guardar.

Migración de archivos a Amazon WorkDocs

WorkDocs Los administradores de Amazon pueden usar el Servicio de WorkDocs migración de Amazon para realizar una migración a gran escala de varios archivos y carpetas a su WorkDocs sitio de Amazon. El Amazon WorkDocs Migration Service funciona con Amazon Simple Storage Service (Amazon S3). Esto te permite migrar archivos compartidos departamentales y archivos compartidos de usuario o disco principal a Amazon WorkDocs.

Durante este proceso, Amazon te WorkDocs proporciona una políticaAWS Identity and Access Management (IAM). Utilice esta política para crear un nuevo rol de IAM que otorgue acceso al Servicio de WorkDocs migración de Amazon para hacer lo siguiente:

- Lea y enumere el bucket de Amazon S3 que designe.
- Lee y escribe en el WorkDocs sitio de Amazon que designes.

Realiza las siguientes tareas para migrar tus archivos y carpetas a Amazon WorkDocs. Antes de comenzar, confirme que cuenta con los siguientes permisos:

- Permisos de administrador para tu WorkDocs sitio de Amazon
- Permisos para crear un rol de IAM

Si tu WorkDocs sitio de Amazon está configurado en el mismo directorio que tu WorkSpaces flota, debes cumplir estos requisitos:

- No utilices Admin como nombre de usuario de tu WorkDocs cuenta de Amazon. El administrador es un rol de usuario reservado en Amazon WorkDocs.
- El tipo de usuario de WorkDocs administrador de Amazon debe ser Usuario de AWS actualizado. Para obtener más información, consulte Información general sobre las funciones de usuario (p. 34) y Editar usuarios (p. 38).

> **Note**
>
> La estructura del directorio, los nombres de los archivos y el contenido de los archivos se conservan al migrar a Amazon WorkDocs. La propiedad y los permisos del archivo están conservados.

Tareas

Paso 1: Preparar el contenido para la migración

Para preparar el contenido para la migración

1. En tu WorkDocs sitio de Amazon, en Mis documentos, crea una carpeta a la que quieras migrar tus archivos y carpetas.
2. Confirme lo siguiente:

   - La carpeta de origen no contiene más de 100 000 archivos y subcarpetas. Las migraciones fallan si superas ese límite.
   - Ningún archivo individual supera los 5 TB.
   - Cada nombre de archivo contiene 255 caracteres o menos. Amazon WorkDocs Drive solo muestra los archivos con una ruta de directorio completa de 260 caracteres o menos.

   Warning

   Intentar migrar archivos o carpetas con nombres que contengan los siguientes caracteres puede causar errores y detener el proceso de migración. Si esto ocurre, seleccione Download report (Descargar informe) para descargar una lista de registro de errores, los archivos que fallaron en la migración y cualquier archivo migrado correctamente.

- Espacios finales: por ejemplo: un espacio adicional al final del nombre de un archivo.
- Períodos al principio o al final: por ejemplo:`.file.file.ppt`,`..`,`...`, `ofile.`
- Tildes al principio o al final: por ejemplo:`file.doc~`,`~file.doc`, o`~$file.doc`
- Nombres de archivos que terminan en**`.tmp`** — Por ejemplo:`file.tmp`
- Nombres de archivos que coincidan exactamente con estos términos que distinguen mayúsculas de minúsculas:`Microsoft User Data`,`Outlook files`,`Thumbs.db`, `oThumbnails`
- Nombres de archivos que contengan alguno de estos caracteres:`*` (asterisco),`/` (barra inclinada hacia atrás),`:` (dos puntos),< (menos que),> (mayor que),`?` (signo de interrogación),`|` (barra vertical o barra vertical),`"` (comillas dobles) o`\ \202E`(código de caracteres 202E).

Paso 2: carga de archivos en Amazon S3

Para cargar archivos en Amazon S3

1. Cree un nuevo bucket de Amazon Simple Storage Service (Amazon S3) en suAWS cuenta en el que desea cargar sus archivos y carpetas. El bucket de Amazon S3 debe encontrarse en la mismaAWS cuenta yAWS región de que su WorkDocs sitio de Amazon. Para obtener más información, consulte Introducción a Amazon Simple Storage Service en la Guía del usuario de Amazon Simple Storage Service.
2. Cargue sus archivos en el bucket de Amazon S3 que creó en el paso anterior. Recomendamos usarloAWS DataSync para cargar archivos y carpetas en el bucket de Amazon S3. DataSync proporciona funciones adicionales de seguimiento, generación de informes y sincronización. Para obtener más información, consulte CómoAWS DataSync funciona y Uso de políticas basadas en la identidad (políticas de IAM) DataSync en la Guía delAWS DataSync usuario.

Paso 3: programación de una migración

Después de completar los pasos 1 y 2, utilice el Servicio de WorkDocs migración de Amazon para programar la migración. El Servicio de Migración puede tardar hasta una semana en procesar tu solicitud

de migración y enviarte un correo electrónico informándote de que puedes iniciar la migración. Si inicia la migración antes de recibir el correo electrónico, la consola de administración muestra un mensaje que le indica que espere.

Cuando programas la migración, la configuración de almacenamiento de tu cuenta de WorkDocs usuario de Amazon cambia automáticamente a Ilimitado.

> **Note**
>
> La migración de archivos que superen el límite WorkDocs de almacenamiento de Amazon puede generar costes adicionales. Para obtener más información, consulte WorkDocs Precios de Amazon.

El Servicio de WorkDocs migración de Amazon proporciona una políticaAWS Identity and Access Management (IAM) que puede utilizar en la migración. Con esta política, se crea una nueva función de IAM que permite al Servicio de WorkDocs migración de Amazon acceder al bucket de Amazon S3 y al WorkDocs sitio de Amazon que usted designe. También te suscribes a las notificaciones por correo electrónico de Amazon SNS para recibir actualizaciones cuando tu solicitud de migración esté programada y cuando comience y finalice.

Para programar una migración

1. En la WorkDocs consola de Amazon, selecciona Aplicaciones, Migraciones.
   - Si es la primera vez que accede al Servicio de WorkDocs migración de Amazon, se le pedirá que se suscriba a las notificaciones por correo electrónico de Amazon SNS. Suscríbase, confirme en el mensaje de correo electrónico que recibirá y seleccione Continue (Continuar).
2. Elija Create Migration (Crear migración).
3. Para Source Type (Tipo de origen). elija Amazon S3.
4. Elija Next (Siguiente).
5. Para la fuente de datos y la validación, en Política de ejemplo, copie la política de IAM proporcionada.
6. Utilice la política de IAM que copió en el paso anterior para crear una nueva política y función de IAM, de la siguiente manera:
   a. Abra la consola de IAM en https://console.aws.amazon.com/iam/.
   b. Elija Policies (Políticas), Create Policy (Crear política).
   c. Elija JSON y pegue la política de IAM que copió anteriormente en el portapapeles.
   d. Elija Review policy (Revisar política). Introduzca un nombre de política y una descripción.
   e. Elija Create Policy (Crear política).
   f. Elija Roles (Roles), Create role (Crear rol).
   g. Seleccione Another AWS account (Otra cuenta de AWS). Para Account ID (ID de la cuenta) introduzca uno de los siguientes valores:
      - Para la región EE. UU. East (Norte de Virginia), escriba`899282061130`
      - Para la región EE. UU. Oeste (Oregón), escriba`814301586344`
      - Para la región de Asia-Pacífico (Singapur), escriba`900469912330`
      - Para la región de Asia-Pacífico (Sídney), escriba`031131923584`
      - Para la región de Asia-Pacífico (Tokio), escriba`178752524102`
      - Para la región de Europa (Irlanda), escriba`191921258524`
   h. Seleccione la nueva política que ha creado y elija Next: Review (Siguiente: Revisar). Si no se puede ver la nueva política, seleccione el icono de actualizar.
   i. Introduzca un nombre de rol y una descripción. Elija Create role (Crear rol).
   j. En la página Roles, en Role name (nombre del rol), elija el nombre del rol que ha creado.

   k. En la página Summary (Resumen), establezca la Maximum CLI/API session duration (Duración máxima de la sesión de CLI/API) en 12 horas.
   l. Copie el Role ARN (ARN del rol) en su portapapeles para utilizarlo en el siguiente paso.
7. Regrese al Servicio de WorkDocs migración de Amazon. Para Fuente de datos y validación, en ARN de rol, pegue el ARN del rol de IAM que copió en el paso anterior.
8. Para Bucket, seleccione el bucket de Amazon S3 desde el que migrar los archivos.
9. Elija Next (Siguiente).
10. En Seleccionar una WorkDocs carpeta de destino, seleccione la carpeta de destino en Amazon WorkDocs a la que desea migrar los archivos.
11. Elija Next (Siguiente).
12. En Review (Revisar), para Title (Título), introduzca un nombre para la migración.
13. Seleccione la fecha y la hora de la migración.
14. Seleccione Send (enviar).

Paso 4: Seguimiento de una migración

Puedes realizar el seguimiento de tu migración desde la página de inicio del Servicio de WorkDocs Migración de Amazon. Para acceder a la página de destino desde el WorkDocs sitio de Amazon, selecciona Aplicaciones, Migraciones. Seleccione su migración para consultar sus detalles y seguir su progreso. También puede seleccionar Cancel Migration si necesita cancelarla o seleccione Update (Actualizar) si necesita actualizar la escala de tiempo de la migración. Después de completar una migración, puede seleccionar Download report (Descargar informe) para descargar un informe de los archivos migrados correctamente, cualquier fallo o error.

Los siguientes estados de migración muestran el estado de su migración:

Programados

La migración está programada pero no se ha iniciado. Puede cancelar migraciones o actualizar los tiempos de inicio de la migración hasta cinco minutos antes del tiempo de inicio programado.

Migrando

La migración se encuentra en progreso.

Correcto

La migración se ha completado.

Parcialmente correcto

La migración se ha completado de forma parcial. Para obtener más detalles, consulte el resumen de la migración y descargue el informe que se proporciona.

Con error

La migración no se ha realizado correctamente. Para obtener más detalles, consulte el resumen de la migración y descargue el informe que se proporciona.

Cancelado

La migración se ha cancelado.

Paso 5: limpieza de recursos

Cuando finalice la migración, elimine la política de migración y el rol que creó en la consola de IAM.

Para eliminar la política y el rol de IAM

1. Abra la consola de IAM en https://console.aws.amazon.com/iam/.
2. Elija Policies (Políticas).
3. Busque y seleccione la política que ha creado.
4. Para Policy actions (Acciones de la política) seleccione Delete (Eliminar).
5. Elija Delete (Eliminar).
6. Elija Roles.
7. Busque el rol que creó y selecciónelo.
8. Elija Delete role (Eliminar rol), Delete (Eliminar).

Cuando se inicia una migración programada, la configuración de almacenamiento de tu cuenta de WorkDocs usuario de Amazon se cambia automáticamente a Ilimitado. Después de la migración, puede cambiar su configuración de Storage (Almacenamiento) al editar su cuenta de usuario desde el Panel de control del administrador. Para obtener más información, consulte Editar usuarios (p. 38).

Solución de problemas de WorkDocsProblemas

La siguiente información puede ayudarle a solucionar problemas con Amazon. WorkDocs.

Problemas

No puedo configurar mi Amazon WorkDocs sitio en un sitio específicoAWSRegión

Si estás configurando un nuevo Amazon WorkDocs sitio, seleccione la región de AWS durante la configuración. Para obtener más información, consulte el tutorial de su caso de uso particular en Introducción a Amazon WorkDocs (p. 20).

¿Quieres configurar mi Amazon? WorkDocs sitio en un dominio existente de Amazon VPC

Al configurar tu nueva Amazon WorkDocs sitio, cree un directorio mediante la virtual private cloud (VPC) existente. Amazon WorkDocs usa este directorio para autenticar a los usuarios.

El usuario necesita restablecer su contraseña

Para restablecer las contraseñas, los usuarios pueden seleccionar la opción ¿Ha olvidado la contraseña? que aparece en la pantalla de inicio de sesión.

Un usuario ha compartido por error un documento confidencial

Para revocar el acceso al documento, elija Compartir por invitación junto al documento y después elimine los usuarios que ya no deben tener acceso. Si el documento se ha compartido con un enlace, elija Compartir un enlace y deshabilite el enlace.

Un usuario ha abandonado la organización y no ha transferido la propiedad del documento

Transfiera la propiedad de los documentos a otro usuario en el Panel de control del administrador. Para obtener más información, consulte Transferir la propiedad de los documentos (p. 39).

Necesidad de implementar Amazon WorkDocs Drive o Amazon WorkDocs Acompañante de múltiples usuarios

Use una política de grupo para realizar la implementación para varios usuarios de una empresa. Para obtener más información, consulte Gestión de identidades y accesos para Amazon WorkDocs (p. 4). Para obtener información específica sobre la implementación de Amazon WorkDocs Diríjase a varios usuarios, consulteImplementación de Amazon WorkDocs Drive en varios equipos (p. 33).

La edición online no funciona

Verifica que tienes Amazon WorkDocs Companion instalado. Para instalar Amazon WorkDocs Acompañante, consulteAplicaciones e integraciones para Amazon WorkDocs.

Administración de Amazon WorkDocs para Amazon Business

Si es administrador de Amazon WorkDocs para Amazon Business, puede gestionar usuarios iniciando sesión enhttps://workdocs.aws/utilizando sus credenciales de Amazon Business.

Para invitar a un nuevo usuario a Amazon WorkDocs para Amazon Business

1. Inicie sesión con sus credenciales de Amazon Business en https://workdocs.aws/.
2. En la página principal de Amazon WorkDocs para Amazon Business, abra el panel de navegación de la izquierda.
3. Seleccione Admin settings (Configuración de administrador).
4. Elija Add people (Agregar personas).
5. En Recipients (Destinatarios), introduzca las direcciones de correo electrónico o los nombres de usuario de los usuarios a invitar.
6. (Opcional) Personalice el mensaje de invitación.
7. Seleccione Done (Listo).

Para buscar un usuario en Amazon WorkDocs para Amazon Business

1. Inicie sesión con sus credenciales de Amazon Business en https://workdocs.aws/.
2. En la página principal de Amazon WorkDocs para Amazon Business, abra el panel de navegación de la izquierda.
3. Seleccione Admin settings (Configuración de administrador).
4. En Search users (Buscar usuarios), introduzca el nombre del usuario y pulse **`Enter`**.

Para seleccionar roles de usuario en Amazon WorkDocs para Amazon Business

1. Inicie sesión con sus credenciales de Amazon Business en https://workdocs.aws/.
2. En la página principal de Amazon WorkDocs para Amazon Business, abra el panel de navegación de la izquierda.
3. Seleccione Admin settings (Configuración de administrador).
4. En People (Personas), junto al usuario, seleccione el Role (Rol) que desea asignar al usuario.

Para eliminar un usuario en Amazon WorkDocs for Amazon Business

1. Inicie sesión con sus credenciales de Amazon Business en https://workdocs.aws/.
2. En la página principal de Amazon WorkDocs para Amazon Business, abra el panel de navegación de la izquierda.
3. Seleccione Admin settings (Configuración de administrador).
4. En People (Personas), elija los puntos suspensivos (...) junto al usuario.
5. Elija Delete (Eliminar).
6. Si se le solicita, introduzca un nuevo usuario al que transferir los archivos del usuario y elija Delete (Eliminar).

Dirección IP y dominios para añadir a la lista de permitidos

Si implementas el filtrado de IP en los dispositivos que acceden a Amazon WorkDocs, añada las siguientes direcciones IP y dominios a su lista de permitidos. Hacerlo permite a Amazon WorkDocs y Amazon WorkDocs Conduzca para conectarse a la WorkDocs service

- zocalo.ap-northeast-1.amazonaws.com
- zocalo.ap-southeast-2.amazonaws.com
- zocalo.eu-west-1.amazonaws.com
- zocalo.eu-central-1.amazonaws.com
- zocalo.us-east-1.amazonaws.com
- zócalo.us-gov-west-1.amazonaws.com
- zocalo.us-west-2.amazonaws.com
- awsapps.com
- amazonaws.com
- cloudfront.net
- aws.amazon.com
- amazonworkdocs.com
- console.aws.amazon.com
- cognito-identity.us-east-1.amazonaws.com
- firehose.us-east-1.amazonaws.com

Si desea utilizar intervalos de direcciones IP, consulteAWSGamas de direcciones IPen elAWSReferencia general.

Historial de documentos

En la siguiente tabla se describen cambios importantes en la Guía de WorkDocs administración de Amazon, a partir de febrero de 2018. Para obtener notificaciones sobre las actualizaciones de esta documentación, puede suscribirse a una fuente RSS.

Cambio	Descripción	Fecha
Nuevos permisos de propietario de archivos (p. 58)	Los administradores ahora pueden proporcionar los permisos Eliminar versión y Recuperar versión. Los permisos forman parte del lanzamiento de la DeleteDocumentVersionAPI.	29 de julio de 2022
Amazon WorkDocs Backup (p. 58)	Se ha eliminado la documentación de Amazon WorkDocs Backup de la Guía de WorkDocs administración de Amazon porque el componente ya no es compatible.	24 de junio de 2021
Administración de Amazon WorkDocs para Amazon Business (p. 58)	Amazon WorkDocs for Amazon Business admite la gestión de usuarios por parte de los administradores. Para obtener más información, consulte Administración de Amazon WorkDocs para Amazon Business en la Guía de WorkDocs administración de Amazon.	26 de marzo de 2020
Migración de archivos a Amazon WorkDocs (p. 58)	WorkDocs Los administradores de Amazon pueden utilizar Amazon WorkDocs Migration Service para realizar una migración a gran escala de varios archivos y carpetas a su WorkDocs sitio de Amazon. Para obtener más información, consulte Migración de archivos a Amazon WorkDocs en la Guía de WorkDocs administración de Amazon.	8 de agosto de 2019
Configuración de la lista de direcciones IP permitidas (p. 58)	La configuración de la lista de direcciones IP permitidas está disponible para filtrar el acceso a tu WorkDocs sitio de Amazon por intervalo de direcciones IP. Para obtener más información, consulte la configuración de la lista de direcciones IP permitidas en la Guía de WorkDocs administración de Amazon.	22 de octubre de 2018

Hancom ThinkFree (p. 58)	Hancom ThinkFree está disponible. Los usuarios pueden crear y editar archivos de Microsoft Office de forma colaborativa desde la aplicación WorkDocs web de Amazon. Para obtener más información, consulte Habilitar Hancom ThinkFree en la Guía de WorkDocs administración de Amazon.	21 de junio de 2018
Abrir con Office Online (p. 58)	Open with Office Online está disponible. Los usuarios pueden editar archivos de Microsoft Office de forma colaborativa desde la aplicación WorkDocs web de Amazon. Para obtener más información, consulte Habilitar Open with Office Online en la Guía de WorkDocs administración de Amazon.	6 de junio de 2018
Solución de problemas (p. 58)	Se ha añadido un tema sobre solución de problemas. Para obtener más información, consulta la sección Solución de WorkDocs problemas de Amazon en la Guía de WorkDocs administración de Amazon.	23 de mayo de 2018
Cambiar el período de retención del compartimento de recuperación (p. 58)	Se puede modificar el periodo de retención de la papelera de recuperación. Para obtener más información, consulte la configuración de retención del compartimento de recuperación en la Guía de WorkDocs administración de Amazon.	27 de febrero de 2018

Glosario de AWS

Para ver la terminología más reciente de AWS, consulte el Glosario de AWS en la Referencia de Glosario de AWS.

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.