aws

Guía de administración

Amazon WorkDocs

Amazon WorkDocs: Guía de administración

Table of Contents

Aviso: las suscripciones de nuevos clientes y las actualizaciones de cuentas ya no están disponibles para Amazon. WorkDocs Obtén más información sobre los pasos de migración aquí: Cómo migrar datos de Amazon WorkDocs.

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.

¿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 diferentes de archivos, según el tipo de soporte de Internet del archivo. Amazon WorkDocs es compatible con todos los formatos de documentos e imágenes habituales, y se añaden tipos de soporte compatibles adicionales constantemente.

Para obtener más información, consulte Amazon WorkDocs.

Acceso a Amazon WorkDocs

Los administradores usan la consola Amazon WorkDocs para 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 y Invitación y administración de usuarios de Amazon WorkDocs.

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

- 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 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 para conocer los tipos de archivos compatibles, 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 utilice. Para obtener más información, consulte Precios.

Cómo empezar

Para comenzar con Amazon WorkDocs, consulte Creación de un sitio de Amazon WorkDocs.

Migración de datos fuera de Amazon WorkDocs

Amazon WorkDocs proporciona dos métodos para migrar datos fuera de un WorkDocs sitio. Esta sección proporciona una descripción general de estos métodos y enlaces a pasos detallados para ejecutar, solucionar problemas y optimizar cada método de migración.

Los clientes tendrán dos opciones para eliminar sus datos de Amazon WorkDocs: la funcionalidad de descarga masiva existente (método 1) o nuestra nueva herramienta de migración de datos (método 2). En los siguientes temas se explica cómo utilizar ambos métodos.

Temas

Método 1: descargar archivos de forma masiva

Si quieres controlar qué archivos migras, puedes descargarlos manualmente de forma masiva. Este método le permite seleccionar solo los archivos que desee y descargarlos a otra ubicación, como su unidad local. Puedes descargar archivos y carpetas desde tu sitio WorkDocs web o desde Amazon WorkDocs Drive.

Recuerde lo siguiente:

- Los usuarios de tu sitio pueden descargar archivos siguiendo los pasos que se indican a continuación. Si lo prefieres, puedes configurar una carpeta compartida, hacer que los usuarios muevan los archivos a esa carpeta y, a continuación, descargar la carpeta a otra ubicación. También puedes transferirte la propiedad y realizar las descargas.
- Para descargar documentos de Microsoft Word con comentarios, consulta Descarga de documentos de Word con comentarios, en la Guía del WorkDocs usuario de Amazon.
- Debes usar Amazon WorkDocs Drive para descargar archivos de más de 5 GB.
- Cuando utilizas Amazon WorkDocs Drive para descargar archivos y carpetas, las estructuras de directorios, los nombres de los archivos y el contenido de los archivos permanecen intactos. La propiedad, los permisos y las versiones de los archivos no se conservan.

Descargar archivos de la web

Este método se utiliza para descargar archivos cuando:

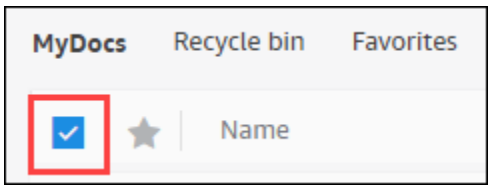
- Solo quieres descargar algunos de los archivos de un sitio.
- Desea descargar documentos de Word con comentarios y hacer que esos comentarios permanezcan en sus documentos respectivos. La herramienta de migración descarga todos los comentarios, pero los escribe en un archivo XML independiente. En ese caso, los usuarios del sitio pueden tener problemas para asociar los comentarios a sus documentos de Word.

Para descargar archivos de la web

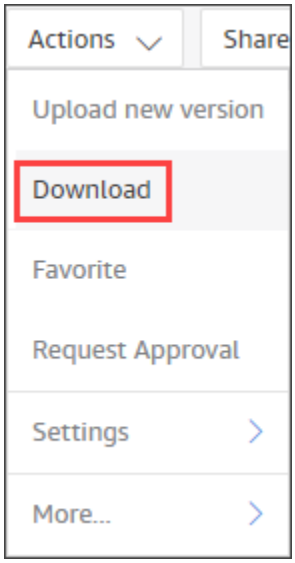
1. Inicia sesión en Amazon WorkDocs.
2. Si es necesario, abre la carpeta que contiene los archivos que quieres descargar.
3. Seleccione la casilla de verificación situada junto a los archivos que desee descargar.

   -O BIEN-

   Selecciona la casilla de verificación situada en la parte superior de la lista para elegir todos los archivos de la carpeta.



4. Abre el menú Acciones y selecciona Descargar. .



En un PC, los archivos descargados aparecen de forma predeterminada en el nombre de la carpeta WorkDocsDownloads Descargas//. En un Macintosh, los archivos aparecen de forma predeterminada en el nombre del disco duro /Usuarios/ nombre de usuario/. WorkDocsDownloads

Descargando carpetas de la web

> **Note**
>
> Al descargar carpetas, también se descargan todos los archivos de las carpetas. Si solo desea descargar algunos de los archivos de una carpeta, mueva los archivos no deseados a otra ubicación o a la papelera de reciclaje y, a continuación, descargue la carpeta.

Para descargar carpetas de la web

1. Inicia sesión en Amazon WorkDocs
2. Selecciona la casilla de verificación situada junto a cada una de las carpetas que quieras descargar.

   -O BIEN-

   Abre las carpetas y selecciona las casillas de verificación situadas junto a las subcarpetas que quieras descargar.
3. Abre el menú Acciones y selecciona Descargar. .

   En un PC, las carpetas descargadas aparecen de forma predeterminada en el nombre de la carpeta WorkDocsDownloads Downloads//. En un Macintosh, los archivos aparecen de forma predeterminada en el nombre del disco duro /Usuarios/ nombre de usuario/. WorkDocsDownloads

Uso de WorkDocs Drive para descargar archivos y carpetas

> **Note**
>
> Debes instalar Amazon WorkDocs Drive para completar los siguientes pasos. Para obtener más información, consulta Instalación de Amazon WorkDocs Drive en la Guía del usuario de Amazon WorkDocs Drive.

Para descargar archivos y carpetas de WorkDocs Drive

1. Inicia el Explorador de archivos o el Finder y abre tu unidad W:.
2. Selecciona las carpetas o los archivos que deseas descargar.
3. Mantén pulsados (haz clic con el botón derecho) en los elementos seleccionados y selecciona Copiar y, a continuación, pega los elementos copiados en su nueva ubicación.

   -O BIEN-

   Arrastra los elementos seleccionados a su nueva ubicación.
4. Elimina los archivos originales de Amazon WorkDocs Drive.

Método 2: usa la herramienta de migración

Utilizas la herramienta de WorkDocs migración de Amazon cuando quieres migrar todos los datos de un WorkDocs sitio.

La herramienta de migración mueve los datos de un sitio a un depósito de Amazon Simple Storage Service. La herramienta crea un archivo ZIP comprimido para cada usuario. El archivo comprimido incluye todos los archivos y carpetas, las versiones, los permisos, los comentarios y las anotaciones de cada uno de los usuarios finales del sitio WorkDocs .

Temas

- Solución de problemas de migraciones
- Ver tu historial de migración

Requisitos previos

Debe tener los siguientes elementos para poder utilizar la herramienta de migración.

- Un bucket de Amazon S3. Para obtener información sobre la creación de un bucket de Amazon S3, consulte Creación de un bucket en la Guía del usuario de Amazon S3. Su bucket debe usar la misma cuenta de IAM y residir en la misma región que su WorkDocs sitio. Además, debes bloquear el acceso público al depósito. Para obtener más información sobre cómo hacerlo, consulte Bloquear el acceso público a su almacenamiento de Amazon S3, en la Guía del usuario de Amazon S3.

  Para conceder WorkDocs permiso a Amazon para cargar tus archivos, configura la política de bucket como se muestra en el siguiente ejemplo. La política utiliza las claves `aws:SourceAccount` y las claves de `aws:SourceArn` condición para reducir el alcance de la política, lo que constituye una práctica recomendada en materia de seguridad.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowWorkDocsFileUpload",
            "Effect": "Allow",
            "Principal": {
                "Service": "workdocs.amazonaws.com"
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::BUCKET-NAME/*",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "AWS-ACCOUNT-ID"
                },
                "ArnLike": {
                    "aws:SourceArn": "arn:aws:workdocs:REGION:AWS-ACCOUNT-
ID:organization/WORKDOCS-DIRECTORY-ID"
                }
            }
        }
```

```
    ]
}
```

> **Note**
>
> - *WORKDOCS-DIRECTORY-ID* es el identificador de la organización de su sitio. WorkDocs Puede consultarlo en la tabla «Mis sitios» de la WorkDocs consola de AWS
> - Para obtener más información sobre la configuración de una política de bucket, consulte Añadir una política de bucket mediante la consola Amazon S3

- Una política de IAM. Para iniciar una migración en la WorkDocs consola, el operador principal de IAM debe tener la siguiente política asociada a su conjunto de permisos:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowStartWorkDocsMigration",
            "Effect": "Allow",
            "Action": [
                "workdocs:StartInstanceExport"
            ],
            "Resource": [
                "arn:aws:workdocs:REGION:AWS-ACCOUNT-ID:organization/WORKDOCS-
DIRECTORY-ID"
            ]
        },
        {
            "Sid": "AllowDescribeWorkDocsMigrations",
            "Effect": "Allow",
            "Action": [
                "workdocs:DescribeInstanceExports",
                "workdocs:DescribeInstances"
            ],
            "Resource": [
                "*"
            ]
        },
        {
            "Sid": "AllowS3Validations",
            "Effect": "Allow",
```

```
            "Action": [
                "s3:HeadBucket",
                "s3:ListBucket",
                "s3:GetBucketPublicAccessBlock",
                "kms:ListAliases"
            ],
            "Resource": [
                "arn:aws:s3:::BUCKET-NAME"
            ]
        },
        {
            "Sid": "AllowS3ListMyBuckets",
            "Effect": "Allow",
            "Action": [
                "s3:ListAllMyBuckets"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

- Si lo desea, puede usar una AWS KMS clave para cifrar los datos en reposo de su depósito. Si no proporciona una clave, se aplicará la configuración de cifrado estándar del depósito. Para obtener más información, consulte Creación de claves en la Guía AWS para desarrolladores del Servicio de administración de claves.

  Para usar una AWS KMS clave, añada las siguientes declaraciones a la política de IAM. Debe usar una clave activa del tipo SYMMETRIC_DEFAULT.

```
{
    "Sid": "AllowKMSMigration",
     "Effect": "Allow",
     "Action": [
         "kms:CreateGrant",
         "kms:DescribeKey"
     ],
     "Resource": [

         "arn:aws:kms:REGION:AWS-ACCOUNT-ID:key/KEY-RESOURCE-ID"
     ]
```

```
}
```

Limitaciones

La herramienta de migración tiene las siguientes limitaciones:

- La herramienta escribe todos los permisos, comentarios y anotaciones de los usuarios en archivos CSV independientes. Debe asignar esos datos a los archivos correspondientes de forma manual.
- Solo puede migrar sitios activos.
- La herramienta está limitada a una migración correcta por sitio por cada período de 24 horas.
- No puede ejecutar migraciones simultáneas del mismo sitio, pero puede ejecutar migraciones simultáneas para sitios diferentes.
- Cada archivo zip tendrá un tamaño máximo de 50 GB. A los usuarios con más de 50 GB de datos se WorkDocs les exportarán varios archivos zip a Amazon S3.
- La herramienta no exporta archivos de más de 50 GB. La herramienta muestra todos los archivos de más de 50 GB en un archivo CSV que tenga el mismo prefijo que los archivos ZIP. ***Por ejemplo, /workdocs/ site-alias/Created-Timestamp-UTC /skippedFiles.csv.*** Puede descargar los archivos de la lista mediante programación o manualmente. Para obtener información sobre la descarga mediante programaciónhttps://docs.aws.amazon.com/workdocs/latest/developerguide/download-documents.html, consulte la Guía para WorkDocs desarrolladores de Amazon. Para obtener información sobre la descarga manual de los archivos, consulte los pasos del Método 1, que se encuentra anteriormente en este tema.
- El archivo zip de cada usuario solo contendrá los archivos o carpetas de su propiedad. Todos los archivos o carpetas que se hayan compartido con el usuario estarán en el archivo zip del usuario propietario de los archivos o carpetas.
- Si una carpeta está vacía (no contiene archivos o carpetas anidados) WorkDocs, no se exportará.
- No se garantiza que los datos (archivos, carpetas, versiones, comentarios, anotaciones) creados después de iniciar el trabajo de migración se incluyan en los datos exportados a S3.
- Puede migrar varios sitios a un bucket de Amazon S3. No necesita crear un bucket por sitio. Sin embargo, debes asegurarte de que tus políticas de IAM y de bucket permitan varios sitios.
- La migración aumenta los costos de Amazon S3, en función de la cantidad de datos que migre al bucket. Para obtener más información, consulte la página de precios de Amazon S3.

Ejecutar la herramienta de migración

En los siguientes pasos se explica cómo ejecutar la herramienta de WorkDocs migración de Amazon.

Para migrar un sitio

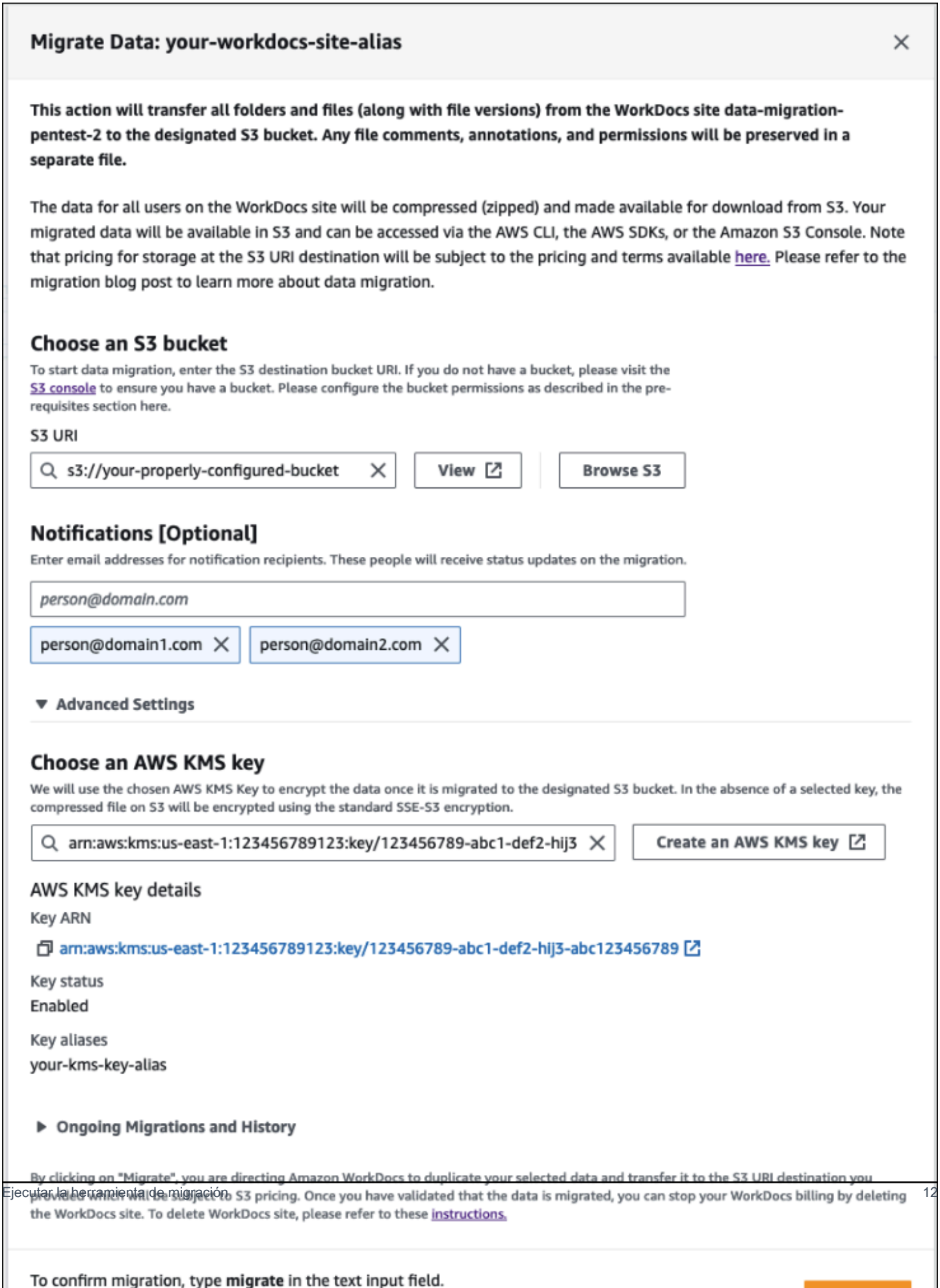
1. Abre la WorkDocs consola de Amazon en https://console.aws.amazon.com/zocalo/.
2. En el panel de navegación, selecciona Mis sitios y, a continuación, selecciona el botón de radio situado junto al sitio que deseas migrar.
3. Abre la lista de acciones y selecciona Migrar datos.
4. En la página del nombre del sitio de Migrate Data, introduce el URI de tu bucket de Amazon S3.

   -O BIEN-

   Selecciona Browse S3 y sigue estos pasos:

   a. Si es necesario, busca el depósito.
   b. Selecciona el botón de radio situado junto al nombre del depósito y, a continuación, selecciona Elegir.
5. (Opcional) En Notificaciones, introduce un máximo de cinco direcciones de correo electrónico. La herramienta envía correos electrónicos sobre el estado de la migración a cada destinatario.
6. (Opcional) En Configuración avanzada, selecciona una clave KMS para cifrar los datos almacenados.
7. Introduzca **`migrate`** en el cuadro de texto para confirmar la migración y, a continuación, seleccione Iniciar migración.

   Aparece un indicador que muestra el estado de la migración. Los tiempos de migración varían en función de la cantidad de datos de un sitio.


Migrate Data: your-workdocs-site-alias
This action will transfer all folders and files (along with file versions) from the WorkDocs site data-migration-pentest-2 to the designated S3 bucket. Any file comments, annotations, and permissions will be preserved in a separate file.
The data for all users on the WorkDocs site will be compressed (zipped) and made available for download from S3. Your migrated data will be available in S3 and can be accessed via the AWS CLI, the AWS SDKs, or the Amazon S3 Console. Note that pricing for storage at the S3 URI destination will be subject to the pricing and terms available here. Please refer to the migration blog post to learn more about data migration.
Choose an S3 bucket
To start data migration, enter the S3 destination bucket URI. If you do not have a bucket, please visit the S3 console to ensure you have a bucket. Please configure the bucket permissions as described in the pre-requisites section here.
S3 URI
s3://your-properly-configured-bucket
View
Browse S3
Notifications [Optional]
Enter email addresses for notification recipients. These people will receive status updates on the migration.
person@domain.com
person@domain1.com
person@domain2.com
Advanced Settings
Choose an AWS KMS key
We will use the chosen AWS KMS Key to encrypt the data once it is migrated to the designated S3 bucket. In the absence of a selected key, the compressed file on S3 will be encrypted using the standard SSE-S3 encryption.
arn:aws:kms:us-east-1:123456789123:key/123456789-abc1-def2-hij3
Create an AWS KMS key
AWS KMS key details
Key ARN
arn:aws:kms:us-east-1:123456789123:key/123456789-abc1-def2-hij3-abc123456789
Key status
Enabled
Key aliases
your-kms-key-alias
Ongoing Migrations and History
By clicking on "Migrate", you are directing Amazon WorkDocs to duplicate your selected data and transfer it to the S3 URI destination you provided which will be subject to S3 pricing. Once you have validated that the data is migrated, you can stop your WorkDocs billing by deleting the WorkDocs site. To delete WorkDocs site, please refer to these instructions.
To confirm migration, type migrate in the text input field.

Cuando finalice la migración:

- La herramienta envía correos electrónicos de «éxito» a las direcciones ingresadas durante la configuración, si las hay.
- ***Su bucket de Amazon S3 contendrá una carpeta /workdocs/ site-alias/ created-timestamp-UTC/.*** Esa carpeta contiene una carpeta comprimida para cada usuario que tenía datos en el sitio. Cada carpeta comprimida contiene las carpetas y los archivos del usuario, incluidos los permisos y los comentarios que mapean los archivos CSV.
- Si un usuario elimina todos sus archivos antes de la migración, no aparecerá ninguna carpeta comprimida para ese usuario.
- Versiones: los documentos con varias versiones tienen un identificador de fecha y hora de creación de _ versión _. La marca de tiempo utiliza milisegundos por época. Por ejemplo, un documento denominado «TestFile.txt» con dos versiones aparece de la siguiente manera:

```
        TestFile.txt (version 2 - latest version)
        TestFile_version_1707437230000.txt
```

- Permisos: en el siguiente ejemplo, se muestra el contenido de un archivo CSV de permisos típico.

```
PathToFile,PrincipalName,PrincipalType,Role
/mydocs/Projects,user1@domain.com,USER,VIEWER
/mydocs/Personal,user2@domain.com,USER,VIEWER
/mydocs/Documentation/Onboarding_Guide.xml,user2@domain.com,USER,CONTRIBUTOR
/mydocs/Documentation/Onboarding_Guide.xml,user1@domain.com,USER,CONTRIBUTOR
/mydocs/Projects/Initiative,user2@domain.com,USER,CONTRIBUTOR
/mydocs/Notes,user2@domain.com,USER,COOWNER
/mydocs/Notes,user1@domain.com,USER,COOWNER
/mydocs/Projects/Initiative/Structures.xml,user3@domain.com,USER,COOWNER
```

- Comentarios: en el siguiente ejemplo, se muestra el contenido de un archivo CSV de comentarios típico.

```
PathToFile,PrincipalName,PostedTimestamp,Text
/mydocs/Documentation/
Onboarding_Guide.xml,user1@domain.com,2023-12-28T20:57:40.781Z,TEST ANNOTATION 1
/mydocs/Documentation/
Onboarding_Guide.xml,user2@domain.com,2023-12-28T22:18:09.812Z,TEST ANNOTATION 2
```

```
/mydocs/Documentation/
Onboarding_Guide.xml,user3@domain.com,2023-12-28T22:20:04.099Z,TEST ANNOTATION 3
/mydocs/Documentation/
Onboarding_Guide.xml,user1@domain.com,2023-12-28T20:56:27.390Z,TEST COMMENT 1
/mydocs/Documentation/
Onboarding_Guide.xml,user2@domain.com,2023-12-28T22:17:10.348Z,TEST COMMENT 2
/mydocs/Documentation/
Onboarding_Guide.xml,user3@domain.com,2023-12-28T22:19:42.821Z,TEST COMMENT 3
/mydocs/Projects/Agora/
Threat_Model.xml,user1@domain.com,2023-12-28T22:21:09.930Z,TEST ANNOTATION 4
/mydocs/Projects/Agora/
Threat_Model.xml,user1@domain.com,2023-12-28T20:57:04.931Z,TEST COMMENT 4
```

- Archivos omitidos: el siguiente ejemplo muestra el contenido de un archivo CSV de archivos omitidos típico. Hemos acortado el identificador y omitido los valores del motivo para una mejor legibilidad.

```
FileOwner,PathToFile,DocumentId,VersionId,SkippedReason
user1@domain.com,/mydocs/LargeFile1.mp4,45e433b5469...,170899345...,The file is too
 large. Please notify the document owner...
user2@domain.com,/mydocs/LargeFile2.pdf,e87f725898c1...,170899696...,The file is too
 large. Please notify the document owner...
```

Descarga de datos migrados de Amazon S3

Dado que la migración aumenta los costes de Amazon S3, puede descargar los datos migrados de Amazon S3 a otra solución de almacenamiento. En este tema se explica cómo descargar los datos migrados y se ofrecen sugerencias para cargar los datos en una solución de almacenamiento.

> **Note**
>
> En los pasos siguientes se explica cómo descargar un archivo o una carpeta a la vez. Para obtener información sobre otras formas de descargar archivos, consulte Descarga de objetos en la Guía del usuario de Amazon S3.

Para descargar datos

1. Abra la consola de Amazon S3 en https://console.aws.amazon.com/s3.
2. Seleccione el segmento de destino y navegue hasta el alias del sitio.

3. Selecciona la casilla de verificación situada junto a la carpeta comprimida.

   -O BIEN-

   Abre la carpeta comprimida y selecciona la casilla de verificación situada junto al archivo o la carpeta de un usuario individual.
4. Elija Descargar.

Sugerencias de soluciones de almacenamiento

Para sitios de gran tamaño, recomendamos aprovisionar una instancia EC2 mediante una Amazon Machine Image compatible basada en Linux para descargar mediante programación los datos de Amazon S3, descomprimirlos y, a continuación, cargarlos en el proveedor de almacenamiento o en el disco local.

Solución de problemas de migraciones

Siga estos pasos para asegurarse de que ha configurado su entorno correctamente:

- Si se produce un error en la migración, aparece un mensaje de error en la pestaña Historial de migraciones de la WorkDocs consola. Revise el mensaje de error.
- Compruebe la configuración de su bucket de Amazon S3.
- Vuelva a ejecutar la migración.

Si el problema continúa, póngase en contacto con AWS Support. Incluya la URL del WorkDocs sitio y el ID del trabajo de migración, que se encuentran en la tabla del historial de migraciones.

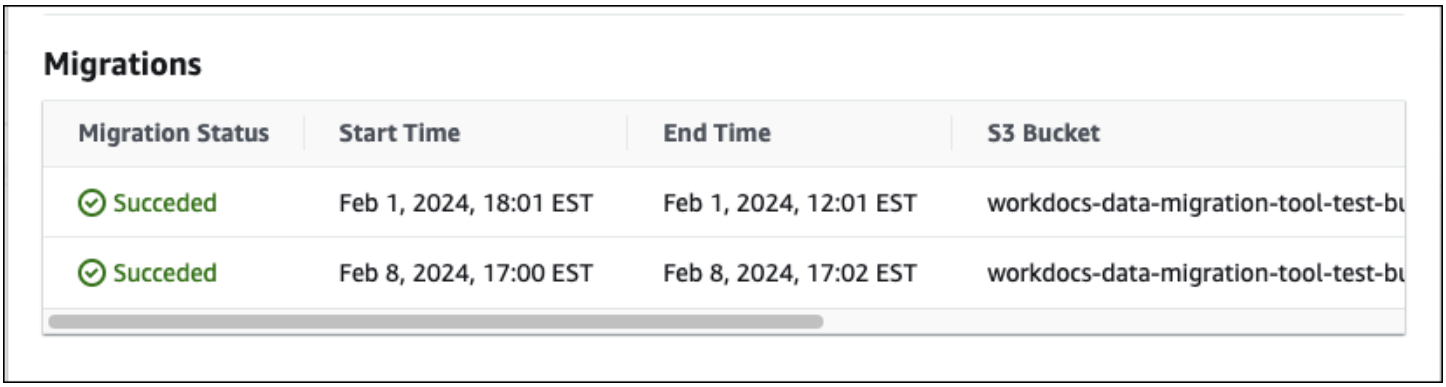
Ver tu historial de migración

En los siguientes pasos se explica cómo ver el historial de migración.

Para ver tu historial

1. Abre la WorkDocs consola de Amazon en https://console.aws.amazon.com/zocalo/.
2. Selecciona el botón de radio situado junto al WorkDocs sitio deseado.
3. Abra la lista de acciones y elija Migrar datos.
4. En la página del nombre del sitio de migración de datos, seleccione Migraciones e historial en curso.

El historial de migraciones aparece en Migraciones. La siguiente imagen muestra un historial típico.



Requisitos previos para Amazon WorkDocs

Para configurar nuevos WorkDocs sitios de Amazon o gestionar los sitios existentes, debes completar las siguientes tareas.

Inscríbase en una Cuenta de AWS

Si no tienes un Cuenta de AWS, complete los pasos siguientes para crear uno.

Para suscribirte a una Cuenta de AWS

1. Abrir https://portal.aws.amazon.com/billing/registro.
2. Siga las instrucciones que se le indiquen.

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

   Cuando te registras en una Cuenta de AWS, un Usuario raíz de la cuenta de AWSse crea. El usuario root tiene acceso a todos Servicios de AWS y los recursos de la cuenta. Como práctica recomendada de seguridad, asigne acceso administrativo a un usuario y utilice únicamente el usuario raíz para realizar tareas que requieren acceso de usuario raíz.

AWS te envía un correo electrónico de confirmación una vez finalizado el proceso de registro. En cualquier momento, puede ver la actividad de su cuenta actual y administrarla accediendo a https://aws.amazon.com/y seleccionando Mi cuenta.

Creación de un usuario con acceso administrativo

Después de suscribirse a una Cuenta de AWS, asegure su Usuario raíz de la cuenta de AWS, habilitar AWS IAM Identity Center y cree un usuario administrativo para no utilizar el usuario root en las tareas diarias.

Proteja su Usuario raíz de la cuenta de AWS

1. Inicie sesión en la AWS Management Consolecomo propietario de la cuenta seleccionando el usuario root e introduciendo su Cuenta de AWS dirección de correo electrónico. En la siguiente página, escriba su contraseña.

Para obtener ayuda para iniciar sesión con un usuario root, consulte Iniciar sesión como usuario root en AWS Sign-In Guía del usuario.

2. Activa la autenticación multifactorial (MFA) para tu usuario root.

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

Creación de un usuario con acceso administrativo

1. Habilite IAM Identity Center.

   Para obtener instrucciones, consulte Habilitar AWS IAM Identity Center en la AWS IAM Identity Center Guía del usuario.

2. En IAM Identity Center, conceda acceso administrativo a un usuario.

   Para ver un tutorial sobre el uso de Directorio de IAM Identity Center como fuente de identidad, consulte Configurar el acceso de los usuarios con la configuración predeterminada Directorio de IAM Identity Center en la AWS IAM Identity Center Guía del usuario.

Iniciar sesión como usuario con acceso de administrador

- Para iniciar sesión con su usuario de IAM Identity Center, utilice el inicio de sesión URL que se envió a su dirección de correo electrónico cuando creó el usuario de IAM Identity Center.

  Para obtener ayuda para iniciar sesión con un usuario de IAM Identity Center, consulte Iniciar sesión en AWS acceda al portal en el AWS Sign-In Guía del usuario.

Concesión de acceso a usuarios adicionales

1. En IAM Identity Center, cree un conjunto de permisos que siga la práctica recomendada de aplicar permisos con privilegios mínimos.

   Para obtener instrucciones, consulte Crear un conjunto de permisos en AWS IAM Identity Center Guía del usuario.

2. Asigne usuarios a un grupo y, a continuación, asigne el acceso de inicio de sesión único al grupo.

Para obtener instrucciones, consulte Añadir grupos en AWS IAM Identity Center Guía del usuario.

Seguridad en Amazon WorkDocs

La seguridad en la nube AWS es la máxima prioridad. Como AWS cliente, usted se beneficia de una arquitectura de centro de datos y red diseñada para cumplir con los requisitos de las organizaciones más sensibles a la seguridad.

La seguridad es una responsabilidad compartida entre usted 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 AWS los servicios en la AWS nube. AWS también le proporciona servicios que puede utilizar de forma segura. Auditores independientes 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 conformidad que se aplican a Amazon WorkDocs, consulta AWS Servicios incluidos en el ámbito de aplicación por programa de conformidad.
- Seguridad en la nube: el AWS servicio que utilices determina tu 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 te ayudan a entender cómo aplicar el modelo de responsabilidad compartida cuando utilizas Amazon WorkDocs.

> **Note**
>
> Los usuarios de una WorkDocs organización pueden colaborar con usuarios ajenos a esa organización enviando un enlace o una invitación a un archivo. Sin embargo, esto solo se aplica a los sitios que utilizan un conector de Active Directory. Consulte la configuración de enlaces compartidos de su sitio y seleccione la opción que mejor se adapte a los requisitos de su empresa.

En los temas siguientes, se muestra cómo configurar Amazon WorkDocs para que cumpla con sus objetivos de seguridad y conformidad. 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

- Registro y supervisión en Amazon WorkDocs
- Validación de conformidad para Amazon WorkDocs
- Resiliencia en Amazon WorkDocs
- Seguridad de infraestructuras en Amazon WorkDocs

Gestión de identidades y accesos para Amazon WorkDocs

AWS Identity and Access Management (IAM) es una Servicio de AWS que ayuda al administrador a controlar de forma segura el acceso a AWS los recursos. IAMlos administradores controlan quién puede autenticarse (iniciar sesión) y quién está autorizado (tiene permisos) para usar los WorkDocs recursos de Amazon. IAMes una Servicio de AWS que puede utilizar sin coste adicional.

Temas

- Público
- Autenticación con identidades
- Administración de acceso mediante políticas
- Cómo WorkDocs trabaja Amazon con IAM
- Ejemplos de políticas WorkDocs basadas en la identidad de Amazon
- Solución de problemas de WorkDocs identidad y acceso a Amazon

Público

La forma de usar AWS Identity and Access Management (IAM) varía según el trabajo que realices en Amazon WorkDocs.

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 al administrador. Si no puedes acceder a una función de Amazon WorkDocs, consultaSolución de problemas de WorkDocs identidad y acceso a Amazon.

Administrador de servicios: si estás a cargo de WorkDocs los recursos de Amazon en tu empresa, probablemente tengas acceso total a Amazon WorkDocs. Es tu trabajo determinar a qué WorkDocs

funciones y recursos de Amazon deben acceder los usuarios de tu servicio. A continuación, debe enviar solicitudes a su IAM administrador para cambiar los permisos de los usuarios del servicio. Revise la información de esta página para comprender los conceptos básicos deIAM. Para obtener más información sobre cómo tu empresa puede utilizar IAM Amazon WorkDocs, consultaCómo WorkDocs trabaja Amazon con IAM.

IAMadministrador: si eres IAM administrador, es posible que desees obtener más información sobre cómo puedes redactar políticas para gestionar el acceso a Amazon WorkDocs. Para ver ejemplos de políticas WorkDocs basadas en la identidad de Amazon que puedes usarIAM, consulta. Ejemplos de políticas WorkDocs basadas en la identidad de Amazon

Autenticación con identidades

La autenticación es la forma en que inicias sesión AWS con tus credenciales de identidad. Debe estar autenticado (con quien haya iniciado sesión AWS) como IAM usuario o asumiendo un IAM rol. Usuario raíz de la cuenta de AWS

Puede iniciar sesión AWS como una identidad federada mediante las credenciales proporcionadas a través de una fuente de identidad. AWS IAM Identity Center Los usuarios (IAMIdentity 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 una identidad federada, el administrador configuró previamente la federación de identidades mediante roles. IAM Cuando accede AWS mediante la federación, asume indirectamente un rol.

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

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

Independientemente del método de autenticación que use, es posible que deba proporcionar información de seguridad adicional. Por ejemplo, le AWS recomienda que utilice la autenticación multifactorial (MFA) para aumentar la seguridad de su cuenta. Para obtener más información, consulte Autenticación multifactorial en la Guía del AWS IAM Identity Center usuario y Uso de la autenticación multifactorial (MFA) AWS en la Guía del IAM usuario.

Usuarios y grupos de IAM

Un IAMusuario es una identidad propia Cuenta de AWS que tiene permisos específicos para una sola persona o aplicación. Siempre que sea posible, recomendamos utilizar credenciales temporales en lugar de crear IAM usuarios con credenciales de larga duración, como contraseñas y claves de acceso. Sin embargo, si tiene casos de uso específicos que requieren credenciales a largo plazo con IAM los usuarios, le recomendamos que rote las claves de acceso. Para obtener más información, consulte Rotar las claves de acceso con regularidad para los casos de uso que requieran credenciales de larga duración en la Guía del IAM usuario.

Un IAMgrupo es una identidad que especifica un conjunto de IAM usuarios. 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 para grandes conjuntos de usuarios. Por ejemplo, puede asignar un nombre a un grupo IAMAdminsy concederle permisos para administrar IAM los recursos.

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 de larga duración permanentes; no obstante, los roles proporcionan credenciales temporales. Para obtener más información, consulte Cuándo crear un IAM usuario (en lugar de un rol) en la Guía del IAM usuario.

IAMroles

Un IAMrol es una identidad dentro de ti Cuenta de AWS que tiene permisos específicos. Es similar a un IAM usuario, pero no está asociado a una persona específica. Puede asumir temporalmente un IAM rol en el AWS Management Console cambiando de rol. Puede asumir un rol llamando a una AWS API operación AWS CLI o o utilizando una operación personalizadaURL. Para obtener más información sobre los métodos de uso de roles, consulte Uso de IAM roles en la Guía del IAM usuario.

IAMlos roles 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 sus permisos. Cuando se autentica una identidad federada, se asocia la identidad al rol y se le conceden los permisos define el rol. Para obtener información sobre los roles para la federación, consulte Creación de un rol para un proveedor de identidad externo en la Guía del IAM usuario. Si usa IAM Identity Center, configura un conjunto de permisos. Para controlar a qué pueden acceder sus identidades después de autenticarse, IAM Identity Center correlaciona el

conjunto de permisos con un rol en. IAM Para obtener información acerca de los conjuntos de permisos, consulte Conjuntos de permisos en la Guía del usuario de AWS IAM Identity Center .

- Permisos IAM de usuario temporales: un IAM usuario o rol puede asumir un IAM rol para asumir temporalmente diferentes permisos para una tarea específica.
- Acceso multicuenta: puedes usar un IAM rol para permitir que alguien (un responsable de confianza) de una cuenta diferente acceda a los recursos de tu cuenta. Los roles son la forma principal de conceder acceso entre cuentas. Sin embargo, con algunos Servicios de AWS, puedes adjuntar una política directamente a un recurso (en lugar de usar un rol como proxy). Para conocer la diferencia entre las funciones y las políticas basadas en recursos para el acceso multicuenta, consulta el tema sobre el acceso a los recursos entre cuentas IAM en la Guía del IAM usuario.
- Acceso entre servicios: algunos Servicios de AWS utilizan funciones en otros. Servicios de AWS Por ejemplo, cuando realizas una llamada en un servicio, es habitual 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 al servicio.
  - Sesiones de acceso directo (FAS): cuando utilizas un IAM usuario o un rol para realizar acciones en AWS ellas, se te considera director. Cuando utiliza algunos servicios, es posible que realice una acción que desencadene otra acción en un servicio diferente. FASutiliza los permisos del principal que llama a an Servicio de AWS, junto con los que solicitan, Servicio de AWS para realizar solicitudes a los servicios descendentes. FASlas solicitudes solo se realizan cuando un servicio recibe una solicitud que requiere interacciones con otros Servicios de AWS recursos para completarse. En este caso, debe tener permisos para realizar ambas acciones. Para obtener información detallada sobre la política a la hora de realizar FAS solicitudes, consulte Reenviar las sesiones de acceso.
  - Función de servicio: una función de servicio es una IAMfunción que un servicio asume para realizar acciones en su nombre. Un IAM administrador puede crear, modificar y eliminar un rol de servicio desde dentroIAM. Para obtener más información, consulte Crear un rol para delegar permisos Servicio de AWS en un rol en el IAMManual del usuario.
  - Función vinculada a un servicio: una función vinculada a un servicio es un tipo de función de servicio que está vinculada a un. Servicio de AWS El servicio puede asumir el rol para realizar una acción en su nombre. Los roles vinculados al servicio aparecen en usted Cuenta de AWS y son propiedad del servicio. Un IAM administrador puede ver los permisos de los roles vinculados al servicio, pero no editarlos.
- Aplicaciones que se ejecutan en Amazon EC2: puedes usar un IAM rol para administrar las credenciales temporales de las aplicaciones que se ejecutan en una EC2 instancia y que realizan

AWS CLI o AWS API solicitan. Esto es preferible a almacenar las claves de acceso en la EC2 instancia. Para asignar un AWS rol a una EC2 instancia y ponerlo a disposición de todas sus aplicaciones, debe crear un perfil de instancia adjunto a la instancia. Un perfil de instancia contiene el rol y permite que los programas que se ejecutan en la EC2 instancia obtengan credenciales temporales. Para obtener más información, consulte Uso de un IAM rol para conceder permisos a aplicaciones que se ejecutan en EC2 instancias de Amazon en la Guía del IAM usuario.

Para saber si se deben usar IAM roles o IAM usuarios, consulte Cuándo crear un IAM rol (en lugar de un usuario) en la Guía del IAM usuario.

Administración de acceso mediante políticas

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

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

De forma predeterminada, los usuarios y los roles no tienen permisos. Para conceder a los usuarios permiso para realizar acciones en los recursos que necesitan, un IAM administrador puede crear IAM políticas. A continuación, el administrador puede añadir las IAM políticas a las funciones y los usuarios pueden asumir las funciones.

IAMlas políticas definen los 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 esa política puede obtener información sobre el rol de AWS Management Console AWS CLI, el o el AWS API.

Políticas basadas en identidad

Las políticas basadas en la identidad son documentos de política de JSON permisos que se pueden adjuntar a una identidad, como un IAM usuario, un grupo de usuarios o un rol. Estas políticas controlan qué acciones pueden realizar los usuarios y los roles, en qué recursos y en

qué condiciones. Para obtener información sobre cómo crear una política basada en la identidad, consulte Creación de IAM políticas en la Guía del usuario. IAM

Las políticas basadas en identidades 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 funciones de su empresa. Cuenta de AWS Las políticas administradas incluyen políticas AWS administradas y políticas administradas por el cliente. Para saber cómo elegir entre una política gestionada o una política integrada, consulte Elegir entre políticas gestionadas y políticas integradas en la Guía del IAM usuario.

Políticas basadas en recursos

Las políticas basadas en recursos son documentos de JSON política que se adjuntan a un recurso. Algunos ejemplos de políticas basadas en recursos son las políticas de confianza de IAM roles 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 asocia 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 en función de recursos. Los 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 puede usar políticas AWS administradas desde una política IAM basada en recursos.

Listas de control de acceso

Las listas de control de acceso (ACLs) controlan qué responsables (miembros de la cuenta, usuarios o roles) tienen permisos para acceder a un recurso. ACLsson similares a las políticas basadas en recursos, aunque no utilizan el formato de documento de JSON políticas.

Amazon S3 AWS WAF y Amazon VPC son ejemplos de servicios compatiblesACLs. Para obtener más informaciónACLs, consulte la descripción general de la lista de control de acceso (ACL) en la Guía para desarrolladores de Amazon Simple Storage Service.

Otros tipos de políticas

AWS admite tipos de políticas adicionales y menos comunes. Estos tipos de políticas pueden establecer el máximo de permisos que los tipos de políticas más frecuentes le conceden.

- Límites de permisos: un límite de permisos es una función avanzada en la que se establecen los permisos máximos que una política basada en la identidad puede conceder a una IAM entidad (IAMusuario o rol). Puede establecer un límite de permisos para una entidad. Los permisos resultantes son la intersección de las políticas basadas en la 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 los límites de los permisos para IAM las entidades en la Guía del IAMusuario.
- Políticas de control de servicios (SCPs): SCPs son JSON políticas que especifican los permisos máximos para una organización o unidad organizativa (OU) AWS Organizations. AWS Organizations es un servicio para agrupar y administrar de forma centralizada varios de los Cuentas de AWS que son propiedad de su empresa. Si habilitas todas las funciones de una organización, puedes aplicar políticas de control de servicios (SCPs) a una o a todas tus cuentas. SCPLimita los permisos de las entidades en las cuentas de los miembros, incluidas las de cada una Usuario raíz de la cuenta de AWS. Para obtener más información sobre OrganizationsSCPs, consulte las políticas de control de servicios en la Guía del AWS Organizations usuario.
- 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 identidades del rol y las políticas de la sesión. Los permisos también pueden proceder de una política en función de recursos. Una denegación explícita en cualquiera de estas políticas anulará el permiso. Para obtener más información, consulte las políticas de sesión en la Guía del IAM usuario.

> **Note**
>
> Amazon WorkDocs no admite las políticas de control de servicios para Slack Organizations.

Varios tipos de políticas

Cuando se aplican varios tipos de políticas a una solicitud, los permisos resultantes son más complicados de entender. Para saber cómo AWS determinar si se debe permitir una solicitud cuando se trata de varios tipos de políticas, consulta la lógica de evaluación de políticas en la Guía del IAM usuario.

Cómo WorkDocs trabaja Amazon con IAM

Antes de gestionar el acceso a Amazon WorkDocs, tienes que entender qué IAM funciones están disponibles para su uso con Amazon WorkDocs. IAM Para obtener una visión general de cómo funcionan Amazon WorkDocs y otros AWS serviciosIAM, consulta AWS los servicios con los que funcionan IAM en la Guía del IAM usuario.

Temas

- Políticas de Amazon WorkDocs basadas en la identidad
- Políticas de Amazon WorkDocs basadas en recursos
- Autorización basada en WorkDocs etiquetas de Amazon
- WorkDocs IAMFunciones en Amazon

Políticas de Amazon WorkDocs basadas en la identidad

Con las políticas IAM basadas en la identidad, puede especificar las acciones permitidas o denegadas. Amazon WorkDocs apoya acciones específicas. Para obtener más información sobre los elementos que utilizas en una JSON política, consulta la referencia sobre los elementos de la IAM JSON política en la Guía del IAM usuario.

Acciones

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

El `Action` elemento de una JSON política describe las acciones que puede utilizar para permitir o denegar el acceso en una política. Las acciones de política suelen tener el mismo nombre que la AWS API operación asociada. Hay algunas excepciones, como las acciones que solo permiten permisos y que no tienen una operación coincidente. API 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 que ejecute la WorkDocs `DescribeUsers` API operación 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 puedes 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 acción `zocalo`. Por ejemplo:
>
> ```
> "Action": [
> "zocalo:*",
> "workdocs:*"
> ],
> ```

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

Recursos

Amazon WorkDocs no admite la especificación de recursos ARNs 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 AWS globales, consulta las claves de contexto de condición AWS globales en la Guía del IAMusuario.

Ejemplos

Para ver ejemplos de políticas de Amazon WorkDocs basadas en la identidad, consulta. Ejemplos de políticas WorkDocs basadas en la identidad de Amazon

Políticas de Amazon WorkDocs basadas en recursos

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 las etiquetas.

WorkDocs IAMFunciones en Amazon

Un IAMrol es una entidad de tu AWS cuenta que tiene permisos específicos.

Uso de credenciales temporales con Amazon WorkDocs

Recomendamos encarecidamente utilizar credenciales temporales para iniciar sesión con la federación, asumir un IAM rol o asumir un rol multicuenta. Para obtener credenciales de seguridad temporales, llame a AWS STS API operaciones como AssumeRoleo GetFederationToken.

Amazon WorkDocs admite el uso de credenciales temporales.

Roles vinculados al servicio

Los roles vinculados a un servicio permiten a AWS los servicios acceder a los recursos de otros servicios para completar una acción en tu nombre. Los roles vinculados al servicio aparecen en tu IAM cuenta y son propiedad del servicio. Un IAM administrador puede ver los permisos de los roles vinculados al servicio, pero no editarlos.

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 tu IAM cuenta y son propiedad de la cuenta. Esto significa que un IAM administrador 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 la identidad de Amazon

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

De forma predeterminada, IAM los usuarios y los roles no tienen permiso para crear o modificar WorkDocs los recursos de Amazon. Tampoco pueden realizar tareas con AWS Management Console AWS CLI, o AWS API. IAMEl administrador debe crear IAM políticas que concedan a los usuarios y roles permisos para realizar API operaciones específicas en los recursos específicos que necesitan. A continuación, el administrador debe adjuntar esas políticas a los IAM usuarios o grupos que requieran esos permisos.

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

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

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

Temas

Prácticas recomendadas sobre las políticas

Las políticas basadas en la identidad determinan si alguien puede crear, acceder o eliminar WorkDocs los recursos de Amazon de 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 identidades:

- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos: para empezar a conceder permisos a sus usuarios y cargas de trabajo, utilice las políticas AWS administradas que otorgan permisos para muchos casos de uso comunes. Están disponibles en su. Cuenta de AWS Le recomendamos que reduzca aún más los permisos definiendo políticas administradas por el AWS cliente que sean específicas para sus casos de uso. Para obtener más información, consulte las políticas AWS gestionadas o las políticas AWS gestionadas para las funciones laborales en la Guía del IAM usuario.
- Aplique permisos con privilegios mínimos: cuando establezca permisos con IAM políticas, 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. Para obtener más información sobre cómo IAM aplicar permisos, consulte Políticas y permisos IAM en la IAM Guía del usuario.
- Utilice las condiciones en IAM las políticas para restringir aún más el acceso: puede añadir 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 medianteSSL. También puedes usar condiciones para conceder el acceso a las acciones del servicio si se utilizan a través de una acción específica Servicio de AWS, por ejemplo AWS CloudFormation. Para obtener más información, consulte los elementos IAM JSON de la política: Condición en la Guía del IAM usuario.
- Utilice IAM Access Analyzer para validar sus IAM políticas y garantizar permisos seguros y funcionales: IAM Access Analyzer valida las políticas nuevas y existentes para que se ajusten

al lenguaje de las políticas (JSON) y IAM a las IAM mejores prácticas. IAMAccess Analyzer proporciona más de 100 comprobaciones de políticas y recomendaciones prácticas para ayudarle a crear políticas seguras y funcionales. Para obtener más información, consulte la validación de políticas de IAM Access Analyzer en la Guía del IAM usuario.

- Requerir autenticación multifactorial (MFA): si se encuentra en una situación en la que se requieren IAM usuarios o un usuario raíz Cuenta de AWS, actívela MFA para aumentar la seguridad. Para solicitarlo MFA cuando se convoque a API las operaciones, añada MFA condiciones a sus políticas. Para obtener más información, consulte Configuración del API acceso MFA protegido en la Guía del IAM usuario.

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

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 permitirte enumerar y ver los detalles de los WorkDocs recursos de Amazon de tu AWS cuenta. Si creas una política basada en la identidad que sea más restrictiva que los permisos mínimos requeridos, la consola no funcionará según lo previsto para las entidades de IAM usuario o rol.

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, consulta Cómo añadir permisos a un usuario en la Guía del IAM usuario.

- AmazonWorkDocsFullAccess
- AWSDirectoryServiceFullAccess
- Amazon EC2FullAccess

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

No es necesario conceder permisos mínimos de consola a los usuarios que solo realicen llamadas al AWS CLI o al AWS API. En su lugar, permita el acceso únicamente a las acciones que coincidan con la API operación que está intentando realizar.

Cómo permitir a los usuarios consultar sus propios permisos

En este ejemplo, se muestra cómo se puede crear una política que permita a IAM los usuarios ver las políticas integradas y administradas asociadas a su identidad de usuario. Esta política incluye permisos para completar esta acción en la consola o mediante programación mediante la tecla o. AWS CLI AWS API

```
{
    "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 concede a los IAM usuarios 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 EC2 operaciones de Amazon es necesario para que Amazon WorkDocs pueda obtener una lista de tus subredes VPCs y tus subredes. El acceso a la AWS Directory Service `DescribeDirectories` operación es necesario para obtener información sobre sus AWS Directory Service directorios.

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

Más ejemplos de políticas WorkDocs basadas en la identidad de Amazon

IAMlos administradores pueden crear políticas adicionales para permitir que un IAM rol o un usuario accedan a Amazon WorkDocs API. 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

Usa la siguiente información para ayudarte a diagnosticar y solucionar problemas comunes que puedas encontrar al trabajar con Amazon WorkDocs yIAM.

Temas

- No estoy autorizado a realizar ninguna acción en Amazon WorkDocs
- No estoy autorizado a realizar lo siguiente: PassRole

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

No estoy autorizado a realizar ninguna acción en Amazon WorkDocs

Si AWS Management Console te indica que no estás autorizado a realizar una acción, debes ponerte en contacto con tu administrador para obtener ayuda. Su administrador es la persona que le facilitó su nombre de usuario y contraseña.

No estoy autorizado a realizar lo siguiente: 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 una función a Amazon WorkDocs.

Algunas te Servicios de AWS permiten transferir una función existente a ese servicio en lugar de crear una nueva función de servicio o una función vinculada al servicio. Para ello, debe tener permisos para transferir el rol al servicio.

El siguiente ejemplo de error se produce cuando un IAM usuario llamado `marymajor` intenta usar la consola para realizar una acción en Amazon WorkDocs. Sin embargo, la acción requiere que el servicio cuente con permisos que otorguen 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 necesitas ayuda, ponte en contacto con tu AWS administrador. 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 admiten políticas basadas en recursos o listas de control de acceso (ACLs), puedes usar esas políticas para permitir que las personas accedan a tus recursos.

Para más información, consulte lo siguiente:

- Para saber si Amazon WorkDocs admite estas funciones, consultaCómo WorkDocs trabaja Amazon con IAM.
- Para obtener más información sobre cómo proporcionar acceso a los recursos de tu propiedad, consulta Cómo proporcionar acceso a un IAM usuario en otro Cuenta de AWS de tu propiedad en la Guía del IAM usuario. Cuentas de AWS
- Para obtener información sobre cómo proporcionar acceso a tus recursos a terceros Cuentas de AWS, consulta Cómo permitir el acceso a recursos que Cuentas de AWS son propiedad de terceros en la Guía del IAM usuario.
- Para obtener información sobre cómo proporcionar acceso mediante la federación de identidades, consulte Proporcionar acceso a usuarios autenticados externamente (federación de identidades) en la Guía del IAM usuario.
- Para saber la diferencia entre el uso de roles y políticas basadas en recursos para el acceso entre cuentas, consulte el acceso a recursos entre cuentas IAM en la Guía del usuario. IAM

Registro y supervisión en Amazon WorkDocs

Los administradores WorkDocs del sitio de Amazon pueden ver y exportar el feed de actividades de un sitio completo. 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
- Uso AWS CloudTrail para registrar WorkDocs API llamadas de Amazon

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 debes 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, elija Actividad.

2. Elija Filtrar y, a continuación, mueva el control deslizante 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 tu PC
   - macOS: `/users/`**`username`**`/WorkDocsDownloads/folder`

   En el archivo exportado se refleja cualquier filtro que haya aplicado.

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

Uso AWS CloudTrail para registrar WorkDocs API llamadas de Amazon

Puedes usar AWS CloudTrail; para registrar las WorkDocs API llamadas de Amazon. CloudTrail proporciona un registro de las acciones realizadas por un usuario, un rol o un AWS servicio en Amazon WorkDocs. CloudTrail captura todas las API llamadas de Amazon WorkDocs como eventos, incluidas las llamadas desde la WorkDocs consola de Amazon y las llamadas en código a Amazon WorkDocs APIs.

Si crea una ruta, puede habilitar la entrega continua de CloudTrail eventos a un bucket de Amazon S3, incluidos los eventos de Amazon WorkDocs. Si no crea una ruta, podrá ver los eventos más recientes en la CloudTrail consola, en el historial de eventos.

La información recopilada 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 al respecto CloudTrail, consulte la Guía AWS CloudTrail del usuario.

WorkDocs Información de Amazon en CloudTrail

CloudTrail está habilitada en tu AWS cuenta al crearla. Cuando se produce una actividad en Amazon WorkDocs, esa actividad se registra en un CloudTrail evento junto con otros eventos de AWS servicio en el historial de eventos. Puedes ver, buscar y descargar los eventos recientes en tu AWS cuenta. Para obtener más información, consulta Cómo ver eventos con el historial de CloudTrail eventos.

Para tener un registro continuo de los eventos de tu AWS cuenta, incluidos los eventos de Amazon WorkDocs, crea una ruta. Un rastro 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. La ruta registra los eventos de todas las regiones de la AWS partición y entrega los archivos de registro al bucket de Amazon S3 que especifique. Además, puede configurar otros AWS servicios para analizar más a fondo los datos de eventos recopilados en los CloudTrail registros y actuar en función de ellos. Para obtener más información, consulte:

- Introducción a la creación de registros de seguimiento
- CloudTrail servicios e integraciones compatibles
- Configuración de SNS las notificaciones de Amazon para CloudTrail
- Recibir archivos de CloudTrail registro de varias regiones y recibir archivos de CloudTrail registro de varias cuentas

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

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

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

Para obtener más información, consulte el CloudTrail userIdentityelemento.

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

Un rastro es una configuración que permite la entrega de eventos como archivos de registro a un bucket de Amazon S3 que usted especifique. CloudTrail Los archivos de registro contienen una o más entradas de registro. Un evento representa una solicitud única de cualquier fuente e incluye información sobre la acción solicitada, la fecha y la hora de la acción, los parámetros de la solicitud, etc. CloudTrail Los archivos de registro no son un registro ordenado de las API llamadas 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 ambas es que la identidad del usuario para las entradas del plano de control es un IAM usuario. 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 IAM usuarios 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_ _ en los registrosSECURITY. REASONS CloudTrail

El siguiente ejemplo muestra dos entradas de CloudTrail registro para Amazon WorkDocs: 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 programa de cumplimiento Servicio de AWS está dentro del ámbito de aplicación de programas de cumplimiento específicos, consulte Servicios de AWS Alcance por programa de de cumplimiento y elija el programa de cumplimiento que le interese. Para obtener información general, consulte Programas de AWS cumplimiento > Programas AWS .

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

Su responsabilidad de cumplimiento al Servicios de AWS utilizarlos viene determinada por la confidencialidad de sus datos, los objetivos de cumplimiento de su empresa y las leyes y reglamentos aplicables. AWS proporciona los siguientes recursos para ayudar con el cumplimiento:

- Guías de inicio rápido sobre seguridad y cumplimiento: estas guías de implementación analizan las consideraciones arquitectónicas y proporcionan los pasos para implementar entornos básicos centrados en AWS la seguridad y el cumplimiento.
- Diseñando una arquitectura basada en la HIPAA seguridad y el cumplimiento en Amazon Web Services: en este documento técnico se describe cómo pueden utilizar las empresas AWS para crear HIPAA aplicaciones aptas.

  > **Note**
  >
  > No todos son aptos. Servicios de AWS HIPAA Para obtener más información, consulta la Referencia de servicios HIPAA aptos.

- AWS Recursos de de cumplimiento: esta colección de libros de trabajo y guías puede aplicarse a su industria y ubicación.
- AWS Guías de cumplimiento para clientes: comprenda el modelo de responsabilidad compartida desde la perspectiva del cumplimiento. En las guías se resumen las mejores prácticas para garantizar la seguridad Servicios de AWS y se orientan a los controles de seguridad en varios marcos (incluidos el Instituto Nacional de Estándares y Tecnología (NIST), el Consejo de Normas de Seguridad del Sector de Tarjetas de Pago (PCI) y la Organización Internacional de Normalización (ISO)).
- Evaluación de los recursos con reglas en la guía para AWS Config desarrolladores: el AWS Config servicio evalúa en qué medida las configuraciones de los recursos cumplen con las prácticas internas, las directrices del sector y las normas.

- AWS Security Hub— Esto Servicio de AWS proporciona una visión completa del estado de su seguridad interior 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.
- Amazon GuardDuty: Servicio de AWS detecta posibles amenazas para sus cargas de trabajo Cuentas de AWS, contenedores y datos mediante la supervisión de su entorno para detectar actividades sospechosas y maliciosas. GuardDuty puede ayudarlo a cumplir con varios requisitos de conformidad, por ejemplo PCIDSS, cumpliendo con los requisitos de detección de intrusiones exigidos por ciertos marcos de cumplimiento.
- AWS Audit Manager— Esto le Servicio de AWS ayuda a auditar continuamente su AWS consumo para simplificar la gestión del riesgo y el cumplimiento de las normativas y los estándares del sector.

Resiliencia en Amazon WorkDocs

La infraestructura AWS global se basa en AWS regiones y zonas de disponibilidad. AWS Las regiones proporcionan varias zonas de disponibilidad aisladas y separadas físicamente, que están conectadas mediante redes de baja latencia, alto rendimiento y alta redundancia. 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 AWS las regiones y las zonas de disponibilidad, consulte Infraestructura global.AWS

Seguridad de infraestructuras 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 Seguridad de la infraestructura en AWS Identity and Access Management en la Guía del IAM usuario y Prácticas recomendadas para la seguridad, la identidad y el cumplimiento en el Centro de AWS arquitectura.

Utilizas API las llamadas AWS publicadas para acceder a Amazon WorkDocs a través de la red. Los clientes deben ser compatibles con Transport Layer Security (TLS) 1.2 y recomendamos

usar la versión TLS 1.3. Los clientes también deben ser compatibles con conjuntos de cifrado con confidencialidad directa total, tales 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 firmarse con un identificador de clave de acceso y una clave de acceso secreta asociada a una entidad IAM principal. También puede utilizar AWS Security Token Service (AWS STS) para generar credenciales de seguridad temporales para firmar solicitudes.

Introducción a Amazon WorkDocs

Amazon WorkDocs utiliza un directorio para almacenar y administrar la información de la organización de los usuarios y sus documentos. Por su parte, usted asocia un directorio a un sitio al aprovisionar ese sitio. Al hacerlo, una característica de Amazon WorkDocs denominada Activación automática añade a los usuarios del directorio del sitio como usuarios administrados, lo que significa que no necesitan credenciales independientes para iniciar sesión en el sitio y pueden compartir archivos y colaborar en ellos. Cada usuario dispone de 1 TB de almacenamiento, a menos que compre más.

Ya no necesita agregar y activar usuarios manualmente, aunque sí puede hacerlo. También puede cambiar los roles y permisos de los usuarios siempre que lo necesite. Para obtener más información al respecto, consulte Invitación y administración de usuarios de Amazon WorkDocs en esta guía.

Si necesita crear directorios, puede hacer lo siguiente:

- Cree un directorio de AD sencillo.
- Cree un directorio de AD Connector para conectarse a su directorio local.
- Permita que Amazon WorkDocs funcione con un directorio de AWS 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 forma pertenece un programa de conformidad, como PCI, FedRAMP o DoD, debe configurar un directorio de AWS Managed Microsoft AD para cumplir los requisitos de conformidad. En los pasos de esta sección se explica cómo usar un directorio de Microsoft AD existente. Para obtener información sobre la creación de un directorio de Microsoft AD, consulte AWS Managed Microsoft AD en la Guía de administración de AWS Directory Service.

Contenido

- Habilitación del inicio de sesión único
- Habilitar la autenticación multifactor
- Promover un usuario a administrador

Creación de un sitio de Amazon WorkDocs

En los pasos de las siguientes secciones se explica cómo configurar un nuevo sitio de Amazon WorkDocs.

Tareas

- Antes de empezar
- Creación de un sitio de Amazon WorkDocs

Antes de empezar

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

- Una cuenta de AWS para crear y administrar sitios de Amazon WorkDocs. No obstante, los usuarios no necesitan una cuenta de AWS para conectarse a Amazon WorkDocs y utilizarlo. Para obtener más información, consulte Requisitos previos para Amazon WorkDocs.
- Si planea usar Simple AD, debe cumplir los requisitos previos identificados en los Requisitos previos de Simple AD de la Guía de administración de AWS Directory Service.
- Un directorio de AWS Managed Microsoft AD si pertenece a un programa de cumplimiento como PCI, FedRAMP o DoD. En los pasos de esta sección se explica cómo usar un directorio de Microsoft AD existente. Para obtener información sobre la creación de un directorio de Microsoft AD, consulte AWS Managed Microsoft AD en la Guía de administración de AWS Directory Service.
- La información del perfil del administrador, incluido el nombre y los apellidos y una dirección de correo electrónico.

Creación de un sitio de Amazon WorkDocs

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

Para crear el sitio Amazon WorkDocs

1. Abra la consola Amazon WorkDocs en https://console.aws.amazon.com/zocalo/.

2. En la página de inicio de la consola, en Crear un sitio de WorkDocs, elija Comience ahora.

   -O BIEN-

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

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

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

   En los pasos siguientes se explica cómo hacer ambas tareas.

   Para usar un directorio existente

   1. Abra la lista Directorios disponibles y elija el directorio que quiera usar.
   2. Elija Habilitar directorio.

   Para crear un directorio

   1. Repita los pasos 1 y 2 anteriores.

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

      Para utilizar Simple AD

      a. Seleccione Simple AD y, a continuación, Siguiente.

         Aparecerá la página Crear sitio de Simple AD.

      b. En Punto de acceso, en el cuadro URL del sitio, introduzca la URL del sitio.
      c. En Configurar administrador de WorkDocs, introduzca la dirección de correo electrónico, el nombre y los apellidos del administrador.

d. Según sea necesario, complete las opciones de Detalles del directorio y Configuración de VPC.

e. Elija Crear sitio de Simple AD.

Para crear un directorio de AD Connector

a. Seleccione AD Connector y, a continuación, elija Siguiente.

Aparecerá la página Crear sitio de AD Connector.

b. Complete todos los campos de la sección Detalles del directorio.

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

d. Si lo desea, complete los campos opcionales en Configuración de VPC.

e. Elija Crear sitio de AD Connector.

Amazon WorkDocs hace lo siguiente:

- Si ha elegido Configurar una VPC en mi nombre en el paso 4 anterior, Amazon WorkDocs creará una VPC para usted. Un directorio de la VPC almacenará la información del usuario y del sitio de Amazon WorkDocs.
- Si ha utilizado Simple AD, Amazon WorkDocs creará un usuario de directorio y lo establecerá como administrador de Amazon WorkDocs. Si ha creado un directorio AD Connector, Amazon WorkDocs establecerá el usuario de directorio existente que ha proporcionado como administrador de WorkDocs.
- Si ha utilizado un directorio existente, Amazon WorkDocs le pedirá que introduzca el nombre de usuario del administrador de Amazon WorkDocs. El usuario debe ser miembro del directorio.

> **Note**
>
> Amazon WorkDocs no notifica a los usuarios sobre el nuevo sitio. Debe comunicarles la URL y comunicarlos que no necesitan credenciales distintas para usar el sitio.

Habilitación del inicio de sesión único

AWS Directory Service permite a los usuarios tener acceso a Amazon WorkDocs desde un equipo que se haya unido al mismo directorio en el que esté registrado Amazon WorkDocs, sin tener que escribir sus credenciales por separado. Los administradores de Amazon WorkDocs pueden habilitar el inicio de sesión único mediante la consola AWS Directory Service. Para obtener más información, consulte Inicio de sesión único en la Guía de administración deAWS Directory Service.

Después de que el administrador de Amazon WorkDocs habilite el inicio de sesión único, es posible que los usuarios del sitio de Amazon WorkDocs 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 de administración de AWS Directory Service.

Habilitar la autenticación multifactor

Utilice la consola AWS Directory Services en https://console.aws.amazon.com/directoryservicev2/ para habilitar la autenticación multifactor en el directorio de AD Connector. Para habilitar la MFA, debe tener una solución de MFA compuesta por un servidor Remote Authentication Dial-In User Service (RADIUS), o disponer de un complemento de MFA para un servidor RADIUS que ya tenga implementado en su infraestructura en las instalaciones. 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 en el sector que proporciona administración de autenticación, autorización y contabilidad para que los usuarios puedan conectarse a servicios de red. AWS Managed Microsoft AD incluye un cliente RADIUS que se conecta al servidor RADIUS sobre el que se ha implementado su solución de MFA. El servidor RADIUS valida el nombre de usuario y el código de OTP. Si el servidor RADIUS valida correctamente al usuario, AWS Managed Microsoft AD autentica al usuario en 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 AWS Managed Microsoft AD y el servidor RADIUS requiere la configuración de grupos de seguridad de AWS que permiten 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 de AWS Directory Service.

> **Note**
>
> La autenticación multifactor no puede utilizarse con los directorios de Simple AD.

Promover un usuario a administrador

Utilice la consola Amazon WorkDocs para promocionar a un usuario a administrador. Siga estos pasos.

Para promocionar un usuario a administrador

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

   Aparecerá la página Administrar sitios de WorkDocs.
3. Seleccione el botón situado junto al sitio que quiera, elija Acciones y, a continuación, elija Configurar un administrador.

   Aparecerá el cuadro de diálogo Establecer administrador de WorkDocs.
4. En el cuadro Nombre de usuario, introduzca el nombre de usuario de la persona a la que quiera promocionar y, a continuación, seleccione Establecer administrador.

También puede usar el panel de control de administración del sitio Amazon WorkDocs para degradar a un administrador. Para obtener más información, consulte Editar usuarios.

Administración de Amazon WorkDocs desde la consola AWS

Puede utilizar estas herramientas para administrar sus sitios de Amazon WorkDocs:

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

Cada una de estas herramientas proporciona un conjunto diferente de acciones, y en los temas de esta sección se explican las acciones que proporciona la consola AWS. Para obtener información sobre el panel de control del administrador del sitio, consulte Administrar Amazon WorkDocs desde el panel de control del administrador del sitio.

Configuración de los administradores del sitio

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

Para establecer un administrador

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

   Aparecerá la página Administrar sitios de WorkDocs, donde se muestra una lista de sus sitios.
3. Elija el botón situado junto al sitio para el que desea configurar un administrador.
4. Abra la lista Acciones y seleccione Establecer un administrador.

   Aparecerá el cuadro de diálogo Establecer administrador de WorkDocs.
5. En el cuadro Nombre de usuario, introduzca el nombre del nuevo administrador y, a continuación, seleccione Establecer administrador.

Reenvío de los correos electrónicos de invitación

Puede reenviar los correos electrónicos de invitación en cualquier momento.

Para reenviar el correo electrónico de invitación

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

   Aparecerá la página Administrar sitios de WorkDocs, donde se muestra una lista de sus sitios.
3. Elija el botón situado junto al sitio para el que desea reenviar correo electrónico.
4. Abra la lista Acciones y elija Reenviar correo electrónico de invitación.

   Aparecerá un mensaje de envío correcto en un banner verde en la parte superior de la página.

Administración de la autenticación multifactor

Puede activar la autenticación multifactor después de crear un sitio de Amazon WorkDocs. Para obtener más información acerca de la autenticación, consulte Habilitar la autenticación multifactor.

Configuración de las direcciones URL de los sitios

> **Note**
>
> Si ha seguido el proceso de creación del sitio que se indican en Introducción a Amazon WorkDocs, ha introducido la URL de un sitio. Como resultado, Amazon WorkDocs hace que el comando Configurar URL del sitio no esté disponible, ya que solo se puede configurar una URL una vez. Solo debe seguir estos pasos si implementa Amazon WorkSpaces y lo integra con Amazon WorkDocs. El proceso de integración de Amazon WorkSpaces requiere que introduzca un número de serie en lugar de la URL de un sitio, por lo que debe introducir la 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 usuario de Amazon WorkSpaces.

Para configurar la URL de un sitio

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

   Aparecerá la página Administrar sitios de WorkDocs, donde se muestra una lista de sus sitios.

3. Seleccione el sitio que ha integrado con Amazon WorkSpaces. La URL contiene el ID de directorio de su instancia de Amazon WorkSpaces, como https://{directory_id}.awsapps.com.
4. Elija el botón situado junto a esa URL, abra la lista Acciones y elija Configurar URL del sitio.

   Aparecerá el cuadro de diálogo Configurar URL del sitio.
5. En el cuadro URL del sitio, introduzca la URL del sitio y, a continuación, seleccione Configurar URL del sitio.
6. En la página Administrar sitios de WorkDocs, elija Actualizar para ver la nueva URL.

Administración de 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 API CreateNotificationSubscription, que puede usar para configurar su propio punto de conexión para procesar los mensajes de SNS que envía WorkDocs. Para obtener más información sobre las notificaciones, consulte Configuración de notificaciones para un usuario o rol de IAM en la Guía para desarrolladores de Amazon WorkDocs.

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

Para crear una notificación

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

   Aparecerá la página Administrar sitios de WorkDocs, donde se muestra una lista de sus sitios.
3. Elija el botón situado al lado del sitio en cuestión.
4. Abra la lista Acciones y seleccione Administrar notificaciones.

   Aparecerá el cuadro de diálogo Establecer administrador de WorkDocs.

5. En el cuadro Nombre de usuario, introduzca el nombre del nuevo administrador y, a continuación, seleccione Establecer administrador.

Para eliminar una notificación

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

   Aparecerá la página Administrar sitios de WorkDocs, donde se muestra una lista de sus sitios.
3. Elija el botón situado junto al sitio para el que desea configurar un administrador.
4. Abra la lista Acciones y seleccione Establecer un administrador.

   Aparecerá el cuadro de diálogo Establecer administrador de WorkDocs.
5. En el cuadro Nombre de usuario, introduzca el nombre del nuevo administrador y, a continuación, seleccione Establecer administrador.

Eliminación de un sitio

Utilice la consola Amazon WorkDocs para eliminar un sitio.

> **Warning**
>
> Si se elimina un sitio, se perderán todos los archivos. Solo debe eliminar un sitio si está absolutamente seguro de que esta información ya no es necesaria.

Para eliminar un sitio

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

   Aparecerá la página Administrar sitios de WorkDocs.
3. Elija el botón situado junto al sitio que quiera eliminar y, luego, seleccione Eliminar.

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

> **Important**
>
> Si no proporciona su propio directorio para Amazon WorkDocs, creamos uno para usted. Cuando elimine el sitio de Amazon WorkDocs, se le aplicará un cargo por el directorio que creemos a menos que lo elimine o lo use para otra aplicación de AWS. Para obtener información sobre precios, consulte Precios de AWS Directory Service.

5. En el cuadro URL del sitio, introduzca la URL del sitio y, a continuación, seleccione Eliminar.

   El sitio se elimina inmediatamente y deja de estar disponible.

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

Utilizas estas herramientas para gestionar tus WorkDocs sitios de Amazon:

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

Cada una de estas herramientas ofrece un conjunto diferente de acciones. Los temas de esta sección explican las acciones que proporciona el panel de control del administrador del sitio. Para obtener información acerca de las tareas disponibles en la consola, consulte Administración de Amazon WorkDocs desde la consola AWS.

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.

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. Seleccione 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.

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. Puedes añadir hasta 500 configuraciones de listas 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 admite la inclusión en listas de direcciones IP denegadas.

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. En Escribir valor de CIDR, introduzca el bloque Enrutamiento entre dominios sin clases (Classless inter-domain routing, CIDR) para los intervalos de direcciones IP, y escoja Añadir.
   - Para permitir el acceso a una sola dirección IP, especifique `/32` como el prefijo de CIDR.
4. Seleccione 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: sitios simples ActiveDirectory

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

Para usar la configuración de seguridad

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

2. En Administrador, elija Abrir panel de control del administrador.
3. Desplácese hacia abajo hasta Seguridad y seleccione Cambiar.

   Aparecerá el cuadro de diálogo Configuración de políticas. La siguiente tabla muestra la configuración de seguridad de los sitios simples ActiveDirectory .

Opción	Descripción
En Elija la configuración de enlaces compartibles, seleccione una de las siguientes opciones:	
No permitir enlaces que se puedan compartir en todo el sitio o públicos	Deshabilita el uso compartido de enlaces para todos los usuarios.
Permitir que los usuarios creen enlaces que se puedan compartir en todo el sitio, pero no permitirles crear enlaces públicos que se puedan compartir	Limita el uso compartido de enlaces solo a los miembros del sitio. Los usuarios administrados pueden crear este tipo de enlace.

Opción	Descripción
Permitir a los usuarios crear enlaces que se puedan compartir en todo el sitio, pero solo los usuarios avanzados pueden crear enlaces públicos que se puedan compartir	Los usuarios administrados 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 administrados pueden crear enlaces públicos y que se puedan compartir en todo el sitio	Los usuarios administrados pueden crear enlaces públicos.

En Activación automática, seleccione o desmarque 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 la primera vez que inician sesión en su sitio.

En Quién debería poder invitar a nuevos usuarios a su WorkDocs sitio, seleccione 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 usuarios nuevos desde cualquier lugar compartiendo archivos o carpetas con ellas.	Permite a los usuarios invitar a nuevos usuarios compartiendo archivos o carpetas con esos usuarios.
Los usuarios pueden invitar a usuarios nuevos de unos cuantos 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, seleccione o anule la selección de la casilla de verificación.

Opción	Descripción
Los usuarios nuevos de su directorio serán usuarios administrados (de manera predeterminada, son usuarios invitados)	Convierte automáticamente a los nuevos usuarios de su directorio en usuarios administrados.

4. Cuando haya finalizado, elija Guardar cambios.

Seguridad: sitios de ActiveDirectory conexión

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

Para usar la configuración de seguridad

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

2. En Administrador, elija Abrir panel de control del administrador.
3. Desplácese hacia abajo hasta Seguridad y seleccione Cambiar.

   Aparecerá el cuadro de diálogo Configuración de políticas. En la siguiente tabla se enumeran y describen las configuraciones de seguridad de los sitios de ActiveDirectory conexión.

Opción	Descripción
En Elija la configuración de enlaces compartibles, seleccione una de las siguientes opciones:	
No permitir enlaces que se puedan compartir en todo el sitio o públicos	Cuando se selecciona, deshabilita el uso compartido de enlaces para todos los usuarios.
Permitir que los usuarios creen enlaces que se puedan compartir en todo el sitio, pero no permitirles crear enlaces públicos que se puedan compartir	Limita el uso compartido de enlaces solo a los miembros del sitio. Los usuarios administr ados pueden crear este tipo de enlace.

Opción	Descripción
Permitir a los usuarios crear enlaces que se puedan compartir en todo el sitio, pero solo los usuarios avanzados pueden crear enlaces públicos que se puedan compartir	Los usuarios administrados 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 administrados pueden crear enlaces públicos y que se puedan compartir en todo el sitio	Los usuarios administrados pueden crear enlaces públicos.

En Activación automática, seleccione o desmarque 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 la primera vez que inician sesión en su sitio.

En ¿Quién debería poder activar los usuarios del directorio en su WorkDocs sitio? , seleccion e una de las siguientes opciones:

Solo los administradores pueden activar a nuevos usuarios desde su directorio.	Permita que solo los administradores activen a nuevos usuarios del directorio.
Los usuarios pueden activar a nuevos usuarios del directorio compartiendo archivos o carpetas con ellos.	Permite a los usuarios activar a usuarios del directorio compartiendo archivos o carpetas con los usuarios del directorio.
Los usuarios pueden activar a usuarios nuevos de unos cuantos dominios específic os compartiendo archivos o carpetas con ellos.	Los usuarios solo pueden compartir archivos o carpetas de usuarios de dominios específic os. Al elegir esta opción, debe ingresar los dominios.

En ¿Quién debería poder invitar a nuevos usuarios a su WorkDocs sitio? , selecciona una de las siguientes opciones:

Opción	Descripción
Compartir con usuarios externos **Note** Las siguientes opciones solo aparecen después de seleccionar esta configuración.	Enables administrators and users to invite new external users to your Amazon WorkDocs site.
Solo los administradores pueden invitar a usuarios externos	Solo los administradores pueden invitar a usuarios externos.
Todos los usuarios administrados pueden invitar a nuevos usuarios	Permite a los usuarios administrados invitar a usuarios externos.
Solo los usuarios avanzados pueden invitar a usuarios externos nuevos.	Permite solo a los usuarios avanzados invitar a usuarios externos nuevos.
En Configurar rol para nuevos usuarios, seleccione una o ambas opciones.	
Los usuarios nuevos de su directorio serán usuarios administrados (de manera predeterminada, son usuarios invitados)	Convierte automáticamente a los nuevos usuarios de su directorio en usuarios administrados.
Los usuarios nuevos externos serán usuarios administrados (de manera predeterminada, son usuarios invitados)	Convierte automáticamente los usuarios externos nuevos en usuarios administrados.

4. Cuando haya finalizado, elija Guardar cambios.

Retención de la papelera de recuperación

Cuando un usuario elimina un archivo, Amazon lo WorkDocs guarda en la papelera de reciclaje del usuario durante 30 días. Posteriormente, Amazon WorkDocs mueve los archivos a un contenedor de recuperación temporal durante 60 días y, a continuación, los elimina permanentemente. Solo los administradores pueden ver la papelera de recuperación temporal. Mediante un cambio en la política

de retención de datos de todo el sitio, los administradores del sitio pueden cambiar el periodo de retención de la papelera de recuperación hasta un mínimo de 0 días y un máximo de 365 días.

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 que deben conservarse los archivos en la papelera de recuperación y elija Guardar.

> **Note**
>
> El periodo de retención predeterminado es de 60 días. Puede utilizar un periodo de 0 a 365 días.

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

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 Invitación y administración de usuarios de Amazon WorkDocs.

Implementación de Amazon WorkDocs Drive en varios ordenadores

Si tiene una flota de equipo unida a un dominio, puede usar Group Policy Objects (GPO) o System Center Configuration Manager (SCCM) para instalar el cliente de Amazon WorkDocs Drive. Puede descargar el cliente de https://amazonworkdocs.com/en/clients.

Mientras lo hace, 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 cumplan los requisitos de instalación de Amazon WorkDocs Drive. Para obtener más información, consulte Instalación de Amazon WorkDocs Drive en la Guía del usuario de Amazon WorkDocs.

> **Note**
>
> Como práctica recomendada al usar GPO o SCCM, instale el cliente de Amazon WorkDocs Drive después de que los usuarios hayan iniciado sesión.

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

- **`SITEID`**: rellena previamente la información del sitio de Amazon WorkDocs para los usuarios durante el registro. Por ejemplo, `SITEID=`*`site-name`*.
- **`DefaultDriveLetter`**: rellena 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 su letra, 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=your_drive_letter REBOOT=REALLYSUPPRESS /norestart /qn
```

Invitación y administración de usuarios de Amazon WorkDocs

De forma predeterminada, al adjuntar un directorio durante la creación del sitio, la característica de activación automática de Amazon WorkDocs añade a todos los usuarios de ese directorio al nuevo sitio como usuarios administrados.

En WorkDocs, los usuarios administrados no necesitan iniciar sesión con credenciales distintas. Pueden compartir archivos y colaborar en ellos, y disponen automáticamente de 1 TB de almacenamiento. Sin embargo, puede desactivar la activación automática cuando solo quiera añadir a algunos de los usuarios de un directorio, y en los pasos que encontrará en las siguientes secciones se explica cómo hacerlo.

Además, puede invitar a usuarios y habilitarlos o deshabilitarlos, así como cambiar los roles y la configuración de los usuarios. También puede promocionar un usuario a administrador. Para obtener más información sobre cómo promocionar a usuarios, consulte Promover un usuario a administrador.

Estas tareas se realizan en el panel de control de administración del cliente web de Amazon WorkDocs y en los pasos de las siguientes secciones se explica cómo hacerlo. Sin embargo, si es la primera vez que utiliza Amazon WorkDocs, dedique unos minutos a conocer los distintos roles de usuario antes de sumergirse en las tareas administrativas.

Contenido

Información general sobre las funciones de usuario

Amazon WorkDocs define los siguientes roles de usuario. Puede modificar los roles de los usuarios editando sus perfiles. Para obtener más información, consulte Editar usuarios.

- 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.
- Usuario avanzado: usuario de pago a quien el administrador le ha concedido un conjunto especial de permisos. Para obtener más información sobre cómo configurar permisos para un usuario avanzado, consulte Seguridad: sitios simples ActiveDirectory y Seguridad: sitios de ActiveDirectory conexión.
- Usuario: usuario de pago que puede guardar archivos y colaborar con otras personas en un sitio de Amazon WorkDocs.
- Usuario invitado: usuario gratuito que solo puede ver archivos. Puede actualizar a los usuarios invitados con los roles de Usuario, Usuario avanzado o Administrador.

> **Note**
>
> Cuando cambia el rol de un usuario invitado, realiza una acción puntual que no puede revertir.

Amazon WorkDocs también define estos tipos de usuarios adicionales.

Usuario de WS

Un usuario con un espacio de trabajo de WorkSpaces asignado.

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

Usuario de WS actualizado

Un usuario con un espacio de trabajo de WorkSpaces asignado y almacenamiento actualizado.

- Acceso a todas las características de Amazon WorkDocs

- Almacenamiento predeterminado de 1 TB (almacenamiento adicional disponible en pago por uso)
- Se aplican cargos mensuales

Usuario de Amazon WorkDocs

Un usuario activo de Amazon WorkDocs sin un espacio de trabajo de WorkSpace asignado.

- Acceso a todas las características de Amazon WorkDocs
- Almacenamiento predeterminado de 1 TB (almacenamiento adicional disponible en pago por uso)
- Se aplican cargos mensuales

Iniciar el panel de control de administración

Utilice el panel de control administrativo del cliente web de Amazon WorkDocs para activar y desactivar la activación automática, y cambiar los roles y la configuración de los usuarios.

Para abrir el panel de control de administración

1. Elija el icono de perfil situado en la esquina superior derecha del cliente de WorkDocs.

2. En Administrador, elija Abrir panel de control del administrador.

> **Note**
>
> Algunas opciones del panel de control son diferentes en los directorios de la nube y los directorios conectados.

Desactivación de la activación automática

Puede desactivar la activación automática cuando no quiera añadir a todos los usuarios de un directorio a un sitio nuevo y cuando quiera establecer permisos y roles diferentes para los usuarios que invite a un sitio nuevo. Al desactivar la activación automática, también puede decidir quién puede

invitar a usuarios nuevos al sitio: usuarios actuales, usuarios avanzados o administradores. En estos pasos se explica cómo realizar ambas tareas.

Para desactivar la activación automática

1. Elija el icono de perfil situado en la esquina superior derecha del cliente de WorkDocs.

2. En Administrador, elija Abrir panel de control del administrador.
3. Desplácese hacia abajo hasta Seguridad y seleccione Cambiar.

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

   Las opciones cambian en Quién debería poder activar a los usuarios del directorio en su sitio de WorkDocs. Puede permitir que los usuarios actuales inviten a usuarios nuevos o puede dar esa posibilidad a usuarios avanzados u otros administradores.
5. Seleccione una opción y, a continuación, seleccione Guardar cambios.

Repita los pasos del 1 al 4 para volver a activar la activación automática.

Administración del uso compartido de enlaces

En este tema se explica cómo administrar el uso compartido de enlaces. Los usuarios de Amazon WorkDocs pueden compartir sus archivos o carpetas mediante enlaces. Pueden compartir enlaces a archivos dentro y fuera de su organización, pero solo pueden compartir los enlaces a carpetas de forma interna. Como administrador, usted administra quién puede compartir enlaces.

Para habilitar el uso compartido de enlaces

1. Elija el icono de perfil situado en la esquina superior derecha del cliente de WorkDocs.

2. En Administrador, elija Abrir panel de control del administrador.
3. Desplácese hacia abajo hasta Seguridad y seleccione Cambiar.

   Aparecerá el cuadro de diálogo Configuración de políticas.
4. En Elija la configuración de enlaces compartibles, seleccione una opción:

   - No permitir enlaces que se puedan compartir en todo el sitio o públicos: deshabilita el uso compartido de enlaces para todos los usuarios.
   - Permitir que los usuarios creen enlaces que se puedan compartir en todo el sitio, pero no permitirles crear enlaces públicos que se puedan compartir: limita el uso compartido de enlaces solo a los miembros del sitio. Los usuarios administrados pueden crear este tipo de enlace.
   - Permitir a los usuarios crear enlaces que se puedan compartir en todo el sitio, pero solo los usuarios avanzados pueden crear enlaces públicos que se puedan compartir: los usuarios administrados pueden crear enlaces en 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 administrados pueden crear enlaces públicos y que se puedan compartir en todo el sitio: los usuarios administrados pueden crear enlaces públicos.
5. Elija Guardar cambios.

Controlar las invitaciones de los usuarios con la activación automática habilitada

Si habilita la activación automática (recuerde que está activada de forma predeterminada), puede ofrecer a los usuarios la posibilidad de invitar a otros usuarios. Puede conceder permiso a cualquiera de las siguientes opciones.

- Todos los usuarios
- Usuarios avanzados
- Administradores

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

Para configurar los permisos de invitación

1. Elija el icono de perfil situado en la esquina superior derecha del cliente de WorkDocs.

2. En Administrador, elija Abrir panel de control del administrador.
3. Desplácese hacia abajo hasta Seguridad y seleccione Cambiar.

   Aparecerá el cuadro de diálogo Configuración de políticas.
4. En Quién debería poder activar a los usuarios del directorio en su sitio de WorkDocs, active la casilla Compartir con usuarios externos, seleccione una de las opciones situadas debajo de la casilla de verificación y, a continuación, seleccione Guardar cambios.

   -O BIEN-

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

Invitar a usuarios nuevos

Puede invitar a usuarios nuevos a unirse a un directorio. También puede habilitar a los usuarios existentes para invitar a nuevos usuarios. Para obtener más información, consulte Seguridad: sitios simples ActiveDirectory y Seguridad: sitios de ActiveDirectory conexión en esta guía.

Para invitar a usuarios nuevos

1. Elija el icono de perfil situado en la esquina superior derecha del cliente de WorkDocs.

2. En Administrador, elija Abrir panel de control del administrador.
3. En Manage users (Administrar usuarios), elija Invite users (Invitar usuarios).
4. En el cuadro de diálogo Invitar a usuarios, para la opción A quién le gustaría invitar, ingrese la dirección de correo electrónico del invitado y haga clic en 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 cuenta de Amazon WorkDocs. 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. Elija el icono de perfil situado en la esquina superior derecha del cliente de WorkDocs.

2. En Administrador, elija Abrir panel de control del administrador.
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.

   Rol

   Especifica si alguien es usuario o administrador. También puede cambiar el tipo de usuario para alguien que tenga asignado un espacio de trabajo de WorkSpaces. Para obtener más información, consulte Información general sobre las funciones de usuario.

   Almacenamiento

   Especifica el límite de almacenamiento de un usuario existente.

5. Elija Guardar cambios.

Deshabilitación de usuarios

Puede deshabilitar el acceso de un usuario cambiando su estado a Inactivo.

Para cambiar el estado del usuario a Inactivo

1. Elija el icono de perfil situado en la esquina superior derecha del cliente de WorkDocs.

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

El usuario inactivado no puede acceder a su sitio de Amazon WorkDocs.

> **Note**
>
> El cambio de un usuario al estado Inactivo no elimina sus archivos, carpetas ni comentarios del sitio de Amazon WorkDocs. 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.

Eliminación de usuarios pendientes

Puede eliminar a los usuarios de Simple AD, AWS Managed Microsoft y AD Connector que tenga el estado Pendiente. Para eliminar a uno de esos usuarios, elija el icono de papelera (🗑) que encontrará junto al nombre del usuario.

El sitio de Amazon WorkDocs siempre debe tener al menos un usuario activo que no sea un usuario invitado. Si necesita eliminar a todos los usuarios, elimine todo el sitio.

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

Transferir la propiedad de los documentos

Puede transferir los archivos y carpetas de un usuario inactivo a un usuario activo. Para obtener más información sobre cómo desactivar a un usuario, consulte Deshabilitación de usuarios.

> **Warning**
>
> Esta acción no se puede deshacer.

Para transferir la propiedad de los documentos

1. Elija el icono de perfil situado en la esquina superior derecha del cliente de WorkDocs.

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

Descarga de las 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, consulte Aplicaciones e integraciones para Amazon WorkDocs.

Para descargar una lista de usuarios

1. Elija el icono de perfil situado en la esquina superior derecha del cliente de WorkDocs.

2. En Administrador, elija Abrir panel de control del administrador.
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 alguna de las ubicaciones siguientes:

   - Windows – `Downloads/WorkDocsDownloads`
   - macOS: *`hard drive`*`/users/`*`username`*`/WorkDocsDownloads/folder`

   > **Note**
   >
   > Las descargas pueden tardar un poco. Además, los archivos no se descargan en su carpeta `/~users`.

Para obtener más información sobre estas funciones de usuario, consulte Información general sobre las funciones de usuario.

Compartir y colaborar

Los usuarios pueden compartir contenido enviando un enlace o una invitación. Los usuarios también pueden colaborar con usuarios externos si habilita el uso compartido externo.

Amazon WorkDocs controla el acceso a las carpetas y archivos mediante 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 hipervínculos de contenido almacenado en Amazon WorkDocs con compañeros de trabajo y usuarios externos, tanto dentro como fuera de su organización. Cuando los usuarios comparten un enlace, pueden configurarlo para admitir una de las siguientes opciones de acceso:

- Todos los miembros del sitio de Amazon WorkDocs pueden buscar, ver y comentar el archivo.
- Cualquier usuario que tenga el enlace, incluso personas que no sean miembros del sitio de Amazon WorkDocs, puede 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.

Compartir por invitación

Cuando habilita el uso compartido mediante invitación, los usuarios de su sitio pueden compartir archivos o carpetas con usuarios individuales y con grupos enviándoles 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 puede crear carpetas del equipo que puede compartir mediante invitación con los grupos que cree.

> **Note**
>
> Las invitaciones para compartir no incluyen a los miembros de grupos anidados. Para incluir a esos miembros, debe añadirlos a la lista Compartir por invitación.

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

Uso compartido externo

El uso compartido externo permite a los usuarios administrados de un sitio de Amazon WorkDocs compartir archivos y carpetas y colaborar con usuarios externos sin incurrir en costos adicionales. Los usuarios del sitio pueden compartir archivos y carpetas con usuarios externos sin necesidad de que los destinatarios sean usuarios de pago del sitio de Amazon WorkDocs. Si habilita el uso compartido externo, los usuarios pueden introducir la dirección de correo electrónico del usuario externo con el que desean compartir el elemento, y establecer los permisos adecuados para compartir con el visualizador. Cuando se añaden usuarios externos, solo se conceden permisos de visualizador, y los demás permisos no están disponibles. Los usuarios externos reciben una notificación por correo electrónico con un enlace al archivo o la carpeta que se ha compartido. Cuando seleccionan el enlace, los usuarios externos tienen acceso al sitio, donde pueden introducir sus credenciales para iniciar sesión en Amazon WorkDocs. 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.

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.

Permisos

Amazon WorkDocs utiliza los permisos para controlar el acceso a las carpetas y los archivos. Los permisos se aplican según los roles de usuario.

Contenido

Roles de usuario

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

- Propietario de la carpeta: propietario de una carpeta o un archivo.
- Copropietario de la carpeta: usuario o grupo que el propietario designa como copropietario de una carpeta o un archivo.
- Colaborador de la carpeta: persona con acceso ilimitado a una carpeta.
- Visualizador de la carpeta: alguien con acceso limitado (permisos de solo lectura) a una carpeta.

Puede aplicar los siguientes roles de usuario a nivel de archivo individual:

- Propietario: propietario de un archivo.

- Copropietario: usuario o grupo que el propietario designa como copropietario de un archivo.
- Colaborador*: persona autorizada a enviar comentarios en el archivo.
- Visualizador: alguien con acceso limitado (permisos de solo lectura) a un archivo.
- Visualizador anónimo: usuario no registrado ajeno a la organización que puede ver un archivo que se haya 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.

* Los colaboradores no pueden cambiar el nombre de las versiones de los archivos existentes. Sin embargo, pueden cargar una nueva versión de un archivo con un nombre diferente.

Permisos para las carpetas compartidas

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

> **Note**
>
> Los permisos aplicados a una carpeta también se aplican a las subcarpetas y archivos que esta contenga.

- Ver: permite ver el contenido de una carpeta compartida.
- Ver subcarpetas: permite ver una subcarpeta.
- Ver uso compartido: permite ver a los demás usuarios con los que se ha compartido una carpeta.
- Descargar carpeta: permite descargar una carpeta.
- Añadir subcarpeta: permite añadir una subcarpeta.
- Compartir: permite compartir la carpeta de nivel superior con otros usuarios.
- Revocar uso compartido: permite revocar el uso compartido de la carpeta de nivel superior.
- Eliminar subcarpeta: permite eliminar una subcarpeta.
- Eliminar carpeta de nivel superior: permite eliminar la carpeta compartida de nivel superior.

	Visualización	Ver subcarpetas	Ver uso compartido	Descargar carpeta	Añadir subcarpeta	Share	Revocar uso compartido	Eliminar subcarpeta	Eliminar carpeta de nivel superior
Propietario de la carpeta	✓	✓	✓	✓	✓	✓	✓	✓	✓
Copropietario de la carpeta	✓	✓	✓	✓	✓	✓	✓	✓	✓
Colaborador de la carpeta	✓	✓	✓	✓	✓				
Visualizador de la carpeta	✓	✓	✓	✓					

Permisos de los archivos de carpetas compartidas

Los siguientes permisos se aplican a los roles de usuario en una carpeta compartida:

- Anotar: permite añadir comentarios a un archivo.
- Eliminar: permite eliminar un archivo de una carpeta compartida.
- Cambiar nombre: permite cambiar el nombre de los archivos.
- Cargar: permite cargar nuevas versiones de un archivo.
- Descargar: permite descargar un archivo. Este es el permiso predeterminado. Puede usar las propiedades de archivo para permitir o prohibir la descarga de los archivos compartidos.

- Impedir la descarga: permite impedir que se descargue un archivo.

> **Note**
>
> - Al seleccionar esta opción, los usuarios con permisos de visualización pueden seguir descargando archivos. Para evitarlo, abra la carpeta compartida y desactive la opción Permitir descargas para cada uno de los archivos que no quiera que descarguen esos usuarios.
> - 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 el cliente WorkDocs web de Amazon.

- Compartir: permite compartir un archivo con otros usuarios.
- Revocar uso compartido: permite revocar el uso compartido de un archivo.
- Ver: permite ver un archivo de una carpeta compartida.
- Ver uso compartido: permite ver a los demás usuarios con los que se ha compartido un archivo.
- Ver anotaciones: permite ver los comentarios de otros usuarios.
- Ver actividad: permite ver el historial de actividades de un archivo.
- Ver versiones: permite ver las versiones anteriores de un archivo.
- Eliminar versiones: permite eliminar una o varias versiones de un archivo.
- Recuperar versiones: permite recuperar una o varias versiones eliminadas de un archivo.
- Ver todos los comentarios privados: permite al propietario o copropietario ver todos los comentarios privados de un documento, incluso si no son respuestas a su comentario.

	Annotate	Delete	Cambio de nombre	Carga	Descarga	Impedir la descarga	Share	Revocar uso compartido	Visualización	Ver uso compartido	Ver anotaciones	Ver actividad	Vista de las versiones	Eliminar versiones	Recuperar versiones	Ver todos los comentarios privados**
Propio	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

	Annota	Delete	Cambi de nombr	Carga	Descarg	Impedi la descarg	Share	Revoc uso compart o	Visualiz ción	Ver uso compart o	Ver anotacio es	Ver actividad	Vista deversione las versione	Elimin	Recuper versione	Ver todos los comentari os privados**
del arch																
Prop io de la carp	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Copi ario de la carp	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Cola or de la carp *	✓			✓	✓				✓	✓	✓	✓	✓			
Visu dor de la carp					✓				✓	✓						

	Annotate	Delete	Cambiar nombre	Cargar	Descargar	Impedir la descarga	Share	Revocar uso compartido	Visualización	Ver uso compartido	Ver anotaciones	Ver actividad	Vista de las versiones	Eliminar versiones	Recuperar versiones	Ver todos los comentarios privados**
Visualizador anónimo									✓	✓						

* En este caso, el propietario del archivo es la persona que ha subido la versión original de un archivo a una carpeta compartida. Los permisos de esta función solo se aplican al archivo propietario, no a todos los archivos de la carpeta compartida.

** Los propietarios y copropietarios pueden ver todos los comentarios privados. Los colaboradores solo pueden ver los comentarios privados en respuesta a sus comentarios.

*** Los colaboradores no pueden cambiar el nombre de las versiones de los archivos existentes. Sin embargo, pueden subir una nueva versión de un archivo con un nombre diferente.

Permisos de los archivos que no están en carpetas compartidas

Los siguientes permisos se aplican a los roles de usuario con respecto a los archivos que no estén en una carpeta compartida:

- Anotar: permite añadir comentarios a un archivo.
- Eliminar: permite eliminar un archivo.
- Cambiar nombre: permite cambiar el nombre de los archivos.
- Cargar: permite cargar nuevas versiones de un archivo.
- Descargar: permite descargar un archivo. Este es el permiso predeterminado. Puede usar las propiedades de archivo para permitir o prohibir la descarga de los archivos compartidos.
- Impedir la descarga: permite 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 el cliente WorkDocs web de Amazon.

- Compartir: permite compartir un archivo con otros usuarios.
- Revocar uso compartido: permite revocar el uso compartido de un archivo.
- Ver: permite ver un archivo.
- Ver uso compartido: permite ver a los demás usuarios con los que se ha compartido un archivo.
- Ver anotaciones: permite ver los comentarios de otros usuarios.
- Ver actividad: permite ver el historial de actividades de un archivo.
- Ver versiones: permite ver las versiones anteriores de un archivo.
- Eliminar versiones: permite eliminar una o varias versiones de un archivo.
- Recuperar versiones: permite recuperar una o varias versiones eliminadas de un archivo.

	Annotat	Delete	Cambio de nombre	Carga	Descarg	Impedir la descarg	Share	Revocar uso compart o	Visualización	Ver uso compart o	Ver anotaciones	Ver actividad	Vista de las versione	Elimina versione	Recuperar versiones
Propio*	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Copropio*	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Colaborador**	✓			✓	✓				✓	✓	✓	✓	✓		
Espectador					✓				✓	✓					

	Annotat	Delete	Cambio de nombre	Carga	Descarg	Impedir la descarg	Share	Revocar uso compartido	Visualización	Ver uso compartido	Ver anotaciones	Ver actividad	Vista de las versiones	Eliminar versiones	Recuperar versiones
Visualizador anón									✓	✓					

* Los propietarios y copropietarios de los archivos pueden ver todos los comentarios privados. Los colaboradores solo pueden ver los comentarios privados en respuesta a sus comentarios.

** Los colaboradores no pueden cambiar el nombre de las versiones de los archivos existentes. Sin embargo, pueden cargar una nueva versión de un archivo con un nombre diferente.

Habilitación de la edición en colaboración

Puede consultar la sección Configuración de la edición online del Panel de control del administrador para habilitar las opciones de edición colaborativa.

Contenido

Habilitación de Hancom ThinkFree

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

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

Para habilitar Hancom ThinkFree

Habilite la edición de Hancom ThinkFree desde el Admin control panel (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

Deshabilite la edición de Hancom ThinkFree desde el Admin control panel (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 Open with Office Online para su sitio de Amazon WorkDocs para que los usuarios puedan crear y editar archivos de Microsoft Office en colaboración desde la aplicación web de Amazon WorkDocs.

Open with Office Online está disponible sin costo adicional para los usuarios de Amazon WorkDocs que dispongan también de una cuenta de trabajo o escuela de Microsoft Office 365 con una 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 utilizar el Amazon WorkDocs Migration Service 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 los recursos compartidos de archivos departamentales y los recursos compartidos de archivos de Home Drive o de usuario a Amazon WorkDocs.

Durante este proceso, Amazon WorkDocs proporciona un AWS Identity and Access Management (IAM) política para ti. Utilice esta política para crear un nuevo IAM rol que conceda acceso a Amazon WorkDocs Migration Service para hacer lo siguiente:

- leer y enumerar los 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 rol de administrador es un usuario reservado en Amazon WorkDocs.
- Su tipo de usuario WorkDocs administrador de Amazon debe ser Upgraded WS User. Para obtener más información, consulte Información general sobre las funciones de usuario y Editar usuarios.

> **Note**
>
> La estructura de directorios, 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: preparación del contenido para la migración
- Paso 2: carga de archivos en Amazon S3
- Paso 3: programación de una migración
- Paso 4: Seguimiento de una migración
- Paso 5: limpieza de recursos

Paso 1: preparación del 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 se supera 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
- Puntos al principio o al final: por ejemplo: `.file`, `.file.ppt`, `.`, `..` o `file.`
- Virgulillas al principio o al final: por ejemplo: `file.doc~`, `~file.doc` o `~$file.doc`
- Nombres de archivo que terminan en **`.tmp`**: por ejemplo, `file.tmp`

- Nombres de archivos que se ajustan exactamente a estos términos que distinguen entre mayúsculas y minúsculas: `Microsoft User Data`, `Outlook files`, `Thumbs.db` o `Thumbnails`
- Nombres de archivos que contienen alguno de estos caracteres: `*` (asterisco), `/` (barra diagonal), `\` (barra diagonal inversa), `:` (dos puntos), < (menor que), > (mayor que), `?` (signo de interrogación), `|` (barra vertical), `"` (comillas dobles) o `\202E` (código de carácter 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 su AWS cuenta en la que quieres subir tus archivos y carpetas. El bucket de Amazon S3 debe estar en el mismo AWS cuenta y AWS Región como tu 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 ha creado en el paso anterior. Te recomendamos que utilices AWS DataSync para cargar sus archivos y carpetas al bucket de Amazon S3. DataSync proporciona funciones adicionales de seguimiento, generación de informes y sincronización. Para obtener más información, consulte Cómo AWS DataSync funciona y utiliza políticas basadas en la identidad (IAMpolíticas) para DataSync en el AWS DataSync Guía del usuario.

Paso 3: programación de una migración

Tras completar los pasos 1 y 2, utilice Amazon WorkDocs Migration Service para programar la migración. El servicio de migración puede tardar hasta una semana en procesar su solicitud de migración y enviarle un correo electrónico indicándole que puede iniciar la migración. Si inicia la migración antes de recibir el correo electrónico, la consola de administración mostrará un mensaje para indicarle 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 conllevar costes adicionales. Para obtener más información, consulta los WorkDocs precios de Amazon.

El Amazon WorkDocs Migration Service ofrece un AWS Identity and Access Management (IAM) política para que la utilices en la migración. Con esta política, crea un nuevo IAM rol que concede a Amazon WorkDocs Migration Service acceso al bucket de Amazon S3 y al WorkDocs sitio de Amazon que usted designe. También te suscribes a las notificaciones SNS por correo electrónico de Amazon para recibir actualizaciones cuando tu solicitud de migración esté programada y cuándo comience y termine.

Para programar una migración

1. En la WorkDocs consola de Amazon, selecciona Apps, Migrations.
   - Si es la primera vez que accede a Amazon WorkDocs Migration Service, se le solicitará que se suscriba a las notificaciones SNS por correo electrónico de Amazon. 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 Ejemplo de política, copia la IAM política proporcionada.
6. Utilice la IAM política que copió en el paso anterior para crear una IAM política y un rol nuevos, de la siguiente manera:
   a. Abra la IAM consola en https://console.aws.amazon.com/iam/.
   b. Elija Policies (Políticas), Create Policy (Crear política).
   c. Elija JSONy pegue la IAM política que copió anteriormente en el portapapeles.
   d. Elija Revisar política. Introduzca un nombre de política y una descripción.
   e. Elija Crear política.
   f. Elija Roles, Crear rol.

g. Selecciona otra AWS cuenta. Para Account ID (ID de la cuenta) introduzca uno de los siguientes valores:

   - Para la región Este de EE. UU. (Norte de Virginia), introduzca `899282061130`.
   - Para la región Oeste de EE. UU. (Oregón), introduzca `814301586344`.
   - Para la región Asia-Pacífico (Singapur), introduzca `900469912330`.
   - Para la región Asia-Pacífico (Sídney), introduzca `031131923584`.
   - Para la región Asia-Pacífico (Tokio), introduzca `178752524102`.
   - Para la región Europa (Irlanda), introduzca `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 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 de resumen, cambia la duración CLI máxima de la API sesión a 12 horas.

l. Copia el rol ARN en el portapapeles para usarlo en el siguiente paso.

7. Regrese al Amazon WorkDocs Migration Service. En Fuente de datos y validación, en Función ARN, pegue la IAM función ARN que copió en el paso anterior.
8. Para Bucket, seleccione el bucket de Amazon S3 del que migrar los archivos.
9. Elija Next (Siguiente).
10. En Selecciona una WorkDocs carpeta de destino, selecciona la carpeta de destino en Amazon WorkDocs a la que quieres 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 Enviar.

Paso 4: Seguimiento de una migración

Puedes realizar el seguimiento de tu migración desde la página de inicio de Amazon WorkDocs Migration Service. Para acceder a la página de destino desde el WorkDocs sitio de Amazon, selecciona Apps, Migrations. 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.

Migrating

La migración se encuentra en progreso.

Success

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 se complete la migración, elimina la política de migración y el rol que creaste desde la IAM consola.

Para eliminar la IAM política y el rol

1. Abra la IAM consola en https://console.aws.amazon.com/iam/.
2. Seleccione Políticas.
3. Busque y seleccione la política que ha creado.
4. Para Policy actions (Acciones de la política) seleccione Delete (Eliminar).

5. Elija 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. Tras la migración, puedes usar el panel de control del administrador para cambiar esa configuración. Para obtener más información, consulte Editar usuarios.

Solución de problemas de Amazon WorkDocs

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

Problemas

No puedo configurar mi sitio de Amazon WorkDocs en una región específica de AWS

Si va a configurar un nuevo sitio de Amazon WorkDocs, 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.

Quiero configurar mi sitio de Amazon WorkDocs en una VPC de Amazon existente

Al configurar su nuevo sitio de Amazon WorkDocs, cree un directorio con la nube privada virtual (VPC) existente. Amazon WorkDocs utiliza un 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.

Necesito implementar Amazon WorkDocs Drive o la aplicación Amazon WorkDocs Companion para varios 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. Para obtener información específica sobre la implementación de Amazon WorkDocs Drive para varios usuarios, consulte Implementación de Amazon WorkDocs Drive en varios ordenadores.

La edición online no funciona

Compruebe que Amazon WorkDocs Companion esté instalado. Para instalar Amazon WorkDocs Companion, consulte Aplicaciones e integraciones para Amazon WorkDocs.

Administración de Amazon WorkDocs para Amazon Business

Si es administrador de Amazon WorkDocs para Amazon Business, puede administrar a los usuarios iniciando sesión en https://workdocs.aws/ con 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 de inicio 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 a 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 de inicio 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 de inicio 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 a un usuario de Amazon WorkDocs para Amazon Business

1. Inicie sesión con sus credenciales de Amazon Business en https://workdocs.aws/.
2. En la página de inicio 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 Eliminar (Delete).
6. Si se le solicita, introduzca un nuevo usuario al que transferir los archivos del usuario y elija Delete (Eliminar).

Direcciones IP y dominios para añadir a su lista de permitidos

Si implementa el filtrado IP en los dispositivos que acceden a Amazon WorkDocs, añada las siguientes direcciones IP y dominios a su lista de permitidos. Esto permite que Amazon WorkDocs y Amazon WorkDocs Drive se conecten al servicio WorkDocs.

- 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
- zocalo.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, consulte los intervalos de direcciones IP de AWS en la referencia general de AWS.

Historial del documento

En la siguiente tabla se describen los cambios importantes en la Guía de WorkDocs administración de Amazon, que comenzarán en 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	Los administradores ahora pueden proporcionar los permisos Eliminar versión y Recuperar versión. Los permisos forman parte de la versión de la DeleteDocumentVersionAPI.	29 de julio de 2022
Amazon WorkDocs Backup	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
Gestión de Amazon WorkDocs para Amazon Business	Amazon WorkDocs for Amazon Business admite la gestión de usuarios por parte de los administradores. Para obtener más información, consulta Cómo gestionar Amazon WorkDocs para Amazon Business en la Guía de WorkDocs administración de Amazon.	26 de marzo de 2020
Migración de archivos a Amazon WorkDocs	WorkDocs Los administradores de Amazon pueden utilizar el Amazon WorkDocs	8 de agosto de 2019

	Migration Service para realizar una migración a gran escala de varios archivos y carpetas a su WorkDocs sitio de Amazon. Para obtener más información, consulta Migración de archivos a Amazon WorkDocs en la Guía de WorkDocs administración de Amazon.	
Configuración de Listas blancas de IP	La configuración de la lista de direcciones IP permitida s está disponible para filtrar el acceso a tu WorkDocs sitio de Amazon por rango de direcciones IP. Para obtener más información, consulta la configuración de la lista de direcciones IP permitidas en la Guía de WorkDocs administr ación de Amazon.	22 de octubre de 2018
Hancom ThinkFree	Hancom ThinkFree está disponible. Los usuarios pueden crear y editar de forma colaborativa archivos de Microsoft Office desde la aplicación WorkDocs web Amazon. Para obtener más información, consulta Cómo habilitar Hancom ThinkFree en la Guía de WorkDocs administración de Amazon.	21 de junio de 2018

Open with Office Online	Open with Office Online está disponible. Los usuarios pueden editar archivos de Microsoft Office de forma colaborativa desde la aplicación WorkDocs web Amazon. Para obtener más información, consulte Habilitar la apertura con Office Online en la Guía de WorkDocs administración de Amazon.	6 de junio de 2018
Solución de problemas	Se ha añadido un tema sobre solución de problemas. Para obtener más información, consulta Solución de problemas de Amazon WorkDocs en la Guía de WorkDocs administración de Amazon.	23 de mayo de 2018
Cambio del periodo de retención de la papelera de recuperación	Se puede modificar el periodo de retención de la papelera de recuperación. Para obtener más información, consulte Configuración de retención de contenedores de recuperación en la Guía de WorkDocs administración de Amazon.	27 de febrero de 2018