Guía del usuario

Terminal de transferencia de datos de AWS

Terminal de transferencia de datos de AWS: Guía del usuario

Table of Contents

¿Qué es el terminal de transferencia de datos?

El terminal de transferencia de datos de AWS es una ubicación física preparada para la red a la que puede llevar sus dispositivos de almacenamiento de datos para una transferencia de datos rápida desde y hacia su servicio en la nube de AWS. Cargue datos capturados de forma remota para facilitar su acceso.

Programe una reserva en una de nuestras instalaciones físicas del terminal de transferencia de datos desde la consola de administración de AWS, llegue a la hora programada y cargue sus datos a los servicios de la nube de AWS con sus propios dispositivos. Una vez que se complete la reserva programada y usted se vaya, la instalación se volverá a proteger y se preparará para la próxima reserva programada.

> **Note**
>
> Por el momento, el terminal de transferencia de datos AWS solo está disponible para los clientes empresariales de AWS.

Para acceder al terminal de transferencia de datos:

- Consola del terminal de transferencia de datos de AWS: https://console.aws.amazon.com/datatransferterminal
- Instalaciones del terminal de transferencia de datos: la ubicación de las instalaciones del terminal de transferencia de datos se proporciona una vez realizada la reserva en la consola. Para obtener más información, consulte Realizar una transferencia de datos.

Características

El uso del terminal de transferencia de datos de AWS facilita la introducción de sus datos en su servicio de la nube de AWS desde ubicaciones remotas. Las siguientes son algunas de las ventajas del terminal de transferencia de datos para sus necesidades de carga remota de datos:

Seguro, privado y exclusivo

Cada instalación del terminal de transferencia de datos es un lugar seguro y privado donde puede realizar grandes transferencias de datos entre su dispositivo de almacenamiento de datos y sus servicios de AWS a través de una conexión de red rápida.

Una consola de reservas exclusiva

Agregue personal autorizado a su equipo de transferencia y programe una reserva en el terminal de transferencia de datos mediante la consola del terminal de transferencia de datos de AWS.

Conexiones de red de fibra óptica

Cada instalación del terminal de transferencia de datos incluye dos conexiones de fibra óptica (LR4) de 100 gigabits (Gbps) para una carga de datos rápida y redundancia.

Control de sus dispositivos de almacenamiento de datos

No es necesario enviar su dispositivo Snowball y esperar a que los datos se carguen en sus servicios de la nube de AWS. Usted controla los dispositivos físicos de almacenamiento de datos durante todo el proceso de transferencia de datos, lo que permite que sus datos lleguen a su destino más rápidamente.

Conceptos clave

El uso del terminal de datos de AWS requiere que un propietario del proceso programe una reserva para que un especialista en transferencia de datos acceda a una instalación del terminal de transferencia de datos. Consulte las siguientes secciones para obtener más información acerca de la terminología del terminal de transferencia de datos.

Temas

Equipo de transferencia

Un equipo de transferencias es un grupo de personal determinado por el propietario de una cuenta de AWS que se puede seleccionar para realizar transferencias de datos en nombre de la

organización. La configuración de un equipo de transferencia incluye darle un nombre al equipo y especificar el personal que lo compone. Recomendamos grupos de cuatro o menos especialistas en transferencia de datos para una sola reserva.

Para obtener más información, consulte Programación de una reserva del terminal de transferencia de datos.

Personal

Por personal nos referimos a las personas que pueden hacer y administrar reservas o que pueden acudir a las instalaciones del terminal de transferencia de datos y utilizarlas. El personal puede ser propietario del proceso, especialista en transferencia de datos o ambos.

Propietario del proceso

- Un propietario del proceso es el propietario de una cuenta de AWS que puede agregar, editar y eliminar personal de su cuenta del terminal de transferencia de datos de AWS.

Especialista en transferencia de datos

- Un especialista en transferencia de datos es una persona que puede acudir a las instalaciones del terminal de transferencia de datos para realizar transacciones de carga de datos. Este personal debe estar autorizado por el propietario del proceso y agregado a su cuenta del terminal de transferencia de datos de AWS. Se requiere una identificación emitida por el gobierno para acceder a una instalación del terminal de transferencia de datos.

Instalaciones

Las instalaciones del terminal de transferencia de datos son centros de datos de propiedad conjunta que están administrados por uno o más proveedores de servicios. Cada instalación requiere que los especialistas en transferencia de datos del terminal de transferencia de datos presenten una prueba de identidad emitida por el gobierno que debe coincidir con los registros de la reserva a fin de acceder a la sala del terminal de transferencia de datos.

Consideraciones sobre la programación

Las reservas se pueden realizar en la consola del terminal de transferencia de datos con una duración de una a seis horas, para cualquier día de la semana y durante todo el año. Las reservas individuales se pueden programar de forma consecutiva, con un intervalo mínimo de una hora entre las reservas. Todas las reservas deben hacerse con al menos 24 horas de anticipación.

El tiempo necesario para realizar una transferencia de datos varía según las velocidades de rendimiento de carga. Tenga en cuenta los siguientes factores que afectan al rendimiento de carga al momento de planificar y programar la reserva de su terminal de transferencia de datos.

Equipo

- Es posible que algunos equipos incluyan ajustes que pueden afectar al rendimiento de carga. Consulte las especificaciones de su equipo para ver las velocidades de rendimiento de carga sugeridas.

Condiciones de la red

- Los momentos de tráfico intenso de la red afectarán a las velocidades de carga de datos y deben tenerse en cuenta al momento de seleccionar una hora para la sesión de transferencia de datos. Planificar la sesión de transferencia de datos para las horas de menor demanda o durante momentos de menor actividad de la red puede mejorar la velocidad de carga.

Tamaño de transferencia de datos

- La conectividad de red del terminal de transferencia de datos está diseñada para transferencias de datos de gran tamaño. Sin embargo, el tamaño de los datos que se transfieren afectará a la duración de la sesión.

Casos de uso

Si bien cualquier cliente empresarial de AWS puede acceder al sistema del terminal de transferencia de datos, ciertos casos de uso pueden beneficiarse más de él.

Conducción autónoma y sistemas avanzados de asistencia al conductor (AD/ADAS): los fabricantes de equipos originales (OEM) y proveedores del sector automotriz generan grandes conjuntos de datos a partir de sus flotas de vehículos autónomos que operan y recopilan datos en numerosas áreas metropolitanas de América del Norte, Europa y la ASEAN. Con el terminal de transferencia de datos, los datos recopilados por estos vehículos de la flota pueden cargarse en el servicio de la nube de AWS y utilizarse para entrenar los modelos de AD/ADAS.

Medios y entretenimiento: los estudios y otros creadores de contenido suelen generar archivos de video y audio (AV) digitales en ubicaciones remotas. Es importante que estos archivos de AV se carguen en la nube de manera oportuna para que los equipos de producción y edición que están en diferentes lugares puedan iniciar los flujos de trabajo en paralelo y en tiempo real. Al utilizar el terminal de transferencia de datos para cargar datos de forma remota, se pueden acortar los plazos de producción, lo que se traduce en una reducción de los costos de producción.

Mapas, fotogrametría e imágenes 3D: las organizaciones que trabajan con aplicaciones de mapeo o imágenes recopilan datos en ubicaciones remotas y necesitan cargar estos archivos visuales en la nube de AWS para su análisis o entrenamiento. El terminal de transferencia de datos minimiza el tiempo que transcurre entre la recopilación y el análisis de estos grandes conjuntos de datos, lo que ayuda a mantener actualizados los datos geoespaciales para los conductores, los agricultores y otros usuarios de esa información.

Servicios relacionados

Los siguientes servicios de AWS proporcionan una experiencia óptima durante el uso del terminal de transferencia de datos.

Servicio de AWS	Descripción
AWS Snowball Edge	El terminal de transferencia de datos de AWS complementa los productos de Snowball al proporcionar una ubicación para cargar más rápidamente a su nube de AWS, lo que minimiza los tiempos de espera para acceder a sus datos.
Amazon S3	Lleve su propio dispositivo a un terminal de transferencia de datos para cargar los datos de forma rápida y segura a su servicio de Amazon S3.

Requisitos técnicos para el uso del terminal de transferencia de datos

Antes de programar una reserva en un terminal de transferencia de datos, deberá asegurarse de contar con el equipo y las configuraciones necesarios para conectarse a la red. Consulte las siguientes pautas para tener una conectividad y una experiencia de red óptimas.

Equipo

Debe llevar dispositivos portátiles para la conectividad, incluidos monitores, un teclado, un ratón y una computadora de escritorio o portátil, al terminal de transferencia de datos para su reserva programada.

Su hardware debe poder funcionar con conexiones de fibra óptica (L4)

> **Note**
>
> Como práctica recomendada de seguridad de datos, asegúrese de que sus datos estén cifrados y protegidos en los dispositivos de almacenamiento que lleve al terminal de transferencia de datos y asegúrese de aplicar políticas de cifrado de datos cuando utiliza el terminal de transferencia de datos. Para obtener más información, consulte Seguridad del terminal de transferencia de datos de AWS

Requisitos de red

Asegúrese de que su dispositivo, servidor o equipo (portátil) esté preparado para conectarse a la red y sea compatible con DHCP. Debería tener lo siguiente para disfrutar de una experiencia de carga de datos óptima:

- Un transceptor óptico QSFP28 LR4 (100GBASE-LR4) de 100 G, compatible con los conectores LC y NIC para las conexiones de cable de fibra proporcionadas en el terminal de transferencia de datos.
- Configuración automática de DHCP de direcciones IP habilitada. Los servidores DNS se asignan automáticamente mediante DHCP.
- Software y controladores de NIC actualizados.

Optimización del rendimiento

Para maximizar el rendimiento durante el uso del terminal de transferencia de datos de AWS, tenga en cuenta las siguientes recomendaciones.

- Hardware recomendado:
  - tarjeta de interfaz de red de 100 Gbps
  - CPU de 16 núcleos
  - 128 GB de RAM
  - Múltiples unidades SSD NVMe en una matriz RAID
- Utilice la biblioteca Common Runtime de AWS(CRT de AWS) para las cargas mediante la interfaz de la línea de comandos de AWS o el SDK de AWS.

  Optimice los ajustes de transferencia de Amazon S3 configurando los siguientes parámetros. Establezca estos valores en la clave superior de `s3` en el archivo de configuración de AWS, ubicación predeterminada `~/.aws/config`.

  ```
  [default]
  s3 =
      preferred_transfer_client = crt
      target_bandwidth = 100Gb/s
      max_concurrent_requests = 20
      multipart_chunksize = 16MB
  ```

  Tenga en cuenta que todos los valores de configuración de Amazon S3 están indentados y anidados bajo la clave superior de `s3`.

  - Opcional: puede establecer los valores anteriores mediante programación usando el comando `aws configure set`. Por ejemplo, a fin de establecer los valores anteriores para el perfil predeterminado, puede ejecutar los siguientes comandos en su lugar:

    ```
    aws configure set default.s3.preferred_transfer_client crt
    aws configure set default.s3.target_bandwidth 100Gb/s
    aws configure set default.s3.max_concurrent_requests 20
    aws configure set default.s3.multipart_chunksize 16MB
    ```

- Si desea establecer estos valores mediante programación para un perfil que no sea el predeterminado, proporcione el indicador `--profile`. Por ejemplo, para establecer la

configuración de un perfil denominado `test-profile`, ejecute un comando como el que se muestra a continuación.

```
aws configure set s3.max_concurrent_requests 20 --profile test-profile
```

- Habilite BBR (Linux) en el dispositivo para obtener un mejor rendimiento.

```
sysctl -w net.core.default_qdisc=fq
sysctl -w net.ipv4.tcp_congestion_control=bbr
```

Más información

Para obtener más información acerca de las configuraciones de Amazon S3 para la línea de comandos de AWS a fin de optimizar la conectividad y el rendimiento de la red, consulte los siguientes recursos.

- Configuración de Amazon S3 para la CLI de AWS en la Referencia de comandos de la CLI de AWS
- Utilizar un cliente S3 de alto rendimiento: cliente S3 basado en CRT AWS en el SDK de Amazon S3 AppStream para Java
- ¿Cómo optimizo el rendimiento cuando utilizo la CLI de AWS para cargar archivos grandes en Amazon S3? en el Centro de conocimientos de AWS

Introducción

Comience a realizar transferencias de datos remotas a sus servicios de la nube de AWS mediante una reserva en una de las instalaciones del terminal de transferencia de datos. Para empezar, necesitará un equipo compatible con la instalación del terminal de transferencia de datos y una cuenta empresarial de AWS.

Revise la sección Requisitos técnicos para utilizar el terminal de trasferencia de datos de esta guía antes de programar una reserva del terminal de transferencia de datos para asegurarse de que dispone de un equipo con las configuraciones óptimas para la transferencia de datos. No todos los dispositivos de almacenamiento de datos y los equipos de conexión de red son compatibles con las conexiones de red de fibra óptica disponibles en las salas.

Cuando se registra en AWS, su cuenta de AWS se registra automáticamente en todos los servicios de AWS, incluido el terminal de transferencia de datos. Solo se le cobrará por los servicios que utilice.

Para configurar el terminal de transferencia de datos, siga los pasos descritos en las secciones siguientes.

Cuando se registra en AWS y configura el terminal de transferencia de datos, puede cambiar de forma opcional el idioma de visualización de la consola de administración de AWS. Para obtener más información, consulte Cambiar el idioma de la consola de administración de AWS en la Guía de introducción de la consola de administración de AWS.

Una vez que tenga una cuenta de AWS, podrá acceder al terminal de transferencia de datos. Para obtener más información acerca de la configuración y el uso del terminal de transferencia de datos de AWS, consulte Programación de una reserva del termina de transferencia de datos.

Registro en una cuenta de AWS

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

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

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

Cuando se registra en una cuenta de AWS, se crea una cuenta de usuario raíz de AWS. Este usuario tiene acceso a todos los recursos y los servicios de AWS en 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 le enviará un correo electrónico de confirmación cuando complete el proceso de registro. Se puede ver la actividad de la cuenta y administrarla en cualquier momento al ingresar en https://aws.amazon.com/ y seleccionar Mi cuenta.

Creación de un usuario con acceso administrativo

Después de registrarse para obtener una cuenta de AWS, proteja su usuario raíz de AWS, habilite IAM Identity Center de AWS y cree un usuario administrativo para no utilizar el usuario raíz en las tareas cotidianas.

1. Inicie sesión en la consola de administración de AWS como el propietario de la cuenta; para ello, elija Usuario raíz e introduzca la dirección de email de su cuenta de AWS. En la siguiente página, escriba su contraseña.

   Para obtener ayuda para iniciar sesión con el usuario raíz, consulte Iniciar sesión como usuario raíz en la Guía de inicio de sesión del usuario de AWS.
2. Active la autenticación multifactor (MFA) para el usuario raíz.

   Para obtener instrucciones, consulte Habilitación de un dispositivo MFA virtual para su usuario raíz de la cuenta de AWS (consola) en la Guía del usuario de IAM.
3. Activar IAM Identity Center.

   Para obtener más información, consulte Habilitación de IAM Identity Center de AWS en la Guía del usuario de IAM Identity Center de AWS.
4. En IAM Identity Center, conceda acceso administrativo a un usuario.

   Para ver un tutorial sobre el uso del directorio de IAM Identity Center como fuente de identidad, consulte Configurar el acceso de los usuarios con el directorio predeterminado de IAM Identity Center en la Guía del usuario de IAM Identity Center de AWS.
5. Para iniciar sesión con el usuario de IAM Identity Center, use la URL de inicio de sesión que se envió a la 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 Inicio de sesión en el portal de acceso de AWS en la Guía de inicio de sesión del usuario de AWS.

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

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

7. 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 la Guía del usuario de IAM Identity Center de AWS.

Programación de una reserva del terminal de transferencia de datos

Para empezar a utilizar el terminal de transferencia de datos de AWS, debe tener una cuenta de AWS e iniciar sesión en la consola del terminal de transferencia de datos en https://console.aws.amazon.com/datatransferterminal. Una vez que haya iniciado sesión en la consola del terminal de transferencia de datos, podrá ver las reservas existentes o hacer una nueva. Para programar una reserva, deberá realizar las siguientes tareas:

1. Cree un equipo de transferencia. Deberá formar un grupo designado de usuarios para crear una reserva y acceder a la instalación del terminal de transferencia de datos y realizar una transferencia de datos. Para obtener más información sobre este tema, consulte Crear un equipo de transferencia.
2. Una vez que haya establecido su equipo, tendrá que agregarle personal. Para obtener más información sobre cómo agregar personal a su equipo de transferencia, consulte Agregar personal.
3. El propietario del proceso puede programar la transferencia de datos con los equipos de la cuenta. Para obtener más información sobre cómo programar la reserva, consulte Especificar los detalles de la reserva.
4. Asegúrese de que los detalles de la reserva sean correctos antes de enviar su solicitud. Una vez que envía la solicitud de reserva, no puede modificarla durante al menos 24 horas. Para obtener más información, consulte Revisar y confirmar su reserva.

Una vez que se procese y confirme su reserva, el equipo de transferencia podrá acceder a la instalación del terminal de transferencia de datos a la hora programada. Para obtener más información, consulte Realizar una transferencia de datos en la instalación del terminal de transferencia de datos.

Creación de un equipo de transferencia

Para acceder a las instalaciones del terminal de transferencia de datos, deberá programar una reserva en la consola de adminstración de AWS. Inicie sesión en su cuenta de AWS para acceder a la consola del terminal de transferencia de datos y complete los siguientes pasos para programar su reserva.

1. En la página de inicio del terminal de transferencia de datos, seleccione el botón Comenzar.
2. Si aún no tiene un equipo de transferencia configurado en su cuenta, el botón Crear reserva estará deshabilitado. Deberá que crear un equipo de transferencia y asignarle un nombre para comenzar.
   a. Seleccione el botón Crear equipo de transferencia.
   b. Asigne un nombre al equipo.
      - El nombre debe empezar por una letra o un número y debe tener entre dos y 64 caracteres.
      - Use únicamente letras, números, puntos y guiones. No se reconocen los caracteres especiales.
      - No incluya información de identificación confidencial.
   c. Cree una descripción del equipo de transferencia.
      - Proporcione una descripción que ayude a identificar al equipo, por ejemplo, que describa el propósito del equipo para un período, una campaña o un proyecto específicos.
   d. Seleccione el botón Crear equipo de transferencia.

      Volverá a la página del equipo de transferencia y su equipo recién creado aparecerá en la sección Equipos de transferencia.

Actualización de los equipos de transferencia en su cuenta del terminal de transferencia de datos

Para configurar un nuevo equipo de transferencia, consulte la sección Programar una reserva del terminal de transferencia de datos de esta guía.

Para modificar o eliminar un equipo de transferencia, haga lo siguiente:

1. En la página Equipos de transferencia, seleccione el equipo de transferencia que desea modificar.
2. Para modificar el nombre y la descripción del equipo de transferencia, seleccione el botón Editar.
3. Para agregar o eliminar personal, seleccione la pestaña personal y siga los pasos que se describen en la sección ¿Cómo modifico, agrego o elimino personal de mi cuenta? de estas preguntas frecuentes.
4. Para agregar o cancelar una reserva para el equipo de transferencia seleccionado, consulte la sección Actualización del personal de su cuenta del terminal de transferencia de datos de estas preguntas frecuentes.

Cómo agregar personal

Agregue propietarios de procesos y especialistas en transferencia de datos a su equipo de transferencia para configurar la transferencia de datos y acceder a la instalación del terminal de transferencia de datos. Para agregar personal a su equipo de transferencia, haga lo siguiente:

1. En la página Equipos de transferencia, seleccione la tarjeta del equipo de transferencia deseado entre las que aparecen en la sección Equipos de transferencia. Aparecerá la página de resumen del equipo de transferencia.
2. Seleccione la pestaña Personal y, a continuación, el botón Registrar persona para agregar personal al equipo de transferencia.
3. Complete los campos con la información necesaria sobre la persona que va a agregar al equipo de transferencia en la página Registrar personal.
   a. Alias del personal: cree un alias único para identificar a la persona.
      - El alias se utiliza para identificar al personal y, al mismo tiempo, proteger su identidad.
      - Puede tener hasta 64 caracteres e incluir letras, números y guiones.
      - No se permite el uso de caracteres especiales.
   b. Nombre: proporcione el nombre de la persona tal como aparece en su identificación emitida por el gobierno.
   c. Apellido: proporcione el apellido de la persona tal como aparece en su identificación emitida por el gobierno.
   d. Dirección de correo electrónico: incluya una dirección de correo electrónico válida para que la persona reciba la información sobre la reserva y las instrucciones para acceder al terminal de transferencia de datos.
4. Seleccione el botón Registrar persona para terminar de agregar a la persona a su equipo de transferencia.

Actualización del personal de su cuenta del terminal de transferencia de datos

Actualmente, no se admite la modificación del personal existente de su cuenta en la consola del terminal de transferencia de datos. AWS Por el momento, solo los propietarios del proceso del terminal de transferencia de datos pueden agregar o eliminar personal.

Para eliminar personal de su cuenta del terminal de transferencia de datos, haga lo siguiente:

1. En la página Equipos de transferencia, seleccione el equipo de transferencia asociado al personal que desea eliminar.
2. En la página de resumen del equipo de transferencia seleccionado, seleccione la pestaña personal.
3. Haga clic en el botón de opción que se encuentra junto al alias que desea eliminar. Tenga en cuenta que solo podrá ver el alias de la persona cuando elimine su perfil.
4. Seleccione el botón Eliminar. Aparece una advertencia para confirmar la acción prevista para el personal seleccionado. Haga clic en el botón Eliminar. Aparecerá un banner en la parte superior de la consola que confirma que se eliminó el personal correctamente.

Especificación de los detalles de la reserva

Las siguientes instrucciones lo ayudarán a programar su reserva del terminal de transferencia de datos en la consola de administración de AWS. Para obtener información sobre el uso de la instalación del terminal de transferencia de datos, consulte Realizar una transferencia de datos.

1. Seleccione el botón Hacer reserva en la pestaña Próximas reservas.
2. Rellene los campos de la página Especificar los detalles de la reserva.
   a. Selección del equipo de transferencia: el equipo de transferencia seleccionado de manera predeterminada aparece primero. Si desea elegir un equipo diferente, haga clic en la flecha desplegable para seleccionar de la lista de equipos de transferencia disponibles.
   b. Propietario del proceso: seleccione el alias del personal que desea que sea responsable de administrar la reserva.
      - Solo se permite un propietario del proceso por reserva y debe ser miembro del personal autorizado en su cuenta de AWS.

        El propietario del proceso también puede incluirse como uno de los especialistas en transferencia de datos para realizar la actividad de transferencia de datos.
   c. Especialista en transferencia de datos: seleccione el miembro del personal que desea que tenga acceso a la instalación del terminal de transferencia de datos para completar la actividad de transferencia de datos. Puede seleccionar más de un miembro del personal, según sea necesario.
      - Se recomienda limitar su equipo de transferencia a no más de cuatro (4) especialistas en transferencia de datos.

d. Información del terminal de transferencia de datos: especifique la instalación del terminal de transferencia de datos, la fecha deseada y la hora específica para la sesión de transferencia de datos.

   i. Instalación del terminal de transferencia de datos: haga clic en la flecha desplegable para seleccionar una instalación del terminal de transferencia de datos.

   > **Note**
   >
   > Cuando hace una reserva, solo se proporcionan las descripciones de las instalaciones. Se proporciona información adicional sobre la ubicación en el correo electrónico de confirmación de la reserva.

   ii. Fecha y hora del terminal de transferencia de datos: haga clic en el campo Buscar una fecha y hora para su reserva para ver el calendario y programar su reserva.

   - Las reservas deben hacerse con un mínimo de 24 horas de antelación y no más de seis (6) meses de anticipación, y solo pueden tener una duración máxima de seis (6) horas. Una sola reserva puede abarcar más de un día para tener en cuenta los escenarios nocturnos, si es necesario.
   - La hora se indica con un reloj de 24 horas y solo se puede reservar en incrementos de horas completas.
   - Para hacer reservas consecutivas, debe crear reservas independientes con al menos una hora entre cada sesión de transferencia de datos.
   - Para obtener información, consulte Consideraciones sobre la programación.

3. Confirme que los detalles de la reserva sean correctos y, a continuación, seleccione el botón Crear para continuar. Esto lo llevará a la página de confirmación, en la que se proporciona un resumen de su reserva.

Cómo revisar y confirmar su reserva

Después de especificar los detalles de su reserva, seleccione el botón Siguiente para continuar y ver la página de resumen. Revise los detalles de su solicitud de reserva del terminal de transferencia de datos en la página Revisar y crear.

- Si está satisfecho con la solicitud, seleccione el botón Crear.
- Si necesita cambiar su reserva, seleccione el botón Anterior.

Una vez que se envíe la solicitud de reserva, el propietario del proceso recibirá un correo electrónico en el que se confirma que la solicitud se ha recibido y se está procesando. Una vez que se apruebe la solicitud, se enviará otro correo electrónico en el que se confirma la reserva y se proporcionan instrucciones para buscar y acceder a la instalación del terminal de transferencia de datos. Para obtener información sobre cómo acceder a la instalación del terminal de transferencia de datos, consulte Realizar una transferencia de datos.

Cómo realizar cambios en su reserva

Se aplica un período de procesamiento de 24 horas para realizar cualquier cambio en su solicitud de reserva del terminal de transferencia de datos.

Después del período de procesamiento, para ver, editar o eliminar su reserva, vaya a la página Equipos de transferencia en la consola.

1. Busque y seleccione la reserva deseada en la tarjeta del equipo.
2. Haga clic en el menú Acciones y seleccione la acción deseada.
   - Ver: si selecciona la opción de visualización, podrá ver los detalles de su reserva, incluidos la fecha, la hora, el lugar y el personal asignado.
   - Editar: puede revisar los detalles de la reserva, incluidos la fecha, la hora, el lugar y el personal asignado. Tenga en cuenta que los cambios deben realizarse 24 horas antes de la fecha de reserva deseada y que las revisiones no se aceptan ni aplican de forma inmediata. El propietario del proceso recibirá la confirmación de la solicitud actualizada.
   - Eliminar: la opción de eliminar le permite cancelar su reserva. La solicitud de cancelación debe hacerse como mínimo 24 horas antes de la fecha de reserva programada. El propietario del proceso recibirá la confirmación de la reserva cancelada cuando se apruebe la solicitud.

Cómo realizar una transferencia de datos en la instalación del terminal de transferencia de datos

El terminal de transferencia de datos es una ubicación segura y de propiedad compartida que proporciona un acceso seguro a la red de AWS. Para acceder a la instalación del terminal de transferencia de datos, asegúrese de tener un correo electrónico de confirmación que incluya la descripción de la ubicación y las instrucciones de acceso. Consulte los temas a continuación para obtener más información acerca de cómo acceder y utilizar la instalación del terminal de transferencia de datos.

Temas

Qué llevar

Los especialistas en transferencia de datos deben llevar los elementos necesarios para realizar una transferencia de datos, como una computadora portátil, unidades flash, unidades de estado sólido (SSD) y Snowball Edge de AWS. Asegúrese de que su equipo esté optimizado para utilizar los cables de red de fibra que se encuentran en la instalación del terminal de transferencia de datos. Para obtener más información acerca de la configuración y los equipos óptimos, consulte Requisitos técnicos para utilizar el terminal de transferencia de datos.

Usted es responsable de la instalación, el uso y el desmontaje del equipo y los artículos que usted y los especialistas en transferencia de datos que lo acompañen lleven a la instalación del terminal de transferencia de datos. Todo lo que se introduzca en la sala debe retirarse al salir. AWS El terminal de transferencia de datos no se hace responsable de los artículos olvidados o perdidos.

La dirección física de la instalación del terminal de transferencia de datos

No se proporcionará la dirección física de la instalación del terminal de transferencia de datos. En cambio, el propietario del proceso y los especialistas en transferencia de datos especificados en la reserva recibirán un correo electrónico con el nombre público que permite realizar búsquedas de la instalación del terminal de transferencia de datos. AWS El terminal de transferencia de datos utiliza el mismo sistema de identificación de ubicación que Direct Connect de AWS, por lo que puede buscar el nombre público en Internet para encontrar la instalación del terminal de transferencia de datos.
Si no recibió un correo electrónico con esta información, confirme con su administrador de cuentas del terminal de transferencia de datos que AWS está incluido en el equipo de transferencia y que su información de correo electrónico es correcta.

Acceso al edificio

Para acceder a la instalación del terminal de transferencia de datos, cada especialista en transferencia de datos debe proporcionar una prueba de identidad o una identificación emitida por el gobierno. Una vez admitido en el edificio, el personal de seguridad lo acompañará hasta su sala del terminal de transferencia de datos.

Equipo previsto en la sala del terminal de transferencia de datos.

Cada instalación del terminal de transferencia de datos debe tener solo dos (2) cables de fibra óptica, una mesa o escritorio y sillas. Si hay algún otro equipo o elemento en la sala, infórmeselo al soporte inmediatamente.

Solución de problemas de conexión de red

Si experimenta problemas de conexión a la red mientras utiliza el terminal de transferencia de datos de AWS, como no poder conectarse a Internet o velocidades de conexión lentas, tenga en cuenta los siguientes consejos de solución de problemas.

Temas

Problemas de conexión del equipo

Si tiene dificultades para establecer una conexión física mientras se encuentra en la sala del terminal de transferencia de datos, tenga en cuenta lo siguiente:

- Cada instalación del terminal de transferencia de datos tendrá dos (2) cables de fibra monomodo LC. Si falta uno o ambos cables, póngase en contacto con el equipo de Soporte técnico de AWS de inmediato.
- Si un cable de fibra óptica no funciona, intente enrollar el cable primero. Si aún así no puede conectarse con el primer cable, intente usar el otro.

Si no puede usar los cables para conectarse, póngase en contacto con el equipo de Soporte técnico de AWS de inmediato.

Solución de problemas de conectividad

Si puede conectar su equipo, pero no puede conectarse a la red, pruebe las siguientes sugerencias de solución de problemas.

- Confirme que la configuración de su equipo cumple con los requisitos de red especificados. Para obtener información, consulte Requisitos técnicos para el uso del terminal de transferencia de datos
- Use el otro cable de fibra óptica para realizar la conexión.

- Reinicie el dispositivo mientras mantiene los cables de fibra óptica conectados.
- Realice un diagnóstico básico de la red en el dispositivo para asegurarse de lo siguiente:
  - DHCP está habilitado
  - Hay una dirección IP asignada a la interfaz de red conectada
  - Los servidores DNS están configurados
  - El reloj del sistema está sincronizado con NTP

Si sigue sin poder conectarse, póngase en contacto con el equipo de Soporte técnico de AWS y proporcione los siguientes resultados en función del sistema operativo (SO) que se ejecute en su dispositivo.

Linux/Unix

- Obtenga la dirección IP y la información de enrutamiento en un terminal o una interfaz de la línea de comandos (CLI). Verifique que se haya asignado una dirección IP a la interfaz de red y que se haya agregado una ruta predeterminada con una dirección de puerta de enlace predeterminada en la tabla de enrutamiento.

```
ip address show
ip route show
```

  - Como alternativa, si `iproute2` no está instalado en el dispositivo y los comandos `ip` no están disponibles, utilice los siguientes comandos:

```
ifconfig
netstat -rn
```

- Recopile la información del servidor DNS. Debería mostrar dos direcciones IP que comienzan con la palabra clave `nameserver`.

```
cat /etc/resolv.conf
```

- Recopile el resultado de las pruebas de conectividad básicas. Reemplace `default_gateway_address` con la dirección IP de la puerta de enlace predeterminada asignada.

```
ping -c 5 <default_gateway_address>
```

```
ping -c 5 s3.amazonaws.com
traceroute s3.amazonaws.com
```

- Recopile el resultado de las pruebas de conectividad de HTTPS. El siguiente comando debería mostrar una respuesta `HTTP 200 OK` de Amazon S3.

```
curl -i https://s3.amazonaws.com/ping
```

Windows

- Obtenga la dirección IP, la información de enrutamiento y del servidor DNS en el símbolo del sistema. Verifique que se haya asignado una dirección IP a la interfaz de red, que se hayan asignado dos servidores DNS y que se haya agregado una ruta predeterminada con una dirección de puerta de enlace predeterminada en la tabla de enrutamiento.

```
ipconfig /all
route print
```

- Recopile el resultado de las pruebas de conectividad básicas en el símbolo del sistema. Reemplace la `default_gateway_address` con la dirección IP de la puerta de enlace predeterminada asignada.

```
ping <default_gateway_address>
ping s3.amazonaws.com
tracert s3.amazonaws.com
```

- Recopile el resultado de la prueba de conectividad de HTTPS en PowerShell. El siguiente comando debería mostrar una respuesta `HTTP 200 OK`.

```
Invoke-WebRequest -Uri "https://s3.amazonaws.com/ping"
```

Network throughput

El rendimiento de la red, que mide la velocidad real de transferencia de datos en una red, puede verse afectado por varios factores. Los siguientes factores pueden afectar a las velocidades de transferencia de datos:

- Hardware: los componentes de hardware del dispositivo pueden reducir las velocidades de conexión durante la carga de datos. Es posible que la CPU y los discos utilizados en el dispositivo estén alcanzando sus límites de rendimiento. Considere usar SSD NVMe en una matriz RAID. Asegúrese de utilizar la biblioteca AWS CRT para obtener un mejor rendimiento y reducir el uso de la CPU.
- Sobrecarga de cifrado: las transmisiones seguras, como HTTPS, aumentan el tiempo de procesamiento debido a la sobrecarga de cifrado.
- Latencia: la latencia se refiere al tiempo que tarda un paquete de datos en viajar desde el origen hasta el destino. Se puede observar una latencia alta cuando se cargan datos en un bucket de Amazon S3 en una región geográfica diferente, lo que puede provocar retrasos en la transferencia de datos y reducir el rendimiento. Se recomienda realizar transferencias de datos dentro de la misma región, siempre que sea posible.
- Pérdida de paquetes: los paquetes perdidos requieren retransmisión, lo que ralentiza la transferencia de datos.

Seguridad del terminal de transferencia de datos de AWS

El terminal de transferencia de datos de AWS proporciona un entorno seguro para realizar transferencias de datos hacia y desde la nube de AWS. Como cualquier otra conexión de fibra de red física, la conexión de la terminal de transferencia de datos no proporciona cifrado predeterminado. Por lo tanto, usted será responsable de aplicar las prácticas recomendadas de cifrado de datos para garantizar que su transferencia de datos sea segura.

La seguridad en la nube en AWS es la máxima prioridad. Como cliente de AWS, se beneficiará de una arquitectura de red y de centros de datos diseñados para satisfacer los requisitos de seguridad de las organizaciones más exigentes.

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

- Seguridad de la nube: AWS es responsable de proteger la infraestructura que ejecuta los servicios de AWS en la nube de AWS. AWS también proporciona servicios que puede utilizar de forma segura. Auditores externos prueban y verifican periódicamente la eficacia de nuestra seguridad en el marco de los programas de conformidad de AWS. Para obtener más información acerca de los programas de conformidad que se aplican al terminal de transferencia de datos de AWS, consulte Servicios de AWS en el ámbito del programa de conformidad.
- Seguridad en la nube: su responsabilidad viene determinada por el servicio de AWS que utilice. También es responsable de otros factores, incluida la confidencialidad de los datos, los requisitos de la empresa y la legislación y la normativa aplicables.

Esta documentación le ayuda a comprender cómo aplicar el modelo de responsabilidad compartida cuando se utiliza el terminal de transferencia de datos. Los siguientes temas le muestran cómo proteger sus datos mientras utiliza el servicio del terminal de transferencia de datos. También puede aprender a utilizar otros servicios de AWS que ayudan a supervisar y proteger los recursos del terminal de transferencia de datos.

Temas

- Registro y supervisión en el terminal de transferencia de datos
- La seguridad de la infraestructura en el terminal de transferencia de datos de AWS

Protección de datos en el terminal de transferencia de datos de AWS

El modelo de responsabilidad compartida de AWS aplica a la protección de datos en el terminal de transferencia de datos de AWS. Tal como se describe en este modelo, AWS es responsable de proteger la infraestructura global que ejecuta toda la nube de AWS. Eres responsable de mantener el control sobre el contenido alojado en esta infraestructura. También es responsable de la configuración de seguridad y de las tareas de administración para los servicios de AWS que utiliza. Para obtener más información sobre la protección, consulte las Preguntas frecuentes sobre la protección de datos. Para obtener información sobre la protección de datos en Europa, consulte la publicación de blog sobre el Modelo de responsabilidad compartida de AWS y el RGPD en el blog de seguridad de AWS.

A los efectos de la protección de datos, se recomienda que proteja las credenciales de la cuenta de AWS y configure cuentas de usuario individuales con IAM Identity Center de AWS o Identity and Access Management (IAM) de .AWS De esta manera, solo se otorgan a cada usuario los permisos necesarios para cumplir sus obligaciones laborales. También recomendamos proteger sus datos de la siguiente manera:

- Utiliza la autenticación multifactor (MFA) en cada cuenta.
- Utiliza SSL/TLS para comunicarse con los recursos de AWS. Exigimos TLS 1.2 y recomendamos TLS 1.3.
- Configure el registro de la actividad del usuario y la API con AWS CloudTrail. Para obtener información sobre cómo utilizar registros de seguimiento de CloudTrail para capturar actividades de AWS, consulte Trabajo con los seguimientos de CloudTrail en la Guía del usuario de CloudTrail de AWS.
- Utilice las soluciones de cifrado de AWS, junto con todos los controles de seguridad predeterminados dentro de los servicios de AWS.
- Utiliza servicios de seguridad administrados avanzados, como Amazon Macie, que lo ayuden a detectar y proteger la información confidencial almacenada en Amazon S3.
- Si necesita módulos criptográficos validados FIPS 140-3 al acceder a AWS a través de una interfaz de la línea de comandos o una API, utiliza un punto de conexión de FIPS. Para obtener

más información sobre los puntos de conexión de FIPS disponibles, consulte Estándar de procesamiento de la información federal (FIPS) 140-3.

Se recomienda encarecidamente no introducir nunca información confidencial o sensible, como por ejemplo, direcciones de correo electrónico de clientes, en etiquetas o campos de formato libre, tales como el campo Nombre. Esto incluye los casos en los que trabaje con el terminal de transferencia de datos u otros servicios de AWS mediante la consola, la API, la CLI de AWS o los SDK de AWS. Cualquier dato que introduzca en etiquetas o campos de formato libre utilizados para los nombres se pueden emplear para los registros de facturación o diagnóstico. Si proporciona una URL a un servidor externo, recomendamos encarecidamente que no incluya información de credenciales en la URL a fin de validar la solicitud para ese servidor.

Cifrado de datos

El terminal de transferencia de datos de AWS proporciona acceso a una conexión de red de alta velocidad para que pueda transferir datos de forma segura entre sistemas de almacenamiento autogestionados y servicios de almacenamiento de AWS. La forma en que se cifran los datos de almacenamiento en tránsito depende de los datos de almacenamiento en tránsito. La administración de los datos y su cifrado en tránsito son responsabilidad de la persona que utiliza el terminal de transferencia de datos.

Cifrado en reposo

El terminal de transferencia de datos de AWS cifra todos los datos en reposo.

El terminal de transferencia de datos solo captura los datos necesarios para las reservas, incluidos los nombres, apellidos y direcciones de correo electrónico de las personas especificadas para asistir y programar la reserva. El objetivo de esta recopilación de datos es confirmar los detalles de la reserva y garantizar el acceso a la sala para llevar a cabo la transferencia de datos. Esta información transaccional no se guarda durante más de 35 días; sin embargo, la información de la cuenta de AWS se conserva durante 10 años.

Cifrado en tránsito

El terminal de transferencia de datos de AWS no cifra los datos en tránsito. Los datos se cifran en tránsito cuando se interactúa con los puntos de conexión de la API del terminal de transferencia de datos para configurar los equipos de transferencia, agregar personal y programar reservas en la consola. Como parte del modelo de responsabilidad compartida de AWS, puede elegir cómo conectarse a los servicios de AWS a través del terminal de transferencia de datos. Le

recomendamos que elija conectarse a los servicios de AWS mediante el cifrado en tránsito sólido, como TLS 1.2 y 1.3.

Por ejemplo, utilice solo conexiones cifradas a través de HTTPS (TLS) mediante la condición aws:SecureTransport en las políticas de bucket de Amazon S3, como se ilustra en la política de bucket a continuación.

Para obtener más información sobre el cifrado de datos en tránsito con otros servicios de AWS, como Amazon S3, consulte Protección de los datos con el cifrado del servidor en la Guía del usuario de Amazon S3.

Administración de claves

El terminal de transferencia de datos de AWS no admite directamente las claves administradas por el cliente. Utilice la compatibilidad con claves administradas por el cliente disponible para los servicios de AWS a los que se conecte durante la reserva del terminal de transferencia de datos. Obtenga más información sobre las claves administradas por el cliente y cómo cifrar sus datos en reposo en la sección Claves de AWS KMS de la Guía para desarrolladores de AWS Key Management Service.

Privacidad del tráfico entre redes

El acceso a la consola del terminal de transferencia de datos se realiza a través de las API de servicio publicadas. Los recursos del terminal de transferencia de datos son independientes de la nube privada virtual (VPC).

Administración de identidades y accesos para el terminal de transferencia de datos

AWS Identity and Access Management (IAM) es un servicio de AWS que ayuda a los administradores a controlar de forma segura el acceso a los recursos de AWS. Los administradores de IAM controlan a qué personas se las puede autenticar (pueden iniciar sesión) y autorizar (tienen permisos) para utilizar recursos del terminal de transferencia de datos. IAM es un servicio de AWS que puede utilizar sin cargo adicional.

Temas

- Administración del acceso con políticas
- Cómo funciona el terminal de transferencia de datos con IAM

Público

La forma en que utilice Identity and Access Management (IAM) de AWS varía en función del trabajo que realice en el terminal de transferencia de datos.

Usuario de servicio: si utiliza el servicio del terminal de transferencia de datos para realizar su trabajo, su administrador le proporciona las credenciales y los permisos que necesita. A medida que utilice más características del terminal de transferencia de datos para realizar el trabajo, es posible que necesite permisos adicionales. Entender cómo se administra el acceso puede ayudarlo a solicitar los permisos correctos al administrador. Si no puede acceder a una característica en el terminal de transferencia de datos, consulte Solución de problemas de identidad y acceso del terminal de transferencia de datos de AWS.

Administrador de servicio: si está a cargo de los recursos del terminal de transferencia de datos de la empresa, probablemente tenga acceso completo al terminal de transferencia de datos. Su trabajo consiste en determinar a qué características y recursos del terminal de transferencia de datos deben acceder sus usuarios del servicio. Luego, debe enviar solicitudes a su administrador de IAM para cambiar los permisos de los usuarios de su servicio. Revise la información de esta página para conocer los conceptos básicos de IAM. Para obtener más información acerca de cómo su empresa puede utilizar la IAM con el terminal de transferencia de datos, consulte Cómo funciona el terminal de transferencia de datos con IAM.

Administrador de IAM: si es un administrador de IAM, es posible que desee obtener información sobre cómo escribir políticas para administrar el acceso al terminal de transferencia de datos. Para ver las políticas basadas en la identidad del terminal de transferencia de datos de ejemplo que puede utilizar en IAM, consulte Ejemplos de políticas basadas en la identidad para el terminal de transferencia de datos de AWS.

Autenticación con identidades

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

Puede iniciar sesión en AWS como una identidad federada mediante las credenciales proporcionadas a través de una fuente de identidad. AWS Los usuarios del Centro de identidades

de IAM, 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, su administrador habrá configurado previamente la federación de identidades mediante roles de IAM. Cuando accede a AWS mediante la federación, está asumiendo un rol de forma indirecta.

Según el tipo de usuario que sea, puede iniciar sesión en la Consola de administración de AWS o en el portal de acceso de AWS. Para obtener más información sobre el inicio de sesión en AWS, consulte Cómo iniciar sesión en su cuenta de AWS en la Guía del usuario de inicio de sesión de AWS.

Si accede a AWS mediante programación, AWS proporciona un kit de desarrollo de software (SDK) y una interfaz de la línea de comandos (CLI) para firmar criptográficamente las solicitudes mediante el uso de las credenciales. Si no usa las herramientas de AWS, debe firmar las solicitudes. Para obtener más información sobre la firma de solicitudes, consulte AWSSignature Versión 4 para solicitudes API en la Guía del usuario de IAM.

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

Usuario raíz de la cuenta de AWS

Cuando se crea una cuenta de AWS, se comienza con una identidad de inicio de sesión que tiene acceso completo a todos los servicios y recursos de AWS de la cuenta. Esta identidad recibe el nombre de usuario raíz de la cuenta de AWS y se accede a ella iniciando sesión con la dirección de email y la contraseña que utilizó para crear la cuenta. Recomendamos encarecidamente que no utilice el usuario raíz para sus tareas diarias. Proteja las credenciales del Usuario raíz y utilícelas solo para las tareas que solo el Usuario raíz pueda realizar. Para ver la lista completa de las tareas que requieren que inicie sesión como usuario raíz, consulta Tareas que requieren credenciales de usuario raíz en la Guía del usuario de IAM.

Identidad federada

Como práctica recomendada, solicite que los usuarios humanos, incluidos los que requieren acceso de administrador, utilicen la federación con un proveedor de identidad para acceder a los servicios de AWS utilizando credenciales temporales.

Una identidad federada es un usuario del directorio de usuarios de su empresa, un proveedor de identidades web, AWS Directory Service, el directorio de Identity Center o cualquier usuario que acceda a los servicios de AWS con credenciales proporcionadas a través de un origen de identidades. Cuando identidades federadas acceden a AWS, asumen roles y los roles proporcionan credenciales temporales.

Para una administración de acceso centralizada, le recomendamos que utilice AWS IAM Identity Center. Puede crear usuarios y grupos en IAM Identity Center o puede conectarse y sincronizarse con un conjunto de usuarios y grupos de su propio origen de identidades para usarlos en todas sus cuentas y aplicaciones de AWS. Para obtener más información sobre IAM Identity Center, consulte ¿Qué es IAM Identity Center? en la Guía del usuario de IAM Identity Center de AWS.

Usuarios y grupos de IAM

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

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

Los usuarios son diferentes de los roles. Un usuario se asocia exclusivamente a una persona o aplicación, pero la intención es que cualquier usuario pueda asumir un rol que necesite. Los usuarios tienen credenciales de larga duración permanentes; no obstante, los roles proporcionan credenciales temporales. Para obtener más información, consulte Casos de uso para usuarios de IAM en la Guía del usuario de IAM.

IAM roles

Un rol de IAM es una identidad dentro de su cuenta de AWS que dispone de permisos específicos. Es similar a un usuario de IAM, pero no está asociado a una determinada persona. Para asumir temporalmente un rol de IAM en la consola de administración de AWS, puede cambiar de un usuario

a un rol de IAM (consola). Puede asumir un rol realizando una llamada a una operación de la CLI de AWS o de la API de AWS, o bien utilizando una URL personalizada. Para más información sobre los métodos para el uso de roles, consulta Métodos para asumir un rol en la Guía del usuario de IAM.

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

- Acceso de usuario federado: para asignar permisos a una identidad federada, puede crear un rol y definir 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 acerca de roles de federación, consulte Crear un rol para un proveedor de identidad de terceros (federación) en la Guía de usuario de IAM. Si utiliza el IAM Identity Center, debe configurar un conjunto de permisos. IAM Identity Center correlaciona el conjunto de permisos con un rol en IAM para controlar a qué puede acceder las identidades después de autenticarse. Para obtener más información sobre los conjuntos de permisos, consulte Conjuntos de permisos en la Guía del usuario de AWS IAM Identity Center.
- Permisos de usuario de IAM temporales: un usuario de IAM puede asumir un rol de IAM para recibir temporalmente permisos distintos que le permitan realizar una tarea concreta.
- Acceso entre cuentas: puede utilizar un rol de IAM para permitir que alguien (una entidad principal de confianza) de otra cuenta acceda a los recursos de la cuenta. Los roles son la forma principal de conceder acceso entre cuentas. Sin embargo, con algunos servicios de AWS, puede asociar una política directamente a un recurso (en lugar de utilizar un rol como proxy). Para obtener información acerca de la diferencia entre los roles y las políticas basadas en recursos para el acceso entre cuentas, consulta Acceso a recursos entre cuentas en IAM en la Guía del usuario de IAM.
- Acceso entre servicios: algunos servicios de AWS utilizan características de otros servicios de AWS. Por ejemplo, cuando realiza una llamada en un servicio, es común que ese servicio ejecute aplicaciones en Amazon EC2 o almacene objetos en Amazon S3. Es posible que un servicio haga esto usando los permisos de la entidad principal, usando un rol de servicio o usando un rol vinculado a un servicio.
  - Reenviar sesiones de acceso (FAS): cuando utiliza un rol o un usuario de IAM para llevar a cabo las acciones en AWS, se le considera una entidad principal. Cuando utiliza algunos servicios, es posible que realice una acción que desencadene otra acción en un servicio diferente. FAS utiliza los permisos de la entidad principal para llamar a un servicio deAWS, combinados con el servicio de AWS solicitante para realizar solicitudes a servicios posteriores. Las solicitudes de FAS solo se realizan cuando un servicio recibe una solicitud que requiere interacciones con otros servicios o recursos de AWS para completarse. En este caso, debe tener permisos para realizar ambas

acciones. Para obtener información sobre las políticas a la hora de realizar solicitudes de FAS, consulte Reenviar sesiones de acceso.

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

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

Administración del acceso con políticas

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

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

De forma predeterminada, los usuarios y los roles no tienen permisos. Un administrador de IAM puede crear políticas de IAM para conceder permisos a los usuarios para realizar acciones en los

recursos que necesitan. A continuación, el administrador puede añadir las políticas de IAM a roles y los usuarios pueden asumirlos.

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

Políticas basadas en identidades

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

Las políticas basadas en 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 asociar a varios usuarios, grupos y roles de su cuenta de AWS. Las políticas administradas incluyen las políticas administradas de AWS y las políticas administradas por el cliente. Para obtener más información sobre cómo elegir una política administrada o una política insertada, consulte Elegir entre políticas administradas y políticas insertadas en la Guía del usuario de IAM.

Políticas basadas en recursos

Las políticas basadas en recursos son documentos de política JSON que se asocian a un recurso. Los ejemplos de políticas basadas en recursos son las políticas de confianza de roles de IAM y las políticas de bucket de Amazon S3. En los servicios que admiten políticas basadas en recursos, los administradores de servicios pueden utilizarlos para controlar el acceso a un recurso específico. Para el recurso al que se 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 basada en recursos. Las entidades principales pueden incluir cuentas, usuarios, roles, usuarios federados o servicios de AWS.

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

Listas de control de acceso (ACL)

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

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

Otros tipos de políticas

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

- Límites de permisos: un límite de permisos es una característica avanzada que le permite establecer los permisos máximos que una política basada en identidad puede conceder a una entidad de IAM (usuario o rol de IAM). Puede establecer un límite de permisos para una 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 Límites de permisos para las entidades de IAM en la Guía del usuario de IAM.
- Políticas de control de servicios (SCP): las SCP son políticas JSON que especifican los permisos máximos para una organización o unidad organizativa (OU) en AWS Organizations. AWS Organizations es un servicio que le permite agrupar y administrar de forma centralizada varias cuentas de AWS que posee su negocio. Si habilita todas las características en una organización, entonces podrá aplicar políticas de control de servicio (SCP) a una o a todas sus cuentas. Las SCP limitan los permisos de las entidades de las cuentas miembro, incluido cada usuario raíz de la cuenta de AWS. Para obtener más información acerca de SCP y Organizations, consulte Políticas de control de servicios en la Guía del usuario de AWS.
- Políticas de control de recursos (RCP): las RCP son políticas JSON que permiten establecer los permisos máximos disponibles para los recursos de las cuentas sin actualizar las políticas de IAM asociadas a cada recurso que posea. La RCP limita los permisos de los recursos en las cuentas de miembros y puede afectar a los permisos efectivos de las identidades, incluidos los usuarios raíz de la cuenta de AWS, independientemente de si pertenecen a su organización. Para obtener más información sobre Organizations y RCP, incluida una lista de los servicios de AWS

que admiten RCP, consulte las Políticas de control de recursos (RCP) en la Guía del usuario de Organizations de AWS.

- Políticas de sesión: las políticas de sesión son políticas avanzadas que se pasan como parámetro cuando se crea una sesión temporal mediante programación para un rol o un usuario federado. Los permisos de la sesión resultantes son la intersección de las políticas basadas en identidad del rol y las políticas de la sesión. Los permisos también pueden proceder de una política basada en recursos. Una denegación explícita en cualquiera de estas políticas anulará el permiso. Para más información, consulte Políticas de sesión en la Guía del usuario de IAM.

Varios tipos de políticas

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

Cómo funciona el terminal de transferencia de datos con IAM

Antes de utilizar IAM para administrar el acceso al terminal de transferencia de datos, obtenga información sobre qué características de IAM se encuentran disponibles con el terminal de transferencia de datos.

Característica de IAM	Compatibilidad con el terminal de transferencia de datos
Políticas basadas en identidades	Sí
Políticas basadas en recursos	No
Acciones de políticas	Sí
Recursos de políticas	Sí
Claves de condición de política	Sí
ACL	No
ABAC (etiquetas en políticas)	No

Característica de IAM	Compatibilidad con el terminal de transferencia de datos
Credenciales temporales	Sí
Permisos de entidades principales	No
Roles de servicio	No
Roles vinculados al servicio	No

Para obtener una perspectiva general sobre cómo funcionan el terminal de transferencia de datos y otros productos de AWS con la mayoría de las características de IAM, consulte Servicios de AWS que funcionan con IAM en la Guía del usuario de IAM.

Políticas basadas en identidades para el terminal de transferencia de datos

Compatibilidad con las políticas basadas en identidad: sí

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

Con las políticas basadas en identidades de IAM, puede especificar las acciones y los recursos permitidos o denegados, así como las condiciones en las que se permiten o deniegan las acciones. No es posible especificar la entidad principal en una política basada en identidad porque se aplica al usuario o rol al que está asociada. Para obtener más información sobre los elementos que puede utilizar en una política de JSON, consulte Referencia de los elementos de la política de JSON de IAM en la Guía del usuario de IAM.

Ejemplos de políticas basadas en identidades para el terminal de transferencia de datos

Para ver ejemplos de políticas basadas en identidades del terminal de transferencia de datos, consulte Ejemplos de políticas basadas en identidades del terminal de transferencia de datos de AWS.

Políticas basadas en recursos del terminal de transferencia de datos

Admite políticas basadas en recursos: no

Las políticas basadas en recursos son documentos de política JSON que se asocian a un recurso. Los ejemplos de políticas basadas en recursos son las políticas de confianza de roles de IAM y las políticas de bucket de Amazon S3. En los servicios que admiten políticas basadas en recursos, los administradores de servicios pueden utilizarlos para controlar el acceso a un recurso específico. Para el recurso al que se 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 basada en recursos. Las entidades principales pueden incluir cuentas, usuarios, roles, usuarios federados o servicios de AWS.

Para habilitar el acceso entre cuentas, puedes especificar toda una cuenta o entidades de IAM de otra cuenta como la entidad principal de una política en función de recursos. Añadir a una política en función de recursos una entidad principal entre cuentas es solo una parte del establecimiento de una relación de confianza. Cuando la entidad principal y el recurso se encuentran en cuentas de AWS diferentes, un administrador de IAM de la cuenta de confianza también debe conceder a la entidad principal (usuario o rol) permiso para acceder al recurso. Para conceder el permiso, adjunte la entidad a una política basada en identidad. Sin embargo, si la política basada en recursos concede acceso a una entidad principal de la misma cuenta, no es necesaria una política basada en identidad adicional. Para obtener más información, consulte Acceso a recursos entre cuentas en IAM en la Guía del usuario de IAM.

Acciones de políticas para el terminal de transferencia de datos

Compatibilidad con las acciones de políticas: sí

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

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

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

Para ver una lista de las acciones del terminal de transferencia de datos, consulte Acciones definidas por el terminal de transferencia de datos de AWS en la Referencia de autorizaciones de servicio.

En las acciones de políticas del terminal de transferencia de datos, se utiliza el siguiente prefijo antes de la acción:

```
datatransferterminal
```

Para especificar varias acciones en una única instrucción, sepárelas con comas.

```
"Action": [
      "datatransferterminal:action1",
      "datatransferterminal:action2"
         ]
```

Para ver ejemplos de políticas basadas en identidades del terminal de transferencia de datos, consulte Ejemplos de políticas basadas en identidades del terminal de transferencia de datos de AWS.

Recursos de políticas para el terminal de transferencia de datos

Compatibilidad con los recursos de políticas: sí

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

El elemento `Resource` de la política JSON especifica el objeto u objetos a los que se aplica la acción. Las instrucciones deben contener un elemento `Resource` o `NotResource`. Como práctica recomendada, especifique un recurso utilizando el Nombre de recurso de Amazon (ARN). Puede hacerlo para acciones que admitan un tipo de recurso específico, conocido como permisos de nivel de recurso.

Para las acciones que no admiten permisos de nivel de recurso, como las operaciones de descripción, utilice un carácter asterisco (*) para indicar que la instrucción se aplica a todos los recursos.

```
"Resource": "*"
```

Para ver una lista de tipos de recursos del terminal de transferencia de datos y sus ARN, consulte Recursos definidos por el terminal de transferencia de datos de AWS en la Referencia de

autorizaciones de servicio. Para obtener información acerca de las acciones con las que puede especificar el ARN de cada recurso, consulte Acciones definidas por el terminal de transferencia de datos de AWS.

Para ver ejemplos de políticas basadas en identidades del terminal de transferencia de datos, consulte Ejemplos de políticas basadas en identidades del terminal de transferencia de datos de AWS.

Claves de condición de políticas para el terminal de transferencia de datos

Compatibilidad con claves de condición de políticas específicas del servicio: sí

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

El elemento `Condition` (o elemento `Condition`*`block`*`) lets you specify conditions in which a statement is in effect. The `Condition`) es opcional. Puedes crear expresiones condicionales que utilizan operadores de condición, tales como igual o menor que, para que la condición de la política coincida con los valores de la solicitud.

Si especifica varios elementos de `Condition` en una instrucción o varias claves en un único elemento de `Condition`, AWS las evalúa mediante una operación `AND` lógica. Si especifica varios valores para una única clave de condición, AWS evalúa la condición con una operación lógica `OR`. Se deben cumplir todas las condiciones antes de que se concedan los permisos de la instrucción.

También puedes utilizar variables de marcador de posición al especificar condiciones. Por ejemplo, puedes conceder un permiso de usuario de IAM para acceder a un recurso solo si está etiquetado con su nombre de usuario de IAM. Para más información, consulte Elementos de la política de IAM: variables y etiquetas en la Guía del usuario de IAM.

AWS admite claves de condición globales y claves de condición específicas del servicio. Para ver todas las claves de condición globales de AWS, consulte Claves de contexto de condición globales de AWS en la Guía del usuario de IAM.

Para ver una lista de las claves de condición del terminal de transferencia de datos, consulte Claves de condición del terminal de transferencia de datos de AWS en la Referencia de autorizaciones de servicio. Para obtener más información acerca de las acciones y los recursos con los que puede utilizar una clave de condición, consulte Acciones definidas por el terminal de transferencia de datos de AWS.

Para ver ejemplos de políticas basadas en identidades del terminal de transferencia de datos, consulte Ejemplos de políticas basadas en identidades del terminal de transferencia de datos de AWS.

ACL en el terminal de transferencia de datos

Compatibilidad con ACL: no

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

ABAC con el terminal de transferencia de datos

Compatibilidad con ABAC (etiquetas en las políticas): no

El control de acceso basado en atributos (ABAC) es una estrategia de autorización que define permisos en función de atributos. En AWS, estos atributos se denominan etiquetas. Se puedes adjuntar etiquetas a entidades de IAM (usuarios o roles) y a muchos recursos de AWS. El etiquetado de entidades y recursos es el primer paso de ABAC. A continuación, designe las políticas de ABAC para permitir operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso al que se intenta acceder.

ABAC es útil en entornos que crecen con rapidez y ayuda en situaciones en las que la administración de las políticas resulta engorrosa.

Para controlar el acceso en función de etiquetas, debe proporcionar información de las etiquetas en el elemento de condición de una política mediante `aws:ResourceTag/[replaceable]key-name ``, , or aws:TagKeys condition keys.` Si un servicio admite las tres claves de condición para cada tipo de recurso, el valor es Sí para el servicio. Si un servicio admite las tres claves de condición solo para algunos tipos de recursos, el valor es Parcial. Para obtener más información sobre ABAC, consulte Definición de permisos con la autorización de ABAC en la Guía del usuario de IAM. Para ver un tutorial con los pasos para configurar ABAC, consulte Uso del control de acceso basado en atributos (ABAC) en la Guía del usuario de IAM.

Uso de credenciales temporales con el terminal de transferencia de datos

Compatibilidad con credenciales temporales: sí

Algunos servicios de AWS no funcionan cuando inicia sesión con credenciales temporales. Para obtener información adicional, incluida la información sobre qué servicios de AWS funcionan con

credenciales temporales, consulte Servicios de AWS que funcionan con IAM en la Guía del usuario de IAM.

Utiliza credenciales temporales si inicia sesión en la consola de administración de AWS con cualquier método, excepto un nombre de usuario y una contraseña. Por ejemplo, cuando accede a AWS utilizando el enlace de inicio de sesión único (SSO) de la empresa, ese proceso crea automáticamente credenciales temporales. También crea credenciales temporales de forma automática cuando inicia sesión en la consola como usuario y luego cambia de rol. Para obtener más información sobre el cambio de roles, consulte Cambio de un usuario a un rol de IAM (consola) en la Guía del usuario de IAM.

Puede crear credenciales temporales de forma manual mediante la AWS CLI o la API de AWS. A continuación, puedes usar esas credenciales temporales para acceder a AWS. AWS recomienda generar credenciales temporales de forma dinámica en lugar de usar claves de acceso a largo plazo. Para obtener más información, consulte Credenciales de seguridad temporales en IAM.

Permisos de entidades principales entre servicios del terminal de transferencia de datos

Compatibilidad con las sesiones de acceso directo (FAS): no

Cuando utiliza un usuario o un rol de IAM para llevar a cabo acciones en AWS, se le considera una entidad principal. Cuando utiliza algunos servicios, es posible que realice una acción que desencadene otra acción en un servicio diferente. FAS utiliza los permisos de la entidad principal para llamar a un servicio deAWS, combinados con el servicio de AWS solicitante para realizar solicitudes a servicios posteriores. Las solicitudes de FAS solo se realizan cuando un servicio recibe una solicitud que requiere interacciones con otros servicios o recursos de AWS para completarse. En este caso, debe tener permisos para realizar ambas acciones. Para obtener información sobre las políticas a la hora de realizar solicitudes de FAS, consulte Reenviar sesiones de acceso.

Roles de servicio para el terminal de transferencia de datos

Compatible con roles de servicio: No

Un rol de servicio es un rol de IAM que asume un servicio para realizar acciones en su nombre. Un administrador de IAM puedes crear, modificar y eliminar un rol de servicio desde IAM. Para obtener más información, consulte Creación de un rol para delegar permisos a un servicio de AWS en la Guía del usuario de IAM.

> **Warning**
>
> Cambiar los permisos de un rol de servicio podría interrumpir la funcionalidad del terminal de transferencia de datos. Edite los roles de servicio solo cuando el terminal de transferencia de datos proporcione orientación para hacerlo.

Roles vinculados a servicios para el terminal de transferencia de datos

Compatibilidad con roles vinculados al servicio: no

Una función vinculada a un servicio es un tipo de función del servicio que está vinculado a un servicio de AWS. El servicio puede asumir el rol para realizar una acción en su nombre. Los roles vinculados a servicios aparecen en la cuenta de AWS y son propiedad del servicio. Un administrador de IAM puede ver, pero no editar, los permisos de los roles vinculados a servicios.

Para más información sobre cómo crear o administrar roles vinculados a servicios, consulta Servicios de AWS que funcionan con IAM. Busque un servicio en la tabla que incluya `Yes` en la columna Rol vinculado a un servicio. Seleccione el vínculo Sí para ver la documentación acerca del rol vinculado a servicios para ese servicio.

Ejemplos de políticas basadas en identidades para el terminal de transferencia de datos de AWS

De forma predeterminada, los usuarios y roles no tienen permiso para crear ni modificar los recursos del terminal de transferencia de datos. Tampoco pueden llevar a cabo tareas mediante la consola de administración de AWS, la interfaz de la línea de comandos AWS (CLI de AWS) ni la API de AWS. Un administrador de IAM puede crear políticas de IAM para conceder permisos a los usuarios para realizar acciones en los recursos que necesitan. A continuación, el administrador puede añadir las políticas de IAM a roles y los usuarios pueden asumirlos.

Para obtener información acerca de cómo crear una política basada en identidades de IAM mediante el uso de estos documentos de políticas JSON de ejemplo, consulte Creación de políticas de IAM (consola) en la Guía del usuario de IAM.

Para obtener más información sobre las acciones y los tipos de recursos definidos por , incluido el formato de los ARN para cada tipo de recurso, consulte Acciones, en la Referencia de autorizaciones de servicio.

Temas

Prácticas recomendadas sobre las políticas

Las políticas basadas en identidades determinan si alguien puede crear, eliminar o acceder a los recursos del terminal de transferencia de datos de la 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 administradas por AWS y continúe con los permisos de privilegio mínimo: a fin de comenzar a conceder permisos a los usuarios y las cargas de trabajo, utilice las políticas administradas por AWS, que conceden permisos para muchos casos de uso comunes. Están disponibles en su cuenta de AWS. Se recomienda definir políticas administradas por el cliente de AWS específicas para sus casos de uso a fin de reducir aún más los permisos. Con el fin de obtener más información, consulte las políticas administradas por AWS o las políticas administradas por AWS para funciones de tarea en la Guía de usuario de IAM.
- Aplique permisos de privilegio mínimo: cuando establezca permisos con políticas de IAM, conceda solo los permisos necesarios para realizar una tarea. Para ello, debe definir las acciones que se pueden llevar a cabo en determinados recursos en condiciones específicas, también conocidos como permisos de privilegios mínimos. Con el fin de obtener más información sobre el uso de IAM para aplicar permisos, consulte Políticas y permisos en IAM en la Guía del usuario de IAM.
- Utilice condiciones en las políticas de IAM para restringir aún más el acceso: puede agregar una condición a sus políticas para limitar el acceso a las acciones y los recursos. Por ejemplo, puede escribir una condición de políticas para especificar que todas las solicitudes deben enviarse utilizando SSL. También puede usar condiciones para conceder acceso a acciones de servicios si se emplean a través de un servicio determinado de AWS como, por ejemplo, AWS CloudFormation. Para obtener más información, consulte Elementos de la política de JSON de IAM: Condición en la Guía del usuario de IAM.
- Utiliza el analizador de acceso de IAM para validar las políticas de IAM con el fin de garantizar la seguridad y funcionalidad de los permisos: el analizador de acceso de IAM valida políticas nuevas y existentes para que respeten el lenguaje (JSON) de las políticas de IAM y las prácticas recomendadas de IAM. El analizador de acceso de IAM proporciona más de 100 verificaciones de políticas y recomendaciones procesables para ayudar a crear políticas seguras y funcionales. Para

más información, consulte Validación de políticas con el Analizador de acceso de IAM en la Guía del usuario de IAM.

- Solicite la autenticación multifactor (MFA): si se encuentra en una situación en la que necesita un usuario raíz o usuarios de IAM en su cuenta de AWS, active la MFA para mayor seguridad. Para exigir la MFA cuando se invoquen las operaciones de la API, añada condiciones de MFA a sus políticas. Para más información, consulte Acceso seguro a la API con MFA en la Guía del usuario de IAM.

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

Uso de la consola del terminal de transferencia de datos

Para acceder a la consola del terminal de transferencia de datos de AWS, debe tener un conjunto mínimo de permisos. Estos permisos deben permitirle registrar y consultar los detalles acerca de los recursos del terminal de transferencia de datos en su cuenta de AWS. Si crea una política basada en identidad que sea más restrictiva que el mínimo de permisos necesarios, la consola no funcionará del modo esperado para las entidades (usuarios o roles) que tengan esa política.

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

Para asegurarse de que los usuarios y los roles puedan seguir utilizando la consola del terminal de transferencia de datos, asocie también a las entidades la política `ConsoleAccess` o `ReadOnly` administrada por AWS del terminal de transferencia de datos. Para obtener más información, consulte Adición de permisos a un usuario en la Guía del usuario de IAM:

Cómo permitir a los usuarios consultar sus propios permisos

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

```
{
    "Version": "2012-10-17",
    "Statement": [
```

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

Solución de problemas de identidad y acceso del terminal de transferencia de datos de AWS

Utilice la siguiente información para diagnosticar y solucionar los problemas habituales que pueden surgir cuando se trabaja con el terminal de transferencia de datos e IAM.

Temas

- No tengo autorización para realizar una acción en el terminal de transferencia de datos
- Quiero permitir a personas externas a mi cuenta de AWS el acceso a mis recursos del terminal de transferencia de datos

No tengo autorización para realizar una acción en el terminal de transferencia de datos

Si no puede ver ni programar reservas en la consola del terminal de transferencia de datos de AWS, es posible que no tenga los permisos necesarios. Póngase en contacto con el administrador de su cuenta para configurar una política de identidad de IAM que le conceda el acceso y los permisos adecuados.

Quiero permitir a personas externas a mi cuenta de AWS el acceso a mis recursos del terminal de transferencia de datos

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

Para obtener más información, consulte lo siguiente:

- Para saber si el terminal de transferencia de datos admite estas características, consulte Cómo funciona el terminal de transferencia de datos con IAM.
- Para obtener información acerca de cómo proporcionar acceso a los recursos de las cuentas de AWS de su propiedad, consulte Proporcionar acceso a un usuario de IAM a otra cuenta de AWS de la que es propietario en la Guía del usuario de IAM.
- Para obtener información acerca de cómo proporcionar acceso a los recursos a cuentas de AWS de terceros, consulte Proporcionar acceso a cuentas de AWS que son propiedad de terceros en la Guía del usuario de IAM.
- Para obtener información sobre cómo proporcionar acceso mediante una federación de identidades, consulte Proporcionar acceso a usuarios autenticados externamente (identidad federada) en la Guía del usuario de IAM.
- Para conocer sobre la diferencia entre las políticas basadas en roles y en recursos para el acceso entre cuentas, consulte Acceso a recursos entre cuentas en IAM en la Guía del usuario de IAM.

Referencias de la API del terminal de transferencia de datos: acciones y recursos

Al crear políticas de Identity and Access Management (IAM) de AWS, esta página puede ayudarlo a comprender la relación entre las operaciones de API del terminal de transferencia de datos de AWS, las acciones correspondientes que puede conceder permisos para realizar y los recursos de AWS para los que puede conceder permiso.

En general, puede agregar los permisos del terminal de transferencia de datos a su política de la siguiente manera:

- Especifique acciones en el elemento `Action` El valor incluye un prefijo `datatransferterminal:` y el nombre de la operación de la API. Por ejemplo, `datatransferterminal:CreateTask`.
- Especifique un recurso AWS relacionado con la acción del elemento `Resource`.

También puede usar claves de condición de AWS en sus políticas del terminal de transferencia de datos. Para ver una lista completa de claves generales de AWS, consulte Claves disponibles en la Guía del usuario de IAM.

Operaciones de la API del terminal de transferencia de datos y acciones correspondientes

CreateTransferTeam

- Acción: `datatransferterminal:CreateTransferTeam`

  Recurso: `None`

GetTransferTeam

- Acción: `datatransferterminal:GetTransferTeam`

  Recurso: `arn:aws::$[replaceable]Partition:datatransferterminal:$[replaceable]Region:$[replaceable]Account:transfer-team/$[replaceable]TransferTeamId````

UpdateTransferTeam

- Acción: `datatransferterminal:UpdateTransferTeam`

  Recurso: `arn:aws::$[replaceable]Partition:datatransferterminal:$[replaceable]Region:$[replaceable]Account:transfer-team/$[replaceable]TransferTeamId````

DeleteTransferTeam

- Acción: `datatransferterminal:DeleteTransferTeam`

  Recurso: `arn:aws::$[replaceable]Partition:datatransferterminal:$[replaceable]Region:$[replaceable]Account:transfer-team/$[replaceable]TransferTeamId````

ListTransferTeams

- Acción: `datatransferterminal:ListTransferTeams`

  Recurso: None

RegisterPerson

- Acción: `datatransferterminal:RegisterPerson`

  Recurso: `arn:aws::$[replaceable]Partition:datatransferterminal:$[replaceable]Region:$[replaceable]Account:transfer-team/$[replaceable]TransferTeamId````

GetPerson

- Acción: `datatransferterminal:GetPerson`

  Recurso: `arn:aws::$[replaceable]Partition:datatransferterminal:$[replaceable]Region:$[replaceable]Account:transfer-team/$[replaceable]TransferTeamId/person/$[replaceable]PersonId````

  Acción dependiente: `datatransferterminal:GetTransferTeam`

  Recurso dependiente: `arn:aws::$[replaceable]Partition:datatransferterminal:$[replaceable]Region:$[replaceable]Account:transfer-team/$[replaceable]TransferTeamId````

DeregisterPerson

- Acción: `datatransferterminal:DeregisterPerson`

  Recurso: `arn:aws::$[replaceable]Partition:datatransferterminal:$[replaceable]Region:$[replaceable]Account:transfer-team/$[replaceable]TransferTeamId/person/$[replaceable]PersonId````

  Acción dependiente: `datatransferterminal:GetTransferTeam`

  Recurso dependiente: `arn:aws::$[replaceable]Partition:datatransferterminal:$[replaceable]Region:$[replaceable]Account:transfer-team/$[replaceable]TransferTeamId````

ListPersons

- Acción: `datatransferterminal:ListPersons`

Recurso: `arn:aws::$[replaceable]Partition:datatransferterminal:$[replaceable]Region:$[replaceable]Account:transfer-team/$[replaceable]TransferTeamId````

CreateReservation

- Acción: `datatransferterminal:CreateReservation`

  Recurso: `arn:aws::$[replaceable]Partition:datatransferterminal:$[replaceable]Region:$[replaceable]Account:transfer-team/$[replaceable]TransferTeamId````

  Acción dependiente: `datatransferterminal:GetTransferTeam`

  Recurso dependiente: `arn:aws::$[replaceable]Partition:datatransferterminal:$[replaceable]Region:$[replaceable]Account:transfer-team/$[replaceable]TransferTeamId````

  Acción dependiente: `datatransferterminal:GetPerson`

  Recurso dependiente: `arn:aws::$[replaceable]Partition:datatransferterminal:$[replaceable]Region:$[replaceable]Account:transfer-team/$[replaceable]TransferTeamId/person/$[replaceable]PersonId````

  Acción dependiente: `datatransferterminal:GetFacility`

  Recurso dependiente: `arn:aws::$[replaceable]Partition:datatransferterminal::facility/$[replaceable]FacilityId````

GetReservation

- Acción: `datatransferterminal:GetReservation`

  Recurso: `arn:aws::$[replaceable]Partition:datatransferterminal:$[replaceable]Region:$[replaceable]Account:transfer-team/$[replaceable]TransferTeamId/reservation/$[replaceable]ReservationId````

  Acción dependiente: `datatransferterminal:GetTransferTeam`

Recurso dependiente: `arn:aws::$[replaceable]Partition:datatransferterminal:$[replaceable]Region:$[replaceable]Account:transfer-team/$[replaceable]TransferTeamId````

UpdateReservation

- Acción: `datatransferterminal:UpdateReservation`

  Recurso: `arn:aws::$[replaceable]Partition:datatransferterminal:$[replaceable]Region:$[replaceable]Account:transfer-team/$[replaceable]TransferTeamId/reservation/$[replaceable]ReservationId````

  Acción dependiente: `datatransferterminal:GetTransferTeam`

  Recurso dependiente: `arn:aws::$[replaceable]Partition:datatransferterminal:$[replaceable]Region:$[replaceable]Account:transfer-team/$[replaceable]TransferTeamId````

  Acción dependiente: `datatransferterminal:GetPerson`

  Recurso dependiente: `arn:aws::$[replaceable]Partition:datatransferterminal:$[replaceable]Region:$[replaceable]Account:transfer-team/$[replaceable]TransferTeamId/person/$[replaceable]PersonId````

DeleteReservation

- Acción: `datatransferterminal:DeleteReservation`

  Recurso: `arn:aws::$[replaceable]Partition:datatransferterminal:$[replaceable]Region:$[replaceable]Account:transfer-team/$[replaceable]TransferTeamId/person/$[replaceable]PersonId````

  Acción dependiente: `datatransferterminal:GetTransferTeam`

  Recurso dependiente: `arn:aws::$[replaceable]Partition:datatransferterminal:$[replaceable]Region:$[replaceable]Account:transfer-team/$[replaceable]TransferTeamId````

ListReservations

- Acción: `datatransferterminal:ListReservations`

Recurso: `arn:aws::$[replaceable]Partition:datatransferterminal:$[replaceable]Region:$[replaceable]Account:transfer-team/$[replaceable]TransferTeamId````

ListFacilities

- Acción: `datatransferterminal:ListFacilities`

  Recurso: None

GetFacility

- Acción: `datatransferterminal:GetFacility`

  Recurso: `arn:aws::$[replaceable]Partition:datatransferterminal:::facility/$[replaceable]FacilityId````

GetFacilityAvailability

- Acción: `datatransferterminal:GetFacilityAvailability`

  Recurso: `arn:aws::$[replaceable]Partition:datatransferterminal:::facility/$[replaceable]FacilityId/availability`

  Acción dependiente: `datatransferterminal:GetFacility`

  Recurso dependiente: `arn:aws::$[replaceable]Partition:datatransferterminal:::facility/$[replaceable]FacilityId/availability`

Validación de conformidad para el terminal de transferencia de datos de AWS

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

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

Su responsabilidad de cumplimiento al utilizar servicios de AWS está determinada por la sensibilidad de sus datos, los objetivos de cumplimiento de su empresa y las leyes y las regulaciones aplicables. AWS proporciona los siguientes recursos para ayudar con el cumplimiento:

- Cumplimiento de seguridad y gobernanza: en estas guías se explican las consideraciones de arquitectura y se proporcionan pasos para implementar las características de seguridad y cumplimiento.
- Referencia de servicios válidos de HIPAA: muestra una lista con los servicios válidos de HIPAA. No todos los servicios de AWS son aptos para HIPAA.
- AWSRecursos de conformidad: este conjunto de manuales y guías podría aplicarse a su sector y ubicación.
- https://d1-awsstatic-com-whitepapers-compliance-AWS-Customer-Compliance-Guides-pdf[AWS Customer Compliance Guides]: comprenda el modelo de responsabilidad compartida desde el punto de vista del cumplimiento. Las guías resumen las prácticas recomendadas para garantizar la seguridad de los servicios de AWS y orientan los controles de seguridad en varios marcos (incluidos el Instituto Nacional de Estándares y Tecnología [NIST], el Consejo de Estándares de Seguridad de la Industria de Tarjetas de Pago [PCI] y la Organización Internacional de Normalización [ISO]).
- Evaluación de recursos con reglas en la guía para desarrolladores de AWS Config: el servicio AWS Config evalúa en qué medida las configuraciones de los recursos cumplen con las prácticas internas, las directrices del sector y las normativas.
- AWS Security Hub: este producto de AWS proporciona una visión completa de su estado de seguridad en AWS. Security Hub utiliza controles de seguridad para evaluar sus recursos de AWS y comprobar su cumplimiento con los estándares y las prácticas recomendadas del sector de la seguridad. Para obtener una lista de los servicios y controles compatibles, consulte la Referencia de controles de Security Hub.
- Amazon GuardDuty: este servicio de AWS detecta posibles amenazas para sus cuentas, cargas de trabajo, contenedores y datos de AWS mediante el monitoreo de su entorno para detectar actividades sospechosas y maliciosas. GuardDuty puede ayudarlo a satisfacer varios requisitos de conformidad, como PCI DSS, cumpliendo los requisitos de detección de intrusos que exigen determinados marcos de conformidad.
- AWS Audit Manager: este servicio de AWS le ayuda a auditar de manera continua su uso de AWS para simplificar la forma en que administra el riesgo y la conformidad con las regulaciones y los estándares del sector.

Resiliencia en el terminal de transferencia de datos de AWS

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

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

El terminal de transferencia de datos de AWS está disponible en todo el mundo. Puede conectarse a cualquier región de AWS que se pueda acceder desde Internet.

Registro y supervisión en el terminal de transferencia de datos

El terminal de transferencia de datos de AWS está integrado con CloudTrail de AWS, un servicio que brinda un registro de las acciones tomadas por un usuario, rol o un servicio de AWS en el terminal de transferencia de datos. CloudTrail captura todas las llamadas a la API para el terminal de transferencia de datos como eventos. Las llamadas capturadas incluyen las llamadas desde la consola del terminal de transferencia de datos y las llamadas de código hacia las operaciones de la API del terminal de transferencia de datos. Si crea un registro de seguimiento, puede habilitar la entrega continua de eventos de CloudTrail a un bucket de Amazon S3, incluidos los eventos para el terminal de transferencia de datos. Si no configura un registro de seguimiento, puede ver los eventos más recientes de la consola de CloudTrail en el Historial de eventos. Con la información recopilada por CloudTrail, puede determinar la solicitud que se ha realizado al terminal de transferencia de datos, la dirección IP desde la que se ha realizado la solicitud, quién la ha realizado, cuándo la ha realizado y los detalles adicionales.

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

Información del terminal de transferencia de datos en CloudTrail

CloudTrail se habilita en su cuenta de AWS cuando la crea. Cuando se produce una actividad en el terminal de transferencia de datos, dicha actividad se registra en un evento de CloudTrail junto

con los eventos de los demás servicios de AWS en Historial de eventos. Se puede ver, buscar y descargar los últimos eventos de la cuenta de AWS. Para más información, consulte Ver eventos con el historial de eventos de CloudTrail.

Para mantener un registro continuo de los eventos en su cuenta de AWS, incluidos los eventos del terminal de transferencia de datos, cree un seguimiento. Un registro de seguimiento permite a CloudTrail enviar archivos de registro a un bucket de Amazon S3. De manera predeterminada, cuando se crea un registro de seguimiento en la consola, el registro de seguimiento se aplica a todas las regiones de AWS. El registro de seguimiento registra los eventos de todas las regiones de la partición de AWS y envía los archivos de registro al bucket de Amazon S3 especificado. También es posible configurar otros servicios de AWS para analizar en profundidad y actuar en función de los datos de eventos recopilados en los registros de CloudTrail. Para más información, consulte los siguientes temas:

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

Todas las acciones del terminal de transferencia de datos están registradas por CloudTrail y documentadas en la sección Referencias de la API del terminal de transferencia de datos: acciones y recursos de esta guía.

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

- Si la solicitud se realizó con las credenciales raíz o las credenciales de usuario de Identity and Access Management (IAM) de AWS.
- Si la solicitud se realizó con credenciales de seguridad temporales de un rol o fue un usuario federado.
- Si la solicitud la realizó otro servicio de AWS.

Para obtener más información, consulte Elemento userIdentity de CloudTrail.

Descripción de las entradas del archivo de registro del terminal de transferencia de datos

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

La seguridad de la infraestructura en el terminal de transferencia de datos de AWS

Al tratarse de un servicio administrado, el terminal de transferencia de datos de AWS está protegido por los procedimientos de seguridad de red globales de AWS que se describen en el documento técnico {https---d0-awsstatic-com-whitepapers-Security-AWS-Security-Whitepaper-pdf}[Amazon Web Services: Overview of Security Processes].

Puede utilizar llamadas a la API publicadas en AWS para acceder al terminal de transferencia de datos a través de la red. Los clientes deben ser compatibles con la seguridad de la capa de transporte (TLS) 1.0 o una versión posterior. Recomendamos TLS 1.2 o una versión posterior. Los clientes también deben ser compatibles con conjuntos de cifrado con confidencialidad directa total (PFS) tales como DHE (Ephemeral Diffie-Hellman) o ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). La mayoría de los sistemas modernos como Java 7 y posteriores son compatibles con estos modos.

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

Historial de documentos para la Guía del usuario del terminal de transferencia de datos

En la siguiente tabla se describe el historial de documentos de esta guía.

Cambio	Descripción	Fecha
Actualización del diseño	Actualizaciones del diseño del documento y pequeñas modificaciones en la redacción y el contenido.	1 de enero de 2025
Publicación inicial	La fecha de lanzamiento de la documentación original.	1 de diciembre de 2024