Guía del usuario

AWS Artifact

AWS Artifact: Guía del usuario

Table of Contents

¿Qué es AWS Artifact?

AWS Artifact proporciona descargas bajo demanda de documentos de AWS seguridad y cumplimiento. Por ejemplo, informes sobre el cumplimiento de las normas de la Organización Internacional de Normalización (ISO) y las normas de seguridad del sector de tarjetas de pago (PCI), e informes sobre los controles de sistemas y organizaciones (SOC). AWS Artifact también proporciona descargas de certificaciones de organismos de acreditación que validan la implementación y la eficacia operativa de los controles de AWS seguridad.

También puede descargar documentos de seguridad y conformidad para los proveedores de software independientes (ISVs) que venden sus productos en AWS Marketplace. AWS Artifact Para obtener más información, consulte AWS Marketplace Vendor Insights.

Además, puede utilizarlos AWS Artifact para revisar, aceptar y realizar un seguimiento del estado de sus acuerdos con AWS usted Cuenta de AWS y con varios miembros Cuentas de AWS de su organización. Para obtener más información sobre los acuerdos en AWS Artifact vigor, consulteGestión de acuerdos en AWS Artifact.

Para demostrar la seguridad y el cumplimiento de la AWS infraestructura y los servicios que utiliza, puede enviar AWS Artifact los documentos a sus auditores o reguladores como artefactos de auditoría. También puede utilizar estos artefactos de auditoría como directrices para evaluar su propia arquitectura de nube y evaluar la eficacia de los controles internos de su empresa. Para obtener más información sobre los artefactos de auditoría, consulte AWS Artifact FAQs.

> **Note**
>
> AWS los clientes son responsables de desarrollar u obtener documentos que demuestren la seguridad y el cumplimiento de sus empresas. Para obtener más información, consulte el Modelo de responsabilidad compartida.

Precios

AWS le proporciona AWS Artifact documentos y acuerdos de forma gratuita.

Empezar con AWS Artifact

Para empezar a usarlo AWS Artifact, prueba sus funciones principales en la AWS Artifact consola. En la consola, puede descargar los informes AWS de seguridad y conformidad, descargar y aceptar acuerdos legales y suscribirse a las notificaciones sobre AWS Artifact los documentos.

Requisitos previos

Para utilizar las funciones de AWS Artifact, debe disponer de un Cuenta de AWS. Para obtener instrucciones de configuración, consulte Configurar una nueva Cuenta de AWS en la Guía del usuario de AWS configuración.

Características

Para obtener instrucciones sobre el uso de las funciones de AWS Artifact, consulte los temas siguientes:

- Descarga de informes
- Administración de acuerdos
- Configuración de notificaciones

Descarga de informes en AWS Artifact

Puede descargar los informes desde la AWS Artifact consola. Al descargar un informe desde AWS Artifact, el informe se genera específicamente para usted y cada informe tiene una marca de agua única. Por este motivo, solamente debe compartir los informes con las personas en las que confía. No envíe por correo electrónico los informes como archivos adjuntos y no los comparta online. Para compartir un informe, usa un servicio seguro para compartir, como Amazon WorkDocs. Algunos informes requieren que acepte los Términos y condiciones antes de poder descargarlos.

Contenido

Descarga de un informe

Para descargar un informe, debe contar con los permisos requeridos. Para obtener más información, consulte Gestión de identidad y acceso en AWS Artifact.

Cuando te registras AWS Artifact, tu cuenta recibe automáticamente permisos para descargar algunos informes. Si tiene problemas para acceder AWS Artifact, siga las instrucciones de la página de referencia AWS Artifact de autorizaciones de servicio.

Para descargar un informe

1. Abra la AWS Artifact consola en https://console.aws.amazon.com/artifact/.
2. En la página de AWS Artifact inicio, selecciona Ver informes.

   En la página Informes, en la pestaña AWS Informes, puede acceder a AWS los informes (por ejemplo, SOC 1/2/3PCI, C5, etc.). En la pestaña Informes de terceros, puedes acceder a los informes de proveedores de software independientes (ISVs) que venden sus productos en AWS Marketplace
3. (Opcional) Para buscar un informe, introduce una palabra clave en el campo de búsqueda. También puede realizar búsquedas específicas de informes en función de columnas

individuales, incluidos el título, la categoría, la serie y la descripción del informe. Por ejemplo, para buscar el informe del Catálogo de controles de conformidad informática en la nube (C5), puede buscar en la columna del título utilizando «Título», el operador «contiene» (:) y el término «C5" ()**`Title : C5`**.

4. (Opcional) Para obtener más información sobre un informe, elija el título del informe para abrir su página de detalles.
5. Seleccione un informe y, a continuación, elija Descargar informe.
6. Es posible que se le pida que acepte los términos y condiciones (Aceptar los términos para descargar el informe) del informe específico que va a descargar. Te recomendamos que leas detenidamente los términos y condiciones. Cuando termines de leer, selecciona He leído y acepto los términos y, a continuación, selecciona Aceptar los términos y descargar el informe.
7. Abre el archivo descargado a través de un PDF visor. Revise los términos y condiciones de aceptación y desplácese hacia abajo para encontrar el informe de auditoría. Los informes pueden incluir información adicional como archivos adjuntos en el PDF documento, así que asegúrese de comprobar si hay archivos adjuntos en el PDF archivo para obtener la documentación de respaldo. Para obtener instrucciones sobre cómo ver los archivos adjuntos, consulteVisualización de los archivos adjuntos de PDF los documentos.

Visualización de los archivos adjuntos de PDF los documentos

Recomendamos las siguientes aplicaciones que actualmente admiten la visualización de PDF archivos adjuntos:

Adobe Acrobat Reader

Descargue la última versión de Adobe Acrobat Reader desde el sitio web de Adobe en. https://get.adobe.com/reader/

Para obtener instrucciones sobre cómo ver los PDF archivos adjuntos en Acrobat Reader, consulte Enlaces y archivos adjuntos en el PDFs sitio web de soporte de Adobe.

Navegador Firefox

1. Descarga la última versión del navegador web Firefox desde el sitio web de Mozilla en https://www.mozilla. org/en-US/firefox/new/.
2. Abre el PDF archivo en el PDF visor integrado de Firefox. Para obtener instrucciones, consulta Ver PDF archivos en Firefox o elige otro visor en el sitio web de soporte de Mozilla.

3. Para ver PDF los archivos adjuntos en el PDF visor integrado de Firefox, selecciona Alternar barra lateral y mostrar archivos adjuntos.

Protección de los documentos

AWS Artifact los documentos son confidenciales y deben mantenerse seguros en todo momento. AWS Artifact utiliza el modelo de responsabilidad AWS compartida para sus documentos. Esto significa que AWS es responsable de mantener los documentos seguros mientras están en la AWS nube, pero usted es responsable de mantenerlos seguros después de descargarlos. AWS Artifact es posible que tengas que aceptar los términos y condiciones antes de poder descargar los documentos. Cada documento descargado tiene una marca de agua única que puede rastrearse.

Solo podrá compartir documentos marcados como confidenciales dentro de su empresa, con las autoridades reguladoras y con los auditores. No tiene permiso para compartir estos documentos con sus clientes o en su sitio web. Le recomendamos encarecidamente que utilice un servicio seguro para compartir documentos, como Amazon WorkDocs, para compartir documentos con otras personas. No envíe los documentos por correo electrónico ni los suba a un sitio que no sea seguro.

Resolución de problemas

Si no puede descargar un documento o recibir un mensaje de error, consulte Solución de problemas en AWS Artifact FAQ.

Gestión de acuerdos en AWS Artifact

Puede utilizarlos AWS Artifact para revisar y gestionar los acuerdos de su organización Cuenta de AWS o de su organización. Por ejemplo, las compañías que están sujetas a la Ley de Portabilidad y Responsabilidad de los Seguros de Salud (Health Insurance Portability and Accountability ActHIPAA) suelen requerir un acuerdo con un socio comercial (BAA) AWS para garantizar que la información de salud protegida (PHI) esté debidamente protegida. En la AWS Artifact consola, puede revisar y aceptar dichos acuerdos, y puede designar uno que pueda tramitarlos legalmente Cuenta de AWS . PHI

Si lo utilizas AWS Organizations, puedes aceptar acuerdos, como uno BAA con AWS, en nombre de todos los miembros Cuentas de AWS de tu organización. Todas las cuentas de los miembros existentes y posteriores quedan cubiertas automáticamente por el acuerdo y pueden tramitarse legalmentePHI.

También puede utilizarla AWS Artifact para confirmar que su organización Cuenta de AWS o su organización ha aceptado un acuerdo y para revisar los términos de un acuerdo aceptado a fin de comprender sus obligaciones. Si tu cuenta u organización ya no necesita usar un acuerdo aceptado, puedes usarlo AWS Artifact para rescindirlo. Si rescindes el acuerdo, pero más tarde te das cuenta de que lo necesitas, puedes volver a activarlo.

Contenido

¿Acepta acuerdos para usted Cuenta de AWS ? AWS Artifact

Puedes usar la AWS Artifact consola para revisar y aceptar acuerdos AWS por tu cuenta Cuenta de AWS.

> **Important**
>
> Antes de aceptar un acuerdo, le recomendamos que se ponga en contacto con su equipo jurídico, de privacidad y de conformidad.

Permisos necesarios

Si eres el administrador de una cuenta, puedes conceder a IAM los usuarios y a los usuarios federados los permisos para acceder a uno o varios de tus acuerdos y gestionarlos. De forma predeterminada, solo los usuarios con privilegios administrativos pueden aceptar un acuerdo. Para aceptar un acuerdo, IAM los usuarios federados deben tener los permisos necesarios.

Para obtener más información, consulte Gestión de identidad y acceso en AWS Artifact.

Para aceptar un acuerdo con AWS

1. Abre la AWS Artifact consola en https://console.aws.amazon.com/artifact/.
2. En el panel AWS Artifact de navegación, elija Acuerdos.
3. Elija la pestaña Account agreements (Acuerdos de la cuenta).
4. Abra la AWS Artifact consola en https://console.aws.amazon.com/artifact/.
5. En el panel de navegación, elija Acuerdos.
6. En la página Acuerdos, realice una de las siguientes acciones:
   - Para aceptar un acuerdo solo para su cuenta, seleccione la pestaña Acuerdos de cuenta.
   - Para aceptar un acuerdo en nombre de su organización, seleccione la pestaña Acuerdos organizativos.
7. Seleccione un acuerdo y, a continuación, elija Descargar acuerdo.

   Aparece el cuadro de diálogo Aceptar NDA la descarga del informe.
8. Antes de poder descargar el acuerdo que ha seleccionado, primero debe aceptar los términos del Acuerdo de AWS Artifact confidencialidad (AWS Artifact NDA).

   a. En el cuadro de diálogo Aceptar NDA la descarga del informe, revise la AWS Artifact NDA.

   b. (Opcional) Para imprimir una copia del AWS Artifact NDA (o guardarla comoPDF), seleccione Imprimir NDA.

   c. Selecciona He leído y acepto todos los términos delNDA.

   d. Para aceptar AWS Artifact NDA y descargar una PDF parte del acuerdo que seleccionaste, selecciona Aceptar NDA y descargar.

9. En un PDF visor, revisa el acuerdo PDF que descargaste.
10. En la AWS Artifact consola, con el acuerdo seleccionado, selecciona Aceptar acuerdo.
11. En el cuadro de diálogo Aceptar acuerdo, haga lo siguiente:

    a. Revise el acuerdo.

    b. Selecciona Acepto todos estos términos y condiciones.

    c. Selecciona Aceptar acuerdo.

12. Elija Aceptar para aceptar el acuerdo de su cuenta.

Rescisión de los acuerdos para su entrada Cuenta de AWSAWS Artifact

Si has utilizado la AWS Artifact consola para aceptar un contrato de pareja Cuenta de AWS, puedes utilizarla para rescindir ese contrato. De lo contrario, consulte Acuerdos fuera de línea en AWS Artifact.

Permisos necesarios

Para rescindir un acuerdo, IAM los usuarios federados deben disponer de los permisos necesarios.

Para obtener más información, consulte Gestión de identidad y acceso en AWS Artifact.

Para rescindir su acuerdo en línea con AWS

1. Abra la AWS Artifact consola en https://console.aws.amazon.com/artifact/.
2. En el panel AWS Artifact de navegación, elija Acuerdos.
3. Elija la pestaña Account agreements (Acuerdos de la cuenta).
4. Seleccione el acuerdo y elija Rescindir acuerdo.
5. Seleccione todas las casillas de verificación para indicar que acepta rescindir el acuerdo.
6. Elija Terminar. Cuando se le indique que confirme, elija Finalizar.

Aceptar acuerdos para su organización en AWS Artifact

Si eres el propietario de la cuenta de administración de una AWS Organizations organización, puedes aceptar un acuerdo AWS en nombre de todos los miembros Cuentas de AWS de la organización.

> **Important**
>
> Antes de aceptar un acuerdo, le recomendamos que se ponga en contacto con su equipo jurídico, de privacidad y de conformidad.

AWS Organizations tiene dos conjuntos de funciones disponibles: las funciones de facturación unificada y todas las funciones. AWS Artifact Para usarlo en su organización, la organización a la que pertenece debe tener habilitadas todas las funciones. Si su organización está configurada solo para la facturación unificada, consulte Habilitar todas las características en la organización en la Guía del usuario de AWS Organizations .

Para aceptar o rescindir los acuerdos de la organización, debe iniciar sesión en la cuenta de administración con los AWS Artifact permisos correctos. Los usuarios de las cuentas de los miembros que tienen `organizations:DescribeOrganization` permisos pueden ver los acuerdos organizativos que se aceptan en su nombre.

Para obtener más información, consulte Administrar las cuentas de una organización AWS Organizations en la Guía del AWS Organizations usuario.

Permisos necesarios

Para aceptar un acuerdo, el propietario de la cuenta de administración debe tener los permisos necesarios.

Para obtener más información, consulte Gestión de identidad y acceso en AWS Artifact.

Para aceptar un acuerdo de una organización

1. Abra la AWS Artifact consola en https://console.aws.amazon.com/artifact/.
2. En el AWS Artifact panel de control, selecciona Acuerdos.
3. Elija la pestaña Organization agreements (Acuerdos de la organización).
4. Abre la AWS Artifact consola en https://console.aws.amazon.com/artifact/.

5. En el panel de navegación, elija Acuerdos.
6. En la página Acuerdos, realice una de las siguientes acciones:
   - Para aceptar un acuerdo solo para su cuenta, seleccione la pestaña Acuerdos de cuenta.
   - Para aceptar un acuerdo en nombre de su organización, seleccione la pestaña Acuerdos organizativos.
7. Seleccione un acuerdo y, a continuación, elija Descargar acuerdo.

   Aparece el cuadro de diálogo Aceptar NDA la descarga del informe.
8. Antes de poder descargar el acuerdo que ha seleccionado, primero debe aceptar los términos del Acuerdo de AWS Artifact confidencialidad (AWS Artifact NDA).

   a. En el cuadro de diálogo Aceptar NDA la descarga del informe, revise la AWS Artifact NDA.
   b. (Opcional) Para imprimir una copia del AWS Artifact NDA (o guardarla comoPDF), seleccione Imprimir NDA.
   c. Selecciona He leído y acepto todos los términos delNDA.
   d. Para aceptar AWS Artifact NDA y descargar una PDF parte del acuerdo que seleccionaste, selecciona Aceptar NDA y descargar.
9. En un PDF visor, revisa el acuerdo PDF que descargaste.
10. En la AWS Artifact consola, con el acuerdo seleccionado, selecciona Aceptar acuerdo.
11. En el cuadro de diálogo Aceptar acuerdo, haga lo siguiente:

    a. Revise el acuerdo.
    b. Selecciona Acepto todos estos términos y condiciones.
    c. Selecciona Aceptar acuerdo.
12. Seleccione Aceptar para aceptar el acuerdo para todas las cuentas existentes y futuras de su organización.

Rescisión de los acuerdos de su organización en AWS Artifact

Si has utilizado la AWS Artifact consola para aceptar un acuerdo en nombre de todas las cuentas de los miembros de una organización AWS Organizations, puedes utilizarla para rescindir ese acuerdo. De lo contrario, consulte Acuerdos fuera de línea en AWS Artifact.

Si se elimina una cuenta de miembro de una organización, esa cuenta de miembro deja de estar cubierta por los acuerdos de la organización. Antes de eliminar las cuentas de los miembros de una

organización, el administrador de la cuenta de administración debe comunicárselo a las cuentas de los miembros para que puedan establecer nuevos acuerdos si es necesario. Puedes ver una lista de los acuerdos de la organización activos en la AWS Artifact consola de la página Acuerdos, en la sección Acuerdos de la organización.

Para obtener más información AWS Organizations, consulte Administrar las cuentas de una organización AWS Organizations en la Guía del AWS Organizations usuario.

Permisos necesarios

Para rescindir un acuerdo, el propietario de la cuenta de administración debe tener los permisos necesarios.

Para obtener más información, consulte Gestión de identidad y acceso en AWS Artifact.

Para rescindir su acuerdo de organización en línea con AWS

1. Abra la AWS Artifact consola en https://console.aws.amazon.com/artifact/.
2. En el AWS Artifact panel de control, selecciona Acuerdos.
3. Elija la pestaña Organization agreements (Acuerdos de la organización).
4. Seleccione el acuerdo y elija Rescindir acuerdo.
5. Seleccione todas las casillas de verificación para indicar que acepta rescindir el acuerdo.
6. Elija Terminar. Cuando se le indique que confirme, elija Finalizar.

Acuerdos fuera de línea en AWS Artifact

Si ya tiene un acuerdo sin conexión, AWS Artifact muestra los acuerdos que ha aceptado sin conexión. Por ejemplo, es posible que la consola muestre el apéndice para socios comerciales fuera de línea (BAA) con el estado Activo. El estado activa indica que el acuerdo se ha aceptado. Para rescindir un acuerdo sin conexión, consulte las directrices e instrucciones de rescisión incluidas con su acuerdo.

Si su cuenta es la cuenta de administración de una AWS Organizations organización, puede utilizarla AWS Artifact para aplicar los términos de su acuerdo de conexión sin conexión a todas las cuentas de la organización. Para aplicar un acuerdo que aceptaste sin conexión a tu organización y a todas las cuentas de la organización, debes tener los permisos necesarios.

Si tu cuenta es una cuenta de miembro de una organización, debes tener los permisos para ver los acuerdos organizativos sin conexión a Internet.

Para obtener más información, consulte Gestión de identidad y acceso en AWS Artifact.

Configuración de las notificaciones por correo electrónico en AWS Artifact

Puede usar la AWS Artifact consola para configurar las notificaciones por correo electrónico para las actualizaciones de los acuerdos y los informes AWS Artifact. AWS Artifact envía estas notificaciones por correo electrónico mediante AWS User Notifications. Para recibir notificaciones AWS Artifact por correo electrónico, primero debe seleccionar los centros de AWS User Notifications notificaciones en la Notificaciones de usuario consola. A continuación, en la AWS Artifact consola, puede crear una configuración para los ajustes de las notificaciones, en la que especifique los destinatarios de las notificaciones y las notificaciones que reciben.

Para configurar las notificaciones AWS Artifact por correo electrónico, debe tener los permisos necesarios para AWS Artifact y AWS User Notifications. Para obtener más información, consulte Gestión de identidad y acceso en AWS Artifact.

Contenido

Requisito previo: seleccione los centros de notificaciones en Notificaciones de usuario

Para poder recibir notificaciones AWS Artifact por correo electrónico, primero debe abrir la Notificaciones de usuario consola y seleccionar los centros de notificaciones en los Regiones de AWS que desee almacenar los datos Notificaciones de usuario . Es necesario seleccionar los centros de notificaciones para AWS User Notifications, que se AWS Artifact utilizan para enviar notificaciones.

Para seleccionar centros de notificaciones

1. Abra la página de centros de notificaciones de la AWS User Notifications consola.
2. Seleccione los centros de notificaciones en los Regiones de AWS que desee almacenar sus AWS User Notifications recursos. De forma predeterminada, sus Notificaciones de usuario

datos se almacenan en la región EE.UU. Este (Virginia del Norte). Notificaciones de usuario replica los datos de tus notificaciones en las demás regiones que selecciones. Para obtener más información, consulte la documentación sobre los centros de notificaciones en la Guía del AWS User Notifications usuario.

3. Elija Guardar y continuar.

Crear una configuración para los ajustes de AWS Artifact notificación

Tras seleccionar los centros de Notificaciones de usuario notificaciones, puede crear una configuración para los ajustes de notificación en la AWS Artifact consola. En la configuración que cree, especifique las direcciones de correo electrónico de los destinatarios en las que desea recibir AWS Artifact las notificaciones. También debe especificar las actualizaciones sobre las que deben recibir notificaciones esos destinatarios, como las actualizaciones de los AWS Artifact acuerdos y las actualizaciones de todos los AWS Artifact informes (o de un subconjunto de ellos).

Para crear una configuración

1. Abre la página de configuración de notificaciones de la AWS Artifact consola.
2. Seleccione Crear configuración.
3. En la página Crear configuración, haga lo siguiente:
   - Para recibir notificaciones de acuerdos, en Acuerdos, mantenga seleccionada la opción Actualizaciones de AWS los acuerdos.
   - Para recibir notificaciones de informes, en Informes, mantenga seleccionada la opción Actualizaciones de AWS los informes.
     a. Para recibir notificaciones de todos los informes, selecciona Todos los informes.
     b. Para recibir notificaciones solo de informes de categorías y series específicas, elija Un subconjunto de informes. A continuación, selecciona las categorías y series que te interesen.
   - En Nombre de la configuración, introduzca un nombre para la configuración.
   - En Correo electrónico, en Destinatarios, introduzca una lista separada por comas de las direcciones de correo electrónico en las que desee recibir correos electrónicos de AWS Artifact notificación.

- (Opcional) Para añadir etiquetas a la configuración de notificaciones, expanda Etiquetas, elija Añadir nueva etiqueta y, a continuación, introduzca las etiquetas como pares de valores clave. Para obtener más información sobre el etiquetado de Notificaciones de usuario los recursos, consulte Etiquetar los AWS User Notifications recursos en la Guía del usuario.AWS User Notifications
- Seleccione Crear configuración.

  Notificaciones de usuario envía un correo electrónico de verificación a cada una de las direcciones de correo electrónico de los destinatarios que haya proporcionado. Para verificar la dirección de correo electrónico, en el correo electrónico de verificación, el destinatario debe elegir Verificar correo electrónico. Solo las direcciones de correo electrónico verificadas recibirán AWS Artifact notificaciones.

Edición de una configuración para los ajustes AWS Artifact de notificación

Tras crear una configuración para los ajustes de AWS Artifact notificación, puede editarla en cualquier momento para cambiarlos. Por ejemplo, para añadir o eliminar destinatarios, cambiar los tipos de notificaciones que reciben y añadir o eliminar etiquetas.

Para editar una configuración

1. Abre la página de configuración de notificaciones de la AWS Artifact consola.
2. Seleccione la configuración que desee editar.
3. Elija Editar.
4. Edite cualquiera de las selecciones y campos de la configuración. Cuando haya terminado, elija Guardar cambios.

   Si has añadido nuevas direcciones de correo electrónico como destinatarios de las notificaciones, AWS User Notifications envía un correo electrónico de verificación a esas direcciones de correo electrónico. Para verificar la dirección de correo electrónico, en el correo electrónico de verificación, el destinatario debe elegir Verificar correo electrónico. Solo las direcciones de correo electrónico verificadas recibirán AWS Artifact notificaciones.

Eliminar una configuración de AWS Artifact notificaciones

Si ya no necesita una configuración que creó para los ajustes de AWS Artifact notificación, puede eliminarla en la AWS Artifact consola.

Para eliminar una configuración

1. Abre la página de configuración de notificaciones de la AWS Artifact consola.
2. Seleccione la configuración que desee eliminar.
3. Elija Eliminar.
4. En el cuadro de diálogo Eliminar configuración, elija Eliminar.

Gestión de identidad y acceso en AWS Artifact

Al registrarse AWS, proporciona una dirección de correo electrónico y una contraseña asociadas a su AWS cuenta. Estas son tus credenciales raíz y te proporcionan acceso completo a todos tus AWS recursos, incluidos los recursos para AWS Artifact. Sin embargo, le recomendamos encarecidamente que no utilice la cuenta raíz en los accesos diarios. También le recomendamos que no comparta las credenciales de la cuenta con otras personas, lo que les proporcionaría acceso completo a su cuenta.

En lugar de iniciar sesión en tu AWS cuenta con credenciales raíz o compartir tus credenciales con otras personas, debes crear una identidad de usuario especial denominada IAMusuario para ti y para cualquier persona que necesite acceder a un documento o acuerdo AWS Artifact. Con este enfoque, puede proporcionar datos de inicio de sesión diferentes a cada uno de los usuarios y concederles únicamente los permisos que necesitan para trabajar con documentos específicos. También puede conceder a varios usuarios de IAM los mismos permisos concediendo los permisos a un grupo de IAM y añadiendo los usuarios de IAM al grupo.

Si ya administras las identidades de los usuarios de forma externa AWS, puedes usar proveedores de IAM identidad en lugar de crear IAM usuarios. Para obtener más información, consulte Proveedores de identidad y federación en la Guía del IAM usuario.

Contenido

Concesión de acceso de usuario a AWS Artifact

Complete los siguientes pasos para conceder permisos a los usuarios en AWS Artifact función del nivel de acceso que necesiten.

Tareas

- Paso 1: Crear una política de IAM
- Paso 2: Cree un IAM grupo y adjunte la política
- Paso 3: Crea IAM usuarios y agrégalos al grupo

Paso 1: Crear una política de IAM

Como IAM administrador, puede crear una política que conceda permisos a AWS Artifact las acciones y los recursos.

Creación de una política de IAM

Utilice el siguiente procedimiento para crear una IAM política que pueda utilizar para conceder permisos a sus IAM usuarios y grupos.

1. Abra la IAM consola en https://console.aws.amazon.com/iam/.
2. En el panel de navegación, seleccione Políticas.
3. Elija Create Policy (Crear política).
4. Seleccione la JSONpestaña.
5. Especifique un documento de política. Puede crear su propia política o bien usar una de las políticas de Ejemplos de IAM políticas para AWS Artifact.
6. Elija Revisar la política. El validador de políticas notifica los errores de sintaxis.
7. En la página Revisar política, introduzca un nombre único que le ayudará a recordar el propósito de la política. También puede proporcionar una descripción.
8. Elija Crear política.

Paso 2: Cree un IAM grupo y adjunte la política

Como IAM administrador, puede crear un grupo y adjuntar la política que creó al grupo. Puede añadir IAM usuarios al grupo en cualquier momento.

Para crear un IAM grupo y adjuntar su política

1. En el panel de navegación, elija Groups (Grupos) y, a continuación, elija Create New Group (Crear nuevo grupo).
2. En Nombre del grupo, introduzca un nombre para el grupo y seleccione Paso siguiente.

3. En el campo de búsqueda, introduzca el nombre de la política que ha creado. Seleccione la casilla de verificación para su política y, a continuación, elija Paso siguiente.
4. Revise el nombre del grupo y las políticas. Cuando esté listo, elija Crear grupo.

Paso 3: Crea IAM usuarios y agrégalos al grupo

Como IAM administrador, puede añadir usuarios a un grupo en cualquier momento. Esto concede a los usuarios los permisos concedidos al grupo.

Para crear un IAM usuario y añadirlo a un grupo

1. En el panel de navegación, elija Users (Usuarios) y, a continuación, elija Add user (Añadir usuario).
2. En Nombre de usuario, introduzca los nombres de uno o más usuarios.
3. Seleccione la casilla de verificación situada junto a AWS Management Console access (Acceso a la consola). Configure una contraseña personalizada o generada automáticamente. Si lo desea, puede seleccionar El usuario debe crear una contraseña nueva la próxima vez que inicie sesión para exigir un restablecimiento de contraseña cuando el usuario inicie sesión por primera vez.
4. Elija Siguiente: permisos.
5. Elija Añadir usuario al grupo y, a continuación, seleccione el grupo que ha creado.
6. Elija Siguiente: etiquetas. Puede agregar etiquetas a sus usuarios.
7. Elija Siguiente: Revisar. Cuando haya terminado, elija Crear usuario.

Migración de informes a permisos detallados para AWS Artifact

Ahora puede utilizar permisos detallados para. AWS Artifact Gracias a estos permisos detallados, tiene un control pormenorizado sobre el acceso a funciones como la aceptación de condiciones y la descarga de informes.

Para acceder a los informes mediante los permisos detallados, puedes utilizar la Política AWSArtifactReportsReadOnlyAccessgestionada o actualizar tus permisos según la siguiente recomendación. Si anteriormente había optado por no usar permisos específicos, debería hacerlo mediante el enlace «aceptar permisos específicos para los informes de AWS Artifact» disponible en la consola de informes.

Tienes la opción de acceder a los informes con permisos antiguos a través del enlace «Excluir los permisos detallados para los informes de AWS Artifact» disponible en la consola si hay algún problema con la actualización a los nuevos permisos.

Migración de informes a nuevos permisos

Migre permisos que no sean específicos de un recurso

Sustituya su política actual que contiene permisos heredados por una política que contenga permisos detallados.

Política antigua:

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Effect": "Allow",
        "Action": [
            "artifact:Get"
        ],
        "Resource": [
            "arn:aws:artifact:::report-package/*"
        ]
    }]
}
```

Nueva política con permisos detallados:

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Effect": "Allow",
        "Action": [
            "artifact:ListReports",
            "artifact:GetReportMetadata",
            "artifact:GetReport",
            "artifact:GetTermForReport"
        ],
        "Resource": "*"
    }]
}
```

Migre los permisos específicos de los recursos

Sustituya su política actual que contiene permisos heredados por una política que contenga permisos detallados. Los permisos comodín de los recursos de informes se han sustituido por claves de condición.

Política antigua:

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Effect": "Allow",
        "Action": [
            "artifact:Get"
        ],
        "Resource": [
            "arn:aws:artifact:::report-package/Certifications and Attestations/SOC/*",
            "arn:aws:artifact:::report-package/Certifications and Attestations/PCI/*",
            "arn:aws:artifact:::report-package/Certifications and Attestations/ISO/*"
        ]
    }]
}
```

Nueva política con permisos y claves de condición detallados:

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Effect": "Allow",
            "Action": [
                "artifact:ListReports"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "artifact:GetReportMetadata",
                "artifact:GetReport",
                "artifact:GetTermForReport"
            ],
            "Resource": "*",
```

```
            "Condition": {
                "StringEquals": {
                    "artifact:ReportSeries": [
                        "SOC",
                        "PCI",
                        "ISO"
                    ],
                    "artifact:ReportCategory": [
                        "Certifications and Attestations"
                    ]
                }
            }
        }
    ]
}
```

Migración a permisos detallados para los acuerdos de Artifact AWS

AWSArtifact ahora permite a los clientes utilizar permisos detallados para los acuerdos. Gracias a estos permisos detallados, los clientes tienen un control pormenorizado sobre el acceso a funciones como la consulta y la aceptación de los acuerdos de confidencialidad, así como la aceptación y rescisión de los acuerdos.

Para acceder a los acuerdos mediante permisos detallados, puede utilizar las políticas gestionadas o las políticas AWSArtifactAgreementsFullAccess gestionadas AWSArtifactAgreementsReadOnlyAccesso actualizar sus permisos según la siguiente recomendación. Si anteriormente había optado por no usar permisos específicos, debe hacerlo mediante el enlace «aceptar permisos específicos para los acuerdos de AWS Artifact» disponible en la consola de acuerdos.

Tienes la opción de acceder a los acuerdos con permisos antiguos a través del enlace «Exclusión de los permisos detallados para los acuerdos de AWS Artifact» disponible en la consola si hay algún problema con la actualización a los nuevos permisos.

Migración a nuevos permisos

La IAM acción antigua «DownloadAgreement» se ha sustituido por la acción «GetAgreement» para descargar los acuerdos no aceptados y por la acción «GetCustomerAgreement» para descargar los acuerdos aceptados. Además, se han introducido medidas más detalladas para controlar el acceso a la consulta y la aceptación de los acuerdos de confidencialidad ()NDAs. Para aprovechar estas

medidas detalladas y mantener la capacidad de ver y ejecutar los acuerdos, los usuarios deben reemplazar su política actual que contiene los permisos heredados por una política que contenga permisos detallados.

Migre los permisos para descargar el acuerdo a nivel de cuenta

Política heredada:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:DownloadAgreement"
      ],
      "Resource": [
        "arn:aws:artifact::*:customer-agreement/*",
        "arn:aws:artifact:::agreement/*"
      ]
    }
  ]
}
```

Nueva política con permisos detallados:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ListAgreementsActions",
      "Effect": "Allow",
      "Action": [
        "artifact:ListAgreements",
        "artifact:ListCustomerAgreements"
      ],
      "Resource": "*"
    },
    {
      "Sid": "GetAgreementActions",
      "Effect": "Allow",
      "Action": [
```

```
        "artifact:GetCustomerAgreement",
        "artifact:GetAgreement",
        "artifact:GetNdaForAgreement",
        "artifact:AcceptNdaForAgreement"
      ],
      "Resource": [
        "arn:aws:artifact::*:customer-agreement/*",
        "arn:aws:artifact:::agreement/*"
      ]
    }
  ]
}
```

Migre los permisos no específicos de los recursos para descargar, aceptar y rescindir los acuerdos a nivel de cuenta

Política heredada:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:AcceptAgreement",
        "artifact:DownloadAgreement",
        "artifact:TerminateAgreement"
      ],
      "Resource": [
        "arn:aws:artifact::*:customer-agreement/*",
        "arn:aws:artifact:::agreement/*"
      ]
    }
  ]
}
```

Nueva política con permisos detallados:

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

```
        "Sid": "ListAgreementActions",
        "Effect": "Allow",
        "Action": [
            "artifact:ListAgreements",
            "artifact:ListCustomerAgreements"
        ],
        "Resource": "*"
      },
      {
        "Sid": "AWSAgreementActions",
        "Effect": "Allow",
        "Action": [
          "artifact:GetAgreement",
          "artifact:AcceptNdaForAgreement",
          "artifact:GetNdaForAgreement",
          "artifact:AcceptAgreement"
        ],
        "Resource": "arn:aws:artifact:::agreement/*"
      },
      {
        "Sid": "CustomerAgreementActions",
        "Effect": "Allow",
        "Action": [
            "artifact:GetCustomerAgreement",
            "artifact:TerminateAgreement"
        ],
        "Resource": "arn:aws:artifact::*:customer-agreement/*"
      }
    ]
}
```

Migre los permisos no específicos de los recursos para descargar, aceptar y rescindir los acuerdos a nivel de la organización

Política heredada:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:AcceptAgreement",
```

```
        "artifact:DownloadAgreement",
        "artifact:TerminateAgreement"
      ],
      "Resource": [
        "arn:aws:artifact::*:customer-agreement/*",
        "arn:aws:artifact:::agreement/*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": "iam:ListRoles",
      "Resource": "arn:aws:iam:::role/*"
    },
    {
      "Effect": "Allow",
      "Action": "iam:CreateServiceLinkedRole",
      "Resource": "arn:aws:iam:::role/aws-service-role/artifact.amazonaws.com/
AWSServiceRoleForArtifact"
    },
    {
      "Effect": "Allow",
      "Action": [
        "organizations:DescribeOrganization",
        "organizations:EnableAWSServiceAccess",
        "organizations:ListAccounts",
        "organizations:ListAWSServiceAccessForOrganization"
      ],
      "Resource": "*"
    }
  ]
}
```

Nueva política con permisos detallados:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ListAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:ListAgreements",
        "artifact:ListCustomerAgreements"
```

```
      ],
      "Resource": "*"
    },
    {
      "Sid": "AWSAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetAgreement",
        "artifact:AcceptNdaForAgreement",
        "artifact:GetNdaForAgreement",
        "artifact:AcceptAgreement"
      ],
      "Resource": "arn:aws:artifact:::agreement/*"
    },
    {
      "Sid": "CustomerAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetCustomerAgreement",
        "artifact:TerminateAgreement"
      ],
      "Resource": "arn:aws:artifact::*:customer-agreement/*"
    },
    {
      "Sid": "CreateServiceLinkedRoleForOrganizationsIntegration",
      "Effect": "Allow",
      "Action": [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource": "arn:aws:iam::*:role/aws-service-role/artifact.amazonaws.com/
AWSServiceRoleForArtifact",
      "Condition": {
        "StringEquals": {
          "iam:AWSServiceName": [
            "artifact.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid": "GetRoleToCheckForRoleExistence",
      "Effect": "Allow",
      "Action": [
        "iam:GetRole"
```

```
      ],
      "Resource": "arn:aws:iam::*:role/aws-service-role/artifact.amazonaws.com/
AWSServiceRoleForArtifact"
    },
    {
      "Sid": "EnableServiceTrust",
      "Effect": "Allow",
      "Action": [
        "organizations:EnableAWSServiceAccess",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganization"
      ],
      "Resource": "*"
    }
  ]
}
```

Migre los permisos específicos de los recursos para descargar, aceptar y rescindir los acuerdos a nivel de cuenta

Política heredada:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:AcceptAgreement",
        "artifact:DownloadAgreement"
      ],
      "Resource": [
        "arn:aws:artifact:::agreement/AWS Business Associate Addendum"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "artifact:TerminateAgreement"
      ],
      "Resource": [
        "arn:aws:artifact::*:customer-agreement/*"
      ]
```

```
    }
  ]
}
```

Nueva política con permisos detallados:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ListAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:ListAgreements",
        "artifact:ListCustomerAgreements"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AWSAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetAgreement",
        "artifact:AcceptNdaForAgreement",
        "artifact:GetNdaForAgreement",
        "artifact:AcceptAgreement"
      ],
      "Resource": "arn:aws:artifact:::agreement/agreement-9c1kBcYznTkcpRIm"
    },
    {
      "Sid": "CustomerAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetCustomerAgreement",
        "artifact:TerminateAgreement"
      ],
      "Resource": "arn:aws:artifact::*:customer-agreement/*"
    }
  ]
}
```

Migre los permisos específicos de los recursos para descargar, aceptar y rescindir los acuerdos a nivel de la organización

Política heredada:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:AcceptAgreement",
        "artifact:DownloadAgreement",
        "artifact:TerminateAgreement"
      ],
      "Resource": [
        "arn:aws:artifact::*:customer-agreement/*",
        "arn:aws:artifact:::agreement/AWS Organizations Business Associate Addendum"
      ]
    },
    {
      "Effect": "Allow",
      "Action": "iam:ListRoles",
      "Resource": "arn:aws:iam:::role/*"
    },
    {
      "Effect": "Allow",
      "Action": "iam:CreateServiceLinkedRole",
      "Resource": "arn:aws:iam:::role/aws-service-role/artifact.amazonaws.com/
AWSServiceRoleForArtifact"
    },
    {
      "Effect": "Allow",
      "Action": [
        "organizations:DescribeOrganization",
        "organizations:EnableAWSServiceAccess",
        "organizations:ListAccounts",
        "organizations:ListAWSServiceAccessForOrganization"
      ],
      "Resource": "*"
    }
  ]
}
```

Nueva política con permisos detallados:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ListAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:ListAgreements",
        "artifact:ListCustomerAgreements"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AWSAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetAgreement",
        "artifact:AcceptNdaForAgreement",
        "artifact:GetNdaForAgreement",
        "artifact:AcceptAgreement"
      ],
      "Resource": "arn:aws:artifact:::agreement/agreement-y03aUwMAEorHtqjv"
    },
    {
      "Sid": "CustomerAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetCustomerAgreement",
        "artifact:TerminateAgreement"
      ],
      "Resource": "arn:aws:artifact::*:customer-agreement/*"
    },
    {
      "Sid": "CreateServiceLinkedRoleForOrganizationsIntegration",
      "Effect": "Allow",
      "Action": [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource": "arn:aws:iam::*:role/aws-service-role/artifact.amazonaws.com/
AWSServiceRoleForArtifact",
      "Condition": {
        "StringEquals": {
          "iam:AWSServiceName": [
```

```
            "artifact.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid": "GetRoleToCheckForRoleExistence",
      "Effect": "Allow",
      "Action": [
        "iam:GetRole"
      ],
      "Resource": "arn:aws:iam::*:role/aws-service-role/artifact.amazonaws.com/
AWSServiceRoleForArtifact"
    },
    {
      "Sid": "EnableServiceTrust",
      "Effect": "Allow",
      "Action": [
        "organizations:EnableAWSServiceAccess",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganization"
      ],
      "Resource": "*"
    }
  ]
}
```

Un mapeo de recursos tradicional a uno más detallado para los acuerdos

Los acuerdos ARN se actualizaron para incluir permisos detallados. Cualquier referencia anterior a los recursos de los acuerdos anteriores debe sustituirse por una nueva. ARN A continuación se muestra el ARN mapeo del acuerdo entre los recursos heredados y los recursos detallados.

Nombre del acuerdo	Permisos de Artifact ARN for Legacy	Artifact ARN para permisos detallados
AWSApéndice para socios comerciales	arn:aws:artifact: ::agreement/ Anexo para socios comercial es AWS	arn:aws:artifact: ::agreeme nt/agreement-9c1 T kBcYzn kcpRIm

Nombre del acuerdo	Permisos de Artifact ARN for Legacy	Artifact ARN para permisos detallados
AWSAnexo sobre violación de datos notificable en Nueva Zelanda	arn:aws:artifact: ::agreeme nt/ Apéndice sobre violación de datos notificable en Nueva Zelanda AWS	arn:aws:artifact: ::agreeme nt/agreement-3 YRq9rGUIu 72r7Gt
AWSApéndice sobre violación de datos de declaración obligatoria en Australia	arn:aws:artifact: :agreemen t/ Apéndice australiano sobre violación de datos notificable AWS	arn:aws:artifact: ::acuerdo /acuerdo - sbLSDe 8 9 bitmAXNr
AWSSECRegla 17a-4 Adición	arn:aws:artifact: ::agreement/ Regla 17a-4 Apéndice AWS SEC	arn:aws:artifact: ::agreeme nt/agreement-bexgr7sjv XAW4Gxu
AWSSECRegla 18a-6 Apéndice	arn:aws:artifact: ::agreement/ Regla 18a-6 Apéndice AWS SEC	arn:aws:artifact: ::agreeme nt/agreement- HZTdNwJuq OKLReXC
AWSApéndice de Organizat ions Business Associate	arn:aws:artifact: ::agreeme nt/ Organizations Business Associate AWS Apéndice	arn:aws:artifact: ::agreeme nt/agreement-y03 aUw MAEorHtqjv
AWSApéndice sobre violación de datos notificable de Organizations Australian	arn:aws:artifact: AWS ::agreement/ Organisat ions Australian Notificable Data Breach Apéndice	arn:aws:artifact: ::acuerdo /acuerdo-Y pDMFXTe PE7kEg4b
AWSApéndice sobre la violación de datos notificab le de Organizations New Zealand	arn:aws:artifact: ::agreement/ Organisations New Zealand Notificable Data Violation AWS Apéndice	arn:aws:artifact: ::agreement/ agreement uojEjr - vOnvrh 3 V52

Ejemplos de IAM políticas para AWS Artifact

Puede crear políticas de permisos que concedan permisos a IAM los usuarios. Puede conceder a los usuarios acceso a los AWS Artifact informes y la posibilidad de aceptar y descargar acuerdos en nombre de una sola cuenta o de una organización.

Los siguientes ejemplos de políticas muestran los permisos que puede asignar a IAM los usuarios en función del nivel de acceso que necesiten.

- Ejemplos de políticas para administrar AWS informes con permisos detallados
- Ejemplos de políticas para gestionar informes de terceros
- Ejemplo de políticas para gestionar acuerdos
- Ejemplos de políticas con las que puede integrarse AWS Organizations
- Ejemplos de políticas para administrar acuerdos de la cuenta de administración
- Ejemplos de políticas para gestionar acuerdos organizativos
- Ejemplos de políticas para gestionar notificaciones

Example Ejemplos de políticas para gestionar AWS los informes mediante permisos detallados

> **Tip**
>
> Debería considerar la posibilidad de utilizar la política AWSArtifactReportsReadOnlyAccess gestionada en lugar de definir la suya propia.

La siguiente política concede permiso para descargar todos los AWS informes mediante permisos específicos.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:ListReports",
        "artifact:GetReportMetadata",
```

```
        "artifact:GetReport",
        "artifact:GetTermForReport"
      ],
      "Resource": "*"
    }
  ]
}
```

La siguiente política concede permiso para descargar únicamente los ISO informes y AWS SOCPCI, a través de permisos específicos.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:ListReports",
        "artifact:GetReportMetadata",
        "artifact:GetReport",
        "artifact:GetTermForReport"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "artifact:ReportSeries": [
            "SOC",
            "PCI",
            "ISO"
          ],
          "artifact:ReportCategory": [
            "Certifications And Attestations"
          ]
        }
      }
    }
  ]
}
```

Example Ejemplos de políticas para gestionar informes de terceros

> **Tip**
>
> Debería considerar la posibilidad de utilizar la política AWSArtifactReportsReadOnlyAccess gestionada en lugar de definir la suya propia.

Los informes de terceros se indican en el IAM recurso`report`.

La siguiente política concede permisos a todas las funcionalidades de informes de terceros.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:ListReports",
        "artifact:GetReportMetadata",
        "artifact:GetReport",
        "artifact:GetTermForReport"
      ],
      "Resource": "*"
    }
  ]
}
```

La siguiente política concede permiso para descargar informes de terceros.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:GetReport",
        "artifact:GetTermForReport"
      ],
      "Resource": "*"
    }
  ]
```

```
}
```

La siguiente política concede permiso para enumerar informes de terceros.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:ListReport"
      ],
      "Resource": "*"
    }
  ]
}
```

La siguiente política otorga permiso para ver los detalles de un informe de terceros en todas las versiones.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:GetReportMetadata"
      ],
      "Resource": [
        "arn:aws:artifact:us-east-1::report/report-jRVRFP8HxUN5zpPh:*"
      ]
    }
  ]
}
```

La siguiente política otorga permiso para ver los detalles de un informe de terceros para una versión específica.

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

```
      "Effect": "Allow",
      "Action": [
        "artifact:GetReportMetadata"
      ],
      "Resource": [
        "arn:aws:artifact:us-east-1::report/report-jRVRFP8HxUN5zpPh:1"
      ]
    }
  ]
}
```

> **Tip**
>
> Deberías considerar la posibilidad de utilizar la AWSArtifactAgreementsReadOnlyAccesspolítica AWSArtifactAgreementsFullAccess gestionada en lugar de definir tu propia política.

Example Ejemplo de políticas para gestionar acuerdos

La siguiente política concede permiso para descargar todos los acuerdos.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:ListAgreements",
        "artifact:ListCustomerAgreements"
      ],
      "Resource": [
        "*"
      ]
    },
    {
      "Sid": "AWSAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetAgreement",
        "artifact:AcceptNdaForAgreement",
```

```
        "artifact:GetNdaForAgreement"
      ],
      "Resource": "arn:aws:artifact:::agreement/*"
    },
    {
      "Sid": "CustomerAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetCustomerAgreement"
      ],
      "Resource": "arn:aws:artifact::*:customer-agreement/*"
    }
  ]
}
```

La siguiente política otorga permiso para aceptar todos los acuerdos.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:ListAgreements"
      ],
      "Resource": [
        "*"
      ]
    },
    {
      "Sid": "AWSAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetAgreement",
        "artifact:AcceptNdaForAgreement",
        "artifact:GetNdaForAgreement",
        "artifact:AcceptAgreement"
      ],
      "Resource": "arn:aws:artifact:::agreement/*"
    }
  ]
}
```

La siguiente política otorga permiso para rescindir todos los acuerdos.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ListAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:ListAgreements",
        "artifact:ListCustomerAgreements"
      ],
      "Resource": "*"
    },
    {
      "Sid": "CustomerAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetCustomerAgreement",
        "artifact:TerminateAgreement"
      ],
      "Resource": "arn:aws:artifact::*:customer-agreement/*"
    }
  ]
}
```

La siguiente política otorga permisos para ver y ejecutar los acuerdos a nivel de cuenta.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ListAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:ListAgreements",
        "artifact:ListCustomerAgreements"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AWSAgreementActions",
      "Effect": "Allow",
```

```
      "Action": [
        "artifact:GetAgreement",
        "artifact:AcceptNdaForAgreement",
        "artifact:GetNdaForAgreement",
        "artifact:AcceptAgreement"
      ],
      "Resource": "arn:aws:artifact:::agreement/*"
    },
    {
      "Sid": "CustomerAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetCustomerAgreement",
        "artifact:TerminateAgreement"
      ],
      "Resource": "arn:aws:artifact::*:customer-agreement/*"
    }
  ]
}
```

Example Ejemplos de políticas con las que se puede integrar AWS Organizations

La siguiente política otorga permiso para crear el IAM rol con el AWS Artifact que se realiza la integración AWS Organizations. La cuenta de administración de la organización debe tener estos permisos para empezar a usar acuerdos de la organización.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "CreateServiceLinkedRoleForOrganizationsIntegration",
      "Effect": "Allow",
      "Action": [
        "iam:CreateServiceLinkedRole",
        "iam:GetRole"
      ],
      "Resource": "arn:aws:iam::*:role/aws-service-role/artifact.amazonaws.com/
AWSServiceRoleForArtifact",
      "Condition": {
        "StringEquals": {
          "iam:AWSServiceName": [
            "artifact.amazonaws.com"
          ]
```

```
        }
      }
    }
  ]
}
```

La siguiente política concede permiso para conceder AWS Artifact los permisos de uso AWS Organizations. La cuenta de administración de la organización debe tener estos permisos para empezar a usar acuerdos de la organización.

```
{
  "Version": "2012-10-17",
  "Statement": [
   {
      "Effect": "Allow",
      "Action": [
        "organizations:EnableAWSServiceAccess",
        "organizations:DescribeOrganization",
        "organizations:ListAWSServiceAccessForOrganization"
      ],
      "Resource": "*"
   }
 ]
}
```

Example Ejemplos de políticas para administrar acuerdos de la cuenta de administración

La siguiente política concede permisos para administrar los acuerdos de la cuenta de administración.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ListAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:ListAgreements",
        "artifact:ListCustomerAgreements"
      ],
      "Resource": "*"
    },
    {
```

```
      "Sid": "AWSAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetAgreement",
        "artifact:AcceptNdaForAgreement",
        "artifact:GetNdaForAgreement",
        "artifact:AcceptAgreement"
      ],
      "Resource": "arn:aws:artifact:::agreement/*"
    },
    {
      "Sid": "CustomerAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetCustomerAgreement",
        "artifact:TerminateAgreement"
      ],
      "Resource": "arn:aws:artifact::*:customer-agreement/*"
    },
    {
      "Sid": "CreateServiceLinkedRoleForOrganizationsIntegration",
      "Effect": "Allow",
      "Action": [
        "iam:CreateServiceLinkedRole",
        "iam:GetRole"
      ],
      "Resource": "arn:aws:iam::*:role/aws-service-role/artifact.amazonaws.com/
AWSServiceRoleForArtifact",
      "Condition": {
        "StringEquals": {
          "iam:AWSServiceName": [
            "artifact.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid": "EnableServiceTrust",
      "Effect": "Allow",
      "Action": [
        "organizations:EnableAWSServiceAccess",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganization"
      ],
```

```
      "Resource": "*"
    }
  ]
}
```

Example Ejemplos de políticas para gestionar acuerdos organizativos

La siguiente política concede permisos para gestionar los acuerdos organizativos. Otro usuario con los permisos necesarios debe configurar los acuerdos organizativos.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ListAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:ListAgreements",
        "artifact:ListCustomerAgreements"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AWSAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetAgreement",
        "artifact:AcceptNdaForAgreement",
        "artifact:GetNdaForAgreement",
        "artifact:AcceptAgreement"
      ],
      "Resource": "arn:aws:artifact:::agreement/*"
    },
    {
      "Sid": "CustomerAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetCustomerAgreement",
        "artifact:TerminateAgreement"
      ],
      "Resource": "arn:aws:artifact::*:customer-agreement/*"
    },
```

```
    {
      "Effect": "Allow",
      "Action": [
        "organizations:DescribeOrganization"
      ],
      "Resource": "*"
    }
  ]
}
```

La siguiente política concede permisos para ver los acuerdos organizativos.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ListAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:ListAgreements",
        "artifact:ListCustomerAgreements"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AWSAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetAgreement",
        "artifact:AcceptNdaForAgreement",
        "artifact:GetNdaForAgreement",
        "artifact:AcceptAgreement"
      ],
      "Resource": "arn:aws:artifact:::agreement/*"
    },
    {
      "Sid": "CustomerAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetCustomerAgreement",
        "artifact:TerminateAgreement"
      ],
      "Resource": "arn:aws:artifact::*:customer-agreement/*"
```

```
    },
    {
      "Effect": "Allow",
      "Action": [
        "organizations:DescribeOrganization"
      ],
      "Resource": "*"
    }
  ]
}
```

Example Ejemplos de políticas para gestionar notificaciones

La siguiente política otorga permisos completos para usar AWS Artifact las notificaciones.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:GetAccountSettings",
        "artifact:PutAccountSettings",
        "notifications:AssociateChannel",
        "notifications:CreateEventRule",
        "notifications:CreateNotificationConfiguration",
        "notifications:DeleteEventRule",
        "notifications:DeleteNotificationConfiguration",
        "notifications:DisassociateChannel",
        "notifications:GetEventRule",
        "notifications:GetNotificationConfiguration",
        "notifications:ListChannels",
        "notifications:ListEventRules",
        "notifications:ListNotificationConfigurations",
        "notifications:ListNotificationHubs",
        "notifications:ListTagsForResource",
        "notifications:TagResource",
        "notifications:UntagResource",
        "notifications:UpdateEventRule",
        "notifications:UpdateNotificationConfiguration",
        "notifications-contacts:CreateEmailContact",
        "notifications-contacts:DeleteEmailContact",
        "notifications-contacts:GetEmailContact",
```

```
        "notifications-contacts:ListEmailContacts",
        "notifications-contacts:SendActivationCode"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

La siguiente política concede permiso para enumerar todas las configuraciones.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:GetAccountSettings",
        "notifications:ListChannels",
        "notifications:ListEventRules",
        "notifications:ListNotificationConfigurations",
        "notifications:ListNotificationHubs",
        "notifications-contacts:GetEmailContact"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

La siguiente política concede permiso para crear una configuración.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:GetAccountSettings",
        "artifact:PutAccountSettings",
        "notifications-contacts:CreateEmailContact",
```

```
        "notifications-contacts:SendActivationCode",
        "notifications:AssociateChannel",
        "notifications:CreateEventRule",
        "notifications:CreateNotificationConfiguration",
        "notifications:ListEventRules",
        "notifications:ListNotificationHubs",
        "notifications:TagResource",
        "notifications-contacts:ListEmailContacts"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

La siguiente política concede permiso para editar una configuración.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:GetAccountSettings",
        "artifact:PutAccountSettings",
        "notifications:AssociateChannel",
        "notifications:DisassociateChannel",
        "notifications:GetNotificationConfiguration",
        "notifications:ListChannels",
        "notifications:ListEventRules",
        "notifications:ListTagsForResource",
        "notifications:TagResource",
        "notifications:UntagResource",
        "notifications:UpdateEventRule",
        "notifications:UpdateNotificationConfiguration",
        "notifications-contacts:GetEmailContact",
        "notifications-contacts:ListEmailContacts"
      ],
      "Resource": [
        "*"
      ]
    }
```

```
  ]
}
```

La siguiente política concede permiso para eliminar una configuración.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "notifications:DeleteNotificationConfiguration",
        "notifications:ListEventRules"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

La siguiente política concede permiso para ver los detalles de una configuración.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "notifications:GetNotificationConfiguration",
        "notifications:ListChannels",
        "notifications:ListEventRules",
        "notifications:ListTagsForResource",
        "notifications-contacts:GetEmailContact"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

La siguiente política concede permiso para registrar o anular el registro de los centros de notificaciones.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "notifications:DeregisterNotificationHub",
        "notifications:RegisterNotificationHub"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

Uso de políticas AWS administradas para AWS Artifact

Una política AWS administrada es una política independiente creada y administrada por AWS. AWS Las políticas administradas están diseñadas para proporcionar permisos para muchos casos de uso comunes, de modo que pueda empezar a asignar permisos a usuarios, grupos y funciones.

Ten en cuenta que es posible que las políticas AWS administradas no otorguen permisos con privilegios mínimos para tus casos de uso específicos, ya que están disponibles para que los usen todos los AWS clientes. Se recomienda definir políticas administradas por el cliente específicas para sus casos de uso a fin de reducir aún más los permisos.

No puedes cambiar los permisos definidos en AWS las políticas administradas. Si AWS actualiza los permisos definidos en una política AWS administrada, la actualización afecta a todas las identidades principales (usuarios, grupos y roles) a las que está asociada la política. AWS es más probable que actualice una política AWS administrada cuando Servicio de AWS se lance una nueva o cuando haya nuevas API operaciones disponibles para los servicios existentes.

Para obtener más información, consulte Políticas administradas de AWS en la Guía del usuario de IAM.

AWS política gestionada: AWSArtifactReportsReadOnlyAccess

Puede adjuntar la política `AWSArtifactReportsReadOnlyAccess` a las identidades de IAM.

Esta política otorga *`read-only`* permisos que permiten publicar, ver y descargar informes.

Detalles de los permisos

Esta política incluye los siguientes permisos.

- `artifact`— Permite a los directores enumerar, ver y descargar informes. AWS Artifact

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:Get",
        "artifact:GetReport",
        "artifact:GetReportMetadata",
        "artifact:GetTermForReport",
        "artifact:ListReports"
      ],
      "Resource": "*"
    }
  ]
}
```

AWS política gestionada: AWSArtifactAgreementsReadOnlyAccess

Puede adjuntar la política `AWSArtifactAgreementsReadOnlyAccess` a las identidades de IAM.

Esta política otorga *`read-only`* acceso a una lista de los acuerdos de servicio de AWS Artifact y a descargar los acuerdos aceptados. También incluye permisos para enumerar y describir los detalles de la organización. Además, la política permite comprobar si existe el rol vinculado al servicio requerido.

Detalles de los permisos

Esta política incluye los siguientes permisos.

- `artifact`— Permite a los directores enumerar todos los acuerdos y ver los acuerdos aceptados desde ellos. AWS Artifact
- `IAM`— Permite a los directores comprobar si el rol vinculado al servicio existe utilizando. GetRole
- `organization`— Permite a los directores describir la organización y enumerar el acceso al servicio para la organización.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ListAgreementsActions",
      "Effect": "Allow",
      "Action": [
        "artifact:ListAgreements",
        "artifact:ListCustomerAgreements"
      ],
      "Resource": "*"
    },
    {
      "Sid": "GetCustomerAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetCustomerAgreement"
      ],
      "Resource": "arn:aws:artifact::*:customer-agreement/*"
    },
    {
      "Sid": "AWSOrganizationActions",
      "Effect": "Allow",
      "Action": [
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganization"
      ],
      "Resource": "*"
    },
    {
      "Sid": "GetRole",
```

```
      "Effect": "Allow",
      "Action": [
        "iam:GetRole"
      ],
      "Resource": "arn:aws:iam::*:role/aws-service-role/artifact.amazonaws.com/
AWSServiceRoleForArtifact"
    }
  ]
}
```

AWS política gestionada: AWSArtifactAgreementsFullAccess

Puede adjuntar la política `AWSArtifactAgreementsFullAccess` a las identidades de IAM.

Esta política otorga *`full`* permisos para publicar, descargar, aceptar y rescindir los acuerdos de AWS Artifact. También incluye permisos para enumerar y habilitar el acceso a los AWS servicios en el servicio de la Organización, además de describir los detalles de la organización. Además, la política permite comprobar si existe el rol vinculado al servicio requerido y crea uno si no existe.

Detalles de los permisos

Esta política incluye los siguientes permisos.

- `artifact`— Permite a los directores enumerar, descargar, aceptar y rescindir los acuerdos. AWS Artifact
- `IAM`— Permite a los directores crear un rol vinculado al servicio y comprobar si el rol vinculado al servicio existe utilizando. GetRole
- `organization`— Permite a los directores describir la organización y enumerar/habilitar el acceso al servicio para la organización.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ListAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:ListAgreements",
        "artifact:ListCustomerAgreements"
```

```
      ],
      "Resource": "*"
    },
    {
      "Sid": "AWSAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetAgreement",
        "artifact:AcceptNdaForAgreement",
        "artifact:GetNdaForAgreement",
        "artifact:AcceptAgreement"
      ],
      "Resource": "arn:aws:artifact:::agreement/*"
    },
    {
      "Sid": "CustomerAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetCustomerAgreement",
        "artifact:TerminateAgreement"
      ],
      "Resource": "arn:aws:artifact::*:customer-agreement/*"
    },
    {
      "Sid": "CreateServiceLinkedRoleForOrganizationsIntegration",
      "Effect": "Allow",
      "Action": [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource": "arn:aws:iam::*:role/aws-service-role/artifact.amazonaws.com/
AWSServiceRoleForArtifact",
      "Condition": {
        "StringEquals": {
          "iam:AWSServiceName": [
            "artifact.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid": "GetRoleToCheckForRoleExistence",
      "Effect": "Allow",
      "Action": [
        "iam:GetRole"
```

```
      ],
      "Resource": "arn:aws:iam::*:role/aws-service-role/artifact.amazonaws.com/
AWSServiceRoleForArtifact"
    },
    {
      "Sid": "EnableServiceTrust",
      "Effect": "Allow",
      "Action": [
        "organizations:EnableAWSServiceAccess",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganization"
      ],
      "Resource": "*"
    }
  ]
}
```

AWS Artifact actualizaciones de las políticas gestionadas AWS

Consulte los detalles sobre las actualizaciones de las políticas AWS administradas AWS Artifact desde que este servicio comenzó a rastrear estos cambios. Para recibir alertas automáticas sobre los cambios en esta página, suscríbase al RSS feed de la página del historial del AWS Artifact documento.

Cambio	Descripción	Fecha
AWS Artifact comenzó a rastrear los cambios	AWS Artifact comenzó a rastrear los cambios de sus políticas AWS gestionadas y las introdujo AWSArtifactReportsReadOnlyAccess.	15 de diciembre de 2023
Se introdujeron acuerdos AWS y políticas gestionadas	Políticas introducidas AWSArtifactAgreementsReadOnlyAccess y AWSArtifactAgreementsFullAccess gestionadas.	2024-11-21

Uso de roles vinculados a servicios de AWS Artifact

AWS Artifact usa AWS Identity and Access Management (IAM) roles vinculados al servicio. Un rol vinculado a un servicio es un tipo único de IAM rol al que se vincula directamente. AWS Artifact Los roles vinculados al servicio están predefinidos AWS Artifact e incluyen todos los permisos que el servicio requiere para llamar a otros AWS servicios en tu nombre.

Un rol vinculado a un servicio facilita la configuración AWS Artifact , ya que no es necesario añadir manualmente los permisos necesarios. AWS Artifact define los permisos de sus funciones vinculadas al servicio y, a menos que se defina lo contrario, solo AWS Artifact puede asumir sus funciones. Los permisos definidos incluyen la política de confianza y la política de permisos, y esa política de permisos no se puede adjuntar a ninguna otra IAM entidad.

Solo puede eliminar un rol vinculado a servicios después de eliminar sus recursos relacionados. Esto protege tus AWS Artifact recursos porque no puedes eliminar inadvertidamente el permiso de acceso a los recursos.

Para obtener información sobre otros servicios que admiten funciones vinculadas a servicios, consulta los AWS servicios que funcionan con ellas IAM y busca los servicios con la palabra Sí en la columna Funciones vinculadas a servicios. Elija una opción Sí con un enlace para ver la documentación acerca del rol vinculado a servicios en cuestión.

Permisos de roles vinculados al servicio para AWS Artifact

AWS Artifact utiliza el rol vinculado al servicio denominado AWSServiceRoleForArtifact: permite recopilar información sobre AWS Artifact una organización mediante. AWS Organizations

El rol AWSServiceRoleForArtifact vinculado al servicio confía en los siguientes servicios para asumir el rol:

- `artifact.amazonaws.com`

La política de permisos de roles denominada AWSArtifactServiceRolePolicy permite AWS Artifact realizar las siguientes acciones en el `organizations` recurso.

- `DescribeOrganization`
- `DescribeAccount`
- `ListAccounts`
- `ListAWSServiceAccessForOrganization`

Crear un rol vinculado a un servicio para AWS Artifact

No necesita crear manualmente un rol vinculado a servicios. Si vas a la pestaña Acuerdos organizativos de una cuenta de administración de la organización y seleccionas el enlace Comenzar en ella AWS Management Console, se AWS Artifact crea automáticamente el rol vinculado al servicio.

Si elimina este rol vinculado a servicios y necesita crearlo de nuevo, puede utilizar el mismo proceso para volver a crear el rol en su cuenta. Si vas a la pestaña Acuerdos organizativos de una cuenta de administración de la organización y seleccionas el enlace Comenzar, vuelve a AWS Artifact crearte el rol vinculado al servicio.

Editar un rol vinculado a un servicio para AWS Artifact

AWS Artifact no permite editar el rol vinculado al AWSServiceRoleForArtifact servicio. Después de crear un rol vinculado a un servicio, no podrá cambiar el nombre del rol, ya que varias entidades podrían hacer referencia al mismo. Sin embargo, puede editar la descripción del rol utilizando. IAM Para obtener más información, consulte Edición de un rol vinculado a un servicio en la Guía del IAMusuario.

Eliminar un rol vinculado a un servicio para AWS Artifact

Si ya no necesita utilizar una característica o servicio que requiere un rol vinculado a un servicio, le recomendamos que elimine dicho rol. De esta forma no tiene una entidad no utilizada que no se monitoree ni mantenga de forma activa. Sin embargo, debe limpiar los recursos del rol vinculado al servicio antes de eliminarlo manualmente.

> **Note**
>
> Si el AWS Artifact servicio utiliza el rol al intentar eliminar los recursos, es posible que la eliminación no se realice correctamente. En tal caso, espere unos minutos e intente de nuevo la operación.

Para eliminar AWS Artifact los recursos utilizados por el AWSServiceRoleForArtifact

1. Visite la tabla de «Acuerdos de organización» en la consola AWS Artifact
2. Rescinda cualquier acuerdo de Organización activo

Para eliminar manualmente el rol vinculado al servicio mediante IAM

Utilice la IAM consola AWS CLI, la o la AWS API para eliminar la función vinculada al AWSServiceRoleForArtifact servicio. Para obtener más información, consulte Eliminar un rol vinculado a un servicio en la Guía del usuario. IAM

Regiones compatibles para AWS Artifact los roles vinculados al servicio

AWS Artifact no admite el uso de funciones vinculadas al servicio en todas las regiones en las que el servicio esté disponible. Puede usar el AWSServiceRoleForArtifact rol en las siguientes regiones.

Nombres de las regiones	Identidad de la región	Support en AWS Artifact
Este de EE. UU. (Norte de Virginia)	us-east-1	Sí
Este de EE. UU. (Ohio)	us-east-2	No
Oeste de EE. UU. (Norte de California)	us-west-1	No
Oeste de EE. UU. (Oregón)	us-west-2	Sí
África (Ciudad del Cabo)	af-south-1	No
Asia-Pacífico (Hong Kong)	ap-east-1	No
Asia-Pacífico (Yakarta)	ap-southeast-3	No
Asia-Pacífico (Bombay)	ap-south-1	No
Asia Pacífico (Osaka)	ap-northeast-3	No
Asia Pacífico (Seúl)	ap-northeast-2	No
Asia-Pacífico (Singapur)	ap-southeast-1	No
Asia Pacífico (Sídney)	ap-southeast-2	No
Asia-Pacífico (Tokio)	ap-northeast-1	No
Canadá (centro)	ca-central-1	No
Europa (Fráncfort)	eu-central-1	No

Nombres de las regiones	Identidad de la región	Support en AWS Artifact
Europa (Irlanda)	eu-west-1	No
Europa (Londres)	eu-west-2	No
Europa (Milán)	eu-south-1	No
Europa (París)	eu-west-3	No
Europa (Estocolmo)	eu-north-1	No
Medio Oriente (Baréin)	me-south-1	No
Oriente Medio (UAE)	me-central-1	No
América del Sur (São Paulo)	sa-east-1	No
AWS GovCloud (EEUU-Este)	us-gov-east-1	No
AWS GovCloud (Estados Unidos-Oeste)	us-gov-west-1	No

Uso de claves de IAM condición para AWS Artifact los informes

Puede utilizar las claves de IAM condición para proporcionar un acceso detallado a los informes AWS Artifact, en función de categorías y series de informes específicas.

Los siguientes ejemplos de políticas muestran los permisos que puede asignar a IAM los usuarios en función de categorías y series de informes específicas.

Example Ejemplos de políticas para administrar el acceso de lectura a AWS los informes

AWS Artifact los informes se indican mediante el IAM recurso,`report`.

La siguiente política otorga permiso para leer todos los AWS Artifact informes de la `Certifications and Attestations` categoría.

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

```
      "Effect": "Allow",
      "Action": [
        "artifact:ListReports"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "artifact:GetReport",
        "artifact:GetReportMetadata",
        "artifact:GetTermForReport"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "artifact:ReportCategory": "Certifications and Attestations"
        }
      }
    }
  ]
}
```

La siguiente política le permite conceder permiso para leer todos los AWS Artifact informes de la SOC serie.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "artifact:ListReports"
            ],
            "Resource": "*"
        },{
            "Effect": "Allow",
            "Action": [
                "artifact:GetReport",
                "artifact:GetReportMetadata",
                "artifact:GetTermForReport"
            ],
            "Resource": [
```

```
                "*"
            ],
            "Condition": {
                "StringEquals": {
                    "artifact:ReportSeries": "SOC",
                    "artifact:ReportCategory": "Certifications and Attestations"
                }
            }
        }
    ]
}
```

La siguiente política le permite conceder permiso para leer todos los AWS Artifact informes excepto los de la `Certifications and Attestations` categoría.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:ListReports"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "artifact:GetReport",
        "artifact:GetReportMetadata",
        "artifact:GetTermForReport"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "artifact:ReportSeries": "SOC",
          "artifact:ReportCategory": "Certifications and Attestations"
        }
      }
    }
  ]
}
```

Registrar AWS Artifact API llamadas con AWS CloudTrail

AWS Artifact está integrado con AWS CloudTrail un servicio que proporciona un registro de las acciones realizadas por un usuario, un rol o un AWS servicio en AWS Artifact. CloudTrail captura API las llamadas AWS Artifact como eventos. Las llamadas capturadas incluyen llamadas desde la AWS Artifact consola y llamadas en código a las AWS Artifact API operaciones. Si crea una ruta, puede habilitar la entrega continua de CloudTrail eventos a un bucket de Amazon S3, incluidos los eventos para AWS Artifact. Si no configura una ruta, podrá ver los eventos más recientes en la CloudTrail consola, en el historial de eventos. Con la información recopilada por usted CloudTrail, puede determinar a AWS Artifact qué dirección IP se realizó la solicitud, quién la realizó, cuándo se realizó y detalles adicionales.

Para obtener más información CloudTrail, consulte la Guía AWS CloudTrail del usuario.

AWS Artifact información en CloudTrail

CloudTrail está habilitada en tu cuenta Cuenta de AWS al crear la cuenta. Cuando se produce una actividad en AWS Artifact, esa actividad se registra en un CloudTrail evento junto con otros eventos de AWS servicio en el historial de eventos. Puede ver, buscar y descargar eventos recientes en su Cuenta de AWS. Para obtener más información, consulte Visualización de eventos con el historial de CloudTrail eventos.

Para tener un registro continuo de tus eventos Cuenta de AWS, incluidos los eventos para AWS Artifact ti, crea una ruta. Un rastro permite CloudTrail entregar archivos de registro a un bucket de Amazon S3. De forma predeterminada, cuando se crea un registro de seguimiento en la consola, el registro de seguimiento se aplica a todas las Regiones de AWS. La ruta registra los eventos de todas las regiones de la AWS partición y envía los archivos de registro al bucket de Amazon S3 que especifique. Además, puede configurar otros AWS servicios para analizar más a fondo los datos de eventos recopilados en los CloudTrail registros y actuar en función de ellos. Para más información, consulte los siguientes temas:

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

AWS Artifact admite el registro de las siguientes acciones como eventos en los archivos de CloudTrail registro:

- ListReports
- GetAccountSettings
- GetReportMetadata
- GetReport
- GetTermForReport
- PutAccountSettings
- AcceptAgreement
- AcceptNdaForAgreement
- GetAgreement
- GetCustomerAgreement
- GetNdaForAgreement
- ListAgreements
- ListCustomerAgreements
- TerminateAgreement

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

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

Para obtener más información, consulte el CloudTrail userIdentityelemento.

Descripción de las entradas de los archivos de AWS Artifact registro

Un rastro es una configuración que permite la entrega de eventos como archivos de registro a un bucket de Amazon S3 que usted especifique. CloudTrail Los archivos de registro contienen una o

más entradas de registro. Un evento representa una solicitud única de cualquier fuente e incluye información sobre la acción solicitada, la fecha y la hora de la acción, los parámetros de la solicitud, etc. CloudTrail Los archivos de registro no son un registro ordenado de las API llamadas públicas, por lo que no aparecen en ningún orden específico.

El siguiente ejemplo muestra una entrada de CloudTrail registro que demuestra la GetReportMetadata acción.


```
{
  "Records": [
    {
      "eventVersion": "1.03",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "A1B2C3D4E5F6G7EXAMPLE",
        "arn": "arn:aws:iam::999999999999:user/myUserName",
        "accountId": "999999999999",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "myUserName"
      },
      "eventTime": "2015-03-18T19:03:36Z",
      "eventSource": "artifact.amazonaws.com",
      "eventName": "GetReportMetadata",
      "awsRegion": "us-east-1",
      "sourceIPAddress": "127.0.0.1",
      "userAgent": "Python-httplib2/0.8 (gzip)",
      "errorCode": "AccessDenied",
      "errorMessage": "User: arn:aws:iam::999999999999:user/myUserName is not
 authorized to perform: artifact:GetReportMetadata on resource: arn:aws:artifact:us-
east-1::report/report-f1DIWBmGa2Lhsadg",
      "requestParameters": null,
      "responseElements": null,
      "requestID": "7aebcd0f-cda1-11e4-aaa2-e356da31e4ff",
      "eventID": "e92a3e85-8ecd-4d23-8074-843aabfe89bf",
      "eventType": "AwsApiCall",
      "recipientAccountId": "999999999999"
    },
    {
      "eventVersion": "1.03",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "A1B2C3D4E5F6G7EXAMPLE",
```

```
        "arn": "arn:aws:iam::999999999999:user/myUserName",
        "accountId": "999999999999",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "myUserName"
      },
      "eventTime": "2015-03-18T19:04:42Z",
      "eventSource": "artifact.amazonaws.com",
      "eventName": "GetReportMetadata",
      "awsRegion": "us-east-1",
      "sourceIPAddress": "127.0.0.1",
      "userAgent": "Python-httplib2/0.8 (gzip)",
      "requestParameters": {
        "reportId": "report-f1DIWBmGa2Lhsadg"
      },
      "responseElements": null,
      "requestID": "a2198ecc-cda1-11e4-aaa2-e356da31e4ff",
      "eventID": "20b84ce5-730f-482e-b2b2-e8fcc87ceb22",
      "eventType": "AwsApiCall",
      "recipientAccountId": "999999999999"
    }
  ]
}
```

Historial de documentos para AWS Artifact

La siguiente tabla proporciona un historial de las AWS Artifact versiones y los cambios relacionados en la Guía del AWS Artifact usuario.

Cambio	Descripción	Fecha
Permisos detallados para la ejecución de acuerdos y políticas gestionadas AWSArtifactAgreementsFullAccess AWSArtifactAgreementsReadOnlyAccess	Permitió un acceso detallado para la ejecución de los AWS Artifact acuerdos y las políticas lanzadas y gestionadas. AWSArtifactAgreementsFullAccess AWSArtifactAgreementsReadOnlyAccess AWS	21 de noviembre de 2024
Acceso detallado a los informes y política gestionada AWSArtifactReportReadOnlyAccess	Se habilitó el acceso detallado a los informes, se habilitaron las claves de condición de AWS Artifact los informes y se lanzó una política gestionada. AWSArtifactReportsReadOnlyAccess	15 de diciembre de 2023
AWS Artifact función vinculada al servicio	Se ha añadido documentación sobre las funciones vinculadas al servicio y se han actualizado ejemplos de políticas de integración. AWS Artifact AWS Organizations	26 de septiembre de 2023
Notificaciones	Publicó la documentación para gestionar las notificaciones y realizó las actualizaciones pertinentes en la AWS Artifact API referencia, la documentación de CloudTrail registro y la	1 de agosto de 2023

	página de gestión de identidad es y accesos.	
Informes de terceros: disponibl es en general	Se agregó la documenta ción de API referencia y la documentación de CloudTrai l registro, y se pusieron a disposición del público general los informes de terceros.	27 de enero de 2023
Informes de terceros (versión preliminar)	Publicó los informes de conformidad de los proveedor es de software independi entes (ISVs) que venden sus productos en AWS Marketpla ce. Se agregaron ejemplos de políticas a la página de administración de identidades y accesos para informes de terceros.	30 de noviembre de 2022
Seguridad	Se agregó una sección a la página de administración de identidad y acceso para evitar problemas de acceso.	20 de diciembre de 2021
Informes	Se eliminó el acuerdo de confidencialidad e introdujeron términos y condiciones para la descarga de informes.	17 de diciembre de 2020
Página de inicio y búsqueda	Se han añadido la página de inicio del servicio y la barra de búsqueda en la página de informes y acuerdos.	15 de mayo de 2020
GovCloud lanzar	Lanzado AWS Artifact en AWS GovCloud (US) Regions.	7 de noviembre de 2019

AWS Organizations acuerdos	Se ha añadido soporte para administrar los acuerdos de una organización.	20 de junio de 2018
Acuerdos	Se ha añadido soporte para la gestión de AWS Artifact acuerdos.	17 de junio de 2017
Versión inicial	Esta versión introduce AWS Artifact.	30 de noviembre de 2016

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