Guía del usuario

AWS Artifact

AWS Artifact: Guía del usuario

Table of Contents

¿Qué es AWS Artifact? 1
Precios 1
Introducción 2
Paso 1: Inscríbase en AWS 2
Paso 2: Descargar un informe 3
Paso 3: Administrar acuerdos 4
Paso 4: Administrar notificaciones 4
Descarga de informes 6
Descarga de un informe 6
Visualización de archivos adjuntos en documentos PDF 7
Protección de los documentos 8
Solución de problemas 8
Administración de acuerdos 9
Acuerdos para una sola cuenta 9
Aceptación de un acuerdo con AWS 9
Rescisión de un acuerdo con AWS 10
Acuerdos para varias cuentas 11
Aceptación de un acuerdo de su organización 12
Rescisión de un acuerdo de la organización 13
Acuerdos sin conexión 13
Administración de las notificaciones 15
Configuración de sus notificaciones 15
Asignación de etiquetas a una configuración 17
Solución de problemas 17
Administración de identidades y accesos 18
Configure el acceso de los usuarios a AWS Artifact 18
Paso 1: Crear una política de IAM 19
Paso 2: Crear un grupo IAM y adjuntar la política 19
Paso 3: Crear usuarios de IAM y añadirlos al grupo 20
Migración a permisos detallados 20
Migración a nuevos permisos 21
Ejemplos de políticas de IAM 23
Uso de políticas administradas de AWS 36
AWSArtifactReportsReadOnlyAccess 37

Actualizaciones de políticas 38
Uso de roles vinculados a servicios 38
Permisos de roles vinculados a servicios para AWS Artifact 39
Creación de un rol vinculado a un servicio para AWS Artifact 39
Modificación de un rol vinculado a un servicio para AWS Artifact 40
Eliminación de un rol vinculado a un servicio para AWS Artifact 40
Regiones admitidas para roles vinculados a servicios AWS Artifact 41
Uso de claves de condición de IAM 42
Registros de CloudTrail 45
..... 45
Información de AWS Artifact en CloudTrail 45
Descripción de las entradas de los archivos de registro de AWS Artifact 46
Historial de revisión 49
..... lii

¿Qué es AWS Artifact?

AWS Artifact proporciona descargas bajo demanda de documentos de seguridad y conformidad de AWS, como certificaciones ISO de AWS, informes del Industria de tarjetas de pago (PCI) e informes de Control de organización de servicios (SOC). Puede enviar los documentos de seguridad y conformidad (también conocidos como elementos de auditoría) a los auditores o a las autoridades reguladoras para demostrar la seguridad y la conformidad de la infraestructura de AWS y los servicios que utiliza. También puede emplear estos documentos como directrices para evaluar su propia arquitectura de nube y valorar la eficacia de los controles internos de la empresa.

Además, AWS Artifact ofrece descargas a pedido de los documentos de seguridad y conformidad, como las certificaciones ISO y los informes de Control de organización de servicios (SOC) de los proveedores de software independientes (ISV) que venden sus productos en AWS Marketplace. Para obtener más información, consulte AWS Marketplace Vendor Insights.

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

También puede utilizar AWS Artifact para revisar, aceptar y rastrear el estado de los acuerdos de AWS, como el BAA (Business Associate Addendum). Un BAA suele ser necesario para las empresas sujetas a la ley estadounidense de portabilidad y responsabilidad de los seguros médicos (HIPAA, Health Insurance Portability and Accountability Act) para garantizar que la información sanitaria protegida (PHI) esté convenientemente a salvo. Con AWS Artifact, puede aceptar los acuerdos con AWS y designar cuentas de AWS que puedan procesar legalmente información restringida. Puede aceptar un acuerdo en nombre de varias cuentas. Para aceptar acuerdos de varias cuentas, use AWS Organizations para crear una organización.

Para obtener más información, consulte AWS Artifact.

Precios

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

Empezar con AWS Artifact

AWS Artifact proporciona un recurso central para los informes AWS de seguridad y conformidad. Entre los recursos disponibles se AWS Artifact incluyen los informes de control de la organización de servicios (SOC), los informes del sector de tarjetas de pago (PCI) y las certificaciones de los organismos de acreditación que validan la implementación y la eficacia operativa de los controles de AWS seguridad. Además, AWS Artifact proporciona acceso bajo demanda a los documentos de seguridad y conformidad, como las certificaciones ISO y los informes de control de la organización de servicios (SOC) de los proveedores de software independientes (ISV) que venden sus productos. AWS Marketplace Para obtener más información, consulte AWS Marketplace Vendor Insights.

AWS Artifact le permite aceptar y gestionar acuerdos legales, como el apéndice sobre socios comerciales (BAA). Si lo utiliza AWS Organizations, puede aceptar acuerdos en nombre de todas las cuentas de su organización. Cuando los acepte, todas las cuentas miembro existentes y posteriores estarán cubiertas automáticamente por el acuerdo.

Tareas

- Paso 1: Inscríbase en AWS
- Paso 2: Descargar un informe
- Paso 3: Administrar acuerdos
- Paso 4: Administrar notificaciones

Paso 1: Inscríbase en AWS

Si no tiene uno Cuenta de AWS, complete los siguientes pasos para crearlo.

Para suscribirte a una Cuenta de AWS

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 e indicar un código de verificación en el teclado del teléfono.

   Cuando te registras en una Cuenta de AWS, Usuario raíz de la cuenta de AWSse crea una. El usuario raíz tendrá acceso a todos los Servicios de AWS y recursos de esa cuenta. Como

práctica recomendada de seguridad, asigne acceso administrativo a un usuario y utilice únicamente al usuario root para realizar tareas que requieran dicho acceso.

Paso 2: Descargar un informe

Puede descargar los informes con Adobe Acrobat Reader. No se admite ningún otro lector de PDF. Para obtener más información, consulte Descarga de informes.

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.
3. En la página de informes, utilice la pestaña de AWS informes para acceder a un AWS informe y vaya a la pestaña de informes de terceros para acceder a los informes de los proveedores de software independientes (ISV) que venden sus productos. AWS Marketplace
4. (Opcional) Introduzca una palabra clave en el campo de búsqueda para buscar un informe.
5. Seleccione un informe y, a continuación, elija Descargar informe.
6. (Opcional) En la pestaña Informes de terceros, puede acceder a la página de detalles de un informe de ISV la hacer clic en el título del Informe para obtener más información sobre el mismo.
7. Es posible que se le pida que acepte los Términos y condiciones que se aplican al informe específico que está descargando. Le recomendamos que los lea atentamente. Cuando haya terminado, seleccione He leído y acepto los términos y, a continuación, seleccione Aceptar los términos y descargar el informe.
8. Abra el archivo descargado con un visor de PDF. 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 documento PDF, así que compruebe si hay archivos adjuntos en el archivo PDF para obtener la documentación complementaria. Consulte aquí las instrucciones sobre cómo ver los archivos adjuntos.

Los informes de terceros solo son accesibles para AWS los clientes que se hayan incorporado a AWS Marketplace Vendor Insights. Para obtener más información, consulta AWS Marketplace Vendor Insights .

Paso 3: Administrar acuerdos

Antes de celebrar un acuerdo, debe descargar y aceptar los términos del acuerdo de confidencialidad (NDA) de AWS Artifact . Cada acuerdo es confidencial y no se puede compartir con otras personas ajenas a su empresa.

Para aceptar un acuerdo 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 Acuerdos de cuenta para gestionar los acuerdos de su cuenta o Acuerdos de organización para gestionar los acuerdos en nombre de su organización.
4. Amplíe la sección del acuerdo.
5. Seleccione Descargar y revisar.
6. Lea la sección Términos y condiciones. Cuando haya terminado, seleccione Aceptar y descargar.
7. Revise el acuerdo y, a continuación, seleccione las casillas de verificación para indicar que está de acuerdo.
8. Seleccione Aceptar para aceptar el acuerdo.

Para obtener más información, consulte Administración de acuerdos.

Paso 4: Administrar notificaciones

Puede suscribirse a las notificaciones para comprobar la disponibilidad de nuevos informes y acuerdos o de actualizaciones de los informes y acuerdos existentes. AWS Artifact utiliza el servicio de notificación de usuarios de AWS para enviar notificaciones. Las notificaciones se envían a las direcciones de correo electrónico que el usuario proporciona durante la configuración de las notificaciones.

Para crear una configuración

1. Abra la página de centros de notificaciones en el servicio de notificaciones de usuarios de AWS
2. Seleccione la(s) región(es) donde desea almacenar sus recursos de notificaciones de usuarios de AWS. De forma predeterminada, los datos de las notificaciones de usuario se almacenarán

en el Este de EE. UU. (Norte de Virginia) y se replicarán en las demás regiones que seleccione. Consulte la documentación de los centros de notificaciones para obtener más información.

3. Haga clic en Crear configuración.
4. Para recibir notificaciones de acuerdos, haga clic en la casilla de verificación Actualizaciones en los acuerdos de AWS.
5. Para recibir notificaciones de informes, haga clic en la casilla de verificación Actualizaciones en los informes de AWS. Para recibir únicamente notificaciones de informes de categorías y series específicas, haga clic en la casilla de verificación de Un subconjunto de informes y, a continuación, haga clic en la casilla de verificación de las categorías y series que le interesen.
6. Ingrese un nombre para su configuración.
7. Introduzca una lista de correos electrónicos separados por comas a los que deben enviarse las notificaciones.
8. (Opcional) Para asignar una etiqueta a la configuración de notificaciones, introduzca los pares clave-valor si expande la sección Etiquetas. Nota: Una etiqueta puede asignar a un recurso de AWS y cada etiqueta consta de una clave y un valor opcional que puede definir. Las etiquetas le ayudan a administrar, buscar y filtrar sus recursos.
9. Haga clic en Submit.
10. Se enviará un correo electrónico de verificación a las direcciones de correo electrónico proporcionadas y los destinatarios del correo electrónico deberán hacer clic en el enlace Verificar correo electrónico incluido en el correo de verificación que se les envíe. Tenga en cuenta que solo las direcciones de correo electrónico verificadas comenzarán a recibir notificaciones.

Para obtener más información, consulte Administración de las notificaciones.

Descarga de informes en AWS Artifact

Puede descargar informes desde la consola de AWS Artifact. Cuando descarga un informe de AWS Artifact, dicho 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. Si necesita compartir un informe, utilice un servicio de uso compartido seguro, como Amazon WorkDocs. Algunos informes requieren que acepte los Términos y condiciones antes de poder descargarlos.

Contenido

- Descarga de un informe
- Visualización de archivos adjuntos en documentos PDF
- Protección de los documentos
- Solución de problemas

Descarga de un informe

Para descargar un informe, debe contar con los permisos requeridos. Para obtener más información, consulte Administración de identidades y accesos en AWS Artifact.

Cuando se inscribe en AWS Artifact, automáticamente se conceden los permisos necesarios a su cuenta para descargar algunos informes. Si tiene problemas para acceder a AWS Artifact, siga las instrucciones de la página de Referencia de autorizaciones de servicio de AWS Artifact.

Para descargar un informe

1. Abra la consola de AWS Artifact en https://console.aws.amazon.com/artifact/.
2. En la página de inicio de AWS Artifact, seleccione Visualización de informes.
3. En la página de Informes, utilice la pestaña Informes de AWS para acceder a un AWS informe y vaya a la pestaña Informes de terceros para acceder a los informes de Proveedores de software independientes (ISV) que venden sus productos en AWS Marketplace.
4. (Opcional) Introduzca una palabra clave en el campo de búsqueda para buscar un informe.
5. Seleccione un informe y, a continuación, elija Descargar informe.

6. (Opcional) En la pestaña Informes de terceros, puede acceder a la página de detalles de un informe de ISV la hacer clic en el título del Informe para obtener más información sobre el mismo.
7. Es posible que se le pida que acepte los Términos y condiciones que se aplican al informe específico que está descargando. Le recomendamos que los lea atentamente. Cuando haya terminado, seleccione He leído y acepto los términos y, a continuación, seleccione Aceptar los términos y descargar el informe.
8. Abra el archivo descargado con un visor de PDF. 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 documento PDF, así que compruebe si hay archivos adjuntos en el archivo PDF para obtener la documentación complementaria. Consulte aquí las instrucciones sobre cómo ver los archivos adjuntos.

Visualización de archivos adjuntos en documentos PDF

Se recomiendan las siguientes aplicaciones que actualmente admiten la visualización de archivos adjuntos en PDF:

Visor de Adobe Acrobat

1. Descargue la versión más reciente de Adobe Acrobat desde aquí.
2. Abra el archivo en el lector de Adobe Acrobat.
3. Para abrir el panel Archivos adjuntos, haga clic en el icono con forma de clip situado a la izquierda del documento PDF o seleccione Ver > Mostrar/Ocultar > Paneles de navegación > Archivos adjuntos.
4. En el panel Archivos adjuntos, haga doble clic en el archivo adjunto para ver el documento.

Navegador Firefox

1. Descargue el navegador Firefox desde aquí
2. Abra el archivo PDF en el navegador Firefox mediante la opción abrir archivo del menú Archivo.
3. Para abrir los archivos adjuntos, haga clic en el icono de la barra lateral situada en la parte superior izquierda de la pantalla.

Protección de los documentos

Los documentos de AWS Artifact son confidenciales y deben estar protegidos en todo momento. AWS Artifact usa el modelo de responsabilidad compartida de AWS para sus documentos. Esto significa que AWS es responsable de mantener los documentos protegidos mientras se encuentran en la nube de AWS, pero que la responsabilidad recae en usted cuando los descarga. AWS Artifactpueden exigirle que acepte los Términos y condiciones antes de poder descargar 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 de uso compartido de documentos seguro, 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.

Solución de problemas

Si no puede descargar un documento o recibir un mensaje de error, consulte la sección Solución de problemas en las preguntas frecuentes de AWS Artifact.

Administración de acuerdos en AWS Artifact

AWS Artifact Agreements le permite usar la AWS Management Console para revisar, aceptar y administrar acuerdos de su cuenta u organización. Por ejemplo, un acuerdo BAA (Business Associate Addendum) suele ser necesario para las empresas sujetas a la ley estadounidense de portabilidad y responsabilidad de los seguros médicos (HIPAA, Health Insurance Portability and Accountability Act) para garantizar que la información sanitaria protegida (PHI) esté convenientemente a salvo. Puede utilizar AWS Artifact para firmar un acuerdo como el acuerdo BAA con AWS y designar una cuenta de AWS que pueda procesar información sanitaria protegida (PHI) legalmente. Si utiliza AWS Organizations puede aceptar acuerdos como el BAA de AWS en nombre de todas las cuentas de la organización. Todas las cuentas miembro existentes y posteriores estarán cubiertas automáticamente por el acuerdo y podrán procesar PHI legalmente.

También puede usar AWS Artifact para confirmar que su cuenta de AWS u organización ha aceptado un acuerdo y para revisar las condiciones del acuerdo aceptado para conocer sus obligaciones. Si su cuenta u organización ya no necesita usar el acuerdo aceptado, puede utilizar AWS Artifact para rescindir el acuerdo. Si termina el contrato pero después lo necesita, puede activarlo de nuevo.

Contenido

- Administración de un acuerdo para una sola cuenta en AWS Artifact
- Administración de un acuerdo para varias cuentas en AWS Artifact
- Administración de un acuerdo sin conexión existente en AWS Artifact

Administración de un acuerdo para una sola cuenta en AWS Artifact

Puede aceptar acuerdos solo para su cuenta aunque su cuenta sea una cuenta miembro de una organización en AWS Organizations. Para obtener más información sobre AWS Organizations, consulte la AWS OrganizationsGuía del usuario de .

Aceptación de un acuerdo con AWS

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

Permisos necesarios

Si usted es un administrador de una cuenta, puede conceder a los usuarios de IAM y federados con funciones los permisos para obtener acceso y administrar uno o varios de sus acuerdos. De forma predeterminada, solo los usuarios con privilegios administrativos pueden aceptar un acuerdo. Para aceptar un acuerdo, los usuarios de IAM y federados deben tener los siguientes permisos:

```
artifact:DownloadAgreement
artifact:AcceptAgreement
```

Para obtener más información, consulte Administración de identidades y accesos.

Para aceptar un acuerdo con AWS

1. Abra la consola de AWS Artifact en https://console.aws.amazon.com/artifact/.
2. En el panel de navegación de AWS Artifact, seleccione Agreements (Acuerdos).
3. Elija la pestaña Account agreements (Acuerdos de la cuenta).
4. Amplíe la sección del acuerdo.
5. Seleccione Descargar y revisar.
6. Lea la sección Términos y condiciones. Cuando haya terminado, seleccione Aceptar y descargar.
7. Revise el acuerdo y, a continuación, seleccione las casillas de verificación para indicar que está de acuerdo.
8. Elija Aceptar para aceptar el acuerdo de su cuenta.

Rescisión de un acuerdo con AWS

Si ha utilizado la consola de AWS Artifact para aceptar un acuerdo, puede usar la consola para rescindirlo. De lo contrario, consulte Acuerdos sin conexión.

Permisos necesarios

Para rescindir un acuerdo, los usuarios de IAM y federados deben tener los siguientes permisos:

```
artifact:TerminateAgreement
```

Para obtener más información, consulte Administración de identidades y accesos.

Para rescindir su acuerdo online con AWS

1. Abra la consola de AWS Artifact en https://console.aws.amazon.com/artifact/.
2. En el panel de navegación de AWS Artifact, seleccione Agreements (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 Terminate (Terminar). Cuando se le indique que confirme, elija Terminate (Rescindir).

Administración de un acuerdo para varias cuentas en AWS Artifact

Si es el propietario de la cuenta de administración de una organización de AWS Organizations, puede aceptar un acuerdo en nombre de todas las cuentas de su organización. Debe iniciar sesión en la cuenta de administración con los permisos de AWS Artifact correctos para aceptar o rescindir acuerdos de la organización. Los usuarios de cuentas miembro con permisos `organizations:DescribeOrganization` pueden consultar los acuerdos de la organización que se aceptan en su nombre.

Si su cuenta no forma parte de una organización, puede crear o unirse a una organización siguiendo las instrucciones que se indican en Creación y administración de una organización en la Guía del usuario de AWS Organizations .

AWS Organizations tiene dos conjuntos de características disponibles: características de facturación unificada y todas las características. Para utilizar AWS Artifact para su organización, la organización a la que pertenezca debe estar habilitada para todas las características. 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.

Si una cuenta miembro se elimina de una organización, dicha cuenta miembro ya no estará cubierta por los acuerdos de la organización. Los administradores de cuentas de administración deben comunicar esto a las cuentas miembro antes de eliminar las cuentas miembro de la organización, para que dichas cuentas miembro puedan formalizar nuevos acuerdos si es necesario. Puede consultar una lista de los acuerdos activos de la organización en Acuerdos de la organización de AWS Artifact.

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

Aceptación de un acuerdo de su organización

Puede aceptar un acuerdo en nombre de todas las cuentas miembro de su organización en AWS Organizations. Antes de aceptar un acuerdo, le recomendamos que se ponga en contacto con su equipo jurídico, de privacidad y de conformidad.

Permisos necesarios

Para aceptar un acuerdo, el propietario de la cuenta de administración debe disponer de los siguientes permisos:

```
artifact:DownloadAgreement
artifact:AcceptAgreement
organizations:DescribeOrganization
organizations:EnableAWSServiceAccess
organizations:ListAWSServiceAccessForOrganization
iam:ListRoles
iam:CreateServiceLinkedRole
```

Para obtener más información, consulte Administración de identidades y accesos.

Para aceptar un acuerdo de una organización

1. Abra la consola de AWS Artifact en https://console.aws.amazon.com/artifact/.
2. En el panel de AWS Artifact, seleccione Agreements (Acuerdos).
3. Elija la pestaña Organization agreements (Acuerdos de la organización).
4. Amplíe la sección del acuerdo.
5. Seleccione Descargar y revisar.
6. Lea la sección Términos y condiciones. Cuando haya terminado, seleccione Aceptar y descargar.
7. Revise el acuerdo y, a continuación, seleccione las casillas de verificación para indicar que está de acuerdo.
8. Elija Accept (Aceptar) para aceptar el acuerdo de todas las cuentas existentes y futuras de su organización.

Rescisión de un acuerdo de la organización

Si ha usado la consola de AWS Artifact para aceptar un acuerdo en nombre de todas las cuentas miembro de una organización, puede usar la consola para rescindir el acuerdo. De lo contrario, consulte Acuerdos sin conexión.

Permisos necesarios

Para rescindir un acuerdo, el propietario de la cuenta de administración debe disponer de los siguientes permisos:

```
artifact:DownloadAgreement
artifact:TerminateAgreement
organizations:DescribeOrganization
organizations:EnableAWSServiceAccess
organizations:ListAWSServiceAccessForOrganization
iam:ListRoles
iam:CreateServiceLinkedRole
```

Para obtener más información, consulte Administración de identidades y accesos.

Para rescindir el acuerdo de su organización online con AWS

1. Abra la consola de AWS Artifact en https://console.aws.amazon.com/artifact/.
2. En el panel de AWS Artifact, seleccione Agreements (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 Terminate (Terminar). Cuando se le indique que confirme, elija Terminate (Rescindir).

Administración de un acuerdo sin conexión existente en AWS Artifact

Si tiene un acuerdo sin conexión existente, AWS Artifact muestra los acuerdos que ha aceptado sin conexión. Por ejemplo, en la consola se podría mostrar el acuerdo Offline Business Associate Addendum (BAA) con el estado Active (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 organización de AWS Organizations, puede usar AWS Artifact para aplicar las condiciones de su contrato sin conexión a todas las cuentas de su organización. Para aplicar un acuerdo que ha aceptado sin conexión a su organización y a todas las cuentas de su organización, debe tener los siguientes permisos:

```
organizations:DescribeOrganization
organizations:EnableAWSServiceAccess
organizations:ListAWSServiceAccessForOrganization
iam:ListRoles
iam:CreateServiceLinkedRole
```

Si su cuenta es una cuenta miembro de una organización, debe tener los siguientes permisos para ver los acuerdos de la organización sin conexión:

```
organizations:DescribeOrganization
```

Para obtener más información, consulte Administración de identidades y accesos.

Administración de las notificaciones en AWS Artifact

Las notificaciones de AWS Artifact le permiten configurar las notificaciones por correo electrónico. En la página de configuración de notificaciones, puede suscribirse a las notificaciones y administrar otras configuraciones de notificaciones como se describe a continuación. AWS Artifact envía las notificaciones mediante el servicio de notificaciones de usuarios de AWS. Para usar las notificaciones de AWS Artifact, debe tener los permisos necesarios para los servicios AWS Artifact y las Notificaciones de usuarios de AWS. Para obtener más información, consulte Administración de identidades y accesos.

Contenido

- Configuración de sus notificaciones
- Asignación de etiquetas a una configuración
- Solución de problemas

Configuración de sus notificaciones

Antes de empezar a recibir notificaciones, tendrás que especificar las regiones en las que se almacenarán los datos de las Notificaciones de usuarios. Siga los pasos que se indican a continuación para configurar centros de notificaciones.

Para configurar la Notificación de hubs

1. Abra la página de centros de notificaciones en el servicio de Notificaciones de usuarios de AWS.
2. Seleccione la(s) región(es) en la(s) que desea almacenar sus recursos de notificaciones de usuarios de AWS. De forma predeterminada, sus datos de notificaciones de usuario se almacenarán en el Este de EE. UU. (Norte de Virginia) y se replicarán en las demás regiones que haya seleccionado. Consulte la documentación de centros de notificaciones para obtener más información.
3. Haga clic en Submit.

Para suscribirse a las notificaciones de

1. Abra la página de configuración de notificaciones de AWS Artifact.

2. Haga clic en el botón Suscribirse a las notificaciones de Artifact para suscribirse a las notificaciones de AWS Artifact.

Para cancelar la suscripción a las notificaciones

1. Abra la página de configuración de notificaciones de AWS Artifact.
2. Haga clic en el botón Suscribirse a las notificaciones de Artifact para cancelar la suscripción a las notificaciones de AWS Artifact.

Para crear una configuración

1. Abra la página de configuración de notificaciones de AWS Artifact.
2. Haga clic en Crear configuración.
3. Para recibir notificaciones de acuerdos, mantenga la casilla de verificación seleccionada junto a Actualizaciones de los acuerdos de AWS.
4. Para recibir notificaciones de informes, mantenga la casilla de verificación seleccionada junto a Actualizaciones en los informes de AWS.
5. Para recibir notificaciones de todos los informes, mantenga seleccionada la casilla de verificación situada junto a Todos los informes.
6. Para recibir notificaciones solo de informes de categorías y series específicas, haga clic en la casilla de verificación correspondiente a Un subconjunto de informes. A continuación, haga clic en la casilla de verificación de las categorías y series que le interesen.
7. Ingrese un nombre para su configuración.
8. Introduzca una lista separada por comas de correos electrónicos a los que se deben enviar las notificaciones.
9. (Opcional) Para asignar una etiqueta a la configuración de notificaciones, introduzca los pares clave-valor si expande la sección Etiquetas. Nota: Una etiqueta puede asignar a un recurso de AWS y cada etiqueta consta de una clave y un valor opcional que puede definir. Las etiquetas le ayudan a administrar, buscar y filtrar sus recursos.
10. Haga clic en Crear configuración.
11. Se enviará un correo electrónico de verificación a las direcciones de correo electrónico proporcionadas y los destinatarios del correo electrónico deberán hacer clic en el enlace Verificar correo electrónico incluido en el correo de verificación que se les envíe. Tenga

en cuenta que solo las direcciones de correo electrónico verificadas comenzarán a recibir notificaciones.

Para editar una configuración

1. Abra la página de configuración de notificaciones de AWS Artifact.
2. Haga clic en la fila de la configuración que desee editar.
3. Haga clic en el botón Editar en la parte superior derecha de la página.
4. Puede editar cualquiera de los campos. Cuando haya realizado el cambio, pulse Guardar cambios.
5. Si ha añadido nuevas direcciones de correo electrónico, se enviará un correo de verificación a cada una de esas direcciones de correo electrónico. Haga clic en el enlace Verificar correo electrónico que aparece en el correo electrónico de verificación.

Para eliminar una configuración

1. Abra la página de configuración de notificaciones de AWS Artifact.
2. Haga clic en la fila de la configuración que desee eliminar.
3. Haga clic en Delete.
4. Cuando haya leído el mensaje de advertencia, haga clic en Eliminar.

Asignación de etiquetas a una configuración

Una etiqueta es una marca que se asigna a un recurso de AWS. Cada etiqueta está formada por una clave y un valor opcional, ambos definidos por el usuario. Las etiquetas le ayudan a administrar, buscar y filtrar sus recursos. Si lo desea, puede establecer etiquetas al crear o editar una configuración. Para obtener más información, consulte Etiquetado de recursos

Solución de problemas

Si recibe un mensaje de error al usar las notificaciones de AWS Artifact, consulte Solución de problemas en las preguntas frecuentes de AWS Artifact.

Administración de identidades y accesos en AWS Artifact

Cuando se inscriba en AWS, tendrá que proporcionar una dirección de correo electrónico y la contraseña asociada a su cuenta de AWS. Estas son las credenciales raíz y proporcionan acceso completo a todos sus recursos de AWS, 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 su cuenta AWS con sus credenciales raíz o de compartir sus credenciales con otras personas, debe crear una identidad de usuario especial llamada usuario de IAM para usted y para cualquier persona que necesite tener acceso a un documento o acuerdo de 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 administra identidades de usuarios fuera de AWS, puede utilizar los proveedores de identidades de IAM en lugar de crear usuarios de IAM. Para obtener más información, consulte Federación y proveedores de identidades en la Guía del usuario de IAM.

Contenido

- Configure el acceso de los usuarios a AWS Artifact
- Migración a permisos detallados
- Ejemplos de políticas de IAM
- Políticas administradas de AWS para AWS Artifact
- Uso de roles vinculados a servicios para AWS Artifact
- Uso de claves de condición de IAM

Configure el acceso de los usuarios a AWS Artifact

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

Tareas

- Paso 1: Crear una política de IAM

- Paso 2: Crear un grupo IAM y adjuntar la política
- Paso 3: Crear usuarios de IAM y añadirlos al grupo

Paso 1: Crear una política de IAM

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

Para crear una política de IAM

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

1. Abra la consola de IAM en https://console.aws.amazon.com/iam/.
2. En el panel de navegación, seleccione Políticas.
3. Elija Create Policy (Crear política).
4. Seleccione la pestaña JSON.
5. Especifique un documento de política. Puede crear su propia política o bien usar una de las políticas de Ejemplos de políticas de IAM.
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. Seleccione Crear política.

Paso 2: Crear un grupo IAM y adjuntar la política

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

Para crear un grupo de IAM y asociar la 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: Crear usuarios de IAM y añadirlos al grupo

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

Para crear un usuario de IAM 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 a permisos detallados

AWS Artifact ahora permite a los clientes utilizar permisos detallados. Gracias a estos permisos detallados, los clientes tendrán un control pormenorizado sobre el acceso a funciones como la aceptación de condiciones y la descarga de informes.

Para acceder a los informes mediante permisos específicos, los clientes deben utilizar la política administración de AWSArtifactReportsReadOnlyAccess o actualizar sus permisos según la siguiente recomendación. Luego, los clientes deben suscribirse mediante el enlace para probar la nueva página de informes de AWS disponible en la consola.

Los usuarios tendrán la opción de acceder a los informes con los permisos anteriores mediante el enlace a la página de informes anterior, disponible en la consola, en caso de que surja algún problema al actualizar los permisos nuevos.

Migración a nuevos permisos

Migre permisos que no sean específicos de un recurso

Los usuarios deben reemplazar la política existente que contiene los permisos heredados por una política que contenga permisos detallados

Política heredada:

```
{
  "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

Los usuarios deben reemplazar su política actual que contiene los 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 heredada:

```
{
  "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 claves de condición y permisos 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"
          ]
        }
      }
    }
  ]
}
```

Ejemplos de políticas de IAM

Puede crear políticas de permisos que concedan permisos a usuarios de IAM. 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.

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

- Ejemplos de políticas para gestionar 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 informes AWS SOC, PCI e ISO mediante permisos detallados.

```
{
  "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 mediante el recurso `report` de IAM.

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 para 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"
      ]
    }
  ]
}
```

Example Ejemplo de políticas para gestionar acuerdos

La siguiente política concede permiso para descargar todos los acuerdos. Los usuarios de IAM también deben tener este permiso para aceptar acuerdos.

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

```
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

La siguiente política concede permiso para aceptar un acuerdo.

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

La siguiente política concede permiso para rescindir un acuerdo.

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

La siguiente política concede permisos para administrar acuerdos de cuenta única.

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

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

La siguiente política otorga permiso para crear el rol de IAM con AWS Organizations el que AWS Artifact se realiza la integración. 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": "iam:ListRoles",
      "Resource": "arn:aws:iam::*:role/*"
    },
    {
      "Effect": "Allow",
      "Action": "iam:CreateServiceLinkedRole",
      "Resource": "arn:aws:iam::*:role/aws-service-role/artifact.amazonaws.com/
AWSServiceRoleForArtifact"
    }
  ]
}
```

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": [
    {
      "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": "*"
    }
  ]
}
```

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

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

La siguiente política concede permisos para ver los acuerdos organizativos.

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

Políticas administradas de AWS para AWS Artifact

Una política administrada de AWS es una política independiente que AWS crea y administra. Las políticas administradas de AWS se diseñan para ofrecer permisos para muchos casos de uso comunes, por lo que puede empezar a asignar permisos a los usuarios, grupos y roles.

Considere que es posible que las políticas administradas por AWS no concedan permisos de privilegio mínimo para los casos de uso concretos, ya que están disponibles para que las utilicen todos los clientes de AWS. Se recomienda definir políticas administradas por el cliente para los casos de uso a fin de reducir aún más los permisos.

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

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

Política administrada de AWS: AWSArtifactReportsReadOnlyAccess

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

Esta política otorga permisos de *`solo lectura`* 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 desde AWS Artifact.

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

```
      "Effect": "Allow",
      "Action": [
        "artifact:Get",
        "artifact:GetReport",
        "artifact:GetReportMetadata",
        "artifact:GetTermForReport",
        "artifact:ListReports"
      ],
      "Resource": "*"
    }
  ]
}
```

Actualizaciones de Artifact en las políticas administradas de AWS

Es posible consultar los detalles sobre las actualizaciones de las políticas administradas de AWS para Artifact debido a que este servicio comenzó a realizar un seguimiento de estos cambios. Para obtener alertas automáticas sobre cambios en esta página, suscríbase a la fuente RSS en la página Historial de documentos de Artifact.

Cambio	Descripción	Fecha
Artifact comenzó a realizar seguimiento de los cambios	Artifact comenzó a realizar un seguimiento de los cambios de las políticas administradas de AWS e introdujo AWSArtifactReportsReadOnlyAccess.	2023-12-15

Uso de roles vinculados a servicios para AWS Artifact

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

Un rol vinculado a un servicio simplifica la configuración de AWS Artifact porque ya no tendrá que añadir manualmente los permisos necesarios. AWS Artifact define los permisos de sus roles

vinculados a servicios y, a menos que esté definido de otra manera, solo AWS Artifact puede asumir sus roles. Los permisos definidos incluyen las políticas de confianza y de permisos, y que la política de permisos no se pueda adjuntar a ninguna otra entidad de IAM.

Solo puede eliminar un rol vinculado a servicios después de eliminar sus recursos relacionados. De esta forma, se protegen los recursos de AWS Artifact, ya que se evita que se puedan eliminar accidentalmente permisos de acceso a los recursos.

Para obtener información sobre otros servicios que admiten roles vinculados a servicios, consulte Servicios de AWS que funcionan con IAM y busque los servicios que muestran Sí en la columna Roles vinculados a servicios. Elija una opción Sí con un enlace para ver la documentación acerca del rol vinculado al servicio en cuestión.

Permisos de roles vinculados a servicios para AWS Artifact

AWS Artifact utiliza el rol vinculado a un servicio denominado AWSServiceRoleForArtifact, que permite a AWS Artifact recopilar información sobre una organización a través del servicio AWS Organizations.

El rol vinculado al servicio AWSServiceRoleForArtifact depende de los siguientes servicios para asumir el rol:

- `artifact.amazonaws.com`

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

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

Creación de un rol vinculado a un servicio para AWS Artifact

No necesita crear manualmente un rol vinculado a servicios. Cuando visita la pestaña Acuerdos de organizaciones en una cuenta de administración de la organización y selecciona el enlace “Comenzar” en AWS Management Console, AWS Artifact crea por usted 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. Cuando visita la pestaña Acuerdos de organizaciones en una cuenta de administración de la organización y selecciona el enlace “Comenzar”, AWS Artifact crea por usted de nuevo el rol vinculado a un servicio.

Modificación de un rol vinculado a un servicio para AWS Artifact

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

Eliminación de 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 servicio AWS Artifact está utilizando el rol cuando intenta eliminar los recursos, la eliminación podría producir un error. En tal caso, espere unos minutos e intente de nuevo la operación.

Para eliminar los recursos de AWS Artifact utilizados por el rol AWSServiceRoleForArtifact

1. Visite la tabla “Acuerdos de organizaciones” en la consola de AWS Artifact
2. Rescinda cualquier acuerdo de Organización activo

Cómo eliminar manualmente el rol vinculado a servicios mediante IAM

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

Regiones admitidas para roles vinculados a servicios AWS Artifact

AWS Artifact no permite el uso de los roles vinculados al servicio en todas las regiones en las que el servicio está disponible. Puede utilizar el rol AWSServiceRoleForArtifact en las siguientes regiones.

Nombre de la región	Identidad de la región	Soporte 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
Europa (Irlanda)	eu-west-1	No
Europa (Londres)	eu-west-2	No
Europa (Milán)	eu-south-1	No

Nombre de la región	Identidad de la región	Soporte en AWS Artifact
Europa (París)	eu-west-3	No
Europa (Estocolmo)	eu-north-1	No
Medio Oriente (Baréin)	me-south-1	No
Medio Oriente (EAU)	me-central-1	No
América del Sur (São Paulo)	sa-east-1	No
AWS GovCloud (Este de EE. UU.)	us-gov-este-1	No
AWS GovCloud (Oeste de EE.UU.)	us-gov-oeste-1	No

Uso de claves de condición de IAM

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

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

Example Ejemplos de políticas para gestionar acceso de lectura a informes de AWS

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

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

```
{
  "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 informes de AWS Artifact de la serie SOC.

```
{
    "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 informes de AWS Artifact excepto los de la categoría `Certifications and Attestations`.

```
{
  "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 llamadas a la API de AWS Artifact con AWS CloudTrail

AWS Artifact se integra con AWS CloudTrail, un servicio que proporciona un registro de las acciones hechas por un usuario, un rol o un servicio de AWS en AWS Artifact. CloudTrail captura las llamadas a la API de AWS Artifact como eventos. Las llamadas capturadas incluyen las llamadas desde la consola de AWS Artifact y las llamadas desde el código a las operaciones de la API de AWS Artifact. 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 AWS Artifact. Si no configura un registro de seguimiento, puede ver los eventos más recientes de la consola de CloudTrail en el Historial de eventos. Mediante la información recopilada por CloudTrail, puede determinar la solicitud que se realizó a AWS Artifact, la dirección IP desde la que se realizó, quién la realizó y cuándo, etc.

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

Información de AWS Artifact en CloudTrail

CloudTrail se habilita en su Cuenta de AWS cuando la crea. Cuando se produce una actividad en AWS Artifact, esa actividad se registra en un evento de CloudTrail junto con otros eventos de servicio de AWS en el Historial de eventos. Puede ver, buscar y descargar los últimos eventos de la Cuenta de AWS. Para obtener más información, consulte Ver eventos con el historial de eventos de CloudTrail.

Para mantener un registro continuo de eventos en la Cuenta de AWS, incluidos los eventos de AWS Artifact, cree un registro de seguimiento. Un registro de seguimiento permite a CloudTrail enviar 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. 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 obtener 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 registros de CloudTrail de varias regiones y Recepción de archivos de registros de CloudTrail de varias cuentas

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

- ListReports
- GetAccountSettings
- GetReportMetadata
- GetReport
- GetTermForReport
- PutAccountSettings

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

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

Descripción de las entradas de los archivos de registro de AWS Artifact

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 log de CloudTrail pueden contener una o varias entradas de log. Un evento representa una solicitud específica realizada desde un origen y contiene información sobre la acción solicitada, la fecha y la hora de la acción, los parámetros de la solicitud, etc. Los archivos de registro de CloudTrail no rastrean el orden en la pila de las llamadas públicas a la API, por lo que estas no aparecen en ningún orden específico.

En el siguiente ejemplo, se muestra una entrada de registro de CloudTrail que ilustra la acción GetReportMetadata.

```
{
  "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 de AWS Artifact

En la tabla siguiente se describen las versiones de las AWS Artifact.

Cambio	Descripción	Fecha
Acceso detallado a los informes y política gestionada por AWS ArtifactReportRead OnlyAccess	Se habilitó el acceso detallado a Artifact Reports, se habilitar on las claves de condición de los informes y se lanzó la política administrada de AWSArtifactReports ReadOnlyAccess.	15 de diciembre de 2023
Rol vinculado a un servicio de AWS Artifact	Se ha añadido documenta ción sobre funciones vinculada s a servicios y políticas de ejemplo actualizadas para la integración de AWS Artifact y AWS Organizations.	26 de septiembre de 2023
Notificaciones	Se ha publicado la documenta ción para administrar las notificaciones y se han realizado las actualizaciones pertinentes en la guía de referencia de la API, la documentación de registro de CloudTrail y la página de AWS Artifact Identity and Access Management.	1 de agosto de 2023
Informes de terceros: disponibl es en general	Se ha añadido documenta ción de referencia de la API y documentación de registro de CloudTrail y se han puesto a	27 de enero de 2023

	disposición del público general los informes de terceros.	
Informes de terceros (versión preliminar)	Se han publicado los informes de conformidad de los Proveedores de software independientes (ISV) que venden sus productos en AWS Marketplace. Además, 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 ha añadido una sección a la página de gestión de identidades y accesos para la prevención del suplente confuso.	20 de diciembre de 2021
Informes	Se ha eliminado el acuerdo de confidencialidad y se han introducido 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
Lanzamiento de GovCloud	Se ha lanzado AWS Artifact en las regiones de GovCloud.	7 de noviembre de 2019
Acuerdos de AWS Organizations	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 acuerdos de AWS Artifact.	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.