Guía del usuario

AWS Well-Architected Tool

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

AWS Well-Architected Tool: Guía del usuario

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Las marcas comerciales y la imagen comercial de Amazon no se pueden utilizar en relación con ningún producto o servicio que no sea de Amazon, de ninguna manera que pueda causar confusión entre los clientes y que menosprecie o desacredite a Amazon. Todas las demás marcas registradas que no son propiedad de Amazon son propiedad de sus respectivos propietarios, que pueden o no estar afiliados, conectados o patrocinados por Amazon.

Table of Contents

Hemos publicado una nueva versión del marco de Well-Architected. También hemos añadido enfoques nuevos y actualizados al Catálogo de enfoques. Obtenga más información sobre los cambios.

¿Qué es AWS Well-Architected Tool?

AWS Well-Architected Tool (AWS WA Tool) es un servicio en la nube que proporciona un proceso coherente para medir la arquitectura utilizando las prácticas recomendadas de AWS. AWS WA Tool le ayudará durante todo el ciclo de vida del producto de las siguientes formas:

- Proporcionándole asistencia para documentar las decisiones que tome
- Ofreciéndole recomendaciones para mejorar la carga de trabajo en función de las prácticas recomendadas
- Guiándole para que las cargas de trabajo sean más fiables, seguras, eficientes y rentables

Ahora, puede utilizar AWS WA Tool para documentar y medir su carga de trabajo con las prácticas recomendadas del marco de AWS Well-Architected. Estas prácticas recomendadas las han desarrollado arquitectos de soluciones de AWS basándose en los años de experiencia invertidos en la creación de soluciones para una amplia variedad de actividades. El marco proporciona un enfoque coherente para medir las arquitecturas y orientación para implementar diseños que se adapten a sus necesidades con el transcurso del tiempo.

Además de las prácticas recomendadas de AWS, puede utilizar enfoques personalizados para medir su carga de trabajo utilizando sus propias prácticas recomendadas. Puede adaptar las preguntas con una perspectiva personalizada para que sean específicas de una tecnología en particular o para ayudarlo a satisfacer las necesidades de gobierno de su organización. Los enfoques personalizados amplían la orientación proporcionada por los enfoques de AWS.

Las integraciones con AWS Trusted Advisor y AWS Service Catalog AppRegistry le ayudan a descubrir más fácilmente la información necesaria para responder preguntas de revisión de AWS Well-Architected Tool.

Este servicio está dirigido a quienes participan en el desarrollo técnico de productos, como los directores de tecnología (CTO), los arquitectos, los desarrolladores y los miembros del equipo de operaciones. Los clientes de AWS utilizan AWS WA Tool para documentar sus arquitecturas, gestionar el lanzamiento de los productos y comprender y gestionar los riesgos de su cartera de tecnología.

Temas

¿Qué es el marco de AWS Well-Architected?

El marco de AWS Well-Architected contiene una serie de preguntas básicas con las que puede comprender cómo una arquitectura determinada puede adecuarse a las prácticas recomendadas de la nube. El marco proporciona un enfoque coherente para evaluar los sistemas con respecto a las cualidades que se esperan de un sistema moderno basado en la nube. En función del estado de la arquitectura, el marco de trabajo sugiere algunas mejoras que pueden hacerse para conseguir esas cualidades.

Al utilizar el marco, conocerá las prácticas recomendadas de arquitectura para diseñar y utilizar sistemas fiables, seguros, eficientes y rentables en la nube. Proporciona un medio para medir sus arquitecturas de forma coherente comparándolas con las prácticas recomendadas e identificar áreas de mejora. El marco se basa en seis pilares: excelencia operativa, seguridad, fiabilidad, eficacia del rendimiento, optimización de costos y sostenibilidad.

Cuando diseñe cargas de trabajo, debe elegir entre estos pilares en función de las necesidades del negocio. Estas decisiones empresariales pueden ayudarle a administrar las prioridades de diseño. En entornos de desarrollo, puede que tenga que optimizar para reducir costos a costa de la fiabilidad. En soluciones críticas, es posible que tenga que optimizar la fiabilidad y estar dispuesto a aceptar un aumento de los costos. En las soluciones de eCommerce, es posible que tenga que dar prioridad al rendimiento, ya que la satisfacción de los clientes puede ayudar a aumentar los ingresos. Sin embargo, por lo general, la excelencia en la seguridad y las operaciones no afecta a los demás pilares.

Para obtener más información sobre el marco, visite el sitio web de AWS Well-Architected.

Glosario de AWS Well-Architected Tool

A continuación se definen los términos comunes que se utilizan en AWS WA Tool y en el marco de AWS Well-Architected.

- Una carga de trabajo identifica un conjunto de componentes que ofrecen un valor comercial. La carga de trabajo suele ser el nivel de detalle sobre el que se comunican los líderes tecnológicos y comerciales. Algunos ejemplos de cargas de trabajo serían sitios web de marketing, sitios web de comercio electrónico, el backend de una aplicación móvil y las plataformas de análisis. Las cargas de trabajo varían en su nivel de complejidad arquitectónica. Pueden ser sencillas, como un sitio web estático, o bien complejas, como arquitecturas de microservicios con varios almacenes de datos y numerosos componentes.

- Los hitos marcan los cambios clave en la arquitectura a medida que evoluciona a lo largo del ciclo de vida del producto: diseño, pruebas, puesta en marcha y producción.
- Los enfoques son un mecanismo que le permiten medir las arquitecturas de forma coherente con arreglo a unas prácticas recomendadas, así como identificar áreas de mejora.

  Además de los enfoques proporcionadas por AWS, también puede crear y usar sus propios enfoques o usar los enfoques que hayan compartido con usted.
- Los Problemas de alto riesgo son opciones arquitectónicas y operativas que AWS ha determinado que pueden tener un impacto negativo significativo en una empresa. Estos problemas de alto riesgo pueden afectar a las operaciones de la organización, los activos y las personas.
- Los Problemas de riesgo medio son opciones arquitectónicas y operativas que AWS ha determinado que pueden afectar negativamente a la empresa, pero en menor medida que los problemas de alto riesgo.

  Para obtener información adicional, consulte Problemas de alto riesgo y problemas de riesgo medio.

Introducción a AWS Well-Architected Tool

Para empezar a usar AWS Well-Architected Tool, primero debe proporcionar los permisos adecuados a sus usuarios, grupos y roles, y activar la compatibilidad con aquellos con los Servicios de AWS que desee usar con AWS WA Tool. A continuación, defina y documente una carga de trabajo. También puede guardar un hito del estado actual de una carga de trabajo.

En los temas siguientes se explica cómo comenzar a utilizar AWS WA Tool. Para ver un tutorial paso a paso que muestra cómo usar AWS Well-Architected Tool, consulte Tutorial: Documentar una carga de trabajo de AWS Well-Architected Tool.

Temas

Proporcionar acceso a usuarios, grupos o roles a AWS WA Tool

Puede conceder a los usuarios, grupos o roles control total o acceso de solo lectura a AWS Well-Architected Tool.

Proporcionar acceso a AWS WA Tool.

1. Para dar acceso, agregue permisos a los usuarios, grupos o roles:

   - Usuarios y grupos en AWS IAM Identity Center:

     Cree un conjunto de permisos. Siga las instrucciones de Creación de un conjunto de permisos en la Guía del usuario de AWS IAM Identity Center.

   - Usuarios gestionados en IAM a través de un proveedor de identidades:

Cree un rol para la federación de identidades. Siga las instrucciones descritas en Creación de un rol para un proveedor de identidad de terceros (federación) en la Guía del usuario de IAM.

- Usuarios de IAM:
  - Cree un rol que el usuario pueda aceptar. Siga las instrucciones descritas en Creación de un rol para un usuario de IAM en la Guía del usuario de IAM.
  - (No recomendado) Adjunte una política directamente a un usuario o añada un usuario a un grupo de usuarios. Siga las instrucciones descritas en Adición de permisos a un usuario (consola) de la Guía del usuario de IAM.

2. Para conceder el control total, aplique la política administrada WellArchitectedConsoleFullAccess al conjunto de permisos o al rol.

   Con el acceso completo, la entidad principal puede realizar todas las acciones en AWS WA Tool. Este acceso es necesario para poder definir, eliminar, ver, actualizar y compartir cargas de trabajo, así como crear y compartir enfoques personalizados.
3. Para conceder el control total, aplique la política administrada WellArchitectedConsoleReadOnlyAccess al conjunto de permisos o al rol. Las entidades principales con este rol solo pueden ver los recursos.

Para obtener más información sobre estas políticas, consulte Políticas administradas de AWS para AWS Well-Architected Tool.

Activación de la compatibilidad en AWS WA Tool con otros servicios de AWS

La activación del acceso a Organization permite a AWS Well-Architected Tool recopilar información sobre la estructura de la organización para compartir recursos con mayor facilidad (consulte the section called “Activar el uso compartido de recursos en AWS Organizations” para obtener más información). La activación de la compatibilidad con Discovery recopila información de AWS Trusted Advisor, AWS Service Catalog AppRegistry y los recursos relacionados (como las pilas de AWS CloudFormation de las colecciones de recursos de AppRegistry) para ayudarlo a descubrir más fácilmente la información necesaria para responder a las preguntas de revisión de Well-Architected y adaptar las comprobaciones de Trusted Advisor a una carga de trabajo.

La activación de la compatibilidad con AWS Organizations o la activación de la compatibilidad con Discovery crea automáticamente un rol vinculado al servicio para su cuenta.

Para activar la compatibilidad de otros servicios con los que AWS WA Tool puede interactuar, consulte la Configuración.

1. Para recopilar información de AWS Organizations, active Activar la compatibilidad de AWS Organizations.
2. Active la compatibilidad de Activar Discovery para recopilar información de otros servicios y recursos de AWS.
3. Seleccione Ver permisos de rol para ver los permisos del rol vinculado al servicio en cuestión o políticas de relación de confianza.
4. Seleccione Guardar configuración.

Activar AppRegistry para una carga de trabajo

El uso de AppRegistry es opcional y los clientes de Business and Enterprise Support de AWS pueden activarlo por carga de trabajo.

Siempre que se active la compatibilidad con Discovery y AppRegistry se asocie a una carga de trabajo nueva o existente, AWS Well-Architected Tool crea un grupo de atributos gestionado por el servicio. El grupo de atributos Metadatos de AppRegistry contiene el ARN de la carga de trabajo, el nombre de la carga de trabajo y los riesgos asociados a la carga de trabajo.

- Cuando la compatibilidad con Discovery está activada, el grupo de atributos se actualiza cada vez que se produce un cambio en la carga de trabajo.
- Cuando se desactiva la compatibilidad con Discovery o se elimina la aplicación de la carga de trabajo, se elimina la información de la carga de trabajo de AWS Service Catalog.

Si desea que una aplicación de AppRegistry gestione los datos obtenidos de Trusted Advisor, defina la Definición de recurso de la carga de trabajo como AppRegistry o Todo. Cree roles para todas las cuentas que posean los recursos propios de su aplicación siguiendo las pautas que se indican en the section called “Activación Trusted Advisor en IAM”.

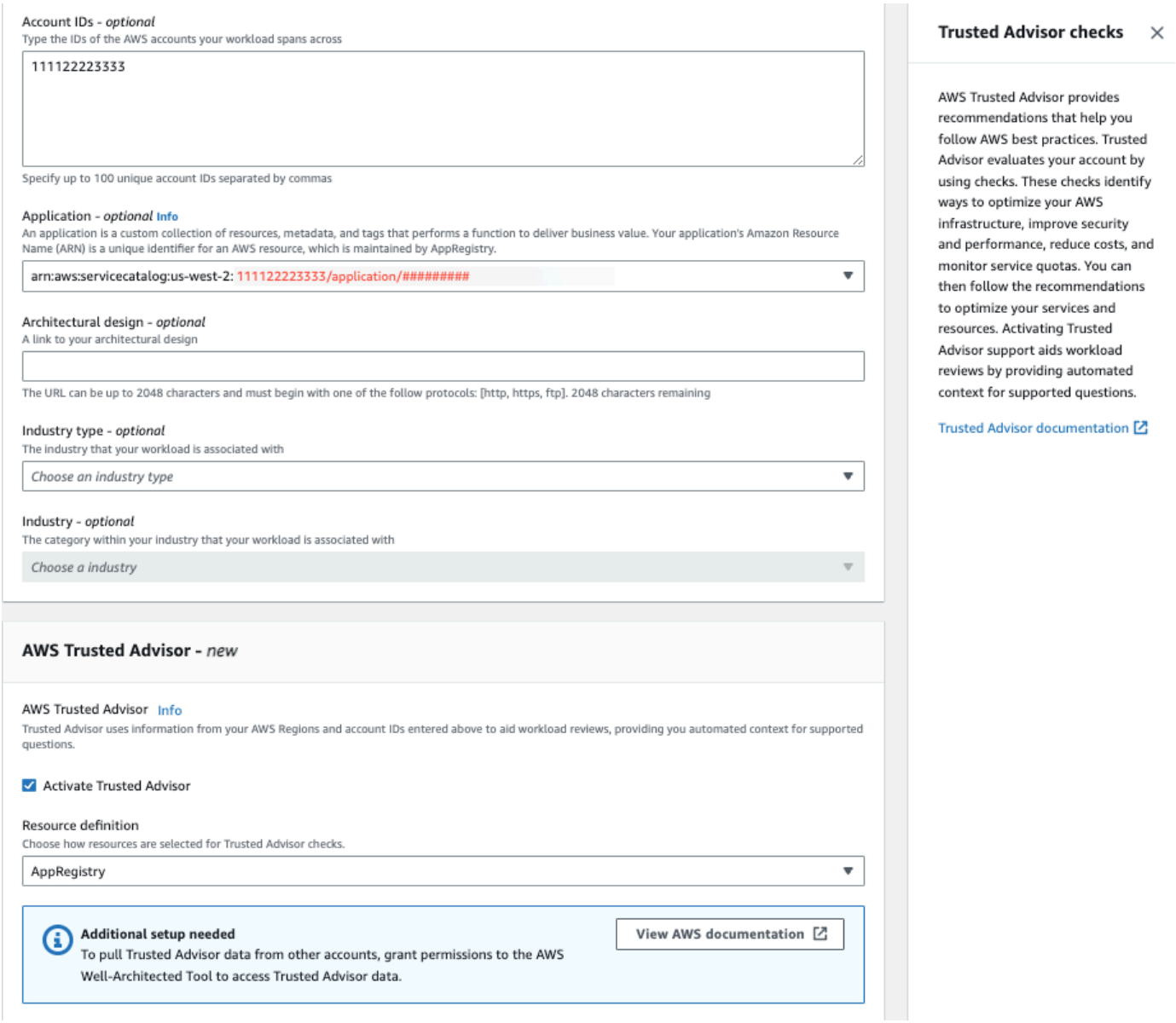
Activar AWS Trusted Advisor para una carga de trabajo

De forma opcional, puede integrar AWS Trusted Advisor y activarlo por carga de trabajo para los clientes de AWS Business and Enterprise Support. La integración de Trusted Advisor con AWS WA Tool no tiene ningún costo, pero para obtener detalles sobre los precios de Trusted Advisor, consulte AWSPlanes de compatibilidad. La activación de Trusted Advisor para las cargas de trabajo puede

proporcionarle un enfoque más integral, automatizado y supervisado para revisar y optimizar sus cargas de trabajo de AWS. Esto puede ayudarlo a mejorar la fiabilidad, la seguridad, el rendimiento y la optimización de costos de sus cargas de trabajo.

Activar Trusted Advisor para una carga de trabajo

1. Para activar Trusted Advisor, los propietarios de la carga de trabajo pueden utilizar AWS WA Tool para actualizar una carga de trabajo existente o crear una nueva carga de trabajo seleccionando Definir carga de trabajo.
2. Introduzca un identificador de cuenta utilizado por Trusted Advisor en el campo ID de cuenta, seleccione un ARN de aplicación en el campo Aplicación, o ambos para activar Trusted Advisor.
3. En la sección AWS Trusted Advisor, seleccione Activar Trusted Advisor.



4. La primera vez Trusted Advisor se activa para una carga de trabajo, aparece una notificación en la que se indica que se va a crear el rol de servicio de IAM. Si selecciona Ver permisos, se muestran los permisos del rol de IAM. Puede ver el Nombre del rol, así como los Permisos y Relaciones de confianza que JSON creó automáticamente para usted en IAM. Una vez creado el rol, para las cargas de trabajo que se activen posteriormente de Trusted Advisor, solo se mostrará la notificación correspondiente de Se necesita configuración adicional.
5. En el menú desplegable Definición de recursos, puede seleccionar Metadatos de carga de trabajo, AppRegistry o Todos. La selección de Definición de recursos define qué datos de AWS WA Tool se obtienen de Trusted Advisor para proporcionar las comprobaciones de estado en la revisión de la carga de trabajo que se corresponden con las mejores prácticas de Well-Architected.

   Metadatos de la carga de trabajo: la carga de trabajo se define mediante los ID de cuenta y Regiones de AWS especificados en la carga de trabajo.

   AppRegistry: la carga de trabajo se define mediante los recursos (como las pilas de AWS CloudFormation) que están presentes en la aplicación de AppRegistry asociada a la carga de trabajo.

   Todo: la carga de trabajo se define mediante los metadatos de la carga de trabajo y los recursos de AppRegistry.
6. Seleccione Siguiente.
7. Aplique el marco de AWS Well-Architected a su carga de trabajo y seleccione Definir carga de trabajo. Las comprobaciones de Trusted Advisor solo están vinculadas al marco de AWS Well-Architected y no a otros enfoques.

AWS WA Tool obtiene datos de Trusted Advisor periódicamente usando los roles creados en IAM. El rol de IAM se crea automáticamente para el propietario de la carga de trabajo. Sin embargo, para ver la información de Trusted Advisor, los propietarios de cualquier cuenta asociada a la carga de trabajo deben ir a IAM y crear un rol. Consulte ??? para obtener más información. Si este rol no existe, AWS WA Tool no puede obtener la información de Trusted Advisor de esa cuenta y se muestra un error.

Para obtener más información sobre cómo crear un rol de AWS Identity and Access Management (IAM), consulte Crear un rol para un servicio de AWS (consola) en la Guía de usuario de IAM.

Activar Trusted Advisor para una carga de trabajo

> **Note**
>
> Los propietarios de las cargas de trabajo deben Activar la compatibilidad con Discovery para sus cuentas antes de crear una carga de trabajo de Trusted Advisor. Al seleccionar Activar la compatibilidad con Discovery, se crea el rol necesario para el propietario de la carga de trabajo. Siga los pasos siguientes para todas las demás cuentas asociadas.

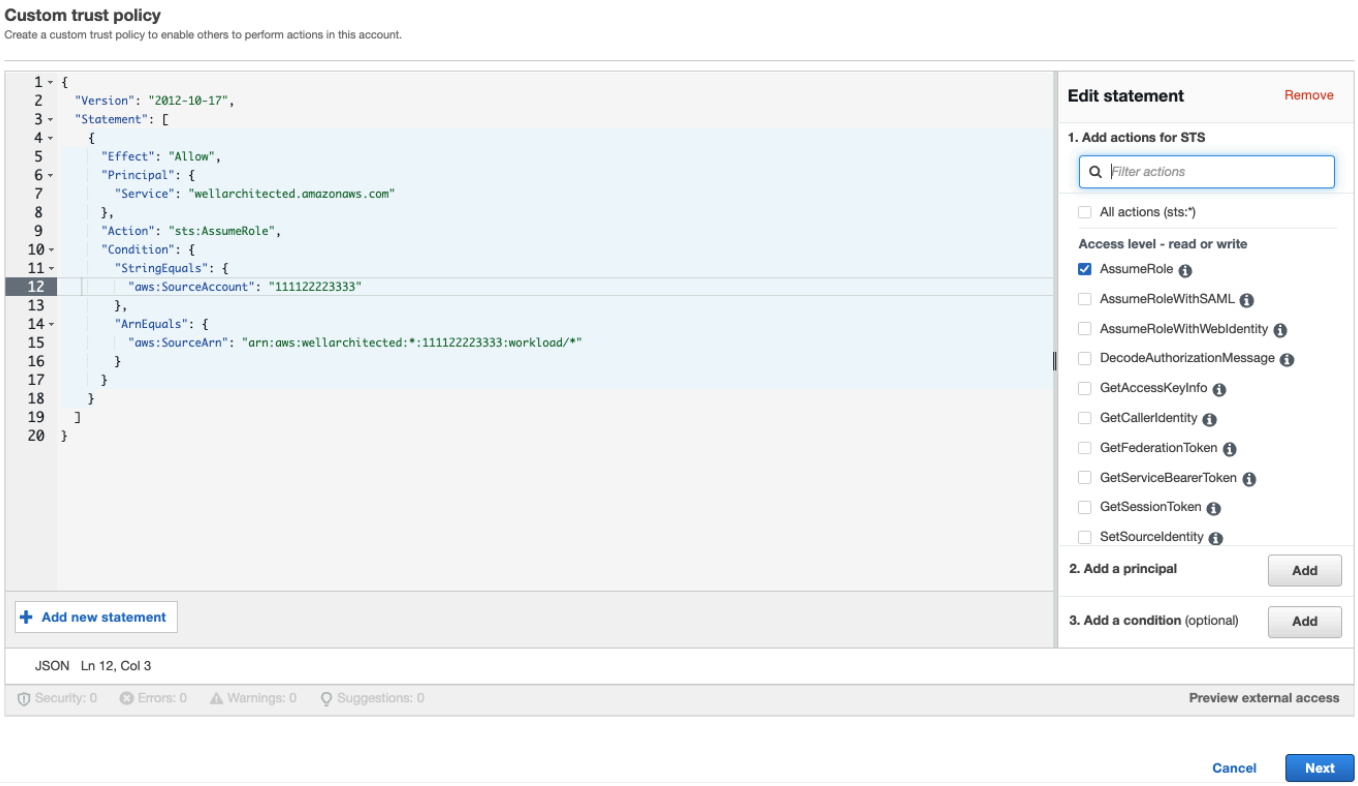
Los propietarios de las cuentas asociadas a las cargas de trabajo que hayan activado Trusted Advisor deben crear un rol en IAM para poder ver la información de Trusted Advisor en AWS Well-Architected Tool.

Crear un rol en IAM para AWS WA Tool para obtener información de Trusted Advisor

1. Inicie sesión en la AWS Management Console y abra la consola de IAM en la https://console.aws.amazon.com/iam/.
2. En el panel de navegación de la consola de IAM, seleccione Roles y, a continuación, seleccione Crear rol.
3. En Tipo de entidad de confianza, seleccione Política de confianza personalizada.
4. Copie y pegue la siguiente Política de confianza personalizada en el campo JSON de la consola de IAM, como se muestra en la siguiente imagen. Sustituya *WORKLOAD_OWNER_ACCOUNT_ID* por el ID de cuenta del propietario de la carga de trabajo y seleccione Siguiente.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "wellarchitected.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "WORKLOAD_OWNER_ACCOUNT_ID"
        },
        "ArnEquals": {
```

```
          "aws:SourceArn":
 "arn:aws:wellarchitected:*:WORKLOAD_OWNER_ACCOUNT_ID:workload/*"
        }
      }
    }
  ]
}
```



Note

El `aws:sourceArn` en el bloque de condiciones de la política de confianza personalizada anterior es `"arn:aws:wellarchitected:*:WORKLOAD_OWNER_ACCOUNT_ID:workload/*"`, que es una condición genérica que establece que este rol puede ser utilizado por AWS WA Tool para todas las cargas de trabajo del propietario de la carga de trabajo. Sin embargo, el acceso se puede limitar a un ARN de carga de trabajo específico o a un conjunto de ARN de carga de trabajo. Para especificar varios ARN, consulte el ejemplo de una política de confianza.

```
{
```

```
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "wellarchitected.amazonaws.com"
            },
            "Action": "sts:AssumeRole",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "WORKLOAD_OWNER_ACCOUNT_ID"
                },
                "ArnEquals": {
                    "aws:SourceArn": [

 "arn:aws:wellarchitected:REGION:WORKLOAD_OWNER_ACCOUNT_ID:workload/
WORKLOAD_ID_1",

 "arn:aws:wellarchitected:REGION:WORKLOAD_OWNER_ACCOUNT_ID:workload/
WORKLOAD_ID_2"
                    ]
                }
            }
        }
    ]
}
```

5. En la página Agregar permisos, en las Políticas de permisos, seleccione Crear política para dar acceso a AWS WA Tool a los datos de lectura de Trusted Advisor. Al seleccionar Crear política, se abre una ventana nueva.

> **Note**
>
> Además, tiene la opción de omitir la creación de los permisos durante la creación del rol y crear una política en línea después de crear el rol. Seleccione Ver rol en el mensaje de creación correcta del rol y seleccione Crear política integrada en el menú desplegable Agregar permisos de la pestaña Permisos.

6. Copie y pegue la siguiente Política de permisos en el editor JSON. En el ARN de `Resource`, sustituya *YOUR_ACCOUNT_ID* con su propio ID de cuenta, especifique la región o un asterisco (*) y seleccione Siguiente: etiquetas.

Para obtener más información sobre los formatos ARN, consulte Nombre de recurso de Amazon (ARN) en la Guía de referencia general de AWS.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "trustedadvisor:DescribeCheckRefreshStatuses",
                "trustedadvisor:DescribeCheckSummaries",
                "trustedadvisor:DescribeRiskResources",
                "trustedadvisor:DescribeAccount",
                "trustedadvisor:DescribeRisk",
                "trustedadvisor:DescribeAccountAccess",
                "trustedadvisor:DescribeRisks",
                "trustedadvisor:DescribeCheckItems"
            ],
            "Resource": [
              "arn:aws:trustedadvisor:*:YOUR_ACCOUNT_ID:checks/*"
            ]
        }
    ]
}
```

7. Si Trusted Advisor está activado para una carga de trabajo y la Definición de recursos está configurada como AppRegistry o Todas, todas las cuentas que posean un recurso en la aplicación AppRegistry adjunta a la carga de trabajo deberán añadir el siguiente permiso a la política de permisos de su rol de Trusted Advisor.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DiscoveryPermissions",
            "Effect": "Allow",
            "Action": [
                "servicecatalog:ListAssociatedResources",
                "tag:GetResources",
                "servicecatalog:GetApplication",
                "resource-groups:ListGroupResources",
                "cloudformation:DescribeStacks",
```

```
                "cloudformation:ListStackResources"
            ],
            "Resource": "*"
        }
    ]
}
```

8. (Opcional) Añada etiquetas. Seleccione Siguiente: revisar.
9. Revise la política de precisión, asígnele un nombre y seleccione Crear política.
10. En la página Agregar permisos para el rol, seleccione el nombre de la política que acaba de crear y, a continuación, seleccione Siguiente.
11. Introduzca el Nombre del rol, que debe usar la siguiente sintaxis: `WellArchitectedRoleForTrustedAdvisor-`*`WORKLOAD_OWNER_ACCOUNT_ID`* y seleccione Crear rol. Sustituya *`WORKLOAD_OWNER_ACCOUNT_ID`* por el ID de cuenta del propietario de la carga de trabajo.

    En la parte superior de la página, verá un mensaje en el que se indica que el rol se creó.
12. Para ver el rol y la política de permisos asociada, en el panel de navegación izquierdo, en Administración de acceso, seleccione Roles y busque el nombre de `WellArchitectedRoleForTrustedAdvisor-`*`WORKLOAD_OWNER_ACCOUNT_ID`*. Seleccione el nombre del rol para comprobar que los Permisos y las Relaciones de confianza son correctas.

Desactivar Trusted Advisor para una carga de trabajo

Desactivar Trusted Advisor para una carga de trabajo

Puede desactivar Trusted Advisor para cualquier carga de trabajo de AWS Well-Architected Tool editando su carga de trabajo y deseleccionando Activar Trusted Advisor. Para obtener más información sobre editar cargas de trabajo, consulte the section called “Edición de una carga de trabajo”.

La desactivación de Trusted Advisor desde AWS WA Tool no elimina los roles creados en IAM. La eliminación de roles de IAM requiere una medida de limpieza independiente. Los propietarios de las cargas de trabajo o los propietarios de las cuentas asociadas deben eliminar los roles de IAM creados cuando Trusted Advisor esté desactivado en AWS WA Tool, o impedir que AWS WA Tool recopile datos de Trusted Advisor para la carga de trabajo.

Eliminar el **`WellArchitectedRoleForTrustedAdvisor`** en IAM

1. Inicie sesión en la AWS Management Console y abra la consola de IAM en la https://console.aws.amazon.com/iam/.
2. En el panel de navegación de la consola de IAM, seleccione Roles.
3. Busque `WellArchitectedRoleForTrustedAdvisor-`*`WORKLOAD_OWNER_ACCOUNT_ID`* y seleccione el nombre del rol.
4. Seleccione Eliminar. En la ventana emergente, escriba el nombre del rol para confirmar la eliminación y vuelva a seleccionar Eliminar.

Para obtener más información sobre cómo eliminar un rol de IAM, consulte Eliminar un rol de IAM (consola) en la Guía del usuario de IAM.

Definición de una carga de trabajo en AWS WA Tool

Una carga de trabajo es un conjunto de componentes que ofrecen un valor comercial. Por ejemplo, las cargas de trabajo pueden ser sitios web de marketing, sitios web de comercio electrónico, el backend de una aplicación móvil y las plataformas de análisis. Definir con precisión una carga de trabajo ayuda a garantizar una revisión exhaustiva de los pilares del marco de AWS Well-Architected.

Para definir una carga de trabajo

1. Inicie sesión en AWS Management Console y abra la consola de AWS Well-Architected Tool en https://console.aws.amazon.com/wellarchitected/.
2. Si es la primera vez que utiliza AWS WA Tool, verá una página en la que aparecen las características del servicio. En la sección Definir una carga de trabajo, elija Definir carga de trabajo.

   Como alternativa, en el panel de navegación izquierdo, elija Cargas de trabajo y seleccione Definir carga de trabajo.

   Para obtener más información sobre cómo AWS utiliza los datos de carga de trabajo, elija ¿Por qué AWS necesita estos datos y cómo se utilizarán?
3. En el cuadro Nombre, escriba un nombre para la carga de trabajo.

> **Note**
>
> El nombre debe tener entre 3 y 100 caracteres. Al menos tres caracteres no deben ser espacios. Los nombres de las cargas de trabajo deben ser únicos. Los espacios y las mayúsculas no se tienen en cuenta al comprobar la exclusividad.

4. En el cuadro Descripción, escriba una descripción de la carga de trabajo. La descripción debe tener entre 3 y 250 caracteres.
5. En el cuadro Propietario de la revisión escriba el nombre, la dirección de correo electrónico o el identificador de la persona o del grupo principal que posee el proceso de revisión de la carga de trabajo.
6. En el cuadro Entorno, elija el entorno de la carga de trabajo:
   - Producción: la carga de trabajo se ejecuta en un entorno de producción.
   - Preproducción: la carga de trabajo se ejecuta en un entorno de preproducción.
7. En la sección Regiones, elija las regiones de la carga de trabajo:
   - Regiones de AWS: elija las regiones de Regiones de AWS donde se ejecuta la carga de trabajo, una a una.
   - Regiones no pertenecientes a AWS: escriba los nombres de las regiones fuera de AWS donde se ejecuta la carga de trabajo. Puede especificar hasta cinco regiones únicas separadas por comas.

   Utilice ambas opciones si procede para su carga de trabajo.
8. (Opcional) En el cuadro ID de cuentas escriba los ID de las cuentas de Cuentas de AWS asociadas a su carga de trabajo. Puede especificar hasta 100 ID de cuenta únicos, separados por comas.

   Si Trusted Advisor está activado, se utilizan todos los ID de cuenta especificados para obtener datos de Trusted Advisor. Consulte Activar AWS Trusted Advisor para una carga de trabajo para conceder permisos a AWS WA Tool para obtener datos de Trusted Advisor en su nombre en IAM.
9. (Opcional) En el cuadro Aplicación, introduzca el ARN de aplicación de una aplicación de la AWS Service Catalog AppRegistry que desee asociar a esta carga de trabajo. Solo se puede especificar un ARN por carga de trabajo y la aplicación y la carga de trabajo deben estar en la misma región.

10. (Opcional) En el cuadro Diseño arquitectónico, introduzca la dirección URL del diseño arquitectónico.
11. (Opcional) En el cuadro Tipo de sector, elija el tipo de sector asociado a su carga de trabajo.
12. (Opcional) En el cuadro Sector, elija el sector que mejor se ajuste a la carga de trabajo.
13. (Opcional) En la sección Trusted Advisor, para activar las comprobaciones de Trusted Advisor para su carga de trabajo, seleccione Activar Trusted Advisor. Es posible que se necesite una configuración adicional para las cuentas asociadas a su carga de trabajo. Consulte the section called “Activar Trusted Advisor” para conceder permisos AWS WA Tool para obtener datos de Trusted Advisor en su nombre. Seleccione entre Metadatos de carga de trabajo, AppRegistry o Todo en la Definición de recursos para definir qué recursos utiliza AWS WA Tool para ejecutar las comprobaciones de Trusted Advisor.
14. (Opcional) En la sección de Jira, para activar la configuración de sincronización de Jira a nivel de carga de trabajo para la carga de trabajo, seleccione Anular la configuración a nivel de cuenta. Es posible que se necesite una configuración adicional para las cuentas asociadas a su carga de trabajo. Consulte Conector de AWS Well-Architected Tool para Jira para empezar a instalar y configurar el conector. Seleccione No sincronizar la carga de trabajo, Sincronizar la carga de trabajo: manual y Sincronizar la carga de trabajo: automática y, si lo desea, introduzca una Clave de proyecto Jira con la que realizar la sincronización.

    > **Note**
    >
    > Si no anula la configuración a nivel de cuenta, las cargas de trabajo utilizarán de forma predeterminada la configuración de sincronización de Jira a nivel de cuenta.

15. (Opcional) En la sección Etiquetas, añada las etiquetas que desee asociar a la carga de trabajo.

    Para obtener más información sobre las etiquetas, consulte Etiquetar los recursos de AWS WA Tool.
16. Elija Siguiente.

    Si un cuadro necesario está en blanco o si un valor especificado no es válido, debe corregir el problema para poder continuar.
17. (Opcional) En el paso Aplicar perfil, asocie un perfil a la carga de trabajo seleccionando un perfil existente, buscando el nombre del perfil o seleccionando Crear perfil para crear un perfil. Elija Siguiente.

18. Elija los enfoques que se aplican a esta carga de trabajo. Se pueden añadir hasta 20 enfoques a una carga de trabajo. Para obtener descripciones de lentes de AWS oficiales, consulte Lentes.

    Las lentes se pueden seleccionar de lentes personalizadas (lentes que ha creado o que se compartieron con la Cuenta de AWS), el catálogo de lentes (lentes oficiales de AWS disponibles para todos los usuarios) o ambos.

    > **Note**
    >
    > La sección de lentes personalizadas está vacía si no ha creado una lente personalizada o si ha compartido una lente personalizada con usted.

    > **Exención de responsabilidad**
    >
    > Al acceder o aplicar enfoques personalizados creados por otro usuario o cuenta de AWS, usted reconoce que los enfoques personalizados creados por otros usuarios y compartidos con usted son contenido de terceros, según se define en el Acuerdo del cliente de AWS.

19. Seleccione Definir carga de trabajo.

    Si un cuadro necesario está en blanco o si un valor especificado no es válido, debe corregir el problema antes de definir la carga de trabajo.

Documentación de una carga de trabajo en AWS WA Tool

Una vez que haya definido una carga de trabajo en AWS Well-Architected Tool, puede documentar su estado abriendo la página Revisar carga de trabajo. Esto le ayuda a evaluar su carga de trabajo y a realizar un seguimiento de su progreso a lo largo del tiempo.

Para documentar el estado de una carga de trabajo

1. Después de definir la carga de trabajo, verá una página en la que se muestran sus datos actuales. Seleccione Iniciar revisión para comenzar.

   De lo contrario, en el panel de navegación izquierdo, seleccione Cargas de trabajo y elija el nombre de la carga de trabajo para abrir la página de detalles. Elija Continuar revisión.

(Opcional) Si hay un perfil asociado a su carga de trabajo, el panel de navegación izquierdo contiene una lista de preguntas de revisión de la carga de trabajo priorizadas que puede utilizar para acelerar el proceso de revisión de la carga de trabajo.

2. Ahora aparece la primera pregunta. Para cada pregunta:

   a. Lea la pregunta y determine si la pregunta se aplica a su carga de trabajo.

      Para obtener más información, elija Información y vea la información en el panel de ayuda.

      - Si la pregunta no se aplica a la carga de trabajo, elija La pregunta no se aplica a esta carga de trabajo.
      - De lo contrario, seleccione en la lista las prácticas recomendadas que está siguiendo actualmente.

        Si en la actualidad no sigue ninguna de las prácticas, seleccione Ninguna de estas.

      Para obtener más información sobre cualquier elemento, elija Información y vea la información en el panel derecho.

   b. (Opcional) Si una o más prácticas recomendadas no se aplican a su carga de trabajo, elija Marcar las prácticas recomendadas que no se aplican a esta carga de trabajo y selecciónelas. Para cada práctica recomendada seleccionada, si lo desea, puede seleccionar un motivo y proporcionar detalles adicionales.

   c. (Opcional) Utilice el cuadro Notas para registrar información relacionada con la pregunta.

      Por ejemplo, puede indicar por qué la pregunta no procede o proporcionar más detalles sobre las prácticas recomendadas seleccionadas.

   d. Seleccione Siguiente para continuar con la siguiente pregunta.

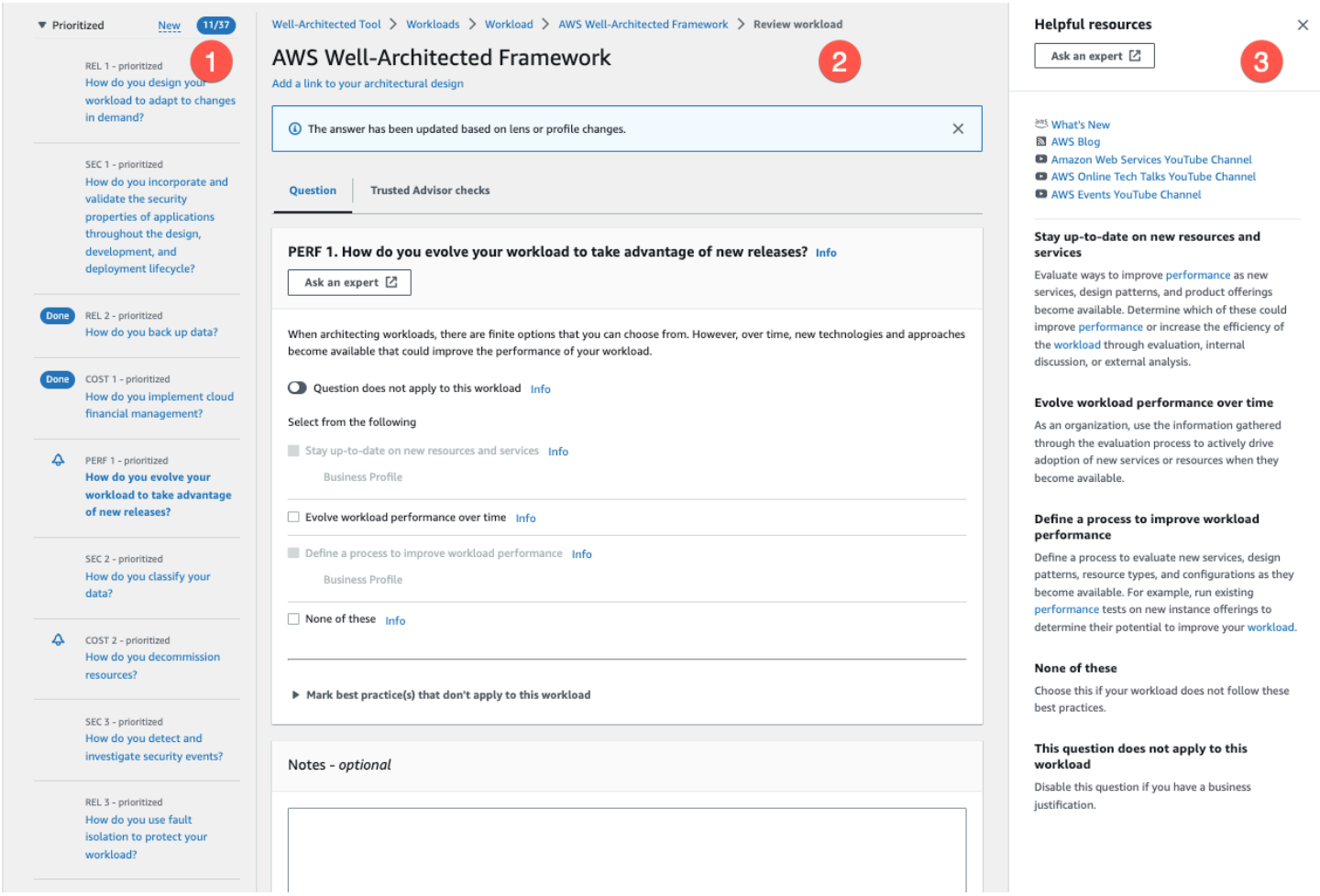
   Repita estos pasos con cada una de las preguntas de los pilares.

3. Elija Guardar y salir en cualquier momento para guardar los cambios y detener la documentación de la carga de trabajo.

Una vez que haya documentado su carga de trabajo, puede volver a las preguntas para seguir revisándola en cualquier momento. Para obtener más información, consulte Reviewing a workload with AWS Well-Architected Framework.

Revisión de una carga de trabajo con el marco de AWS Well-Architected

Puede revisar su carga de trabajo en la consola, en la página Revisar carga de trabajo. En esta página, se proporcionan las prácticas recomendadas y recursos útiles para el rendimiento de la carga de trabajo.



1. Para abrir la página Revisar carga de trabajo, en la página de detalles de la carga de trabajo, seleccione Continúe revisando. El panel de navegación izquierdo muestra las preguntas de cada pilar. Las preguntas que ha respondido están marcadas como Listas. El número de preguntas respondidas en cada pilar se muestra junto al nombre del pilar.

   Puede desplazarse a preguntas de otros pilares eligiendo el nombre del pilar y, a continuación, eligiendo la pregunta que desee responder.

(Opcional) Si hay un perfil asociado a su carga de trabajo, AWS WA Tool utiliza la información del perfil para determinar qué preguntas de la revisión de la carga de trabajo tienen prioridad y cuáles no son aplicables a su empresa. En el panel de navegación izquierdo, puede utilizar las preguntas priorizadas para acelerar el proceso de revisión de la carga de trabajo. Aparece un icono de notificación junto a las preguntas que se acaban de añadir a la lista de preguntas priorizadas.

2. En el panel central, se muestra la pregunta actual. Seleccione las prácticas recomendadas que está siguiendo. Elija Info (Información) para obtener información adicional acerca de la pregunta o de la práctica recomendada. Seleccione Pregunte a un experto para acceder a la comunidad AWS re:Post dedicada a AWS Well-Architected. AWS re:post es una comunidad de preguntas y respuestas basada en temas que sustituye a los foros de AWS. Con re:post, puede encontrar respuestas, responder preguntas, unirse a un grupo, seguir temas populares y votar por sus preguntas y respuestas favoritas.

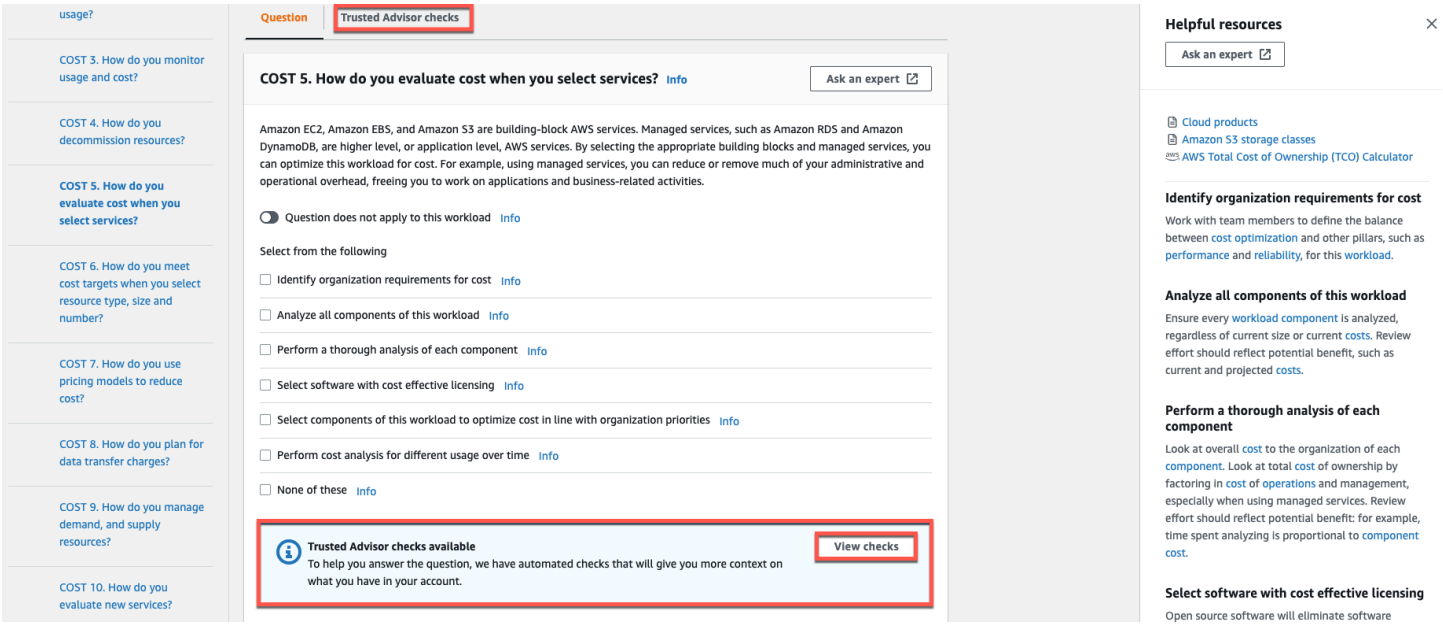
   (Opcional) Para indicar que una o más prácticas recomendadas no se aplican, elija Marcar las prácticas recomendadas que no se aplican a esta carga de trabajo y selecciónelas.

   Utilice los botones de la parte inferior de este panel para ir a la siguiente pregunta, volver a la pregunta anterior o guardar los cambios y salir.

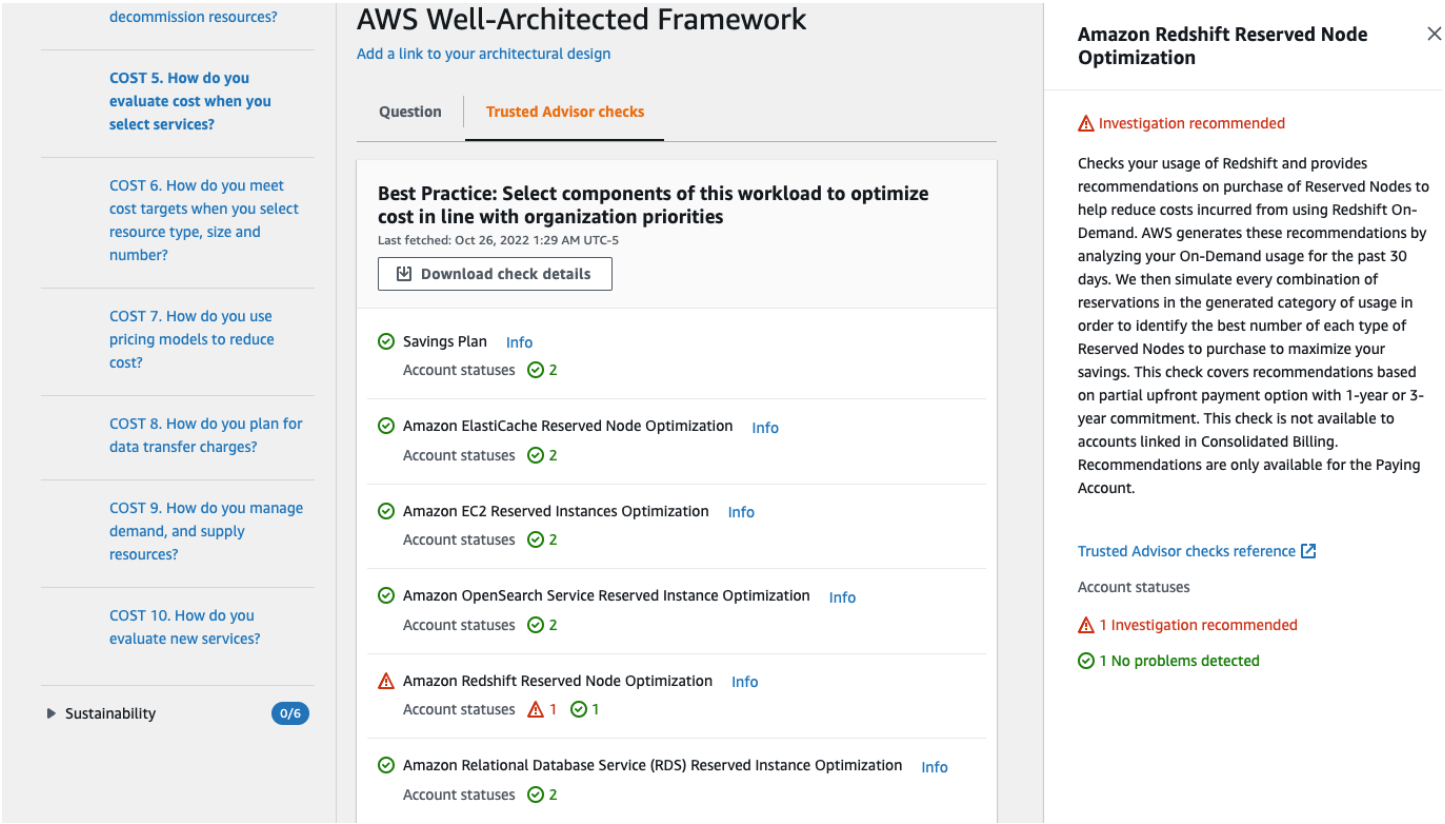
3. En el panel de ayuda derecho, se muestra información adicional y recursos útiles. Seleccione Pregunte a un experto para acceder a la comunidad AWS re:post dedicada a AWS Well-Architected. En esta comunidad, puede hacer preguntas relacionadas con el diseño, la creación, la implementación y el funcionamiento de las cargas de trabajo en AWS.

Visualización de las comprobaciones de Trusted Advisor de su carga de trabajo

Si Trusted Advisor está activada para su carga de trabajo, aparecerá una pestaña de Comprobaciones de Trusted Advisor junto a la Pregunta. Si hay alguna comprobación disponible como práctica recomendada, aparecerá una notificación de que hay comprobaciones de Trusted Advisor disponibles tras seleccionar la pregunta. Si selecciona Ver comprobaciones, accederá a la pestaña de Comprobaciones de Trusted Advisor.



En la pestaña Comprobaciones de Trusted Advisor, puede ver información más detallada sobre las comprobaciones recomendadas de Trusted Advisor, ver los enlaces a la documentación de Trusted Advisor en el panel de Recursos de ayuda o Descargar los detalles de las comprobaciones, que proporcionan un informe de las comprobaciones de Trusted Advisor y el estado de cada una de las mejores prácticas en un archivo CSV.



Las categorías de comprobaciones de Trusted Advisor se muestran en forma de iconos de colores y el número situado junto a cada icono indica el número de cuentas en ese estado.

- Acción recomendada (rojo): Trusted Advisor recomienda una acción para la verificación.
- Investigación recomendada (amarillo): Trusted Advisor detecta un posible problema para la verificación.
- No se han detectado problemas (verde): Trusted Advisor no detecta ningún problema para la verificación.
- Elementos excluidos (gris): el número de verificaciones que tienen elementos excluidos, como los recursos que desea que se omita una verificación.

Para obtener más información sobre las comprobaciones de Trusted Advisor proporcionadas, consulte Ver categorías de comprobaciones en la Guía del usuario de Soporte.

Al seleccionar el enlace de Información situado junto a cada comprobación de Trusted Advisor, se muestra información sobre la comprobación en el panel de Recursos de ayuda. Para obtener más información, consulte el tema Referencia de comprobaciones de AWS Trusted Advisor en la Guía del usuario de Soporte.

Guardado de un hito para una carga de trabajo en AWS WA Tool

Puede guardar un hito de una carga de trabajo en cualquier momento. Un hito registra el estado actual de la carga de trabajo.

Guardar un hito

1. En la página de detalles de la carga de trabajo, seleccione Guardar hito.
2. En el cuadro Nombre de hito, escriba un nombre para el hito.

> **Note**
>
> El nombre debe tener entre 3 y 100 caracteres. Al menos tres caracteres no deben ser espacios. Los nombres de hitos asociados a una carga de trabajo deben ser únicos. Los espacios y las mayúsculas no se tienen en cuenta al comprobar la exclusividad.

3. Seleccione Guardar.

Después de guardar un hito, no podrá cambiar los datos de la carga de trabajo que se capturó en dicho hito.

Para obtener más información, consulte Hitos.

Tutorial: Documente una carga de trabajo de AWS Well-Architected Tool

En este tutorial, se describe cómo se utiliza AWS Well-Architected Tool para documentar y medir una carga de trabajo. Este ejemplo ilustra paso a paso cómo se define y documenta una carga de trabajo de un sitio web comercio electrónico de venta al por menor.

Temas

Paso 1: Definir una carga de trabajo

Para empezar, defina una carga de trabajo. Hay dos formas de definir una carga de trabajo. En este tutorial, no vamos a definir una carga de trabajo a partir de una plantilla de revisión. Para obtener más información sobre cómo definir una carga de trabajo a partir de una plantilla de revisión, consulte the section called “Definición de una carga de trabajo”.

Para definir una carga de trabajo

1. Inicie sesión en AWS Management Console y abra la consola de AWS Well-Architected Tool en https://console.aws.amazon.com/wellarchitected/.

   > **Note**
   >
   > El usuario que documente el estado de la carga de trabajo debe tener permisos de acceso completo a AWS WA Tool.

2. En la sección Definir una carga de trabajo, elija Definir carga de trabajo.
3. En el cuadro Nombre, escriba **`Retail Website - North America`** como nombre de la carga de trabajo.
4. En el cuadro Descripción, especifique una descripción de la carga de trabajo.

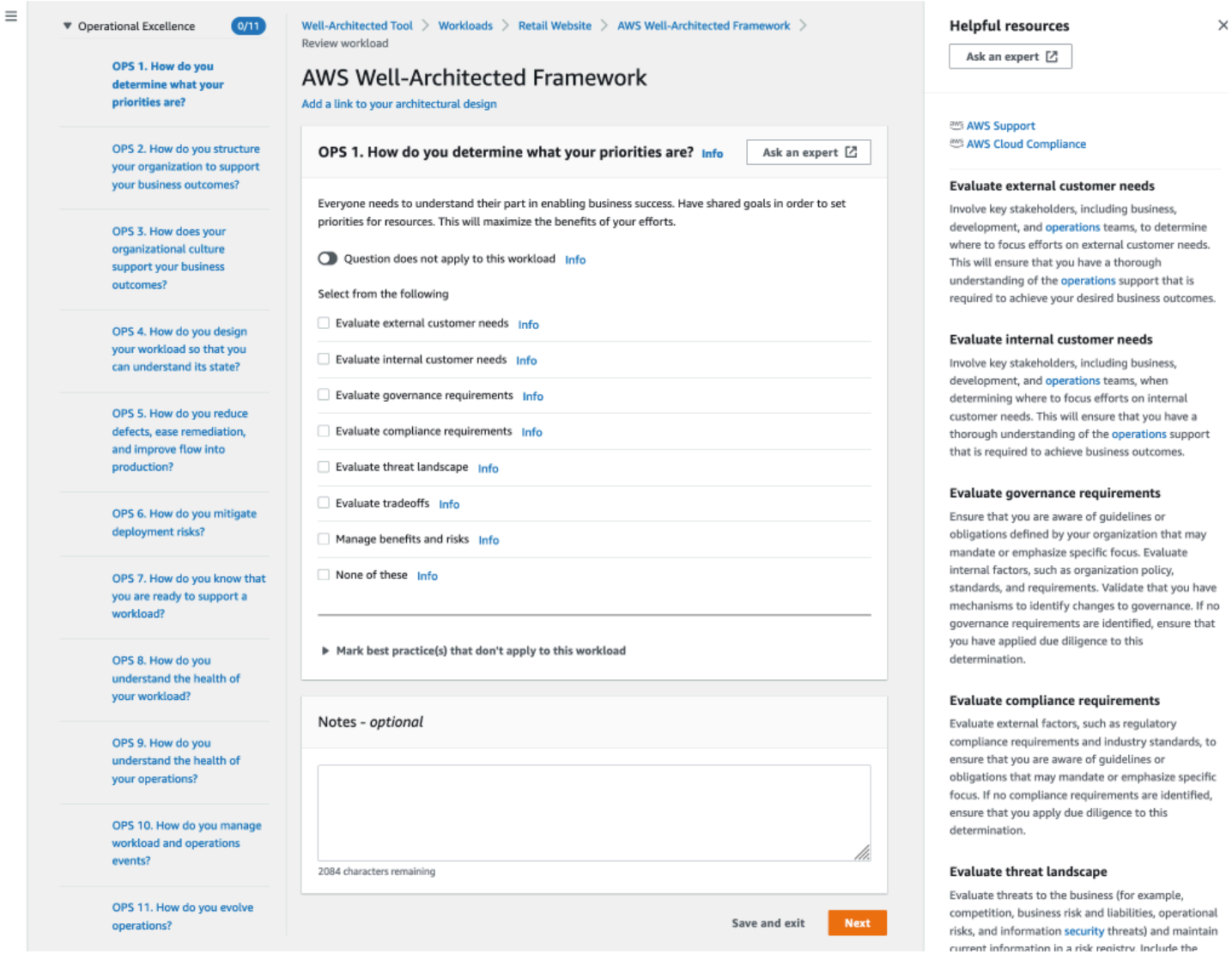
5. En el cuadro Propietario de la revisión, escriba el nombre de la persona responsable del proceso de revisión de la carga de trabajo.
6. En el cuadro Entorno, indique que la carga de trabajo se encuentra en un entorno de producción.
7. Nuestra carga de trabajo se ejecuta tanto en AWS como en nuestro centro de datos local:
    a. Seleccione Regiones de AWS y elija las dos regiones de Norteamérica donde se ejecuta la carga de trabajo.
    b. Seleccione también Regiones que no pertenecen a AWS, y escriba un nombre para nuestro centro de datos local.
8. El cuadro de ID de cuenta es opcional. No asocie ninguna Cuentas de AWS a esta carga de trabajo.
9. El cuadro de Solicitud es opcional. No introduzca un ARN de aplicación para esta carga de trabajo.
10. El cuadro del Diagrama arquitectónico es opcional. No asocie un diagrama arquitectónico a esta carga de trabajo.
11. Los cuadros Tipo de sector y Sector son opcionales y no están especificados en esta carga de trabajo.
12. La sección Trusted Advisor es opcional. No Active la compatibilidad con Trusted Advisor para esta carga de trabajo.
13. La sección de Jira es opcional. No marque la casilla Anular la configuración a nivel de cuenta de la sección de Jira para esta carga de trabajo.
14. Para este ejemplo, no aplique ninguna etiqueta a la carga de trabajo. Seleccione Siguiente.
15. El paso Aplicar perfil es opcional. No aplique un perfil a esta carga de trabajo. Seleccione Siguiente.
16. Para este ejemplo, aplique el enfoque del marco de AWS Well-Architected, que se selecciona automáticamente. Elija Definir carga de trabajo para guardar estos valores y definir la carga de trabajo.
17. Una vez definida la carga de trabajo, seleccione Comenzar revisión para empezar a documentar el estado de la carga de trabajo.

Paso 2: Documentar el estado de la carga de trabajo

Para documentar el estado de la carga de trabajo, se le presentan preguntas del enfoque seleccionado que abarcan los pilares del marco de AWS Well-Architected: excelencia operativa, seguridad, fiabilidad, eficiencia de rendimiento, optimización de costos y sostenibilidad.

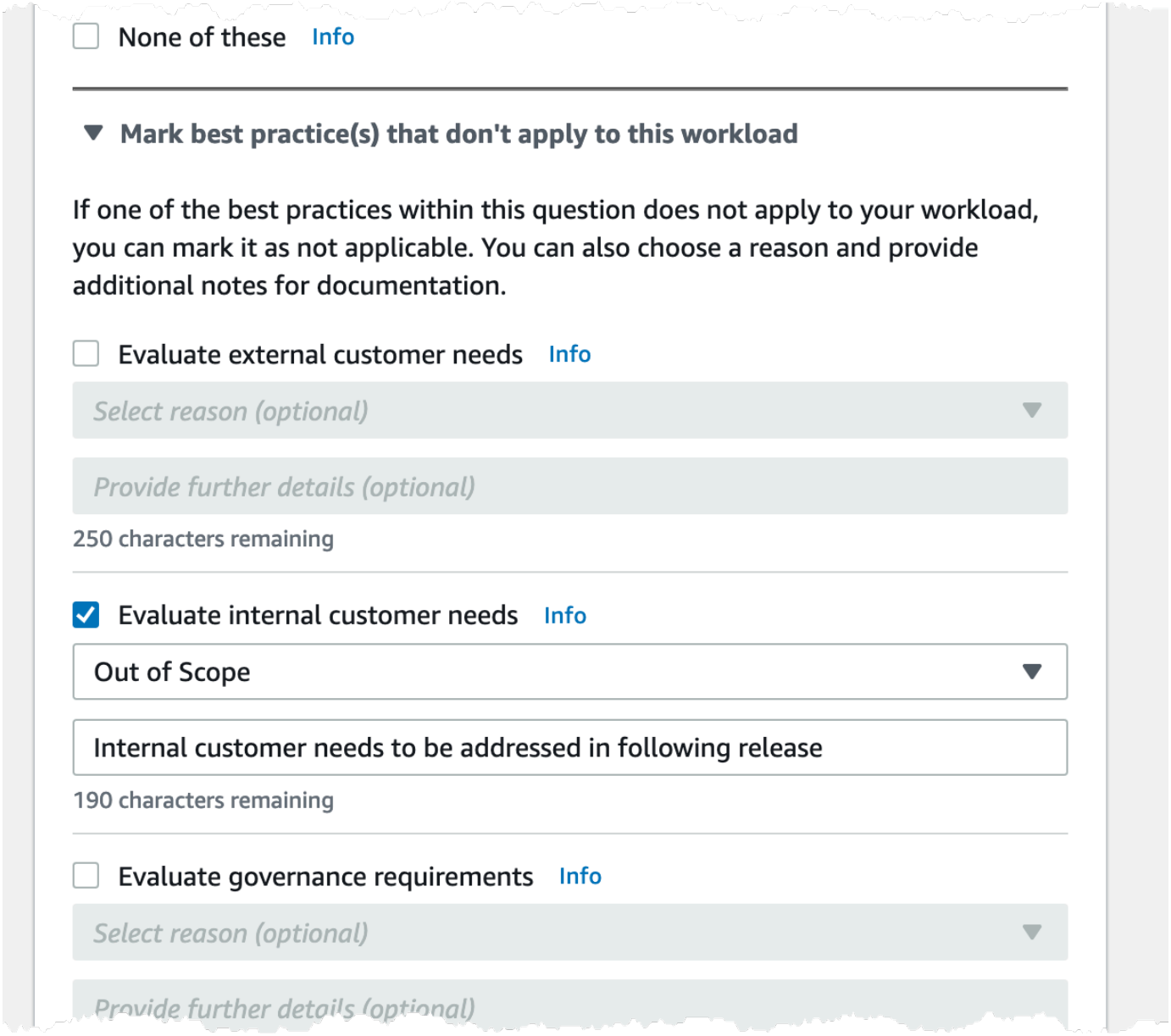
En cada pregunta, elija la prácticas recomendadas que está siguiendo en la lista proporcionada. Si necesita información acerca de una práctica recomendada, seleccione Información y vea la información adicional y los recursos en el panel derecho.

Seleccione Preguntar a un experto para acceder a la comunidad AWS re:post dedicada a AWS Well-Architected. En esta comunidad, puede hacer preguntas relacionadas con el diseño, la creación, la implementación y el funcionamiento de las cargas de trabajo en AWS.



1. Seleccione Siguiente para pasar a la siguiente pregunta. Puede utilizar el panel izquierdo para desplazarse a otra pregunta del mismo pilar o a una pregunta de uno de los otros pilares.
2. Si elige La pregunta no se aplica a esta carga de trabajo o Ninguna de estas, AWS recomienda que incluya el motivo en el cuadro opcional Notas. Estas notas se incluyen en el informe de la carga de trabajo y pueden resultar útiles en el futuro cuando se realicen cambios en la carga de trabajo.

> **Note**
>
> Si lo desea, puede marcar una o más prácticas recomendadas individuales como no aplicables. Elija Marcar las mejores prácticas que no se apliquen a esta carga de trabajo y seleccione las mejores prácticas que no se apliquen. Si lo desea, puede seleccionar un motivo y proporcionar detalles adicionales. Repita este procedimiento para cada práctica recomendada que no se aplique.



> **Note**
>
> Puede pausar este proceso en cualquier momento seleccionando Guardar y salir. Para reanudarlo más tarde, abra la consola de AWS WA Tool y elija Cargas de trabajo en el panel de navegación izquierdo.

3. Seleccione el nombre de la carga de trabajo para abrir la página de detalles.
4. Elija Continuar revisión y desplácese hasta donde lo dejó.

5. Después de completar todas las preguntas, aparecerá una página con información general sobre la carga de trabajo. Puede revisar estos detalles ahora o acceder a ellos más adelante haciendo clic en Cargas de trabajo en el panel de navegación izquierdo y seleccionando el nombre de la carga de trabajo.

Después de documentar el estado de la carga de trabajo por primera vez, debe guardar un hito y generar un informe.

Los hitos capturan el estado actual de la carga de trabajo y le permiten medir el progreso a medida que se aplican los cambios de su plan de mejora.

Desde la página de detalles de la carga de trabajo:

1. En la sección de Información general sobre la carga de trabajo, pulse el botón Guardar hito.
2. Introduzca **`Version 1.0 - initial review`** como Nombre del hito.
3. Seleccione Guardar.
4. Para generar un informe de carga de trabajo, seleccione el enfoque deseado, elija Generar informe y se creará un archivo PDF. Este archivo contiene el estado de la carga de trabajo, el número de riesgos identificados y una lista de las mejoras sugeridas.

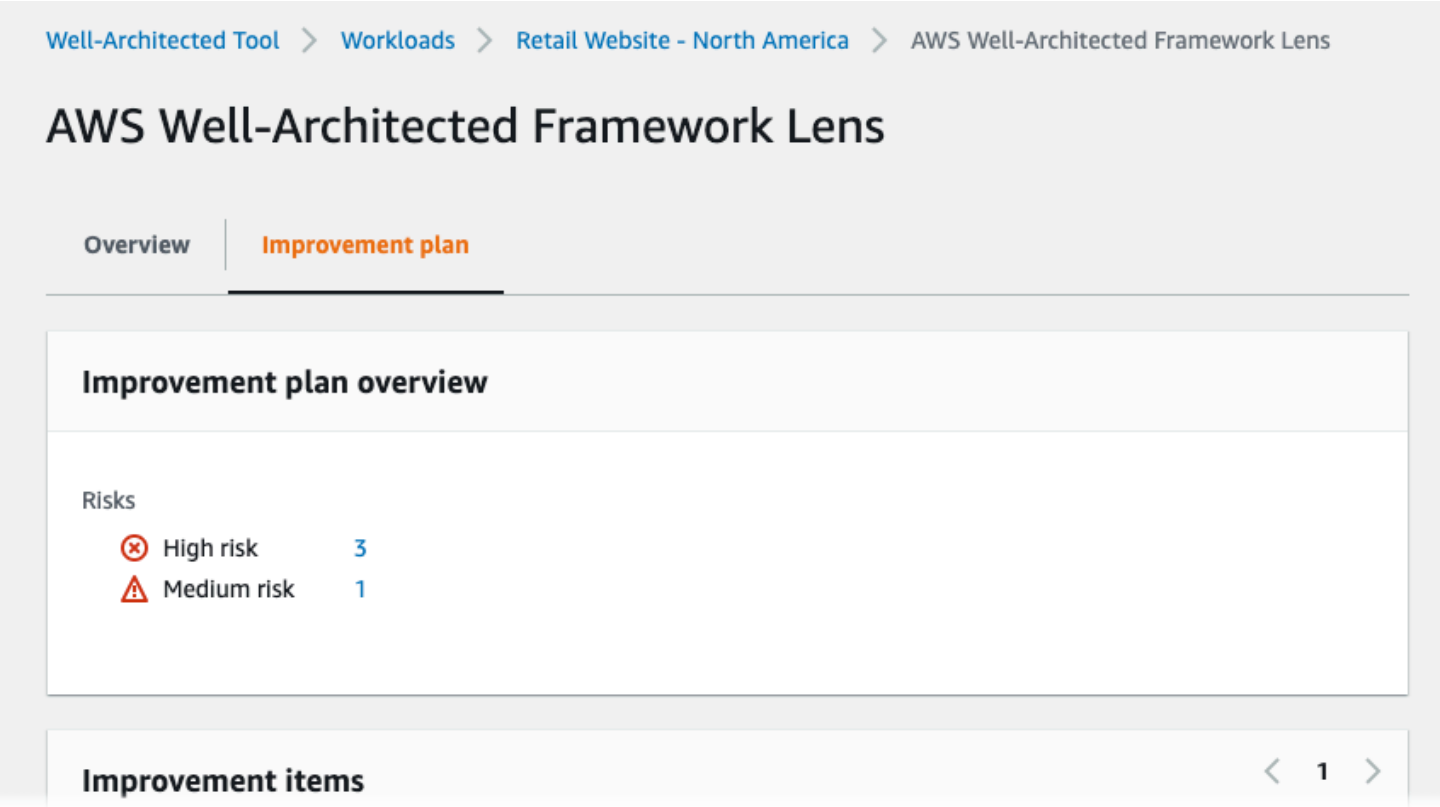
Paso 3: Revisar el plan de mejora

En función de las prácticas recomendadas seleccionadas, AWS WA Tool identificará las áreas de riesgo alto y medio según las medidas del enfoque del marco de AWS Well-Architected.

Paso 3: Revisar el plan de mejora

1. Elija el marco de AWS Well-Architected de la sección Enfoques de la página Información general.
2. A continuación, elija Plan de mejora.

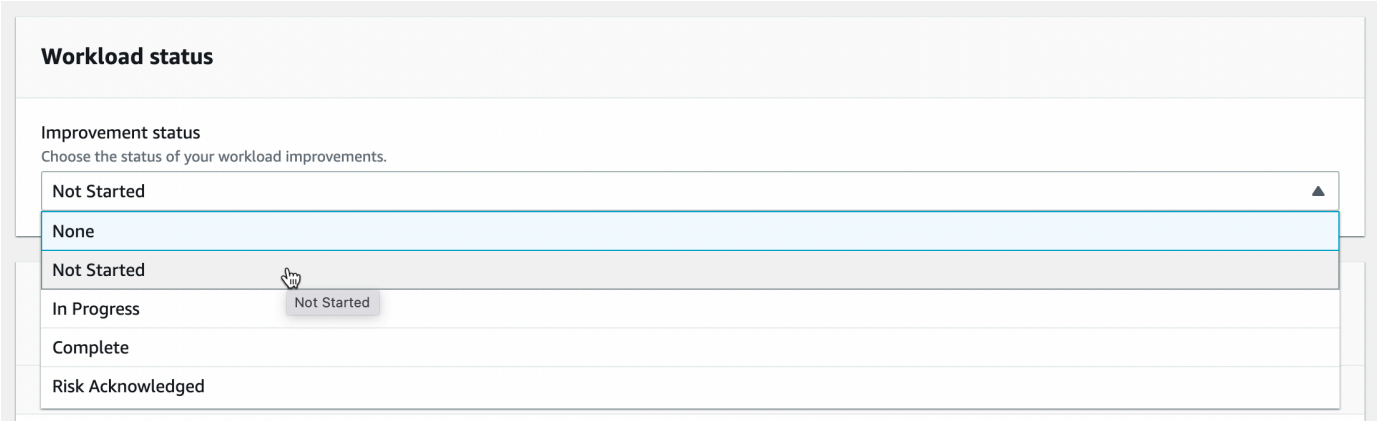
En el caso de esta carga de trabajo de ejemplo concreta, se identificaron tres problemas de riesgo alto y un problema de riesgo medio mediante el enfoque del marco de AWS Well-Architected.



Actualice el valor de Estado de mejora de la carga de trabajo para indicar que aún no se han iniciado mejoras en la carga de trabajo.

Para cambiar el Estado de la mejora:

1. En el plan de mejora, haga clic en el nombre de la carga de trabajo (**`Retail Website - North America`**) en la barra de navegación situada en la parte superior de la página.
2. Haga clic en la pestaña Propiedades.
3. Vaya a la sección Estado de la carga de trabajo y seleccione No iniciada en la lista desplegable.



4. Vuelva al plan de mejora desde la pestaña Propiedades haciendo clic en la pestaña Descripción general y, a continuación, en el enlace del marco de AWSWell-Architected de la sección Enfoques. A continuación, haga clic en la pestaña Plan de mejora situada en la parte superior de la página.

En la sección Elementos de mejora, se muestran los elementos de mejora recomendados identificados en la carga de trabajo. Las preguntas se ordenan en función de la prioridad de los pilares establecida. Los problemas de alto riesgo aparecen en primer lugar, seguidos de los problemas de riesgo medio.

Amplíe Elementos de mejora recomendados para mostrar las prácticas recomendadas de una pregunta. Cada acción de mejora recomendada se enlaza a orientación especializada y detallada para ayudarle a eliminar, o al menos mitigar, los riesgos identificados.

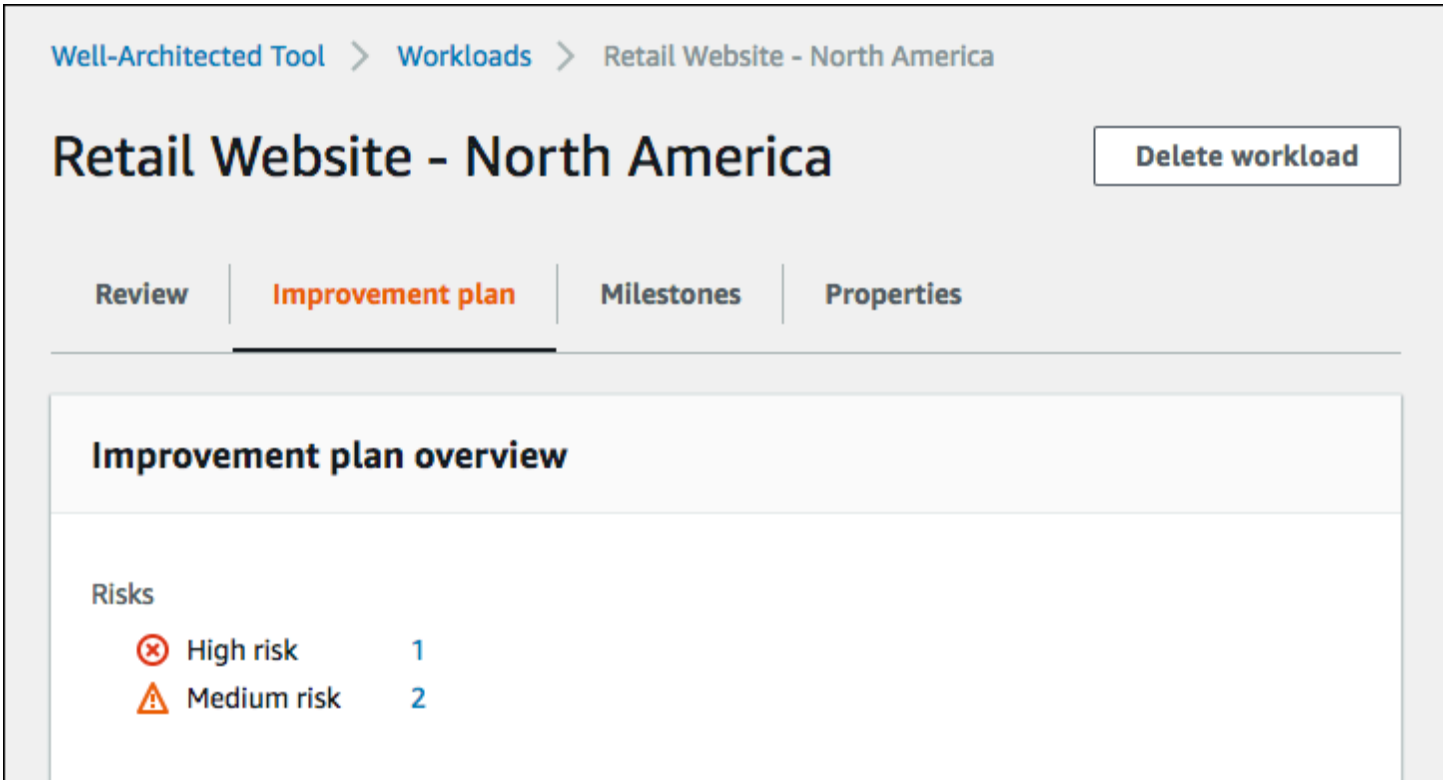
Si hay un perfil asociado a la carga de trabajo, se muestra un recuento de los riesgos priorizados en la sección de Información general del plan de mejora. También puede filtrar la lista de Elementos de mejora seleccionando Priorizados por perfil. La lista de elementos de mejora muestra una etiqueta de Priorizados.

Paso 4: Realizar mejoras y medir el progreso

Durante este plan de mejora, uno de los problemas de alto riesgo se solucionó agregando compatibilidad con Amazon CloudWatch y AWS Auto Scaling a la carga de trabajo.

Desde la sección de Elementos de mejora:

1. Elija la pregunta relevante y actualice las prácticas recomendadas seleccionadas para reflejar los cambios. Se añaden Notas para registrar las mejoras.
2. A continuación, seleccione Guardar y salir para actualizar el estado de la carga de trabajo.
3. Después de realizar los cambios, puede volver al Plan de mejora y ver el efecto que dichos cambios tuvieron en la carga de trabajo. En este ejemplo, esas acciones han mejorado el perfil de riesgo, lo que reduce el número de problemas de alto riesgo de tres a uno.



Puede guardar un hito en este punto e ir después a Hitos para ver cómo ha mejorado la carga de trabajo.

Cargas de trabajo

Una carga de trabajo es un conjunto de recursos y código que ofrece valor comercial, como una aplicación orientada al cliente o un proceso de backend.

Una carga de trabajo podría consistir en un subconjunto de recursos en una sola Cuenta de AWS o ser un conjunto de varios recursos que abarcan varias Cuentas de AWS. Un negocio pequeño podría tener solo algunas cargas de trabajo, mientras que uno grande podría tener miles.

La página Cargas de trabajo, disponible en el panel de navegación izquierdo, contiene información sobre sus cargas de trabajo y cualquier carga de trabajo que hayan compartido con usted.

Para cada carga de trabajo se muestra la siguiente información:

Nombre

El nombre de la carga de trabajo.

Propietario

El ID de la Cuenta de AWS que es la propietaria de la carga de trabajo.

Preguntas contestadas

El número de preguntas contestadas.

Riesgos altos

El número de problemas de alto riesgo identificados.

Riesgos medios

El número de problemas de riesgo medio identificados.

Estado de mejora

El estado de la mejora que ha establecido para la carga de trabajo:

- Ninguna
- No iniciada
- En curso
- Completado
- Riesgo entendido

Última actualización

La fecha y la hora a las que se actualizó por última vez la carga de trabajo.

Después de elegir una carga de trabajo de la lista:

- Para revisar los detalles de la carga de trabajo, elija Ver detalles.
- Para cambiar las propiedades de la carga de trabajo, elija Editar.
- Para gestionar el uso compartido de la carga de trabajo con otras Cuentas de AWS, usuarios, AWS Organizations o unidades organizativas (OU), seleccione Ver detalles y, a continuación, Recursos compartidos.
- Para eliminar la carga de trabajo y todos sus hitos, elija Eliminar. Solo el propietario de la carga de trabajo puede eliminarla.

> **Warning**
>
> La eliminación de una carga de trabajo no se puede deshacer. Todos los datos asociados a la carga de trabajo se eliminan.

Problemas de alto riesgo y problemas de riesgo medio

Los problemas de alto riesgo identificados en el AWS Well-Architected Tool son opciones arquitectónicas y operativas que AWS ha determinado que pueden tener un impacto negativo significativo en una empresa. Estos problemas de alto riesgo pueden afectar a las operaciones de la organización, los activos y las personas. Los problemas de riesgo medio también pueden afectar negativamente a las empresas, pero en menor medida. Estos problemas se basan en sus respuestas en el AWS Well-Architected Tool. Los clientes de AWS y AWS aplican ampliamente las prácticas recomendadas correspondientes. Estas prácticas recomendadas son la orientación definida por los enfoques y el marco de AWS Well-Architected.

> **Note**
>
> Estas son directrices solamente y los clientes deben evaluar y medir el impacto que tendría en su negocio no implementar las prácticas recomendadas. Si existen motivos técnicos o empresariales específicos que impidan aplicar una práctica recomendada a la carga de trabajo, el riesgo podría ser inferior al indicado. AWS sugiere que los clientes documenten

estos motivos y la forma en que afectan a las prácticas recomendadas en las notas sobre la carga de trabajo. Para todos los problemas de alto riesgo y riesgo medio identificados, AWS recomienda a los clientes implementar las prácticas recomendadas tal y como se define en el AWS Well-Architected Tool. Si se aplica la práctica recomendada, indique que el problema se ha resuelto marcando la mejor práctica como se cumple en el AWS Well-Architected Tool. Si los clientes deciden no implementar la práctica recomendada, AWS recomienda que documenten la aprobación de nivel empresarial aplicable y los motivos para no implementarla.

Definición de una carga de trabajo en AWS Well-Architected Tool

Hay dos formas de definir una carga de trabajo. En la página Cargas de trabajo, AWS WA Tool puede definir una carga de trabajo sin una plantilla. O bien, en la página de Revisión de plantillas, puede utilizar una plantilla de revisión existente o crear una plantilla nueva para definir una carga de trabajo.

Para definir una carga de trabajo desde la página Cargas de trabajo

1. En el panel de navegación izquierdo, elija Cargas de trabajo.
2. Seleccione el menú desplegable Definir carga de trabajo.
3. Seleccione Definir carga de trabajo. O bien, si ha creado una plantilla de revisión y desea definir una carga de trabajo a partir de ella, elija Definir a partir de la plantilla de revisión.
4. Siga las instrucciones en the section called “Definir una carga de trabajo” para especificar las propiedades de la carga de trabajo o (si lo desea) aplique perfiles y enfoques.

Para definir una carga de trabajo a partir de la página de plantillas de revisión

1. En el panel de navegación izquierdo, seleccione Plantillas de revisión.
2. Seleccione el nombre de una plantilla de revisión existente o siga las instrucciones en the section called “Creación de una plantilla de revisión” para crear una nueva plantilla de revisión.
3. Elija Definir carga de trabajo a partir de una plantilla.
4. Siga las instrucciones en the section called “Definición de una carga de trabajo a partir de una plantilla” para crear la carga de trabajo a partir de la plantilla de revisión.

Visualización de una carga de trabajo en AWS Well-Architected Tool

Puede ver los detalles de las cargas de trabajo que posee y las cargas de trabajo que se han compartido con usted.

Para ver una carga de trabajo

1. Inicie sesión en AWS Management Console y abra la consola de AWS Well-Architected Tool en https://console.aws.amazon.com/wellarchitected/.
2. En el panel de navegación izquierdo, elija Cargas de trabajo.
3. Seleccione la carga de trabajo que desea ver de una de las siguientes formas:
   - Elija el nombre de la carga de trabajo.
   - Seleccione la carga de trabajo y elija Ver detalles.

Aparece la página de detalles de la carga de trabajo.

> **Note**
>
> Se agregó un campo obligatorio, Propietario de la revisión, para permitirle identificar fácilmente a la persona o al grupo principal que es responsable del proceso de revisión.
> La primera vez que vea una carga de trabajo definida antes de que se agregase este campo, se le notificará este cambio. Elija Editar para definir el campo Propietario de la revisión; no será necesario realizar más acciones.
> Elija Confirmar para aplazar la configuración del campo Propietario de la revisión. Durante los próximos 60 días, se mostrará un banner para recordarle que el campo está en blanco. Para quitar el banner, edite la carga de trabajo y especifique un valor en Propietario de la revisión. Si no establece el campo en la fecha especificada, el acceso a la carga de trabajo quedará restringido. Podrá seguir viendo la carga de trabajo y eliminarla, pero no podrá editarla, excepto para establecer el campo Propietario de la revisión. El acceso compartido a la carga de trabajo no se ve afectado mientras el acceso está limitado.

Edición de una carga de trabajo en AWS Well-Architected Tool

Puede editar los detalles de una carga de trabajo que posee.

Para editar una carga de trabajo

1. Inicie sesión en AWS Management Console y abra la consola de AWS Well-Architected Tool en https://console.aws.amazon.com/wellarchitected/.
2. En el panel de navegación izquierdo, elija Cargas de trabajo.
3. Seleccione la carga de trabajo que desee editar y haga clic en Editar.
4. Realice los cambios que desee en la carga de trabajo.

   Para obtener una descripción de cada uno de los campos, consulte Definición de una carga de trabajo en AWS WA Tool.

   > **Note**
   >
   > Al actualizar una carga de trabajo existente, puede Activar Trusted Advisor, lo que crea automáticamente el rol de IAM para el propietario de la carga de trabajo. Los propietarios de las cuentas asociadas a las cargas de trabajo con Trusted Advisor activado deben crear un rol en IAM. Para obtener más información, consulte the section called “Activación Trusted Advisor en IAM”.

5. Elija Guardar para guardar los cambios en la carga de trabajo.

   Si un cuadro necesario está en blanco o si un valor especificado no es válido, debe corregir el problema antes de guardar las actualizaciones en la carga de trabajo.

Cómo compartir una carga de trabajo en AWS Well-Architected Tool

Puede compartir una carga de trabajo de su propiedad con otras Cuentas de AWS, usuarios, organización y unidades organizativas (OU) de la misma Región de AWS.

> **Note**
>
> Solo puede compartir cargas de trabajo dentro de la misma Región de AWS.
> Al compartir una carga de trabajo con otra Cuenta de AWS, si el destinatario no tiene el permiso `wellarchitected:UpdateShareInvitation`, no podrá aceptar la invitación

para compartir. Consulte the section called “Proporcionar acceso a AWS WA Tool.” para ver ejemplos de políticas de permisos.

Uso compartido de una carga de trabajo con otras Cuentas de AWS y usuarios

1. Inicie sesión en AWS Management Console y abra la consola de AWS Well-Architected Tool en https://console.aws.amazon.com/wellarchitected/.
2. En el panel de navegación izquierdo, elija Cargas de trabajo.
3. Seleccione una carga de trabajo que posea de una de las siguientes maneras:
   - Elija el nombre de la carga de trabajo.
   - Seleccione la carga de trabajo y elija Ver detalles.
4. Seleccione Recursos compartidos. A continuación, seleccione Crear y Crear recursos compartidos con usuarios o cuentas para crear una invitación a una carga de trabajo.
5. Introduzca el ID de la Cuenta de AWS de 12 dígitos o el ARN del usuario con el que desea compartir la carga de trabajo.
6. Seleccione el permiso que desea conceder.

   Solo lectura

   Proporciona acceso de solo lectura a la carga de trabajo.

   Colaborador

   Proporciona acceso de actualización a las respuestas y las notas y acceso de solo lectura al resto de la carga de trabajo.
7. Elija Crear para enviar una invitación a la carga de trabajo a la Cuenta de AWS o al usuario especificado.

Si la invitación a la carga de trabajo no se acepta en un plazo de siete días, la invitación caducará automáticamente.

Si un usuario y la Cuenta de AWS del usuario tienen invitaciones a la carga de trabajo, la invitación a la carga de trabajo con el nivel más alto de permiso se aplica al usuario.

> **Important**
>
> Antes de compartir una carga de trabajo con una organización o unidad organizativa (OU), debe habilitar el acceso a AWS Organizations.

Para compartir una carga de trabajo con su organización o unidades organizativas

1. Inicie sesión en AWS Management Console y abra la consola de AWS Well-Architected Tool en https://console.aws.amazon.com/wellarchitected/.
2. En el panel de navegación izquierdo, elija Cargas de trabajo.
3. Seleccione una carga de trabajo que posea de una de las siguientes maneras:
   - Elija el nombre de la carga de trabajo.
   - Seleccione la carga de trabajo y elija Ver detalles.
4. Seleccione Recursos compartidos. A continuación, elija Crear y Crear recursos compartidos para organizaciones.
5. En la página Crear carga de trabajo compartida, elija si desea conceder permisos a toda la organización o a una o más unidades organizativas.
6. Seleccione el permiso que desea conceder.

   Solo lectura

   Proporciona acceso de solo lectura a la carga de trabajo.

   Colaborador

   Proporciona acceso de actualización a las respuestas y las notas y acceso de solo lectura al resto de la carga de trabajo.
7. Seleccione Crear para compartir la carga de trabajo.

Para ver quién tiene acceso compartido a una carga de trabajo, seleccione Recursos compartidos en la página Visualización de detalles de las cargas de trabajo en AWS Well-Architected Tool.

Para evitar que una entidad comparta cargas de trabajo, adjunte una política que deniegue acciones `wellarchitected:CreateWorkloadShare`.

También puede compartir los enfoques personalizados de su propiedad con otras Cuentas de AWS, usuarios, su organización y unidades organizativas de la misma Región de AWS. Consulte Cómo compartir un enfoque personalizado en AWS WA Tool para obtener más información.

Consideraciones a la hora de compartir cargas de trabajo de AWS Well-Architected Tool

Una carga de trabajo se puede compartir con hasta 20 Cuentas de AWS diferentes y usuarios. Una carga de trabajo solo puede compartirse con cuentas y usuarios que se encuentran en la misma Región de AWS que la carga de trabajo.

Para compartir una carga de trabajo en una región introducida después del 20 de marzo de 2019, tanto usted como la Cuenta de AWS deben habilitar la región en la AWS Management Console. Para obtener más información, consulte Infraestructura global de AWS.

Puede compartir una carga de trabajo con una Cuenta de AWS, usuarios individuales en una cuenta o ambos. Cuando comparte una carga de trabajo con una Cuenta de AWS, todos los usuarios de esa cuenta tienen acceso a la carga de trabajo. Si solo los usuarios específicos de una cuenta precisan acceso, siga la práctica recomendada de otorgar el privilegio mínimo y comparta la carga de trabajo individualmente con esos usuarios.

Si tanto una Cuenta de AWS como un usuario en la cuenta tienen invitaciones a la carga de trabajo, la invitación a la carga de trabajo con el permiso máximo determina el permiso del usuario para la carga de trabajo. Si elimina la invitación a la carga de trabajo para el usuario, el acceso del usuario viene determinado por la invitación a la carga de trabajo para la Cuenta de AWS. Elimine las invitaciones de carga de trabajo para eliminar el acceso del usuario a la carga de trabajo.

Antes de compartir una carga de trabajo con una organización o una o más unidad organizativa (OU), debe habilitar el acceso a AWS Organizations.

Si comparte una carga de trabajo con una organización y con una o más unidades organizativas, la invitación a la carga de trabajo con los permisos de nivel más alto determina el permiso de la cuenta para acceder a la carga de trabajo.

Habilitación del uso compartido de AWS Organizations

1. Inicie sesión en AWS Management Console y abra la consola de AWS Well-Architected Tool en https://console.aws.amazon.com/wellarchitected/.
2. En el panel de navegación izquierdo, elija Configuración.

3. Seleccione Habilitar el soporte de AWS Organizations.
4. Elija Guardar configuración.

Eliminación del acceso compartido en AWS Well-Architected Tool

Puede eliminar una invitación a la carga de trabajo. La eliminación de una invitación a la carga de trabajo quita el acceso compartido a la carga de trabajo.

Para eliminar el acceso compartido a una carga de trabajo

1. Inicie sesión en AWS Management Console y abra la consola de AWS Well-Architected Tool en https://console.aws.amazon.com/wellarchitected/.
2. En el panel de navegación izquierdo, elija Cargas de trabajo.
3. Seleccione la carga de trabajo de una de las siguientes formas:
   - Elija el nombre de la carga de trabajo.
   - Seleccione la carga de trabajo y elija Ver detalles.
4. Seleccione Recursos compartidos.
5. Seleccione invitación a la carga de trabajo que va a eliminar y elija Eliminar.
6. Elija Eliminar para confirmar.

Si un usuario la Cuenta de AWS del usuario tienen invitaciones a la carga de trabajo, debe eliminar las dos invitaciones de carga de trabajo para eliminar el permiso del usuario a la carga de trabajo.

Modificación del acceso compartido en AWS Well-Architected Tool

Puede modificar una invitación a la carga de trabajo pendiente o aceptada.

Para modificar el acceso compartido a una carga de trabajo

1. Inicie sesión en AWS Management Console y abra la consola de AWS Well-Architected Tool en https://console.aws.amazon.com/wellarchitected/.
2. En el panel de navegación izquierdo, elija Cargas de trabajo.
3. Seleccione una carga de trabajo que posea de una de las siguientes maneras:
   - Elija el nombre de la carga de trabajo.
   - Seleccione la carga de trabajo y elija Ver detalles.

4. Seleccione Recursos compartidos.
5. Seleccione invitación a la carga de trabajo que va a modificar y elija Editar.
6. Seleccione el nuevo permiso que desea conceder a la cuenta de Cuenta de AWS o al usuario.

   Solo lectura

   Proporciona acceso de solo lectura a la carga de trabajo.

   Colaborador

   Proporciona acceso de actualización a las respuestas y las notas y acceso de solo lectura al resto de la carga de trabajo.
7. Seleccione Guardar.

Si la invitación a la carga de trabajo modificada no se acepta en un plazo de siete días, caducará automáticamente.

Aceptación y rechazo de invitaciones a una carga de trabajo en AWS Well-Architected Tool

Una invitación a la carga de trabajo es una solicitud para compartir una carga de trabajo que pertenece a otra Cuenta de AWS. Si acepta la invitación a la carga de trabajo, la carga de trabajo se agrega a las páginas Cargas de trabajo y Panel. Si rechaza la invitación a la carga de trabajo, se elimina de la lista de invitaciones de carga de trabajo.

Tiene siete días para aceptar una invitación a la carga de trabajo. Si no acepta la invitación en el plazo de siete días, caducará automáticamente.

> **Note**
>
> Las cargas de trabajo solo se pueden compartir dentro de la misma Región de AWS.

Para aceptar o rechazar una invitación a la carga de trabajo

1. Inicie sesión en AWS Management Console y abra la consola de AWS Well-Architected Tool en https://console.aws.amazon.com/wellarchitected/.
2. En el panel de navegación izquierdo, seleccione Invitaciones a las cargas de trabajo.

3. Seleccione invitación a la carga de trabajo que desea aceptar o rechazar.
   - Para aceptar la invitación a la carga de trabajo, elija Aceptar.

     La carga de trabajo se agrega a las páginas Cargas de trabajo y Panel.
   - Para rechazar la invitación a la carga de trabajo, seleccione Rechazar.

     La invitación a la carga de trabajo se elimina de la lista.

Para rechazar el acceso compartido después de que se haya aceptado una invitación a la carga de trabajo, seleccione Rechazar recurso compartido en la página Visualización de detalles de las cargas de trabajo en AWS Well-Architected Tool de la carga de trabajo.

Eliminación de una carga de trabajo en AWS Well-Architected Tool

Cuando ya no necesite una carga de trabajo, puede eliminarla. Al eliminar una carga de trabajo, se eliminan todos los datos asociados a la carga de trabajo, incluido cualquier hito e invitación de recurso compartido de carga de trabajo. Solo el propietario de una carga de trabajo puede eliminarla.

> **Warning**
>
> La eliminación de una carga de trabajo no se puede deshacer. Todos los datos asociados a la carga de trabajo se eliminan de forma permanente.

Para eliminar una carga de trabajo

1. Inicie sesión en AWS Management Console y abra la consola de AWS Well-Architected Tool en https://console.aws.amazon.com/wellarchitected/.
2. En el panel de navegación izquierdo, elija Cargas de trabajo.
3. Seleccione la carga de trabajo que desee eliminar y elija Eliminar.
4. En la ventana Eliminar, elija Eliminar para confirmar la eliminación de la carga de trabajo y sus hitos.

Para evitar que una entidad elimine cargas de trabajo, adjunte una política que deniegue acciones `wellarchitected:DeleteWorkload`.

Generación de un informe de carga de trabajo en AWS Well-Architected Tool

Puede generar un informe de carga de trabajo de un enfoque. El informe contiene sus respuestas a las preguntas de la carga de trabajo, las notas y el número actual de riesgos altos y medios identificados en la carga de trabajo. Si una pregunta tiene uno o varios riesgos identificados, el plan de mejora asociado con esa pregunta indicará las acciones que pueden realizarse para mitigarlos.

Si su carga de trabajo tiene un perfil asociado, la información general del perfil y los riesgos priorizados se muestran en el informe de carga de trabajo.

Los informes le permiten compartir información detallada sobre la carga de trabajo con otros usuarios que no tienen acceso a AWS Well-Architected Tool.

Para generar un informe de carga de trabajo

1. Inicie sesión en AWS Management Console y abra la consola de AWS Well-Architected Tool en https://console.aws.amazon.com/wellarchitected/.
2. En el panel de navegación izquierdo, elija Cargas de trabajo.
3. Seleccione la carga de trabajo deseada y elija Ver detalles.
4. Seleccione el enfoque para la que desea generar un informe y elija Generar informe.

   El informe se genera y se puede descargar o ver.

Visualización de detalles de las cargas de trabajo en AWS Well-Architected Tool

La página de detalles de la carga de trabajo proporciona información sobre la carga de trabajo, incluidos los hitos, el plan de mejora y cualquier recurso compartido de la carga de trabajo. Utilice las pestañas en la parte superior de la página para desplazarse por las diferentes secciones de detalles.

Para eliminar la carga de trabajo, seleccione Eliminar carga de trabajo. Solo el propietario de una carga de trabajo puede eliminarla.

Para eliminar el acceso a una carga de trabajo compartida, seleccione Rechazar recurso compartido.

Temas

La pestaña Información general de AWS Well-Architected Tool

Al visualizar inicialmente una carga de trabajo, la pestaña Información general es la primera información mostrada. Esta pestaña indica el estado general de la carga de trabajo, seguido del estado de cada enfoque.

Si no ha completado todas las preguntas, aparecerá un banner para recordarle que debe comenzar o continuar con la documentación de la carga de trabajo.

En la sección Información general de la carga de trabajo, se indica el estado general actual de la carga de trabajo y las notas que haya escrito en Notas de la carga de trabajo. Elija Editar para actualizar el estado o las notas.

Para obtener el estado actual de la carga de trabajo, seleccione Guardar hito. Los hitos son inmutables y no se pueden cambiar una vez que se guardan.

Para continuar la documentación del estado de la carga de trabajo, elija Comenzar revisión y seleccione el enfoque deseado.

La pestaña Hitos de AWS Well-Architected Tool

Para mostrar los hitos de su carga de trabajo, elija la pestaña Hitos.

Después de seleccionar un hito, elija Generar informe para crear el informe de la carga de trabajo asociada al hito. El informe contiene sus respuestas a las preguntas de la carga de trabajo, las notas y el número de riesgos altos y medios presentes en la carga de trabajo en el momento en que se guardó el hito.

Puede ver detalles sobre el estado de la carga de trabajo en el momento de un hito específico:

- Eligiendo el nombre del hito.
- Seleccionando el hito y eligiendo Ver hito.

La pestaña Propiedades de AWS Well-Architected Tool

Para mostrar las propiedades de su carga de trabajo, elija la pestaña Propiedades. Inicialmente, estas propiedades son los valores que se especificaron cuando se definió la carga de trabajo. Seleccione Editar para realizar cambios. Solo el propietario de la carga de trabajo puede realizar cambios.

Para obtener descripciones de las propiedades, consulte Definición de una carga de trabajo en AWS WA Tool.

La pestaña Recursos compartidos de AWS Well-Architected Tool

Para mostrar o modificar las invitaciones de carga de trabajo, seleccione la pestaña Recursos compartidos. Esta pestaña sólo se muestra al propietario de una carga de trabajo.

Se muestra la siguiente información para cada Cuenta de AWS y usuario que tiene acceso compartido a la carga de trabajo:

Entidad principal

El ID de Cuenta de AWS o el ARN de usuario con acceso compartido a la carga de trabajo.

Status

El estado de la invitación a la carga de trabajo.

- Pendiente

  La invitación está a la espera de ser aceptada o rechazada. Si una invitación a la carga de trabajo no se acepta en un plazo de siete días, caducará automáticamente.

- Aceptada

  La invitación fue aceptada.

- Rechazada

  La invitación fue rechazada.

- Vencido

  No se aceptó ni rechazó la invitación en un plazo de siete días.

Permiso

Permiso concedido a la Cuenta de AWS o al usuario.

- Solo lectura

  La entidad principal tiene acceso de sólo lectura a la carga de trabajo.

- Colaborador

  La entidad principal puede acceder a las respuestas de actualización y a las notas y tiene acceso de solo lectura al resto de la carga de trabajo.

Detalles del permiso

Descripción detallada del permiso.

Para compartir la carga de trabajo con otra Cuenta de AWS o usuario en la misma Región de AWS, seleccione Crear. Una carga de trabajo se puede compartir con hasta 20 Cuentas de AWS diferentes y usuarios.

Para eliminar una invitación a una carga de trabajo, seleccione la invitación y elija Eliminar.

Para modificar una invitación a una carga de trabajo, seleccione la invitación y elija Editar.

Uso de enfoques en AWS WA Tool

En AWS Well-Architected Tool, puede usar enfoques para medir las arquitecturas de forma coherente con arreglo a unas prácticas recomendadas, así como identificar áreas de mejora. El enfoque del marco de AWS Well-Architected se aplica automáticamente cuando se define una carga de trabajo.

Una carga de trabajo puede tener aplicados uno o varios enfoques. Cada enfoque tiene su propio conjunto de preguntas, prácticas recomendadas, notas y plan de mejora.

Hay dos tipos de lentes que se pueden aplicar a las cargas de trabajo: lentes del catálogo de enfoques y lentes personalizadas.

- Catálogo de lentes: lentes oficiales creadas y mantenidas por AWS. El catálogo de enfoques está disponible para todos los usuarios y no requiere ninguna instalación adicional para su uso.
- Lentes personalizadas: definidas por el usuario que no son de contenido oficial de AWS. Puede crear lentes personalizadas con sus propios pilares, preguntas, prácticas recomendadas y planes de mejora, así como compartir lentes personalizadas con otras Cuentas de AWS.

Se pueden agregar cinco lentes a la vez a una carga de trabajo, con un máximo de 20 lentes a un carga de trabajo.

Si se elimina un enfoque de una carga de trabajo, se conservan los datos asociados con el enfoque. Los datos se restauran si vuelve a agregar el enfoque a la carga de trabajo.

Cómo agregar un enfoque a una carga de trabajo en AWS WA Tool

Agregar una lente a una carga de trabajo le ayuda a comprender mejor los puntos fuertes y débiles de la arquitectura, a identificar las mejoras y a garantizar que las cargas de trabajo sigan las prácticas recomendadas.

Para agregar un enfoque a una carga de trabajo

1. Inicie sesión en AWS Management Console y abra la consola de AWS Well-Architected Tool en https://console.aws.amazon.com/wellarchitected/.
2. En el panel de navegación izquierdo, elija Cargas de trabajo.

3. Seleccione la carga de trabajo deseada y elija Ver detalles.
4. Seleccione la lente que desea agregar y elija Guardar.

   Las lentes se pueden seleccionar de las lentes personalizadas, del catálogo de enfoques o de ambos.

Se pueden añadir hasta 20 enfoques a una carga de trabajo.

Para obtener más información sobre el catálogo de enfoques de AWS, consulte Enfoques de AWS Well-Architected. Tenga en cuenta que no todos los documentos técnicos sobre lentes se proporcionan como lentes en el catálogo de enfoques.

> **Exención de responsabilidad**
>
> Al acceder o aplicar enfoques personalizados creados por otro usuario o cuenta de AWS, usted reconoce que los enfoques personalizados creados por otros usuarios y compartidos con usted son contenido de terceros, según se define en el Acuerdo del cliente de AWS.

Eliminación de un enfoque de una carga de trabajo en AWS WA Tool

Si un enfoque ya no es pertinente para su carga de trabajo, puede quitarlo.

Para eliminar un enfoque de una carga de trabajo

1. Inicie sesión en AWS Management Console y abra la consola de AWS Well-Architected Tool en https://console.aws.amazon.com/wellarchitected/.
2. En el panel de navegación izquierdo, elija Cargas de trabajo.
3. Seleccione la carga de trabajo deseada y elija Ver detalles.
4. Anule la selección de la lente que desea quitar y elija Guardar.

   El enfoque del marco de AWS Well-Architected no se puede eliminar de una carga de trabajo.

Se conservan los datos asociados con el enfoque. Si el enfoque se vuelve a agregar a la carga de trabajo, los datos se restauran.

Visualización de los detalles de los enfoques para una carga de trabajo en AWS WA Tool

Puede ver los detalles de sus enfoques en la consola de AWS Well-Architected Tool. Para ver los detalles de un enfoque, seleccione el enfoque que desee.

Pestaña Información general

La pestaña Información general contiene información general sobre el enfoque, como el número de preguntas respondidas. Desde esta pestaña, puede continuar revisando una carga de trabajo, generar un informe o editar las notas del enfoque.

Pestaña Plan de mejora

La pestaña Plan de mejora contiene una lista de acciones recomendadas para mejorar la carga de trabajo. Puede filtrar las recomendaciones en función del riesgo y del pilar.

Pestaña Recursos compartidos

En el caso de un enfoque personalizado, la pestaña Recursos compartidos proporciona una lista de entidades principales de IAM con los que se ha compartido el enfoque.

Enfoques personalizados para cargas de trabajo en AWS WA Tool

Puede crear enfoques personalizados con sus propios pilares, preguntas, prácticas recomendadas y plan de mejora. Puede aplicar enfoques personalizados a una carga de trabajo de la misma manera que aplica los enfoques proporcionados por AWS. También puede compartir los enfoques personalizados que cree con otras Cuentas de AWS, y los enfoques personalizados que sean propiedad de otras personas se pueden compartir con usted.

Puede adaptar las preguntas con un enfoque personalizado para que sean específicas de una tecnología en particular, lo ayuden a satisfacer las necesidades de gobierno de su organización o ampliar la orientación proporcionada por el marco de Well-Architected y los enfoques de AWS. Al igual que los enfoques actuales, puede realizar un seguimiento del progreso a lo largo del tiempo mediante la creación de hitos y proporcionar información periódica sobre el estado mediante la generación de informes.

Temas

- Creación de un enfoque personalizado para una carga de trabajo en AWS WA Tool
- Vista previa de un enfoque personalizado para una carga de trabajo en AWS WA Tool
- Publicación de un enfoque personalizado en AWS WA Tool por primera vez
- Publicación de una actualización de un enfoque personalizado en AWS WA Tool
- Cómo compartir un enfoque personalizado en AWS WA Tool
- Cómo agregar etiquetas a un enfoque personalizado en AWS WA Tool
- Eliminación de un enfoque personalizado en AWS WA Tool
- Especificación del formato del enfoque en AWS WA Tool

Visualización de enfoques personalizados en AWS WA Tool

Puede ver los detalles de los enfoques personalizados de su propiedad y los enfoques personalizados que se hayan compartido con usted.

Visualización de un enfoque

1. Inicie sesión en AWS Management Console y abra la consola de AWS Well-Architected Tool en https://console.aws.amazon.com/wellarchitected/.
2. En el panel de navegación izquierdo, elija Enfoques personalizados.

   > **Note**
   >
   > La sección de lentes personalizadas está vacía si no ha creado una lente personalizada o si ha compartido una lente personalizada con usted.

3. Elija los enfoques personalizados que desea ver:
   - De mi propiedad: muestra los enfoques personalizados que ha creado.
   - Compartidas conmigo: muestra enfoques personalizados que se han compartido con usted.
4. Seleccione el enfoque personalizado que desea ver de una de las siguientes formas:
   - Elija el nombre del enfoque.
   - Seleccione el enfoque y elija Ver detalles.

Se abre la página Visualización de los detalles de los enfoques para una carga de trabajo en AWS WA Tool.

La página de Enfoques personalizados tiene los subcampos siguientes:

Nombre

Nombre del enfoque

Propietario

El ID de la Cuenta de AWS que posee el enfoque personalizado.

Estado

El estado PUBLICADO significa que el enfoque personalizado se ha publicado y se puede aplicar a las cargas de trabajo o compartirla con otras Cuentas de AWS.

El estado BORRADOR significa que el enfoque personalizado se ha creado pero aún no se ha publicado. Se debe publicar un enfoque personalizado antes de poder aplicarla a las cargas de trabajo o compartirla.

Versión

Nombre de la versión del enfoque personalizado.

Última actualización

La fecha y la hora a las que se actualizó por última vez el enfoque personalizado.

Creación de un enfoque personalizado para una carga de trabajo en AWS WA Tool

Para crear un enfoque personalizado

1. Inicie sesión en AWS Management Console y abra la consola de AWS Well-Architected Tool en https://console.aws.amazon.com/wellarchitected/.
2. En el panel de navegación izquierdo, elija Enfoques personalizados.
3. Seleccione Crear enfoque personalizado.
4. Seleccione Descargar archivo para descargar el archivo de plantilla JSON.
5. Abra el archivo de plantilla JSON con su editor de texto favorito y añada los datos para su enfoque personalizado. Estos datos incluyen los pilares, las preguntas, las mejores prácticas y los enlaces a los planes de mejora.

Consulte Especificación del formato del enfoque en AWS WA Tool para obtener más información. Un enfoque personalizado no puede superar los 500 KB de tamaño.

6. Seleccione Elegir archivo y seleccione su archivo JSON.
7. (Opcional) En la sección Etiquetas, añada las etiquetas que desee asociar a el enfoque personalizado.
8. Seleccione Enviar y previsualizar para obtener una vista previa del enfoque personalizado o Enviar para enviar el enfoque personalizado sin previsualizar.

   Si elige Enviar y previsualizar su enfoque personalizado, puede seleccionar Siguiente para navegar por la vista previa del enfoque o seleccionar Salir de la vista previa para volver a las Enfoques personalizados.

Si se produce un error en la validación, edite el archivo JSON e intente crear de nuevo el enfoque personalizado.

Una vez que AWS WA Tool valida el archivo JSON, el enfoque personalizado se muestra en Enfoques personalizados.

Una vez creado un enfoque personalizado, pasa a estar en estado BORRADOR. Debe publicar el enfoque para poder aplicarla a cargas de trabajo o compartirla con otras Cuentas de AWS.

Puede crear hasta 15 enfoques personalizados en una Cuenta de AWS.

> **Exención de responsabilidad**
>
> No incluya ni recopile información de identificación personal (PII) de los usuarios finales u otras personas identificables en sus enfoques personalizados o a través de ellos. Si sus enfoques personalizados o los que compartimos con usted y utilizan en su cuenta incluyen o recopilan información de identificación personal, usted es responsable de: garantizar que la PII incluida se procese de conformidad con la legislación aplicable, proporcionar los avisos de privacidad adecuados y obtener los consentimientos necesarios para procesar dichos datos.

Vista previa de un enfoque personalizado para una carga de trabajo en AWS WA Tool

Para obtener una vista previa de un enfoque personalizado

1. Inicie sesión en AWS Management Console y abra la consola de AWS Well-Architected Tool en https://console.aws.amazon.com/wellarchitected/.
2. En el panel de navegación izquierdo, elija Enfoques personalizados.
3. Solo se pueden previsualizar los enfoques en estado BORRADOR. Seleccione el enfoque personalizado con estado BORRADOR que desee y elija Vista previa de la experiencia.
4. Seleccione Siguiente para navegar por la vista previa del enfoque.
5. (Opcional) Para revisar su plan de mejora, seleccione las prácticas recomendadas en cada pregunta de la vista previa y seleccione Actualizar según las respuestas para poner a prueba su lógica de riesgo. Si es necesario realizar cambios, puede actualizar las Reglas de riesgo de su plantilla JSON antes de publicarlas.
6. Seleccione Salir de la vista previa para volver al enfoque personalizado.

> **Note**
>
> También puede previsualizar un enfoque personalizado seleccionando Enviar y previsualizar al Crear un enfoque personalizado.

Publicación de un enfoque personalizado en AWS WA Tool por primera vez

Para publicar un enfoque personalizado

1. Inicie sesión en AWS Management Console y abra la consola de AWS Well-Architected Tool en https://console.aws.amazon.com/wellarchitected/.
2. En el panel de navegación izquierdo, elija Enfoques personalizados.
3. Seleccione el enfoque personalizado que desee y elija Publicar enfoque.
4. En el cuadro Nombre de la versión, introduzca un identificador único para el cambio de versión. Este valor puede tener hasta 32 caracteres y solo debe contener caracteres alfanuméricos y puntos (“.”).
5. Seleccione Publicar enfoque personalizado.

Una vez publicado un enfoque personalizado, pasa al estado PUBLICADA.

El enfoque personalizado ahora se puede aplicar a las cargas de trabajo o se puede compartir con otras Cuentas de AWS o usuarios.

Publicación de una actualización de un enfoque personalizado en AWS WA Tool

Para publicar una actualización de un enfoque personalizado existente

1. Inicie sesión en AWS Management Console y abra la consola de AWS Well-Architected Tool en https://console.aws.amazon.com/wellarchitected/.
2. En el panel de navegación izquierdo, elija Enfoques personalizados.
3. Seleccione el enfoque personalizado que desee y elija Editar.
4. Si no tiene listo un archivo JSON actualizado, seleccione Descargar archivo para descargar una copia del enfoque personalizado actual. Edite el archivo JSON descargado con el editor de textos que prefiera y realice los cambios que desee.
5. Seleccione Seleccionar archivo para seleccionar y actualizar el archivo JSON, y elija Enviar y previsualizar para obtener una vista previa del enfoque personalizado, o Enviar para enviar el enfoque personalizado sin previsualizar.

   Un enfoque personalizado no puede superar los 500 KB de tamaño.

   Una vez que AWS WA Tool valida el archivo JSON, el enfoque personalizado se muestra en Enfoques personalizados en el estado BORRADOR.
6. Seleccione el enfoque personalizado de nuevo y elija Publicar enfoque.
7. Seleccione Revisar los cambios antes de publicar para comprobar que los cambios realizados en el enfoque personalizado son correctos. Esto incluye la validación de:

   - El nombre del enfoque personalizado
   - Los nombres de los pilares
   - Las preguntas nuevas, actualizadas y eliminadas

   Seleccione Siguiente.
8. Especifique el tipo de cambio de versión.

Versión principal

Indica que se han realizado cambios sustanciales en el enfoque. Úselo para cambios que afecten al significado del enfoque personalizado.

Cualquier carga de trabajo con el enfoque aplicado recibirá una notificación de la disponibilidad de una nueva versión del enfoque personalizado.

Los cambios principales de la versión no se aplican automáticamente a las cargas de trabajo que utilizan el enfoque.

Versión secundaria

Indica que se han realizado cambios secundarios en el enfoque. Úselo para cambios pequeños, como cambios de texto o actualizaciones de los enlaces URL.

Los cambios secundarios de la versión se aplican automáticamente a las cargas de trabajo que utilizan el enfoque personalizado.

Seleccione Siguiente.

9. En el cuadro Nombre de la versión, introduzca un identificador único para el cambio de versión. Este valor puede tener hasta 32 caracteres y solo debe contener caracteres alfanuméricos y puntos (“.”).
10. Seleccione Publicar enfoque personalizado.

    Una vez publicado un enfoque personalizado, pasa al estado PUBLICADA.

El enfoque personalizado actualizado ahora se puede aplicar a las cargas de trabajo o se puede compartir con otras Cuentas de AWS o usuarios.

Si la actualización supone un cambio de versión importante, se notificará a todas las cargas de trabajo que tengan instalada la versión anterior del enfoque de que hay una nueva versión disponible y se les ofrecerá la opción de actualizarla.

Las actualizaciones de versiones menores se aplican de forma automática sin notificación.

Puede crear hasta 100 versiones de un enfoque personalizado.

Cómo compartir un enfoque personalizado en AWS WA Tool

Puede compartir un enfoque personalizado con otras Cuentas de AWS, usuarios, AWS Organizations y unidades organizativas (OU).

Para compartir un enfoque personalizado con otras Cuentas de AWS y usuarios

1. Inicie sesión en AWS Management Console y abra la consola de AWS Well-Architected Tool en https://console.aws.amazon.com/wellarchitected/.
2. En el panel de navegación izquierdo, elija Enfoques personalizados.
3. Seleccione el enfoque personalizado que desea compartir y elija Ver detalles.
4. En la página de Visualización de los detalles de los enfoques para una carga de trabajo en AWS WA Tool, elija Recursos compartidos. A continuación, seleccione Crear y Crear recursos compartidos con usuarios o cuentas para crear una invitación compartida a una carga de trabajo.
5. Introduzca el ID de la Cuenta de AWS de 12 dígitos o el ARN del usuario con el que desea compartir el enfoque personalizado.
6. Elija Crear para enviar una invitación para compartir el enfoque a la Cuenta de AWS o al usuario especificado.

Puede compartir un enfoque personalizado con un máximo de 300 Cuentas de AWS o usuarios.

Si la invitación para compartir el enfoque no se acepta en un plazo de siete días, la invitación caducará automáticamente.

> **Important**
>
> Antes de compartir un enfoque personalizado con una organización o unidad organizativa (OU), debe habilitar el acceso a AWS Organizations.

Para compartir un enfoque personalizado con su organización o unidades organizativas

1. Inicie sesión en AWS Management Console y abra la consola de AWS Well-Architected Tool en https://console.aws.amazon.com/wellarchitected/.
2. En el panel de navegación izquierdo, elija Enfoques personalizados.
3. Seleccione el enfoque personalizado que desee compartir.

4. En la página de Visualización de los detalles de los enfoques para una carga de trabajo en AWS WA Tool, elija Recursos compartidos. A continuación, elija Crear y Crear recursos compartidos para organizaciones.
5. En la página Crear enfoque personalizado compartido, elija si desea conceder permisos a toda la organización o a una o más unidades organizativas.
6. Seleccione Crear para compartir el enfoque personalizado.

Para ver quién tiene acceso compartido a un enfoque personalizado, seleccione Recursos compartidos en la página Visualización de los detalles de los enfoques para una carga de trabajo en AWS WA Tool.

> **Exención de responsabilidad**
>
> Al compartir sus enfoques personalizados con otras Cuentas de AWS, acepta que AWS pondrá sus enfoques personalizados a disposición de esas otras cuentas. Esas otras cuentas pueden seguir accediendo a sus enfoques personalizados compartidos y utilizándolas incluso si elimina el perfil de su propia Cuenta de AWS o cancela su Cuenta de AWS.

Cómo agregar etiquetas a un enfoque personalizado en AWS WA Tool

Añadir etiquetas a un enfoque personalizado

1. Inicie sesión en AWS Management Console y abra la consola de AWS Well-Architected Tool en https://console.aws.amazon.com/wellarchitected/.
2. En el panel de navegación izquierdo, elija Enfoques personalizados.
3. Seleccione el enfoque personalizado que desea actualizar.
4. En la sección Etiquetas, elija Administrar etiquetas.
5. Seleccione Agregar etiqueta nueva e ingrese la Clave y el Valor de la etiqueta que desea añadir.
6. Seleccione Guardar.

Para eliminar una etiqueta, elija Eliminar junto a la etiqueta que desee eliminar.

Eliminación de un enfoque personalizado en AWS WA Tool

Para eliminar un enfoque personalizado

1. Inicie sesión en AWS Management Console y abra la consola de AWS Well-Architected Tool en https://console.aws.amazon.com/wellarchitected/.
2. En el panel de navegación izquierdo, elija Enfoques personalizados.
3. Seleccione el enfoque personalizado que desea eliminar y elija Eliminar.
4. Seleccione Eliminar.

   A las cargas de trabajo existentes con el enfoque aplicado se les notifica que el enfoque personalizado se ha eliminado, pero que pueden seguir utilizándola. El enfoque personalizado ya no se puede aplicar a nuevas cargas de trabajo.

> **Exención de responsabilidad**
>
> Al compartir sus enfoques personalizados con otras Cuentas de AWS, acepta que AWS pondrá sus enfoques personalizados a disposición de esas otras cuentas. Esas otras cuentas pueden seguir accediendo a sus enfoques personalizados compartidos y utilizándolas incluso si elimina el perfil de su propia Cuenta de AWS o cancela su Cuenta de AWS.

Especificación del formato del enfoque en AWS WA Tool

Los enfoques se definen mediante un formato JSON específico. Cuando empiece a crear un enfoque personalizado, tendrá la opción de descargar una plantilla de archivo JSON. Puede utilizar este archivo como base para sus enfoques personalizados, ya que define la estructura básica de los pilares, las preguntas, las mejores prácticas y el plan de mejora.

Sección de enfoques

En esta sección se definen los atributos de la propio enfoque personalizado. Este es su nombre y descripción.

- `schemaVersion`: la versión del esquema de enfoques personalizados que se va a utilizar. Establecido por la plantilla, no lo cambie.

- `name`: nombre del enfoque. El nombre puede tener hasta 128 caracteres.
- `description`: descripción textual del enfoque. Este texto se muestra al seleccionar enfoques para añadirlos durante la creación de la carga de trabajo o al seleccionar un enfoque para aplicarlo posteriormente a una carga de trabajo existente. La descripción puede tener una longitud máxima de 2048 caracteres.

```
   "schemaVersion": "2021-11-01",
   "name": "Company Policy ABC",
   "description": "This lens provides a set of specific questions to assess compliance
with company policy ABC-2021 as revised on 2021/09/01.",
```

Sección de pilares

En esta sección se definen los pilares asociados al enfoque personalizado. Puede asignar sus preguntas a los pilares del marco de AWS Well-Architected, definir sus propios pilares o ambos.

Puede definir hasta 10 pilares en un enfoque personalizado.

- `id`: ID del pilar. El identificador puede tener entre 3 y 128 caracteres y solo caracteres alfanuméricos y guion bajo (“_”). Los ID utilizados en un pilar deben ser únicos.

  Al asignar sus preguntas a los pilares del marco, utilice los siguientes identificadores:

  - `operationalExcellence`
  - `security`
  - `reliability`
  - `performance`
  - `costOptimization`
  - `sustainability`
- `name`: nombre del pilar. El nombre puede tener hasta 128 caracteres.

```
    "pillars": [
       {
           "id": "company_Privacy",
           "name": "Privacy Excellence",
           .
```

```
            .
            .
        },
        {
            "id": "company_Security",
            "name": "Security",
            .
            .
            .
        }
    ]
```

Sección de preguntas

En esta sección se definen las preguntas asociadas a un pilar.

Puede definir hasta 20 preguntas en un pilar en un enfoque personalizado.

- `id`: ID de la pregunta. El identificador puede tener entre 3 y 128 caracteres y solo caracteres alfanuméricos y guion bajo («_»). Los ID utilizados en una pregunta deben ser únicos.
- `title`: título de la pregunta. El título puede tener hasta 128 caracteres.
- `description`: describe la pregunta con más detalle. La descripción puede tener una longitud máxima de 2048 caracteres.
- `helpfulResource displayText`: opcional. Texto que proporciona información útil sobre la pregunta. El texto puede tener hasta 2048 caracteres. Si se especifica, el argumento `helpfulResource url` también se debe especificar.
- `helpfulResource url`: opcional. Un recurso de URL que explica la pregunta con más detalle. La dirección URL debe comenzar por `http://` o `https://`.

> **Note**
>
> Al sincronizar una carga de trabajo de enfoque personalizado con Jira, las preguntas muestran tanto el “id” como el “título” de la pregunta.
> El formato utilizado en los tickets de Jira es `[ QuestionID ] QuestionTitle`.

```
"questions": [
```

```
    {
        "id": "privacy01",
        "title": "How do you ensure HR conversations are private?",
        "description": "Career and benefits discussions should occur on secure channels
 only and be audited regularly for compliance.",
        "helpfulResource": {
            "displayText": "This is helpful text for the first question",
            "url": "https://example.com/poptquest01_help.html"
        },
        .
        .
        .
    },
    {
        "id": "privacy02",
        "title": "Is your team following the company privacy policy?",
        "description": "Our company requires customers to opt-in to data use and does
 not disclose customer data to third parties either individually or in aggregate.",
        "helpfulResource": {
            "displayText": "This is helpful text for the second question",
            "url": "https://example.com/poptquest02_help.html"
        },
        .
        .
        .
    }
]
```

Sección de opciones

En esta sección se definen las opciones asociadas a una pregunta.

Puede definir hasta 15 opciones para una pregunta en un enfoque personalizado.

- `id`: ID de la elección. El identificador puede tener entre 3 y 128 caracteres y solo caracteres alfanuméricos y guion bajo (“_”). Se debe especificar un identificador único para cada opción de la pregunta. Añadir una opción con el sufijo de _no servirá como opción `None of these` para la pregunta.
- `title`: título del caso El título puede tener hasta 128 caracteres.
- `helpfulResource displayText`: opcional. Texto que proporciona información útil sobre una opción. El texto puede tener hasta 2048 caracteres. Debe incluirse si `helpfulResource url` se especifica.

- `helpfulResource url`: opcional. Un recurso de URL que explica la opción con más detalle. La dirección URL debe comenzar por `http://` o `https://`.
- `improvementPlan displayText`: texto que describe cómo se puede mejorar una elección. El texto puede tener hasta 2048 caracteres. Se requiere un `improvementPlan` para cada opción, excepto para una opción `None of these`.
- `improvementPlan url`: opcional. Un recurso de URL que puede ayudar a mejorar. La dirección URL debe comenzar por `http://` o `https://`.
- `additionalResources type`: opcional. El tipo de recursos adicionales. El valor puede ser `HELPFUL_RESOURCE` o `IMPROVEMENT_PLAN`.
- `additionalResources content`: opcional. Especifica los valores `displayText` y `url` del recurso adicional. Se pueden especificar hasta cinco recursos útiles adicionales y hasta cinco elementos adicionales del plan de mejora para elegir.
  - `displayText`: opcional. Texto que describe el recurso útil o el plan de mejora. El texto puede tener hasta 2048 caracteres. Debe incluirse si `url` se especifica.
  - `url`: opcional. Un recurso de URL para el recurso útil o el plan de mejora. La dirección URL debe comenzar por `http://` o `https://`.

> **Note**
>
> Al sincronizar una carga de trabajo de enfoque personalizado con Jira, las opciones muestran el “id” de la pregunta y la elección, así como el “título” de la elección. El formato que se utiliza es `[ QuestionID | ChoiceID ] ChoiceTitle`.

```
   "choices": [
        {
            "id": "choice_1",
            "title": "Option 1",
            "helpfulResource": {
                "displayText": "This is helpful text for the first choice",
                "url": "https://example.com/popt01_help.html"
            },
            "improvementPlan": {
                "displayText": "This is text that will be shown for improvement of
this choice.",
                "url": "https://example.com/popt01_iplan.html"
            }
```

```
        },
        {
            "id": "choice_2",
            "title": "Option 2",
            "helpfulResource": {
                "displayText": "This is helpful text for the second choice",
                "url": "https://example.com/hr_manual_CORP_1.pdf"
            },
            "improvementPlan": {
                "displayText": "This is text that will be shown for improvement of
this choice.",
                "url": "https://example.com/popt02_iplan_01.html"
            },
            "additionalResources":[
               {
                 "type": "HELPFUL_RESOURCE",
                 "content": [
                   {
                     "displayText": "This is the second set of helpful text for this
choice.",
                     "url": "https://example.com/hr_manual_country.html"
                   },
                   {
                     "displayText": "This is the third set of helpful text for this
choice.",
                     "url": "https://example.com/hr_manual_city.html"
                   }
                 ]
               },
               {
                 "type": "IMPROVEMENT_PLAN",
                 "content": [
                   {
                     "displayText": "This is additional text that will be shown for
improvement of this choice.",
                     "url": "https://example.com/popt02_iplan_02.html"
                   },
                   {
                     "displayText": "This is the third piece of improvement plan
text.",
                     "url": "https://example.com/popt02_iplan_03.html"
                   }
                   {
```

```
                    "displayText": "This is the fourth piece of improvement plan
text.",
                    "url": "https://example.com/popt02_iplan_04.html"
                  }
                ]
              }
            ]
        },
        {
             "id": "option_no",
             "title": "None of these",
             "helpfulResource": {
               "displayText": "Choose this if your workload does not follow these best
practices.",
               "url": "https://example.com/popt02_iplan_none.html"
             }

           }
```

Sección de reglas de riesgo

En esta sección se define cómo las opciones seleccionadas determinan el nivel de riesgo.

Puede definir un máximo de tres reglas de riesgo por pregunta, una para cada nivel de riesgo.

- `condition`: una expresión booleana de las opciones que se asigna a un nivel de riesgo para la pregunta o `default`.

  Debe haber una regla de riesgo `default` para cada pregunta.
- `risk`: indica el riesgo asociado a la afección. Los valores válidos son `HIGH_RISK`, `MEDIUM_RISK` y `NO_RISK`.

El orden de sus reglas de riesgo es significativo. La primera `condition` que evalúa `true` establece el riesgo de la pregunta. Un patrón común a la hora de implementar las reglas de riesgo es empezar con las reglas con menos riesgo (y normalmente las más detalladas) y luego ir bajando hasta llegar a las reglas con más riesgo (y menos específicas).

Por ejemplo:

```
"riskRules": [
```

```
        {
          "condition": "choice_1 && choice_2 && choice_3",
          "risk": "NO_RISK"
        },
        {
          "condition": "((choice_1 || choice_2) && choice_3) || (!choice_1 &&
choice_3)",
          "risk": "MEDIUM_RISK"
        },
        {
          "condition": "default",
          "risk": "HIGH_RISK"
        }
]
```

Si la pregunta tiene tres opciones (`choice_1`, `choice_2` y `choice_3`), estas reglas de riesgo dan como resultado el siguiente comportamiento:

- si se seleccionan las tres opciones, no hay riesgo.
- Si se selecciona `choice_1` o `choice_2` y `choice_3` está seleccionado, el riesgo es medio.
- Si `choice_1` no está seleccionado pero `choice_3` está seleccionado, el riesgo también es medio.
- Si no se cumplía ninguna de estas condiciones previas, existe un riesgo alto.

Actualización de enfoques en AWS WA Tool

El enfoque del marco de AWS Well-Architected y otros enfoques proporcionados por AWS se actualizan a medida que se introducen nuevos servicios, se mejoran las prácticas recomendadas existentes para los sistemas basados en la nube y se agregan nuevas prácticas recomendadas. Cuando hay disponible una nueva versión de un enfoque, AWS WA Tool se actualiza para reflejar las últimas prácticas recomendadas. Cualquier carga de trabajo nueva que se defina utiliza la nueva versión del enfoque.

La actualización del enfoque también se produce cuando se publica una nueva versión principal de un enfoque personalizado que se ha aplicado a una carga de trabajo o a una plantilla de revisión.

Una actualización de enfoque podría constar de cualquier combinación de:

- Incorporación de nuevas preguntas o prácticas recomendadas

- Eliminación de preguntas o prácticas antiguas que ya no se recomiendan
- Actualización de preguntas o prácticas recomendadas existentes
- Agregado o eliminación de pilares

Se conservan sus respuestas a las preguntas existentes.

> **Note**
>
> No se puede deshacer una actualización de enfoque. Una vez que se haya actualizado una carga de trabajo a la última versión del enfoque, no podrá volver a la versión anterior del enfoque.

Determinación de qué enfoque actualizar en AWS WA Tool

Para ver qué cargas de trabajo no utilizan la versión más reciente de los enfoques, consulte la página de Notificaciones.

Para cada carga de trabajo se muestra la siguiente información en la página Notificaciones:

Recurso

Nombre de la plantilla de carga de trabajo o revisión.

Tipo de recurso

El tipo de recurso. Puede ser una carga de trabajo o plantilla de revisión.

Recurso asociado

El nombre del enfoque.

Tipo de notificación

El tipo de notificación de actualización.

- No actual: la carga de trabajo está utilizando una versión del enfoque que ya no es actual. Actualice a la versión de la versión de enfoque actual para obtener una mejor orientación.
- Obsoleto: la carga de trabajo está utilizando una versión del enfoque que ya no refleja las prácticas recomendadas. Actualice a la versión actual del enfoque.
- Eliminado: la carga de trabajo utiliza un enfoque que su propietario ha eliminado.

Versión en uso

La versión de el enfoque utilizado actualmente para la carga de trabajo.

Versión disponible actual

La versión del enfoque está disponible para actualizarse, o Ninguno si se ha eliminado el enfoque.

Para actualizar el enfoque asociado a una carga de trabajo, seleccione la carga de trabajo y elija Actualizar versión del enfoque.

Actualización de un enfoque en AWS WA Tool

Los enfoques se pueden actualizar para cargas de trabajo y plantillas de revisión.

> **Note**
>
> No se puede deshacer una actualización de enfoque. Una vez que se haya actualizado una carga de trabajo o plantilla de revisión a la última versión del enfoque, no podrá volver a la versión anterior del enfoque.

Actualización de un enfoque para una carga de trabajo

1. En la página de Notificaciones, seleccione la carga de trabajo que desee actualizar y elija Actualizar la versión del enfoque. Se muestra información sobre lo que ha cambiado en cada pilar.

   > **Note**
   >
   > También puede seleccionar Ver las actualizaciones disponibles en la pestaña Información general de la carga de trabajo.

2. Antes de actualizar el enfoque para una carga de trabajo, se crea un hito para guardar el estado de su carga de trabajo existente para futuras referencias. Introduzca un nombre único para el hito en el campo Nombre del hito.
3. Seleccione la casilla de Confirmación situada junto a Comprendo y acepto estos cambios y pulse Guardar.

Una vez que se haya actualizado el enfoque, podrá ver la versión anterior del enfoque en la pestaña Hitos.

Actualización de un enfoque para una plantilla de revisión

1. Para actualizar el enfoque de una plantilla de revisión, elija
2. En la página de Notificaciones, seleccione la plantilla de revisión que desee actualizar y elija Actualizar la versión del enfoque. Se muestra información sobre lo que ha cambiado en cada pilar.

   > **Note**
   >
   > También puede seleccionar Ver las actualizaciones disponibles en la pestaña Descripción general de la plantilla de revisión.

3. Seleccione la casilla de Confirmación situada junto a Comprendo y acepto estos cambios y elija Actualizar y editar las respuestas de la plantilla para ajustar las respuestas a las preguntas de mejores prácticas para su plantilla de revisión, o Actualizar para actualizar el enfoque sin ajustar las respuestas de la plantilla.

Catálogo de enfoques para AWS WA Tool

El Catálogo de enfoques es una recopilación de enfoques de AWS oficiales, creados para AWS Well-Architected Tool que ofrecen tecnología actualizada y las prácticas recomendadas centradas en el sector. Estas lentes están disponibles para todos los usuarios y no requieren ninguna instalación adicional para su uso.

La siguiente tabla describe todas las lentes oficiales de AWS disponibles actualmente en el catálogo de enfoques.

Nombre de la lente	Descripción
AWS Well-Architected Framework	Se ha aplicado de forma predeterminada a todas las cargas de trabajo. Recopilación de prácticas recomendadas de arquitectura para diseñar y utilizar sistemas fiables, seguros, eficientes y rentables en la nube.

Nombre de la lente	Descripción
Movilidad conectada	Prácticas recomendadas para integrar la tecnología en los sistemas de transporte y mejorar la experiencia general de movilidad.
Compilación de contenedores	Proporciona las prácticas recomendadas sobre el proceso de diseño y compilación de contenedores.
Análisis de datos	Contiene información que AWS ha recopilado a partir de casos prácticos reales y le ayuda a obtener información sobre los elementos clave de diseño de las cargas de trabajo de análisis de Well-Architected, junto con recomenda ciones de mejora.
DevOps	Describe un enfoque estructurado que las organizaciones de todos los tamaños pueden seguir para cultivar una cultura de alta velocidad y centrada en la seguridad, capaz de ofrecer un valor empresarial sustancial mediante tecnologías modernas y las mejores prácticas de DevOps.
Industria de servicios financieros	Las prácticas recomendadas para diseñar sus cargas de trabajo del sector de servicios financieros en AWS.
IA generativa	Prácticas recomendadas para diseñar las cargas de trabajo de IA generativa en AWS.
Administración pública	Prácticas recomendadas para el diseño y la prestación de servicios gubernamentales en AWS.

Nombre de la lente	Descripción
Enfoque del sector sanitario	Prácticas recomendadas y orientación sobre cómo diseñar, implementar y administrar las cargas de trabajo de atención sanitaria en la Nube de AWS.
IoT	Prácticas recomendadas para administrar las cargas de trabajo del Internet de las cosas (IoT) en AWS.
Fusiones y adquisiciones	Prácticas recomendadas para la integración de la carga de trabajo y la migración a la nube durante las fusiones y adquisiciones.
Machine Learning	Prácticas recomendadas para administrar los recursos y cargas de trabajo de machine learning en AWS.
Migración	Prácticas recomendadas sobre cómo migrar a Nube de AWS.
SaaS	Se centra en diseñar, implementar y diseñar la arquitectura de las cargas de trabajo de software como servicio (SaaS) en la Nube de AWS.
SAP	Principios de diseño y prácticas recomendadas para cargas de trabajo de SAP en la Nube de AWS.
Aplicaciones sin servidor	Prácticas recomendadas para crear cargas de trabajo sin servidor en AWS. Cubre casos como microservicios RESTful, backends de aplicaciones móviles, procesamiento de transmisiones y aplicaciones web.

Plantillas de revisión en AWS WA Tool

Puede crear plantillas de revisión en AWS WA Tool que contengan respuestas predefinidas para las preguntas de mejores prácticas para el marco de Well-Architected y enfoques personalizados. Las plantillas de revisión de Well-Architected reducen la necesidad de completar manualmente las mismas respuestas para las mejores prácticas que son comunes en varias cargas de trabajo al realizar una revisión de Well-Architected, y ayudan a impulsar la coherencia y la estandarización de las mejores prácticas en todos los equipos y cargas de trabajo.

Puede crear una plantilla de revisión para responder a las preguntas más habituales sobre las mejores prácticas o crear notas, que se pueden compartir con otro usuario o cuenta de IAM, o con una organización o unidad organizativa de la misma Región de AWS. Puede definir una carga de trabajo a partir de una plantilla de revisión, lo que le ayuda a ampliar las prácticas recomendadas más comunes y a reducir la redundancia en sus cargas de trabajo.

Creación de una plantilla de revisión en AWS WA Tool

Para crear una plantilla de revisión

1. En el panel de navegación izquierdo, seleccione Plantillas de revisión.
2. Seleccione Crear plantilla.
3. En la página Especificar los detalles de la plantilla, proporcione un Nombre y una Descripción para la plantilla de revisión.
4. (Opcional) En las secciones Notas de la plantilla y Etiquetas, añada las notas o etiquetas de la plantilla que desee asociar a la plantilla de revisión. Las notas añadidas se aplican a todas las cargas de trabajo que utilizan la plantilla de revisión, mientras que las etiquetas son específicas de la plantilla de revisión.

   Para obtener más información sobre las etiquetas, consulte Etiquetar los recursos de AWS WA Tool.
5. Seleccione Siguiente.
6. En la página Aplicar enfoques, seleccione los enfoques que desee aplicar a la plantilla de revisión. El número máximo de enfoques que se puede aplicar es 20.

   Las lentes se pueden seleccionar de las lentes personalizadas, del catálogo de enfoques o de ambos.

> **Note**
>
> Los enfoques que se comparten con usted no se pueden aplicar a la plantilla de revisión.

7. Seleccione Crear plantilla.

Para empezar a responder a las preguntas de la plantilla de revisión que acaba de crear

1. En la pestaña Descripción general de la plantilla, en la alerta de información Empezar a responder a las preguntas, seleccione el enfoque en el menú desplegable Responder a las preguntas.

> **Note**
>
> También puede ir a la sección Enfoques, seleccionar el enfoque y elegir Responder las preguntas.

2. Para cada enfoque que haya aplicado a su plantilla de revisión, responda a las preguntas correspondientes y seleccione Guardar y salir cuando haya terminado.

Una vez creada la plantilla de revisión, puede definir una nueva carga de trabajo a partir de ella.

La pestaña Descripción general de la plantilla de revisión debe reflejar el número total de Preguntas respondidas en la sección de Detalles de la plantilla y las Preguntas respondidas para cada enfoque en la sección de Enfoques.

Edición de una plantilla de revisión en AWS WA Tool

Para editar una plantilla de revisión

1. En el panel de navegación izquierdo, seleccione Plantillas de revisión.
2. Seleccione el nombre de la plantilla de revisión que desea editar.
3. Para actualizar el Nombre, la Descripción o las Notas de la plantilla para la plantilla de revisión, seleccione Editar en la sección de Detalles de la plantilla de la pestaña Descripción general.
   a. Realice los cambios que desee en el Nombre, la Descripción o las Notas de la plantilla.
   b. Seleccione Guardar plantilla para actualizar la plantilla de revisión con los cambios.

4. Para actualizar los enfoques que se aplican a la plantilla de revisión, en la sección Enfoques de la pestaña Descripción general, seleccione Editar enfoques aplicados.
   a. Seleccione o desactive las casillas de verificación de los enfoques que desee añadir o eliminar.

      Las lentes se pueden seleccionar o no seleccionar de las lentes personalizadas, del catálogo de enfoques o de ambos.
   b. Elija Guardar para guardar los cambios.
5. Para actualizar las respuestas a las preguntas de prácticas recomendadas sobre el enfoque, en la sección Enfoques de la pestaña Información general, seleccione el nombre del enfoque.
   a. En la sección Información general del enfoque, seleccione Responder preguntas.

      > **Note**
      >
      > Si lo desea, puede seleccionar el nombre del enfoque en el menú desplegable Revisar plantillas del panel de navegación izquierdo para ir a la sección de Información general del enfoque.
   b. Seleccione o desactive las casillas de verificación situadas junto a las respuestas de práctica recomendada que desee cambiar.
   c. Para guardar y aplicar los cambios, elija Guardar.

Compartir una plantilla de revisión en AWS WA Tool

Las plantillas de revisión se pueden compartir con usuarios o cuentas, o se pueden compartir con toda una organización o unidad organizativa.

Para compartir una plantilla de revisión

1. En el panel de navegación izquierdo, seleccione Plantillas de revisión.
2. Seleccione el nombre de la plantilla de revisión que desea compartir.
3. Seleccione la pestaña Recursos compartidos.
4. Para compartir con un usuario o una cuenta, seleccione Crear y luego Compartir con usuarios de IAM o cuentas. En el cuadro Enviar invitaciones, especifique los ID de usuario o cuenta y seleccione Crear.
5. Para compartir en una organización o unidad organizativa, seleccione Crear y seleccione Compartir con las organizaciones. Para compartir con toda una organización, seleccione Otorgar

permisos a toda la organización. Para compartir con una unidad organizativa, seleccione Otorgar permisos a unidades organizativas individuales, especifique la unidad organizativa en el cuadro y seleccione Crear.

> **Important**
>
> Antes de compartir un perfil con una organización o unidad organizativa (OU), debe habilitar el acceso a AWS Organizations.

Definición de una carga de trabajo a partir de una plantilla en AWS WA Tool

Puede definir una carga de trabajo a partir de una plantilla de revisión que haya creado o de una plantilla de revisión que se haya compartido con usted. No puede definir una nueva carga de trabajo a partir de una plantilla de revisión que se haya eliminado y, si la plantilla de revisión contiene una versión anticuada de un enfoque, debe actualizar la plantilla de revisión antes de poder definir una nueva carga de trabajo a partir de ella. Para obtener información sobre cómo actualizar una plantilla de revisión, consulte the section called “Actualización del enfoque”.

> **Note**
>
> Para definir una carga de trabajo a partir de una plantilla de revisión, debe tener habilitados los permisos de IAM para crear una carga de trabajo: `wellarchitected:CreateWorkload`, y los siguientes permisos de plantilla de revisión: `wellarchitected:GetReviewTemplate`, `wellarchitected:GetReviewTemplateAnswer`, `wellarchitected:ListReviewTemplateAnswers` y `wellarchitected:GetReviewTemplateLensReview`. Para obtener más información sobre los permisos de IAM, consulte la Guía del usuario de AWS Identity and Access Management.

Para definir una carga de trabajo a partir de una plantilla de revisión

1. En el panel de navegación izquierdo, seleccione Plantillas de revisión.

2. Seleccione el nombre de la plantilla de revisión a partir de la cual desea definir una carga de trabajo.
3. Elija Definir carga de trabajo a partir de una plantilla.

> **Note**
>
> También puede elegir Definir a partir de una plantilla de revisión en el menú desplegable Definir carga de trabajo de la página Cargas de trabajo.

4. En el paso Seleccionar la plantilla de revisión, seleccione la tarjeta de plantilla de revisión y seleccione Siguiente.
5. En el paso Especificar las propiedades, rellene los campos obligatorios para las propiedades de la carga de trabajo y seleccione Siguiente. Para obtener más información, consulte the section called “Definir una carga de trabajo”.
6. (Opcional) En el paso Aplicar perfil, asocie un perfil a la carga de trabajo seleccionando un perfil existente, buscando el nombre del perfil o seleccionando Crear perfil para crear un perfil. Seleccione Siguiente.

   Los perfiles de Well-Architected y las plantillas de revisión se pueden utilizar en conjunto. Las preguntas que vienen rellenadas previamente en la plantilla de revisión permanecen respondidas durante la carga de trabajo y se priorizan en función de su perfil.
7. (Opcional) En el paso Aplicar lentes, tiene la opción de elegir aplicar lentes adicionales de lentes personalizadas o del catálogo de enfoques que aún no se hayan aplicado a la plantilla de revisión.
8. Seleccione Definir carga de trabajo.

Eliminación de una plantilla de revisión en AWS WA Tool

Para eliminar una plantilla de revisión

1. En el panel de navegación izquierdo, seleccione Plantillas de revisión.
2. En la sección Plantillas de revisión, elija la plantilla de revisión que desea eliminar y, en el menú desplegable Acciones, seleccione Eliminar.

> **Note**
>
> También puede seleccionar el nombre de la plantilla y elegir Eliminar en la pestaña Descripción general de la plantilla de revisión.

3. En el cuadro de diálogo Eliminar plantilla de revisión, introduzca el nombre de la plantilla de revisión en el campo para confirmar la eliminación.
4. Seleccione Eliminar.

No puede crear una nueva carga de trabajo a partir de una plantilla de revisión que se haya eliminado. Si ha compartido una plantilla de revisión que ha eliminado con otros usuarios, cuentas u organizaciones de IAM, estos no podrán crear cargas de trabajo a partir de ella.

Uso de perfiles en AWS WA Tool

Puede crear perfiles para proporcionar el contexto de su empresa e identificar los objetivos que le gustaría alcanzar al realizar una revisión de Well-Architected. AWS Well-Architected Tool utiliza la información recopilada de su perfil para ayudarle a centrarse en una lista priorizada de preguntas relevantes para su empresa durante la revisión de la carga de trabajo. Adjuntar un perfil a su carga de trabajo también le ayuda a ver qué riesgos se priorizan para abordarlos en su plan de mejora.

Puede crear un perfil desde la página de Perfiles y asociarlo a una nueva carga de trabajo, o puede añadir un perfil a una carga de trabajo existente.

Crear un perfil

Para crear un perfil

1. En el panel de navegación izquierdo, seleccione Perfiles.
2. Seleccione Crear perfil.
3. En la sección Propiedades del perfil, proporcione un Nombre y una Descripción para su perfil.
4. Para afinar la información priorizada para su empresa en el plan de revisión y mejora de la carga de trabajo, seleccione las respuestas que sean más relevantes para su empresa en la sección de Preguntas del perfil.
5. (Opcional) En la sección Etiquetas, añada las etiquetas que desee asociar al perfil.

   Para obtener más información sobre las etiquetas, consulte Etiquetar los recursos de AWS WA Tool.
6. Seleccione Guardar. Aparece un mensaje de confirmación cuando el perfil se ha creado correctamente.

Cuando se crea un perfil, se muestra la descripción general del perfil. La descripción general muestra los datos asociados al perfil, incluidos el nombre, la descripción, el ARN, las fechas de creación y actualización y las respuestas a las preguntas del perfil. Desde la página de resumen del perfil, puede editar, eliminar o compartir su perfil.

Edición de un perfil en AWS WA Tool

Para editar un perfil

1. Seleccione Perfiles en el panel de navegación izquierdo o seleccione Ver perfil en la sección Perfiles de la carga de trabajo.
2. Seleccione el nombre del perfil de seguridad que desea actualizar.
3. Seleccione Editar en la página de Descripción general del perfil.
4. Realice las actualizaciones necesarias en las preguntas del perfil.
5. Seleccione Guardar.

Cómo compartir un perfil en AWS WA Tool

Los perfiles se pueden compartir con usuarios o cuentas, o se pueden compartir con toda una organización o unidad organizativa.

Para compartir un perfil

1. En el panel de navegación izquierdo, seleccione Perfiles.
2. Seleccione el nombre del perfil de seguridad que desea compartir.
3. Seleccione la pestaña Recursos compartidos.
4. Para compartir con un usuario o una cuenta, seleccione Crear y luego Crear recursos compartidos para usuarios o cuentas de IAM. En el cuadro Enviar invitaciones, especifique los ID de usuario o cuenta y seleccione Crear.
5. Para compartir en una organización o unidad organizativa, seleccione Crear y seleccione Crear recursos compartidos para las organizaciones. Para compartir con toda una organización, seleccione Otorgar permisos a toda la organización. Para compartir con una unidad organizativa, seleccione Otorgar permisos a unidades organizativas individuales, especifique la unidad organizativa en el cuadro y seleccione Crear.

> **Important**
>
> Antes de compartir un perfil con una organización o unidad organizativa (OU), debe habilitar el acceso a AWS Organizations.

Cómo añadir un perfil a una carga de trabajo en AWS WA Tool

Puede añadir un perfil a una carga de trabajo existente o, al definir una carga de trabajo, para acelerar el proceso de revisión de la carga de trabajo. AWS WA Tool utiliza la información recopilada de su perfil para priorizar las preguntas de la revisión de la carga de trabajo que son relevantes para su empresa.

Para obtener más información sobre cómo añadir un perfil al definir una carga de trabajo, consulte the section called “Definir una carga de trabajo”.

Para añadir un perfil a una carga de trabajo existente

1. Seleccione Cargas de trabajo en el panel de navegación izquierdo y seleccione el nombre de la carga de trabajo que desee asociar a un perfil.

   > **Note**
   >
   > Solo se puede asociar un perfil a una carga de trabajo.

2. En la sección Perfil, seleccione Añadir perfil.
3. Seleccione el perfil que desee aplicar a la carga de trabajo de la lista de perfiles disponibles o elija Crear perfil. Para obtener más información, consulte the section called “Crear un perfil”.
4. Seleccione Guardar.

El Resumen de la carga de trabajo muestra un recuento de las preguntas priorizadas respondidas y los riesgos priorizados en función de la información del perfil asociado. Seleccione Continuar revisando para abordar las preguntas prioritarias en la revisión de la carga de trabajo. Para obtener más información, consulte the section called “Documentación de una carga de trabajo”.

La sección Perfil muestra el nombre, la descripción, el ARN, la versión y la fecha de la última actualización del perfil asociado a la carga de trabajo.

Eliminación de un perfil de una carga de trabajo en AWS WA Tool

Al eliminar un perfil de la carga de trabajo, se revierte la carga de trabajo a la versión anterior a la que estaba asociado el perfil, y las preguntas y los riesgos relacionados con la revisión de la carga de trabajo ya no tienen prioridad.

Para eliminar un perfil de una carga de trabajo

1. En la sección Perfiles de la carga de trabajo, seleccione Eliminar.
2. Para confirmar la eliminación, escriba el nombre del perfil en el campo de entrada de texto.
3. Seleccione Eliminar.

Una notificación en la que se indica que el perfil se ha eliminado correctamente de la carga de trabajo. Al eliminar un perfil, se revierte la carga de trabajo a la versión anterior a la que estaba asociado el perfil, y las preguntas y los riesgos relacionados con la revisión de la carga de trabajo ya no tienen prioridad.

Eliminación de un perfil de AWS WA Tool

Si ha creado un perfil, puede eliminarlo de la lista de perfiles disponibles en AWS WA Tool.

Al eliminar un perfil de la página de Perfiles, no se elimina el perfil de ninguna carga de trabajo asociada. Puede seguir utilizando los perfiles que estaban compartidos y asociados a una carga de trabajo antes de eliminarlos. Sin embargo, no se pueden asociar cargas de trabajo nuevas a un perfil eliminado. the section called “Notificaciones de perfil” se envían a los propietarios de las cargas de trabajo mediante perfiles eliminados.

> **Exención de responsabilidad**
>
> Al compartir sus perfiles con otras Cuentas de AWS, acepta que AWS pondrá sus perfiles a disposición de esas otras cuentas. Esas otras cuentas pueden seguir accediendo a sus perfiles compartidos y utilizándolos incluso si elimina el perfil de su propia Cuenta de AWS o cancela su Cuenta de AWS.

Para eliminar un perfil de su lista de perfiles

1. En el panel de navegación izquierdo, seleccione Perfiles.
2. Seleccione el nombre del perfil de seguridad que desea eliminar.
3. Seleccione Eliminar.
4. Para confirmar la eliminación, escriba el nombre del perfil en el campo de entrada de texto.
5. Seleccione Eliminar.

Si desea mantener un perfil en su lista de Perfiles, pero eliminarlo de una carga de trabajo, consulte the section called “Eliminación de un perfil de una carga de trabajo”.

Conector de AWS Well-Architected Tool para Jira

Puede usar el conector de AWS Well-Architected Tool para Jira para vincular su cuenta de Jira con AWS Well-Architected Tool y sincronizar los elementos de mejora de sus cargas de trabajo con los proyectos de Jira, a fin de ayudarle a crear un mecanismo de ciclo cerrado a la hora de implementar las mejoras.

El conector proporciona sincronización automática y manual. Para obtener más información, consulte Configuring the connector.

El conector se puede configurar a nivel de cuenta y a nivel de carga de trabajo, con la opción de anular la configuración a nivel de cuenta por carga de trabajo. A nivel de carga de trabajo, también puede optar por excluir por completo una carga de trabajo de la sincronización.

Puede elegir que los elementos de mejora se sincronicen con el proyecto predeterminado de WA Jira o especificar una clave de proyecto existente con la que sincronizarlos. En el nivel de carga de trabajo, puede sincronizar cada carga de trabajo con un proyecto de Jira único si es necesario.

> **Note**
>
> El conector solo admite proyectos de Scrum y Kanban en Jira.

Cuando los elementos de mejora se sincronizan con Jira, se organizan de la siguiente manera:

- Proyecto: WA (o proyecto existente que especifique)
- Epic: carga de trabajo
- Task: pregunta
- Subtarea: prácticas recomendadas
- Etiqueta: pilar

Tras configurar la sincronización de la cuenta de Jira en la página Configuración, podrá configurar el conector de Jira y sincronizar elementos de mejora con su cuenta de Jira.

Configuración del conector

Para instalar el conector

> **Note**
>
> Todos los pasos siguientes se realizan en su cuenta de Jira, no en su Cuenta de AWS.

1. Inicie sesión en su cuenta de Jira.
2. En la barra de navegación superior, seleccione Aplicaciones y, a continuación, seleccione Explorar más aplicaciones.
3. En la página Descubra aplicaciones e integraciones para Jira, escriba AWS Well-Architected. A continuación, elija el conector de AWS Well-Architected Tool para Jira.
4. En la página de la aplicación, seleccione Obtener aplicación.
5. En el panel Añadir a Jira, seleccione Obtener ahora.
6. Una vez instalada la aplicación, para completar la configuración, seleccione Configurar.
7. En la página Configuración de AWS Well-Architected Tool, elija Conectar una nueva Cuenta de AWS.
8. Especifique su AccessKeyId y la clave secreta. Opcional: introduzca su token de sesión. A continuación, elija Conectar.

   > **Note**
   >
   > Asegúrese de que su cuenta tenga el permiso `wellarchitected:ConfigureIntegration`. Este permiso es necesario para añadir Cuentas de AWS a Jira.
   > Se pueden conectar varias Cuentas de AWS a AWS WA Tool.

   > **Note**
   >
   > Como práctica recomendada de seguridad, se aconseja encarecidamente utilizar credenciales de IAM de corta duración. Para obtener más información sobre cómo crear un AccessKeyId y una clave secreta para su Cuenta de AWS, consulte Administrar

las claves de acceso (consola) y, para obtener información detallada sobre el uso de credenciales a corto plazo, consulte Requesting temporary credentials.

9. Para las Regiones, seleccione las Regiones de AWS que desee conectar. A continuación, elija Conectar.

Configuración del proyecto Jira

Cuando utilice proyectos personalizados, asegúrese de tener los siguientes tipos de incidencia en la configuración de su proyecto:

- Scrum: Epic, Story, Subtarea
- Kanban: Epic, Story, Subtarea

Para obtener más información sobre la gestión de los tipos de incidencias, consulte Atlassian Support | Add, edit, and delete an issue type.

Para verificar el estado del conector en AWS Well-Architected Tool

1. Inicie sesión en su Cuenta de AWS y navegue hasta AWS Well-Architected Tool.
2. Elija Configuración en el panel de navegación izquierdo.
3. En la sección Sincronización de cuentas de Jira, en Estado de conexión de la aplicación Jira, busque el estado Configurado.

El conector ya está instalado y listo para configurarlo. Para configurar los ajustes de sincronización de Jira a nivel de cuenta y carga de trabajo, consulte Configuring the connector.

Configuración del conector de

Con el conector de AWS Well-Architected Tool para Jira, puede configurar la sincronización de Jira a nivel de cuenta, nivel de carga de trabajo o ambos. Puede configurar los ajustes de Jira a nivel de carga de trabajo independientemente de los ajustes a nivel de cuenta, o bien anular los ajustes a nivel de cuenta en una carga de trabajo específica para especificar el comportamiento de sincronización de la carga de trabajo. También puede configurar los ajustes de Jira al definir una carga de trabajo.

El conector proporciona dos métodos de sincronización: sincronización automática y manual. En ambos métodos de sincronización, los cambios que se realizan en AWS WA Tool se reflejan en su proyecto de Jira, y los cambios que se realizan en Jira se vuelven a sincronizar con AWS WA Tool.

> **Important**
>
> Al usar la sincronización automática, acepta que AWS WA Tool modifique su carga de trabajo en respuesta a los cambios en Jira.
> Si tiene información confidencial que no desea sincronizar con Jira, no introduzca esa información en el campo Notas de sus cargas de trabajo.

- Sincronización automática: el conector actualiza automáticamente su proyecto de Jira y su carga de trabajo cada vez que se actualiza una pregunta, lo que incluye seleccionar o deseleccionar una práctica recomendada y completar una pregunta.
- Sincronización manual: debe seleccionar Sincronizar con Jira en el panel de carga de trabajo si quiere sincronizar los elementos de mejora entre Jira y la AWS WA Tool. También puede elegir qué pilares y preguntas específicos quiere sincronizar. Para obtener más información, consulte Sincronización de una carga de trabajo.

Para configurar el conector a nivel de cuenta

1. Elija Configuración en el panel de navegación izquierdo.
2. En el panel de Sincronización de cuentas de Jira, seleccione Editar.
3. En Tipo de sincronización, seleccione una de las opciones siguientes:
    a. Para sincronizar automáticamente las cargas de trabajo cuando se realizan cambios, seleccione Automática.
    b. Para elegir manualmente cuándo sincronizar las cargas de trabajo, seleccione Manual.
4. De forma predeterminada, el conector crea un proyecto de WA Jira. Para especificar su propia clave de proyecto de Jira, haga lo siguiente:
    a. Seleccione Anular la clave de proyecto de Jira predeterminada.
    b. Introduzca su Clave de proyecto de Jira.

> **Note**
>
> La Clave de proyecto de Jira especificada se usa para todas las cargas de trabajo, a menos que cambie el proyecto a nivel de carga de trabajo.

5. Elija Guardar configuración.

Para configurar el conector a nivel de carga de trabajo

1. Seleccione Cargas de trabajo en el panel de navegación izquierdo y seleccione el nombre de la carga de trabajo que desee configurar.
2. Seleccione Propiedades.
3. En el panel de Jira, seleccione Editar.
4. Para configurar los ajustes de Jira de la carga de trabajo, seleccione Anular la configuración a nivel de cuenta.

> **Note**
>
> Anular la configuración a nivel de cuenta debe estar seleccionado para aplicar la configuración específica de la carga de trabajo.

5. Para Sincronizar la anulación, seleccione una de las siguientes opciones:
   a. Para excluir la carga de trabajo de la sincronización de Jira, seleccione No sincronizar la carga de trabajo.
   b. Para elegir manualmente cuándo sincronizar la carga de trabajo, seleccione Sincronizar la carga de trabajo: manual.
   c. Para sincronizar automáticamente los cambios en la carga de trabajo, seleccione Sincronizar carga de trabajo: automática.
6. (Opcional) Para la Clave del proyecto de Jira, introduzca la clave del proyecto con la que desee sincronizar la carga de trabajo. Esta clave de proyecto puede ser diferente de la clave de proyecto a nivel de cuenta.

   Si no especifica una clave de proyecto, el conector crea un proyecto WA Jira.
7. Seleccione Guardar.

Para obtener información detallada sobre cómo realizar una sincronización manual, consulte Sincronizar una carga de trabajo.

Sincronización de una carga de trabajo

Para la sincronización automática, el conector sincroniza automáticamente los elementos de mejora cuando actualizas una carga de trabajo (por ejemplo, cuando responde una pregunta o selecciona una nueva práctica recomendada).

Tanto en la sincronización manual como en la automática, cualquier cambio realizado en Jira (como completar una pregunta o una práctica recomendada) se sincroniza de nuevo con AWS Well-Architected Tool.

Para sincronizar manualmente una carga de trabajo

1. Cuando esté todo listo para sincronizar la carga de trabajo con Jira, seleccione Cargas de trabajo en el panel de navegación izquierdo. Después, seleccione la carga de trabajo que quiera sincronizar.
2. En la descripción general de la carga de trabajo, seleccione Sincronizar con Jira.
3. Seleccione los enfoques que quiera sincronizar.
4. En Preguntas para sincronizar con Jira, seleccione las preguntas o los pilares completos que quiera sincronizar con el proyecto de Jira.
    - Para cualquier pregunta que quiera quitar, seleccione el icono X situado junto al título de la pregunta.
5. Seleccione Sincronizar.

Desinstalación del conector

Para desinstalar completamente el conector de AWS Well-Architected Tool para Jira, realice las siguientes tareas:

- Desactive la sincronización de Jira en cualquier carga de trabajo que anule la configuración de sincronización a nivel de cuenta.
- Desactive la sincronización de Jira a nivel de cuenta.
- Desvincule su Cuenta de AWS en Jira.
- Desinstale el conector de su cuenta de Jira.

Para desactivar el conector a nivel de cuenta

> **Note**
>
> Se realizan los siguientes pasos en su Cuenta de AWS.

1. Elija Configuración en el panel de navegación izquierdo.
2. En la sección Sincronización de cuentas de Jira, seleccione Editar.
3. Desactive la opción Activar la sincronización de cuentas de Jira.
4. Elija Guardar configuración.

Para desvincular una Cuenta de AWS

> **Note**
>
> Todos los pasos siguientes se realizan en su cuenta de Jira, no en su Cuenta de AWS.

1. Inicie sesión en su cuenta de Jira.
2. En la barra de navegación superior, seleccione Aplicaciones y, a continuación, seleccione Administrar sus aplicaciones.
3. Seleccione la flecha desplegable situada junto a Conector de AWS Well-Architected Tool para Jira y, a continuación, seleccione Configurar.
4. En el panel de configuración de AWS Well-Architected Tool, para desvincular una Cuenta de AWS, seleccione X en Acciones.

Para desinstalar el conector

> **Note**
>
> Todos los pasos siguientes se realizan en su cuenta de Jira, no en su Cuenta de AWS. Recomendamos comprobar que todas las Cuentas de AWS conectadas estén desvinculadas en la configuración del conector antes de desinstalarlo.

1. Inicie sesión en su cuenta de Jira.
2. En la barra de navegación superior, seleccione Aplicaciones y, a continuación, seleccione Administrar sus aplicaciones.
3. Seleccione la flecha desplegable situada junto a Conector de AWS Well-Architected Tool para Jira.
4. Seleccione Desinstalar y, a continuación, seleccione Desinstalar aplicación.

Hitos

Los hitos registran el estado de una carga de trabajo en un momento determinado.

Guarde los hitos después de completar inicialmente todas las preguntas asociadas a una carga de trabajo. A medida que cambie su carga de trabajo en función de los elementos de su plan de mejora, puede guardar hitos adicionales para medir el progreso.

Siempre que realice mejoras en una carga de trabajo, es recomendable guardar un hito.

Guardar un hito

Un hito registra el estado actual de una carga de trabajo. El propietario de una carga de trabajo puede guardar un hito en cualquier momento.

Guardar un hito

1. En la página de detalles de la carga de trabajo, seleccione Guardar hito.
2. En el cuadro Nombre de hito, escriba un nombre para el hito.

> **Note**
>
> El nombre debe tener entre 3 y 100 caracteres. Al menos tres caracteres no deben ser espacios. Los nombres de hitos asociados a una carga de trabajo deben ser únicos. Los espacios y las mayúsculas no se tienen en cuenta al comprobar la exclusividad.

3. Elija Guardar para guardar el hito.

Después de guardar un hito, no podrá cambiar los datos de la carga de trabajo registrados. Al eliminar una carga de trabajo, los hitos asociados también se eliminan.

Visualización de hitos

Puede ver los hitos de una carga de trabajo de las siguientes formas:

- En la página de detalles de la carga de trabajo, elija Milestones (Hitos) y elija el hito que desea ver.
- En la página Panel, elija la carga de trabajo y, en la sección Hitos, elija el hito que desea ver.

Generación de un informe de hitos

Puede generar un informe de hitos. El informe contiene sus respuestas a las preguntas de la carga de trabajo, las notas y los riesgos altos y medios que existían cuando se guardó el hito.

Un informe le permite compartir información detallada sobre el hito con otros usuarios que no tienen acceso a AWS Well-Architected Tool.

Para generar un informe de hitos

1. Seleccione el hito de una de las siguientes formas.
   - En la página de detalles de la carga de trabajo, elija Hitos y elija el hito.
   - En la página Panel, elija la carga de trabajo con el hito que desea incluir en el informe. En la sección Hitos, elija el hito.
2. Elija Generar informe para generar un informe.

   Se genera el archivo PDF y puede descargarlo o verlo.

Uso compartido de invitaciones

Una invitación para compartir es una solicitud para compartir una carga de trabajo, un enfoque personalizado o una plantilla de revisión propiedad de otra cuenta de AWS. Se puede compartir una carga de trabajo con todos los usuarios en una cuenta de Cuenta de AWS, usuarios individuales o ambos.

- Si acepta una invitación a la carga de trabajo, la carga de trabajo se agrega a las páginas Cargas de trabajo y Panel.
- Si acepta una invitación para un enfoque personalizado, el enfoque se añadirá a su página de Enfoques personalizados.
- Si acepta una invitación de perfil, el perfil se añadirá a su página de Perfiles.
- Si acepta una invitación para revisar una plantilla, la plantilla se añadirá a su página de Revisión de plantillas.

Si rechaza la invitación, se eliminará de la lista.

> **Note**
>
> Las cargas de trabajo, los enfoques personalizados, los perfiles y las plantillas de revisión solo se pueden compartir dentro de la misma Región de AWS.

El propietario de la carga de trabajo o el enfoque personalizado controla quién tiene acceso compartido.

La página Compartir invitaciones, disponible en el panel de navegación izquierdo, contiene información sobre sus invitaciones a la carga de trabajo y los enfoques personalizados pendientes.

Para cada invitación a la carga de trabajo se muestra la siguiente información:

Nombre

El nombre de la carga de trabajo, el enfoque personalizado o la plantilla de revisión que se va a compartir.

Tipo de recurso

El tipo de invitación, ya sea carga de trabajo, enfoque personalizado, perfiles o plantilla de revisión.

Propietario

El ID de la Cuenta de AWS que es la propietaria de la carga de trabajo.

Permiso

El permiso que concede a la carga de trabajo.

- Solo lectura

  Proporciona acceso de solo lectura a la carga de trabajo, al enfoque personalizado, a los perfiles o a la plantilla de revisión.

- Colaborador

  Proporciona acceso de actualización a las respuestas y las notas y acceso de solo lectura al resto de la carga de trabajo. Este permiso solo está disponible para las cargas de trabajo.

Detalles del permiso

Descripción detallada del permiso.

Aceptar una invitación para compartir

Para aceptar una invitación a compartir

1. Seleccione la invitación para compartir que desea aceptar.
2. Seleccione Aceptar.

Para las invitaciones a la carga de trabajo, la carga de trabajo se agrega a las páginas Cargas de trabajo y Panel. En el caso de las invitaciones con enfoques personalizados, el enfoque personalizado se añade a la página de Enfoques personalizados. En el caso de las invitaciones de perfil, el perfil se añade a la página de Perfiles. En el caso de las invitaciones para revisar plantillas, la plantilla se añadirá a su página de Revisión de plantillas.

Tiene siete días para aceptar una invitación. Si no acepta la invitación en el plazo de siete días, caducará automáticamente.

Si un usuario y la cuenta de Cuenta de AWS han aceptado las invitaciones a la carga de trabajo, la invitación a la carga de trabajo para el usuario determina el permiso del usuario.

Rechazar una invitación para compartir

Para rechazar una invitación para compartir

1. Seleccione la invitación a la carga de trabajo o el enfoque personalizado que desea aceptar o rechazar.
2. Seleccione Rechazar.

La invitación se quita de la lista.

Notificaciones

La página de Notificaciones muestra las diferencias de versión de las cargas de trabajo y revisa las plantillas que tienen enfoques y perfiles asociados. Puede actualizar a la versión más reciente de un enfoque o perfil para una carga de trabajo desde la página de notificaciones.

Notificaciones de enfoques

Cuando hay disponible una nueva versión de un enfoque, aparece un banner en la parte superior de la página de Cargas de trabajo o Revisar plantillas para notificarlo. Si ve una carga de trabajo específica o una plantilla de revisión que utilice un enfoque desactualizado, también verá un banner que indica que hay disponible una nueva versión del enfoque.

Elija Ver actualizaciones disponibles para ver una lista de las cargas de trabajo o plantillas de revisión que se pueden actualizar.

Consulte the section called “Actualización del enfoque” para obtener instrucciones sobre cómo actualizar un enfoque para una carga de trabajo o una plantilla de revisión.

Cuando el propietario de un enfoque compartido lo elimine, si tiene una carga de trabajo asociada al enfoque eliminado, recibirá una notificación en la que se le indicará que puede seguir utilizando el enfoque en su carga de trabajo actual, pero no podrá añadirlo a nuevas cargas de trabajo.

Notificaciones de perfil

Se proporcionan dos tipos de Notificaciones de perfil:

- Actualización de perfil
- Eliminación de perfil

Cuando se edita un perfil asociado a una carga de trabajo (para obtener más información, consulte the section called “Edición de un perfil”), se muestra una notificación de que hay una nueva versión del perfil en las Notificaciones del perfil.

Cuando el propietario de un perfil compartido lo elimine, si tiene una carga de trabajo asociada al perfil eliminado, recibirá una notificación en la que se le indicará que puede seguir utilizando el perfil en su carga de trabajo actual, pero no podrá añadirlo a nuevas cargas de trabajo.

Actualización de una versión de perfil

1. En el panel de navegación izquierdo, elija Notificaciones.
2. Seleccione el nombre de la carga de trabajo en la lista de la pestaña Notificaciones del perfil o utilice la barra de búsqueda para buscar por nombre de la carga de trabajo.
3. Elija Actualizar versión del perfil.
4. En la sección Reconocimiento, seleccione la casilla de confirmación correspondiente a Comprendo y acepto estos cambios.
5. (Opcional) Si decide guardar un hito, seleccione la casilla Guardar un hito e introduzca un Nombre de hito.
6. Seleccione Guardar.

Una vez actualizado el perfil, se muestran el número de versión más reciente y la fecha de actualización en la sección Perfil de la carga de trabajo.

Para obtener más información, consulte Perfiles.

Panel de control

El panel, disponible en la parte izquierda, le permite acceder a las cargas de trabajo y sus problemas asociados de riesgo medio y alto. También puede incluir las cargas de trabajo que se han compartido con usted. El Panel consta de cuatro secciones.

- Resumen: muestra el número total de cargas de trabajo, cuántas presentan riesgos altos y medios y el número total de problemas de riesgo alto y medio en todas las cargas de trabajo.
- Problemas del marco de Well-Architected por pilar: muestra una representación gráfica de los problemas de riesgo alto y medio por pilar para todas sus cargas de trabajo.
- Problemas del marco de Well-Architected por carga de trabajo: muestra los problemas de riesgo alto y medio por pilar para todas sus cargas de trabajo.
- Problemas del marco de Well-Architected por elemento del plan de mejora: muestra los elementos del plan de mejora para todas sus cargas de trabajo.

Resumen

Esta sección muestra el número total de cargas de trabajo y el número de cargas de trabajo con problemas de riesgo alto y medio desde el punto de vista del marco de Well-Architected y todos los demás enfoques. Se muestra el número total de problemas de riesgo alto y medio en todas las cargas de trabajo, ya sean de su propiedad o compartidas con su Cuenta de AWS.

Seleccione Incluir las cargas de trabajo que se han compartido conmigo para que las estadísticas resumidas, el informe consolidado y las demás secciones del panel reflejen tanto sus cargas de trabajo como las que se han compartido con usted.

Seleccione Generar informe para que se cree un informe consolidado en un archivo PDF.

El nombre del informe tiene el formato de: `wellarchitected_consolidatedreport_`*`account-ID`*`.pdf`.

Problemas del marco de Well-Architected por pilar

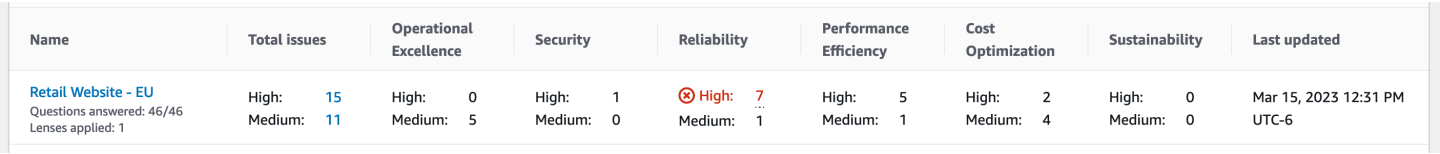
La sección Problemas del marco de Well-Architected por pilar muestra una representación gráfica del número de problemas de riesgo alto y medio por pilar para todas las cargas de trabajo.

Utilice las secciones restantes del panel para pasar de un nivel de detalle al siguiente.

> **Note**
>
> En esta sección solo se incluyen los problemas del enfoque del marco de Well-Architected.

Problemas del marco de Well-Architected por carga de trabajo

La sección Problemas por carga de trabajo del marco de Well-Architected muestra información para cada carga de trabajo.



Name	Total issues	Operational Excellence	Security	Reliability	Performance Efficiency	Cost Optimization	Sustainability	Last updated
Retail Website - EU Questions answered: 46/46 Lenses applied: 1	High: 15 Medium: 11	High: 0 Medium: 5	High: 1 Medium: 0	High: 7 Medium: 1	High: 5 Medium: 1	High: 2 Medium: 4	High: 0 Medium: 0	Mar 15, 2023 12:31 PM UTC-6

Para cada carga de trabajo se muestra la siguiente información:

Nombre

El nombre de la carga de trabajo. También se muestran el número de preguntas respondidas y el número de enfoques aplicados a la carga de trabajo.

Elija el nombre de la carga de trabajo para visitar la página de detalles de la carga de trabajo y ver los hitos, los planes de mejora y las acciones compartidas.

Total de problemas

El número total de problemas identificados por el marco de Well-Architected para la carga de trabajo.

Elija el número de problemas de riesgo alto o medio para ver los planes de mejora recomendados para dichos problemas.

Excelencia operativa

El número de problemas de alto riesgo (HRI) y de riesgo medio (MRI) identificados en la carga de trabajo del pilar de la excelencia operativa.

Seguridad

El número de HRI y MRI identificados para el pilar de seguridad.

Fiabilidad

El número de HRI y MRI identificados para el pilar de fiabilidad.

Eficacia del rendimiento

El número de HRI y MRI identificados para el pilar de eficacia del rendimiento.

Optimización de costes

El número de HRI y MRI identificados para el pilar de optimización de costes.

Sostenibilidad

El número de HRI y MRI identificados para el pilar de sostenibilidad.

Última actualización

La fecha y la hora a las que se actualizó por última vez la carga de trabajo.

Para cada carga de trabajo, se destaca el pilar con el mayor número de problemas de alto riesgo (HRI).

> **Note**
>
> En esta sección solo se incluyen los problemas del enfoque del marco de Well-Architected.

Problemas del marco de Well-Architected por elemento del plan de mejora

La sección Problemas del marco de Well-Architected por elemento del plan de mejora muestra los elementos del plan de mejora para todas sus cargas de trabajo. Puede filtrar los elementos en función del pilar y la gravedad.

Para cada plan de mejora se muestra la siguiente información:

Elemento de mejora

El nombre del elemento del plan de mejora.

Elija el nombre para mostrar las mejores prácticas asociadas al elemento del plan de mejora.

Pilar

El pilar asociado al elemento de mejora.

Riesgo

Indica si el problema asociado es de riesgo alto o medio.

Cargas de trabajo aplicables

La cantidad de cargas de trabajo a las que se aplica este plan de mejora.

Seleccione un elemento del plan de mejora para ver las cargas de trabajo aplicables.

> **Note**
>
> En esta sección solo se incluyen los elementos del plan de mejora del enfoque del marco de Well-Architected.

Seguridad en AWS Well-Architected Tool

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

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

- Seguridad de la nube: AWS es responsable de proteger la infraestructura que ejecuta servicios de AWS en la Nube de AWS. AWS también le proporciona servicios que puede utilizar de forma segura. Los auditores externos prueban y verifican periódicamente la eficacia de nuestra seguridad como parte de los Programas de conformidad de AWS . Para obtener información sobre los programas de conformidad que se aplican a AWS Well-Architected Tool, consulte AWS Services in Scope by Compliance Program.
- Seguridad en la nube: su responsabilidad se determina según el servicio de AWSque utiliza. También es responsable de otros factores, incluida la confidencialidad de los datos, los requisitos de la empresa y la legislación y la normativa aplicables.

Esta documentación le ayuda a comprender cómo aplicar el modelo de responsabilidad compartida a la hora de utilizar AWS WA Tool. Los siguientes temas le mostrarán cómo configurar AWS WA Tool para satisfacer sus objetivos de seguridad y de conformidad. También puede aprender a utilizar otros servicios de AWS que lo ayuden a monitorizar y proteger los recursos de AWS WA Tool.

Temas

Protección de los datos en AWS Well-Architected Tool

El modelo de responsabilidad compartida, y de AWS se aplica a la protección de datos de AWS Well-Architected Tool. Como se describe en este modelo, AWS es responsable de proteger la infraestructura global que ejecuta toda la Nube de AWS. Eres responsable de mantener el control sobre el contenido alojado en esta infraestructura. También eres responsable de las tareas de administración y configuración de seguridad para los Servicios de AWS que utiliza. Para obtener más información sobre la privacidad de los datos, consulta las Preguntas frecuentes sobre la privacidad de datos. Para obtener información sobre la protección de datos en Europa, consulta la publicación de blog sobre el Modelo de responsabilidad compartida de AWS y GDPR en el Blog de seguridad de AWS.

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

- Utiliza la autenticación multifactor (MFA) en cada cuenta.
- Utiliza SSL/TLS para comunicarse con los recursos de AWS. Se recomienda el uso de TLS 1.2 y recomendamos TLS 1.3.
- Configure los registros de API y de actividad de los usuarios con AWS CloudTrail. Para obtener información sobre cómo utilizar registros de seguimiento de CloudTrail para capturar actividades de AWS, consulta Working with CloudTrail trails en la Guía del usuario de AWS CloudTrail.
- Utiliza las soluciones de cifrado de AWS, junto con todos los controles de seguridad predeterminados dentro de los servicios de Servicios de AWS.
- Utiliza servicios de seguridad administrados avanzados, como Amazon Macie, que lo ayuden a detectar y proteger los datos confidenciales almacenados en Amazon S3.
- Si necesita módulos criptográficos validados FIPS 140-3 al acceder a AWS a través de una interfaz de línea de comandos o una API, utiliza un punto de conexión de FIPS. Para obtener más información sobre los puntos de conexión de FIPS disponibles, consulta Estándar de procesamiento de la información federal (FIPS) 140-3.

Se recomienda encarecidamente no introducir nunca información confidencial o sensible, como por ejemplo, direcciones de correo electrónico de clientes, en etiquetas o campos de formato libre, tales como el campo Nombre. Esto incluye las situaciones en las que debe trabajar con la AWS

WA Tool u otros Servicios de AWS a través de la consola, la API, la AWS CLI o los SDK de AWS. Cualquier dato que ingrese en etiquetas o campos de texto de formato libre utilizados para nombres se puede emplear para los registros de facturación o diagnóstico. Si proporciona una URL a un servidor externo, recomendamos encarecidamente que no incluya la información de las credenciales en la URL para validar la solicitud para ese servidor.

Cifrado en reposo

Todos los datos que AWS WA Tool almacena se cifran en reposo.

Cifrado en tránsito

Todos los datos enviados que tienen como origen o destino AWS WA Tool se cifran en tránsito.

Cómo utiliza AWS sus datos

El equipo de AWS Well-Architected recopila datos agregados del AWS Well-Architected Tool para proporcionar y mejorar el servicio AWS WA Tool a los clientes. Los datos individuales de los clientes se pueden compartir con los equipos de Cuenta de AWS para respaldar los esfuerzos de nuestros clientes por mejorar sus cargas de trabajo y su arquitectura. El equipo de AWS Well-Architected solo puede acceder a las propiedades de la carga de trabajo y a las opciones seleccionadas para cada pregunta. AWS no comparte ningún dato de AWS WA Tool fuera de AWS.

Las propiedades de carga de trabajo a las que tiene acceso el equipo de AWS Well-Architected incluyen:

- Nombre de carga de trabajo
- Propietario de la revisión
- Entorno
- Regiones
- ID de cuenta
- Tipo de sector

El equipo de AWS Well-Architected no tiene acceso a:

- Descripción de la carga de trabajo
- Diseño de arquitectura

- Cualquier nota que haya introducido

Administración de identidades y accesos para AWS Well-Architected Tool

AWS Identity and Access Management (IAM) es un Servicio de AWS que ayuda a los administradores a controlar de forma segura el acceso a los recursos de AWS. Los administradores de IAM controlan quién está autenticado (ha iniciado sesión) y autorizado (tiene permisos) para utilizar recursos de AWS WA Tool. IAM es un Servicio de AWS que se puede utilizar sin cargo adicional.

Temas

Público

La forma en que utilice AWS Identity and Access Management (IAM) difiere en función del trabajo que realice en AWS WA Tool.

Usuario de servicio: si utiliza el servicio de AWS WA Tool para realizar su trabajo, su administrador le proporciona las credenciales y los permisos que necesita. A medida que utilice más características de AWS WA Tool para realizar su trabajo, es posible que necesite permisos adicionales. Entender cómo se administra el acceso puede ayudarle a solicitar los permisos correctos al administrador. Si no puede acceder a una característica en AWS WA Tool, consulte Solución de problemas de identidades de AWS Well-Architected Tool y accesos.

Administrador de servicio: si está a cargo de los recursos de AWS WA Tool en su empresa, probablemente tenga acceso completo a AWS WA Tool. Su trabajo consiste en determinar a qué

características y recursos de AWS WA Tool deben acceder los usuarios del servicio. A continuación, debe enviar solicitudes a su administrador de IAM para cambiar los permisos de los usuarios de sus servicios. Revise la información de esta página para conocer los conceptos básicos de IAM. Para obtener más información sobre cómo su empresa puede utilizar IAM con AWS WA Tool, consulte Cómo AWS Well-Architected Tool funciona con IAM.

Administrador de IAM: si es un administrador de IAM, es posible que quiera conocer más detalles sobre cómo escribir políticas para administrar el acceso a AWS WA Tool. Para consultar ejemplos de políticas basadas en identidad de AWS WA Tool que puede utilizar en IAM, consulte AWS Well-Architected Tool ejemplos de políticas basadas en identidad de .

Autenticación con identidades

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

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

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

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

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

Usuario raíz de Cuenta de AWS

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

Identidad federada

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

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

Para una administración de acceso centralizada, le recomendamos que utiliza AWS IAM Identity Center. Puede crear usuarios y grupos en el IAM Identity Center o puede conectarse y sincronizar con un conjunto de usuarios y grupos de su propia fuente de identidad para usarlos en todas sus aplicaciones y Cuentas de AWS. Para obtener más información, consulta ¿Qué es el Centro de identidades de IAM? en la Guía del usuario de AWS IAM Identity Center.

Usuarios y grupos de IAM

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

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

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

Roles de IAM

Un rol de IAM es una identidad de la Cuenta de AWS que dispone de permisos específicos. Es similar a un usuario de IAM, pero no está asociado a una persona determinada. Para asumir temporalmente un rol de IAM en la AWS Management Console, puede cambiar de una función de usuario a un rol de IAM (consola). Puedes asumir un rol llamando a una operación de la AWS CLI o de la API de AWS, o utilizando una URL personalizada. Para más información sobre los métodos para el uso de roles, consulta Métodos para asumir un rol en la Guía del usuario de IAM.

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

- Acceso de usuario federado: para asignar permisos a una identidad federada, puede crear un rol y definir sus permisos. Cuando se autentica una identidad federada, se asocia la identidad al rol y se le conceden los permisos define el rol. Para obtener información acerca de roles de federación, consulte Crear un rol para un proveedor de identidad de terceros (federación) en la Guía de usuario de IAM. Si utiliza el IAM Identity Center, debe configurar un conjunto de permisos. IAM Identity Center correlaciona el conjunto de permisos con un rol en IAM para controlar a qué pueden acceder las identidades después de autenticarse. Para obtener información acerca de los conjuntos de permisos, consulta Conjuntos de permisos en la Guía del usuario de AWS IAM Identity Center.
- Permisos de usuario de IAM temporales: un usuario de IAM puede asumir un rol de IAM para recibir temporalmente permisos distintos que le permitan realizar una tarea concreta.
- Acceso entre cuentas: puede utilizar un rol de IAM para permitir que alguien (una entidad principal de confianza) de otra cuenta acceda a los recursos de la cuenta. Los roles son la forma principal de conceder acceso entre cuentas. No obstante, con algunos Servicios de AWS se puede adjuntar una política directamente a un recurso (en lugar de utilizar un rol como representante). Para

obtener información acerca de la diferencia entre los roles y las políticas basadas en recursos para el acceso entre cuentas, consulta Acceso a recursos entre cuentas en IAM en la Guía del usuario de IAM.

- Acceso entre servicios: algunos Servicios de AWS utilizan características de otros Servicios de AWS. Por ejemplo, cuando realiza una llamada en un servicio, es común que ese servicio ejecute aplicaciones en Amazon EC2 o almacene objetos en Amazon S3. Es posible que un servicio haga esto usando los permisos de la entidad principal, usando un rol de servicio o usando un rol vinculado a servicios.
  - Reenviar sesiones de acceso (FAS): cuando utiliza un rol o un usuario de IAM para llevar a cabo las acciones en AWS, se le considera una entidad principal. Cuando utiliza algunos servicios, es posible que realice una acción que desencadene otra acción en un servicio diferente. FAS utiliza los permisos de la entidad principal para llamar a un Servicio de AWS, combinados con el Servicio de AWS solicitante para realizar solicitudes a servicios posteriores. Las solicitudes de FAS solo se realizan cuando un servicio recibe una solicitud que requiere interacciones con otros Servicios de AWS o recursos para completarse. En este caso, debe tener permisos para realizar ambas acciones. Para obtener información sobre las políticas a la hora de realizar solicitudes de FAS, consulte Reenviar sesiones de acceso.
  - Rol de servicio: un rol de servicio es un rol de IAM que adopta un servicio para realizar acciones en su nombre. Un administrador de IAM puede crear, modificar y eliminar un rol de servicio desde IAM. Para obtener más información, consulte Creación de un rol para delegar permisos a un Servicio de AWS en la Guía del usuario de IAM.
  - Rol vinculado a los servicios: un rol vinculado a servicios es un tipo de rol de servicio que está vinculado a un Servicio de AWS. El servicio puede asumir el rol para realizar una acción en su nombre. Los roles vinculados a servicios aparecen en la Cuenta de AWS y son propiedad del servicio. Un administrador de IAM puede ver, pero no editar, los permisos de los roles vinculados a servicios.
- Aplicaciones que se ejecutan en Amazon EC2: puede utilizar un rol de IAM que le permita administrar credenciales temporales para las aplicaciones que se ejecutan en una instancia de EC2 y realizan solicitudes a la AWS CLI o a la API de AWS. Es preferible hacerlo de este modo a almacenar claves de acceso en la instancia de EC2. Para asignar un rol de AWS a una instancia de EC2 y ponerla a disposición de todas las aplicaciones, cree un perfil de instancia adjuntado a la instancia. Un perfil de instancia contiene el rol y permite a los programas que se ejecutan en la instancia de EC2 obtener credenciales temporales. Para obtener más información, consulte Uso de un rol de IAM para conceder permisos a aplicaciones que se ejecutan en instancias Amazon EC2 en la Guía del usuario de IAM.

Administración de acceso mediante políticas

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

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

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

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

Políticas basadas en identidades

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

Las políticas basadas en identidades pueden clasificarse además como políticas insertadas o políticas administradas. Las políticas insertadas se integran directamente en un único usuario, grupo o rol. Las políticas administradas son políticas independientes que puedes adjuntar a varios usuarios, grupos y roles de su Cuenta de AWS. Las políticas gestionadas incluyen las políticas gestionadas de AWS y las políticas gestionadas por el cliente. Para obtener más información sobre cómo elegir una política administrada o una política insertada, consulte Elegir entre políticas administradas y políticas insertadas en la Guía del usuario de IAM.

Políticas basadas en recursos

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

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

Listas de control de acceso (ACL)

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

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

Otros tipos de políticas

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

- Límites de permisos: un límite de permisos es una característica avanzada que le permite establecer los permisos máximos que una política basada en identidad puede conceder a una entidad de IAM (usuario o rol de IAM). Puedes establecer un límite de permisos para una entidad. Los permisos resultantes son la intersección de las políticas basadas en la identidad de la entidad y los límites de permisos. Las políticas basadas en recursos que especifiquen el usuario o rol en el campo `Principal` no estarán restringidas por el límite de permisos. Una denegación explícita en cualquiera de estas políticas anulará el permiso. Para obtener más información sobre los límites de los permisos, consulta Límites de permisos para las entidades de IAM en la Guía del usuario de IAM.

- Políticas de control de servicio (SCP): las SCP son políticas de JSON que especifican los permisos máximos de una organización o una unidad organizativa en AWS Organizations. AWS Organizations es un servicio que le permite agrupar y administrar de manera centralizada varias Cuentas de AWS que posea su empresa. Si habilita todas las características en una empresa, entonces podrá aplicar políticas de control de servicio (SCP) a una o todas sus cuentas. Una SCP limita los permisos para las entidades de las cuentas de miembro, incluido cada Usuario raíz de la cuenta de AWS. Para obtener más información acerca de SCP y Organizations, consulta Políticas de control de servicios en la Guía del usuario de AWS Organizations.
- Políticas de control de recursos (RCP): las RCP son políticas JSON que permiten establecer los permisos máximos disponibles para los recursos de las cuentas sin actualizar las políticas de IAM asociadas a cada recurso que posea. La RCP limita los permisos de los recursos en las cuentas de miembros y puede afectar a los permisos efectivos de las identidades, incluidos los Usuario raíz de la cuenta de AWS, independientemente de si pertenecen a su organización. Para obtener más información sobre Organizations y RCP, incluida una lista de los Servicios de AWS que admiten RCP, consulte Políticas de control de recursos (RCP) en la Guía del usuario de AWS Organizations.
- Políticas de sesión: las políticas de sesión son políticas avanzadas que se pasan como parámetro cuando se crea una sesión temporal mediante programación para un rol o un usuario federado. Los permisos de la sesión resultantes son la intersección de las políticas basadas en identidades del rol y las políticas de la sesión. Los permisos también pueden proceder de una política en función de recursos. Una denegación explícita en cualquiera de estas políticas anulará el permiso. Para más información, consulte Políticas de sesión en la Guía del usuario de IAM.

Varios tipos de políticas

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

Cómo AWS Well-Architected Tool funciona con IAM

Antes de utilizar IAM para administrar el acceso a AWS WA Tool, conozca qué características de IAM se pueden utilizar con AWS WA Tool.

Características de IAM que puede utilizar con AWS Well-Architected Tool

Característica de IAM	Compatibilidad con AWS WA Tool
Políticas basadas en identidad	Sí
Políticas basadas en recursos	No
Acciones de políticas	Sí
Recursos de políticas	Sí
Claves de condición de política (específicas del servicio)	Sí
ACL	No
ABAC (etiquetas en políticas)	Sí
Credenciales temporales	Sí
Permisos de entidades principales	Sí
Roles de servicio	No
Roles vinculados al servicio	No

Para obtener una perspectiva general sobre cómo funcionan AWS WA Tool y otros servicios de AWS con las características de IAM, consulte Servicios de AWS que funcionan con IAM en la Guía del usuario de IAM.

Políticas de AWS WA Tool basadas en identidades

Compatibilidad con las acciones de políticas: sí

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

El elemento `Action` de una política JSON describe las acciones que puede utilizar para conceder o denegar el acceso en una política. Las acciones de la política generalmente tienen el mismo nombre que la operación de API de AWS asociada. Hay algunas excepciones, como acciones de

solo permiso que no tienen una operación de API coincidente. También hay algunas operaciones que requieren varias acciones en una política. Estas acciones adicionales se denominan acciones dependientes.

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

Políticas basadas en recursos de AWS WA Tool

Admite políticas basadas en recursos: no

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

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

Acciones de política para AWS WA Tool

Compatibilidad con las acciones de políticas: sí

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

El elemento `Action` de una política JSON describe las acciones que puede utilizar para conceder o denegar el acceso en una política. Las acciones de la política generalmente tienen el mismo nombre que la operación de API de AWS asociada. Hay algunas excepciones, como acciones de

solo permiso que no tienen una operación de API coincidente. También hay algunas operaciones que requieren varias acciones en una política. Estas acciones adicionales se denominan acciones dependientes.

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

Las acciones de políticas de AWS WA Tool utilizan el siguiente prefijo antes de la acción: `wellarchitected:`. Por ejemplo, para permitir que una entidad defina una carga de trabajo, un administrador debe asociar una política que permita acciones `wellarchitected:CreateWorkload`. Del mismo modo, para evitar que una entidad elimine cargas de trabajo, el administrador puede asociar una política que deniegue las acciones `wellarchitected:DeleteWorkload`. Las instrucciones de política deben incluir un elemento `Action` o `NotAction`. AWS WA Tool define su propio conjunto de acciones que describen las tareas que se pueden realizar con este servicio.

Para ver una lista de las acciones de AWS WA Tool, consulte Acciones definidas por AWS Well-Architected Tool en la Referencia de autorizaciones de servicio.

Recursos de políticas

Compatibilidad con los recursos de políticas: sí

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

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

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

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

Para ver una lista de los tipos de recursos de AWS WA Tool y sus ARN, consulte Recursos definidos por AWS Well-Architected Tool en la Referencia de autorizaciones de servicio. Para obtener

información sobre las acciones con las que puede especificar el ARN de cada recurso, consulte Acciones definidas por AWS Well-Architected Tool.

El recurso de la carga de trabajo de AWS WA Tool tiene el siguiente ARN:

```
arn:${Partition}:wellarchitected:${Region}:${Account}:workload/${ResourceId}
```

Para obtener más información acerca del formato de los ARN, consulte Nombres de recursos de Amazon (ARN) y espacios de nombres de servicios de AWS.

Encontrará el ARN en la página Workload properties (Propiedades de la carga de trabajo) de una carga de trabajo. Por ejemplo, para especificar una carga de trabajo específica:

```
"Resource": "arn:aws:wellarchitected:us-
west-2:123456789012:workload/11112222333344445555666677778888"
```

Para especificar todas las cargas de trabajo que pertenecen a una determinada cuenta, utilice el carácter comodín (*):

```
"Resource": "arn:aws:wellarchitected:us-west-2:123456789012:workload/*"
```

Algunas acciones de AWS WA Tool, como las empleadas para crear y mostrar recursos, no se pueden llevar a cabo en un recurso específico. En dichos casos, debe utilizar el carácter comodín (*).

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

Para ver una lista de los tipos de recursos de AWS WA Tool y sus ARN, consulte Recursos definidos por AWS Well-Architected Tool en la Referencia de autorizaciones de servicio. Para obtener información sobre las acciones con las que puede especificar el ARN de cada recurso, consulte Acciones definidas por AWS Well-Architected Tool.

Claves de condición de políticas para AWS WA Tool

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

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

El elemento `Condition` (o bloque de `Condition`) permite especificar condiciones en las que entra en vigor una instrucción. El elemento `Condition` es opcional. Puedes crear expresiones

condicionales que utilizan operadores de condición, tales como igual o menor que, para que la condición de la política coincida con los valores de la solicitud.

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

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

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

AWS WA Tool proporciona una clave de condición específica del servicio (`wellarchitected:JiraProjectKey`) y admite el uso de algunas claves de condición globales. Para ver todas las claves de condición globales de AWS, consulte Claves de contexto de condición globales de AWS en la Referencia de autorizaciones de servicio.

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

El elemento `Condition` (o bloque de `Condition`) permite especificar condiciones en las que entra en vigor una instrucción. El elemento `Condition` es opcional. Puedes crear expresiones condicionales que utilizan operadores de condición, tales como igual o menor que, para que la condición de la política coincida con los valores de la solicitud.

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

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

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

ACL en AWS WA Tool

Compatibilidad con ACL: no

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

Autorización basada en etiquetas de AWS WA Tool

Admite ABAC (etiquetas en las políticas): sí

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

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

Para controlar el acceso en función de etiquetas, debe proporcionar información de las etiquetas en el elemento de condición de una política utilizando las claves de condición `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` o `aws:TagKeys`.

Si un servicio admite las tres claves de condición para cada tipo de recurso, el valor es Sí para el servicio. Si un servicio admite las tres claves de condición solo para algunos tipos de recursos, el valor es Parcial.

Para obtener más información sobre ABAC, consulte Definición de permisos con la autorización de ABAC en la Guía del usuario de IAM. Para ver un tutorial con los pasos para configurar ABAC, consulte Uso del control de acceso basado en atributos (ABAC) en la Guía del usuario de IAM.

Uso de credenciales temporales con AWS WA Tool

Compatibilidad con credenciales temporales: sí

Algunos Servicios de AWS no funcionan cuando inicia sesión con credenciales temporales. Para obtener información adicional, incluida la información sobre qué Servicios de AWS funcionan con credenciales temporales, consulta Servicios de AWS que funcionan con IAM en la Guía del usuario de IAM.

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

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

Permisos de entidades principales entre servicios de AWS WA Tool

Admite sesiones de acceso directo (FAS): sí

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

Roles de servicio para AWS WA Tool

Compatible con roles de servicio: No

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

Roles vinculados a servicios de AWS WA Tool

Compatibilidad con roles vinculados al servicio: no

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

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

AWS Well-Architected Tool ejemplos de políticas basadas en identidad de

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

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

Temas

- Prácticas recomendadas relativas a políticas
- Mediante la consola de AWS WA Tool
- Permitir a los usuarios consultar sus propios permisos
- Conceder acceso completo a las cargas de trabajo
- Conceder acceso de solo lectura a las cargas de trabajo
- Acceder a una carga de trabajo específica
- Uso de una clave de condición específica del servicio para el conector de AWS Well-Architected Tool para Jira

Prácticas recomendadas relativas a políticas

Las políticas basadas en identidades determinan si alguien puede crear, acceder o eliminar los recursos de AWS WA Tool de la cuenta. Estas acciones pueden generar costes adicionales para su Cuenta de AWS. Siga estas directrices y recomendaciones al crear o editar políticas basadas en identidades:

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

a sus políticas. Para más información, consulte Acceso seguro a la API con MFA en la Guía del usuario de IAM.

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

Mediante la consola de AWS WA Tool

Para acceder a la consola de AWS Well-Architected Tool, debe tener un conjunto mínimo de permisos. Estos permisos deben permitirle enumerar y consultar los detalles sobre los recursos de AWS WA Tool en su Cuenta de AWS. Si crea una política basada en identidades que sea más restrictiva que el mínimo de permisos necesarios, la consola no funcionará del modo esperado para las entidades (usuarios o roles) que tengan esa política.

Para asegurarse de que esas entidades puedan seguir usando la consola de AWS WA Tool, asocie también la siguiente política administrada de AWS a las entidades:

```
WellArchitectedConsoleReadOnlyAccess
```

Para permitir la creación, modificación y eliminación de cargas de trabajo, asocie la siguiente política administrada de AWS a las entidades:

```
WellArchitectedConsoleFullAccess
```

Para obtener más información, consulte Adición de permisos a un usuario en la Guía del usuario de IAM.

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

Permitir a los usuarios consultar sus propios permisos

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

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

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

Conceder acceso completo a las cargas de trabajo

En este ejemplo, desea conceder a un usuario de su Cuenta de AWS acceso completo a las cargas de trabajo. Con el acceso completo, el usuario puede realizar todas las acciones en AWS WA Tool. Este acceso es necesario para poder definir, eliminar, ver y actualizar cargas de trabajo.

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

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

Conceder acceso de solo lectura a las cargas de trabajo

En este ejemplo, desea conceder a un usuario de su Cuenta de AWS acceso de solo lectura a las cargas de trabajo. Con el acceso de solo lectura, el usuario exclusivamente puede ver las cargas de trabajo de AWS WA Tool.

```
{
   "Version": "2012-10-17",
   "Statement" : [
     {
     "Effect" : "Allow",
     "Action" : [
          "wellarchitected:Get*",
          "wellarchitected:List*"
     ],
     "Resource": "*"
     }
   ]
}
```

Acceder a una carga de trabajo específica

En este ejemplo, desea conceder a un usuario de su Cuenta de AWS acceso de solo lectura a una de las cargas de trabajo, 99999999999955555555555566666666, que se encuentra en la región `us-west-2`. El ID de la cuenta es 777788889999.

```
{
   "Version": "2012-10-17",
   "Statement" : [
     {
     "Effect" : "Allow",
     "Action" : [
          "wellarchitected:Get*",
          "wellarchitected:List*"
     ],
```

```
     "Resource": "arn:aws:wellarchitected:us-
west-2:777788889999:workload/99999999999955555555555666666666"
     }
   ]
}
```

Uso de una clave de condición específica del servicio para el conector de AWS Well-Architected Tool para Jira

En este ejemplo, se muestra cómo usar la clave de condición específica del servicio `wellarchitected:JiraProjectKey` para controlar qué proyectos de Jira se pueden vincular a las cargas de trabajo de su cuenta.

A continuación se describen los usos pertinentes de la clave de condición:

- **`CreateWorkload:`** al solicitar `wellarchitected:JiraProjectKey` a `CreateWorkload`, puede definir qué proyectos personalizados de Jira se pueden vincular a cualquier carga de trabajo creada por el usuario. Por ejemplo, si un usuario intenta crear una nueva carga de trabajo con el proyecto ABC, pero la política solo especifica el PQR del proyecto, se deniega la acción.
- **`UpdateWorkload:`** al solicitar `wellarchitected:JiraProjectKey` a `UpdateWorkload`, puede definir qué proyectos personalizados de Jira se pueden vincular a esta carga de trabajo concreta o a cualquier carga de trabajo. Por ejemplo, si un usuario intenta actualizar una carga de trabajo existente con el proyecto ABC, pero la política especifica el PQR del proyecto, se deniega la acción. Además, si el usuario tiene una carga de trabajo vinculada al proyecto PQR e intenta actualizarla para vincularla al proyecto ABC, se deniega la acción.
- **`UpdateGlobalSettings:`** al solicitar `wellarchitected:JiraProjectKey` a `UpdateGlobalSettings`, puede definir qué proyectos personalizados de Jira se pueden vincular a la Cuenta de AWS. La configuración a nivel de cuenta protege las cargas de trabajo de su cuenta y no anula la configuración de Jira a nivel de cuenta. Por ejemplo, si un usuario tiene acceso a `UpdateGlobalSettings`, no podrá vincular las cargas de trabajo de su cuenta a ningún proyecto que no esté especificado en la política.

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Sid": "VisualEditor0",
   "Effect": "Allow",
```

```
    "Action": [
     "wellarchitected:UpdateGlobalSettings",
     "wellarchitected:CreateWorkload"
    ],
    "Resource": "*",
    "Condition": {
     "StringEqualsIfExists": {
      "wellarchitected:JiraProjectKey": ["ABC, PQR"]
     }
    }
   },
   {
    "Sid": "VisualEditor1",
    "Effect": "Allow",
    "Action": [
     "wellarchitected:UpdateWorkload"
    ],
    "Resource": "WORKLOAD_ARN",
    "Condition": {
     "StringEqualsIfExists": {
      "wellarchitected:JiraProjectKey": ["ABC, PQR"]
     }
    }
   }
  ]
}
```

Políticas administradas de AWS para AWS Well-Architected Tool

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 de 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 específicas para sus 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: WellArchitectedConsoleFullAccess

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

La política concede acceso total a AWS Well-Architected Tool.

Detalles de los permisos

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

Política administrada de AWS: WellArchitectedConsoleReadOnlyAccess

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

Esta política concede acceso de solo lectura a AWS Well-Architected Tool.

Detalles de los permisos

```
{
   "Version": "2012-10-17",
   "Statement" : [
     {
     "Effect" : "Allow",
     "Action" : [
          "wellarchitected:Get*",
          "wellarchitected:List*"
          "wellarchitected:ExportLens"
```

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

Política administrada de AWS: AWSWellArchitectedOrganizationsServiceRolePolicy

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

Esta política otorga los permisos administrativos en AWS Organizations necesarios para respaldar la integración de AWS Well-Architected Tool con Organizations. Estos permisos permiten que la cuenta de administración de la organización permita compartir recursos con AWS WA Tool.

Detalles de los permisos

Esta política incluye los siguientes permisos.

- `organizations:ListAWSServiceAccessForOrganization`: permite a las entidades principales comprobar si el acceso al servicio de AWS está habilitado para AWS WA Tool.
- `organizations:DescribeAccount`: permite a las entidades principales recuperar información de sobre una cuenta en una organización.
- `organizations:DescribeOrganization`: permite a las entidades principales recuperar información sobre la configuración de la organización.
- `organizations:ListAccounts`: permite a las entidades principales recuperar la lista de cuentas que pertenecen a una organización.
- `organizations:ListAccountsForParent`: permite a las entidades principales recuperar la lista de cuentas que pertenecen a una organización de un determinado nodo raíz en la organización.
- `organizations:ListChildren`: permite a las entidades principales recuperar la lista de cuentas y las unidades organizativas que pertenecen a una organización de un determinado nodo raíz en la organización.
- `organizations:ListParents`: permite a las entidades principales recuperar la lista de elementos principales inmediatos especificada por la unidad organizativa o la cuenta de una organización.
- `organizations:ListRoots`: permite a las entidades principales recuperar la lista de todos los nodos raíz de una organización.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "organizations:ListAWSServiceAccessForOrganization",
                "organizations:DescribeAccount",
                "organizations:DescribeOrganization",
                "organizations:ListAccounts",
                "organizations:ListAccountsForParent",
                "organizations:ListChildren",
                "organizations:ListParents",
                "organizations:ListRoots"
            ],
            "Resource": "*"
        }
    ]
}
```

Política administrada de AWS: AWSWELLArchitectedDiscoveryServiceRolePolicy

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

Esta política permite a AWS Well-Architected Tool acceder a los servicios de AWS y recursos relacionados con los recursos de AWS WA Tool.

Detalles de los permisos

Esta política incluye los siguientes permisos.

- `trustedadvisor:DescribeChecks`: enumera los cheques Trusted Advisor disponibles.
- `trustedadvisor:DescribeCheckItems`: obtiene datos de cheques Trusted Advisor, incluidos el estado y los recursos marcados por Trusted Advisor.
- `servicecatalog:GetApplication`: obtiene los detalles de una aplicación de AppRegistry.
- `servicecatalog:ListAssociatedResources`: muestra los recursos asociados a una aplicación de AppRegistry.
- `cloudformation:DescribeStacks`: obtiene los detalles de las pilas de AWS CloudFormation.

- `cloudformation:ListStackResources`: enumera los recursos asociados a las pilas de AWS CloudFormation.
- `resource-groups:ListGroupResources`: enumera los recursos de un ResourceGroup.
- `tag:GetResources`: necesario para ListGroupreResources.
- `servicecatalog:CreateAttributeGroup`: crea un grupo de atributos gestionado por el servicio cuando es necesario.
- `servicecatalog:AssociateAttributeGroup`: asocia un grupo de atributos gestionado por un servicio a una aplicación de AppRegistry.
- `servicecatalog:UpdateAttributeGroup`: actualiza un grupo de atributos gestionado por un servicio.
- `servicecatalog:DisassociateAttributeGroup`: desasocia un grupo de atributos gestionado por un servicio a una aplicación de AppRegistry.
- `servicecatalog:DeleteAttributeGroup`: elimina un grupo de atributos gestionado por el servicio cuando es necesario.

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Effect": "Allow",
   "Action": [
    "trustedadvisor:DescribeChecks",
    "trustedadvisor:DescribeCheckItems"
   ],
   "Resource": [
    "*"
   ]
  },
  {
   "Effect": "Allow",
   "Action": [
    "cloudformation:DescribeStacks",
    "cloudformation:ListStackResources",
    "resource-groups:ListGroupResources",
    "tag:GetResources"
   ],
   "Resource": [
    "*"
```

```
    ]
   },
   {
    "Effect": "Allow",
    "Action": [
     "servicecatalog:ListAssociatedResources",
     "servicecatalog:GetApplication",
     "servicecatalog:CreateAttributeGroup"
    ],
    "Resource": [
     "*"
    ]
   },
   {
    "Effect": "Allow",
    "Action": [
     "servicecatalog:AssociateAttributeGroup",
     "servicecatalog:DisassociateAttributeGroup"
    ],
    "Resource": [
     "arn:*:servicecatalog:*:*:/applications/*",
     "arn:*:servicecatalog:*:*:/attribute-groups/AWS_WellArchitected-*"
    ]
   },
   {
    "Effect": "Allow",
    "Action": [
     "servicecatalog:UpdateAttributeGroup",
     "servicecatalog:DeleteAttributeGroup"
    ],
    "Resource": [
     "arn:*:servicecatalog:*:*:/attribute-groups/AWS_WellArchitected-*"
    ]
   }
  ]
}
```

Actualizaciones de AWS a políticas administradas de AWS WA Tool

Consulte los detalles relativos a las actualizaciones de las políticas administradas de AWS para AWS WA Tool desde que este servicio empezara a realizar el seguimiento de estos cambios. Para obtener alertas automáticas sobre cambios en esta página, suscríbase a la fuente RSS en la página de historial de documentos de AWS WA Tool.

Cambio	Descripción	Fecha
Cambios en la política administrada de AWS WA Tool	Se agregó `"wellarchitected:Export*"` a `WellArchitectedConsoleReadOnlyAccess`.	22 de junio de 2023
Política de roles de servicio agregada de AWS WA Tool	`AWSWellArchitectedDiscoveryServiceRolePolicy` añadida para permitir a AWS Well-Architected Tool acceder a los servicios y los recursos de AWS que se relaciona con los recursos de AWS WA Tool.	3 de mayo de 2023
AWS WA Tool: permisos agregados	Se ha añadido una nueva acción de concesión `ListAWSServiceAccessForOrganization` parar permitir a AWS WA Tool acceder si el acceso de servicio de AWS está habilitado para AWS WA Tool.	22 de julio de 2022
AWS WA Tool comenzó el seguimiento de los cambios	AWS WA Tool comenzó el seguimiento de los cambios de las políticas administradas de AWS.	22 de julio de 2022

Solución de problemas de identidades de AWS Well-Architected Tool y accesos

Utilice la siguiente información para diagnosticar y solucionar los problemas comunes que puedan surgir cuando trabaje con AWS WA Tool e IAM.

Temas

No tengo autorización para realizar una acción en AWS WA Tool

Si la AWS Management Console le indica que no está autorizado para llevar a cabo una acción, debe ponerse en contacto con su gestionador para recibir ayuda. El gestionador es la persona que le proporcionó las credenciales de inicio de sesión.

En el siguiente ejemplo, se produce un error cuando el usuario *mateojackson* intenta utilizar la consola para realizar la acción DeleteWorkload, ya que no tiene permisos para ello.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to
 perform: wellarchitected:DeleteWorkload on resource: 11112222333344445555666677778888
```

En este ejemplo, debe pedir al administrador que actualice sus políticas para que pueda obtener acceso al recurso `11112222333344445555666677778888` a través de la acción `wellarchitected:DeleteWorkload`.

Respuesta frente a incidencias en AWS Well-Architected Tool

La respuesta frente a incidencias de AWS Well-Architected Tool es una responsabilidad de AWS. AWS tiene una política y un programa formales y documentados que rigen la respuesta frente a incidencias.

Los problemas operativos de AWS con gran alcance se publican en AWS Service Health Dashboard.

Los problemas operativos también se publican en las cuentas individuales a través de AWS Health Dashboard. Para obtener más información sobre cómo usar la AWS Health Dashboard, consulte la Guía de usuario de AWS Health.

Validación de conformidad en AWS Well-Architected Tool

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

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

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

- Cumplimiento de seguridad y gobernanza: en estas guías se explican las consideraciones de arquitectura y se proporcionan pasos para implementar las características de seguridad y cumplimiento.
- Referencia de servicios válidos de HIPAA: muestra una lista con los servicios válidos de HIPAA. No todos los Servicios de AWS son aptos para HIPAA.
- Recursos de conformidad de AWS: este conjunto de manuales y guías podría aplicarse a su sector y ubicación.
- Guías de cumplimiento para clientes de AWS: comprenda el modelo de responsabilidad compartida desde el punto de vista del cumplimiento. Las guías resumen las mejores prácticas para garantizar la seguridad de los Servicios de AWS y orientan los controles de seguridad en varios marcos (incluidos el Instituto Nacional de Estándares y Tecnología (NIST, por sus siglas en inglés), el Consejo de Estándares de Seguridad de la Industria de Tarjetas de Pago (PCI, por sus siglas en inglés) y la Organización Internacional de Normalización (ISO, por sus siglas en inglés)).
- Evaluación de recursos con reglas en la Guía para desarrolladores de AWS Config: el servicio AWS Config evalúa en qué medida las configuraciones de sus recursos cumplen las prácticas internas, las directrices del sector y las normativas.
- AWS Security Hub: este Servicio de AWS proporciona una visión completa de su estado de seguridad en AWS. Security Hub utiliza controles de seguridad para evaluar sus recursos de AWS y comprobar su cumplimiento con los estándares y las prácticas recomendadas del sector de la seguridad. Para obtener una lista de los servicios y controles compatibles, consulta la Referencia de controles de Security Hub.
- Amazon GuardDuty: este Servicio de AWS detecta posibles amenazas para sus Cuentas de AWS, cargas de tarea, contenedores y datos mediante la supervisión de su entorno para detectar actividades sospechosas y maliciosas. GuardDuty puedes ayudarlo a satisfacer varios requisitos de conformidad, como PCI DSS, cumpliendo los requisitos de detección de intrusos que exigen determinados marcos de conformidad.

- AWS Audit Manager: este servicio de Servicio de AWS le ayuda a auditar continuamente el uso de AWS con el fin de simplificar la forma en que administra el riesgo y la conformidad con las normativas y los estándares del sector.

Resiliencia en AWS Well-Architected Tool

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

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

Seguridad de la infraestructura en AWS Well-Architected Tool

Como se trata de un servicio administrado, AWS Well-Architected Tool está protegido por la seguridad de red global de AWS. Para obtener información sobre los servicios de seguridad de AWS y cómo AWSprotege la infraestructura, consulte Seguridad en la nube de AWS. Para diseñar su entorno de AWS con las prácticas recomendadas de seguridad de infraestructura, consulte Protección de la infraestructura en Portal de seguridad de AWS Well-Architected Framework.

Puede utilizar llamadas a la API publicadas en AWS para obtener acceso a AWS WA Tool a través de la red. Los clientes deben admitir lo siguiente:

- Seguridad de la capa de transporte (TLS). Exigimos TLS 1.2 y recomendamos TLS 1.3.
- Conjuntos de cifrado con confidencialidad directa total (PFS) como DHE (Ephemeral Diffie-Hellman) o ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). La mayoría de los sistemas modernos como Java 7 y posteriores son compatibles con estos modos.

Además, las solicitudes deben estar firmadas mediante un ID de clave de acceso y una clave de acceso secreta que esté asociada a una entidad principal de IAM. También puedes utilizar AWS

Security Token Service (AWS STS) para generar credenciales de seguridad temporales para firmar solicitudes.

Configuración y análisis de vulnerabilidades en AWS Well-Architected Tool

La configuración y los controles de TI son una responsabilidad compartida entre AWS y usted, nuestro cliente. Para obtener más información, consulte el modelo de responsabilidad compartida de AWS.

Prevención de la sustitución confusa entre servicios

El problema del suplente confuso es un problema de seguridad en el que una entidad que no tiene permiso para realizar una acción puede obligar a una entidad con más privilegios a realizar la acción. En AWS, la suplantación entre servicios puede dar lugar al problema de la sustitución confusa. La suplantación entre servicios puedes producirse cuando un servicio (el servicio que lleva a cabo las llamadas) llama a otro servicio (el servicio al que se llama). El servicio que lleva a cabo las llamadas se puedes manipular para utilizar sus permisos a fin de actuar en función de los recursos de otro cliente de una manera en la que no debe tener permiso para acceder. Para evitarlo, AWS proporciona herramientas que lo ayudan a proteger sus datos para todos los servicios con entidades principales de servicio a las que se les ha dado acceso a los recursos de su cuenta.

Se recomienda utilizar las claves de contexto de condición global `aws:SourceArn` y `aws:SourceAccount` en las políticas de recursos para limitar los permisos que AWS Well-Architected Tool concede a otro servicio para el recurso. Utiliza `aws:SourceArn` si desea que solo se asocie un recurso al acceso entre servicios. Utiliza `aws:SourceAccount` si quiere permitir que cualquier recurso de esa cuenta se asocie al uso entre servicios.

La forma más eficaz de protegerse contra el problema de la sustitución confusa es utilizar la clave de contexto de condición global de `aws:SourceArn` con el ARN completo del recurso. Si no conoce el ARN completo del recurso o si está especificando varios recursos, utilice la clave de condición de contexto global `aws:SourceArn` con caracteres comodines (*) para las partes desconocidas del ARN. Por ejemplo, `arn:aws:wellarchitected:*:123456789012:*`.

Si el valor de `aws:SourceArn` no contiene el ID de cuenta, como un ARN de bucket de Amazon S3, debe utilizar ambas claves de contexto de condición global para limitar los permisos.

El valor de `aws:SourceArn` debe ser una carga de trabajo o un enfoque.

El siguiente ejemplo muestra cómo se pueden utilizar las claves contextuales de condición global `aws:SourceArn` y `aws:SourceAccount` en AWS WA Tool para evitar el problema del adjunto confundido.

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Sid": "ConfusedDeputyPreventionExamplePolicy",
    "Effect": "Allow",
    "Principal": {
      "Service": "wellarchitected.amazonaws.com"
    },
    "Action": "wellarchitected:ActionName",
    "Resource": [
      "arn:aws:wellarchitected:::ResourceName/*"
    ],
    "Condition": {
      "ArnLike": {
        "aws:SourceArn": "arn:aws:wellarchitected:*:123456789012:*"
      },
      "StringEquals": {
        "aws:SourceAccount": "123456789012"
      }
    }
  }
}
```

Compartir los recursos de AWS WA Tool

Para compartir un recurso de su propiedad, haga lo siguiente:

- Activar el uso compartido de recursos en AWS Organizations (opcional)
- Compartir una carga de trabajo
- Compartir un enfoque personalizado
- Compartir un perfil
- Compartir una plantilla de revisión

> **Notas**
>
> - Al compartir un recurso, estará disponible para que lo usen entidades principales ajenas a la Cuenta de AWS que creó el recurso. Al compartir no se modifican los permisos que se aplican al recurso en la cuenta que lo creó.
> - AWS WA Tool es un servicio regional. Las entidades principales con las que comparte pueden acceder únicamente a los recursos compartidos de las Regiones de AWS en las que se crearon.
> - Para compartir recursos en una región introducida después del 20 de marzo de 2019, tanto usted como Cuenta de AWS debe habilitar la región en la AWS Management Console. Para obtener más información, consulte Infraestructura global de AWS.

Activar el uso compartido de recursos en AWS Organizations

Cuando su cuenta esté administrada por AWS Organizations, puede aprovechar para compartir recursos más fácilmente. Con o sin organizaciones, un usuario puede compartir con cuentas individuales. Sin embargo, si su cuenta pertenece a una organización, puede compartir con cuentas individuales, así como con todas las cuentas de la organización o de una OU, sin necesidad de enumerar cada cuenta.

Para compartir recursos dentro de una organización, primero debe usar la consola de AWS WA Tool o AWS Command Line Interface (AWS CLI) para habilitar el uso compartido con AWS Organizations. Cuando comparte recursos en su organización, AWS WA Tool no envía invitaciones

a las entidades principales. Las entidades principales de su organización obtienen acceso a los recursos compartidos sin necesidad de intercambiar invitaciones.

Al activar el uso compartido de recursos en su organización, AWS WA Tool crea un rol vinculado a un servicio denominado `AWSServiceRoleForWellArchitected`. Este rol, que solo lo puede asumir el servicio AWS WA Tool, otorga a AWS WA Tool permiso para recuperar información sobre la organización de la que es miembro utilizando la política administrada de AWS `AWSWellArchitectedOrganizationsServiceRolePolicy`.

Si ya no necesita compartir recursos con toda la organización o con determinadas OU, puede deshabilitar el uso compartido de recursos.

Requisitos

- Solo puede realizar estos pasos si ha iniciado sesión como entidad principal en la cuenta de administración de la organización.
- La organización debe tener todas las características habilitadas. Para obtener más información, consulte Habilitar todas las características en la organización en la Guía del usuario de AWS Organizations.

> **Important**
>
> Debe activar la opción de compartir con AWS Organizations mediante la consola de AWS WA Tool. Así se asegurará de crear el rol vinculado al servicio `AWSServiceRoleForWellArchitected`. Si activa el acceso de confianza con AWS Organizations utilizando la consola de AWS Organizations o el comando enable-aws-service-access de la AWS CLI, el rol vinculado al servicio `AWSServiceRoleForWellArchitected` no se creará y no podrá compartir recursos dentro de la organización.

Para activar el uso compartido de recursos dentro de la organización

1. Inicie sesión en AWS Management Console y abra la consola de AWS Well-Architected Tool en https://console.aws.amazon.com/wellarchitected/.

   Debe iniciar sesión como entidad principal en la cuenta de administración de la organización.
2. En el panel de navegación izquierdo, elija Configuración.
3. Seleccione Activar compatibilidad con AWS Organizations.

4. Elija Guardar configuración.

Para deshabilitar el uso compartido de recursos dentro de la organización

1. Inicie sesión en AWS Management Console y abra la consola de AWS Well-Architected Tool en https://console.aws.amazon.com/wellarchitected/.

   Debe iniciar sesión como entidad principal en la cuenta de administración de la organización.
2. En el panel de navegación izquierdo, elija Configuración.
3. Anule la selección de Activar compatibilidad con AWS Organizations.
4. Elija Guardar configuración.

Etiquetar los recursos de AWS WA Tool

Para ayudarle a administrar sus recursos de AWS WA Tool, puede asignar sus propios metadatos a cada recurso en forma de etiquetas. En este tema se describe qué son las etiquetas y cómo crearlas.

Contenido

Conceptos básicos de etiquetas

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 permiten clasificar los recursos de AWS según, por ejemplo, su finalidad, propietario o entorno. Cuando tenga muchos recursos del mismo tipo, puede identificar rápidamente un recurso específico en función de las etiquetas que le haya asignado. Por ejemplo, puede definir un conjunto de etiquetas para los servicios de AWS WA Tool para ayudarle a realizar un seguimiento del propietario y del nivel de pila de cada servicio. Le recomendamos que diseñe un conjunto coherente de claves de etiqueta para cada tipo de recurso.

Además, las etiquetas no se asignan a los recursos automáticamente. Después de agregar una etiqueta, puede editar las claves y los valores de las etiquetas o eliminar etiquetas de un recurso en cualquier momento. Si elimina un recurso, también se eliminará cualquier etiqueta asignada a dicho recurso.

Las etiquetas no tienen ningún significado semántico para AWS WA Tool, por lo que se interpretan estrictamente como cadenas de caracteres. Puede establecer el valor de una etiqueta como una cadena vacía, pero no puede asignarle un valor nulo. Si añade una etiqueta con la misma clave que una etiqueta existente en ese recurso, el nuevo valor sobrescribirá al antiguo.

Puede trabajar con etiquetas utilizando la AWS Management Console, la AWS CLI y la API de AWS WA Tool.

Si utiliza AWS Identity and Access Management (IAM), puede controlar qué usuarios de su Cuenta de AWS tienen permiso para crear, editar o eliminar etiquetas.

Etiquetar los recursos

Puede etiquetar recursos nuevos o existentes de AWS WA Tool.

Si utiliza la consola de AWS WA Tool, puede aplicar etiquetas a los recursos de nueva creación o a los recursos existentes cuando lo desee. Para las cargas de trabajo existentes, puede aplicar etiquetas a través de la pestaña Propiedades. Para los enfoques , los perfiles y las plantillas de revisión personalizadas existentes, puede aplicar etiquetas a través de la pestaña Descripción general.

Si utiliza la API de AWS WA Tool, la AWS CLI o un SDK de AWS, puede aplicar etiquetas a los recursos nuevos mediante el parámetro de `tags` en la acción de la API pertinente o utilizar la acción de la API de `TagResource` para aplicar etiquetas a los recursos existentes. Para obtener más información, consulte TagResource.

Además, algunas acciones de creación de recursos le permiten especificar etiquetas para un recurso al crearlo. Si no se pueden aplicar etiquetas durante la creación del recurso, el proceso de creación de recursos falla. Esto garantiza que los recursos que pretendía etiquetar en el momento de su creación se creen con etiquetas específicas o no se creen en absoluto. Si etiqueta recursos en el momento de su creación, no es necesario ejecutar scripts de etiquetado personalizados después de la creación del recurso.

En la tabla siguiente se describen los recursos de AWS WA Tool que se pueden etiquetar y aquellos que se pueden etiquetar en el momento de su creación.

Compatibilidad con el etiquetado de recursos de AWS WA Tool

Recurso	Admite etiquetas	Admite la propagación de etiquetas	Admite el etiquetado durante la creación (API de AWS WA Tool, AWS CLI y SDK de AWS)
Cargas de trabajo de AWS WA Tool	Sí	No	Sí

Recurso	Admite etiquetas	Admite la propagación de etiquetas	Admite el etiquetado durante la creación (API de AWS WA Tool, AWS CLI y SDK de AWS)
Enfoques personalizados de AWS WA Tool	Sí	No	Sí
Perfiles de AWS WA Tool	Sí	No	Sí
Plantillas de revisión de AWS WA Tool	Sí	No	Sí

Restricciones de las etiquetas

Se aplican las siguientes restricciones básicas a las etiquetas:

- Número máximo de etiquetas por recurso: 50
- Para cada recurso, cada clave de etiqueta debe ser única y solo puede tener un valor.
- Longitud máxima de la clave: 128 caracteres Unicode en UTF-8
- Longitud máxima del valor: 256 caracteres Unicode en UTF-8
- Si se utiliza su esquema de etiquetado en múltiples servicios y recursos de AWS, recuerde que otros servicios pueden tener restricciones sobre caracteres permitidos. Los caracteres permitidos generalmente son: letras, números y espacios representables en UTF-8, además de los siguientes caracteres: + - = . _ : / @.
- Las claves y los valores de las etiquetas distinguen entre mayúsculas y minúsculas.
- No utilice `aws:`, `AWS:` ni ninguna combinación de mayúsculas o minúsculas del mismo como prefijo para claves o valores, ya que está reservado para uso de AWS. Las claves y valores de etiquetas que tienen este prefijo no se pueden editar. Las etiquetas que tengan este prefijo no cuentan para el límite de etiquetas por recurso.

Uso de etiquetas mediante la consola

Con la consola de AWS WA Tool puede administrar las etiquetas asociadas a los recursos nuevos o existentes.

Adición de etiquetas a un recurso individual durante su creación

Puede agregar etiquetas a los recursos de AWS WA Tool cuando los crea.

Adición y eliminación de etiquetas en un recurso individual

AWS WA Tool le permite añadir o eliminar las etiquetas asociadas a sus recursos directamente desde la pestaña Propiedades para una carga de trabajo y desde la pestaña Información general para enfoques, plantillas de revisión y perfiles personalizados.

Para agregar o eliminar una etiqueta en una carga de trabajo

1. Inicie sesión en AWS Management Console y abra la consola de AWS Well-Architected Tool en https://console.aws.amazon.com/wellarchitected/.
2. En la barra de navegación, elija la región a utilizar.
3. En el panel de navegación izquierdo, elija Cargas de trabajo.
4. Seleccione la carga de trabajo que desea modificar y elija Propiedades.
5. En la sección Etiquetas, elija Administrar etiquetas.
6. Agregue o elimine sus etiquetas según sea necesario.
   - Para agregar una etiqueta, elija Agregar nueva etiqueta y, a continuación, ingrese la Clave y el Valor.
   - Para eliminar una etiqueta, elija Eliminar.
7. Repita este proceso para cada etiqueta que desee agregar, modificar o eliminar. Elija Guardar para guardar los cambios.

Para agregar o eliminar una etiqueta en un enfoque personalizado

1. Inicie sesión en AWS Management Console y abra la consola de AWS Well-Architected Tool en https://console.aws.amazon.com/wellarchitected/.
2. En la barra de navegación, elija la región a utilizar.
3. En el panel de navegación, elija Enfoques personalizados.

4. Seleccione el nombre del enfoque personalizado que desea modificar.
5. En la sección Etiquetas de la pestaña Descripción general, elija Administrar etiquetas.
6. Agregue o elimine sus etiquetas según sea necesario.
   - Para agregar una etiqueta, elija Agregar nueva etiqueta y, a continuación, ingrese la Clave y el Valor.
   - Para eliminar una etiqueta, elija Eliminar.
7. Repita este proceso para cada etiqueta que desee agregar, modificar o eliminar. Elija Guardar para guardar los cambios.

Para agregar o eliminar una etiqueta en un perfil

1. Inicie sesión en AWS Management Console y abra la consola de AWS Well-Architected Tool en https://console.aws.amazon.com/wellarchitected/.
2. En la barra de navegación, elija la región a utilizar.
3. En el panel de navegación, elija Perfiles.
4. Seleccione el nombre del perfil que desea modificar.
5. En la sección Etiquetas de la pestaña Descripción general, elija Administrar etiquetas.
6. Agregue o elimine sus etiquetas según sea necesario.
   - Para agregar una etiqueta, elija Agregar nueva etiqueta y, a continuación, ingrese la Clave y el Valor.
   - Para eliminar una etiqueta, elija Eliminar.
7. Repita este proceso para cada etiqueta que desee agregar, modificar o eliminar. Elija Guardar para guardar los cambios.

Para agregar o eliminar una etiqueta en una plantilla de revisión

1. Inicie sesión en AWS Management Console y abra la consola de AWS Well-Architected Tool en https://console.aws.amazon.com/wellarchitected/.
2. En la barra de navegación, elija la región a utilizar.
3. En el panel de navegación, elija Plantillas de lanzamiento.
4. Seleccione el nombre de la plantilla de revisión que desea modificar.
5. En la sección Etiquetas de la pestaña Descripción general, elija Administrar etiquetas.

6. Agregue o elimine sus etiquetas según sea necesario.
   - Para agregar una etiqueta, elija Agregar nueva etiqueta y, a continuación, ingrese la Clave y el Valor.
   - Para eliminar una etiqueta, elija Eliminar.
7. Repita este proceso para cada etiqueta que desee agregar, modificar o eliminar. Elija Guardar para guardar los cambios.

Uso de etiquetas mediante la API

Utilice las siguientes operaciones de la API de AWS WA Tool para agregar, actualizar, enumerar y eliminar las etiquetas de sus recursos.

Compatibilidad con el etiquetado de recursos de AWS WA Tool

Tarea	Acción de la API
Agregar o sobrescribir una o varias etiquetas.	TagResource
Eliminar una o varias etiquetas.	UntagResource
Enumera las etiquetas de un recurso.	ListTagsForResource

Algunas acciones de creación de recursos le permiten especificar etiquetas al crear el recurso. Las siguientes acciones admiten etiquetado durante la creación.

Tarea	Acción de la API
Creación de una carga de trabajo	CreateWorkload
Importar un nuevo enfoque	Importar enfoque
Creación de un perfil	Crear perfil
Crear una plantilla de revisión	CreateReviewTemplate

Registro de llamadas a la API de AWS WA Tool con AWS CloudTrail

AWS Well-Architected Tool 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 WA Tool. CloudTrail captura todas las llamadas a la API de AWS WA Tool como eventos. Las llamadas capturadas incluyen las llamadas desde la consola de AWS WA Tool y las llamadas desde el código a las operaciones de la API de AWS WA Tool. 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 WA Tool. Si no configura un registro de seguimiento, puede ver los eventos más recientes en la consola de CloudTrail en el Historial de eventos. Mediante la información recopilada por CloudTrail, puede determinar la solicitud que se realizó a AWS WA Tool, la dirección IP desde la que se realizó, quién la realizó y cuándo, etc.

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

Información de AWS WA Tool en CloudTrail

CloudTrail se habilita en su Cuenta de AWS cuando se crea la cuenta. Cuando se produce actividad en AWS WA Tool, dicha 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 eventos recientes en su 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 WA Tool, 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 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

- Recepción de archivos de registro de CloudTrail de varias regiones y Recepción de archivos de registro de CloudTrail de varias cuentas

CloudTrail registra todas las acciones de AWS WA Tool y se documentan en Acciones definidas por AWS Well-Architected Tool. Por ejemplo, las llamadas a las acciones `CreateWorkload`, `DeleteWorkload` y `CreateWorkloadShare` generan entradas en los archivos de registro de CloudTrail.

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

- Si la solicitud se realizó con las credenciales del usuario o 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 WA Tool

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

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

```
   {
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE:dev-dsk-xiulan-2a-1111111c.us-
west-2.amazon.com",
```

```
        "arn": "arn:aws:sts::444455556666:assumed-role/well-architected-api-svc-integ-
test-read-write/dev-dsk-xiulan-2a-1111111c.us-west-2.amazon.com",
        "accountId": "444455556666",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AIDACKCEVSQ6C2EXAMPLE",
                "arn": "arn:aws:iam::444455556666:role/well-architected-api-svc-integ-
test-read-write",
                "accountId": "444455556666",
                "userName": "well-architected-api-svc-integ-test-read-write"
            },
            "webIdFederationData": {},
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2020-10-14T03:41:39Z"
            }
        }
    },
    "eventTime": "2020-10-14T04:43:13Z",
    "eventSource": "wellarchitected.amazonaws.com",
    "eventName": "CreateWorkload",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "198.51.100.178",
    "userAgent": "aws-internal/3 aws-sdk-java/1.11.848
 Linux/4.9.217-0.1.ac.205.84.332.metal1.x86_64 OpenJDK_64-Bit_Server_VM/25.262-b10
 java/1.8.0_262 vendor/Oracle_Corporation",
    "requestParameters": {
           "ClientRequestToken": "08af866a-0238-4070-89c2-b689ca8339f7",
           "Description": "***",
           "AwsRegions": [
               "us-west-2"
           ],
           "ReviewOwner": "***",
           "Environment": "PRODUCTION",
           "Name": "***",
           "Lenses": [
               "wellarchitected",
               "serverless"
           ]
    },
    "responseElements": {
```

```
        "Arn": "arn:aws:wellarchitected:us-
west-2:444455556666:workload/8cdcdf7add10b181fdd3f686dacffdac",
        "Id": "8cdcdf7add10b181fdd3f686dacffdac"
    },
    "requestID": "22bad4e3-aa51-4ff1-b480-712ee07cedbd",
    "eventID": "50849dfd-36ed-418e-a901-49f6ac7087e8",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "recipientAccountId": "444455556666"
}
```

EventBridge

AWS Well-Architected Tool envía eventos a Amazon EventBridge cuando se toman medidas en recursos de Well-Architected. Puede utilizar EventBridge y estos eventos para registrar reglas que realicen acciones, como enviar una notificación cuando una alarma cambie de estado. Para obtener más información, consulte What is Amazon EventBridge? (¿Qué es Amazon EventBridge?).

> **Note**
>
> Los eventos se entregan según el «mejor esfuerzo», es decir, en la medida que sea posible.

Las siguientes acciones dan lugar a eventos de EventBridge:

- Relacionado con carga de trabajo
  - Crear o eliminar una carga de trabajo
  - Crear un hito
  - Actualizar las propiedades de una carga de trabajo
  - Compartir o dejar de compartir una carga de trabajo
  - Actualizar el estado de una invitación para compartir
  - Cómo añadir y eliminar etiquetas
  - Actualizar una respuesta
  - Actualizar notas de revisión
  - Añadir o quitar un enfoque de una carga de trabajo
- Relacionado con enfoques
  - Importar o exportar un enfoque personalizado
  - Publicar un enfoque personalizado
  - Eliminar un enfoque personalizado
  - Compartir o dejar de compartir un enfoque personalizado
  - Actualizar el estado de una invitación para compartir
  - Añadir o quitar un enfoque de una carga de trabajo

Ejemplos de eventos de AWS WA Tool

En esta sección se incluyen eventos de ejemplo de AWS Well-Architected Tool.

Actualizar una respuesta en una carga de trabajo


```
{
  "version":"0",
  "id":"00de336a-83cc-b80b-f0e6-f44c88a96050",
  "detail-type":"AWS API Call via CloudTrail",
  "source":"aws.wellarchitected",
  "account":"123456789012",
  "time":"2022-02-17T08:01:25Z",
  "region":"us-west-2",
  "resources":[],
  "detail":{
     "eventVersion":"1.08",
     "userIdentity":{
        "type":"AssumedRole",
        "principalId":"AROA4JUSXMN5ZR6S7LZNP:sample-user",
        "arn":"arn:aws:sts::123456789012:assumed-role/Admin/example-user",
        "accountId":"123456789012",
        "accessKeyId":"AKIAIOSFODNN7EXAMPLE",
        "sessionContext":{
           "sessionIssuer":{
              "type":"Role",
              "principalId":"AROA4JUSXMN5ZR6S7LZNP",
              "arn":"arn:aws:iam::123456789012:role/Admin",
              "accountId":"123456789012",
              "userName":"Admin"
           },
           "webIdFederationData":{},
           "attributes":{
              "creationDate":"2022-02-17T07:21:54Z",
              "mfaAuthenticated":"false"
           }
        }
     },
     "eventTime":"2022-02-17T08:01:25Z",
     "eventSource":"wellarchitected.amazonaws.com",
     "eventName":"UpdateAnswer",
     "awsRegion":"us-west-2",
```

```
      "sourceIPAddress":"10.246.162.39",
      "userAgent":"aws-internal/3 aws-sdk-java/1.12.127
 Linux/5.4.156-94.273.amzn2int.x86_64 OpenJDK_64-Bit_Server_VM/25.312-b07
 java/1.8.0_312 vendor/Oracle_Corporation cfg/retry-mode/standard",
      "requestParameters":{
         "Status":"Acknowledged",
         "SelectedChoices":"***",
         "ChoiceUpdates":"***",
         "QuestionId":"priorities",
         "WorkloadId":"ee73fda518f9bd4aa804c6252e4e37b0",
         "IsApplicable":true,
         "LensAlias":"wellarchitected",
         "Reason":"NONE",
         "Notes":"***"
      },
      "responseElements":{
         "Answer":"***",
         "LensAlias":"wellarchitected",
         "WorkloadId":"ee73fda518f9bd4aa804c6252e4e37b0"
      },
      "requestID":"7bae1153-26a8-4dc0-9307-68b17b107619",
      "eventID":"8339c258-4ddd-48aa-ab21-3f82ce9d79cd",
      "readOnly":false,
      "eventType":"AwsApiCall",
      "managementEvent":true,
      "recipientAccountId":"123456789012",
      "eventCategory":"Management"
   }
}
```


Publicar un enfoque personalizado


```
{
   "version":"0",
   "id":"4054a34b-60a9-53c1-3146-c1a384dba41b",
   "detail-type":"AWS API Call via CloudTrail",
   "source":"aws.wellarchitected",
   "account":"123456789012",
   "time":"2022-02-17T08:58:34Z",
   "region":"us-west-2",
   "resources":[],
```

```
   "detail":{
      "eventVersion":"1.08",
      "userIdentity":{
         "type":"AssumedRole",
         "principalId":"AROA4JUSXMN5ZR6S7LZNP:example-user",
         "arn":"arn:aws:sts::123456789012:assumed-role/Admin/example-user",
         "accountId":"123456789012",
         "accessKeyId":"AKIAIOSFODNN7EXAMPLE",
         "sessionContext":{
            "sessionIssuer":{
               "type":"Role",
               "principalId":"AROA4JUSXMN5ZR6S7LZNP",
               "arn":"arn:aws:iam::123456789012:role/Admin",
               "accountId":"123456789012",
               "userName":"Admin"
            },
            "webIdFederationData":{},
            "attributes":{
               "creationDate":"2022-02-17T07:21:54Z",
               "mfaAuthenticated":"false"
            }
         }
      },
      "eventTime":"2022-02-17T08:58:34Z",
      "eventSource":"wellarchitected.amazonaws.com",
      "eventName":"CreateLensVersion",
      "awsRegion":"us-west-2",
      "sourceIPAddress":"10.246.162.39",
      "userAgent":"aws-internal/3 aws-sdk-java/1.12.127
 Linux/5.4.156-94.273.amzn2int.x86_64 OpenJDK_64-Bit_Server_VM/25.312-b07
 java/1.8.0_312 vendor/Oracle_Corporation cfg/retry-mode/standard",
      "requestParameters":{
         "IsMajorVersion":true,
         "LensVersion":"***",
         "ClientRequestToken":"03f46163-e95c-4455-8479-266373aa09c7",
         "LensAlias":"***"
      },
      "responseElements":{
         "LensArn":"arn:aws:wellarchitected:us-
west-2:123456789012:lens/6261deecb9def44f9aecc938ca25d94e",
         "LensVersion":"***"
      },
      "requestID":"167b7051-980d-42ee-9967-0b4b3163e948",
      "eventID":"c7ef2b47-419d-45b7-8982-fbade9b558c7",
```

```
      "readOnly":false,
      "eventType":"AwsApiCall",
      "managementEvent":true,
      "recipientAccountId":"123456789012",
      "eventCategory":"Management"
   }
}
```

Historial del documento

En la siguiente tabla se describe la documentación de esta versión de la AWS Well-Architected Tool.

- Versión de la API: la más reciente
- Última actualización de la documentación: 17 de abril de 2025

Cambio	Descripción	Fecha
Lente nueva	Esta versión ha agregado una lente nueva al Catálogo de lentes.	17 de abril de 2025
Enfoques nuevos y actualizados	Esta versión agregó un enfoque nuevo al Catálogo de enfoques y actualizó otro enfoque.	27 de junio de 2024
Jira	Esta versión agregó el conector de AWS Well-Architected Tool para Jira.	16 de abril de 2024
Enfoques nuevos	Esta versión agregó nuevos enfoques al Catálogo de enfoques.	26 de marzo de 2024
Funcionalidad actualizada	Esta versión agrega la característica del catálogo de enfoques a AWS WA Tool.	26 de noviembre de 2023
Funcionalidad actualizada	Esta versión añade la característica Revisar plantillas a AWS WA Tool.	3 de octubre de 2023
Actualización de política administrada por WellArchitectedConsoleAdOnlyAccess	Se agregó `"wellarchitected:ExportLens"`	22 de junio de 2023

	a `WellArchitectedConsoleReadOnlyAccess` .	
Funcionalidad actualizada	Esta versión añade la característica Perfiles a AWS WA Tool.	13 de junio de 2023
Funcionalidad actualizada	Esta versión mejora la integración de AWS Trusted Advisor y AWS Service Catalog AppRegistry, y la añade `AWSWellArchitectedDiscoveryServiceRolePolicy` a las políticas administradas de AWS.	3 de mayo de 2023
Actualización del contenido	Se actualizó la página del panel para incluir información detallada sobre los riesgos y el plan de mejora. También se agregó la posibilidad de crear un informe consolidado de la carga de trabajo.	30 de marzo de 2023
Actualización del contenido	Se ha corregido el nombre de la política WellArchitectedConsoleReadOnlyAccess.	19 de enero de 2023
Se ha actualizado la guía de IAM para AWS WA Tool	Guía modificada para implementar las prácticas recomendadas de IAM. Para obtener más información, consulte Prácticas recomendadas de seguridad en IAM.	4 de enero de 2023
Funcionalidad actualizada	Esta versión quita el enfoque FTR de la herramienta.	14 de diciembre de 2022

Funcionalidad actualizada	Esta versión añade la integración de AWS Trusted Advisor y AWS Service Catalog AppRegistry.	7 de noviembre de 2022
Actualización del contenido	Se ha corregido un problema en el ejemplo de JSON de enfoque personalizado para `choices`.	29 de septiembre de 2022
Actualización del contenido	Se actualizó la sección `choices` de la especificación JSON de enfoque personalizado.	2 de agosto de 2022
Funcionalidad actualizada	Esta versión añade el seguimiento de los cambios en sus políticas administradas de AWS y ha añadido una nueva acción para conceder el permiso `ListAWSServiceAccessForOrganization` a `AWSWellArchitectedOrganizationsServiceRolePolicy`.	22 de julio de 2022
Se agregó el uso compartido de organizaciones	Esta versión añade la posibilidad de compartir cargas de trabajo y enfoques personalizados con una organización y unidades organizativas (OU).	30 de junio de 2022

Funcionalidad actualizada	Esta versión añade la posibilidad de especificar recursos adicionales para las opciones de un enfoque personalizado, previsualizar un enfoque personalizado antes de publicarla y añadir etiquetas a los enfoques personalizados.	21 de junio de 2022
Funcionalidad actualizada	Esta versión añade la posibilidad de acceder a la comunidad de AWS Well-Architected en AWS Re:post.	31 de mayo de 2022
Funcionalidad actualizada	Esta versión añade el pilar de la sostenibilidad y pequeñas actualizaciones al Tutorial.	31 de marzo de 2022
Compatibilidad con EventBridge añadida	AWS WA Tool envía ahora un evento a Amazon EventBridge cuando se realiza un cambio en un recurso de Well-Architected.	3 de marzo de 2022
Funcionalidad actualizada	Las mejores prácticas individuales ahora se pueden marcar como no aplicables.	14 de julio de 2021
Etiquetado de recursos disponible	Esta versión añade la posibilidad de añadir etiquetas a las cargas de trabajo.	3 de marzo de 2021
API está ahora disponible	En esta versión se añade la API de AWS WA Tool. AWS CloudTrail se agregó información de registro.	16 de diciembre de 2020

Funcionalidad actualizada	Esta versión añade los enfoques FTR y SaaS a la herramienta.	3 de diciembre de 2020
Protección de datos actualizada	Información de protección de datos actualizada.	5 de noviembre de 2020
Actualización del contenido	Se ha aclarado que, tras actualizar una carga de trabajo para utilizar un enfoque nuevo, no se puede volver a la versión anterior.	8 de julio de 2020
Actualización del contenido	Se aclaró el uso compartido y Regiones de AWS se introdujo después del 20 de marzo de 2019.	24 de junio de 2020
Funcionalidad actualizada	El acceso a un recurso compartido de carga de trabajo se elimina inmediatamente cuando se rechaza una invitación de recurso compartido de carga de trabajo. El acceso compartido se concede cuando se acepta el recurso compartido.	17 de junio de 2020
Actualización del contenido	Se han agregado definiciones para los problemas de alto riesgo y los problemas de riesgo medio.	12 de junio de 2020
Actualización del contenido	Se ha agregado una sección acerca de cómo utiliza sus datos AWS.	21 de mayo de 2020

Funcionalidad actualizada	En esta versión se agrega un propietario de la revisión a la carga de trabajo.	1 de abril de 2020
Funcionalidad actualizada	Esta versión añade un enlace de diagrama arquitectónico a la carga de trabajo.	10 de marzo de 2020
Actualización del contenido	Se ha aclarado que los recursos compartidos de la carga de trabajo son específicos de la región de Región de AWS.	10 de enero de 2020
Funcionalidad actualizada	Esta versión agrega el uso compartido de la carga de trabajo.	9 de enero de 2020
Actualización del contenido	La sección de seguridad se ha actualizado con las últimas directrices.	6 de diciembre de 2019
Funcionalidad actualizada	En esta versión, los campos relacionados con el sector son opcionales cuando se define una carga de trabajo.	19 de agosto de 2019
Funcionalidad actualizada	Esta versión añade elementos de plan de mejoras al informe de carga de trabajo.	29 de julio de 2019
Funcionalidad actualizada	La versión añade la acción DeleteWorkload a la política.	18 de julio de 2019
Actualización del contenido	El contenido de esta guía se ha actualizado con correcciones menores.	19 de junio de 2019

Actualización del contenido	El contenido de esta guía se ha actualizado con correcciones menores.	30 de mayo de 2019
Funcionalidad actualizada	Esta versión es compatible con la actualización de la versión del marco utilizada para una revisión de carga de trabajo.	1 de mayo de 2019
Funcionalidad actualizada	Esta versión incorpora la posibilidad de especificar regiones que no pertenecen a Regiones de AWS al definir una carga de trabajo.	14 de febrero de 2019
Disponibilidad general de AWS Well-Architected Tool	Esta versión presenta AWS Well-Architected Tool.	29 de noviembre de 2018

Glosario de AWS

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