

Guía del usuario

AWS Well-Architected Tool



AWS Well-Architected Tool: Guía del usuario

Copyright © 2024 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

.....	vii
¿Qué es AWS Well-Architected Tool?	1
El AWS Well-Architected Framework	2
Definiciones	2
Introducción	4
Proporcionar acceso a AWS WA Tool	4
Activar las integraciones	5
Activando AppRegistry	6
Activando Trusted Advisor	6
Definir una carga de trabajo	14
Documentación de una carga de trabajo	17
Revise la página de carga de trabajo	18
Trusted Advisor cheques	19
Guardar un hito	21
Tutorial	23
Paso 1: Definir una carga de trabajo	23
Paso 2: Documentar el estado de la carga de trabajo	24
Paso 3: Revisar el plan de mejora	28
Paso 4: Realizar mejoras y medir el progreso	30
Cargas de trabajo	32
Problemas de alto riesgo y problemas de riesgo medio	33
Definir una carga de trabajo	34
Visualizar una carga de trabajo	35
Editar una carga de trabajo	35
Compartir una carga de trabajo	36
Consideraciones para compartir	39
Eliminar acceso compartido	40
Modificar el acceso compartido	40
Aceptar y rechazar invitaciones a cargas de trabajo	41
Eliminar una carga de trabajo	42
Generación de un informe de carga de trabajo	42
Detalles de la carga de trabajo	43
Pestaña Información general	44
Hitos	44

Pestaña Propiedades	44
Pestaña Recursos compartidos	45
Enfoques	47
Agregar un enfoque	47
Eliminación de un enfoque	48
Detalles del enfoque	48
Pestaña Información general	48
Pestaña Plan de mejora	49
Pestaña Recursos compartidos	49
Enfoques personalizados	49
Visualización de enfoques personalizados	50
Crear un enfoque	51
Vista previa de un enfoque	52
Publicar un enfoque	53
Publicar una actualización de enfoque	53
Compartir un enfoque	55
Añadir etiquetas a un enfoque	57
Eliminar un enfoque	57
Especificación del formato del enfoque	58
Actualización de enfoques	65
Selección de la actualización de enfoque	65
Actualización del enfoque	66
Catálogo de enfoques	68
Plantillas de revisión	71
Crear una plantilla de revisión	71
Editar una plantilla de revisión	72
Compartir una plantilla de revisión	73
Definir una carga de trabajo a partir de una plantilla	74
Eliminar una plantilla de revisión	75
Perfiles	77
Crear un perfil	77
Editar un perfil	78
Compartir un perfil	78
Añadir un perfil a una carga de trabajo	79
Eliminar un perfil de una carga de trabajo	79
Eliminar un perfil	80

Jira	82
Configuración del conector	83
Configuración del conector de	84
Sincronizar una carga de trabajo	87
Desinstalar el conector	87
Hitos	90
Guardar un hito	90
Visualización de hitos	90
Generación de un informe de hitos	91
Compartir invitaciones	92
Aceptar una invitación para compartir	93
Rechazar una invitación para compartir	94
Notificaciones	95
Notificaciones de lentes	95
Notificaciones de perfil	95
Panel	97
Resumen	97
Problemas de Well-Architected Framework por pilar	97
Problemas de Well-Architected Framework por carga de trabajo	98
Problemas de Well-Architected Framework por elemento del plan de mejora	99
Seguridad	101
Protección de datos	102
Cifrado en reposo	103
Cifrado en tránsito	103
¿Cómo AWS utiliza sus datos	103
Administración de identidades y accesos	104
Público	104
Autenticación con identidades	105
Administración de acceso mediante políticas	109
¿Cómo AWS Well-Architected Tool funciona con IAM	111
Ejemplos de políticas basadas en identidades	119
AWS políticas gestionadas	126
Resolución de problemas	132
Respuesta frente a incidencias	133
Validación de conformidad	133
Resiliencia	134

Seguridad de la infraestructura	135
Configuración y análisis de vulnerabilidades	135
Prevención de la sustitución confusa entre servicios	136
Compartir los recursos	138
Activar el uso compartido de recursos en AWS Organizations	138
Etiquetar sus recursos	141
Conceptos básicos de etiquetas	141
Etiquetar los recursos	142
Restricciones de las etiquetas	143
Uso de etiquetas mediante la consola	144
Adición de etiquetas a un recurso individual durante su creación	144
Adición y eliminación de etiquetas en un recurso individual	144
Uso de etiquetas mediante la API	146
Registro	147
Información de AWS WA Tool en CloudTrail	147
Descripción de las entradas de los archivos de registro de AWS WA Tool	148
EventBridge	151
Ejemplos de eventos de AWS WA Tool	152
Historial de documentos	156
Glosario de AWS	163

Puedes usar el AWS Well-Architected Tool conector para Jira para vincular tu cuenta de Jira y sincronizar los elementos de mejora entre tus cargas de trabajo y los proyectos de Jira. AWS Well-Architected Tool

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

¿Qué es 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:

- 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 AWS Well-Architected Framework. 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 lentes personalizadas 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 lentes personalizadas amplían la orientación proporcionada por las lentes 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 Well-Architected.

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

- [El AWS Well-Architected Framework](#)

- [Definiciones](#)

El AWS Well-Architected Framework

El [AWS Well-Architected Framework](#) 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](#).

Definiciones

En AWS WA Tool y el AWS Well-Architected Framework:

- 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.
- Las lentes 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 las lentes proporcionadas por AWS, también puede crear y usar sus propias lentes o usar las lentes 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](#).

Empezar con AWS Well-Architected Tool

En esta sección se describe cómo empezar con AWS WA Tool.

Temas

- [Proporcionar a los usuarios, grupos o roles acceso a AWS WA Tool](#)
- [Activar la compatibilidad con otros servicios de AWS](#)
- [Definir una carga de trabajo](#)
- [Documentación de una carga de trabajo](#)
- [Guardar un hito](#)

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

En este paso, concedes acceso a AWS WA Tool.

Proporcione 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 descritas en [Crear un conjunto de permisos](#) en la Guía del usuario de AWS IAM Identity Center .

- Usuarios administrados 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.

El acceso total permite al director realizar todas las acciones en él 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 [AWS políticas gestionadas para AWS Well-Architected Tool](#).

Activar la compatibilidad con otros servicios de AWS

La activación del acceso AWS WA Tool a la organización permite 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 compatibilidad con Activation Discovery recopila información de [AWS Trusted Advisor](#) los recursos relacionados y los recursos relacionados (como las AWS CloudFormation pilas de colecciones de AppRegistry recursos) para ayudarlo a descubrir más fácilmente la información necesaria para responder a las preguntas de revisión de Well-Architected y adaptar las comprobaciones a una carga de trabajo. [AWS Service Catalog AppRegistry](#) Trusted Advisor

Al activar o activar el soporte para Discovery AWS Organizations, se crea automáticamente un rol vinculado al servicio para su cuenta.

Para activar la compatibilidad con otros servicios con los que AWS WA Tool puedes interactuar, ve a Configuración.

1. Para recopilar información AWS Organizations, activa Activar el AWS Organizations soporte.
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.

Activación AppRegistry para una carga de trabajo

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

Siempre que la compatibilidad con Discovery esté activada y AppRegistry esté asociada a una carga de trabajo nueva o existente, se AWS WA Tool crea un grupo de atributos gestionados por el servicio. El grupo de atributos Metadatos 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 AppRegistry aplicación gestione los datos obtenidos Trusted Advisor, defina la definición de recursos de la carga de trabajo como Todos AppRegistry todos. 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”](#).

Activación AWS Trusted Advisor para una carga de trabajo

La integración con AWS Trusted Advisor es opcional y se puede activar por carga de trabajo para los clientes de AWS Business y Enterprise Support. La integración Trusted Advisor no tiene ningún costo AWS WA Tool, pero para obtener detalles sobre Trusted Advisor los precios, consulte [AWS Support Plans](#).

Activar Trusted Advisor para una carga de trabajo

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

Account IDs - optional
Type the IDs of the AWS accounts your workload spans across

111122223333

Specify up to 100 unique account IDs separated by commas

Application - optional [Info](#)
An application is a custom collection of resources, metadata, and tags that performs a function to deliver business value. Your application's Amazon Resource Name (ARN) is a unique identifier for an AWS resource, which is maintained by AppRegistry.

arn:aws:servicecatalog:us-west-2:111122223333/application/#####

Architectural design - optional
A link to your architectural design

The URL can be up to 2048 characters and must begin with one of the follow protocols: [http, https, ftp]. 2048 characters remaining

Industry type - optional
The industry that your workload is associated with

Choose an industry type

Industry - optional
The category within your industry that your workload is associated with

Choose a industry

AWS Trusted Advisor - new

AWS Trusted Advisor [Info](#)
Trusted Advisor uses information from your AWS Regions and account IDs entered above to aid workload reviews, providing you automated context for supported questions.

Activate Trusted Advisor

Resource definition
Choose how resources are selected for Trusted Advisor checks.

AppRegistry

 **Additional setup needed**
To pull Trusted Advisor data from other accounts, grant permissions to the AWS Well-Architected Tool to access Trusted Advisor data.

View AWS documentation 

Trusted Advisor checks ×

AWS Trusted Advisor provides recommendations that help you follow AWS best practices. Trusted Advisor evaluates your account by using checks. These checks identify ways to optimize your AWS infrastructure, improve security and performance, reduce costs, and monitor service quotas. You can then follow the recommendations to optimize your services and resources. Activating Trusted Advisor support aids workload reviews by providing automated context for supported questions.

[Trusted Advisor documentation](#) 

4. La primera vez Trusted Advisor que se activa 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 o AppRegistryTodos. La selección de definiciones de recursos define de qué se AWS WA Tool obtienen los datos 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 identificadores de cuenta y se Regiones de AWS especifica en la carga de trabajo.

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

Todo: la carga de trabajo se define mediante los metadatos y los AppRegistry recursos de la carga de trabajo.

6. Elija Siguiente.
7. Aplique AWS Well-Architected Framework a su carga de trabajo y elija Definir carga de trabajo. Trusted Advisor los controles solo están vinculados al AWS Well-Architected Framework y no a otros lentes.

AWS WA Tool Periódicamente obtiene datos del Trusted Advisor uso de las funciones creadas 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, no AWS WA Tool puede obtener Trusted Advisor información sobre esa cuenta y muestra un error.

Para obtener más información sobre la creación de un rol en AWS Identity and Access Management (IAM), consulte [Crear un rol para un AWS servicio \(consola\)](#) en la Guía del usuario de IAM.

Activación Trusted Advisor para una carga de trabajo en IAM

Note

Los propietarios de las cargas de trabajo deben activar el soporte de Discovery para sus cuentas antes de crear una Trusted Advisor carga de trabajo. 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 se hayan activado Trusted Advisor deben crear un rol en IAM para poder ver la Trusted Advisor información. AWS WA Tool

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

1. Inicie sesión en la consola de IAM AWS Management Console y ábrala en. <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/*"
        }
      }
    }
  ]
}
```

Custom trust policy

Create a custom trust policy to enable others to perform actions in this account.

```

1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Effect": "Allow",
6       "Principal": {
7         "Service": "wellarchitected.amazonaws.com"
8       },
9       "Action": "sts:AssumeRole",
10      "Condition": {
11        "StringEquals": {
12          "aws:SourceAccount": "111122223333"
13        },
14        "ArnEquals": {
15          "aws:SourceArn": "arn:aws:wellarchitected:*:111122223333:workload/*"
16        }
17      }
18    }
19  ]
20 }

```

Edit statement Remove

1. Add actions for STS

Q Filter actions

All actions (sts:)

Access level - read or write

AssumeRole ⓘ

AssumeRoleWithSAML ⓘ

AssumeRoleWithWebIdentity ⓘ

DecodeAuthorizationMessage ⓘ

GetAccessKeyInfo ⓘ

GetCallerIdentity ⓘ

GetFederationToken ⓘ

GetServiceBearerToken ⓘ

GetSessionToken ⓘ

SetSourceIdentity ⓘ

2. Add a principal Add

3. Add a condition (optional) Add

+ Add new statement

JSON Ln 12, Col 3

Security: 0 Errors: 0 Warnings: 0 Suggestions: 0 Preview external access

Cancel Next

Note

El `aws:sourceArn` 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 esta función puede ser utilizada por el propietario de la carga de trabajo 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 Añadir permisos, en las políticas de permisos, selecciona Crear política para dar AWS WA Tool acceso a los datos de lectura. 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/*"
    ]
  }
]
}

```

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

```

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

```

- (Opcional) Agregue 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 desactivarla Trusted Advisor para cualquier carga de trabajo AWS WA Tool editando su carga de trabajo y deseleccionando Activar. Trusted Advisor Para obtener más información sobre editar cargas de trabajo, consulte [the section called “Editar una carga de trabajo”](#).

La desactivación Trusted Advisor desde AWS WA Tool no elimina las funciones creadas 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 las funciones de IAM creadas al Trusted Advisor desactivarlas o dejar de recopilar Trusted Advisor datos para la carga AWS WA Tool de trabajo. AWS WA Tool

Eliminar el **WellArchitectedRoleForTrustedAdvisor** en IAM

1. Inicie sesión en la consola de IAM AWS Management Console y ábrala en. <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.

Definir una carga de trabajo

El siguiente paso consiste en definir una carga de trabajo.

Para definir una carga de trabajo

1. Inicie sesión en la AWS Well-Architected Tool consola AWS Management Console y ábrala en <https://console.aws.amazon.com/wellarchitected/>.
2. Si es la primera vez que lo utilizas AWS WA Tool, verás una página en la que se presentan las funciones 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 se AWS utilizan los datos de la carga de trabajo, selecciona ¿Por qué se AWS necesitan 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 Regiones de AWS dónde se ejecuta su carga de trabajo, de uno en uno.
- No AWS regiones: introduzca los nombres de las regiones fuera de AWS donde se ejecuta su 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, cualquier ID de cuenta especificado se utilizará para obtener datos Trusted Advisor. Consulte [Activar AWS Trusted Advisor una carga de trabajo](#) para conceder AWS WA Tool permisos para obtener Trusted Advisor datos 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 "Activando Trusted Advisor"](#) esta sección para conceder AWS WA Tool permisos para obtener Trusted Advisor datos en su nombre. Seleccione entre Metadatos de carga de trabajo o Todos en Definición de recurso para definir qué recursos se AWS WA Tool utilizan para ejecutar las Trusted Advisor comprobaciones. AppRegistry
14. (Opcional) En la sección Jira, para activar la configuración de sincronización de Jira a nivel de carga de trabajo para la carga de trabajo, selecciona Anular la configuración a nivel de cuenta. Es posible que se necesite una configuración adicional para las cuentas asociadas a su carga de trabajo. Consulta [AWS Well-Architected Tool Connector para Jira](#) para empezar a instalar y configurar el conector. Seleccione No sincronizar carga de trabajo, Sincronizar carga de trabajo: Manual y Sincronizar carga de trabajo: Automática y, si lo deseas, introduce una clave de proyecto de Jira con la que realizar la sincronización.

Note

Si no anulas 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. Seleccione 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 ver las descripciones de los lentes oficiales, consulte Lentes. AWS](#)

Los lentes se pueden seleccionar entre [lentes personalizados](#) (lentes que has creado o que has compartido contigo Cuenta de AWS), el [catálogo de lentes](#) (lentes AWS oficiales 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 lentes personalizadas creadas por otro AWS usuario o cuenta, usted reconoce que las lentes personalizadas creadas por otros usuarios y compartidas con usted son contenido de terceros, tal como se define en el Acuerdo con el AWS cliente.

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

Después de definir una carga de trabajo, debe documentar su estado.

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.

Para volver a las preguntas, vaya a la página de detalles de la carga de trabajo y seleccione **Continuar revisión**.

Revise la página de carga de trabajo

La página de revisión de la carga de trabajo tiene tres paneles.

The screenshot shows the 'Review workload' page in the AWS Well-Architected Tool. The page is divided into three main panels:

- Panel 1 (Left Sidebar):** A list of prioritized questions. The first question, 'How do you design your workload to adapt to changes in demand?' (REL 1 - prioritized), is highlighted with a red circle '1'. Other questions include 'How do you incorporate and validate the security properties...', 'How do you back up data?', 'How do you implement cloud financial management?', 'How do you evolve your workload to take advantage of new releases?' (PERF 1 - prioritized), 'How do you classify your data?', 'How do you decommission resources?', 'How do you detect and investigate security events?', and 'How do you use fault isolation to protect your workload?'.
- Panel 2 (Main Content Area):** The selected question 'PERF 1. How do you evolve your workload to take advantage of new releases?' is displayed. It includes a notification: 'The answer has been updated based on lens or profile changes.' Below the question, there are 'Trusted Advisor checks' and a list of options to select from: 'Stay up-to-date on new resources and services', 'Evolve workload performance over time', and 'Define a process to improve workload performance'. There is also an option to 'Mark best practice(s) that don't apply to this workload'. A red circle '2' highlights the question title.
- Panel 3 (Right Sidebar):** A 'Helpful resources' section with a link to 'Ask an expert' and a list of links to AWS resources like 'What's New', 'AWS Blog', and various YouTube channels. A red circle '3' highlights the 'Ask an expert' button.

1. 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. [Elige Pregúntale a un experto para acceder a la comunidad AWS Re:post dedicada a Well-Architected AWS](#) . AWS Re:post es una comunidad basada en temas que reemplaza a los foros. question-and-answer 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. [Elige Pregúntale a un experto para acceder a la comunidad AWS Re:post dedicada a Well-Architected AWS](#) . En esta comunidad, puede hacer preguntas relacionadas con el diseño, la creación, la implementación y el funcionamiento de las cargas de trabajo en AWS.

Trusted Advisor cheques

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

The screenshot shows the 'Trusted Advisor checks' tab for the question 'COST 5. How do you evaluate cost when you select services?'. The main content area lists several options for evaluation, such as 'Identify organization requirements for cost' and 'Analyze all components of this workload'. A 'View checks' button is highlighted in a red box. Below the list, a message states 'Trusted Advisor checks available' and provides a link to view more context. The right-hand panel contains helpful resources like 'Cloud products', 'Amazon S3 storage classes', and 'AWS Total Cost of Ownership (TCO) Calculator'.

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

The screenshot shows the 'Trusted Advisor checks' tab for the question 'Best Practice: Select components of this workload to optimize cost in line with organization priorities'. The main content area lists several checks, such as 'Savings Plan', 'Amazon ElastiCache Reserved Node Optimization', and 'Amazon Redshift Reserved Node Optimization', each with a status indicator and a link to view details. A 'Download check details' button is also present. The right-hand panel contains helpful resources like 'Amazon Redshift Reserved Node Optimization' and 'Trusted Advisor checks reference'.

Las categorías de cheques se Trusted Advisor muestran como 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.
- Se recomienda investigar (amarillo): Trusted Advisor detecta un posible problema con la comprobación.
- No se detectó ningún problema (verde): Trusted Advisor no detecta ningún problema en la comprobación.
- 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 que se Trusted Advisor proporcionan, consulte [Ver las categorías de comprobaciones](#) en la Guía del AWS Support usuario.

Al seleccionar el enlace de información situado junto a cada Trusted Advisor comprobación, 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 AWS Support .

Guardar un hito

Puede guardar los hitos 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

En este tutorial se describe el uso 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](#)
- [Paso 2: Documentar el estado de la carga de trabajo](#)
- [Paso 3: Revisar el plan de mejora](#)
- [Paso 4: Realizar mejoras y medir el progreso](#)

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 “Definir una carga de trabajo”](#).

Para definir una carga de trabajo

1. Inicie sesión en la AWS Well-Architected Tool consola AWS Management Console y ábrala 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 AWS tanto en nuestro centro de datos local como en él:
 - a. Seleccione Regiones de AWS y elija las dos regiones de Norteamérica donde se ejecuta la carga de trabajo.
 - b. Seleccione también AWS regiones que no sean regionales e introduzca un nombre para el 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 anules 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 la lente AWS Well-Architected Framework, 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 desde el punto de vista seleccionado que abarcan los pilares del AWS Well-Architected Framework: excelencia operativa, seguridad, confiabilidad, eficiencia del 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.

[Elige Pregúntale a un experto para acceder a la comunidad AWS Re:post dedicada a Well-Architected AWS](#). En esta comunidad, puede hacer preguntas relacionadas con el diseño, la creación, la implementación y el funcionamiento de las cargas de trabajo en AWS.

The screenshot displays the AWS Well-Architected Tool interface. On the left, a sidebar lists 11 Operational Excellence (OPS) questions. The main content area shows the first question: "OPS 1. How do you determine what your priorities are?". Below the question, there is a radio button option "Question does not apply to this workload" and a list of checkboxes for various evaluation criteria: Evaluate external customer needs, Evaluate internal customer needs, Evaluate governance requirements, Evaluate compliance requirements, Evaluate threat landscape, Evaluate tradeoffs, and Manage benefits and risks. A "None of these" option is also present. At the bottom of the question area, there is a "Mark best practice(s) that don't apply to this workload" link. Below the question area is a "Notes - optional" section with a text input field and a character count of "2084 characters remaining". On the right side, there is a "Helpful resources" panel with an "Ask an expert" button and links to AWS Support and AWS Cloud Compliance. Below these are sections for "Evaluate external customer needs", "Evaluate internal customer needs", "Evaluate governance requirements", "Evaluate compliance requirements", and "Evaluate threat landscape", each with a brief description of what to evaluate.

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 selecciona La pregunta no se aplica a esta carga de trabajo o Ninguna de estas opciones, le AWS recomienda que incluya el motivo en el cuadro de 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.

None of these [Info](#)

▼ **Mark best practice(s) that don't apply to this workload**

If one of the best practices within this question does not apply to your workload, you can mark it as not applicable. You can also choose a reason and provide additional notes for documentation.

Evaluate external customer needs [Info](#)

Select reason (optional) ▼

Provide further details (optional)

250 characters remaining

Evaluate internal customer needs [Info](#)

Out of Scope ▼

Internal customer needs to be addressed in following release

190 characters remaining

Evaluate governance requirements [Info](#)

Select reason (optional) ▼

Provide further details (optional)

Note

Puede pausar este proceso en cualquier momento seleccionando Guardar y salir. Para reanudarlo más tarde, abra la AWS WA Tool consola 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

Basándose en las mejores prácticas seleccionadas, AWS WA Tool identifica las áreas de riesgo alto y medio comparadas con el enfoque del AWS Marco de Buena Arquitectura.

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.

Para este ejemplo concreto de carga de trabajo, el enfoque de AWS Well-Architected Framework identificó tres problemas de alto riesgo y un problema de riesgo medio.

Well-Architected Tool > Workloads > Retail Website - North America > AWS Well-Architected Framework Lens

AWS Well-Architected Framework Lens

Overview | **Improvement plan**

Improvement plan overview

Risks

⊗ High risk	3
⚠ Medium risk	1

Improvement items

< 1 >

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.

Workload status

Improvement status
Choose the status of your workload improvements.

Not Started

None

Not Started

In Progress

Complete

Risk Acknowledged

Not Started

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 AWS Well-Architected de la sección Enfoques. A continuación, haga clic en la pestaña del plan de mejora 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

Como parte de este plan de mejora, se abordó uno de los problemas de alto riesgo añadiendo Amazon CloudWatch y AWS Auto Scaling soporte 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.

Well-Architected Tool > Workloads > Retail Website - North America

Retail Website - North America

Delete workload

Review | **Improvement plan** | Milestones | Properties

Improvement plan overview

Risks

 High risk	1
 Medium risk	2

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:

- Ninguno
- No iniciada
- En progreso
- Control
- 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 las lentes y el AWS Well-Architected Framework.

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 óptima 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 mejores prácticas 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.

Definir una carga de trabajo

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 lentes.

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 “Crear 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 “Definir una carga de trabajo a partir de una plantilla”](#) para crear la carga de trabajo a partir de la plantilla de revisión.

Visualizar una carga de trabajo

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.

Editar una carga de trabajo

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 [Definir una carga de trabajo](#).

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.

Compartir una carga de trabajo

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.

Para compartir 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 [Detalles de la carga de trabajo](#).

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

También puede compartir las lentes personalizadas de su propiedad con otras Cuentas de AWS, usuarios, su organización y unidades organizativas de la misma Región de AWS. Consulte [Compartir un enfoque personalizado](#) para obtener más información.

Consideraciones para compartir

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.

Para habilitar el 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 compatibilidad con AWS Organizations.
4. Elija Guardar configuración.

Eliminar acceso compartido

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.

Modificar el acceso compartido

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.

Aceptar y rechazar invitaciones a cargas de trabajo

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 [Detalles de la carga de trabajo](#) de la carga de trabajo.

Eliminar una carga de trabajo

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

Puede generar un informe de carga de trabajo de una lente. 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 la lente para la que desea generar un informe y elija Generar informe.

El informe se genera y se puede descargar o ver.

Detalles de la carga de trabajo

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

- [Pestaña Información general](#)
- [Hitos](#)
- [Pestaña Propiedades](#)
- [Pestaña Recursos compartidos](#)

Pestaña Información general

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 lente.

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 la lente deseada.

Hitos

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.

Pestaña Propiedades

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 [Definir una carga de trabajo](#).

Pestaña Recursos compartidos

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.

Estado

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.

Enfoques

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. 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 creados y mantenidos por AWS. El catálogo de enfoques está disponible para todos los usuarios y no requiere ninguna instalación adicional para su uso.
- [Lentes personalizadas: lentes](#) definidas por el usuario que no son de contenido AWS oficial. 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 una 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.

Para agregar un enfoque a una carga de trabajo

Para agregar un enfoque a una carga de trabajo

1. Inicie sesión en la AWS Well-Architected Tool consola AWS Management Console y ábrala 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 AWS lentes, visite [AWS Well-Architected Lenses](#). 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 lentes personalizadas creadas por otro AWS usuario o cuenta, usted reconoce que las lentes personalizadas creadas por otros usuarios y compartidas con usted son contenido de terceros, según se define en el Acuerdo con el AWS cliente.

Para eliminar un enfoque de una carga de trabajo

Para eliminar un enfoque de una carga de trabajo

1. Inicie sesión en la AWS Well-Architected Tool consola AWS Management Console y ábrala 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 del enfoque que desea quitar y elija Guardar.

La perspectiva de AWS un marco de arquitectura bien diseñada 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.

Detalles del enfoque

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

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

- [Visualización de enfoques personalizados](#)
- [Crear un enfoque personalizado](#)
- [Vista previa de un enfoque personalizado](#)
- [Publicar un enfoque personalizado por primera vez](#)
- [Publicar una actualización de un enfoque personalizado](#)
- [Compartir un enfoque personalizado](#)
- [Añadir etiquetas a un enfoque personalizado](#)
- [Eliminar un enfoque personalizado](#)
- [Especificación del formato del enfoque](#)

Visualización de enfoques personalizados

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 la AWS Well-Architected Tool consola AWS Management Console y ábrala en https://console.aws.amazon.com/wellarchitected/.](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 [Detalles del enfoque](#).

La página de Enfoques personalizados tiene los subcampos siguientes:

Nombre

Nombre del enfoque

Propietario

El Cuenta de AWS identificador propietario del objetivo personalizado.

Status

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.

Crear un enfoque personalizado

Para crear un enfoque personalizado

1. Inicie sesión en la AWS Well-Architected Tool consola AWS Management Console y ábrala 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](#) 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 AWS WA Tool validado el archivo JSON, la lente personalizada aparecerá en Lentes personalizadas.

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 obtener una vista previa de un enfoque personalizado

1. Inicie sesión AWS Management Console y abra la AWS Well-Architected Tool consola 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](#).

Publicar un enfoque personalizado por primera vez

Para publicar un enfoque personalizado

1. Inicie sesión en la AWS Well-Architected Tool consola AWS Management Console y ábrala 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.

Publicar una actualización de un enfoque personalizado

Para publicar una actualización de un enfoque personalizado existente

1. Inicie sesión en la AWS Well-Architected Tool consola AWS Management Console y ábrala 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 AWS WA Tool validado el archivo JSON, la lente personalizada aparecerá en el estado **Borrador de lentes personalizadas**.

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.

Compartir un enfoque personalizado

Puede compartir una lente personalizada con otros Cuentas de AWS usuarios y unidades organizativas (OU). AWS Organizations

Para compartir una lente personalizada con Cuentas de AWS otros usuarios

1. Inicie sesión en la AWS Well-Architected Tool consola AWS Management Console y ábrala 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 [Detalles del enfoque](#), 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 Cuenta de AWS ID de 12 dígitos o el ARN del usuario con el que quiere compartir el objetivo personalizado.
6. Seleccione Crear para enviar una invitación a compartir lentes al usuario Cuenta de AWS o usuario especificado.

Puede compartir un objetivo personalizado con un máximo de 300 Cuentas de AWS 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 la AWS Well-Architected Tool consola AWS Management Console y ábrala 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 [Detalles del enfoque](#), 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 [Detalles del enfoque](#).

 Exención de responsabilidad

Al compartir tus lentes personalizadas con otras personas Cuentas de AWS, confirmas que las AWS pondrás a disposición de esas otras cuentas. Esas otras cuentas pueden seguir accediendo a tus lentes personalizadas compartidas y usándolas, incluso si eliminas las lentes personalizadas de las tuyas Cuenta de AWS o cancelas las tuyas Cuenta de AWS.

Añadir etiquetas a un enfoque personalizado

Añadir etiquetas a un enfoque personalizado

1. Inicie sesión en la AWS Well-Architected Tool consola AWS Management Console y ábrala 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.

Eliminar un enfoque personalizado

Para eliminar un enfoque personalizado

1. Inicie sesión en la AWS Well-Architected Tool consola AWS Management Console y ábrala 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 tus lentes personalizadas con otras personas Cuentas de AWS, confirmas que las AWS pondrás a disposición de esas otras cuentas. Esas otras cuentas pueden seguir accediendo a tus lentes personalizadas compartidas y usándolas, incluso si eliminas las lentes personalizadas de las tuyas Cuenta de AWS o cancelas las tuyas Cuenta de AWS.

Especificación del formato del enfoque

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 AWS Well-Architected Framework, 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 Lens personalizada con Jira, las preguntas muestran tanto el «identificador» 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 Lens personalizada con Jira, las opciones muestran el «identificador» de la pregunta y la elección, así como el «título» de la elección.

El formato utilizado 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

El enfoque AWS del marco de buena arquitectura y otros lentes proporcionados AWS por se actualizan a medida que se introducen nuevos servicios, se perfeccionan las mejores prácticas existentes para los sistemas basados en la nube y se agregan nuevas mejores prácticas. Cuando una nueva versión de un lente está disponible, AWS WA Tool se actualiza para reflejar las mejores prácticas más recientes. 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.

Selección de la actualización de enfoque

La página Actualizaciones de enfoque muestra información para cada carga de trabajo que no está utilizando la versión de enfoque más actual.

Para cada carga de trabajo se muestra la siguiente información:

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 del enfoque

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

El catálogo de lentes es una colección de lentes oficiales AWS creadas AWS WA Tool que ofrecen la up-to-date tecnología y las mejores prácticas centradas en la industria. Estas lentes están disponibles para todos los usuarios y no requieren ninguna instalación adicional para su uso.

En la siguiente tabla se describen todos los lentes AWS oficiales disponibles actualmente en el catálogo de lentes.

Nombre	Descripción
AWS Marco Well-Architected	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.
Movilidad conectada	Mejores prácticas para integrar la tecnología a en los sistemas de transporte y mejorar la experiencia general de movilidad.
Construcción de contenedores	Proporciona las prácticas recomendadas sobre el proceso de diseño y compilación de contenedores.
Análisis de datos	Contiene información AWS recopilada a partir de casos prácticos del mundo real y le ayuda

Nombre	Descripción
	a conocer los elementos clave de diseño de las cargas de trabajo de análisis de Well-Architected, junto con recomendaciones de mejora.
DevOps	Describe un enfoque estructurado que las organizaciones de todos los tamaños pueden seguir para cultivar una cultura acelerada y centrada en la seguridad, capaz de ofrecer un valor empresarial sustancial mediante tecnologías modernas y mejores prácticas. DevOps
Gobierno	Mejores prácticas para diseñar y prestar servicios gubernamentales en AWS.
Industria de la salud	Prácticas recomendadas y orientación sobre cómo diseñar, implementar y administrar las cargas de trabajo de atención sanitaria en la Nube de AWS.
IoT	Mejores prácticas para administrar sus cargas de trabajo de Internet de las cosas (IoT) en AWS.
Creación de valor en fusiones y adquisiciones	Proporciona una serie de preguntas adicionales que hay que tener en cuenta a la hora de buscar formas de impulsar el crecimiento de la empresa, por ejemplo, en el ámbito de las fusiones y adquisiciones de capital privado.
Machine Learning	Mejores prácticas para gestionar sus recursos y cargas de trabajo de Machine Learning en AWS.
Migración	Mejores prácticas sobre cómo migrar a. Nube de AWS

Nombre	Descripción
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 mejores prácticas para las cargas de trabajo de SAP en el Nube de AWS.
Aplicaciones sin servidor	Prácticas recomendadas para crear cargas de trabajo sin servidor a partir de. AWS Cubre casos como microservicios RESTful, backends de aplicaciones móviles, procesamiento de transmisiones y aplicaciones web.

Plantillas de revisión

Puede crear plantillas de revisión en AWS WA Tool que contengan respuestas predefinidas para las preguntas de mejores prácticas de Well-Architected Framework y lentes personalizadas. 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.

Crear una plantilla de revisión

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 lentes, seleccione las lentes que desee aplicar a la plantilla de revisión. El número máximo de lentes que se puede aplicar es 20.

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

 Note

Los lentes 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 la lente en el menú desplegable Responder a las preguntas.

 Note

También puede ir a la sección Lentes, seleccionar la lente y elegir Responder preguntas.

2. Para cada lente 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 lente en la sección de Lentes.

Editar una plantilla de revisión

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 lentes que se aplican a la plantilla de revisión, en la sección Lentes de la pestaña Descripción general, seleccione Editar lentes aplicadas.
 - a. Seleccione o desactive las casillas de verificación de las lentes 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 mejores prácticas sobre la lente, en la sección Lentes de la pestaña Descripción general, seleccione el nombre de la lente.
 - a. En la sección Información general de la lente, seleccione Responder preguntas.

 Note

Si lo desea, puede seleccionar el nombre de la lente en el menú desplegable Revisar plantillas del panel de navegación izquierdo para ir a la sección de Información general de la lente.

- b. Seleccione o desactive las casillas de verificación situadas junto a las respuestas recomendadas que desee cambiar.
 - c. Para guardar y aplicar los cambios, elija Guardar.

Compartir una plantilla de revisión

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](#).

Definir una carga de trabajo a partir de una plantilla

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 una lente, 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 acerca de los permisos de IAM, consulte la [Guía del usuario de Identity and Access Management de AWS](#).

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](#). Elija Siguiente.

[Los perfiles de Well-Architected](#) y las plantillas de revisión se pueden utilizar en conjunto. Las preguntas que vienen rellenas 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.

Eliminar una plantilla de revisión

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.

Perfiles

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 ayudarlo 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.

Editar un perfil

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.

Compartir un perfil

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](#).

Añadir un perfil a una carga de trabajo

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.

Eliminar un perfil de una carga de trabajo

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.

Eliminar 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 “Eliminar un perfil de una carga de trabajo”](#).

AWS Well-Architected Tool Conector para Jira

Puedes usar AWS Well-Architected Tool Connector for Jira para vincular tu cuenta de Jira AWS Well-Architected Tool y sincronizarlos con los elementos de mejora de tus cargas de trabajo con los proyectos de Jira, a fin de ayudarte 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 [Configuración del conector](#).

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 puedes optar por excluir por completo una carga de trabajo de la sincronización.

Puedes 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, puedes 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 especifiques)
- Epic: Carga de trabajo
- Tarea: Pregunta
- Subtarea: Mejores prácticas
- Etiqueta: Pilar

Tras configurar la sincronización de la cuenta de Jira en la página de configuración, podrás [configurar el conector de Jira y sincronizar los elementos de mejora con tu](#) cuenta de Jira.

Configurar el conector

Para instalar el conector

Note

Todos los pasos siguientes se realizan en tu cuenta de Jira, no en la tuya Cuenta de AWS.

1. Inicia sesión en tu cuenta de Jira.
2. En la barra de navegación superior, selecciona Aplicaciones y, a continuación, selecciona Explorar más aplicaciones.
3. En la página Descubre aplicaciones e integraciones para Jira, escribe Well-Architected AWS . A continuación, elige el conector para Jira AWS Well-Architected Tool .
4. En la página de la aplicación, selecciona Obtener aplicación.
5. En el panel Añadir a Jira, selecciona Consíguela ahora.
6. Una vez instalada la aplicación, para completar la configuración, selecciona Configurar.
7. En la página AWS Well-Architected Tool de configuración, elija Conectar una nueva Cuenta de AWS.
8. Introduzca su AccessKeyID y clave secreta. Opcional: introduce tu token de sesión. A continuación, selecciona Connect.

Note

Asegúrate de que tu cuenta tiene el permiso `wellarchitected:ConfigureIntegration`. Estos permisos son necesarios para añadirlos Cuentas de AWS a Jira.

Se Cuentas de AWS pueden conectar varios. AWS WA Tool

Note

Como práctica recomendada de seguridad, se recomienda encarecidamente utilizar credenciales de IAM de corta duración. Para obtener más información sobre cómo crear un AccessKeyidentificador y una clave secreta para usted Cuenta de AWS, consulte

[Administrar las claves de acceso \(consola\)](#) y, para obtener más información sobre el uso de credenciales de corta duración, consulte [Solicitud de credenciales temporales](#).

9. En el caso de las regiones, selecciona la que Regiones de AWS deseas conectar. A continuación, selecciona Connect.

Configuración del proyecto de Jira

Cuando utilices proyectos personalizados, asegúrate de tener los siguientes tipos de problemas en la configuración del proyecto:

- Scrum: épica, historia, subtarea
- Kanban: épica, tarea, subtarea

Para obtener más información sobre la gestión de los tipos de problema, consulta [Atlassian Support | Añadir, editar y eliminar un tipo de problema](#).

Para comprobar 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. Selecciona Configuración en el panel de navegación izquierdo.
3. En la sección de sincronización de la cuenta de Jira, en el estado de conexión de la aplicación de Jira, comprueba el estado Configurado.

El conector ya está configurado y listo para configurarse. Para configurar los ajustes de sincronización de Jira a nivel de cuenta y carga de trabajo, consulta [Configuración del conector](#).

Configuración del conector de

Con el AWS Well-Architected Tool conector para Jira, puedes configurar la sincronización de Jira a nivel de cuenta, nivel de carga de trabajo o ambos. Puedes 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 puedes 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 Jira AWS WA Tool se reflejan en tu 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, aceptas AWS WA Tool modificar tu carga de trabajo en respuesta a los cambios en Jira.

Si tienes información confidencial que no deseas sincronizar con Jira, no introduzcas esta información en el campo Notas de tus cargas de trabajo.

- Sincronización automática: el conector actualiza automáticamente tu proyecto de Jira y tu 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: debes seleccionar Sincronizar con Jira en el panel de carga de trabajo si quieres sincronizar los elementos de mejora entre Jira y la. AWS WA Tool También puedes elegir qué pilares y preguntas específicos quieres sincronizar. Para obtener más información, consulta [Sincronizar una carga](#) de trabajo.

Para configurar el conector a nivel de cuenta

1. Seleccione Configuración en el panel de navegación izquierdo.
2. En el panel de sincronización de cuentas de Jira, selecciona Editar.
3. En el tipo de sincronización, selecciona una de las siguientes opciones:
 - a. Para sincronizar automáticamente las cargas de trabajo cuando se realicen cambios, seleccione Automático.
 - b. Para elegir manualmente cuándo sincronizar las cargas de trabajo, selecciona 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. Introduce tu clave de proyecto de Jira.

 Note

La clave de proyecto de Jira especificada se usa para todas las cargas de trabajo, a menos que cambies 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 desea configurar.
2. Seleccione Propiedades.
3. En el panel de Jira, selecciona Editar.
4. Para configurar los ajustes de Jira de la carga de trabajo, selecciona Anular los ajustes a nivel de cuenta.

 Note

Se debe seleccionar la configuración de anulación a nivel de cuenta para aplicar la configuración específica de la carga de trabajo.

5. Para anular la sincronización, selecciona una de las siguientes opciones:
 - a. Para excluir la carga de trabajo de la sincronización de Jira, selecciona No sincronizar la carga de trabajo.
 - b. Para elegir manualmente cuándo sincronizar la carga de trabajo, selecciona Sincronizar carga de trabajo: manual.
 - c. Para sincronizar automáticamente los cambios en la carga de trabajo, selecciona Sincronizar carga de trabajo: automática.
6. (Opcional) En el caso de la clave del proyecto de Jira, introduce la clave del proyecto con la que deseas sincronizar la carga de trabajo. Esta clave de proyecto puede ser diferente de la clave de proyecto a nivel de cuenta.

Si no especificas una clave de proyecto, el conector crea un proyecto de WA Jira.

7. Seleccione Guardar.

Para obtener información detallada sobre cómo realizar una sincronización manual, consulte [Sincronizar una](#) carga de trabajo.

Sincronizar una carga de trabajo

Para la sincronización automática, el conector sincroniza automáticamente los elementos de mejora cuando se actualiza una carga de trabajo (por ejemplo, cuando se responde a una pregunta o se 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 estés listo para sincronizar tu carga de trabajo con Jira, selecciona Cargas de trabajo en el panel de navegación izquierdo. A continuación, selecciona la carga de trabajo que quieres sincronizar.
2. En la descripción general de la carga de trabajo, selecciona Sincronizar con Jira.
3. Selecciona la lente que quieres sincronizar.
4. Para que Questions se sincronice con Jira, selecciona las preguntas o los pilares completos que quieras sincronizar con el proyecto de Jira.
 - Para cualquier pregunta que quieras eliminar, selecciona el icono X situado junto al título de la pregunta.
5. Selecciona Sincronizar.

Desinstalar el conector

Para desinstalar completamente el AWS Well-Architected Tool Connector for Jira, lleve a cabo las siguientes tareas:

- Desactiva la sincronización de Jira en cualquier carga de trabajo que anule la configuración de sincronización a nivel de cuenta
- Desactiva la sincronización de Jira a nivel de cuenta
- Desvincula tu Cuenta de AWS cuenta de Jira
- Desinstala el conector de tu cuenta de Jira

Para desactivar el conector a nivel de cuenta

Note

Los siguientes pasos se llevan a cabo en su Cuenta de AWS.

1. Seleccione Configuración en el panel de navegación izquierdo.
2. En la sección de sincronización de cuentas de Jira, selecciona Editar.
3. Desactiva la opción Activar la sincronización de la cuenta de Jira.
4. Elija Guardar configuración.

Para desvincular una Cuenta de AWS

Note

Todos los pasos siguientes se realizan en tu cuenta de Jira, no en la tuya. Cuenta de AWS

1. Inicia sesión en tu cuenta de Jira.
2. En la barra de navegación superior, selecciona Aplicaciones y, a continuación, selecciona Administrar tus aplicaciones.
3. Selecciona la flecha desplegable situada junto a AWS Well-Architected Tool Connector for Jira y, a continuación, selecciona Configurar.
4. En el panel AWS Well-Architected Tool de configuración, para desvincular una Cuenta de AWS, selecciona X en Acciones.

Para desinstalar el conector

Note

Todos los pasos siguientes se realizan en tu cuenta de Jira, no en la tuya Cuenta de AWS. Recomendamos comprobar que todas las conexiones Cuentas de AWS estén desvinculadas en la configuración del conector antes de desinstalarlo.

1. Inicia sesión en tu cuenta de Jira.
2. En la barra de navegación superior, selecciona Aplicaciones y, a continuación, selecciona Administrar tus aplicaciones.
3. Selecciona la flecha desplegable situada junto a AWS Well-Architected Tool Connector for Jira.
4. Selecciona Desinstalar y, a continuación, selecciona 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.

Compartir invitaciones

Una invitación para compartir es una solicitud para compartir una carga de trabajo, una lente personalizada o una plantilla de revisión propiedad de otra cuenta 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 una lente personalizada, la lente se añadirá a su página de Lentes personalizadas.
- 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, las lentes personalizadas, 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 la lente personalizada 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 las lentes personalizadas pendientes.

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

Nombre

El nombre de la carga de trabajo, la lente personalizada o la plantilla de revisión que se va a compartir.

Tipo de recurso

El tipo de invitación, ya sea carga de trabajo, lente personalizada, 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, a la lente personalizada, 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 lentes personalizadas, la lente personalizada se añade a la página de Lentes personalizadas. 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 la lente personalizada que desea aceptar o rechazar.
2. Seleccione Rechazar.

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

Notificaciones

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

Notificaciones de lentes

Cuando hay disponible una nueva versión de una lente, 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 una lente desactualizada, también verá un banner que indica que hay disponible una nueva versión de lente.

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 una lente para una carga de trabajo o una plantilla de revisión.

Cuando el propietario de una lente compartida la elimine, si tiene una carga de trabajo asociada a la lente eliminada, recibirá una notificación en la que se le indicará que puede seguir utilizando la lente en su carga de trabajo actual, pero no podrá añadirla 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 “Editar 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.

Para actualizar 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 Entiendo 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

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 de Well-Architected Framework por pilar:** muestra una representación gráfica de los problemas de riesgo alto y medio por pilar para todas sus cargas de trabajo.
- **Problemas de Well-Architected Framework por carga de trabajo:** muestra los problemas de riesgo alto y medio por pilar para todas sus cargas de trabajo.
- **Problemas de Well-Architected Framework 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 de Well-Architected Framework y todos los demás lentes. 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 de Well-Architected Framework por pilar

La sección Problemas de Well-Architected Framework 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 de la lente Well-Architected Framework.

Problemas de Well-Architected Framework por carga de trabajo

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

Name	Total issues	Operational Excellence	Security	Reliability	Performance Efficiency	Cost Optimization	Sustainability	Last updated
Retail Website - EU <small>Questions answered: 46/46 Lenses applied: 1</small>	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 lentes aplicadas 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 Well-Architected Framework 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 de la lente Well-Architected Framework.

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

La sección Problemas de Well-Architected Framework 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 de la lente Well-Architected Framework.

Seguridad en AWS Well-Architected Tool

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

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

- Seguridad de la nube: AWS es responsable de proteger la infraestructura que ejecuta AWS los servicios en la 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 [AWS programas](#) de de . Para obtener más información sobre los programas de cumplimiento aplicables AWS Well-Architected Tool, consulte [AWS Servicios incluidos en el ámbito de aplicación por programa de conformidad y AWS servicios incluidos](#) .
- Seguridad en la nube: su responsabilidad viene determinada por el AWS servicio que utilice. Usted también es responsable de otros factores, incluida la confidencialidad de los datos, los requisitos de la empresa y la legislación y los reglamentos aplicables.

Esta documentación le ayuda a comprender cómo aplicar el modelo de responsabilidad compartida cuando se utiliza AWS WA Tool. Los siguientes temas muestran cómo configurarlo AWS WA Tool para cumplir sus objetivos de seguridad y conformidad. También aprenderá a utilizar otros AWS servicios que le ayudan a supervisar y proteger sus AWS WA Tool recursos.

Temas

- [Protección de datos en AWS Well-Architected Tool](#)
- [Administración de identidad y acceso para AWS Well-Architected Tool](#)
- [Respuesta a incidentes en AWS Well-Architected Tool](#)
- [Validación de conformidad para AWS Well-Architected Tool](#)
- [Resiliencia en AWS Well-Architected Tool](#)
- [Seguridad de la infraestructura en AWS Well-Architected Tool](#)
- [Análisis de configuración y vulnerabilidad en AWS Well-Architected Tool](#)
- [Prevención de la sustitución confusa entre servicios](#)

Protección de datos en AWS Well-Architected Tool

El modelo de [responsabilidad AWS compartida modelo](#) se aplica a la protección de datos en AWS Well-Architected Tool. Como se describe en este modelo, AWS es responsable de proteger la infraestructura global que ejecuta todos los Nube de AWS. Usted es responsable de mantener el control sobre el contenido alojado en esta infraestructura. Usted también es 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, consulte las [Preguntas frecuentes sobre la privacidad de datos](#). Para obtener información sobre la protección de datos en Europa, consulte la publicación de blog sobre el [Modelo de responsabilidad compartida de AWS y GDPR](#) en el Blog de seguridad de AWS .

Con fines de protección de datos, le recomendamos que proteja Cuenta de AWS las credenciales y configure los usuarios 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:

- Utilice la autenticación multifactor (MFA) en cada cuenta.
- Utilice SSL/TLS para comunicarse con los recursos. AWS Se recomienda el uso de TLS 1.2 y recomendamos TLS 1.3.
- Configure la API y el registro de actividad de los usuarios con. AWS CloudTrail
- Utilice soluciones de AWS cifrado, junto con todos los controles de seguridad predeterminados Servicios de AWS.
- Utilice 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 por FIPS 140-2 para acceder a AWS través de una interfaz de línea de comandos o una API, utilice un punto final FIPS. Para obtener más información sobre los puntos de conexión de FIPS disponibles, consulte [Estándar de procesamiento de la información federal \(FIPS\) 140-2](#).

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 cuando trabaja AWS WA Tool o Servicios de AWS utiliza la consola, la API o los SDK. AWS CLI AWS Cualquier dato que ingrese en etiquetas o campos 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 almacenados por AWS WA Tool se cifran en reposo.

Cifrado en tránsito

Todos los datos enviados y recibidos AWS WA Tool se cifran en tránsito.

¿Cómo AWS utiliza sus datos

El equipo de AWS Well-Architected recopila datos agregados para brindar y mejorar AWS Well-Architected Tool el servicio a AWS WA Tool los clientes. Los datos individuales de los clientes se pueden compartir con Cuenta de AWS los equipos 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 AWS WA Tool externo a. AWS

Las propiedades de carga de trabajo a las que tiene AWS acceso el equipo de 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 identidad y acceso para AWS Well-Architected Tool

AWS Identity and Access Management (IAM) es una herramienta Servicio de AWS que ayuda al administrador a controlar de forma segura el acceso a AWS los recursos. Los administradores de IAM controlan quién puede autenticarse (iniciar sesión) y quién puede autorizarse (tener permisos) para usar los recursos. AWS WA Tool La IAM es una Servicio de AWS opción que puede utilizar sin coste adicional.

Temas

- [Público](#)
- [Autenticación con identidades](#)
- [Administración de acceso mediante políticas](#)
- [¿Cómo AWS Well-Architected Tool funciona con IAM](#)
- [AWS Well-Architected Tool ejemplos de políticas basadas en la identidad](#)
- [AWS políticas gestionadas para AWS Well-Architected Tool](#)
- [Solución de problemas AWS Well-Architected Tool de identidad y acceso](#)

Público

La forma de usar AWS Identity and Access Management (IAM) varía según el trabajo en el que se realice. AWS WA Tool

Usuario del servicio: si utiliza el AWS WA Tool servicio para realizar su trabajo, el administrador le proporcionará las credenciales y los permisos que necesita. A medida que vaya utilizando más AWS WA Tool funciones para realizar su trabajo, es posible que necesite permisos adicionales. Entender cómo se administra el acceso puede ayudarlo a solicitar los permisos correctos al administrador. Si no puede acceder a una característica en AWS WA Tool, consulte [Solución de problemas AWS Well-Architected Tool de identidad y acceso](#).

Administrador de servicios: si estás a cargo de AWS WA Tool los recursos de tu empresa, es probable que tengas acceso total a ellos AWS WA Tool. Su trabajo consiste en determinar a qué AWS WA Tool funciones y recursos deben acceder los usuarios del servicio. Luego, debe enviar solicitudes a su administrador de IAM para cambiar los permisos de los usuarios de su servicio. Revise la información de esta página para conocer los conceptos básicos de IAM. Para obtener más

información sobre cómo su empresa puede utilizar la IAM 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. Para ver ejemplos de políticas AWS WA Tool basadas en la identidad que puede utilizar en IAM, consulte. [AWS Well-Architected Tool ejemplos de políticas basadas en la identidad](#)

Autenticación con identidades

La autenticación es la forma de iniciar sesión AWS con sus credenciales de identidad. Debe estar autenticado (con quien haya iniciado sesión AWS) como usuario de IAM o asumiendo una función de IAM. Usuario raíz de la cuenta de AWS

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

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

Si accede AWS mediante programación, AWS proporciona un kit de desarrollo de software (SDK) y una interfaz de línea de comandos (CLI) para firmar criptográficamente sus solicitudes con sus credenciales. Si no utilizas AWS herramientas, debes firmar las solicitudes tú mismo. Para obtener más información sobre cómo usar el método recomendado para firmar las solicitudes usted mismo, consulte [Firmar las solicitudes de la AWS 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, le AWS recomienda que utilice 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 [Uso de la autenticación multifactor \(MFA\) en AWS](#) en la Guía del usuario de IAM.

Cuenta de AWS usuario root

Al crear una Cuenta de AWS, comienza con una identidad de inicio de sesión que tiene acceso completo a todos Servicios de AWS los recursos de la cuenta. Esta identidad se denomina usuario Cuenta de AWS raíz y se accede a ella iniciando sesión con la dirección de correo electrónico y la contraseña que utilizaste para crear la cuenta. Recomendamos encarecidamente que no utilice el usuario raíz para sus tareas diarias. Proteja las credenciales del usuario raíz y utilícelas solo para las tareas que solo el usuario raíz pueda realizar. Para ver la lista completa de las tareas que requieren que inicie sesión como usuario raíz, consulte [Tareas que requieren credenciales de usuario raíz](#) en la Guía del usuario de IAM.

Identidad federada

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

Una identidad federada es un usuario del directorio de usuarios de su empresa, un proveedor de identidades web AWS Directory Service, el directorio del Centro de Identidad o cualquier usuario al que acceda Servicios de AWS mediante las credenciales proporcionadas a través de una fuente de identidad. Cuando las identidades federadas acceden Cuentas de AWS, asumen funciones y las funciones proporcionan credenciales temporales.

Para una administración de acceso centralizada, le recomendamos que utilice AWS IAM Identity Center. Puede crear usuarios y grupos en el Centro de identidades de IAM, o puede conectarse y sincronizarse con un conjunto de usuarios y grupos de su propia fuente de identidad para usarlos en todas sus Cuentas de AWS aplicaciones. Para obtener más información, consulte [¿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 propia Cuenta de AWS que tiene permisos específicos para una sola persona o aplicación. Siempre que sea posible, recomendamos emplear credenciales temporales, en lugar de crear usuarios de IAM que tengan credenciales de larga duración como contraseñas y claves de acceso. No obstante, si tiene casos de uso específicos que requieran credenciales de larga duración con usuarios de IAM, recomendamos rotar las claves de acceso. Para más información, consulte [Rotar las claves de acceso periódicamente para casos de uso que requieran credenciales de larga duración](#) en la Guía del usuario de IAM.

Un [grupo de IAM](#) es una identidad que especifica un conjunto de usuarios de IAM. No puede iniciar sesión como grupo. Puede usar 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 permanentes a largo plazo y los roles proporcionan credenciales temporales. Para más información, consulte [Cuándo crear un usuario de IAM \(en lugar de un rol\)](#) en la Guía del usuario de IAM.

Roles de IAM

Un [rol de IAM](#) es una identidad dentro de usted Cuenta de AWS que tiene permisos específicos. Es similar a un usuario de IAM, pero no está asociado a una determinada persona. Puede asumir temporalmente una función de IAM en el AWS Management Console [cambiando](#) de función. Puede asumir un rol llamando a una operación de AWS API AWS CLI o utilizando una URL personalizada. Para más información sobre los métodos para el uso de roles, consulte [Uso de roles de IAM](#) 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 para federación, consulte [Creación de un rol para un proveedor de identidades de terceros](#) en la Guía del usuario de IAM. Si utiliza 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, consulte [Conjuntos de permisos](#) en la Guía del usuario de AWS IAM Identity Center .
- **Permisos de usuario de IAM temporales:** un usuario de IAM puede asumir un rol de IAM para recibir temporalmente permisos distintos que le permitan realizar una tarea concreta.
- **Acceso entre cuentas:** puede utilizar un rol de IAM para permitir que alguien (una entidad principal de confianza) de otra cuenta acceda a los recursos de la cuenta. Los roles son la forma principal de conceder acceso entre cuentas. Sin embargo, con algunas Servicios de AWS, puedes adjuntar una política directamente a un recurso (en lugar de usar un rol como proxy). Para conocer la

diferencia entre las funciones y las políticas basadas en recursos para el acceso entre cuentas, consulte el tema sobre el acceso a los [recursos entre cuentas en IAM en la Guía del usuario de IAM](#).

- **Acceso entre servicios:** algunos utilizan funciones en otros. Servicios de AWS 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 al servicio.
- **Sesiones de acceso directo (FAS):** cuando utilizas un usuario o un rol de IAM para realizar acciones en ellas AWS, se te considera director. Cuando utiliza algunos servicios, es posible que realice una acción que desencadene otra acción en un servicio diferente. El FAS utiliza los permisos del principal que llama Servicio de AWS y los solicita Servicio de AWS para realizar solicitudes a los servicios descendentes. Las solicitudes de FAS solo se realizan cuando un servicio recibe una solicitud que requiere interacciones con otros Servicios de AWS recursos para completarse. En este caso, debe tener permisos para realizar ambas acciones. Para obtener información 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.
- **Función vinculada al servicio:** una función vinculada a un servicio es un tipo de función de servicio que está vinculada a un. Servicio de AWS El servicio puede asumir el rol para realizar una acción en su nombre. Los roles vinculados al servicio aparecen en usted Cuenta de AWS y son propiedad del servicio. Un administrador de IAM puede ver, pero no editar, los permisos de los roles vinculados a servicios.
- **Aplicaciones que se ejecutan en Amazon EC2:** puede usar un rol de IAM para administrar las credenciales temporales de las aplicaciones que se ejecutan en una instancia EC2 y realizan AWS CLI solicitudes a la API. AWS Es preferible hacerlo de este modo a almacenar claves de acceso en la instancia de EC2. Para asignar una AWS función a una instancia EC2 y ponerla a disposición de todas sus aplicaciones, debe crear un perfil de instancia adjunto a la instancia. Un perfil de instancia contiene el rol y permite a los programas que se ejecutan en la instancia de EC2 obtener credenciales temporales. Para 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.

Para obtener información sobre el uso de los roles de IAM, consulte [Cuándo crear un rol de IAM \(en lugar de un usuario\)](#) en la Guía del usuario de IAM.

Administración de acceso mediante políticas

El acceso se controla AWS creando políticas y adjuntándolas a AWS identidades o recursos. Una política es un objeto AWS que, cuando se asocia a una identidad o un recurso, define sus permisos. AWS evalúa estas políticas cuando un director (usuario, usuario raíz o sesión de rol) realiza una solicitud. Los permisos en las políticas determinan si la solicitud se permite o se deniega. La mayoría de las políticas se almacenan AWS como 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 usar las políticas de AWS JSON 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 utilice para realizar la operación. Por ejemplo, suponga que dispone de una política que permite la acción `iam:GetRole`. Un usuario con esa política puede obtener información sobre el rol de la API AWS Management Console AWS CLI, la o la AWS API.

Políticas basadas en identidades

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

Las políticas basadas en identidades pueden clasificarse además como políticas insertadas o políticas administradas. Las políticas insertadas se integran directamente en un único usuario, grupo o rol. Las políticas administradas son políticas independientes que puede adjuntar a varios usuarios, grupos y roles de su Cuenta de AWS empresa. Las políticas administradas incluyen políticas AWS administradas y políticas administradas por el cliente. Para 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. 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. Los principales pueden incluir cuentas, usuarios, roles, usuarios federados o. Servicios de AWS

Las políticas basadas en recursos son políticas insertadas que se encuentran en ese servicio. No puedes usar políticas AWS gestionadas de IAM 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 y Amazon VPC son ejemplos de servicios que admiten las ACL. AWS WAF Para obtener más información sobre las ACL, consulte [Información general de Lista de control de acceso \(ACL\)](#) en la Guía para desarrolladores de Amazon Simple Storage Service.

Otros tipos de políticas

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

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

de los permisos, consulte [Límites de permisos para las entidades de IAM](#) en la Guía del usuario de IAM.

- **Políticas de control de servicios (SCP):** las SCP son políticas de JSON que especifican los permisos máximos para una organización o unidad organizativa (OU). AWS Organizations es un servicio para agrupar y gestionar de forma centralizada varios de los Cuentas de AWS que son propiedad de su empresa. Si habilita todas las características en una organización, entonces podrá aplicar políticas de control de servicio (SCP) a una o a todas sus cuentas. El SCP limita los permisos de las entidades en las cuentas de los miembros, incluidas las de cada una. Usuario raíz de la cuenta de AWS Para obtener más información acerca de Organizations y las SCP, consulte [Funcionamiento de las SCP](#) 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 saber cómo AWS determinar si se debe permitir una solicitud cuando se trata de varios tipos de políticas, consulte la [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 gestionar el acceso AWS WA Tool, infórmese sobre las funciones de IAM disponibles para su uso. AWS WA Tool

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

Característica de IAM	AWS WA Tool soporte
Políticas basadas en identidades	Sí
Políticas basadas en recursos	No

Característica de IAM	AWS WA Tool soporte
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 visión general de cómo AWS WA Tool funcionan otros AWS servicios con la mayoría de las funciones de IAM, consulte [AWS los servicios que funcionan con IAM](#) en la Guía del usuario de IAM.

Políticas de AWS WA Tool basadas en identidades

Admite acciones de política	Sí
-----------------------------	----

Los administradores pueden usar las políticas de AWS JSON 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 políticas suelen tener el mismo nombre que la operación de AWS API 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 dentro AWS WA Tool

Compatibilidad con las políticas basadas en recursos	No
--	----

Las políticas basadas en recursos son documentos de política JSON que se asocian a un recurso. 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. Los principales pueden incluir cuentas, usuarios, roles, usuarios federados o. Servicios de AWS

Para habilitar el acceso entre cuentas, puede 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 el principal y el recurso son diferentes Cuentas de AWS, el administrador de IAM de la cuenta de confianza también debe conceder a la entidad principal (usuario o rol) permiso para acceder al recurso. Para conceder el permiso, adjunte la entidad a una política basada en identidad. Sin embargo, si la política en función de recursos concede el acceso a una entidad principal de la misma cuenta, no es necesaria una política basada en identidad adicional. Para obtener más información, consulte el tema [Acceso a recursos entre cuentas en IAM en](#) la Guía del usuario de IAM.

Acciones políticas para AWS WA Tool

Admite acciones de política	Sí
-----------------------------	----

Los administradores pueden usar las políticas de AWS JSON 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 políticas suelen tener el mismo nombre que la operación de AWS API 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 políticas 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 AWS WA Tool acciones, consulte las [acciones definidas por AWS Well-Architected Tool](#) en la Referencia de autorización del servicio.

Recursos de políticas

Admite recursos de políticas

Sí

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

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

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

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

Para ver una lista de los tipos de AWS WA Tool recursos y sus ARN, consulte [los recursos definidos AWS Well-Architected Tool en la](#) Referencia de autorización de servicios. 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 AWS WA Tool de carga de trabajo tiene el siguiente ARN:

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

Para obtener más información sobre el formato de los ARN, consulte Nombres de [recursos de Amazon \(ARN\) y espacios de nombres de AWS servicio](#).

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 AWS WA Tool acciones, como las de crear y enumerar cargas de trabajo, no se pueden realizar en un recurso específico. En dichos casos, debe utilizar el carácter comodín (*).

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

Para ver una lista de los tipos de AWS WA Tool recursos y sus ARN, consulte los [recursos definidos por AWS Well-Architected Tool](#) en la Referencia de autorización de servicios. 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 la política para AWS WA Tool

Admite claves de condición de políticas específicas del servicio	Sí
--	----

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

El elemento `Condition` (o bloque de `Condition`) permite especificar condiciones en las que entra en vigor una instrucción. El elemento `Condition` es opcional. Puede crear expresiones condicionales que utilicen [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 mediante una OR operación lógica. Se deben cumplir todas las condiciones antes de que se concedan los permisos de la instrucción.

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

AWS admite claves de condición globales y claves de condición específicas del servicio. Para ver todas las claves de condición AWS globales, consulte las claves de [contexto de condición AWS globales 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 AWS globales, consulte las claves de [contexto de condición AWS globales](#) en la Referencia de autorización de servicios.

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

El elemento `Condition` (o bloque de `Condition`) permite especificar condiciones en las que entra en vigor una instrucción. El elemento `Condition` es opcional. Puede crear expresiones condicionales que utilicen [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 mediante una OR operación lógica. Se deben cumplir todas las condiciones antes de que se concedan los permisos de la instrucción.

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

AWS admite claves de condición globales y claves de condición específicas del servicio. Para ver todas las claves de condición AWS globales, consulte las claves de [contexto de condición AWS globales en la Guía](#) del usuario de IAM.

ACL en AWS WA Tool

Admite las 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. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a muchos AWS recursos. 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 [¿Qué es 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.

Utilizar credenciales temporales con AWS WA Tool

Compatible con el uso de credenciales temporales	Sí
--	----

Algunos Servicios de AWS no funcionan cuando inicias sesión con credenciales temporales. Para obtener información adicional, incluidas las que Servicios de AWS funcionan con credenciales temporales, consulta Cómo [Servicios de AWS funcionan con IAM](#) en la Guía del usuario de IAM.

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

Puedes crear credenciales temporales manualmente mediante la AWS CLI API o. AWS A continuación, puede utilizar esas credenciales temporales para acceder AWS. AWS recomienda generar credenciales temporales de forma dinámica en lugar de utilizar claves de acceso a largo plazo. Para más información, consulte [Credenciales de seguridad temporales en IAM](#).

Permisos principales entre servicios para AWS WA Tool

Admite Forward access sessions (FAS)	Sí
--------------------------------------	----

Cuando utilizas un usuario o un rol de IAM para realizar acciones en él AWS, se te considera principal. Cuando utiliza algunos servicios, es posible que realice una acción que desencadene otra

acción en un servicio diferente. FAS utiliza los permisos del principal que llama y los que solicita Servicio de AWS para realizar solicitudes a los servicios descendentes. Servicio de AWS Las solicitudes de FAS solo se realizan cuando un servicio recibe una solicitud que requiere interacciones con otros Servicios de AWS recursos para completarse. En este caso, debe tener permisos para realizar ambas acciones. Para obtener información detallada sobre las políticas a la hora de realizar solicitudes de FAS, consulte [Forward access sessions](#).

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.

Funciones vinculadas al servicio para AWS WA Tool

Compatible con roles vinculados al servicio	No
---	----

Un rol vinculado a un servicio 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 al servicio aparecen en usted Cuenta de AWS y son propiedad del servicio. Un administrador de IAM puede ver, pero no editar, los permisos de los roles vinculados a servicios.

Para más información sobre cómo crear o administrar roles vinculados a servicios, consulte [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 la identidad

De forma predeterminada, los usuarios y roles no tienen permiso para crear, ver ni modificar recursos de AWS WA Tool . Tampoco pueden realizar tareas con la API AWS Management Console AWS CLI, o 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 Connector for Jira AWS Well-Architected Tool](#)

Prácticas recomendadas relativas a políticas

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

- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos: para empezar a conceder permisos a sus usuarios y cargas de trabajo, utilice las políticas AWS administradas que otorgan permisos para muchos casos de uso comunes. Están disponibles en su Cuenta de AWS. Le recomendamos que reduzca aún más los permisos definiendo políticas administradas por el AWS cliente que sean específicas para sus casos de uso. Con el fin de obtener más información, consulte las [políticas administradas por AWS](#) o las [políticas administradas por AWS para funciones de trabajo](#) en la Guía de usuario de IAM.
- Aplique permisos de privilegio mínimo: cuando establezca permisos con políticas de IAM, conceda solo los permisos necesarios para realizar una tarea. Para ello, debe definir las acciones que se pueden llevar a cabo en determinados recursos en condiciones específicas, también conocidos

como permisos de privilegios mínimos. Con el fin de obtener más información sobre el uso de IAM para aplicar permisos, consulte [Políticas y permisos en IAM](#) en la Guía del usuario de IAM.

- Utilice condiciones en las políticas de IAM para restringir aún más el acceso: puede agregar una condición a sus políticas para limitar el acceso a las acciones y los recursos. Por ejemplo, puede escribir una condición de políticas para especificar que todas las solicitudes deben enviarse utilizando SSL. También puedes usar condiciones para conceder el acceso a las acciones del servicio si se utilizan a través de una acción específica Servicio de AWS, por ejemplo AWS CloudFormation. Para obtener más información, consulte [Elementos de la política de JSON de IAM: Condición](#) en la Guía del usuario de IAM.
- Utilice 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 [Política de validación de Analizador de acceso de IAM](#) en la Guía de usuario de IAM.
- Requerir autenticación multifactor (MFA): si tiene un escenario que requiere usuarios de IAM o un usuario raíz en Cuenta de AWS su cuenta, active la MFA para mayor seguridad. Para solicitar la MFA cuando se invocan las operaciones de la API, agregue las condiciones de la MFA a sus políticas. Para más información, consulte [Configuración del acceso a una API protegido por MFA](#) en la Guía de usuario de IAM.

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

Mediante la consola de AWS WA Tool

Para acceder a la AWS Well-Architected Tool consola, debe tener un conjunto mínimo de permisos. Estos permisos deben permitirle enumerar y ver detalles sobre los AWS WA Tool recursos de su cuenta 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 garantizar que esas entidades puedan seguir utilizando la AWS WA Tool consola, adjunte también la siguiente política AWS gestionada 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 concedas permisos mínimos de consola a los usuarios que solo realizan llamadas a la API AWS CLI o a la AWS API. 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 administradas e insertadas que se asocian a la identidad de sus usuarios. Esta política incluye permisos para completar esta acción en la consola o mediante programación mediante la API AWS CLI o AWS .

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ViewOwnUserInfo",
      "Effect": "Allow",
      "Action": [
        "iam:GetUserPolicy",
        "iam:ListGroupsWithUser",
        "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, quieres conceder a un usuario acceso Cuenta de AWS total a tus cargas de trabajo. El acceso total permite al usuario 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 acceso de Cuenta de AWS solo lectura a sus 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 acceso de Cuenta de AWS solo lectura a una de sus cargas de trabajo en la región. 99999999999955555555555556666666 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 Connector for Jira AWS Well-Architected Tool

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 tu cuenta.

A continuación, se describen los usos relevantes de la clave de condición:

- **CreateWorkload:** Al `wellarchitected:JiraProjectKey` solicitarlo `CreateWorkload`, puedes 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 solicitarlo `wellarchitected:JiraProjectKeyUpdateWorkload`, puedes definir qué proyectos personalizados de Jira se pueden vincular a esta carga de trabajo concreta o a cualquier otra 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 `wellarchitected:JiraProjectKey` solicitarlo `UpdateGlobalSettings`, puedes definir qué proyectos personalizados de Jira se pueden vincular al. Cuenta de AWS La configuración a nivel de cuenta protege las cargas de trabajo de tu 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 tu 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"]
  }
}
]
```

AWS políticas gestionadas para AWS Well-Architected Tool

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

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

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

Para obtener más información, consulte [Políticas administradas de AWS](#) en la Guía del usuario de IAM.

AWS política gestionada: WellArchitectedConsoleFullAccess

Puede adjuntar la política WellArchitectedConsoleFullAccess a las identidades de IAM.

Esta política otorga acceso completo a AWS Well-Architected Tool.

Detalles de los permisos

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

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

AWS política gestionada: WellArchitectedConsoleReadOnlyAccess

Puede adjuntar la política WellArchitectedConsoleReadOnlyAccess a las identidades de IAM.

Esta política otorga 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": "*"
    }
  ]
}
```

AWS política gestionada: AWSWellArchitectedOrganizationsServiceRolePolicy

Puede adjuntar la política AWSWellArchitectedOrganizationsServiceRolePolicy a las identidades de IAM.

Esta política otorga los permisos administrativos necesarios para respaldar la AWS Well-Architected Tool integración con Organizations. AWS 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 los directores comprobar si el acceso AWS al servicio 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": "*"    
}    
]    
}
```

AWS política gestionada: AWSWellArchitectedDiscoveryServiceRolePolicy

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

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

Detalles de los permisos

Esta política incluye los siguientes permisos.

- `trustedadvisor:DescribeChecks`— Enumera Trusted Advisor los cheques disponibles.
- `trustedadvisor:DescribeCheckItems`— Obtiene los datos de los Trusted Advisor cheques, incluidos el estado y los recursos marcados por. Trusted Advisor
- `servicecatalog:GetApplication`— Obtiene los detalles de una aplicación. AppRegistry
- `servicecatalog:ListAssociatedResources`—Muestra los recursos asociados a una AppRegistry aplicación.
- `cloudformation:DescribeStacks`: obtiene los detalles de las pilas de AWS CloudFormation .
- `cloudformation:ListStackResources`—Muestra los recursos asociados a las AWS CloudFormation pilas.
- `resource-groups:ListGroupResources`—Muestra los recursos de un. ResourceGroup
- `tag:GetResources`— Necesario para. ListGroupResources
- `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 AppRegistry aplicación.
- `servicecatalog:UpdateAttributeGroup`: actualiza un grupo de atributos gestionado por un servicio.

- `servicecatalog:DisassociateAttributeGroup`—Disocia un grupo de atributos gestionados por un servicio de una aplicación. 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": [
  "servicelog:AssociateAttributeGroup",
  "servicelog:DisassociateAttributeGroup"
],
"Resource": [
  "arn:*:servicelog:*/*/applications/*",
  "arn:*:servicelog:*/*/attribute-groups/AWS_WellArchitected-*"
]
},
{
"Effect": "Allow",
"Action": [
  "servicelog:UpdateAttributeGroup",
  "servicelog>DeleteAttributeGroup"
],
"Resource": [
  "arn:*:servicelog:*/*/attribute-groups/AWS_WellArchitected-*"
]
}
]
}

```

AWS WA Tool actualizaciones de las políticas gestionadas AWS

Consulte los detalles sobre las actualizaciones de las políticas AWS administradas AWS WA Tool desde que este servicio comenzó a realizar el seguimiento de estos cambios. Para recibir alertas automáticas sobre los cambios en esta página, suscríbese a la fuente RSS de la página del [historial del AWS WA Tool documento](#).

Cambio	Descripción	Fecha
AWS WA Tool política gestionada modificada	Se agregó "wellarchitected:Export*" a WellArchitectedConsoleReadOnlyAccess.	22 de junio de 2023
AWS WA Tool política de roles de servicio agregada	Se agregó AWSWellArchitectedDiscoveryServiceRolePolicy para permitir AWS Well-Architected	3 de mayo de 2023

Cambio	Descripción	Fecha
	Tool el acceso a AWS los servicios y recursos relacionados con AWS WA Tool los recursos.	
AWS WA Tool permisos añadidos	Se ha añadido una nueva acción de concesión <code>ListAWSServiceAccessForOrganization</code> AWS WA Tool para comprobar si el acceso al AWS servicio está habilitado AWS WA Tool.	22 de julio de 2022
AWS WA Tool comenzó a rastrear los cambios	AWS WA Tool comenzó a realizar un seguimiento de los cambios de sus políticas AWS gestionadas.	22 de julio de 2022

Solución de problemas AWS Well-Architected Tool de identidad y acceso

Utilice la siguiente información como ayuda para diagnosticar y solucionar los problemas habituales que pueden surgir al trabajar con un AWS WA Tool IAM.

Temas

- [No estoy autorizado a realizar ninguna acción en AWS WA Tool](#)

No estoy autorizado a realizar ninguna acción en AWS WA Tool

Si AWS Management Console le indica que no está autorizado a realizar una acción, debe ponerse en contacto con su administrador para obtener ayuda. El administrador 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 a incidentes en AWS Well-Architected Tool

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

AWS los problemas operativos con un amplio impacto se publican en el [AWS Service Health Dashboard](#).

Los problemas operativos también se publican en las cuentas individuales a través de AWS Health Dashboard. Para obtener información sobre cómo utilizar el AWS Health Dashboard, consulte la [Guía del AWS Health usuario](#).

Validación de conformidad para AWS Well-Architected Tool

Para saber si uno Servicio de AWS está dentro del ámbito de aplicación de programas de cumplimiento específicos, consulte [Servicios de AWS Alcance por programa de cumplimiento](#) [Servicios de AWS](#) de cumplimiento y elija el programa de cumplimiento que le interese. Para obtener información general, consulte Programas de [AWS cumplimiento > Programas AWS](#).

Puede descargar informes de auditoría de terceros utilizando AWS Artifact. Para obtener más información, consulte [Descarga de informes en AWS Artifact](#).

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

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

Note

No Servicios de AWS todas cumplen con los requisitos de la HIPAA. Para más información, consulte la [Referencia de servicios compatibles con HIPAA](#).

- [AWS Recursos de](#) de cumplimiento: esta colección de libros de trabajo y guías puede aplicarse a su industria y ubicación.
- [AWS Guías de cumplimiento para clientes](#): comprenda el modelo de responsabilidad compartida desde el punto de vista del cumplimiento. Las guías resumen las mejores prácticas para garantizar la seguridad Servicios de AWS y orientan los controles de seguridad en varios marcos (incluidos el Instituto Nacional de Estándares y Tecnología (NIST), el Consejo de Normas de Seguridad del Sector de Tarjetas de Pago (PCI) y la Organización Internacional de Normalización (ISO)).
- [Evaluación de los recursos con reglas](#) en la guía para AWS Config desarrolladores: el AWS Config servicio evalúa en qué medida las configuraciones de los recursos cumplen con las prácticas internas, las directrices del sector y las normas.
- [AWS Security Hub](#)— Esto Servicio de AWS proporciona una visión completa del estado de su seguridad interior AWS. Security Hub utiliza controles de seguridad para evaluar sus recursos de AWS y comprobar su cumplimiento con los estándares y las prácticas recomendadas del sector de la seguridad. Para obtener una lista de los servicios y controles compatibles, consulte la [Referencia de controles de Security Hub](#).
- [Amazon GuardDuty](#): Servicio de AWS detecta posibles amenazas para sus cargas de trabajo Cuentas de AWS, contenedores y datos mediante la supervisión de su entorno para detectar actividades sospechosas y maliciosas. GuardDuty puede ayudarlo a cumplir con varios requisitos de conformidad, como el PCI DSS, al cumplir con los requisitos de detección de intrusiones exigidos por ciertos marcos de cumplimiento.
- [AWS Audit Manager](#)— Esto le Servicio de AWS ayuda a auditar continuamente su AWS uso para simplificar la gestión del riesgo y el cumplimiento de las normativas y los estándares del sector.

Resiliencia en AWS Well-Architected Tool

La infraestructura AWS global se basa en zonas Regiones de AWS de disponibilidad. Regiones de AWS proporcionan varias zonas de disponibilidad aisladas y separadas físicamente, que están conectadas mediante redes de baja latencia, alto rendimiento y alta redundancia. Con las zonas de disponibilidad, puede diseñar y utilizar aplicaciones y bases de datos que realizan una conmutación

por error automática entre zonas de disponibilidad sin interrupciones. Las zonas de disponibilidad tienen una mayor disponibilidad, tolerancia a errores y escalabilidad que las infraestructuras tradicionales de centros de datos únicos o múltiples.

[Para obtener más información sobre las zonas de disponibilidad Regiones de AWS y las zonas de disponibilidad, consulte Infraestructura global.AWS](#)

Seguridad de la infraestructura en AWS Well-Architected Tool

Como servicio gestionado, AWS Well-Architected Tool está protegido por la seguridad de la red AWS global. Para obtener información sobre los servicios AWS de seguridad y cómo se AWS protege la infraestructura, consulte [Seguridad AWS en la nube](#). Para diseñar su AWS entorno utilizando las mejores prácticas de seguridad de la infraestructura, consulte [Protección de infraestructuras en un marco](#) de buena AWS arquitectura basado en el pilar de la seguridad.

Utiliza las llamadas a la API AWS publicadas para acceder a AWS WA Tool 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 de seguridad de IAM principal. También puede utilizar [AWS Security Token Service](#) (AWS STS) para generar credenciales de seguridad temporales para firmar solicitudes.

Análisis de configuración y vulnerabilidad en AWS Well-Architected Tool

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

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 de identidad entre servicios puede provocar el confuso problema de un diputado. La suplantación entre servicios puede 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 puede 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 [aws:SourceAccount](#) global [aws:SourceArn](#) las claves de contexto en las políticas de recursos para limitar los permisos que se AWS Well-Architected Tool otorgan a otro servicio al recurso. Utilice `aws:SourceArn` si desea que solo se asocie un recurso al acceso entre servicios. Utilice `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.

En el siguiente ejemplo, se muestra cómo utilizar las claves de contexto de condición `aws:SourceAccount` global `aws:SourceArn` y las claves contextuales AWS WA Tool para evitar el confuso problema de los diputados.

```
{
  "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 una lente personalizada](#)
- [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 `AWWellArchitectedOrganizationsServiceRolePolicy`.

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.
- Su 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. Esto garantiza que se cree el rol `AWSServiceRoleForWellArchitected` vinculado al servicio. 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](#)
- [Etiquetar los recursos](#)
- [Restricciones de las etiquetas](#)
- [Uso de etiquetas mediante la consola](#)
- [Uso de etiquetas mediante la API](#)

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 las lentes, 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 o 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 o durante la creación (API de AWS WA Tool, AWS CLI y SDK de AWS)
Lentes personalizadas 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 Descripción general para lentes, perfiles y plantillas de revisión personalizadas.

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 una lente personalizada

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 Lentes personalizadas.

4. Seleccione el nombre de la lente personalizada 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
Crear una carga de trabajo	CreateWorkload
Importar una nueva lente	Importar lente
Crear un perfil	Crear perfil
Crear una plantilla de revisión	Cree una plantilla de revisión

Registrar 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 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 de la consola de CloudTrail en el Historial de eventos. Mediante la información recopilada por CloudTrail, puede determinar la solicitud que se realizó a AWS WA Tool, la dirección IP desde la que se realizó, quién la realizó y cuándo, etc.

Para obtener más información acerca de CloudTrail, consulte la [Guía del usuario de AWS CloudTrail](#).

Información de AWS WA Tool en CloudTrail

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

Para mantener un registro continuo de eventos en la Cuenta de AWS, incluidos los eventos de AWS 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 obtener más información, consulte los siguientes temas:

- [Introducción a la creación de registros de seguimiento](#)
- [Servicios e integraciones compatibles con CloudTrail](#)

- [Configuración de notificaciones de Amazon SNS para CloudTrail](#)
- [Recibir archivos de registro de CloudTrail de varias regiones](#) y [Recibir 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 log 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 registros en un bucket de Amazon S3 que especifique. Los archivos log de CloudTrail pueden contener una o varias entradas de log. Un evento representa una solicitud específica realizada desde un origen y contiene información sobre la acción solicitada, la fecha y la hora de la acción, los parámetros de la solicitud, etc. Los archivos de registro de CloudTrail no rastrean el orden en la pila de las llamadas públicas a la API, por lo que estas no aparecen en ningún orden específico.

En el siguiente ejemplo, se muestra una entrada de registro de CloudTrail que ilustra la acción `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 una lente de una carga de trabajo
- Relacionado con lentes
 - Importar o exportar una lente personalizada
 - Publicar una lente personalizada
 - Eliminar una lente personalizada
 - Compartir o dejar de compartir una lente personalizada
 - Actualizar el estado de una invitación para compartir
 - Añadir o quitar una lente 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": "ARO4JUSXMN5ZR6S7LZNP:sample-user",
      "arn": "arn:aws:sts::123456789012:assumed-role/Admin/example-user",
      "accountId": "123456789012",
      "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
      "sessionContext": {
        "sessionIssuer": {
          "type": "Role",
          "principalId": "ARO4JUSXMN5ZR6S7LZNP",
          "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 una lente personalizada

```

{
  "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":"ARO0A4JUSXMN5ZR6S7LZNP:example-user",
    "arn":"arn:aws:sts::123456789012:assumed-role/Admin/example-user",
    "accountId":"123456789012",
    "accessKeyId":"AKIAIOSFODNN7EXAMPLE",
    "sessionContext":{
      "sessionIssuer":{
        "type":"Role",
        "principalId":"ARO0A4JUSXMN5ZR6S7LZNP",
        "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: 16 de abril de 2024

Cambio	Descripción	Fecha
Jira	En esta versión se agregó el AWS Well-Architected Tool conector para Jira.	16 de abril de 2024
Lentes nuevas	Esta versión agregó nuevos lentes al catálogo de lentes.	26 de marzo de 2024
Funcionalidad actualizada	Esta versión añade la función de catálogo de lentes a AWS WA Tool.	26 de noviembre de 2023
Funcionalidad actualizada	Esta versión añade la función de revisión de plantillas a AWS WA Tool.	3 de octubre de 2023
WellArchitectedConsoleReadOnlyAccess política gestionada actualizada	Se agregó "wellarchitected:ExportLens" a WellArchitectedConsoleReadOnlyAccess .	22 de junio de 2023
Funcionalidad actualizada	Esta versión añade la función de perfiles a AWS WA Tool.	13 de junio de 2023
Funcionalidad actualizada	Esta versión mejora la AWS Service Catalog AppRegistry integración AWS Trusted Advisor y la añade AWS WellArchitectedDis	3 de mayo de 2023

	<code>coveryServiceRolePolicy</code> a las políticas AWS gestionadas.	
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 <code>WellArchitectedConsoleReadOnlyAccess</code> .	19 de enero de 2023
Se actualizó la guía de IAM para AWS WA Tool	Se ha actualizado la guía 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 AWS Service Catalog AppRegistry integración AWS Trusted Advisor y.	7 de noviembre de 2022
Actualización del contenido	Se ha corregido un problema en el ejemplo de JSON de enfoque personalizado para <code>choices</code> .	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 AWS gestionadas y ha añadido una nueva acción para conceder el ListAWSServiceAccessForOrganization permiso aAWSWellArchitectedOrganizationsServiceRolePolicy .	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 Re:post. AWS	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
EventBridge soporte agregado	AWS WA Tool ahora envía un evento a Amazon EventBridge cuando se realiza un cambio en un recurso de Well-Architected.	3 de marzo de 2022
Se agregaron enfoques personalizados	Se ha añadido la posibilidad de añadir enfoques personalizados.	29 de noviembre de 2021
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	Esta versión añade la AWS WA Tool API. 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 agregó una sección sobre cómo se AWS usan sus datos.	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 aclaró que las cargas de trabajo compartidas son Región de AWS específicas para cada persona.	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 DeleteWorkload acción 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](#)

En esta versión se añade la posibilidad de especificar que no es así Regiones de AWS al definir una carga de trabajo.

14 de febrero de 2019

[AWS Well-Architected Tool disponibilidad general](#)

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.