Guía del usuario

AWS Support

Versión de API 2013-04-15

AWS Support: Guía del usuario

Table of Contents

Empezar con AWS Support

AWS Support ofrece una gama de planes que brindan acceso a herramientas y experiencia que respaldan el éxito y el buen estado operativo de sus AWS soluciones. Todos los planes de soporte ofrecen acceso ininterrumpido al servicio de atención al cliente, a AWS la documentación, a los documentos técnicos y a los foros de soporte. Si necesita soporte técnico y más recursos para planificar, implementar y mejorar su AWS entorno, puede elegir un plan de soporte para su caso de AWS uso.

Notas

- Para crear un caso de soporte en el AWS Management Console, consulteCreación de un caso de soporte.
- Para obtener más información sobre los diferentes AWS Support planes, consulte Comparar AWS Support planes y¿Cambiar AWS Support los planes.
- Los planes de soporte ofrecen diferentes tiempos de respuesta para sus casos. Consulte Elección de la gravedad y Tiempos de respuesta.

Temas

Creación de casos de soporte y administración de casos

En el AWS Management Console, puede crear tres tipos de casos de clientes en AWS Support:

- Los casos de Soporte de cuenta y facturación están disponibles para todos los clientes de AWS . Puede obtener ayuda para preguntas acerca de la facturación y la cuenta.

- Las solicitudes de aumento del límite de servicio están disponibles para todos los clientes de AWS . Para más información acerca de las cuotas de servicio predeterminadas, anteriormente denominadas límites, consulte Cuotas de servicio de AWS, en la Referencia general de AWS.
- Los casos de Soporte técnico le ponen en contacto con el servicio de asistencia técnica para obtener ayuda en cuestiones técnicas y, en algunos casos, aplicaciones de terceros. Si tiene el plan de soporte Basic, no puede crear un caso de soporte técnico.

> **Notas**
>
> - Para cambiar el plan de soporte, consulte ¿Cambiar AWS Support los planes.
> - Para cerrar su cuenta, consulte Cierre de una cuenta en la Guía del usuario de AWS Billing .
> - Para encontrar temas comunes de solución de problemas Servicios de AWS, consulteRecursos para la resolución de problemas.
> - Si es cliente de una empresa AWS Partner que forma parte del Resold Support y lo utiliza AWS Partner Network, póngase en contacto con usted AWS Partner directamente para cualquier problema relacionado con la facturación. AWS Support no puede ayudar con problemas no técnicos para Resold Support, como la facturación y la administración de cuentas. Para obtener más información, consulte los temas siguientes:
>   - Cómo pueden AWS los socios determinar AWS Support los planes de una organización
>   - Compatibilidad guiada por AWS Partner

Creación de un caso de soporte

Puede crear un caso de soporte técnico en el Centro de asistencia de la AWS Management Console.

> **Notas**
>
> - Puede iniciar sesión en Support Center como usuario root de su AWS cuenta o como usuario AWS Identity and Access Management (IAM). Para obtener más información, consulte Administre el acceso al AWS Support Centro.

- Si no puede iniciar sesión en el Centro de asistencia ni crear un caso de soporte, puede utilizar la página Contacte con nosotros en su lugar. Puede utilizar esta página para obtener ayuda con problemas relacionados con las cuentas y la facturación.

Crear un caso de soporte

1. Inicie sesión en la AWS Support Center Console.

   > **Tip**
   >
   > En AWS Management Console, también puede elegir el icono del signo de interrogación () y, a continuación, elegir Support Center.

2. Elija Crear caso.
3. Seleccione una de las siguientes opciones:

   - Cuenta y facturación
   - Técnica
   - Para aumentar la cuota de servicios, elija Looking for service limit increases? (¿Busca aumentos del límite de servicio?) y siga las instrucciones para Creación de un aumento de cuotas de servicio.

4. Elija Service (Servicio) ,Category (Categoría) ySeverity (Gravedad).

   > **Tip**
   >
   > Puede utilizar las soluciones recomendadas que aparecen para las preguntas frecuentes.

5. Elija Next step: Additional information (Paso siguiente: Información adicional).
6. En la página Additional information (Información adicional), para Subject (Asunto), introduzca un título sobre su problema.
7. En Description (Descripción), siga las instrucciones para describir su caso, como se indica a continuación:

   - Mensajes de error que ha recibido

- Pasos de solución de problemas que ha seguido
- Cómo accede al servicio:
  - AWS Management Console
  - AWS Command Line Interface (AWS CLI)
  - Operaciones de la API

8. (Opcional) Elija Attach files (Adjuntar archivos) para añadir cualquier archivo relevante a su caso, como registros de errores o capturas de pantalla. Puede adjuntar hasta tres archivos. Cada archivo puede ser de hasta 5 MB.
9. Elija Siguiente paso: Resuelva ahora o póngase en contacto con nosotros.
10. En la página Contacte con nosotros, elija su idioma preferido.
11. Cambie el método de contacto preferido. Puede elegir una de las siguientes opciones:

    a. Web: reciba una respuesta en el Centro de Soporte.

    b. Chat: inicie un chat en vivo con un agente de soporte. Si no puede conectarse a un chat, consulte Resolución de problemas.

    c. Phone (Teléfono): reciba una llamada telefónica de un agente de soporte. Si elige esta opción, ingrese la siguiente información:

       - País o región
       - Número de teléfono
       - (Opcional) Extensión

    > **Notas**
    >
    > - Las opciones de contacto que se muestran dependen del tipo de caso y de su plan de soporte.
    > - Puede elegir Discard draft (Descarte el borrador) para eliminar el borrador de su caso de soporte.

12. (Opcional) Si tiene un plan Business, Enterprise OnRamp o Support Enterprise, se muestra la opción Additional contacts (Contactos adicionales). Puede ingresar las direcciones de correo electrónico de las personas a las que se va enviar una notificación cuando cambie el estado del caso. Si ha iniciado sesión como usuario de IAM, incluya su dirección de correo electrónico. Si

ha iniciado sesión con su dirección de correo electrónico y contraseña de la cuenta raíz, no es necesario que incluya su dirección de correo electrónico.

> **Note**
>
> Si tiene el plan de soporte Basic, la opción Additional contacts (Contactos adicionales) no está disponible. Sin embargo, el contacto Operational (Operativo) especificado en la sección Alternate Contacts (Contactos alternativos) de la página My Account (Mi cuenta) recibe copias de la correspondencia del caso, pero solo para los tipos de caso específicos de cuenta, facturación y soporte técnico.

13. Revise los detalles de su caso y elija Submit (Enviar). Aparecerán el número de ID del caso y el resumen.

Descripción del problema

Incluya una descripción lo más detallada posible. Incluya la información pertinente de los recursos, junto con cualquier otra información que pudiera contribuir a entender el problema. Por ejemplo, para resolver los problemas de rendimiento, incluya marcas temporales y registros. Para solicitudes de características o preguntas de orientación general, incluya una descripción de su entorno y el propósito. En todos los casos, siga la guía de Descripción orientativa que aparece en el formulario de envío de caso.

Si proporciona la máxima información posible, aumenta la probabilidad de que su caso se pueda resolver rápidamente.

Elección de la gravedad

Es posible que esté inclinado a crear siempre un caso de soporte con la máxima gravedad que permita su plan de soporte. Sin embargo, le recomendamos que elija las máximas gravedades para los casos que no puedan solucionarse o que afecten directamente a las aplicaciones de producción. Para obtener información sobre la creación de sus servicios para que la pérdida de recursos únicos no afecte a sus aplicaciones, consulte el documento técnico Building Fault-Tolerant Applications on AWS.

En la tabla siguiente se enumeran los niveles de gravedad, los tiempos de respuesta y problemas de ejemplo.

Notas

- No puede cambiar el código de gravedad de un caso de soporte después de crearlo. Si su situación cambia, trabaje con el AWS Support agente para su caso de soporte.
- Para obtener más información sobre el nivel de gravedad, consulte la Referencia de la API de AWS Support.

Gravedad	Código del nivel de gravedad	Tiempo de primera respuesta	Descripción y plan de soporte
General guidance	`low`	24 horas	Tiene una pregunta de desarrollo general o quiere solicitar una característica. (Plan de soporte Developer*, Business, Enterprise On-Ramp o Enterprise)
System impaired	`normal`	12 horas	Las funciones no críticas de su aplicación tienen un comportamiento anómalo o tiene una pregunta de desarrollo prioritaria. (Plan de soporte Developer*, Business, Enterprise On-Ramp o Enterprise)
Production system impaired	`high`	4 horas	Las funciones importantes de su aplicación se han deteriorado o degradado. (Plan de soporte Business, Enterprise On-Ramp o Enterprise)
Production system down	`urgent`	1 hora	Su negocio se ve afectado significativamente . Funciones importantes de su aplicación no están disponibles. (Plan de soporte Business, Enterprise On-Ramp o Enterprise)
Business-critical system down	`critical`	15 minutos	Su empresa está en riesgo. Hay funciones críticas de su aplicación que no están disponibl es (plan de soporte Enterprise). Tenga en

Gravedad	Código del nivel de gravedad	Tiempo de primera respuesta	Descripción y plan de soporte
			cuenta que en el plan de soporte Enterprise On-Ramp es de 30 minutos.

Tiempos de respuesta

Hacemos todo lo posible por responder a la solicitud inicial en el plazo indicado. Para obtener información sobre el alcance del soporte de cada AWS Support plan, consulte AWS Support las características.

Si tiene un plan de soporte Business, Enterprise On-Ramp o Enterprise, tiene acceso a Soporte técnico las 24 horas, los 7 días de la semana. *En el plan de soporte Developer, los objetivos de respuesta para los casos se calculan en horas laborables. El horario comercial abarca generalmente desde las 08:00 hasta las 18:00 horas en el país del cliente, excepto fines de semana y días festivos. Estos tiempos pueden variar en países con varias zonas horarias. La información del país del cliente aparece en la sección Información de contacto de la página Cuenta en la AWS Management Console.

> **Note**
>
> Si elige el japonés como idioma de contacto de preferencia para los casos de soporte, el soporte en japonés estará disponible de la siguiente manera:
>
> - Si necesita el servicio de atención al cliente para casos de soporte no técnico, o si tiene un plan de soporte para desarrolladores y necesita soporte técnico, el soporte en japonés está disponible durante el horario laboral en Japón, definido desde las 9 h hasta las 18 h, hora estándar de Japón (GMT+9), excepto en días festivos y fines de semana.
> - Si tiene un plan de soporte Business, Enterprise On-Ramp o Enterprise, el soporte técnico está disponible las 24 horas, los 7 días de la semana en japonés.
>
> Si elige el chino como idioma de contacto de preferencia para los casos de soporte, el soporte en chino estará disponible de la siguiente manera:

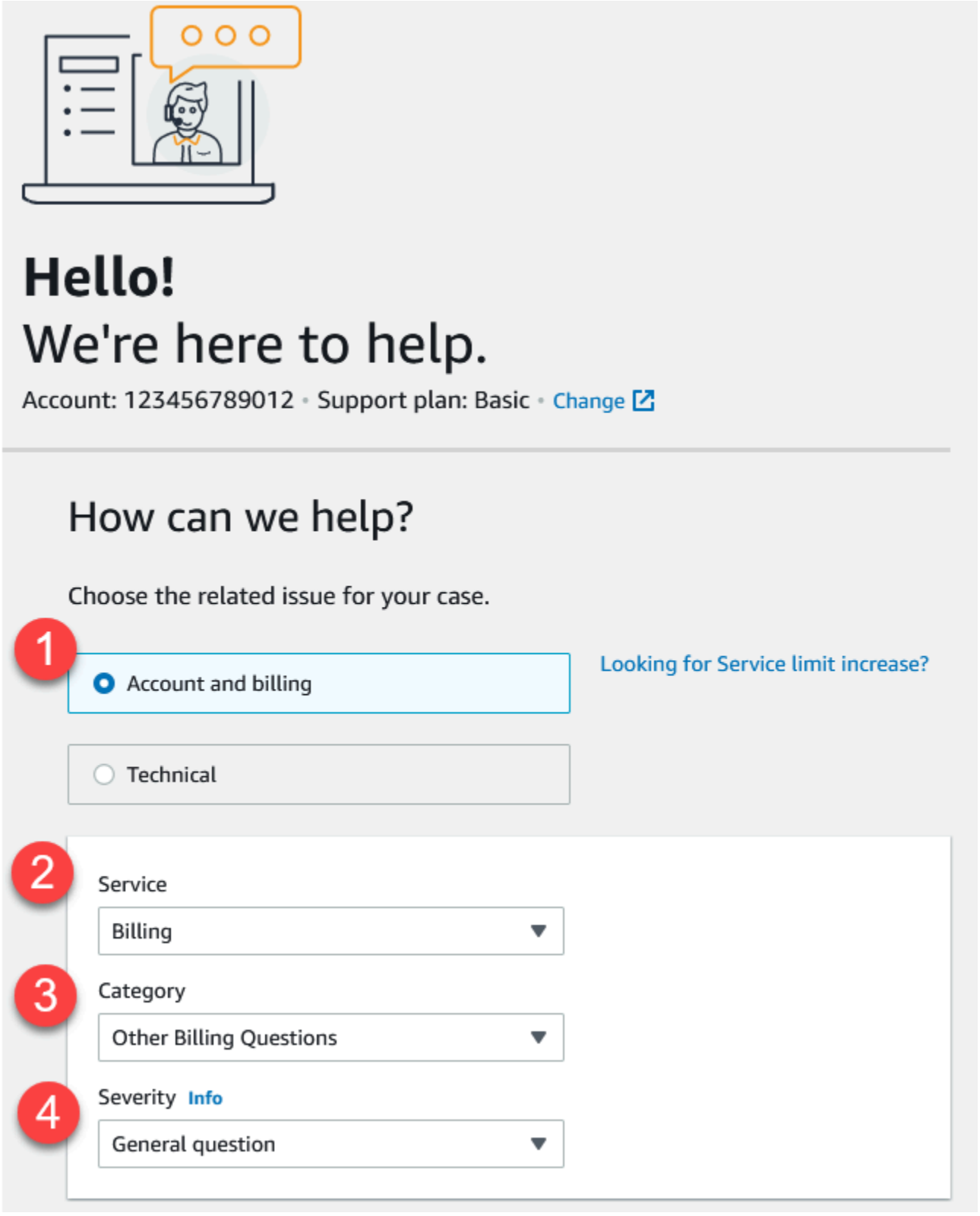
- Si necesita servicio de atención al cliente para casos de soporte no técnico, el soporte en chino está disponible desde las 9 h hasta las 18 h (GMT+8), excepto en días festivos y fines de semana.
- Si tiene un plan de soporte para desarrolladores, el soporte técnico en chino está disponible durante el horario laboral, generalmente desde las 8 h hasta las 18 h de su país, según lo establecido en Mi cuenta, excepto en días festivos y fines de semana. Estos horarios pueden variar en países con varias zonas horarias.
- Si tiene un plan de soporte Business, Enterprise On-Ramp o Enterprise, el soporte técnico está disponible las 24 horas, los 7 días de la semana en chino.

Si elige el coreano como idioma de contacto de preferencia para los casos de soporte, el soporte en coreano estará disponible de la siguiente manera:

- Si necesita servicio de atención al cliente para casos de soporte no técnico, el soporte en coreano está disponible durante el horario laboral de Corea, definido desde las 9 h hasta las 18 h, hora estándar de Corea (GMT+9), excepto en días festivos y fines de semana.
- Si tiene un plan de soporte para desarrolladores, el soporte técnico en coreano está disponible durante el horario laboral, generalmente desde las 8 h hasta las 18 h de su país, según lo establecido en Mi cuenta, excepto en días festivos y fines de semana. Estos horarios pueden variar en países con varias zonas horarias.
- Si tiene un plan de soporte Business, Enterprise On-Ramp o Enterprise, el soporte técnico está disponible las 24 horas, los 7 días de la semana en coreano.

Ejemplo: Crear un caso de soporte para cuentas y facturación

El siguiente ejemplo es un caso de soporte para un problema de facturación y cuenta.



1. Crear caso: elija el tipo de caso que quiere crear. En este ejemplo, el tipo de caso es Cuenta y facturación.

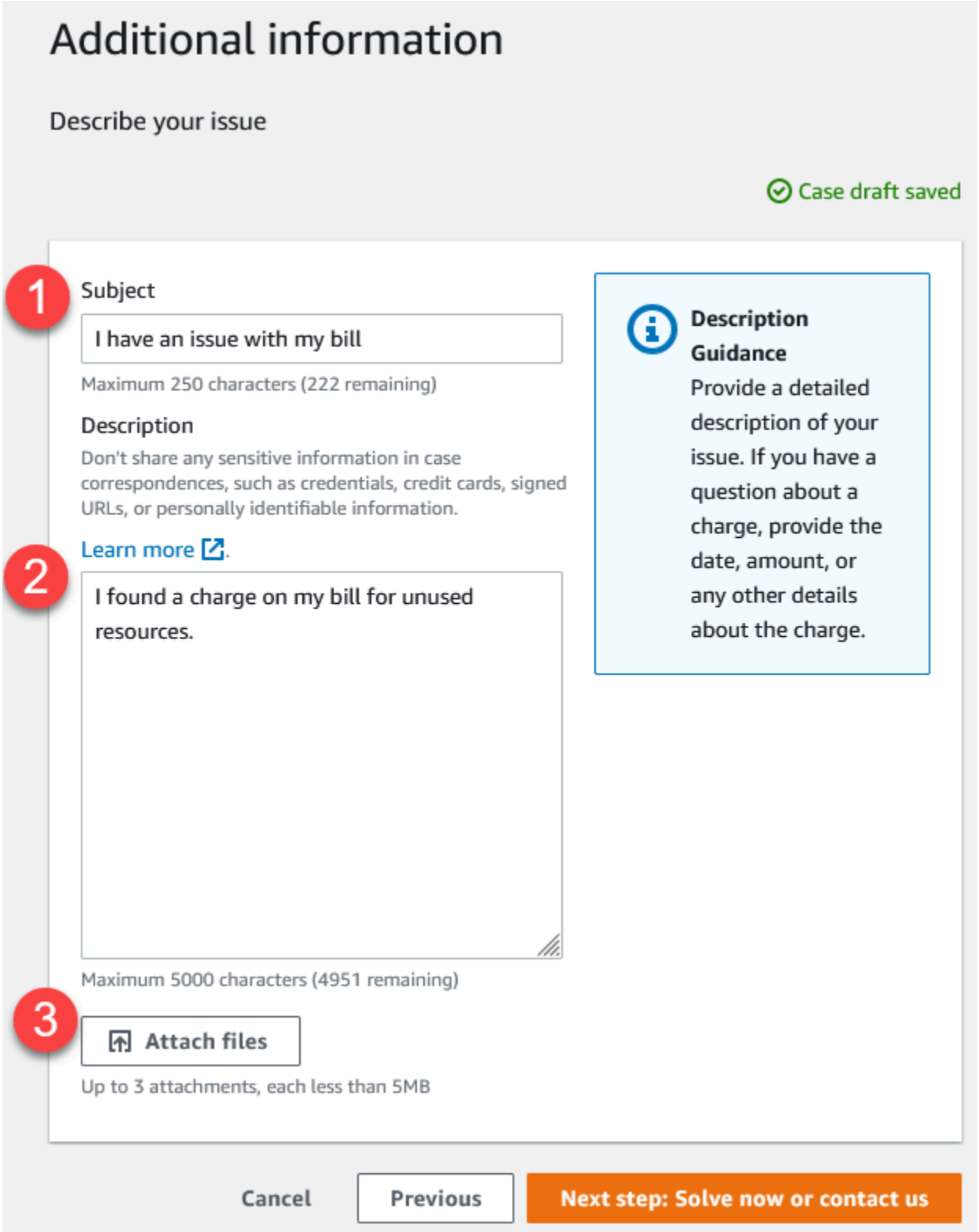
> **Note**
>
> Si tiene el plan de soporte Basic, no puede crear un caso de soporte técnico.

2. Service (Servicio): si su pregunta afecta a varios servicios, elija el servicio más adecuado.
3. Category (Categoría): elija la categoría que mejor se adapte a su caso de uso. Al elegir una categoría, los vínculos a la información que podría resolver el problema aparecen debajo.
4. Severity (Severidad): los clientes con un plan de soporte de pago pueden elegir el nivel de severidad General guidance (Orientación general) (respuesta en 1 día) o System impaired (Error del sistema) (tiempo de respuesta de 12 horas). Los clientes con un plan de soporte Business también pueden elegir Production system impaired (respuesta en 4 horas) o Production system down (respuesta en 1 hora). Los clientes con un plan de soporte Enterprise On-Ramp o Enterprise pueden elegir Business-critical system down (Sistema crítico para la empresa inactivo) (respuesta en 15 minutos para el soporte Enterprise y respuesta en 30 minutos para Enterprise On-Ramp).

   Los tiempos de respuesta se refieren a la primera respuesta de AWS Support. Estos tiempos de respuesta no se aplican a las respuestas posteriores. Para problemas de terceros, los tiempos de respuesta puede ser más largos, en función de la disponibilidad del personal cualificado. Para más información, consulte Elección de la gravedad.

   > **Note**
   >
   > En función de la elección de categoría, es posible que se le solicite más información.

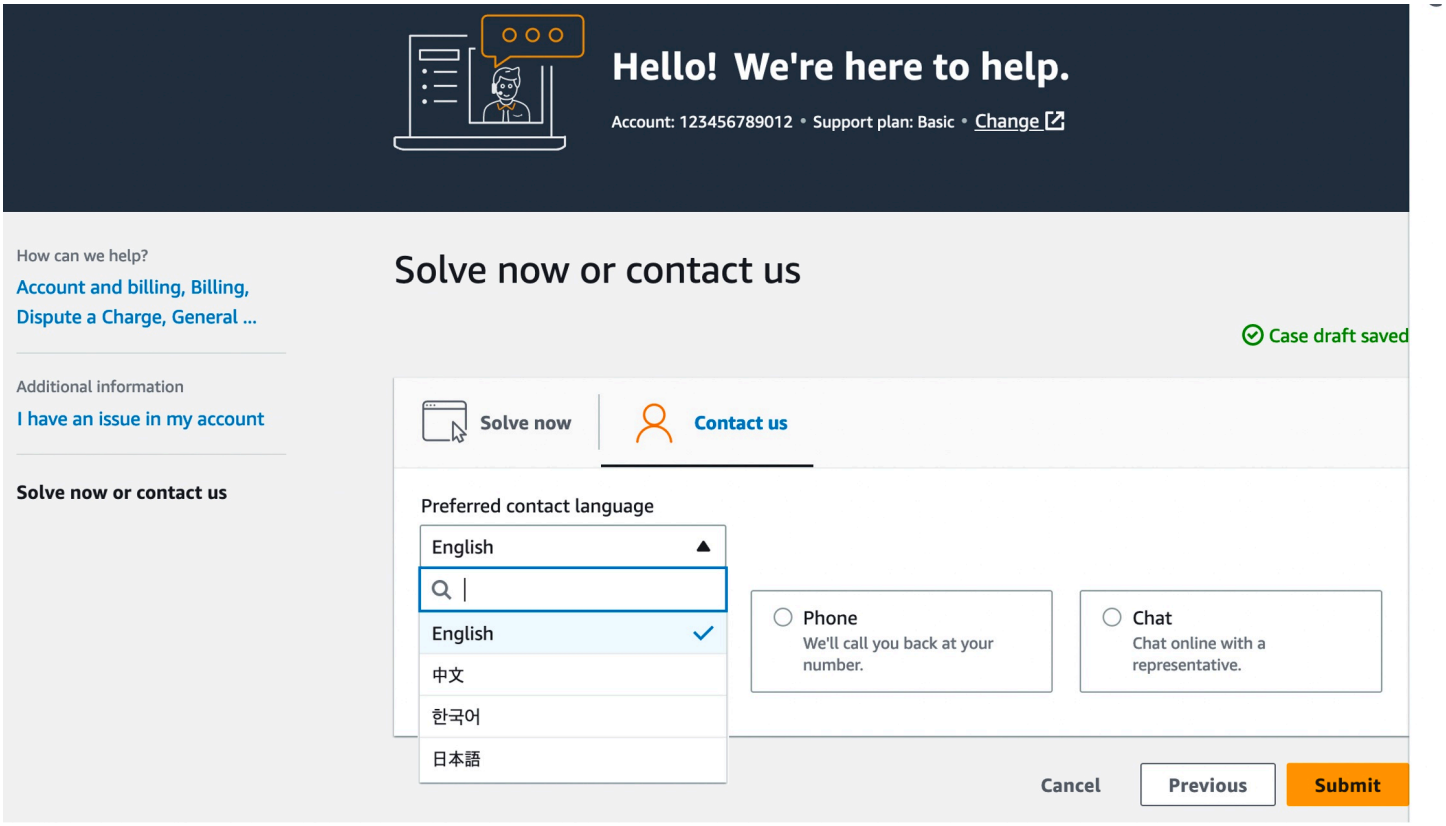
Después de especificar el tipo de caso y la clasificación, puede especificar la descripción y cómo desea ser contactado.



1. Subject (Asunto): ingrese un título que describa brevemente su problema.

2. Description (Descripción): describa su caso de soporte. Esta es la información más importante que va a proporcionar a AWS Support. Para algunas combinaciones de servicio y categoría, aparece un mensaje con información relacionada. Utilice estos enlaces para ayudar a resolver el problema. Para más información, consulte Descripción del problema.
3. Attachments (Archivos adjuntos): las capturas de pantalla y otros archivos adjuntos pueden ayudar a los agentes de soporte a resolver su caso más rápido. Puede adjuntar hasta tres archivos. Cada archivo puede ser de hasta 5 MB.

Después de agregar los detalles de su caso, puede elegir cómo desea que lo contacten.



1. Idioma de contacto de preferencia: elija el idioma que prefiera. En la actualidad, puede elegir entre chino, inglés, japonés o coreano. El plan de soporte mostrará las opciones de contacto personalizadas en el idioma de preferencia.
2. Elija un método de contacto. Las opciones de contacto que se muestran dependen del tipo de caso y de su plan de soporte.
   - Si elige Web, puede leer y responder a los avances del caso en el Centro de asistencia.

- Elija Chat o Phone (Teléfono). Si selecciona Phone (Teléfono), se solicita un número de devolución de llamada.

3. Seleccione Submit (Enviar) cuando haya completado la información y esté listo para crear el caso.

> **Note**
>
> Si elige el japonés como idioma de contacto de preferencia para los casos de soporte, el soporte en japonés estará disponible de la siguiente manera:
>
> - Si necesita el servicio de atención al cliente para casos de soporte no técnico, o si tiene un plan de soporte para desarrolladores y necesita soporte técnico, el soporte en japonés está disponible durante el horario laboral en Japón, definido desde las 9 h hasta las 18 h, hora estándar de Japón (GMT+9), excepto en días festivos y fines de semana.
> - Si tiene un plan de soporte Business, Enterprise On-Ramp o Enterprise, el soporte técnico está disponible las 24 horas, los 7 días de la semana en japonés.
>
> Si elige el chino como idioma de contacto de preferencia para los casos de soporte, el soporte en chino estará disponible de la siguiente manera:
>
> - Si necesita servicio de atención al cliente para casos de soporte no técnico, el soporte en chino está disponible desde las 9 h hasta las 18 h (GMT+8), excepto en días festivos y fines de semana.
> - Si tiene un plan de soporte para desarrolladores, el soporte técnico en chino está disponible durante el horario laboral, generalmente desde las 8 h hasta las 18 h de su país, según lo establecido en Mi cuenta, excepto en días festivos y fines de semana. Estos horarios pueden variar en países con varias zonas horarias.
> - Si tiene un plan de soporte Business, Enterprise On-Ramp o Enterprise, el soporte técnico está disponible las 24 horas, los 7 días de la semana en chino.
>
> Si elige el coreano como idioma de contacto de preferencia para los casos de soporte, el soporte en coreano estará disponible de la siguiente manera:
>
> - Si necesita servicio de atención al cliente para casos de soporte no técnico, el soporte en coreano está disponible durante el horario laboral de Corea, definido desde las 9 h hasta las 18 h, hora estándar de Corea (GMT+9), excepto en días festivos y fines de semana.

- Si tiene un plan de soporte para desarrolladores, el soporte técnico en coreano está disponible durante el horario laboral, generalmente desde las 8 h hasta las 18 h de su país, según lo establecido en Mi cuenta, excepto en días festivos y fines de semana. Estos horarios pueden variar en países con varias zonas horarias.
- Si tiene un plan de soporte Business, Enterprise On-Ramp o Enterprise, el soporte técnico está disponible las 24 horas, los 7 días de la semana en coreano.

Resolución de problemas

Si tiene dificultades para crear o administrar el caso de soporte, consulte la siguiente información de solución de problemas.

Quiero volver a abrir un chat en vivo de mi caso

Puede responder al caso de soporte existente para abrir otra ventana de chat. Para más información, consulte Actualización de un caso de soporte existente.

No puedo conectarme a un chat en vivo

Si eligió la opción Chat pero no puede conectarse a la ventana de chat, realice primero las siguientes comprobaciones:

- Asegúrese de haber configurado el navegador para que permita ventanas emergentes en el Centro de soporte.

  > **Note**
  >
  > Revise la configuración del navegador. Para obtener más información, consulte los sitios web de Ayuda de Chrome y Soporte de Firefox.

- Asegúrese de haber configurado la red para poder utilizar AWS Support:
  - La red puede acceder al punto de conexión `*.connect.us-east-1.amazonaws.com`.

    > **Note**
    >
    > En AWS GovCloud (US), el punto de conexión es `*.connect-fips.us-east-1.amazonaws.com`.

- El firewall admite conexiones de socket web.

Si sigue sin poder conectarse a la ventana del chat, póngase en contacto con AWS Support mediante las opciones de contacto por correo electrónico o teléfono.

Creación de un aumento de cuotas de servicio

Para mejorar el rendimiento de su servicio, solicite aumentos de sus cuotas de servicio (anteriormente denominadas límites).

> **Note**
>
> También puede utilizar el servicio Service Quotas para solicitar aumentos directamente para sus servicios. Actualmente, las Service Quotas no admiten cuotas de servicio para todos los servicios. Para obtener más información, consulte ¿Qué es Service Quotas? en la Guía del usuario de Service Quotas.

Para crear un caso de soporte para un aumento de cuotas de servicios.

1. Inicie sesión en AWS Support Center Console.

   > **Tip**
   >
   > En la AWS Management Console, también puede elegir el icono de signo de interrogación
   > ()
   > y luego Support Center (Centro de soporte).

2. Elija Create case (Crear caso).
3. Elija Looking for service limit increases? (¿Busca aumentos del límite de servicio?)
4. Para solicitar un aumento, siga las instrucciones. Las posibles opciones incluyen lo siguiente:

   - Tipo de límite
   - Gravedad

> **Note**
>
> En función de la elección de categoría, es posible que las instrucciones soliciten más información.

5. Para Requests (Solicitudes), elija la Region (Región).
6. En Limit (Límite), elija el tipo de límite para el servicio.
7. En New limit value (Nuevo valor de límite), indique el valor que desea.
8. (Opcional) Para solicitar otro aumento, elija Add another request (Agregar otra solicitud).
9. En Case description (Descripción del caso), describa su caso de soporte.
10. En Contact options (Opciones de contacto), elija su idioma preferido y cómo quiere que lo contacten. Puede elegir una de las siguientes opciones:
    - Web: reciba una respuesta en el Centro de Soporte.
    - Chat: inicie un chat en vivo con un agente de soporte. Si no puede conectarse a un chat, consulte Resolución de problemas.
    - Phone (Teléfono): reciba una llamada telefónica de un agente de soporte. Si elige esta opción, ingrese la siguiente información:
      - País/Región
      - Número de teléfono
      - (Opcional) Extensión
11. Elija Submit (Enviar). Aparecerán el número de ID del caso y el resumen.

Actualización, resolución y reapertura de su caso

Una vez creado el caso de soporte, puede monitorear el estado del caso en el Centro de asistencia. Un caso nuevo comienza con el estado Sin asignar. Cuando un agente de soporte empieza a trabajar en un caso, el estado cambia a Trabajo en curso. El agente de soporte puede responder a su caso para pedir más información (Acción del cliente pendiente) o para informarle de que el caso se está investigando (Acción de Amazon pendiente).

Cuando su caso se actualice, recibirá un correo electrónico con la correspondencia y un enlace al caso en Centro de asistencia. Utilice el enlace del mensaje de correo electrónico para ir al caso de soporte. No puede responder a las correspondencias del caso por correo electrónico.

Notas

- Debe iniciar sesión en la Cuenta de AWS desde la que se envió el caso de soporte. Si inicia sesión como usuario de AWS Identity and Access Management (IAM), debe tener los permisos necesarios para ver casos de soporte técnico. Para obtener más información, consulte Administre el acceso al AWS Support Centro.
- Si no responde al caso en unos días, AWS Support lo resuelve automáticamente.
- Los casos de soporte que han estado resueltos durante más de 14 días no se pueden volver a abrir. Si tiene un problema similar relacionado con el caso resuelto, puede crear un caso relacionado. Para obtener más información, consulte Creación de un caso relacionado.

Temas

Actualización de un caso de soporte existente

Puede actualizar su caso para proporcionar más información al agente de soporte. Por ejemplo, puede responder a las correspondencias, iniciar otro chat en vivo, agregar destinatarios de correo electrónico adicionales, etc. Sin embargo, no puede actualizar la gravedad de un caso después de crearlo. Para obtener más información, consulte Elección de la gravedad.

Para actualizar un caso de soporte existente

1. Inicie sesión en AWS Support Center Console.

   Tip

   En la AWS Management Console, también puede elegir el icono de signo de interrogación

()
y luego Support Center (Centro de soporte).

2. En Open support cases (Casos de soporte abiertos), elija el Subject (Asunto) del caso de soporte.
3. Elija Reply (Responder). En la sección Correspondence (Correspondencia), también puede realizar cualquiera de los siguientes cambios:
   - Proporcionar la información que solicitó el agente de soporte
   - Cargar archivos adjuntos
   - Cambiar el método de contacto preferido
   - Agregar direcciones de correo electrónico para recibir actualizaciones de casos
4. Elija Submit (Enviar).

> **Tip**
>
> Si cerró una ventana de chat y desea iniciar otro chat en vivo, puede agregar una Reply (Respuesta) al caso de soporte, elegir Chat (Chat) y, a continuación, seleccionar Submit (Enviar). Se abre una nueva ventana de chat emergente.

Resolución de un caso de soporte

Cuando esté satisfecho con la respuesta o se solucione su problema, puede resolver el caso en el Centro de asistencia.

Para resolver un caso de soporte

1. Inicie sesión en AWS Support Center Console.

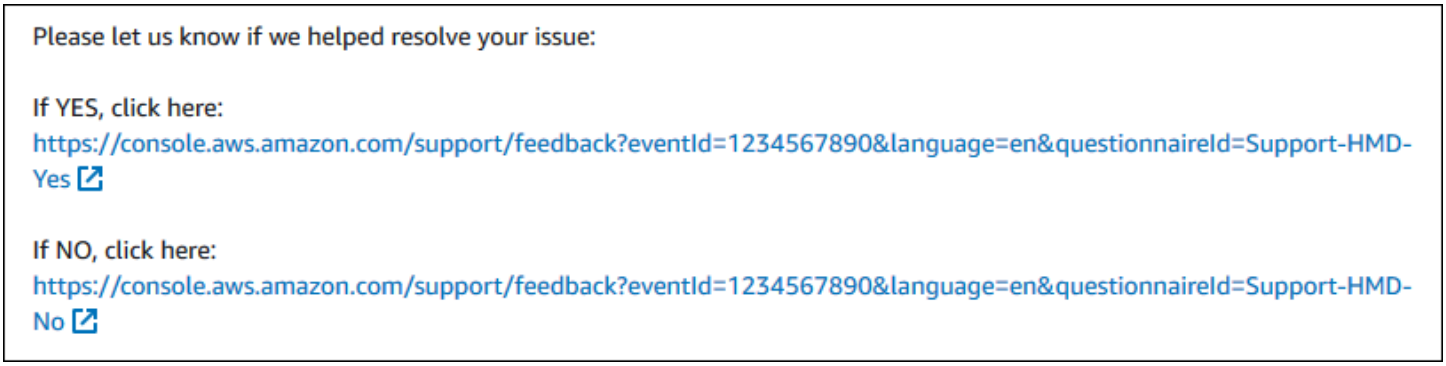
> **Tip**
>
> En la AWS Management Console, también puede elegir el icono de signo de interrogación
> ()
> y luego Support Center (Centro de soporte).

2. En Open support cases (Casos de soporte abiertos), elija el Subject (Asunto) del caso de soporte que desea resolver.
3. (Opcional) Elija Reply (Responder) y, en la sección Correspondence (Correspondencia), ingrese por qué resuelve el caso y, a continuación, elija Submit (Enviar). Por ejemplo, puede ingresar información sobre cómo solucionó el problema por su cuenta en caso de que necesite esta información para futuras referencias.
4. Elija Resolve case (Resolver el caso).
5. En el cuadro de diálogo, elija Ok (Aceptar) para resolver el caso.

> **Note**
>
> Si AWS Support ha resuelto su caso, puede utilizar el enlace de comentarios para ofrecer más información sobre su experiencia con AWS Support.

Example : Enlaces de comentarios

La siguiente captura de pantalla muestra los enlaces de comentarios en la correspondencia de un caso en el Centro de asistencia.



Reapertura de un caso resuelto

Si vuelve a experimentar el mismo problema, puede volver a abrir el caso original. Proporcione detalles acerca de cuándo se produjo de nuevo el problema y qué pasos ha intentado para solucionar el problema. Incluya cualquier número de caso relacionado para que el agente de soporte pueda consultar las correspondencias anteriores.

Notas

- Puede reabrir el caso de soporte hasta 14 días desde que se resolvió el problema. Sin embargo, no puede reabrir un caso que haya estado inactivo durante más de 14 días. Puede crear un caso nuevo o un caso relacionado. Para obtener más información, consulte Creación de un caso relacionado.
- Si reabre un caso existente que tiene información diferente a la del problema actual, es posible que el agente de soporte le pida que cree un caso nuevo.

Para reabrir un caso resuelto

1. Inicie sesión en AWS Support Center Console.

   Tip

   En la AWS Management Console, también puede elegir el icono de signo de interrogación
   ()
   y luego Support Center (Centro de soporte).

2. Elija View all cases (Ver todos los casos) y, a continuación, elija el Subject (Asunto) o el Case ID (Identificador del caso) del caso de soporte que desee reabrir.
3. Elija Reopen case (Reabrir caso).
4. En Correspondence (Correspondencia), en Reply (Responder), ingrese los detalles del caso.
5. (Opcional) Elija Choose files (Elegir archivos) para adjuntar archivos a su caso. Puede adjuntar un máximo de 3 archivos.
6. En Contact Methods (Métodos de contacto), elija una de las siguientes opciones:
   - Web: reciba una notificación por correo electrónico y el Centro de asistencia.
   - Chat (Conversación): converse en línea con un agente de soporte.
   - Phone (Teléfono): reciba una llamada telefónica de un agente de soporte.
7. (Opcional) En Additional contacts (Contactos adicionales), ingrese las direcciones de correo electrónico de otras personas que desea que reciban correspondencias del caso.
8. Revise los detalles de su caso y elija Submit (Enviar).

Creación de un caso relacionado

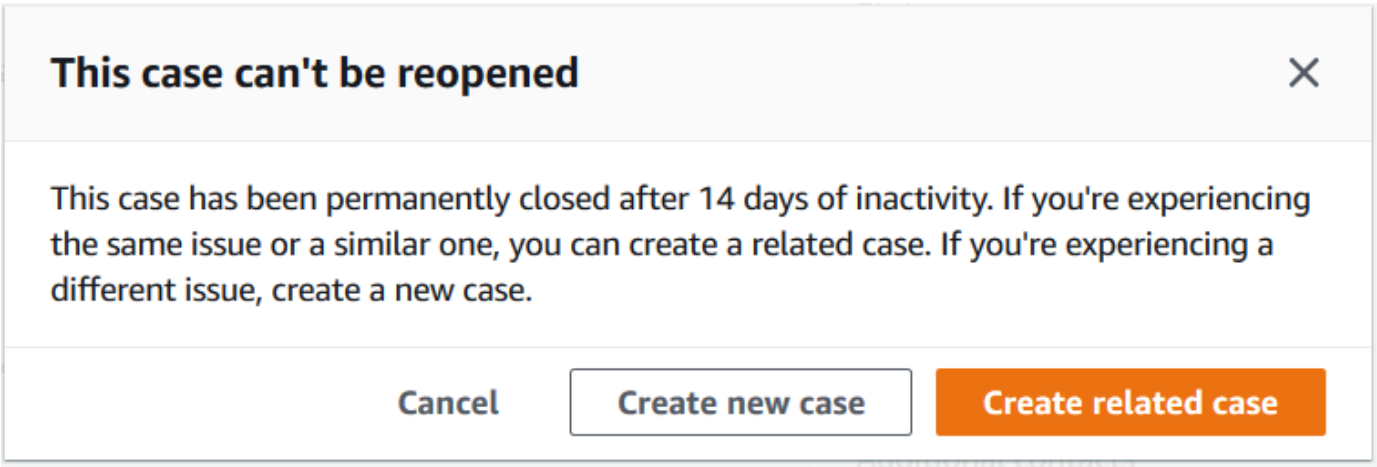
Después de 14 días de inactividad, no puede reabrir un caso resuelto. Si tiene un problema similar relacionado con el caso resuelto, puede crear un caso relacionado. Este caso relacionado incluirá un enlace al caso previamente resuelto, de modo que el agente de soporte podrá revisar los detalles del caso anterior y las correspondencias. Si tiene un problema diferente, le recomendamos que cree un caso nuevo.

Para crear un caso relacionado

1. Inicie sesión en AWS Support Center Console.

   > **Tip**
   >
   > En la AWS Management Console, también puede elegir el icono de signo de interrogación
   > ( )
   > y luego Support Center (Centro de soporte).

2. Elija View all cases (Ver todos los casos) y, a continuación, elija el Subject (Asunto) o el Case ID (Identificador del caso) del caso de soporte que desee reabrir.
3. Elija Reopen case (Reabrir caso).
4. En el cuadro de diálogo, elija Create related case (Crear caso relacionado). La información del caso anterior se agregará automáticamente al caso relacionado. Si tiene un problema diferente, elija Create new case (Crear caso nuevo).

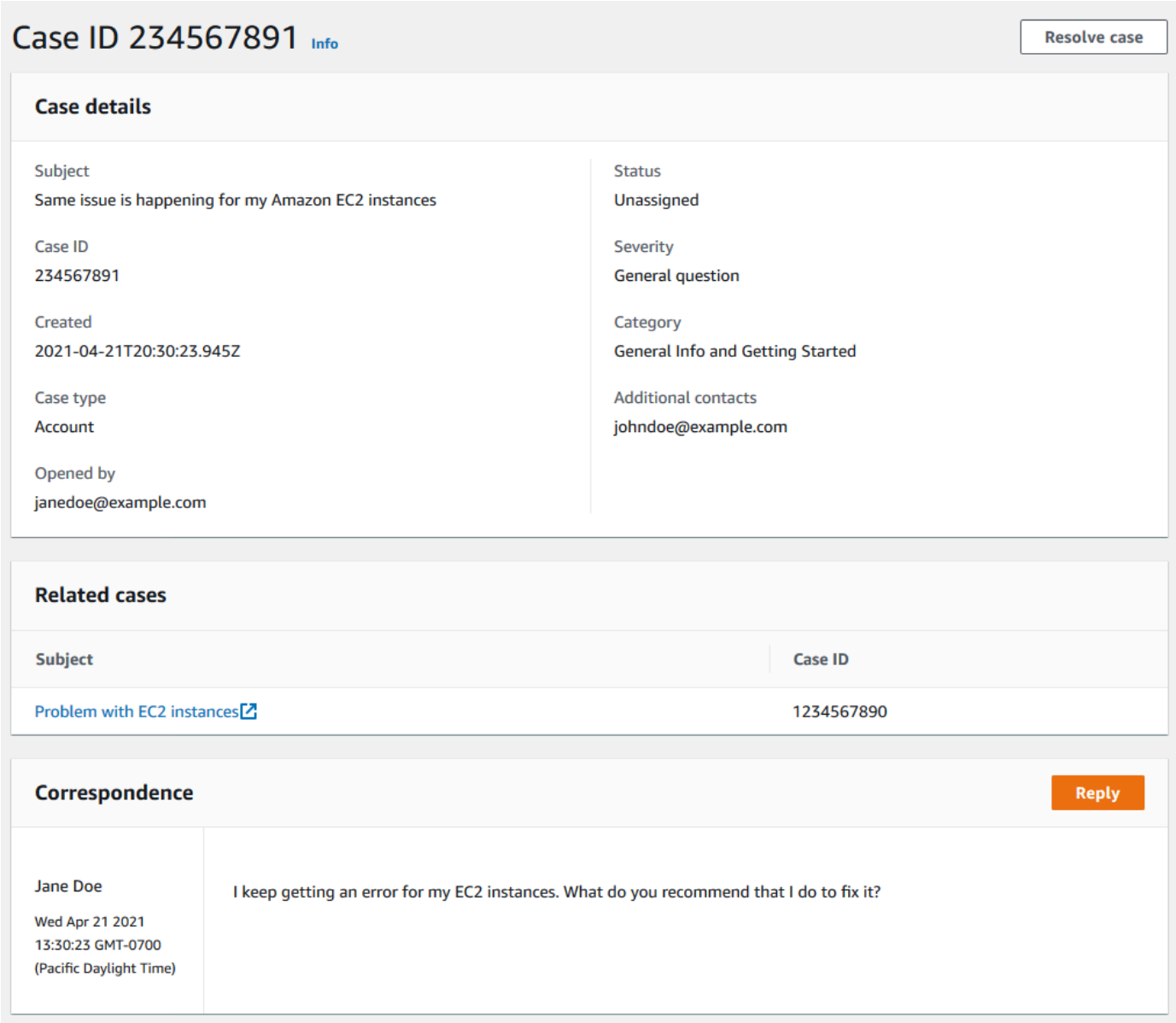
   

5. Para crear el caso, siga los mismos pasos. Consulte Creación de un caso de soporte.

> **Note**
>
> De forma predeterminada, su caso relacionado tiene el mismo Type (Tipo), Category (Categoría) y Severity (Severidad) que el caso anterior. Puede actualizar los detalles del caso según sea necesario.

6. Revise los detalles de su caso y elija Submit (Enviar).

Después de crear el caso, el caso anterior aparece en la sección Related cases (Casos relacionados), como en el ejemplo siguiente.



Historial de casos

Puede consultar la información del historial de casos hasta 24 meses después de haber creado el caso.

AWS Support Recomendaciones

> **Note**
>
> AWS Support Las recomendaciones se proporcionan como un «servicio de vista previa», tal como se define en las condiciones del AWS servicio. El servicio de vista previa está sujeto a cambios y cancelaciones. Más información.

AWS Support Recommendations te ofrece asistencia personalizada para solucionar problemas técnicos y relacionados con la cuenta durante el proceso de creación de casos en la consola AWS Support central. AWS Support Las recomendaciones se basan en los detalles del caso y en la cuenta en la que se ha iniciado sesión para responder con soluciones personalizadas que resuelvan el problema.

Para analizar los problemas, AWS Support Recommendations consulta información (como el AccountID, los identificadores de AWS recursos o el mensaje de error) en el ámbito de las políticas o los permisos de usuario aprobados. Más información.

Temas

- Administrar el acceso a AWS Support las recomendaciones
- Supervisión y registro de AWS Support recomendaciones

Administrar el acceso a AWS Support las recomendaciones

> **Note**
>
> AWS Support Las recomendaciones se proporcionan como un «servicio de vista previa», tal como se define en las condiciones del AWS servicio. El servicio de vista previa está sujeto a cambios y cancelaciones. Más información.

Puedes usar AWS Identity and Access Management (IAM) para gestionar el acceso a AWS Support las recomendaciones en la consola AWS Support central durante el proceso de creación de casos.

Temas

AWS Support Recomendaciones, acciones

Puede especificar AWS Support las acciones de recomendación en una política de IAM para proporcionar acceso total, denegar el acceso completo o proporcionar o denegar el acceso a acciones específicas.

Acción	Descripción
`StartSupportTroubleshooting`	Inicie una sesión guiada de solución de problemas para ayudar a diagnosticar y resolver los problemas técnicos o de la cuenta durante el proceso de creación de casos en la consola AWS Support central.
`GetSupportTroubleshootingResponse`	Recupera el estado actual y los resultados de una sesión de solución de problemas iniciada con StartSupportTroubleshooting. Incluye solicitudes interactivas de más información y recomendaciones para resolver el problema en función de las respuestas anteriores.

Ejemplos de políticas de IAM para las recomendaciones AWS Support

Puede utilizar los siguientes ejemplos de políticas para gestionar el acceso a AWS Support las recomendaciones.

Acceso completo a AWS Support las recomendaciones

La siguiente política permite a los usuarios un acceso total a AWS Support las recomendaciones.

```
{
```

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

Denegar el acceso a AWS Support las recomendaciones

La siguiente política no permite a los usuarios acceder a AWS Support las recomendaciones.

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

Supervisión y registro de AWS Support recomendaciones

> **Note**
>
> AWS Support Las recomendaciones se proporcionan como un «servicio de vista previa», según se define en las condiciones del AWS servicio. El servicio de vista previa está sujeto a cambios y cancelaciones. Más información.

La supervisión es una parte importante del mantenimiento de la fiabilidad, la disponibilidad y el rendimiento de AWS Support Recommendations y del resto de tus AWS soluciones. AWS proporciona la siguiente herramienta de supervisión para ver AWS Support las recomendaciones, informar cuando algo va mal y tomar medidas automáticas cuando sea necesario:

- AWS CloudTrailcaptura las llamadas a la API y los eventos relacionados realizados por su AWS cuenta o en su nombre y entrega los archivos de registro a un bucket de Amazon S3 que especifique. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron las llamadas. Para obtener más información, consulte la Guía del usuario de AWS CloudTrail.

Temas

Registrar llamadas de AWS Support recomendaciones con AWS CloudTrail

> **Note**
>
> AWS Support Las recomendaciones se proporcionan como un «servicio de vista previa», tal como se define en las condiciones del AWS servicio. El servicio de vista previa está sujeto a cambios y cancelaciones. Más información.

AWS Support Las recomendaciones están integradas con AWS CloudTrail un servicio que proporciona un registro de las acciones realizadas por un usuario, un rol o un AWS servicio. CloudTrail captura las llamadas a la API para AWS Support las recomendaciones como eventos. Las llamadas capturadas incluyen las llamadas desde la consola AWS Support central y las llamadas en código a las AWS Support Recomendaciones.

Si crea un registro, puede habilitar la entrega continua de CloudTrail eventos a un bucket de Amazon Simple Storage Service (Amazon S3), incluidos los eventos AWS Support de Recommendations. Si no configura una ruta, podrá ver los eventos más recientes en la CloudTrail consola, en el historial de eventos.

Con la información recopilada por CloudTrail, puedes determinar la solicitud que se realizó a AWS Support Recommendations, la dirección IP desde la que se realizó la solicitud, quién la hizo, cuándo se realizó y detalles adicionales.

Para obtener más información CloudTrail, incluido cómo configurarla y habilitarla, consulta la Guía del AWS CloudTrail usuario.

AWS Support Información sobre recomendaciones en CloudTrail

CloudTrail está habilitada en su AWS cuenta al crear la cuenta. Cuando se produce una actividad de eventos admitida en AWS Support las Recomendaciones, esa actividad se registra en un CloudTrail evento junto con otros eventos de AWS servicio en el historial de eventos. Puedes ver, buscar y descargar los eventos recientes en tu AWS cuenta. Para obtener más información, consulta Cómo ver eventos con el historial de CloudTrail eventos.

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

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

Todas las llamadas de AWS Support Recommendations son registradas por CloudTrail. Cada entrada de registro o evento contiene información sobre quién generó la solicitud. La información de identidad del usuario lo ayuda a determinar lo siguiente:

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

Para obtener más información, consulte el elemento CloudTrail UserIdentity.

También puede agrupar los archivos de registro de AWS Support recomendaciones de varias AWS regiones y AWS cuentas en un único bucket de Amazon S3.

Descripción de las entradas del archivo de registro de AWS Support recomendaciones

Un rastro es una configuración que permite la entrega de eventos como archivos de registro a un bucket de Amazon S3 que usted especifique. CloudTrail Los archivos de registro contienen una o más entradas de registro. Un evento representa una única solicitud desde cualquier origen. Incluye información sobre la operación solicitada, la fecha y la hora de la operación, los parámetros de la solicitud, etc. CloudTrail Los archivos de registro no son un registro de pila ordenado de las llamadas a las API públicas, por lo que no aparecen en ningún orden específico.

Example : entrada de registro de **`StartSupportTroubleshooting`**

En el siguiente ejemplo, se muestra una entrada de CloudTrail registro de la `StartSupportTroubleshooting` operación.


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::111122223333:user/Admin",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    },
    "eventTime": "2023-09-11T16:34:13Z",
    "eventSource": "supportrecommendations.amazonaws.com",
    "eventName": "StartSupportTroubleshooting",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "72.21.198.67",
    "userAgent": "signin.amazonaws.com",
    "requestParameters": {
        "message": "..."
    },
    "responseElements": null,
    "requestID": "4c4d5fc8-c403-4f82-9544-41f820e0fa01",
    "eventID": "2f4630ac-5c27-4f0d-b93f-63742d6fc85e",
    "readOnly": true,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```

Example : entrada de registro de **`GetSupportTroubleshootingResponse`**

En el siguiente ejemplo, se muestra una entrada de CloudTrail registro de la `GetSupportTroubleshootingResponse` operación.


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::111122223333:user/Admin",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    },
    "eventTime": "2023-09-11T16:34:13Z",
    "eventSource": "supportrecommendations.amazonaws.com",
    "eventName": "GetSupportTroubleshootingResponse",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "72.21.198.67",
    "userAgent": "signin.amazonaws.com",
    "requestParameters": {
        "conversationId": "..."
    },
    "responseElements": null,
    "requestID": "4c4d5fc8-c403-4f82-9544-41f820e0fa01",
    "eventID": "2f4630ac-5c27-4f0d-b93f-63742d6fc85e",
    "readOnly": true,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```


AWS Support Utilizándolo con un AWS SDK

AWS Los kits de desarrollo de software (SDK) están disponibles para muchos lenguajes de programación populares. Cada SDK proporciona una API, ejemplos de código y documentación que facilitan a los desarrolladores la creación de aplicaciones en su lenguaje preferido.

Documentación de SDK	Ejemplos de código
AWS SDK for C++	AWS SDK for C++ ejemplos de código
AWS CLI	AWS CLI ejemplos de código
AWS SDK for Go	AWS SDK for Go ejemplos de código
AWS SDK for Java	AWS SDK for Java ejemplos de código
AWS SDK for JavaScript	AWS SDK for JavaScript ejemplos de código
AWS SDK para Kotlin	AWS SDK para Kotlin ejemplos de código
AWS SDK for .NET	AWS SDK for .NET ejemplos de código
AWS SDK for PHP	AWS SDK for PHP ejemplos de código
AWS Tools for PowerShell	Herramientas para ejemplos PowerShell de código
AWS SDK for Python (Boto3)	AWS SDK for Python (Boto3) ejemplos de código
AWS SDK for Ruby	AWS SDK for Ruby ejemplos de código
AWS SDK para Rust	AWS SDK para Rust ejemplos de código
AWS SDK para SAP ABAP	AWS SDK para SAP ABAP ejemplos de código
AWS SDK para Swift	AWS SDK para Swift ejemplos de código

Ejemplo de disponibilidad

¿No encuentra lo que necesita? Solicite un ejemplo de código a través del enlace de Enviar comentarios que se encuentra al final de esta página.

Acerca de la API de AWS Support

La API de AWS Support proporciona acceso a algunas de las características del Centro de asistencia de AWS.

La API ofrece dos grupos de operaciones diferentes:

- Las operaciones Administración de casos de soporte para administrar todo el ciclo de vida de sus casos de soporte de AWS, desde la creación de un caso hasta su resolución
- operaciones AWS Trusted Advisor para acceder a las verificaciones de AWS Trusted Advisor

> **Note**
>
> Para poder usar la API de AWS Support, debe contar con un plan de soporte Business, Enterprise On-Ramp o Enterprise. Para más información, consulte AWS Support.

Para obtener más información sobre las operaciones y los tipos de datos proporcionados por AWS Support, consulte la Referencia de la API de AWS Support.

Temas

- Administración de casos de soporte
- AWS Trusted Advisor
- puntos de conexión
- Compatibilidad en los SDK de AWS

Administración de casos de soporte

Puede utilizar la API para llevar a cabo las siguientes tareas:

- Abrir un caso de soporte
- Obtener una lista e información detallada sobre los casos de soporte recientes
- Filtrar la búsqueda de casos de soporte por fechas e identificadores de casos, incluidos casos resueltos

- Agregar comunicaciones y archivos adjuntos a los casos, y agregar destinatarios de correo electrónico para las correspondencias de los casos. Puede adjuntar hasta tres archivos. Cada archivo puede ser de hasta 5 MB
- Resolver sus casos

La AWS Support API admite el CloudTrail registro para las operaciones de administración de casos de soporte. Para más información, consulte Registrar llamadas a la API de AWS Support con AWS CloudTrail.

Para obtener ejemplos del código que demuestras cómo administrar todo el ciclo de vida de un caso de soporte, consulte Code examples for AWS Support using AWS SDKs (Ejemplos de código para mediante SDK).

AWS Trusted Advisor

Puede utilizar las operaciones Trusted Advisor para llevar a cabo las tareas siguientes:

- Obtener los nombres e identificadores de las verificaciones de Trusted Advisor
- Solicitar que se lleve a cabo una verificación de Trusted Advisor en su cuenta y recursos de AWS
- Obtener resúmenes e información detallada de los resultados de las verificaciones de Trusted Advisor
- Actualizar sus verificaciones de Trusted Advisor
- Obtener el estado de cada verificación de Trusted Advisor

La AWS Support API admite el CloudTrail registro de Trusted Advisor las operaciones. Para más información, consulte Información de AWS Trusted Advisor en el registro de CloudTrail.

Puedes usar Amazon CloudWatch Events para supervisar los cambios en los resultados de tus comprobacionesTrusted Advisor. Para más información, consulte Supervisión de los resultados de los AWS Trusted Advisor controles con Amazon EventBridge.

Para ver el código Java de ejemplo que muestra cómo usar las operaciones de Trusted Advisor, consulte Trusted Advisor Utilización como servicio web.

puntos de conexión

AWS Support es un servicio global. Esto significa que cualquier punto de conexión que utilice actualizará sus casos de asistencia en la Support Center Console.

Por ejemplo, si usa el punto de conexión Este de EE. UU. (Norte de Virginia) para crear un caso, puede usar el punto de conexión Oeste de EE. UU. (Oregón) o el punto de conexión Europa (Irlanda) para agregar una correspondencia al mismo caso.

Puede usar el siguiente punto de conexión para la API de AWS Support:

- Este de EE. UU. (Norte de Virginia) https://support.us-east-1.amazonaws.com
- Oeste de EE. UU. (Oregón) https://support.us-west-2.amazonaws.com
- Europa (Irlanda) https://support.eu-west-1.amazonaws.com

> **Important**
>
> - Si llamas a la CreateCaseoperación para crear casos de soporte de prueba, te recomendamos que incluyas un asunto, como TEST CASE-Please ignore. Cuando termines con tu caso de soporte técnico de prueba, llama a la ResolveCaseoperación para resolverlo.
> - Para llamar a las operaciones AWS Trusted Advisor de la API de AWS Support, debe usar el punto de conexión Este de EE. UU. (Norte de Virginia). En la actualidad, los puntos de conexión Oeste de EE. UU. (Oregón) y Europa (Irlanda) no admiten las operaciones Trusted Advisor.

Para obtener más información acerca de los puntos de conexión de AWS, consulte Cuotas y puntos de conexión de AWS Support en Referencia general de Amazon Web Services.

Compatibilidad en los SDK de AWS

Los kits de desarrollo de software (SDK) de AWS y AWS Command Line Interface (AWS CLI) incluyen soporte para la API de AWS Support.

Para obtener una lista de los idiomas compatibles con la AWS Support API, elige un nombre de operación, por ejemplo CreateCase, y en la sección Vea también, elige el idioma que prefieras.

AWS Support Planes

Puedes cambiar AWS Support los planes de tu cuenta en función de las necesidades de tu empresa.

Temas

Características de los AWS Support planes

AWS Support ofrece cinco planes de soporte:

- Basic
- Desarrollador
- Usuarios
- Enterprise On-Ramp
- Enterprise

El plan Basic ofrece soporte para preguntas relacionadas con la cuenta y la facturación, así como de las cuotas del servicio. Los demás planes ofrecen una serie de casos de soporte técnico con pay-by-the-month precios y sin contratos a largo plazo.

Todos los AWS clientes tienen acceso automático las 24 horas del día, los 7 días de la semana a estas funciones de Basic Support:

- O ne-on-one respuestas a preguntas sobre cuentas y facturación
- Foros de soporte
- Comprobación es de estado de servicios
- Documentación, documentos técnicos y guías de prácticas recomendadas

Los clientes con un plan de soporte Developer tienen acceso a estas características adicionales:

- Orientación sobre prácticas recomendadas
- Herramientas de diagnóstico del lado del cliente

- Soporte de arquitectura básica: orientación sobre cómo utilizar AWS productos, funciones y servicios de forma conjunta
- Admite un número ilimitado de casos de soporte que cualquier usuario con permisos puede abrir.

Además, los clientes con un plan de soporte Business, Enterprise On-Ramp o Enterprise tienen acceso a las siguientes características:

- Guía sobre casos de uso: qué AWS productos, funciones y servicios utilizar para satisfacer mejor sus necesidades específicas.
- AWS Trusted Advisor— Una función que inspecciona los entornos de AWS Support los clientes e identifica oportunidades para ahorrar dinero, cerrar las brechas de seguridad y mejorar la confiabilidad y el rendimiento del sistema. Puede acceder a todos los Trusted Advisor cheques.
- La AWS Support API para interactuar con Support Center y Trusted Advisor. Puede usar la API de AWS Support para automatizar la administración de casos de soporte y las operaciones de Trusted Advisor .
- Soporte para software de terceros: ayuda con la configuración y los sistemas operativos de instancias de Amazon Elastic Compute Cloud (Amazon EC2). Además, ayuda con el rendimiento de los componentes de software de terceros más populares en AWS. El soporte de software de terceros no está disponible para los clientes con planes de soporte básico o para desarrolladores.
- Admite un número ilimitado de usuarios AWS Identity and Access Management (IAM) que pueden abrir casos de soporte técnico.

Además, los clientes con un plan de soporte Enterprise On-Ramp o Enterprise tienen acceso a las siguientes características:

- Orientación sobre la arquitectura de aplicaciones: orientación a través de asesoramiento sobre cómo los servicios trabajan en conjunto para atender su caso de uso, carga de trabajo o aplicación específicos.
- Administración de eventos de infraestructura: compromiso a corto plazo con AWS Support para obtener un conocimiento más profundo de su caso de uso. Después del análisis, proporcione orientación arquitectónica y de escalado para un evento.
- Gerente técnico de cuenta: trabaje con un gerente técnico de cuenta (TAM) para sus casos de uso específicos y aplicaciones.
- Atención prioritaria.
- Revisiones empresariales de la gestión.

Para obtener más información sobre las funciones y los precios de cada plan de soporte, consulte AWS Supporty compare AWS Support planes. Algunas características, como el soporte telefónico o por chat en cualquier momento, no están disponibles en todos los idiomas.

¿Cambiar AWS Support los planes

Puede usar la consola de AWS Support planes para cambiar su plan de soporte Cuenta de AWS. Para cambiar tu plan de soporte, debes tener permisos AWS Identity and Access Management (de IAM) o iniciar sesión en tu cuenta como usuario root. Para obtener más información, consulte Gestione el acceso a los planes AWS Support y AWS políticas gestionadas para AWS Support los planes.

Para cambiar el plan de soporte

1. Inicie sesión en la consola de AWS Support planes en https://console.aws.amazon.com/support/plans/home.
2. (Opcional) En la página AWS Support Plans (Planes de), compare los planes de soporte. Para obtener más información sobre los precios, consulte la página de detalles del precio.
3. (Opcional) En AWS Support pricing example, (Ejemplo de precio de) elija See examples, (Ver ejemplos) y a continuación, elija una de las opciones del plan de soporte para ver el costo estimado.
4. Cuando se decida por un plan, elija Review downgrade (Revisar versión anterior) o Review upgrade (Revisar actualización) para el plan que quiera.

   > **Notas**
   >
   > - Si se suscribe a un plan de soporte de pago, es responsable de una suscripción mínima de un mes de AWS Support. Para obtener más información, consulte las preguntas frecuentes acerca de AWS Support.
   > - Si tiene un plan Enterprise On-Ramp o Enterprise Support, en el cuadro de diálogo Change plan confirmation (Confirmación de cambio de plan), contacte con AWS Support para cambiar el plan de soporte.

5. En el cuadro de diálogo Change plan confirmation (Confirmación de cambio de plan), puede expandir los elementos de soporte para ver las características que quiera agregar o eliminar de su cuenta.

En Pricing (Precios), puede ver los cargos únicos proyectados para el nuevo plan de soporte.

6. Elija Accept and agree (Aceptar).

Información relacionada

Para obtener más información sobre AWS Support los planes, consulta las AWS Support preguntas frecuentes. También puede elegir Contact us (Contáctenos) en la consola de planes de Support.

Para cerrar su cuenta, consulte Cierre de una cuenta en la Guía del usuario de AWS Billing .

AWS Trusted Advisor

Trusted Advisor se basa en las mejores prácticas aprendidas al atender a cientos de miles de AWS clientes. Trusted Advisor inspecciona su AWS entorno y, a continuación, hace recomendaciones cuando existen oportunidades para ahorrar dinero, mejorar la disponibilidad y el rendimiento del sistema o ayudar a cerrar las brechas de seguridad.

Si tienes un plan Basic o Developer Support, puedes usar la Trusted Advisor consola para acceder a todas las comprobaciones de la categoría Límites de servicio y a seis comprobaciones de la categoría Seguridad.

Si tienes un plan Business, Enterprise On-Ramp o Enterprise Support, puedes usar la Trusted Advisor consola y la AWS Trusted Advisor API para acceder a todas las Trusted Advisor comprobaciones. También puedes usar Amazon CloudWatch Events para supervisar el estado de los Trusted Advisor cheques. Para obtener más información, consulte Supervisión de los resultados de los AWS Trusted Advisor controles con Amazon EventBridge.

Puede acceder Trusted Advisor en AWS Management Console. Para obtener más información sobre cómo controlar el acceso a la Trusted Advisor consola, consulteGestione el acceso a AWS Trusted Advisor.

Para obtener más información, consulte Trusted Advisor.

Temas

- Comience con Recommendations de Trusted Advisor
- Comience a utilizar la Trusted Advisor API
- Trusted Advisor Utilización como servicio web
- Vista organizativa para AWS Trusted Advisor
- Ver comprobaciones de AWS Trusted Advisor con tecnología de AWS Config
- Visualización de controles de AWS Security Hub en AWS Trusted Advisor
- Optar AWS Compute Optimizer por recibir Trusted Advisor cheques
- Introducción a AWS Trusted Advisor Priority
- Primeros pasos con AWS Trusted Advisor Engage (vista previa)
- AWS Trusted Advisor comprobar referencia
- Registro de cambios para AWS Trusted Advisor

Comience con Recommendations de Trusted Advisor

Puedes usar la página de Trusted Advisor recomendaciones de la Trusted Advisor consola para revisar los resultados de tus comprobaciones Cuenta de AWS y, a continuación, seguir los pasos recomendados para solucionar cualquier problema. Por ejemplo, Trusted Advisor puede recomendar que elimine recursos no utilizados para reducir la factura mensual, como una instancia de Amazon Elastic Compute Cloud (Amazon EC2).

También puedes usar la AWS Trusted Advisor API para realizar operaciones en tus Trusted Advisor comprobaciones. Para obtener más información consulte la AWS Trusted Advisor API Reference

Temas

Inicie sesión en la Trusted Advisor consola

Puede ver las comprobaciones y el estado de cada una de ellas en la Trusted Advisor consola.

> **Note**
>
> Debe tener permisos AWS Identity and Access Management (de IAM) para acceder a la Trusted Advisor consola. Para obtener más información, consulte Gestione el acceso a AWS Trusted Advisor.

Para iniciar sesión en la consola Trusted Advisor

1. Inicie sesión en la Trusted Advisor consola en https://console.aws.amazon.com/trustedadvisor/home.

2. En la página Recommendations de Trusted Advisor , vea el resumen de cada categoría de verificación:

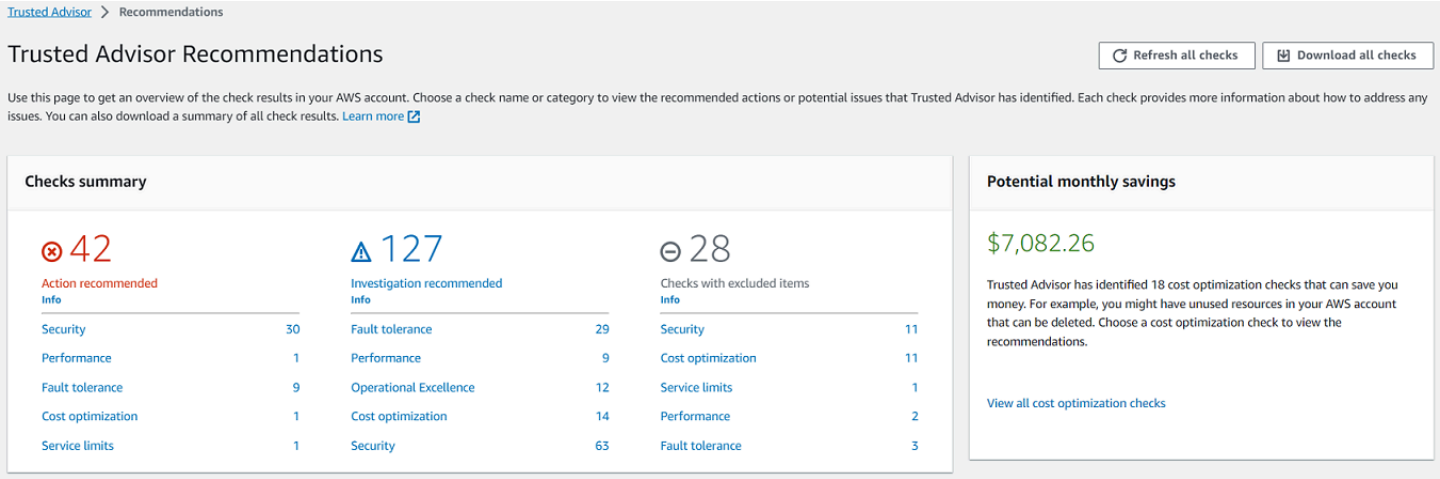
   - Acción recomendada (rojo): Trusted Advisor recomienda una acción para la comprobación. Por ejemplo, una verificación que detecta un problema de seguridad para los recursos de IAM podría recomendar pasos urgentes.
   - Investigación recomendada (amarillo): Trusted Advisor detecta un posible problema para la verificación. Por ejemplo, una verificación que alcanza una cuota para un recurso podría recomendar formas de eliminar recursos no utilizados.
   - Comprobaciones con elementos excluidos (gris): número de comprobaciones que tienen elementos excluidos, como recursos que usted desee que una comprobación ignore. Por ejemplo, pueden tratarse de instancias de Amazon EC2 que no desea que evalúe la verificación.

3. En la página Recommendatios de Trusted Advisor puede hacer lo siguiente:

   - Para actualizar todas las verificaciones de su cuenta, elija Refresh all checks (Actualizar todas las verificaciones).
   - Para crear un archivo .xls que incluya todos los resultados de las verificaciones, elija Download all checks (Descargar todas las verificaciones).
   - En Checks summary (Resumen de verificaciones), elija una categoría de verificación, como Security (Seguridad), para ver los resultados.
   - En Potential monthly savings (Posible ahorro mensual), puede ver cuánto podría ahorrar para su cuenta y las verificaciones de optimización de costos para conocer recomendaciones.
   - En Recent changes (Cambios recientes), puede ver los cambios en los estados de verificación en los últimos 30 días. Elija un nombre de verificación para ver los últimos resultados de esa verificación o elija el icono de flecha para ver la página siguiente.

Example : Trusted Advisor Recomendaciones

El siguiente ejemplo muestra un resumen de los resultados de la comprobación de una Cuenta de AWS.



Ver categorías de verificación

Puede ver las descripciones de verificación y los resultados de las siguientes categorías de verificación:

- Optimización de costos: recomendaciones que pueden hacerle ahorrar dinero. Estas verificaciones resaltan los recursos no utilizados y las oportunidades de reducir su factura.
- Performance (Rendimiento): recomendaciones que pueden mejorar la velocidad y la capacidad de respuesta de sus aplicaciones.
- Seguridad: recomendaciones de configuración de seguridad que pueden hacer que su AWS solución sea más segura.
- Tolerancia a errores: recomendaciones que ayudan a aumentar la resiliencia de la AWS solución. Estas comprobaciones destacan las deficiencias de redundancia y los recursos utilizados en exceso.
- Cuotas de servicio: verifica el uso de su cuenta y si su cuenta se acerca al límite (también conocido como cuotas) o lo supera para los servicios y los recursos de AWS .
- Excelencia operativa: recomendaciones para ayudarlo a operar su AWS entorno de manera eficaz y a escala.

Para ver categorías de verificación

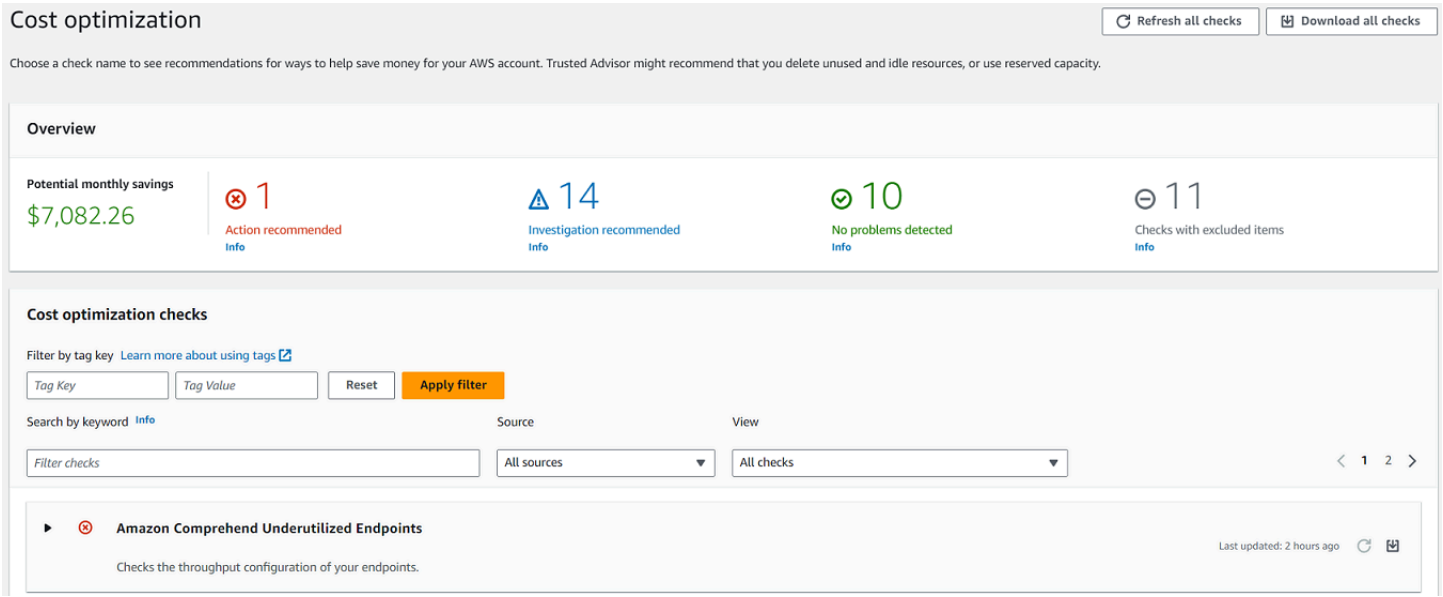
1. Inicie sesión en la Trusted Advisor consola en https://console.aws.amazon.com/trustedadvisor/home.
2. En el panel de navegación, elija la categoría de la verificación.
3. En la página de la categoría, vea el resumen de cada categoría de verificación:

- Acción recomendada (rojo): Trusted Advisor recomienda una acción para la comprobación.
- Investigación recomendada (amarillo): Trusted Advisor detecta un posible problema para la verificación.
- 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.

4. Para cada verificación, elija el icono de actualización ( ) para actualizar esta verificación.
5. Elija el icono de descarga ( ) para crear un archivo.xls que incluya los resultados de esta verificación.

Example : categoría Optimización de costos

El siguiente ejemplo muestra 10 cheques (verdes) que no presentan ningún problema.



Ver verificaciones específicas

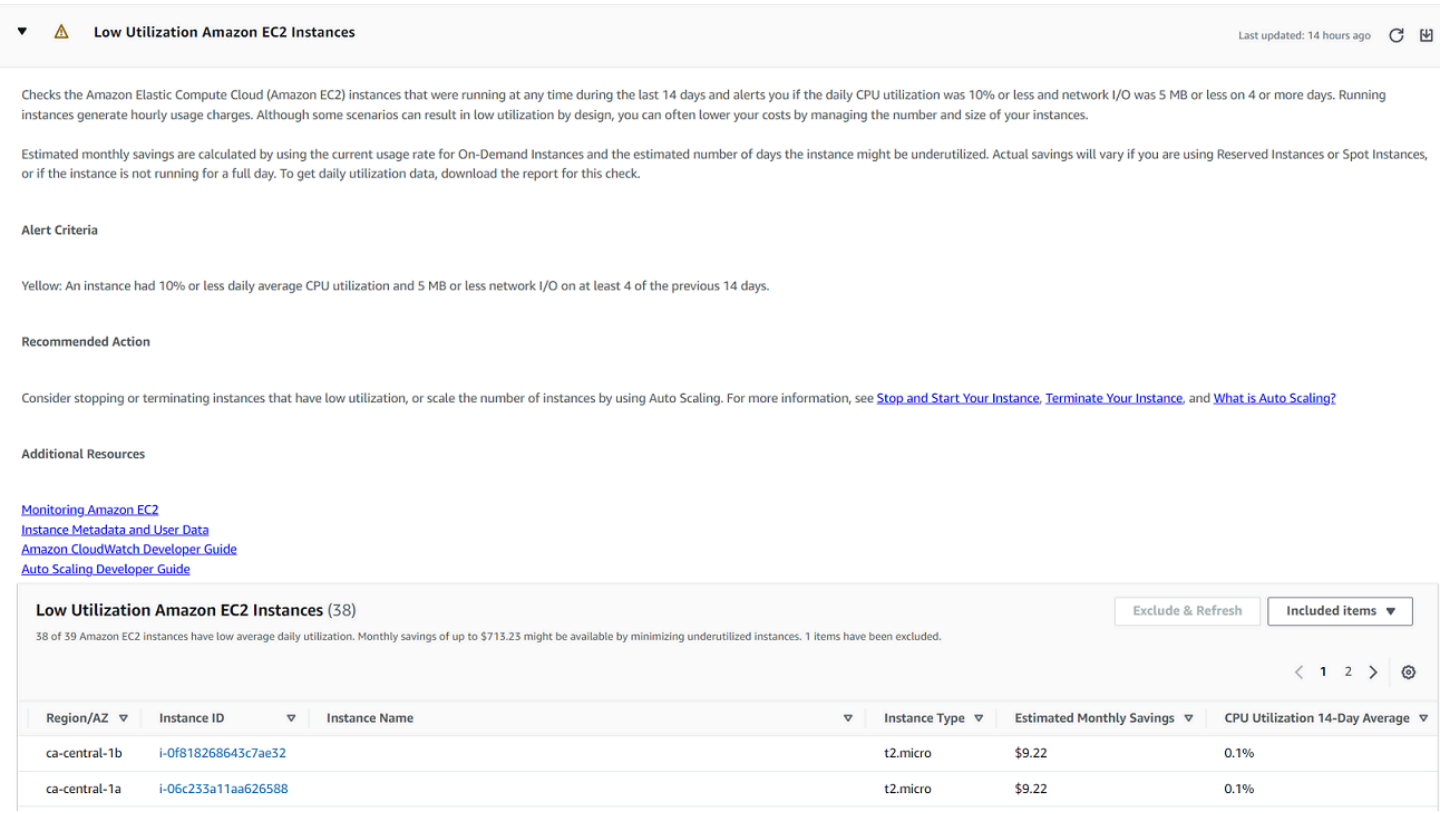
Expanda una verificación para ver la descripción completa de la verificación, los recursos afectados, los pasos recomendados y los vínculos para obtener más información.

Para ver una verificación específica

1. Inicie sesión en la Trusted Advisor consola en https://console.aws.amazon.com/trustedadvisor/home.
2. En el panel de navegación, elija una categoría de verificación.
3. Elija el nombre del cheque para ver la descripción y los siguientes detalles:
   - Alert Criteria (Criterios de alerta): describe el umbral en el que una verificación cambiará de estado.
   - Recommended Action (Acción recomendada): describe las acciones recomendadas para esta verificación.
   - Additional Resources (Recursos adicionales): enumera la documentación de AWS relacionada.
   - Una tabla que muestra los elementos afectados de su cuenta. Puede incluir o excluir estos elementos de los resultados de la verificación.
4. (Opcional) Para excluir elementos para que no aparezcan en los resultados de la verificación:
   a. Seleccione un elemento y elija Exclude & Refresh (Excluir y actualizar).
   b. Para ver todos los elementos excluidos, elija Excluded items (Elementos excluidos).
5. (Opcional) Para incluir elementos para que la verificación los evalúe de nuevo:
   a. Elija Excluded items (Elementos excluidos), seleccione un elemento y, a continuación, elija Include & Refresh (Incluir y actualizar).
   b. Para ver todos los elementos incluidos, elija Included items (Elementos incluidos).
6. Elija el icono de configuración ().
   En el cuadro de diálogo Preferences (Preferencias), puede especificar el número de elementos o las propiedades que desea mostrar y, a continuación, seleccione Confirm (Confirmar).

Example : verificación de Optimización de costos

La siguiente verificación Bajo uso de instancias de Amazon EC2 muestra las instancias afectadas en la cuenta. Esta comprobación identifica 38 instancias de Amazon EC2 que tienen un uso bajo y recomienda detener o terminar los recursos.



Filtrar sus verificaciones

En las páginas de categorías de verificación, puede especificar los resultados de verificación que desea ver. Por ejemplo, puede filtrar por verificaciones que hayan detectado errores en su cuenta, de modo que pueda investigar primero los problemas urgentes.

Si tiene cheques que evalúan los elementos de su cuenta, como AWS los recursos, puede usar filtros de etiquetas para mostrar solo los elementos que tienen la etiqueta especificada.

Para filtrar las verificaciones

1. Inicie sesión en la Trusted Advisor consola en https://console.aws.amazon.com/trustedadvisor/home.
2. En el panel de navegación o en la página Recommendations de Trusted Advisor , elija la categoría de verificación.
3. En Search by keyword (Buscar por palabra clave), ingrese una palabra clave del nombre o la descripción de la verificación para filtrar los resultados.
4. Para la lista View (Vista), especifique las verificaciones que desea ver:

   - All checks (Todas las verificaciones): muestra todas las verificaciones para esta categoría.

- Action recommended (Acción recomendada): enumera las verificaciones que recomiendan tomar medidas. Estas verificaciones están resaltadas en rojo.
- Investigation recommended (Investigación recomendada): enumera las verificaciones que recomiendan tomar una posible medida. Estas verificaciones están resaltadas en amarillo.
- No problems detected (No se han detectado problemas): enumera las verificaciones que no tienen ningún problema. Estas verificaciones están resaltadas en verde.
- Checks with excluded items (Verificaciones con elementos excluidos): muestra las verificaciones que especificó para excluir elementos de los resultados de la verificación.

5. Si ha añadido etiquetas a sus AWS recursos, como instancias o AWS CloudTrail rutas de Amazon EC2, puede filtrar los resultados para que las comprobaciones solo muestren los elementos que tienen la etiqueta especificada.

   Para filtrar por etiquetas, ingrese un valor y una clave de etiqueta y, a continuación, elija Apply filter (Aplicar filtro).
6. En la tabla de la verificación, los resultados de la verificación solo muestran los elementos que tienen la clave y el valor especificados.
7. Para borrar el filtro por etiquetas, elija Reset (Restablecer).

Información relacionada

Para obtener más información sobre el etiquetado Trusted Advisor, consulte los siguientes temas:

- AWS Support habilita las capacidades de etiquetado para Trusted Advisor
- Etiquetado de recursos de AWS en Referencia general de AWS.

Actualizar resultados de verificaciones

Puede actualizar las verificaciones para obtener los resultados más recientes de su cuenta. Si tienes un plan Developer o Basic Support, puedes iniciar sesión en la Trusted Advisor consola para actualizar las comprobaciones. Si tienes un plan Business, Enterprise On-Ramp o Enterprise Support, actualiza Trusted Advisor automáticamente los cheques de tu cuenta semanalmente.

Para actualizar los cheques Trusted Advisor

1. Navegue hasta la AWS Trusted Advisor consola en https://console.aws.amazon.com/trustedadvisor.

2. En la página de Trusted Advisor recomendaciones o de una categoría de comprobación, selecciona Actualizar todas las comprobaciones.

También puede actualizar verificaciones específicas de las siguientes maneras:

- Elija el icono de actualización () para una verificación individual.
- Use la operación RefreshTrustedAdvisorCheck de la API.

> **Notas**
>
> - Trusted Advisor actualiza automáticamente algunas comprobaciones varias veces al día, como las de AWS Well-Architectedalto riesgo relacionadas con la comprobación de fiabilidad. Los cambios pueden tardar algunas horas en aparecer en la cuenta. En el caso de las verificaciones actualizadas automáticamente, no puede elegir el icono de actualización () para actualizar los resultados de forma manual.
> - Si AWS Security Hub habilitaste tu cuenta, no podrás usar la Trusted Advisor consola para actualizar los controles de Security Hub. Para obtener más información, consulte Actualizar los hallazgos de Security Hub.

Descargar los resultados de la verificación

Puedes descargar los resultados de las comprobaciones para obtener información general sobre tu cuenta. Trusted Advisor Puede descargar los resultados de todas las verificaciones o de una verificación específica.

Para descargar los resultados de los cheques desde Trusted Advisor Recomendaciones

1. Navegue hasta la AWS Trusted Advisor consola en https://console.aws.amazon.com/trustedadvisor.

- Para descargar todos los resultados de las verificaciones, en Recommendations de Trusted Advisor o en una página de categoría de verificación, elija Descargar todas las verificaciones.
- Para descargar un resultado de verificación para una verificación específica, elija el nombre de la verificación y, a continuación, elija el icono de descarga ( )

2. Guarde o abra el archivo .xls. El archivo contiene la misma información de resumen de la consola de Trusted Advisor , como el nombre de la verificación, la descripción, el estado, los recursos afectados, etc.

Vista organizativa

Puedes configurar la función de visualización de la organización para crear un informe para todas las cuentas de los miembros de tu AWS organización. Para obtener más información, consulte Vista organizativa para AWS Trusted Advisor.

Preferencias

En la página Administrar Trusted Advisor, puede deshabilitar Trusted Advisor.

En la página Notifications (Notificaciones), puede configurar sus mensajes de correo electrónico semanales para el resumen de la comprobación. Consulte Configurar las preferencias de notificación.

En la página Tu organización, puedes activar o desactivar el acceso de confianza con AWS Organizations. Esto es obligatorio para la característica Vista organizativa para AWS Trusted Advisor, Trusted Advisor Priority y Trusted Advisor Engage.

Configurar las preferencias de notificación

Especifique quién puede recibir los mensajes de Trusted Advisor correo electrónico semanales con los resultados de las comprobaciones y el idioma. Una vez a la semana, recibes una notificación por correo electrónico sobre el resumen de la comprobación de Trusted Advisor las recomendaciones.

Las notificaciones por correo electrónico de Trusted Advisor las recomendaciones no incluyen los resultados de Trusted Advisor Priority. Para obtener más información, consulte Administración de notificaciones de Trusted Advisor Priority.

Para configurar las preferencias de notificación

1. Inicia sesión en la Trusted Advisor consola en https://console.aws.amazon.com/trustedadvisor/home.
2. En el panel de navegación, en Preferences (Preferencias), elija Notifications (Notificaciones).
3. En Recommendations, seleccione a quién quiere notificar los resultados de la comprobación. Puedes añadir y eliminar contactos desde la página de configuración de la cuenta de la AWS Billing and Cost Management consola.
4. Para Language (Idioma), elija el idioma del mensaje de correo electrónico.
5. Elija Save your preferences (Guardar preferencias).

Configurar la vista organizativa

Si configuraste tu cuenta con AWS Organizations, puedes crear informes para todas las cuentas de los miembros de tu organización. Para obtener más información, consulte Vista organizativa para AWS Trusted Advisor.

Desactivar Trusted Advisor

Al deshabilitar este servicio, Trusted Advisor no realizará ninguna comprobación en su cuenta. Cualquier persona que intente acceder a la Trusted Advisor consola o utilizar las operaciones de la API recibirá un mensaje de error de acceso denegado.

Para inhabilitar Trusted Advisor

1. Inicie sesión en la Trusted Advisor consola en https://console.aws.amazon.com/trustedadvisor/home.
2. En el panel de navegación, en Preferences (Preferencias), elija Manage Trusted Advisor (Administrar).
3. En Trusted Advisor, desactive Enabled (Habilitado). Esta acción se deshabilita Trusted Advisor para todos los cheques de tu cuenta.
4. A continuación, puedes eliminar manualmente el de tu cuenta. Para obtener más información, consulte Eliminación de un rol vinculado a un servicio de Trusted Advisor.

Información relacionada

Para obtener más información Trusted Advisor, consulte los siguientes temas:

- ¿Cómo empiezo a usarlo Trusted Advisor?
- AWS Trusted Advisor comprobar referencia

Comience a utilizar la Trusted Advisor API

La referencia de la AWS Trusted Advisor API está destinada a los programadores que necesitan información detallada sobre las operaciones y los tipos de datos de la Trusted Advisor API. Esta API proporciona acceso a Trusted Advisor las recomendaciones para su cuenta o para todas las cuentas de su AWS organización. La Trusted Advisor API utiliza métodos HTTP que devuelven los resultados en formato JSON.

> **Note**
>
> - Debe tener un plan Business, Enterprise On-Ramp o Enterprise Support para usar la API Trusted Advisor
> - Si llamas a la AWS Trusted Advisor API desde una cuenta que no tiene un plan Business, Enterprise On-Ramp o Enterprise Support, recibirás una excepción de acceso denegado. Para obtener más información sobre cómo cambiar su plan de soporte, consulte AWS Support.

Puedes usar la AWS Trusted Advisor API para obtener una lista de comprobaciones y sus descripciones, recomendaciones y recursos para hacer recomendaciones. También puedes actualizar el ciclo de vida de las recomendaciones. Para gestionar las recomendaciones, utiliza las siguientes operaciones de API:

- Usa las operaciones ListChecksListRecommendationsGetRecommendation, y ListRecommendationResourcesAPI para ver las recomendaciones y las cuentas y los recursos correspondientes.
- Usa la operación UpdateRecommendationLifecycleAPI para actualizar el ciclo de vida de una recomendación gestionada por Trusted Advisor Priority.
- Usa la operación de la BatchUpdateRecommendationResourceExclusionAPI para incluir o excluir uno o más recursos de tus Trusted Advisor resultados.
- Las llamadas ListOrganizationRecommendationsGetOrganizationRecommendation, ListOrganizationRecommendationResourcesListOrganizationRecommendationAccounts, y a la UpdateOrganizationRecommendationLifecycleAPI solo admiten las recomendaciones gestionadas

por Trusted Advisor Priority. Estas recomendaciones también se denominan recomendaciones priorizadas. Puede ver y gestionar sus recomendaciones priorizadas desde una cuenta de administración o de administrador delegado si ha activado Trusted Advisor Priority. Si Priority no está activada, recibirá una excepción de acceso denegado cuando realice las solicitudes.

Para obtener más información, consulte AWS Trusted Advisor la Guía del usuario de AWS Support.

Para la autenticación de las solicitudes, consulte el proceso de firma de la versión 4 de Signature.

Trusted Advisor Utilización como servicio web

> **Note**
>
> Trusted Advisor la API AWS Trusted Advisor Support no admitirá las operaciones en 2024. Utilice la nueva AWS Trusted Advisor API para acceder mediante programación a las comprobaciones y recomendaciones de las mejores prácticas.

El AWS Support servicio le permite escribir aplicaciones con las que interactuar. AWS Trusted Advisor En este tema se muestra cómo obtener una lista de Trusted Advisor comprobaciones, actualizar una de ellas y, a continuación, obtener los resultados detallados de la comprobación. Estas tareas se han demostrado en Java. Para obtener información de soporte para otros idiomas, consulte Herramientas para Amazon Web Services

Temas

- Obtenga la lista de Trusted Advisor comprobaciones disponibles
- Actualiza la lista de Trusted Advisor comprobaciones disponibles
- Realice un sondeo y Trusted Advisor compruebe si hay cambios de estado
- Solicita el resultado de una Trusted Advisor comprobación
- Muestra los detalles de una Trusted Advisor verificación

Obtenga la lista de Trusted Advisor comprobaciones disponibles

El siguiente fragmento de código Java crea una instancia de un AWS Support cliente que puedes usar para llamar a todas las operaciones de la Trusted Advisor API. A continuación, el código obtiene la lista de Trusted Advisor comprobaciones y sus `CheckId` valores correspondientes mediante una

llamada a la operación de DescribeTrustedAdvisorChecksAPI. Puede utilizar esta información para crear interfaces de usuario que permiten a los usuarios seleccionar la comprobación que desean ejecutar o actualizar.

```
private static AWSSupport createClient()
{
    return AWSSupportClientBuilder.defaultClient();
}
// Get the List of Available Trusted Advisor Checks
public static void getTAChecks() {
    // Possible language parameters: "en" (English), "ja" (Japanese), "fr" (French),
 "zh" (Chinese)
    DescribeTrustedAdvisorChecksRequest request = new
 DescribeTrustedAdvisorChecksRequest().withLanguage("en");
    DescribeTrustedAdvisorChecksResult result =
 createClient().describeTrustedAdvisorChecks(request);
    for (TrustedAdvisorCheckDescription description : result.getChecks()) {
        // Do something with check description.
        System.out.println(description.getId());
        System.out.println(description.getName());
    }
}
```

Actualiza la lista de Trusted Advisor comprobaciones disponibles

El siguiente fragmento de código Java crea una instancia de un AWS Support cliente que puede utilizar para actualizar Trusted Advisor los datos.

```
// Refresh a Trusted Advisor Check
// Note: Some checks are refreshed automatically, and they cannot be refreshed by using
 this operation.
// Specifying the check ID of a check that is automatically refreshed causes an
 InvalidParameterValue error.
public static void refreshTACheck(final String checkId) {
    RefreshTrustedAdvisorCheckRequest request = new
 RefreshTrustedAdvisorCheckRequest().withCheckId(checkId);
    RefreshTrustedAdvisorCheckResult result =
 createClient().refreshTrustedAdvisorCheck(request);
    System.out.println("CheckId: " + result.getStatus().getCheckId());
    System.out.println("Milliseconds until refreshable: " +
 result.getStatus().getMillisUntilNextRefreshable());
    System.out.println("Refresh Status: " + result.getStatus().getStatus());
```

```
}
```

Realice un sondeo y Trusted Advisor compruebe si hay cambios de estado

Tras enviar la solicitud para ejecutar una Trusted Advisor comprobación a fin de generar los datos de estado más recientes, se utiliza la operación de la DescribeTrustedAdvisorCheckRefreshStatusesAPI para solicitar el progreso de la ejecución de la comprobación y cuando haya nuevos datos listos para la comprobación.

El siguiente fragmento de código Java obtiene el estado de la comprobación solicitada en la siguiente sección, utilizando el valor correspondiente en la variable `CheckId`. Además, el código muestra varios otros usos del Trusted Advisor servicio:

1. Puede hacer una llamada a `getMillisUntilNextRefreshable` recorriendo los objetos contenidos en la instancia `DescribeTrustedAdvisorCheckRefreshStatusesResult`. Puede utilizar el valor devuelto para comprobar si desea que el código continúe actualizando la comprobación.
2. Si `timeUntilRefreshable` equivale a cero, puede solicitar una actualización de la comprobación.
3. Con el estado devuelto, puede seguir sondeando los cambios de estado; el fragmento de código establece el intervalo de sondeo a una recomendación de diez segundos. Si el estado es `enqueued` o `in_progress`, el bucle devuelve y solicita otro estado. Si la llamada devuelve `successful`, el bucle termina.
4. Finalmente, el código devuelve una instancia de un tipo de datos `DescribeTrustedAdvisorCheckResultResult` que puede utilizar para recorrer la información generada con la comprobación.

Nota: utilice una única solicitud de actualización antes de sondear el estado de la solicitud.

```
// Retrieves TA refresh statuses. Multiple checkId's can be submitted.
public static List<TrustedAdvisorCheckRefreshStatus> getTARefreshStatus(final String...
 checkIds) {
    DescribeTrustedAdvisorCheckRefreshStatusesRequest request =
            new
 DescribeTrustedAdvisorCheckRefreshStatusesRequest().withCheckIds(checkIds);
    DescribeTrustedAdvisorCheckRefreshStatusesResult result =
            createClient().describeTrustedAdvisorCheckRefreshStatuses(request);
    return result.getStatuses();
```

```
}
// Retrieves a TA check status, and checks to see if it has finished processing.
public static boolean isTACheckStatusInTerminalState(final String checkId) {
    // Since we only submitted one checkId to getTARefreshStatus, just retrieve the
 only element in the list.
    TrustedAdvisorCheckRefreshStatus status = getTARefreshStatus(checkId).get(0);
    // Valid statuses are:
    // 1. "none", the check has never been refreshed before.
    // 2. "enqueued", the check is waiting to be processed.
    // 3. "processing", the check is in the midst of being processed.
    // 4. "success", the check has succeeded and finished processing - refresh data is
 available.
    // 5. "abandoned", the check has failed to process.
    return status.getStatus().equals("abandoned") ||
 status.getStatus().equals("success");
}
// Enqueues a Trusted Advisor check refresh. Periodically polls the check refresh
 status for completion.
public static TrustedAdvisorCheckResult getFreshTACheckResult(final String checkId)
 throws InterruptedException {
    refreshTACheck(checkId);
    while(!isTACheckStatusInTerminalState(checkId)) {
        Thread.sleep(10000);
    }
    return getTACheckResult(checkId);
}
// Retrieves fresh TA check data whenever possible.
// Note: Some checks are refreshed automatically, and they cannot be refreshed by using
 this operation. This method
// is only functional for checks that can be refreshed using the
 RefreshTrustedAdvisorCheck operation.
public static void pollForTACheckResultChanges(final String checkId) throws
 InterruptedException {
    String checkResultStatus = null;
    do {
        TrustedAdvisorCheckResult result = getFreshTACheckResult(checkId);
        if (checkResultStatus != null && !checkResultStatus.equals(result.getStatus()))
 {
            break;
        }
        checkResultStatus = result.getStatus();
        // The rule refresh has completed, but due to throttling rules the checks may
 not be refreshed again
        // for a short period of time.
```

```
        // Since we only submitted one checkId to getTARefreshStatus, just retrieve the
 only element in the list.
        TrustedAdvisorCheckRefreshStatus refreshStatus =
 getTARefreshStatus(checkId).get(0);
        Thread.sleep(refreshStatus.getMillisUntilNextRefreshable());
    } while(true);
    // Signal that a TA check has changed check result status here.
}
```

Solicita el resultado de una Trusted Advisor comprobación

Tras seleccionar la comprobación de los resultados detallados que desee, envíe una solicitud mediante la operación de la API de DescribeTrustedAdvisorCheckresultados.

> **Tip**
>
> Los nombres y las descripciones de las Trusted Advisor comprobaciones están sujetos a cambios. Le recomendamos que especifique el ID de verificación en su código para identificar de forma exclusiva una verificación. Puede utilizar la operación de la DescribeTrustedAdvisorChecksAPI para obtener el ID del cheque.

El siguiente fragmento de código Java utiliza la instancia `DescribeTrustedAdvisorChecksResult` referida por la variable `result`, que se ha obtenido en el fragmento de código anterior. En lugar de definir una comprobación de forma interactiva a través de una interfaz de usuario, después de enviar la solicitud para su ejecución, el fragmento envía una solicitud de ejecución de la primera comprobación de la lista especificando un valor de índice de 0 en cada llamada `result.getChecks().get(0)`. A continuación, el código define una instancia de `DescribeTrustedAdvisorCheckResultRequest`, que se pasa a una instancia de `DescribeTrustedAdvisorCheckResultResult` llamada `checkResult`. Puede utilizar las estructuras miembros de este tipo de datos para ver los resultados de la comprobación.

```
// Request a Trusted Advisor Check Result
public static TrustedAdvisorCheckResult getTACheckResult(final String checkId) {
    DescribeTrustedAdvisorCheckResultRequest request = new
 DescribeTrustedAdvisorCheckResultRequest()
            // Possible language parameters: "en" (English), "ja" (Japanese),
 "fr" (French), "zh" (Chinese)
            .withLanguage("en")
```

```
            .withCheckId(checkId);
    DescribeTrustedAdvisorCheckResultResult requestResult =
 createClient().describeTrustedAdvisorCheckResult(request);
    return requestResult.getResult();
}
```

Nota: Al solicitar el resultado de una Trusted Advisor comprobación no se generan datos de resultados actualizados.

Muestra los detalles de una Trusted Advisor verificación

El siguiente fragmento de código Java recorre en iteración la `DescribeTrustedAdvisorCheckResultResult` instancia devuelta en la sección anterior para obtener una lista de los recursos marcados por la verificación. Trusted Advisor

```
// Show ResourceIds for flagged resources.
for (TrustedAdvisorResourceDetail flaggedResource :
    result1.getResult().getFlaggedResources())
{
    System.out.println(
        "The resource for this ResourceID has been flagged: " +
        flaggedResource.getResourceId());
}
```

Vista organizativa para AWS Trusted Advisor

La vista organizativa le permite ver las verificaciones de Trusted Advisor para todas las cuentas de su AWS Organizations. Después de habilitar esta característica, puede crear informes para agregar los resultados de las verificaciones de todas las cuentas de miembros de la organización. El informe incluye un resumen de los resultados de las verificaciones e información sobre los recursos afectados para cada cuenta. Por ejemplo, puede utilizar los informes para identificar qué cuentas de su organización utilizan AWS Identity and Access Management (IAM) con la verificación Uso de IAM o si ha recomendado acciones para buckets de Amazon Simple Storage Service (Amazon S3) con la verificación de permisos de bucket de Amazon S3.

Temas

- Requisitos previos
- Habilitar la vista organizativa

- Actualizar las verificaciones de Trusted Advisor
- Crear informes de vista organizativa
- Ver el resumen del informe
- Descargar un informe de vista organizativa
- Desactivar la vista organizativa
- Uso de políticas de IAM para permitir el acceso a la vista organizativa
- Uso de otros servicios de AWS para ver informes de Trusted Advisor

Requisitos previos

Para habilitar la vista organizativa, debe cumplir los siguientes requisitos:

- Sus cuentas deben formar parte de una organización AWS.
- Su organización debe tener habilitadas todas las características para las organizaciones. Para obtener más información, consulte Habilitar todas las características en la organización en la Guía del usuario de AWS Organizations.
- La cuenta de administración de su organización debe tener un plan de soporte Business, Enterprise On-Ramp o Enterprise. Puede encontrar su plan de soporte en el Centro de AWS Support o desde la página Planes de soporte. Consulte Comparar planes de AWS Support.
- Debe haber iniciado sesión como usuario en la cuenta de administración (o haber asumido un rol equivalente). Tanto si inicia sesión como usuario de IAM o como rol de IAM, debe tener una política con los permisos necesarios. Consulte Uso de políticas de IAM para permitir el acceso a la vista organizativa.

Habilitar la vista organizativa

Una vez que haya cumplido los requisitos previos, siga estos pasos para habilitar la vista organizativa. Cuando habilite esta característica, ocurrirá lo siguiente:

- Trusted Advisor se habilitará como un servicio de confianza en su organización. Para obtener más información, consulte Habilitar el acceso de confianza con más servicios de AWS en la Guía del usuario de AWS Organizations.
- El rol vinculado al servicio de `AWSServiceRoleForTrustedAdvisorReporting` se crea para usted en la cuenta de administración de su organización. Este rol incluye los permisos que Trusted

Advisor necesita para llamar a Organizations en su nombre. Este rol vinculado al servicio está bloqueado y no puede eliminarlo manualmente. Para obtener más información, consulte Uso de roles vinculados a servicios de Trusted Advisor.

Habilita la vista organizativa desde la consola de Trusted Advisor.

Para habilitar la vista organizativa

1. Inicie sesión como administrador en la cuenta de administración de la organización y abra la consola de AWS Trusted Advisor en https://console.aws.amazon.com/trustedadvisor.
2. En el panel de navegación, en Preferences (Preferencias), elija Your organization (Su organización).
3. En Enable trusted access with AWS Organizations (Habilitar el acceso de confianza con), active Enabled (Habilitado).

> **Note**
>
> La habilitación de la vista organizativa para la cuenta de administración no proporciona las mismas verificaciones para todas las cuentas de miembro. Por ejemplo, si todas sus cuentas de miembro cuentan con soporte básico, esas cuentas no tendrán las mismas verificaciones disponibles que su cuenta de administración. El plan AWS Support determina qué verificaciones Trusted Advisor hay disponibles para una cuenta.

Actualizar las verificaciones de Trusted Advisor

Antes de crear un informe para su organización, le recomendamos que actualice los estados de sus verificaciones de Trusted Advisor. Puede descargar un informe sin actualizar sus verificaciones de Trusted Advisor, pero es posible que el informe no tenga la información más reciente.

Si tiene un plan de soporte Business, Enterprise On-Ramp o Enterprise, Trusted Advisor actualiza de forma automática y semanal las verificaciones de su cuenta.

> **Note**
>
> Si tiene cuentas en su organización que tienen un plan de soporte Basic o de desarrollador, un usuario de esas cuentas debe iniciar sesión en la consola de Trusted Advisor para

actualizar las verificaciones. No puede actualizar las verificaciones de todas las cuentas desde la cuenta de administración de la organización.

Para actualizar las verificaciones de Trusted Advisor

1. Vaya a la consola de AWS Trusted Advisor en https://console.aws.amazon.com/trustedadvisor.
2. En la página Recommendations de Trusted Advisor, elija Refresh all checks (Actualizar todas las comprobaciones). De este modo, actualizará todas las verificaciones de su cuenta.

También puede actualizar verificaciones específicas de las siguientes maneras:

- Use la operación de la API RefreshTrustedAdvisorCheck.
- Elija el icono de actualización () para una verificación individual.

Crear informes de vista organizativa

Después de habilitar la vista organizativa, puede crear informes para que pueda ver los resultados de las verificaciones de Trusted Advisor de su organización.

Puede crear un máximo de 50 informes. Si crea más informes, Trusted Advisor elimina el más antiguo. Los informes eliminados no se pueden recuperar.

Para crear informes de vista organizativa

1. Inicie sesión con la cuenta de administración de la organización y abra la consola de AWS Trusted Advisor en https://console.aws.amazon.com/trustedadvisor.
2. En el panel de navegación, elija Organizational View (Vista organizativa).
3. Elija Create report (Crear informe).
4. De forma predeterminada, el informe incluye todas las Regiones, categorías de verificación, verificaciones y estados de recursos de AWS. En la página Create report (Crear informe), puede usar las opciones de filtro para personalizar el informe. Por ejemplo, puede borrar la opción All (Todos) de Region (Región) y, a continuación, especificar las regiones individuales que se van a incluir en el informe.

a. Ingrese un Name (Nombre) para el informe.

b. En Format (Formato), elija JSON o CSV.

c. En Region (Región), especifique la Región de AWS o elija All (Todas).

d. En Check category (Categoría de verificación), elija la categoría de verificación o elija All (Todas).

e. En Checks (Verificaciones), elija las verificaciones específicas de la categoría o elija All (Todas).

> **Note**
>
> El filtro Check category (Categoría de verificación) reemplaza el filtro Checks (Verificaciones). Por ejemplo, si elige la categoría Security (Seguridad) y, a continuación, elija un nombre de verificación específico, el informe incluye todos los resultados de verificaciones de esa categoría. Para crear un informe de solo verificaciones específicas, deje el valor predeterminado All (Todas) en Check category (Categoría de verificación) y, a continuación, elija los nombres de las verificaciones.

f. Para Resource status (Estado del recurso), elija el estado que desea filtrar, como Warning (Advertencia), o elija All (Todos).

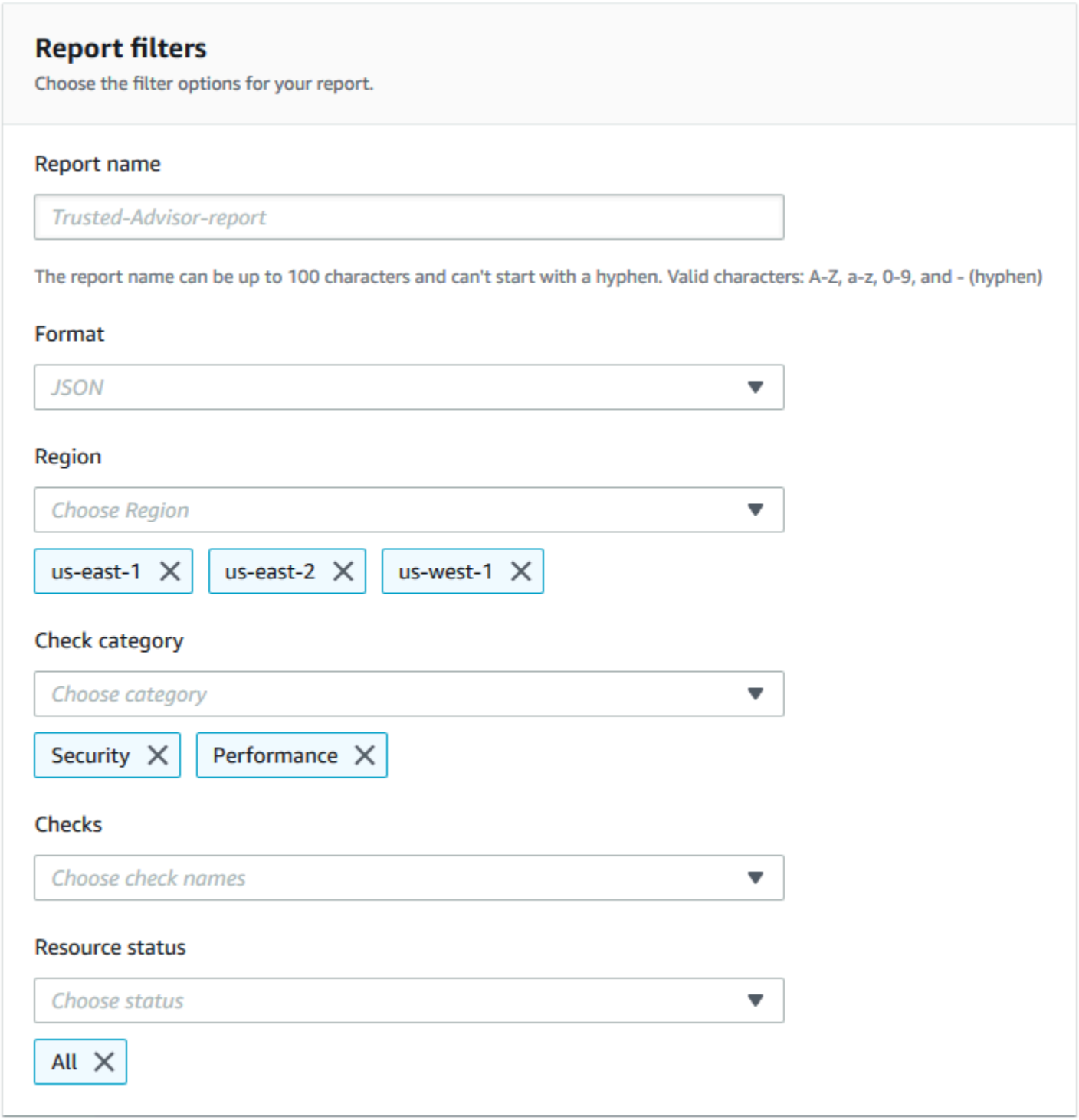
5. En Organización de AWS, seleccione las unidades organizativas que desea incluir en el informe. Para obtener más información acerca de las unidades organizativas, consulte Administración de unidades organizativas en la Guía del usuario de AWS Organizations.

6. Elija Create report (Crear informe).

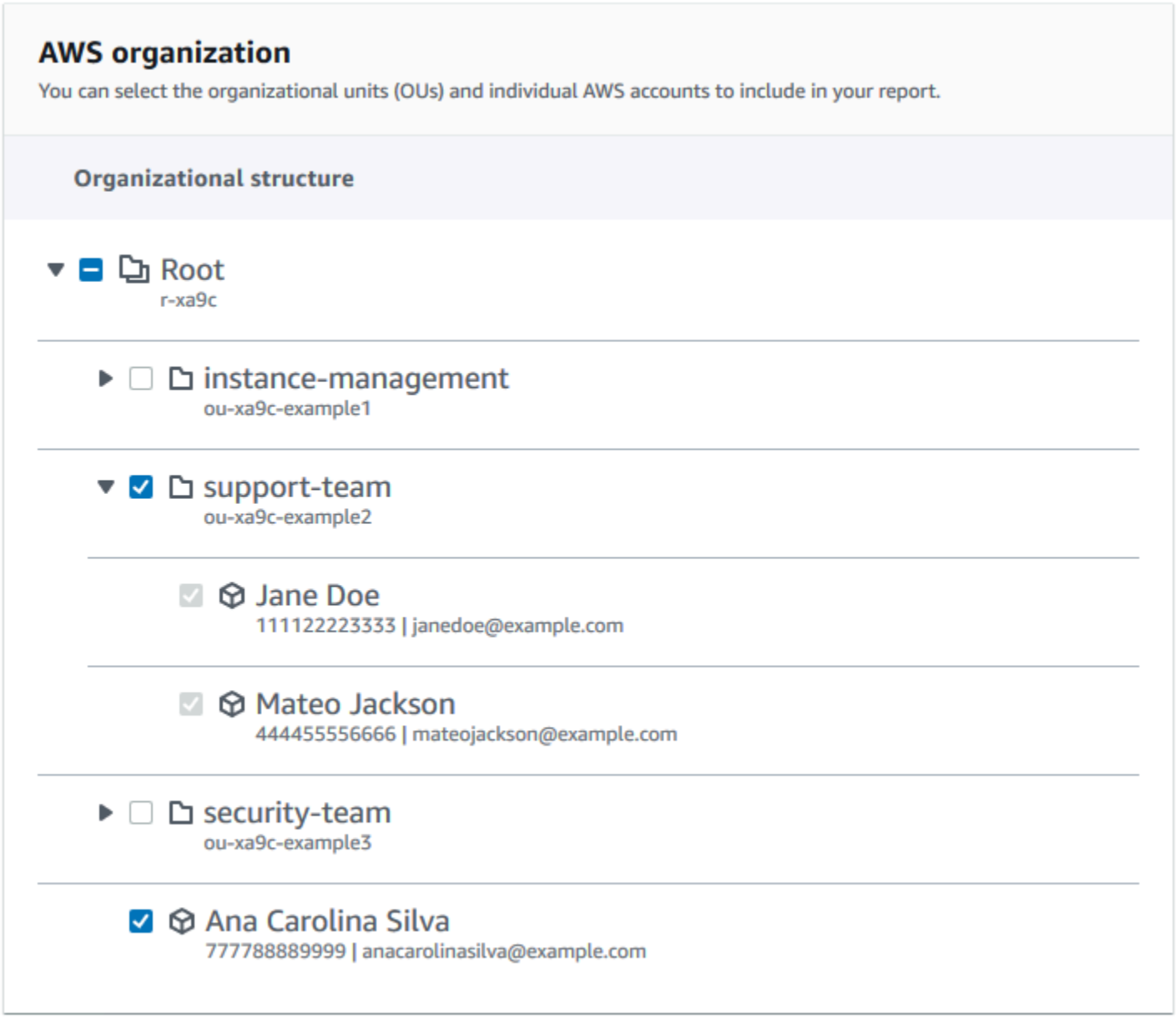
Example : Crear opciones de filtro de informe

En el siguiente ejemplo se crea un informe JSON para lo siguiente:

- Tres regiones de AWS
- Todas las verificaciones de Security (Seguridad) y Performance (Rendimiento)



En el siguiente ejemplo, el informe incluye la unidad organizativa support-team (equipo de soporte) y una cuenta de AWS que forman parte de la organización.



Notas

- El tiempo que tarda en crear el informe depende del número de cuentas de la organización y del número de recursos de cada cuenta.
- No puede crear más de un informe a la vez a menos que el informe actual se haya estado ejecutando durante más de 6 horas.
- Actualice la página si no ve que el informe aparezca en la página.

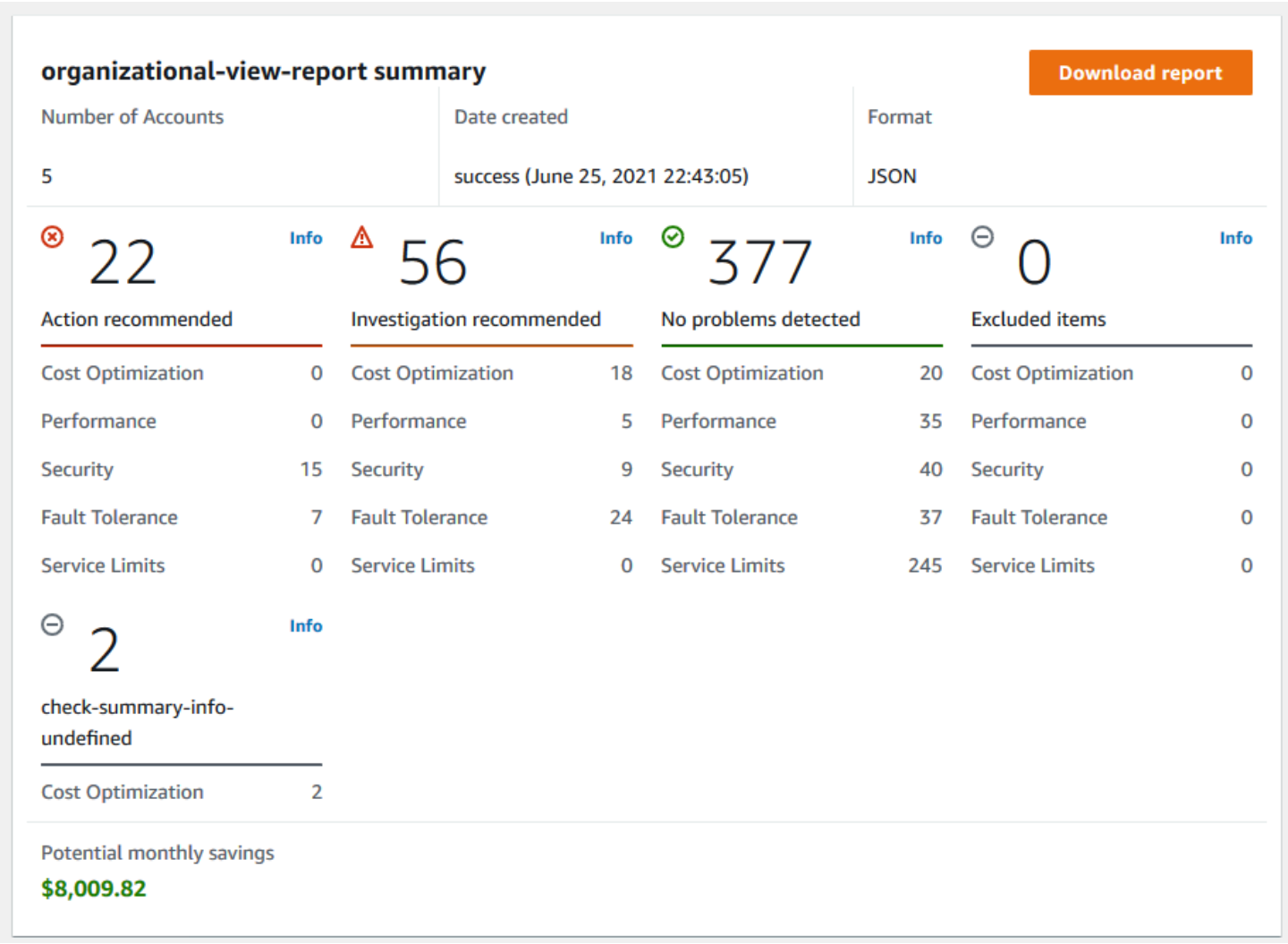
Ver el resumen del informe

Una vez que el informe esté listo, puede ver el resumen del informe en la consola de Trusted Advisor. Esto le permite ver rápidamente el resumen de los resultados de las verificaciones en toda la organización.

Para ver el resumen del informe

1. Inicie sesión con la cuenta de administración de la organización y abra la consola de AWS Trusted Advisor en https://console.aws.amazon.com/trustedadvisor.
2. En el panel de navegación, elija Organizational View (Vista organizativa).
3. Elija el nombre del informe.
4. En la página Summary (Resumen), vea los estados de verificación de cada categoría. También puede elegir Download report (Descargar informe).

Example : Resumen del informe de una organización



Descargar un informe de vista organizativa

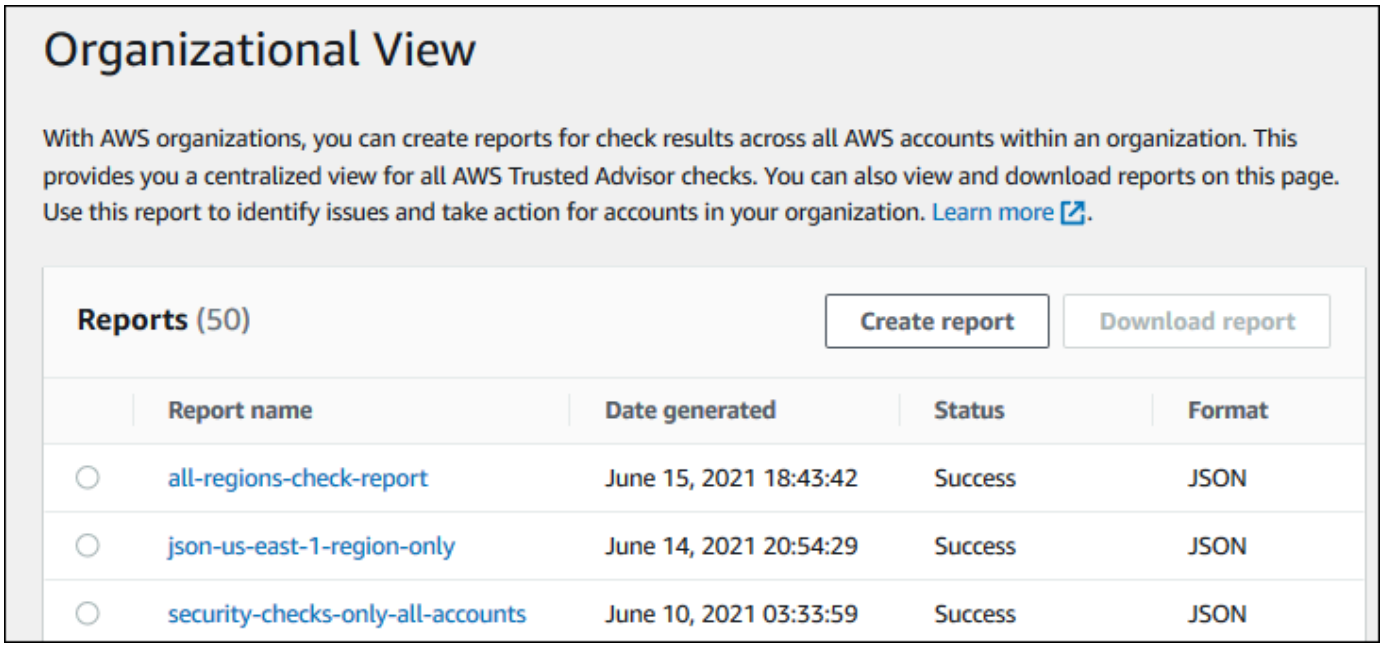
Una vez que el informe esté listo, descárguelo desde la consola de Trusted Advisor. El informe es un archivo .zip que contiene tres archivos:

- `summary.json`: contiene un resumen de los resultados de la verificación de cada categoría de verificación.
- `schema.json`: contiene el esquema de las verificaciones especificadas en el informe.
- Un archivo de recursos (.json o .csv): contiene información detallada sobre los estados de verificación de los recursos de la organización.

Para descargar un informe de vista organizativa

1. Inicie sesión con la cuenta de administración de la organización y abra la consola de AWS Trusted Advisor en https://console.aws.amazon.com/trustedadvisor.
2. En el panel de navegación, elija Organizational View (Vista organizativa).

   En la página Organizational View (Vista organizativa) se muestran los informes disponibles para descargar.
3. Seleccione un informe, elija Download report (Descargar informe) y, a continuación, guarde el archivo. Solo se puede descargar un informe a la vez.



4. Descomprima el archivo.
5. Utilice un editor de texto para abrir el archivo `.json` o una aplicación de hoja de cálculo para abrir el archivo `.csv`.

> **Note**
>
> Es posible que reciba varios archivos si el informe es de 5 MB o más.

Example : archivo summary.json

El archivo `summary.json` muestra el número de cuentas de la organización y los estados de las verificaciones en cada categoría.

Trusted Advisor utiliza el siguiente código de color para los resultados de la verificación:

- `Green`: Trusted Advisor no detecta ningún problema para la verificación.
- `Yellow`: Trusted Advisor detecta un posible problema para la verificación.
- `Red`: Trusted Advisor detecta un error y recomienda una acción para la verificación.
- `Blue`: Trusted Advisor no puede determinar el estado de la verificación.

En el ejemplo siguiente, dos verificaciones son `Red`, una es `Green` y una es `Yellow`.


```
{
    "numAccounts": 3,
    "filtersApplied": {
        "accountIds": ["123456789012","111122223333","111111111111"],
        "checkIds": "All",
        "categories": [
            "security",
            "performance"
        ],
        "statuses": "All",
        "regions": [
            "us-west-1",
            "us-west-2",
            "us-east-1"
        ],
        "organizationalUnitIds": [
            "ou-xa9c-EXAMPLE1",
            "ou-xa9c-EXAMPLE2"
        ]
    },
    "categoryStatusMap": {
        "security": {
            "statusMap": {
                "ERROR": {
                    "name": "Red",
                    "count": 2
                },
                "OK": {
                    "name": "Green",
                    "count": 1
                },
                "WARN": {
```

```
                    "name": "Yellow",
                    "count": 1
                }
            },
            "name": "Security"
        }
    },
    "accountStatusMap": {
        "123456789012": {
            "security": {
                "statusMap": {
                    "ERROR": {
                        "name": "Red",
                        "count": 2
                    },
                    "OK": {
                        "name": "Green",
                        "count": 1
                    },
                    "WARN": {
                        "name": "Yellow",
                        "count": 1
                    }
                },
                "name": "Security"
            }
        }
    }
}
```

Example : archivo schema.json

El archivo `schema.json` incluye el esquema de las verificaciones en el informe. En el ejemplo siguiente se incluyen los ID y las propiedades de las verificaciones de la política de contraseñas de IAM (Yw2K9puPzl) y la rotación de claves de IAM (DqdJqYeRm5).

```
{
    "Yw2K9puPzl": [
        "Password Policy",
        "Uppercase",
        "Lowercase",
        "Number",
        "Non-alphanumeric",
```

```
        "Status",
        "Reason"
    ],
    "DqdJqYeRm5": [
        "Status",
        "IAM User",
        "Access Key",
        "Key Last Rotated",
        "Reason"
    ],
    ...
}
```

Example : archivo resources.csv

El archivo `resources.csv` incluye información sobre los recursos de la organización. En este ejemplo se muestran algunas de las columnas de datos que aparecen en el informe, como las siguientes:

- ID de cuenta de la cuenta afectada
- El ID de la verificación de Trusted Advisor
- El ID del recurso
- Marca de tiempo del informe
- El nombre completo de la verificación de Trusted Advisor
- La categoría de verificación de Trusted Advisor
- El ID de cuenta de la unidad organizativa (OU) principal o la raíz

AccountId	CheckId	ResourceId	TimeStamp	CheckName	Category
1.11122E+11	Qch7DwouX1	LnW14f1M40NMjmMLvY5	1.58983E+12	Low Utilization Amazon EC2 Instances	Cost Optimizing
1.11122E+11	HCP4007jGY	dJrQZXw36ZdswBeo9WUl	1.58983E+12	Security Groups - Specific Ports Unrestricted	Security
1.11122E+11	HCP4007jGY	1hzakmTbWd5UmAM_a0L	1.58983E+12	Security Groups - Specific Ports Unrestricted	Security
4.44456E+11	1iG5NDGVre	dJrQZXw36ZdswBeo9WUl	1.58983E+12	Security Groups - Unrestricted Access	Security
4.44456E+11	1iG5NDGVre	1hzakmTbWd5UmAM_a0L	1.58983E+12	Security Groups - Unrestricted Access	Security
4.44456E+11	Pfx0RwqBli	vioZmlba45kf2JWIe_W0j5	1.58983E+12	Amazon S3 Bucket Permissions	Security
4.44456E+11	Pfx0RwqBli	wAvASS3YOwy6WWxlBHf	1.58983E+12	Amazon S3 Bucket Permissions	Security
1.23457E+11	Pfx0RwqBli	LIc4zRaUSiIGRSlmqaMa5V	1.58983E+12	Amazon S3 Bucket Permissions	Security
1.23457E+11	Pfx0RwqBli	gWB27TMXof2evYzMSYBg	1.58983E+12	Amazon S3 Bucket Permissions	Security
7.77789E+11	Pfx0RwqBli	M3LBsF0e15Cl9Mxppapcx	1.58983E+12	Amazon S3 Bucket Permissions	Security
7.77789E+11	Yw2K9puPzl	47DEQpj8HBSa-_TImW-5J	1.58983E+12	IAM Password Policy	Security
7.77789E+11	H7IgTzjTYb	1xHQ5ovV8bS0H1Z-t7Kbib	1.58983E+12	Amazon EBS Snapshots	Fault Tolerance
7.77789E+11	wuy7G1zxql	10F6p6VAF0F-MuL6Dc-dl1	1.58983E+12	Amazon EC2 Availability Zone Balance	Fault Tolerance

El archivo de recursos solo contiene entradas si existe un resultado de verificación en el nivel de recurso. Es posible que no vea verificaciones en el informe por los siguientes motivos:

- Algunas verificaciones, como MFA on Root Account (MFA en la cuenta raíz) no tienen recursos y no aparecerán en el informe. Las verificaciones sin recursos aparecen en el archivo `summary.json`.
- Algunas verificaciones solo muestran los recursos si son `Red` o `Yellow`. Si todos los recursos son `Green`, es posible que no aparezcan en el informe.
- Si una cuenta no está habilitada para un servicio que requiere la verificación, es posible que la verificación no aparezca en el informe. Por ejemplo, si no utiliza instancias reservadas de Amazon Elastic Compute Cloud (EC2) en su organización, la verificación de Amazon EC2 Reserved Instance Lease Expiration no aparecerá en el informe.
- La cuenta no ha actualizado los resultados de la verificación. Esto puede ocurrir cuando los usuarios con un plan de soporte Basic o de desarrollador inician sesión en la consola de Trusted Advisor por primera vez. Si tiene un plan de soporte Business, Enterprise On-Ramp o Enterprise, puede demorar hasta una semana desde que registra la cuenta para que los usuarios vean los resultados de las verificaciones. Para obtener más información, consulte Actualizar las verificaciones de Trusted Advisor.
- Si solo la cuenta de administración de la organización ha habilitado las recomendaciones para las verificaciones, el informe no incluirá recursos para otras cuentas de la organización.

Para el archivo de recursos, puede utilizar un software común, como Microsoft Excel, para abrir el formato de archivo .csv. Puede utilizar el archivo .csv para un análisis único de todas las verificaciones de todas las cuentas de su organización. Si desea utilizar el informe con una aplicación, puede descargarlo como un archivo.json en su lugar.

El formato de archivo .json proporciona más flexibilidad que el formato de archivo .csv para casos de uso avanzados, como la agregación y el análisis avanzado con varios conjuntos de datos. Por ejemplo, puede utilizar una interfaz SQL con un servicio de AWS, como Amazon Athena, para ejecutar consultas en sus informes. También puede utilizar Amazon QuickSight para crear paneles y visualizar sus datos. Para obtener más información, consulte Uso de otros servicios de AWS para ver informes de Trusted Advisor.

Desactivar la vista organizativa

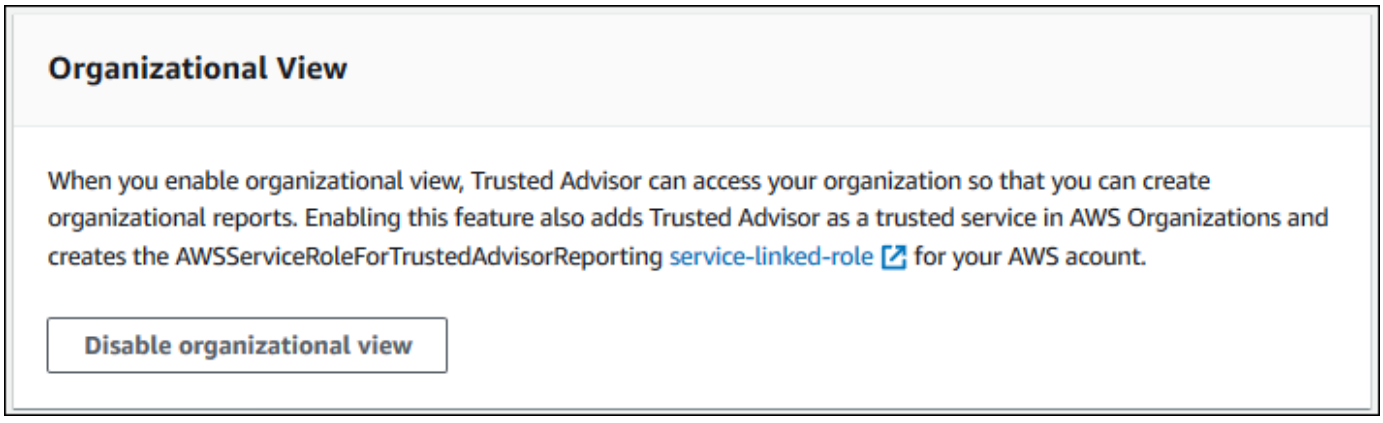
Siga este procedimiento para desactivar la vista organizativa. Debe iniciar sesión con la cuenta de administración de la organización o asumir un rol con los permisos necesarios para desactivar esta característica. No puede desactivar esta característica desde otra cuenta de la organización.

Cuando desactive esta característica, ocurrirá lo siguiente:

- Trusted Advisor se elimina como servicio de confianza en Organizations.
- El rol vinculado al servicio de `AWSServiceRoleForTrustedAdvisorReporting` se desbloquea en la cuenta de administración de su organización. Esto significa que puede eliminarlo manualmente, si es necesario.
- No puede crear, ver ni descargar informes para su organización. Para tener acceso a los informes creados anteriormente, debe volver a habilitar la vista organizativa desde la consola de Trusted Advisor. Consulte Habilitar la vista organizativa.

Para desactivar la vista organizativa de Trusted Advisor

1. Inicie sesión con la cuenta de administración de la organización y abra la consola de AWS Trusted Advisor en https://console.aws.amazon.com/trustedadvisor.
2. En el panel de navegación, elija Preferences (Preferencias).
3. En Organizational View (Vista organizativa), elija (Disable organizational view (Desactivar la vista organizativa).



Después de desactivar la vista organizativa, Trusted Advisor ya no agrega verificaciones de otras cuentas de AWS en la organización. Sin embargo, el rol vinculado al servicio de `AWSServiceRoleForTrustedAdvisorReporting` permanece en la cuenta de administración de

la organización hasta que lo elimine a través de la consola de IAM, la API de IAM o AWS Command Line Interface (AWS CLI). Para obtener más información, consulte Eliminar un rol vinculado a un servicio en la Guía del usuario de IAM.

> **Note**
>
> Puede usar otros servicios de AWS para consultar y visualizar los datos para los informes de vista organizativa. Para obtener más información, consulte los siguientes recursos:
>
> - Ver recomendaciones de AWS Trusted Advisor a escala con AWS Organizations en el Blog de Administración y Gobernanza de AWS
> - Uso de otros servicios de AWS para ver informes de Trusted Advisor

Uso de políticas de IAM para permitir el acceso a la vista organizativa

Puede utilizar las siguientes políticas de AWS Identity and Access Management (IAM) para permitir que los usuarios o roles de su cuenta tengan acceso a la vista organizativa en AWS Trusted Advisor.

Example : Acceso completo a la vista organizativa

La siguiente política permite obtener acceso completo a la característica de vista organizativa. Un usuario con estos permisos puede hacer lo siguiente:

- Habilitar y desactivar vista organizativa
- Crear, ver y descargar informes

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ReadStatement",
            "Effect": "Allow",
            "Action": [
                "organizations:ListAccountsForParent",
                "organizations:ListAccounts",
                "organizations:ListRoots",
                "organizations:DescribeOrganization",
                "organizations:ListOrganizationalUnitsForParent",
                "organizations:ListAWSServiceAccessForOrganization",
```

```
                "trustedadvisor:DescribeAccount",
                "trustedadvisor:DescribeChecks",
                "trustedadvisor:DescribeCheckSummaries",
                "trustedadvisor:DescribeAccountAccess",
                "trustedadvisor:DescribeOrganization",
                "trustedadvisor:DescribeReports",
                "trustedadvisor:DescribeServiceMetadata",
                "trustedadvisor:DescribeOrganizationAccounts",
                "trustedadvisor:ListAccountsForParent",
                "trustedadvisor:ListRoots",
                "trustedadvisor:ListOrganizationalUnitsForParent"
            ],
            "Resource": "*"
        },
        {
            "Sid": "CreateReportStatement",
            "Effect": "Allow",
            "Action": [
                "trustedadvisor:GenerateReport"
            ],
            "Resource": "*"
        },
        {
            "Sid": "ManageOrganizationalViewStatement",
            "Effect": "Allow",
            "Action": [
                "organizations:EnableAWSServiceAccess",
                "organizations:DisableAWSServiceAccess",
                "trustedadvisor:SetOrganizationAccess"
            ],
            "Resource": "*"
        },
        {
            "Sid": "CreateServiceLinkedRoleStatement",
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "arn:aws:iam::*:role/aws-service-role/
reporting.trustedadvisor.amazonaws.com/AWSServiceRoleForTrustedAdvisorReporting"
        }
    ]
}
```

Example : Acceso de lectura a la vista organizativa

La siguiente política permite obtener acceso de solo lectura a la característica de vista organizativa de Trusted Advisor. Un usuario con estos permisos solo puede ver y descargar informes existentes.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ReadStatement",
            "Effect": "Allow",
            "Action": [
                "organizations:ListAccountsForParent",
                "organizations:ListAccounts",
                "organizations:ListRoots",
                "organizations:DescribeOrganization",
                "organizations:ListOrganizationalUnitsForParent",
                "organizations:ListAWSServiceAccessForOrganization",
                "trustedadvisor:DescribeAccount",
                "trustedadvisor:DescribeChecks",
                "trustedadvisor:DescribeCheckSummaries",
                "trustedadvisor:DescribeAccountAccess",
                "trustedadvisor:DescribeOrganization",
                "trustedadvisor:DescribeReports",
                "trustedadvisor:ListAccountsForParent",
                "trustedadvisor:ListRoots",
                "trustedadvisor:ListOrganizationalUnitsForParent"
            ],
            "Resource": "*"
        }
    ]
}
```

También puede crear su propia política de IAM. Para obtener más información, consulte Creación de políticas de IAM en la Guía del usuario de IAM.

> **Note**
>
> Si ha habilitado AWS CloudTrail en su cuenta, los siguientes roles pueden aparecer en sus entradas de registro:

- `AWSServiceRoleForTrustedAdvisorReporting`: el rol vinculado a un servicio que Trusted Advisor utiliza para acceder a las cuentas de la organización.
- `AWSServiceRoleForTrustedAdvisor`: el rol vinculado a un servicio que Trusted Advisor utiliza para acceder a los servicios de la organización.

Para obtener más información acerca de los roles vinculados a servicios, consulte Uso de roles vinculados a servicios de Trusted Advisor.

Uso de otros servicios de AWS para ver informes de Trusted Advisor

Siga este tutorial para cargar y ver sus datos utilizando otros servicios de AWS. En este tema, cree un bucket de Amazon Simple Storage Service (Amazon S3) para almacenar su informe y una plantilla de AWS CloudFormation para crear recursos en la cuenta. A continuación, puede utilizar Amazon Athena para analizar o ejecutar consultas para su informe o Amazon QuickSight para visualizar esos datos en un panel.

Para obtener información y ejemplos para visualizar los datos del informe, consulte Ver recomendaciones de AWS Trusted Advisor a escala con AWS Organizations en el Blog de Administración y Gobernanza de AWS.

Requisitos previos

Antes de comenzar este tutorial, asegúrese de que cumple los siguientes requisitos:

- Inicie sesión como usuario de AWS Identity and Access Management (IAM) con permisos de administrador.
- Uso de la región de AWS EE. UU. Este (Norte de Virginia) para configurar rápidamente los servicios y recursos de AWS.
- Cree una cuenta de Amazon QuickSight. Para obtener más información, consulte Introducción al análisis de datos en Amazon QuickSight en la Guía del usuario de Amazon QuickSight.

Carga del informe en Amazon S3

Después de descargar su informe de `resources.json`, cargue el archivo en Amazon S3. Debe utilizar un bucket en la región EE. UU. Este (Norte de Virginia).

Para cargar el informe en un bucket de Amazon S3

1. Inicie sesión en la AWS Management Console en https://console.aws.amazon.com/.
2. Use el Selector de región y elija la región EE. UU. Este (Norte de Virginia).
3. Abra la consola de Amazon S3 en https://console.aws.amazon.com/s3.
4. En la lista de buckets, elija un bucket de S3 y, a continuación, copie el nombre. En el procedimiento siguiente, utilice el nombre.
5. En la página *bucket-name (nombre del bucket)*, elija Create folder (Crear carpeta), ingrese el nombre **folder1** y elija Save (Guardar).
6. Elija folder1.
7. En folder1, elija Upload (Cargar) y elija el archivo de `resources.json`.
8. Elija Next (Siguiente), conserve las opciones predeterminadas y, a continuación, elija Upload (Cargar).

> **Note**
>
> Si carga un nuevo informe a este bucket, cambie el nombre de los archivos de `.json` cada vez que los cargue para que no sobrescriba los informes existentes. Por ejemplo, puede agregar la marca de tiempo a cada archivo, como `resources-timestamp.json`, `resources-timestamp2.json`, etc.

Creación de sus recursos mediante AWS CloudFormation

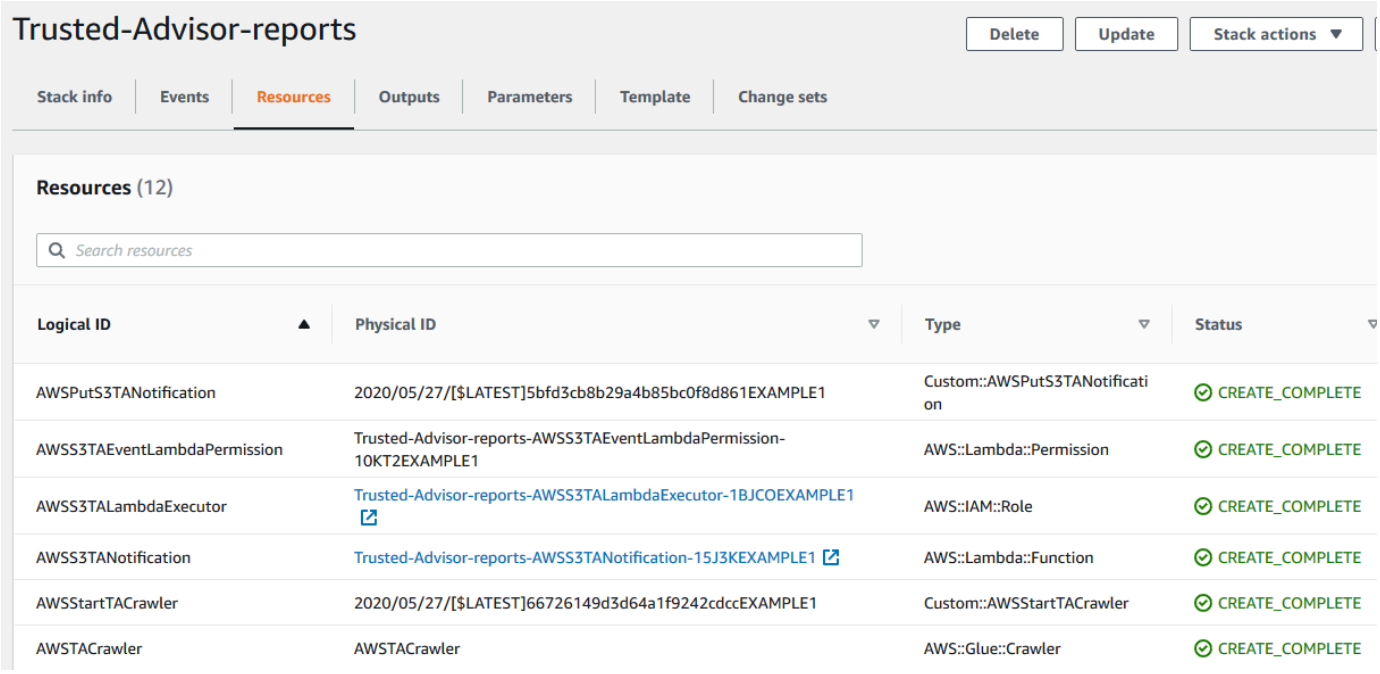
Después de cargar el informe en Amazon S3, cargue la siguiente plantilla de YAML a AWS CloudFormation. Esta plantilla le dice a AWS CloudFormation qué recursos crear para su cuenta para que otros servicios puedan usar los datos del informe en el bucket de S3. La plantilla crea recursos para IAM, AWS Lambda y AWS Glue.

Para crear sus recursos con AWS CloudFormation

1. Descargue el archivo trusted-advisor-reports-template.zip.
2. Descomprima el archivo.
3. Abra el archivo de la plantilla en un editor de texto.
4. En los parámetros `BucketName` y `FolderName`, reemplace los valores de *your-bucket-name-here* y *folder1* con el nombre del bucket y el nombre de la carpeta de su cuenta.

5. Guarde el archivo.
6. Abra la consola de AWS CloudFormation en https://console.aws.amazon.com/cloudformation.
7. Si aún no lo ha hecho, en el Selector de región, elija la región EE. UU. Este (Norte de Virginia).
8. En el panel de navegación, seleccione Stacks (Pilas).
9. Elija Create stack (Crear pila) y elija With new resources (standard) (Con nuevos recursos [estándar]).
10. En la página Create stack (Crear pila), en Specifiy template (Especificar una plantilla), elija Upload a template file (Cargar un archivo de plantilla) y, a continuación, elija Choose file (Elegir archivo).
11. Elija el archivo YAML y elija Next (Siguiente).
12. En la página Specify stack details (Especificar detalles de la pila), ingrese un nombre para la pila, como **`Organizational-view-Trusted-Advisor-reports`**, y haga clic en Next (Siguiente).
13. En la página Configure stack options (Configurar opciones de la pila), mantenga las opciones predeterminadas y elija Next (Siguiente).
14. En la página Review **`Organizational-view-Trusted-Advisor-reports`** (Revisar), revise las opciones. En la parte inferior de la página, active la casilla de verificación I acknowledge that AWS CloudFormation might create IAM resources (Reconozco que podría crear recursos de IAM).
15. Elija Crear pila.

    La pila tarda unos 5 minutos en crearse.
16. Después de que la pila se cree correctamente, se muestra la pestaña Resources (Recursos), como en el ejemplo siguiente.



Consultar los datos en Amazon Athena

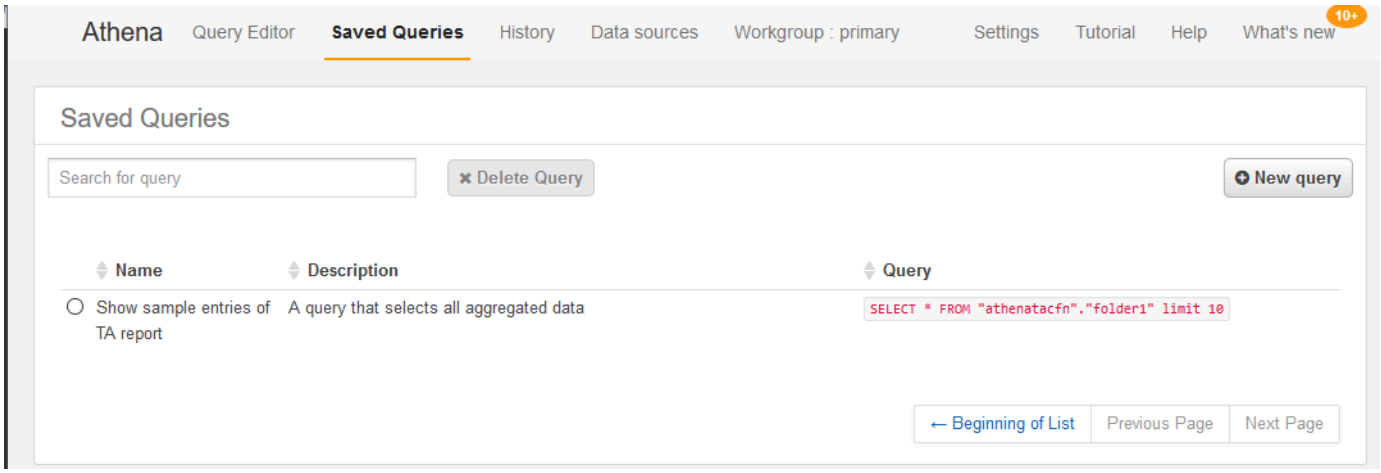
Después de tener sus recursos, puede ver los datos en Athena. Utilice Athena para crear consultas y analizar los resultados del informe, como buscar resultados de verificaciones específicas para cuentas de la organización.

> **Notas**
>
> - Elija la región EE. UU. Este (Norte de Virginia).
> - Si es nuevo en Athena, debe especificar una ubicación para los resultados de la consulta para poder ejecutar una consulta para el informe. Le recomendamos que especifique un bucket de S3 diferente para esta ubicación. Para obtener más información, consulte Especificación de una ubicación para los resultados de la consulta en la Guía del usuario de Amazon Athena.

Para consultar los datos en Athena

1. Abra la consola de Athena en https://console.aws.amazon.com/athena/.
2. Si aún no lo ha hecho, en el Selector de región, elija la región EE. UU. Este (Norte de Virginia).
3. Elija Saved Queries (Consultas guardadas) y, en el campo de búsqueda, ingrese **`Show sample`**.

4. Elija la consulta que aparece, como Mostrar entradas de muestra del informe TA.



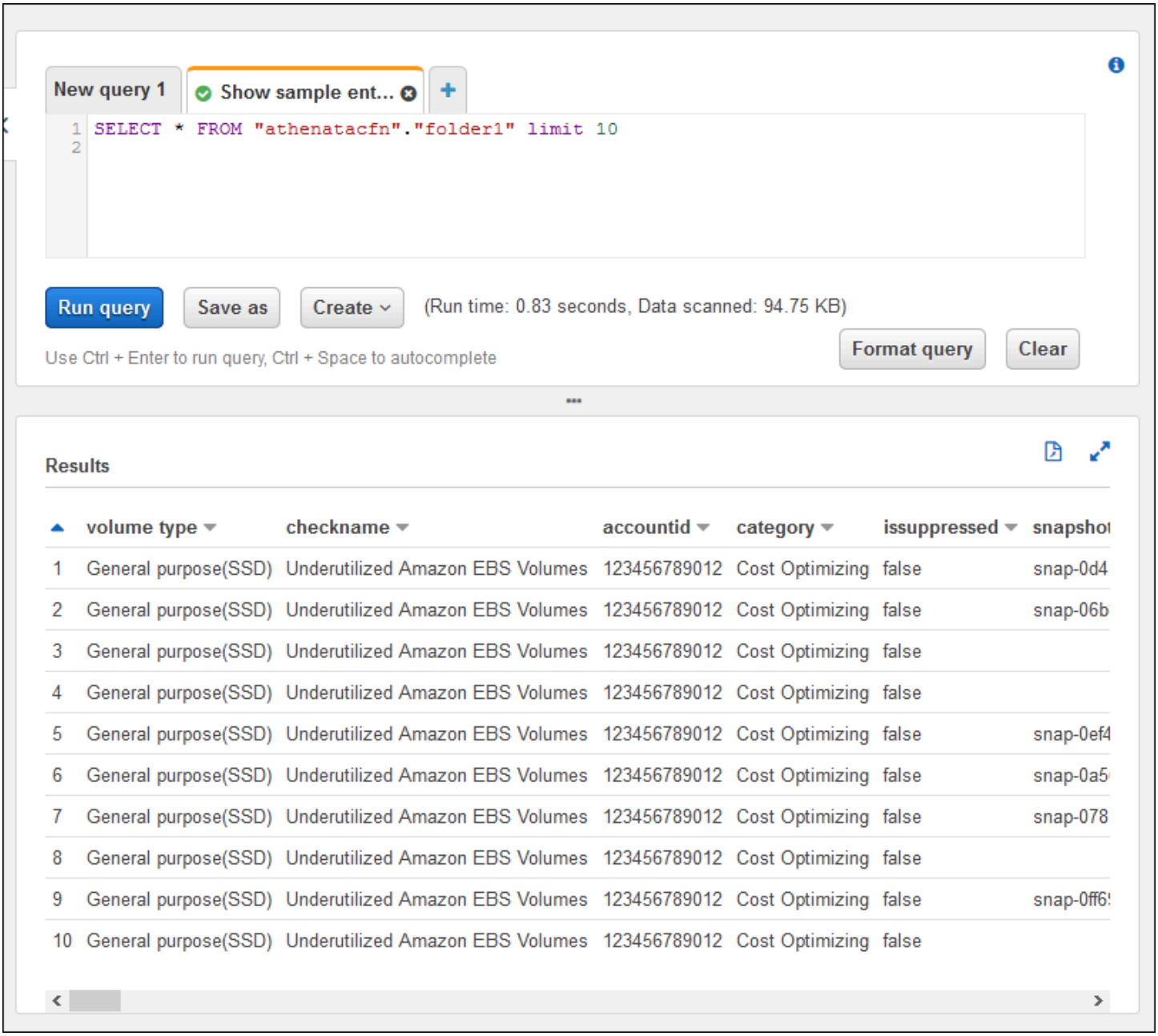
La consulta debe ser similar a la siguiente.

```
SELECT * FROM "athenatacfn"."folder1" limit 10
```

5. Elija Run Query (Ejecutar consulta). Aparecerán los resultados de la consulta.

Example : Consulta de Athena

En el ejemplo siguiente se muestran 10 entradas de muestra del informe.



Si desea obtener más información, consulte Ejecución de consultas SQL mediante Amazon Athena en la Guía del usuario de Amazon Athena.

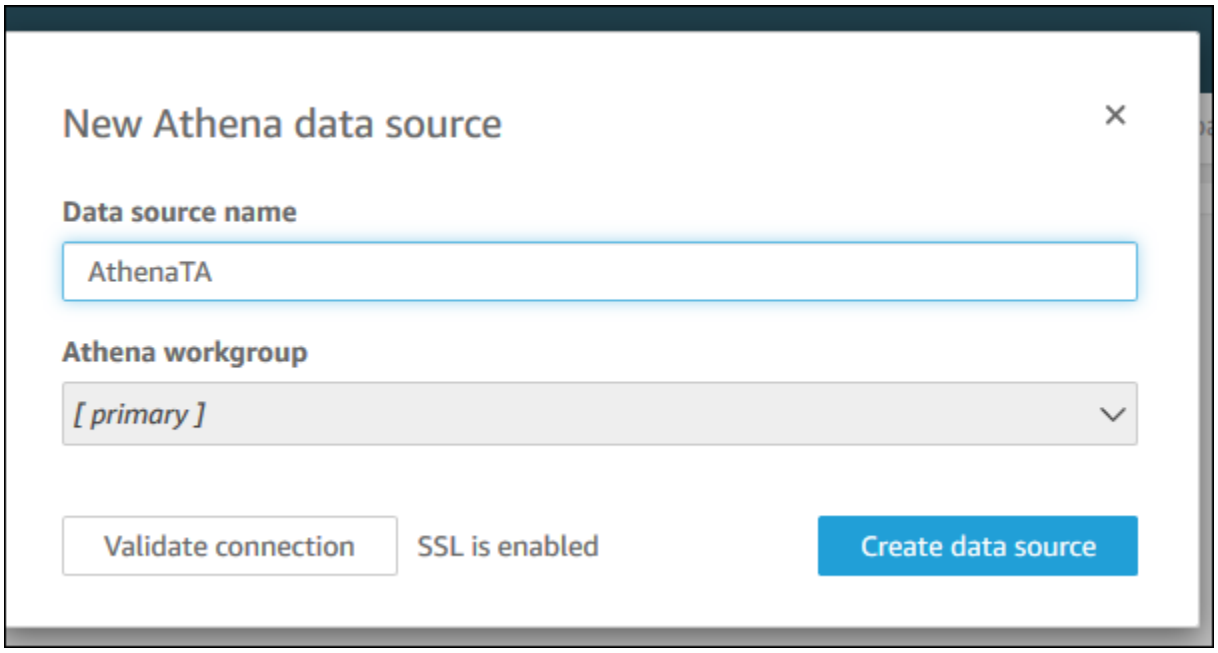
Crear un panel en Amazon QuickSight

También puede configurar Amazon QuickSight para que pueda ver sus datos en un panel y visualizar la información del informe.

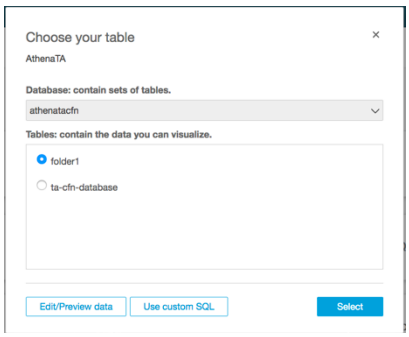
> **Note**
>
> Debe usar la región EE. UU. Este (Norte de Virginia).

Para crear un panel en Amazon QuickSight

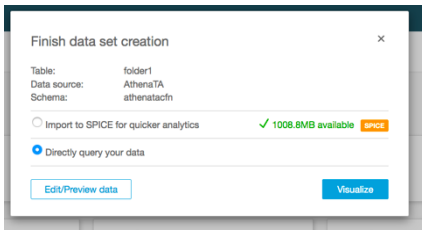
1. Vaya a la consola de Amazon QuickSight e inicie sesión con su cuenta.
2. Elija New analysis (Análisis nuevo), New dataset (Nuevo conjunto de datos) y haga clic en Athena.
3. En el cuadro de diálogo New Athena data source (Nuevo origen de datos de Athena), ingrese un nombre del origen de datos, como AthenaTA y luego elija Create data source (Crear origen de datos).



4. En el cuadro de diálogo Choose your table (Elija su tabla), elija la tabla athenatacfn, elija folder1 y luego Select (Seleccionar).



5. En el cuadro de diálogo Finish data set creation (Finalizar creación del conjunto de datos), elija Directly query your data (Consulta directa de sus datos) y elija Visualize (Visualizar).

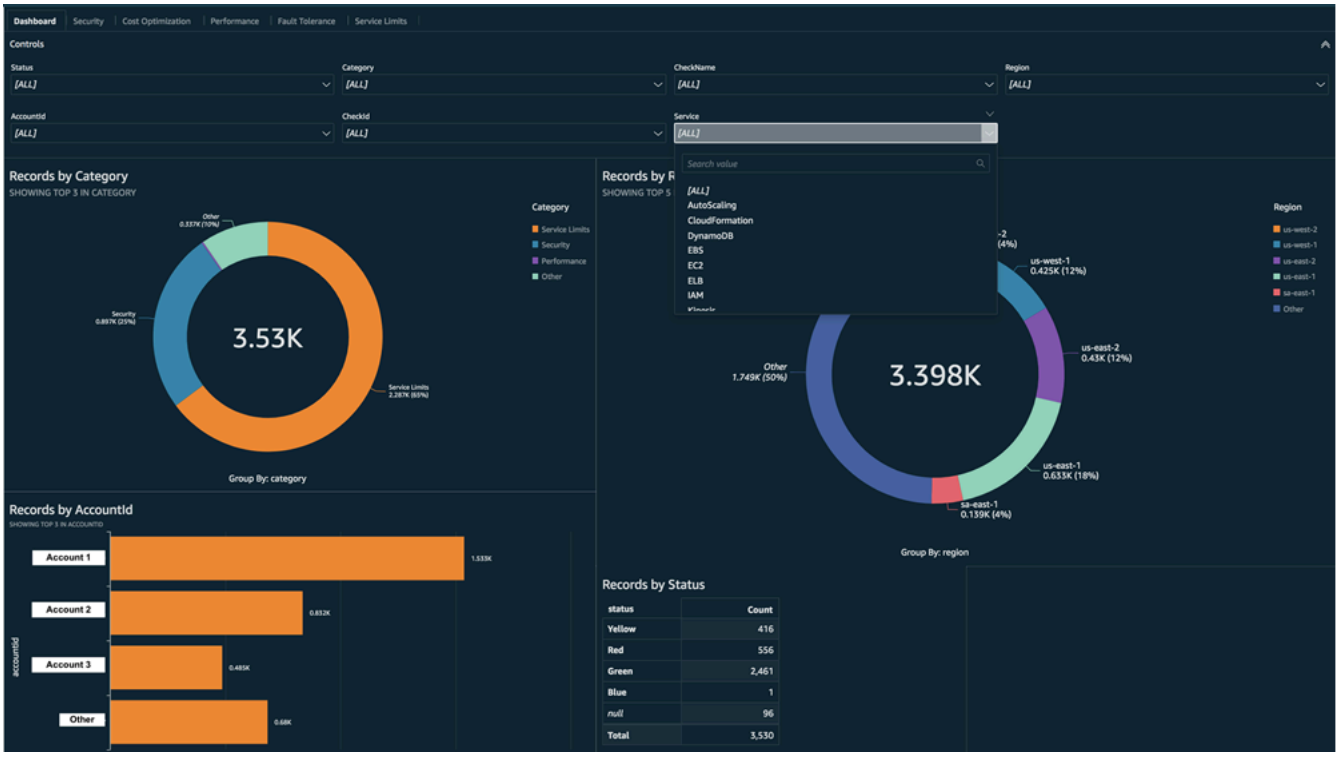


Ahora puede crear un panel en Amazon QuickSight. Para obtener más información, consulte Uso de Paneles en la Guía del usuario de Amazon QuickSight.

Example : Panel de Amazon QuickSight

En el siguiente panel de ejemplo se muestra información acerca de las verificaciones de Trusted Advisor, como las siguientes:

- ID de cuenta afectados
- Resumen por regiones de AWS
- Categorías de verificación
- Estados de verificaciones
- Número de entradas en el informe para cada cuenta



> **Note**
>
> Si tiene errores de permisos al crear el panel, asegúrese de que Amazon QuickSight puede utilizar Athena. Para obtener más información, consulte No puedo conectarme a Amazon Athena en la Guía del usuario de Amazon QuickSight.

Para obtener más información y ejemplos para visualizar los datos del informe, consulte Ver recomendaciones de AWS Trusted Advisor a escala con AWS Organizations en el Blog de Administración y Gobernanza de AWS.

Solución de problemas

Si tiene problemas con este tutorial, consulte las siguientes sugerencias para la solución de problemas.

No veo los datos más recientes en mi informe

Al crear un informe, la característica de vista organizativa no actualiza automáticamente las verificaciones de Trusted Advisor en su organización. Para obtener los resultados de las verificaciones más recientes, actualice las verificaciones de la cuenta de administración y de cada

cuenta de miembro de la organización. Para obtener más información, consulte Actualizar las verificaciones de Trusted Advisor.

Tengo columnas duplicadas en el informe

La consola de Athena puede mostrar el siguiente error en la tabla si el informe tiene columnas duplicadas.

```
HIVE_INVALID_METADATA: Hive metadata for table folder1 is invalid: Table descriptor contains duplicate columns
```

Por ejemplo, si agregó una columna en el informe que ya existe, esto puede causar problemas al intentar ver los datos del informe en la consola de Athena. Puede seguir estos pasos para solucionar este problema.

Buscar columnas duplicadas

Puede utilizar la consola de AWS Glue para ver el esquema e identificar rápidamente si tiene columnas duplicadas en el informe.

Para buscar columnas duplicadas

1. Abra la consola de AWS Glue en https://console.aws.amazon.com/glue/.
2. Si aún no lo ha hecho, en el Selector de región, elija la región EE. UU. Este (Norte de Virginia).
3. En el panel de navegación, elija Tables (Tablas).
4. Elija el nombre de su carpeta, como ***folder1*** y, a continuación, en Schema (Esquema), vea los valores de Column name (Nombre de la columna).

   Si tiene una columna duplicada, debe cargar un nuevo informe en su bucket de Amazon S3. Consulte la siguiente sección de Cargar un nuevo informe.

Cargar un nuevo informe

Una vez que haya identificado la columna duplicada, le recomendamos que sustituya el informe existente por uno nuevo. Esto garantiza que los recursos creados a partir de este tutorial utilicen los datos de informe más recientes de su organización.

Para cargar un nuevo informe

1. Si aún no lo ha hecho, actualice sus verificaciones de Trusted Advisor para las cuentas de su organización. Consulte Actualizar las verificaciones de Trusted Advisor.
2. Cree y descargue otro informe JSON en la consola de Trusted Advisor. Consulte Crear informes de vista organizativa. En este tutorial debe utilizar un archivo JSON.
3. Inicie sesión en la AWS Management Console y abra la consola de Amazon S3 en https://console.aws.amazon.com/s3/.
4. Elija su bucket de Amazon S3 y elija la carpeta *`folder1`*.
5. Seleccione los informes de *`resources`*`.json` anteriores y elija Delete (Eliminar).
6. En la página Delete objects (Eliminar objetos), en Permanently delete objects? (¿Desea eliminar los objetos de forma permanente?), ingrese **`permanently delete`** y haga clic en Delete objects (Eliminar objetos).
7. En su bucket de S3, elija Upload (Cargar) y, a continuación, especifique el nuevo informe. Esta acción actualiza automáticamente su tabla de Athena y los recursos de rastreador de AWS Glue con los datos de informe más recientes. Puede tardar varios minutos en actualizar los recursos.
8. Ingrese una nueva consulta en la consola de Athena. Consulte Consultar los datos en Amazon Athena.

> **Note**
>
> Si sigue teniendo problemas con este tutorial, puede crear un caso de soporte técnico en el Centro de AWS Support.

Ver comprobaciones de AWS Trusted Advisor con tecnología de AWS Config

AWS Config es un servicio que evalúa, audita y analiza de manera continua las configuraciones de los recursos en función de la configuración deseada. AWS Configproporciona reglas administradas, que son comprobaciones de conformidad predefinidas y personalizables que AWS Config utiliza para evaluar si los recursos de AWS cumplen con las prácticas recomendadas más comunes.

La consola de AWS Config lo guiará en la configuración y la activación de las reglas administradas. Además, puede utilizar la AWS Command Line Interface (AWS CLI) o la API de AWS Config para

pasar el código JSON que define la configuración de una regla administrada. Puede personalizar el comportamiento de una regla administrada para adaptarla a sus necesidades. Puede personalizar los parámetros de la regla para definir los atributos que deben tener los recursos para cumplir la regla. Para obtener más información acerca de la activación de AWS Config, consulte la Guía para desarrolladores de AWS Config.

Las reglas administradas de AWS Config impulsan un conjunto de comprobaciones de Trusted Advisor en todas las categorías. Cuando se habilitan determinadas reglas administradas, las comprobaciones de Trusted Advisor correspondientes se habilitan de manera automática. Para ver qué comprobaciones de Trusted Advisor son impulsadas por reglas administradas de AWS Config específicas, consulte AWS Trusted Advisor comprobar referencia.

Los comprobaciones con tecnología de AWS Config están disponibles para los clientes que tengan los siguientes planes: AWS Business Support, AWS Enterprise On-Ramp y AWS Enterprise Support. Si habilita AWS Config y tiene uno de estos planes AWS Support, verá de manera automática recomendaciones impulsadas por las reglas administradas de AWS Config implementadas correspondientes.

> **Note**
>
> Los resultados de estas comprobaciones se actualizan de manera automática en función de las actualizaciones activadas por cambios de las reglas administradas de AWS Config. No se permiten las solicitudes de actualización. Actualmente, no se pueden excluir recursos de estas comprobaciones.

Solución de problemas

Si tiene problemas con esta integración, consulte la siguiente información de solución de problemas.

Contenido

- Acabo de habilitar la grabación y las reglas administradas para AWS Config, pero no veo las comprobaciones de Trusted Advisor correspondientes.
- Implementé la misma regla administrada de AWS Config dos veces, ¿qué veré en Trusted Advisor?
- Desactivé la grabación para AWS Config en una región de AWS. ¿Qué veré en Trusted Advisor?

Acabo de habilitar la grabación y las reglas administradas para AWS Config, pero no veo las comprobaciones de Trusted Advisor correspondientes.

Una vez que la regla de AWS Config genere los resultados de la evaluación, podrá verlos en Trusted Advisor prácticamente en tiempo real. Si tiene problemas con esta característica, cree un caso de soporte técnico en el Centro de AWS Support.

Implementé la misma regla administrada de AWS Config dos veces, ¿qué veré en Trusted Advisor?

Verá entradas independientes en los resultados de la comprobación de Trusted Advisor para cada regla administrada que instale.

Desactivé la grabación para AWS Config en una región de AWS. ¿Qué veré en Trusted Advisor?

Si desactiva el registro de recursos para AWS Config en una región de AWS, Trusted Advisor dejará de recibir datos para las reglas administradas y las comprobaciones correspondientes de esa región. Los resultados de las reglas administradas existentes permanecen en AWS Config y en Trusted Advisor hasta que AWS Config caduca, según la política de retención de registros. Si se elimina una regla administrada, los datos de comprobación de Trusted Advisor suelen eliminarse casi en tiempo real.

Visualización de controles de AWS Security Hub en AWS Trusted Advisor

Después de habilitar AWS Security Hub para la Cuenta de AWS, puede ver los controles de seguridad y sus hallazgos en el la consola de Trusted Advisor. Puede emplear los controles de Security Hub para identificar las vulnerabilidades de seguridad de la cuenta, de la misma forma que puede utilizar las verificaciones de Trusted Advisor. Puede ver el estado de la verificación, la lista de recursos afectados y, a continuación, seguir las recomendaciones de Security Hub para solucionar los problemas de seguridad. Puede utilizar esta característica a fin de buscar recomendaciones de seguridad de Trusted Advisor y Security Hub en una ubicación conveniente.

Notas

- Desde Trusted Advisor, puede ver los controles del estándar de seguridad Prácticas de seguridad básicas recomendadas de AWS, excepto aquellos con Category: Recover >

Resilience (Categoría: Recuperar > Resiliencia). Para obtener una lista de los controles admitidos, consulte Controles de las prácticas de seguridad básicas recomendadas de AWS en la Guía del usuario de AWS Security Hub.

Para obtener más información sobre las categorías de Security Hub, consulte Categorías de control.

- Actualmente, cuando Security Hub añade nuevos controles al estándar de seguridad de las Prácticas de seguridad básicas recomendadas de AWS, puede haber una demora de dos a cuatro semanas antes de poder verlas en Trusted Advisor. Este plazo es el máximo esfuerzo y no está garantizado.

Temas

Requisitos previos

Debe cumplir los siguientes requisitos para habilitar la integración de Security Hub con Trusted Advisor:

- Para poder utilizar esta característica, debe contar con un plan de soporte Business, Enterprise On-Ramp o Enterprise. Puede encontrar su plan de soporte en AWS Support Center o en la página Planes de soporte. Para obtener más información, consulte Comparar planes de AWS Support.
- Debe habilitar el registro de recursos en AWS Config para las Regiones de AWS que desea incluir en los controles de Security Hub. Para obtener más información, consulte Habilitación y configuración de AWS Config.
- Debe habilitar Security Hub y seleccionar el estándar de seguridad Prácticas de seguridad básicas recomendadas de AWS v1.0.0. Si aún no lo ha hecho, consulte Configuración de AWS Security Hub en la Guía del usuario de AWS Security Hub.

> **Note**
>
> Si ya ha completado los requisitos previos, puede ir a Ver los hallazgos de Security Hub.

Acerca de las cuentas de AWS Organizations

Si ya ha completado los requisitos previos de una cuenta de administración, esta integración se habilita automáticamente para todas las cuentas miembro de la organización. Las cuentas miembro individuales no necesitan contactar a AWS Support para habilitar esta característica. Sin embargo, las cuentas miembro de la organización deben habilitar Security Hub si desean ver los hallazgos en Trusted Advisor.

Si desea desactivar esta integración para una cuenta miembro específica, consulte Desactivar esta característica para cuentas de AWS Organizations.

Ver los hallazgos de Security Hub

Una vez habilitado Security Hub para la cuenta, los hallazgos de Security Hub pueden tardar hasta 24 horas en aparecer en la página Security (Seguridad) de la consola de Trusted Advisor.

Para ver los resultados de Security Hub en Trusted Advisor

1. Vaya a consola de Trusted Advisor y luego elija la categoría Security (Seguridad).
2. En el campo Search by keyword (Buscar por palabra clave), introduzca el nombre o la descripción del control.

   > **Tip**
   >
   > En Source (Fuente), puede elegir AWS Security Hub para filtrar los controles de Security Hub.

3. Elija el nombre del control de Security Hub para ver la siguiente información:

   - Description (Descripción): describe cómo este control verifica si hay vulnerabilidades de seguridad en la cuenta.
   - Source (Fuente): determina si la verificación proviene de AWS Trusted Advisor o AWS Security Hub. Para los controles de Security Hub, puede buscar por ID de control.

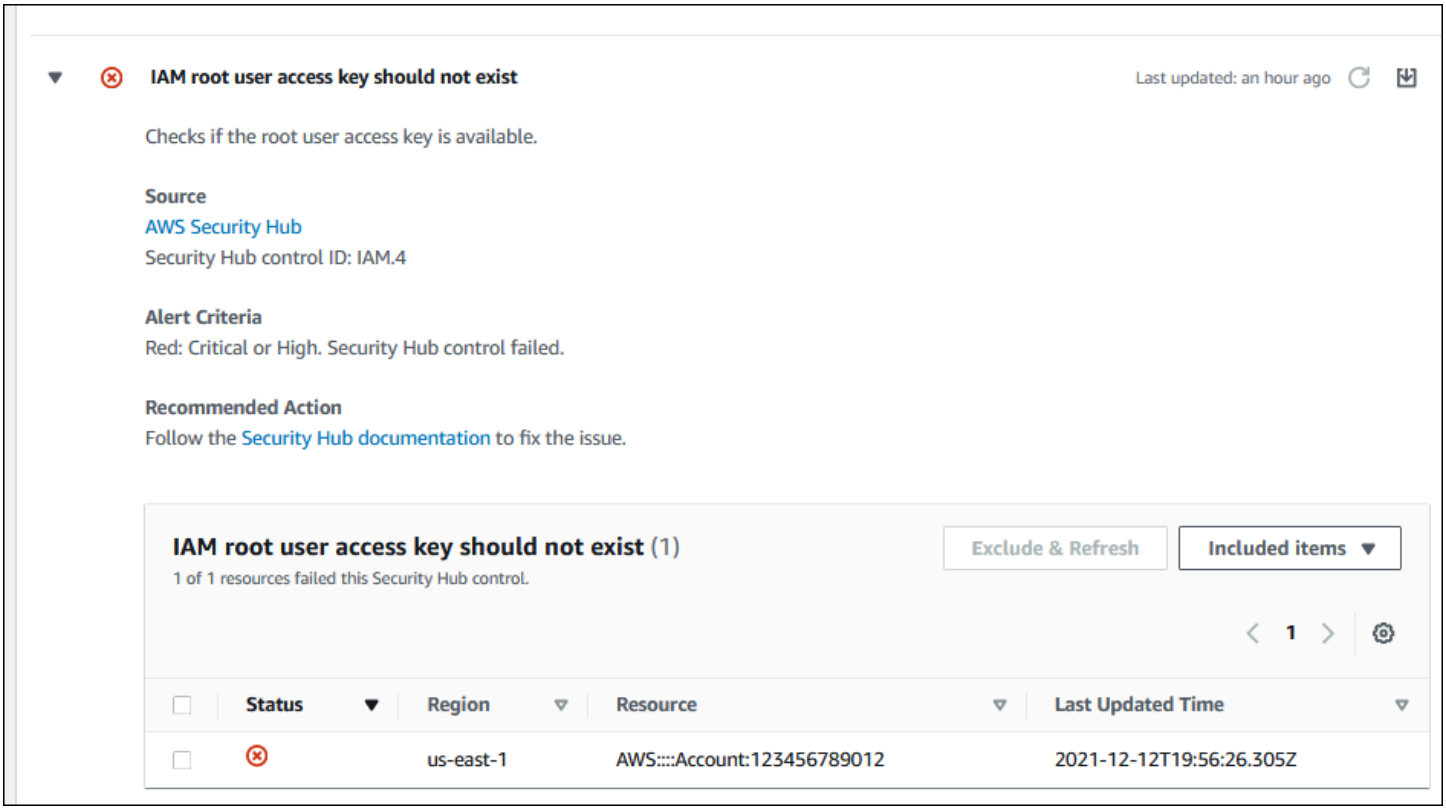
- Alert Criteria (Criterios de alerta): indica el estado del control. Por ejemplo, si Security Hub detecta un problema importante, el estado puede ser Red: Critical or High (Rojo: crítico o alto).
- Recommended Action (Acción recomendada): utilice el enlace a la documentación de Security Hub para encontrar los pasos recomendados y solucionar el problema.
- Security Hub resources (Recursos de Security Hub): puede encontrar los recursos de la cuenta en los que Security Hub ha detectado un problema.

Notas

- Debe utilizar Security Hub para excluir recursos de los hallazgos. En la actualidad, no puede utilizar la consola de Trusted Advisor para excluir elementos de los controles de Security Hub. Para obtener más información, consulte Establecimiento del estado de flujo de trabajo de los hallazgos.
- La característica de vista organizativa admite esta integración con Security Hub. Puede ver los hallazgos de los controles de Security Hub en toda la organización y, a continuación, crear y descargar informes. Para obtener más información, consulte Vista organizativa para AWS Trusted Advisor.

Example Ejemplo: el control de Security Hub para la clave de acceso de usuario de IAM no debería existir

A continuación se muestra un ejemplo de búsqueda de un control de Security Hub en la consola de Trusted Advisor.



Actualizar los hallazgos de Security Hub

Una vez habilitado un estándar de seguridad, Security Hub puede tardar hasta dos horas en obtener hallazgos de los recursos. Luego, esos datos pueden tardar hasta 24 horas en aparecer en la consola de Trusted Advisor. Si ha habilitado recientemente el estándar de seguridad Prácticas de seguridad básicas recomendadas de AWS v1.0.0, vuelva a verificar la consola de Trusted Advisor más tarde.

> **Note**
>
> - La programación de cada control de Security Hub es periódica o se activa por cambios. En la actualidad, no puede utilizar la consola de Trusted Advisor o la API de AWS Support para actualizar los controles de Security Hub. Para obtener más información, consulte Programar la ejecución de verificaciones de seguridad.
> - Debe utilizar Security Hub si desea excluir recursos de los hallazgos. En la actualidad, no puede utilizar la consola de Trusted Advisor para excluir elementos de los controles de Security Hub. Para obtener más información, consulte Establecimiento del estado de flujo de trabajo de los hallazgos.

Desactivar Security Hub desde Trusted Advisor

Siga este procedimiento si no desea que la información de Security Hub aparezca en la consola de Trusted Advisor. Este procedimiento solo desactiva la integración de Security Hub con Trusted Advisor. No afectará las configuraciones establecidas en Security Hub. Puede seguir utilizando la consola de Security Hub para ver los controles de seguridad, los recursos y las recomendaciones.

Para desactivar la integración de Security Hub

1. Contacte a AWS Support y solicite la desactivación de la integración de Security Hub con Trusted Advisor.

   Después de que AWS Support deshabilita esta característica, Security Hub ya no envía datos a Trusted Advisor. Los datos de Security Hub se eliminarán de Trusted Advisor.
2. Si desea volver a habilitar esta integración, contacte a AWS Support.

Desactivar esta característica para cuentas de AWS Organizations

Si ya ha completado los requisitos previos para una cuenta de administración, la integración de Security Hub se eliminará automáticamente de todas las cuentas miembro de la organización. Las cuentas miembro individuales de la organización no necesitan contactar a AWS Support por separado.

Si usted es una cuenta miembro de una organización, puede contactar a AWS Support para eliminar esta característica solo de su cuenta.

Solución de problemas

Si tiene problemas con esta integración, consulte la siguiente información para obtener una solución.

Contenido

- Veo múltiples Regiones de AWS para el mismo recurso afectado para una comprobación de Security Hub
- He desactivado Security Hub o AWS Config en una región
- Mi control está archivado en Security Hub, pero sigo viendo los resultados en Trusted Advisor
- Aún no puedo ver los hallazgos de Security Hub

No veo los hallazgos de Security Hub en la consola de Trusted Advisor

Asegúrese de haber completado los siguientes pasos:

- Usted cuenta con un plan Business, Enterprise On-Ramp o Enterprise.
- Usted ha habilitado el registro de recursos en AWS Config dentro de la misma región que Security Hub.
- Usted ha habilitado Security Hub y ha seleccionado el estándar de seguridad Prácticas de seguridad básicas recomendadas de AWS v1.0.0.
- Los nuevos controles de Security Hub se añaden como comprobaciones en Trusted Advisor en un plazo de dos a cuatro semanas. Consulte la nota.

Para obtener más información, consulte Requisitos previos.

He configurado Security Hub y AWS Config correctamente, pero siguen faltando mis hallazgos

Obtener hallazgos de los recursos puede tardar hasta dos horas. Luego, esos datos pueden tardar hasta 24 horas en aparecer en la consola de Trusted Advisor. Vuelva a verificar la consola de Trusted Advisor más tarde.

> **Notas**
>
> - Solo los hallazgos de los controles sobre las Prácticas de seguridad básicas recomendadas de AWS aparecerán en Trusted Advisor, excepto aquellos con Category: Recover > Resilience (Categoría: Recuperar > Resiliencia).
> - Si hay un problema de servicio con Security Hub o si Security Hub no está disponible, los resultados pueden tardar hasta 24 horas en aparecer en Trusted Advisor. Vuelva a verificar la consola de Trusted Advisor más tarde.

Quiero deshabilitar controles específicos de Security Hub

Security Hub envía los datos a Trusted Advisor automáticamente. Si desactiva un control de Security Hub o ya no tiene recursos para ese control, los hallazgos no aparecerán en Trusted Advisor.

Puede iniciar sesión en la consola de Security Hub y verificar si el control está habilitado o desactivado.

Si deshabilita un control de Security Hub o deshabilita todos los controles del estándar de seguridad Prácticas de seguridad básicas recomendadas de AWS, sus hallazgos se archivan en los próximos cinco días. Este periodo de cinco días para el archivo es aproximado y de mejor esfuerzo solamente, y no está garantizado. Cuando se archivan los resultados, se eliminan de Trusted Advisor.

Para obtener más información, consulte los siguientes temas:

- Deshabilitación y habilitación de controles individuales
- Deshabilitación o habilitación de un estándar de seguridad

Quiero encontrar los recursos de Security Hub excluidos

Desde la consola de Trusted Advisor, puede elegir el nombre del control de Security Hub y, a continuación, la opción Excluded items (Elementos excluidos). Esta opción muestra todos los recursos que se suprimieron en Security Hub.

Si el estado de flujo de trabajo de un recurso se establece en `SUPPRESSED`, ese recurso es un elemento excluido en Trusted Advisor. No se pueden suprimir los recursos de Security Hub desde la consola de Trusted Advisor. Para ello, utilice la consola de Security Hub. Para obtener más información, consulte Establecimiento del estado de flujo de trabajo de los hallazgos.

Quiero habilitar o desactivar esta característica para una cuenta miembro que pertenece a una organización de AWS

De forma predeterminada, las cuentas miembro heredan la característica de la cuenta de administración para AWS Organizations. Si la cuenta de administración ha habilitado la característica, todas las cuentas de la organización también la tendrán. Si tiene una cuenta miembro y desea realizar cambios específicos en esta, debe contactar a AWS Support.

Veo múltiples Regiones de AWS para el mismo recurso afectado para una comprobación de Security Hub

Algunos Servicios de AWS son globales y no son específicos de una región, como IAM y Amazon CloudFront. De forma predeterminada, los recursos globales como los buckets de Amazon S3 aparecen en la región Este de EE. UU. (Norte de Virginia).

Para las comprobaciones de Security Hub que evalúan los recursos de los servicios globales, es posible que vea más de un elemento para los recursos afectados. Por ejemplo: si la comprobación `Hardware MFA should be enabled for the root user` identifica que su cuenta no ha activado esta característica, verá varias regiones en la tabla para el mismo recurso.

Puede configurar Security Hub y AWS Config para que no aparezcan varias regiones para el mismo recurso. Para mayor información, consulte AWS Controles de prácticas básicas recomendadas que quizás desee desactivar.

He desactivado Security Hub o AWS Config en una región

Si detiene el registro de recursos con AWS Config o desactiva Security Hub en una Región de AWS, Trusted Advisor ya no recibirá datos de ningún control en esa región. Trusted Advisor elimina los resultados de Security Hub en un plazo de 7 a 9 días. Este plazo es el máximo esfuerzo y no está garantizado. Para obtener más información, consulte Deshabilitar Security Hub.

Para deshabilitar esta característica de la cuenta, consulte Desactivar Security Hub desde Trusted Advisor.

Mi control está archivado en Security Hub, pero sigo viendo los resultados en Trusted Advisor

Cuando el estado de `RecordState` cambia a `ARCHIVED` correspondiente a una búsqueda, Trusted Advisor elimina la búsqueda de ese control de Security Hub de su cuenta. Es posible que siga viendo el resultado en Trusted Advisor hasta 7 a 9 días antes de que se elimine. Este plazo es el máximo esfuerzo y no está garantizado.

Aún no puedo ver los hallazgos de Security Hub

Si sigue teniendo problemas con esta característica, puede crear un caso de soporte técnico en AWS Support Center.

Optar AWS Compute Optimizer por recibir Trusted Advisor cheques

Compute Optimizer es un servicio que analiza las métricas de configuración y utilización de sus recursos de AWS . Este servicio informa si sus recursos están configurados correctamente para obtener eficiencia y fiabilidad. También sugiere qué mejoras puede implementar para aumentar el rendimiento de la carga de trabajo. Con Compute Optimizer, ves las mismas recomendaciones en tus Trusted Advisor comprobaciones.

Puede optar por abrir su Cuenta de AWS única cuenta o todas las cuentas de los miembros que forman parte de una organización. AWS Organizations Para obtener más información, consulte la Introducción de la Guía del usuario de AWS Compute Optimizer .

Una vez que haya elegido Compute Optimizer, las siguientes comprobaciones reciben datos de las funciones Lambda y de los volúmenes de Amazon EBS. La generación de resultados y las recomendaciones de optimización pueden demorar hasta 12 horas. En ese caso, la visualización de los resultados puede tardar hasta 48 horas en Trusted Advisor realizarse las siguientes comprobaciones:

Optimización de costos

- Volúmenes con exceso de aprovisionamiento de Amazon EBS
- AWS Lambda funciones sobreaprovisionadas para el tamaño de la memoria

Rendimiento

- Volúmenes con falta de aprovisionamiento de Amazon EBS
- AWS Lambda funciones insuficientemente aprovisionadas para el tamaño de la memoria

Notas

- Los resultados de estas comprobaciones se actualizan automáticamente varias veces al día. No se permiten las solicitudes de actualización. Puede que los cambios tarden unas horas en aparecer. Actualmente, no se pueden excluir recursos de estas comprobaciones.
- Trusted Advisor ya tiene los cheques Amazon EBS Volumes subutilizados y Amazon EBS Magnetic Volumes sobreutilizados.

Una vez que haya elegido Compute Optimizer, le recomendamos que utilice los nuevos volúmenes con exceso de aprovisionamiento de Amazon EBS y las comprobaciones de volúmenes con falta de aprovisionamiento de Amazon EBS.

Información relacionada

Para obtener más información, consulte los temas siguientes:

- Ver las recomendaciones de volúmenes de Amazon EBS en la Guía del usuario de AWS Compute Optimizer
- Visualización de las recomendaciones de funciones Lambda en la Guía del usuario de AWS Compute Optimizer
- Configuración de la memoria de funciones Lambda en la Guía para desarrolladores de AWS Lambda
- Solicite modificaciones a sus volúmenes de Amazon EBS en la Guía del usuario de Amazon EC2

Introducción a AWS Trusted Advisor Priority

Trusted Advisor Priority ayuda a proteger y optimizar su Cuenta de AWS para seguir mejor las prácticas recomendadas de AWS. Con Trusted Advisor Priority, el equipo de Cuenta de AWS puede supervisar de forma proactiva su cuenta y crear recomendaciones priorizadas cuando identifique oportunidades en su nombre.

Por ejemplo, el equipo de cuentas puede identificar si el usuario raíz de su cuenta de AWS carece de autenticación multifactor (MFA). El equipo de cuentas puede crear una recomendación para que pueda tomar medidas inmediatas en relación con una comprobación, como `MFA on Root Account`. La recomendación aparece como una recomendación priorizada en la página de Trusted Advisor Priority de la consola de Trusted Advisor. A continuación, debe seguir las recomendaciones para resolver el asunto en cuestión.

Las recomendaciones de Trusted Advisor Priority tienen los siguientes dos orígenes:

- Servicios de AWS: servicios tales comoTrusted Advisor, AWS Security Hub, y AWS Well-Architected crean recomendaciones automáticamente. El equipo de cuentas comparte estas recomendaciones para que aparezcan en Trusted Advisor Priority.

- Equipo de cuentas: el equipo de cuentas puede crear recomendaciones manuales.

Trusted Advisor Priority lo ayuda a centrarse en las recomendaciones más importantes. Puede monitorear el ciclo de vida de la recomendación junto con el equipo de cuentas, desde el momento en que dicho equipo la haya compartido hasta el momento en que usted la confirme, resuelva o descarte. Puede usar Trusted Advisor Priority para encontrar recomendaciones para todas las cuentas de miembros de su organización.

Temas

Requisitos previos

Para utilizar Trusted Advisor Priority, debe cumplir con los siguientes requisitos:

- Debe tener un plan Enterprise Support.
- Su cuenta debe formar parte de una organización que tenga habilitadas todas las características de AWS Organizations. Para obtener más información, consulte Habilitar todas las características en la organización en la Guía del usuario de AWS Organizations.
- Su organización debe tener habilitado el acceso de confianza de Trusted Advisor. Para habilitar el acceso de confianza, inicie sesión con la cuenta de administración. Abra la página Tu organización en la consola de Trusted Advisor.

- Para ver las recomendaciones de Trusted Advisor Priority para su cuenta, debe iniciar sesión en su cuenta de AWS.
- Para ver las recomendaciones agregadas de toda la organización, debe iniciar sesión en la cuenta de administración de la organización o en una cuenta de administrador delegado. Para obtener instrucciones sobre cómo registrar cuentas de administrador delegado, consulte Registro de administradores delegados.
- Debe tener permisos de AWS Identity and Access Management (IAM) para acceder a Trusted Advisor Priority. Para obtener más información acerca del control de acceso a Trusted Advisor Priority, consulte Gestione el acceso a AWS Trusted Advisor y AWS políticas gestionadas para AWS Trusted Advisor.

Habilitar Trusted Advisor Priority

Solicite a su equipo de cuentas que habilite esta característica. Debe tener un plan de soporte empresarial y ser el propietario de la cuenta de administración de su organización. Si la página de Trusted Advisor Priority de la consola indica que se necesita acceso de confianza con AWS Organizations, elija Habilitar el acceso de confianza con AWS Organizations. Para obtener más información, consulte la sección Requisitos previos.

Ver recomendaciones priorizadas

Una vez que el equipo de cuentas habilite Trusted Advisor Priority, podrá ver las recomendaciones más recientes para su cuenta de AWS.

Ver sus recomendaciones priorizadas

1. Inicie sesión en la consola de Trusted Advisor en https://console.aws.amazon.com/trustedadvisor/home.
2. En la página Trusted Advisor Priority, podrá ver los siguientes elementos:

   Si utiliza una cuenta de administración o de administrador delegado de AWS Organizations, cambie a la pestaña Mi cuenta.

   - Acciones necesarias: número de recomendaciones que están pendientes de respuesta o en curso.
   - Overview (Información general): la siguiente información:
     - Recomendaciones descartadas en los últimos 90 días

- Recomendaciones resueltas en los últimos 90 días
- Recomendaciones sin actualización en más de 30 días
- Tiempo medio para resolver recomendaciones

3. En la pestaña Activas, en Recomendaciones priorizadas activas se muestran las recomendaciones que el equipo de cuentas priorizó. La pestaña Cerradas muestra las recomendaciones resueltas o descartadas.

   - Para filtrar los resultados, use las siguientes opciones:

     - Recommendation (Recomendación): ingrese palabras clave para buscar por nombre. Puede ser un nombre de comprobación o un nombre personalizado creado por el equipo de cuentas.
     - Estado: si la recomendación está pendiente de respuesta, en curso, descartada o resuelta.
     - Fuente: el origen de una recomendación priorizada. La recomendación puede provenir de Servicios de AWS, el equipo de su Cuenta de AWS o un evento de servicio planificado.
     - Categoría: la categoría de la recomendación, como la seguridad o la optimización de costos.
     - Age (Antigüedad): cuando el equipo de cuentas compartió la recomendación.

4. Elija una recomendación para obtener más información acerca de los detalles, los recursos afectados y las acciones recomendadas. A continuación, puede confirmar o descartar la recomendación.

Para ver las recomendaciones priorizadas en todas las cuentas de su organización de AWS

Tanto la cuenta de administración como los administradores delegados de Trusted Advisor Priority pueden ver las recomendaciones agregadas de toda la organización.

> **Note**
>
> Las cuentas de miembros no tienen acceso a las recomendaciones agregadas.

1. Inicie sesión en la consola de Trusted Advisor en https://console.aws.amazon.com/trustedadvisor/home.
2. En la página de Trusted Advisor Priority, asegúrese de estar en la pestaña Mi organización.

3. Para ver las recomendaciones para una cuenta, seleccione una cuenta de la lista desplegable Seleccione una cuenta de su organización. O bien, puede ver las recomendaciones de todas sus cuentas.

   En la pestaña Mi organización, podrá ver los siguientes elementos:

   - Acciones necesarias: la cantidad de recomendaciones en su organización que están pendientes de respuesta o en curso.
   - Información general: se muestran los siguientes elementos:

     - Recomendaciones descartadas en los últimos 90 días.

     - Recomendaciones resueltas en los últimos 90 días.

     - Recomendaciones sin actualización en más de 30 días.

     - Tiempo promedio para resolver recomendaciones.

4. En la pestaña Activas, en la sección Recomendaciones priorizadas activas se muestran las recomendaciones que el equipo de cuentas priorizó. La pestaña Cerradas muestra las recomendaciones resueltas o descartadas.

   Para filtrar los resultados, use las siguientes opciones:

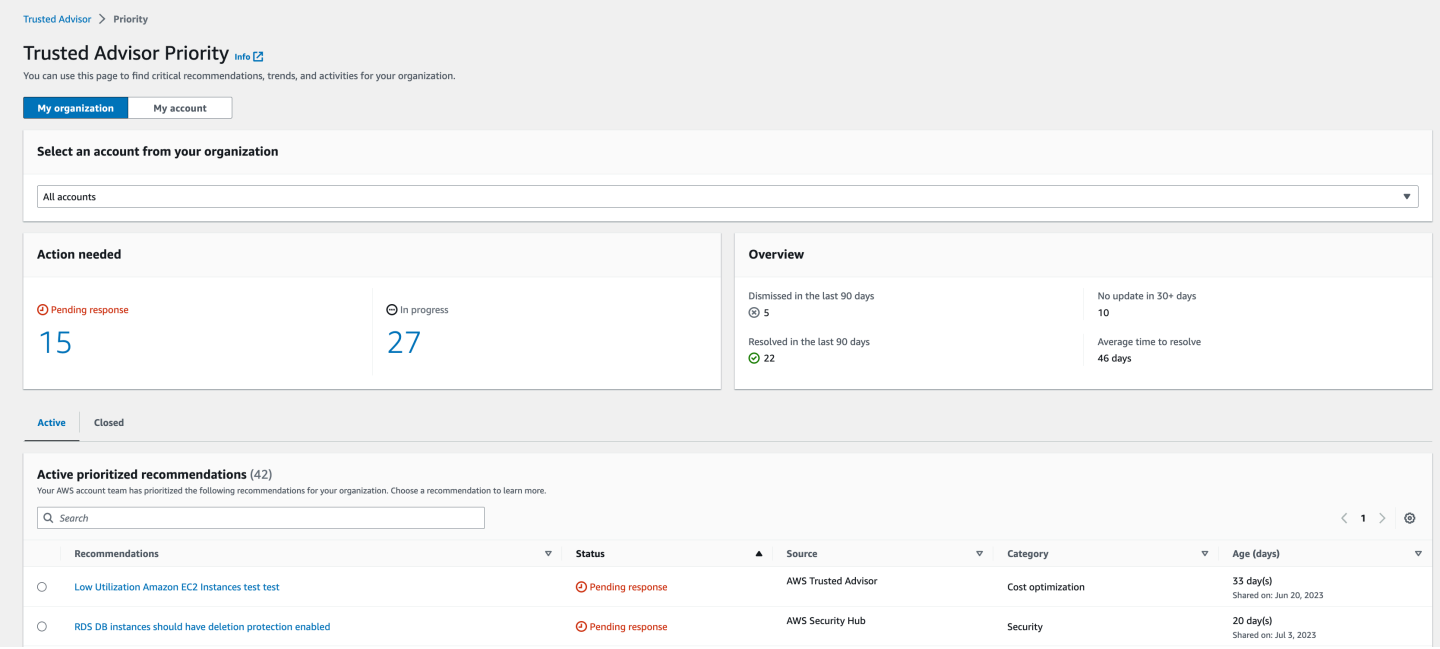
   - Recommendation (Recomendación): ingrese palabras clave para buscar por nombre. Puede ser un nombre de comprobación o un nombre personalizado creado por el equipo de cuentas.
   - Estado: si la recomendación está pendiente de respuesta, en curso, descartada o resuelta.
   - Fuente: el origen de una recomendación priorizada. La recomendación puede provenir de Servicios de AWS, el equipo de su Cuenta de AWS o un evento de servicio planificado.
   - Categoría: la categoría de la recomendación, como la seguridad o la optimización de costos.
   - Age (Antigüedad): cuando el equipo de cuentas compartió la recomendación.

5. Elija una recomendación para ver los detalles adicionales, las cuentas y los recursos afectados, y las acciones recomendadas. A continuación, puede confirmar o descartar la recomendación.

Example : recomendaciones de Trusted Advisor Priority

En el siguiente ejemplo se muestran 15 recomendaciones que están pendientes de respuesta y otras 27 que están en curso en la sección Acción necesaria. En la siguiente imagen se muestran

dos de las recomendaciones que están pendientes de respuesta en la pestaña Recomendación priorizada activa.



Confirmación de una recomendación

En la pestaña Activas, puede obtener más información sobre la recomendación, y luego decidir si quiere confirmarla.

Para confirmar una recomendación

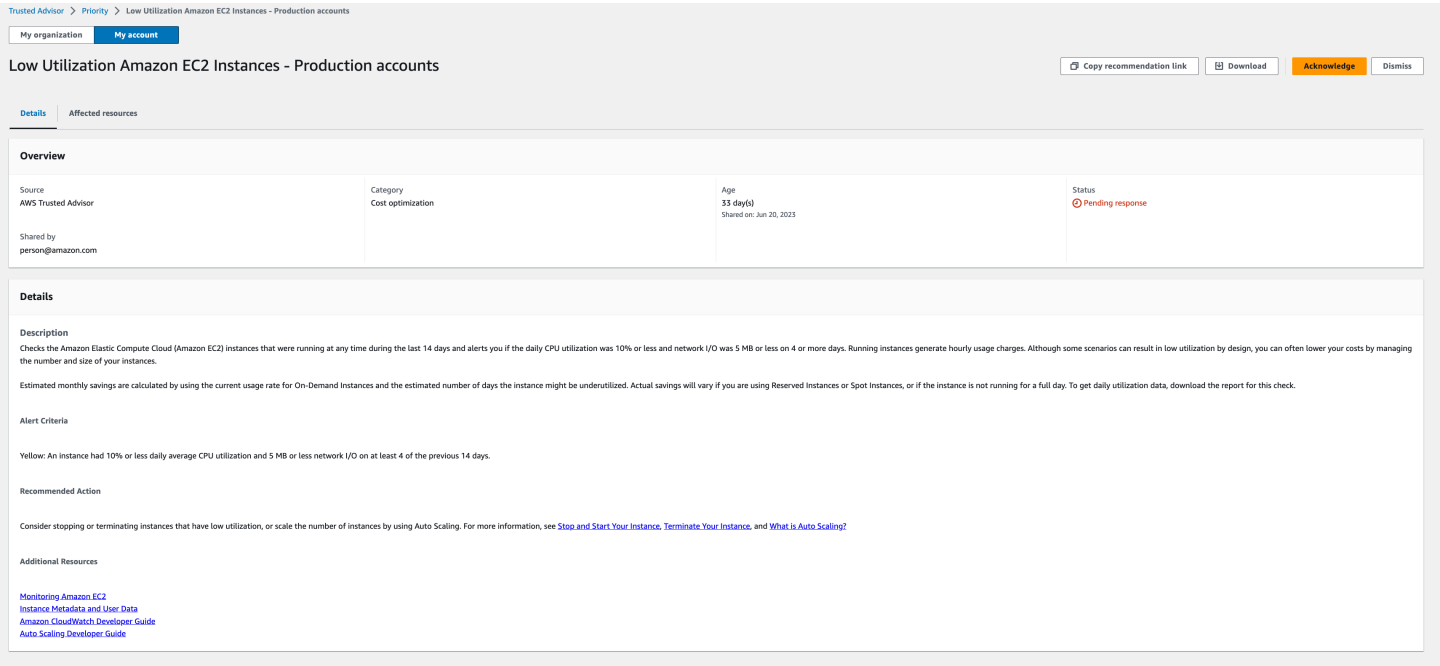
1. Inicie sesión en la consola de Trusted Advisor en https://console.aws.amazon.com/trustedadvisor/home.
2. Si utiliza una cuenta de administración o de administrador delegado de AWS Organizations, cambie a la pestaña Mi cuenta.
3. En la página Trusted Advisor Priority, en la pestaña Active (Activo), elija un nombre de recomendación.
4. En la sección Detalles, puede consultar las acciones recomendadas para resolver la recomendación.
5. En la sección Recursos afectados, puede revisar los recursos afectados y filtrarlos por Estado.
6. Seleccione Confirmar.
7. En el cuadro de diálogo Confirmar recomendación, seleccione Confirmar.

El estado de la recomendación cambia a In progress (En curso). Las recomendaciones en curso o pendientes de respuesta aparecen en la pestaña Active (Activo) en la página de Trusted Advisor Priority.

8. Realice las acciones recomendadas para resolver la recomendación. Para más información, consulte Resolver una recomendación.

Example : Recomendación manual de Trusted Advisor Priority

En la siguiente imagen se muestra la recomendación Instancias de EC2 de bajo uso que está pendiente de respuesta.



Para confirmar una recomendación para todas las cuentas de su organización de AWS

La cuenta de administración o los administradores delegados de Trusted Advisor pueden confirmar una recomendación para todas las cuentas afectadas.

> **Note**
>
> Las cuentas de miembros no tienen acceso a las recomendaciones agregadas.

1. Inicie sesión en la consola de Trusted Advisor en https://console.aws.amazon.com/trustedadvisor/home.

2. En la página de Trusted Advisor Priority, asegúrese de estar en la pestaña Mi organización.
3. En la pestaña Activas, seleccione el nombre de una recomendación.
4. Seleccione Confirmar.
5. En el cuadro de diálogo Confirmar recomendación, seleccione Confirmar.

   El estado de la recomendación cambia a In progress (En curso).
6. Realice las acciones recomendadas para resolver la recomendación. Para más información, consulte Resolver una recomendación.
7. Para ver los detalles de una recomendación, elija el nombre de la recomendación.

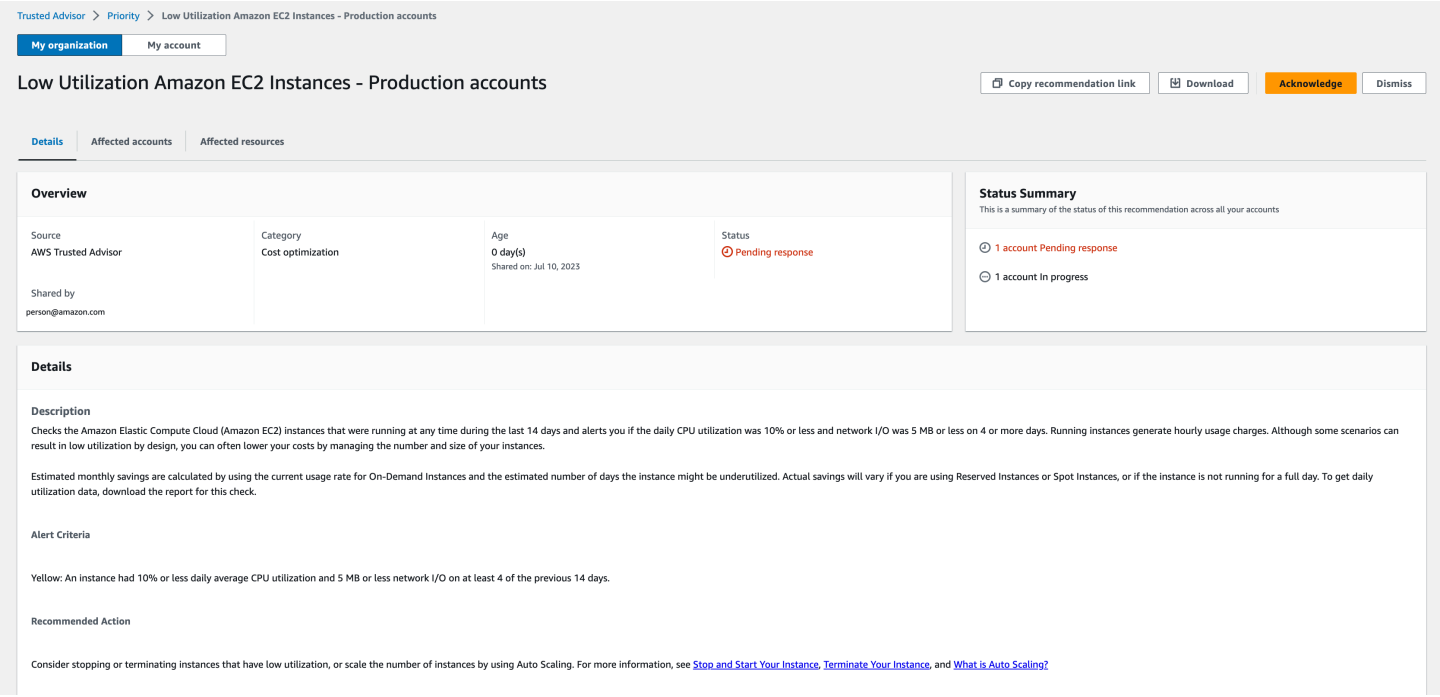
   En la sección Detalles, puede revisar la siguiente información sobre la recomendación:

   - La Información general de la recomendación y una sección de Detalles que incluye las acciones que se deben completar.

     Un Resumen de estado que muestra las recomendaciones para todas las cuentas afectadas.
   - En la sección Cuentas afectadas, puede revisar los recursos afectados de todas las cuentas. Puede filtrar por Número de cuenta y Estado.
   - En la sección Recursos afectados, puede revisar los recursos afectados de todas las cuentas. Puede filtrar por Número de cuenta y Estado.

Example : Recomendación manual de Trusted Advisor Priority

La siguiente imagen muestra la recomendación Instancias de Amazon EC2 de bajo uso que está pendiente de respuesta. Una cuenta afectada confirmó la recomendación. Otra cuenta está pendiente de respuesta, por lo que el estado de la recomendación es Pendiente de respuesta.



Descartar una recomendación

También puede descartar una recomendación. Esto significa que usted confirma la recomendación, pero no va a atenderla. Puede descartar una recomendación si no es relevante para su cuenta. Por ejemplo, si está utilizando una Cuenta de AWS de prueba y tiene previsto eliminarla, no es necesario que realice las acciones recomendadas.

Para descartar una recomendación

1. Inicie sesión en la consola de Trusted Advisor en https://console.aws.amazon.com/trustedadvisor/home.
2. Si utiliza una cuenta de administración o de administrador delegado de AWS Organizations, cambie a la pestaña Mi cuenta.
3. En la página Trusted Advisor Priority, en la pestaña Active (Activo), elija un nombre de recomendación.
4. En la página de detalles de la recomendación, revise la información sobre los recursos afectados.
5. Si esta recomendación no es relevante para su cuenta, seleccione Descartar.
6. En el cuadro de diálogo Descartar recomendación), seleccione el motivo por el que no va a atender la recomendación.

7. (Opcional) Ingrese una nota que detalle el motivo por el que descarta la recomendación. Si selecciona Otros, debe ingresar una descripción en la sección Nota.
8. Seleccione Descartar. El estado de la recomendación cambia a Descartada y aparece en la pestaña Cerradas de la página de Trusted Advisor Priority.

Para descartar una recomendación para todas las cuentas de su organización de AWS

La cuenta de administración o el administrador delegado de Trusted Advisor Priority pueden descartar una recomendación para todas las cuentas.

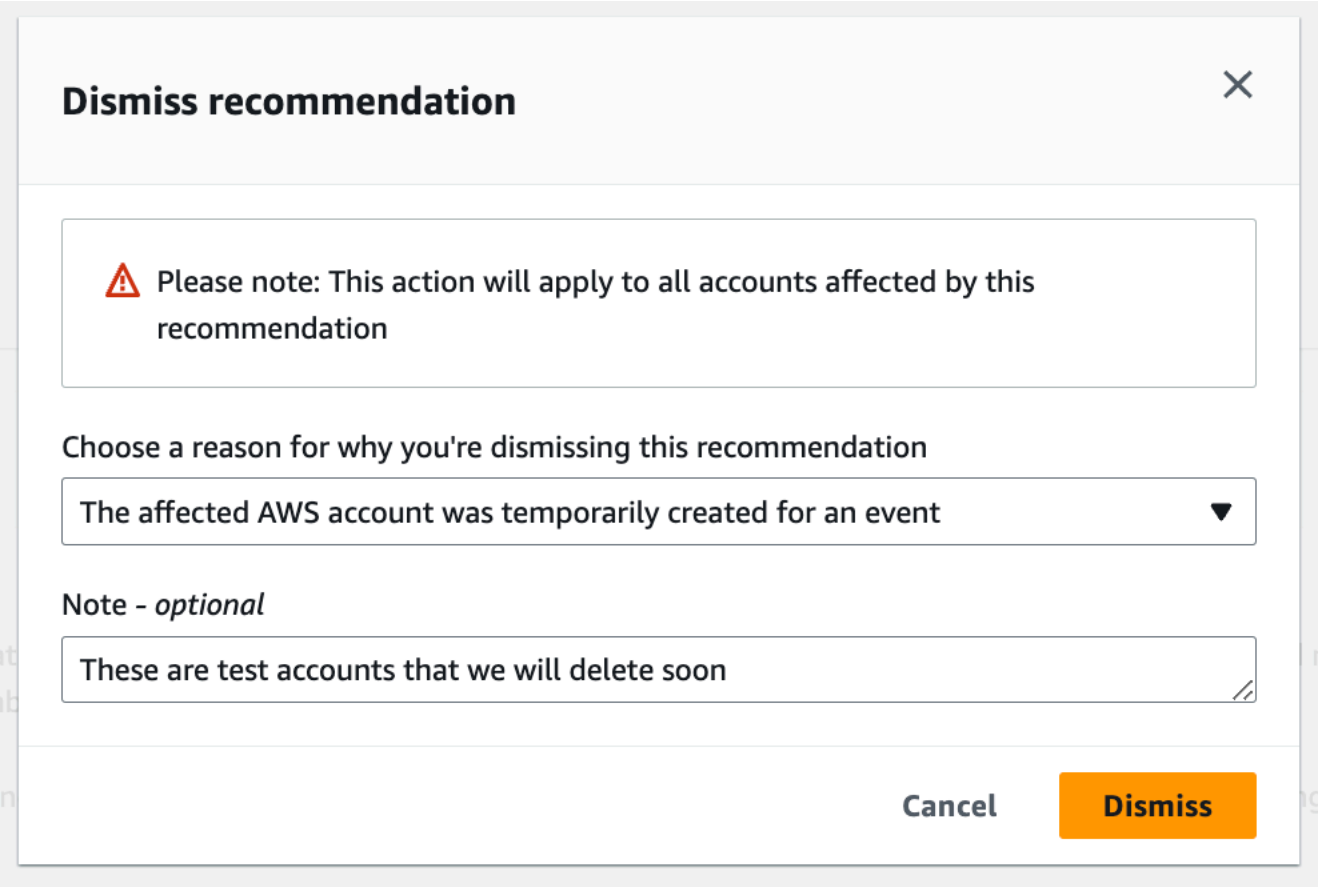
1. Inicie sesión en la consola de Trusted Advisor en https://console.aws.amazon.com/trustedadvisor/home.
2. En la página de Trusted Advisor Priority, asegúrese de estar en la pestaña Mi organización.
3. En la pestaña Activas, seleccione el nombre de una recomendación.
4. Si esta recomendación no es relevante para su cuenta, seleccione Descartar.
5. En el cuadro de diálogo Descartar recomendación), seleccione el motivo por el que no va a atender la recomendación.
6. (Opcional) Ingrese una nota que detalle el motivo por el que descarta la recomendación. Si elige Otros, debe ingresar una descripción en la sección Nota.
7. Seleccione Descartar. El estado de la recomendación cambia a Descartada. La recomendación aparece en la pestaña Cerradas de la página de Trusted Advisor Priority.

> **Note**
>
> Puede seleccionar el nombre de la recomendación y luego Ver nota para consultar el motivo por el que se descartó. Si fue el equipo de cuentas el que se encargó de descartar la recomendación, su dirección de correo electrónico aparecerá junto a la nota.

Trusted Advisor Priority también notifica al equipo de cuentas que se ha descartado la recomendación.

Example : Descartar una recomendación en Trusted Advisor Priority

El siguiente ejemplo muestra cómo se puede descartar una recomendación.



Resolver una recomendación

Después de confirmar la recomendación y realizar las acciones recomendadas, puede resolver la recomendación.

> **Tip**
>
> Una vez que se ha resuelto una recomendación, no se puede reabrirla. Si desea volver a revisar la recomendación más adelante, consulte Descartar una recomendación.

Para resolver una recomendación

1. Inicie sesión en la consola de Trusted Advisor en https://console.aws.amazon.com/trustedadvisor/home.
2. En la página de Trusted Advisor Priority, asegúrese de estar en la pestaña Mi organización.
3. En la página Trusted Advisor Priority, seleccione la recomendación y, a continuación, elija Resolve (Resolver).

4. En el cuadro de diálogo Resolver recomendación, seleccione Resolver. Las recomendaciones resueltas aparecen en la pestaña Closed (Cerrado) de la página de Trusted Advisor Priority. Trusted Advisor Priority notifica al equipo de cuentas que resolvió la recomendación.

Para resolver una recomendación para todas las cuentas de su organización de AWS

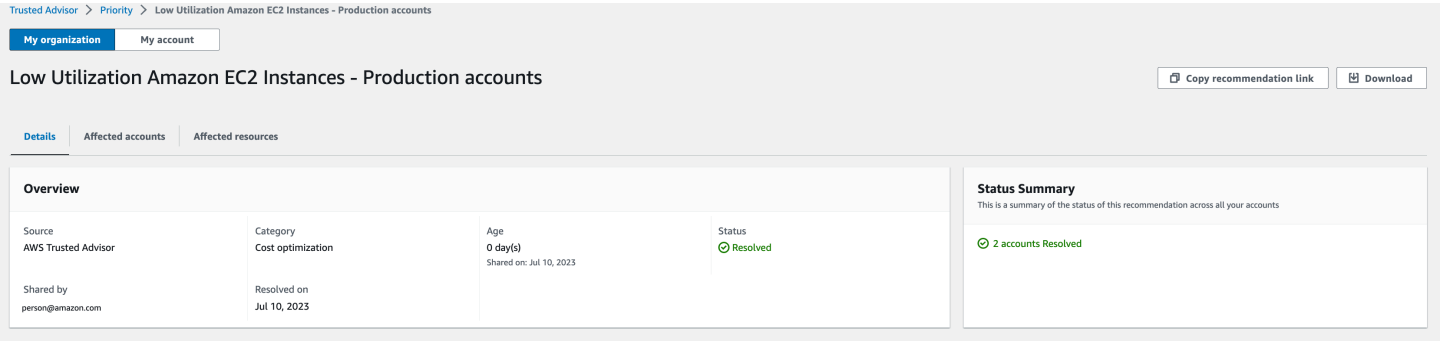
La cuenta de administración o los administradores delegados de Trusted Advisor Priority pueden resolver una recomendación para todas las cuentas.

> **Note**
>
> Las cuentas de miembros no tienen acceso a las recomendaciones agregadas.

1. Inicie sesión en la consola de Trusted Advisor en https://console.aws.amazon.com/trustedadvisor/home.
2. Si utiliza una cuenta de administración o de administrador delegado de AWS Organizations, cambie a la pestaña Mi cuenta.
3. En la pestaña Activas, seleccione el nombre de una recomendación.
4. Si la recomendación no es relevante para su cuenta, elija Resolver.
5. En el cuadro de diálogo Resolver recomendación, seleccione Resolver. Las recomendaciones resueltas aparecen en la pestaña Closed (Cerrado) de la página de Trusted Advisor Priority. Trusted Advisor Priority notifica al equipo de cuentas que resolvió la recomendación.

Example : Recomendación manual de Trusted Advisor Priority

En el siguiente ejemplo se muestra una recomendación de Instancias de Amazon EC2 de bajo uso resuelta.



Reapertura de una recomendación

Después de descartar una recomendación, usted o el equipo de cuentas pueden reabrirla.

Para reabrir una recomendación

1. Inicie sesión en la consola de Trusted Advisor en https://console.aws.amazon.com/trustedadvisor/home.
2. Si utiliza una cuenta de administración o de administrador delegado de AWS Organizations, cambie a la pestaña Mi cuenta.
3. En la página Trusted Advisor Priority, elija la pestaña Closed (Cerrado).
4. En Recomendaciones cerradas, seleccione la recomendación Descartada, y luego Reabrir.
5. En el cuadro de diálogo Reabrir recomendación, describa por qué va a reabrir la recomendación.
6. Elija Reopen (Reabrir). El estado de la recomendación cambia a In progress (En curso) y aparece en la pestaña Active (Activo).

   > **Tip**
   >
   > Puede elegir el nombre de la recomendación y luego, Ver nota para conocer el motivo de la reapertura. Si fue el equipo de cuentas el que se encargó de reabrir la recomendación, su nombre aparecerá junto a la nota.

7. Siga los pasos que se indican en los detalles de la recomendación.

Para volver a abrir una recomendación para todas las cuentas de su organización de AWS

La cuenta de administración o los administradores delegados de Trusted Advisor Priority pueden volver a abrir una recomendación para todas las cuentas.

> **Note**
>
> Las cuentas de miembros no tienen acceso a las recomendaciones agregadas.

1. Inicie sesión en la consola de Trusted Advisor en https://console.aws.amazon.com/trustedadvisor/home.
2. En la página de Trusted Advisor Priority, asegúrese de estar en la pestaña Mi organización.

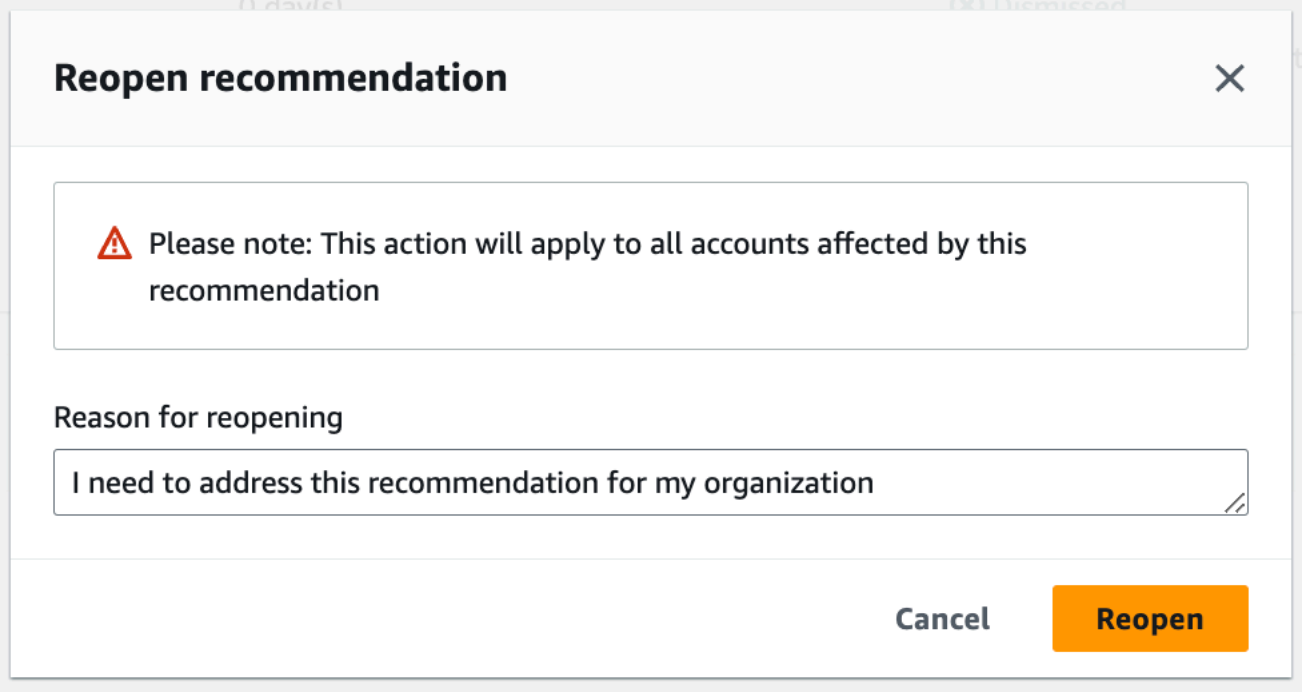
3. En Recomendaciones cerradas, seleccione la recomendación Descartada, y luego Reabrir.
4. En el cuadro de diálogo Reabrir recomendación, describa por qué va a reabrir la recomendación.
5. Elija Reopen (Reabrir). El estado de la recomendación cambia a In progress (En curso) y aparece en la pestaña Active (Activo).

> **Tip**
>
> Puede seleccionar el nombre de la recomendación y luego Ver nota para consultar el motivo de la reapertura. Si fue el equipo de cuentas el que se encargó de reabrir la recomendación, su nombre aparecerá junto a la nota.

6. Siga los pasos que se indican en los detalles de la recomendación.

Example : reapertura de una recomendación de Trusted Advisor Priority

En el siguiente ejemplo, se muestra una recomendación que quiere volver a abrir.



Descargar detalles de las recomendaciones

También puede descargar los resultados de una recomendación por prioridad desde Trusted Advisor Priority.

> **Note**
>
> Actualmente, solo puede descargar una recomendación a la vez.

Para descargar una recomendación

1. Inicie sesión en la consola de Trusted Advisor en https://console.aws.amazon.com/trustedadvisor/home.
2. En la página Trusted Advisor Priority, seleccione la recomendación y, a continuación, elija Download (Descargar).
3. Abra el archivo para ver los detalles de la recomendación.

Registro de administradores delegados

Puede agregar cuentas de miembros que pertenecen a su organización como administradores delegados. Las cuentas de administradores delegados pueden revisar, confirmar, resolver, descartar y reabrir recomendaciones en Trusted Advisor Priority.

Después de registrar una cuenta, debe conceder al administrador delegado los permisos de AWS Identity and Access Management necesarios para acceder a Trusted Advisor Priority. Para obtener más información, consulte Gestione el acceso a AWS Trusted Advisor y AWS políticas gestionadas para AWS Trusted Advisor.

Puede registrar hasta cinco cuentas de miembros. Solo la cuenta de administración puede agregar administradores delegados para la organización. Para registrar o anular el registro de un administrador delegado, debe iniciar sesión en la cuenta de administración de la organización.

Para registrar un administrador delegado

1. Inicie sesión en la consola de Trusted Advisor en https://console.aws.amazon.com/trustedadvisor/home con la cuenta de administración.
2. En el panel de navegación, en Preferences (Preferencias), elija Your organization (Su organización).
3. En Delegated administrator (Administrador delegado), elija Register new account (Registrar una cuenta nueva).

4. En el cuadro de diálogo, ingrese el ID de cuenta del miembro y, a continuación, elija Register (Registrar).
5. (Opcional) Para anular el registro de una cuenta, seleccione una cuenta y elija Deregister (Anular registro). En el cuadro de diálogo, vuelva a elegir Deregister (Anular registro).

Anulación del registro de administradores delegados

Al anular el registro de una cuenta de miembro, esa cuenta ya no tendrá el mismo acceso a Trusted Advisor Priority que la cuenta de administración. Las cuentas que ya no son administradores delegados no recibirán notificaciones de Trusted Advisor Priority por correo electrónico.

Para anular el registro de un administrador delegado

1. Inicie sesión en la consola de Trusted Advisor en https://console.aws.amazon.com/trustedadvisor/home con la cuenta de administración.
2. En el panel de navegación, en Preferences (Preferencias), elija Your organization (Su organización).
3. En Administrador delegado, seleccione una cuenta y luego, elija Anular registro.
4. En el cuadro de diálogo, elija Deregister (Anular registro).

Administración de notificaciones de Trusted Advisor Priority

Trusted Advisor Priority envía notificaciones por correo electrónico. Este tipo de notificación incluye un resumen de las recomendaciones que el equipo de cuentas priorizó. Puede especificar la frecuencia de recepción de las actualizaciones de Trusted Advisor Priority.

Si registró las cuentas de miembros como administradores delegados, también pueden configurar sus cuentas para recibir notificaciones de Trusted Advisor Priority por correo electrónico.

Las notificaciones de Trusted Advisor Priority por correo electrónico no incluyen los resultados de las comprobaciones de cuentas individuales y son independientes de las notificaciones semanales del panel Trusted Advisor Recommendations. Para más información, consulte Configurar las preferencias de notificación.

> **Note**
>
> Solo la cuenta de administración o el administrador delegado pueden configurar las notificaciones por correo electrónico de Trusted Advisor Priority.

Para administrar sus notificaciones de Trusted Advisor Priority

1. Inicie sesión en la consola de Trusted Advisor en https://console.aws.amazon.com/trustedadvisor/home con una cuenta de administración o de administrador delegado.
2. En el panel de navegación, en Preferences (Preferencias), elija Notifications (Notificaciones).
3. En Priority, puede seleccionar las siguientes opciones.
   a. Daily (Diariamente): reciba una notificación por correo electrónico todos los días.
   b. Weekly (Semanalmente): reciba una notificación por correo electrónico una vez a la semana.
   c. Elija las notificaciones que quiere recibir:
      - Resumen de recomendaciones priorizadas
      - Fechas de resolución
4. En Destinatarios, seleccione otros contactos que desee que reciban las notificaciones por correo electrónico. Puede agregar y eliminar contactos de la página Account Settings (Configuración de cuenta) en la AWS Billing and Cost Management consola.
5. En Language (Idioma), elija el idioma de la notificación por correo electrónico.
6. Elija Save your preferences (Guardar preferencias).

> **Note**
>
> Trusted Advisor Priority envía notificaciones por correo electrónico desde la dirección noreply@notifications.trustedadvisor.us-west-2.amazonaws.com. Es posible que tenga que comprobar que su cliente de correo electrónico no identifique estos correos electrónicos como spam.

Deshabilitar Trusted Advisor Priority

Contacte con su equipo de cuentas y solicite que deshabilite esta característica. Una vez deshabilitada esta característica, las recomendaciones priorizadas dejarán de aparecer en la consola de Trusted Advisor.

Si deshabilita Trusted Advisor Priority y, a continuación, vuelve a habilitarlo más tarde, aún podrá ver las recomendaciones que envió el equipo de cuentas antes de que deshabilitara Trusted Advisor Priority.

Primeros pasos con AWS Trusted Advisor Engage (vista previa)

> **Note**
>
> AWS Trusted Advisor Engage está en versión de vista previa y sujeto a cambios. Puede ver una vista previa de las condiciones del servicio aquí https://aws.amazon.com/service-terms/.

Puede usar AWS Trusted Advisor Engage para aprovechar al máximo sus planes de AWS Support, ya que permiten que vea, solicite y haga un seguimiento de todas sus interacciones proactivas y se comunique con el equipo de su Cuenta de AWS sobre las interacciones en curso.

Por ejemplo, puede solicitar una “revisión empresarial de administración” para el equipo de su Cuenta de AWS desde la página de Engage de la consola de AWS Trusted Advisor. A continuación, se asignará un experto de AWS a su solicitud y se encargará de hacer un seguimiento de todo el proceso de interacción.

Temas

- Buscar interacciones

Requisitos previos

Debe tomar las medidas necesarias para cumplir los siguientes requisitos para poder utilizar Trusted Advisor Engage:

- Debe tener un plan Enterprise On-Ramp Support.
- Su cuenta debe formar parte de una organización que tenga habilitadas todas las características de AWS Organizations. Para obtener más información, consulte Habilitar todas las características en la organización en la Guía del usuario de AWS Organizations.
- Su organización debe tener habilitado el acceso de confianza a Trusted Advisor. Para habilitar el acceso de confianza, inicie sesión con la cuenta de administración y vaya a la página Su organización en la consola de Trusted Advisor.
- Debe tener permisos de AWS Identity and Access Management (IAM) para acceder a Trusted Advisor Engage. Para obtener más información sobre el control de acceso a Trusted Advisor Engage, consulte Gestione el acceso a AWS Trusted Advisor.

> **Note**
>
> Se puede crear una solicitud de interacción con cualquier cuenta de una organización de AWS. Si una cuenta propietaria de una interacción se traslada a otra organización de AWS, solo la cuenta podrá acceder a la interacción. Para limitar los controles, consulte Ejemplo de políticas de control de servicios para AWS Trusted Advisor.

Consultar el panel de interacciones

Una vez que haya obtenido los derechos de acceso, podrá acceder a la página de Trusted Advisor Engage de la consola de Trusted Advisor para ver un panel en el que podrá administrar las interacciones con el equipo de su Cuenta de AWS.

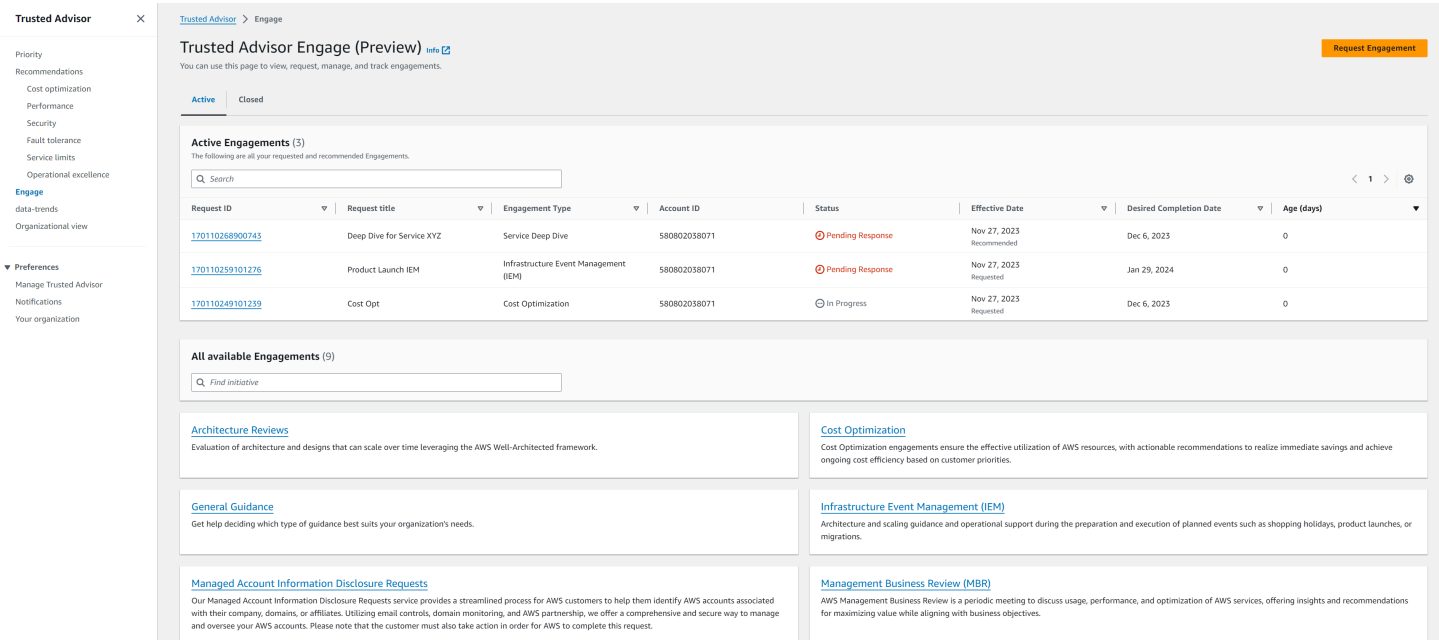
Para administrar sus interacciones:

1. Inicie sesión en la consola de Trusted Advisor en https://console.aws.amazon.com/trustedadvisor/home.

2. En la página de Trusted Advisor Engage, puede ver:

   - El botón Solicitud de interacción
   - La tabla Interacciones activas
   - La tabla Interacciones cerradas
   - El catálogo Todas las interacciones disponibles

Example : Panel de interacciones



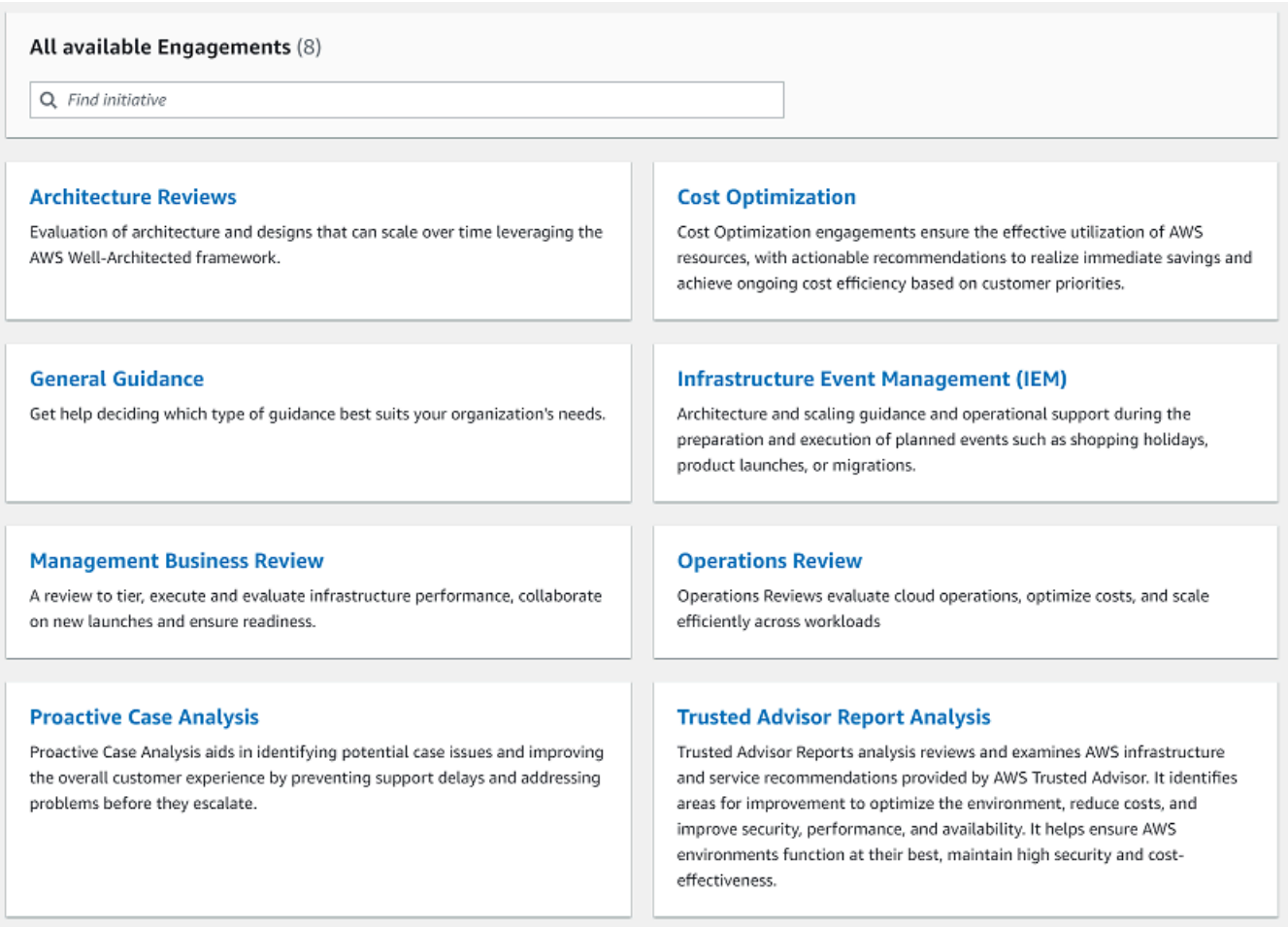
Consultar el catálogo de tipos de interacción

Puede consultar el catálogo de tipos de interacción para encontrar los últimos tipos de interacciones que puede solicitar al equipo de su Cuenta de AWS.

Consultar el catálogo de tipos de interacción:

1. Inicie sesión en la consola de Trusted Advisor en https://console.aws.amazon.com/trustedadvisor/home.
2. En la página de Trusted Advisor Engage, encontrará el catálogo de tipos de interacción.

Example : Catálogo de tipos de interacción



Solicitar una interacción

Puede solicitar interacciones al equipo de su Cuenta de AWS de acuerdo con los tipos de interacción incluidos en su plan de AWS Support.

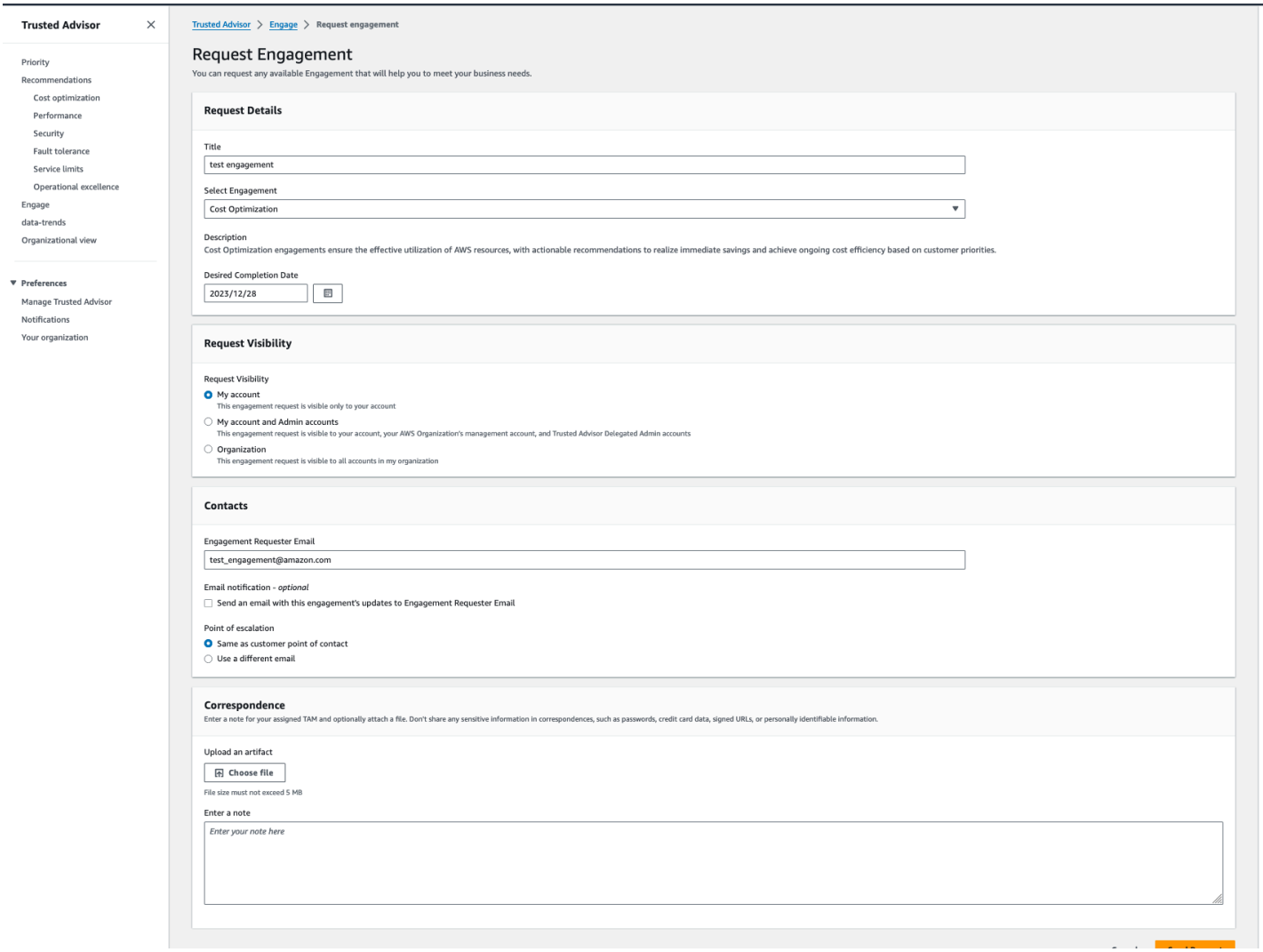
Para solicitar una interacción, haga lo siguiente:

1. Inicie sesión en la consola de Trusted Advisor en https://console.aws.amazon.com/trustedadvisor/home.
2. En la página de Trusted Advisor Engage, seleccione Solicitar interacción.
3. Rellene lo siguiente:
   - Title (Título)
   - Seleccionar interacción: el tipo de interacción que desea solicitar.

- Fecha de finalización deseada: la fecha de finalización deseada de la interacción. Cada tipo de interacción tiene un plazo de entrega diferente que se calcula en la fecha de finalización mínima deseada.
- Visibilidad de la solicitud:
  - Mi cuenta: esta solicitud de interacción solo es visible en su cuenta.
  - Mi cuenta y las cuentas de administrador: esta solicitud de interacción está visible en su cuenta, en la cuenta de administración y en las cuentas de todos los administradores delegados de su organización de AWS.
  - Organización: esta solicitud de participación está visible para todas las cuentas de su organización de AWS.
- Correo electrónico del solicitante de la participación: la dirección de correo electrónico que AWS se utilizará como punto de contacto principal para esta participación.
- Configuración de notificaciones por correo electrónico: elija si el correo electrónico del solicitante de la participación recibirá notificaciones por correo electrónico sobre la participación.
- Punto de escalamiento: la dirección de correo electrónico que AWS utilizará cuando se requiera un escalamiento para esta interacción.
- Correspondencia: una nota y un archivo adjunto opcional para que pueda proporcionar detalles de esta interacción.

4. Seleccionar Enviar solicitud.

Example : Solicitar una interacción



Editar una interacción

Puede editar los detalles de su solicitud de interacción.

Para editar una interacción, haga lo siguiente:

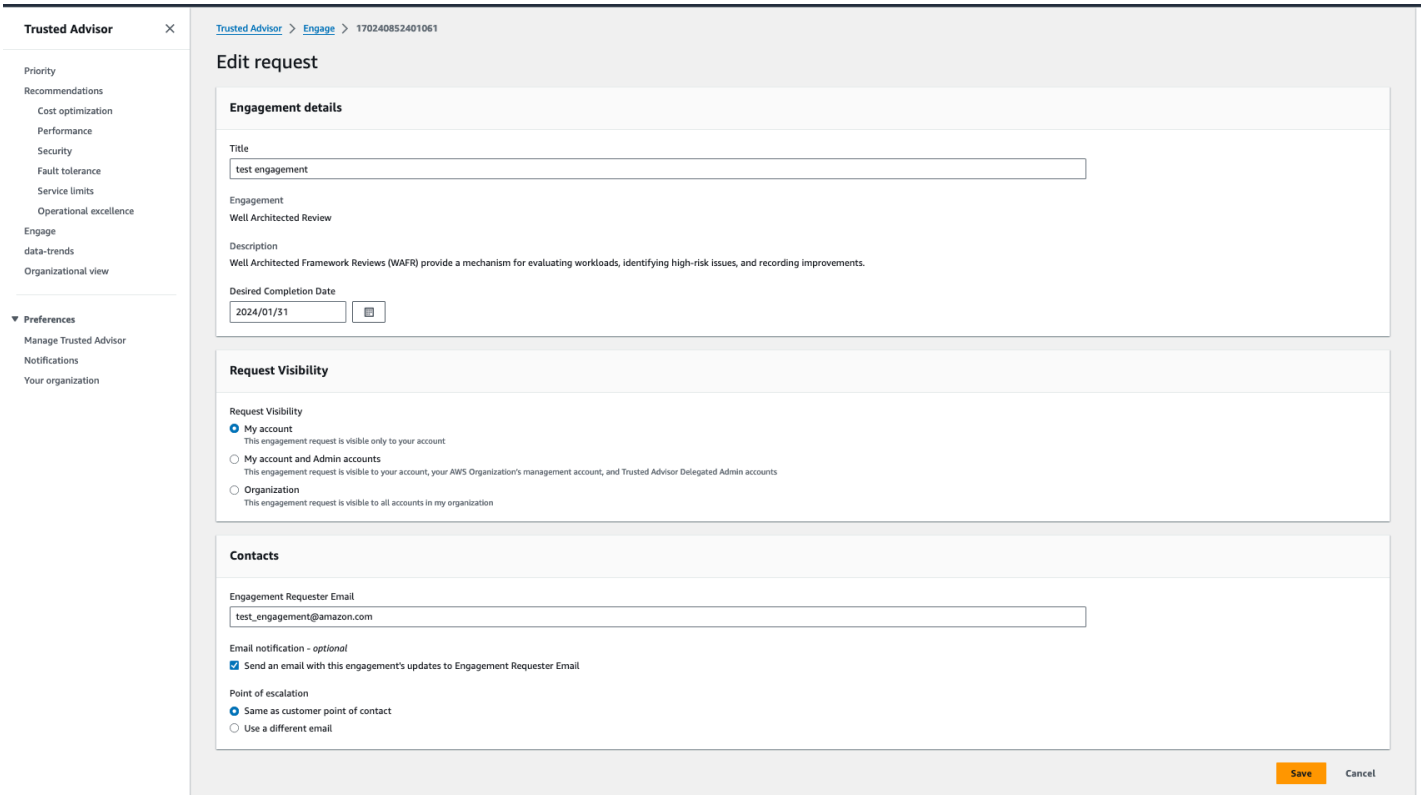
1. Inicie sesión en la consola de Trusted Advisor en https://console.aws.amazon.com/trustedadvisor/home.
2. En la página de Trusted Advisor Engage, seleccione una interacción existente.
3. Seleccione Editar.
4. Puede editar lo siguiente:

   - Title (Título)

- Fecha de finalización deseada: la fecha de finalización deseada de la interacción. Cada tipo de interacción tiene un plazo de entrega diferente que se calcula en la fecha de finalización mínima deseada.
- Visibilidad de la solicitud:
  - Mi cuenta: esta solicitud de interacción solo es visible en su cuenta.
  - Mi cuenta y las cuentas de administrador: esta solicitud de interacción está visible en su cuenta, en la cuenta de administración y en las cuentas de todos los administradores delegados de su organización de AWS.
  - Organización: esta solicitud de participación está visible para todas las cuentas de su organización de AWS.
- Correo electrónico del solicitante de la participación: la dirección de correo electrónico que AWS se utilizará como punto de contacto principal para esta participación.
- Configuración de notificaciones por correo electrónico: elija si el correo electrónico del solicitante de la participación recibirá notificaciones por correo electrónico sobre la participación.
- Punto de escalamiento: la dirección de correo electrónico que AWS utilizará cuando se requiera el escalamiento para esta interacción.

5. Elija Guardar.

Example : Editar la interacción



Enviar archivos adjuntos y notas

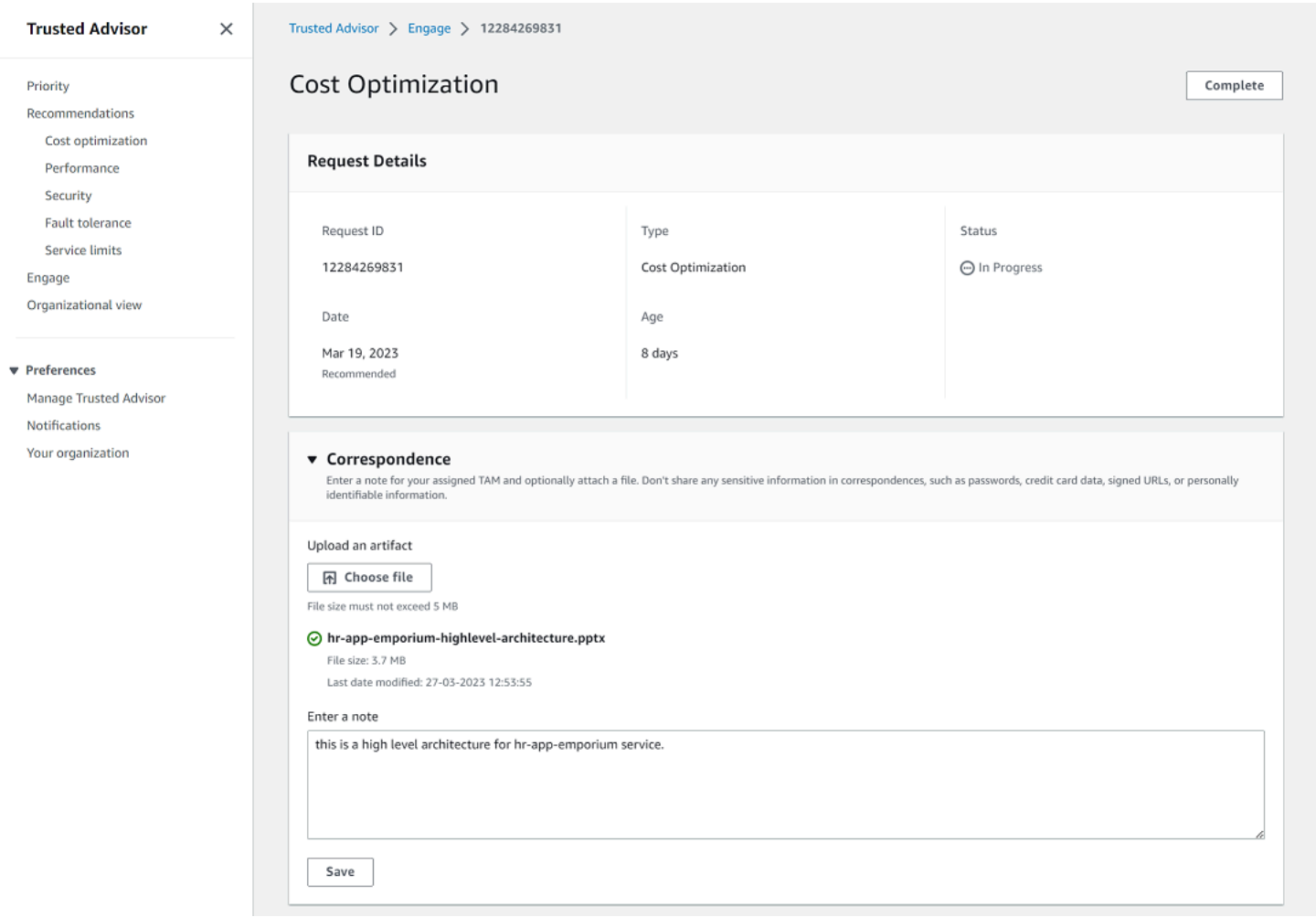
Puede comunicarse con el equipo de su Cuenta de AWS en relación con las interacciones individuales enviando notas y archivos adjuntos para respaldar su solicitud de interacción. Puede incluir un único archivo adjunto y una nota por comunicación, solo puede adjuntar archivos a una interacción con la misma Cuenta de AWS que haya solicitado la interacción y no puede eliminar los archivos adjuntos ni las notas después de enviar una comunicación.

Para adjuntar archivos o agregar notas a una solicitud de interacción activa, haga lo siguiente:

1. Inicie sesión en la consola de Trusted Advisor en https://console.aws.amazon.com/trustedadvisor/home.
2. En la página de Trusted Advisor Engage, elija el ID de la interacción activa a la que quiere adjuntar archivos o agregar notas.
3. Elija Correspondencia para expandir el formulario.
4. Introduzca una nota para el TAM asignado y, si lo desea, adjunte un archivo. No comparta información confidencial, como contraseñas, datos de tarjetas de crédito, URL firmadas o información de identificación personal en las correspondencias.

5. Elija Guardar.

Example : Agregue una nota y adjunte el archivo a una interacción



Modificación del estado de la interacción

Puede modificar el estado de las interacciones para cancelar las interacciones que están pendientes de respuesta, completar las interacciones que están en curso y volver a abrir las interacciones que se marcaron como canceladas o cerradas.

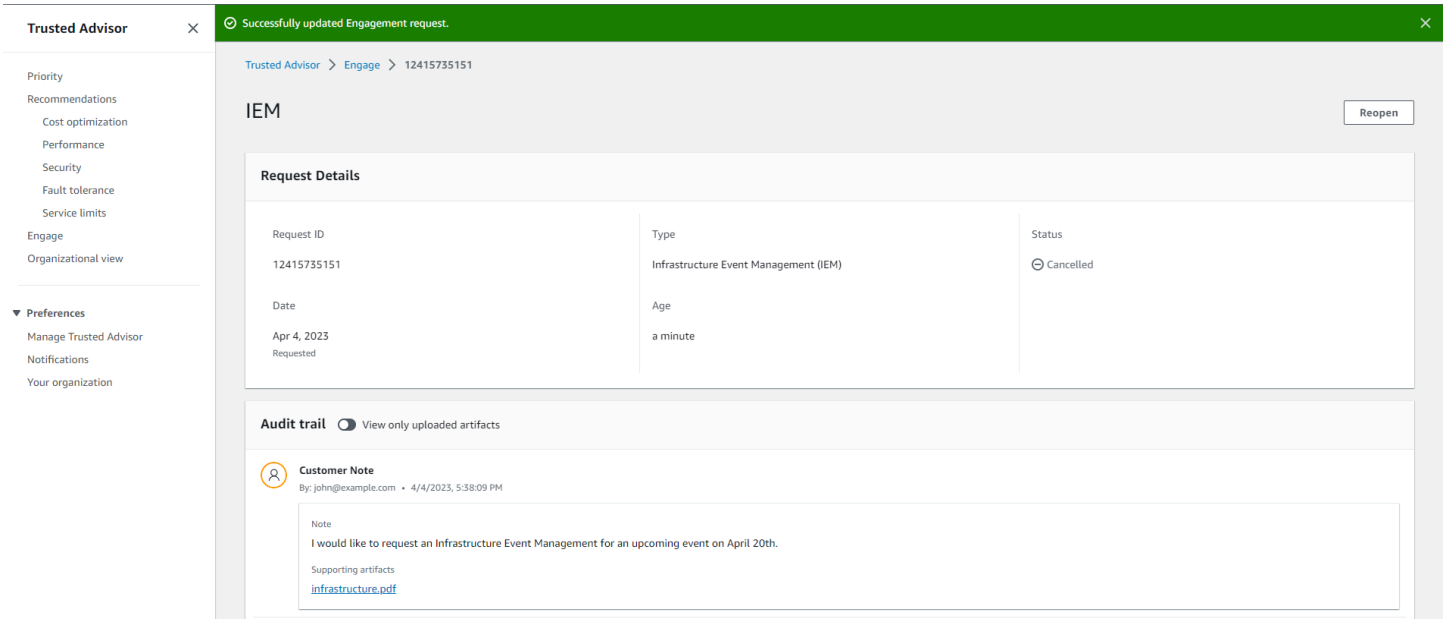
Para modificar el estado de una interacción, haga lo siguiente:

1. Inicie sesión en la consola de Trusted Advisor en https://console.aws.amazon.com/trustedadvisor/home.
2. En la página Trusted Advisor Engage, elija el ID de la interacción activa cuyo estado quisiera cambiar.

3. En la página de los detalles de la interacción, puede cambiar el estado a Cancelada o Completada.

   - Puede seleccionar Cancelar si el estado de la interacción es Pendiente de respuesta.
   - Puede seleccionar Completado cuando el estado de interacción es En curso.
   - Puede seleccionar Reabrir para las interacciones cerradas. Las interacciones canceladas pasan a Pendiente de respuesta, mientras que las interacciones completas pasan a En curso.

Example : Cambiar el estado de la interacción



Diferencie entre interacciones recomendadas y solicitadas

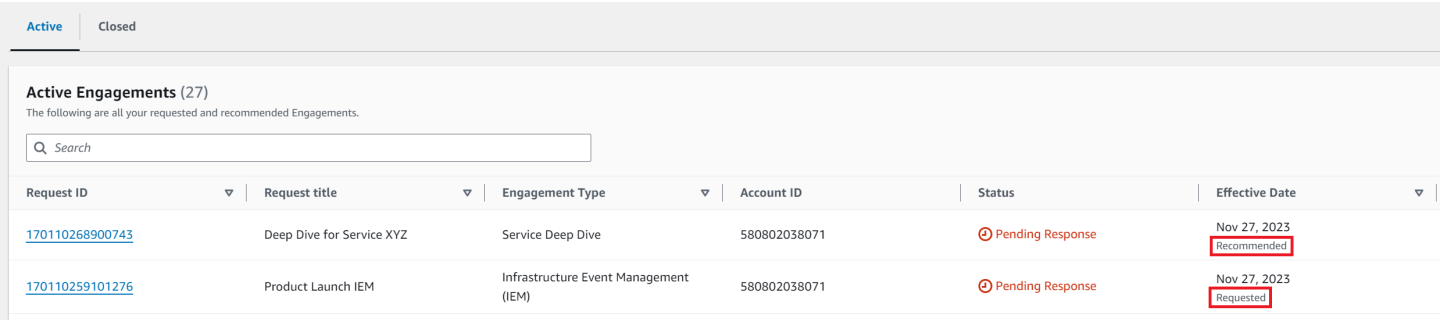
Puede identificar el origen de las interacciones para saber si usted las solicitó o si el equipo de su Cuenta de AWS las recomendó.

Para ver los diferentes orígenes de las Interacciones activas, haga lo siguiente:

1. Inicie sesión en la consola de Trusted Advisor en https://console.aws.amazon.com/trustedadvisor/home.
2. En la página Trusted AdvisorEngage, consulta la columna Fecha de entrada en vigor para distinguir entre las interacciones recomendadas y las solicitadas:

   - Recomendadas: solicitudes de interacción creadas por los equipos de su Cuenta de AWS.
   - Solicitadas: solicitudes de interacción creadas por el usuario.

Example : Distinga entre las interacciones recomendadas y las solicitadas



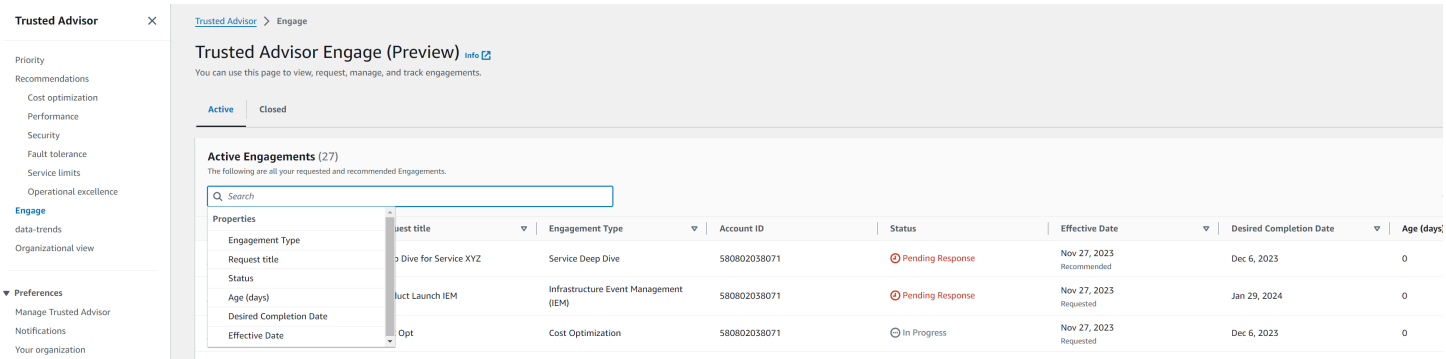
Buscar interacciones

Puede buscar sus interacciones activas y cerradas existentes mediante filtros.

Para buscar interacciones, haga lo siguiente:

1. Inicie sesión en la consola de Trusted Advisor en https://console.aws.amazon.com/trustedadvisor/home.
2. En la página de Trusted Advisor Engage, puede seleccionar uno de los siguientes filtros:
   - Edad (días)
   - Tipo de interacción
   - Título de la solicitud
   - Status
   - Fecha de finalización deseada
   - Fecha de entrada en vigor

Example : Buscar interacciones



AWS Trusted Advisor comprobar referencia

Puede ver todos los nombres, descripciones e ID de los Trusted Advisor cheques en la siguiente referencia. También puede iniciar sesión en la consola de Trusted Advisor para ver más información sobre las verificaciones, las acciones recomendadas y sus estados.

Si tiene un plan de soporte Business, Enterprise On-Ramp o Enterprise, también puede utilizar la API de AWS Trusted Advisor y la AWS Command Line Interface (AWS CLI) para obtener acceso a las verificaciones. Para obtener más información, consulte los temas siguientes:

- Comience a utilizar la Trusted Advisor API
- AWS Trusted Advisor Referencia de la API

> **Note**
>
> Si dispone de un plan de soporte Basic y Developer, puede utilizar la consola de Trusted Advisor para obtener acceso a todas las verificaciones de la categoría Límites de los servicios y a las verificaciones siguientes de la categoría de seguridad:
>
> - Instantáneas públicas de Amazon EBS
> - Instantáneas públicas de Amazon RDS
> - Permisos de bucket de Amazon S3
> - MFA en la cuenta raíz
> - Grupos de seguridad: puertos específicos sin restricciones

Categorías de verificación

- Optimización de costos
- Rendimiento
- Seguridad
- Tolerancia a errores
- Límites de los servicios
- Excelencia operativa

Optimización de costos

Puede utilizar las siguientes verificaciones para la categoría de optimización de costos.

Nombres de la verificación

- La cuenta de AWS no forma parte de AWS Organizations
- Puntos de enlace infrautilizados de Amazon Comprehend
- Volúmenes con exceso de aprovisionamiento de Amazon EBS
- Consolidación de las instancias de Amazon EC2 para Microsoft SQL Server
- Instancias de Amazon EC2 con exceso de aprovisionamiento para Microsoft SQL Server
- Instancias de Amazon EC2 detenidas
- Amazon EC2 Reserved Instance Lease Expiration
- Optimización de instancias reservadas de Amazon EC2
- Repositorio de Amazon ECR sin política de ciclo de vida configurada
- Optimización de nodos ElastiCache reservados de Amazon
- Optimización de instancias reservadas de Amazon OpenSearch Service
- Amazon RDS Idle DB Instances
- Optimización del nodo reservado de Amazon Redshift
- Optimización de instancias reservadas de Amazon Relational Database Service (RDS)
- Conjuntos de registros de recursos de latencia en Amazon Route 53
- Política de ciclo de vida del bucket de Amazon S3 configurada
- Configuración incompleta de cancelación de carga multiparte de Amazon S3
- Buckets habilitados para versiones de Amazon S3 sin políticas de ciclo de vida configuradas
- Funciones de AWS Lambda con tiempos de espera excesivos
- Funciones de AWS Lambda con elevadas tasas de error
- Funciones AWS Lambda con exceso de aprovisionamiento para el tamaño de la memoria
- Problemas de alto riesgo de AWS Well-Architected para la optimización de costos
- Balanceadores de carga inactivos
- Utilización baja de instancias de Amazon EC2
- Savings Plan
- Direcciones IP elásticas no asociadas

- Volúmenes de Amazon EBS infrautilizados
- Underutilized Amazon Redshift Clusters

La cuenta de AWS no forma parte de AWS Organizations

Descripción

Comprueba si una cuenta de AWS forma parte de AWS Organizations en la cuenta de administración correspondiente.

AWS Organizations es un servicio de administración de cuentas que tiene como objetivo consolidar varias cuentas de AWS en una organización administrada de forma centralizada. Esto permite estructurar cuentas de forma centralizada para consolidar la facturación e implementar políticas de propiedad y seguridad a medida que las cargas de trabajo escalan en AWS.

Puede especificar el identificador de la cuenta de administración mediante el MasterAccountIdparámetro de las AWS Config reglas.

Para obtener más información, consulte ¿Qué es AWS Organizations?

> **Note**
>
> Los resultados de esta verificación se actualizan automáticamente varias veces al día y no se permiten las solicitudes de actualización. Puede que los cambios tarden unas horas en aparecer. Actualmente, no puede excluir recursos de esta verificación.

ID de la verificación

`c18d2gz127`

Fuente

`AWS Config Managed Rule: account-part-of-organizations`

Criterios de alerta

Amarillo: esta cuenta de AWS no forma parte de AWS Organizations.

Acción recomendada

Agregue esta cuenta de AWS como parte de AWS Organizations.

Para obtener más información, consulte Tutorial: Creación y configuración de una organización.

Columnas de informes

- Status
- Región
- Resource
- Regla de AWS Config
- Parámetros de entrada
- Hora de la última actualización

Puntos de enlace infrautilizados de Amazon Comprehend

Descripción

Verifica la configuración de rendimiento de los puntos de enlace. Esta verificación le avisa cuando los puntos de enlace no se utilizan activamente para solicitudes de inferencia en tiempo real. Un punto de enlace que no se utiliza durante más de 15 días consecutivos se considera infrautilizada. Todos los puntos de enlace acumulan cargos en función del conjunto de rendimiento y del tiempo durante el cual el punto de enlace está activo.

> **Note**
>
> Esta verificación se actualiza automáticamente una vez al día. Actualmente, no puede excluir recursos de esta verificación.

ID de la verificación

`Cm24dfsM12`

Criterios de alerta

Amarillo: el punto de conexión está activo, pero no se ha utilizado para solicitudes de inferencia en tiempo real en los últimos 15 días.

Acción recomendada

Si el punto de conexión no se ha utilizado en los últimos 15 días, le recomendamos que defina una política de escalado para el recurso mediante Auto Scaling de aplicaciones.

Si el punto de conexión tiene una política de escalado definida y no se ha utilizado en los últimos 30 días, considere eliminar el punto de conexión y utilizar la inferencia asíncrona. Para obtener más información, consulte Deleting an endpoint with Amazon Comprehend (Eliminación de un punto de conexión con Amazon Comprehend).

Columnas de informes

- Status
- Región
- ARN de punto de conexión
- Unidad de inferencia aprovisionada
- AutoScaling Estado
- Motivo
- Hora de la última actualización

Volúmenes con exceso de aprovisionamiento de Amazon EBS

Descripción

Compruebe los volúmenes de Amazon Elastic Block Store (Amazon EBS) que se estaban ejecutando en cualquier momento durante el período de revisión. Esta comprobación le avisa si hay exceso de aprovisionamiento de volúmenes de EBS para sus cargas de trabajo. Cuando tiene volúmenes con exceso de aprovisionamiento, paga los recursos no utilizados. Aunque algunos escenarios pueden dar lugar a una baja optimización por diseño, a menudo se pueden reducir los costos si se cambia la configuración de los volúmenes de EBS. Los ahorros mensuales estimados se calculan con la tasa de uso actual para volúmenes de EBS. Los ahorros reales variarán si el volumen no está presente durante un mes completo.

> **Note**
>
> Los resultados de esta verificación se actualizan automáticamente varias veces al día y no se permiten las solicitudes de actualización. Puede que los cambios tarden unas horas en aparecer. Actualmente, no puede excluir recursos de esta verificación.

ID de la verificación

`COr6dfpM03`

Criterios de alerta

Amarillo: un volumen de EBS que se aprovisionó en exceso durante el periodo retroactivo. Para determinar si un volumen está sobreaprovisionado, tenemos en cuenta todas las CloudWatch métricas predeterminadas (incluidas las IOPS y el rendimiento). El algoritmo utilizado para identificar los volúmenes de EBS sobreaprovisionados sigue las prácticas recomendadas de AWS. El algoritmo se actualiza cuando se identifica un nuevo patrón.

Acción recomendada

Considere reducir el tamaño de los volúmenes que tienen baja utilización.

Para obtener más información, consulte Optar AWS Compute Optimizer por recibir Trusted Advisor cheques.

Columnas de informes

- Status
- Región
- ID de volumen
- Tipo de volumen
- Tamaño del volumen (GB)
- IOPS de referencia de volumen
- IOPS por ráfagas de volumen
- Rendimiento por ráfagas de volumen
- Tipo de volumen recomendado
- Tamaño de volumen recomendado (GB)
- IOPS de referencia de volumen recomendado
- IOPS por ráfagas de volumen recomendado
- Rendimiento de referencia de volumen recomendado
- Rendimiento por ráfagas de volumen recomendado
- Periodo retroactivo (días)
- Oportunidad de ahorro (%)
- Ahorros mensuales estimados
- Divisa de ahorros mensuales estimados

- Hora de la última actualización

Consolidación de las instancias de Amazon EC2 para Microsoft SQL Server

Descripción

Verifica las instancias de Amazon Elastic Compute Cloud (Amazon EC2) en las que se ha ejecutado SQL Server en las últimas 24 horas. Esta verificación le avisa si la instancia tiene menos de la cantidad mínima de licencias de SQL Server. Según la Guía de licencias de Microsoft SQL Server, paga 4 licencias de vCPU incluso si una instancia tiene solo 1 o 2 vCPU. Puede consolidar instancias de SQL Server más pequeñas para ayudar a reducir los costos.

> **Note**
>
> Los resultados de esta verificación se actualizan automáticamente varias veces al día y no se permiten las solicitudes de actualización. Puede que los cambios tarden unas horas en aparecer. Actualmente, no puede excluir recursos de esta verificación.

ID de la verificación

`Qsdfp3A4L2`

Criterios de alerta

Amarillo: una instancia con SQL Server tiene menos de 4 vCPU.

Acción recomendada

Considere consolidar cargas de trabajo de SQL Server más pequeñas en instancias con al menos 4 vCPU.

Recursos adicionales

- Microsoft SQL Server en AWS
- Licencias de Microsoft en AWS
- Guía de licencias de Microsoft SQL Server

Columnas de informes

- Status
- Región

- ID de instancia
- Tipo de instancia
- vCPU
- vCPU mínimo
- Edición de SQL Server
- Hora de la última actualización

Instancias de Amazon EC2 con exceso de aprovisionamiento para Microsoft SQL Server

Descripción

Verifica las instancias de Amazon Elastic Compute Cloud (Amazon EC2) en las que se ha ejecutado SQL Server en las últimas 24 horas. Una base de datos de SQL Server tiene un límite de capacidad de computación para cada instancia. Una instancia con SQL Server Standard Edition puede utilizar hasta 48 vCPU. Una instancia con SQL Server Web puede utilizar hasta 32 vCPU. Esta verificación le avisa si una instancia supera este límite de vCPU.

Si la instancia tiene exceso de aprovisionamiento, se paga el precio completo sin obtener una mejora en el rendimiento. Puede administrar la cantidad y el tamaño de las instancias para ayudar a reducir los costos.

Los ahorros mensuales estimados se calculan utilizando la misma familia de instancias con la cantidad máxima de vCPU que puede utilizar una instancia de SQL Server y los precios bajo demanda. El ahorro real variará si utiliza Instancias reservadas (RI) o si la instancia no se ejecuta durante todo un día.

> **Note**
>
> Los resultados de esta verificación se actualizan automáticamente varias veces al día y no se permiten las solicitudes de actualización. Puede que los cambios tarden unas horas en aparecer. Actualmente, no puede excluir recursos de esta verificación.

ID de la verificación

`Qsdfp3A4L1`

Criterios de alerta

- Rojo: una instancia con la edición SQL Server Standard tiene más de 48 vCPU.
- Rojo: una instancia con la edición SQL Server Web tiene más de 32 vCPU.

Acción recomendada

Para la edición SQL Server Standard, considere cambiar a una instancia de la misma familia de instancias con 48 vCPU. Para la edición SQL Server Web, considere cambiar a una instancia de la misma familia de instancias con 32 vCPU. Si se trata de un uso intensivo de memoria, considere cambiar a instancias R5 optimizadas para memoria. Para obtener más información, consulte Best Practices for Deploying Microsoft SQL Server on Amazon EC2 (Prácticas recomendadas para implementar Microsoft SQL Server en Amazon EC2).

Recursos adicionales

- Microsoft SQL Server en AWS
- Puede utilizar Launch Wizard para simplificar la implementación de SQL Server en EC2.

Columnas de informes

- Status
- Región
- ID de instancia
- Tipo de instancia
- vCPU
- Edición de SQL Server
- Máximo de vCPU
- Tipo de instancia recomendado
- Ahorros mensuales estimados
- Hora de la última actualización

Instancias de Amazon EC2 detenidas

Descripción

Comprueba si hay instancias de Amazon EC2 detenidas desde hace más de 30 días.

Puede especificar el valor del número de días permitido en los parámetros. AllowedDaysAWS Config

Para obtener más información, consulte ¿Por qué se me cobra por Amazon EC2 cuando se cancelan todas mis instancias?

> **Note**
>
> Los resultados de esta verificación se actualizan automáticamente varias veces al día y no se permiten las solicitudes de actualización. Puede que los cambios tarden unas horas en aparecer. Actualmente, no puede excluir recursos de esta verificación.

ID de la verificación

`c18d2gz150`

Fuente

`AWS Config Managed Rule: ec2-stopped-instance`

Criterios de alerta

- Amarillo: hay instancias de Amazon EC2 detenidas durante una cantidad de días superior a la permitida.

Acción recomendada

Revise las instancias de Amazon EC2 que han estado detenidas durante 30 días o más. Para evitar incurrir en costos innecesarios, termine las instancias que ya no sean necesarias.

Para obtener más información, consulte Terminar la instancia.

Recursos adicionales

- Precios de Amazon EC2 bajo demanda

Columnas de informes

- Status
- Región
- Resource
- Regla de AWS Config
- Parámetros de entrada
- Hora de la última actualización

Amazon EC2 Reserved Instance Lease Expiration

Descripción

Verifica las instancias reservadas de Amazon EC2 que están programadas para caducar en los próximos 30 días, o bien las que hayan caducado en los 30 días anteriores.

Las instancias reservadas no se renuevan automáticamente. Puede seguir utilizando las instancias de Amazon EC2 cubiertas por la reserva sin interrupciones, aunque se le cobrarán los precios de instancias bajo demanda. Las nuevas instancias reservadas pueden tener los mismos parámetros que las caducadas, o bien puede adquirir instancias reservadas con parámetros diferentes.

El ahorro mensual estimado es la diferencia entre el precio de las instancias bajo demanda y los de las instancias reservadas del mismo tipo.

ID de la verificación

`1e93e4c0b5`

Criterios de alerta

- Amarillo: la asignación de la instancia reservada vence en menos de 30 días.
- Amarillo: la asignación de la instancia reservada vence en los 30 días anteriores.

Acción recomendada

Considere comprar una nueva instancia reservada para reemplazar la que está a punto de vencer. Para obtener más información, consulte Cómo adquirir instancias reservadas y Comprar instancias reservadas.

Recursos adicionales

- Instancias reservadas
- Tipos de instancias

Columnas de informes

- Status
- Zona
- Tipo de instancia
- Plataforma
- Recuento de instancias

- Costo mensual actual
- Ahorros mensuales estimados
- Fecha de vencimiento
- ID de Instancia reservada
- Motivo

Optimización de instancias reservadas de Amazon EC2

Descripción

Una parte importante de usar AWS consiste en encontrar el equilibrio entre la compra de instancias reservadas y el uso de instancias bajo demanda. Esta verificación proporciona recomendaciones sobre qué IR ayudarán a reducir los costos incurridos por el uso de instancias bajo demanda.

Estas recomendaciones se crean a partir del análisis de su uso de instancias bajo demanda durante los últimos 30 días. A continuación, se clasifica el uso en categorías aptas para reservas. Luego se simulan todas las combinaciones de reservas en la categoría de uso generada para identificar el número recomendado de cada tipo de IR que se debe comprar. Este proceso de simulación y optimización permite maximizar los ahorros de costos. Esta verificación cubre recomendaciones basadas en instancias reservadas estándar con la opción de pago inicial parcial.

Esta verificación no está disponible para las cuentas vinculadas a la facturación unificada. Las recomendaciones para esta verificación solo están disponibles para la cuenta de pago.

ID de la verificación

`cX3c2R1chu`

Criterios de alerta

Amarillo: optimizar el uso de IR de pago parcial inicial puede ayudar a reducir los costos.

Acción recomendada

Consulte la página de Cost Explorer para obtener recomendaciones más detalladas y personalizadas. Además, consulte la guía de compra para comprender cómo comprar IR y las opciones disponibles.

Recursos adicionales

- Puede encontrar información sobre las IR y cómo pueden ahorrarle dinero aquí.
- Para obtener más información sobre esta recomendación, consulte Preguntas sobre la comprobación de optimización de instancias en las Preguntas frecuentes de Trusted Advisor.

Columnas de informes

- Región
- Tipo de instancia
- Plataforma
- Cantidad recomendada de IR a comprar
- Utilización media prevista de IR
- Ahorros estimados con recomendaciones (mensual)
- Costo inicial de las IR
- Costos estimados de IR (mensual)
- Costo bajo demanda estimado después de la compra de IR recomendada (mensual)
- Punto de equilibrio estimado (meses)
- Periodo retroactivo (días)
- Plazo (años)

Repositorio de Amazon ECR sin política de ciclo de vida configurada

Descripción

Comprueba si un repositorio privado de Amazon ECR tiene configurada al menos una política de ciclo de vida. Las políticas de ciclo de vida permiten definir un conjunto de reglas para limpiar de manera automática imágenes de contenedor antiguas o no utilizadas. Esto permite controlar la administración del ciclo de vida de las imágenes, permite organizar mejor los repositorios de Amazon ECR, y ayuda a reducir los costos generales de almacenamiento.

Para obtener más información, consulte Políticas de ciclo de vida.

ID de la verificación

```
c18d2gz128
```

Fuente

```
AWS Config Managed Rule: ecr-private-lifecycle-policy-configured
```

Criterios de alerta

Amarillo: un repositorio privado de Amazon ECR no tiene ninguna política de ciclo de vida configurada.

Acción recomendada

Considere la posibilidad de crear al menos una política de ciclo de vida para su repositorio privado de Amazon ECR.

Para obtener más información, consulte Creación de una política de ciclo de vida.

Recursos adicionales

- Políticas de ciclo de vida
- Creación de una política de ciclo de vida
- Ejemplos de políticas de ciclo de vida

Columnas de informes

- Status
- Región
- Resource
- Regla de AWS Config
- Parámetros de entrada
- Hora de la última actualización

Optimización de nodos ElastiCache reservados de Amazon

Descripción

Comprueba el uso que haces de los nodos reservados ElastiCache y ofrece recomendaciones al momento de adquirirlos. Estas recomendaciones se ofrecen para reducir los costos incurridos por el uso de ElastiCache On-Demand. Estas recomendaciones se crean a partir del análisis de su uso de instancias bajo demanda durante los últimos 30 días.

El análisis se utiliza para simular cada combinación de reservas en la categoría de uso generado. Esto permite recomendar el número de cada tipo de nodo reservado que se debe comprar para maximizar el ahorro. Esta verificación cubre recomendaciones basadas en la opción de pago inicial parcial con un compromiso de 1 o 3 años.

Esta verificación no está disponible para las cuentas vinculadas a la facturación unificada. Las recomendaciones para esta verificación solo están disponibles para la cuenta de pago.

ID de la verificación

`h3L1otH3re`

Criterios de alerta

Amarillo: Optimizar la compra de nodos ElastiCache reservados puede ayudar a reducir los costos.

Acción recomendada

Consulte la página Cost Explorer para obtener recomendaciones más detalladas, opciones de personalización (por ejemplo, período retrospectivo, opción de pago, etc.) y para comprar ElastiCache nodos reservados.

Recursos adicionales

- Puede encontrar información sobre los nodos ElastiCache reservados y cómo pueden ahorrarle dinero aquí.
- Para obtener más información sobre esta recomendación, consulte Preguntas sobre la comprobación de optimización de instancias en las Preguntas frecuentes de Trusted Advisor.
- Para obtener una descripción más detallada de los campos, consulte la documentación de Cost Explorer.

Columnas de informes

- Región
- Familia
- Node Type
- Descripción del producto
- Cantidad recomendada de nodos reservados a comprar
- Utilización media prevista de nodos reservados
- Ahorros estimados con recomendaciones (mensual)
- Costo inicial de los nodos reservados
- Costo estimado de los nodos reservados (mensual)
- Costo bajo demanda estimado después de la compra de nodos reservados recomendada (mensual)

- Punto de equilibrio estimado (meses)
- Periodo retroactivo (días)
- Plazo (años)

Optimización de instancias reservadas de Amazon OpenSearch Service

Descripción

Comprueba el uso que hace de Amazon OpenSearch Service y ofrece recomendaciones sobre la compra de instancias reservadas. Estas recomendaciones se ofrecen para reducir los costes derivados del uso de OpenSearch On-Demand. Estas recomendaciones se crean a partir del análisis de su uso de instancias bajo demanda durante los últimos 30 días.

El análisis se utiliza para simular cada combinación de reservas en la categoría de uso generado. Esto permite recomendar el número de cada tipo de instancia reservada que se debe comprar para maximizar el ahorro. Esta verificación cubre recomendaciones basadas en la opción de pago inicial parcial con un compromiso de 1 o 3 años.

Esta verificación no está disponible para las cuentas vinculadas a la facturación unificada. Las recomendaciones para esta verificación solo están disponibles para la cuenta de pago.

ID de la verificación

`7ujm6yhn5t`

Criterios de alerta

Amarillo: la optimización de la compra de instancias reservadas de Amazon OpenSearch Service puede ayudar a reducir los costos.

Acción recomendada

Consulte la página Cost Explorer para obtener recomendaciones más detalladas, opciones de personalización (por ejemplo, período retrospectivo, opción de pago, etc.) y para comprar instancias reservadas de Amazon OpenSearch Service.

Recursos adicionales

- Puede encontrar información sobre las instancias reservadas de Amazon OpenSearch Service y sobre cómo pueden ahorrarle dinero aquí.
- Para obtener más información sobre esta recomendación, consulte Preguntas sobre la comprobación de optimización de instancias en las Preguntas frecuentes de Trusted Advisor.

- Para obtener una descripción más detallada de los campos, consulte la documentación de Cost Explorer.

Columnas de informes

- Región
- Clase de instancia
- Tamaño de instancia
- Cantidad recomendada de instancias reservadas a comprar
- Utilización media prevista de instancias reservadas
- Ahorros estimados con recomendación (mensual)
- Costo inicial de las instancias reservadas
- Costo estimado de las instancias reservadas (mensual)
- Costo bajo demanda estimado después de la compra de instancias reservadas recomendada (mensual)
- Punto de equilibrio estimado (meses)
- Periodo retroactivo (días)
- Plazo (años)

Amazon RDS Idle DB Instances

Descripción

Verifica la configuración de Amazon Relational Database Service (Amazon RDS) para las instancias de base de datos (DB) que estén inactivas.

Si una instancia de base de datos no ha tenido conexión durante un periodo prolongado de tiempo, puede eliminar la instancia para reducir los costos. Se considera que una instancia de base de datos está inactiva si dicha instancia no ha tenido conexión en los últimos 7 días. Si se necesita almacenamiento persistente para los datos de la instancia, puede utilizar opciones de menor costo, como, por ejemplo, tomar y conservar una instantánea de base de datos. Las instantáneas de base de datos que se crean manualmente se conservan hasta que las elimine.

ID de la verificación

`Ti39halfu8`

Criterios de alerta

Amarillo: una instancia de base de datos activa no ha tenido conexión en los últimos 7 días.

Acción recomendada

Considere tomar una instantánea de la instancia de base de datos inactiva y, a continuación, detenerla o eliminarla. Al detener la instancia de base de datos, se eliminan algunos de sus costos, pero no se eliminan los costos de almacenamiento. Una instancia detenida mantiene todos los respaldos automatizados en función del periodo de retención configurado. Detener una instancia de base de datos suele implicar costos adicionales en comparación con eliminar la instancia y, a continuación, conservar solo la instantánea final. Consulte Parada de una instancia de Amazon RDS temporalmente y Eliminación de una instancia de base de datos con una instantánea final.

Recursos adicionales

Copia de seguridad y restauración

Columnas de informes

- Región
- Nombre de instancia de base de datos
- Multi-AZ
- Tipo de instancia
- Almacenamiento aprovisionado (GB)
- Días desde la última conexión
- Ahorros mensuales estimados (bajo demanda)

Optimización del nodo reservado de Amazon Redshift

Descripción

Verifica el uso de Amazon Redshift y proporciona recomendaciones sobre la compra de nodos reservados para ayudar a reducir los costos incurridos por el uso de Amazon Redshift bajo demanda.

Estas recomendaciones se generan a partir del análisis de su uso de instancias bajo demanda durante los últimos 30 días. El análisis se utiliza para simular cada combinación de reservas en la categoría de uso generado. Esto permite identificar el número óptimo de cada tipo

de nodo reservado que se debe comprar para maximizar el ahorro. Esta verificación cubre recomendaciones basadas en la opción de pago inicial parcial con un compromiso de 1 o 3 años.

Esta verificación no está disponible para las cuentas vinculadas a la facturación unificada. Las recomendaciones para esta verificación solo están disponibles para la cuenta de pago.

ID de la verificación

`1qw23er45t`

Criterios de alerta

Amarillo: la optimización de la compra de nodos reservados de Amazon Redshift puede ayudar a reducir los costos.

Acción recomendada

Consulte la página de Cost Explorer para obtener recomendaciones más detalladas, opciones de personalización (por ejemplo, periodo retrospectivo, opción de pago, etc.) y para comprar nodos reservados de Amazon Redshift.

Recursos adicionales

- Puede encontrar información sobre los nodos reservados de Amazon Redshift y cómo pueden ahorrarle dinero aquí.
- Para obtener más información sobre esta recomendación, consulte Preguntas sobre la comprobación de optimización de instancias en las Preguntas frecuentes de Trusted Advisor.
- Para obtener una descripción más detallada de los campos, consulte la documentación de Cost Explorer.

Columnas de informes

- Región
- Familia
- Node Type
- Cantidad recomendada de nodos reservados a comprar
- Utilización media prevista de nodos reservados
- Ahorros estimados con recomendación (mensual)
- UpFront Coste de los nodos reservados
- Costo estimado de los nodos reservados (mensual)
- Costo bajo demanda estimado después de la compra de nodos reservados recomendada (mensual)

- Punto de equilibrio estimado (meses)
- Periodo retroactivo (días)
- Plazo (años)

Optimización de instancias reservadas de Amazon Relational Database Service (RDS)

Descripción

Verifica el uso de RDS y proporciona recomendaciones sobre la compra de instancias reservadas para ayudar a reducir los costos incurridos por el uso de RDS bajo demanda.

Estas recomendaciones se generan a partir del análisis de su uso de instancias bajo demanda durante los últimos 30 días. El análisis se utiliza para simular cada combinación de reservas en la categoría de uso generado. Esto permite identificar el número óptimo de cada tipo de instancia reservada que se debe comprar para maximizar el ahorro. Esta verificación cubre recomendaciones basadas en la opción de pago inicial parcial con un compromiso de 1 o 3 años.

Esta verificación no está disponible para las cuentas vinculadas a la facturación unificada. Las recomendaciones para esta verificación solo están disponibles para la cuenta de pago.

ID de la verificación

`1qazXsw23e`

Criterios de alerta

Amarillo: optimizar la compra de instancias reservadas de Amazon RDS puede ayudar a reducir los costos.

Acción recomendada

Consulte la página de Cost Explorer para obtener recomendaciones más detalladas, opciones de personalización (por ejemplo, periodo retrospectivo, opción de pago, etc.) y para comprar instancias reservadas de Amazon RDS.

Recursos adicionales

- Puede encontrar información sobre las instancias reservadas de Amazon RDS y cómo pueden ahorrarle dinero aquí.
- Para obtener más información sobre esta recomendación, consulte Preguntas sobre la comprobación de optimización de instancias en las Preguntas frecuentes de Trusted Advisor.

- Para obtener una descripción más detallada de los campos, consulte la documentación de Cost Explorer.

Columnas de informes

- Región
- Familia
- Tipo de instancia
- Modelo de licencia
- Database Edition (Edición de la base de datos)
- Motor de base de datos
- Deployment Option (Opción de implementación)
- Cantidad recomendada de instancias reservadas a comprar
- Utilización media prevista de instancias reservadas
- Ahorros estimados con recomendación (mensual)
- Costo inicial de las instancias reservadas
- Costo estimado de las instancias reservadas (mensual)
- Costo bajo demanda estimado después de la compra de instancias reservadas recomendada (mensual)
- Punto de equilibrio estimado (meses)
- Periodo retroactivo (días)
- Plazo (años)

Conjuntos de registros de recursos de latencia en Amazon Route 53

Descripción

Verifica si hay conjuntos de registros de latencia de Amazon Route 53 configurados de manera ineficaz.

Para permitir que Amazon Route 53 dirija consultas a la Región de AWS con la menor latencia de red posible, debe crear conjuntos de registros de recursos de latencia para un nombre de dominio determinado (como ejemplo.com) en distintas regiones. Si solo crea un conjunto de registros de recursos de latencia para un nombre de dominio, todas las consultas se dirigirán a una región y deberá pagar tarifas adicionales por el enrutamiento basado en la latencia sin obtener beneficios.

Las zonas alojadas creadas mediante los servicios de AWS no aparecerán en los resultados de la verificación.

ID de la verificación

`51fC20e7I2`

Criterios de alerta

Amarillo: solo se ha configurado un conjunto de registros de recursos de latencia para un nombre de dominio en particular.

Acción recomendada

Si tiene recursos en varias regiones, asegúrese de definir un conjunto de registros de recursos de latencia para cada región. Consulte Enrutamiento basado en latencia.

Si tiene recursos solo en una Región de AWS, considere crear recursos en más de una Región de AWS y defina conjuntos de registros de recursos de latencia para cada una; consulte Enrutado basado en latencia.

Si no desea utilizar varias Regiones de AWS, debe utilizar un conjunto de registros de recursos sencillo. Consulte Trabajar con conjuntos de registros de recursos.

Recursos adicionales

- Guía para desarrolladores de Amazon Route 53
- Precios de Amazon Route 53

Columnas de informes

- Nombre de zona alojada
- ID de zona alojada
- Nombre de conjunto de registros de recursos
- Tipo de conjunto de registros de recursos

Política de ciclo de vida del bucket de Amazon S3 configurada

Descripción

Comprueba si un bucket de Amazon S3 tiene configurada una política de ciclo de vida. Una política de ciclo de vida de Amazon S3 garantiza que los objetos de Amazon S3 dentro del bucket se almacenen de forma rentable durante todo su ciclo de vida. Esto es importante para cumplir

con los requisitos normativos de almacenamiento y retención de datos. La configuración de políticas es un conjunto de reglas que definen las acciones que el servicio Amazon S3 aplica a un grupo de objetos. Una política de ciclo de vida permite automatizar la transición de los objetos a clases de almacenamiento de menor costo o eliminarlos a medida que envejecen. Por ejemplo, puede hacer la transición de un objeto al almacenamiento de Amazon S3 Standard-IA 30 días después de su creación, o a Amazon S3 Glacier después de 1 año.

También puede definir la caducidad del objeto para que Amazon S3 lo elimine en su nombre después de un periodo de tiempo determinado.

Puede ajustar la configuración de la comprobación mediante los parámetros de las reglas de AWS Config.

Para obtener más información, consulte Administración del ciclo de vida del almacenamiento.

> **Note**
>
> Los resultados de esta verificación se actualizan automáticamente varias veces al día y no se permiten las solicitudes de actualización. Puede que los cambios tarden unas horas en aparecer. Actualmente, no puede excluir recursos de esta verificación.

ID de la verificación

`c18d2gz100`

Fuente

`AWS Config Managed Rule: s3-lifecycle-policy-check`

Criterios de alerta

Amarillo: el bucket de Amazon S3 no tiene configurada ninguna política de ciclo de vida.

Acción recomendada

Asegúrese de tener configurada una política de ciclo de vida en su bucket de Amazon S3.

Si su organización no cuenta con una política de retención, considere la posibilidad de utilizar Amazon S3 Intelligent-Tiering para optimizar los costos.

Para obtener información acerca de cómo definir la política de ciclo de vida de Amazon S3, consulte Configurar el ciclo de vida de un bucket.

Para obtener información acerca de Amazon S3 Intelligent-Tiering, consulte Clase de almacenamiento Amazon S3 Intelligent-Tiering.

Recursos adicionales

Configuración del ciclo de vida en un bucket

Ejemplos de configuración del ciclo de vida de S3

Columnas de informes

- Status
- Región
- Resource
- Regla de AWS Config
- Parámetros de entrada

Configuración incompleta de cancelación de carga multiparte de Amazon S3

Descripción

Comprueba que cada bucket de Amazon S3 esté configurado con una regla de ciclo de vida para anular las cargas multiparte que permanezcan incompletas después de 7 días. Se recomienda utilizar una regla de ciclo de vida para anular estas cargas incompletas y eliminar el almacenamiento asociado.

> **Note**
>
> Los resultados de esta comprobación se actualizan automáticamente una o más veces al día y no se admiten solicitudes de actualización. Puede que los cambios tarden unas horas en aparecer. Actualmente, no puede excluir recursos de esta verificación.

ID de la verificación

`c1cj39rr6v`

Criterios de alerta

Amarillo: el depósito de configuración del ciclo de vida no contiene una regla de ciclo de vida que aborte todas las cargas multiparte que queden incompletas después de 7 días.

Acción recomendada

Revisa la configuración del ciclo de vida de los buckets sin una regla de ciclo de vida que elimine todas las cargas multiparte incompletas. Es poco probable que se completen las cargas que no se completen después de 24 horas. Haz clic aquí para seguir las instrucciones de creación de una regla de ciclo de vida. Se recomienda que se aplique a todos los objetos del bucket. Si necesitas aplicar otras acciones del ciclo de vida a los objetos seleccionados de tu depósito, puedes tener varias reglas con distintos filtros. Consulta el panel de control de Storage Lens o llama a la ListMultipartUpload API para obtener más información.

Recursos adicionales

Crear una configuración de ciclo de vida

Detección y eliminación de cargas multiparte incompletas para reducir los costes de Amazon S3

Carga y copia de objetos mediante la carga multiparte

Elementos de configuración del ciclo de vida

Elementos para describir las acciones del ciclo de vida

Configuración del ciclo de vida para anular las cargas de varias partes

Columnas de informes

- Status
- Región
- Nombre del bucket
- ARN de bucket
- Regla de ciclo de vida para eliminar una MPU incompleta
- Días después de la iniciación
- Hora de la última actualización

Buckets habilitados para versiones de Amazon S3 sin políticas de ciclo de vida configuradas

Descripción

Comprueba si los buckets habilitados para la versión de Amazon S3 tienen configurada una política de ciclo de vida.

Para obtener más información, consulte Administración del ciclo de vida del almacenamiento.

Puede especificar los nombres de los buckets que quiere comprobar mediante los parámetros bucketNames de las reglas de AWS Config.

> **Note**
>
> Los resultados de esta verificación se actualizan automáticamente varias veces al día y no se permiten las solicitudes de actualización. Puede que los cambios tarden unas horas en aparecer. Actualmente, no puede excluir recursos de esta verificación.

ID de la verificación

`c18d2gz171`

Fuente

`AWS Config Managed Rule: s3-version-lifecycle-policy-check`

Criterios de alerta

Amarillo: un bucket habilitado para la versión de Amazon S3 que no tiene una política de ciclo de vida configurada.

Acción recomendada

Configure políticas de ciclo de vida para buckets de Amazon S3 para administrar los objetos de modo que se almacenen de manera rentable durante todo el ciclo de vida.

Para obtener más información, consulte Configuración del ciclo de vida en un bucket.

Recursos adicionales

Administración del ciclo de vida del almacenamiento

Configuración del ciclo de vida en un bucket

Columnas de informes

- Status
- Región
- Resource

- Regla de AWS Config
- Parámetros de entrada
- Hora de la última actualización

Funciones de AWS Lambda con tiempos de espera excesivos

Descripción

Verifica las funciones de Lambda con elevadas tasas de tiempo de espera que pueden provocar altos costos.

Los cargos de Lambda se basan en el tiempo de ejecución y el número de solicitudes para su función. Los tiempos de espera de las funciones provocan errores que pueden provocar reintentos. Las funciones de reintento incurrirán además en cargos de solicitudes y tiempo de ejecución.

> **Note**
>
> Los resultados de esta verificación se actualizan automáticamente varias veces al día y no se permiten las solicitudes de actualización. Puede que los cambios tarden unas horas en aparecer. Actualmente, no puede excluir recursos de esta verificación.

ID de la verificación

`L4dfs2Q3C3`

Criterios de alerta

Amarillo: funciones en las que >10 % de las invocaciones terminan en un error debido a un tiempo de espera agotado en un día determinado dentro de los últimos 7 días.

Acción recomendada

Inspeccione el registro de funciones y los rastreos de X-Ray para determinar el factor que contribuye a la alta duración de la función. Implemente el registro en el código en las partes relevantes, como antes o después de las llamadas a la API o las conexiones a la base de datos. De forma predeterminada, los tiempos de espera de los clientes del SDK de AWS pueden ser superiores a la duración de la función configurada. Ajuste los clientes de conexión de API y SDK para que vuelvan a intentarlo o fallen dentro del tiempo de espera de la función. Si la duración

esperada es superior al tiempo de espera configurado, puede aumentar la configuración del tiempo de espera de la función. Para obtener más información, consulte Monitorización y solución de problemas de aplicaciones de Lambda.

Recursos adicionales

- Monitorización y solución de problemas de aplicaciones de Lambda
- SDK de tiempo de espera de reintentos de la función Lambda
- Uso de AWS Lambda con AWS X-Ray
- Acceder a CloudWatch los registros de Amazon para AWS Lambda
- Aplicación de ejemplo de procesamiento de errores para AWS Lambda

Columnas de informes

- Status
- Región
- ARN de función
- Tasa máxima de tiempo de espera diario
- Fecha de tasa máxima de tiempo de espera diario
- Tasa promedio de tiempo de espera diario
- Configuración de tiempo de espera de función (milisegundos)
- Pérdida de costos informáticos diarios
- Promedio de invocaciones diarias
- Invocaciones diarias actuales
- Tasa de tiempo de espera diario actual
- Hora de la última actualización

Funciones de AWS Lambda con elevadas tasas de error

Descripción

Verifica las funciones de Lambda con elevadas tasas de error que pueden provocar altos costos.

Los cargos de Lambda se basan en el número de solicitudes y el tiempo de ejecución agregado para su función. Los errores de funciones pueden provocar reintentos que incurren en cargos adicionales.

> **Note**
>
> Los resultados de esta verificación se actualizan automáticamente varias veces al día y no se permiten las solicitudes de actualización. Puede que los cambios tarden unas horas en aparecer. Actualmente, no puede excluir recursos de esta verificación.

ID de la verificación

`L4dfs2Q3C2`

Criterios de alerta

Amarillo: funciones en las que >10 % de las invocaciones terminan en error en un día determinado dentro de los últimos 7 días.

Acción recomendada

Tenga en cuenta estas directrices para reducir errores. Los errores de la función incluyen errores devueltos por el código de la función y los errores devueltos por el tiempo de ejecución de la función.

Para ayudarle a solucionar los errores de Lambda, Lambda se integra con servicios como Amazon y. CloudWatch AWS X-Ray Puede utilizar una combinación de registros, métricas, alarmas y rastreos de X-Ray para detectar e identificar rápidamente problemas en el código de la función, la API u otros recursos que admiten la aplicación. Para obtener más información, consulte Monitorización y solución de problemas de aplicaciones de Lambda.

Para obtener más información sobre el manejo de errores con tiempos de ejecución específicos, consulte Control de errores y reintentos automáticos en AWS Lambda.

Para obtener la solución de problemas adicionales, consulte Solución de problemas de Lambda.

También puede elegir entre un ecosistema de herramientas de monitoreo y observabilidad proporcionadas por socios de AWS Lambda. Para obtener más información, consulte Socios de AWS Lambda.

Recursos adicionales

- Control de errores y reintentos automáticos en AWS Lambda
- Monitorización y solución de problemas de aplicaciones de Lambda
- SDK de tiempo de espera de reintentos de la función Lambda

- Solución de problemas de Lambda
- Errores de invocación de la API
- Aplicación de ejemplo de procesamiento de errores para AWS Lambda

Columnas de informes

- Status
- Región
- ARN de función
- Tasa máxima de errores diarios
- Fecha de la tasa máxima de errores
- Tasa promedio de errores diarios
- Pérdida de costos informáticos diarios
- Promedio de invocaciones diarias
- Invocaciones diarias actuales

  Tasa de errores diarios actual
- Hora de la última actualización

Funciones AWS Lambda con exceso de aprovisionamiento para el tamaño de la memoria

Descripción

Compruebe las funciones AWS Lambda que se invocaron al menos una vez durante el período de revisión. Esta comprobación le avisa si alguna de las funciones Lambda se aprovisionó en exceso para el tamaño de la memoria. Cuando tiene funciones Lambda con exceso de aprovisionamiento para los tamaños de la memoria, paga por recursos no utilizados. Aunque algunos escenarios pueden dar lugar a una baja utilización por diseño, a menudo se pueden reducir los costos si se cambia la configuración de la memoria de sus funciones Lambda. Los ahorros mensuales estimados se calculan con la tasa de uso actual para funciones Lambda.

> **Note**
>
> Los resultados de esta verificación se actualizan automáticamente varias veces al día y no se permiten las solicitudes de actualización. Puede que los cambios tarden unas horas en aparecer. Actualmente, no puede excluir recursos de esta verificación.

ID de la verificación

`C0r6dfpM05`

Criterios de alerta

Amarillo: una función de Lambda que se aprovisionó en exceso para el tamaño de la memoria durante el periodo retroactivo. Para determinar si una función Lambda está sobreaprovisionada, tenemos en cuenta todas las CloudWatch métricas predeterminadas de esa función. El algoritmo utilizado para identificar las funciones de Lambda sobreaprovisionadas para el tamaño de la memoria sigue las prácticas recomendadas de AWS. El algoritmo se actualiza cuando se identifica un nuevo patrón.

Acción recomendada

Considere reducir el tamaño de la memoria de las funciones de Lambda.

Para obtener más información, consulte Optar AWS Compute Optimizer por recibir Trusted Advisor cheques.

Columnas de informes

- Status
- Región
- Nombre de la función
- Versión de la función
- Tamaño de la memoria (MB)
- Tamaño de la memoria recomendado (MB)
- Periodo retroactivo (días)
- Oportunidad de ahorro (%)
- Ahorros mensuales estimados
- Divisa de ahorros mensuales estimados

- Hora de la última actualización

Problemas de alto riesgo de AWS Well-Architected para la optimización de costos

Descripción

Verifica si hay problemas de alto riesgo para las cargas de trabajo en el pilar de optimización de costos. Esta verificación se basa en las revisiones de AWS-Well Architected. Los resultados de las verificaciones dependen de si ha completado la evaluación de la carga de trabajo con AWS Well-Architected.

> **Note**
>
> Los resultados de esta verificación se actualizan automáticamente varias veces al día y no se permiten las solicitudes de actualización. Puede que los cambios tarden unas horas en aparecer. Actualmente, no puede excluir recursos de esta verificación.

ID de la verificación

`Wxdfp4B1L1`

Criterios de alerta

- Rojo: se identificó al menos un problema activo de alto riesgo en el pilar de optimización de costos de AWS Well-Architected.
- Verde: no se detectaron problemas activos de alto riesgo en el pilar de optimización de costos de AWS Well-Architected.

Acción recomendada

AWS Well-Architected detectó problemas de alto riesgo durante la evaluación de la carga de trabajo. Estos problemas presentan oportunidades para reducir el riesgo y ahorrar dinero. Inicie sesión en la herramienta AWS Well-Architected para revisar las respuestas y tomar medidas para resolver los problemas activos.

Columnas de informes

- Status
- Región
- ARN de carga de trabajo

- Nombre de carga de trabajo
- Nombre del revisor
- Tipo de carga de trabajo
- Fecha de inicio de carga de trabajo
- Fecha de la última modificación de carga de trabajo
- Cantidad de HRI identificados para la optimización de costos
- Cantidad de HRI resueltos para la optimización de costos
- Cantidad de preguntas respondidas para la optimización de costos
- Cantidad total de preguntas en el pilar de optimización de costos
- Hora de la última actualización

Balanceadores de carga inactivos

Descripción

Verifica la configuración de Elastic Load Balancing en busca de balanceadores de carga inactivos.

Todos los balanceadores de carga configurados acumulan cargos. Si un balanceador de carga no tiene ninguna instancia de backend asociada o si el tráfico de red está muy limitado, el balanceador de carga no se utiliza de manera eficaz. Esta verificación actualmente solo verifica el tipo de Classic Load Balancer en el servicio ELB. No incluye otros tipos de ELB (Application Load Balancer, Network Load Balancer).

ID de la verificación

`hjLMh88uM8`

Criterios de alerta

- Amarillo: un equilibrador de carga no tiene instancias de back-end activas.
- Amarillo: un equilibrador de carga no tiene instancias de back-end en buen estado.
- Amarillo: un equilibrador de carga ha recibido menos de 100 solicitudes por día durante los últimos 7 días.

Acción recomendada

Si el equilibrador de carga no tiene instancias de back-end activas, considere registrar instancias o eliminar el equilibrador de carga. Consulte Registering Your Amazon EC2 Instances with Your

Load Balancer (Registro de instancias de Amazon EC2 con el equilibrador de carga) o Delete Your Load Balancer (Eliminar el equilibrador de carga).

Si el equilibrador de carga no tiene instancias de back-end en buen estado, consulte Troubleshooting Elastic Load Balancing: Health Check Configuration (Solución de problemas de Elastic Load Balancing: configuración de la comprobación de estado).

Si el equilibrador de carga ha tenido un recuento de solicitudes bajo, considere eliminar el equilibrador de carga. Consulte Eliminar el equilibrador de carga.

Recursos adicionales

- Administración de equilibradores de carga
- Solución de problemas de Elastic Load Balancing

Columnas de informes

- Región
- Nombre del equilibrador de carga
- Motivo
- Ahorros mensuales estimados

Utilización baja de instancias de Amazon EC2

Descripción

Verifica las instancias de Amazon Elastic Compute Cloud (Amazon EC2) que han estado en ejecución en cualquier momento durante los últimos 14 días. Esta verificación le avisa si el uso diario de la CPU fue del 10 % o inferior y si la E/S de red fue de 5 MB o inferior durante al menos 4 días.

Las instancias de ejecución generan cargos por uso por hora. Aunque algunas situaciones pueden dar lugar a un bajo uso por diseño, a menudo se pueden reducir los costos al administrar el número y el tamaño de las instancias.

Los ahorros mensuales estimados se calculan utilizando la tasa de uso actual de las instancias bajo demanda y el número estimado de días en que la instancia podría estar infrautilizada. El ahorro real variará si utiliza instancias reservadas o instancias puntuales, o si la instancia no se ejecuta durante un día completo. Para obtener datos del uso diario, descargue el informe de esta verificación.

ID de la verificación

Qch7DwouX1

Criterios de alerta

Amarillo: una instancia tuvo un uso de CPU promedio diario del 10 % o menos y una E/S de red de 5 MB o menos en al menos 4 de los 14 días anteriores.

Acción recomendada

Considere detener o terminar las instancias que tienen una baja utilización o escale el número de instancias mediante Auto Scaling. Para obtener más información, consulte Detener e iniciar la instancia, Terminar una instancia y ¿Qué es Auto Scaling?

Recursos adicionales

- Monitoreo de Amazon EC2
- Metadatos de instancia y datos de usuario
- Guía CloudWatch del usuario de Amazon
- Guía para desarrolladores de Auto Scaling

Columnas de informes

- Región/AZ
- ID de instancia
- Nombre de instancia
- Tipo de instancia
- Ahorros mensuales estimados
- Utilización promedio de la CPU de 14 días
- Promedio de E/S de red de 14 días
- Cantidad de días de baja utilización

Savings Plan

Descripción

Verifica el uso de Amazon EC2, Fargate y Lambda durante los últimos 30 días y proporciona recomendaciones de compra de Savings Plan. Estas recomendaciones permiten comprometerse

con una cantidad de uso consistente en dólares por hora durante un periodo de uno o tres años a cambio de tarifas con descuento.

Estas proceden de AWS Cost Explorer, que puede obtener información más detallada sobre las recomendaciones. También puede comprar un Savings Plan mediante Cost Explorer. Estas recomendaciones deben considerarse como una alternativa a sus recomendaciones de RI. Se recomienda actuar solo en un conjunto de recomendaciones. Actuar en ambos conjuntos puede dar lugar a un exceso de compromiso.

Esta verificación no está disponible para las cuentas vinculadas a la facturación unificada. Las recomendaciones para esta verificación solo están disponibles para la cuenta de pago.

ID de la verificación

`vZ2c2W1srf`

Criterios de alerta

Amarillo: la optimización de la compra de Savings Plans puede ayudar a reducir los costos.

Acción recomendada

Consulte la página de Cost Explorer para obtener recomendaciones más detalladas y personalizadas y comprar Savings Plans.

Recursos adicionales

- Guía del usuario de Savings Plans
- Preguntas frecuentes sobre Savings Plans

Columnas de informes

- Tipo de Savings Plans
- Opción de pago
- Costo inicial
- Compromiso de compra por hora
- Utilización promedio estimada
- Ahorros mensuales estimados
- Porcentaje de ahorro estimado
- Plazo (años)
- Periodo retroactivo (días)

Direcciones IP elásticas no asociadas

Descripción

Verifica las direcciones IP elásticas (EIP) que no están asociadas a ninguna instancia de Amazon Elastic Compute Cloud (Amazon EC2) en ejecución.

Las direcciones IP estáticas están diseñadas para la informática en la nube dinámica. A diferencia de las direcciones IP estáticas tradicionales, las EIP enmascaran el error de una instancia o zona de disponibilidad mediante la reasignación de una dirección IP pública a otra instancia de su cuenta. Se impone un cargo nominal para las EIP que no estén asociadas a una instancia en ejecución.

ID de la verificación

`Z4AUBRNSmz`

Criterios de alerta

Amarillo: una dirección IP elástica (EIP) asignada no está asociada a una instancia de Amazon EC2 en ejecución.

Acción recomendada

Asocie el EIP con una instancia activa en ejecución o libere el EIP no asociado. Para obtener más información, consulte Asociación de una dirección IP elástica a una instancia en ejecución diferente y Liberación de una dirección IP elástica.

Recursos adicionales

Direcciones IP elásticas

Columnas de informes

- Región
- Dirección IP

Volúmenes de Amazon EBS infrautilizados

Descripción

Verifica las configuraciones de volúmenes de Amazon Elastic Block Store (Amazon EBS) y avisa cuando los volúmenes están infrautilizados.

Los cargos comienzan cuando se crea un volumen. Se considera que un volumen está infrautilizado si permanece desconectado o tiene una actividad de escritura muy baja (excluyendo los volúmenes de arranque) durante un periodo de tiempo. Se recomienda eliminar los volúmenes infrautilizados para reducir los costos.

ID de la verificación

`DAvU99Dc4C`

Criterios de alerta

Amarillo: un volumen no está asociado o tuvo menos de 1 IOPS por día durante los últimos 7 días.

Acción recomendada

Considere crear una instantánea y eliminar el volumen para reducir los costos. Para obtener más información, consulte Creación de una instantánea de Amazon EBS y Eliminar un volumen Amazon EBS.

Recursos adicionales

- Amazon Elastic Block Store (Amazon EBS)
- Monitorización del estado de los volúmenes

Columnas de informes

- Región
- ID de volumen
- Nombre del volumen
- Tipo de volumen
- Tamaño del volumen
- Costo mensual de almacenamiento
- ID de instantánea
- Nombre de la instantánea
- Antigüedad de la instantánea

> **Note**
>
> Si ha optado por AWS Compute Optimizer en su cuenta, se recomienda utilizar la comprobación de volúmenes con exceso de aprovisionamiento de Amazon EBS en su lugar.

Para obtener más información, consulte Optar AWS Compute Optimizer por recibir Trusted Advisor cheques.

Underutilized Amazon Redshift Clusters

Descripción

Verifica la configuración de Amazon Redshift en busca de clústeres que estén infrautilizados.

Si un clúster de Amazon Redshift no ha tenido conexión durante un periodo de tiempo prolongado o si utiliza una cantidad baja de recursos de CPU, puede utilizar opciones de menor costo, como, por ejemplo, reducir el tamaño del clúster o cerrar el clúster y tomar una instantánea final. Las instantáneas finales se conservan incluso después de eliminar el clúster.

ID de la verificación

`G31sQ1E9U`

Criterios de alerta

- Amarillo: un clúster en ejecución no ha tenido conexión en los últimos 7 días.
- Amarillo: un clúster en ejecución tuvo una utilización promedio de CPU inferior al 5 % en todo el clúster durante el 99 % de los últimos 7 días.

Acción recomendada

Considere cerrar el clúster y tomar una instantánea final o reducir el tamaño del clúster. Consulte Cierre y eliminación de clústeres y Redimensionamiento de un clúster.

Recursos adicionales

Guía CloudWatch del usuario de Amazon

Columnas de informes

- Status
- Región
- Clúster
- Tipo de instancia
- Motivo
- Ahorros mensuales estimados

Rendimiento

Mejore el rendimiento de su servicio con la verificación de las cuotas de servicio (anteriormente denominadas límites), para poder aprovechar el rendimiento aprovisionado, monitorear las instancias sobreutilizadas y detectar los recursos no utilizados.

Puede utilizar las siguientes verificaciones para la categoría de rendimiento.

Nombres de la verificación

- Clúster de base de datos Amazon Aurora con aprovisionamiento insuficiente para la carga de trabajo de lectura
- El escalado automático de Amazon DynamoDB no está habilitado
- La optimización de Amazon EBS no está habilitada
- Configuración de datos adjuntos de volumen de IOPS provisionadas (SSD) de Amazon EBS
- Volúmenes con falta de aprovisionamiento de Amazon EBS
- El grupo de Amazon EC2 Auto Scaling no está asociado a una plantilla de lanzamiento
- Optimización del rendimiento de Amazon EC2 a EBS
- El tipo de virtualización de EC2 es paravirtual
- Límite máximo de memoria de Amazon ECS
- Optimización del modo de rendimiento de Amazon EFS
- El parámetro de autovacuum de Amazon RDS está desactivado
- Los clústeres de bases de datos de Amazon RDS solo admiten un volumen de hasta 64 TiB
- Instancias de base de datos de Amazon RDS en los clústeres con clases de instancias heterogéneas
- Instancias de base de datos de Amazon RDS en los clústeres con tamaños de instancia heterogéneos
- Los parámetros de memoria de base de datos de Amazon RDS difieren de los predeterminados
- El parámetro enable_indexonlyscan de Amazon RDS está desactivado
- El parámetro enable_indexscan de Amazon RDS está desactivado
- El parámetro general_logging de Amazon RDS está activado
- Parámetro InnoDB_change_buffering de Amazon RDS que utiliza un valor inferior al óptimo
- El parámetro innodb_open_files de Amazon RDS es bajo

- El parámetro innodb_stats_persistent de Amazon RDS está desactivado
- Instancia de Amazon RDS con aprovisionamiento insuficiente para la capacidad del sistema
- El volumen magnético Amazon RDS está en uso
- Los grupos de parámetros de Amazon RDS no utilizan páginas enormes
- El parámetro de caché de consultas de Amazon RDS está activado
- Es necesaria la actualización de la clase de instancia de Amazon RDS Resources
- Recursos de Amazon RDS: es necesaria la actualización de las versiones principales
- Recursos de Amazon RDS que utilizan la edición de fin del motor de soporte con licencia incluida
- Conjuntos de registros de recursos de alias en Amazon Route 53
- Funciones AWS Lambda con falta de aprovisionamiento para el tamaño de la memoria
- AWS Lambda Funciones sin límite de simultaneidad configuradas
- Problemas de alto riesgo de AWS Well-Architected para el rendimiento
- CloudFront Nombres de dominio alternativos
- CloudFront Optimización de la entrega de contenido
- CloudFront Reenvío de encabezados y porcentaje de aciertos de caché
- Uso elevado de instancias de Amazon EC2

Clúster de base de datos Amazon Aurora con aprovisionamiento insuficiente para la carga de trabajo de lectura

Descripción

Comprueba si el clúster de base de datos Amazon Aurora tiene los recursos necesarios para soportar una carga de trabajo de lectura.

ID de la verificación

`c1qf5bt038`

Criterios de alerta

Amarillo:

Aumento de las lecturas de la base de datos: la carga de la base de datos era alta y la base de datos leía más filas de las que escribía o actualizaba las filas.

Acción recomendada

Se recomienda ajustar las consultas para reducir la carga de la base de datos o añadir una instancia de base de datos de lectura a su clúster de base de datos con la misma clase y tamaño de instancia que la instancia de base de datos de escritura del clúster. La configuración actual tiene al menos una instancia de base de datos con una carga de base de datos continuamente alta, causada principalmente por las operaciones de lectura. Distribuya estas operaciones agregando otra instancia de base de datos al clúster y dirigiendo la carga de trabajo de lectura al punto de conexión de solo lectura del clúster de base de datos.

Recursos adicionales

Un clúster de base de datos Aurora tiene un punto final de lector para conexiones de solo lectura. Este punto final utiliza el equilibrio de carga para gestionar las consultas que más contribuyen a la carga de la base de datos en el clúster de base de datos. El punto final del lector dirige estas declaraciones a las réplicas de lectura de Aurora y reduce la carga en la instancia principal. El punto final del lector también escala la capacidad de gestionar consultas SELECT simultáneas con la cantidad de réplicas de lectura de Aurora en el clúster.

Para obtener más información, consulte Añadir réplicas de Aurora a un clúster de base de datos y Administrar el rendimiento y el escalado de los clústeres de base de datos Aurora.

Columnas de informes

- Status
- Región
- Recurso
- Aumento de la lectura (recuento) de la base de datos
- Último período de detección
- Hora de la última actualización

El escalado automático de Amazon DynamoDB no está habilitado

Descripción

Comprueba si las tablas de Amazon DynamoDB y los índices secundarios globales tienen habilitado el escalado automático o bajo demanda.

El escalado automático de Amazon DynamoDB utiliza el servicio Auto Scaling de aplicaciones para ajustar de manera dinámica la capacidad de rendimiento aprovisionada en su nombre en

respuesta a los patrones de tráfico reales. Esto permite a una tabla o índice secundario global incrementar su capacidad de lectura y escritura aprovisionada para abastecer incrementos repentinos del tráfico sin limitaciones controladas. Cuando la carga de trabajo disminuye, el Auto Scaling de aplicaciones puede reducir el rendimiento para evitar que tenga que pagar por una capacidad aprovisionada que no se utiliza.

Puede ajustar la configuración de la comprobación mediante los parámetros de sus AWS Config reglas.

Para obtener más información, consulte Administración automática de la capacidad de rendimiento con el escalado automático de DynamoDB.

> **Note**
>
> Los resultados de esta verificación se actualizan automáticamente varias veces al día y no se permiten las solicitudes de actualización. Puede que los cambios tarden unas horas en aparecer. Actualmente, no puede excluir recursos de esta verificación.

ID de la verificación

`c18d2gz136`

Origen

AWS Config Regla gestionada: dynamodb-autoscaling-enabled

Criterios de alerta

Amarillo: el escalado automático no está habilitado para las tablas de DynamoDB ni para los índices secundarios globales.

Acción recomendada

A menos que ya disponga de un mecanismo para escalar de manera automática el rendimiento aprovisionado de su tabla de DynamoDB o los índices secundarios globales en función de los requisitos de la carga de trabajo, considere la posibilidad de activar el escalado automático para sus tablas de Amazon DynamoDB.

Para obtener más información, consulte Uso de la consola de administración de AWS con el escalado automático de DynamoDB.

Recursos adicionales

Administración automática de la capacidad de rendimiento con el escalado automático de DynamoDB

Columnas de informes

- Status
- Región
- Recurso
- AWS Config Regla
- Parámetros de entrada
- Hora de la última actualización

La optimización de Amazon EBS no está habilitada

Descripción

Comprueba si la optimización de Amazon EBS está habilitada para las instancias de Amazon EC2.

Una instancia optimizada para Amazon EBS utiliza una pila de configuración optimizada y proporciona capacidad adicional y dedicada para las E/S de Amazon EBS. Esta optimización proporciona el mejor rendimiento para sus volúmenes de Amazon EBS, ya que minimiza la contención entre las E/S de Amazon EBS y otro tráfico procedente de la instancia.

Para obtener más información, consulte Instancias optimizadas para Amazon EBS.

> **Note**
>
> Los resultados de esta verificación se actualizan automáticamente varias veces al día y no se permiten las solicitudes de actualización. Puede que los cambios tarden unas horas en aparecer. Actualmente, no puede excluir recursos de esta verificación.

ID de la verificación

`c18d2gz142`

Origen

AWS Config Regla gestionada: ebs-optimized-instance

Criterios de alerta

Amarillo: la optimización de Amazon EBS no está habilitada en las instancias de Amazon EC2 compatibles.

Acción recomendada

Active la optimización de Amazon EBS en las instancias compatibles.

Para obtener más información, consulte Habilitación de la optimización de EBS en el lanzamiento.

Recursos adicionales

Instancias optimizadas para Amazon EBS

Columnas de informes

- Status
- Región
- Recurso
- AWS Config Regla
- Parámetros de entrada
- Hora de la última actualización

Configuración de datos adjuntos de volumen de IOPS provisionadas (SSD) de Amazon EBS

Descripción

Verifica los volúmenes de IOPS provisionadas (SSD) conectados a una instancia de Amazon Elastic Compute Cloud (Amazon EC2) optimizable de Amazon EBS que no está optimizada para EBS.

Los volúmenes de IOPS provisionadas (SSD) de Amazon Elastic Block Store (Amazon EBS) están diseñados para ofrecer el rendimiento esperado solo cuando están conectados a una instancia optimizada para EBS.

ID de la verificación

`PPkZrjsH2q`

Criterios de alerta

Amarillo: una instancia de Amazon EC2 que se puede optimizar para EBS tiene un volumen de IOPS aprovisionadas (SSD) adjunto, pero la instancia no está optimizada para EBS.

Acción recomendada

Cree una instancia nueva optimizada para EBS, separe el volumen y vuelva a adjuntarlo a la instancia nueva. Para obtener más información, consulte Instancias optimizadas para Amazon EBS y Adjuntar un volumen de Amazon EBS a una instancia.

Recursos adicionales

- Tipos de volúmenes de Amazon EBS
- Rendimiento de los volúmenes de Amazon EBS

Columnas de informes

- Status
- Región/AZ
- ID de volumen
- Nombre del volumen
- Asociación de volúmenes
- ID de instancia
- Tipo de instancia
- Optimización de EBS

Volúmenes con falta de aprovisionamiento de Amazon EBS

Descripción

Compruebe los volúmenes de Amazon Elastic Block Store (Amazon EBS) que se estaban ejecutando en cualquier momento durante el período de revisión. Esta comprobación le avisa si hay falta de aprovisionamiento de volúmenes de EBS para sus cargas de trabajo. Un alto uso coherente puede indicar un rendimiento optimizado y constante, pero también puede indicar que una aplicación no tiene suficientes recursos.

> **Note**
>
> Los resultados de esta verificación se actualizan automáticamente varias veces al día y no se permiten las solicitudes de actualización. Puede que los cambios tarden unas horas en aparecer. Actualmente, no puede excluir recursos de esta verificación.

ID de la verificación

`COr6dfpM04`

Criterios de alerta

Amarillo: un volumen de EBS que se aprovisionó de forma insuficiente durante el periodo retroactivo. Para determinar si un volumen tiene un aprovisionamiento insuficiente, tenemos en cuenta todas las CloudWatch métricas predeterminadas (incluidas las IOPS y el rendimiento). El algoritmo utilizado para identificar los volúmenes de EBS con aprovisionamiento insuficiente sigue las prácticas recomendadas. AWS El algoritmo se actualiza cuando se identifica un nuevo patrón.

Acción recomendada

Considere aumentar el tamaño de los volúmenes que tienen una alta utilización.

Para obtener más información, consulte Optar AWS Compute Optimizer por recibir Trusted Advisor cheques.

Columnas de informes

- Status
- Región
- ID de volumen
- Tipo de volumen
- Tamaño del volumen (GB)
- IOPS de referencia de volumen
- IOPS por ráfagas de volumen
- Rendimiento por ráfagas de volumen
- Tipo de volumen recomendado
- Tamaño de volumen recomendado (GB)
- IOPS de referencia de volumen recomendado

- IOPS por ráfagas de volumen recomendado
- Rendimiento de referencia de volumen recomendado
- Rendimiento por ráfagas de volumen recomendado
- Periodo retroactivo (días)
- Riesgo de rendimiento
- Hora de la última actualización

El grupo de Amazon EC2 Auto Scaling no está asociado a una plantilla de lanzamiento

Descripción

Comprueba si se crea un grupo de Amazon EC2 Auto Scaling a partir de una plantilla de lanzamiento de Amazon EC2.

Utilice una plantilla de lanzamiento para crear sus grupos de Amazon EC2 Auto Scaling y garantizar el acceso a las características y las mejoras más recientes del grupo de escalado automático. Por ejemplo, el control de versiones y varios tipos de instancias.

Para obtener más información, consulte Plantillas de lanzamiento.

> **Note**
>
> Los resultados de esta verificación se actualizan automáticamente varias veces al día y no se permiten las solicitudes de actualización. Puede que los cambios tarden unas horas en aparecer. Actualmente, no puede excluir recursos de esta verificación.

ID de la verificación

`c18d2gz102`

Origen

AWS Config Regla gestionada: autoscaling-launch-template

Criterios de alerta

Amarillo: el grupo de Amazon EC2 Auto Scaling no está asociado a una plantilla de lanzamiento válida.

Acción recomendada

Utilice una plantilla de lanzamiento de Amazon EC2 para crear grupos de Amazon EC2 Auto Scaling.

Para obtener más información, consulte Creación de una plantilla de lanzamiento para un grupo de escalado automático.

Recursos adicionales

- Plantillas de lanzamiento
- Creación de una plantilla de lanzamiento

Columnas de informes

- Status
- Región
- Recurso
- AWS Config Regla
- Parámetros de entrada
- Hora de la última actualización

Optimización del rendimiento de Amazon EC2 a EBS

Descripción

Verifica los volúmenes de Amazon EBS cuyo rendimiento puede verse afectado por la capacidad de rendimiento máximo de la instancia de Amazon EC2 a la que están conectados.

Para optimizar el rendimiento, debe asegurarse de que el rendimiento máximo de una instancia de Amazon EC2 es mayor que el rendimiento máximo agregado de los volúmenes de EBS conectados. Esta verificación calcula el rendimiento total del volumen de EBS para cada periodo de cinco minutos del día anterior (basado en la hora universal coordinada (UTC)) para cada instancia optimizada para EBS y le avisa si el uso en más de la mitad de esos periodos fue superior al 95 % del rendimiento máximo de la instancia EC2.

ID de la verificación

`Bh2xRR2FGH`

Criterios de alerta

Amarillo: el día anterior (UTC), el rendimiento total (megabytes/segundos) de los volúmenes de EBS adjuntos a la instancia de EC2 superó el 95 % del rendimiento publicado entre la instancia y los volúmenes de EBS durante más del 50 % de las veces.

Acción recomendada

Compare el rendimiento máximo de los volúmenes de Amazon EBS (consulte Tipos de volumen de Amazon EBS) con el rendimiento máximo de la instancia de Amazon EC2 a la que están adjuntados. Consulte Tipos de instancias que admiten la optimización de EBS.

Considere adjuntar los volúmenes a una instancia que admita un mayor rendimiento en Amazon EBS para lograr un rendimiento óptimo.

Recursos adicionales

- Tipos de volúmenes de Amazon EBS
- Instancias optimizadas para Amazon EBS
- Monitorización del estado de los volúmenes
- Adjuntar un volumen de Amazon EBS a una instancia
- Desconectar un volumen de Amazon EBS de una instancia
- Eliminar un volumen de Amazon EBS

Columnas de informes

- Status
- Región
- ID de instancia
- Tipo de instancia
- Tiempo cerca del máximo

El tipo de virtualización de EC2 es paravirtual

Descripción

Comprueba si el tipo de virtualización de una instancia de Amazon EC2 es paravirtual.

Una práctica recomendada es utilizar instancias de máquina virtual de hardware (HVM) en lugar de instancias paravirtuales, siempre que sea posible. Esto se debe a las mejoras en la

virtualización de HVM y a la disponibilidad de los controladores PV para AMI HVM, que cerraron la brecha de rendimiento que existía históricamente entre los invitados PV y HVM. Es importante tener en cuenta que los tipos de instancias de la generación actual no admiten AMI PV. Por lo tanto, la elección de un tipo de instancia HVM brinda mejor rendimiento y compatibilidad con el hardware moderno.

Para obtener más información, consulte Tipos de virtualización de AMI de Linux.

> **Note**
>
> Los resultados de esta verificación se actualizan automáticamente varias veces al día y no se permiten las solicitudes de actualización. Puede que los cambios tarden unas horas en aparecer. Actualmente, no puede excluir recursos de esta verificación.

ID de la verificación

`c18d2gz148`

Origen

AWS Config Regla administrada: ec2-paravirtual-instance-check

Criterios de alerta

Amarillo: el tipo de virtualización de las instancias de Amazon EC2 es paravirtual.

Acción recomendada

Utilice la virtualización HVM para sus instancias de Amazon EC2 y utilice un tipo de instancia compatible.

Para obtener información acerca de cómo elegir el tipo de virtualización adecuado, consulte Compatibilidad para cambiar el tipo de instancia.

Recursos adicionales

Compatibilidad para cambiar el tipo de instancia

Columnas de informes

- Status
- Región

- Recurso
- AWS Config Regla
- Parámetros de entrada
- Hora de la última actualización

Límite máximo de memoria de Amazon ECS

Descripción

Comprueba si las definiciones de tareas de Amazon ECS tienen un límite de memoria establecido para las definiciones de contenedor. La cantidad total de memoria reservada para todos los contenedores dentro de una tarea debe ser menor que el valor de memoria de la tarea.

Para obtener más información, consulte Definiciones de contenedor.

> **Note**
>
> Los resultados de esta verificación se actualizan automáticamente varias veces al día y no se permiten las solicitudes de actualización. Puede que los cambios tarden unas horas en aparecer. Actualmente, no puede excluir recursos de esta verificación.

ID de la verificación

`c18d2gz176`

Origen

AWS Config Regla gestionada: ecs-task-definition-memory -hard-limit

Criterios de alerta

Amarillo: el límite máximo de memoria de Amazon ECS no está establecido.

Acción recomendada

Asigne memoria a sus tareas de Amazon ECS para evitar quedarse sin memoria. Si el contenedor intenta superar la memoria especificada, el contenedor se termina.

Para obtener más información, consulte ¿Cómo puedo asignar memoria a tareas en Amazon ECS?.

Recursos adicionales

Reserva de clúster

Columnas de informes

- Status
- Región
- Recurso
- AWS Config Regla
- Parámetros de entrada
- Hora de la última actualización

Optimización del modo de rendimiento de Amazon EFS

Descripción

Comprueba si el sistema de archivos de Amazon EFS del cliente está configurado actualmente para utilizar el modo de rendimiento por ráfagas.

Los sistemas de archivos con el modo de rendimiento por ráfaga de EFS [1] ofrecen un nivel básico y constante de rendimiento (50 KiB/s por GiB de datos en el almacenamiento estándar de EFS) y utilizan un modelo de créditos para ofrecer niveles más altos de “rendimiento por ráfagas” cuando hay “créditos de ráfagas” disponibles. Cuando los créditos de ráfaga se agotan, el rendimiento del sistema de archivos se limita a este nivel básico inferior, lo que puede provocar lentitud, tiempos de espera u otras formas de impacto en el rendimiento de las aplicaciones o los usuarios finales.

ID de la verificación

`c1dfprch02`

Criterios de alerta

- Amarillo: el sistema de archivos utiliza el modo de rendimiento por ráfaga.

Acción recomendada

Para permitir que los usuarios y las aplicaciones logren el rendimiento deseado, se recomienda actualizar la configuración del sistema de archivos al modo de rendimiento elástico [2]. Cuando se configura el modo de rendimiento elástico, el sistema de archivos puede alcanzar hasta 10 GiB/s de rendimiento de lectura o 3 GiB/s de rendimiento de escritura, según la región de AWS

[3], y usted solo paga por el rendimiento que utiliza. Tenga en cuenta que puede actualizar la configuración del sistema de archivos para cambiar entre los modos de rendimiento elástico y por ráfaga cuando lo desee, y que los sistemas de archivos en modo de rendimiento elástico generan cargos adicionales por la transferencia de datos [4].

Recursos adicionales

- [1] Modos de rendimiento de Amazon EFS
- [2] Modo de rendimiento elástico de Amazon EFS
- [3] Cuotas y límites de Amazon EFS
- [4] Precios de Amazon EFS

Columnas de informes

- Status
- Región
- ID del sistema de archivos de EFS
- Modo de rendimiento
- Hora de la última actualización

El parámetro de autovacuum de Amazon RDS está desactivado

Descripción

El parámetro autovacuum está desactivado en sus instancias de base de datos. Desactivar autovacuum aumenta la sobrecarga de la tabla y del índice y afecta al rendimiento.

Le recomendamos que active autovacuum en sus grupos de parámetros de base de datos.

> **Note**
>
> Los resultados de esta verificación se actualizan automáticamente varias veces al día y no se permiten las solicitudes de actualización. Puede que los cambios tarden unas horas en aparecer. Actualmente, no puede excluir recursos de esta verificación.

> **Note**
>
> Cuando se detiene una instancia de base de datos o un clúster de base de datos, puede ver las recomendaciones de Amazon RDS en un plazo Trusted Advisor de 3

a 5 días. Transcurridos cinco días, las recomendaciones no estarán disponibles en Trusted Advisor. Para ver las recomendaciones, abra la consola de Amazon RDS y, a continuación, seleccione Recomendaciones.
Si elimina una instancia de base de datos o un clúster de base de datos, las recomendaciones asociadas a esas instancias o clústeres no estarán disponibles en Trusted Advisor la consola de administración de Amazon RDS.

ID de la verificación

`c1qf5bt025`

Criterios de alerta

Amarillo: los grupos de parámetros de base de datos tienen la aspiradora automática desactivada.

Acción recomendada

Active el parámetro autovacuum en sus grupos de parámetros de la base de datos.

Recursos adicionales

La base de datos PostgreSQL requiere un mantenimiento periódico, lo que se conoce como aspiración. Autovacuum en PostgreSQL automatiza la ejecución de los comandos VACCUUM y ANALYZE. Este proceso recopila las estadísticas de la tabla y elimina las filas muertas. Cuando la aspiradora automática está desactivada, el aumento de la tabla, la saturación del índice y las estadísticas obsoletas repercuten en el rendimiento de la base de datos.

Para obtener más información, consulte Descripción del autovacuum en entornos de Amazon RDS for PostgreSQL.

Columnas de informes

- Status
- Región
- Recurso
- Nombre del parámetro
- Valor recomendado
- Hora de la última actualización

Los clústeres de bases de datos de Amazon RDS solo admiten un volumen de hasta 64 TiB

Descripción

Sus clústeres de base de datos admiten volúmenes de hasta 64 TiB Las últimas versiones del motor admiten volúmenes de hasta 128 TiB. Le recomendamos que actualice la versión de motor del clúster de base de datos a las versiones más recientes para admitir volúmenes de hasta 128 TiB.

> **Note**
>
> Los resultados de esta verificación se actualizan automáticamente varias veces al día y no se permiten las solicitudes de actualización. Puede que los cambios tarden unas horas en aparecer. Actualmente, no puede excluir recursos de esta verificación.

> **Note**
>
> Cuando se detiene una instancia de base de datos o un clúster de base de datos, puede ver las recomendaciones de Amazon RDS en un plazo Trusted Advisor de 3 a 5 días. Transcurridos cinco días, las recomendaciones no estarán disponibles en Trusted Advisor. Para ver las recomendaciones, abra la consola de Amazon RDS y, a continuación, seleccione Recomendaciones.
> Si elimina una instancia de base de datos o un clúster de base de datos, las recomendaciones asociadas a esas instancias o clústeres no estarán disponibles en Trusted Advisor la consola de administración de Amazon RDS.

ID de la verificación

`c1qf5bt017`

Criterios de alerta

Amarillo: los clústeres de bases de datos solo admiten volúmenes de hasta 64 TiB.

Acción recomendada

Actualice la versión del motor de su clúster de base de datos para que admita volúmenes de hasta 128 TiB.

Recursos adicionales

Al ampliar la aplicación en un único clúster de base de datos de Amazon Aurora, es posible que no alcance el límite si el límite de almacenamiento es de 128 TiB. El aumento del límite de almacenamiento ayuda a evitar la eliminación de los datos o la división de la base de datos en varias instancias.

Para obtener más información, consulte los límites de tamaño de Amazon Aurora.

Columnas de informes

- Status
- Región
- Recurso
- Nombre del motor
- Versión del motor actual
- Valor recomendado
- Hora de la última actualización

Instancias de base de datos de Amazon RDS en los clústeres con clases de instancias heterogéneas

Descripción

Le recomendamos que utilice la misma clase de instancia de base de datos para todas las instancias de base de datos en su clúster de base de datos.

> **Note**
>
> Los resultados de esta verificación se actualizan automáticamente varias veces al día y no se permiten las solicitudes de actualización. Puede que los cambios tarden unas horas en aparecer. Actualmente, no puede excluir recursos de esta verificación.

> **Note**
>
> Cuando se detiene una instancia de base de datos o un clúster de base de datos, puede ver las recomendaciones de Amazon RDS en un plazo Trusted Advisor de 3

a 5 días. Transcurridos cinco días, las recomendaciones no estarán disponibles en Trusted Advisor. Para ver las recomendaciones, abra la consola de Amazon RDS y, a continuación, seleccione Recomendaciones.
Si elimina una instancia de base de datos o un clúster de base de datos, las recomendaciones asociadas a esas instancias o clústeres no estarán disponibles en Trusted Advisor la consola de administración de Amazon RDS.

ID de la verificación

`c1qf5bt009`

Criterios de alerta

Rojo: los clústeres de bases de datos tienen las instancias de base de datos con clases de instancias heterogéneas.

Acción recomendada

Utilice la misma clase y tamaño de instancia de base de datos para todas las instancias de base de datos del clúster de base de datos.

Recursos adicionales

Cuando las instancias de base de datos de su clúster de base de datos utilizan clases o tamaños de instancias de base de datos diferentes, puede producirse un desequilibrio en la carga de trabajo de las instancias de base de datos. Durante una conmutación por error, una de las instancias de base de datos de lectura pasa a ser una instancia de base de datos de escritura. Si las instancias de base de datos utilizan la misma clase y tamaño de instancia de base de datos, la carga de trabajo se puede equilibrar para las instancias de base de datos de su clúster de base de datos.

Para obtener más información, consulte Réplicas de Aurora.

Columnas de informes

- Status
- Región
- Recurso
- Valor recomendado
- Nombre del motor
- Hora de la última actualización

Instancias de base de datos de Amazon RDS en los clústeres con tamaños de instancia heterogéneos

Descripción

Le recomendamos que utilice la misma clase de instancia de base de datos para todas las instancias de base de datos en su clúster de base de datos.

> **Note**
>
> Los resultados de esta verificación se actualizan automáticamente varias veces al día y no se permiten las solicitudes de actualización. Puede que los cambios tarden unas horas en aparecer. Actualmente, no puede excluir recursos de esta verificación.

> **Note**
>
> Cuando se detiene una instancia de base de datos o un clúster de base de datos, puede ver las recomendaciones de Amazon RDS en un plazo Trusted Advisor de 3 a 5 días. Transcurridos cinco días, las recomendaciones no estarán disponibles en Trusted Advisor. Para ver las recomendaciones, abra la consola de Amazon RDS y, a continuación, seleccione Recomendaciones.
> Si elimina una instancia de base de datos o un clúster de base de datos, las recomendaciones asociadas a esas instancias o clústeres no estarán disponibles en Trusted Advisor la consola de administración de Amazon RDS.

ID de la verificación

`c1qf5bt008`

Criterios de alerta

Rojo: los clústeres de bases de datos tienen instancias de base de datos con tamaños de instancia heterogéneos.

Acción recomendada

Utilice la misma clase y tamaño de instancia de base de datos para todas las instancias de base de datos del clúster de base de datos.

Recursos adicionales

Cuando las instancias de base de datos de su clúster de base de datos utilizan diferentes clases o tamaños de instancias de base de datos, puede producirse un desequilibrio en la carga de trabajo de las instancias de base de datos. Durante una conmutación por error, una de las instancias de base de datos de lectura pasa a ser una instancia de base de datos de escritura. Si las instancias de base de datos utilizan la misma clase y tamaño de instancia de base de datos, la carga de trabajo se puede equilibrar para las instancias de base de datos de su clúster de base de datos.

Para obtener más información, consulte Réplicas de Aurora.

Columnas de informes

- Status
- Región
- Recurso
- Valor recomendado
- Nombre del motor
- Hora de la última actualización

Los parámetros de memoria de base de datos de Amazon RDS difieren de los predeterminados

Descripción

Los parámetros de memoria de las instancias de base de datos difieren considerablemente de los valores predeterminados. Esta configuración puede afectar al rendimiento y provocar errores.

Recomendamos restablecer los parámetros de memoria personalizados para la instancia de base de datos a sus valores predeterminados en el grupo de parámetros de la base de datos.

> **Note**
>
> Los resultados de esta verificación se actualizan automáticamente varias veces al día y no se permiten las solicitudes de actualización. Puede que los cambios tarden unas horas en aparecer. Actualmente, no puede excluir recursos de esta verificación.

> **Note**
>
> Cuando se detiene una instancia de base de datos o un clúster de base de datos, puede ver las recomendaciones de Amazon RDS en un plazo Trusted Advisor de 3 a 5 días. Transcurridos cinco días, las recomendaciones no estarán disponibles en Trusted Advisor. Para ver las recomendaciones, abra la consola de Amazon RDS y, a continuación, seleccione Recomendaciones.
> Si elimina una instancia de base de datos o un clúster de base de datos, las recomendaciones asociadas a esas instancias o clústeres no estarán disponibles en Trusted Advisor la consola de administración de Amazon RDS.

ID de la verificación

`c1qf5bt020`

Criterios de alerta

Amarillo: los grupos de parámetros de base de datos tienen parámetros de memoria que difieren considerablemente de los valores predeterminados.

Acción recomendada

Restablezca los parámetros de memoria a sus valores predeterminados.

Recursos adicionales

Para obtener más información, consulte Best practices for configuring parameters for Amazon RDS for MySQL, part 1: Parameters related to performance.

Columnas de informes

- Status
- Región
- Recurso
- Nombre del parámetro
- Valor recomendado
- Hora de la última actualización

El parámetro enable_indexonlyscan de Amazon RDS está desactivado

Descripción

El planificador u optimizador de consultas no puede usar el plan de análisis de solo índice si está desactivado.

Se recomienda establecer el valor del parámetro enable_indexonlyscan en 1.

> **Note**
>
> Los resultados de esta verificación se actualizan automáticamente varias veces al día y no se permiten las solicitudes de actualización. Puede que los cambios tarden unas horas en aparecer. Actualmente, no puede excluir recursos de esta verificación.

> **Note**
>
> Cuando se detiene una instancia de base de datos o un clúster de base de datos, puede ver las recomendaciones de Amazon RDS en un plazo Trusted Advisor de 3 a 5 días. Transcurridos cinco días, las recomendaciones no estarán disponibles en Trusted Advisor. Para ver las recomendaciones, abra la consola de Amazon RDS y, a continuación, seleccione Recomendaciones.
> Si elimina una instancia de base de datos o un clúster de base de datos, las recomendaciones asociadas a esas instancias o clústeres no estarán disponibles en Trusted Advisor la consola de administración de Amazon RDS.

ID de la verificación

`c1qf5bt028`

Criterios de alerta

Amarillo: los grupos de parámetros de base de datos tienen el parámetro enable_indexonlyscan desactivado.

Acción recomendada

Establezca el parámetro enable_indexonlyscan en 1.

Recursos adicionales

Al desactivar el parámetro enable_indexonlyscan, se impide que el planificador de consultas seleccione un plan de ejecución óptimo. El planificador de consultas utiliza un tipo de plan diferente, como el escaneo de índices, que puede aumentar el coste de la consulta y el tiempo de ejecución. El tipo de plan de escaneo solo con índices recupera los datos sin acceder a los datos de la tabla.

Para obtener más información, consulte enable_indexonlyscan (boolean) en el sitio web de documentación de PostgreSQL.

Columnas de informes

- Status
- Región
- Recurso
- Nombre del parámetro
- Valor recomendado
- Hora de la última actualización

El parámetro enable_indexscan de Amazon RDS está desactivado

Descripción

El planificador u optimizador de consultas no puede usar el plan de análisis de índice si está desactivado.

Se recomienda establecer el valor del parámetro enable_indexscan en 1.

> **Note**
>
> Los resultados de esta verificación se actualizan automáticamente varias veces al día y no se permiten las solicitudes de actualización. Puede que los cambios tarden unas horas en aparecer. Actualmente, no puede excluir recursos de esta verificación.

> **Note**
>
> Cuando se detiene una instancia de base de datos o un clúster de base de datos, puede ver las recomendaciones de Amazon RDS en un plazo Trusted Advisor de 3 a 5 días. Transcurridos cinco días, las recomendaciones no estarán disponibles en Trusted Advisor. Para ver las recomendaciones, abra la consola de Amazon RDS y, a continuación, seleccione Recomendaciones.
> Si elimina una instancia de base de datos o un clúster de base de datos, las recomendaciones asociadas a esas instancias o clústeres no estarán disponibles en Trusted Advisor la consola de administración de Amazon RDS.

ID de la verificación

`c1qf5bt029`

Criterios de alerta

Amarillo: los grupos de parámetros de base de datos tienen el parámetro enable_indexscan desactivado.

Acción recomendada

Establezca el parámetro enable_indexscan en 1.

Recursos adicionales

Al desactivar el parámetro enable_indexscan, se impide que el planificador de consultas seleccione un plan de ejecución óptimo. El planificador de consultas utiliza un tipo de plan diferente, como el escaneo de índices, que puede aumentar el coste de la consulta y el tiempo de ejecución.

Para obtener más información, consulte enable_indexscan (boolean) en el sitio web de documentación de PostgreSQL.

Columnas de informes

- Status
- Región
- Recurso
- Nombre del parámetro
- Valor recomendado

- Hora de la última actualización

El parámetro general_logging de Amazon RDS está activado

Descripción

El registro general está activado para su instancia de base de datos. Esta configuración es útil para solucionar los problemas de la base de datos. Sin embargo, la activación del registro general aumenta la cantidad de operaciones de E/S y el espacio de almacenamiento asignado, lo que puede provocar problemas de contención y una degradación del rendimiento.

Compruebe sus requisitos para el uso del registro general. Se recomienda establecer el valor del parámetro general_logging en 0.

> **Note**
>
> Los resultados de esta verificación se actualizan automáticamente varias veces al día y no se permiten las solicitudes de actualización. Puede que los cambios tarden unas horas en aparecer. Actualmente, no puede excluir recursos de esta verificación.

> **Note**
>
> Cuando se detiene una instancia de base de datos o un clúster de base de datos, puede ver las recomendaciones de Amazon RDS en un plazo Trusted Advisor de 3 a 5 días. Transcurridos cinco días, las recomendaciones no estarán disponibles en Trusted Advisor. Para ver las recomendaciones, abra la consola de Amazon RDS y, a continuación, seleccione Recomendaciones.
> Si elimina una instancia de base de datos o un clúster de base de datos, las recomendaciones asociadas a esas instancias o clústeres no estarán disponibles en Trusted Advisor la consola de administración de Amazon RDS.

ID de la verificación

`c1qf5bt037`

Criterios de alerta

Amarillo: los grupos de parámetros de base de datos tienen activado general_logging.

Acción recomendada

Compruebe sus requisitos para el uso del registro general. Si no es obligatorio, se recomienda establecer el valor del parámetro general_logging en 0.

Recursos adicionales

El registro de consultas general se activa cuando el valor del parámetro general_logging es 1. El registro de consultas general contiene registros de las operaciones del servidor de la base de datos. El servidor escribe información en este registro cuando los clientes se conectan o se desconectan y los registros contienen cada sentencia SQL recibida de los clientes. El registro de consultas general resulta útil cuando se sospecha que se ha producido un error en un cliente y se desea buscar la información que el cliente va a enviar al servidor de la base de datos.

Para obtener más información, consulte Descripción general de los registros de bases de datos de RDS para MySQL.

Columnas de informes

- Status
- Región
- Recurso
- Nombre del parámetro
- Valor recomendado
- Hora de la última actualización

Parámetro InnoDB_change_buffering de Amazon RDS que utiliza un valor inferior al óptimo

Descripción

El cambio de almacenamiento en búfer permite a una instancia de base de datos de MySQL aplazar algunas escrituras necesarias para mantener los índices secundarios. Esta característica era útil en entornos con discos lentos. El cambio en la configuración del almacenamiento en búfer mejoró ligeramente el rendimiento de la base de datos, pero provocó un retardo en la recuperación tras un fallo y prolongó los tiempos de apagado durante la actualización.

Se recomienda establecer el valor del parámetro innodb_change_buffering en NONE.

> **Note**
>
> Los resultados de esta verificación se actualizan automáticamente varias veces al día y no se permiten las solicitudes de actualización. Puede que los cambios tarden unas horas en aparecer. Actualmente, no puede excluir recursos de esta verificación.

> **Note**
>
> Cuando se detiene una instancia de base de datos o un clúster de base de datos, puede ver las recomendaciones de Amazon RDS en un plazo Trusted Advisor de 3 a 5 días. Transcurridos cinco días, las recomendaciones no estarán disponibles en Trusted Advisor. Para ver las recomendaciones, abra la consola de Amazon RDS y, a continuación, seleccione Recomendaciones.
> Si elimina una instancia de base de datos o un clúster de base de datos, las recomendaciones asociadas a esas instancias o clústeres no estarán disponibles en Trusted Advisor la consola de administración de Amazon RDS.

ID de la verificación

`c1qf5bt021`

Criterios de alerta

Amarillo: los grupos de parámetros de base de datos tienen el parámetro innodb_change_buffering establecido en un valor óptimo bajo.

Acción recomendada

Defina el valor del parámetro innodb_change_buffering en NONE en sus grupos de parámetros de base de datos.

Recursos adicionales

Para obtener más información, consulte Best practices for configuring parameters for Amazon RDS for MySQL, part 1: Parameters related to performance.

Columnas de informes

- Status
- Región

- Recurso
- Nombre del parámetro
- Valor recomendado
- Hora de la última actualización

El parámetro innodb_open_files de Amazon RDS es bajo

Descripción

El parámetro innodb_open_files controla el número de archivos que InnoDB puede abrir a la vez. InnoDB abre todos los archivos de registro y de espacio de tablas del sistema cuando se ejecuta mysqld.

Su instancia de base de datos tiene un valor bajo para la cantidad máxima de archivos que InnoDB puede abrir a la vez. Se recomienda establecer el parámetro innodb_open_files en un valor mínimo de 65.

> **Note**
>
> Los resultados de esta verificación se actualizan automáticamente varias veces al día y no se permiten las solicitudes de actualización. Puede que los cambios tarden unas horas en aparecer. Actualmente, no puede excluir recursos de esta verificación.

> **Note**
>
> Cuando se detiene una instancia de base de datos o un clúster de base de datos, puede ver las recomendaciones de Amazon RDS en un plazo Trusted Advisor de 3 a 5 días. Transcurridos cinco días, las recomendaciones no estarán disponibles en Trusted Advisor. Para ver las recomendaciones, abra la consola de Amazon RDS y, a continuación, seleccione Recomendaciones.
> Si elimina una instancia de base de datos o un clúster de base de datos, las recomendaciones asociadas a esas instancias o clústeres no estarán disponibles en Trusted Advisor la consola de administración de Amazon RDS.

ID de la verificación

`c1qf5bt033`

Criterios de alerta

Amarillo: los grupos de parámetros de base de datos tienen mal configurada la configuración de abrir archivos de InnoDB.

Acción recomendada

Establezca el parámetro innodb_open_files en un valor mínimo de 65.

Recursos adicionales

El parámetro innodb_open_files controla el número de archivos que InnoDB puede abrir a la vez. InnoDB mantiene abiertos todos los archivos de registro y los archivos del espacio de tablas del sistema cuando se ejecuta mysqld. InnoDB también necesita abrir algunos archivos.ibd, si se utiliza el modelo de file-per-table almacenamiento. Cuando la configuración de innodb_open_files es baja, esto afecta al rendimiento de la base de datos y es posible que el servidor no se inicie.

Para obtener más información, consulte Opciones de inicio y variables de sistema de InnoDB: innodb_open_files en el sitio web de documentación. MySql

Columnas de informes

- Status
- Región
- Recurso
- Nombre del parámetro
- Valor recomendado
- Hora de la última actualización

El parámetro innodb_stats_persistent de Amazon RDS está desactivado

Descripción

Su instancia de base de datos no está configurada para conservar las estadísticas de InnoDB en el disco. Cuando las estadísticas no están almacenadas, se vuelven a calcular cada vez que la instancia se reinicia y se accede a la tabla. Esto provoca variaciones en el plan de ejecución de las consultas. Puede modificar el valor de este parámetro global a nivel de tabla.

Se recomienda establecer el valor del parámetro innodb_stats_persistent en ON.

> **Note**
>
> Los resultados de esta verificación se actualizan automáticamente varias veces al día y no se permiten las solicitudes de actualización. Puede que los cambios tarden unas horas en aparecer. Actualmente, no puede excluir recursos de esta verificación.

> **Note**
>
> Cuando se detiene una instancia de base de datos o un clúster de base de datos, puede ver las recomendaciones de Amazon RDS en un plazo Trusted Advisor de 3 a 5 días. Transcurridos cinco días, las recomendaciones no estarán disponibles en Trusted Advisor. Para ver las recomendaciones, abra la consola de Amazon RDS y, a continuación, seleccione Recomendaciones.
> Si elimina una instancia de base de datos o un clúster de base de datos, las recomendaciones asociadas a esas instancias o clústeres no estarán disponibles en Trusted Advisor la consola de administración de Amazon RDS.

ID de la verificación

`c1qf5bt032`

Criterios de alerta

Amarillo: los grupos de parámetros de base de datos tienen estadísticas del optimizador que no se conservan en el disco.

Acción recomendada

Establezca el valor del parámetro innodb_stats_persistent en ON.

Recursos adicionales

Si el parámetro innodb_stats_persistent está establecido en ON, las estadísticas del optimizador se conservan cuando se reinicia la instancia. Esto mejora la estabilidad del plan de ejecución y el rendimiento uniforme de las consultas. Puede modificar la persistencia de las estadísticas globales a nivel de tabla mediante la cláusula STATS_PERSISTENT al crear o modificar una tabla.

Para obtener más información, consulte Best practices for configuring parameters for Amazon RDS for MySQL, part 1: Parameters related to performance.

Columnas de informes

- Status
- Región
- Recurso
- Nombre del parámetro
- Valor recomendado
- Hora de la última actualización

Instancia de Amazon RDS con aprovisionamiento insuficiente para la capacidad del sistema

Descripción

Comprueba si la instancia de Amazon RDS o la instancia de base de datos de Amazon Aurora tienen la capacidad de sistema necesaria para funcionar.

ID de la verificación

`c1qf5bt039`

Criterios de alerta

Amarillo:

Muertes por falta de memoria: cuando un proceso en el host de la base de datos se detiene debido a una reducción de la memoria a nivel del sistema operativo, el contador de muertes por falta de memoria (OOM) aumenta.

Intercambio excesivo: los valores de las métricas os.memory.swap.in y os.memory.swap.out eran altos.

Acción recomendada

Se recomienda ajustar las consultas para utilizar menos memoria o utilizar un tipo de instancia de base de datos con mayor memoria asignada. Cuando la instancia se queda sin memoria, esto afecta al rendimiento de la base de datos.

Recursos adicionales

No ut-of-memory se detectaron errores: el kernel de Linux invoca el asesino por falta de memoria (OOM) cuando los procesos que se ejecutan en el host requieren más memoria que la disponible físicamente en el sistema operativo. En este caso, el OOM Killer revisa todos los procesos en ejecución y detiene uno o más procesos para liberar memoria del sistema y mantenerlo en funcionamiento.

Se detecta un intercambio: cuando no hay suficiente memoria en el host de la base de datos, el sistema operativo envía al disco del espacio de intercambio unas cuantas páginas utilizadas como mínimo. Este proceso de descarga afecta al rendimiento de la base de datos.

Para obtener más información, consulte Tipos de instancias de Amazon RDS y Escalado de su instancia de Amazon RDS.

Columnas de informes

- Status
- Región
- Recurso
- O ut-of-memory habilidades (recuento)
- Intercambio excesivo (recuento)
- Último período de detección
- Hora de la última actualización

El volumen magnético Amazon RDS está en uso

Descripción

Sus instancias de base de datos utilizan el almacenamiento magnético. El almacenamiento magnético no se recomienda para la mayoría de las instancias de base de datos. Elija un tipo de almacenamiento diferente: de uso general (SSD) o IOPS aprovisionadas.

> **Note**
>
> Los resultados de esta verificación se actualizan automáticamente varias veces al día y no se permiten las solicitudes de actualización. Puede que los cambios tarden unas horas en aparecer. Actualmente, no puede excluir recursos de esta verificación.

> **Note**
>
> Cuando se detiene una instancia de base de datos o un clúster de base de datos, puede ver las recomendaciones de Amazon RDS en un plazo Trusted Advisor de 3 a 5 días. Transcurridos cinco días, las recomendaciones no estarán disponibles en Trusted Advisor. Para ver las recomendaciones, abra la consola de Amazon RDS y, a continuación, seleccione Recomendaciones.
> Si elimina una instancia de base de datos o un clúster de base de datos, las recomendaciones asociadas a esas instancias o clústeres no estarán disponibles en Trusted Advisor la consola de administración de Amazon RDS.

ID de la verificación

`c1qf5bt000`

Criterios de alerta

Amarillo: los recursos de Amazon RDS utilizan almacenamiento magnético.

Acción recomendada

Elija un tipo de almacenamiento diferente: de uso general (SSD) o IOPS aprovisionadas.

Recursos adicionales

El almacenamiento magnético es un tipo de almacenamiento de una generación anterior. El tipo de almacenamiento recomendado para los nuevos requisitos de almacenamiento es el de uso general (SSD) o las IOPS aprovisionadas. Estos tipos de almacenamiento proporcionan un rendimiento superior y uniforme y opciones de tamaño de almacenamiento mejoradas.

Para obtener más información, consulte Volúmenes de generaciones anteriores.

Columnas de informes

- Status
- Región
- Recurso
- Valor recomendado
- Nombre del motor
- Hora de la última actualización

Los grupos de parámetros de Amazon RDS no utilizan páginas enormes

Descripción

Las páginas grandes pueden aumentar la escalabilidad de la base de datos, pero la instancia de base de datos no utiliza páginas grandes. Le recomendamos que establezca el valor del parámetro use_large_pages en SOLO en el grupo de parámetros de base de datos de su instancia de base de datos.

> **Note**
>
> Los resultados de esta verificación se actualizan automáticamente varias veces al día y no se permiten las solicitudes de actualización. Puede que los cambios tarden unas horas en aparecer. Actualmente, no puede excluir recursos de esta verificación.

> **Note**
>
> Cuando se detiene una instancia de base de datos o un clúster de base de datos, puede ver las recomendaciones de Amazon RDS en un plazo Trusted Advisor de 3 a 5 días. Transcurridos cinco días, las recomendaciones no estarán disponibles en Trusted Advisor. Para ver las recomendaciones, abra la consola de Amazon RDS y, a continuación, seleccione Recomendaciones.
> Si elimina una instancia de base de datos o un clúster de base de datos, las recomendaciones asociadas a esas instancias o clústeres no estarán disponibles en Trusted Advisor la consola de administración de Amazon RDS.

ID de la verificación

`c1qf5bt024`

Criterios de alerta

Amarillo: los grupos de parámetros de base de datos no utilizan páginas grandes.

Acción recomendada

Establezca el valor del parámetro use_large_pages en SOLO en sus grupos de parámetros de base de datos.

Recursos adicionales

Para obtener más información, consulte Cómo activar una instancia de RDS HugePages para Oracle.

Columnas de informes

- Status
- Región
- Recurso
- Nombre del parámetro
- Valor recomendado
- Hora de la última actualización

El parámetro de caché de consultas de Amazon RDS está activado

Descripción

Cuando los cambios requieran que se purgue la caché de consultas, parecerá que la instancia de base de datos se ha bloqueado. La mayoría de las cargas de trabajo no se benefician de una caché de consultas. La caché de consultas se quitó de la versión 8.0 de MySQL. Es recomendable que establezca el parámetro query_cache_type en 0.

> **Note**
>
> Los resultados de esta verificación se actualizan automáticamente varias veces al día y no se permiten las solicitudes de actualización. Puede que los cambios tarden unas horas en aparecer. Actualmente, no puede excluir recursos de esta verificación.

> **Note**
>
> Cuando se detiene una instancia de base de datos o un clúster de base de datos, puede ver las recomendaciones de Amazon RDS en un plazo Trusted Advisor de 3 a 5 días. Transcurridos cinco días, las recomendaciones no estarán disponibles en Trusted Advisor. Para ver las recomendaciones, abra la consola de Amazon RDS y, a continuación, seleccione Recomendaciones.

Si elimina una instancia de base de datos o un clúster de base de datos, las recomendaciones asociadas a esas instancias o clústeres no estarán disponibles en Trusted Advisor la consola de administración de Amazon RDS.

ID de la verificación

`c1qf5bt022`

Criterios de alerta

Amarillo: los grupos de parámetros de base de datos tienen la caché de consultas activada.

Acción recomendada

Defina el valor del parámetro query_cache_type en 0 en sus grupos de parámetros de base de datos.

Recursos adicionales

Para obtener más información, consulte Best practices for configuring parameters for Amazon RDS for MySQL, part 1: Parameters related to performance.

Columnas de informes

- Status
- Región
- Recurso
- Nombre del parámetro
- Valor recomendado
- Hora de la última actualización

Es necesaria la actualización de la clase de instancia de Amazon RDS Resources

Descripción

La base de datos ejecuta una clase de instancia de base de datos de la generación anterior. Hemos sustituido las clases de instancias de base de datos de una generación anterior por clases de instancias de base de datos con mejor coste o rendimiento, o ambos. Le recomendamos que ejecute su instancia de base de datos con una clase de instancia de base de datos de una generación más reciente.

> **Note**
>
> Los resultados de esta verificación se actualizan automáticamente varias veces al día y no se permiten las solicitudes de actualización. Puede que los cambios tarden unas horas en aparecer. Actualmente, no puede excluir recursos de esta verificación.

> **Note**
>
> Cuando se detiene una instancia de base de datos o un clúster de base de datos, puede ver las recomendaciones de Amazon RDS en un plazo Trusted Advisor de 3 a 5 días. Transcurridos cinco días, las recomendaciones no estarán disponibles en Trusted Advisor. Para ver las recomendaciones, abra la consola de Amazon RDS y, a continuación, seleccione Recomendaciones.
> Si elimina una instancia de base de datos o un clúster de base de datos, las recomendaciones asociadas a esas instancias o clústeres no estarán disponibles en Trusted Advisor la consola de administración de Amazon RDS.

ID de la verificación

`c1qf5bt015`

Criterios de alerta

Rojo: las instancias de base de datos utilizan una clase de instancia de base de datos que ha llegado al final del soporte.

Acción recomendada

Actualice a la última clase de instancia de base de datos.

Recursos adicionales

Para obtener más información, consulte Motores de base de datos compatibles para clases de instancia de base de datos.

Columnas de informes

- Status
- Región

- Recurso
- Clase de instancia de base de datos
- Valor recomendado
- Nombre del motor
- Hora de la última actualización

Recursos de Amazon RDS: es necesaria la actualización de las versiones principales

Descripción

No se admiten las bases de datos con la versión principal actual del motor de base de datos. Le recomendamos que actualice a la última versión principal, que incluye nuevas funciones y mejoras.

> **Note**
>
> Los resultados de esta verificación se actualizan automáticamente varias veces al día y no se permiten las solicitudes de actualización. Puede que los cambios tarden unas horas en aparecer. Actualmente, no puede excluir recursos de esta verificación.

> **Note**
>
> Cuando se detiene una instancia de base de datos o un clúster de base de datos, puede ver las recomendaciones de Amazon RDS en un plazo Trusted Advisor de 3 a 5 días. Transcurridos cinco días, las recomendaciones no estarán disponibles en Trusted Advisor. Para ver las recomendaciones, abra la consola de Amazon RDS y, a continuación, seleccione Recomendaciones.
> Si elimina una instancia de base de datos o un clúster de base de datos, las recomendaciones asociadas a esas instancias o clústeres no estarán disponibles en Trusted Advisor la consola de administración de Amazon RDS.

ID de la verificación

`c1qf5bt014`

Criterios de alerta

Rojo: los recursos de RDS utilizan las versiones principales que ya no son compatibles.

Acción recomendada

Actualización a la versión principal más reciente del motor de base de datos.

Recursos adicionales

Amazon RDS lanza nuevas versiones de los motores de bases de datos compatibles para mantener sus bases de datos con la versión más reciente. Las nuevas versiones publicadas pueden incluir correcciones de errores, mejoras de seguridad y otras mejoras en el motor de base de datos. Puede minimizar el tiempo de inactividad necesario para la actualización de la instancia de base de datos mediante una implementación azul/verde.

Para obtener más información, consulte los siguientes recursos:

- Actualización de una versión del motor de instancias de base de datos
- Actualizaciones de Amazon Aurora
- Uso de Amazon RDS Blue/Green Deployments para actualizaciones de bases de datos

Columnas de informes

- Status
- Región
- Recurso
- Nombre del motor
- Versión actual del motor
- Valor recomendado
- Hora de la última actualización

Recursos de Amazon RDS que utilizan la edición de fin del motor de soporte con licencia incluida

Descripción

Le recomendamos que actualice la versión principal a la última versión del motor compatible con Amazon RDS para continuar con el soporte de licencia actual. La versión del motor de su base de datos no será compatible con la licencia actual.

> **Note**
>
> Los resultados de esta verificación se actualizan automáticamente varias veces al día y no se permiten las solicitudes de actualización. Puede que los cambios tarden unas horas en aparecer. Actualmente, no puede excluir recursos de esta verificación.

> **Note**
>
> Cuando se detiene una instancia de base de datos o un clúster de base de datos, puede ver las recomendaciones de Amazon RDS en un plazo Trusted Advisor de 3 a 5 días. Transcurridos cinco días, las recomendaciones no estarán disponibles en Trusted Advisor. Para ver las recomendaciones, abra la consola de Amazon RDS y, a continuación, seleccione Recomendaciones.
> Si elimina una instancia de base de datos o un clúster de base de datos, las recomendaciones asociadas a esas instancias o clústeres no estarán disponibles en Trusted Advisor la consola de administración de Amazon RDS.

ID de la verificación

`c1qf5bt016`

Criterios de alerta

Rojo: los recursos de Amazon RDS utilizan la edición del motor de fin de soporte con un modelo con licencia incluida.

Acción recomendada

Le recomendamos que actualice su base de datos a la última versión compatible de Amazon RDS para seguir utilizando el modelo con licencia.

Recursos adicionales

Para obtener más información, consulte las actualizaciones de las versiones principales de Oracle.

Columnas de informes

- Status
- Región

- Recurso
- Nombre del motor
- Versión del motor actual
- Valor recomendado
- Nombre del motor
- Hora de la última actualización

Conjuntos de registros de recursos de alias en Amazon Route 53

Descripción

Verifica los conjuntos de registros de recursos que se pueden cambiar a conjuntos de registros de recursos de alias para mejorar el rendimiento y ahorrar dinero.

Un conjunto de registros de recursos de alias enruta las consultas de DNS a un AWS recurso (por ejemplo, un balanceador de cargas de Elastic Load Balancing o un bucket de Amazon S3) o a otro conjunto de registros de recursos de Route 53. Cuando utilizas conjuntos de registros de recursos de alias, Route 53 enruta tus consultas de DNS a AWS los recursos de forma gratuita.

Las zonas alojadas creadas por AWS los servicios no aparecerán en los resultados de la comprobación.

ID de la verificación

`B913Ef6fb4`

Criterios de alerta

- Amarillo: un conjunto de registros de recursos es un CNAME para un sitio web de Amazon S3.
- Amarillo: un conjunto de registros de recursos es un CNAME para una CloudFront distribución de Amazon.
- Amarillo: un conjunto de registros de recursos es un CNAME para un equilibrador de carga de Elastic Load Balancing.

Acción recomendada

Reemplace los conjuntos de registros de recursos de CNAME enumerados por conjuntos de registros de recursos de alias; consulte Elección entre conjuntos de registros de recursos de alias y sin alias.

También debes cambiar el tipo de registro de CNAME a A o AAAA, según el recurso. AWS Consulte Valores que se especifican al crear o editar conjuntos de registros de recursos de Amazon Route 53.

Recursos adicionales

Enrutar las consultas a los recursos AWS

Columnas de informes

- Status
- Nombre de zona alojada
- ID de zona alojada
- Nombre de conjunto de registros de recursos
- Tipo de conjunto de registros de recursos
- Identificador de los conjuntos de registros de recursos
- Alias Target

Funciones AWS Lambda con falta de aprovisionamiento para el tamaño de la memoria

Descripción

Comprueba las AWS Lambda funciones que se invocaron al menos una vez durante el período retrospectivo. Esta comprobación le avisa si alguna de las funciones Lambda tuvo falta de aprovisionamiento para el tamaño de la memoria. Cuando tiene funciones Lambda con falta de aprovisionamiento para el tamaño de la memoria, estas funciones tardan más en completarse.

> **Note**
>
> Los resultados de esta verificación se actualizan automáticamente varias veces al día y no se permiten las solicitudes de actualización. Puede que los cambios tarden unas horas en aparecer. Actualmente, no puede excluir recursos de esta verificación.

ID de la verificación

`COr6dfpM06`

Criterios de alerta

Amarillo: una función de Lambda que se aprovisionó de forma insuficiente para el tamaño de la memoria durante el periodo retroactivo. Para determinar si una función de Lambda está insuficientemente aprovisionada, tenemos en cuenta todas las CloudWatch métricas predeterminadas de esa función. El algoritmo utilizado para identificar las funciones Lambda mal aprovisionadas en cuanto al tamaño de la memoria sigue las prácticas recomendadas. AWS El algoritmo se actualiza cuando se identifica un nuevo patrón.

Acción recomendada

Considere aumentar el tamaño de la memoria de las funciones de Lambda.

Para obtener más información, consulte Optar AWS Compute Optimizer por recibir Trusted Advisor cheques.

Columnas de informes

- Status
- Región
- Nombre de la función
- Versión de la función
- Tamaño de la memoria (MB)
- Tamaño de la memoria recomendado (MB)
- Periodo retroactivo (días)
- Riesgo de rendimiento
- Hora de la última actualización

AWS Lambda Funciones sin límite de simultaneidad configuradas

Descripción

Comprueba si AWS Lambda las funciones están configuradas con un límite de ejecución simultánea a nivel de función.

La simultaneidad es la cantidad de solicitudes en tránsito que la función de AWS Lambda administra al mismo tiempo. Para cada solicitud simultánea, Lambda aprovisiona una instancia independiente del entorno de ejecución.

Puede especificar el límite mínimo y máximo de simultaneidad mediante los parámetros de simultaneidad LimitLow y ConcurrencyLimitAlto de sus reglas. AWS Config

Para obtener más información, consulte Escalado de funciones de Lambda

> **Note**
>
> Los resultados de esta verificación se actualizan automáticamente varias veces al día y no se permiten las solicitudes de actualización. Puede que los cambios tarden unas horas en aparecer. Actualmente, no puede excluir recursos de esta verificación.

ID de la verificación

`c18d2gz181`

Origen

AWS Config Regla gestionada: lambda-concurrency-check

Criterios de alerta

Amarillo: la función de Lambda no tiene un límite de simultaneidad configurado.

Acción recomendada

Asegúrese de que las funciones de Lambda tengan configurada la simultaneidad. Un límite de simultaneidad para las funciones de Lambda ayuda a garantizar que la función procese las solicitudes de forma fiable y predecible. Un límite de simultaneidad reduce el riesgo de que la función se sature debido a un aumento repentino de tráfico.

Para obtener más información, consulte Configuración de la simultaneidad reservada.

Recursos adicionales

- Escalado de la función de Lambda
- Configuración de la simultaneidad reservada

Columnas de informes

- Status
- Región
- Recurso

- AWS Config Regla
- Parámetros de entrada
- Hora de la última actualización

Problemas de alto riesgo de AWS Well-Architected para el rendimiento

Descripción

Verifica si hay problemas de alto riesgo para las cargas de trabajo en el pilar de rendimiento. Esta verificación se basa en las revisiones de AWS-Well Architected. Los resultados de las verificaciones dependen de si ha completado la evaluación de la carga de trabajo con AWS Well-Architected.

> **Note**
>
> Los resultados de esta verificación se actualizan automáticamente varias veces al día y no se permiten las solicitudes de actualización. Puede que los cambios tarden unas horas en aparecer. Actualmente, no puede excluir recursos de esta verificación.

ID de la verificación

`Wxdfp4B1L2`

Criterios de alerta

- Rojo: Se identificó al menos un problema activo de alto riesgo en el pilar de rendimiento de AWS Well-Architected.
- Verde: No se detectó ningún problema activo de alto riesgo en el pilar de rendimiento de AWS Well-Architected.

Acción recomendada

AWS Well-Architected detectó problemas de alto riesgo durante la evaluación de la carga de trabajo. Estos problemas presentan oportunidades para reducir el riesgo y ahorrar dinero. Inicie sesión en la herramienta AWS Well-Architected para revisar las respuestas y tomar medidas para resolver los problemas activos.

Columnas de informes

- Status

- Región
- ARN de carga de trabajo
- Nombre de carga de trabajo
- Nombre del revisor
- Tipo de carga de trabajo
- Fecha de inicio de carga de trabajo
- Fecha de la última modificación de carga de trabajo
- Cantidad de HRI identificados para el rendimiento
- Cantidad de HRI resueltos para el rendimiento
- Cantidad de preguntas contestadas para el rendimiento
- Cantidad total de preguntas en el pilar de rendimiento
- Hora de la última actualización

CloudFront Nombres de dominio alternativos

Descripción

Comprueba CloudFront las distribuciones de Amazon en busca de nombres de dominio alternativos (CNAME) que tengan una configuración de DNS incorrecta.

Si una CloudFront distribución incluye nombres de dominio alternativos, la configuración de DNS de los dominios debe dirigir las consultas de DNS a esa distribución.

> **Note**
>
> Esta comprobación supone que el DNS de Amazon Route 53 y la CloudFront distribución de Amazon están configurados de la misma manera Cuenta de AWS. Por lo tanto, la lista de alertas podría incluir recursos que funcionan según lo esperado debido a la configuración de DNS fuera de esta Cuenta de AWS.

ID de la verificación

`N420c450f2`

Criterios de alerta

- Amarillo: una CloudFront distribución incluye nombres de dominio alternativos, pero la configuración de DNS no está configurada correctamente con un registro CNAME o un registro de recursos de alias de Amazon Route 53.
- Amarillo: una CloudFront distribución incluye nombres de dominio alternativos, pero no Trusted Advisor pudo evaluar la configuración de DNS porque había demasiados redireccionamientos.
- Amarillo: una CloudFront distribución incluye nombres de dominio alternativos, pero no ha Trusted Advisor podido evaluar la configuración de DNS por algún otro motivo, muy probablemente debido a un tiempo de espera.

Acción recomendada

Actualice la configuración de DNS para dirigir las consultas de DNS a la CloudFront distribución; consulte Uso de nombres de dominio alternativos (CNAME).

Si utiliza Amazon Route 53 como servicio de DNS, consulte Enrutamiento del tráfico a una distribución CloudFront web de Amazon mediante el uso de su nombre de dominio. Si la comprobación superó el tiempo de espera, intente actualizarla.

Recursos adicionales

Guía para CloudFront desarrolladores de Amazon

Columnas de informes

- Status
- ID de distribución
- Nombre de dominio de distribución
- Nombre de dominio alternativo
- Motivo

CloudFront Optimización de la entrega de contenido

Descripción

Comprueba los casos en los que la transferencia de datos desde los depósitos de Amazon Simple Storage Service (Amazon S3) podría acelerarse mediante CloudFront Amazon, AWS el servicio de entrega de contenido global.

Cuando se configura CloudFront para entregar su contenido, las solicitudes de contenido se redirigen automáticamente a la ubicación perimetral más cercana donde se almacena el contenido en caché. Este enrutamiento permite enviar contenido a los usuarios con el mejor rendimiento posible. Una alta proporción de datos transferidos al exterior en comparación con los datos almacenados en el depósito indica que te vendría bien utilizar Amazon CloudFront para entregar los datos.

ID de la verificación

`796d6f3D83`

Criterios de alerta

- Amarillo: la cantidad de datos que se transfieren del bucket a los usuarios mediante solicitudes GET en los 30 días anteriores a la comprobación es al menos 25 veces superior a la cantidad promedio de datos almacenados en el bucket.
- Rojo: la cantidad de datos que se transfieren del bucket a los usuarios mediante solicitudes GET en los 30 días anteriores a la comprobación es de al menos 10 TB y al menos 25 veces superior a la cantidad promedio de datos almacenados en el bucket.

Acción recomendada

Considere la posibilidad de CloudFront utilizarla para obtener un mejor rendimiento. Consulta los detalles CloudFront del producto de Amazon.

Si los datos transferidos son de 10 TB al mes o más, consulta los CloudFront precios de Amazon para explorar los posibles ahorros de costos.

Recursos adicionales

- Guía para CloudFront desarrolladores de Amazon
- Caso práctico de AWS : PBS

Columnas de informes

- Status
- Región
- Nombre del bucket
- Almacenamiento de S3 (GB)
- Transferencia de datos de salida (GB)
- Relación entre transferencia y almacenamiento

CloudFront Reenvío de encabezados y porcentaje de aciertos de caché

Descripción

Comprueba los encabezados de las solicitudes HTTP que recibe CloudFront actualmente del cliente y los reenvía al servidor de origen.

Algunos encabezados, como la fecha o el agente de usuario, reducen significativamente la proporción de aciertos de la caché (la proporción de solicitudes que se atienden desde una CloudFront memoria caché perimetral). Esto aumenta la carga en su origen y reduce el rendimiento, ya que CloudFront debe reenviar más solicitudes a su origen.

ID de la verificación

`N415c450f2`

Criterios de alerta

Amarillo: una o más cabeceras de solicitud que se CloudFront reenvíen a tu origen podrían reducir considerablemente la ratio de aciertos de la caché.

Acción recomendada

Considere si los encabezados de solicitud ofrecen tantos beneficios como para justificar el efecto negativo en la tasa de acceso a la caché. Si tu origen devuelve el mismo objeto independientemente del valor de un encabezado determinado, te recomendamos que no lo configures CloudFront para reenviar ese encabezado al origen. Para obtener más información, consulta CloudFront Cómo configurar la caché de objetos en función de los encabezados de las solicitudes.

Recursos adicionales

- Aumentar la proporción de solicitudes que se atienden desde cachés CloudFront perimetrales
- CloudFront Informes de estadísticas de caché
- Encabezados y CloudFront comportamiento de las solicitudes HTTP

Columnas de informes

- ID de distribución
- Nombre de dominio de distribución
- Patrón de ruta de comportamiento de la caché
- Encabezados

Uso elevado de instancias de Amazon EC2

Descripción

Verifica las instancias de Amazon Elastic Compute Cloud (Amazon EC2) que han estado en ejecución en cualquier momento durante los últimos 14 días. Se envía una alerta si el uso diario de la CPU fue superior al 90 % en cuatro o más días.

Un uso elevado continuo puede indicar que el rendimiento está optimizado y es constante. Sin embargo, también puede indicar que una aplicación no tiene suficientes recursos. Para obtener datos de uso diario de la CPU, descargue el informe de esta verificación.

ID de la verificación

`ZRxQlPsb6c`

Criterios de alerta

Amarillo: una instancia tuvo una utilización de la CPU superior al promedio diario del 90 % durante al menos 4 de los 14 días anteriores.

Acción recomendada

Considere agregar más instancias. Para obtener información acerca de cómo escalar la cantidad de instancias en función de la demanda, consulte ¿Qué es Auto Scaling?

Recursos adicionales

- Monitoreo de Amazon EC2
- Metadatos de instancia y datos de usuario
- Guía CloudWatch del usuario de Amazon
- Guía del usuario de Amazon EC2 Auto Scaling

Columnas de informes

- Región/AZ
- ID de instancia
- Tipo de instancia
- Nombre de instancia
- Utilización promedio de la CPU de 14 días
- Cantidad de días con un uso de CPU superior al 90 %

Seguridad

Puede utilizar las siguientes verificaciones para la categoría de seguridad.

> **Note**
>
> Si has activado Security Hub para ti Cuenta de AWS, puedes ver tus resultados en la Trusted Advisor consola. Para obtener más información, consulte Visualización de controles de AWS Security Hub en AWS Trusted Advisor.
> Puede ver todos los controles del estándar de seguridad AWS Foundational Security Best Practices, excepto los controles que tienen la categoría: Recuperación > Resiliencia. Para obtener una lista de los controles admitidos, consulte Controles de las prácticas de seguridad básicas recomendadas de AWS en la Guía del usuario de AWS Security Hub .

Nombres de la verificación

- Período de retención de Amazon CloudWatch Log Group
- Instancias de Amazon EC2 con fin del soporte para Microsoft SQL Server
- Instancias de Amazon EC2 con final de la compatibilidad con Microsoft Windows Server
- Fin del soporte estándar para las instancias Amazon EC2 con Ubuntu LTS
- Los clientes de Amazon EFS no utilizan data-in-transit cifrado
- Instantáneas públicas de Amazon EBS
- El cifrado de almacenamiento Aurora de Amazon RDS está desactivado
- Se requiere una actualización de la versión secundaria del motor Amazon RDS
- Instantáneas públicas de Amazon RDS
- Amazon RDS Security Group Access Risk
- El cifrado de almacenamiento de Amazon RDS está desactivado
- Registros CNAME no coincidentes de Amazon Route 53 que apuntan directamente a buckets S3
- Marco de políticas de remitentes y conjuntos de registros de recursos MX de Amazon Route 53
- Permisos de bucket de Amazon S3
- Registros de acceso al servidor Amazon S3 activados
- Conexiones de emparejamiento de Amazon VPC con la resolución de DNS deshabilitada

- AWS Backup Vault sin una política basada en recursos para evitar la eliminación de los puntos de recuperación
- AWS CloudTrail Registro
- AWS Lambda Funciones que utilizan tiempos de ejecución obsoletos
- Problemas de alto riesgo de AWS Well-Architected para la seguridad
- CloudFrontCertificados SSL personalizados en el almacén de certificados de IAM
- CloudFront Certificado SSL en el servidor de origen
- Seguridad del agente de escucha de ELB
- Grupos de seguridad de ELB
- Exposed Access Keys
- Rotación de claves de acceso de IAM
- Política de contraseñas de IAM
- MFA en la cuenta raíz
- Grupos de seguridad: puertos específicos sin restricciones
- Grupos de seguridad: acceso sin restricciones

Período de retención de Amazon CloudWatch Log Group

Descripción

Comprueba si el período de retención del grupo de CloudWatch registros de Amazon está establecido en 365 días o en otro número especificado.

De forma predeterminada, los registros se conservan de forma indefinida y no caducan nunca. Sin embargo, puede ajustar la política de retención de cada grupo de registro para cumplir con las normativas del sector o los requisitos legales durante un periodo específico.

Puede especificar el tiempo mínimo de retención y los nombres de los grupos de registros mediante los parámetros LogGroupNombres y MinRetentionTiempo de sus AWS Config reglas.

> **Note**
>
> Los resultados de esta verificación se actualizan automáticamente varias veces al día y no se permiten las solicitudes de actualización. Puede que los cambios tarden unas horas en aparecer. Actualmente, no puede excluir recursos de esta verificación.

ID de la verificación

`c18d2gz186`

Origen

`AWS Config Managed Rule: cw-loggroup-retention-period-check`

Criterios de alerta

Amarillo: el período de retención de un grupo de CloudWatch registros de Amazon es inferior al número mínimo de días deseado.

Acción recomendada

Configura un período de retención de más de 365 días para los datos de registro almacenados en Amazon CloudWatch Logs a fin de cumplir con los requisitos de conformidad.

Para obtener más información, consulte Cambiar la retención de datos de registro en CloudWatch los registros.

Recursos adicionales

Alterar la retención de CloudWatch registros

Columnas de informes

- Status
- Región
- Recurso
- AWS Config Regla
- Parámetros de entrada
- Hora de la última actualización

Instancias de Amazon EC2 con fin del soporte para Microsoft SQL Server

Descripción

Verifica las versiones de SQL Server en las instancias de Amazon Elastic Compute Cloud (Amazon EC2) en ejecución durante las últimas 24 horas. Esta verificación le avisa si a las versiones les queda poco tiempo de soporte o si dicho soporte ya se ha vencido. Cada versión de SQL Server ofrece 10 años de soporte, que incluyen 5 años de soporte general y 5 años de

asistencia ampliada. Una vez que se vence el plazo de soporte, la versión de SQL Server no recibirá actualizaciones de seguridad periódicas. La ejecución de aplicaciones con versiones de SQL Server no compatibles puede suponer riesgos de seguridad o conformidad.

> **Note**
>
> Los resultados de esta verificación se actualizan automáticamente varias veces al día y no se permiten las solicitudes de actualización. Puede que los cambios tarden unas horas en aparecer. Actualmente, no puede excluir recursos de esta verificación.

ID de la verificación

`Qsdfp3A4L3`

Criterios de alerta

- Rojo: una instancia de EC2 tiene una versión de SQL Server que ha llegado al fin del soporte.
- Amarillo: una instancia de EC2 tiene una versión de SQL Server que llegará al fin del soporte en 12 meses.

Acción recomendada

Para modernizar las cargas de trabajo de SQL Server, considere refactorizar a bases de datos nativas de Nube de AWS como Amazon Aurora. Para obtener más información, consulte Modernizar las cargas de trabajo de Windows con. AWS

Para pasar a una base de datos completamente administrada, considere redefinir la plataforma a Amazon Relational Database Service (Amazon RDS). Para obtener más información, consulte Amazon RDS para SQL Server.

Para actualizar SQL Server en Amazon EC2, considere utilizar el runbook de automatización a fin de simplificar la actualización. Para obtener más información, consulte la Documentación de AWS Systems Manager.

Si no puede actualizar SQL Server en Amazon EC2, considere el Programa de migración de la finalización del soporte (EMP) para Windows Server. Para obtener más información, consulte el sitio web de EMP.

Recursos adicionales

- Prepárese para la finalización del soporte de SQL Server con AWS

- Microsoft SQL Server en AWS

Columnas de informes

- Status
- Región
- ID de instancia
- Versión de SQL Server
- Ciclo de soporte
- Fin del soporte
- Hora de la última actualización

Instancias de Amazon EC2 con final de la compatibilidad con Microsoft Windows Server

Descripción

Esta verificación le avisa si a las versiones les queda poco tiempo de soporte o si dicho soporte ya se ha vencido. Cada versión de Windows Server ofrece 10 años de soporte. Esto incluye 5 años de soporte general y 5 años de soporte ampliado. Una vez que se llega al final de la compatibilidad, la versión de Windows Server no recibirá actualizaciones de seguridad periódicas. Si ejecuta aplicaciones con versiones de Windows Server no compatibles, pone en riesgo la seguridad o la conformidad de estas aplicaciones.

> **Note**
>
> Los resultados de esta verificación se actualizan automáticamente varias veces al día y no se permiten las solicitudes de actualización. Puede que los cambios tarden unas horas en aparecer. Actualmente, no puede excluir recursos de esta verificación.

ID de la verificación

`Qsdfp3A4L4`

Criterios de alerta

- Rojo: una instancia de EC2 tiene una versión de Windows Server que ha llegado al final de la compatibilidad (Windows Server 2003, 2003 R2, 2008 y 2008 R2).

- Amarillo: una instancia de EC2 tiene una versión de Windows Server que llegará al final de la compatibilidad en menos de 18 meses (Windows Server 2012 y 2012 R2).

Acción recomendada

Para modernizar sus cargas de trabajo de Windows Server, considere las distintas opciones disponibles en Modernize Windows Workloads con. AWS

Para actualizar las cargas de trabajo de Windows Server para que se ejecuten en versiones más recientes de este, puede usar un manual de procedimientos. Para obtener más información, consulte la documentación de AWS Systems Manager.

Siga el conjunto de pasos que se indican a continuación:

- Actualice la versión de Windows Server
- Haga una parada y comience después de la actualización
- Si utiliza EC2Config, migre a EC2Launch

Columnas de informes

- Status
- Región
- ID de instancia
- Versión de Windows Server
- Ciclo de soporte
- Fin del soporte
- Hora de la última actualización

Fin del soporte estándar para las instancias Amazon EC2 con Ubuntu LTS

Descripción

Esta comprobación le avisa si las versiones están cerca o han llegado al final del soporte estándar. Es importante tomar medidas, ya sea migrando al siguiente LTS o actualizándolo a Ubuntu Pro. Cuando finalice el soporte, sus máquinas LTS de la versión 18.04 no recibirán ninguna actualización de seguridad. Con una suscripción a Ubuntu Pro, su implementación de Ubuntu 18.04 LTS podrá recibir un mantenimiento de seguridad ampliado (ESM) hasta 2028. Las vulnerabilidades de seguridad que no se hayan reparado exponen sus sistemas a los piratas informáticos y corren el riesgo de sufrir una violación grave.

> **Note**
>
> Los resultados de esta verificación se actualizan automáticamente varias veces al día y no se permiten las solicitudes de actualización. Puede que los cambios tarden unas horas en aparecer. Actualmente, no puede excluir recursos de esta verificación.

ID de la verificación

`c1dfprch15`

Criterios de alerta

Rojo: una instancia de Amazon EC2 tiene una versión de Ubuntu que ha llegado al final del soporte estándar (Ubuntu 18.04 LTS, 18.04.1 LTS, 18.04.2 LTS, 18.04.3 LTS, 18.04.4 LTS, 18.04.5 LTS y 18.04.6 LTS).

Amarillo: una instancia de Amazon EC2 tiene una versión de Ubuntu que finalizará el soporte estándar en menos de 6 meses (Ubuntu 20.04 LTS, 20.04.1 LTS, 20.04.2 LTS, 20.04.3 LTS, 20.04.4 LTS, 20.04.5 LTS y 20.04.6 LTS).

Verde: todas las instancias de Amazon EC2 son compatibles.

Acción recomendada

Para actualizar las instancias LTS de Ubuntu 18.04 a una versión LTS compatible, siga los pasos que se mencionan en este artículo. Para actualizar las instancias de Ubuntu 18.04 LTS a Ubuntu Pro, visita la AWS License Manager consola y sigue los pasos que se mencionan en la guía del usuario.AWS License Manager También puedes consultar el blog de Ubuntu, donde se muestra una demostración paso a paso de la actualización de las instancias de Ubuntu a Ubuntu Pro.

Recursos adicionales

Para obtener información sobre los precios, ponte en contacto con AWS Support.

Columnas de informes

- Status
- Región
- Versión Ubuntu Lts
- Fecha prevista de fin de soporte
- ID de instancia

- Ciclo de soporte
- Hora de la última actualización

Los clientes de Amazon EFS no utilizan data-in-transit cifrado

Descripción

Comprueba si el sistema de archivos Amazon EFS está montado mediante data-in-transit cifrado. AWS recomienda que los clientes utilicen el data-in-transit cifrado en todos los flujos de datos para protegerlos de la exposición accidental o del acceso no autorizado. Amazon EFS recomienda a los clientes utilizar la configuración de montaje «-o tls» mediante el asistente de montaje de Amazon EFS para cifrar los datos en tránsito mediante TLS v1.2.

ID de la verificación

`c1dfpnchv1`

Criterios de alerta

Amarillo: uno o más clientes NFS de su sistema de archivos Amazon EFS no utilizan la configuración de montaje recomendada que proporciona data-in-transit cifrado.

Verde: todos los clientes NFS de su sistema de archivos Amazon EFS utilizan la configuración de montaje recomendada que proporciona data-in-transit cifrado.

Acción recomendada

Para aprovechar la función de data-in-transit cifrado de Amazon EFS, le recomendamos que vuelva a montar el sistema de archivos mediante el asistente de montaje de Amazon EFS y la configuración de montaje recomendada.

> **Note**
>
> Algunas distribuciones de Linux no incluyen una versión de stunnel que admita las funciones de TLS de forma predeterminada. Si utiliza una distribución de Linux no compatible (consulte las distribuciones compatibles aquí), le recomendamos que la actualice antes de volver a montarla con la configuración de montaje recomendada.

Recursos adicionales

- Cifrar los datos en tránsito

Columnas de informes

- Status
- Región
- ID del sistema de archivos de EFS
- Como ocurre con las conexiones no cifradas
- Hora de la última actualización

Instantáneas públicas de Amazon EBS

Descripción

Comprueba la configuración de permisos para las instantáneas de volumen de Amazon Elastic Block Store (Amazon EBS) y te avisa si alguna instantánea es de acceso público.

Al hacer pública una instantánea, concedes a todos Cuentas de AWS y a los usuarios acceso a todos los datos de la instantánea. Para compartir una instantánea solo con usuarios o cuentas específicos, márcala como privada. A continuación, especifique el usuario o las cuentas con los que desea compartir los datos de la instantánea. Tenga en cuenta que si ha activado Bloquear el acceso público en el modo «bloquear todo lo que se comparte», sus instantáneas públicas no serán de acceso público y no aparecerán en los resultados de esta comprobación.

> **Note**
>
> Los resultados de esta verificación se actualizan automáticamente varias veces al día y no se permiten las solicitudes de actualización. Puede que los cambios tarden unas horas en aparecer.

ID de la verificación

`ePs02jT06w`

Criterios de alerta

Rojo: la instantánea del volumen de EBS es de acceso público.

Acción recomendada

A menos que esté seguro de que quiere compartir todos los datos de la instantánea con todos Cuentas de AWS los usuarios, modifique los permisos: marque la instantánea como privada y,

a continuación, especifique las cuentas a las que quiere conceder permisos. Para obtener más información, consulte Compartir una instantánea de Amazon EBS. Utilice Bloquear el acceso público para las instantáneas de EBS para controlar la configuración que permite el acceso público a sus datos. Esta comprobación no se puede excluir de la vista de la Trusted Advisor consola.

Para modificar los permisos de las instantáneas directamente, utilice un manual de instrucciones en la AWS Systems Manager consola. Para obtener más información, consulte `AWSSupport-ModifyEBSSnapshotPermission`.

Recursos adicionales

Instantáneas de Amazon EBS

Columnas de informes

- Status
- Región
- ID de volumen
- ID de instantánea
- Descripción

El cifrado de almacenamiento Aurora de Amazon RDS está desactivado

Descripción

Amazon RDS admite el cifrado en reposo para todos los motores de bases de datos mediante las claves que usted administra. AWS Key Management Service En una instancia de base de datos activa con cifrado de Amazon RDS, los datos almacenados en reposo en el almacenamiento están cifrados, de forma similar a las copias de seguridad, las réplicas de lectura y las instantáneas automatizadas.

Si el cifrado no está activado al crear un clúster de base de datos Aurora, debe restaurar una instantánea descifrada en un clúster de base de datos cifrado.

> **Note**
>
> Los resultados de esta verificación se actualizan automáticamente varias veces al día y no se permiten las solicitudes de actualización. Puede que los cambios tarden unas horas en aparecer. Actualmente, no puede excluir recursos de esta verificación.

> **Note**
>
> Cuando se detiene una instancia de base de datos o un clúster de base de datos, puede ver las recomendaciones de Amazon RDS en un plazo Trusted Advisor de 3 a 5 días. Transcurridos cinco días, las recomendaciones no estarán disponibles en Trusted Advisor. Para ver las recomendaciones, abra la consola de Amazon RDS y, a continuación, seleccione Recomendaciones.
> Si elimina una instancia de base de datos o un clúster de base de datos, las recomendaciones asociadas a esas instancias o clústeres no estarán disponibles en Trusted Advisor la consola de administración de Amazon RDS.

ID de la verificación

`c1qf5bt005`

Criterios de alerta

Rojo: los recursos Aurora de Amazon RDS no tienen el cifrado activado.

Acción recomendada

Active el cifrado de los datos en reposo de su clúster de base de datos.

Recursos adicionales

Puede activar el cifrado al crear una instancia de base de datos o utilizar una solución alternativa para activar el cifrado en una instancia de base de datos activa. No puede modificar un clúster de base de datos descifrado por un clúster de base de datos cifrado. Sin embargo, puede restaurar una instantánea descifrada en un clúster de base de datos cifrado. Al restaurar desde la instantánea descifrada, debe especificar una AWS KMS clave.

Para obtener más información, consulte Cifrado de recursos de Amazon Aurora.

Columnas de informes

- Status
- Región
- Recurso
- Nombre del motor
- Hora de la última actualización

Se requiere una actualización de la versión secundaria del motor Amazon RDS

Descripción

Los recursos de su base de datos no están ejecutando la última versión secundaria del motor de base de datos. La última versión secundaria contiene las últimas revisiones de seguridad y otras mejoras.

> **Note**
>
> Los resultados de esta verificación se actualizan automáticamente varias veces al día y no se permiten las solicitudes de actualización. Puede que los cambios tarden unas horas en aparecer. Actualmente, no puede excluir recursos de esta verificación.

> **Note**
>
> Cuando se detiene una instancia de base de datos o un clúster de base de datos, puede ver las recomendaciones de Amazon RDS en un plazo Trusted Advisor de 3 a 5 días. Transcurridos cinco días, las recomendaciones no estarán disponibles en Trusted Advisor. Para ver las recomendaciones, abra la consola de Amazon RDS y, a continuación, seleccione Recomendaciones.
> Si elimina una instancia de base de datos o un clúster de base de datos, las recomendaciones asociadas a esas instancias o clústeres no estarán disponibles en Trusted Advisor la consola de administración de Amazon RDS.

ID de la verificación

`c1qf5bt003`

Criterios de alerta

Rojo: los recursos de Amazon RDS no ejecutan la última versión secundaria del motor de base de datos.

Acción recomendada

Actualice a la última versión del motor.

Recursos adicionales

Le recomendamos que mantenga su base de datos con la última versión secundaria del motor de base de datos, ya que esta versión incluye las correcciones de seguridad y funcionalidad más recientes. Las actualizaciones de las versiones secundarias del motor de base de datos contienen solo los cambios que son compatibles con versiones secundarias anteriores de la misma versión principal del motor de base de datos.

Para obtener más información, consulte Cómo actualizar la versión del motor de la instancia de base de datos.

Columnas de informes

- Status
- Región
- Recurso
- Nombre del motor
- Versión del motor actual
- Valor recomendado
- Hora de la última actualización

Instantáneas públicas de Amazon RDS

Descripción

Verifica la configuración de permisos de las instantáneas de base de datos de Amazon Relational Database Service (Amazon RDS) y le avisa si hay alguna instantánea marcada como pública.

Al hacer pública una instantánea, concedes a todos Cuentas de AWS y a los usuarios acceso a todos los datos de la instantánea. Si desea compartir una instantánea solo con usuarios o cuentas específicos, marque la instantánea como privada. A continuación, especifique el usuario o las cuentas con las que desea compartir los datos de la instantánea.

> **Note**
>
> Los resultados de esta verificación se actualizan automáticamente varias veces al día y no se permiten las solicitudes de actualización. Puede que los cambios tarden unas horas en aparecer.

ID de la verificación

`rSs93HQwa1`

Criterios de alerta

Rojo: la instantánea de Amazon RDS está marcada como pública.

Acción recomendada

A menos que esté seguro de que quiere compartir todos los datos de la instantánea con todos Cuentas de AWS los usuarios, modifique los permisos: marque la instantánea como privada y, a continuación, especifique las cuentas a las que desea conceder permisos. Para obtener más información, consulte Compartir una instantánea de base de datos o una instantánea de clúster de base de datos. Esta comprobación no se puede excluir de la vista de la Trusted Advisor consola.

Para modificar los permisos de las instantáneas directamente, puede utilizar un manual de instrucciones en la AWS Systems Manager consola. Para obtener más información, consulte `AWSSupport-ModifyRDSSnapshotPermission`.

Recursos adicionales

Copia de seguridad y restauración de instancias de base de datos de Amazon RDS

Columnas de informes

- Status
- Región
- Instancia de base de datos o ID de clúster
- ID de instantánea

Amazon RDS Security Group Access Risk

Descripción

Verifica las configuraciones de grupos de seguridad de Amazon Relational Database Service (Amazon RDS) y avisa cuando una regla de grupo de seguridad concede un acceso excesivamente permisivo a la base de datos. Se recomienda configurar las reglas de grupo de seguridad para permitir el acceso solo desde grupos de seguridad específicos de Amazon Elastic Compute Cloud (Amazon EC2) o desde una dirección IP específica.

ID de la verificación

`nNauJisYIT`

Criterios de alerta

- Amarillo: una regla de un grupo de seguridad de base de datos hace referencia a un grupo de seguridad de Amazon EC2 que otorga acceso global en uno de estos puertos: 20, 21, 22, 1433, 1434, 3306, 3389, 4333, 5432, 5500.
- Amarillo: una regla de grupo de seguridad de base de datos da acceso a más de una única dirección IP (el sufijo de la regla CIDR no es /0 ni /32).
- Rojo: una regla de grupo de seguridad de base de datos otorga acceso global (el sufijo de la regla CIDR es /0).

Acción recomendada

Revise las reglas de los grupos de seguridad y limite el acceso a intervalos de IP o direcciones IP autorizadas. Para editar un grupo de seguridad, utilice la API AuthorizeDB Ingress o SecurityGroup la. AWS Management Console Para obtener más información, consulte Trabajo con grupos de seguridad de base de datos.

Recursos adicionales

- Grupos de seguridad de Amazon RDS
- Enrutamiento entre dominios sin clases
- Lista de números de puertos TCP y UDP

Columnas de informes

- Status
- Región
- Nombre de grupo de seguridad RDS
- Regla de entrada
- Motivo

El cifrado de almacenamiento de Amazon RDS está desactivado

Descripción

Amazon RDS admite el cifrado en reposo para todos los motores de bases de datos mediante las claves que usted administra. AWS Key Management Service En una instancia de base de datos activa con cifrado de Amazon RDS, los datos almacenados en reposo en el almacenamiento

están cifrados, de forma similar a las copias de seguridad, las réplicas de lectura y las instantáneas automatizadas.

Si el cifrado no está activado al crear una instancia de base de datos, debe restaurar una copia cifrada de la instantánea descifrada antes de activar el cifrado.

> **Note**
>
> Los resultados de esta verificación se actualizan automáticamente varias veces al día y no se permiten las solicitudes de actualización. Puede que los cambios tarden unas horas en aparecer. Actualmente, no puede excluir recursos de esta verificación.

> **Note**
>
> Cuando se detiene una instancia de base de datos o un clúster de base de datos, puede ver las recomendaciones de Amazon RDS en un plazo Trusted Advisor de 3 a 5 días. Transcurridos cinco días, las recomendaciones no estarán disponibles en Trusted Advisor. Para ver las recomendaciones, abra la consola de Amazon RDS y, a continuación, seleccione Recomendaciones.
> Si elimina una instancia de base de datos o un clúster de base de datos, las recomendaciones asociadas a esas instancias o clústeres no estarán disponibles en Trusted Advisor la consola de administración de Amazon RDS.

ID de la verificación

`c1qf5bt006`

Criterios de alerta

Rojo: los recursos de Amazon RDS no tienen el cifrado activado.

Acción recomendada

Active el cifrado de los datos en reposo de su instancia de base de datos.

Recursos adicionales

Puede cifrar una instancia de base de datos solo cuando la crea. Para cifrar una instancia de base de datos activa existente:

Cree una copia cifrada de la instancia de base de datos original

1. Cree una instantánea de la instancia de la base de datos.
2. Cree una copia cifrada de la instantánea creada en el paso 1.
3. Restaure una instancia de base de datos a partir de la instantánea cifrada.

Para obtener más información, consulte los siguientes recursos:

- Cifrado de los recursos de Amazon RDS
- Copiar una instantánea de base de datos

Columnas de informes

- Status
- Región
- Recurso
- Nombre del motor
- Hora de la última actualización

Registros CNAME no coincidentes de Amazon Route 53 que apuntan directamente a buckets S3

Descripción

Comprueba las zonas alojadas de Amazon Route 53 con registros CNAME que apuntan directamente a los nombres de host del bucket de Amazon S3 y alerta si su CNAME no coincide con el nombre del bucket de S3.

ID de la verificación

`c1ng44jvbm`

Criterios de alerta

Rojo: la zona alojada de Amazon Route 53 tiene registros CNAME que indican que los nombres de host de los buckets de S3 no coinciden.

Verde: no se han encontrado registros CNAME que no coincidan en tu zona alojada de Amazon Route 53.

Acción recomendada

Al apuntar los registros CNAME a los nombres de host de los buckets de S3, debe asegurarse de que existe un bucket coincidente para cualquier registro CNAME o alias que configure. De este modo, evitas el riesgo de que tus registros CNAME sean falsificados. También evitas que cualquier AWS usuario no autorizado aloje contenido web defectuoso o malintencionado en tu dominio.

Para evitar apuntar los registros CNAME directamente a los nombres de host del bucket de S3, considere la posibilidad de utilizar el control de acceso de origen (OAC) para acceder a los activos web del bucket de S3 a través de Amazon. CloudFront

Para obtener más información sobre cómo asociar CNAME a un nombre de host de un bucket de Amazon S3, consulte Personalización de las URL de Amazon S3 con registros CNAME.

Recursos adicionales

- Cómo asociar un nombre de host a un bucket de Amazon S3
- Restringir el acceso a un origen de Amazon S3 con CloudFront

Columnas de informes

- Status
- ID de zona alojada
- Zona alojada (ARN)
- Registros CNAME coincidentes
- Registros CNAME que no coinciden
- Hora de la última actualización

Marco de políticas de remitentes y conjuntos de registros de recursos MX de Amazon Route 53

Descripción

En cada conjunto de registros de recursos MX, esta verificación verifica que el conjunto de registros de recursos TXT o SPF contiene un registro SPF válido. El registro debe comenzar por "`v=spf1`". El registro SPF especifica los servidores que están autorizados para enviar correo electrónico para su dominio, lo que ayuda a detectar y detener la suplantación de direcciones de correo electrónico y a reducir el spam. Route 53 recomienda usar un registro TXT en lugar de

un registro SPF. Trusted Advisor muestra esta marca en verde siempre que cada conjunto de registros de recursos MX tenga al menos un registro SPF o TXT.

ID de la verificación

`c9D319e7sG`

Criterios de alerta

Amarillo: un conjunto de registros de recursos MX no tiene un registro de recursos TXT o SPF que contenga un valor SPF válido.

Acción recomendada

Para cada conjunto de registros de recursos MX, cree un conjunto de registros de recursos TXT que contenga un valor SPF válido. Para obtener más información, consulte Marco de directivas de remitentes: sintaxis de registro SPF y Creación de conjuntos de registros de recursos con la consola Amazon Route 53.

Recursos adicionales

- Marco de directivas de remitentes
- Registro MX

Columnas de informes

- Nombre de zona alojada
- ID de zona alojada
- Nombre de conjunto de registros de recursos
- Status

Permisos de bucket de Amazon S3

Descripción

Comprueba los depósitos de Amazon Simple Storage Service (Amazon S3) que tienen permisos de acceso abierto o que permiten el acceso a cualquier usuario autenticado. AWS

Esta verificación examina los permisos de bucket explícitos, así como las políticas de bucket que podrían invalidar dichos permisos. No se recomienda conceder permisos de acceso a la lista a todos los usuarios para un bucket de Amazon S3. Estos permisos pueden permitir que usuarios no deseados generen listas de objetos en el bucket a una frecuencia elevada, lo que

puede dar lugar a cargos superiores a los esperados. Los permisos que otorgan acceso de carga y eliminación a todos los usuarios pueden provocar vulnerabilidades de seguridad en su bucket.

ID de la verificación

`Pfx0RwqBli`

Criterios de alerta

- Amarillo: el bucket ACL permite el acceso a la lista a Everyone (Todos) o a Any Authenticated AWS User (Cualquier usuario autenticado).
- Amarillo: una política de bucket permite cualquier tipo de acceso abierto.
- Amarillo: la política de bucket tiene instrucciones que otorgan acceso público. La configuración Denegar el acceso público y entre cuentas a los buckets que tengan políticas públicas está activada y tiene restringido el acceso solo a los usuarios autorizados de esa cuenta hasta que se eliminen las instrucciones públicas.
- Amarillo: Trusted Advisor no tiene permiso para comprobar la política o la política no se ha podido evaluar por otros motivos.
- Rojo: la lista de control de acceso (ACL) de los buckets permite el acceso de carga y eliminación a Everyone (Todos) o Any Authenticated AWS User (Cualquier usuario de autenticado).

Acción recomendada

Si un bucket permite el acceso abierto, determine si este tipo de acceso es realmente necesario. De lo contrario, actualice los permisos del bucket para restringir el acceso al propietario o a usuarios específicos. Utilice el bloqueo del acceso público de Amazon S3 para controlar la configuración que permite el acceso público a los datos. Consulte Configuración de permisos de acceso a buckets y objetos.

Recursos adicionales

Administración de permisos de acceso para los recursos de Amazon S3

Columnas de informes

- Status
- Nombre de la región
- Parámetro de API de la región
- Nombre del bucket
- ACL permite acceso a la lista

- ACL permite cargar/eliminar
- La política permite el acceso

Registros de acceso al servidor Amazon S3 activados

Descripción

Comprueba la configuración de registro de los depósitos de Amazon Simple Storage Service.

Cuando se habilita el registro de acceso al servidor, los registros de acceso detallados se entregan cada hora en un bucket especificado. Los registros de acceso contienen detalles sobre cada solicitud, como, por ejemplo, el tipo de solicitud, los recursos especificados en la solicitud y la fecha y hora en que se procesó la solicitud. De forma predeterminada, el registro de bucket no está habilitado. Debe habilitar el registro si desea llevar a cabo auditorías de seguridad u obtener más información sobre los usuarios y los patrones de uso.

Cuando el registro está habilitado inicialmente, la configuración se valida automáticamente. No obstante, las modificaciones futuras pueden dar lugar a errores de registro. Esta comprobación examina los permisos explícitos de los buckets de Amazon S3. Se recomienda utilizar políticas de bucket para controlar los permisos de bucket; sin embargo, también se pueden utilizar las ACL.

ID de la verificación

`c1fd6b96l4`

Criterios de alerta

- Amarillo: el bucket no tiene habilitado el registro de acceso al servidor.
- Amarillo: los permisos del bucket de destino no incluyen la cuenta raíz, por lo que Trusted Advisor no puede comprobarla.
- Rojo: el bucket de destino no existe.
- Rojo: el bucket de destino y el bucket de origen tienen propietarios diferentes.
- Rojo: el emisor de registros no tiene permisos de escritura en el bucket de destino.
- Verde: el bucket tiene habilitado el registro de acceso al servidor, el destino ya existe y los permisos para escribir en él

Acción recomendada

Habilite el registro de buckets para la mayoría de los buckets. Consulte Habilitación del registro con la consola y Habilitación de registros mediante programación.

Si los permisos del bucket de destino no incluyen la cuenta raíz y quiere que Trusted Advisor compruebe el estado de registro, agregue la cuenta raíz como beneficiario. Consulte Edición de permisos de bucket.

Si el bucket de destino no existe, seleccione un bucket existente como destino o cree uno nuevo y selecciónelo. Consulte Administración del registro de buckets.

Si el origen y el destino tienen propietarios diferentes, cambie el bucket de destino por uno que tenga el mismo propietario que el bucket de origen. Consulte Administración del registro de buckets.

Si el repartidor de registros no tiene permisos de escritura para el destino (la escritura no está habilitada), otorgue permisos de carga o eliminación al grupo de entrega de registros. Se recomienda usar políticas de bucket en lugar de las ACL. Consulte Edición de los permisos de los buckets y los permisos para la entrega de registros.

Recursos adicionales

Trabajando con cubos

Server access logging (Registro de acceso del servidor)

Formato de registro de acceso al servidor

Eliminar archivos de registro

Columnas de informes

- Status
- Región
- ARN de recurso
- Nombre del bucket
- Nombre del destino
- El destino existe
- Mismo propietario
- Escritura habilitada
- Motivo
- Hora de la última actualización

Conexiones de emparejamiento de Amazon VPC con la resolución de DNS deshabilitada

Descripción

Comprueba si las conexiones de emparejamiento de VPC tienen la resolución de DNS activada tanto para las VPC que aceptan como para las que solicitan.

La resolución de DNS para una conexión de emparejamiento de VPC permite la resolución de nombres de host DNS públicos en direcciones IPv4 privadas cuando se realizan consultas desde la VPC. Esto permite el uso de nombres de DNS para la comunicación entre los recursos de las VPC emparejadas. La resolución de DNS en las conexiones de emparejamiento de VPC hace que el desarrollo y la administración sean más sencillos y menos propensos a errores, y garantiza que los recursos siempre se comuniquen de forma privada a través de la conexión de emparejamiento de VPC.

Puede especificar los ID de VPC mediante los parámetros de VPCID de sus reglas. AWS Config

Para obtener más información, consulte Habilitación de la resolución de DNS para la conexión de emparejamiento de VPC.

> **Note**
>
> Los resultados de esta verificación se actualizan automáticamente varias veces al día y no se permiten las solicitudes de actualización. Puede que los cambios tarden unas horas en aparecer. Actualmente, no puede excluir recursos de esta verificación.

ID de la verificación

```
c18d2gz124
```

Origen

```
AWS Config Managed Rule: vpc-peering-dns-resolution-check
```

Criterios de alerta

Amarillo: la resolución de DNS no está habilitada para las VPC que aceptan ni para las que solicitan en una conexión de emparejamiento de VPC.

Acción recomendada

Active la resolución de DNS para sus conexiones de emparejamiento de VPC.

Recursos adicionales

- Modificación de las opciones de conexión de emparejamiento de VPC
- Atributos de DNS en la VPC

Columnas de informes

- Status
- Región
- Recurso
- AWS Config Regla
- Parámetros de entrada
- Hora de la última actualización

AWS Backup Vault sin una política basada en recursos para evitar la eliminación de los puntos de recuperación

Descripción

Comprueba si los AWS Backup almacenes tienen una política basada en recursos adjunta que impide la eliminación de los puntos de recuperación.

La política basada en recursos evita la eliminación inesperada de puntos de recuperación, lo que permite reforzar el control de acceso con privilegios mínimos a los datos de copia de seguridad.

Puede especificar los AWS Identity and Access Management ARN que no desee que la regla registre en el parámetro principal ArnList de las reglas. AWS Config

> **Note**
>
> Los resultados de esta verificación se actualizan automáticamente varias veces al día y no se permiten las solicitudes de actualización. Puede que los cambios tarden unas horas en aparecer. Actualmente, no puede excluir recursos de esta verificación.

ID de la verificación

`c18d2gz152`

Origen

`AWS Config Managed Rule: backup-recovery-point-manual-deletion-disabled`

Criterios de alerta

Amarillo: hay AWS Backup almacenes que no tienen una política basada en los recursos que impida la eliminación de los puntos de recuperación.

Acción recomendada

Cree políticas basadas en recursos para sus AWS Backup almacenes a fin de evitar la eliminación inesperada de los puntos de recuperación.

La política debe incluir una declaración de «Denegar» con permisos de copia de seguridad: DeleteRecovery punto, copia de seguridad: y copia de seguridad: UpdateRecovery PointLifecycle permisos. PutBackupVaultAccessPolicy

Para obtener más información, consulte Configuración de políticas de acceso en almacenes de copias de seguridad.

Columnas de informes

- Status
- Región
- Recurso
- AWS Config Regla
- Parámetros de entrada
- Hora de la última actualización

AWS CloudTrail Registro

Descripción

Comprueba el uso de AWS CloudTrail. CloudTrail proporciona una mayor visibilidad de tu actividad Cuenta de AWS al registrar la información sobre las llamadas a la AWS API realizadas en la cuenta. Puede utilizar estos registros para determinar, por ejemplo, qué acciones llevó a

cabo un usuario determinado durante un periodo de tiempo específico o qué usuarios llevaron a cabo acciones en un recurso determinado durante un periodo de tiempo especificado.

Dado que CloudTrail entrega los archivos de registro a un bucket de Amazon Simple Storage Service (Amazon S3) CloudTrail , debe tener permisos de escritura para el bucket. Si se aplica un registro de seguimiento a todas las regiones (la opción predeterminada cuando se crea un nuevo registro de seguimiento), este aparecerá varias veces en el informe de Trusted Advisor .

ID de la verificación

`vjafUGJ9H0`

Criterios de alerta

- Amarillo: CloudTrail informa de los errores de entrega del registro de una ruta.
- Rojo: no se creó un registro de seguimiento para una región o se desactivó el registro de un seguimiento.

Acción recomendada

Para crear un registro de seguimiento o iniciar el registro desde la consola, vaya a la consola de AWS CloudTrail.

Para iniciar el registro, consulte Detener e iniciar la ejecución de un registro de seguimiento.

Si tiene errores de entrega de registros, compruebe que el bucket exista y que la política necesaria esté adjuntada al bucket. Consulte Política de bucket de Amazon S3.

Recursos adicionales

- AWS CloudTrail Guía del usuario
- Regiones admitidas
- Servicios admitidos

Columnas de informes

- Status
- Región
- Nombre de registro de seguimiento
- Estado de registro
- Nombre del bucket
- Fecha de la última entrega

AWS Lambda Funciones que utilizan tiempos de ejecución obsoletos

Descripción

Comprueba si hay funciones Lambda cuya versión $LATEST esté configurada para usar un tiempo de ejecución que se acerca a la obsolescencia o que esté en desuso. Los tiempos de ejecución obsoletos no son aptos para recibir actualizaciones de seguridad ni soporte técnico

> **Note**
>
> Los resultados de esta verificación se actualizan automáticamente varias veces al día y no se permiten las solicitudes de actualización. Puede que los cambios tarden unas horas en aparecer. Actualmente, no puede excluir recursos de esta verificación.

Las versiones publicadas de las funciones Lambda son inmutables, lo que significa que se pueden invocar pero no actualizar. Solo se puede actualizar la versión `$LATEST` de una función de Lambda. Para obtener más información, consulte Versiones de la función Lambda.

ID de la verificación

`L4dfs2Q4C5`

Criterios de alerta

- Rojo: la versión $LATEST de la función está configurada para usar un tiempo de ejecución que ya está obsoleto.
- Amarillo: la versión $LATEST de la función se ejecuta en un entorno de ejecución que dejará de estar disponible en un plazo de 180 días.

Acción recomendada

Si tiene funciones que se ejecutan en un tiempo de ejecución que estará obsoleto en breve, debe prepararse para migrar a un tiempo de ejecución compatible. Para obtener más información, consulte Política de soporte de tiempo de ejecución.

Le recomendamos que elimine las versiones de funciones anteriores que ya no utilice.

Recursos adicionales

Tiempos de ejecución de Lambda

Columnas de informes

- Status

- Región
- ARN de función
- Tiempo de ejecución
- Días hasta la obsolescencia
- Fecha de obsolescencia
- Promedio de invocaciones diarias
- Hora de la última actualización

Problemas de alto riesgo de AWS Well-Architected para la seguridad

Descripción

Verifica si hay problemas de alto riesgo para las cargas de trabajo en el pilar de seguridad. Esta verificación se basa en las revisiones de AWS-Well Architected. Los resultados de las verificaciones dependen de si ha completado la evaluación de la carga de trabajo con AWS Well-Architected.

> **Note**
>
> Los resultados de esta verificación se actualizan automáticamente varias veces al día y no se permiten las solicitudes de actualización. Puede que los cambios tarden unas horas en aparecer. Actualmente, no puede excluir recursos de esta verificación.

ID de la verificación

`Wxdfp4B1L3`

Criterios de alerta

- Rojo: Se identificó al menos un problema activo de alto riesgo en el pilar de seguridad de AWS Well-Architected.
- Verde: No se detectó ningún problema activo de alto riesgo en el pilar de seguridad de AWS Well-Architected.

Acción recomendada

AWS Well-Architected detectó problemas de alto riesgo durante la evaluación de la carga de trabajo. Estos problemas presentan oportunidades para reducir el riesgo y ahorrar dinero. Inicie

sesión en la herramienta AWS Well-Architected para revisar las respuestas y tomar medidas para resolver los problemas activos.

Columnas de informes

- Status
- Región
- ARN de carga de trabajo
- Nombre de carga de trabajo
- Nombre del revisor
- Tipo de carga de trabajo
- Fecha de inicio de carga de trabajo
- Fecha de la última modificación de carga de trabajo
- Cantidad de HRI identificados para la seguridad
- Cantidad de HRI resueltos para la seguridad
- Cantidad de preguntas de seguridad
- Cantidad total de preguntas en el pilar de seguridad
- Hora de la última actualización

CloudFrontCertificados SSL personalizados en el almacén de certificados de IAM

Descripción

Comprueba los certificados SSL en busca de nombres de dominio CloudFront alternativos en el almacén de certificados de IAM. Esta verificación le avisa si un certificado ha caducado, si caducará pronto, si utiliza cifrado obsoleto o si no está configurado correctamente para la distribución.

Cuando caduca un certificado personalizado para un nombre de dominio alternativo, es posible que los navegadores que muestran tu CloudFront contenido muestren un mensaje de advertencia sobre la seguridad de tu sitio web. Los certificados cifrados mediante el algoritmo hash SHA-1 están pronto estarán obsoletos para navegadores web como, por ejemplo, Chrome y Firefox.

Un certificado debe contener un nombre de dominio que coincida con el nombre de dominio de origen o el nombre de dominio del encabezado de host de una solicitud de lector. Si no coincide, CloudFront devuelve al usuario el código de estado HTTP 502 (puerta de enlace incorrecta). Para obtener más información, consulte Usar nombres de dominio alternativos y HTTPS.

ID de la verificación

N425c450f2

Criterios de alerta

- Rojo: un certificado SSL personalizado ha caducado.
- Amarillo: un certificado SSL personalizado caduca en los próximos siete días.
- Amarillo: un certificado SSL personalizado se cifró mediante el algoritmo hash SHA-1.
- Amarillo: uno o varios de los nombres de dominio alternativos de la distribución no aparecen en el campo Common Name (Nombre común) ni en el campo Subject Alternative Names (Nombres alternativos del sujeto) del certificado SSL personalizado.

Acción recomendada

Renueve un certificado caducado o que esté a punto de caducar.

Reemplace el certificado que se cifró con el algoritmo hash SHA-1 por otro que se haya cifrado con el algoritmo hash SHA-256.

Reemplace el certificado por otro que contenga los valores aplicables en los campos Common Name (Nombre común) o Subject Alternative Domain Names (Nombres de dominio alternativos del sujeto).

Recursos adicionales

Usar una conexión HTTPS para acceder a los objetos

Columnas de informes

- Status
- ID de distribución
- Nombre de dominio de distribución
- Nombre del certificado
- Motivo

CloudFront Certificado SSL en el servidor de origen

Descripción

Verifica el servidor de origen en busca de certificados SSL que hayan caducado, que estén a punto de caducar, que no se encuentren o que utilicen un cifrado obsoleto. Si un certificado

presenta uno de estos problemas, CloudFront responde a las solicitudes de contenido con el código de estado HTTP 502, Bad Gateway.

Los certificados que se cifraron mediante el algoritmo hash SHA-1 comienzan a estar obsoletos en navegadores web como Chrome y Firefox. En función del número de certificados SSL que tengas asociados a tus CloudFront distribuciones, esta comprobación puede añadir unos céntimos al mes a tu factura con tu proveedor de alojamiento web, por ejemplo, AWS si utilizas Amazon EC2 o Elastic Load Balancing como origen de la distribución. CloudFront Esta comprobación no valida la cadena de su certificado de origen ni las autoridades de certificación. Puede comprobarlos en su configuración. CloudFront

ID de la verificación

`N430c450f2`

Criterios de alerta

- Rojo: un certificado SSL de su origen falta o ha caducado.
- Amarillo: un certificado SSL de su origen caduca en los próximos treinta días.
- Amarillo: un certificado SSL de su origen se cifró mediante el algoritmo hash SHA-1.
- Amarillo: no se encuentra un certificado SSL de su origen. Es posible que la conexión haya dado error debido a que se agotó el tiempo de espera o a otros problemas de conexión HTTPS.

Acción recomendada

Renueve el certificado en el origen si ha caducado o está a punto de caducar.

Agregue un certificado si no existe uno.

Reemplace el certificado que se cifró con el algoritmo hash SHA-1 por otro que se haya cifrado con el algoritmo hash SHA-256.

Recursos adicionales

Uso de nombres de dominio alternativos y HTTPS

Columnas de informes

- Status
- ID de distribución
- Nombre de dominio de distribución
- Origen

- Motivo

Seguridad del agente de escucha de ELB

Descripción

Comprueba si hay balanceadores de carga con dispositivos de escucha que no utilizan las configuraciones de seguridad recomendadas para la comunicación cifrada. AWS recomienda utilizar un protocolo seguro (HTTPS o SSL), políticas de up-to-date seguridad y sistemas de cifrado y protocolos seguros.

Cuando se utiliza un protocolo seguro para una conexión frontend (del cliente al balanceador de carga), las solicitudes se cifran entre los clientes y el balanceador de carga, lo que crea un entorno más seguro. Elastic Load Balancing proporciona políticas de seguridad predefinidas con cifrados y protocolos que cumplen con las mejores prácticas AWS de seguridad. Las nuevas versiones de las políticas predefinidas se publican a medida que están disponibles las nuevas configuraciones.

ID de la verificación

`a2sEc6ILx`

Criterios de alerta

- Amarillo: un equilibrador de carga no tiene agentes de escucha que utilicen un protocolo seguro (HTTPS o SSL).
- Amarillo: un agente de escucha del equilibrador de carga utiliza una política de seguridad SSL predefinida desactualizada.
- Amarillo: un agente de escucha del equilibrador de carga utiliza un cifrado o un protocolo no recomendado.
- Rojo: un agente de escucha del equilibrador de carga utiliza un cifrado o un protocolo inseguro.

Acción recomendada

Si es necesario que el tráfico al equilibrador de carga sea seguro, utilice el protocolo HTTPS o SSL para la conexión fron-tend.

Actualice el equilibrador de carga a la última versión de la política de seguridad SSL predefinida.

Utilice únicamente los cifrados y protocolos recomendados.

Para obtener más información, consulte Configuraciones de agentes de escucha de Elastic Load Balancing.

Recursos adicionales

- Referencia rápida de configuraciones de agentes de escucha
- Actualice la configuración de la negociación SSL del equilibrador de carga
- Configuraciones de negociación SSL para Elastic Load Balancing
- Tabla de políticas de seguridad SSL

Columnas de informes

- Status
- Región
- Nombre del equilibrador de carga
- Puerto del equilibrador de carga
- Motivo

Grupos de seguridad de ELB

Descripción

Verifica si hay balanceadores de carga configurados con un grupo de seguridad que falta o un grupo de seguridad que permite el acceso a puertos que no están configurados para el balanceador de carga.

Si se elimina un grupo de seguridad asociado a un balanceador de carga, el balanceador de carga no funcionará como se esperaba. El riesgo de pérdida de datos o de ataques maliciosos aumenta si un grupo de seguridad permite el acceso a puertos que no están configurados para el balanceador de carga.

ID de la verificación

`xSqX82fQu`

Criterios de alerta

- Amarillo: las reglas de entrada de un grupo de seguridad de Amazon VPC asociadas a un equilibrador de carga permiten el acceso a puertos que no están definidos en la configuración del agente de escucha del equilibrador de carga.
- Rojo: no existe un grupo de seguridad asociado a un equilibrador de carga.

Acción recomendada

Configure las reglas del grupo de seguridad para restringir el acceso solo a aquellos puertos y protocolos definidos en la configuración del agente de escucha del equilibrador de carga, además del protocolo de ICMP para admitir la detección de MTU de ruta. Consulte Agentes de escucha para el equilibrador de carga clásico y Grupos de seguridad para equilibradores de carga de una VPC.

Si falta un grupo de seguridad, aplique un grupo de seguridad nuevo al equilibrador de carga. Cree reglas de grupos de seguridad que restrinjan el acceso solo a esos puertos y protocolos que se han definido en la configuración del agente de escucha del equilibrador de carga. Consulte Grupos de seguridad para los equilibradores de carga de una VPC.

Recursos adicionales

- Guía del usuario de Elastic Load Balancing
- Configuración del equilibrador de carga clásico

Columnas de informes

- Status
- Región
- Nombre del equilibrador de carga
- ID de grupos de seguridad
- Motivo

Exposed Access Keys

Descripción

Verifica los repositorios de código populares en busca de claves de acceso que se hayan expuesto al público y de usos irregulares de Amazon Elastic Compute Cloud (Amazon EC2) que podrían ser el resultado de claves de acceso comprometidas.

Las claves de acceso constan de un ID de clave de acceso y una clave de acceso secreta. Las claves de acceso expuestas suponen un riesgo de seguridad para su cuenta y para otros usuarios. Además, pueden ocasionar cargos excesivos por actividades no autorizadas o abusos e infracciones del Acuerdo de cliente de AWS.

Si su clave de acceso se ha visto expuesta, tome medidas de inmediato para proteger su cuenta. Para proteger su cuenta de cargos excesivos, limita AWS temporalmente su capacidad de crear

algunos AWS recursos. Esto no hace que su cuenta sea segura. Solo limita parcialmente el uso no autorizado que podría ocasionar cargos adicionales.

> **Note**
>
> Esta verificación no garantiza la identificación de las claves de acceso expuestas ni de las instancias EC2 comprometidas. En última instancia, usted es responsable de la protección y la seguridad de sus claves de acceso y AWS recursos.
> Los resultados de esta comprobación se actualizan de manera automática, y no se permiten las solicitudes de actualización. Actualmente, no puede excluir recursos de esta verificación.

Si se indica una fecha límite para una clave de acceso, AWS puede suspenderla Cuenta de AWS si el uso no autorizado no se detiene antes de esa fecha. Si cree que esta alerta es un error, póngase en contacto con AWS Support.

Trusted Advisor Es posible que la información que se muestra en no refleje el estado más reciente de su cuenta. Las claves de acceso expuestas se marcan como resueltas cuando se han resuelto todas las claves de acceso expuestas de la cuenta. Esta sincronización de datos puede llevar hasta una semana.

ID de la verificación

`12Fnkpl8Y5`

Criterios de alerta

- Rojo: potencialmente comprometida: AWS ha identificado un identificador de clave de acceso y la correspondiente clave de acceso secreta que han quedado expuestos en Internet y que pueden haber estado comprometidos (utilizados).
- Rojo: Expuesto: AWS ha identificado un identificador de clave de acceso y la correspondiente clave de acceso secreta que han estado expuestos en Internet.
- Rojo: sospechoso: uso irregular de Amazon EC2 indica que una clave de acceso puede haberse visto comprometida, pero no se ha identificado como expuesta en Internet.

Acción recomendada

Elimine la clave de acceso afectada lo antes posible. Si la clave está asociada a un usuario de IAM, consulte Administración de las claves de acceso de los usuarios de IAM.

Compruebe si se ha producido un uso no autorizado en la cuenta. Inicie sesión en la AWS Management Console y compruebe cada consola de servicio para detectar recursos sospechosos. Preste especial atención a las instancias de Amazon EC2 en ejecución, las solicitudes de instancias de spot, las claves de acceso y los usuarios de IAM. También puede comprobar el uso general en la Consola de administración de costos y facturación.

Recursos adicionales

- Mejores prácticas para administrar las claves de AWS acceso
- AWS Directrices de auditoría de seguridad

Columnas de informes

- ID de clave de acceso)
- Nombre de usuario (IAM o raíz)
- Tipo de fraude
- ID de caso
- Hora de actualización
- Ubicación
- Fecha límite
- Uso (USD por día)

Rotación de claves de acceso de IAM

Descripción

Verifica si hay claves de acceso de IAM activas que no se han rotado en los últimos 90 días.

Cuando se rotan las claves de acceso de forma periódica, se reduce la posibilidad de que pueda utilizarse una clave comprometida sin su conocimiento para acceder a los recursos. A efectos de esta verificación, se considera como última fecha y hora de rotación la fecha y la hora en que se creó o activó la clave de acceso. El número y la fecha de la clave de acceso proceden de la información de `access_key_1_last_rotated` y `access_key_2_last_rotated` del informe de credenciales de IAM más reciente.

Dado que la frecuencia de regeneración de un informe de credenciales está restringida, es posible que al actualizar esta comprobación no se reflejen los cambios recientes. Para obtener más información, consulte Obtención de informes de credenciales para la cuenta de Cuenta de AWS.

Para crear y rotar las claves de acceso, un usuario debe tener los permisos adecuados. Para obtener más información, consulte Permitir a los usuarios administrar sus propias contraseñas, claves de acceso y claves SSH.

ID de la verificación

`DqdJqYeRm5`

Criterios de alerta

- Verde: la clave de acceso está activa y se ha rotado en los últimos 90 días.
- Amarillo: la clave de acceso está activa y se ha rotado en los últimos 2 años, pero hace más de 90 días.
- Rojo: la clave de acceso está activa y no se ha rotado en los últimos 2 años.

Acción recomendada

Rote con regularidad las claves de acceso. Consulte Rotación de las claves de acceso y Administración de las claves de acceso de los usuarios de IAM.

Recursos adicionales

- Prácticas recomendadas de IAM
- Cómo rotar las claves de acceso de los usuarios de IAM

Columnas de informes

- Status
- Usuario de IAM
- Clave de acceso
- Última clave rotada
- Motivo

Política de contraseñas de IAM

Descripción

Verifica la política de contraseñas de su cuenta y avisa cuando no se ha habilitado una política de contraseñas o si no se han habilitado los requisitos de contenido de contraseñas.

Los requisitos de contenido de contraseñas aumentan la seguridad general del entorno de AWS al requerir la creación de contraseñas de usuario seguras. Al crear o cambiar una política de

contraseñas, el cambio se aplica de inmediato para los nuevos usuarios, pero no requiere que los usuarios existentes cambien sus contraseñas.

ID de la verificación

`Yw2K9puPzl`

Criterios de alerta

- Amarillo: hay una política de contraseñas habilitada, pero al menos un requisito del contenido no está habilitado.
- Rojo: no hay una política de contraseñas habilitada.

Acción recomendada

Si algunos requisitos de contenido no estuvieran habilitados, considere habilitarlos. Si no hay una política de contraseñas habilitada, cree y configure una. Consulte Configuración de una política de contraseñas de la cuenta para usuarios de IAM.

Recursos adicionales

Administración de contraseñas

Columnas de informes

- Política de contraseñas
- Mayúsculas
- Minúsculas
- Número
- No alfanuméricos

MFA en la cuenta raíz

Descripción

Verifica la cuenta raíz y advierte si la autenticación multifactor (MFA) no está habilitada.

Para aumentar la seguridad, le recomendamos que proteja su cuenta mediante la MFA, que requiere que el usuario introduzca un código de autenticación único desde su hardware o dispositivo virtual de MFA al interactuar con los sitios web y los AWS Management Console sitios web asociados.

ID de la verificación

`7DAFEmoDos`

Criterios de alerta

Rojo: la MFA no está habilitada en la cuenta raíz.

Acción recomendada

Inicie sesión en su cuenta raíz y active un dispositivo MFA. Consulte Comprobación de estado de MFA y Configuración de un dispositivo MFA.

Recursos adicionales

Uso de dispositivos de autenticación multifactor (MFA) con AWS

Grupos de seguridad: puertos específicos sin restricciones

Descripción

Verifica los grupos de seguridad en busca de reglas que permitan el acceso sin restricciones (0.0.0.0/0) a puertos específicos.

El acceso sin restricciones aumenta las posibilidades de que se produzcan actividades maliciosas (hackeos, denial-of-service ataques, pérdida de datos). Los puertos con mayor riesgo se marcan en rojo y los que tienen menos riesgo en amarillo. Los puertos marcados en verde son los que suelen utilizar aplicaciones que requieren acceso sin restricciones, como, por ejemplo, HTTP y SMTP.

Si ha configurado de manera intencionada sus grupos de seguridad de esta manera, le recomendamos que utilice medidas de seguridad adicionales para proteger su infraestructura (como, por ejemplo, tablas IP).

> **Note**
>
> Esta verificación solo evalúa los grupos de seguridad que haya creado y sus reglas de entrada de direcciones IPv4. Los grupos de seguridad que crea AWS Directory Service se marcan en rojo o amarillo; sin embargo, no suponen ningún riesgo de seguridad y se pueden omitir o excluir con toda tranquilidad. Para obtener más información, consulte las Preguntas frecuentes sobre Trusted Advisor.

> **Note**
>
> Esta comprobación no incluye el caso de uso en el que una lista de prefijos gestionada por el cliente concede acceso a 0.0.0.0/0 y se utiliza como fuente con un grupo de seguridad.

ID de la verificación

`HCP4007jGY`

Criterios de alerta

- Verde: el acceso a los puertos 80, 25, 443 o 465 no está sujeto a restricciones.
- Rojo: el acceso a los puertos 20, 21, 1433, 1434, 3306, 3389, 4333, 5432 o 5500 no está sujeto a restricciones.
- Amarillo: el acceso a cualquier otro puerto no está sujeto a restricciones.

Acción recomendada

Restrinja el acceso solo a aquellas direcciones IP que lo necesiten. Para restringir el acceso a una dirección IP específica, establezca el sufijo en /32 (por ejemplo, 192.0.2.10/32). Asegúrese de eliminar las reglas excesivamente permisivas después de crear reglas más restrictivas.

Recursos adicionales

- Grupos de seguridad de Amazon EC2

  Lista de números de puertos TCP y UDP
- Enrutamiento entre dominios sin clases

Columnas de informes

- Status
- Región
- Nombre de grupo de seguridad
- ID de grupo de seguridad
- Protocolo
- Del puerto
- Al puerto

Grupos de seguridad: acceso sin restricciones

Descripción

Verifica los grupos de seguridad en busca de reglas que permitan el acceso sin restricciones a un recurso.

El acceso sin restricciones aumenta las posibilidades de que se produzcan actividades maliciosas (piratería informática, denial-of-service ataques, pérdida de datos).

> **Note**
>
> Esta verificación solo evalúa los grupos de seguridad que haya creado y sus reglas de entrada de direcciones IPv4. Los grupos de seguridad que crea AWS Directory Service se marcan en rojo o amarillo; sin embargo, no suponen ningún riesgo de seguridad y se pueden omitir o excluir con toda tranquilidad. Para obtener más información, consulte las Preguntas frecuentes sobre Trusted Advisor.

> **Note**
>
> Esta comprobación no incluye el caso de uso en el que una lista de prefijos gestionada por el cliente concede acceso a 0.0.0.0/0 y se utiliza como fuente con un grupo de seguridad.

ID de la verificación

`1iG5NDGVre`

Criterios de alerta

Rojo: una regla del grupo de seguridad tiene una dirección IP de origen con un sufijo /0 para otros puertos aparte del 25, 80 o 443.

Acción recomendada

Restrinja el acceso solo a aquellas direcciones IP que lo necesiten. Para restringir el acceso a una dirección IP específica, establezca el sufijo en /32 (por ejemplo, 192.0.2.10/32). Asegúrese de eliminar las reglas excesivamente permisivas después de crear reglas más restrictivas.

Recursos adicionales

- Grupos de seguridad de Amazon EC2
- Enrutamiento entre dominios sin clases

Columnas de informes

- Status
- Región
- Nombre de grupo de seguridad
- ID de grupo de seguridad
- Protocolo
- Del puerto
- Al puerto
- Rango de IP

Tolerancia a errores

Puede utilizar las siguientes verificaciones para la categoría de tolerancia a errores.

Nombres de la verificación

- ALB Multi-AZ
- La característica de búsqueda de datos anteriores del clúster de Amazon Aurora MySQL no está habilitada
- Accesibilidad de instancias de base de datos de Amazon Aurora
- Conmutación por error CloudFront de Amazon Origin
- Riesgo de acceso a los puntos de enlace de Amazon Comprehend
- Clústeres de zona de disponibilidad única de Amazon DocumentDB
- Recuperación de Amazon oint-in-time DynamoDB P
- La tabla de Amazon DynamoDB no está incluida en el plan de copia de seguridad
- Amazon EBS no está incluido en el plan AWS Backup
- Instantáneas de Amazon EBS
- Amazon EC2 Auto Scaling no tiene la característica de comprobación de estado del ELB habilitada
- El grupo de Amazon EC2 Auto Scaling tiene la característica de reequilibrio de capacidad habilitada

- Amazon EC2 Auto Scaling no se implementa en varias zonas de disponibilidad o no cumple con el número mínimo de zonas de disponibilidad
- Balance de zona de disponibilidad de Amazon EC2
- La supervisión detallada de Amazon EC2 no está habilitada
- Amazon ECS AWS registra el controlador en modo de bloqueo
- Servicio de Amazon ECS con una única zona de disponibilidad
- Estrategia de ubicación multi-AZ de Amazon ECS
- Redundancia sin destinos de montaje de Amazon EFS
- Amazon EFS no está en el AWS Backup plan
- Clústeres ElastiCache Multi-AZ de Amazon
- Amazon ElastiCache Redis Clusters Automatic Backup
- Clústeres Multi-AZ Amazon MemoryDB
- Los agentes de Amazon MSK alojan demasiadas particiones
- Dominios OpenSearch de Amazon Service con menos de tres nodos de datos
- Copias de seguridad de Amazon RDS
- Los clústeres de base de datos de Amazon RDS tienen una instancia de base de datos
- Clústeres de bases de datos de Amazon RDS con todas las instancias en la misma zona de disponibilidad
- Clústeres de bases de datos de Amazon RDS con todas las instancias de lectura en la misma zona de disponibilidad
- La supervisión mejorada de la instancia de base de datos de Amazon RDS no está habilitada
- Las instancias de base de datos de Amazon RDS tienen desactivado el escalado automático de almacenamiento
- Las instancias de base de datos de Amazon RDS que no utilizan la implementación Multi-AZ
- Amazon RDS DiskQueueDepth
- Amazon RDS FreeStorageSpace
- El parámetro log_output de Amazon RDS está establecido en una tabla
- La configuración del parámetro innodb_default_row_format de Amazon RDS no es segura
- El parámetro innodb_flush_log_at_trx_commit de Amazon RDS no es 1
- El parámetro max_user_connections de Amazon RDS es bajo
- Amazon RDS Multi-AZ

- Amazon RDS no está en el plan AWS Backup
- Las réplicas de lectura de Amazon RDS están abiertas en modo grabable
- Las copias de seguridad automatizadas de recursos de Amazon RDS están desactivadas
- El parámetro sync_binlog de Amazon RDS está desactivado
- El clúster de base de datos de RDS no tiene habilitada la replicación Multi-AZ
- Instancia de reserva Multi-AZ de RDS no habilitada
- Amazon RDS ReplicaLag
- El parámetro synchronous_commit de Amazon RDS está desactivado
- Instantánea automática de clúster de Amazon Redshift
- Comprobaciones de estado eliminadas de Amazon Route 53
- Conjuntos de registros de recursos de conmutación por error en Amazon Route 53
- Conjuntos de registros de recursos con alto valor de TTL en Amazon Route 53
- Delegaciones de servidores de nombres de Amazon Route 53
- Amazon Route 53 Resolver Redundancia de zonas de disponibilidad de puntos finales
- Registro de bucket de Amazon S3
- La replicación de bucket de Amazon S3 no está habilitada
- Amazon S3 Bucket Versioning
- Los equilibradores de carga de aplicaciones, las redes y las puertas de enlace no abarcan varias zonas de disponibilidad
- IP con escalado automático disponible en subredes
- Comprobación de estado de grupos de Auto Scaling
- Recursos de grupos de Auto Scaling
- Los clústeres de AWS CloudHSM que ejecutan instancias de HSM en una sola AZ
- AWS Direct Connect Resiliencia de ubicación
- AWS Lambda funciona sin configurar una cola de letra muerta
- AWS Lambda Sobre los destinos de los eventos de falla
- Funciones habilitadas para VPC de AWS Lambda sin redundancia Multi-AZ
- AWS Resilience Hub Comprobación de componentes de la aplicación
- AWS Resilience Hub política incumplida
- AWS Resilience Hub puntuaciones de resiliencia
- AWS Resilience Hub edad de evaluación

- AWS Site-to-Site VPN tiene al menos un túnel en estado INACTIVO
- Problemas de alto riesgo de AWS Well-Architected para la fiabilidad
- El equilibrador de carga clásico no tiene configuradas varias zonas de disponibilidad
- Connection Draining de ELB
- Optimización del balanceador de carga
- Independencia de la zona de disponibilidad de la puerta de enlace de NAT
- Equilibrador de carga cruzado del equilibrador de carga de red
- NLB: recurso con acceso a Internet en una subred privada
- NLB Multi-AZ
- Número de Regiones de AWS en un conjunto de réplicas de Incident Manager
- Comprobación de aplicaciones con zona de disponibilidad única
- Interfaz de VPC: interfaces de red de punto final en varias zonas de disponibilidad
- Redundancia de túnel de VPN
- Redundancia de la zona de disponibilidad de ActiveMQ
- Redundancia de la zona de disponibilidad de RabbitMQ

ALB Multi-AZ

Descripción

Comprueba si los balanceadores de carga de aplicaciones están configurados para usar más de una zona de disponibilidad (AZ). Una zona de disponibilidad es una ubicación diferente que queda aislada en caso de error en otras zonas. Configure el balanceador de carga en varias zonas de disponibilidad de la misma región para mejorar la disponibilidad de la carga de trabajo.

> **Note**
>
> Los resultados de esta verificación se actualizan automáticamente varias veces al día y no se permiten las solicitudes de actualización. Puede que los cambios tarden unas horas en aparecer. Actualmente, no puede excluir recursos de esta verificación.

ID de la verificación

`c1dfprch08`

Criterios de alerta

Amarillo: el ALB está en una única zona de disponibilidad.

Verde: el ALB tiene dos o más AZ.

Acción recomendada

Asegúrese de que el balanceador de carga esté configurado con al menos dos zonas de disponibilidad.

Para obtener más información, consulte Zonas de disponibilidad del equilibrador de carga de aplicación.

Recursos adicionales

Para obtener más información, consulte la siguiente documentación sobre :

- Cómo funciona Elastic Load Balancing
- Regiones, zonas de disponibilidad y zonas locales

Columnas de informes

- Status
- Región
- Nombre de ALB
- Regla ALB
- ARN DE LABORATORIO
- Número de zonas de disponibilidad
- Hora de la última actualización

La característica de búsqueda de datos anteriores del clúster de Amazon Aurora MySQL no está habilitada

Descripción

Compruebe si el clúster de Amazon Aurora MySQL tiene habilitada la característica de búsqueda de datos anteriores.

La característica de búsqueda de datos anteriores del clúster de Amazon Aurora MySQL permite restaurar un clúster de base de datos Aurora a un momento anterior sin crear un clúster nuevo.

Permite revertir la base de datos a un momento específico en el tiempo dentro de un período de retención, sin necesidad de restaurar desde una instantánea.

Puede ajustar el intervalo de tiempo de retroceso (horas) en el BacktrackWindowInHoursparámetro de las reglas. AWS Config

Para obtener más información, consulte Búsqueda de datos anteriores de un clúster de bases de datos de Aurora.

> **Note**
>
> Los resultados de esta verificación se actualizan automáticamente varias veces al día y no se permiten las solicitudes de actualización. Puede que los cambios tarden unas horas en aparecer. Actualmente, no puede excluir recursos de esta verificación.

ID de la verificación

`c18d2gz131`

Origen

`AWS Config Managed Rule: aurora-mysql-backtracking-enabled`

Criterios de alerta

Amarillo: la característica de búsqueda de datos anteriores de los clústeres de Amazon Aurora MySQL no está habilitada.

Acción recomendada

Active la característica de búsqueda de datos anteriores del clúster de Amazon Aurora MySQL.

Para obtener más información, consulte Búsqueda de datos anteriores de un clúster de bases de datos de Aurora.

Recursos adicionales

Búsqueda de datos anteriores de un clúster de base de datos de Aurora

Columnas de informes

- Status
- Región

- Recurso
- AWS Config Regla
- Parámetros de entrada
- Hora de la última actualización

Accesibilidad de instancias de base de datos de Amazon Aurora

Descripción

Verifica los casos en los que un clúster de base de datos de Amazon Aurora tenga instancias privadas y públicas.

En caso de error en la instancia principal, se puede promover una réplica a una instancia principal. Si dicha réplica es privada, los usuarios que solo tengan acceso público ya no podrán conectarse a la base de datos después de la conmutación por error. Se recomienda que todas las instancias de base de datos de un clúster tengan la misma accesibilidad.

ID de la verificación

`xuy7H1avtl`

Criterios de alerta

Amarillo: las instancias de un clúster de base de datos de Aurora tienen una accesibilidad diferente (una combinación de pública y privada).

Acción recomendada

Modificar la configuración `Publicly Accessible` de las instancias en el clúster de base de datos para que todas sean públicas o privadas. Para obtener información más detallada, consulte las instrucciones para instancias de MySQL en Modificación de una instancia de base de datos que ejecuta el motor de base de datos MySQL.

Recursos adicionales

Tolerancia a errores de un clúster de base de datos de Aurora

Columnas de informes

- Status
- Región
- Clúster

- Instancias de bases de datos públicas
- Instancias de bases de datos privadas
- Motivo

Conmutación por error CloudFront de Amazon Origin

Descripción

Comprueba que un grupo de origen esté configurado para las distribuciones que incluyen dos orígenes en Amazon CloudFront.

Para obtener más información, consulte Optimización de la alta disponibilidad con la conmutación por error de CloudFront origen.

> **Note**
>
> Los resultados de esta verificación se actualizan automáticamente varias veces al día y no se permiten las solicitudes de actualización. Puede que los cambios tarden unas horas en aparecer. Actualmente, no puede excluir recursos de esta verificación.

ID de la verificación

`c18d2gz112`

Origen

`AWS Config Managed Rule: cloudfront-origin-failover-enabled`

Criterios de alerta

Amarillo: la conmutación por error de Amazon CloudFront Origin no está habilitada.

Acción recomendada

Asegúrese de activar la función de conmutación por error de origen en sus CloudFront distribuciones para garantizar una alta disponibilidad de la entrega de contenido a los usuarios finales. Al activar esta característica, el tráfico se direcciona automáticamente al servidor de origen de respaldo si el servidor de origen principal no está disponible. Esto minimiza el posible tiempo de inactividad y garantiza la disponibilidad continua del contenido.

Columnas de informes

- Status
- Región
- Recurso
- AWS Config Regla
- Parámetros de entrada
- Hora de la última actualización

Riesgo de acceso a los puntos de enlace de Amazon Comprehend

Descripción

Comprueba los permisos de la clave AWS Key Management Service (AWS KMS) de un punto final en el que se cifró el modelo subyacente mediante claves administradas por el cliente. Si la clave administrada por el cliente está desactivada, o si se ha modificado la política de clave para modificar los permisos permitidos para Amazon Comprehend, la disponibilidad del punto de enlace podría verse afectada.

> **Note**
>
> Los resultados de esta verificación se actualizan automáticamente varias veces al día y no se permiten las solicitudes de actualización. Puede que los cambios tarden unas horas en aparecer. Actualmente, no puede excluir recursos de esta verificación.

ID de la verificación

`Cm24dfsM13`

Criterios de alerta

Rojo: la clave administrada por el cliente está deshabilitada o se ha modificado la política de claves para modificar los permisos autorizados para el acceso a Amazon Comprehend.

Acción recomendada

Si la clave administrada por el cliente estaba deshabilitada, le recomendamos habilitarla. Para obtener más información, consulte Habilitar claves. Si se modificó la política de claves y desea

seguir utilizando el punto final, le recomendamos que actualice la política de AWS KMS claves. Para obtener más información, consulte Cambiar una política de claves.

Recursos adicionales

AWS KMS Permisos

Columnas de informes

- Status
- Región
- ARN de punto de conexión
- ARN de modelo
- KMS KeyId
- Hora de la última actualización

Clústeres de zona de disponibilidad única de Amazon DocumentDB

Descripción

Comprueba si hay clústeres de Amazon DocumentDB configurados como Single-AZ.

La ejecución de cargas de trabajo de Amazon DocumentDB en una arquitectura Single-AZ no es suficiente para cargas de trabajo muy críticas y la recuperación de un fallo de un componente puede tardar hasta 10 minutos. Los clientes deben implementar instancias de réplica en zonas de disponibilidad adicionales para garantizar la disponibilidad durante el mantenimiento, los fallos de instancias, los fallos de los componentes o los fallos de la zona de disponibilidad.

> **Note**
>
> Los resultados de esta comprobación se actualizan automáticamente una o más veces al día y no se admiten solicitudes de actualización. Puede que los cambios tarden unas horas en aparecer. Actualmente, no puede excluir recursos de esta verificación.

ID de la verificación

`c15vnddn2x`

Criterios de alerta

Amarillo: el clúster de Amazon DocumentDB tiene instancias en menos de tres zonas de disponibilidad.

Verde: el clúster de Amazon DocumentDB tiene instancias en tres zonas de disponibilidad.

Acción recomendada

Si su aplicación requiere una alta disponibilidad, modifique la instancia de base de datos para habilitar Multi-AZ mediante instancias de réplica. Consulte Alta disponibilidad y replicación de Amazon DocumentDB

Recursos adicionales

Descripción de la tolerancia a errores del clúster de Amazon DocumentDB

Regiones y zonas de disponibilidad

Columnas de informes

- Status
- Región
- Zona de disponibilidad
- DB Cluster Identifier (Identificador de clúster de base de datos)
- ARN del clúster de base de datos
- Hora de la última actualización

Recuperación de Amazon oint-in-time DynamoDB P

Descripción

Compruebe si la recuperación a un momento dado está habilitada para las tablas de Amazon DynamoDB.

La recuperación a un momento dado protege a las tablas de DynamoDB de operaciones accidentales de escritura o eliminación. Al habilitar la recuperación a un momento dado, ya no tiene que preocuparse por crear, mantener o planificar copias de seguridad bajo demanda. La recuperación a un momento dado restaura la tabla a cualquier momento de los últimos 35 días. DynamoDB mantiene backups acumulativos de la tabla.

Para obtener más información, consulte oint-in-time Recuperación de P para DynamoDB.

> **Note**
>
> Los resultados de esta verificación se actualizan automáticamente varias veces al día y no se permiten las solicitudes de actualización. Puede que los cambios tarden unas horas en aparecer. Actualmente, no puede excluir recursos de esta verificación.

ID de la verificación

`c18d2gz138`

Origen

`AWS Config Managed Rule: dynamodb-pitr-enabled`

Criterios de alerta

Amarillo: la oint-in-time recuperación de P no está habilitada para las tablas de DynamoDB.

Acción recomendada

Active la point-in-time recuperación en Amazon DynamoDB para realizar copias de seguridad continuas de los datos de la tabla.

Para obtener más información, consulte oint-in-time Recuperación de P: cómo funciona.

Recursos adicionales

oint-in-time Recuperación de PC para DynamoDB

Columnas de informes

- Status
- Región
- Recurso
- AWS Config Regla
- Parámetros de entrada
- Hora de la última actualización

La tabla de Amazon DynamoDB no está incluida en el plan de copia de seguridad

Descripción

Comprueba si las tablas de Amazon DynamoDB forman parte de un plan. AWS Backup

AWS Backup proporciona copias de seguridad incrementales para las tablas de DynamoDB que capturan los cambios realizados desde la última copia de seguridad. La inclusión de tablas de DynamoDB en AWS Backup un plan ayuda a proteger los datos de situaciones de pérdida accidental de datos y automatiza el proceso de copia de seguridad. Esto proporciona una solución de respaldo confiable y escalable para las tablas de DynamoDB, lo que garantiza que los datos valiosos estén protegidos y disponibles para su recuperación según sea necesario.

Para obtener más información, consulte Crear copias de seguridad de tablas de DynamoDB con AWS Backup

> **Note**
>
> Los resultados de esta verificación se actualizan automáticamente varias veces al día y no se permiten las solicitudes de actualización. Puede que los cambios tarden unas horas en aparecer. Actualmente, no puede excluir recursos de esta verificación.

ID de la verificación

`c18d2gz107`

Origen

`AWS Config Managed Rule: dynamodb-in-backup-plan`

Criterios de alerta

Amarillo: la tabla Amazon DynamoDB no está incluida en el plan. AWS Backup

Acción recomendada

Asegúrese de que las tablas de Amazon DynamoDB formen parte de un plan. AWS Backup

Recursos adicionales

Copias de seguridad programadas

¿Qué es? AWS Backup

Creación de planes de copia de seguridad mediante la consola de AWS Backup

Columnas de informes

- Status
- Región
- Recurso
- AWS Config Regla
- Parámetros de entrada
- Hora de la última actualización

Amazon EBS no está incluido en el plan AWS Backup

Descripción

Comprueba si los volúmenes de Amazon EBS están presentes en los planes de backup de. AWS Backup

Incluya los volúmenes de Amazon EBS en un AWS Backup plan para automatizar las copias de seguridad periódicas de los datos almacenados en esos volúmenes. Esto evita la pérdida de datos, simplifica la gestión de datos y posibilita la restauración cuando sea necesario. Un plan de copia de seguridad garantiza la seguridad de los datos y garantiza que se cumplan los objetivos de tiempo y punto de recuperación (RTO/RPO) de las aplicaciones y servicios.

Para obtener más información, consulte Creación de un plan de copia de seguridad

> **Note**
>
> Los resultados de esta verificación se actualizan automáticamente varias veces al día y no se permiten las solicitudes de actualización. Puede que los cambios tarden unas horas en aparecer. Actualmente, no puede excluir recursos de esta verificación.

ID de la verificación

`c18d2gz106`

Origen

```
AWS Config Managed Rule: ebs-in-backup-plan
```

Criterios de alerta

Amarillo: el volumen de Amazon EBS no está incluido en el AWS Backup plan.

Acción recomendada

Asegúrese de que sus volúmenes de Amazon EBS formen parte de un AWS Backup plan.

Recursos adicionales

Creación de planes de respaldo mediante la consola AWS Backup

¿Qué es AWS Backup?

Primeros pasos 3: creación de una copia de seguridad programada

Columnas de informes

- Status
- Región
- Recurso
- AWS Config Regla
- Parámetros de entrada
- Hora de la última actualización

Instantáneas de Amazon EBS

Descripción

Verifica la antigüedad de las instantáneas de los volúmenes de Amazon Elastic Block Store (Amazon EBS) (disponibles o en uso).

Aunque los volúmenes de Amazon EBS se replican, pueden producirse errores. Las instantáneas se conservan en Amazon Simple Storage Service (Amazon S3) para un almacenamiento y una recuperación duraderos. point-in-time

ID de la verificación

```
H7IgTzjTYb
```

Criterios de alerta

- Amarillo: la instantánea de volumen más reciente tiene entre 7 y 30 días.
- Rojo: la instantánea de volumen más reciente tiene más de 30 días.
- Rojo: el volumen no tiene una instantánea.

Acción recomendada

Cree instantáneas semanales o mensuales de los volúmenes. Para obtener más información, consulte Creación de una instantánea de Amazon EBS.

Recursos adicionales

Amazon Elastic Block Store (Amazon EBS)

Columnas de informes

- Status
- Región
- ID de volumen
- Nombre del volumen
- ID de instantánea
- Nombre de la instantánea
- Antigüedad de la instantánea
- Asociación de volúmenes
- Motivo

Amazon EC2 Auto Scaling no tiene la característica de comprobación de estado del ELB habilitada

Descripción

Compruebe si los grupos de Amazon EC2 Auto Scaling asociados a un equilibrador de carga clásico utilizan las comprobaciones de estado del Elastic Load Balancing. Las comprobaciones de estado predeterminadas de un grupo de escalado automático son solo comprobaciones de estado de EC2. Si una instancia no supera estas comprobaciones de estado, se marca como en mal estado y se termina. En ese caso, Amazon EC2 Auto Scaling lanza una instancia de remplazo. La comprobación de estado del Elastic Load Balancing monitorea las instancias de

Amazon EC2 de forma periódica para detectar y terminar las instancias en mal estado y, a continuación, lanzar nuevas instancias.

Para obtener más información, consulte Añadir comprobaciones de estado de Elastic Load Balancing.

> **Note**
>
> Los resultados de esta verificación se actualizan automáticamente varias veces al día y no se permiten las solicitudes de actualización. Puede que los cambios tarden unas horas en aparecer. Actualmente, no puede excluir recursos de esta verificación.

ID de la verificación

`c18d2gz104`

Origen

`AWS Config Managed Rule: autoscaling-group-elb-healthcheck-required`

Criterios de alerta

Amarillo: las comprobaciones de estado de Elastic Load Balancing del grupo Amazon EC2 Auto Scaling asociado al equilibrador de carga clásico no están habilitadas.

Acción recomendada

Asegúrese de que los grupos de escalado automático asociados a un equilibrador de carga clásico utilizan las comprobaciones de estado de Elastic Load Balancing.

Las comprobaciones de estado de Elastic Load Balancing indican si el equilibrador de carga está en buen estado y disponible para gestionar las solicitudes. Esto garantiza una alta disponibilidad de la aplicación.

Para más información, consulte Adición de comprobaciones de estado de Elastic Load Balancing a un grupo de escalado automático

Columnas de informes

- Status
- Región
- Recurso

- AWS Config Regla
- Parámetros de entrada
- Hora de la última actualización

El grupo de Amazon EC2 Auto Scaling tiene la característica de reequilibrio de capacidad habilitada

Descripción

Compruebe si la característica de reequilibrio de capacidad está habilitada para los grupos de Amazon EC2 Auto Scaling que utilizan varios tipos de instancia.

Configurar a los grupos de Amazon EC2 Auto Scaling con la característica de reequilibrio de capacidad garantiza que las instancias de Amazon EC2 se distribuyan uniformemente en las zonas de disponibilidad, independientemente de los tipos de instancia y de las opciones de compra. Utiliza una política de seguimiento de objetivos asociada al grupo, como el uso de la CPU o el tráfico de red.

Para obtener más información, consulte Grupos de escalado automático con varios tipos de instancia y opciones de compra.

> **Note**
>
> Los resultados de esta verificación se actualizan automáticamente varias veces al día y no se permiten las solicitudes de actualización. Puede que los cambios tarden unas horas en aparecer. Actualmente, no puede excluir recursos de esta verificación.

ID de la verificación

`AWS Config c18d2gz103`

Origen

AWS Config Regla gestionada: autoscaling-capacity-rebalancing

Criterios de alerta

Amarillo: la característica de reequilibrio de capacidad del grupo de Amazon EC2 Auto Scaling no está habilitada.

Acción recomendada

Asegúrese de que la característica de reequilibrio de capacidad esté habilitada para los grupos de Amazon EC2 Auto Scaling que utilizan varios tipos de instancia.

Para obtener más información, consulte Habilitar reequilibrio de capacidad (consola)

Columnas de informes

- Status
- Región
- Recurso
- AWS Config Regla
- Parámetros de entrada
- Hora de la última actualización

Amazon EC2 Auto Scaling no se implementa en varias zonas de disponibilidad o no cumple con el número mínimo de zonas de disponibilidad

Descripción

Compruebe si el grupo de Amazon EC2 Auto Scaling se implementa en varias zonas de disponibilidad o en el número mínimo de zonas de disponibilidad especificado. Implemente instancias de Amazon EC2 en varias zonas de disponibilidad para garantizar una alta disponibilidad.

Puede ajustar el número mínimo de zonas de disponibilidad mediante el AvailibilityZones parámetro min de sus AWS Config reglas.

Para obtener más información, consulte Grupos de escalado automático con varios tipos de instancia y opciones de compra.

ID de la verificación

```
c18d2gz101
```

Origen

```
AWS Config Managed Rule: autoscaling-multiple-az
```

Criterios de alerta

Rojo: el grupo de Amazon EC2 Auto Scaling no tiene configuradas varias zonas de disponibilidad o no cumple con el número mínimo de zonas de disponibilidad especificado.

Acción recomendada

Asegúrese de que el grupo de Amazon EC2 Auto Scaling esté configurado con varias zonas de disponibilidad. Implemente instancias de Amazon EC2 en varias zonas de disponibilidad para garantizar una alta disponibilidad.

Recursos adicionales

Creación de un grupo de escalado automático mediante una plantilla de lanzamiento

Crear un grupo de escalado automático mediante una configuración de lanzamiento

Columnas de informes

- Status
- Región
- Recurso
- AWS Config Regla
- Parámetros de entrada
- Hora de la última actualización

Balance de zona de disponibilidad de Amazon EC2

Descripción

Verifica la distribución de instancias de Amazon Elastic Compute Cloud (Amazon EC2) entre las zonas de disponibilidad de una región.

Las zonas de disponibilidad son ubicaciones diferentes aisladas de los errores que se producen en otras zonas de disponibilidad. Proporcionan conectividad de red económica y de baja latencia entre las zonas de disponibilidad de la misma región. Al lanzar instancias en múltiples zonas de disponibilidad de una misma región, puede proteger sus aplicaciones frente a los puntos de error únicos.

ID de la verificación

`wuy7G1zxql`

Criterios de alerta

- Amarillo: la región tiene instancias en varias zonas, pero la distribución es desigual (la diferencia entre los recuentos de instancias más altos y más bajos en las zonas de disponibilidad utilizadas es superior al 20 %).
- Rojo: la región solo tiene instancias en una única zona de disponibilidad.

Acción recomendada

Equilibre las instancias de Amazon EC2 de manera uniforme en varias zonas de disponibilidad. Para ello, lance instancias manualmente o utilice Auto Scaling para hacerlo automáticamente. Para obtener más información, consulte Lanzar la instancia y Usar un equilibrador de carga con un grupo de escalado automático.

Recursos adicionales

Guía del usuario de Amazon EC2 Auto Scaling

Columnas de informes

- Status
- Región
- Instancias de zona a
- Instancias de zona b
- Instancias de zona c
- Instancias de zona e
- Instancias de zona f
- Motivo

La supervisión detallada de Amazon EC2 no está habilitada

Descripción

Compruebe si la supervisión detallada está habilitada para las instancias de Amazon EC2.

La supervisión detallada de Amazon EC2 proporciona métricas más frecuentes, publicadas a intervalos de un minuto, en lugar de los intervalos de cinco minutos utilizados en la supervisión básica de Amazon EC2. Habilitar la supervisión detallada de Amazon EC2 le permite administrar mejor los recursos de Amazon EC2, de modo que pueda encontrar tendencias y actuar con mayor rapidez.

Para obtener más información, consulte Supervisión básica y detallada.

> **Note**
>
> Los resultados de esta verificación se actualizan automáticamente varias veces al día y no se permiten las solicitudes de actualización. Puede que los cambios tarden unas horas en aparecer. Actualmente, no puede excluir recursos de esta verificación.

ID de la verificación

`AWS Config c18d2gz144`

Origen

AWS Config Regla administrada: ec2-instance-detailed-monitoring-enabled

Criterios de alerta

Amarillo: la supervisión detallada no está habilitada para las instancias de Amazon EC2.

Acción recomendada

Active la supervisión detallada de sus instancias de Amazon EC2 para aumentar la frecuencia con la que se publican los datos de métricas de Amazon EC2 en CloudWatch Amazon (de 5 a 1 minuto).

Columnas de informes

- Status
- Región
- Recurso
- AWS Config Regla
- Parámetros de entrada
- Hora de la última actualización

Amazon ECS AWS registra el controlador en modo de bloqueo

Descripción

Comprueba las definiciones de tareas de Amazon ECS configuradas con el controlador de registro AWS Logs en modo de bloqueo. Un controlador configurado en el modo de bloqueo pone en riesgo la disponibilidad del sistema.

> **Note**
>
> Los resultados de esta comprobación se actualizan automáticamente una o más veces al día y no se admiten solicitudes de actualización. Puede que los cambios tarden unas horas en aparecer. Actualmente, no puede excluir recursos de esta verificación.

ID de la verificación

`c1dvkm4z6b`

Criterios de alerta

Amarillo: el modo de parámetro de configuración de registro del controlador awslogs está configurado como bloqueado o ausente. Si falta un parámetro de modo, se indica una configuración de bloqueo predeterminada.

Verde: la definición de tareas de Amazon ECS no utiliza el controlador awslogs o el controlador awslogs está configurado en modo sin bloqueo.

Acción recomendada

Para mitigar el riesgo de disponibilidad, considere la posibilidad de cambiar la configuración del controlador de AWS registros de la definición de tareas de bloqueante a no bloqueante. En el modo sin bloqueo, tendrá que establecer un valor para el max-buffer-size parámetro. Para obtener más información y orientación sobre los parámetros de configuración, consulte. Consulte Evitar la pérdida de registros con el modo sin bloqueo en el controlador de registro del contenedor de AWS registros

Recursos adicionales

Uso del controlador de registro AWS de registros

Elegir las opciones de registro de contenedores para evitar la contrapresión

Evitar la pérdida de registros con el modo sin bloqueo en el controlador de AWS registros del contenedor Logs

Columnas de informes

- Status
- Región
- Definición de tarea (ARN)
- Nombres de definiciones de contenedores
- Hora de la última actualización

Servicio de Amazon ECS con una única zona de disponibilidad

Descripción

Compruebe que la configuración del servicio utiliza una única zona de disponibilidad (AZ).

Una zona de disponibilidad es una ubicación diferente que queda aislada en caso de error en otras zonas. Esto permite una conectividad de red económica y de baja latencia entre zonas de disponibilidad dentro de una misma Región de AWS. Al lanzar instancias en múltiples zonas de disponibilidad de una misma región, puede proteger a sus aplicaciones de un único punto de error.

> **Note**
>
> Los resultados de esta verificación se actualizan automáticamente varias veces al día y no se permiten las solicitudes de actualización. Puede que los cambios tarden unas horas en aparecer. Actualmente, no puede excluir recursos de esta verificación.

ID de la verificación

`c1z7dfpz01`

Criterios de alerta

- Amarillo: un servicio de Amazon ECS ejecuta todas las tareas en una única zona de disponibilidad.
- Verde: un servicio de Amazon ECS ejecuta tareas en al menos dos zonas de disponibilidad diferentes.

Acción recomendada

Cree al menos una tarea más para el servicio en una zona de disponibilidad diferente.

Recursos adicionales

Capacidad y disponibilidad de Amazon ECS

Columnas de informes

- Status
- Región
- Nombre del clúster ECS/nombre del servicio ECS
- Número de zonas de disponibilidad
- Hora de la última actualización

Estrategia de ubicación multi-AZ de Amazon ECS

Descripción

Compruebe que su servicio de Amazon ECS utilice la estrategia de ubicación por distribución en función de la zona de disponibilidad (AZ). Esta estrategia distribuye las tareas entre las distintas zonas de disponibilidad de la misma forma Región de AWS y puede ayudar a proteger sus aplicaciones frente a un único punto de fallo.

Para las tareas que se ejecutan como parte de un servicio de Amazon ECS, la distribución es la estrategia de ubicación de tareas por defecto.

Esta comprobación también verifica que la distribución sea la primera o la única estrategia de la lista de estrategias de ubicación habilitadas.

> **Note**
>
> Los resultados de esta verificación se actualizan automáticamente varias veces al día y no se permiten las solicitudes de actualización. Puede que los cambios tarden unas horas en aparecer. Actualmente, no puede excluir recursos de esta verificación.

ID de la verificación

`c1z7dfpz02`

Criterios de alerta

- Amarillo: la distribución por zona de disponibilidad no está habilitada o no es la primera estrategia de la lista de estrategias de ubicación habilitadas para su servicio de Amazon ECS.
- Verde: la distribución por zona de disponibilidad es la primera estrategia de la lista de estrategias de ubicación habilitadas o la única estrategia de ubicación habilitada para su servicio de Amazon ECS.

Acción recomendada

Utilice la estrategia de distribución de tareas para distribuir las tareas entre varias zonas de disponibilidad. Compruebe que la distribución por zonas de disponibilidad sea la primera estrategia para todas las estrategias de ubicación de tareas habilitadas o la única estrategia utilizada. Si opta por administrar la ubicación de las zonas de disponibilidad, puede utilizar un servicio duplicado en otra zona de disponibilidad para mitigar estos riesgos.

Recursos adicionales

Estrategias de ubicación de tareas de Amazon ECS

Columnas de informes

- Status
- Región
- Nombre del clúster ECS/nombre del servicio ECS
- La estrategia de distribución de tareas ha sido habilitada y aplicada correctamente
- Hora de la última actualización

Redundancia sin destinos de montaje de Amazon EFS

Descripción

Compruebe si los puntos de montaje existen en varias zonas de disponibilidad para un sistema de archivos de Amazon EFS.

Una zona de disponibilidad es una ubicación diferente que queda aislada en caso de error en otras zonas. Al crear puntos de montaje en varias zonas de disponibilidad separadas geográficamente dentro de una región de AWS, los sistemas de archivos de Amazon EFS pueden alcanzar los niveles más altos de disponibilidad y de durabilidad.

> **Note**
>
> Los resultados de esta verificación se actualizan automáticamente varias veces al día y no se permiten las solicitudes de actualización. Puede que los cambios tarden unas horas en aparecer. Actualmente, no puede excluir recursos de esta verificación.

ID de la verificación

`c1dfprch01`

Criterios de alerta

- Amarillo: el sistema de archivos tiene 1 punto de montaje creado en una única zona de disponibilidad.

  Verde: el sistema de archivos tiene 2 o más puntos de montaje creados en varias zonas de disponibilidad.

Acción recomendada

Para los sistemas de archivos EFS que utilizan clases de almacenamiento de una zona, le recomendamos que cree nuevos sistemas de archivos que utilicen clases de almacenamiento estándar mediante la restauración de una copia de seguridad en un nuevo sistema de archivos. Luego, cree puntos de montaje en varias zonas de disponibilidad.

Para los sistemas de archivos EFS que utilizan clases de almacenamiento estándar, se recomienda crear puntos de montaje en varias zonas de disponibilidad.

Recursos adicionales

- Administración de los puntos de montaje mediante la consola de Amazon EFS
- Cuotas y límites de Amazon EFS

Columnas de informes

- Status
- Región
- ID del sistema de archivos de EFS
- Número de puntos de montaje
- Número de zonas de disponibilidad
- Hora de la última actualización

Amazon EFS no está en el AWS Backup plan

Descripción

Comprueba si los sistemas de archivos Amazon EFS están incluidos en los planes de backup con AWS Backup.

AWS Backup es un servicio de respaldo unificado diseñado para simplificar la creación, migración, restauración y eliminación de copias de seguridad y, al mismo tiempo, mejorar la elaboración de informes y la auditoría.

Para obtener más información, consulte Backing up your Amazon EFS file systems (Copias de seguridad de los sistemas de archivos Amazon EFS).

ID de la verificación

`c18d2gz117`

Origen

`AWS Config Managed Rule: EFS_IN_BACKUP_PLAN`

Criterios de alerta

Rojo: Amazon EFS no está incluido en el AWS Backup plan.

Acción recomendada

Asegúrese de que sus sistemas de archivos Amazon EFS estén incluidos en su AWS Backup plan para protegerlos contra la pérdida accidental o la corrupción de los datos.

Recursos adicionales

Copia de seguridad de los sistemas de archivos de Amazon EFS

Backup y restauración de Amazon EFS mediante AWS Backup.

Columnas de informes

- Status
- Región
- Recurso
- AWS Config Regla
- Parámetros de entrada
- Hora de la última actualización

Clústeres ElastiCache Multi-AZ de Amazon

Descripción

Comprueba los ElastiCache clústeres que se despliegan en una única zona de disponibilidad (AZ). Esta comprobación avisa si Multi-AZ está inactiva en un clúster.

Las implementaciones en varias zonas de disponibilidad mejoran la disponibilidad de los ElastiCache clústeres al replicar de forma asíncrona en réplicas de solo lectura de una zona de disponibilidad diferente. Cuando se realiza un mantenimiento planificado del clúster o si un nodo principal no está disponible, se convierte automáticamente una réplica en principal. ElastiCache Esta conmutación por error permite reanudar las operaciones de escritura del clúster y no requiere la intervención de un administrador.

> **Note**
>
> Los resultados de esta verificación se actualizan automáticamente varias veces al día y no se permiten las solicitudes de actualización. Puede que los cambios tarden unas horas en aparecer. Actualmente, no puede excluir recursos de esta verificación.

ID de la verificación

`ECHdfsQ402`

Criterios de alerta

- Verde: Multi-AZ está activa en el clúster.
- Amarillo: Multi-AZ está inactiva en el clúster.

Acción recomendada

Cree al menos una réplica por partición, en una AZ diferente a la principal.

Recursos adicionales

Para obtener más información, consulte Minimizar el tiempo de inactividad en ElastiCache Redis con Multi-AZ.

Columnas de informes

- Status
- Región

- Nombre del clúster
- Hora de la última actualización

Amazon ElastiCache Redis Clusters Automatic Backup

Descripción

Comprueba si los clústeres de Amazon ElastiCache for Redis tienen activada la copia de seguridad automática y si el período de retención de instantáneas supera el límite especificado o predeterminado de 15 días. Cuando las copias de seguridad automáticas están habilitadas, ElastiCache crea una copia de seguridad del clúster a diario.

Puede especificar el límite de retención de instantáneas que desee mediante los RetentionPeriod parámetros de instantáneas de sus AWS Config reglas.

Para obtener más información, consulte Backup and restore ElastiCache for Redis.

> **Note**
>
> Los resultados de esta verificación se actualizan automáticamente varias veces al día y no se permiten las solicitudes de actualización. Puede que los cambios tarden unas horas en aparecer. Actualmente, no puede excluir recursos de esta verificación.

ID de la verificación

`c18d2gz178`

Origen

`AWS Config Managed Rule: elasticache-redis-cluster-automatic-backup-check`

Criterios de alerta

Rojo: los clústeres de Amazon ElastiCache for Redis no tienen activada la copia de seguridad automática o el período de retención de instantáneas está por debajo del límite.

Acción recomendada

Asegúrese de que los clústeres de Amazon ElastiCache for Redis tengan la copia de seguridad automática activada y que el período de retención de instantáneas supere el límite especificado o

predeterminado de 15 días. Las copias de seguridad automáticas pueden ayudarle a protegerse frente a la pérdida de datos. En caso de error, puede crear un nuevo clúster y restaurar los datos de la copia de seguridad más reciente.

Para obtener más información, consulte Backup and restore ElastiCache for Redis.

Recursos adicionales

Para obtener más información, consulte Programar copias de seguridad automáticas.

Columnas de informes

- Status
- Región
- Nombre del clúster
- Hora de la última actualización

Clústeres Multi-AZ Amazon MemoryDB

Descripción

Verifica los clústeres MemoryDB que se implementan en una sola zona de disponibilidad (AZ). Esta comprobación avisa si Multi-AZ está inactiva en un clúster.

Las implementaciones en varias AZ mejoran la disponibilidad del clúster MemoryDB mediante la replicación asincrónica en réplicas de solo lectura en una AZ diferente. Cuando se lleva a cabo el mantenimiento planificado del clúster o si un nodo principal no está disponible, MemoryDB promueve automáticamente una réplica al nodo principal. Esta conmutación por error permite reanudar las operaciones de escritura del clúster y no requiere la intervención de un administrador.

> **Note**
>
> Los resultados de esta verificación se actualizan automáticamente varias veces al día y no se permiten las solicitudes de actualización. Puede que los cambios tarden unas horas en aparecer. Actualmente, no puede excluir recursos de esta verificación.

ID de la verificación

`MDBdfsQ401`

Criterios de alerta

- Verde: Multi-AZ está activa en el clúster.
- Amarillo: Multi-AZ está inactiva en el clúster.

Acción recomendada

Cree al menos una réplica por partición, en una AZ diferente a la principal.

Recursos adicionales

Para obtener más información, consulte Minimización del tiempo de inactividad en MemoryDB con Multi-AZ.

Columnas de informes

- Status
- Región
- Nombre del clúster
- Hora de la última actualización

Los agentes de Amazon MSK alojan demasiadas particiones

Descripción

Compruebe que los agentes de un clúster de Managed Streaming for Kafka (MSK) no tengan asignadas más particiones de las recomendadas.

ID de la verificación

`Cmsvnj8vf1`

Criterios de alerta

- Rojo: el agente de MSK ha alcanzado o superado el 100 % del límite máximo de particiones recomendado
- Amarillo: el MSK ha alcanzado el 80 % del límite máximo de particiones recomendado

Acción recomendada

Siga las prácticas recomendadas por MSK para escalar el clúster de MSK o eliminar las particiones no utilizadas.

Recursos adicionales

- Ajustar el tamaño del clúster

Columnas de informes

- Status
- Región
- ARN del clúster
- ID del agente
- Recuento de particiones

Dominios OpenSearch de Amazon Service con menos de tres nodos de datos

Descripción

Comprueba si los dominios OpenSearch de Amazon Service están configurados con al menos tres nodos de datos y ZoneAwarenessEnabled es verdadero. Si ZoneAwarenessEnabled está activado, Amazon OpenSearch Service garantiza que cada fragmento principal y su réplica correspondiente se asignen en distintas zonas de disponibilidad.

Para obtener más información, consulta Cómo configurar un dominio Multi-AZ en Amazon OpenSearch Service.

> **Note**
>
> Los resultados de esta verificación se actualizan automáticamente varias veces al día y no se permiten las solicitudes de actualización. Puede que los cambios tarden unas horas en aparecer. Actualmente, no puede excluir recursos de esta verificación.

ID de la verificación

```
c18d2gz183
```

Origen

```
AWS Config Managed Rule: opensearch-data-node-fault-tolerance
```

Criterios de alerta

Amarillo: los dominios OpenSearch de Amazon Service están configurados con menos de tres nodos de datos.

Acción recomendada

Asegúrese de que los dominios OpenSearch de Amazon Service estén configurados con un mínimo de tres nodos de datos. Configure un dominio Multi-AZ para mejorar la disponibilidad del clúster de Amazon OpenSearch Service mediante la asignación de nodos y la replicación de datos en tres zonas de disponibilidad de la misma región. Esta acción previene la pérdida de datos y minimiza el tiempo de inactividad en caso de error en el nodo o en el centro de datos (zona de disponibilidad).

Para obtener más información, consulte Aumentar la disponibilidad de Amazon OpenSearch Service mediante la implementación en tres zonas de disponibilidad.

Recursos adicionales

- Aumente la disponibilidad de Amazon OpenSearch Service mediante la implementación en tres zonas de disponibilidad

Columnas de informes

- Status
- Región
- Recurso
- AWS Config Regla
- Parámetros de entrada
- Hora de la última actualización

Copias de seguridad de Amazon RDS

Descripción

Verifica si hay copias de seguridad automatizadas de instancias de bases de datos de Amazon RDS.

De forma predeterminada, las copias de seguridad están habilitadas con un periodo de retención de un día. Las copias de seguridad reducen el riesgo de pérdida inesperada de datos y permiten la point-in-time recuperación.

ID de la verificación

`opQPADkZvH`

Criterios de alerta

Rojo: el periodo de retención de copia de seguridad en una instancia de base de datos es de 0 días.

Acción recomendada

Establezca el periodo de retención para la copia de seguridad automatizada de la instancia de base de datos en 1 a 35 días, lo que sea adecuado según los requisitos de la aplicación. Consulte Trabajo con copias de seguridad automatizadas.

Recursos adicionales

Introducción a Amazon RDS

Columnas de informes

- Status
- Región/AZ
- Instancia de base de datos
- ID de VPC
- Período de retención de backup

Los clústeres de base de datos de Amazon RDS tienen una instancia de base de datos

Descripción

Añada al menos otra instancia de base de datos al clúster de base de datos para mejorar la disponibilidad y el rendimiento.

> **Note**
>
> Los resultados de esta verificación se actualizan automáticamente varias veces al día y no se permiten las solicitudes de actualización. Puede que los cambios tarden unas horas en aparecer. Actualmente, no puede excluir recursos de esta verificación.

> **Note**
>
> Cuando se detiene una instancia de base de datos o un clúster de base de datos, puede ver las recomendaciones de Amazon RDS en un plazo Trusted Advisor de 3 a 5 días. Transcurridos cinco días, las recomendaciones no estarán disponibles en Trusted Advisor. Para ver las recomendaciones, abra la consola de Amazon RDS y, a continuación, seleccione Recommendations.
> Si elimina una instancia de base de datos o un clúster de base de datos, las recomendaciones asociadas a esas instancias o clústeres no estarán disponibles en Trusted Advisor la consola de administración de Amazon RDS.

ID de la verificación

`c1qf5bt011`

Criterios de alerta

Amarillo: los clústeres de bases de datos solo tienen una instancia de base de datos.

Acción recomendada

Agregue una instancia de base de datos de lectura al clúster de base de datos.

Recursos adicionales

En la configuración actual, se utiliza una instancia de base de datos para las operaciones de lectura y escritura. Puede añadir otra instancia de base de datos para permitir la redistribución de la lectura y una opción de conmutación por error.

Para obtener más información, consulte Alta disponibilidad para Amazon Aurora.

Columnas de informes

- Status
- Región
- Recurso
- Nombre del motor
- Clase de instancia de base de datos
- Hora de la última actualización

Clústeres de bases de datos de Amazon RDS con todas las instancias en la misma zona de disponibilidad

Descripción

Actualmente, los clústeres de base de datos se encuentran en una sola zona de disponibilidad. Utilice varias zonas de disponibilidad para mejorar la disponibilidad.

> **Note**
>
> Los resultados de esta verificación se actualizan automáticamente varias veces al día y no se permiten las solicitudes de actualización. Puede que los cambios tarden unas horas en aparecer. Actualmente, no puede excluir recursos de esta verificación.

> **Note**
>
> Cuando se detiene una instancia de base de datos o un clúster de base de datos, puede ver las recomendaciones de Amazon RDS en un plazo Trusted Advisor de 3 a 5 días. Transcurridos cinco días, las recomendaciones no estarán disponibles en Trusted Advisor. Para ver las recomendaciones, abra la consola de Amazon RDS y, a continuación, seleccione Recommendations.
> Si elimina una instancia de base de datos o un clúster de base de datos, las recomendaciones asociadas a esas instancias o clústeres no estarán disponibles en Trusted Advisor la consola de administración de Amazon RDS.

ID de la verificación

`c1qf5bt007`

Criterios de alerta

Amarillo: los clústeres de bases de datos tienen todas las instancias en la misma zona de disponibilidad.

Acción recomendada

Agregue las instancias de base de datos a varias zonas de disponibilidad de su clúster de base de datos.

Recursos adicionales

Se recomienda añadir las instancias de base de datos a varias zonas de disponibilidad de un clúster de base de datos. Al añadir instancias de base de datos a varias zonas de disponibilidad, se mejora la disponibilidad del clúster de base de datos.

Para obtener más información, consulte Alta disponibilidad para Amazon Aurora.

Columnas de informes

- Status
- Región
- Recurso
- Nombre del motor
- Hora de la última actualización

Clústeres de bases de datos de Amazon RDS con todas las instancias de lectura en la misma zona de disponibilidad

Descripción

El clúster de base de datos dispone de todas las instancias de lector en la misma zona de disponibilidad. Le recomendamos que distribuya las instancias de Reader en varias zonas de disponibilidad de su clúster de base de datos.

La distribución aumenta la disponibilidad de la base de datos y mejora el tiempo de respuesta al reducir la latencia de la red entre los clientes y la base de datos.

> **Note**
>
> Los resultados de esta verificación se actualizan automáticamente varias veces al día y no se permiten las solicitudes de actualización. Puede que los cambios tarden unas horas en aparecer. Actualmente, no puede excluir recursos de esta verificación.

> **Note**
>
> Cuando se detiene una instancia de base de datos o un clúster de base de datos, puede ver las recomendaciones de Amazon RDS en un plazo Trusted Advisor de 3

a 5 días. Transcurridos cinco días, las recomendaciones no estarán disponibles en Trusted Advisor. Para ver las recomendaciones, abra la consola de Amazon RDS y, a continuación, seleccione Recommendations.
Si elimina una instancia de base de datos o un clúster de base de datos, las recomendaciones asociadas a esas instancias o clústeres no estarán disponibles en Trusted Advisor la consola de administración de Amazon RDS.

ID de la verificación

`c1qf5bt018`

Criterios de alerta

Rojo: los clústeres de bases de datos tienen las instancias de lectura en la misma zona de disponibilidad.

Acción recomendada

Distribuya las instancias de lectura en varias zonas de disponibilidad.

Recursos adicionales

Las zonas de disponibilidad (AZ) son ubicaciones distintas entre sí para proporcionar aislamiento en caso de interrupciones en cada AWS región. Es recomendable que distribuya la instancia principal y las instancias de lectura del clúster de base de datos entre varias AZ para mejorar la disponibilidad del clúster de base de datos. Puede crear un clúster Multi-AZ mediante la API AWS Management Console AWS CLI, o Amazon RDS al crear el clúster. También puede modificar el clúster de Aurora ya existente y convertirlo en un clúster multi-AZ agregando una nueva instancia de lector y especificando una AZ distinta.

Para obtener más información, consulte Alta disponibilidad para Amazon Aurora.

Columnas de informes

- Status
- Región
- Recurso
- Nombre del motor
- Hora de la última actualización

La supervisión mejorada de la instancia de base de datos de Amazon RDS no está habilitada

Descripción

Compruebe si las instancias de base de datos de Amazon RDS tienen habilitada la supervisión mejorada.

La supervisión de Amazon RDS proporciona métricas en tiempo real para el sistema operativo (SO) en el que se ejecuta la instancia de base de datos. Puede ver todas las métricas del sistema y la información de procesos de las instancias de base de datos de RDS en la consola de Amazon RDS. También puede personalizar el panel de control. Con la supervisión mejorada, puede ver el estado operativo de la instancia de Amazon RDS prácticamente en tiempo real, lo que le permite responder a los problemas operativos con mayor rapidez.

Puede especificar el intervalo de monitorización deseado mediante el parámetro MonitoringInterval de sus reglas. AWS Config

Para obtener más información, consulte Descripción general de la supervisión mejorada y las Métricas del sistema operativo en la supervisión mejorada.

> **Note**
>
> Los resultados de esta verificación se actualizan automáticamente varias veces al día y no se permiten las solicitudes de actualización. Puede que los cambios tarden unas horas en aparecer. Actualmente, no puede excluir recursos de esta verificación.

ID de la verificación

```
c18d2gz158
```

Origen

```
AWS Config Managed Rule: rds-enhanced-monitoring-enabled
```

Criterios de alerta

Amarillo: las instancias de base de datos de Amazon RDS no tienen habilitada la supervisión mejorada o no están configuradas con el intervalo deseado.

Acción recomendada

Habilite la supervisión mejorada de las instancias de base de datos de Amazon RDS para mejorar la visibilidad del estado operativo de las mismas.

Para obtener más información sobre la supervisión mejorada de Amazon RDS, consulte Supervisión de las métricas del SO con la supervisión mejorada.

Recursos adicionales

Métricas del sistema operativo en Supervisión mejorada

Columnas de informes

- Status
- Región
- Recurso
- AWS Config Regla
- Parámetros de entrada
- Hora de la última actualización

Las instancias de base de datos de Amazon RDS tienen desactivado el escalado automático de almacenamiento

Descripción

El escalado automático del almacenamiento de Amazon RDS no está activado en la instancia de base de datos. Cuando se produce un aumento en la carga de trabajo de la base de datos, el escalado automático de RDS Storage escala automáticamente la capacidad de almacenamiento sin tiempo de inactividad.

> **Note**
>
> Los resultados de esta verificación se actualizan automáticamente varias veces al día y no se permiten las solicitudes de actualización. Puede que los cambios tarden unas horas en aparecer. Actualmente, no puede excluir recursos de esta verificación.

> **Note**
>
> Cuando se detiene una instancia de base de datos o un clúster de base de datos, puede ver las recomendaciones de Amazon RDS en un plazo Trusted Advisor de 3 a 5 días. Transcurridos cinco días, las recomendaciones no estarán disponibles en Trusted Advisor. Para ver las recomendaciones, abra la consola de Amazon RDS y, a continuación, seleccione Recommendations.
> Si elimina una instancia de base de datos o un clúster de base de datos, las recomendaciones asociadas a esas instancias o clústeres no estarán disponibles en Trusted Advisor la consola de administración de Amazon RDS.

ID de la verificación

`c1qf5bt013`

Criterios de alerta

Rojo: las instancias de base de datos no tienen activado el escalado automático del almacenamiento.

Acción recomendada

Active el escalado automático del almacenamiento de Amazon RDS con un umbral de almacenamiento máximo especificado.

Recursos adicionales

El escalado automático del almacenamiento de Amazon RDS escala automáticamente la capacidad de almacenamiento sin tiempo de inactividad cuando aumenta la carga de trabajo de la base de datos. El escalado automático del almacenamiento monitorea el uso del almacenamiento y aumenta automáticamente la capacidad cuando el uso se acerca a la capacidad de almacenamiento aprovisionada. Puede especificar un límite máximo de almacenamiento que Amazon RDS puede asignar a la instancia de base de datos. El escalado automático del almacenamiento no conlleva ningún coste adicional. Solo paga por los recursos de Amazon RDS que se asignen a su instancia de base de datos. Le recomendamos que active el escalado automático del almacenamiento de Amazon RDS.

Para obtener más información, consulte Administrar la capacidad automáticamente con el escalado automático de almacenamiento de Amazon RDS.

Columnas de informes

- Status
- Región
- Recurso
- Valor recomendado
- Nombre del motor
- Hora de la última actualización

Las instancias de base de datos de Amazon RDS que no utilizan la implementación Multi-AZ

Descripción

Recomendamos usar la implementación multi-AZ. Las implementaciones multi-AZ mejoran la disponibilidad y la durabilidad de la instancia de base de datos.

> **Note**
>
> Los resultados de esta verificación se actualizan automáticamente varias veces al día y no se permiten las solicitudes de actualización. Puede que los cambios tarden unas horas en aparecer. Actualmente, no puede excluir recursos de esta verificación.

> **Note**
>
> Cuando se detiene una instancia de base de datos o un clúster de base de datos, puede ver las recomendaciones de Amazon RDS en un plazo Trusted Advisor de 3 a 5 días. Transcurridos cinco días, las recomendaciones no estarán disponibles en Trusted Advisor. Para ver las recomendaciones, abra la consola de Amazon RDS y, a continuación, seleccione Recommendations.
> Si elimina una instancia de base de datos o un clúster de base de datos, las recomendaciones asociadas a esas instancias o clústeres no estarán disponibles en Trusted Advisor la consola de administración de Amazon RDS.

ID de la verificación

`c1qf5bt019`

Criterios de alerta

Amarillo: las instancias de base de datos no utilizan la implementación Multi-AZ.

Acción recomendada

Configure Multi-AZ para las instancias de base de datos afectadas.

Recursos adicionales

En una implementación Multi-AZ de Amazon RDS, Amazon RDS crea automáticamente una instancia de base de datos principal y replica los datos en una instancia de una zona de disponibilidad diferente. Cuando detecta un error, Amazon RDS realiza automáticamente la conmutación por error a una instancia en espera sin intervención manual.

Para obtener más información, consulte Precios.

Columnas de informes

- Status
- Región
- Recurso
- Nombre del motor
- Hora de la última actualización

Amazon RDS DiskQueueDepth

Descripción

Comprueba si la CloudWatch métrica DiskQueueDepth muestra que el número de escrituras en cola en el almacenamiento de la base de datos de la instancia RDS ha aumentado hasta un nivel en el que debería sugerirse una investigación operativa.

ID de la verificación

`Cmsvnj8db3`

Criterios de alerta

- Rojo: la DiskQueueDepth CloudWatch métrica ha superado los 10

- Amarillo: la DiskQueueDepth CloudWatch métrica es mayor que 5 pero menor o igual a 10
- Verde: el DiskQueueDepth CloudWatch sistema métrico es menor o igual a 5

Acción recomendada

Considere la posibilidad de pasarse a instancias y volúmenes de almacenamiento que admitan las características de lectura y escritura.

Columnas de informes

- Status
- Región
- ARN de una instancia de base de datos
- DiskQueueDepth Métrico

Amazon RDS FreeStorageSpace

Descripción

Comprueba si la FreeStorageSpace CloudWatch métrica de una instancia de base de datos de RDS ha superado un umbral razonable desde el punto de vista operativo.

ID de la verificación

`Cmsvnj8db2`

Criterios de alerta

- Rojo: FreeStorageSpace ha alcanzado o superado el 90% de la capacidad total
- Amarillo: FreeStorageSpace se encuentra entre el 80% y el 90% de la capacidad total
- Verde: FreeStorageSpace es inferior al 80% de la capacidad total

Acción recomendada

Amplíe el espacio de almacenamiento de la instancia de base de datos de RDS que se está quedando sin espacio de almacenamiento gratuito mediante la consola de administración de Amazon RDS, la API de Amazon RDS o la interfaz de línea de comandos de AWS.

Columnas de informes

- Status
- Región
- ARN de una instancia de base de datos

- FreeStorageSpace Métrica (MB)
- Almacenamiento asignado a instancia de base de datos (MB)
- Porcentaje de almacenamiento de instancias de base de datos utilizado

El parámetro log_output de Amazon RDS está establecido en una tabla

Descripción

Cuando log_output se establece en TABLE, se utiliza más espacio de almacenamiento que cuando log_output se establece en FILE. Se recomienda establecer el parámetro en FILE para evitar alcanzar el límite de tamaño de almacenamiento.

> **Note**
>
> Los resultados de esta verificación se actualizan automáticamente varias veces al día y no se permiten las solicitudes de actualización. Puede que los cambios tarden unas horas en aparecer. Actualmente, no puede excluir recursos de esta verificación.

> **Note**
>
> Cuando se detiene una instancia de base de datos o un clúster de base de datos, puede ver las recomendaciones de Amazon RDS en un plazo Trusted Advisor de 3 a 5 días. Transcurridos cinco días, las recomendaciones no estarán disponibles en Trusted Advisor. Para ver las recomendaciones, abra la consola de Amazon RDS y, a continuación, seleccione Recommendations.
> Si elimina una instancia de base de datos o un clúster de base de datos, las recomendaciones asociadas a esas instancias o clústeres no estarán disponibles en Trusted Advisor la consola de administración de Amazon RDS.

ID de la verificación

`c1qf5bt023`

Criterios de alerta

Amarillo: los grupos de parámetros de base de datos tienen el parámetro log_output establecido en TABLE.

Acción recomendada

Establezca el valor del parámetro log_output en FILE en sus grupos de parámetros de base de datos.

Recursos adicionales

Para obtener más información, consulte Archivos de registro de bases de datos MySQL.

Columnas de informes

- Status
- Región
- Recurso
- Nombre del parámetro
- Valor recomendado
- Hora de la última actualización

La configuración del parámetro innodb_default_row_format de Amazon RDS no es segura

Descripción

La instancia de base de datos encuentra un problema conocido: una tabla creada en una versión de MySQL anterior a la 8.0.26 con el formato de fila establecido en COMPACT o REDUNDANT es inaccesible e irrecuperable cuando el índice supera los 767 bytes.

Se recomienda establecer el valor del parámetro innodb_default_row_format en DYNAMIC.

> **Note**
>
> Los resultados de esta verificación se actualizan automáticamente varias veces al día y no se permiten las solicitudes de actualización. Puede que los cambios tarden unas horas en aparecer. Actualmente, no puede excluir recursos de esta verificación.

> **Note**
>
> Cuando se detiene una instancia de base de datos o un clúster de base de datos, puede ver las recomendaciones de Amazon RDS en un plazo Trusted Advisor de 3

a 5 días. Transcurridos cinco días, las recomendaciones no estarán disponibles en Trusted Advisor. Para ver las recomendaciones, abra la consola de Amazon RDS y, a continuación, seleccione Recommendations.
Si elimina una instancia de base de datos o un clúster de base de datos, las recomendaciones asociadas a esas instancias o clústeres no estarán disponibles en Trusted Advisor la consola de administración de Amazon RDS.

ID de la verificación

`c1qf5bt036`

Criterios de alerta

Rojo: los grupos de parámetros de base de datos tienen una configuración insegura para el parámetro innodb_default_row_format.

Acción recomendada

Establezca el parámetro innodb_default_row_format en DYNAMIC.

Recursos adicionales

Cuando se crea una tabla con una versión de MySQL anterior a 8.0.26 con row_format establecido en COMPACT o REDUNDANT, no se exige la creación de índices con un prefijo clave inferior a 767 bytes. Una vez reiniciada la base de datos, no se puede acceder a estas tablas ni recuperarlas.

Para obtener más información, consulte Cambios en MySQL 8.0.26 (20 de julio de 2021, disponibilidad general) n en el sitio web de documentación de MySQL.

Columnas de informes

- Status
- Región
- Recurso
- Nombre del parámetro
- Valor recomendado
- Hora de la última actualización

El parámetro innodb_flush_log_at_trx_commit de Amazon RDS no es 1

Descripción

El valor del parámetro innodb_flush_log_at_trx_commit de la instancia de base de datos no es un valor seguro. Este parámetro controla la persistencia de las operaciones de confirmación en el disco.

Se recomienda establecer el parámetro innodb_flush_log_at_trx_commit en 1.

> **Note**
>
> Los resultados de esta verificación se actualizan automáticamente varias veces al día y no se permiten las solicitudes de actualización. Puede que los cambios tarden unas horas en aparecer. Actualmente, no puede excluir recursos de esta verificación.

> **Note**
>
> Cuando se detiene una instancia de base de datos o un clúster de base de datos, puede ver las recomendaciones de Amazon RDS en un plazo Trusted Advisor de 3 a 5 días. Transcurridos cinco días, las recomendaciones no estarán disponibles en Trusted Advisor. Para ver las recomendaciones, abra la consola de Amazon RDS y, a continuación, seleccione Recommendations.
> Si elimina una instancia de base de datos o un clúster de base de datos, las recomendaciones asociadas a esas instancias o clústeres no estarán disponibles en Trusted Advisor la consola de administración de Amazon RDS.

ID de la verificación

`c1qf5bt030`

Criterios de alerta

Amarillo: los grupos de parámetros de base de datos tienen el valor innodb_flush_log_at_trx_commit establecido en un valor distinto de 1.

Acción recomendada

Establezca el valor del parámetro innodb_flush_log_at_trx_commit en 1

Recursos adicionales

La transacción de la base de datos es duradera cuando el búfer de registro se guarda en el almacenamiento duradero. Sin embargo, guardar en el disco afecta al rendimiento. Según el valor establecido para el parámetro innodb_flush_log_at_trx_commit, el comportamiento de cómo se escriben y guardan los registros en el disco puede variar.

- Cuando el valor del parámetro es 1, los registros se escriben y guardan en el disco después de cada transacción confirmada.
- Cuando el valor del parámetro es 0, los registros se escriben y guardan en el disco una vez por segundo.
- Cuando el valor del parámetro es 2, los registros se escriben después de confirmar cada transacción y se guardan en el disco una vez por segundo. Los datos se mueven del búfer de memoria de InnoDB a la caché del sistema operativo, que también se encuentra en la memoria.

> **Note**
>
> Cuando el valor del parámetro no es 1, InnoDB no asegura las propiedades ACID. Es posible que las transacciones recientes del último segundo se pierdan si la base de datos se bloquea.

Para obtener más información, consulte Best practices for configuring parameters for Amazon RDS for MySQL, part 1: Parameters related to performance.

Columnas de informes

- Status
- Región
- Recurso
- Nombre del parámetro
- Valor recomendado
- Hora de la última actualización

El parámetro max_user_connections de Amazon RDS es bajo

Descripción

La instancia de base de datos tiene un valor bajo para el número máximo de conexiones simultáneas para cada cuenta de base de datos.

Se recomienda establecer el parámetro max_user_connections en un número superior a 5.

> **Note**
>
> Los resultados de esta verificación se actualizan automáticamente varias veces al día y no se permiten las solicitudes de actualización. Puede que los cambios tarden unas horas en aparecer. Actualmente, no puede excluir recursos de esta verificación.

> **Note**
>
> Cuando se detiene una instancia de base de datos o un clúster de base de datos, puede ver las recomendaciones de Amazon RDS en un plazo Trusted Advisor de 3 a 5 días. Transcurridos cinco días, las recomendaciones no estarán disponibles en Trusted Advisor. Para ver las recomendaciones, abra la consola de Amazon RDS y, a continuación, seleccione Recommendations.
> Si elimina una instancia de base de datos o un clúster de base de datos, las recomendaciones asociadas a esas instancias o clústeres no estarán disponibles en Trusted Advisor la consola de administración de Amazon RDS.

ID de la verificación

`c1qf5bt034`

Criterios de alerta

Amarillo: los grupos de parámetros de base de datos tienen max_user_connections mal configurado.

Acción recomendada

Aumente el valor del parámetro max_user_connections a un número superior a 5.

Recursos adicionales

La configuración max_user_connections controla el número máximo de conexiones simultáneas permitidas para una cuenta de usuario de MySQL. Si se alcanza este límite de conexión, se producen errores en las operaciones de administración de instancias de Amazon RDS, como las copias de seguridad, la aplicación de parches y los cambios de parámetros.

Para obtener más información, consulte Configuración de los límites de recursos de la cuenta en el sitio web de documentación de MySQL.

Columnas de informes

- Status
- Región
- Recurso
- Nombre del parámetro
- Valor recomendado
- Hora de la última actualización

Amazon RDS Multi-AZ

Descripción

Verifica las instancias de base de datos que están implementadas en una implementan en una sola zona de disponibilidad (AZ).

Las implementaciones Multi-AZ mejoran la disponibilidad de la base de datos mediante la replicación sincrónica en una instancia en espera de otra zona de disponibilidad distinta. Durante el mantenimiento planificado de la base de datos o en caso de error en una instancia de base de datos o zona de disponibilidad, Amazon RDS conmuta por error automáticamente a la instancia en espera. Dicha conmutación por error permite reanudar rápidamente las operaciones de base de datos sin intervención administrativa. Dado que Amazon RDS no admite la implementación Multi-AZ para Microsoft SQL Server, esta verificación no examina las instancias de SQL Server.

ID de la verificación

`f2iK5R6Dep`

Criterios de alerta

Amarillo: una instancia de base de datos se implementa en una única zona de disponibilidad.

Acción recomendada

Si la aplicación requiere alta disponibilidad, modifique la instancia de base de datos para habilitar la implementación Multi-AZ. Consulte Alta disponibilidad (Multi-AZ).

Recursos adicionales

Regiones y zonas de disponibilidad

Columnas de informes

- Status
- Región/AZ
- Instancia de base de datos
- ID de VPC
- Multi-AZ

Amazon RDS no está en el plan AWS Backup

Descripción

Compruebe si las instancias de base de datos de Amazon RDS están incluidas en un plan de copia de seguridad en AWS Backup.

AWS Backup es un servicio de respaldo totalmente administrado que facilita la centralización y automatización del respaldo de los datos en todos AWS los servicios.

Incluir la instancia de base de datos de Amazon RDS en un plan de copia de seguridad es importante para hacer cumplir las normativas, para la recuperación de desastres, para las políticas empresariales de protección de datos y para los objetivos de continuidad empresarial.

Para obtener más información, consulte ¿Qué es AWS Backup?.

> **Note**
>
> Los resultados de esta verificación se actualizan automáticamente varias veces al día y no se permiten las solicitudes de actualización. Puede que los cambios tarden unas horas en aparecer. Actualmente, no puede excluir recursos de esta verificación.

ID de la verificación

```
c18d2gz159
```

Origen

```
AWS Config Managed Rule: rds-in-backup-plan
```

Criterios de alerta

Amarillo: una instancia de base de datos de Amazon RDS no está incluida en un plan de respaldo con AWS Backup.

Acción recomendada

Incluya sus instancias de base de datos de Amazon RDS en un plan de respaldo con AWS Backup.

Para obtener información adicional, consulte Copia de seguridad y restauración de Amazon RDS mediante AWS Backup.

Recursos adicionales

Asignación de recursos a un plan de copia de seguridad

Columnas de informes

- Status
- Región
- Recurso
- AWS Config Regla
- Parámetros de entrada
- Hora de la última actualización

Las réplicas de lectura de Amazon RDS están abiertas en modo grabable

Descripción

Su instancia de base de datos tiene la réplica de lectura en modo de escritura, lo que permite actualizaciones de los clientes.

Le recomendamos que establezca el parámetro read_only en TrueIf Replica para que las réplicas de lectura no estén en modo grabable.

> **Note**
>
> Los resultados de esta verificación se actualizan automáticamente varias veces al día y no se permiten las solicitudes de actualización. Puede que los cambios tarden unas horas en aparecer. Actualmente, no puede excluir recursos de esta verificación.

> **Note**
>
> Cuando se detiene una instancia de base de datos o un clúster de base de datos, puede ver las recomendaciones de Amazon RDS en un plazo Trusted Advisor de 3 a 5 días. Transcurridos cinco días, las recomendaciones no estarán disponibles en Trusted Advisor. Para ver las recomendaciones, abra la consola de Amazon RDS y, a continuación, seleccione Recommendations.
> Si elimina una instancia de base de datos o un clúster de base de datos, las recomendaciones asociadas a esas instancias o clústeres no estarán disponibles en Trusted Advisor la consola de administración de Amazon RDS.

ID de la verificación

`c1qf5bt035`

Criterios de alerta

Amarillo: los grupos de parámetros de base de datos activan el modo grabable para las réplicas de lectura.

Acción recomendada

Establezca el valor del parámetro read_only en Replica. TrueIf

Recursos adicionales

El parámetro read_only controla el permiso de escritura de los clientes en una instancia de base de datos. El valor predeterminado de este parámetro es TrueIf Replica. Para una instancia de TrueIfréplica, Replica establece el valor read_only en ON (1) y desactiva cualquier actividad de escritura de los clientes. Para una instancia maestro/de escritura, TrueIfReplica establece el valor en OFF (0) y habilita la actividad de escritura de los clientes de la instancia. Cuando la réplica de lectura se abre en modo grabable, los datos almacenados en esta instancia pueden diferir de los de la instancia principal, lo que provoca errores de replicación.

Para obtener más información, consulte Prácticas recomendadas para configurar los parámetros de Amazon RDS for MySQL, parte 2: Parámetros relacionados con la replicación, en el sitio web de documentación de MySQL.

Columnas de informes

- Status
- Región
- Recurso
- Nombre del parámetro
- Valor recomendado
- Hora de la última actualización

Las copias de seguridad automatizadas de recursos de Amazon RDS están desactivadas

Descripción

Las copias de seguridad automatizadas están deshabilitadas en sus recursos de base de datos. Las copias de seguridad automatizadas permiten la point-in-time recuperación de su instancia de base de datos.

> **Note**
>
> Los resultados de esta verificación se actualizan automáticamente varias veces al día y no se permiten las solicitudes de actualización. Puede que los cambios tarden unas horas en aparecer. Actualmente, no puede excluir recursos de esta verificación.

> **Note**
>
> Cuando se detiene una instancia de base de datos o un clúster de base de datos, puede ver las recomendaciones de Amazon RDS en un plazo Trusted Advisor de 3 a 5 días. Transcurridos cinco días, las recomendaciones no estarán disponibles en Trusted Advisor. Para ver las recomendaciones, abra la consola de Amazon RDS y, a continuación, seleccione Recommendations.

Si elimina una instancia de base de datos o un clúster de base de datos, las recomendaciones asociadas a esas instancias o clústeres no estarán disponibles en Trusted Advisor la consola de administración de Amazon RDS.

ID de la verificación

`c1qf5bt001`

Criterios de alerta

Rojo: los recursos de Amazon RDS no tienen activadas las copias de seguridad automáticas

Acción recomendada

Active las copias de seguridad automatizadas con un período de retención de hasta 14 días.

Recursos adicionales

Las copias de seguridad automatizadas permiten point-in-time la recuperación de sus instancias de base de datos. Recomendamos activar las copias de seguridad automatizadas. Al activar las copias de seguridad automatizadas para una instancia de base de datos, Amazon RDS realiza automáticamente una copia de seguridad completa de los datos a diario durante el período de copia de seguridad que prefiera. La copia de seguridad captura los registros de transacciones cuando hay actualizaciones en su instancia de base de datos. Obtendrá un almacenamiento de respaldo equivalente al tamaño de almacenamiento de su instancia de base de datos sin coste adicional.

Para obtener más información, consulte los siguientes recursos:

- Permitir copias de seguridad automatizadas
- Desmitificando los costos de almacenamiento de backup de Amazon RDS

Columnas de informes

- Status
- Región
- Recurso
- Valor recomendado
- Nombre del motor
- Hora de la última actualización

El parámetro sync_binlog de Amazon RDS está desactivado

Descripción

La sincronización del registro binario con el disco no se aplica antes de que la confirmación de las transacciones se reconozca en la instancia de base de datos.

Se recomienda establecer el valor del parámetro sync_binlog en 1.

> **Note**
>
> Los resultados de esta verificación se actualizan automáticamente varias veces al día y no se permiten las solicitudes de actualización. Puede que los cambios tarden unas horas en aparecer. Actualmente, no puede excluir recursos de esta verificación.

> **Note**
>
> Cuando se detiene una instancia de base de datos o un clúster de base de datos, puede ver las recomendaciones de Amazon RDS en un plazo Trusted Advisor de 3 a 5 días. Transcurridos cinco días, las recomendaciones no estarán disponibles en Trusted Advisor. Para ver las recomendaciones, abra la consola de Amazon RDS y, a continuación, seleccione Recommendations.
> Si elimina una instancia de base de datos o un clúster de base de datos, las recomendaciones asociadas a esas instancias o clústeres no estarán disponibles en Trusted Advisor la consola de administración de Amazon RDS.

ID de la verificación

`c1qf5bt031`

Criterios de alerta

Amarillo: los grupos de parámetros de base de datos tienen el registro binario sincrónico desactivado.

Acción recomendada

Establezca el parámetro sync_binlog en 1.

Recursos adicionales

El parámetro sync_binlog controla cómo MySQL envía el registro binario al disco. Cuando el valor de este parámetro se establece en 1, se activa la sincronización del registro binario con el disco antes de que se confirmen las transacciones. Cuando el valor de este parámetro se establece en 0, se desactiva la sincronización del registro binario con el disco. Por lo general, el servidor MySQL depende del sistema operativo para enviar el registro binario al disco con regularidad de forma similar a otros archivos. El valor del parámetro sync_binlog establecido en 0 puede mejorar el rendimiento. Sin embargo, durante un corte de energía o un fallo del sistema operativo, el servidor pierde todas las transacciones confirmadas que no estaban sincronizadas con los registros binarios.

Para obtener más información, consulte Prácticas recomendadas para configurar los parámetros de Amazon RDS for MySQL, parte 2: Parámetros relacionados con la replicación.

Columnas de informes

- Status
- Región
- Recurso
- Nombre del parámetro
- Valor recomendado
- Hora de la última actualización

El clúster de base de datos de RDS no tiene habilitada la replicación Multi-AZ

Descripción

Compruebe si los clústeres de base de datos de Amazon RDS tienen habilitada la replicación Multi-AZ.

Un clúster de base de datos Multi-AZ tiene una instancia de base de datos del escritor y dos instancias de base de datos del lector en tres zonas de disponibilidad diferentes. Los clústeres de base de datos Multi-AZ proporcionan alta disponibilidad, mayor capacidad para cargas de trabajo de lectura y menor latencia en comparación con las implementaciones Multi-AZ.

Para obtener más información, consulte Crear un clúster de base de datos Multi-AZ.

> **Note**
>
> Los resultados de esta verificación se actualizan automáticamente varias veces al día y no se permiten las solicitudes de actualización. Puede que los cambios tarden unas horas en aparecer. Actualmente, no puede excluir recursos de esta verificación.

ID de la verificación

`c18d2gz161`

Origen

`AWS Config Managed Rule: rds-cluster-multi-az-enabled`

Criterios de alerta

Amarillo: el clúster de base de datos de Amazon RDS no tiene configurada la replicación Multi-AZ

Acción recomendada

Active la implementación del clúster de base de datos Multi-AZ al crear un clúster de base de datos de Amazon RDS.

Para obtener más información, consulte Crear un clúster de base de datos Multi-AZ.

Recursos adicionales

Implementaciones de clústeres de base de datos Multi-AZ

Columnas de informes

- Status
- Región
- Recurso
- AWS Config Regla
- Parámetros de entrada
- Hora de la última actualización

Instancia de reserva Multi-AZ de RDS no habilitada

Descripción

Compruebe si las instancias de base de datos de Amazon RDS tienen una réplica de reserva Multi-AZ configurada.

Amazon RDS Multi-AZ proporciona alta disponibilidad y durabilidad para las instancias de base de datos al replicar los datos en una réplica de reserva dentro de una zona de disponibilidad diferente. Esto proporciona una conmutación por error automática, mejora el rendimiento y mejora la durabilidad de los datos. En una implementación de instancia de base de datos Multi-AZ, Amazon RDS aprovisiona y mantiene automáticamente una réplica síncrona en espera dentro de una zona de disponibilidad diferente. La instancia de base de datos principal se replica de forma síncrona en distintas zonas de disponibilidad en una réplica en espera para proporcionar redundancia de datos y minimizar los picos de latencia durante las copias de seguridad del sistema. La ejecución de una instancia de base de datos con alta disponibilidad mejora la disponibilidad durante el mantenimiento planificado del sistema. También ayuda a proteger las bases de datos contra los errores de las instancias de base de datos y las interrupciones de las zonas de disponibilidad.

Para obtener más información, consulte Implementaciones de instancias de base de datos Multi-AZ.

> **Note**
>
> Los resultados de esta verificación se actualizan automáticamente varias veces al día y no se permiten las solicitudes de actualización. Puede que los cambios tarden unas horas en aparecer. Actualmente, no puede excluir recursos de esta verificación.

ID de la verificación

`c18d2gz156`

Origen

`AWS Config Managed Rule: rds-multi-az-support`

Criterios de alerta

Amarillo: el clúster de base de datos de Amazon RDS no tiene configurada la replicación Multi-AZ

Acción recomendada

Active la implementación del clúster de base de datos Multi-AZ al crear un clúster de base de datos de Amazon RDS.

Esta comprobación no se puede excluir de la vista de la Trusted Advisor consola.

Recursos adicionales

Implementaciones de instancias de base de datos Multi-AZ

Columnas de informes

- Status
- Región
- Recurso
- AWS Config Regla
- Parámetros de entrada
- Hora de la última actualización

Amazon RDS ReplicaLag

Descripción

Comprueba si la ReplicaLag CloudWatch métrica de una instancia de base de datos de RDS ha superado un umbral razonable desde el punto de vista operativo durante la semana pasada.

ReplicaLag La métrica mide el número de segundos que una réplica de lectura está por detrás de la instancia principal. El retraso en la replicación se produce cuando las actualizaciones asíncronas realizadas en la réplica de lectura no pueden seguir el ritmo de las actualizaciones que se producen en la instancia de base de datos principal. En caso de que se produzca un error en la instancia principal, ReplicaLag es posible que falten datos en la réplica de lectura si están por encima de un umbral razonable desde el punto de vista operativo.

ID de la verificación

`Cmsvnj8db1`

Criterios de alerta

- Rojo: la ReplicaLag métrica ha superado los 60 segundos al menos una vez a la semana.
- Amarillo: la ReplicaLag métrica ha superado los 10 segundos al menos una vez durante la semana.

- Verde: ReplicaLag dura menos de 10 segundos.

Acción recomendada

Existen varias causas posibles ReplicaLag para que el aumento supere los niveles operacionalmente seguros. Por ejemplo, puede deberse a instancias de réplica lanzadas o reemplazadas recientemente a partir de copias de seguridad antiguas y a que estas réplicas requieran un tiempo considerable para “ponerse al día” con la instancia de base de datos principal y las transacciones en vivo. Esto ReplicaLag puede disminuir con el tiempo a medida que se vaya poniendo al día. También puede que la velocidad de transacción que se puede lograr en la instancia de base de datos principal sea superior a la que puede igualar el proceso de replicación o la infraestructura de réplica. Esto ReplicaLag puede aumentar con el tiempo a medida que la replicación no pueda mantener el ritmo del rendimiento de la base de datos principal. Por último, la carga de trabajo puede estar sobrecargada a lo largo de diferentes períodos del día, mes, etc., lo que ocasiona retrasos ocasionales. ReplicaLag Su equipo debería investigar qué posible causa raíz ha contribuido a que la base de datos esté sobrecargada y, posiblemente, cambiar el tipo de instancia de la base de datos u otras características de la carga de trabajo para garantizar que la continuidad de los datos en la réplica se ajuste a sus necesidades. ReplicaLag

Recursos adicionales

- Uso de réplicas de lectura para Amazon RDS para PostgreSQL
- Uso de la replicación de MySQL en Amazon RDS
- Uso de réplicas de lectura de MySQL

Columnas de informes

- Status
- Región
- ARN de una instancia de base de datos
- ReplicaLag Métrica

El parámetro synchronous_commit de Amazon RDS está desactivado

Descripción

Cuando el parámetro synchronous_commit está desactivado, se pueden perder datos si la base de datos se bloquea. La durabilidad de la base de datos está en riesgo.

Se recomienda activar el parámetro synchronous_commit.

> **Note**
>
> Los resultados de esta verificación se actualizan automáticamente varias veces al día y no se permiten las solicitudes de actualización. Puede que los cambios tarden unas horas en aparecer. Actualmente, no puede excluir recursos de esta verificación.

> **Note**
>
> Cuando se detiene una instancia de base de datos o un clúster de base de datos, puede ver las recomendaciones de Amazon RDS en un plazo Trusted Advisor de 3 a 5 días. Transcurridos cinco días, las recomendaciones no estarán disponibles en Trusted Advisor. Para ver las recomendaciones, abra la consola de Amazon RDS y, a continuación, seleccione Recommendations.
> Si elimina una instancia de base de datos o un clúster de base de datos, las recomendaciones asociadas a esas instancias o clústeres no estarán disponibles en Trusted Advisor la consola de administración de Amazon RDS.

ID de la verificación

`c1qf5bt026`

Criterios de alerta

Rojo: los grupos de parámetros de base de datos tienen el parámetro synchronous_commit desactivado.

Acción recomendada

Active el parámetro synchronous_commit en sus grupos de parámetros de base de datos.

Recursos adicionales

El parámetro synchronous_commit define la finalización del proceso de registro anticipado (WAL) antes de que el servidor de base de datos envíe una notificación correcta al cliente. Esta confirmación se denomina confirmación asíncrona porque el cliente la reconoce antes de que WAL guarde la transacción en el disco. Si el parámetro synchronous_commit está desactivado, es

posible que se pierdan las transacciones, que la durabilidad de la instancia de base de datos se vea comprometida y que se pierdan datos cuando una base de datos se bloquea.

Para obtener más información, consulte Archivos de registro de bases de datos MySQL.

Columnas de informes

- Status
- Región
- Recurso
- Nombre del parámetro
- Valor recomendado
- Hora de la última actualización

Instantánea automática de clúster de Amazon Redshift

Descripción

Compruebe si las instantáneas automatizadas están habilitadas para sus clústeres de Amazon Redshift.

Amazon Redshift realiza instantáneas progresivas de forma automática que hacen un seguimiento de los cambios realizados en el clúster desde la instantánea automatizada anterior. Las instantáneas automatizadas conservan todos los datos requeridos para restaurar un clúster a partir de una instantánea. Para desactivar las instantáneas automatizadas, establezca el período de retención en cero. No puede deshabilitar las instantáneas automatizadas para los tipos de nodos RA3.

Puede especificar el período de retención mínimo y máximo que desee mediante los parámetros MinRetentionMaxRetentionPeríodo y Período de sus AWS Config reglas.

Instantáneas y copias de seguridad de Amazon Redshift

> **Note**
>
> Los resultados de esta verificación se actualizan automáticamente varias veces al día y no se permiten las solicitudes de actualización. Puede que los cambios tarden unas horas en aparecer. Actualmente, no puede excluir recursos de esta verificación.

ID de la verificación

`c18d2gz135`

Origen

`AWS Config Managed Rule: redshift-backup-enabled`

Criterios de alerta

Rojo: Amazon Redshift no tiene configuradas las instantáneas automatizadas dentro del período de retención deseado.

Acción recomendada

Asegúrese de que las instantáneas automatizadas estén habilitadas para los clústeres de Amazon Redshift.

Para obtener más información, consulte Administración de instantáneas a través de la consola.

Recursos adicionales

Instantáneas y copias de seguridad de Amazon Redshift

Para obtener más información, consulte Trabajar con copias de seguridad.

Columnas de informes

- Status
- Región
- Recurso
- AWS Config Regla
- Parámetros de entrada
- Hora de la última actualización

Comprobaciones de estado eliminadas de Amazon Route 53

Descripción

Verifica los conjuntos de registros de recursos asociados con las comprobaciones de estado que se han eliminado.

Route 53 no le impide eliminar una comprobación de estado asociada con uno o varios conjuntos de registros de recursos. Si elimina una comprobación de estado sin actualizar los conjuntos de registros de recursos asociados, el enrutamiento de las consultas de DNS para la configuración de conmutación por error a nivel de DNS no funcionará según lo previsto.

Las zonas alojadas creadas por AWS los servicios no aparecerán en los resultados de la comprobación.

ID de la verificación

`Cb877eB72b`

Criterios de alerta

Amarillo: un conjunto de registros de recursos está asociado a una comprobación de estado que se ha eliminado.

Acción recomendada

Cree una nueva comprobación de estado y asóciela al conjunto de registros de recursos. Consulte Creación, actualización y eliminación de comprobaciones de estado y Adición de comprobaciones de estado a conjuntos de registros de recursos.

Recursos adicionales

- Comprobaciones de estado de Amazon Route 53 y conmutación por error de DNS
- Cómo funcionan las comprobaciones de estado en configuraciones simples de Amazon Route 53

Columnas de informes

- Nombre de zona alojada
- ID de zona alojada
- Nombre de conjunto de registros de recursos
- Tipo de conjunto de registros de recursos
- Identificador de los conjuntos de registros de recursos

Conjuntos de registros de recursos de conmutación por error en Amazon Route 53

Descripción

Verifica si hay conjuntos de registros de recursos de conmutación por error de Amazon Route 53 que tienen una configuración incorrecta.

Cuando las comprobaciones de estado de Amazon Route 53 determinan que el recurso principal no está en buen estado, Amazon Route 53 responde a las consultas con un conjunto de registros de recursos de copia de seguridad secundario. Debe crear conjuntos de registros de recursos primarios y secundarios configurados correctamente para que la conmutación por error funcione.

Las zonas alojadas creadas por AWS los servicios no aparecerán en los resultados de la comprobación.

ID de la verificación

`b73EEdD790`

Criterios de alerta

- Amarillo: un conjunto principal de registros de recursos de conmutación por error no tiene un conjunto secundario de registros de recursos correspondiente.
- Amarillo: un conjunto secundario de registros de recursos de conmutación por error no tiene un conjunto principal de registros de recursos correspondiente.
- Amarillo: los conjuntos de registros de recursos principales y secundarios que tienen el mismo nombre se asocian a la misma comprobación de estado.

Acción recomendada

Si falta un conjunto de recursos de conmutación por error, cree el conjunto de registros de recursos correspondiente. Consulte Creación de conjuntos de registros de recursos de conmutación por error.

Si los conjuntos de registros de recursos están asociados a la misma comprobación de estado, cree comprobaciones de estado separadas para cada uno. Consulte Creación, actualización y eliminación de comprobaciones de estado.

Recursos adicionales

Comprobaciones de estado de Amazon Route 53 y conmutación por error de DNS

Columnas de informes

- Nombre de zona alojada
- ID de zona alojada
- Nombre de conjunto de registros de recursos
- Tipo de conjunto de registros de recursos

- Motivo

Conjuntos de registros de recursos con alto valor de TTL en Amazon Route 53

Descripción

Comprueba si hay conjuntos de registros de recursos que puedan beneficiarse de tener un valor más bajo time-to-live (TTL).

El TTL es el número de segundos durante los cuales los solucionadores de DNS almacenan un conjunto de registro de recursos en la caché. Cuando se especifica un valor de TTL alto, los solucionadores de DNS tardan más tiempo en solicitar registros de DNS actualizados, lo que puede causar retrasos innecesarios en el redireccionamiento del tráfico. Por ejemplo, un TTL alto crea un retraso entre el momento en que la conmutación por error a nivel de DNS detecta un error de punto de enlace y el momento en que responde al volver a enrutar el tráfico.

Las zonas alojadas creadas por AWS los servicios no aparecerán en los resultados de la comprobación.

ID de la verificación

`C056F80cR3`

Criterios de alerta

- Amarillo: un conjunto de registros de recursos cuya política de enrutamiento es conmutación por error tiene un TTL superior a 60 segundos.
- Amarillo: un conjunto de registros de recursos con una comprobación de estado asociada tiene un TTL superior a 60 segundos.

Acción recomendada

Ingrese un valor TTL de 60 segundos para los conjuntos de registros de recursos de la lista. Para obtener más información, consulte Trabajar con conjuntos de registros de recursos.

Recursos adicionales

Comprobaciones de estado de Amazon Route 53 y conmutación por error de DNS

Columnas de informes

- Status
- Nombre de zona alojada
- ID de zona alojada

- Nombre de conjunto de registros de recursos
- Tipo de conjunto de registros de recursos
- ID del conjunto de registros de recursos
- TTL

Delegaciones de servidores de nombres de Amazon Route 53

Descripción

Verifica las zonas alojadas de Amazon Route 53 para las que el registrador de dominios o DNS no utiliza los servidores de nombres de Route 53 correctos.

Cuando se crea una zona alojada, Route 53 asigna un conjunto de delegación de cuatro servidores de nombres. Los nombres de estos servidores son ns–###.awsdns-##.com, .net, .org y .co.uk, donde ### y ## suelen representar números diferentes. Para que Route 53 pueda enrutar consultas de DNS para su dominio, antes debe actualizar la configuración del servidor de nombres del registrador para quitar los servidores de nombres que asignó el registrador. A continuación, debe agregar los cuatro servidores de nombres en el conjunto de delegación de Route 53. Para obtener la máxima disponibilidad, debe agregar los cuatro servidores de nombres de Route 53.

Las zonas alojadas creadas por AWS los servicios no aparecerán en los resultados de la comprobación.

ID de la verificación

`cF171Db240`

Criterios de alerta

Amarillo: una zona alojada en la que el registrador del dominio no utiliza los cuatro servidores de nombres de Route 53 del conjunto de delegación.

Acción recomendada

Agregue o actualice los registros del servidor de nombres con el registrador o con el servicio DNS actual de su dominio para incluir los cuatro servidores de nombres del conjunto de delegación de Route 53. Para encontrar estos valores, consulte Obtención de servidores de nombres para una zona alojada. Para obtener información sobre cómo agregar o actualizar registros del servidor de nombres, consulte Creación y migración de dominios y subdominios a Amazon Route 53.

Recursos adicionales

Uso de zonas hospedadas

Columnas de informes

- Nombre de zona alojada
- ID de zona alojada
- Cantidad de delegaciones de servidores de nombres utilizadas

Amazon Route 53 Resolver Redundancia de zonas de disponibilidad de puntos finales

Descripción

Compruebe si la configuración del servicio tiene direcciones IP especificadas en al menos dos zonas de disponibilidad (AZ) para garantizar la redundancia. Una zona de disponibilidad es una ubicación diferente que queda aislada en caso de error en otras zonas. Al especificar instancias en múltiples zonas de disponibilidad de una misma región, puede proteger a sus aplicaciones de un único punto de error.

ID de la verificación

`Chrv231ch1`

Criterios de alerta

- Amarillo: las direcciones IP se especifican solo en una zona de disponibilidad
- Verde: las direcciones IP se especifican en al menos dos zonas de disponibilidad

Acción recomendada

Especificar las direcciones IP al menos en dos zonas de disponibilidad para la redundancia.

Recursos adicionales

- Si necesita más de un punto de conexión para la interfaz de red elástica para garantizar la disponibilidad en todo momento, le recomendamos que cree al menos una interfaz de red más de la que necesita para asegurarse de disponer de capacidad adicional para gestionar posibles sobretensiones de tráfico. La interfaz de red adicional también garantiza la disponibilidad durante las operaciones de servicio, como mantenimiento o actualizaciones.
- Alta disponibilidad para puntos de enlace de Resolver

Columnas de informes

- Status

- Región
- ARN de recurso
- Número de zonas de disponibilidad

Registro de bucket de Amazon S3

Descripción

Verifica la configuración de registro de los buckets de Amazon Simple Storage Service (Amazon S3).

Cuando se habilita el registro de acceso al servidor, los registros de acceso detallados se entregan cada hora en un bucket especificado. Los registros de acceso contienen detalles sobre cada solicitud, como, por ejemplo, el tipo de solicitud, los recursos especificados en la solicitud y la fecha y hora en que se procesó la solicitud. De forma predeterminada, el registro de bucket no está habilitado. Debe habilitar el registro si desea llevar a cabo auditorías de seguridad u obtener más información sobre los usuarios y los patrones de uso.

Cuando el registro está habilitado inicialmente, la configuración se valida automáticamente. No obstante, las modificaciones futuras pueden dar lugar a errores de registro. Esta verificación examina los permisos de bucket explícitos de Amazon S3, pero no examina las políticas de bucket asociadas que podrían invalidar los permisos de bucket.

ID de la verificación

`BueAdJ7NrP`

Criterios de alerta

- Amarillo: el bucket no tiene habilitado el registro de acceso al servidor.
- Amarillo: los permisos del bucket de destino no incluyen la cuenta raíz, por lo que Trusted Advisor no se puede comprobar.
- Rojo: el bucket de destino no existe.
- Rojo: el bucket de destino y el bucket de origen tienen propietarios diferentes.
- Rojo: el emisor de registros no tiene permisos de escritura en el bucket de destino.

Acción recomendada

Habilite el registro de buckets para la mayoría de los buckets. Consulte Habilitación del registro con la consola y Habilitación de registros mediante programación.

Si los permisos del bucket de destino no incluyen la cuenta raíz y quieres Trusted Advisor comprobar el estado del registro, añade la cuenta raíz como beneficiaria. Consulte Edición de permisos de bucket.

Si el bucket de destino no existe, seleccione un bucket existente como destino o cree uno nuevo y selecciónelo. Consulte Administración del registro de buckets.

Si el origen y el destino tienen propietarios diferentes, cambie el bucket de destino por uno que tenga el mismo propietario que el bucket de origen. Consulte Administración del registro de buckets.

Si el emisor de registros no tiene permisos de escritura en el destino (no está habilitada la escritura), conceda permisos de carga/eliminación al grupo de entrega de registros. Consulte Edición de permisos de bucket.

Recursos adicionales

- Trabajo con buckets
- Registro de acceso al servidor
- Formato de registro de acceso al servidor
- Eliminación de archivos de registro

Columnas de informes

- Status
- Región
- Nombre del bucket
- Nombre del destino
- El destino existe
- Mismo propietario
- Escritura habilitada
- Motivo

La replicación de bucket de Amazon S3 no está habilitada

Descripción

Compruebe si los buckets de Amazon S3 tienen reglas de replicación habilitadas para la replicación entre regiones, la replicación en la misma región o ambas.

La replicación consiste en la copia automática y asincrónica de objetos entre depósitos de la misma región o de regiones diferentes. AWS La replicación copia los objetos recientemente creados y las actualizaciones de objetos de un bucket de origen a un bucket o buckets de destino. Utilice la replicación de bucket de Amazon S3 para mejorar la resiliencia y la conformidad de sus aplicaciones y almacenamiento de datos.

Para obtener más información, consulte Replicar objetos.

> **Note**
>
> Los resultados de esta verificación se actualizan automáticamente varias veces al día y no se permiten las solicitudes de actualización. Puede que los cambios tarden unas horas en aparecer. Actualmente, no puede excluir recursos de esta verificación.

ID de la verificación

`c18d2gz119`

Origen

`AWS Config Managed Rule: s3-bucket-replication-enabled`

Criterios de alerta

Amarillo: las reglas de replicación de bucket de Amazon S3 no están habilitadas para la replicación entre regiones, la replicación en la misma región o ambas.

Acción recomendada

Active las reglas de replicación de bucket de Amazon S3 para mejorar la resiliencia y la conformidad de sus aplicaciones y almacenamiento de datos.

Para obtener más información, consulte Ver trabajos de copia de seguridad y puntos de recuperación y Configuración de la replicación.

Recursos adicionales

Tutoriales: ejemplos para configurar la replicación

Columnas de informes

- Status
- Región
- Recurso

- AWS Config Regla
- Parámetros de entrada
- Hora de la última actualización

Amazon S3 Bucket Versioning

Descripción

Verifica si existen buckets de Amazon Simple Storage Service que no tengan el habilitado el control de versiones o que lo tienen suspendido.

Cuando el control de versiones está habilitado, puede recuperarse fácilmente de acciones no deseadas del usuario y de errores de la aplicación. El control de versiones permite conservar, recuperar y restaurar cualquier versión de cualquier objeto almacenado en un bucket. Puede utilizar reglas de ciclo de vida para administrar todas las versiones de los objetos, así como sus costos asociados mediante el archivo automático de los objetos en la clase de almacenamiento de Glacier. Las reglas también se pueden configurar para eliminar versiones de los objetos una vez transcurrido un periodo de tiempo especificado. También puede requerir la autenticación multifactor (MFA) para las eliminaciones de cualquier objeto o para cualquier cambio de configuración de los buckets.

El control de versiones no se puede desactivar después de haberlo habilitado. Sin embargo, se puede suspender, lo que impide que se creen nuevas versiones de objetos. El uso del control de versiones puede aumentar los costos de Amazon S3, ya que se paga por el almacenamiento de varias versiones de un objeto.

ID de la verificación

`R365s2Qddf`

Criterios de alerta

- Verde: se ha habitado el control de versiones para el bucket.
- Amarillo: no se ha habitado el control de versiones para el bucket.
- Amarillo: el control de versiones está suspendido para el bucket.

Acción recomendada

Habilite el control de versiones de buckets en la mayoría de los buckets para evitar que se eliminen o sobrescriban accidentalmente. Consulte Uso del control de versiones y Habilitación del control de versiones mediante programación.

Si el control de versiones del bucket está suspendido, considere volver a habilitar el control de versiones. Para obtener información sobre el trabajo con objetos en un bucket con control de versiones suspendido, consulte Administración de objetos en un bucket con control de versiones suspendido.

Cuando el control de versiones está habilitado o suspendido, puede definir las reglas de configuración del ciclo de vida para marcar determinadas versiones de objetos como vencidas o para eliminar permanentemente las versiones de objetos innecesarias. Para obtener más información, consulte Administración del ciclo de vida de los objetos.

La eliminación con MFA requiere una autenticación adicional cuando se cambia el estado de control de versiones del bucket o cuando se eliminan las versiones de un objeto. Se requiere que el usuario ingrese sus credenciales y un código desde un dispositivo de autenticación aprobado. Para obtener más información, consulte Eliminación MFA.

Recursos adicionales

Trabajo con buckets

Columnas de informes

- Status
- Región
- Nombre del bucket
- Control de versiones
- Eliminación con MFA habilitada

Los equilibradores de carga de aplicaciones, las redes y las puertas de enlace no abarcan varias zonas de disponibilidad

Descripción

Compruebe si los equilibradores de carga (equilibrador de carga de aplicaciones, redes y puertas de enlace) están configurados con subredes en varias zonas de disponibilidad.

Puede especificar las zonas de disponibilidad mínima que desee en los AvailabilityZones parámetros mínimos de sus AWS Config reglas.

Para obtener más información, consulte Zonas de disponibilidad para el equilibrador de carga de aplicación, Zonas de disponibilidad - Equilibrador de carga de red y Crear un equilibrador de carga de puerta de enlace.

> **Note**
>
> Los resultados de esta verificación se actualizan automáticamente varias veces al día y no se permiten las solicitudes de actualización. Puede que los cambios tarden unas horas en aparecer. Actualmente, no puede excluir recursos de esta verificación.

ID de la verificación

`c18d2gz169`

Origen

`AWS Config Managed Rule: elbv2-multiple-az`

Criterios de alerta

Amarillo: equilibradores de carga de aplicaciones, redes o puertas de enlace configurados con subredes en menos de dos zonas de disponibilidad.

Acción recomendada

Configure sus equilibradores de carga de aplicaciones, redes y puertas de enlace con subredes en varias zonas de disponibilidad.

Recursos adicionales

Zonas de disponibilidad para el equilibrador de carga de aplicación

Zonas de disponibilidad (Elastic Load Balancing)

Creación de un equilibrador de carga de puerta de enlace

Columnas de informes

- Status
- Región
- Recurso
- AWS Config Regla
- Parámetros de entrada
- Hora de la última actualización

IP con escalado automático disponible en subredes

Descripción

Compruebe que queden suficientes IP disponibles en las subredes de destino. Tener suficientes IP disponibles para su uso será útil cuando el grupo de escalado automático alcance su tamaño máximo y necesite lanzar instancias adicionales.

ID de la verificación

`Cjxm268ch1`

Criterios de alerta

- Rojo: el número máximo de instancias y direcciones IP que puede crear un ASG supera el número de direcciones IP que quedan en las subredes configuradas.
- Verde: hay suficientes direcciones IP disponibles para el resto de la escala posible en el ASG.

Acción recomendada

Aumentar el número de direcciones IP disponibles

Columnas de informes

- Status
- Región
- ARN de recurso
- Número máximo de instancias que se pueden crear
- Número de instancias disponibles

Comprobación de estado de grupos de Auto Scaling

Descripción

Examina la configuración de la comprobación de estado de los grupos de Auto Scaling.

Si Elastic Load Balancing se está utilizando para un grupo de Auto Scaling, se recomienda habilitar una comprobación de estado de Elastic Load Balancing. Si no se utiliza ninguna comprobación de estado de Elastic Load Balancing, Auto Scaling solo podrá actuar en función del estado de la instancia de Amazon Elastic Compute Cloud (Amazon EC2). Auto Scaling no actuará en la aplicación que esté en ejecución en la instancia.

ID de la verificación

CL0G40CD08

Criterios de alerta

- Amarillo: un grupo de escalado automático tiene un equilibrador de carga asociado, pero la comprobación de estado de Elastic Load Balancing no está habilitada.
- Amarillo: un grupo de escalado automático no tiene un equilibrador de carga asociado, pero la comprobación de estado de Elastic Load Balancing está habilitada.

Acción recomendada

Si el grupo de escalado automático tiene un equilibrador de carga asociado, pero la comprobación de estado de Elastic Load Balancing no está habilitada, consulte Adición de una comprobación de estado de Elastic Load Balancing al grupo de escalado automático.

Si la comprobación de estado de Elastic Load Balancing está habilitada, pero no hay un equilibrador de carga asociado al grupo de escalado automático, consulte Configuración de una aplicación con escalado automático y balanceo de carga.

Recursos adicionales

Guía del usuario de Amazon EC2 Auto Scaling

Columnas de informes

- Status
- Región
- Nombre del grupo de escalado automático
- Equilibrador de carga asociado
- Comprobación de estado

Recursos de grupos de Auto Scaling

Descripción

Verifica la disponibilidad de los recursos asociados con las configuraciones de lanzamiento y los grupos de Auto Scaling.

Los grupos de Auto Scaling que apuntan a recursos que no están disponibles no pueden lanzar nuevas instancias de Amazon Elastic Compute Cloud (Amazon EC2). Cuando se configura

correctamente, Auto Scaling hace que el número de instancias de Amazon EC2 aumente sin problemas durante los picos de demanda y disminuya automáticamente durante los periodos de menor demanda. Los grupos de Auto Scaling y las configuraciones de lanzamiento que apuntan a recursos que no están disponibles no funcionan según lo previsto.

ID de la verificación

`8CNsSllI5v`

Criterios de alerta

- Rojo: un grupo de escalado automático está asociado a un equilibrador de carga eliminado.
- Rojo: una configuración de lanzamiento está asociada a una imagen de máquina de Amazon (AMI) eliminada.

Acción recomendada

Si el equilibrador de carga se ha eliminado, cree uno nuevo o cree un grupo de destino y asócielo al grupo de escalado automático, o cree un nuevo grupo de escalado automático sin el equilibrador de carga. Para obtener información acerca de la creación de un nuevo grupo de escalado automático con un nuevo equilibrador de carga, consulte Configuración de una aplicación con escalado automático y balanceo de carga. Para obtener información sobre cómo crear un nuevo grupo de escalado automático sin un equilibrador de carga, consulte Crear un grupo de escalado automático en Introducción a Auto Scaling con la consola.

Si se ha eliminado la AMI, cree una nueva plantilla de lanzamiento o una versión de plantilla de lanzamiento mediante una AMI válida y asóciela a un grupo de escalado automático. Consulte Crear configuración de lanzamiento en Introducción a Auto Scaling con la consola.

Recursos adicionales

- Solución de problemas de Auto Scaling: AMI de Amazon EC2
- Solución de problemas de Auto Scaling: configuración del equilibrador de carga
- Guía del usuario de Amazon EC2 Auto Scaling

Columnas de informes

- Status
- Región
- Nombre del grupo de escalado automático
- Tipo de lanzamiento

- Tipo de recurso
- Nombre del recurso

Los clústeres de AWS CloudHSM que ejecutan instancias de HSM en una sola AZ

Descripción

Comprueba los clústeres que ejecutan las instancias de HSM en una única zona de disponibilidad (AZ). Esta comprobación avisa si sus clústeres corren el riesgo de no tener la copia de seguridad más reciente.

> **Note**
>
> Los resultados de esta verificación se actualizan automáticamente varias veces al día y no se permiten las solicitudes de actualización. Puede que los cambios tarden unas horas en aparecer. Actualmente, no puede excluir recursos de esta verificación.

ID de la verificación

`hc0dfs7601`

Criterios de alerta

- Amarillo: un clúster de CloudHSM ejecuta todas las instancias de HSM en una única zona de disponibilidad durante más de 1 hora.
- Verde: un clúster de CloudHSM ejecuta todas las instancias de HSM en al menos dos zonas de disponibilidad diferentes.

Acción recomendada

Cree al menos una instancia más para el clúster en una zona de disponibilidad diferente.

Recursos adicionales

Mejores prácticas para AWS CloudHSM

Columnas de informes

- Status
- Región

- ID del clúster
- Número de instancias de HSM
- Hora de la última actualización

AWS Direct Connect Resiliencia de ubicación

Descripción

Comprueba la resistencia del AWS Direct Connect utilizado para conectar su entorno local a cada puerta de enlace de Direct Connect o puerta de enlace privada virtual.

Esta comprobación le avisa si alguna puerta de enlace de Direct Connect o puerta de enlace privada virtual no está configurada con interfaces virtuales en al menos dos ubicaciones distintas de Direct Connect. La falta de resiliencia de la ubicación puede provocar un tiempo de inactividad inesperado durante el mantenimiento, un corte de fibra, un fallo del dispositivo o un fallo total de la ubicación.

> **Note**
>
> Los resultados de esta verificación se actualizan automáticamente varias veces al día y no se permiten las solicitudes de actualización. Puede que los cambios tarden unas horas en aparecer.

> **Note**
>
> Direct Connect se implementa con Transit Gateway mediante la puerta de enlace Direct Connect.

ID de la verificación

`c1dfpnchv2`

Criterios de alerta

Rojo: la puerta de enlace Direct Connect o la puerta de enlace privada virtual está configurada con una o más interfaces virtuales en un único dispositivo de Direct Connect.

Amarillo: la puerta de enlace Direct Connect o puerta de enlace privada virtual está configurada con interfaces virtuales en varios dispositivos de Direct Connect en una única ubicación de Direct Connect.

Verde: la puerta de enlace Direct Connect o la puerta de enlace privada virtual está configurada con interfaces virtuales en dos o más ubicaciones distintas de Direct Connect.

Acción recomendada

Para aumentar la resiliencia de ubicación de Direct Connect, puede configurar la puerta de enlace Direct Connect o la puerta de enlace privada virtual para conectarse a al menos dos ubicaciones distintas de Direct Connect. Para obtener más información, consulte la recomendación de AWS Direct Connect resiliencia.

Recursos adicionales

AWS Direct Connect Recomendaciones de resiliencia

AWS Direct Connect Prueba de conmutación por error

Columnas de informes

- Status
- Región
- Hora de la última actualización
- Estado de resiliencia
- Ubicación
- ID de la conexión
- ID de puerta de enlace

AWS Lambda funciona sin configurar una cola de letra muerta

Descripción

Comprueba si una AWS Lambda función está configurada con una cola de letras muertas.

Una cola de texto sin procesar es una función AWS Lambda que permite capturar y analizar los eventos fallidos, lo que proporciona una forma de gestionar esos eventos en consecuencia. Es posible que el código genere una excepción, agote el tiempo de espera o se quede sin memoria, dando lugar a ejecuciones asíncronas fallidas de la función de Lambda. Una cola de mensajes

fallidos almacena los mensajes de las invocaciones fallidas, lo que proporciona una forma de gestionar los mensajes y solucionar los errores.

Puede especificar el recurso de cola de letra muerta que desea comprobar mediante el parámetro dLQarns de sus reglas. AWS Config

Para obtener más información, consulte Colas de mensajes fallidos.

> **Note**
>
> Los resultados de esta verificación se actualizan automáticamente varias veces al día y no se permiten las solicitudes de actualización. Puede que los cambios tarden unas horas en aparecer. Actualmente, no puede excluir recursos de esta verificación.

ID de la verificación

```
c18d2gz182
```

Origen

```
AWS Config Managed Rule: lambda-dlq-check
```

Criterios de alerta

Amarillo: la AWS Lambda función no tiene configurada ninguna cola de letras muertas.

Acción recomendada

Asegúrese de que sus AWS Lambda funciones tengan una cola de texto sin procesar configurada para controlar la gestión de los mensajes en todas las invocaciones asíncronas fallidas.

Para obtener más información, consulte Colas de mensajes fallidos.

Recursos adicionales

- Diseño robusto de aplicaciones sin servidor con colas de mensajes fallidos de AWS Lambda

Columnas de informes

- Status
- Región
- Recurso
- AWS Config Regla

- Parámetros de entrada
- Hora de la última actualización

AWS Lambda Sobre los destinos de los eventos de falla

Descripción

Compruebe que las funciones Lambda de su cuenta tengan configurado un destino de eventos de error o una cola de mensajes fallidos (DLQ) para las invocaciones asíncronas, de modo que los registros de las invocaciones fallidas se puedan direccionar a un destino para su posterior investigación o procesamiento.

> **Note**
>
> Los resultados de esta verificación se actualizan automáticamente varias veces al día y no se permiten las solicitudes de actualización. Puede que los cambios tarden unas horas en aparecer. Actualmente, no puede excluir recursos de esta verificación.

ID de la verificación

`c1dfprch05`

Criterios de alerta

- Amarillo: la característica no tiene configurado ningún destino de eventos de error ni ninguna DLQ.

Acción recomendada

Configure el destino de eventos de error o la DLQ para que sus funciones de Lambda envíen las invocaciones fallidas junto con otros detalles a uno de los servicios de AWS de destino disponibles para su posterior depuración o procesamiento.

Recursos adicionales

- Invocación asíncrona
- AWS Lambda Sobre los destinos de los eventos de error

Columnas de informes

- Status
- Región

- La característica con la versión que está marcada.
- Porcentaje de solicitudes asincrónicas caídas en el día actual
- Solicitudes asíncronas del día actual
- Porcentaje promedio diario de solicitudes asincrónicas caídas
- Promedio de solicitudes asíncronas diarias
- Hora de la última actualización

Funciones habilitadas para VPC de AWS Lambda sin redundancia Multi-AZ

Descripción

Comprueba la versión $LATEST de las funciones Lambda habilitadas para VPC que son vulnerables a la interrupción del servicio en una sola zona de disponibilidad. Se recomienda que las funciones habilitadas para VPC estén conectadas a varias zonas de disponibilidad para una alta disponibilidad.

> **Note**
>
> Los resultados de esta verificación se actualizan automáticamente varias veces al día y no se permiten las solicitudes de actualización. Puede que los cambios tarden unas horas en aparecer. Actualmente, no puede excluir recursos de esta verificación.

ID de la verificación

`L4dfs2Q4C6`

Criterios de alerta

Amarillo: la versión $LATEST de una función Lambda habilitada para VPC está conectada a subredes de una única zona de disponibilidad.

Acción recomendada

Al configurar funciones para el acceso a la VPC, elija subredes en varias zonas de disponibilidad a fin de garantizar una alta disponibilidad.

Recursos adicionales

- Configuración de una función Lambda para obtener acceso a los recursos en una PC

- Resiliencia en AWS Lambda

Columnas de informes

- Status
- Región
- ARN de función
- ID de VPC
- Promedio de invocaciones diarias
- Hora de la última actualización

AWS Resilience Hub Comprobación de componentes de la aplicación

Descripción

Comprueba si un componente de la aplicación (AppComponent) de la aplicación es irrecuperable. Si an AppComponent no se recupera en caso de una interrupción, es posible que se produzca una pérdida de datos desconocida y un tiempo de inactividad del sistema.

> **Note**
>
> Los resultados de esta verificación se actualizan automáticamente varias veces al día y no se permiten las solicitudes de actualización. Puede que los cambios tarden unas horas en aparecer.

ID de la verificación

`RH23stmM04`

Criterios de alerta

Rojo: AppComponent es irrecuperable.

Acción recomendada

Para garantizar que la suya AppComponent sea recuperable, revise e implemente las recomendaciones de resiliencia y, a continuación, realice una nueva evaluación. Para obtener más información sobre la revisión de las recomendaciones de resiliencia, consulte Recursos adicionales.

Recursos adicionales

Revisar las recomendaciones de resiliencia

Conceptos de AWS Resilience Hub

AWS Resilience Hub Guía del usuario

Columnas de informes

- Status
- Región
- Nombre de la aplicación
- AppComponent Nombre
- Hora de la última actualización

AWS Resilience Hub política incumplida

Descripción

Comprueba Resilience Hub en busca de aplicaciones que no cumplen con el objetivo de tiempo de recuperación (RTO) y el objetivo de punto de recuperación (RPO) que define la política. La comprobación avisa si su aplicación no cumple con los objetivos de RTO y RPO que ha establecido para una aplicación en Resilience Hub.

> **Note**
>
> Los resultados de esta comprobación se actualizan de manera automática, y no se permiten las solicitudes de actualización. Actualmente, no puede excluir recursos de esta verificación.

ID de la verificación

`RH23stmM02`

Criterios de alerta

- Verde: la aplicación tiene una política y cumple los objetivos de RTO y RPO.
- Amarillo: la aplicación aún no se ha evaluado.

- Rojo: la aplicación tiene una política, pero no cumple los objetivos de RTO y RPO.

Acción recomendada

Inicie sesión en la consola de Resilience Hub y revise las recomendaciones para que su aplicación cumpla con los objetivos de RTO y RPO.

Recursos adicionales

Conceptos de Resilience Hub

Columnas de informes

- Status
- Región
- Nombre de la aplicación
- Hora de la última actualización

AWS Resilience Hub puntuaciones de resiliencia

Descripción

Comprueba si ha realizado una evaluación para sus aplicaciones en Resilience Hub. Esta comprobación avisa si sus puntuaciones de resiliencia están por debajo de un valor específico.

> **Note**
>
> Los resultados de esta comprobación se actualizan de manera automática, y no se permiten las solicitudes de actualización. Actualmente, no puede excluir recursos de esta verificación.

ID de la verificación

`RH23stmM01`

Criterios de alerta

- Verde: la aplicación tiene una puntuación de resiliencia de 70 o superior.
- Amarillo: la aplicación tiene una puntuación de resiliencia de 40 a 69.
- Amarillo: la aplicación aún no se ha evaluado.

- Rojo: la aplicación tiene una puntuación de resiliencia inferior a 40.

Acción recomendada

Inicie sesión en la consola de Resilience Hub y ejecute una evaluación de su aplicación. Revise las recomendaciones para mejorar la puntuación de resiliencia.

Recursos adicionales

Conceptos de Resilience Hub

Columnas de informes

- Status
- Región
- Nombre de la aplicación
- Puntuación de resiliencia de la aplicación
- Hora de la última actualización

AWS Resilience Hub edad de evaluación

Descripción

Compruebe el tiempo transcurrido desde la última vez que ejecutó una evaluación de la aplicación. Esta comprobación le avisa si no ha realizado una evaluación de la aplicación durante un número específico de días.

> **Note**
>
> Los resultados de esta verificación se actualizan automáticamente varias veces al día y no se permiten las solicitudes de actualización. Puede que los cambios tarden unas horas en aparecer. Actualmente, no puede excluir recursos de esta verificación.

ID de la verificación

`RH23stmM03`

Criterios de alerta

- Verde: la evaluación de la aplicación se llevó a cabo en los últimos 30 días.
- Amarillo: la evaluación de la aplicación no se ha realizado en los últimos 30 días.

Acción recomendada

Inicie sesión en la consola de Resilience Hub y ejecute una evaluación de su aplicación.

Recursos adicionales

Conceptos de Resilience Hub

Columnas de informes

- Status
- Región
- Nombre de la aplicación
- Días transcurridos desde la última evaluación
- Tiempo de ejecución de la última evaluación
- Hora de la última actualización

AWS Site-to-Site VPN tiene al menos un túnel en estado INACTIVO

Descripción

Comprueba el número de túneles que están activos para cada uno de tus AWS Site-to-Site VPN s.

Una VPN debe tener siempre dos túneles configurados. Esto proporciona redundancia en caso de interrupción o mantenimiento planificado de los dispositivos del punto de conexión de AWS. Para determinados componentes de hardware, solo hay un túnel activo a la vez. Si una VPN no tiene ningún túnel activo, es posible que se apliquen cargos por la VPN.

Para obtener más información, consulte ¿Qué es AWS Site-to-Site VPN?

> **Note**
>
> Los resultados de esta verificación se actualizan automáticamente varias veces al día y no se permiten las solicitudes de actualización. Puede que los cambios tarden unas horas en aparecer. Actualmente, no puede excluir recursos de esta verificación.

ID de la verificación

`c18d2gz123`

Origen

```
AWS Config Managed Rule: vpc-vpn-2-tunnels-up
```

Criterios de alerta

Amarillo: al menos uno de los túneles de una Site-to-Site VPN está inactivo.

Acción recomendada

Asegúrese de que haya dos túneles configurados para las conexiones VPN. Y, si su hardware lo admite, asegúrese de que ambos túneles estén activos. Si ya no necesita la conexión de VPN, elimínela para evitar gastos.

Para obtener más información, consulte Su dispositivo de puerta de enlace de cliente y el contenido disponible en el Centro de conocimientos de AWS.

Recursos adicionales

- AWS Site-to-Site VPN Guía del usuario
- Adición de una puerta de enlace privada virtual a la VPC

Columnas de informes

- Status
- Región
- Recurso
- AWS Config Regla
- Parámetros de entrada
- Hora de la última actualización

Problemas de alto riesgo de AWS Well-Architected para la fiabilidad

Descripción

Verifica si hay problemas de alto riesgo para las cargas de trabajo en el pilar de fiabilidad. Esta verificación se basa en las revisiones de AWS-Well Architected. Los resultados de las verificaciones dependen de si ha completado la evaluación de la carga de trabajo con AWS Well-Architected.

> **Note**
>
> Los resultados de esta verificación se actualizan automáticamente varias veces al día y no se permiten las solicitudes de actualización. Puede que los cambios tarden unas horas en aparecer. Actualmente, no puede excluir recursos de esta verificación.

ID de la verificación

`Wxdfp4B1L4`

Criterios de alerta

- Rojo: Se identificó al menos un problema activo de alto riesgo en el pilar de confiabilidad de AWS Well-Architected.
- Verde: No se detectó ningún problema activo de alto riesgo en el pilar de confiabilidad de AWS Well-Architected.

Acción recomendada

AWS Well-Architected detectó problemas de alto riesgo durante la evaluación de la carga de trabajo. Estos problemas presentan oportunidades para reducir el riesgo y ahorrar dinero. Inicie sesión en la herramienta AWS Well-Architected para revisar las respuestas y tomar medidas para resolver los problemas activos.

Columnas de informes

- Status
- Región
- ARN de carga de trabajo
- Nombre de carga de trabajo
- Nombre del revisor
- Tipo de carga de trabajo
- Fecha de inicio de carga de trabajo
- Fecha de la última modificación de carga de trabajo
- Cantidad de HRI identificados para la fiabilidad
- Cantidad de HRI resueltos para la fiabilidad
- Cantidad de preguntas contestadas para la fiabilidad

- Cantidad total de preguntas en el pilar de fiabilidad
- Hora de la última actualización

El equilibrador de carga clásico no tiene configuradas varias zonas de disponibilidad

Descripción

Compruebe si el equilibrador de carga clásico abarca varias zonas de disponibilidad (AZ).

Un equilibrador de carga distribuye el tráfico entrante de aplicaciones en varias instancias EC2 en varias zonas de disponibilidad. De forma predeterminada, el balanceador de carga distribuye equitativamente el tráfico entre las zonas de disponibilidad que se habilitan para el balanceador de carga. Si una Zona de Disponibilidad experimenta una interrupción, los nodos del equilibrador de carga reenvían automáticamente las solicitudes a las instancias registradas y saludables en una o más zonas de disponibilidad.

Puede ajustar el número mínimo de zonas de disponibilidad mediante el AvailabilityZones parámetro mínimo de sus reglas AWS Config

Para obtener más información, consulte ¿Qué es el equilibrador de carga clásico?.

> **Note**
>
> Los resultados de esta verificación se actualizan automáticamente varias veces al día y no se permiten las solicitudes de actualización. Puede que los cambios tarden unas horas en aparecer. Actualmente, no puede excluir recursos de esta verificación.

ID de la verificación

```
c18d2gz154
```

Origen

```
AWS Config Managed Rule: clb-multiple-az
```

Criterios de alerta

Amarillo: el equilibrador de carga clásico no tiene configuradas varias zonas de disponibilidad o no cumple con la cantidad mínima de zonas de disponibilidad especificada.

Acción recomendada

Asegúrese de que sus equilibradores de carga clásicos tengan configuradas varias zonas de disponibilidad. Distribuya el equilibrador de carga entre varias zonas de disponibilidad para asegurarse de que la aplicación tenga una alta disponibilidad.

Para obtener más información, consulte Tutorial: crear un equilibrador de carga clásico.

Columnas de informes

- Status
- Región
- Recurso
- AWS Config Regla
- Parámetros de entrada
- Hora de la última actualización

Connection Draining de ELB

Descripción

Verifica si hay balanceadores de carga que no tienen habilitado Connection Draining.

Cuando Connection Draining no está habilitado y se anula el registro de una instancia de Amazon EC2 desde un balanceador de carga, el balanceador de carga detiene el enrutamiento del tráfico a dicha instancia y cierra la conexión. Cuando se habilita Connection Draining, el balanceador de carga deja de enviar nuevas solicitudes a la instancia cuyo registro se anuló, pero mantiene la conexión abierta para servir las solicitudes activas.

ID de la verificación

`7qGXsKIUw`

Criterios de alerta

Amarillo: el drenaje de conexiones no está habilitado para un equilibrador de carga.

Acción recomendada

Habilite el drenaje de conexiones para el equilibrador de carga. Para obtener más información, consulte Drenaje de conexiones y Habilitar o deshabilitar el drenaje de conexiones para el equilibrador de carga.

Recursos adicionales

Conceptos de Elastic Load Balancing

Columnas de informes

- Status
- Región
- Nombre del equilibrador de carga
- Motivo

Optimización del balanceador de carga

Descripción

Verifica la configuración del balanceador de carga.

Para ayudar a aumentar el nivel de tolerancia a errores en Amazon Elastic Compute Cloud (Amazon EC2) al utilizar Elastic Load Balancing, se recomienda ejecutar un número igual de instancias en las distintas zonas de disponibilidad de una región. Los balanceadores de carga configurados acumulan cargos, por lo que esta es también una verificación de optimización de costos.

ID de la verificación

`iqdCTZKCUp`

Criterios de alerta

- Amarillo: hay un equilibrador de carga habilitado para una sola zona de disponibilidad.
- Amarillo: hay un equilibrador de carga habilitado para una zona de disponibilidad que no tiene instancias activas.
- Amarillo: las instancias de Amazon EC2 que se registran con un equilibrador de carga se distribuyen de forma desigual en las zonas de disponibilidad. (La diferencia entre los recuentos de instancias más altos y más bajos en las zonas de disponibilidad utilizadas es superior a 1 y la diferencia es más del 20 % del recuento más alto).

Acción recomendada

Asegúrese de que el equilibrador de carga apunte a instancias activas y en buen estado en al menos dos zonas de disponibilidad. Para obtener más información, consulte Agregar zona de disponibilidad.

Si el equilibrador de carga está configurado para una zona de disponibilidad sin instancias en buen estado o si hay un desequilibrio de instancias en las zonas de disponibilidad, determine si todas las zonas de disponibilidad son necesarias. Omita las zonas de disponibilidad innecesarias y asegúrese de que haya una distribución equilibrada de las instancias en las zonas de disponibilidad restantes. Para obtener más información, consulte Eliminar zona de disponibilidad.

Recursos adicionales

- Regiones y zonas de disponibilidad
- Administración de equilibradores de carga
- Prácticas recomendadas para evaluar Elastic Load Balancing

Columnas de informes

- Status
- Región
- Nombre del equilibrador de carga
- N.° de zonas
- Instancias de zona a
- Instancias de zona b
- Instancias de zona c
- Instancias de zona d
- Instancias de zona e
- Instancias de zona f
- Motivo

Independencia de la zona de disponibilidad de la puerta de enlace de NAT

Descripción

Compruebe si las puertas de enlace NAT están configuradas con independencia de la zona de disponibilidad (AZ).

Una puerta de enlace NAT permite que los recursos de su subred privada se conecten de forma segura a servicios fuera de la subred mediante las direcciones IP de la puerta de enlace NAT y elimina cualquier tráfico entrante no solicitado. Cada puerta de enlace NAT funciona dentro de una zona de disponibilidad (AZ) designada y se crea con redundancia únicamente en esa zona de disponibilidad. Por lo tanto, los recursos de una zona de disponibilidad determinada deben

utilizar una puerta de enlace NAT en la misma zona de disponibilidad para que cualquier posible interrupción de una puerta de enlace NAT o de su zona de disponibilidad no afecte a los recursos de otra zona de disponibilidad.

> **Note**
>
> Los resultados de esta verificación se actualizan automáticamente varias veces al día y no se permiten las solicitudes de actualización. Puede que los cambios tarden unas horas en aparecer. Actualmente, no puede excluir recursos de esta verificación.

ID de la verificación

`c1dfptbg10`

Criterios de alerta

- Rojo: el tráfico de la subred en una zona de disponibilidad se enruta a través de una puerta de enlace NAT en una zona de disponibilidad diferente.
- Verde: el tráfico de la subred en una zona de disponibilidad se enruta a través de una puerta de enlace NAT en la misma zona de disponibilidad.

Acción recomendada

Compruebe la zona de disponibilidad de la subred y dirija el tráfico a través de una puerta de enlace NAT en la misma zona de disponibilidad.

Si no hay ninguna puerta de enlace NAT en la zona de disponibilidad, cree una y, a continuación, dirija el tráfico de la subred a través de ella.

Si tiene la misma tabla de enrutamiento asociada a las subredes de diferentes zonas de disponibilidad, mantenga esta tabla de enrutamiento asociada a las subredes que residen en la misma zona de disponibilidad que la puerta de enlace NAT y, en el caso de las subredes de la otra zona de disponibilidad, asocie una tabla de enrutamiento independiente a una ruta a una puerta de enlace NAT en esta otra zona de disponibilidad.

Le recomendamos que elija un período de mantenimiento para los cambios de arquitectura en Amazon VPC.

Recursos adicionales

- Cómo crear una puerta de enlace NAT

- ¿Cómo configurar las rutas para diferentes casos de uso de una puerta de enlace NAT

Columnas de informes

- Status
- Región
- Zona de disponibilidad de NAT
- ID de NAT
- Zona de disponibilidad de la subred
- ID de subred
- ID de la tabla de enrutamiento
- ARN de NAT
- Hora de la última actualización

Equilibrador de carga cruzado del equilibrador de carga de red

Descripción

Compruebe si el equilibrador de carga entre zonas está habilitado en los equilibradores de carga de red.

El equilibrador de carga entre zonas ayuda a mantener una distribución uniforme del tráfico entrante entre las instancias de distintas zonas de disponibilidad. Esto evita que el equilibrador de carga enrute todo el tráfico a instancias de la misma zona de disponibilidad, lo que puede provocar una distribución irregular del tráfico y una posible sobrecarga. La característica también contribuye a la fiabilidad de las aplicaciones al redirigir de forma automática el tráfico a instancias en buen estado de otras zonas de disponibilidad en caso de que se produzca un error en una sola zona de disponibilidad.

Para obtener más información, consulte Equilibrador de carga entre zonas.

> **Note**
>
> Los resultados de esta verificación se actualizan automáticamente varias veces al día y no se permiten las solicitudes de actualización. Puede que los cambios tarden unas horas en aparecer. Actualmente, no puede excluir recursos de esta verificación.

ID de la verificación

`c18d2gz105`

Origen

`AWS Config Managed Rule: nlb-cross-zone-load-balancing-enabled`

Criterios de alerta

- Amarillo: el equilibrador de carga de red no tiene habilitado el equilibrador de carga entre zonas.

Acción recomendada

Asegúrese de que el equilibrador de carga entre zonas esté habilitado en los equilibradores de carga de red.

Recursos adicionales

Equilibrador de carga entre zonas (equilibradores de carga de red)

Columnas de informes

- Status
- Región
- Recurso
- AWS Config Regla
- Parámetros de entrada
- Hora de la última actualización

NLB: recurso con acceso a Internet en una subred privada

Descripción

Comprueba si un Network Load Balancer (NLB) orientado a Internet está configurado con una subred privada. Se debe configurar un Network Load Balancer (NLB) con acceso a Internet en las subredes públicas para recibir tráfico. Una subred pública se define como una subred que tiene una ruta directa a una puerta de enlace a Internet. Si la subred está configurada como privada, su zona de disponibilidad (AZ) no recibe tráfico, lo que puede provocar problemas de disponibilidad.

> **Note**
>
> Los resultados de esta verificación se actualizan automáticamente varias veces al día y no se permiten las solicitudes de actualización. Puede que los cambios tarden unas horas en aparecer. Actualmente, no puede excluir recursos de esta verificación.

ID de la verificación

`c1dfpnchv4`

Criterios de alerta

Rojo: NLB está configurado con una o más subredes privadas

Verde: no hay ninguna subred privada configurada para el NLB con conexión a Internet

Acción recomendada

Confirma que las subredes configuradas en un balanceador de cargas con conexión a Internet sean públicas. Una subred pública se define como una subred que tiene una ruta directa a una puerta de enlace a Internet. Use una de las siguientes opciones:

- Cree un nuevo balanceador de carga y seleccione una subred diferente con una ruta directa a una puerta de enlace de Internet.
- Cambia la subred que actualmente está conectada al balanceador de cargas de privada a pública. Para ello, cambie su tabla de enrutamiento y asocie una puerta de enlace a Internet.

Recursos adicionales

- Configure un balanceador de carga y un listener
- Subredes para su VPC
- Asocie una puerta de enlace a una tabla de enrutamiento

Columnas de informes

- Status
- Región
- NLB Arn
- Nombre NLB
- ID de subred

- Esquema NLB
- Tipo de subred
- Hora de la última actualización

NLB Multi-AZ

Descripción

Comprueba si los balanceadores de carga de red están configurados para usar más de una zona de disponibilidad (AZ). Una zona de disponibilidad es una ubicación diferente que queda aislada en caso de error en otras zonas. Configure el balanceador de carga en varias zonas de disponibilidad de la misma región para mejorar la disponibilidad de la carga de trabajo.

> **Note**
>
> Los resultados de esta verificación se actualizan automáticamente varias veces al día y no se permiten las solicitudes de actualización. Puede que los cambios tarden unas horas en aparecer. Actualmente, no puede excluir recursos de esta verificación.

ID de la verificación

`c1dfprch09`

Criterios de alerta

Amarillo: el NLB se encuentra en una única zona de disponibilidad.

Verde: NLB tiene dos o más AZ.

Acción recomendada

Asegúrese de que el balanceador de carga esté configurado con al menos dos zonas de disponibilidad.

Recursos adicionales

Para obtener más información, consulte la siguiente documentación sobre :

- Zonas de disponibilidad
- AWS WellArchitected: despliegue la carga de trabajo en múltiples ubicaciones

- Regiones y zonas de disponibilidad

Columnas de informes

- Status
- Región
- Número de zonas de disponibilidad
- NLB ARN
- Nombre NLB
- Hora de la última actualización

Número de Regiones de AWS en un conjunto de réplicas de Incident Manager

Descripción

Comprueba que la configuración de un conjunto de replicación de Incident Manager utiliza más de uno Región de AWS para admitir la conmutación por error y la respuesta regionales. En el caso de los incidentes creados por CloudWatch alarmas o EventBridge eventos, Incident Manager crea un incidente al Región de AWS igual que la regla de alarma o evento. Si Incident Manager no está disponible temporalmente en esa región, el sistema intenta crear un incidente en otra región dentro del conjunto de replicación. Si el conjunto de replicación incluye solo una región, el sistema no podrá crear un registro de incidentes mientras el administrador de incidentes no esté disponible.

> **Note**
>
> Los resultados de esta verificación se actualizan automáticamente varias veces al día y no se permiten las solicitudes de actualización. Puede que los cambios tarden unas horas en aparecer. Actualmente, no puede excluir recursos de esta verificación.

ID de la verificación

`cIdfp1js9r`

Criterios de alerta

- Verde: el conjunto de replicación contiene más de una región.
- Amarillo: el conjunto de replicación contiene una región.

Acción recomendada

Agregue al menos una región más al conjunto de replicación.

Recursos adicionales

Para obtener más información, consulte Administración de incidentes entre regiones.

Columnas de informes

- Status
- Multiregión
- Conjunto de replicación
- Hora de la última actualización

Comprobación de aplicaciones con zona de disponibilidad única

Descripción

Compruebe a través de patrones de red si el tráfico de red de salida se direcciona a través de una única zona de disponibilidad (AZ).

Una zona de disponibilidad es una ubicación diferente que queda aislada de cualquier impacto en otras zonas. Al distribuir el servicio entre varias zonas de disponibilidad, se limita el radio de alcance de un error en una zona de distribución.

> **Note**
>
> Los resultados de esta verificación se actualizan automáticamente varias veces al día y no se permiten las solicitudes de actualización. Puede que los cambios tarden unas horas en aparecer. Actualmente, no puede excluir recursos de esta verificación.

ID de la verificación

`c1dfptbg11`

Criterios de alerta

- Amarillo: su aplicación solo puede implementarse en una zona de disponibilidad, según los patrones observados de salida de red. Si esto es cierto y su aplicación espera una alta disponibilidad, le recomendamos que aprovisione los recursos de la aplicación e implemente los flujos de red para utilizar varias zonas de disponibilidad.

Acción recomendada

Si su aplicación requiere alta disponibilidad, considere implementar una arquitectura Multi-AZ para obtener mayor disponibilidad.

Columnas de informes

- Status
- Región
- ID de VPC
- Hora de la última actualización

Interfaz de VPC: interfaces de red de punto final en varias zonas de disponibilidad

Descripción

Comprueba si los puntos finales de la interfaz de AWS PrivateLink VPC están configurados para usar más de una zona de disponibilidad (AZ). Una zona de disponibilidad es una ubicación diferente que queda aislada en caso de error en otras zonas. Esto permite una conectividad de red económica y de baja latencia entre zonas de disponibilidad de la misma región. AWS Seleccione subredes en varias zonas de disponibilidad al crear puntos finales de interfaz para ayudar a proteger sus aplicaciones frente a un único punto de fallo.

> **Note**
>
> Actualmente, esta comprobación solo incluye los puntos finales de la interfaz.

> **Note**
>
> Los resultados de esta verificación se actualizan automáticamente varias veces al día y no se permiten las solicitudes de actualización. Puede que los cambios tarden unas horas en aparecer. Actualmente, no puede excluir recursos de esta verificación.

ID de la verificación

`c1dfprch10`

Criterios de alerta

Amarillo: el punto final de la VPC está en una única zona de disponibilidad.

Verde: el punto final de la VPC está en al menos dos zonas de disponibilidad.

Acción recomendada

Asegúrese de que el punto final de la interfaz de VPC esté configurado con al menos dos zonas de disponibilidad.

Recursos adicionales

Para obtener más información, consulte la siguiente documentación sobre :

- Acceda a un AWS servicio mediante un punto final de VPC de interfaz
- Dirección IP privada de la interfaz de red del punto final
- AWS PrivateLink conceptos
- Regiones y zonas de disponibilidad

Columnas de informes

- Status
- Región
- ID de punto final de VPC
- Es Multi AZ
- Hora de la última actualización

Redundancia de túnel de VPN

Descripción

Verifica el número de túneles que están activos para cada una de las VPN.

Una VPN debe tener siempre dos túneles configurados. Esto proporciona redundancia en caso de interrupción o mantenimiento planificado de los dispositivos del punto de enlace AWS . Para determinados componentes de hardware, solo hay un túnel activo a la vez. Si una VPN no tiene ningún túnel activo, es posible que se apliquen cargos por la VPN. Para obtener más información, consulte la Guía del administrador de AWS Client VPN.

ID de la verificación

`S45wrEXrLz`

Criterios de alerta

- Amarillo: una VPN tiene un túnel activo (esto es normal para determinado hardware).
- Amarillo: una VPN no tiene túneles activos.

Acción recomendada

Asegúrese de que haya dos túneles configurados para su conexión VPN y de que ambos estén activos si su hardware es compatible. Si ya no necesita la conexión de VPN, puede eliminarla para evitar gastos. Para obtener más información, consulte Su puerta de enlace de cliente o Eliminación de una conexión de VPN.

Recursos adicionales

- AWS Guía del usuario de la VPN Site-to-Site
- Adición de una gateway privada virtual de hardware a la VPC

Columnas de informes

- Status
- Región
- ID de VPN
- VPC
- Gateway privada virtual
- Gateway de cliente
- Túneles activos
- Motivo

Redundancia de la zona de disponibilidad de ActiveMQ

Descripción

Compruebe que los agentes de Amazon MQ para ActiveMQ estén configurados para una alta disponibilidad con un agente activo/de reserva en varias zonas de disponibilidad.

> **Note**
>
> Los resultados de esta verificación se actualizan automáticamente varias veces al día y no se permiten las solicitudes de actualización. Puede que los cambios tarden unas horas en aparecer. Actualmente, no puede excluir recursos de esta verificación.

ID de la verificación

`c1t3k8mqv1`

Criterios de alerta

- Amarillo: un agente de Amazon MQ para ActiveMQ está configurado en una única zona de disponibilidad.

  Verde: un agente de Amazon MQ para ActiveMQ está configurado en al menos dos zonas de disponibilidad.

Acción recomendada

Cree un nuevo agente con el modo de implementación activo/de reserva.

Recursos adicionales

- Creación de un agente ActiveMQ

Columnas de informes

- Status
- Región
- ID del agente ActiveMQ
- Tipos de motores del broker
- Modo de implementación
- Hora de la última actualización

Redundancia de la zona de disponibilidad de RabbitMQ

Descripción

Compruebe que los agentes de Amazon MQ para RabbitMQ estén configurados con instancias de clúster distribuidas en varias zonas de disponibilidad para garantizar una alta disponibilidad.

> **Note**
>
> Los resultados de esta verificación se actualizan automáticamente varias veces al día y no se permiten las solicitudes de actualización. Puede que los cambios tarden unas horas en aparecer. Actualmente, no puede excluir recursos de esta verificación.

ID de la verificación

`c1t3k8mqv2`

Criterios de alerta

- Amarillo: un agente de Amazon MQ para RabbitMQ está configurado en una única zona de disponibilidad.

  Verde: un agente de Amazon MQ para RabbitMQ está configurado en varias zonas de disponibilidad.

Acción recomendada

Cree un nuevo agente con el modo de implementación de clúster.

Recursos adicionales

- Creación de un agente RabbitMQ

Columnas de informes

- Status
- Región
- ID del agente RabbitMQ
- Tipos de motores del agente
- Modo de implementación
- Hora de la última actualización

Límites de los servicios

Consulte las siguientes verificaciones para la categoría de cuotas de servicio (también conocida como cuotas).

Todas las comprobaciones de esta categoría tienen las siguientes descripciones:

Criterios de alerta

- Amarillo: se ha alcanzado el 80 % del límite.
- Rojo: se ha alcanzado el 100 % del límite.
- Azul: Trusted Advisor no ha podido recuperar la utilización o los límites en una o más Regiones de AWS.

Acción recomendada

Si cree que va a superar un límite de servicio, solicite un aumento directamente desde la consola Service Quotas. Si Service Quotas aún no admite su servicio, puede abrir un caso de soporte en el Centro de soporte.

Columnas de informes

- Status
- Servicio
- Region
- Cantidad límite
- Utilización actual

> **Note**
>
> - Los valores se basan en una instantánea, por lo que su uso actual puede diferir. Los datos de cuota y de uso pueden tardar hasta 24 horas en reflejar los cambios. En los casos en los que las cuotas se hayan incrementado recientemente, es posible que vea temporalmente un uso que excede la cuota.

Nombres de la verificación

- Grupos de Auto Scaling
- Configuraciones de lanzamiento de Auto Scaling
- CloudFormation Pilas
- Capacidad de lectura de DynamoDB
- Capacidad de escritura de DynamoDB
- Instantáneas activas de EBS
- Almacenamiento de volúmenes de HDD en frío (sc1) de EBS
- Almacenamiento de volúmenes de SSD de uso general (gp2) de EBS
- Almacenamiento de volúmenes de SSD de uso general (gp3) de EBS
- Almacenamiento de volúmenes magnéticos (estándar) de EBS
- IOPS agregadas de volúmenes de IOPS provisionadas (SSD) de EBS

- Almacenamiento de volúmenes de SSD de IOPS provisionadas (io1) de EBS
- Almacenamiento de volúmenes de SSD de IOPS provisionadas (io2) de EBS
- Almacenamiento de volúmenes de HDD con rendimiento optimizado (st1) de EBS
- Instancias bajo demanda de EC2
- Asignaciones de instancias reservadas de EC2
- Direcciones IP elásticas de EC2-Classic
- Dirección IP elástica de EC2-VPC
- Application Load Balancers de ELB
- Classic Load Balancers de ELB
- Network Load Balancers de ELB
- Grupo de IAM
- Perfiles de instancias de IAM
- Políticas de IAM
- Roles de IAM
- Certificados de servidor de IAM
- Usuarios de IAM
- Particiones de Kinesis por región
- Uso del almacenamiento de código de Lambda
- Grupos de parámetros de clústeres de RDS
- Roles de clústeres de RDS
- Clústeres de RDS
- Instancias de base de datos de RDS
- Instantáneas manuales de base de datos de RDS
- Grupos de parámetros de base de datos de RDS
- Grupos de seguridad de base de datos de RDS
- Suscripciones de eventos de RDS
- Autenticaciones máximas por grupo de seguridad de RDS
- Grupos de opciones de RDS
- Réplicas de lectura por maestro de RDS
- Instancias reservadas de RDS

- Grupos de subredes de RDS
- Subredes por grupo de subredes de RDS
- Cuota de almacenamiento total de RDS
- Zonas alojadas de Route 53
- Máximo de comprobaciones de estado de Route 53
- Conjuntos de delegación reutilizables de Route 53
- Políticas de tráfico de Route 53
- Instancias de políticas de tráfico de Route 53
- Cuota de envío diaria de SES
- VPC
- Gateways de Internet de VPC

Grupos de Auto Scaling

Descripción

Verifica si el uso supera el 80 % de la cuota de grupos de Auto Scaling.

ID de la verificación

`fW7HH0l7J9`

Recursos adicionales

Cuotas de Auto Scaling

Configuraciones de lanzamiento de Auto Scaling

Descripción

Verifica si el uso supera el 80 % de la cuota de configuraciones de lanzamiento de Auto Scaling.

ID de la verificación

`aW7HH0l7J9`

Recursos adicionales

Cuotas de Auto Scaling

CloudFormation Pilas

Descripción

Comprueba si el uso supera el 80% de la cuota de CloudFormation pilas.

ID de la verificación

`gW7HH0l7J9`

Recursos adicionales

Cuotas de AWS CloudFormation

Capacidad de lectura de DynamoDB

Descripción

Verifica si el uso supera el 80 % del límite de rendimiento aprovisionado de DynamoDB para lecturas por Cuenta de AWS.

ID de la verificación

`6gtQddfEw6`

Recursos adicionales

Cuotas de DynamoDB

Capacidad de escritura de DynamoDB

Descripción

Verifica si el uso supera el 80 % del límite de rendimiento aprovisionado de DynamoDB para escrituras por Cuenta de AWS.

ID de la verificación

`c5ftjdfkMr`

Recursos adicionales

Cuotas de DynamoDB

Instantáneas activas de EBS

Descripción

Verifica si el uso supera el 80 % de la cuota de instantáneas activas de EBS.

ID de la verificación

`eI7KK0l7J9`

Recursos adicionales

Límites de Amazon EBS

Almacenamiento de volúmenes de HDD en frío (sc1) de EBS

Descripción

Verifica si el uso supera el 80 % de la cuota de almacenamiento de volúmenes de HDD en frío (sc1) de EBS.

ID de la verificación

`gH5CC0e3J9`

Recursos adicionales

Límites de Amazon EBS

Almacenamiento de volúmenes de SSD de uso general (gp2) de EBS

Descripción

Verifica si el uso supera el 80 % de la cuota de almacenamiento de volúmenes de SSD de uso general (gp2) de EBS.

ID de la verificación

`dH7RR0l6J9`

Recursos adicionales

Límites de Amazon EBS

Almacenamiento de volúmenes de SSD de uso general (gp3) de EBS

Descripción

Verifica si el uso supera el 80 % de la cuota de almacenamiento de volúmenes de SSD de uso general (gp3) de EBS.

ID de la verificación

`dH7RR0l6J3`

Recursos adicionales

Límites de Amazon EBS

Almacenamiento de volúmenes magnéticos (estándar) de EBS

Descripción

Verifica si el uso supera el 80 % de la cuota de almacenamiento de volúmenes magnéticos (estándar) de EBS.

ID de la verificación

`cG7HH0l7J9`

Recursos adicionales

Límites de Amazon EBS

IOPS agregadas de volúmenes de IOPS provisionadas (SSD) de EBS

Descripción

Verifica si el uso supera el 80 % de la cuota de IOPS agregadas de volúmenes de IOPS provisionadas (SSD) de EBS.

ID de la verificación

`tV7YY0l7J9`

Recursos adicionales

Límites de Amazon EBS

Almacenamiento de volúmenes de SSD de IOPS provisionadas (io1) de EBS

Descripción

Verifica si el uso supera el 80 % de la cuota de almacenamiento de volúmenes de SSD de IOPS provisionadas (io1) de EBS.

ID de la verificación

`gI7MM0l7J9`

Recursos adicionales

Límites de Amazon EBS

Almacenamiento de volúmenes de SSD de IOPS provisionadas (io2) de EBS

Descripción

Verifica si el uso supera el 80 % de la cuota de almacenamiento de volúmenes de SSD de IOPS provisionadas (io2) de EBS.

ID de la verificación

`gI7MM0l7J2`

Recursos adicionales

Límites de Amazon EBS

Almacenamiento de volúmenes de HDD con rendimiento optimizado (st1) de EBS

Descripción

Verifica si el uso supera el 80 % de la cuota de almacenamiento de volúmenes de HDD con rendimiento optimizado (st1) de EBS.

ID de la verificación

`wH7DD0l3J9`

Recursos adicionales

Límites de Amazon EBS

Instancias bajo demanda de EC2

Descripción

Verifica si el uso supera el 80 % de la cuota de instancias bajo demanda de EC2.

ID de la verificación

`0Xc6LMYG8P`

Recursos adicionales

Cuotas de Amazon EC2

Asignaciones de instancias reservadas de EC2

Descripción

Verifica si el uso supera el 80 % de la cuota de asignación de instancias reservadas de EC2.

ID de la verificación

`iH7PP0l7J9`

Recursos adicionales

Cuotas de Amazon EC2

Direcciones IP elásticas de EC2-Classic

Descripción

Verifica si el uso supera el 80 % de la cuota de direcciones IP elásticas de EC2-Classic.

ID de la verificación

`aW9HH0l8J6`

Recursos adicionales

Cuotas de Amazon EC2

Dirección IP elástica de EC2-VPC

Descripción

Verifica si el uso supera el 80 % de la cuota de direcciones IP elásticas de EC2-VPC.

ID de la verificación

`lN7RR0l7J9`

Recursos adicionales

Cuotas de IP elásticas de VPC

Application Load Balancers de ELB

Descripción

Verifica si el uso supera el 80 % de la cuota de Application Load Balancers de ELB.

ID de la verificación

`EM8b3yLRTr`

Recursos adicionales

Cuotas de Elastic Load Balancing

Classic Load Balancers de ELB

Descripción

Verifica si el uso supera el 80 % de la cuota de Classic Load Balancers de ELB.

ID de la verificación

`iK7O00l7J9`

Recursos adicionales

Cuotas de Elastic Load Balancing

Network Load Balancers de ELB

Descripción

Verifica si el uso supera el 80 % de la cuota de Network Load Balancers de ELB.

ID de la verificación

`8wIqYSt25K`

Recursos adicionales

Cuotas de Elastic Load Balancing

Grupo de IAM

Descripción

Verifica si el uso supera el 80 % de la cuota de grupo de IAM.

ID de la verificación

`sU7XX0l7J9`

Recursos adicionales

Cuotas de IAM

Perfiles de instancias de IAM

Descripción

Verifica si el uso supera el 80 % de la cuota de perfiles de instancias de IAM.

ID de la verificación

`n07SS0l7J9`

Recursos adicionales

Cuotas de IAM

Políticas de IAM

Descripción

Verifica si el uso supera el 80 % de la cuota de políticas de IAM.

ID de la verificación

`pR7UU0l7J9`

Recursos adicionales

Cuotas de IAM

Roles de IAM

Descripción

Verifica si el uso supera el 80 % de la cuota de roles de IAM.

ID de la verificación

`oQ7TT0l7J9`

Recursos adicionales

Cuotas de IAM

Certificados de servidor de IAM

Descripción

Verifica si el uso supera el 80 % de la cuota de certificados de servidor de IAM.

ID de la verificación

`rT7WW0l7J9`

Recursos adicionales

Cuotas de IAM

Usuarios de IAM

Descripción

Verifica si el uso supera el 80 % de la cuota de usuarios de IAM.

ID de la verificación

`qS7VV0l7J9`

Recursos adicionales

Cuotas de IAM

Particiones de Kinesis por región

Descripción

Verifica si el uso supera el 80 % de cuota de particiones de Kinesis por región.

ID de la verificación

`bW7HH0l7J9`

Recursos adicionales

Cuotas de Kinesis

Uso del almacenamiento de código de Lambda

Descripción

Comprueba si el uso del almacenamiento de código supera el 80 % del límite de la cuenta.

> **Note**
>
> Los resultados de esta verificación se actualizan automáticamente varias veces al día y no se permiten las solicitudes de actualización. Puede que los cambios tarden unas horas en aparecer. Actualmente, no puede excluir recursos de esta verificación.

ID de la verificación

`c1dfprch07`

Criterios de alerta

- Amarillo: se ha alcanzado el 80 % del límite.

Acción recomendada

Identifique las funciones o las versiones de Lambda que no utilice y elimínelas para liberar espacio de almacenamiento de código en su cuenta en la región. Si necesita almacenamiento adicional, cree un caso de soporte en el Centro de soporte. Si cree que va a superar un límite de servicio, solicite un aumento directamente desde la consola Service Quotas. Si Service Quotas aún no admite su servicio, puede abrir un caso de soporte en el Centro de soporte.

Recursos adicionales

- Uso del almacenamiento de código de Lambda

Columnas de informes

- Status
- Region
- El ARN de la función calificada para este recurso.
- El uso de almacenamiento del código de la función es MegaBytes de 2 decimales.
- La cantidad de versiones de la función
- Hora de la última actualización

Grupos de parámetros de clústeres de RDS

Descripción

Verifica si el uso supera el 80 % de la cuota de grupos de parámetros de clústeres de RDS.

ID de la verificación

`jtlIMO3qZM`

Recursos adicionales

Cuotas de Amazon RDS

Roles de clústeres de RDS

Descripción

Verifica si el uso supera el 80 % de la cuota de roles de clústeres de RDS.

ID de la verificación

`7fuccf1Mx7`

Recursos adicionales

Cuotas de Amazon RDS

Clústeres de RDS

Descripción

Verifica si el uso supera el 80 % de la cuota de clústeres de RDS.

ID de la verificación

`gjqMBn6pjz`

Recursos adicionales

Cuotas de Amazon RDS

Instancias de base de datos de RDS

Descripción

Verifica si el uso supera el 80 % de la cuota de instancias de base de datos de RDS.

ID de la verificación

`XG0aXHpIEt`

Recursos adicionales

Cuotas de Amazon RDS

Instantáneas manuales de base de datos de RDS

Descripción

Verifica si el uso supera el 80 % de la cuota de instantáneas manuales de base de datos de RDS.

ID de la verificación

`dV84wpqRUs`

Recursos adicionales

Cuotas de Amazon RDS

Grupos de parámetros de base de datos de RDS

Descripción

Verifica si el uso supera el 80 % de la cuota de grupos de parámetros de base de datos de RDS.

ID de la verificación

`jEECYg2YVU`

Recursos adicionales

Cuotas de Amazon RDS

Grupos de seguridad de base de datos de RDS

Descripción

Verifica si el uso supera el 80 % de la cuota de grupos de seguridad de base de datos de RDS.

ID de la verificación

`gfZAn3W7wl`

Recursos adicionales

Cuotas de Amazon RDS

Suscripciones de eventos de RDS

Descripción

Verifica si el uso supera el 80 % de la cuota de suscripciones de eventos de RDS.

ID de la verificación

`keAhfbH5yb`

Recursos adicionales

Cuotas de Amazon RDS

Autenticaciones máximas por grupo de seguridad de RDS

Descripción

Verifica si el uso supera el 80 % de la cuota de autenticaciones máximas por grupo de seguridad de RDS.

ID de la verificación

`dBkuNCvqn5`

Recursos adicionales

Cuotas de Amazon RDS

Grupos de opciones de RDS

Descripción

Verifica si el uso supera el 80 % de la cuota de grupos de opciones de RDS.

ID de la verificación

`3Njm0DJQO9`

Recursos adicionales

Cuotas de Amazon RDS

Réplicas de lectura por maestro de RDS

Descripción

Verifica si el uso supera el 80 % de la cuota de réplicas de lectura por maestro de RDS.

ID de la verificación

`pYW8UkYz2w`

Recursos adicionales

Cuotas de Amazon RDS

Instancias reservadas de RDS

Descripción

Verifica si el uso supera el 80 % de la cuota de instancias reservadas de RDS.

ID de la verificación

`UUDv0a5r34`

Recursos adicionales

Cuotas de Amazon RDS

Grupos de subredes de RDS

Descripción

Verifica si el uso supera el 80 % de la cuota de grupos de subredes de RDS.

ID de la verificación

`dYWBaXaaMM`

Recursos adicionales

Cuotas de Amazon RDS

Subredes por grupo de subredes de RDS

Descripción

Verifica si el uso supera el 80 % de la cuota de subredes por grupo de subredes de RDS.

ID de la verificación

`jEhCtdJK0Y`

Recursos adicionales

Cuotas de Amazon RDS

Cuota de almacenamiento total de RDS

Descripción

Verifica si el uso supera el 80 % de la cuota de almacenamiento total de RDS.

ID de la verificación

`P1jhKWEmLa`

Recursos adicionales

Cuotas de Amazon RDS

Zonas alojadas de Route 53

Descripción

Verifica si el uso supera el 80 % de la cuota de zonas alojadas por cuenta de Route 53.

ID de la verificación

`dx3xfcdfMr`

Recursos adicionales

Cuotas de Route 53

Máximo de comprobaciones de estado de Route 53

Descripción

Verifica si el uso supera el 80 % de la cuota de máximo de comprobaciones de estado de Route 53 por cuenta.

ID de la verificación

`ru4xfcdfMr`

Recursos adicionales

Cuotas de Route 53

Conjuntos de delegación reutilizables de Route 53

Descripción

Verifica si el uso supera el 80 % de la cuota de conjuntos de delegación reutilizables por cuenta de Route 53.

ID de la verificación

`ty3xfcdfMr`

Recursos adicionales

Cuotas de Route 53

Políticas de tráfico de Route 53

Descripción

Verifica si el uso supera el 80 % de la cuota de políticas de tráfico por cuenta de Route 53.

ID de la verificación

`dx3xfbjfMr`

Recursos adicionales

Cuotas de Route 53

Instancias de políticas de tráfico de Route 53

Descripción

Verifica si el uso supera el 80 % de la cuota de instancias de políticas de tráfico por cuenta de Route 53.

ID de la verificación

`dx8afcdfMr`

Recursos adicionales

Cuotas de Route 53

Cuota de envío diaria de SES

Descripción

Verifica si el uso supera el 80 % de la cuota de envío diaria de Amazon SES.

ID de la verificación

`hJ7NN0l7J9`

Recursos adicionales

Cuotas de Amazon SES

VPC

Descripción

Verifica si el uso supera el 80 % de la cuota de VPC.

ID de la verificación

`jL7PP0l7J9`

Recursos adicionales

Cuotas de VPC

Gateways de Internet de VPC

Descripción

Verifica si el uso supera el 80 % de la cuota de gateways de Internet de VPC.

ID de la verificación

`kM7QQ0l7J9`

Recursos adicionales

Cuotas de VPC

Excelencia operativa

Puede utilizar las siguientes comprobaciones para la categoría de excelencia operativa.

Nombres de la verificación

- La Amazon API Gateway no registra los registros de ejecución
- API de REST de Amazon API Gateway sin rastreo de X-Ray habilitado
- Registro de CloudFront acceso a Amazon configurado
- La acción CloudWatch de alarma de Amazon está desactivada
- Instancia de Amazon EC2 no gestionada por AWS Systems Manager
- Repositorio de Amazon ECR con la inmutabilidad de etiquetas desactivada
- Desactivación de la información de contenedores en clústeres de Amazon ECS
- El registro de tareas de Amazon ECS no está habilitado
- El registro OpenSearch de Amazon Service CloudWatch no está configurado
- Instancias de base de datos de Amazon RDS en los clústeres con grupos de parámetros heterogéneos
- La supervisión mejorada de Amazon RDS está desactivada
- Amazon RDS Performance Insights está desactivado
- El parámetro track_counts de Amazon RDS está desactivado
- Registro de auditoría de clústeres de Amazon Redshift
- Amazon S3 no tiene habilitadas las notificaciones de eventos
- Los temas de Amazon SNS no registran el estado de entrega de los mensajes
- Amazon VPC sin registros de flujo
- Equilibradores de carga de aplicaciones y equilibradores de carga clásicos sin registros de acceso habilitados
- AWS CloudFormation Notificación de pila
- AWS CloudTrail registro de eventos de datos para objetos en un bucket de S3
- AWS CodeBuild Registro de proyectos
- AWS CodeDeploy Reversión automática y monitor activados
- AWS CodeDeploy Lambda utiliza all-at-once la configuración de implementación
- AWS Elastic Beanstalk Los informes de salud mejorados no están configurados
- AWS Elastic Beanstalk con las actualizaciones de plataforma gestionadas deshabilitadas
- AWS Fargate la versión de la plataforma no es la más reciente
- AWS Systems Manager La Asociación de Directores Estatales no cumple con las normas

- CloudTrail las rutas no están configuradas con Amazon CloudWatch Logs
- La protección contra eliminación de Elastic Load Balancing no está habilitada para los equilibradores de carga
- Comprobación de la protección contra eliminación de clústeres de bases de datos de RDS
- Comprobación automática de la actualización de la versión secundaria de la instancia de base de datos de RDS

La Amazon API Gateway no registra los registros de ejecución

Descripción

Comprueba si Amazon API Gateway tiene CloudWatch los registros activados en el nivel de registro deseado.

Active el CloudWatch registro de los métodos o rutas de WebSocket API de REST en Amazon API Gateway para recopilar los registros de ejecución en CloudWatch los registros de las solicitudes recibidas por sus API. La información contenida en los registros de ejecución ayuda a identificar y solucionar los problemas relacionados con la API.

Puede especificar el ID del nivel de registro (ERROR, INFO) en el parámetro LoggingLevel de las reglas. AWS Config

Consulte la API de REST o la documentación de la WebSocket API para obtener más información sobre cómo CloudWatch iniciar sesión en Amazon API Gateway.

> **Note**
>
> Los resultados de esta verificación se actualizan automáticamente varias veces al día y no se permiten las solicitudes de actualización. Puede que los cambios tarden unas horas en aparecer. Actualmente, no puede excluir recursos de esta verificación.

ID de la verificación

```
c18d2gz125
```

Origen

```
AWS Config Managed Rule: api-gw-execution-logging-enabled
```

Criterios de alerta

Amarillo: la configuración de CloudWatch registro para la recopilación de registros de ejecución no está habilitada en el nivel de registro deseado para una Amazon API Gateway.

Acción recomendada

Active el CloudWatch registro de los registros de ejecución de las API REST de Amazon API Gateway o WebSocket las API con el nivel de registro adecuado (ERROR, INFO).

Para obtener más información, consulte Creación de un registro de flujo

Recursos adicionales

- Configuración del CloudWatch registro de una API REST en API Gateway
- Configurar el registro para una WebSocket API

Columnas de informes

- Status
- Región
- Recurso
- AWS Config Regla
- Parámetros de entrada
- Hora de la última actualización

API de REST de Amazon API Gateway sin rastreo de X-Ray habilitado

Descripción

Comprueba si las API REST de Amazon API Gateway tienen AWS X-Ray el rastreo activado.

Active el rastreo de X-Ray en las API de REST para permitir que API Gateway muestree las solicitudes de invocación de la API mediante la información de rastreo. Esto le permite aprovechar para rastrear y analizar las solicitudes AWS X-Ray a medida que viajan a través de las API REST de API Gateway hacia los servicios descendentes.

Para obtener más información, consulte Rastreo de solicitudes de las API de REST mediante X-Ray.

> **Note**
>
> Los resultados de esta verificación se actualizan automáticamente varias veces al día y no se permiten las solicitudes de actualización. Puede que los cambios tarden unas horas en aparecer. Actualmente, no puede excluir recursos de esta verificación.

ID de la verificación

`c18d2gz126`

Origen

`AWS Config Managed Rule: api-gw-xray-enabled`

Criterios de alerta

Amarillo: el rastreo de X-Ray no está activado en una API de REST de API Gateway.

Acción recomendada

Habilite el rastreo de X-Ray para las API de REST de API Gateway.

Para obtener más información, consulte Configuración AWS X-Ray con las API REST de API Gateway.

Recursos adicionales

- Rastreo de solicitudes de usuario a las API de REST mediante X-Ray
- ¿Qué es AWS X-Ray?

Columnas de informes

- Status
- Región
- Recurso
- AWS Config Regla
- Parámetros de entrada
- Hora de la última actualización

Registro de CloudFront acceso a Amazon configurado

Descripción

Comprueba si CloudFront las distribuciones de Amazon están configuradas para capturar información de los registros de acceso al servidor Amazon S3. Los registros de acceso al servidor Amazon S3 contienen información detallada sobre cada solicitud de usuario que CloudFront recibe.

Puede ajustar el nombre del bucket de Amazon S3 para almacenar los registros de acceso al servidor mediante el BucketName parámetro S3 de sus AWS Config reglas.

Para obtener más información, consulte Configuración y uso de registros estándar (registros de acceso).

> **Note**
>
> Los resultados de esta verificación se actualizan automáticamente varias veces al día y no se permiten las solicitudes de actualización. Puede que los cambios tarden unas horas en aparecer. Actualmente, no puede excluir recursos de esta verificación.

ID de la verificación

`c18d2gz110`

Origen

`AWS Config Managed Rule: cloudfront-accesslogs-enabled`

Criterios de alerta

Amarillo: el registro de CloudFront acceso a Amazon no está activado

Acción recomendada

Asegúrese de activar el registro de CloudFront acceso para recopilar información detallada sobre cada solicitud de usuario que CloudFront reciba.

Puede habilitar los registros estándar cuando crea o actualiza una distribución.

Para obtener más información, consulte Valores que especifica cuando crea o actualiza una distribución.

Recursos adicionales

- Valores que deben especificarse cuando se crea o actualiza una distribución
- Configuración y uso de registros estándar (registros de acceso)

Columnas de informes

- Status
- Región
- Recurso
- AWS Config Regla
- Parámetros de entrada
- Hora de la última actualización

La acción CloudWatch de alarma de Amazon está desactivada

Descripción

Comprueba si la acción CloudWatch de alarma de Amazon está desactivada.

Puedes utilizarla AWS CLI para activar o desactivar la función de acción de tu alarma. O bien, puedes deshabilitar o habilitar la función de acción mediante programación mediante el AWS SDK. Cuando la función de acción de alarma está desactivada, CloudWatch no realiza ninguna acción definida en ningún estado (OK, INSUFFICIENT_DATA, ALARM).

> **Note**
>
> Los resultados de esta verificación se actualizan automáticamente varias veces al día y no se permiten las solicitudes de actualización. Puede que los cambios tarden unas horas en aparecer. Actualmente, no puede excluir recursos de esta verificación.

ID de la verificación

```
c18d2gz109
```

Origen

```
AWS Config Managed Rule: cloudwatch-alarm-action-enabled-check
```

Criterios de alerta

Amarillo: la acción de CloudWatch alarma de Amazon no está habilitada. No se lleva a cabo ninguna acción en ningún estado de alarma.

Acción recomendada

Activa las acciones en tus CloudWatch alarmas a menos que tengas un motivo válido para desactivarlas, por ejemplo, con fines de prueba.

Si la CloudWatch alarma ya no es necesaria, elimínela para evitar incurrir en costes innecesarios.

Para obtener más información, consulta enable-alarm-actions en la Referencia de AWS CLI comandos y func (*) en la Referencia de la API CloudWatch SDK EnableAlarmActions for Go AWS .

Columnas de informes

- Status
- Región
- Recurso
- AWS Config Regla
- Parámetros de entrada
- Hora de la última actualización

Instancia de Amazon EC2 no gestionada por AWS Systems Manager

Descripción

Comprueba si las instancias de Amazon EC2 de su cuenta están gestionadas por. AWS Systems Manager

Systems Manager ayuda a comprender y controlar el estado actual de la instancia de Amazon EC2 y las configuraciones del sistema operativo. Con Systems Manager, puede recopilar información de configuración e inventario del software sobre su flota de instancias, incluido el software instalado en ellas. Esto permite realizar un seguimiento detallado de la configuración del sistema, los niveles de parches del sistema operativo, las configuraciones de las aplicaciones y otros detalles sobre su implementación.

Para obtener más información, consulte Configuración de Systems Manager para instancias de EC2.

> **Note**
>
> Los resultados de esta verificación se actualizan automáticamente varias veces al día y no se permiten las solicitudes de actualización. Puede que los cambios tarden unas horas en aparecer. Actualmente, no puede excluir recursos de esta verificación.

ID de la verificación

`c18d2gz145`

Origen

`AWS Config Managed Rule: ec2-instance-managed-by-systems-manager`

Criterios de alerta

Amarillo: las instancias de Amazon EC2 no se administran mediante Systems Manager.

Acción recomendada

Configure la instancia de Amazon EC2 para que se administre mediante Systems Manager.

Esta comprobación no se puede excluir de la vista de la Trusted Advisor consola.

Para obtener más información, consulte ¿Por qué mi instancia de EC2 no se muestra como nodo administrado o muestra un estado de "Conexión perdida" en Systems Manager?.

Recursos adicionales

Configuración de Systems Manager para instancias de EC2

Columnas de informes

- Status
- Región
- Recurso
- AWS Config Regla
- Parámetros de entrada
- Hora de la última actualización

Repositorio de Amazon ECR con la inmutabilidad de etiquetas desactivada

Descripción

Comprueba si un repositorio privado de Amazon ECR tiene activada la inmutabilidad de las etiquetas de imagen.

Habilite la inmutabilidad de etiquetas de imagen para un repositorio de Amazon ECR privado para evitar así que se sobrescriban las etiquetas de imagen. Esto permite confiar en las etiquetas descriptivas como un mecanismo fiable para rastrear e identificar las imágenes de forma única. Por ejemplo, si la inmutabilidad de las etiquetas de imagen está activada, los usuarios pueden utilizar una etiqueta de imagen de forma fiable para correlacionar una versión de la imagen implementada con la versión que produjo dicha imagen.

Para obtener más información, consulte Mutabilidad de etiquetas de imagen.

> **Note**
>
> Los resultados de esta verificación se actualizan automáticamente varias veces al día y no se permiten las solicitudes de actualización. Puede que los cambios tarden unas horas en aparecer. Actualmente, no puede excluir recursos de esta verificación.

ID de la verificación

`c18d2gz129`

Origen

`AWS Config Managed Rule: ecr-private-tag-immutability-enabled`

Criterios de alerta

Amarillo: un repositorio privado de Amazon ECR no tiene habilitada la inmutabilidad de etiquetas.

Acción recomendada

Habilite la inmutabilidad de las etiquetas de imagen en sus repositorios privados de Amazon ECR.

Para obtener más información, consulte Mutabilidad de etiquetas de imagen.

Columnas de informes

- Status

- Región
- Recurso
- AWS Config Regla
- Parámetros de entrada
- Hora de la última actualización

Desactivación de la información de contenedores en clústeres de Amazon ECS

Descripción

Comprueba si Amazon CloudWatch Container Insights está activado en sus clústeres de Amazon ECS.

CloudWatch Container Insights recopila, agrega y resume las métricas y los registros de sus aplicaciones y microservicios contenerizados. Las métricas incluyen la utilización de recursos como CPU, memoria, disco y red.

Para obtener más información, consulte Amazon ECS CloudWatch Container Insights.

> **Note**
>
> Los resultados de esta verificación se actualizan automáticamente varias veces al día y no se permiten las solicitudes de actualización. Puede que los cambios tarden unas horas en aparecer. Actualmente, no puede excluir recursos de esta verificación.

ID de la verificación

`c18d2gz173`

Origen

`AWS Config Managed Rule: ecs-container-insights-enabled`

Criterios de alerta

Amarillo: el clúster de Amazon ECS no tiene habilitada la información de contenedores.

Acción recomendada

Active CloudWatch Container Insights en sus clústeres de Amazon ECS.

Para obtener más información, consulte Uso de la Información de contenedores.

Recursos adicionales

Información sobre CloudWatch contenedores de Amazon ECS

Columnas de informes

- Status
- Región
- Recurso
- AWS Config Regla
- Parámetros de entrada
- Hora de la última actualización

El registro de tareas de Amazon ECS no está habilitado

Descripción

Comprueba si la configuración del registro está establecida en las definiciones de tareas activas de Amazon ECS.

Cuando se comprueba la configuración de los registros en las definiciones de tareas de Amazon ECS, se asegura de que los registros generados por los contenedores estén correctamente configurados y almacenados. Esto ayuda a identificar y solucionar los problemas con mayor rapidez, a optimizar el rendimiento y a cumplir los requisitos de conformidad.

De forma predeterminada, los registros que se capturan muestran la salida del comando que aparecería normalmente en un terminal interactivo si el contenedor se ejecutara localmente. El controlador awslogs pasa estos registros de Docker a Amazon Logs. CloudWatch

Para obtener más información, consulte Uso del controlador de registros awslogs.

> **Note**
>
> Los resultados de esta verificación se actualizan automáticamente varias veces al día y no se permiten las solicitudes de actualización. Puede que los cambios tarden unas horas en aparecer. Actualmente, no puede excluir recursos de esta verificación.

ID de la verificación

`c18d2gz175`

Origen

`AWS Config Managed Rule: ecs-task-definition-log-configuration`

Criterios de alerta

Amarillo: la definición de tareas de Amazon ECS no tiene una configuración de registro.

Acción recomendada

Considere la posibilidad de especificar la configuración del controlador de registro en la definición del contenedor para enviar la información de registro a CloudWatch Logs o a un controlador de registro diferente.

Para obtener más información, consulte LogConfiguration.

Recursos adicionales

Considere la posibilidad de especificar la configuración del controlador de registro en la definición del contenedor para enviar la información de registro a CloudWatch Logs o a un controlador de registro diferente.

Para obtener más información, consulte Ejemplificación de definiciones de tareas.

Columnas de informes

- Status
- Región
- Recurso
- AWS Config Regla
- Parámetros de entrada
- Hora de la última actualización

El registro OpenSearch de Amazon Service CloudWatch no está configurado

Descripción

Comprueba si los dominios OpenSearch de Amazon Service están configurados para enviar registros a Amazon CloudWatch Logs.

La supervisión de los registros es fundamental para mantener la fiabilidad, la disponibilidad y el rendimiento del OpenSearch Servicio.

Los registros lentos de búsqueda, los registros lentos de índice y los registros de errores son útiles para la solución de problemas de rendimiento y estabilidad de la carga de trabajo. Estos registros deben estar habilitados para capturar datos.

Puede especificar los tipos de registro que desea filtrar (error, búsqueda, índice) mediante el parámetro logTypes de sus AWS Config reglas.

Para obtener más información, consulta Monitorización de los dominios OpenSearch de Amazon Service.

> **Note**
>
> Los resultados de esta verificación se actualizan automáticamente varias veces al día y no se permiten las solicitudes de actualización. Puede que los cambios tarden unas horas en aparecer. Actualmente, no puede excluir recursos de esta verificación.

ID de la verificación

`c18d2gz184`

Origen

`AWS Config Managed Rule: opensearch-logs-to-cloudwatch`

Criterios de alerta

Amarillo: Amazon OpenSearch Service no tiene una configuración de registro con Amazon CloudWatch Logs

Acción recomendada

Configure los dominios de OpenSearch servicio para publicar CloudWatch registros en Logs.

Para obtener más información, consulte Habilitación de la publicación de registros (consola).

Recursos adicionales

- Métricas OpenSearch de clústeres de Monitoring Service con Amazon CloudWatch

Columnas de informes

- Status

- Región
- Recurso
- AWS Config Regla
- Parámetros de entrada
- Hora de la última actualización

Instancias de base de datos de Amazon RDS en los clústeres con grupos de parámetros heterogéneos

Descripción

Recomendamos que todas las instancias de base de datos del clúster de base de datos utilicen el mismo grupo de parámetros de base de datos.

> **Note**
>
> Los resultados de esta verificación se actualizan automáticamente varias veces al día y no se permiten las solicitudes de actualización. Puede que los cambios tarden unas horas en aparecer. Actualmente, no puede excluir recursos de esta verificación.

> **Note**
>
> Cuando se detiene una instancia de base de datos o un clúster de base de datos, puede ver las recomendaciones de Amazon RDS en un plazo Trusted Advisor de 3 a 5 días. Transcurridos cinco días, las recomendaciones no estarán disponibles en Trusted Advisor. Para ver las recomendaciones, abra la consola de Amazon RDS y, a continuación, seleccione Recommendations.
> Si elimina una instancia de base de datos o un clúster de base de datos, las recomendaciones asociadas a esas instancias o clústeres no estarán disponibles en Trusted Advisor la consola de administración de Amazon RDS.

ID de la verificación

`c1qf5bt010`

Criterios de alerta

Amarillo: los clústeres de bases de datos tienen las instancias de base de datos con grupos de parámetros heterogéneos.

Acción recomendada

Asocie la instancia de base de datos con el grupo de parámetros de base de datos asociado a la instancia de escritura de su clúster de base de datos.

Recursos adicionales

Cuando las instancias de base de datos de su clúster de base de datos utilizan diferentes grupos de parámetros de base de datos, puede producirse un comportamiento incoherente durante una conmutación por error o problemas de compatibilidad entre las instancias de base de datos de su clúster de base de datos.

Para obtener más información, consulte Trabajo con los grupos de parámetros.

Columnas de informes

- Status
- Región
- Recurso
- Valor recomendado
- Nombre del motor
- Hora de la última actualización

La supervisión mejorada de Amazon RDS está desactivada

Descripción

Los recursos de la base de datos no tienen activada la monitorización mejorada. El monitoreo mejorado proporciona métricas del sistema operativo en tiempo real para el monitoreo y la solución de problemas.

> **Note**
>
> Los resultados de esta verificación se actualizan automáticamente varias veces al día y no se permiten las solicitudes de actualización. Puede que los cambios tarden unas horas en aparecer. Actualmente, no puede excluir recursos de esta verificación.

> **Note**
>
> Cuando se detiene una instancia de base de datos o un clúster de base de datos, puede ver las recomendaciones de Amazon RDS en un plazo Trusted Advisor de 3 a 5 días. Transcurridos cinco días, las recomendaciones no estarán disponibles en Trusted Advisor. Para ver las recomendaciones, abra la consola de Amazon RDS y, a continuación, seleccione Recommendations.
> Si elimina una instancia de base de datos o un clúster de base de datos, las recomendaciones asociadas a esas instancias o clústeres no estarán disponibles en Trusted Advisor la consola de administración de Amazon RDS.

ID de la verificación

`c1qf5bt004`

Criterios de alerta

Amarillo: los recursos de Amazon RDS no tienen activada la supervisión mejorada.

Acción recomendada

Active la monitorización mejorada

Recursos adicionales

La supervisión mejorada para Amazon RDS proporciona una visibilidad adicional del estado de las instancias de base de datos. Le recomendamos que active la supervisión mejorada. Cuando la opción de supervisión mejorada está activada para su instancia de base de datos, recopila las métricas fundamentales del sistema operativo y la información del proceso.

Para obtener más información sobre la supervisión mejorada de Amazon RDS, consulte Supervisión de las métricas del SO con la supervisión mejorada.

Columnas de informes

- Status
- Región
- Recurso
- Valor recomendado
- Nombre del motor

- Hora de la última actualización

Amazon RDS Performance Insights está desactivado

Descripción

Amazon RDS Performance Insights monitorea la carga de las instancias de base de datos para ayudarle a analizar y resolver los problemas de rendimiento de las bases de datos. Le recomendamos que active Información de rendimiento.

> **Note**
>
> Los resultados de esta verificación se actualizan automáticamente varias veces al día y no se permiten las solicitudes de actualización. Puede que los cambios tarden unas horas en aparecer. Actualmente, no puede excluir recursos de esta verificación.

> **Note**
>
> Cuando se detiene una instancia de base de datos o un clúster de base de datos, puede ver las recomendaciones de Amazon RDS en un plazo Trusted Advisor de 3 a 5 días. Transcurridos cinco días, las recomendaciones no estarán disponibles en Trusted Advisor. Para ver las recomendaciones, abra la consola de Amazon RDS y, a continuación, seleccione Recommendations.
> Si elimina una instancia de base de datos o un clúster de base de datos, las recomendaciones asociadas a esas instancias o clústeres no estarán disponibles en Trusted Advisor la consola de administración de Amazon RDS.

ID de la verificación

`c1qf5bt012`

Criterios de alerta

Amarillo: los recursos de Amazon RDS no tienen activado Performance Insights.

Acción recomendada

Activar Información de rendimiento.

Recursos adicionales

Performance Insights utiliza un método de recopilación de datos ligero que no afecta al rendimiento de las aplicaciones. Performance Insights le ayuda a evaluar rápidamente la carga de la base de datos.

Para obtener más información, consulte Supervisión de la carga de la base de datos con Performance Insights en Amazon RDS.

Columnas de informes

- Status
- Región
- Recurso
- Valor recomendado
- Nombre del motor
- Hora de la última actualización

El parámetro track_counts de Amazon RDS está desactivado

Descripción

Cuando el parámetro track_counts está desactivado, la base de datos no recopila las estadísticas de actividad de la base de datos. Autovacuum necesita estas estadísticas para funcionar correctamente.

Se recomienda establecer el parámetro track_counts en 1

> **Note**
>
> Los resultados de esta verificación se actualizan automáticamente varias veces al día y no se permiten las solicitudes de actualización. Puede que los cambios tarden unas horas en aparecer. Actualmente, no puede excluir recursos de esta verificación.

> **Note**
>
> Cuando se detiene una instancia de base de datos o un clúster de base de datos, puede ver las recomendaciones de Amazon RDS en un plazo Trusted Advisor de 3

a 5 días. Transcurridos cinco días, las recomendaciones no estarán disponibles en Trusted Advisor. Para ver las recomendaciones, abra la consola de Amazon RDS y, a continuación, seleccione Recommendations.
Si elimina una instancia de base de datos o un clúster de base de datos, las recomendaciones asociadas a esas instancias o clústeres no estarán disponibles en Trusted Advisor la consola de administración de Amazon RDS.

ID de la verificación

`c1qf5bt027`

Criterios de alerta

Amarillo: los grupos de parámetros de base de datos tienen el parámetro track_counts desactivado.

Acción recomendada

Establezca el parámetro track_counts en 1

Recursos adicionales

Cuando el parámetro track_counts está desactivado, se deshabilita la recopilación de estadísticas de actividad de la base de datos. El daemon del autovacuum requiere las estadísticas recopiladas para identificar las tablas de autovacuum y autoanalyze.

Para obtener más información, consulte Estadísticas en tiempo de ejecución de PostgreSQL en el sitio web de documentación de PostgreSQL.

Columnas de informes

- Status
- Región
- Recurso
- Valor del parámetro
- Valor recomendado
- Hora de la última actualización

Registro de auditoría de clústeres de Amazon Redshift

Descripción

Comprueba si los clústeres de Amazon Redshift tienen habilitado el registro de auditoría de bases de datos. Amazon Redshift registra información acerca de las conexiones y las actividades del usuario en la base de datos.

Puede especificar el nombre de bucket de Amazon S3 de registro que desee para que coincida con el parámetro bucketNames de sus AWS Config reglas.

Para obtener más información, consulte Registro de auditoría de la base de datos.

> **Note**
>
> Los resultados de esta verificación se actualizan automáticamente varias veces al día y no se permiten las solicitudes de actualización. Puede que los cambios tarden unas horas en aparecer. Actualmente, no puede excluir recursos de esta verificación.

ID de la verificación

`c18d2gz134`

Origen

`AWS Config Managed Rule: redshift-audit-logging-enabled`

Criterios de alerta

Amarillo: un clúster de Amazon Redshift tiene deshabilitado el registro de auditoría de bases de datos

Acción recomendada

Habilite el registro y el monitoreo de los clústeres de Amazon Redshift.

Para obtener más información, consulte Configuración de la auditoría mediante la consola.

Recursos adicionales

Registro y monitoreo en Amazon Redshift

Columnas de informes

- Status

- Región
- Recurso
- AWS Config Regla
- Parámetros de entrada
- Hora de la última actualización

Amazon S3 no tiene habilitadas las notificaciones de eventos

Descripción

Comprueba si las notificaciones de eventos de Amazon S3 están habilitadas o están configuradas correctamente con el destino o los tipos deseados.

La característica de notificaciones de eventos de Amazon S3 envía avisos cuando se producen ciertos eventos en los buckets de S3. Amazon S3 puede enviar mensajes de notificación a colas de Amazon SQS, temas y funciones de Amazon SNS. AWS Lambda

Puede especificar el destino y los tipos de eventos que desee mediante los parámetros DestinationARN y EventTypes de sus reglas. AWS Config

Para obtener más información, consulte Notificaciones de eventos de Amazon S3.

> **Note**
>
> Los resultados de esta verificación se actualizan automáticamente varias veces al día y no se permiten las solicitudes de actualización. Puede que los cambios tarden unas horas en aparecer. Actualmente, no puede excluir recursos de esta verificación.

ID de la verificación

`c18d2gz163`

Origen

`AWS Config Managed Rule: s3-event-notifications-enabled`

Criterios de alerta

Amarillo: Amazon S3 no tiene habilitadas las notificaciones de eventos o no está configurado con el destino o los tipos deseados.

Acción recomendada

Configure las notificaciones de eventos de Amazon S3 para los eventos de objetos y buckets.

Para obtener más información, consulte Habilitación y configuración de notificaciones de eventos mediante la consola de Amazon S3.

Columnas de informes

- Status
- Región
- Recurso
- AWS Config Regla
- Parámetros de entrada
- Hora de la última actualización

Los temas de Amazon SNS no registran el estado de entrega de los mensajes

Descripción

Comprueba si los temas de Amazon SNS tienen activado el registro del estado de entrega de mensajes.

Configure los temas de Amazon SNS para registrar el estado de entrega de los mensajes a fin de proporcionar una mejor perspectiva operativa. Por ejemplo, el registro de entrega de mensajes verifica si un mensaje se entregó a un punto de conexión de Amazon SNS en particular. Además, ayuda a identificar la respuesta enviada desde el punto de conexión.

Para obtener más información, consulte Estado de entrega de mensajes de Amazon SNS.

> **Note**
>
> Los resultados de esta verificación se actualizan automáticamente varias veces al día y no se permiten las solicitudes de actualización. Puede que los cambios tarden unas horas en aparecer. Actualmente, no puede excluir recursos de esta verificación.

ID de la verificación

`c18d2gz121`

Origen

`AWS Config Managed Rule: sns-topic-message-delivery-notification-enabled`

Criterios de alerta

Amarillo: el registro del estado de entrega de mensajes no está habilitado para un tema de Amazon SNS.

Acción recomendada

Habilite el registro del estado de entrega de mensajes para sus temas de SNS.

Para obtener más información, consulte Configuración del registro del estado de entrega mediante la Consola de administración de AWS.

Columnas de informes

- Status
- Región
- Recurso
- AWS Config Regla
- Parámetros de entrada
- Hora de la última actualización

Amazon VPC sin registros de flujo

Descripción

Comprueba si los registros de flujo de Amazon Virtual Private Cloud se crearon para una VPC.

Puede especificar el tipo de tráfico mediante el parámetro TrafficType en sus AWS Config reglas.

Para obtener más información, consulte Registro del tráfico de IP con los registros de flujo de la VPC.

> **Note**
>
> Los resultados de esta verificación se actualizan automáticamente varias veces al día y no se permiten las solicitudes de actualización. Puede que los cambios tarden unas horas en aparecer. Actualmente, no puede excluir recursos de esta verificación.

ID de la verificación

`c18d2gz122`

Origen

`AWS Config Managed Rule: vpc-flow-logs-enabled`

Criterios de alerta

Amarillo: las VPC no tienen registros de flujo de Amazon VPC.

Acción recomendada

Cree registros de flujo de la VPC para cada una de sus VPC.

Para obtener más información, consulte Creación de un registro de flujo

Columnas de informes

- Status
- Región
- Recurso
- AWS Config Regla
- Parámetros de entrada
- Hora de la última actualización

Equilibradores de carga de aplicaciones y equilibradores de carga clásicos sin registros de acceso habilitados

Descripción

Comprueba si los equilibradores de carga de aplicaciones y los equilibradores de carga clásicos tienen habilitados los registros de acceso.

Elastic Load Balancing proporciona registros de acceso que capturan información detallada sobre las solicitudes enviadas al equilibrador de carga. Cada registro contiene distintos datos, como el momento en que se recibió la solicitud, la dirección IP del cliente, las latencias, las rutas de solicitud y las respuestas del servidor. Puede utilizar estos registros de acceso para analizar los patrones de tráfico y solucionar problemas.

El registro de acceso es una característica opcional de Elastic Load Balancing que está desactivada de forma predeterminada. Una vez que se ha habilitado el registro de acceso del

equilibrador de carga, Elastic Load Balancing captura los registros y los almacena en el bucket de Amazon S3 que haya especificado.

Puede especificar el registro de acceso (bucket) de Amazon S3 que quiere comprobar mediante el BucketNames parámetro s3 de sus AWS Config reglas.

Para obtener más información, consulte Registros de acceso del equilibrador de carga de aplicación o Registros de acceso del equilibrador de carga clásico.

> **Note**
>
> Los resultados de esta verificación se actualizan automáticamente varias veces al día y no se permiten las solicitudes de actualización. Puede que los cambios tarden unas horas en aparecer. Actualmente, no puede excluir recursos de esta verificación.

ID de la verificación

`c18d2gz167`

Origen

`AWS Config Managed Rule: elb-logging-enabled`

Criterios de alerta

Amarillo: la característica de registros de acceso no está habilitada para un equilibrador de carga de aplicación ni un equilibrador de carga clásico.

Acción recomendada

Habilite los registros de acceso para los equilibradores de carga de aplicaciones y equilibradores de carga clásicos.

Para obtener más información, consulte Habilitación de los registros de acceso del equilibrador de carga de aplicación o Habilitación de los registros de acceso del equilibrador de carga clásico.

Columnas de informes

- Status
- Región
- Recurso
- AWS Config Regla

- Parámetros de entrada
- Hora de la última actualización

AWS CloudFormation Notificación de pila

Descripción

Comprueba si todas tus AWS CloudFormation pilas utilizan Amazon SNS para recibir notificaciones cuando se produce un evento.

Puede configurar esta comprobación para buscar ARN de temas específicos de Amazon SNS mediante los parámetros de sus reglas. AWS Config

Para obtener más información, consulte Configuración de las opciones de AWS CloudFormation pila.

> **Note**
>
> Los resultados de esta verificación se actualizan automáticamente varias veces al día y no se permiten las solicitudes de actualización. Puede que los cambios tarden unas horas en aparecer. Actualmente, no puede excluir recursos de esta verificación.

ID de la verificación

`c18d2gz111`

Origen

`AWS Config Managed Rule: cloudformation-stack-notification-check`

Criterios de alerta

Amarillo: las notificaciones de eventos de Amazon SNS para tus AWS CloudFormation stacks no están activadas.

Acción recomendada

Asegúrese de que sus AWS CloudFormation pilas utilicen Amazon SNS para recibir notificaciones cuando se produzca un evento.

La supervisión de los eventos de la pila le ayuda a responder rápidamente a las acciones no autorizadas que puedan alterar su AWS entorno.

Recursos adicionales

¿Cómo puedo recibir una alerta por correo electrónico cuando mi CloudFormation pila de AWS pase al estado ROLLBACK_IN_PROGRESS?

Columnas de informes

- Status
- Región
- Recurso
- AWS Config Regla
- Parámetros de entrada
- Hora de la última actualización

AWS CloudTrail registro de eventos de datos para objetos en un bucket de S3

Descripción

Comprueba si al menos una AWS CloudTrail ruta registra los eventos de datos de Amazon S3 para todos sus buckets de Amazon S3.

Para obtener más información, consulte el Registro de llamadas a la API de Amazon S3 mediante AWS CloudTrail.

> **Note**
>
> Los resultados de esta verificación se actualizan automáticamente varias veces al día y no se permiten las solicitudes de actualización. Puede que los cambios tarden unas horas en aparecer. Actualmente, no puede excluir recursos de esta verificación.

ID de la verificación

```
c18d2gz166
```

Origen

```
AWS Config Managed Rule: cloudtrail-s3-dataevents-enabled
```

Criterios de alerta

Amarillo: el registro de AWS CloudTrail eventos para los buckets de Amazon S3 no está configurado

Acción recomendada

Habilite el registro de CloudTrail eventos para los buckets y objetos de Amazon S3 para realizar un seguimiento de las solicitudes de acceso al bucket de destino.

Para obtener más información, consulte Habilitar el registro de CloudTrail eventos para buckets y objetos de S3.

Columnas de informes

- Status
- Región
- Recurso
- AWS Config Regla
- Parámetros de entrada
- Hora de la última actualización

AWS CodeBuild Registro de proyectos

Descripción

Comprueba si el entorno AWS CodeBuild del proyecto utiliza el registro. Las opciones de registro pueden ser registros en Amazon CloudWatch Logs, integrados en un bucket de Amazon S3 específico, o ambos. Habilitar el registro en un CodeBuild proyecto puede ofrecer varios beneficios, como la depuración y la auditoría.

Puede especificar el nombre del bucket o grupo de CloudWatch registros de Amazon S3 para almacenar los registros mediante el parámetro s3 BucketNames o cloud WatchGroup Names de sus AWS Config reglas.

Para obtener más información, consulte Monitorización de AWS CodeBuild.

> **Note**
>
> Los resultados de esta verificación se actualizan automáticamente varias veces al día y no se permiten las solicitudes de actualización. Puede que los cambios tarden unas horas en aparecer. Actualmente, no puede excluir recursos de esta verificación.

ID de la verificación

`c18d2gz113`

Origen

`AWS Config Managed Rule: codebuild-project-logging-enabled`

Criterios de alerta

Amarillo: el registro de AWS CodeBuild proyectos no está activado.

Acción recomendada

Asegúrese de que el registro esté activado en su AWS CodeBuild proyecto. Esta comprobación no se puede excluir de la vista de la AWS Trusted Advisor consola.

Para obtener más información, consulte Inicio de sesión y supervisión AWS CodeBuild.

Columnas de informes

- Status
- Región
- Recurso
- AWS Config Regla
- Parámetros de entrada
- Hora de la última actualización

AWS CodeDeploy Reversión automática y monitor activados

Descripción

Comprueba si el grupo de implementación está configurado con la reversión automática de la implementación y el monitoreo de la implementación con alarmas asociadas. Si algo sale mal

durante una implementación, esta se revierte automáticamente y la aplicación permanece en un estado estable

Para obtener más información, consulte Reimplementar y revertir una implementación con. CodeDeploy

> **Note**
>
> Los resultados de esta verificación se actualizan automáticamente varias veces al día y no se permiten las solicitudes de actualización. Puede que los cambios tarden unas horas en aparecer. Actualmente, no puede excluir recursos de esta verificación.

ID de la verificación

`c18d2gz114`

Origen

`AWS Config Managed Rule: codedeploy-auto-rollback-monitor-enabled`

Criterios de alerta

Amarillo: la reversión AWS CodeDeploy automática de la implementación y la supervisión de la implementación no están habilitadas.

Acción recomendada

Configure un grupo de implementación o una implementación para que se restauren automáticamente si una implementación produce un error o si se supera un umbral de monitoreo que haya especificado.

Configure la alarma para que monitoree varias métricas, como el uso de la CPU, el uso de la memoria o del tráfico de red, durante el proceso de implementación. Si alguna de estas métricas supera ciertos umbrales, las alarmas se activan y la implementación se detiene o se revierte.

Para obtener información sobre cómo configurar las reversiones automáticas y las alarmas para sus grupos de implementación, consulte Configuración de opciones avanzadas para un grupo de implementación.

Recursos adicionales

¿Qué es? CodeDeploy

Columnas de informes

- Status
- Región
- Recurso
- AWS Config Regla
- Parámetros de entrada
- Hora de la última actualización

AWS CodeDeploy Lambda utiliza all-at-once la configuración de implementación

Descripción

Comprueba si el grupo de AWS CodeDeploy despliegue de la plataforma de AWS Lambda cómputo utiliza la configuración all-at-once de despliegue.

Para reducir el riesgo de que se produzcan errores en el despliegue de las funciones de Lambda CodeDeploy, se recomienda utilizar la configuración de despliegue lineal o canario en lugar de la opción predeterminada, en la que todo el tráfico se desplaza de la función Lambda original a la función actualizada a la vez.

Para obtener más información, consulte Versiones de la función de Lambda y Configuración de implementación.

> **Note**
>
> Los resultados de esta verificación se actualizan automáticamente varias veces al día y no se permiten las solicitudes de actualización. Puede que los cambios tarden unas horas en aparecer. Actualmente, no puede excluir recursos de esta verificación.

ID de la verificación

```
c18d2gz115
```

Origen

```
AWS Config Managed Rule: codedeploy-lambda-allatonce-traffic-shift-
disabled
```

Criterios de alerta

Amarillo: la implementación de AWS CodeDeploy Lambda usa la configuración de all-at-once implementación para transferir todo el tráfico a las funciones de Lambda actualizadas de una sola vez.

Acción recomendada

Utilice la configuración de despliegue Canary o Linear del grupo de CodeDeploy despliegue para la plataforma de cómputo Lambda.

Recursos adicionales

Configuración de implementación

Columnas de informes

- Status
- Región
- Recurso
- AWS Config Regla
- Parámetros de entrada
- Hora de la última actualización

AWS Elastic Beanstalk Los informes de salud mejorados no están configurados

Descripción

Comprueba si un AWS Elastic Beanstalk entorno está configurado para mejorar los informes de estado.

Los informes de estado mejorados de Elastic Beanstalk proporcionan métricas de rendimiento detalladas, como el uso de la CPU, el uso de la memoria, el tráfico de red y la información del estado de la infraestructura, como la cantidad de instancias y el estado del equilibrador de carga.

Para obtener más información, consulte Informes y monitoreo de estado mejorados.

> **Note**
>
> Los resultados de esta verificación se actualizan automáticamente varias veces al día y no se permiten las solicitudes de actualización. Puede que los cambios tarden unas horas en aparecer. Actualmente, no puede excluir recursos de esta verificación.

ID de la verificación

`c18d2gz108`

Origen

`AWS Config Managed Rule: beanstalk-enhanced-health-reporting-enabled`

Criterios de alerta

Amarillo: el entorno de Elastic Beanstalk no está configurado para informes de estado mejorados

Acción recomendada

Compruebe si el entorno de Elastic Beanstalk está configurado para informes de estado mejorados.

Para obtener más información, consulte Habilitación de informes de estado mejorados mediante la consola de Elastic Beanstalk.

Recursos adicionales

- Habilitación de informes de estado mejorados de Elastic Beanstalk
- Informes y monitoreo de estado mejorados

Columnas de informes

- Status
- Región
- Recurso
- AWS Config Regla
- Parámetros de entrada
- Hora de la última actualización

AWS Elastic Beanstalk con las actualizaciones de plataforma gestionadas deshabilitadas

Descripción

Comprueba si las actualizaciones de la plataforma administradas en las plantillas de configuración y los entornos de Elastic Beanstalk están habilitadas.

AWS Elastic Beanstalk publica periódicamente actualizaciones de la plataforma para proporcionar correcciones, actualizaciones de software y nuevas funciones. Con las actualizaciones de la plataforma administradas, Elastic Beanstalk puede hacer actualizaciones de la plataforma automáticamente para nuevos parches y versiones secundarias de la plataforma.

Puede especificar el nivel de actualización que desee en los UpdateLevelparámetros de sus AWS Config reglas.

Para obtener más información, consulte Actualización de la versión de la plataforma del entorno de Elastic Beanstalk.

> **Note**
>
> Los resultados de esta verificación se actualizan automáticamente varias veces al día y no se permiten las solicitudes de actualización. Puede que los cambios tarden unas horas en aparecer. Actualmente, no puede excluir recursos de esta verificación.

ID de la verificación

`c18d2gz177`

Origen

`AWS Config Managed Rule: elastic-beanstalk-managed-updates-enabled`

Criterios de alerta

Amarillo: las actualizaciones AWS Elastic Beanstalk gestionadas de la plataforma no están configuradas en absoluto, ni siquiera a nivel secundario o de parche.

Acción recomendada

Habilite las actualizaciones de la plataforma administradas en sus entornos de Elastic Beanstalk o configúrelas en un nivel secundario o de actualización.

Para obtener más información, consulte Actualizaciones de la plataforma administradas.

Recursos adicionales

- Habilitación de informes de estado mejorados de Elastic Beanstalk
- Informes y monitoreo de estado mejorados

Columnas de informes

- Status
- Región
- Recurso
- AWS Config Regla
- Parámetros de entrada
- Hora de la última actualización

AWS Fargate la versión de la plataforma no es la más reciente

Descripción

Comprueba si Amazon ECS ejecuta la última versión de la plataforma de AWS Fargate. La versión de la plataforma de Fargate hace referencia a un entorno en tiempo de ejecución específico para la infraestructura de tareas de Fargate. Se trata de una combinación de la versión del kernel y la versión del tiempo de ejecución del contenedor. Se publican nuevas versiones de la plataforma a medida que evoluciona el entorno de tiempo de ejecución. Por ejemplo, si hay actualizaciones del kernel o del sistema operativo, características nuevas, correcciones de errores o actualizaciones de seguridad.

Para obtener más información, consulte Mantenimiento de las tareas de Fargate.

> **Note**
>
> Los resultados de esta verificación se actualizan automáticamente varias veces al día y no se permiten las solicitudes de actualización. Puede que los cambios tarden unas horas en aparecer. Actualmente, no puede excluir recursos de esta verificación.

ID de la verificación

`c18d2gz174`

Origen

```
AWS Config Managed Rule: ecs-fargate-latest-platform-version
```

Criterios de alerta

Amarillo: Amazon ECS no se ejecuta en la versión de la plataforma Fargate más reciente.

Acción recomendada

Actualice a la versión de la plataforma Fargate más reciente.

Para obtener más información, consulte Mantenimiento de las tareas de Fargate.

Columnas de informes

- Status
- Región
- Recurso
- AWS Config Regla
- Parámetros de entrada
- Hora de la última actualización

AWS Systems Manager La Asociación de Directores Estatales no cumple con las normas

Descripción

Comprueba si el estado de conformidad de la AWS Systems Manager asociación es CONFORME o NO tras la ejecución de la asociación en la instancia.

State Manager, una capacidad de AWS Systems Manager, es un servicio de administración de la configuración seguro y escalable que automatiza el proceso de mantener los nodos administrados y otros AWS recursos en el estado que usted defina. Una asociación de administradores de estado es una configuración que se asigna a AWS los recursos. La configuración define el estado que desea mantener para sus recursos, por lo que sirve de ayuda para alcanzar el objetivo, como evitar las desviaciones de configuración en sus instancias de Amazon EC2.

Para obtener más información, consulte Systems Manager de AWS Systems Manager.

> **Note**
>
> Los resultados de esta verificación se actualizan automáticamente varias veces al día y no se permiten las solicitudes de actualización. Puede que los cambios tarden unas horas en aparecer. Actualmente, no puede excluir recursos de esta verificación.

ID de la verificación

`c18d2gz147`

Origen

`AWS Config Managed Rule: ec2-managedinstance-association-compliance-status-check`

Criterios de alerta

Amarillo: el estado de conformidad de la AWS Systems Manager asociación es NO CUMPLE CON LAS NORMAS.

Acción recomendada

Valide el estado de las asociaciones de State Manager y, a continuación, tome las medidas necesarias para que el estado vuelva a ser COMPLIANT.

Para obtener más información, consulte Acerca de Systems Manager.

Recursos adicionales

AWS Systems Manager State Manager

Columnas de informes

- Status
- Región
- Recurso
- AWS Config Regla
- Parámetros de entrada
- Hora de la última actualización

CloudTrail las rutas no están configuradas con Amazon CloudWatch Logs

Descripción

Comprueba si los AWS CloudTrail senderos están configurados para enviar CloudWatch registros a Logs.

Supervise los archivos de CloudTrail registro con CloudWatch registros para activar una respuesta automática cuando se recopilen eventos críticos AWS CloudTrail.

Para obtener más información, consulte Supervisión de archivos de CloudTrail registro con CloudWatch registros.

> **Note**
>
> Los resultados de esta verificación se actualizan automáticamente varias veces al día y no se permiten las solicitudes de actualización. Puede que los cambios tarden unas horas en aparecer. Actualmente, no puede excluir recursos de esta verificación.

ID de la verificación

`c18d2gz164`

Origen

`AWS Config Managed Rule: cloud-trail-cloud-watch-logs-enabled`

Criterios de alerta

Amarillo: no AWS CloudTrail está configurado con la integración CloudWatch de registros.

Acción recomendada

Configure CloudTrail las rutas para enviar los eventos de registro a CloudWatch los registros.

Para obtener más información, consulte Creación de CloudWatch alarmas para CloudTrail eventos: ejemplos.

Columnas de informes

- Status
- Región

- Recurso
- AWS Config Regla
- Parámetros de entrada
- Hora de la última actualización

La protección contra eliminación de Elastic Load Balancing no está habilitada para los equilibradores de carga

Descripción

Comprueba si la protección contra eliminación está activada para los equilibradores de carga.

Elastic Load Balancing admite la protección contra eliminación de los equilibradores de carga de aplicaciones, los equilibradores de carga de red y los equilibradores de carga de la puerta de enlace. Para evitar que el equilibrador de carga se elimine por error, habilite la protección contra eliminación. La protección contra eliminación se desactiva de forma predeterminada cuando crea un equilibrador de carga. Si sus equilibradores de carga forman parte de un entorno de producción, considere activar la protección contra eliminación.

El registro de acceso es una característica opcional de Elastic Load Balancing que está desactivada de forma predeterminada. Una vez que se ha habilitado el registro de acceso del equilibrador de carga, Elastic Load Balancing captura los registros y los almacena en el bucket de Amazon S3 que haya especificado.

Para obtener más información, consulte Protección contra eliminación de equilibradores de carga de aplicación, Protección contra eliminación de equilibradores de carga de red o Protección contra eliminación de equilibradores de carga de la puerta de enlace.

> **Note**
>
> Los resultados de esta verificación se actualizan automáticamente varias veces al día y no se permiten las solicitudes de actualización. Puede que los cambios tarden unas horas en aparecer. Actualmente, no puede excluir recursos de esta verificación.

ID de la verificación

`c18d2gz168`

Origen

```
AWS Config Managed Rule: elb-deletion-protection-enabled
```

Criterios de alerta

Amarillo: la protección contra eliminación no está habilitada para un equilibrador de carga.

Acción recomendada

Active los equilibradores de carga de aplicaciones, los equilibradores de carga de red y los equilibradores de carga de la puerta de enlace.

Para obtener más información, consulte Protección contra eliminación de equilibradores de carga de aplicación, Protección contra eliminación de equilibradores de carga de red o Protección contra eliminación de equilibradores de carga de la puerta de enlace.

Columnas de informes

- Status
- Región
- Recurso
- AWS Config Regla
- Parámetros de entrada
- Hora de la última actualización

Comprobación de la protección contra eliminación de clústeres de bases de datos de RDS

Descripción

Comprueba si los clústeres de base de datos de Amazon RDS tienen habilitada la protección contra eliminación.

Cuando se configura la protección contra eliminación para un clúster, ningún usuario podrá eliminar la base de datos.

La protección contra la eliminación está disponible para Amazon Aurora y RDS para MySQL, RDS para MariaDB, RDS para Oracle, RDS para PostgreSQL y RDS para las instancias de bases de datos de SQL Server en todas las regiones. AWS

Para obtener más información, consulte Protección contra eliminación para clústeres de Aurora.

ID de la verificación

`c18d2gz160`

Origen

`AWS Config Managed Rule: rds-cluster-deletion-protection-enabled`

Criterios de alerta

Amarillo: tiene clústeres de base de datos de Amazon RDS que no tienen habilitada la protección contra eliminación.

Acción recomendada

Active la protección contra eliminación creando un clúster de base de datos de Amazon RDS.

Solo puede eliminar clústeres que no tengan habilitada la protección contra eliminación. Cuando habilita la protección contra eliminación, se agrega una capa de protección adicional y se evita la pérdida de datos por la eliminación accidental o no accidental de una instancia de base de datos. La protección contra eliminación también ayuda a cumplir los requisitos de conformidad normativa y a garantizar la continuidad empresarial.

Para obtener más información, consulte Protección contra eliminación para clústeres de Aurora.

> **Note**
>
> Los resultados de esta verificación se actualizan automáticamente varias veces al día y no se permiten las solicitudes de actualización. Puede que los cambios tarden unas horas en aparecer. Actualmente, no puede excluir recursos de esta verificación.

Recursos adicionales

Protección contra eliminación para clústeres de Aurora

Columnas de informes

- Status
- Región
- Recurso

- AWS Config Regla
- Parámetros de entrada
- Hora de la última actualización

Comprobación automática de la actualización de la versión secundaria de la instancia de base de datos de RDS

Descripción

Comprueba si las instancias de base de datos de Amazon RDS tienen configuradas las actualizaciones automáticas para las versiones secundarias.

Active las actualizaciones automáticas de las versiones secundarias de una instancia de Amazon RDS para asegurarse de que la base de datos ejecute siempre la versión segura y estable más reciente. Las actualizaciones secundarias proporcionan actualizaciones de seguridad, correcciones de errores y mejoras de rendimiento y mantienen la compatibilidad con las aplicaciones existentes.

Para obtener más información, consulte Cómo actualizar la versión del motor de la instancia de base de datos.

> **Note**
>
> Los resultados de esta verificación se actualizan automáticamente varias veces al día y no se permiten las solicitudes de actualización. Puede que los cambios tarden unas horas en aparecer. Actualmente, no puede excluir recursos de esta verificación.

ID de la verificación

`c18d2gz155`

Origen

`AWS Config Managed Rule: rds-automatic-minor-version-upgrade-enabled`

Criterios de alerta

Amarillo: la instancia de base de datos de RDS no tiene activadas las actualizaciones automáticas de las versiones secundarias.

Acción recomendada

Active las actualizaciones automáticas de las versiones secundarias creando una instancia de base de datos de Amazon RDS.

Cuando activa la actualización de la versión secundaria, la versión de la base de datos se actualiza automáticamente si ejecuta una versión secundaria del motor de bases de datos menor que la versión de actualización manual del motor.

Columnas de informes

- Status
- Región
- Recurso
- AWS Config Regla
- Parámetros de entrada
- Hora de la última actualización

Registro de cambios para AWS Trusted Advisor

Consulte el siguiente tema para ver los cambios recientes en las Trusted Advisor comprobaciones.

> **Note**
>
> Si utilizas la Trusted Advisor consola o la AWS Support API, las comprobaciones que se hayan eliminado no aparecerán en los resultados de las comprobaciones. Si utilizas alguna de las comprobaciones eliminadas, como especificar el ID de la comprobación en una operación de la AWS Support API o en tu código, debes eliminar estas comprobaciones para evitar errores en las llamadas a la API.

Para obtener más información sobre las verificaciones disponibles, consulte AWS Trusted Advisor comprobar referencia.

Se han eliminado 5 comprobaciones y se ha añadido 1 comprobación

Trusted Advisor El 15 de mayo de 2024 se eliminaron 3 comprobaciones de tolerancia a fallos, 1 comprobación de rendimiento y 1 comprobación de seguridad:

- Uso de IAM
- Equilibrio de carga entre zonas ELB
- Volúmenes magnéticos de Amazon EBS sobreutilizados
- Elevado número de reglas de grupo de seguridad de EC2 aplicadas a una instancia
- Elevado número de reglas en un grupo de seguridad de EC2

Trusted Advisor se agregó 1 nuevo control de seguridad el 15 de mayo de 2024:

- Registros de acceso al servidor Amazon S3 habilitados

Para obtener más información, consulte AWS Trusted Advisor comprobar referencia.

Se eliminaron los controles de tolerancia a errores

Trusted Advisor La comprobación de tolerancia a tres errores quedó obsoleta el 25 de abril de 2024:

- AWS Direct Connect Redundancia de conexión
- AWS Direct Connect Redundancia de ubicación
- AWS Direct Connect Redundancia de interfaz virtual

Para obtener más información, consulte AWS Trusted Advisor comprobar referencia.

Nueva comprobación de tolerancia a errores

Trusted Advisor se agregó 1 verificación de tolerancia a errores el 29 de febrero de 2024:

- NLB: recurso con acceso a Internet en una subred privada

Para obtener más información, consulte AWS Trusted Advisor comprobar referencia.

Se actualizaron las comprobaciones de seguridad y tolerancia a errores

Trusted Advisor El 28 de marzo de 2024 se añadió 1 nueva comprobación de tolerancia a fallos y se modificaron 1 comprobación de tolerancia a fallos y 1 comprobación de seguridad existentes:

- Se agregó AWS Resilience Hub la verificación de componentes de la aplicación
- Funciones actualizadas AWS Lambda habilitadas para VPC sin redundancia Multi-AZ

- Funciones actualizadas AWS Lambda que utilizan tiempos de ejecución obsoletos

Para obtener más información, consulte AWS Trusted Advisor comprobar referencia.

Nueva comprobación de tolerancia a errores

Trusted Advisor se agregó 1 verificación de tolerancia a fallas el 31 de enero de 2024:

- AWS Direct Connect Resiliencia de ubicación

Para obtener más información, consulte AWS Trusted Advisor comprobar referencia.

Verificación de tolerancia a fallas actualizada

Trusted Advisor Se modificó 1 comprobación de tolerancia a fallos el 8 de enero de 2024:

- El parámetro innodb_flush_log_at_trx_commit de Amazon RDS no es 1

Para obtener más información, consulte AWS Trusted Advisor comprobar referencia.

Comprobación de seguridad actualizada

Trusted Advisor modificó 1 control de seguridad el 21 de diciembre de 2023:

- AWS Lambda Funciones que utilizan tiempos de ejecución obsoletos

Para obtener más información, consulte AWS Trusted Advisor comprobar referencia.

Nuevas comprobaciones de seguridad y rendimiento

Trusted Advisor se agregaron 2 nuevos controles de seguridad y 2 nuevos controles de rendimiento el 20 de diciembre de 2023:

- Los clientes de Amazon EFS no utilizan data-in-transit cifrado
- Clúster de base de datos Amazon Aurora con aprovisionamiento insuficiente para la carga de trabajo de lectura
- Instancia de Amazon RDS con aprovisionamiento insuficiente para la capacidad del sistema
- Fin del soporte estándar para las instancias Amazon EC2 con Ubuntu LTS

Para obtener más información, consulte AWS Trusted Advisor comprobar referencia.

Nueva comprobación de seguridad

Trusted Advisor se agregó 1 nuevo control de seguridad el 15 de diciembre de 2023:

- Registros CNAME no coincidentes de Amazon Route 53 que apuntan directamente a los buckets S3

Para obtener más información, consulte AWS Trusted Advisor comprobar referencia.

Nuevas comprobaciones de tolerancia a errores y optimización de costes

Trusted Advisor El 7 de diciembre de 2023 se agregaron 2 nuevas comprobaciones de tolerancia a fallos y 1 nueva comprobación de optimización de costes:

- Clústeres Single-AZ de Amazon DocumentDB
- Configuración incompleta de cancelación de carga multiparte de Amazon S3
- Amazon ECS AWS registra el controlador en modo de bloqueo

Para obtener más información, consulte AWS Trusted Advisor comprobar referencia.

Nuevas comprobaciones de tolerancia a errores

Trusted Advisor el 17 de noviembre de 2023 se agregaron 3 nuevas comprobaciones de tolerancia a errores:

- ALB Multi-AZ
- NLB Multi-AZ
- Interfaz de VPC: interfaces de red de punto final en varias zonas de disponibilidad

Para obtener más información, consulte AWS Trusted Advisor comprobar referencia.

Nuevas comprobaciones para Amazon RDS

Trusted Advisor añadió 37 cheques nuevos para Amazon RDS el 15 de noviembre de 2023.

Para obtener más información, consulte AWS Trusted Advisor comprobar referencia.

¿Nueva API AWS Trusted Advisor

AWS Trusted Advisor presenta nuevas API que le permiten acceder mediante programación a las comprobaciones de mejores prácticas, recomendaciones y recomendaciones priorizadas de Trusted Advisor. Trusted Advisor Las API le permiten integrarse mediante programación Trusted Advisor con su herramienta operativa preferida para automatizar y optimizar sus cargas de trabajo a escala. Disponibles para los clientes de Business, Enterprise On-Ramp o Enterprise Support, las nuevas API proporcionan acceso a Trusted Advisor las recomendaciones para su cuenta o para todas las cuentas vinculadas dentro de una cuenta de pago. Los clientes de Enterprise Support con acceso a cuentas de administración o de administrador delegado también pueden recuperar mediante programación las recomendaciones priorizadas en toda su organización.

Las nuevas Trusted Advisor API sustituirán a las 3 funcionalidades que anteriormente se ofrecían a través de AWS Support API (SAPI). SAPI seguirá ofreciendo información sobre casos y otro tipo de soporte.

Trusted Advisor Por lo general, las API están disponibles en las regiones EE.UU. Este (Ohio), EE.UU. Este (Norte de Virginia), EE.UU. Oeste (Oregón), Asia Pacífico (Seúl), Asia Pacífico (Sídney) y Europa (Irlanda).

Para obtener más información, visite la página AWS Trusted Advisor de API.

Trusted Advisor comprobar la eliminación

Trusted Advisor eliminó los siguientes cheques el 9 de noviembre de 2023.

Nombre de la verificación	Categoría de verificación	ID de la verificación
Los volúmenes de EBS deben adjuntarse a las instancias EC2	Seguridad	`Hs4Ma3G119`
Los buckets de S3 deben tener habilitado el cifrado del servidor	Seguridad	`Hs4Ma3G167`
CloudFront las distribuciones deben tener habilitada la identidad de acceso de origen	Seguridad	`Hs4Ma3G195`

Integración de los AWS Config cheques en Trusted Advisor

Trusted Advisor se agregaron 64 cheques nuevos activados AWS Config el 30 de octubre de 2023.

Para obtener más información, consulte Ver comprobaciones de AWS Trusted Advisor con tecnología de AWS Config.

Nuevas comprobaciones de tolerancia a errores

Trusted Advisor agregó los siguientes controles el 12 de octubre de 2023.

- Amazon RDS ReplicaLag
- Amazon RDS FreeStorageSpace
- Amazon RDS DiskQueueDepth
- Amazon Route 53 Resolver Redundancia de zonas de disponibilidad de puntos finales
- IP con escalado automático disponible en subredes
- Los agentes de Amazon MSK alojan demasiadas particiones

Para obtener más información, consulte la categoría Tolerancia a errores.

Nueva comprobación de límites de servicio

Trusted Advisor agregó la siguiente comprobación el 17 de agosto de 2023.

- Uso del almacenamiento de código de Lambda

Para obtener más información, consulte la categoría Límites de los servicios.

Nueva comprobación de tolerancia a errores

Trusted Advisor agregó el siguiente cheque el 3 de agosto de 2023.

- AWS Lambda Sobre los destinos de los eventos fallidos

Para obtener más información, consulte la categoría Tolerancia a errores.

Nuevas comprobaciones de tolerancia a errores y de rendimiento

Trusted Advisor agregó los siguientes controles el 1 de junio de 2023.

- Redundancia sin destinos de montaje de Amazon EFS
- Optimización del modo de rendimiento de Amazon EFS
- Redundancia de la zona de disponibilidad de ActiveMQ
- Redundancia de la zona de disponibilidad de RabbitMQ

Para obtener más información, consulte la categoría Tolerancia a errores y la Rendimiento.

Nuevas comprobaciones de tolerancia a errores

Trusted Advisor agregó los siguientes controles el 16 de mayo de 2023.

- Independencia de la zona de disponibilidad de la puerta de enlace de NAT
- Comprobación de aplicaciones con zona de disponibilidad única

Para obtener más información, consulte la categoría Tolerancia a errores.

Nuevas comprobaciones de tolerancia a errores

Trusted Advisor agregó los siguientes cheques el 27 de abril de 2023.

- Número de Regiones de AWS en un conjunto de réplicas de Incident Manager
- AWS Resilience Hub edad de evaluación

Para obtener más información, consulte la categoría Tolerancia a errores.

Expansión regional de las comprobaciones de tolerancia a errores de Amazon ECS

Trusted Advisor amplió los siguientes controles a otras regiones el 27 de abril de 2023. Trusted Advisor Los cheques de Amazon ECS ahora están disponibles en todas las regiones en las que Amazon ECS está disponible de forma general.

- Servicio de Amazon ECS con una única zona de disponibilidad

- Estrategia de ubicación multi-AZ de Amazon ECS

Las regiones a las que se expandió son las siguientes: África (Ciudad del Cabo), Asia-Pacífico (Hong Kong), Asia-Pacífico (Hyderabad), Asia-Pacífico (Yakarta), Asia-Pacífico (Melbourne), Europa (Milán), Europa (España), Europa (Zúrich), Medio Oriente (Baréin) y Medio Oriente (Emiratos Árabes Unidos).

Nuevas comprobaciones de tolerancia a errores

Trusted Advisor añadió los siguientes controles el 30 de marzo de 2023.

- Servicio de Amazon ECS con una única zona de disponibilidad
- Estrategia de ubicación multi-AZ de Amazon ECS

Para obtener más información, consulte la categoría Tolerancia a errores.

Nuevas comprobaciones de tolerancia a errores

Trusted Advisor agregó los siguientes cheques el 15 de diciembre de 2022.

- AWS CloudHSM clústeres que ejecutan instancias de HSM en una única zona de disponibilidad
- Clústeres ElastiCache Multi-AZ de Amazon
- Clústeres Multi-AZ Amazon MemoryDB

Para recibir los resultados de Trusted Advisor sus AWS CloudHSM clústeres y de MemoryDB, debe tener clústeres en sus zonas de disponibilidad. ElastiCache Para obtener más información, consulte la siguiente documentación sobre :

- AWS CloudHSM Guía del usuario
- Guía para desarrolladores de Amazon MemoryDB para Redis
- Guía del usuario ElastiCache de Amazon for Redis

Trusted Advisor actualizó la siguiente información de verificación el 15 de diciembre de 2022.

- AWS Resilience Hub política infringida: el nombre de la aplicación se actualizó por el nombre de la aplicación

- AWS Resilience Hub Puntuaciones de resiliencia: el nombre de la aplicación y la puntuación de resiliencia de la aplicación se actualizaron por el nombre de la aplicación y la puntuación de resiliencia de la aplicación

Para obtener más información, consulte la categoría Tolerancia a errores.

Actualizaciones de la Trusted Advisor integración con AWS Security Hub

Trusted Advisor realizó la siguiente actualización el 17 de noviembre de 2022.

Si inhabilitas Security Hub o AWS Config para una Región de AWS, Trusted Advisor ahora eliminas las comprobaciones de control correspondientes en un Región de AWS plazo de 7 a 9 días. Anteriormente, el plazo para eliminar los datos del Security Hub Trusted Advisor era de 90 días.

Para más información, consulte las siguientes secciones del tema Solución de problemas:

- He desactivado Security Hub o AWS Config en una región
- Mi control está archivado en Security Hub, pero sigo viendo los resultados en Trusted Advisor

Nuevas comprobaciones de tolerancia a errores en AWS Resilience Hub

Trusted Advisor agregó las siguientes comprobaciones el 17 de noviembre de 2022.

- AWS Resilience Hub política incumplida
- AWS Resilience Hub puntajes de resiliencia

Puede utilizar estas comprobaciones para ver el estado más reciente de la política y la puntuación de resiliencia de sus aplicaciones. Resilience Hub le proporciona un lugar central para definir, rastrear y gestionar la resiliencia y disponibilidad de las aplicaciones.

Para recibir los resultados de Trusted Advisor sus aplicaciones de Resilience Hub, debe implementar una AWS aplicación y usar Resilience Hub para realizar un seguimiento de la capacidad de recuperación de la aplicación. Para obtener más información, consulte la Guía del usuario de AWS Resilience Hub.

Para recibir resultados Trusted Advisor para sus clústeres ElastiCache y los de MemoryDB, debe tener clústeres en sus zonas de disponibilidad. Para obtener más información, consulte la siguiente documentación sobre :

- Guía para desarrolladores de Amazon MemoryDB para Redis
- Guía del usuario ElastiCache de Amazon for Redis

Para obtener más información, consulte la categoría Tolerancia a errores.

Actualización de la consola Trusted Advisor

Trusted Advisor agregó el siguiente cambio el 16 de noviembre de 2022.

El Trusted Advisor panel de control de la consola ahora es Trusted Advisor Recomendaciones. La página Recommendations de Trusted Advisor sigue mostrando los resultados de las comprobaciones y las comprobaciones disponibles para cada categoría de su Cuenta de AWS.

Este cambio de nombre solo actualiza la Trusted Advisor consola. Puede seguir utilizando la Trusted Advisor consola y Trusted Advisor las operaciones de la AWS Support API como de costumbre.

Para obtener más información, consulte Comience con Recommendations de Trusted Advisor.

Nuevas comprobaciones para Amazon EC2

Trusted Advisor agregó la siguiente verificación el 1 de septiembre de 2022.

- Instancias de Amazon EC2 con final de la compatibilidad con Microsoft Windows Server

Para obtener más información, consulte la categoría Seguridad.

Se agregaron comprobaciones de Security Hub a Trusted Advisor

A partir del 23 de junio de 2022, Trusted Advisor solo es compatible con los controles de Security Hub disponibles hasta el 7 de abril de 2022. Esta versión admite todos los controles del estándar de seguridad AWS Foundational Security Best Practices, excepto los controles de la categoría: Recuperación > Resiliencia. Para obtener más información, consulte Visualización de controles de AWS Security Hub en AWS Trusted Advisor.

Para obtener una lista de los controles admitidos, consulte Controles de las prácticas de seguridad básicas recomendadas de AWS en la Guía del usuario de AWS Security Hub .

Se agregaron cheques de AWS Compute Optimizer

Trusted Advisor agregó los siguientes cheques el 4 de mayo de 2022.

Nombre de la verificación	Categoría de verificación	ID de la verificación
Volúmenes con exceso de aprovisionamiento de Amazon EBS	Optimización de costes	`COr6dfpM03`
Volúmenes con falta de aprovisionamiento de Amazon EBS	Rendimiento	`COr6dfpM04`
AWS Lambda funciones sobreaprovisionadas para el tamaño de la memoria	Optimización de costes	`COr6dfpM05`
AWS Lambda funciones insuficientemente aprovisio nadas para el tamaño de la memoria	Rendimiento	`COr6dfpM06`

Debe optar por Compute Optimizer Cuenta de AWS para que estas comprobaciones puedan recibir datos de sus recursos de Lambda y Amazon EBS. Para obtener más información, consulte Optar AWS Compute Optimizer por recibir Trusted Advisor cheques.

Actualizaciones de la comprobación de las claves de acceso expuestas

Trusted Advisor actualizó la siguiente verificación el 25 de abril de 2022.

Nombre de la verificación	Categoría de verificación	ID de la verificación
Exposed Access Keys	Seguridad	`12Fnkpl8Y5`

Trusted Advisor ahora actualiza esta comprobación automáticamente. Esta comprobación no se puede actualizar manualmente desde la Trusted Advisor consola o la AWS Support API. Si la aplicación o el código actualizan esta comprobación por ti Cuenta de AWS, te recomendamos que la actualices para que no vuelva a actualizarla. De lo contrario, se producirá el error `InvalidParameterValue`.

Las claves de acceso que se hayan excluido antes de esta actualización dejarán de excluirse y aparecerán como recursos afectados. No se pueden excluir las claves de acceso de los resultados de las comprobaciones. Para obtener más información, consulte Exposed Access Keys.

> **Note**
>
> Si creó la suya Cuenta de AWS después del 25 de abril de 2022, los resultados de la comprobación de las claves de acceso expuestas muestran inicialmente el icono gris (), incluso en el caso de las claves de acceso no expuestas. Esto significa que Trusted Advisor no ha identificado ningún cambio durante la comprobación.
> Si Trusted Advisor identifica un recurso en riesgo, el estado cambia al icono de acción recomendada ().
> Después de corregir o eliminar el recurso, el resultado de la comprobación muestra el icono de marca de comprobación ().

Verificaciones actualizadas para AWS Direct Connect

Trusted Advisor actualizó las siguientes comprobaciones el 29 de marzo de 2022.

Nombre de la verificación	Categoría de verificación	ID de la verificación
AWS Direct Connect Redundancia de conexión	Tolerancia a errores	`0t121N1Ty3`
AWS Direct Connect Redundancia de ubicación	Tolerancia a errores	`8M012Ph3U5`
AWS Direct Connect Redundancia de interfaz virtual	Tolerancia a errores	`4g3Nt5M1Th`

- El valor de la columna Region (Región) ahora muestra el Región de AWS código en lugar del nombre completo. Por ejemplo, los recursos del Este de EE. UU. (Norte de Virginia) tendrán ahora el valor `us-east-1`.
- El valor de la columna Time Stamp (Marca temporal) ahora aparece en la formato RFC 3339, como `2022-03-30T01:02:27.000Z`.
- Los recursos que no tienen ningún problema detectado ahora aparecerán en la tabla de verificaciones. Estos recursos tendrán un icono de marca de verificación ( ) junto a ellos.

  Anteriormente, en la tabla solo aparecían los recursos que Trusted Advisor se recomendaba investigar. Estos recursos tienen un icono de advertencia ( ) junto a ellos.

AWS Security Hub controles agregados a la AWS Trusted Advisor consola

AWS Trusted Advisor añadió 111 controles de Security Hub a la categoría Seguridad el 18 de enero de 2022.

Puede ver sus hallazgos sobre los controles de Security Hub en el estándar de seguridad AWS Foundational Security Best Practices. Esta integración no incluye controles con Category: Recover > Resilience (Categoría: Recuperar > Resiliencia).

Para obtener más información acerca de esta característica, consulte Visualización de controles de AWS Security Hub en AWS Trusted Advisor.

Nuevas verificaciones para Amazon EC2 y AWS Well-Architected

Trusted Advisor agregó las siguientes comprobaciones el 20 de diciembre de 2021.

- Consolidación de las instancias de Amazon EC2 para Microsoft SQL Server
- Instancias de Amazon EC2 con exceso de aprovisionamiento para Microsoft SQL Server
- Instancias de Amazon EC2 con fin del soporte para Microsoft SQL Server
- Problemas de alto riesgo de AWS Well-Architected para la optimización de costos
- Problemas de alto riesgo de AWS Well-Architected para el rendimiento

- Problemas de alto riesgo de AWS Well-Architected para la seguridad
- Problemas de alto riesgo de AWS Well-Architected para la fiabilidad

Para obtener más información, consulte Referencia de verificaciones de AWS Trusted Advisor.

Nombre de cheque actualizado para Amazon OpenSearch Service

Trusted Advisor actualizé el nombre del Amazon OpenSearch Service Reserved Instance Optimization cheque el 8 de septiembre de 2021.

Las verificaciones, la categoría y el ID de la verificación no se han cambiado.

Nombre de la verificación	Categoría de verificación	ID de la verificación
Optimización de instancias reservadas de Amazon OpenSearch Service	Optimización de costes	`7ujm6yhn5t`

> **Note**
>
> Si lo utilizas Trusted Advisor para CloudWatch las métricas de Amazon, el nombre de la métrica de esta comprobación también se actualiza. Para obtener más información, consulte Creación de alarmas de Amazon CloudWatch para supervisar las métricas de AWS Trusted Advisor.

Se han agregado verificaciones de almacenamiento de volúmenes de Amazon Elastic Block Store

Trusted Advisor añadí las siguientes comprobaciones el 8 de junio de 2021.

Nombre de la verificación	Categoría de verificación	ID de la verificación
Almacenamiento de volúmenes de SSD de uso general (gp3) de EBS	Límites de los servicios	`dH7RR0l6J3`

Nombre de la verificación	Categoría de verificación	ID de la verificación
Almacenamiento de volúmenes de SSD de IOPS provisionadas (io2) de EBS	Límites de los servicios	gI7MM0l7J2

Se agregaron cheques para AWS Lambda

Trusted Advisor agregó los siguientes cheques el 8 de marzo de 2021.

Nombre de la verificación	Categoría de verificación	ID de la verificación
AWS Lambda Funciones con tiempos de espera excesivos	Optimización de costes	L4dfs2Q3C3
AWS Lambda Funciones con altas tasas de error	Optimización de costes	L4dfs2Q3C2
AWS Lambda Funciones que utilizan tiempos de ejecución obsoletos	Seguridad	L4dfs2Q4C5
AWS Lambda Funciones habilitadas para VPC sin redundancia Multi-AZ	Tolerancia a errores	L4dfs2Q4C6

Para obtener más información sobre cómo utilizar estas comprobaciones con Lambda, consulte un ejemplo de AWS Trusted Advisor flujo de trabajo para ver las recomendaciones en la Guía para AWS Lambda desarrolladores.

Trusted Advisor comprobar la eliminación

Trusted Advisor se retiró el siguiente cheque AWS GovCloud (US) Region el 8 de marzo de 2021.

Nombre de la verificación	Categoría de verificación	ID de la verificación
Direcciones IP elásticas de EC2	Límites de los servicios	aW9HH0l8J6

Se han actualizado verificaciones de Amazon Elastic Block Store

Trusted Advisor actualizó la unidad de volumen de Amazon EBS de gibibyte (GiB) a tebibyte (TiB) para las siguientes comprobaciones el 5 de marzo de 2021.

> **Note**
>
> Si lo utilizas Trusted Advisor para CloudWatch las métricas de Amazon, también se actualizan los nombres de las métricas de estas cinco comprobaciones. Para obtener más información, consulte Creación de alarmas de Amazon CloudWatch para supervisar las métricas de AWS Trusted Advisor.

Nombre de la verificación	Categoría de verificación	ID de la verificación	CloudWatch Métrica actualizada para ServiceLimit
Almacenamiento de volúmenes de HDD en frío (sc1) de EBS	Límites de los servicios	gH5CC0e3J9	Almacenamiento de volúmenes de HDD en frío (sc1) (TiB)
Almacenamiento de volúmenes de SSD de uso general (gp2) de EBS	Límites de los servicios	dH7RR0l6J9	Almacenamiento de volúmenes de SSD de uso general (gp2) (TiB)
Almacenamiento de volúmenes magnéticos (estándar) de EBS	Límites de los servicios	cG7HH0l7J9	Almacenamiento de volúmenes magnéticos (estándar) (TiB)

Nombre de la verificación	Categoría de verificación	ID de la verificación	CloudWatch Métrica actualizada para ServiceLimit
Almacenamiento de volúmenes de SSD de IOPS provisionadas (io1) de EBS	Límites de los servicios	`gI7MM0l7J9`	Almacenamiento IOPS provisionadas (SSD) (TiB)
Almacenamiento de volúmenes de HDD con rendimiento optimizado (st1) de EBS	Límites de los servicios	`wH7DD0l3J9`	Almacenamiento de volúmenes de HDD con rendimiento optimizado (st1) (TiB)

Trusted Advisor eliminación de cheques

> **Note**
>
> Trusted Advisor eliminó los siguientes cheques el 18 de noviembre de 2020.

Verificaciones eliminadas el 18 de noviembre de 2020	Categoría de verificación	ID de la verificación
Servicio EC2config para instancias de Windows de EC2	Tolerancia a errores	`V77iOLlBqz`
Versión del controlador de ENA para instancias de Windows de EC2	Tolerancia a errores	`TyfdMXG69d`
Versión del controlador de NVMe para instancias de Windows de EC2	Tolerancia a errores	`yHAGQJV9K5`

Verificaciones eliminadas el 18 de noviembre de 2020	Categoría de verificación	ID de la verificación
Versión del controlador de PV para instancias de Windows de EC2	Tolerancia a errores	`Wnwm9Il5bG`
Volúmenes activos de EBS	Límites de los servicios	`fH7LL0l7J9`

Amazon Elastic Block Store ya no tiene límite de número de volúmenes que se pueden aprovisionar.

Puede monitorear sus instancias de Amazon EC2 y verificar que estén actualizadas mediante el Distribuidor Systems Manager de AWS, otras herramientas de terceros, o bien puede escribir sus propios scripts para devolver la información del controlador para Windows Management Instrumentation (WMI).

Trusted Advisor eliminación de cheques

Trusted Advisor eliminó el siguiente cheque el 18 de febrero de 2020.

Nombre de la verificación	Categoría de verificación	ID de la verificación
Límites de los servicios	Rendimiento	`eW7HH0l7J9`

AWS Support Aplicación en Slack

Puedes usar la AWS Support aplicación para gestionar tus casos de AWS asistencia en Slack. Invita a los miembros de tu equipo a los canales de chat, responde a las actualizaciones de casos y conversa directamente con los agentes de asistencia. Usa la AWS Support aplicación para gestionar rápidamente los casos de asistencia en Slack.

Usa la AWS Support aplicación para hacer lo siguiente:

- Crear, actualizar, buscar y resolver casos de soporte en los canales de Slack
- Adjuntar archivos en casos de soporte
- Solicitar aumentos de cuota desde Service Quotas
- Compartir los detalles del caso de soporte con su equipo sin abandonar el canal de Slack
- Iniciar una sesión de chat en vivo con agentes de soporte

Al crear, actualizar o resolver un caso de soporte en la AWS Support aplicación, el caso también se actualiza en AWS Support Center Console. No es necesario iniciar sesión en la consola del centro de soporte para administrar sus casos de soporte por separado.

> **Notas**
>
> - Los tiempos de respuesta para los casos de soporte son los mismos, independientemente de que haya creado el caso desde Slack o desde la consola del centro de soporte.
> - Puede crear un caso para el soporte de cuentas y facturación, los aumentos de la cuota de servicio y el soporte técnico.

Temas

- Únase a una sesión de chat en vivo con AWS Support
- Búsqueda de casos de soporte en Slack
- Resolución de un caso de soporte en Slack
- Reapertura de un caso de soporte en Slack
- Solicitud de aumentos en la cuota de servicio
- Eliminación de la configuración de un canal de Slack de la aplicación AWS Support
- Eliminación de una configuración de espacio de trabajo de Slack de la aplicación AWS Support
- Comandos de la aplicación AWS Support en Slack
- Ver correspondencias de la aplicación AWS Support en la AWS Support Center Console
- Creación de recursos de la aplicación AWS Support en Slack con AWS CloudFormation

Requisitos previos

Debe cumplir con los siguientes requisitos para usar la aplicación AWS Support en Slack:

- Usted cuenta con un plan Business, Enterprise On-Ramp o Enterprise. Puede encontrar su plan de soporte en la AWS Support Center Console o en la página Support plans (Planes de soporte). Para obtener más información, consulte Comparar planes de AWS Support.
- Tiene un espacio de trabajo y un canal de Slack para su organización. Debe ser administrador del espacio de trabajo de Slack o tener permiso para agregar aplicaciones a ese espacio de trabajo. Para obtener más información, consulte el Centro de ayuda de Slack.
- Inicie sesión en la Cuenta de AWS como un rol o usuario de AWS Identity and Access Management (IAM) con los permisos necesarios. Para obtener más información, consulte Administración del acceso al widget de la aplicación AWS Support.
- Deberá crear un rol de IAM que tenga los permisos necesarios para llevar a cabo acciones en su nombre. La aplicación AWS Support usa este rol para hacer llamadas de API a diferentes servicios. Para obtener más información, consulte Administración del acceso a la aplicación AWS Support.

Temas

- Administración del acceso al widget de la aplicación AWS Support
- Administración del acceso a la aplicación AWS Support

Administración del acceso al widget de la aplicación AWS Support

Puede adjuntar una política de AWS Identity and Access Management (IAM) para conceder a un usuario de IAM permiso para configurar el widget de la aplicación AWS Support en la AWS Support Center Console.

Para obtener más información sobre cómo adjuntar una política a una entidad de IAM, consulte Adding IAM identity permissions (console) (Adición de permisos de identidad de IAM [consola]) en la Guía del usuario de IAM.

> **Note**
>
> También puede iniciar sesión como usuario raíz en su Cuenta de AWS, pero no es recomendable hacerlo. Para obtener más información acerca del acceso de usuario raíz, consulte Proteger las credenciales de usuario raíz y no utilizarlas para las tareas cotidianas en la Guía del usuario de IAM.

Política de IAM de ejemplo

Puede adjuntar la siguiente política a una entidad, como un grupo o un usuario de IAM. Esta política permite al usuario autorizar un espacio de trabajo de Slack y configurar los canales de Slack en la consola del centro de soporte.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "supportapp:GetSlackOauthParameters",
                "supportapp:RedeemSlackOauthCode",
                "supportapp:DescribeSlackChannels",
                "supportapp:ListSlackWorkspaceConfigurations",
                "supportapp:ListSlackChannelConfigurations",
                "supportapp:CreateSlackChannelConfiguration",
                "supportapp:DeleteSlackChannelConfiguration",
                "supportapp:DeleteSlackWorkspaceConfiguration",
                "supportapp:GetAccountAlias",
                "supportapp:PutAccountAlias",
```

```
                "supportapp:DeleteAccountAlias",
                "supportapp:UpdateSlackChannelConfiguration",
                "iam:ListRoles"
            ],
            "Resource": "*"
        }
    ]
}
```

Permisos necesarios para conectar la aplicación AWS Support () a Slack

La aplicación AWS Support () incluye acciones de solo permiso que no se corresponden directamente con una operación de API. Estas acciones se indican en la Referencia de autorización de servicio con [solo permiso].

La aplicación AWS Support utiliza las siguientes acciones de API para conectarse a Slack y, a continuación, muestra sus canales públicos de Slack en AWS Support Center Console:

- `supportapp:GetSlackOauthParameters`
- `supportapp:RedeemSlackOauthCode`
- `supportapp:DescribeSlackChannels`

Estas acciones API no se han diseñado para que se llamen desde el código. Por lo tanto, estas acciones de API no se incluyen en la AWS CLI ni en los SDK de AWS.

Administración del acceso a la aplicación AWS Support

Una vez que tenga los permisos para el widget de la aplicación AWS Support, también deberá crear un rol de AWS Identity and Access Management (IAM). Este rol lleva a cabo acciones de otros Servicios de AWS, como la API de AWS Support y Service Quotas.

A continuación, adjunte una política de IAM a este rol para que tenga los permisos necesarios para completar estas acciones. Elija este rol cuando cree la configuración de su canal de Slack en la consola del centro de soporte.

Los usuarios de su canal de Slack tienen los mismos permisos que se conceden al rol de IAM. Por ejemplo, si especifica el acceso de solo lectura a sus casos de soporte, los usuarios de su canal de Slack podrán ver sus casos de soporte, pero no podrán actualizarlos.

> **Important**
>
> Cuando solicita un chat en vivo con un agente de soporte y elige un canal privado nuevo como su canal de chat en vivo de preferencia, la aplicación AWS Support crea un canal de Slack independiente. Este canal tiene los mismos permisos que el canal en el que creó el caso o inició el chat.
> Si cambia el rol o la política de IAM, los cambios se aplicarán al canal de Slack que configuró y a todos los nuevos canales de Slack de chat en vivo que crea la aplicación AWS Support.

Siga estos procedimientos para crear su política y rol de IAM.

Temas

- Utilice una política administrada de AWS o cree una política administrada por el cliente
- Crear un rol de IAM
- Solución de problemas

Utilice una política administrada de AWS o cree una política administrada por el cliente

Para conceder permisos a su rol, puede utilizar una política administrada de AWS o una política administrada por el cliente.

> **Tip**
>
> Si no quiere crear una política de forma manual, puede usar una política administrada de AWS en su lugar y omitir este procedimiento. Las políticas administradas tienen automáticamente los permisos necesarios para la aplicación AWS Support. No es necesario actualizar las políticas manualmente. Para obtener más información, consulte AWS políticas gestionadas para AWS Support la aplicación en Slack.

Siga este procedimiento para crear una política administrada por el cliente para su rol. Este procedimiento usa el editor de políticas JSON en la consola de IAM.

Para crear una política administrada por el cliente para la AWS Support

1. Inicie sesión en la AWS Management Console y abra la consola de IAM en https://console.aws.amazon.com/iam/.

2. En el panel de navegación, seleccione Policies (Políticas).
3. Elija Create Policy (Crear política).
4. Seleccione la pestaña JSON.
5. Ingrese su JSON y, a continuación, sustituya el JSON predeterminado en el editor. Puede usar la política de ejemplo.
6. Elija Next: Tags (Siguiente: etiquetas).
7. (Opcional) Puede usar etiquetas como pares clave-valor para agregar metadatos a la política.
8. Elija Next: Review (Siguiente: revisar).
9. En la página Review policy (Revisar política), ingrese un Name (Nombre), como *AWSSupportAppRolePolicy*, y una Description (Descripción) (opcional).
10. Revise la página Summary (Resumen) para ver los permisos que permite la política y, a continuación, elija Create policy (Crear política).

Esta política define las acciones que puede llevar a cabo el rol. Para obtener más información, consulte Creación de políticas de IAM (Consola) en la Guía del usuario de IAM.

Política de IAM de ejemplo

Puede asociar la siguiente política de ejemplo a su rol de IAM. Esta política permite que el rol tenga todos los permisos para todas las acciones necesarias para la aplicación AWS Support. Después de configurar un canal de Slack con el rol, todos los usuarios de su canal tendrán los mismos permisos.

> **Note**
>
> Para ver una lista de las políticas administradas de AWS, consulte AWS políticas gestionadas para AWS Support la aplicación en Slack.

Puede actualizar la política para eliminar un permiso de la aplicación AWS Support.

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

```
                "servicequotas:GetServiceQuota",
                "servicequotas:RequestServiceQuotaIncrease",
                "support:AddAttachmentsToSet",
                "support:AddCommunicationToCase",
                "support:CreateCase",
                "support:DescribeCases",
                "support:DescribeCommunications",
                "support:DescribeSeverityLevels",
                "support:InitiateChatForCase",
                "support:ResolveCase"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "*",
            "Condition": {
                "StringEquals": {"iam:AWSServiceName": "servicequotas.amazonaws.com"}
            }
        }
    ]
}
```

Para obtener descripciones de cada medida, consulte los siguientes temas en la referencia de autorizaciones de servicio:

- Acciones, recursos y claves de condiciones para AWS Support
- Acciones, recursos y claves de condición para Service Quotas
- Acciones, recursos y claves de condiciones para AWS Identity and Access Management

Crear un rol de IAM

Después de crear esta política, debe crear el rol de IAM y, a continuación, asociar la política a ese rol. Este rol se elige al crear una configuración de canal de Slack en la consola del centro de soporte.

Para crear un rol para la aplicación AWS Support

1. Inicie sesión en la AWS Management Console y abra la consola de IAM en https://console.aws.amazon.com/iam/.
2. En el panel de navegación, seleccione Roles y luego seleccione Create role.

3. En Select trusted entity (Seleccionar entidad de confianza), elija Servicio de AWS.
4. Elija Aplicación AWS Support
5. Elija Siguiente: Permisos.
6. Ingrese un nombre para la política. Puede elegir la política administrada de AWS o elegir una política administrada por el cliente que haya creado, como *AWSSupportAppRolePolicy*. A continuación, seleccione la casilla situada junto a la política.
7. Elija Next: Tags (Siguiente: etiquetas).
8. (Opcional) Puede usar etiquetas como valores clave-valor para agregar metadatos al rol.
9. Elija Next: Review (Siguiente: revisar).
10. En Role name (Nombre del rol), ingrese un nombre; por ejemplo, *AWSSupportAppRole*.
11. (Opcional) En Role description (Descripción del rol), ingrese una descripción para el rol.
12. Revise el rol y, a continuación, seleccione Create role. Ahora puede elegir este rol al configurar un canal de Slack en la consola del Centro de soporte. Consulte Configuración de un canal de Slack.

Para obtener más información, consulte Creación de un rol para un servicio de AWS en la Guía del usuario de IAM.

Solución de problemas

Consulte los siguientes temas para administrar el acceso a la aplicación AWS Support.

Contenido

Quiero restringir acciones específicas a usuarios específicos de mi canal de Slack

De forma predeterminada, los usuarios de su canal de Slack tienen los mismos permisos especificados en la política de IAM que asocia al rol de IAM que crea. Esto significa que cualquier persona del canal tiene acceso de lectura o escritura a sus casos de soporte, independientemente de si tiene o no una Cuenta de AWS o un usuario de IAM.

Recomendamos que siga las siguientes prácticas recomendadas:

- Configure canales privados de Slack con la aplicación AWS Support.
- Solo invite a su canal a los usuarios que necesiten acceder a sus casos de soporte.
- Use una política de IAM que tenga los permisos mínimos necesarios para la aplicación AWS Support. Consulte AWS políticas gestionadas para AWS Support la aplicación en Slack.

Cuando configuro un canal de Slack, no veo el rol de IAM que he creado

Si su rol de IAM no aparece en la lista IAM role for the AWS Support App (Rol de IAM para la aplicación), significa que el rol no tiene la aplicación AWS Support () como entidad de confianza o que se eliminó el rol. Puede actualizar el rol actual o crear otro. Consulte Crear un rol de IAM.

A mi rol de IAM le falta un permiso

El rol de IAM que cree para su canal de Slack necesita permisos para llevar a cabo las acciones que desea. Por ejemplo, si quiere que sus usuarios de Slack creen casos de soporte, el rol debe tener el mismo permiso `support:CreateCase`. La aplicación AWS Support asume este rol para llevar a cabo estas acciones en su nombre.

Si recibe un error acerca de la falta de un permiso de la aplicación AWS Support, compruebe que la política adjunta a su rol tenga los permisos necesarios.

Consulte la Política de IAM de ejemplo anterior.

Un error de Slack indica que mi rol de IAM no es válido

Compruebe que eligió el rol correcto para la configuración de su canal.

Para verificar su rol

1. Inicie sesión en AWS Support Center Console desde la página https://console.aws.amazon.com/support/app#/config.
2. Elija el canal que configuró con la aplicación AWS Support.
3. En la sección Permissions (Permisos), busque el nombre del rol de IAM que eligió.
    - Para cambiar el rol, elija Edit (Editar), otro rol y, a continuación, Save (Guardar).
    - Para actualizar el rol o la política asociada al rol, inicie sesión en la consola de IAM.

La aplicación AWS Support indica que me falta un rol de IAM para Service Quotas

Debe tener el rol `AWSServiceRoleForServiceQuotas` en su cuenta para solicitar aumentos de cuota desde Service Quotas. Si recibe un error acerca de un recurso que falta, complete uno de los pasos siguientes:

- Para solicitar un aumento de la cuota, use la consola de Service Quotas. Después de hacer una solicitud correcta, Service Quotas crea este rol automáticamente. A continuación, puede usar la aplicación AWS Support para solicitar aumentos de cuotas en Slack. Para obtener más información, consulte Requesting a quota increase (Solicitud de un aumento de cuota).
- Actualice la política de IAM que se adjunta al rol. Esto concede los permisos del rol a Service Quotas. La siguiente sección de la Política de IAM de ejemplo permite que la aplicación AWS Support cree el rol de Service Quotas.

```
{
    "Effect": "Allow",
    "Action": "iam:CreateServiceLinkedRole",
    "Resource": "*",
    "Condition": {
        "StringEquals": {"iam:AWSServiceName": "servicequotas.amazonaws.com"}
     }
}
```

Si elimina el rol de IAM que configura para su canal, debe crearlo manualmente o actualizar la política de IAM para permitir que la aplicación AWS Support cree uno.

Autorización de un espacio de trabajo de Slack

Una vez que autorice su espacio de trabajo y dé a la aplicación AWS Support el permiso para acceder a él, necesitará un rol de AWS Identity and Access Management (IAM) para su Cuenta de AWS. La aplicación AWS Support usa este rol para llamar a las operaciones de la API desde AWS Support y Service Quotas en su nombre. Por ejemplo, la aplicación AWS Support usa el rol para llamar a la operación `CreateCase` para crear un caso de soporte en Slack en su nombre.

Notas

- El canal de Slack hereda los permisos del rol de IAM. Esto significa que cualquier usuario del canal de Slack tiene los mismos permisos que se especifican en la política de IAM asociada al rol.

  Por ejemplo, si su política de IAM permite que el rol tenga permisos completos de lectura y escritura para los casos de soporte, cualquier persona de su canal de Slack podrá crear, actualizar y resolver los casos de soporte. Si su política de IAM concede al rol permisos de solo lectura, los usuarios de su canal de Slack solo tendrán permisos de lectura para los casos de soporte.
- Le recomendamos que agregue los espacios de trabajo y los canales de Slack que necesita para administrar sus operaciones de soporte. Le recomendamos que configure los canales privados y que solo invite a los usuarios requeridos.

Debe autorizar cada espacio de trabajo de Slack que quiera usar para su Cuenta de AWS. Si tiene varias Cuentas de AWS, debe iniciar sesión en cada una de ellas y repetir el siguiente procedimiento para autorizar el espacio de trabajo. Si su cuenta pertenece a una organización de AWS Organizations y quiere autorizar varias cuentas, vaya a Authorize multiple accounts (Autorización de varias cuentas).

Para autorizar el espacio de trabajo de Slack para su Cuenta de AWS

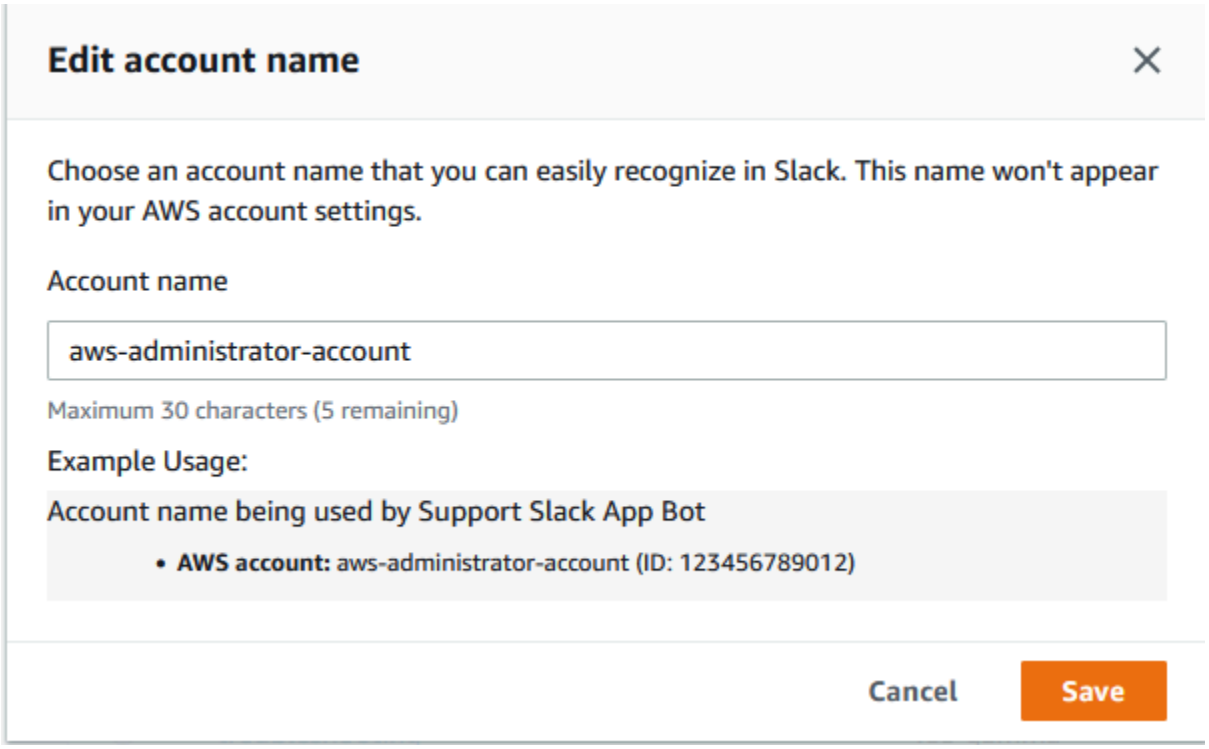
1. Inicie sesión en la AWS Support Center Console y elija Slack configuration (Configuración de Slack).
2. En la página Getting started (Introducción), elija Authorize workspace (Autorizar espacio de trabajo).
3. Si aún no inició sesión en Slack, en la página Sign in to your workspace (Iniciar sesión en su espacio de trabajo), ingrese el nombre del espacio de trabajo y, a continuación, elija Continue (Continuar).
4. En la página AWS Support is requesting permission to access the your-workspace-name (solicita permiso para acceder a [nombre del espacio de trabajo] de Slack), elija Allow (Permitir).

> **Note**
>
> Si no puede permitir que Slack acceda a su espacio de trabajo, asegúrese de que tenga permisos de su administrador de Slack para agregar la aplicación AWS Support al espacio de trabajo. Consulte Requisitos previos.

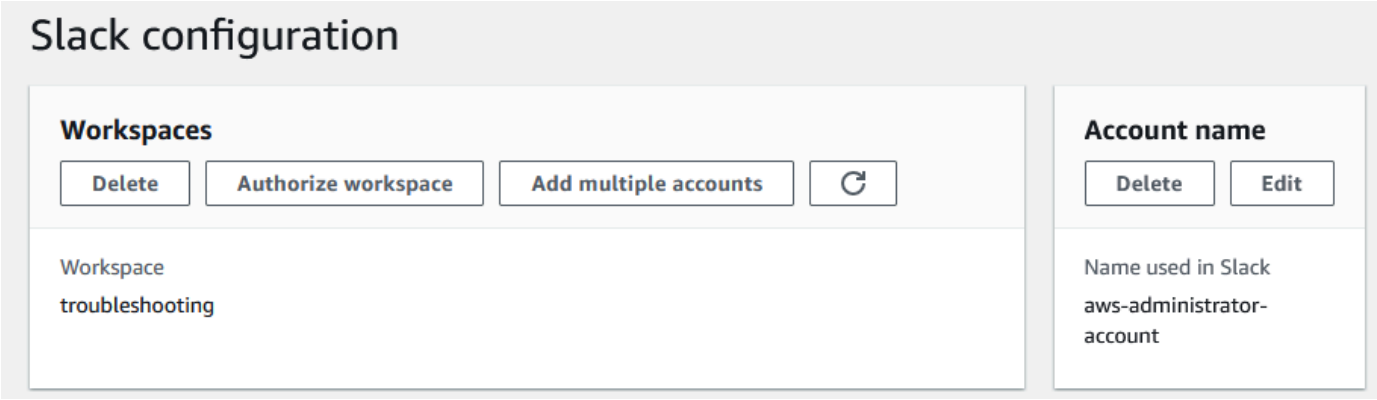
En la página Slack configuration (Configuración de Slack), el nombre de su espacio de trabajo aparece en Workspaces (Espacios de trabajo).

5. (Opcional) Para agregar más espacios de trabajo, elija Authorize workspace (Autorizar espacio de trabajo) y repita los pasos 3 y 4. Puede agregar hasta cinco espacios de trabajo a su cuenta.
6. (Opcional) De forma predeterminada, el número del ID de la Cuenta de AWS aparece como el nombre de la cuenta en su canal de Slack. Para cambiar este valor, en Account name (Nombre de la cuenta), elija Edit (Editar), ingrese el nombre de la cuenta y, a continuación, elija Save (Guardar).

> **Tip**
>
> Use un nombre que usted y su equipo puedan reconocer fácilmente. La aplicación AWS Support usa este nombre para identificar su cuenta en el canal de Slack. Puede actualizar este nombre en cualquier momento.



Su espacio de trabajo y el nombre de la cuenta aparecen en la página Slack configuration (Configuración de Slack).



Autorización de varias cuentas

Para autorizar que varias Cuentas de AWS usen espacios de trabajo de Slack, puede utilizar AWS CloudFormation o Terraform para crear recursos de la AWS Support.

Configuración de un canal de Slack

Después de autorizar su espacio de trabajo de Slack, podrá configurar sus canales de Slack para que usen la aplicación AWS Support.

El canal al que invita y agrega la aplicación AWS Support es donde podrá crear y buscar casos, y recibir notificaciones de estos. Este canal muestra actualizaciones de casos, como los creados recientemente o los resueltos, correspondencias agregadas y detalles de casos compartidos.

El canal de Slack hereda los permisos del rol de IAM. Esto significa que cualquier usuario del canal de Slack tiene los mismos permisos que se especifican en la política de IAM asociada al rol.

Por ejemplo, si su política de IAM permite que el rol tenga permisos completos de lectura y escritura para los casos de soporte, cualquier persona de su canal de Slack podrá crear, actualizar y resolver los casos de soporte. Si su política de IAM concede al rol permisos de solo lectura, los usuarios de su canal de Slack solo tendrán permisos de lectura para los casos de soporte.

Puede agregar hasta 20 canales a una cuenta. Un canal de Slack puede tener hasta 100 Cuentas de AWS. Esto significa que solo 100 cuentas pueden agregar el mismo canal de Slack a la aplicación AWS Support. Le recomendamos que solo agregue las cuentas que necesita para administrar los casos de soporte de su organización. Esto puede reducir la cantidad de notificaciones que recibe en el canal para que usted y su equipo tengan menos distracciones.

Cada Cuenta de AWS debe configurar un canal de Slack por separado en la aplicación AWS Support. De esta manera, la aplicación AWS Support puede acceder a los casos de soporte de esa Cuenta de AWS. Si otra Cuenta de AWS de su organización ya invitó a la aplicación AWS Support al canal de Slack, vaya al paso 3.

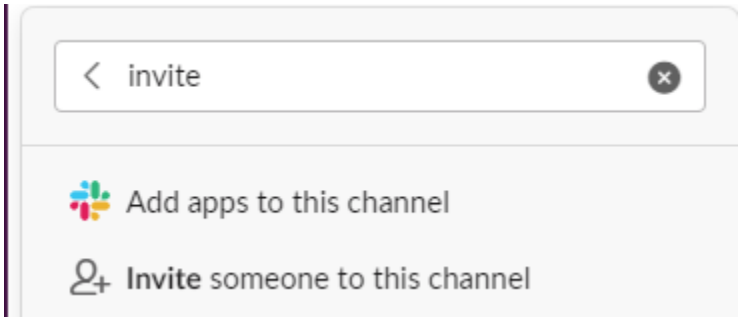
> **Note**
>
> Puede configurar los canales que forman parte de Slack Connect y los canales que se comparten con varios espacios de trabajo. Sin embargo, solo el primer espacio de trabajo que configuró el canal compartido para un Cuenta de AWS puede usar la AWS Support aplicación. La aplicación AWS Support devuelve un mensaje de error si intenta configurar el mismo canal de Slack para otro espacio de trabajo.

Para configurar un canal de Slack

1. Desde su aplicación de Slack, elija el canal que quiere usar con la aplicación AWS Support.

2. Siga estos pasos para invitar a la aplicación AWS Support a su canal:

   a. Elija el icono + e ingrese `invite`. A, a continuación, cuando se le solicite, elija Add apps to this channel (Agregar aplicaciones a este canal).

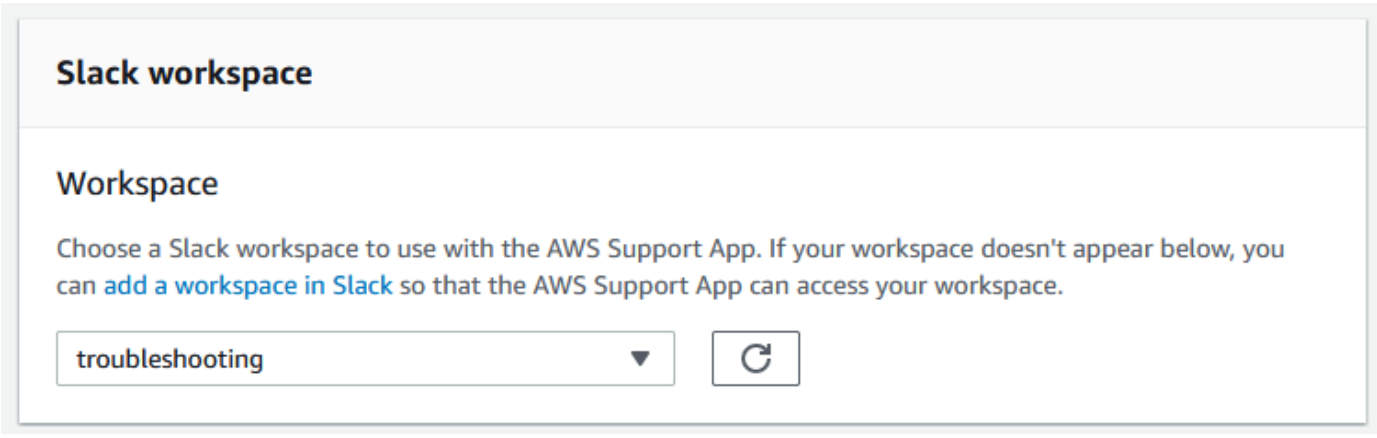
   

   b. Para buscar la aplicación, en Add apps to channelName (Agregar aplicaciones a channelName) ingrese AWS Support App (Aplicación).

   c. Elija Agregar junto a la Aplicación AWS Support.

3. Inicie sesión en la consola del Centro de soporte y elija Slack configuration (Configuración de Slack).
4. Elija Add channel (Agregar canal).
5. En la página Add channel (Agregar canal), en Workspace (Espacio de trabajo), elija el nombre del espacio de trabajo que autorizó anteriormente. Puede elegir el icono de actualización si el nombre del espacio de trabajo no aparece en la lista.



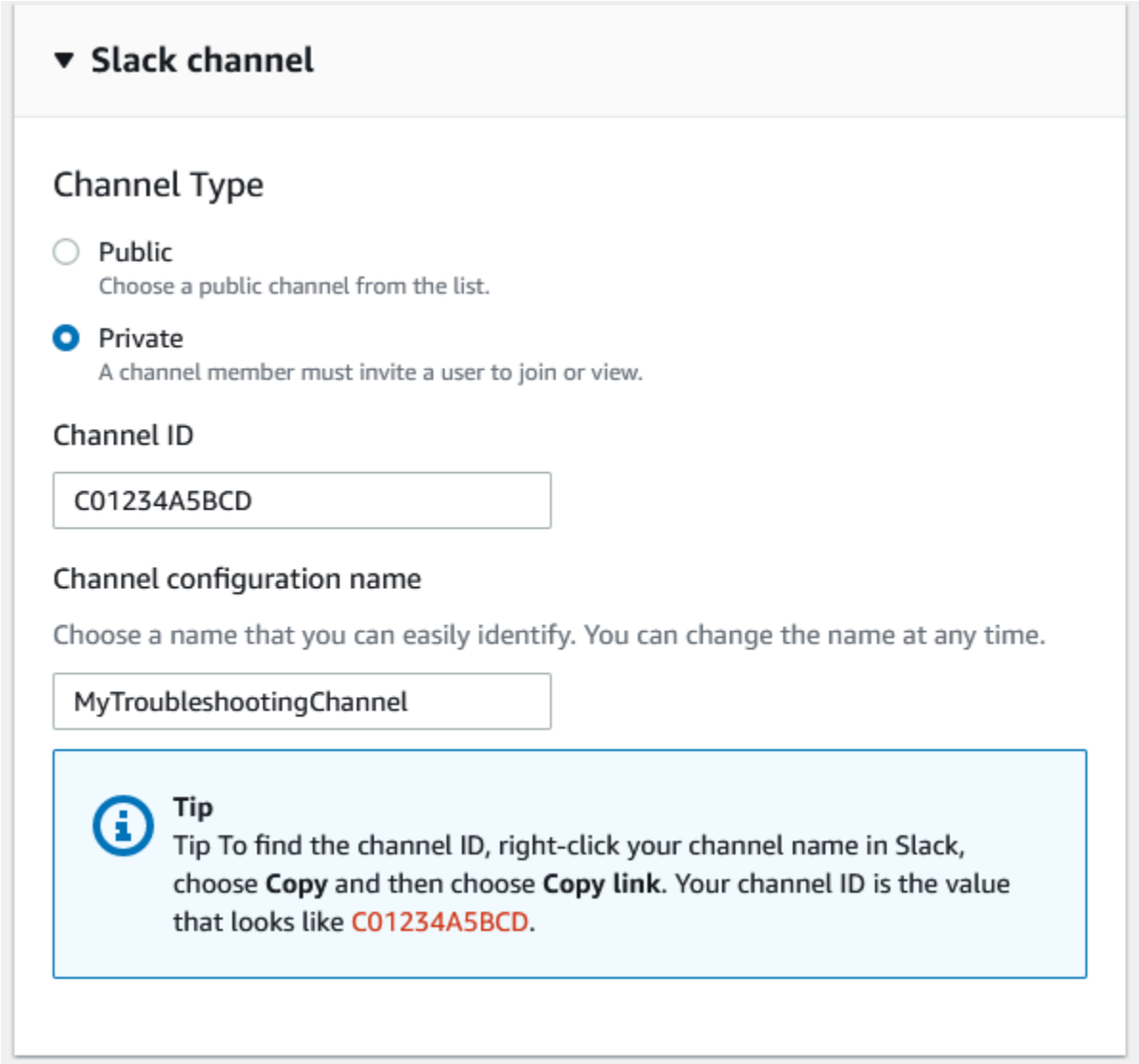
6. En Slack channel (Canal de Slack), en Channel type (Tipo de canal), elija una de las siguientes opciones:

   - Public (Público): en Public channel (Canal público), elija el canal de Slack al que invitó a la aplicación AWS Support (paso 2). Si su canal no aparece en la lista, seleccione el icono de actualización e inténtelo de nuevo.
   - Private (Privado): en Channel ID (ID de canal), ingrese el ID o la URL del canal de Slack al que invitó a la aplicación AWS Support.

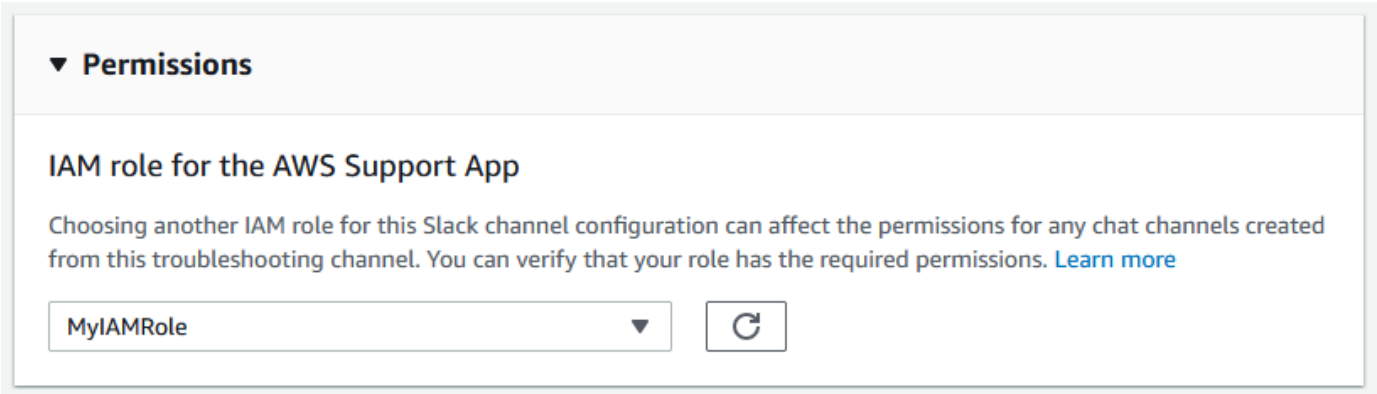
   > **Tip**
   >
   > Para encontrar el ID de canal, abra el menú contextual (haga clic con el botón derecho) del nombre del canal en Slack y, a continuación, elija Copy (Copiar) y, a continuación, Copy link (Copiar enlace). El ID de canal es el valor que es similar a *C01234A5BCD*.

7. En Channel configuration name (Nombre de configuración de canal), ingrese un nombre que identifique fácilmente la configuración de su canal de Slack para la aplicación AWS Support. Este nombre solo aparece en su Cuenta de AWS y no en Slack. Puede cambiar el nombre de la configuración del canal más adelante.

   El tipo de canal de Slack podría tener el siguiente aspecto.



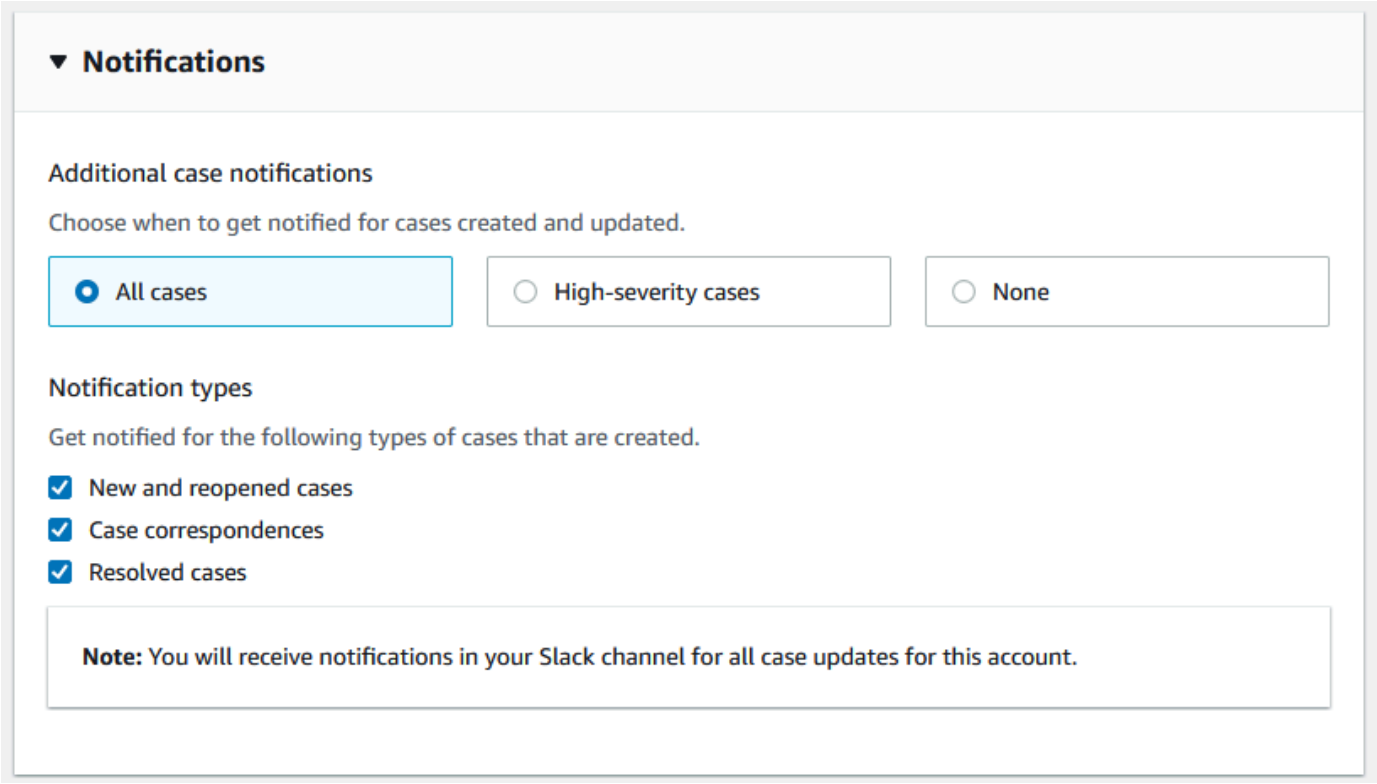
8. En Permissions (Permisos), en IAM role for the AWS Support App in Slack (Rol de IAM de la aplicación en Slack), elija un rol que haya creado para la aplicación AWS Support. Solo los roles que tienen la aplicación AWS Support como entidad de confianza aparecen en la lista.



> **Note**
>
> Si no ha creado ningún rol o no lo ve en la lista, consulte Administración del acceso a la aplicación AWS Support.

9. En Notifications (Notificaciones), especifique cómo quiere recibir notificaciones de los casos.
   - All cases (Todos los casos): reciba notificaciones de todas las actualizaciones de casos.
   - High-severity cases (Casos de alta gravedad): reciba notificaciones solo en los casos que afecten a un sistema de producción o superior. Para obtener más información, consulte Elección de la gravedad.
   - None (Ninguna): no recibirá notificaciones de actualizaciones de casos.
10. (Opcional) Si elige All cases (Todos los casos) o High-severity cases (Casos de alta gravedad), debe seleccionar al menos una de las siguientes opciones:
    - New and reopened cases (Casos nuevos y reabiertos)
    - Case correspondences (Correspondencias de casos)
    - Resolved cases (Casos resueltos)

    El siguiente canal recibe notificaciones de casos de todas las actualizaciones de estos en Slack.



11. Revise su configuración y elija Add channel (Agregar canal). Su canal aparece en la página Slack configuration (Configuración de Slack).

Actualización de la configuración del canal de Slack

Después de configurar su canal de Slack, puede actualizarlo más adelante para cambiar el rol de IAM o las notificaciones de casos.

Para actualizar la configuración del canal de Slack

1. Inicie sesión en la consola del Centro de soporte y elija Slack configuration (Configuración de Slack).
2. En Channels (Canales), elija la configuración de canal que quiera.
3. En la página ***channelName***, puede hacer las siguientes tareas:
   - Elegir Rename (Renombrar) para actualizar el nombre de la configuración de su canal. Este nombre solo aparece en su Cuenta de AWS y no aparecerá en Slack.
   - Elegir Delete (Eliminar) para eliminar la configuración de canales de la aplicación AWS Support. Consulte Eliminación de la configuración de un canal de Slack de la aplicación AWS Support.

- Elegir Open in Slack (Abrir en Slack) para abrir el canal de Slack en su navegador.
- Elegir Edit (Editar) para cambiar el rol de IAM o las notificaciones.

Creación de casos de soporte en un canal de Slack

Después de autorizar su espacio de trabajo de Slack y agregar su canal de Slack, puede crear un caso de soporte en dicho canal.

Para crear un caso de soporte en Slack

1. En su canal de Slack, ingrese el comando siguiente:

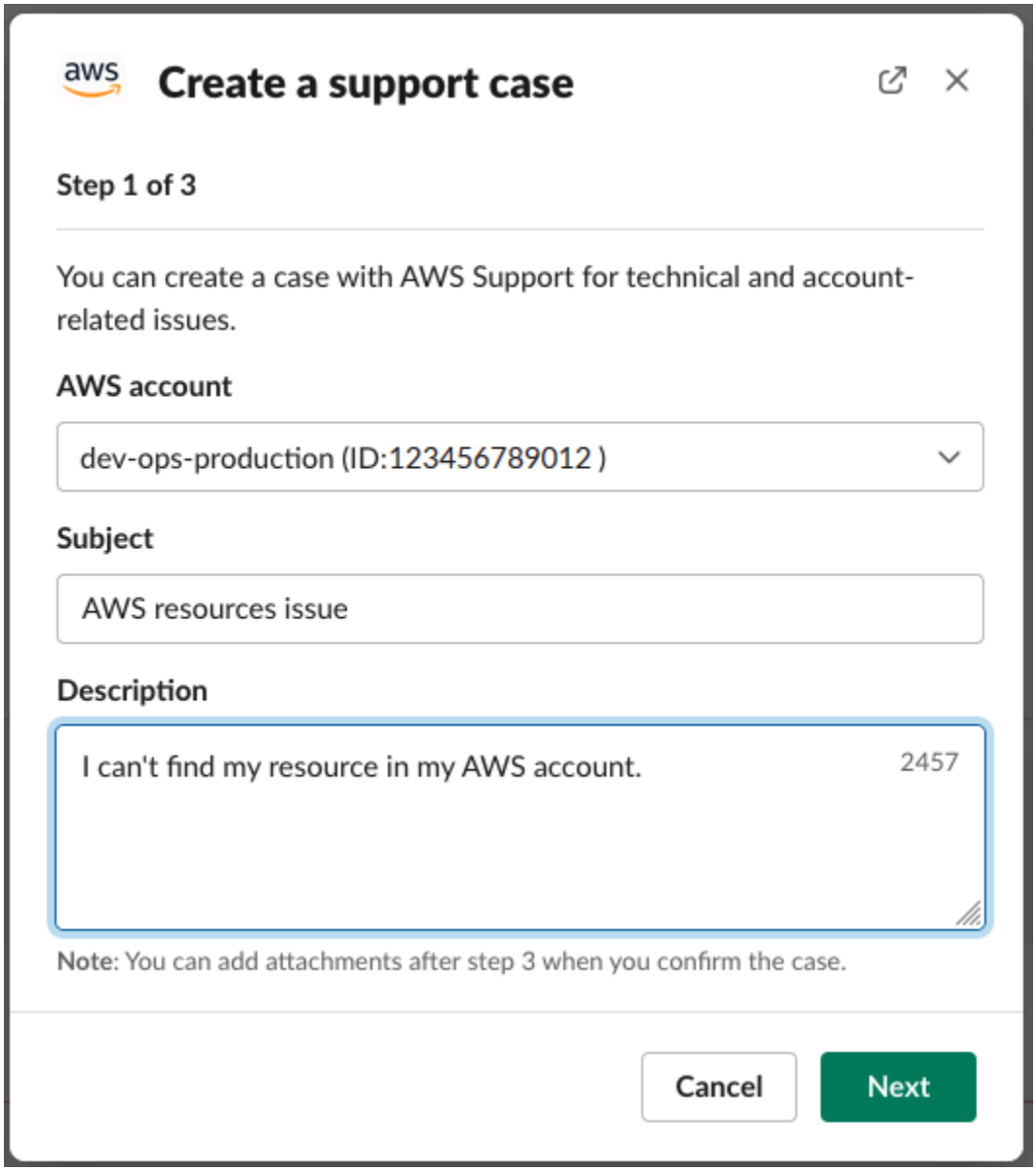
   ```
   /awssupport create
   ```

2. En el cuadro de diálogo Create a support case (Crear un caso de soporte), haga lo siguiente:

   a. Si configuró más de una cuenta para este canal de Slack, en la Cuenta de AWS, elija el ID de cuenta. Si creó un nombre de cuenta, este valor aparece junto al ID de cuenta. Para obtener más información, consulte Autorización de un espacio de trabajo de Slack.

   b. En Subject (Asunto), ingrese un título para el caso de soporte.

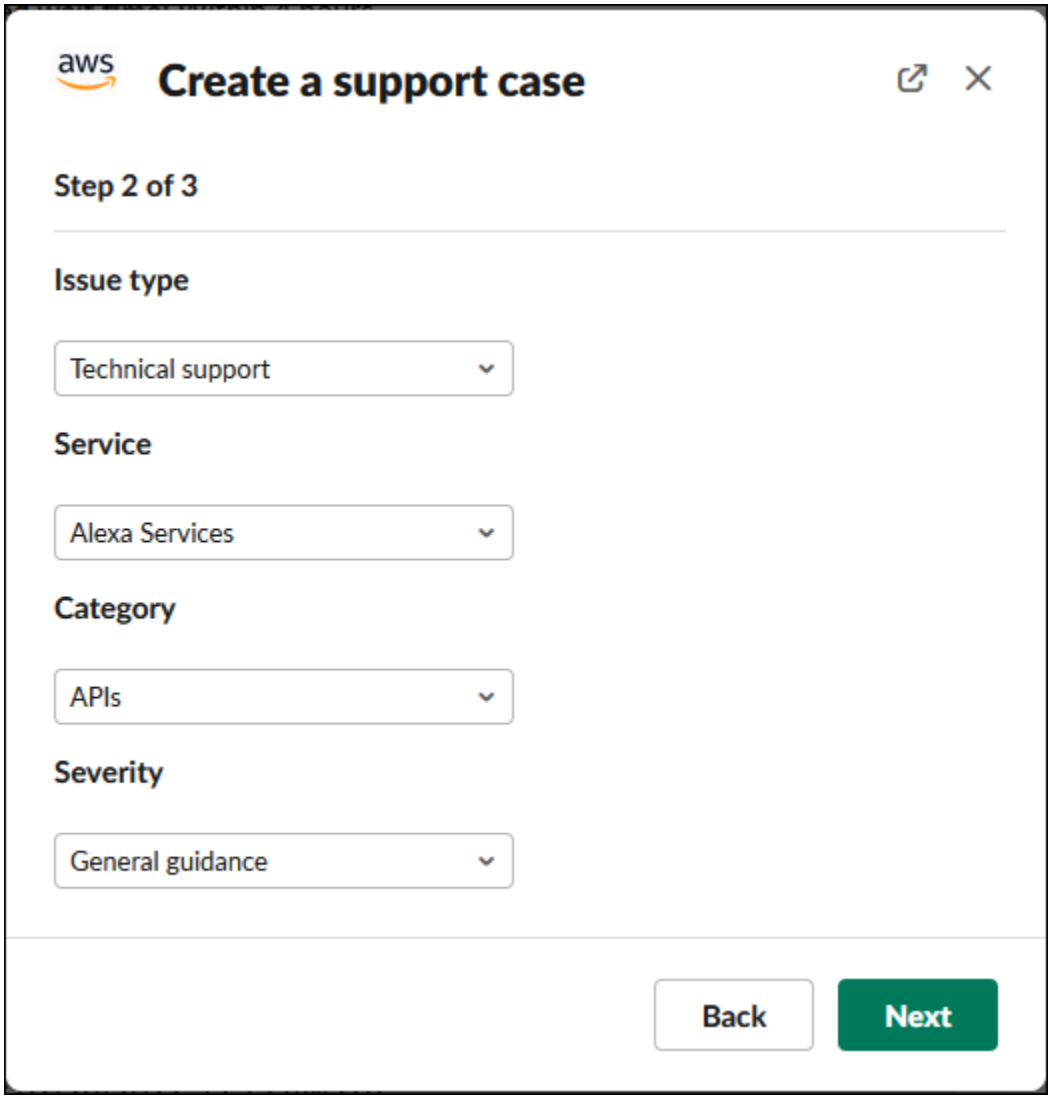
   c. En Description (Descripción), describa dicho caso. Proporcione detalles sobre, por ejemplo, cómo utilizar un Servicio de AWS y qué pasos ha seguido para solucionar problemas.



3. Elija Next (Siguiente).
4. En el cuadro de diálogo Create a support case (Crear un caso de soporte), especifique las opciones siguientes:

   a. Elija el Issue type (Tipo de problema).
   b. Elija el Service (Servicio).
   c. Elija la Category (Categoría).
   d. Elige la Severity (Gravedad).
   e. Revise los detalles de su caso y elija Next (Siguiente).

      El siguiente ejemplo muestra un caso de soporte técnico para Alexa Services.

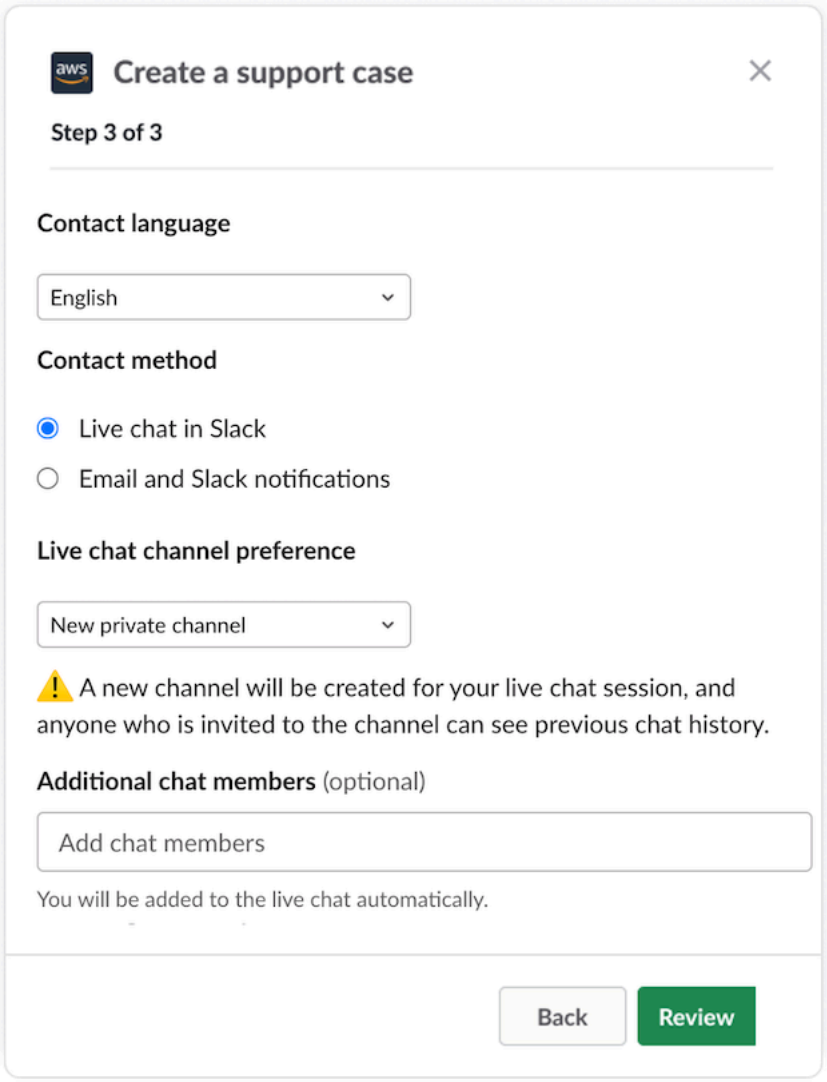


5. En Contact language (Idioma de contacto), elija el idioma que prefiera para el caso de soporte.

> **Note**
>
> El idioma japonés no está disponible para el chat en directo en Slack para casos de cuentas y facturación.

6. En Contact method (Método de contacto), elija Email and Slack notifications (Notificaciones en Slack y por correo electrónico) o Live chat in Slack (Chat en vivo en Slack).

   En el siguiente ejemplo se muestra cómo elegir un chat en directo en Slack.



a. Si elige Chat en vivo en Slack, elija Canal privado nuevo o Canal actual como Canal de chat en vivo de preferencia. El Canal privado nuevo creará un canal privado independiente para que pueda comunicarse con el agente de AWS Support, y el Canal actual utilizará un hilo en el canal actual para que pueda comunicarse con el agente de AWS Support.

b. (Opcional) Si elige Live chat in Slack (Chat en vivo en Slack), puede ingresar los nombres de otros miembros de Slack. En Canal privado nuevo, la aplicación AWS Support lo agregará de manera automática a usted y a los miembros seleccionados al canal nuevo. En Canal actual, la aplicación AWS Support lo etiquetará de manera automática a usted y a los miembros seleccionados en el hilo de chat cuando el agente de AWS Support se una.

> **Important**
>
> - Recomendamos que solo agregue a los miembros del chat a los que quiera conceder acceso a los detalles del caso de soporte y al historial de chat.
> - Si inicia una nueva sesión de chat en vivo para un caso de soporte existente, la aplicación AWS Support utiliza el mismo canal o hilo de chat que se utilizó para un chat en vivo anterior. La aplicación AWS Support también utiliza la misma preferencia de canal de chat en vivo que se utilizaba anteriormente.
> - La opción de Canal actual solo está disponible si el chat se solicita desde un canal privado. Recomendamos que utilice esta opción solo si desea que todos los miembros del canal tengan acceso al chat.

7. (Opcional) En Additional contacts to notify (Contactos adicionales a los que notificar), ingrese las direcciones de correo electrónico que también deben recibir actualizaciones sobre este caso de soporte. Puede agregar hasta 10 direcciones de correo electrónico.
8. Elija Review.
9. En el canal de Slack, revise los detalles del caso. Puede hacer lo siguiente:
   - Elija Edit (Editar) para cambiar los detalles del caso.
   - Agregue un archivo a su caso. Para ello, siga estos pasos:
     a. Elija Attach file (Adjuntar archivo), elija el icono + en Slack y, a continuación, Your computer (Mi equipo).
     b. Vaya al archivo y elíjalo.
     c. En el cuadro de diálogo Upload a file (Cargar un archivo), ingrese `@awssupport` y pulse el icono

        para enviar el mensaje.

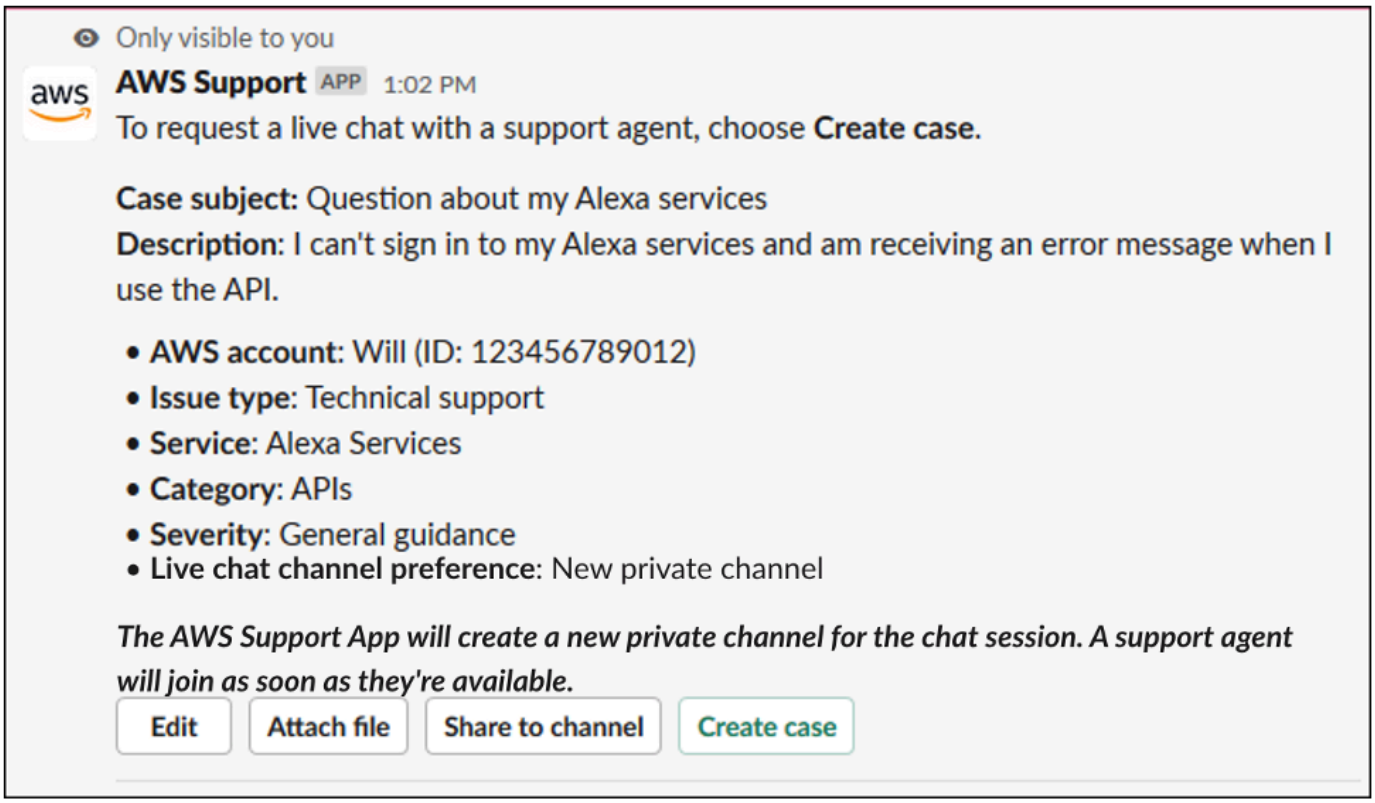
> **Notas**
>
> - Puede adjuntar hasta tres archivos. Cada archivo puede ser de hasta 5 MB.

- Si adjunta un archivo a su caso de soporte, debe presentar su caso en el plazo de 1 hora. Si no lo hace, debe volver a agregar los archivos.

- Elija Share to channel (Compartir en el canal) para compartir los detalles del caso con otras personas en el canal de Slack. Puede usar esta opción para compartir los detalles del caso con su equipo antes de crear el caso.

10. Revise los detalles de su caso y, a continuación, elija Create case (Crear caso).

    El siguiente ejemplo muestra un caso de soporte técnico para Alexa Services.



    Después de crear un caso de soporte, es posible que los detalles del caso tarden unos minutos en aparecer.

11. Cuando se actualice dicho caso, puede elegir See details (Ver detalles) para ver la información del caso. A continuación puede hacer lo siguiente:

    - Elija Share to channel (Compartir en el canal) para compartir los detalles del caso con otras personas en el canal de Slack.
    - Elija Reply (Responder) para agregar una correspondencia.
    - Elija Resolve case (Resolver el caso).

> **Note**
>
> Si no eligió recibir actualizaciones automáticas de casos en Slack, puede buscar el caso de soporte para encontrar la opción See details (Ver detalles).

Respuesta a casos de soporte en Slack

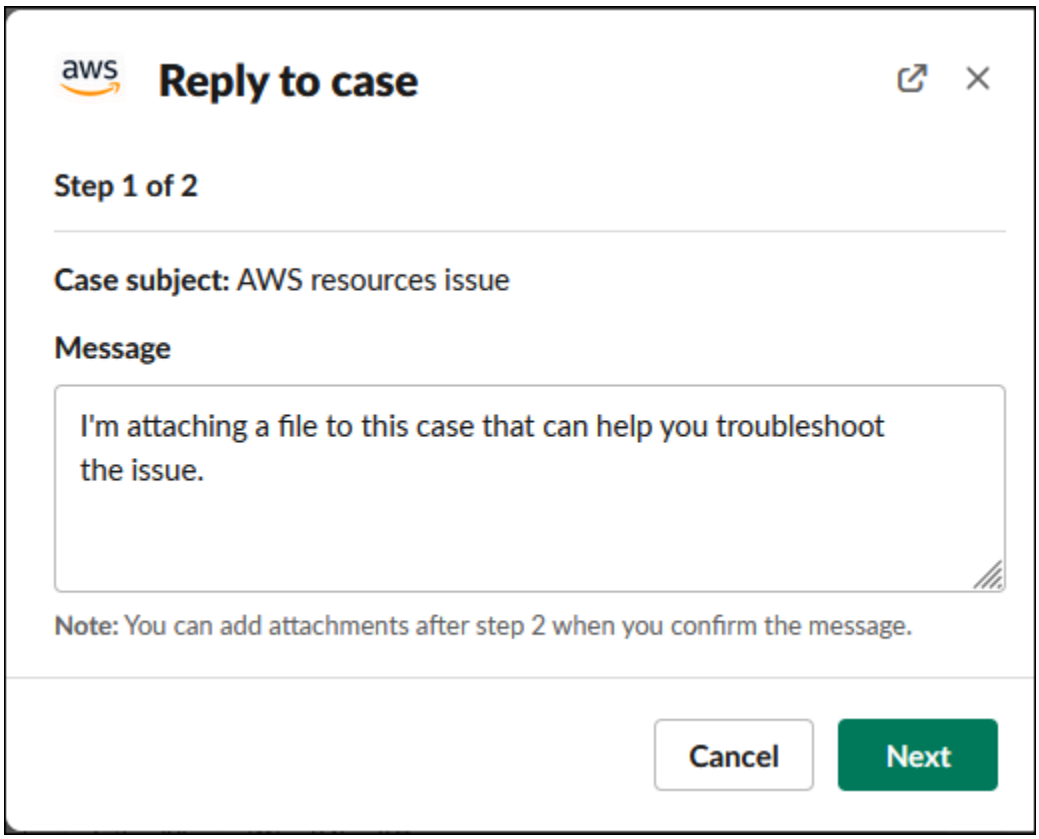
Puede agregar actualizaciones a su caso como información y archivos adjuntos, y responder a las respuestas del agente de asistencia.

> **Note**
>
> - También puede utilizar el AWS Support Center Console para responder a los agentes de asistencia. Para obtener más información, consulte Actualización, resolución y reapertura de su caso.
> - No se pueden agregar correspondencias a casos desde los canales de chat creados por la aplicación AWS Support. Los canales de chat en vivo solo envían mensajes a los agentes durante el chat en vivo.

Para responder a un caso de soporte en Slack

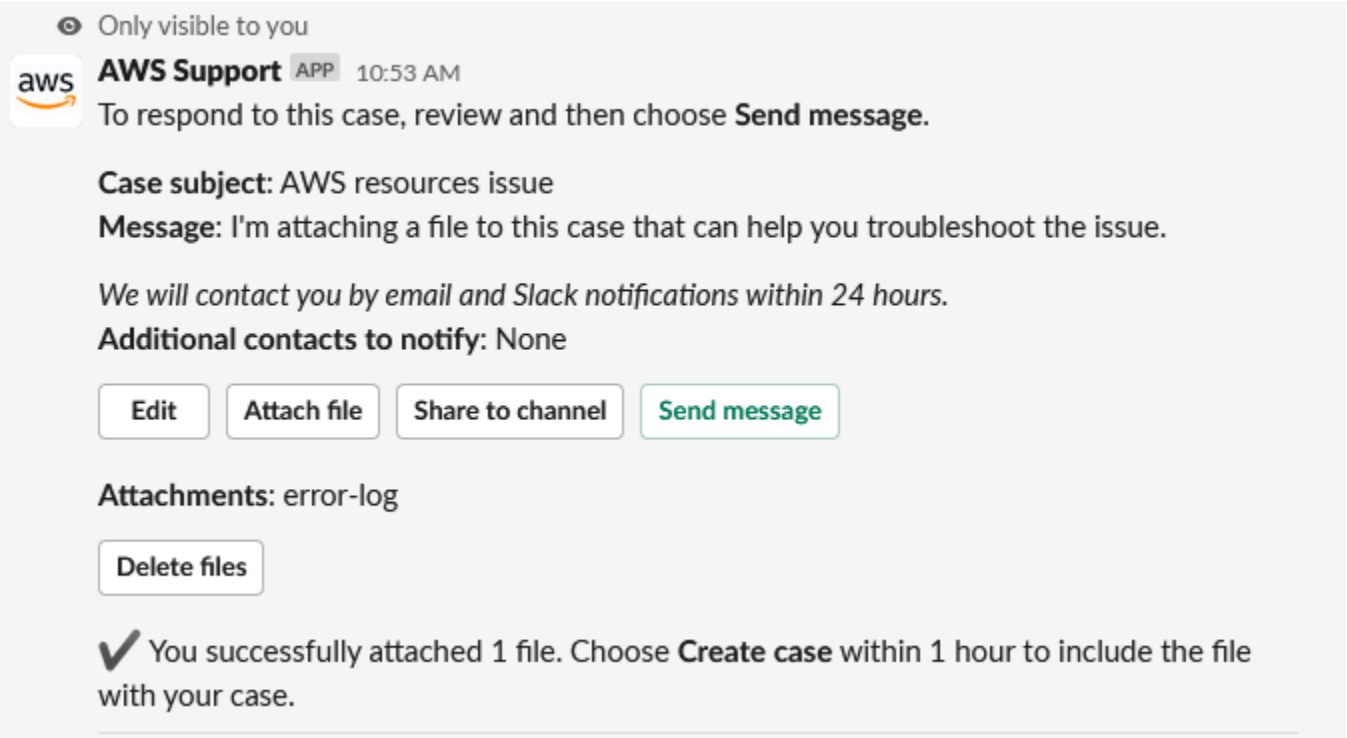
1. En su canal de Slack, elija el caso al que quiere responder. Puede ingresar `/awssupport search` para encontrar su caso de soporte.
2. Elija See details (Ver detalles) junto al caso que quiere revisar.
3. En la parte inferior de los detalles del caso, elija Reply (Responder).

4. En el cuadro de diálogo Reply to case (Responder al caso), ingrese una breve descripción del problema en el campo Message (Mensaje). A continuación, elija Next.



5. Elija un método de contacto. Los métodos de contacto disponibles dependen del tipo de caso y del plan de soporte.
6. (Opcional) En Additional contacts to notify (Contactos adicionales a los que notificar), ingrese las direcciones de correo electrónico adicionales que quiere que reciban actualizaciones sobre este caso de soporte. Puede agregar hasta 10 direcciones de correo electrónico.
7. Elija Review. A continuación, puede elegir si quiere editar su respuesta, adjuntar archivos o compartirla en el canal.
8. Cuando haya terminado de responder, elija Send message (Enviar mensaje).
9. (Opcional) Para ver la correspondencia anterior de su caso, elija Previous correspondence (Correspondencia anterior). Para ver los mensajes acortados, seleccione Show full message (Mostrar mensaje completo).

Example : respuesta a un caso en Slack



Únase a una sesión de chat en vivo con AWS Support

Cuando solicitas un chat en directo para tu caso, eliges usar un nuevo canal de chat o un hilo del canal actual para ti y el AWS Support agente. Utilice este canal o hilo de chat para comunicarse con el agente de soporte y cualquier otra persona a la que haya invitado al chat en vivo.

Important

Cualquier persona que se una a un canal con chat en vivo puede ver los detalles del caso de soporte específico y el historial de chat. Se recomienda añadir solo a los usuarios que necesiten acceder a tus casos de asistencia. Cualquier miembro de un canal o un hilo de chat también puede participar en un chat activo.

Note

Los canales e hilos de chat en vivo también reciben notificaciones cuando se agrega una correspondencia al caso fuera de la sesión de chat en vivo. Esto ocurre antes, durante y después de una sesión de chat, por lo que puedes usar un canal o hilo de chat para

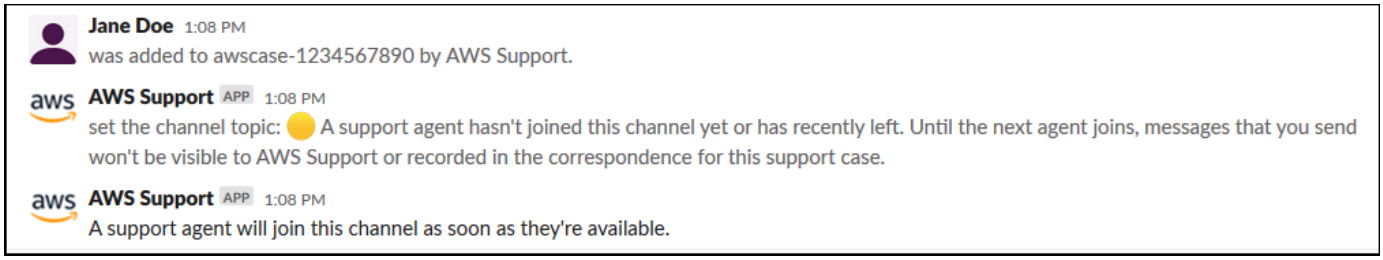
monitorear todas las actualizaciones de un caso. Si has elegido usar un nuevo canal de chat, usa el canal de configuración al que has invitado a la AWS Support aplicación para responder a estas correspondencias.

Para unirse a una sesión de chat en vivo AWS Support en un canal nuevo

1. En la aplicación de Slack, navega hasta el canal que la AWS Support aplicación cree para ti. El nombre del canal incluye el ID de su caso de soporte; por ejemplo, *awscase-1234567890*.

   > **Note**
   >
   > La AWS Support aplicación añade un mensaje fijo al canal de chat en directo que contiene detalles sobre tu caso de asistencia. Desde el mensaje anclado, puede finalizar el chat o resolver el caso. Puede encontrar todos los mensajes anclados en este canal debajo del nombre de este.

2. Cuando el agente de soporte se una al canal, podrá hablar sobre su caso de soporte. Hasta que un agente de asistencia no se una al canal, no verá los mensajes de ese chat y los mensajes no aparecerán en la correspondencia de tu caso.

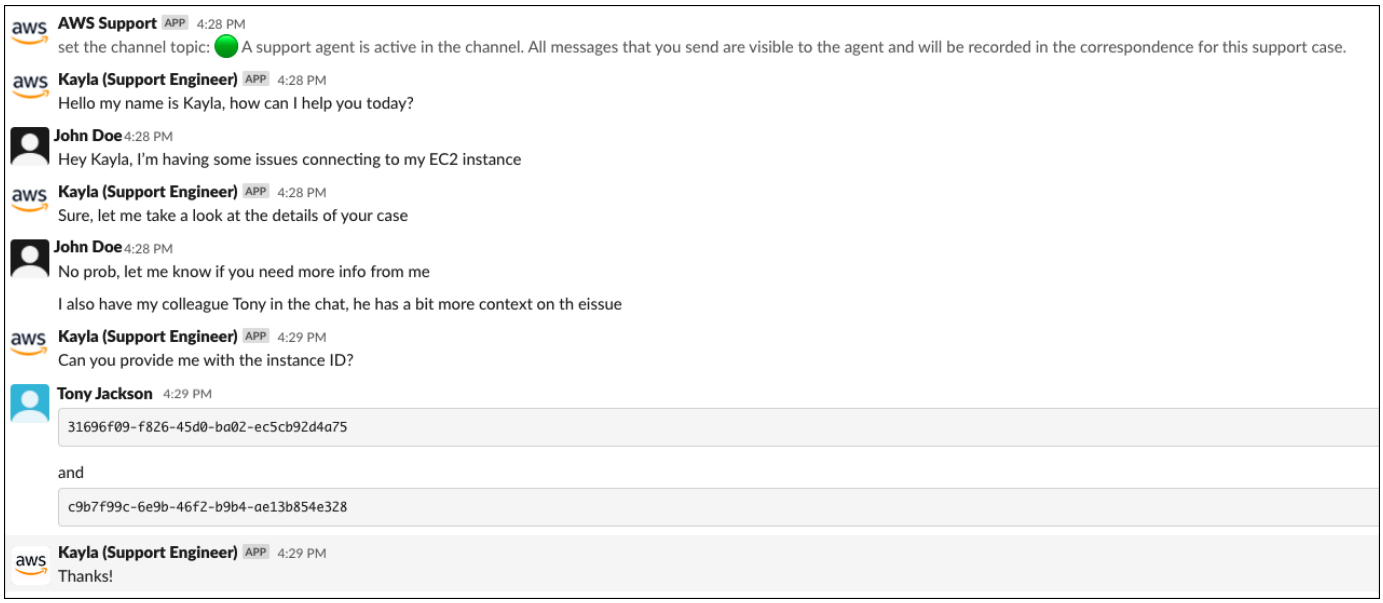
3. (Opcional) Agregue otros miembros al canal de chat. De forma predeterminada, los canales de chat son privados.
4. Una vez que el agente de soporte se une al chat, el canal está activo y la aplicación AWS Support graba el chat.

   Puede hablar con el agente sobre su caso de soporte y cargar cualquier archivo adjunto al canal. La AWS Support aplicación guarda automáticamente los archivos y el registro del chat en la correspondencia de tu caso.

> **Note**
>
> Cuando hables con un agente de asistencia, ten en cuenta las siguientes diferencias entre Slack y la AWS Support aplicación:
>
> - Los agentes de soporte no pueden ver los mensajes o hilos compartidos. Para compartir el texto de un mensaje o hilo, ingrese el texto como un mensaje nuevo.
> - Si edita o elimina un mensaje, el agente seguirá viendo el mensaje original. Debe volver a ingresar el mensaje nuevo para mostrar la revisión.

Example : sesión de chat en vivo

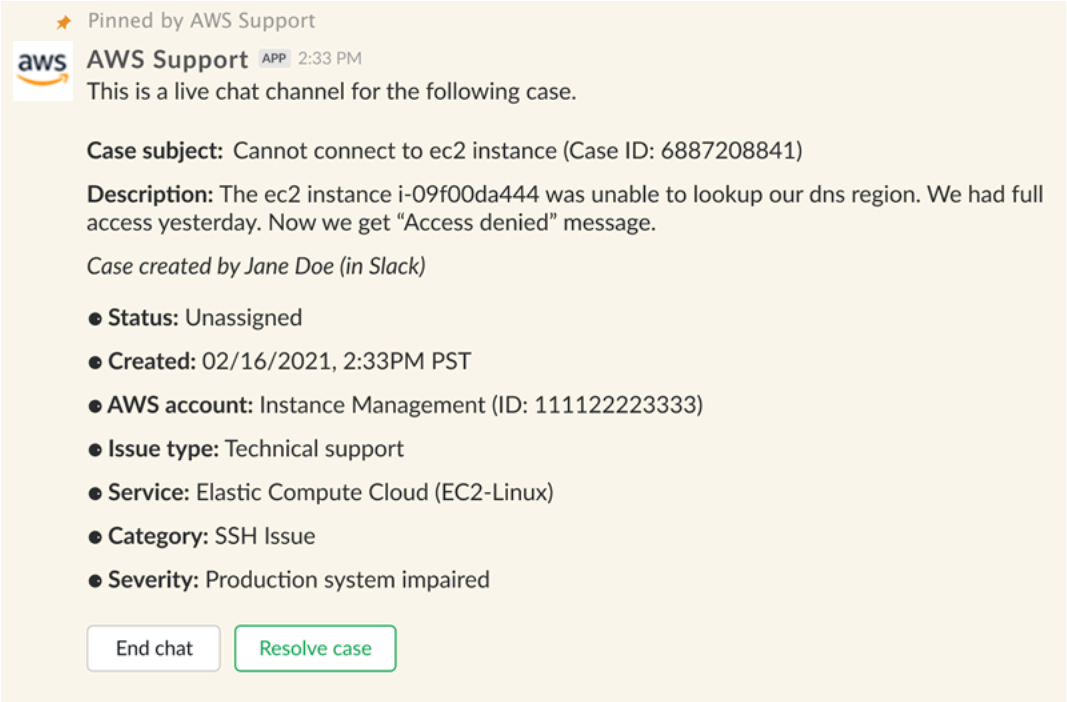
A continuación, se muestra un ejemplo de sesión de chat en vivo con un agente de soporte para solucionar un problema de conectividad en dos instancias de Amazon Elastic Compute Cloud (Amazon EC2).



5. (Opcional) Para detener el chat en vivo, elija End chat (Finalizar chat). El agente de soporte abandona el canal y la AWS Support aplicación deja de grabar el chat en directo. Puede encontrar el historial del chat adjunto a la correspondencia de este caso de soporte.
6. Si el problema se resolvió, puede elegir Resolve case (Resolver caso) en el mensaje anclado o ingresar `/awssupport resolve`.

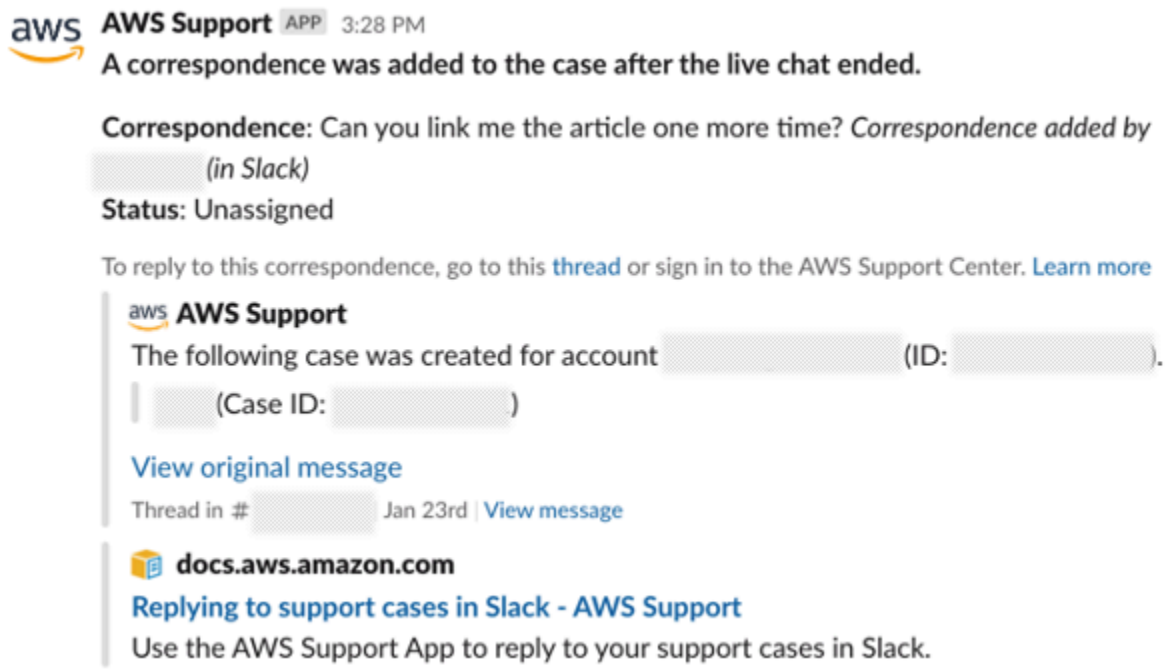
Example : finalización de un chat en vivo

En el siguiente mensaje anclado, se muestran los detalles del caso de una instancia de Amazon EC2. Puede encontrar los mensajes anclados debajo del nombre del canal de Slack.



Example : Notificación de correspondencia en un canal de chat

A continuación se muestra un ejemplo de un canal de chat en vivo que recibe una notificación cuando otro colaborador agrega una actualización después de que el chat haya finalizado.

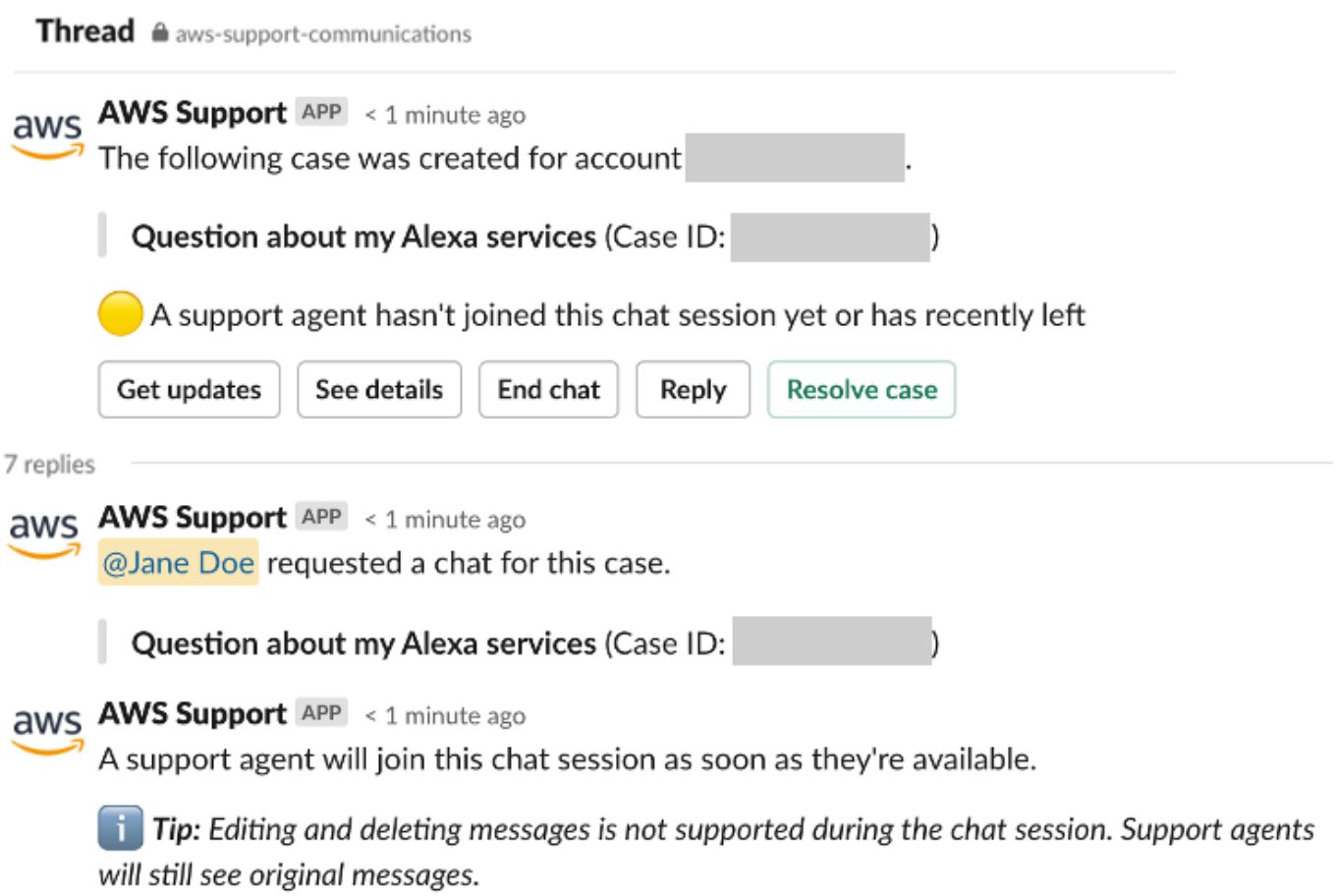


La notificación indicará el estado del chat (solicitado, en curso o finalizado) y si la correspondencia la ha agregado un agente u otro colaborador. La aplicación de Support también intentará retomar el hilo o canal original de Slack donde se solicitó este chat. Puede responder al caso desde ese canal, o bien desde cualquier otro canal con acceso al caso.

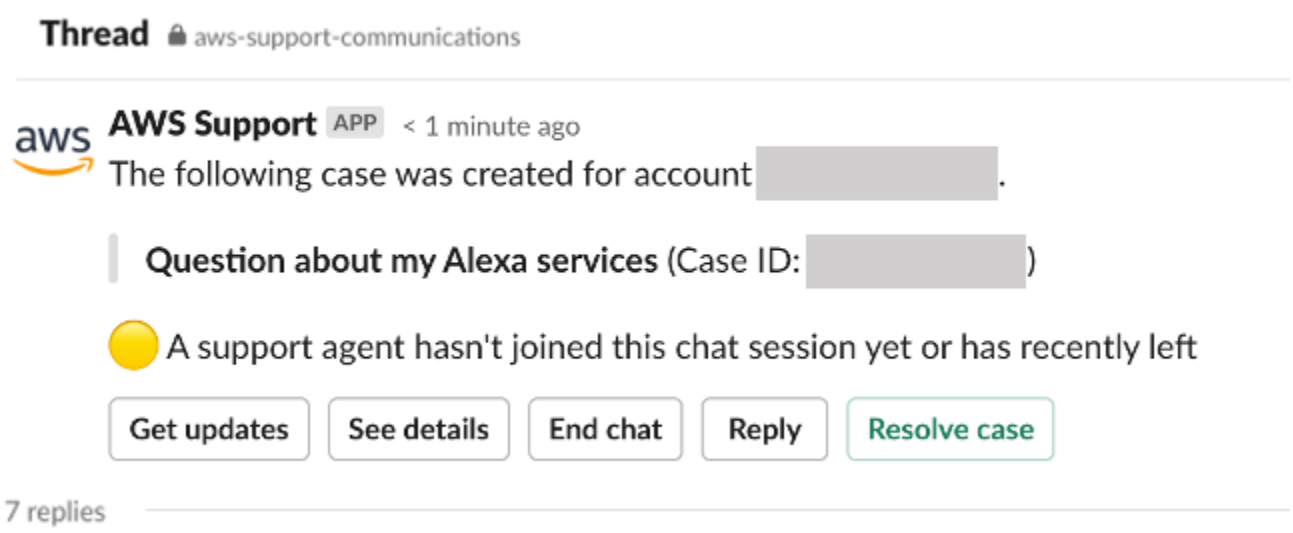
Para unirse a una sesión de chat AWS Support en vivo desde el canal actual

1. En la aplicación de Slack, navega hasta el hilo del canal actual que la AWS Support aplicación usa para el chat. En la mayoría de los casos, será el hilo que se inició cuando se creó el caso por primera vez.
2. Cuando el agente de soporte se una al hilo, usted podrá hablar sobre su caso de soporte. Hasta que un agente de soporte no se una al hilo, el agente no verá los mensajes en el hilo, y los mensajes no aparecerán en la correspondencia de su caso cuando finalice el chat.

> **Note**
>
> Los mensajes que se envíen a este canal fuera del hilo de chat nunca se ven AWS Support, ni siquiera cuando el chat está activo.



3. (Opcional) Etiquete a otros miembros del canal para notificarlos en el hilo de chat.
4. Una vez que el agente de soporte se une al chat, el hilo de chat se activa y la AWS Support aplicación graba el chat. De forma similar a la nueva opción de canal de chat, puede conversar con el agente sobre su caso de soporte y cargar cualquier archivo adjunto al hilo. La AWS Support aplicación guarda automáticamente los archivos y el registro del chat en la correspondencia de su caso.
5. (Opcional) Para detener el chat en vivo, elija Finalizar chat en el mensaje inicial de este hilo. El agente de soporte abandona el hilo y la AWS Support aplicación deja de grabar el chat en vivo. Puede encontrar el historial del chat adjunto a la correspondencia de este caso de soporte.
6. Si el problema se resolvió, puede elegir Resolver caso en el mensaje inicial de este hilo.



Búsqueda de casos de soporte en Slack

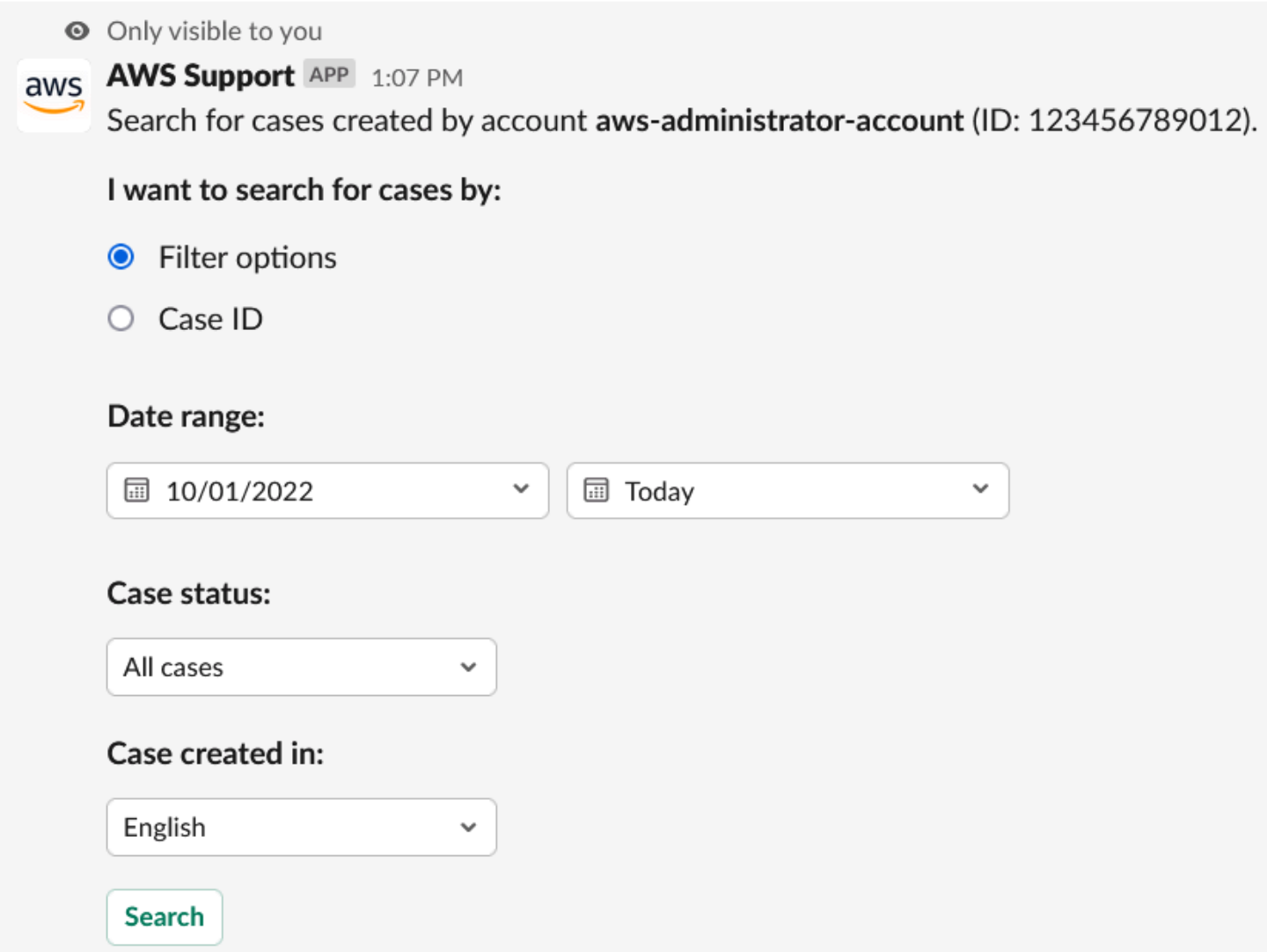
Desde el canal de Slack, puede buscar casos de soporte de la Cuenta de AWS y de otras que también configuraron el mismo canal y espacio de trabajo. Por ejemplo, si su cuenta (123456789012) y la cuenta de su compañero de trabajo (111122223333) configuraron el mismo espacio de trabajo y los mismos canales en la AWS Support Center Console, puede usar la aplicación AWS Support para buscar y actualizar los casos de soporte mutuamente.

Para filtrar los resultados de la búsqueda, puede utilizar las siguientes opciones:

- ID de cuenta
- ID de caso
- Estado del caso
- Idioma de contacto
- Rango de fechas

Example : buscar casos en Slack

El siguiente ejemplo muestra cómo buscar por opciones de filtro en una sola cuenta especificando el intervalo de fechas, estado del caso e idioma del contacto.



Para buscar un caso de soporte en Slack

1. En el canal de Slack, ingrese el comando siguiente:

   ```
   /awssupport search
   ```

2. Para la opción I want to search for cases by: (Quiero buscar casos por:), elija una de las siguientes opciones:

   A. Filter options (Opciones de filtro) – puede filtrar los casos con las siguientes opciones:

   - Cuenta de AWS – esta lista solo aparece si tiene varias cuentas en este canal.
   - Date range (Intervalo de fechas) – fecha en la que se creó el caso.
   - Case status (Estado del caso) – el estado actual del caso, como, All open cases (Todos los casos abiertos) o Resolved (Resuelto).

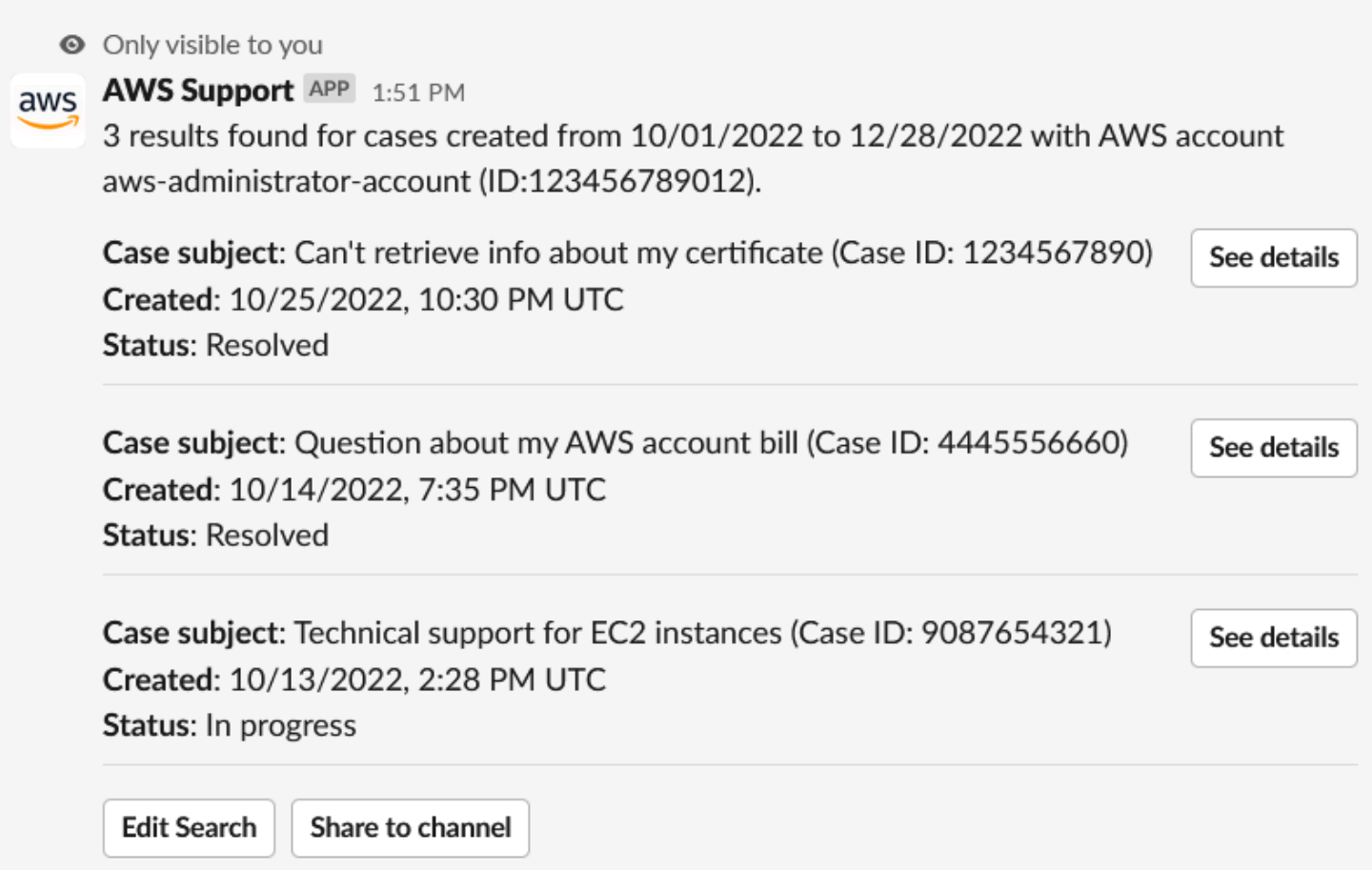
- Case created in (Caso creado en) el idioma de contacto del caso.

B. Case ID (ID del caso): ingrese el ID del caso. Solo puede ingresar un ID de caso a la vez. Si tiene varias cuentas en el canal, elija la Cuenta de AWS para buscar el caso.

3. Elija Search (Buscar). Los resultados de la búsqueda aparecen en Slack.

Utilice los resultados de búsqueda

El siguiente ejemplo devuelve tres casos de soporte de una Cuenta de AWS.



Una vez que reciba los resultados de búsqueda, puede hacer lo siguiente:

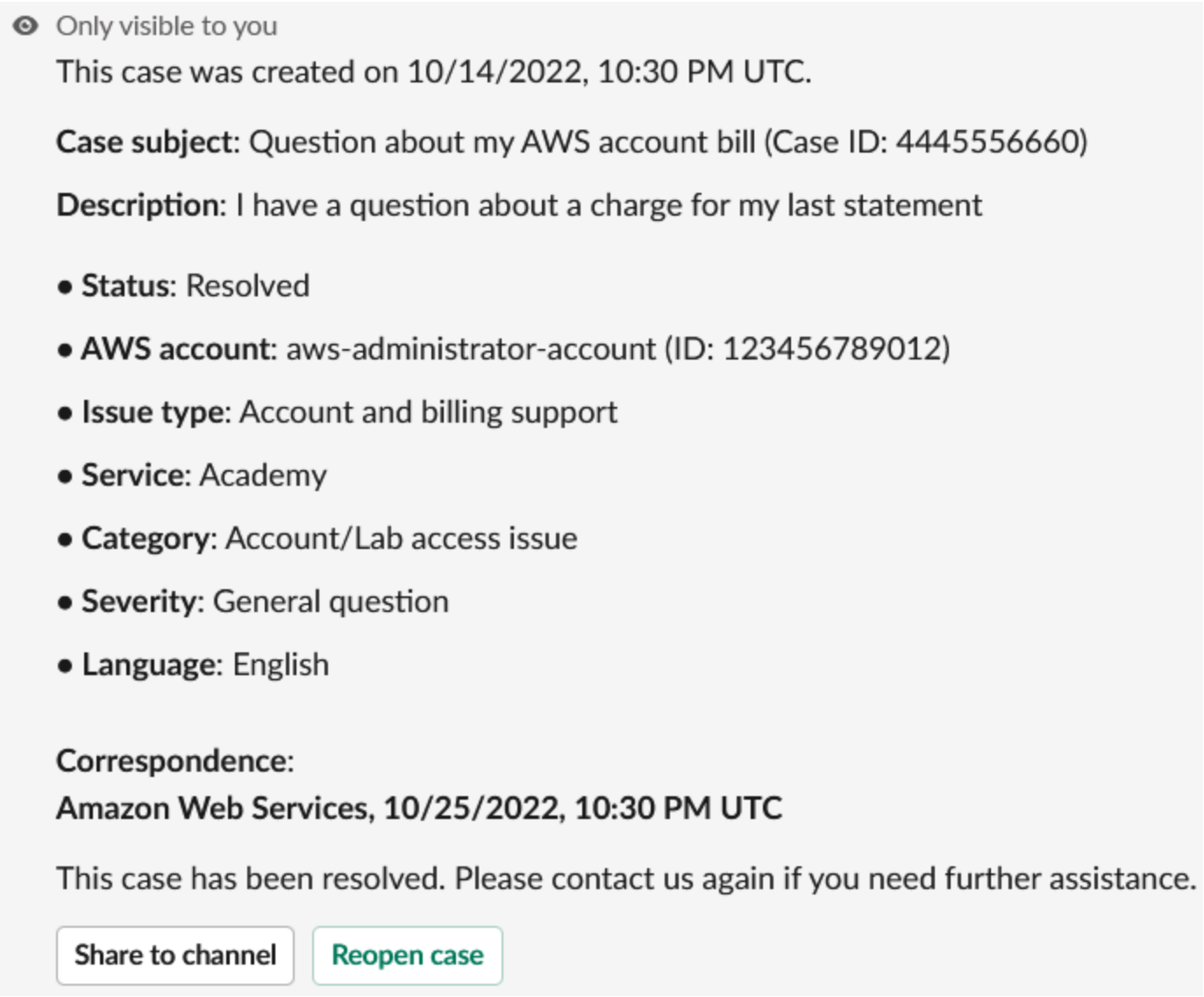
Para utilizar los resultados de búsqueda

1. Seleccione Edit Search (Editar búsqueda) para cambiar las opciones de filtro o el ID del caso anteriores.
2. Elija Share to channel (Compartir en el canal) para compartir los resultados de la búsqueda en el canal.

3. Elija See details (Ver detalles) para ver más información sobre un caso. Puede elegir Show full message (Mostrar mensaje completo) para ver el resto de la correspondencia más reciente.
4. Si buscó por opciones de filtro, los resultados de la búsqueda pueden mostrar varios casos. Elija los 5 resultados siguientes o los 5 resultados anteriores para ver los 5 casos siguientes o anteriores.

Example : resolver un caso de soporte

En el siguiente ejemplo, se muestra un caso de soporte resuelto por un problema de cuenta y facturación tras seleccionar See details (Ver detalles).

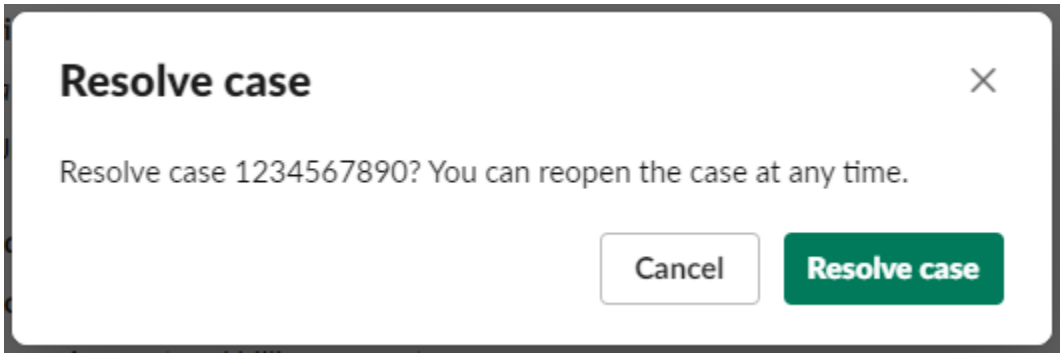


Resolución de un caso de soporte en Slack

Si ya no necesita el caso de soporte o ya solucionó el problema, puede resolverlo directamente en Slack. Esto también resuelve el caso en la AWS Support Center Console. Después de resolver un caso, puede reabrirlo más adelante.

Para resolver un caso de soporte en Slack

1. En su canal de Slack, navegue hasta el caso de soporte. Consulte Búsqueda de casos de soporte en Slack.
2. Elija See details (Ver detalles) del caso.
3. Elija Resolve case (Resolver el caso).
4. En el cuadro de diálogo Resolve case (Resolver caso), elija Resolve case (Resolver caso). Puede reabrir un caso en el canal de Slack o desde la consola del Centro de soporte.

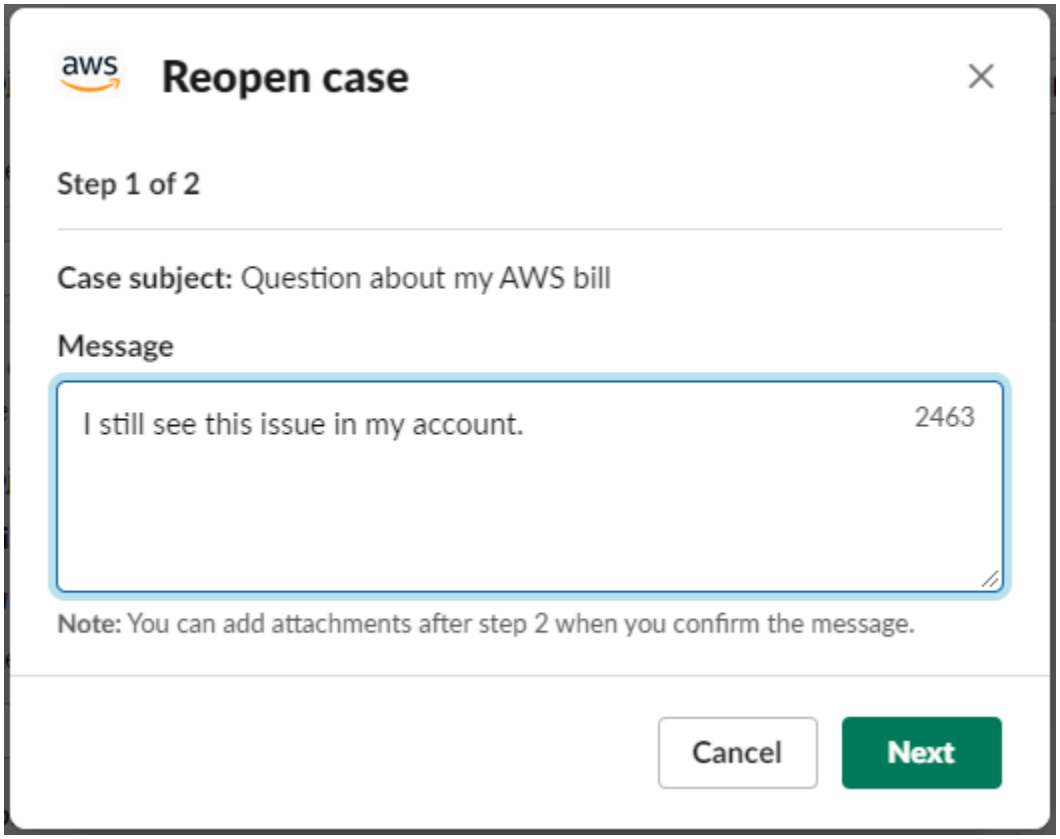


Reapertura de un caso de soporte en Slack

Después de resolver un caso de soporte, puede reabrir el caso desde Slack.

Para reabrir un caso de soporte en Slack

1. Busque el caso de soporte para reabrirlo en Slack. Consulte Búsqueda de casos de soporte en Slack.
2. Elija See details (Ver detalles).
3. Elija Reopen case (Reabrir caso).
4. En el cuadro de diálogo Reopen case (Volver a abrir el caso), ingrese una breve descripción del problema en el campo Message (Mensaje).
5. Elija Next (Siguiente).



6. (Opcional) Ingrese contactos adicionales.
7. Elija Review.
8. Revise los detalles de su caso y, a continuación, elija Send message (Enviar mensaje). El caso se reabre. Si solicitó un chat en vivo nuevo con un agente de soporte, Slack utiliza el mismo canal o hilo de chat que se utilizó para un chat en vivo previo. Si solicitó un chat en vivo en un canal nuevo y aún no se lo han concedido, se abrirá un canal de chat nuevo. Si solicitó un chat en vivo en el canal actual y aún no se lo han concedido, se utilizará un hilo en el canal actual.

Solicitud de aumentos en la cuota de servicio

Puede solicitar aumentos en la cuota de servicio de su cuenta desde su canal de Slack.

Para solicitar aumentos en la cuota de servicio

1. En el canal de Slack, ingrese el comando siguiente:

   ```
   /awssupport quota
   ```

2. En el cuadro de diálogo Increase service quota (Aumentar cuota de servicio), ingrese la siguiente información:

   a. Elija el icono Cuenta de AWS.

   b. Elija el icono Región de AWS.

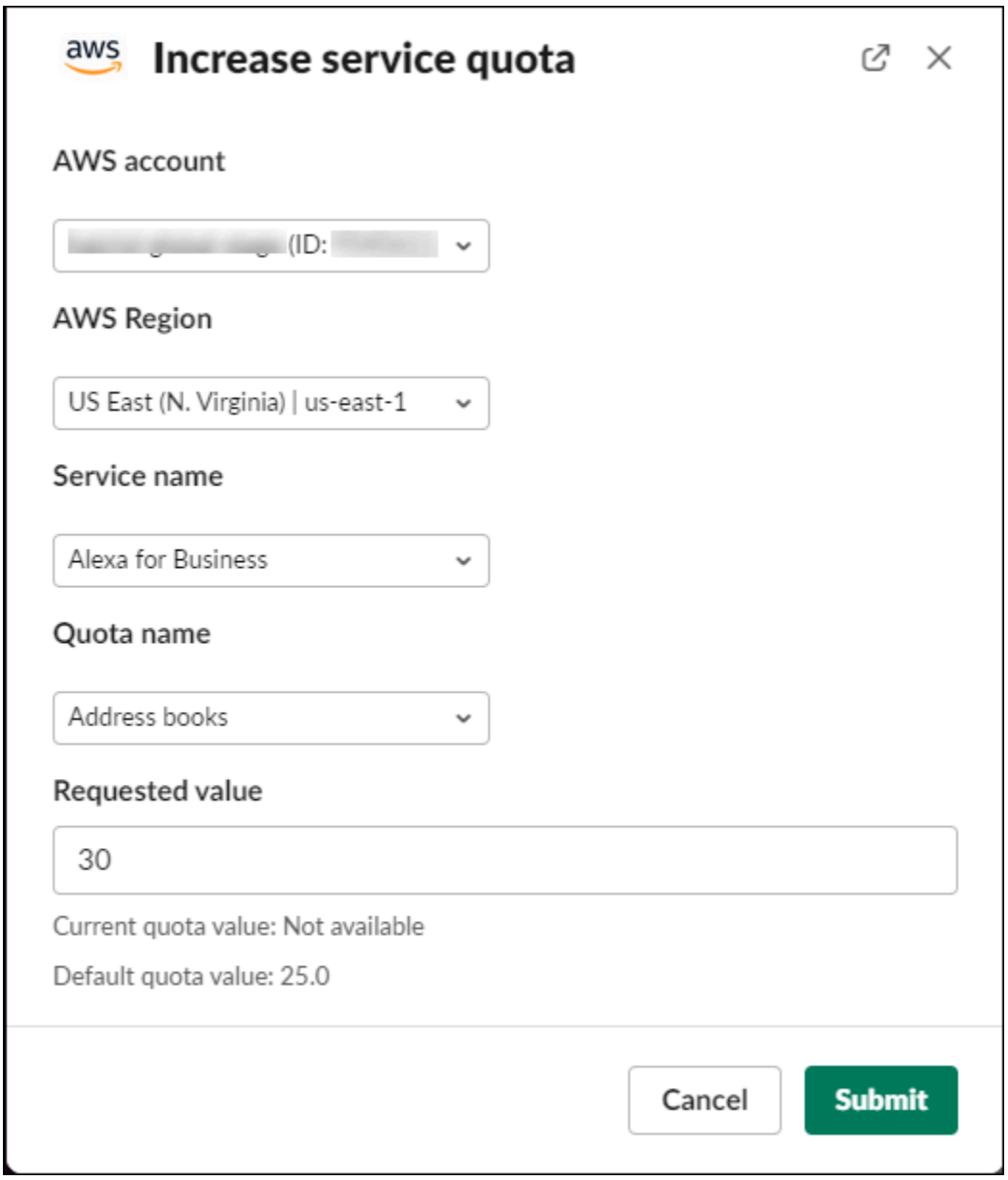
   c. Elija el Service name (Nombre del servicio).

   d. Elija el Quota name (Nombre de la cuota).

   e. Ingrese el Requested value (Valor solicitado) para el aumento de la cuota. Debe ingresar un valor superior a la cuota predeterminada.

3. Elija Submit (Enviar).

Example : aumento en la cuota para Alexa for Business



También puede ver sus solicitudes desde la consola de Service Quotas. Para obtener más información, consulte Solicitud de un aumento de cuota en la Guía del usuario de Service Quotas.

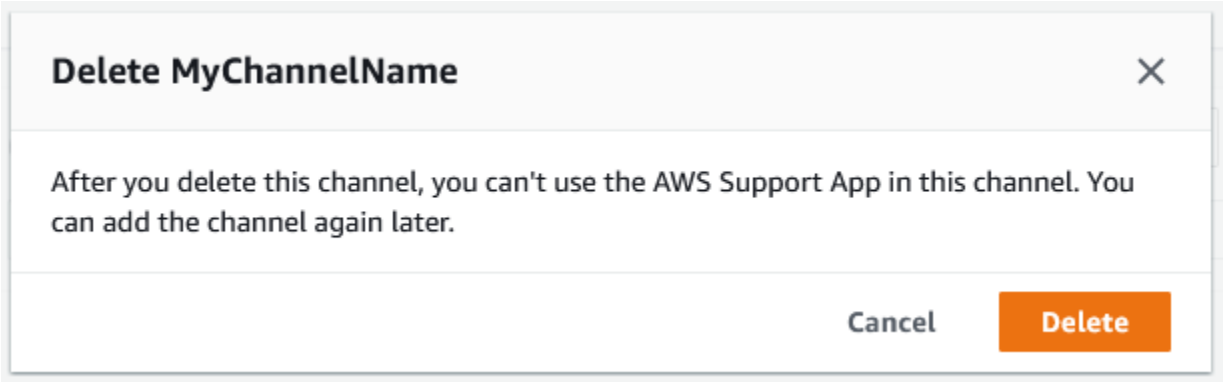
Eliminación de la configuración de un canal de Slack de la aplicación AWS Support

Puede eliminar la configuración de un canal desde la aplicación AWS Support si no la necesita. Esta acción solo elimina el canal de la aplicación AWS Support y la AWS Support Center Console. Su canal no se elimina de Slack.

Puede agregar hasta 20 canales a su Cuenta de AWS. Si ya alcanzó esta cuota, debe eliminar un canal antes de poder agregar otro.

Para eliminar la configuración de un canal de Slack

1. Inicie sesión en la consola del Centro de soporte y elija Slack configuration (Configuración de Slack).
2. En la página Slack configuration (Configuración de Slack), en Channels (Canales), elija el nombre del canal y, a continuación, elija Delete (Eliminar).
3. En el cuadro de diálogo Delete channel name (Eliminar nombre del canal), elija Delete (Eliminar). Puede volver a agregar este canal a la aplicación AWS Support más adelante.



Eliminación de una configuración de espacio de trabajo de Slack de la aplicación AWS Support

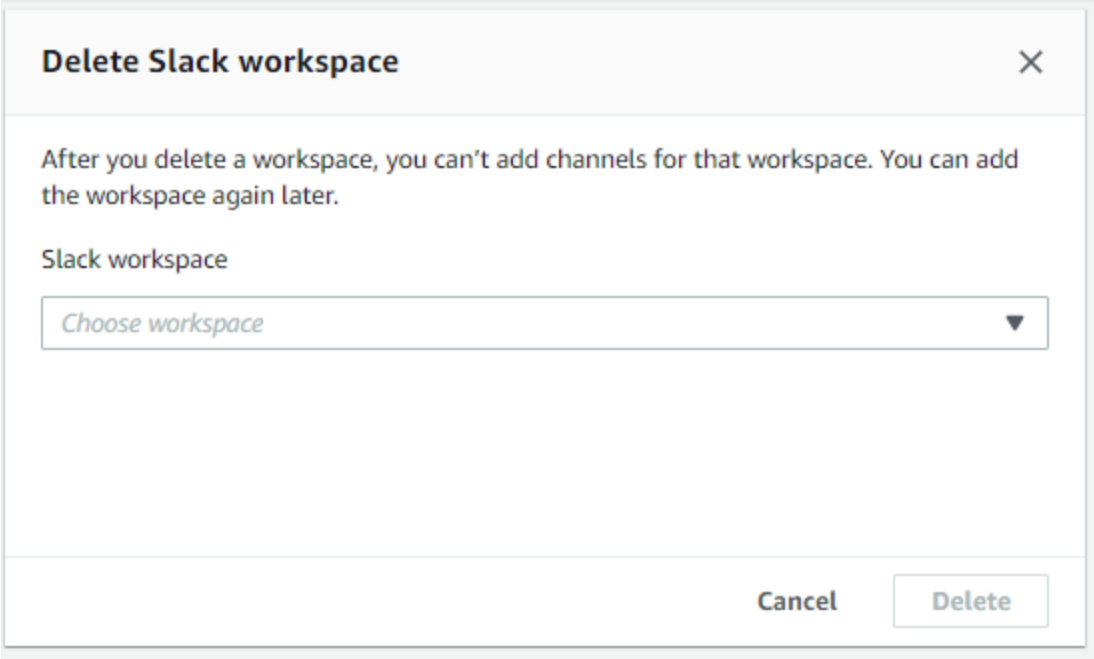
Puede eliminar la configuración de un espacio de trabajo de la aplicación AWS Support si no la necesita. Esta acción solo elimina el espacio de trabajo de la aplicación AWS Support y la AWS Support Center Console. Su espacio de trabajo no se elimina de Slack.

Puede agregar hasta 5 espacios de trabajo en su Cuenta de AWS. Si ya alcanzó esta cuota, debe eliminar un espacio de trabajo de Slack antes de agregar otro.

> **Note**
>
> Si agregó canales de este espacio de trabajo a la aplicación AWS Support, antes debe eliminar estos canales para poder eliminar el espacio de trabajo. Consulte Eliminación de la configuración de un canal de Slack de la aplicación AWS Support.

Para eliminar una configuración de espacio de trabajo de Slack

1. Inicie sesión en la AWS Support Center Console y elija Slack configuration (Configuración de Slack).
2. En la página Slack configuration (Configuración de Slack), en Slack workspaces (Espacios de trabajo de Slack), elija Delete a workspace (Eliminar un espacio de trabajo).
3. En el cuadro de diálogo Delete Slack workspace (Eliminar espacio de trabajo de Slack), elija el nombre del espacio de trabajo de Slack y, a continuación, elija Delete (Eliminar). Puede volver a agregar el espacio de trabajo a su Cuenta de AWS más adelante.



Comandos de la aplicación AWS Support en Slack

Comandos del canal de Slack

Puede ingresar los siguientes comandos en el canal de Slack al que invitó a la aplicación AWS Support. El nombre de este canal de Slack también aparece como canal configurado en la AWS Support Center Console.

`/awssupport create` o `/awssupport create-case`

Cree un caso de soporte.

`/awssupport search` o `/awssupport search-case`

Busque casos. Puede buscar casos de soporte para las Cuentas de AWS que configuró la aplicación AWS Support para el mismo canal de Slack.

`/awssupport quota` o `/awssupport service-quota-increase`

Solicite un aumento de cuota de servicio.

Comandos del canal de chat en vivo

Puede ingresar los siguientes comandos en el canal de chat en vivo. Este es el canal que la aplicación AWS Support crea para usted si desea elegir un canal nuevo para comunicarse con AWS Support Los canales de chat incluyen el ID de su caso de soporte; por ejemplo, *awscase-1234567890*.

> **Note**
>
> Los siguientes comandos no están disponibles cuando se utiliza un hilo en el canal actual para un chat en vivo. En cambio, utilice los botones adjuntos al mensaje inicial del hilo para finalizar un chat, invitar a un agente nuevo o resolver el caso.

`/awssupport endchat`

Elimine al agente de soporte y finalice la sesión de chat en vivo.

`/awssupport invite`

Invite a un nuevo agente de soporte a este canal.

`/awssupport resolve`

Resuelva este caso de soporte.

Ver correspondencias de la aplicación AWS Support en la AWS Support Center Console

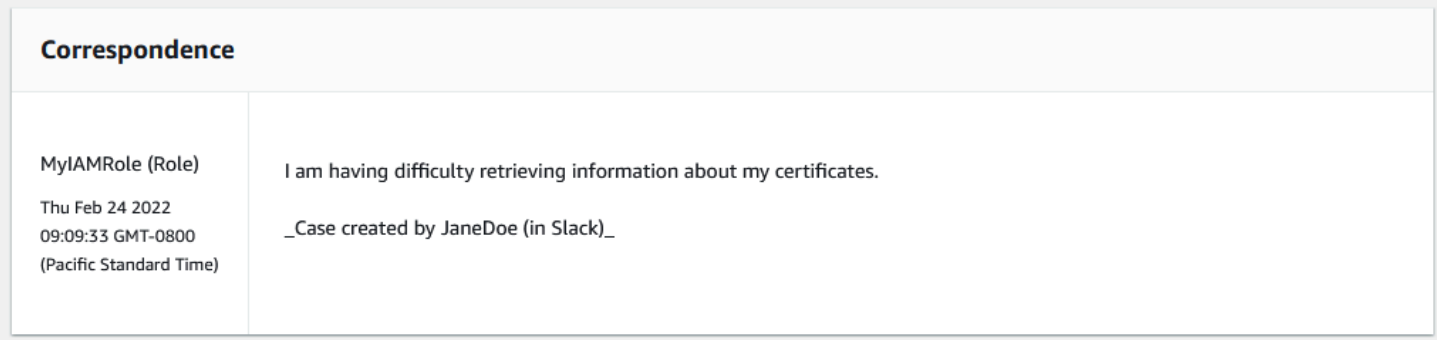
Al crear, actualizar o resolver casos de soporte de su cuenta en el canal de Slack, también puede iniciar sesión en la consola del centro de soporte para ver dichos casos. Puede ver la correspondencia del caso para determinar si este se actualizó en el canal de Slack, ver el historial de conversaciones con un agente de soporte y buscar los archivos adjuntos que haya cargado desde Slack.

Para ver las correspondencias de casos desde Slack

1. Inicie sesión en la AWS Support Center Console de su cuenta.
2. Elija su caso de soporte.
3. En Correspondence (Correspondencia), puede ver si el caso se creó y actualizó desde el canal de Slack.

Example : caso de soporte

En la siguiente captura de pantalla, Jane Doe reabrió un caso de soporte en Slack. Esta correspondencia aparece para el caso de soporte en la consola del centro de soporte.



Creación de recursos de la aplicación AWS Support en Slack con AWS CloudFormation

La aplicación AWS Support en Slack está integrada con AWS CloudFormation, un servicio que le ayuda a modelar y configurar sus recursos de AWS para que pueda dedicar menos tiempo a crear y administrar sus recursos e infraestructura. Puede crear una plantilla que describa todos los recursos de AWS que desea (como AccountAlias y SlackChannelConfiguration) y AWS CloudFormation aprovisiona y configura estos recursos.

Cuando usa AWS CloudFormation, puede reutilizar la plantilla para configurar sus recursos de la aplicación AWS Support de forma coherente y reiterada. Solo tiene que describir los recursos una vez y luego aprovisionar los mismos recursos una y otra vez en varias Cuentas de AWS y regiones.

Aplicación AWS Support y plantillas de AWS CloudFormation

Para aprovisionar y configurar los recursos de la aplicación AWS Support y sus servicios relacionados, debe conocer las plantillas de AWS CloudFormation. Las plantillas son archivos de texto con formato de tipo JSON o YAML. Estas plantillas describen los recursos que desea aprovisionar en sus pilas de AWS CloudFormation. Si no está familiarizado con JSON o YAML, puede utilizar Designer de AWS CloudFormation para comenzar a utilizar las plantillas de AWS CloudFormation. Para obtener más información, consulte ¿Qué es Designer de AWS CloudFormation? en la Guía del usuario de AWS CloudFormation.

La aplicación AWS Support admite la creación de AccountAlias y SlackChannelConfiguration en AWS CloudFormation. Para obtener más información, incluidos ejemplos de plantillas JSON y YAML para estos recursos, consulte la referencia del tipo de recurso de la aplicación AWS Support en la Guía del usuario de AWS CloudFormation.

Creación de recursos de configuración de Slack para su organización

Puede utilizar plantillas de CloudFormation para crear los recursos que necesita para la aplicación AWS Support. Si usted es la cuenta de gestión de su organización, puede utilizar las plantillas para crear estos recursos para sus cuentas miembro en AWS Organizations.

Por ejemplo, puede utilizar una plantilla para crear la misma configuración del área de trabajo de Slack para todas las cuentas de la organización, pero luego utilizar plantillas separadas para crear diferentes configuraciones de canales de Slack para Cuentas de AWS o unidades organizativas (OU)

específicas. También puede utilizar una plantilla para crear una configuración de área de trabajo de Slack para que las cuentas miembro puedan configurar los canales de Slack que deseen para sus Cuentas de AWS.

Puede elegir si desea utilizar plantillas de CloudFormation o no. Si no utiliza plantillas de CloudFormation, puede completar los siguientes pasos manuales en su lugar:

- Cree los recursos de la aplicación AWS Support en la AWS Support Center Console.
- Cree un caso de soporte con AWS Support para autorizar varias cuentas a utilizar la aplicación AWS Support.
- Llame a la operación de la API RegisterSlackWorkspaceForOrganization para registrar un espacio de trabajo de Slack para su cuenta. La pila de CloudFormation denomina a esta operación de API por usted.

Siga estos procedimientos para cargar la plantilla de CloudFormation en su organización. Puede utilizar las plantillas de ejemplo de la página de referencia del tipo de origen de la aplicaciónAWS Support.

Las plantillas le indican a CloudFormation que cree los siguientes recursos:

- Una configuración de canal de Slack.
- Una configuración del área de trabajo de Slack.
- Un rol de IAM con el nombre `AWSSupportSlackAppCFNRole`. Se adjunta la política administrada de AWSSupportAppFullAccess AWS.

Contenido

Actualización de las plantillas de CloudFormation para Slack

Para empezar, utilice las siguientes plantillas para crear la pila. Debe reemplazar las plantillas con valores válidos para su área de trabajo y canal de Slack.

> **Note**
>
> No recomendamos el uso de la plantilla para crear un recurso AccountAlias para su organización. El recurso AccountAlias identifica de forma exclusiva una Cuenta de AWS en la aplicaciónAWS Support. Sus cuentas miembro pueden introducir un nombre de cuenta en la Center Console. Para obtener más información, consulte Autorización de un espacio de trabajo de Slack.

Para actualizar sus plantillas de CloudFormation para Slack

1. Si usted es la cuenta de administración de una organización, debe autorizar manualmente un área de trabajo de Slack para su cuenta antes de que sus cuentas miembro puedan utilizar CloudFormation para crear los recursos. Si aún no lo ha hecho, consulte Autorización de un espacio de trabajo de Slack.
2. En la página de referencia del tipo de origen de la aplicación AWS Support, copie la plantilla JSON o YAML del recurso que desee.
3. En un editor de texto, pegue la plantilla en un archivo nuevo.
4. En la plantilla, especifique los parámetros que desee. Como mínimo, sustituya los valores de los siguientes campos:

   - `TeamId` con el ID de su área de trabajo de Slack
   - `ChannelId` con el ID del canal de Slack
   - `ChannelName` con un nombre para identificar la configuración del canal de Slack

   > **Tip**
   >
   > Para encontrar los ID del espacio de trabajo y del canal, abra su canal de Slack en un navegador. En la URL, el ID de su espacio de trabajo es el primer identificador y el ID del canal es el segundo. Por ejemplo, en https://app.slack.com/client/T012ABCDEFG/C01234A5BCD, T012ABCDEFG es el ID del espacio de trabajo y C01234A5BCD es el ID del canal.

5. Guarde el archivo como archivo JSON o YAML.

Cree una pila para la cuenta de administración

A continuación, debe crear una pila para la cuenta de administración de la organización. Este paso llama a la operación de la API RegisterSlackWorkspaceForOrganization y autoriza el área de trabajo con Slack.

> **Note**
>
> Le recomendamos que cargue la plantilla de configuración del área de trabajo de Slack que actualizó en el procedimiento anterior para la cuenta de administración. No es necesario cargar la plantilla de configuración del canal de Slack a menos que también esté configurando la cuenta de administración para utilizar la aplicación AWS Support.

Para crear una pila para la cuenta de administración

1. Inicie sesión en la AWS Management Console con la cuenta de administración de su organización.
2. Abra la consola de AWS CloudFormation en https://console.aws.amazon.com/cloudformation.
3. Si aún no lo ha hecho, en el Region selector (Selector de regiones), elija una de las siguientes Regiones de AWS:
   - Europa (Fráncfort)
   - Europa (Irlanda)
   - Europa (Londres)
   - Este de EE. UU. (Norte de Virginia)
   - Este de EE. UU. (Ohio)
   - Oeste de EE. UU. (Oregón)
   - Asia-Pacífico (Singapur)
   - Asia-Pacífico (Tokio)
   - Canadá (centro)
4. Siga el procedimiento para crear una pila. Para más información, consulte Creación de una pila en la consola de AWS CloudFormation.

   Después de que CloudFormation cree correctamente la pila, puede utilizar la misma plantilla para crear un conjunto de pilas para su organización.

Creación de un conjunto de pilas para su organización

A continuación, utilice la misma plantilla para la configuración del área de trabajo de Slack para crear un conjunto de pilas con permisos `service-managed`. Puede utilizar conjuntos de pilas para crear la pila para toda su organización o especificar las OU que desee. Para más información, consulte Creación de un conjunto de pila.

Este procedimiento también llama a la operación API RegisterSlackWorkspaceForOrganization. Esta operación de API autoriza el área de trabajo con Slack para las cuentas de los miembros.

Para crear un conjunto de pilas para su organización

1. Inicie sesión en la AWS Management Console con la cuenta de administración de su organización.
2. Abra la consola de AWS CloudFormation en https://console.aws.amazon.com/cloudformation.
3. Si aún no lo ha hecho, en el Region selector, elija la misma Región de AWS que utilizó en el procedimiento anterior.
4. En el panel de navegación, seleccione StackSets.
5. Seleccione Create StackSet (Crear StackSet).
6. En la página Choose a template (Elegir una plantilla), mantenga las opciones predeterminadas para las siguientes opciones:
   - En Permissions (Permisos), elija Service-managed permissions (Permisos administrados por servicios).
   - En Prerequisite - Prepare template (Requisito previo: preparar la plantilla), mantenga Template is ready (La plantilla está lista).
7. Para Specify template (Especificar plantilla), seleccione Upload a template file (Actualizar un archivo de plantilla) y, a continuación, elija Choose file (Elegir archivo).
8. Elija el archivo YAML y después elija Next (Siguiente).
9. En la página Specify StackSet details (Especificar detalles de StackSet), introduzca un nombre de pila como **`support-app-slack-workspace`**, introduzca una descripción y, a continuación, seleccione Next (Siguiente).
10. En la página Configure StackSet options (Configurar opciones de StackSet), mantenga las opciones predeterminadas y elija Next (Siguiente).

11. En la página Set deployment options (Configurar opciones de implementación), en Add stacks to stack set (Agregar pilas al conjunto de pilas), mantenga la opción predeterminada Deploy new stacks (Implementar nuevas pilas).
12. En Deployment targets (Destinos de implementación), elija si desea crear la pila para toda la organización o para OU específicas Si elige una OU, introduzca el ID de la OU.
13. En Specify regions (Especificar regiones), introduzca solo una de las siguientes opcionesRegiones de AWS:

    - Europa (Fráncfort)
    - Europa (Irlanda)
    - Europa (Londres)
    - Este de EE. UU. (Norte de Virginia)
    - Este de EE. UU. (Ohio)
    - Oeste de EE. UU. (Oregón)
    - Asia-Pacífico (Singapur)
    - Asia-Pacífico (Tokio)
    - Canadá (centro)

    > Notas:
    >
    > - Para agilizar su flujo de trabajo, le recomendamos que utilice la misma Región de AWS que eligió en el paso 3.
    > - Elegir más de una Región de AWS puede causar conflictos con la creación de su pila.

14. En las Deployment options (opciones de implementación), en Failure tolerance: optional (Tolerancia a fallos: opcional), introduzca el número de cuentas en las que las pilas pueden fallar antes de que CloudFormation detenga la operación. Le recomendamos que introduzca el número de cuentas que desea agregar, menos uno. Por ejemplo, si su OU especificada tiene 10 cuentas miembro, introduzca 9. Esto significa que aunque CloudFormation falle la operación 9 veces, al menos una cuenta tendrá éxito.
15. Elija Next (Siguiente).
16. En la página Review (Revisar), revise las opciones y seleccione Submit (Enviar). Puede comprobar el estado de su pila en la pestaña Stack instances (Instancias de pila).

17. ((Opcional) Repita este procedimiento para cargar una plantilla para la configuración de un canal de Slack. La plantilla de ejemplo también crea el rol de IAM y adjunta una política administrada de AWS. Este rol tiene los permisos necesarios para acceder a otros servicios en su nombre. Para obtener más información, consulte Administración del acceso a la aplicación AWS Support.

    Si no crea un conjunto de pilas para crear la configuración del canal de Slack, sus cuentas miembro pueden configurar manualmente el canal de Slack. Para obtener más información, consulte Configuración de un canal de Slack.

Después de que CloudFormation cree las pilas, cada cuenta miembro puede iniciar sesión en la Support Center Console y encontrar sus áreas de trabajo y canales de Slack configurados. A continuación, pueden utilizar la aplicación AWS Support para su Cuenta de AWS. Consulte Creación de casos de soporte en un canal de Slack.

> **Tip**
>
> Si necesita cargar una plantilla nueva, le recomendamos que utilice la misma Región de AWS que especificó anteriormente.

Más información sobre CloudFormation

Para obtener más información acerca de CloudFormation, consulte los siguientes recursos:

- AWS CloudFormation
- Guía del usuario de AWS CloudFormation
- Referencia de la API de AWS CloudFormation
- Guía del usuario de la interfaz de la línea de comandos de AWS CloudFormation

Crear recursos de AWS Support mediante Terraform

También puede utilizar Terraform para crear los recursos de la aplicación AWS Support para su Cuenta de AWS. Terraform es una herramienta de infraestructura como código que puede utilizar para sus aplicaciones en la nube. Puede utilizar Terraform para crear recursos de la aplicación AWS Support en lugar de implementar una pila de CloudFormation en una cuenta.

Después de instalar Terraform, puede especificar los recursos de la aplicación AWS Support que desee. Terraform llama a la operación de API RegisterSlackWorkspaceForOrganization para registrar un espacio de trabajo de Slack para usted y crea sus recursos. A continuación, puede iniciar sesión en la Support Center Console y encontrar sus áreas de trabajo y canales de Slack configurados.

Notas

- Si es la cuenta de administración de una organización, debe autorizar manualmente un área de trabajo de Slack para su cuenta antes de que sus cuentas miembro puedan utilizar Terraform para crear los recursos. Si aún no lo ha hecho, consulte Autorización de un espacio de trabajo de Slack.
- A diferencia de los conjuntos de pilas de CloudFormation, no puede utilizar Terraform para crear los recursos de la aplicación AWS Support para una OU de su organización.
- También puede encontrar el historial de eventos para estas actualizaciones de Terraform en AWS CloudTrail. El `eventSource` para estos eventos será `cloudcontrolapi.amazonaws.com` y `supportapp.amazonaws.com`. Para obtener más información, consulte Registro de llamadas a la API de la aplicación AWS Support en Slack mediante AWS CloudTrail.

Más información

Para más información sobre Terraform, consulte los siguientes temas:

- Instalación de Terraform
- Tutorial de Terraform: cree infraestructura para AWS
- `awscc_support_app_account_alias`
- `awscc_supportapp_slack_workspace_configuration`
- `awscc_supportapp_slack_channel_configuration`

Seguridad en AWS Support

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

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

- Seguridad de la nube: AWS es responsable de proteger la infraestructura que ejecuta AWS los servicios en la AWS nube. 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 conformidad aplicables AWS Support, consulte AWS los servicios incluidos en el ámbito de aplicación por programa de conformidad .
- 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 Support. Los siguientes temas muestran cómo configurarlo AWS Support para cumplir sus objetivos de seguridad y conformidad. También aprenderá a utilizar otros Amazon Web Services que le ayudan a supervisar y proteger sus AWS Support recursos.

Temas

Protección de datos en AWS Support

El modelo de responsabilidad AWS compartida modelo se aplica a la protección de datos en AWS Support. 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 Support 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 información de credenciales en la URL a fin de validar la solicitud para ese servidor.

Seguridad para sus casos AWS Support

Al crear un caso de soporte, usted es el propietario de la información que incluye en él. AWS no accede a tus Cuenta de AWS datos sin tu permiso. AWS no comparte su información con terceros.

Cuando cree un caso de soporte, tenga en cuenta lo siguiente:

- AWS Support utiliza los permisos definidos en la función `AWSServiceRoleForSupport` vinculada al servicio para llamar a otras personas Servicios de AWS que se encarguen de solucionar los problemas de los clientes por usted. Para obtener más información, consulte Uso de roles vinculados al servicio y políticas administradas:. AWS SupportAWS AWSSupportServiceRolePolicy
- Puede ver las llamadas a la API AWS Support que se produjeron en su. Cuenta de AWS Por ejemplo, puede ver la información de registro cuando un usuario de su cuenta crea o resuelve un caso de soporte. Para obtener más información, consulta Registrar llamadas a la AWS Support API con AWS CloudTrail.
- Puedes usar la AWS Support API para llamar a la `DescribeCases` API. Esta API devuelve información sobre el caso de soporte, como el ID del caso, la fecha de creación y resolución, y las correspondencias con el agente de soporte. Puede ver los detalles del caso hasta 12 meses después de su creación. Para obtener más información, consulta DescribeCasesla referencia de la AWS Support API.
- Sus casos de soporte siguen la Validación de la conformidad en AWS Support.
- Cuando creas un caso de soporte, AWS no accede a tu cuenta. Si es necesario, los agentes de soporte usan una herramienta para compartir la pantalla con el fin de verla de forma remota e identificar y solucionar problemas. Esta herramienta es de solo lectura. AWS Support no puede actuar en su nombre durante la sesión de pantalla compartida. Debe dar su consentimiento para compartir pantalla con un agente de soporte. Para obtener más información, consulte las preguntas frecuentes acerca de AWS Support.
- Puedes cambiar tu AWS Support plan para obtener la ayuda que necesitas para tu cuenta. Para obtener más información, consulta Comparar AWS Support planes y Cambiar tu AWS Support plan.

Administración de identidad y acceso para AWS Support

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 Support La IAM es una Servicio de AWS opción que puede utilizar sin coste adicional.

Temas

Público

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

Usuario del servicio: si utiliza el AWS Support servicio para realizar su trabajo, el administrador le proporcionará las credenciales y los permisos que necesita. A medida que vaya utilizando más AWS Support 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 Support, consulte Solución de problemas de AWS Support identidad y acceso.

Administrador de servicios: si estás a cargo de AWS Support los recursos de tu empresa, probablemente tengas acceso total a ellos AWS Support. Su trabajo consiste en determinar a qué AWS Support 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 Support, consulte¿Cómo AWS Support 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 Support basadas en la identidad que puede utilizar en IAM, consulte. AWS Support 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 AWSen la Guía del usuario de IAM.

AWS usuario raíz de la cuenta

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.

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 obtener información acerca de la diferencia entre los roles y las políticas basadas en recursos para el acceso entre cuentas, consulte Cómo los roles de IAM difieren de las políticas basadas en recursos en la Guía del usuario de IAM.
- Acceso entre servicios: algunos Servicios de AWS utilizan funciones en otros Servicios de AWS. Por ejemplo, cuando realiza una llamada en un servicio, es común que ese servicio ejecute aplicaciones en Amazon EC2 o almacene objetos en Amazon S3. Es posible que un servicio haga esto usando los permisos de la entidad principal, usando un rol de servicio o usando un rol vinculado 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.

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 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 Support funciona con IAM

Antes de utilizar IAM para gestionar el acceso AWS Support, debe comprender las funciones de IAM disponibles para su uso. AWS SupportPara obtener una visión general de cómo funcionan con IAM AWS Support y otros AWS servicios, consulte los AWS servicios que funcionan con IAM en la Guía del usuario de IAM.

Para obtener información sobre cómo administrar el acceso para AWS Support usar IAM, consulte Administrar el acceso para. AWS Support

Temas

- Políticas de AWS Support basadas en identidades

- AWS Support Funciones de IAM

Políticas de AWS Support basadas en identidades

Con las políticas basadas en identidades de IAM, puede especificar los recursos y las acciones permitidas o denegadas, así como las condiciones en las que se permiten o deniegan las acciones. AWS Support es compatible con acciones específicas. Para obtener más información acerca de los elementos que utiliza en una política de JSON, consulte Referencia de los elementos de las políticas de JSON de IAM en la Guía del usuario de IAM.

Acciones

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 Support utilizan el siguiente prefijo antes de la acción:`support:`. Por ejemplo, para conceder a alguien permiso para ejecutar una instancia de Amazon EC2 con la operación `RunInstances` de la API de Amazon EC2, debe incluir la acción `ec2:RunInstances` en la política. Las instrucciones de política deben incluir un elemento `Action` o `NotAction`. AWS Support define su propio conjunto de acciones que describen las tareas que se pueden realizar con este servicio.

Para especificar varias acciones en una única instrucción, sepárelas con comas del siguiente modo:

```
"Action": [
      "ec2:action1",
      "ec2:action2"
```

Puede utilizar caracteres comodín para especificar varias acciones (*). Por ejemplo, para especificar todas las acciones que comiencen con la palabra `Describe`, incluya la siguiente acción:

```
"Action": "ec2:Describe*"
```

Para ver una lista de AWS Support acciones, consulte las acciones definidas por AWS Support en la Guía del usuario de IAM.

Ejemplos

Para ver ejemplos de políticas AWS Support basadas en la identidad, consulte. AWS Support ejemplos de políticas basadas en la identidad

AWS Support Funciones de IAM

Un rol de IAM es una entidad de tu AWS cuenta que tiene permisos específicos.

Usar credenciales temporales con AWS Support

Puede utilizar credenciales temporales para iniciar sesión con federación, asumir un rol de IAM o asumir un rol de acceso entre cuentas. Las credenciales de seguridad temporales se obtienen llamando a operaciones de AWS STS API como AssumeRoleo GetFederationToken.

AWS Support admite el uso de credenciales temporales.

Roles vinculados al servicio

Las funciones vinculadas al servicio permiten a AWS los servicios acceder a los recursos de otros servicios para completar una acción en su nombre. Los roles vinculados a servicios aparecen en la cuenta de IAM y son propiedad del servicio. Un administrador de IAM puede ver, pero no editar, los permisos de los roles vinculados a servicios.

AWS Support admite funciones vinculadas al servicio. Para obtener más información sobre la creación o la administración de funciones AWS Support vinculadas a servicios, consulte. Uso de roles vinculados a servicios de AWS Support

Roles de servicio

Esta característica permite que un servicio asuma un rol de servicio en su nombre. Este rol permite que el servicio obtenga acceso a los recursos de otros servicios para completar una acción en su nombre. Los roles de servicio aparecen en su cuenta de IAM y son propiedad de la cuenta. Esto significa que un administrador de IAM puede cambiar los permisos de este rol. Sin embargo, hacerlo podría deteriorar la funcionalidad del servicio.

AWS Support admite funciones de servicio.

AWS Support ejemplos de políticas basadas en la identidad

De forma predeterminada, los usuarios y los roles de IAM no tienen permiso para crear, ver ni modificar recursos de AWS Support . 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 adjuntar esas políticas a los usuarios o grupos de IAM que necesiten esos permisos.

Para obtener más información acerca de cómo crear una política basada en identidad de IAM con estos documentos de políticas de 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 Support
- Permitir a los usuarios consultar sus propios permisos

Prácticas recomendadas relativas a políticas

Las políticas basadas en identidad son muy eficaces. Determinan si alguien puede crear AWS Support recursos de tu cuenta, acceder a ellos o eliminarlos. Siga estas directrices y recomendaciones al crear o editar políticas basadas en identidades:

- Comience a utilizar las políticas AWS gestionadas: para empezar a AWS Support utilizarlas rápidamente, utilice las políticas AWS gestionadas para conceder a sus empleados los permisos que necesitan. Estas políticas ya están disponibles en su cuenta, y las mantiene y actualiza AWS. Para obtener más información, consulte Cómo empezar a usar permisos con políticas AWS administradas en la Guía del usuario de IAM.
- Conceder privilegios mínimos: al crear políticas personalizadas, conceda solo los permisos necesarios para llevar a cabo una tarea. Comience con un conjunto mínimo de permisos y conceda permisos adicionales según sea necesario. Por lo general, es más seguro que comenzar con permisos demasiado tolerantes e intentar hacerlos más estrictos más adelante. Para obtener más información, consulte Conceder privilegios mínimos en la Guía del usuario de IAM.
- Habilitar MFA para operaciones confidenciales: para mayor seguridad, obligue a los usuarios de IAM a que utilicen la autenticación multifactor (MFA) para acceder a recursos u operaciones de API

confidenciales. Para obtener más información, consulte Uso de la autenticación multifactor (MFA) en AWS en la Guía del usuario de IAM.

- Utilizar condiciones de política para mayor seguridad: en la medida en que sea práctico, defina las condiciones en las que sus políticas basadas en identidad permitan el acceso a un recurso. Por ejemplo, puede escribir condiciones para especificar un rango de direcciones IP permitidas desde el que debe proceder una solicitud. También puede escribir condiciones para permitir solicitudes solo en un intervalo de hora o fecha especificado o para solicitar el uso de SSL o MFA. Para obtener más información, consulte Elementos de la política JSON de IAM: condición en la Guía del usuario de IAM.

Mediante la consola de AWS Support

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

Para asegurarse de que esas entidades puedan seguir utilizando la AWS Support consola, adjunte también la siguiente política AWS administrada a las entidades. Para obtener más información, consulte Agregar 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:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

Uso de roles vinculados a servicios

AWS Support y AWS Trusted Advisor utilice funciones vinculadas al AWS Identity and Access Management servicio (IAM). Un rol vinculado al servicio es un rol de IAM único que está vinculado directamente a y. AWS Support Trusted Advisor En cada caso, el rol vinculado a un servicio es un rol predefinido. Esta función incluye todos los permisos AWS Support o requisitos para llamar Trusted Advisor a otros AWS servicios en su nombre. En los temas siguientes se explica lo que hacen las funciones vinculadas a los servicios y cómo trabajar con ellas en AWS Support y. Trusted Advisor

Temas

- Uso de roles vinculados a servicios de AWS Support
- Uso de roles vinculados a servicios de Trusted Advisor

Uso de roles vinculados a servicios de AWS Support

AWS Support las herramientas recopilan información sobre sus AWS recursos mediante llamadas a la API para proporcionar servicio al cliente y soporte técnico. Para aumentar la transparencia y la auditabilidad de las actividades de soporte, AWS Support utiliza una función vinculada al servicio AWS Identity and Access Management (IAM).

La función `AWSServiceRoleForSupport` vinculada al servicio es una función de IAM única a la que se vincula directamente. AWS Support Esta función vinculada al servicio está predefinida e incluye los permisos necesarios para llamar a otros AWS servicios AWS Support en su nombre.

El rol vinculado a servicios `AWSServiceRoleForSupport` confía en el servicio `support.amazonaws.com` para asumir el rol.

Para proporcionar estos servicios, los permisos predefinidos de la función permiten AWS Support acceder a los metadatos de los recursos, no a los datos de los clientes. Solo AWS Support las herramientas pueden asumir esta función, que existe en tu AWS cuenta.

Redactamos campos que podrían contener datos de clientes. Por ejemplo, los `Output` campos `Input` y del GetExecutionhistorial de la llamada a la AWS Step Functions API no están visibles para ellos AWS Support. Usamos AWS KMS keys para cifrar los campos confidenciales. Estos campos están redactados en la respuesta de la API y los AWS Support agentes no los ven.

> **Note**
>
> AWS Trusted Advisor utiliza un rol independiente vinculado al servicio de IAM para acceder a AWS los recursos de tu cuenta y ofrecer recomendaciones y comprobaciones sobre las mejores prácticas. Para obtener más información, consulte Uso de roles vinculados a servicios de Trusted Advisor.

La función `AWSServiceRoleForSupport` vinculada al servicio permite que los clientes puedan ver todas las llamadas a la AWS Support API. AWS CloudTrail Esto ayuda a cumplir con los requisitos de supervisión y auditoría, ya que proporciona una forma transparente de entender las acciones que se llevan a AWS Support cabo en su nombre. Para obtener información al respecto CloudTrail, consulte la Guía AWS CloudTrail del usuario.

Permisos de roles vinculados a servicios de AWS Support

Este rol usa la política `AWSSupportServiceRolePolicy` AWS gestionada. Esta política administrada está adjunta al rol y permite que el permiso del rol lleve a cabo acciones en su nombre.

Estas acciones pueden incluir las siguientes:

- Servicios de facturación, administrativos, de soporte y otros servicios al AWS cliente: el servicio de atención al cliente utiliza los permisos otorgados por la política gestionada para prestar una serie de servicios como parte de su plan de soporte. Esto incluye investigar y responder a preguntas relacionadas con la cuenta y la facturación, proporcionar soporte administrativo para la cuenta, aumentar las cuotas de servicio y ofrecer otros tipos de atención al cliente.
- Procesamiento de los atributos del servicio y los datos de uso de tu AWS cuenta: AWS Support es posible que utilices los permisos otorgados por la política gestionada para acceder a los atributos del servicio y a los datos de uso de tu AWS cuenta. Esta política te AWS Support permite proporcionar asistencia técnica, administrativa y de facturación para tu cuenta. Los atributos de servicio incluyen los identificadores de recursos, las etiquetas de metadatos, los roles y los permisos de su cuenta. Los datos de uso incluyen las políticas de uso, las estadísticas de uso y los análisis.
- Mantener el estado operativo de su cuenta y sus recursos: AWS Support utiliza herramientas automatizadas para realizar acciones relacionadas con el soporte operativo y técnico.

Para obtener más información sobre los servicios y acciones permitidos, consulte la política de AWSSupportServiceRolePolicy en la consola de IAM.

> **Note**
>
> AWS Support actualiza automáticamente la `AWSSupportServiceRolePolicy` política una vez al mes para añadir permisos para nuevos AWS servicios y acciones.

Para obtener más información, consulte AWS políticas gestionadas para AWS Support.

Crear un rol vinculado a un servicio para AWS Support

No necesita crear manualmente un rol `AWSServiceRoleForSupport`. Al crear una AWS cuenta, este rol se crea y configura automáticamente para usted.

> **Important**
>
> Si lo utilizaste AWS Support antes de que empezara a admitir roles vinculados al servicio, entonces AWS creaste el `AWSServiceRoleForSupport` rol en tu cuenta. Para obtener más información, consulte Un nuevo rol ha aparecido en la cuenta de IAM.

Editar y eliminar un rol vinculado a un servicio para AWS Support

Puede utilizar IAM para editar la descripción del rol vinculado a servicio `AWSServiceRoleForSupport`. Para obtener más información, consulte Editar un rol vinculado a servicios en la Guía del usuario de IAM.

El `AWSServiceRoleForSupport` rol es necesario AWS Support para proporcionar soporte administrativo, operativo y técnico a su cuenta. Como resultado, este rol no se puede eliminar a través de la consola, la API o AWS Command Line Interface (AWS CLI) de IAM. De esta forma, se protege su cuenta de AWS , ya que usted no podrá eliminar accidentalmente los permisos necesarios para administrar los servicios de soporte.

Para obtener más información sobre el rol de `AWSServiceRoleForSupport` o sus usos, póngase en contacto con AWS Support.

Uso de roles vinculados a servicios de Trusted Advisor

AWS Trusted Advisor usa el rol vinculado al AWS Identity and Access Management servicio (IAM). Un rol vinculado a un servicio es un rol de IAM único al que se vincula directamente. AWS Trusted Advisor Los roles vinculados al servicio están predefinidos e incluyen todos los permisos que el servicio requiere para llamar a otros AWS servicios en tu nombre. Trusted Advisor Trusted Advisor utiliza esta función para comprobar su uso AWS y ofrecer recomendaciones para mejorar su AWS entorno. Por ejemplo, Trusted Advisor analiza el uso de sus instancias de Amazon Elastic Compute Cloud (Amazon EC2) para ayudarle a reducir los costes, aumentar el rendimiento, tolerar los fallos y mejorar la seguridad.

> **Note**
>
> AWS Support utiliza una función independiente vinculada al servicio de IAM para acceder a los recursos de su cuenta y proporcionar servicios de facturación, administrativos y de soporte. Para obtener más información, consulte Uso de roles vinculados a servicios de AWS Support.

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

Temas

- Permisos de roles vinculados a servicios de Trusted Advisor
- Administración de permisos de roles vinculados a servicios
- Creación de un rol vinculado a un servicio de Trusted Advisor
- Modificación de un rol vinculado a servicios de Trusted Advisor
- Eliminación de un rol vinculado a un servicio de Trusted Advisor

Permisos de roles vinculados a servicios de Trusted Advisor

Trusted Advisor utiliza dos funciones vinculadas al servicio:

- AWSServiceRoleForTrustedAdvisor— Esta función confía en que el Trusted Advisor servicio asuma la función de acceder a AWS los servicios en su nombre. La política de permisos del rol permite el acceso Trusted Advisor de solo lectura a todos AWS los recursos. Esta función simplifica la tarea de empezar a utilizar tu AWS cuenta, ya que no tienes que añadir los permisos necesarios para ella. Trusted Advisor Cuando abres una AWS cuenta, Trusted Advisor crea este rol para ti. Los permisos definidos incluyen la política de confianza y la política de permisos. No se puede adjuntar la política de permisos a ninguna otra entidad de IAM.

  Para obtener más información sobre la política adjunta, consulte AWSTrustedAdvisorServiceRolePolicy.
- AWSServiceRoleForTrustedAdvisorReporting: este rol confía en el servicio de Trusted Advisor para asumir el rol de la característica de vista organizativa. Esta función se habilita Trusted Advisor como un servicio de confianza en su AWS Organizations organización. Trusted Advisor crea este rol para usted cuando habilita la vista organizacional.

  Para obtener más información sobre la política adjunta, consulte AWSTrustedAdvisorReportingServiceRolePolicy.

  Puede utilizar la vista organizativa para crear informes y Trusted Advisor comprobar los resultados de todas las cuentas de la organización. Para obtener más información acerca de esta característica, consulte Vista organizativa para AWS Trusted Advisor.

Administración de permisos de roles vinculados a servicios

Debe configurar permisos para permitir a una entidad de IAM (como un usuario, grupo o rol) crear, editar o eliminar un rol vinculado a servicios. En los siguientes ejemplos, se utiliza el rol vinculado a servicio de `AWSServiceRoleForTrustedAdvisor`.

Example : permitir que una entidad de IAM cree el rol vinculado a servicio de **`AWSServiceRoleForTrustedAdvisor`**

Este paso solo es necesario si la Trusted Advisor cuenta está deshabilitada, se elimina el rol vinculado al servicio y el usuario debe volver a crear el rol para volver a habilitarlo. Trusted Advisor

Agregue la siguiente instrucción a la política de permisos de la entidad de IAM para crear el rol vinculado al servicio.

```
{
    "Effect": "Allow",
    "Action": [
        "iam:CreateServiceLinkedRole",
        "iam:PutRolePolicy"
    ],
    "Resource": "arn:aws:iam::*:role/aws-service-role/trustedadvisor.amazonaws.com/
AWSServiceRoleForTrustedAdvisor*",
    "Condition": {"StringLike": {"iam:AWSServiceName": "trustedadvisor.amazonaws.com"}}
}
```

Example : permitir a una entidad de IAM editar la descripción del rol vinculado a servicio **`AWSServiceRoleForTrustedAdvisor`**

Solo puede editar la descripción para el rol de `AWSServiceRoleForTrustedAdvisor`. Puede agregar la siguiente instrucción a la política de permisos de la entidad de IAM para editar la descripción del rol vinculado al servicio.

```
{
    "Effect": "Allow",
    "Action": [
        "iam:UpdateRoleDescription"
    ],
    "Resource": "arn:aws:iam::*:role/aws-service-role/trustedadvisor.amazonaws.com/
AWSServiceRoleForTrustedAdvisor*",
    "Condition": {"StringLike": {"iam:AWSServiceName": "trustedadvisor.amazonaws.com"}}
}
```

Example : permitir a una entidad de IAM eliminar el rol vinculado a servicio de **`AWSServiceRoleForTrustedAdvisor`**

Puede agregar la siguiente instrucción a la política de permisos de la entidad de IAM para eliminar el rol vinculado al servicio.

```
{
    "Effect": "Allow",
    "Action": [
        "iam:DeleteServiceLinkedRole",
        "iam:GetServiceLinkedRoleDeletionStatus"
    ],
    "Resource": "arn:aws:iam::*:role/aws-service-role/trustedadvisor.amazonaws.com/
AWSServiceRoleForTrustedAdvisor*",
    "Condition": {"StringLike": {"iam:AWSServiceName": "trustedadvisor.amazonaws.com"}}
}
```

También puede usar una política AWS administrada, por ejemplo, para proporcionar AdministratorAccessacceso total a. Trusted Advisor

Creación de un rol vinculado a un servicio de Trusted Advisor

No necesita crear manualmente el rol vinculado al servicio `AWSServiceRoleForTrustedAdvisor`. Al abrir una AWS cuenta, Trusted Advisor crea automáticamente el rol vinculado al servicio.

> **Important**
>
> Si utilizabas el Trusted Advisor servicio antes de que comenzara a admitir roles vinculados al servicio, entonces Trusted Advisor ya creaste el `AWSServiceRoleForTrustedAdvisor` rol en tu cuenta. Para obtener más información, consulte Un nuevo rol ha aparecido en mi cuenta de IAM en la Guía del usuario de IAM.

Si su cuenta no tiene el rol vinculado a servicio `AWSServiceRoleForTrustedAdvisor`, Trusted Advisor no funcionará según lo previsto. Esto podría ocurrir si alguien desactivara Trusted Advisor en su cuenta y, a continuación, eliminara el rol vinculado al servicio. En este caso, puede utilizar IAM para crear el rol vinculado al servicio `AWSServiceRoleForTrustedAdvisor` y, a continuación, habilitar de nuevo Trusted Advisor.

Para habilitar Trusted Advisor (consola)

1. Utilice la consola de IAM o la API de IAM para crear un rol vinculado a un servicio para. AWS CLI Trusted Advisor Para obtener más información, consulte Crear un rol vinculado al servicio.
2. Inicie sesión en y AWS Management Console, a continuación, navegue hasta la consola en. Trusted Advisor https://console.aws.amazon.com/trustedadvisor

   El banner de estado Trusted Advisor desactivado aparecerá en la consola.
3. Selecciona Habilitar Trusted Advisor rol en el banner de estado. Si no se detecta el `AWSServiceRoleForTrustedAdvisor` necesario, el banner de estado permanece desactivado.

Modificación de un rol vinculado a servicios de Trusted Advisor

Dado que varias entidades pueden hacer referencia al rol vinculado al servicio, no puede cambiar su nombre después de crearlo. Sin embargo, puede utilizar la consola de IAM o la API de IAM para editar la descripción del rol. AWS CLI Para obtener más información, consulte Editar un rol vinculado a servicios en la Guía del usuario de IAM.

Eliminación de un rol vinculado a un servicio de Trusted Advisor

Si no necesita usar las funciones o los servicios de Trusted Advisor, puede eliminar el `AWSServiceRoleForTrustedAdvisor` rol. Debe deshabilitarlo Trusted Advisor antes de poder eliminar este rol vinculado al servicio. Esto impide que se eliminen los permisos necesarios para las operaciones de Trusted Advisor . Al inhabilitar Trusted Advisor, deshabilita todas las funciones del servicio, incluidas las notificaciones y el procesamiento sin conexión. Además, si inhabilitas Trusted Advisor la cuenta de un miembro, también se verá afectada la cuenta de pagador independiente, lo que significa que no recibirás Trusted Advisor cheques que identifiquen formas de ahorrar costes. No puede obtener acceso a la consola de Trusted Advisor . Las llamadas a la API Trusted Advisor devuelven un error de acceso denegado.

Debe volver a crear el rol vinculado al servicio de `AWSServiceRoleForTrustedAdvisor` en la cuenta para que pueda volver a habilitar Trusted Advisor.

Primero debes inhabilitarlo Trusted Advisor en la consola para poder eliminar el rol `AWSServiceRoleForTrustedAdvisor` vinculado al servicio.

Para inhabilitarlo Trusted Advisor

1. Inicie sesión en AWS Management Console y navegue hasta la Trusted Advisor consola enhttps://console.aws.amazon.com/trustedadvisor.
2. En el panel de navegación, elija Preferences (Preferencias).
3. En la sección Service Linked Role Permissions (Permisos de roles vinculados a servicios), elija Disable (Desactivar) Trusted Advisor.
4. En el cuadro de diálogo de confirmación, elija OK (Aceptar) para confirmar que desea desactivar Trusted Advisor.

Tras la desactivación Trusted Advisor, se Trusted Advisor desactivarán todas las funciones y la Trusted Advisor consola mostrará solo el cartel de estado de desactivado.

A continuación, puede utilizar la consola de IAM AWS CLI, la API de IAM o la API de IAM para eliminar el rol vinculado al Trusted Advisor servicio denominado. `AWSServiceRoleForTrustedAdvisor` Para obtener más información, consulte Eliminación de un rol vinculado a servicios en la Guía del usuario de IAM.

AWS políticas gestionadas para AWS Support

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

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

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

Temas

AWS políticas gestionadas para AWS Support

AWS Support tiene las siguientes políticas gestionadas.

Contenido

AWS política gestionada: AWSSupportServiceRolePolicy

AWS Support utiliza la política AWSSupportServiceRolePolicy AWS gestionada. Esta política administrada se adjunta al rol vinculado al servicio de `AWSServiceRoleForSupport`. La política permite al rol vinculado al servicio completar acciones en su nombre. No puede adjuntar esta política a sus entidades de IAM. Para obtener más información, consulte Permisos de roles vinculados a servicios de AWS Support.

Para obtener una lista de los cambios en la política, consulteAWS Support actualizaciones de las políticas AWS gestionadas y Cambios en los permisos de AWSSupportServiceRolePolicy.

AWS Support actualizaciones de las políticas AWS gestionadas

Consulte los detalles sobre las actualizaciones de las políticas AWS administradas AWS Support desde que estos servicios comenzaron a rastrear estos cambios. Para obtener alertas automáticas sobre cambios en esta página, suscríbase a la fuente RSS en la página de Historial de documentos.

En la siguiente tabla se describen las actualizaciones importantes de las políticas AWS Support administradas desde el 17 de febrero de 2022.

AWS Support

Cambio	Descripción	Fecha
AWSSupportServiceRolePolicy: actualización de una política actual	Se agregaron 17 permisos nuevos a los siguiente s servicios para realizar acciones que ayuden a solucionar los problemas de los clientes relacionados con la facturación, la asistencia administrativa y la asistencia técnica: • Amazon CloudWatch Network Monitor: para solucionar problemas relacionados con el servicio Network Monitor. • Amazon CloudWatch Logs: para depurar problemas relacionados con Amazon CloudWatch Logs. • Amazon Managed Streaming for Apache Kafka: para solucionar problemas relacionados con Amazon Managed Streaming for Apache Kafka. • Amazon Managed Service for Prometheus: para solucionar problemas relacionados con el Amazon	22 de marzo de 2024

Cambio	Descripción	Fecha
	Managed Service for Prometheus.	

Cambio	Descripción	Fecha
AWSSupportServiceRolePolicy: actualización de una política actual	Se agregaron 63 permisos nuevos a los siguiente s servicios para realizar acciones que ayuden a solucionar los problemas de los clientes relacionados con la facturación, la asistencia administrativa y la asistencia técnica: • AWS Salas limpias: para solucionar problemas relacionados con las salas AWS limpias. • CodeConnections — Para solucionar problemas relacionados con. CodeConnections • Amazon EKS: para depurar problemas relacionados con Amazon EKS. • Image Builder: para depurar problemas relacionados con el Image Builder. • Amazon Inspector2: para solucionar problemas relacionados con Amazon Inspector2. • Amazon Inspector Scan: para depurar problemas relacionados con el Amazon Inspector Scan. • Amazon CloudWatch Logs: para solucionar problemas	17 de enero de 2024

Cambio	Descripción	Fecha
	relacionados con Amazon CloudWatch Logs. • AWS Outposts — Para solucionar problemas relacionados con. AWS Outposts • Amazon RDS: para depurar problemas relacionados con Amazon RDS. • AWS IAM Identity Center — Para solucionar problemas relacionados con. AWS IAM Identity Center • Amazon S3 Express: para depurar problemas relacionados con Amazon S3 Express. • AWS Trusted Advisor — Para solucionar problemas relacionados con. AWS Trusted Advisor	

Cambio	Descripción	Fecha
AWSSupportServiceRolePolicy: actualización de una política actual	Se agregaron 126 permisos nuevos a los siguiente s servicios para realizar acciones que ayuden a solucionar los problemas de los clientes relacionados con la facturación, la asistencia administrativa y la asistencia técnica: • AWS Direct Connect — Para solucionar problemas relacionados con el AWS Direct Connect servicio. • Amazon SageMaker : para solucionar problemas relacionados con el SageMaker servicio de Amazon. • Amazon AppStream : para depurar problemas relacionados con Amazon AppStream. • Explorador de recursos de AWS — Para depurar problemas relacionados con. Explorador de recursos de AWS • Amazon Redshift sin servidor: para soluciona r problemas relacionados con Amazon Redshift sin servidor.	6 de diciembre de 2023

Cambio	Descripción	Fecha
	• Amazon ElastiCache : para solucionar problemas relacionados con Amazon ElastiCache. • Amazon Comprehend: para solucionar problemas relacionados con Amazon Comprehend. • Amazon EC2: para solucionar problemas relacionados con Amazon EC2. • Amazon Elastic Kubernetes Service: para depurar problemas relacionados con Amazon Elastic Kubernetes Service. • AWS Elastic Disaster Recovery — Para solucionar problemas relacionados con. AWS Elastic Disaster Recovery • AWS AppSync — Para depurar problemas relacionados con. AWS AppSync • Amazon CloudWatch Logs: para solucionar problemas relacionados con Amazon CloudWatch Logs. • AWS Health — Para depurar problemas	

Cambio	Descripción	Fecha
	relacionados con el AWS Health Servicio. • Amazon Connect: para depurar problemas relacionados con Amazon Connect. • AWS Snowball — Para solucionar problemas relacionados con. AWS Snowball • AWS Health Procesamiento de imágenes: para solucionar problemas relacionados con el procesamiento de imágenes. AWS Health	

Cambio	Descripción	Fecha
AWSSupportServiceRolePolicy: actualización de una política actual	Se agregaron 163 permisos nuevos a los siguientes servicios para llevar a cabo acciones que ayudan a solucionar problemas de los clientes relacionados con la facturación, la administración y el soporte técnico: • Amazon CloudFront : para solucionar problemas relacionados con el CloudFront servicio. • Amazon EC2: para solucionar problemas relacionados con el servicio Amazon EC2. • Amazon AppStream : para depurar problemas relacionados con Amazon AppStream. • AWS WAF — Para depurar problemas relacionados con el firewall de aplicaciones AWS web. • Amazon Connect: para solucionar problemas relacionados con Amazon Connect. • AWS IoT — Para depurar problemas relacionados con. AWS IoT • Amazon Route 53: para solucionar problemas	27 de octubre de 2023

Cambio	Descripción	Fecha
	relacionados con Amazon Route 53. • AWS Acceso verificado: para solucionar problemas relacionados con el servicio de acceso AWS verificado. • Amazon Simple Email Service: para depurar problemas relaciona dos con Amazon Simple Email Service. • AWS Elastic Beanstalk — Para solucionar problemas relacionados con. AWS Elastic Beanstalk • Amazon DynamoDB: para depurar problemas relacionados con Amazon DynamoDB. • AWS EC2 Image Builder: para solucionar problemas relacionados con EC2 Image AWS Builder. • AWS Outposts — Para depurar problemas relacionados con el servicio. AWS Outposts • AWS Glue — Para depurar problemas relacionados con. AWS Glue • AWS Directory Service — Para solucionar problemas	

Cambio	Descripción	Fecha
	relacionados con. AWS Directory Service • AWS Elastic Disaster Recovery — Para solucionar problemas relacionados con. AWS Elastic Disaster Recovery • AWS Step Functions — Para depurar problemas relacionados con. AWS Step Functions • Amazon EMR: para solucionar problemas relacionados con Amazon EMR. • Amazon Relational Database Service: para solucionar problemas relacionados con Amazon Relational Database Service. • Amazon EC2 Systems Manager: para depurar problemas relacionados con Amazon EC2 Systems Manager.	

Cambio	Descripción	Fecha
AWSSupportServiceRolePolicy: actualización de una política actual	Se agregaron 176 permisos nuevos a los siguientes servicios para llevar a cabo acciones que ayudan a solucionar problemas de los clientes relacionados con la facturación, la administración y el soporte técnico: • AWS Glue — Para solucionar problemas relacionados con el servicio AWS Glue • Amazon EMR: para solucionar problemas relacionados con el servicio Amazon EMR. • Amazon Security Lake: para depurar problemas relacionados con Amazon Security Lake. • AWS Systems Manager — Para depurar problemas relacionados con el servicio Systems Manager. • Amazon Verified Permissions: para solucionar problemas relacionados con Amazon Verified Permissions. • AWS IAM Access Analyzer: para depurar problemas relacionados con el servicio IAM Access Analyzer.	28 de agosto de 2023

Cambio	Descripción	Fecha
	• AWS Backup — Para solucionar problemas relacionados con. AWS Backup • AWS Database Migration Service — Para solucionar problemas relacionados con el servicio DMS. • Amazon DynamoDB: para depurar problemas relacionados con DynamoDB. • Amazon Elastic Container Registry (Amazon ECR): para solucionar problemas relacionados con Amazon Elastic Container Registry (Amazon ECR). • Amazon Elastic Container Service: para depurar problemas relacionados con Amazon Elastic Container Service. • Amazon Elastic Kubernetes Service: para solucionar problemas relacionados con Amazon Elastic Kubernetes Service. • Amazon EMR sin servidor: para depurar problemas	

Cambio	Descripción	Fecha
	relacionados con el servicio Amazon EMR sin servidor. • AWS Identity and Access Management — Para solucionar problemas relacionados con. AWS Identity and Access Management • AWS Network Firewall: para solucionar problemas relacionados con AWS Network Firewall. • AWS HealthOmics — Para depurar problemas relacionados con. AWS HealthOmics • Amazon QuickSight : para depurar problemas relacionados con Amazon QuickSight. • Amazon Relational Database Service: para solucionar problemas relacionados con Amazon Relational Database Service. • Amazon Redshift: para solucionar problemas relacionados con Amazon Redshift. • Amazon Redshift sin servidor: para depurar problemas relacionados con	

Cambio	Descripción	Fecha
	el servicio Amazon Redshift sin servidor. • Amazon SageMaker : para depurar problemas relacionados con Amazon SageMaker.	

Cambio	Descripción	Fecha
AWSSupportServiceRolePolicy: actualización de una política actual	Se agregaron 141 permisos nuevos a los siguientes servicios para llevar a cabo acciones que ayudan a solucionar problemas de los clientes relacionados con la facturación, la administración y el soporte técnico: • Lambda: para solucionar problemas relacionados con el servicio Lambda. • Amazon Lex: para solucionar problemas relacionados con el servicio Amazon Lex. • AWS Transfer: para depurar problemas relacionados con el servicio de transferencia. • AWS Amplify — Para depurar problemas relacionados con el servicio Amplify. • Amazon EventBridge Pipes: para solucionar problemas de permisos y facturación relacionados con Pipes. • Amazon EventBridge : para depurar problemas relacionados con Amazon EventBridge • Amazon CloudWatch Logs: para solucionar problemas relacionados con Amazon CloudWatch Logs.	26 de junio de 2023

Cambio	Descripción	Fecha
	• AWS Systems Manager — Para solucionar problemas relacionados con Systems Manager. • Amazon CloudWatch : para depurar problemas relacionados CloudWatch con. • Amazon ElastiCache : para solucionar problemas relacionados con Amazon ElastiCache. • Amazon Athena: para depurar problemas relacionados con Athena. • AWS Elastic Disaster Recovery — Para soluciona r problemas relaciona dos con Elastic Disaster Recovery. • Amazon CloudWatch : para solucionar problemas de configuración de Amazon CloudWatch. • Amazon EC2: para depurar problemas relacionados con el servicio EC2. • AWS Certificate Manager — Para solucionar problemas relacionados con Certificate Manager. • Amazon EventBridge Scheduler: para solucionar	

Cambio	Descripción	Fecha
	problemas relacionados con Scheduler. EventBridge • Amazon OpenSearch Service: para solucionar problemas relacionados OpenSearch con. • Amazon EventBridge Schemas: para depurar problemas relacionados con los esquemas. EventBridge • AWS Notificaciones de usuario: para solucionar problemas relacionados con las notificaciones de usuario. • Amazon CloudWatch Application Insights: para solucionar problemas relacionados con CloudWatch Application Insights. • Amazon DynamoDB: para solucionar problemas relacionados con DynamoDB. • Clústeres elásticos de Amazon DocumentDB: para solucionar problemas relacionados con los clústeres elásticos de DocumentDB.	

Cambio	Descripción	Fecha
AWSSupportServiceRolePolicy: actualización de una política actual	Se agregaron 53 permisos nuevos a los siguientes servicios para llevar a cabo acciones que ayudan a solucionar problemas de los clientes relacionados con la facturación, la administración y el soporte técnico: • Auto Scaling: para solucionar problemas relacionados con el servicio Auto Scaling. • Amazon CloudWatch : para solucionar problemas relacionados con Amazon CloudWatch. • AWS Compute Optimizer — Para solucionar problemas relacionados con Compute Optimizer. • Amazon CloudWatch Evidently: para solucionar problemas relacionados con Evidently. • Generador de imágenes de EC2: para solucionar problemas relacionados con el servicio del generador de imágenes. • AWS IoT TwinMaker — Para solucionar problemas relacionados con. AWS IoT TwinMaker	2 de mayo de 2023

Cambio	Descripción	Fecha
	• Amazon CloudWatch Logs: para solucionar problemas relacionados con Amazon CloudWatch Logs. • Amazon Pinpoint: para solucionar problemas relacionados con Amazon Pinpoint. • AWS Enlace OAM: para depurar problemas relacionados con los recursos de OAM. • AWS Outposts — Para solucionar problemas relacionados con. AWS Outposts • Amazon RDS: para depurar problemas relacionados con Amazon RDS. • Explorador de recursos de AWS — Para solucionar problemas relacionados con el Explorador de recursos. • Amazon CloudWatch RUM: para solucionar problemas de configuración de los recursos del servicio RUM. • Amazon SNS: para solucionar problemas relacionados con Amazon SNS. • Amazon CloudWatch Synthetics: para solucionar	

Cambio	Descripción	Fecha
	problemas relacionados con Synthetics. CloudWatch	

Cambio	Descripción	Fecha
AWSSupportServiceRolePolicy: actualización de una política actual	Se agregaron 52 permisos nuevos a los siguientes servicios para llevar a cabo acciones que ayudan a solucionar problemas de los clientes relacionados con la facturación, la administración y el soporte técnico: • AWS Backup gateway — Para solucionar problemas relacionados con Backup Gateway. • Amazon S3: para depurar problemas relacionados con Amazon S3. • AWS Application Migration Service — Para solucionar problemas relacionados con el Servicio de migración de aplicaciones. • AWS Salas limpias: para depurar problemas relacionados con las salas AWS limpias; • AWS Systems Manager para SAP: para solucionar problemas relacionados AWS Systems Manager con SAP. • Amazon VPC Lattice: para depurar problemas	16 de marzo de 2023

Cambio	Descripción	Fecha
	relacionados con Amazon VPC Lattice.	

Cambio	Descripción	Fecha
AWSSupportServiceRolePolicy: actualización de una política actual	Se agregaron 220 permisos nuevos a los siguientes servicios para llevar a cabo acciones que ayudan a solucionar problemas de los clientes relacionados con la facturación, la administración y el soporte técnico: • Amazon Athena: AWS Support para permitir el desarrollo de herramientas que se puedan utilizar para ayudar a los clientes con sus consultas relacionadas con Athena. • Amazon Chime: para solucionar problemas relacionados con Amazon Chime. • Amazon CloudWatch Internet Monitor: para depurar problemas relacionados con Internet Monitor. • Amazon Comprehend: para solucionar problemas relacionados con Amazon Comprehend. • Amazon Elastic Compute Cloud: para depurar problemas relacionados con las funciones de puerta	10 de enero de 2023

Cambio	Descripción	Fecha
	de enlace Transit Connect Gateway y de multidifusión. • Amazon EventBridge Pipes: para solucionar problemas relacionados con EventBridge Pipes. • Amazon Interactive Video Service: permite consultar AWS Support los recursos de Amazon IVS para solucionar problemas de los clientes. • Amazon FSx: para permitir el desarrollo de herramientas AWS Support que admitan la importación y exportación de un repositorio de datos de Amazon FSx. • Amazon GameLift : para solucionar problemas relacionados con Amazon GameLift. • AWS Glue: para solucionar problemas relacionados con AWS Glue Data Quality. • Amazon Kinesis Video Streams: para solucionar problemas relacionados con Kinesis Video Streams. • Amazon Managed Service para Prometheus: para solucionar problemas relacionados con Amazon	

Cambio	Descripción	Fecha
	Managed Service para Prometheus. • Amazon Managed Streaming para Apache Kafka: para solucionar problemas relacionados con Amazon MSK Connect. • AWS Network Manager — Para solucionar problemas relacionados con Network Manager. • Amazon Nimble Studio: para depurar problemas relacionados con Nimble Studio. • Amazon Personalize: para depurar problemas relacionados con Amazon Personalize. • Amazon Pinpoint: para solucionar problemas relacionados con Amazon Pinpoint. • AWS HealthOmics — Para solucionar problemas relacionados con. HealthOmics • Amazon Transcribe: para depurar problemas relacionados con Amazon Transcribe.	

Cambio	Descripción	Fecha
AWSSupportServiceRolePolicy: actualización de una política actual	Se agregaron 47 permisos nuevos a los siguientes servicios para llevar a cabo acciones que ayudan a solucionar problemas de los clientes relacionados con la facturación, la administración y el soporte técnico: • AWS Application Migration Service — Para solucionar problemas de replicación y lanzamiento. • AWS CloudFormation ganchos: permiten AWS Support desarrollar herramientas de automatización que puedan ayudar a resolver problemas. • Amazon Elastic Kubernetes Service: para solucionar problemas relacionados con Amazon EKS. • AWS IoT FleetWise: para solucionar problemas relacionados con AWS IoT FleetWise. • AWS Mainframe Modernization — Para depurar problemas relacionados con la modernización del mainframe. • AWS Outposts — Para ayudar a AWS Support	4 de octubre de 2022

Cambio	Descripción	Fecha
	obtener una lista de hosts y activos dedicados. • AWS Private 5G: para solucionar problemas relacionados con Private 5G. • AWS Tiros: para depurar problemas relacionados con Tiros.	

Cambio	Descripción	Fecha
AWSSupportServiceRolePolicy: actualización de una política actual	Se agregaron 46 permisos nuevos a los siguientes servicios para llevar a cabo acciones que ayudan a solucionar problemas de los clientes relacionados con la facturación, la administración y el soporte técnico: • Amazon Managed Streaming para Apache Kafka: para solucionar problemas relacionados con Amazon MSK. • AWS DataSync — Para solucionar problemas relacionados DataSync con. • AWS Elastic Disaster Recovery — Para solucionar problemas de replicación y lanzamiento. • Amazon GameSparks : para solucionar problemas relacionados GameSparks con. • AWS IoT TwinMaker — Para depurar problemas relacionados con. AWS IoT TwinMaker • AWS Lambda — Para ver la URL de configuración de una función para solucionar problemas.	17 de agosto de 2022

Cambio	Descripción	Fecha
	• Amazon Lookout for Equipment: para solucionar problemas relacionados con Lookout for Equipment. • Amazon Route 53 y Amazon Route 53 Resolver: para obtener configura ciones de resolución que AWS Support permitan comprobar el comportam iento de resolución de DNS de una VPC.	

Cambio	Descripción	Fecha
AWSSupportServiceRolePolicy: actualización de una política actual	Se agregaron permisos nuevos a los siguientes servicios para llevar a cabo acciones que ayudan a solucionar problemas de los clientes relacionados con la facturación, la administración y el soporte técnico: • Amazon CloudWatch Logs: para ayudar a solucionar problemas relacionados con CloudWatch los registros. • Amazon Interactive Video Service: para ayudar a AWS Support comprobar los recursos existentes de Amazon IVS en busca de casos de asistencia relacionados con fraude o cuentas comprometidas. • Amazon Inspector: para solucionar problemas relacionados con Amazon Inspector. Se eliminaron los permisos para servicios, como Amazon WorkLink. Amazon WorkLink dejó de estar disponible el 19 de abril de 2022.	23 de junio de 2022

Cambio	Descripción	Fecha
AWSSupportServiceRolePolicy: actualización de una política actual	Se han agregado 25 permisos nuevos a los siguientes servicios para llevar a cabo acciones que ayudan a solucionar problemas de los clientes relacionados con la facturación, la administración y el soporte técnico: • AWS Amplify UI Builder: para solucionar problemas relacionados con la generación de componentes y temas. • Amazon AppStream : para solucionar problemas recuperando recursos para funciones que se lanzaron recientemente. • AWS Backup — Para solucionar problemas relacionados con los trabajos de copia de seguridad. • AWS CloudFormation — Realizar diagnósticos sobre problemas relacionados con la IAM, la extensión y el control de versiones. • Amazon Kinesis: para solucionar problemas relacionados con Kinesis. • AWS Transfer Family — Para solucionar problemas	27 de abril de 2022

Cambio	Descripción	Fecha
	relacionados con Transfer Family.	

Cambio	Descripción	Fecha

AWSSupportServiceRolePolicy: actualización de una política actual	Se han agregado 54 permisos nuevos a los siguientes servicios para llevar a cabo acciones que ayudan a solucionar problemas de los clientes relacionados con la facturación, la administración y el soporte técnico:
	• Amazon Elastic Compute Cloud
	  • Para solucionar problemas relacionados con el cliente y listas con prefijos administrados de AWS.
	  • Para solucionar problemas relacionados con Amazon VPC IP Address Manager (IPAM).
	• AWS Network Manager: para solucionar problemas relacionados con Network Manager.
	• Savings Plans: para obtener metadatos sobre los compromisos pendientes del Savings Plan.
	• AWS Serverless Application Repository — Mejorar y respaldar las acciones de respuesta como parte de la investigación y resolución de los casos de soporte.
		14 de marzo de 2022

Cambio	Descripción	Fecha
	• Amazon WorkSpaces Web: para depurar y solucionar problemas con los servicios WorkSpaces web.	

Cambio	Descripción	Fecha
AWSSupportServiceRolePolicy: actualización de una política actual	Se han agregado 74 permisos nuevos a los siguientes servicios para llevar a cabo acciones que ayudan a solucionar problemas de los clientes relacionados con la facturación, la administración y el soporte técnico: • AWS Application Migration Service — Para admitir la replicación sin agentes en el Servicio de migración de aplicaciones. • AWS CloudFormation — Para realizar diagnósticos de problemas relacionados con la IAM, las extensiones y el control de versiones. • Amazon CloudWatch Logs: para validar las políticas de recursos. • Papelera de reciclaje de Amazon EC2: para obtener metadatos sobre las reglas de retención de la papelera de reciclaje. • AWS Elastic Disaster Recovery — Para solucionar problemas de replicación y lanzamiento en las cuentas de los clientes.	17 de febrero de 2022

Cambio	Descripción	Fecha
	• Amazon FSx: permite ver la descripción de las instantán eas de Amazon FSx. • Amazon Lightsail: para ver los metadatos y los detalles de las configuraciones de los buckets de Lightsail. • Amazon Macie: para ver configuraciones de Macie, tales como trabajos de clasificación, identificadores de datos personalizados, expresiones regulares y hallazgos. • Amazon S3: para recopilar metadatos y configura ciones para buckets de S3 de Amazon. • AWS Storage Gateway — Para ver los metadatos sobre las políticas de creación automática de cintas de los clientes. • Elastic Load Balancing: permite ver la descripción de los límites de recursos al utilizar la consola Service Quotas. Para obtener más informaci ón, consulte Cambios en los permisos de AWSSuppor tServiceRolePolicy.	

Cambio	Descripción	Fecha
Registro de cambios publicado	Registro de cambios de las políticas AWS Support gestionadas.	17 de febrero de 2022

Cambios en los permisos de AWSSupportServiceRolePolicy

La mayoría de los permisos se `AWSSupportServiceRolePolicy` han agregado AWS Support para poder llamar a una operación de API con el mismo nombre. Sin embargo, algunas operaciones de API requieren permisos que tienen un nombre diferente.

En la siguiente tabla solo se enumeran las operaciones de la API que requieren permisos con un nombre diferente. En esta tabla se describen estas diferencias a partir del 17 de febrero de 2022.

Date	Nombre de operación de la API	Permisos de IAM necesarios
Permisos agregados el 17 de febrero de 2022	`s3.GetBucketAnalyticsConfiguration`	`s3:GetAnalyticsConfiguration`
	`s3.ListBucketAnalyticsConfiguration`	
	`s3.GetBucketNotificationConfiguration`	`s3:GetBucketNotification`
	`s3.GetBucketEncryption`	`s3:GetEncryptionConfiguration`
	`s3.GetBucketIntelligentTieringConfiguration`	`s3:GetIntelligentTieringConfiguration`
	`s3.ListBucketIntelligentTieringConfiguration`	

Date	Nombre de operación de la API	Permisos de IAM necesarios
	s3.GetBucketInventoryConfiguration s3.ListBucketInventoryConfiguration	s3:GetInventoryConfiguration
	s3.GetBucketLifecycleConfiguration	s3:GetLifecycleConfiguration
	s3.GetBucketMetricsConfiguration s3.ListBucketMetricsConfiguration	s3:GetMetricsConfiguration
	s3.GetBucketReplication	s3:GetReplicationConfiguration
	s3.HeadBucket s3.ListObjects	s3:ListBucket
	s3.ListBuckets	s3:ListAllMyBuckets
	s3.ListMultipartUploads	s3:ListBucketMultipartUploads
	s3.ListObjectVersions	s3:ListBucketVersions
	s3.ListParts	s3:ListMultipartUploadParts

AWS políticas gestionadas para AWS Support la aplicación en Slack

> **Note**
>
> Para acceder y ver los casos de soporte en el AWS Support Center Console, consulteAdministre el acceso al AWS Support Centro.

AWS Support La aplicación tiene las siguientes políticas administradas.

Contenido

- AWS política gestionada: AWSSupportAppFullAccess
- AWS política gestionada: AWSSupportAppReadOnlyAccess
- AWS Support Actualizaciones de la aplicación para las políticas gestionadas AWS

AWS política gestionada: AWSSupportAppFullAccess

Puede usar la política administrada de AWSSupportAppFullAccess para conceder al rol de IAM los permisos para las configuraciones de sus canales de Slack. También puede adjuntar la política AWSSupportAppFullAccess a sus entidades de IAM.

Para obtener más información, consulte AWS Support Aplicación en Slack.

Esta política otorga permisos que permiten a la entidad realizar AWS Support acciones de Service Quotas e IAM para la AWS Support aplicación.

Detalles de los permisos

Esta política incluye los permisos siguientes:

- `servicequotas`: describe sus cuotas y solicitudes de servicio existentes y crea aumentos de cuotas de servicio para su cuenta.
- `support`: crea, actualiza y resuelve sus casos de soporte. Actualiza y describe la información sobre sus casos, como los archivos adjuntos, las correspondencias y los niveles de gravedad. Inicia sesiones de chat en vivo con un agente de soporte.

- `iam`: crea un rol vinculado a un servicio para Service Quotas.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "servicequotas:GetRequestedServiceQuotaChange",
                "servicequotas:GetServiceQuota",
                "servicequotas:RequestServiceQuotaIncrease",
                "support:AddAttachmentsToSet",
                "support:AddCommunicationToCase",
                "support:CreateCase",
                "support:DescribeCases",
                "support:DescribeCommunications",
                "support:DescribeSeverityLevels",
                "support:InitiateChatForCase",
                "support:ResolveCase"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "*",
            "Condition": {
                "StringEquals": {"iam:AWSServiceName": "servicequotas.amazonaws.com"}
            }
        }
    ]
}
```

Para obtener más información, consulte Administración del acceso a la aplicación AWS Support.

AWS política gestionada: AWSSupportAppReadOnlyAccess

La AWSSupportAppReadOnlyAccesspolítica otorga permisos que permiten a la entidad realizar acciones de AWS Support aplicación de solo lectura. Para obtener más información, consulte AWS Support Aplicación en Slack.

Detalles de los permisos

Esta política incluye los permisos siguientes:

- `support`: describe los detalles del caso de soporte y las comunicaciones agregadas a los casos de soporte.

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

AWS Support Actualizaciones de la aplicación para las políticas gestionadas AWS

Consulta los detalles sobre las actualizaciones de las políticas AWS gestionadas de AWS Support la aplicación desde que este servicio comenzó a realizar el seguimiento de estos cambios. Para obtener alertas automáticas sobre cambios en esta página, suscríbase a la fuente RSS en la página de Historial de documentos.

En la siguiente tabla se describen las actualizaciones importantes de las políticas administradas por la AWS Support aplicación desde el 17 de agosto de 2022.

AWS Support Aplicación

Cambio	Descripción	Fecha
AWSSupportAppFullAccessy AWSSupportAppReadOnlyAccess Nuevas políticas AWS gestionadas para la AWS Support aplicación	Puede usar estas políticas para el rol de IAM que configure para la configuración de su canal de Slack. Para obtener más información, consulte Administración del acceso a la aplicación AWS Support.	19 de agosto de 2022
Registro de cambios publicado	Registro de cambios de las políticas gestionadas por la AWS Support aplicación.	19 de agosto de 2022

AWS políticas gestionadas para AWS Trusted Advisor

Trusted Advisor tiene las siguientes políticas AWS gestionadas.

Contenido

- AWS política gestionada: AWSTrustedAdvisorPriorityFullAccess
- AWS política gestionada: AWSTrustedAdvisorPriorityReadOnlyAccess
- Política administrada por AWS : AWSTrustedAdvisorServiceRolePolicy
- AWS política gestionada: AWSTrustedAdvisorReportingServiceRolePolicy
- Actualizaciones de Trusted Advisor en las políticas administradas de AWS

AWS política gestionada: AWSTrustedAdvisorPriorityFullAccess

La AWSTrustedAdvisorPriorityFullAccesspolítica otorga acceso completo a Trusted Advisor Priority. Esta política también permite al usuario añadir cuentas de administrador delegado para Trusted Advisor Priority Trusted Advisor como servicio de confianza AWS Organizations y especificarlas.

Detalles de los permisos

En la primera declaración, la política debe incluir los siguientes permisos para `trustedadvisor`:

- Describe su cuenta y su organización.
- Describe los riesgos identificados por Trusted Advisor Priority. Los permisos le permiten descargar y actualizar el estado del riesgo.
- Describe las configuraciones de las notificaciones Trusted Advisor prioritarias por correo electrónico. Los permisos le permiten configurar las notificaciones por correo electrónico y deshabilitarlas para los administradores delegados.
- Se configura Trusted Advisor para que su cuenta pueda activarse AWS Organizations.

En la segunda declaración, la política debe incluir los siguientes permisos para `organizations`:

- Describe tu Trusted Advisor cuenta y tu organización.
- Muestra las Servicios de AWS que ha habilitado para usar Organizations.

En la tercera declaración, la política debe incluir los siguientes permisos para `organizations`:

- Muestra los administradores delegados para Trusted Advisor Priority.
- Habilita y deshabilita el acceso confiable con Organizations.

En la cuarta declaración, la política debe incluir los siguientes permisos para `iam`:

- Crea el rol vinculado al servicio `AWSServiceRoleForTrustedAdvisorReporting`.

En la quinta declaración, la política debe incluir los siguientes permisos para `organizations`:

- Le permite registrar y anular el registro de los administradores delegados de Trusted Advisor Priority.

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Sid": "AWSTrustedAdvisorPriorityFullAccess",
   "Effect": "Allow",
   "Action": [
    "trustedadvisor:DescribeAccount*",
    "trustedadvisor:DescribeOrganization",
```

```
    "trustedadvisor:DescribeRisk*",
    "trustedadvisor:DownloadRisk",
    "trustedadvisor:UpdateRiskStatus",
    "trustedadvisor:DescribeNotificationConfigurations",
    "trustedadvisor:UpdateNotificationConfigurations",
    "trustedadvisor:DeleteNotificationConfigurationForDelegatedAdmin",
    "trustedadvisor:SetOrganizationAccess"
   ],
   "Resource": "*"
  },
  {
   "Sid": "AllowAccessForOrganization",
   "Effect": "Allow",
   "Action": [
    "organizations:DescribeAccount",
    "organizations:DescribeOrganization",
    "organizations:ListAWSServiceAccessForOrganization"
   ],
   "Resource": "*"
  },
  {
   "Sid": "AllowListDelegatedAdministrators",
   "Effect": "Allow",
   "Action": [
    "organizations:ListDelegatedAdministrators",
    "organizations:EnableAWSServiceAccess",
    "organizations:DisableAWSServiceAccess"
   ],
   "Resource": "*",
   "Condition": {
    "StringEquals": {
     "organizations:ServicePrincipal": [
      "reporting.trustedadvisor.amazonaws.com"
     ]
    }
   }
  },
  {
   "Sid": "AllowCreateServiceLinkedRole",
   "Effect": "Allow",
   "Action": "iam:CreateServiceLinkedRole",
   "Resource": "arn:aws:iam::*:role/aws-service-role/
reporting.trustedadvisor.amazonaws.com/AWSServiceRoleForTrustedAdvisorReporting",
   "Condition": {
```

```
    "StringLike": {
     "iam:AWSServiceName": "reporting.trustedadvisor.amazonaws.com"
    }
   }
  },
  {
   "Sid": "AllowRegisterDelegatedAdministrators",
   "Effect": "Allow",
   "Action": [
    "organizations:RegisterDelegatedAdministrator",
    "organizations:DeregisterDelegatedAdministrator"
   ],
   "Resource": "arn:aws:organizations::*:*",
   "Condition": {
    "StringEquals": {
     "organizations:ServicePrincipal": [
      "reporting.trustedadvisor.amazonaws.com"
     ]
    }
   }
  }
 ]
}
```

AWS política gestionada: AWSTrustedAdvisorPriorityReadOnlyAccess

La AWSTrustedAdvisorPriorityReadOnlyAccesspolítica concede permisos de solo lectura a Trusted Advisor Priority, incluido el permiso para ver las cuentas de administrador delegadas.

Detalles de los permisos

En la primera declaración, la política debe incluir los siguientes permisos para `trustedadvisor`:

- Describe su Trusted Advisor cuenta y su organización.
- Describe los riesgos identificados en Trusted Advisor Priority y permite descargarlos.
- Describe las configuraciones de las notificaciones Trusted Advisor prioritarias por correo electrónico.

En la segunda y tercera declaración, la política incluye los siguientes permisos para `organizations`:

- Describe su organización con Organizations.

- Muestra las Servicios de AWS que ha habilitado para usar Organizations.
- Muestra los administradores delegados con prioridad Trusted Advisor

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Sid": "AWSTrustedAdvisorPriorityReadOnlyAccess",
   "Effect": "Allow",
   "Action": [
    "trustedadvisor:DescribeAccount*",
    "trustedadvisor:DescribeOrganization",
    "trustedadvisor:DescribeRisk*",
    "trustedadvisor:DownloadRisk",
    "trustedadvisor:DescribeNotificationConfigurations"
   ],
   "Resource": "*"
  },
  {
   "Sid": "AllowAccessForOrganization",
   "Effect": "Allow",
   "Action": [
    "organizations:DescribeOrganization",
    "organizations:ListAWSServiceAccessForOrganization"
   ],
   "Resource": "*"
  },
  {
   "Sid": "AllowListDelegatedAdministrators",
   "Effect": "Allow",
   "Action": [
    "organizations:ListDelegatedAdministrators"
   ],
   "Resource": "*",
   "Condition": {
    "StringEquals": {
     "organizations:ServicePrincipal": [
      "reporting.trustedadvisor.amazonaws.com"
     ]
    }
   }
  }
```

```
 ]
}
```

Política administrada por AWS : AWSTrustedAdvisorServiceRolePolicy

Esta política se adjunta al rol vinculado al servicio de `AWSServiceRoleForTrustedAdvisor`. Permite al rol vinculado al servicio llevar a cabo acciones en su nombre. No puede adjuntar AWSTrustedAdvisorServiceRolePolicy a sus entidades de AWS Identity and Access Management (IAM). Para obtener más información, consulte Uso de roles vinculados a servicios de Trusted Advisor.

Esta política concede permisos administrativos que autorizan al rol vinculado al servicio acceder a Servicios de AWS. Estos permisos permiten que las comprobaciones Trusted Advisor evalúen su cuenta.

Detalles de los permisos

Esta política incluye los siguientes permisos.

- `accessanalyzer`— Describe AWS Identity and Access Management Access Analyzer los recursos
- `Auto Scaling`: describe los recursos y las cuotas de cuenta de Amazon EC2 Auto Scaling
- `cloudformation`— Describe AWS CloudFormation (CloudFormation) las cuotas y acumulaciones de cuentas
- `cloudfront`— Describe las CloudFront distribuciones de Amazon
- `cloudtrail`— Describe AWS CloudTrail (CloudTrail) las rutas
- `dynamodb`: describe los recursos y las cuotas de cuenta de Amazon DynamoDB
- `dynamodbaccelerator`— Describe los recursos de DynamoDB Accelerator
- `ec2`: describe las cuotas de cuenta y los recursos de Amazon Elastic Compute Cloud (Amazon EC2)
- `elasticloadbalancing`: describe las cuotas de cuenta y los recursos de Elastic Load Balancing (ELB)
- `iam`: obtiene recursos de IAM, como credenciales, políticas de contraseñas y certificados
- `networkfirewall`— Describe los recursos AWS Network Firewall

- `kinesis`: describe las cuotas de cuenta de Amazon Kinesis (Kinesis)
- `rds`: describe recursos de Amazon Relational Database Service (Amazon RDS)
- `redshift`: describe recursos de Amazon Redshift
- `route53`: describe los recursos y las cuotas de cuenta de Amazon Route 53
- `s3`: describe los recursos de Amazon Simple Storage Service (Amazon S3)
- `ses`: obtiene cuotas de envío de Amazon Simple Email Service (Amazon SES)
- `sqs`: enumera colas de Amazon Simple Queue Service (Amazon SQS)
- `cloudwatch`— Obtiene las estadísticas métricas de Amazon CloudWatch CloudWatch Events (Events)
- `ce`: obtiene recomendaciones de Cost Explorer Service (Cost Explorer)
- `route53resolver`— Obtiene los puntos finales y los recursos de Amazon Route 53 Resolver Resolver
- `kafka`: obtiene recursos de Amazon Managed Streaming para Apache Kafka
- `ecs`— Obtiene los recursos de Amazon ECS
- `outposts`— Obtiene AWS Outposts recursos

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "access-analyzer:ListAnalyzers"
                "autoscaling:DescribeAccountLimits",
                "autoscaling:DescribeAutoScalingGroups",
                "autoscaling:DescribeLaunchConfigurations",
                "ce:GetReservationPurchaseRecommendation",
                "ce:GetSavingsPlansPurchaseRecommendation",
                "cloudformation:DescribeAccountLimits",
                "cloudformation:DescribeStacks",
                "cloudformation:ListStacks",
                "cloudfront:ListDistributions",
                "cloudtrail:DescribeTrails",
                "cloudtrail:GetTrailStatus",
                "cloudtrail:GetTrail",
                "cloudtrail:ListTrails",
```

```
                "cloudtrail:GetEventSelectors",
                "cloudwatch:GetMetricStatistics",
                "cloudwatch:ListMetrics",
                "dax:DescribeClusters",
                "dynamodb:DescribeLimits",
                "dynamodb:DescribeTable",
                "dynamodb:ListTables",
                "ec2:DescribeAddresses",
                "ec2:DescribeReservedInstances",
                "ec2:DescribeInstances",
                "ec2:DescribeVpcs",
                "ec2:DescribeInternetGateways",
                "ec2:DescribeImages",
                "ec2:DescribeNatGateways",
                "ec2:DescribeVolumes",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSubnets",
                "ec2:DescribeRegions",
                "ec2:DescribeReservedInstancesOfferings",
                "ec2:DescribeRouteTables",
                "ec2:DescribeSnapshots",
                "ec2:DescribeVpcEndpoints",
                "ec2:DescribeVpnConnections",
                "ec2:DescribeVpnGateways",
                "ec2:DescribeLaunchTemplateVersions",
                "ec2:GetManagedPrefixListEntries",
                "ecs:DescribeTaskDefinition",
                "ecs:ListTaskDefinitions"
                "elasticloadbalancing:DescribeAccountLimits",
                "elasticloadbalancing:DescribeInstanceHealth",
                "elasticloadbalancing:DescribeLoadBalancerAttributes",
                "elasticloadbalancing:DescribeLoadBalancerPolicies",
                "elasticloadbalancing:DescribeLoadBalancerPolicyTypes",
                "elasticloadbalancing:DescribeLoadBalancers",
                "elasticloadbalancing:DescribeTargetGroups",
                "elasticloadbalancing:DescribeTargetHealth",
                "iam:GenerateCredentialReport",
                "iam:GetAccountPasswordPolicy",
                "iam:GetAccountSummary",
                "iam:GetCredentialReport",
                "iam:GetServerCertificate",
                "iam:ListServerCertificates",
                "iam:ListSAMLProviders",
                "kinesis:DescribeLimits",
```

```
                "kafka:DescribeClusterV2",
                "kafka:ListClustersV2",
                "kafka:ListNodes",
                "network-firewall:ListFirewalls",
                "network-firewall:DescribeFirewall",
                "outposts:GetOutpost",
                "outposts:ListAssets",
                "outposts:ListOutposts",
                "rds:DescribeAccountAttributes",
                "rds:DescribeDBClusters",
                "rds:DescribeDBEngineVersions",
                "rds:DescribeDBInstances",
                "rds:DescribeDBParameterGroups",
                "rds:DescribeDBParameters",
                "rds:DescribeDBSecurityGroups",
                "rds:DescribeDBSnapshots",
                "rds:DescribeDBSubnetGroups",
                "rds:DescribeEngineDefaultParameters",
                "rds:DescribeEvents",
                "rds:DescribeOptionGroupOptions",
                "rds:DescribeOptionGroups",
                "rds:DescribeOrderableDBInstanceOptions",
                "rds:DescribeReservedDBInstances",
                "rds:DescribeReservedDBInstancesOfferings",
                "rds:ListTagsForResource",
                "redshift:DescribeClusters",
                "redshift:DescribeReservedNodeOfferings",
                "redshift:DescribeReservedNodes",
                "route53:GetAccountLimit",
                "route53:GetHealthCheck",
                "route53:GetHostedZone",
                "route53:ListHealthChecks",
                "route53:ListHostedZones",
                "route53:ListHostedZonesByName",
                "route53:ListResourceRecordSets",
                "route53resolver:ListResolverEndpoints",
                "route53resolver:ListResolverEndpointIpAddresses",
                "s3:GetAccountPublicAccessBlock",
                "s3:GetBucketAcl",
                "s3:GetBucketPolicy",
                "s3:GetBucketPolicyStatus",
                "s3:GetBucketLocation",
                "s3:GetBucketLogging",
                "s3:GetBucketVersioning",
```

```
                "s3:GetBucketPublicAccessBlock",
                "s3:GetLifecycleConfiguration",
                "s3:ListBucket",
                "s3:ListAllMyBuckets",
                "ses:GetSendQuota",
                "sqs:GetQueueAttributes",
                "sqs:ListQueues"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS política gestionada: AWSTrustedAdvisorReportingServiceRolePolicy

Esta política se adjunta a la función `AWSServiceRoleForTrustedAdvisorReporting` vinculada al servicio que permite realizar acciones Trusted Advisor para la función de visualización de la organización. No puede adjuntar AWSTrustedAdvisorReportingServiceRolePolicy a sus entidades de IAM. Para obtener más información, consulte Uso de roles vinculados a servicios de Trusted Advisor.

Esta política otorga permisos administrativos que permiten al rol vinculado al servicio realizar acciones. AWS Organizations

Detalles de los permisos

Esta política incluye los siguientes permisos.

- `organizations`: describe su organización y enumera el acceso al servicio, las cuentas, los elementos principales, los elementos secundarios y las unidades organizativas

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "organizations:DescribeOrganization",
                "organizations:ListAWSServiceAccessForOrganization",
                "organizations:ListAccounts",
```

```
                "organizations:ListAccountsForParent",
                "organizations:ListDelegatedAdministrators",
                "organizations:ListOrganizationalUnitsForParent",
                "organizations:ListChildren",
                "organizations:ListParents",
                "organizations:DescribeOrganizationalUnit",
                "organizations:DescribeAccount"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

Actualizaciones de Trusted Advisor en las políticas administradas de AWS

Consulte los detalles sobre las actualizaciones de las políticas AWS administradas Trusted Advisor desde que estos servicios comenzaron a realizar el seguimiento de estos cambios. AWS Support Para obtener alertas automáticas sobre cambios en esta página, suscríbase a la fuente RSS en la página de Historial de documentos.

En la siguiente tabla se describen las actualizaciones importantes de las políticas Trusted Advisor administradas desde el 10 de agosto de 2021.

Trusted Advisor

Cambio	Descripción	Fecha
AWSTrustedAdvisorServiceRolePolicy Actualización de una política existente.	Trusted Advisor agregó nuevas acciones para conceder los `sqs:GetQueueAttributes` permisos `access-analyzer:ListAnalyzers` `cloudwatch:ListMetrics` `dax:DescribeClusters` ,`ec2:DescribeNatGat`	11 de junio de 2024

Cambio	Descripción	Fecha
	eways ,ec2:Descr ibeRouteT ables ,ec2:Descr ibeVpcEndpoints , ec2:GetManagedPref ixListEnt ries elasticlo adbalanci ng:DescribeTargetH ealth ,iam:ListS AMLProviders ,, kafka:DescribeClus terV2 network-f irewall:ListFirewa lls network-f irewall:DescribeFi rewall y.	
AWSTrustedAdvisorS erviceRolePolicy Actualización a una política existente.	Trusted Advisor agregó nuevas acciones para conceder cloudtrai l:GetTrail cloudtrai l:ListTrails cloudtrail:GetEven tSelectors outposts: GetOutpost los outposts:ListOutpo sts permisos outposts: ListAssets y.	18 de enero de 2024

Cambio	Descripción	Fecha
AWSTrustedAdvisorPriorityFullAccess Actualización a una política existente.	Trusted Advisor actualizó la política `AWSTrustedAdvisorPriorityFullAccess` AWS gestionada para incluir los identificadores de las declaraciones.	6 de diciembre de 2023
AWSTrustedAdvisorPriorityReadOnlyAccess Actualización a una política existente.	Trusted Advisor actualizó la política `AWSTrustedAdvisorPriorityReadOnlyAccess` AWS gestionada para incluir los identificadores de las declaraciones.	6 de diciembre de 2023
AWSTrustedAdvisorServiceRolePolicy: actualización de una política actual	Trusted Advisor agregó nuevas acciones para conceder los `ecs:ListTaskDefinitions` permisos `ec2:DescribeRegions` `s3:GetLifecycleConfiguration` `ecs:DescribeTaskDefinition` y.	9 de noviembre de 2023

Cambio	Descripción	Fecha
AWSTrustedAdvisorServiceRolePolicy: actualización de una política actual	Trusted Advisor agregó nuevas acciones `route53resolver:ListResolverEndpoints` de IAM `route53resolver:ListResolverEndpointIpAddresses` `kafka:ListClustersV2` e `ec2:DescribeSubnets` `kafka:ListNodes` incorporó nuevas comprobaciones de resiliencia.	14 de septiembre de 2023
AWSTrustedAdvisorReportingServiceRolePolicy La versión 2 de la política gestionada se asocia a una función vinculada al Trusted Advisor `AWSServiceRoleForTrustedAdvisorReporting` servicio	Actualice la política AWS gestionada a la versión 2 para el rol vinculado al Trusted Advisor `AWSServiceRoleForTrustedAdvisorReporting` servicio. La versión 2 agregará una acción de IAM más: `organizations:ListDelegatedAdministrators`	28 de febrero de 2023
AWSTrustedAdvisorPriorityFullAccess y AWSTrustedAdvisorPriorityReadOnlyAccess Nuevas políticas AWS gestionadas para Trusted Advisor	Trusted Advisor se agregaron dos nuevas políticas administradas que puede usar para controlar el acceso a Trusted Advisor Priority.	17 de agosto de 2022

Cambio	Descripción	Fecha
AWSTrustedAdvisorServiceRolePolicy: actualización de una política actual	Trusted Advisor se han añadido nuevas acciones para conceder los `GetAccountPublicAccessBlock` permisos `DescribeTargetGroups` y. El permiso `DescribeTargetGroup` es necesario para que la Comprobación de estado de grupos de Auto Scaling pueda recuperar balanceadores de carga no clásicos adjuntos a un grupo de Auto Scaling. El permiso `GetAccountPublicAccessBlock` es necesario para que la verificación Permisos de bucket de Amazon S3 pueda recuperar la configuración de acceso público del bloque para una Cuenta de AWS.	10 de agosto de 2021
Registro de cambios publicado	Trusted Advisor comenzó a realizar un seguimiento de los cambios de sus políticas AWS gestionadas.	10 de agosto de 2021

AWS políticas gestionadas para AWS Support los planes

AWS Support Plans tiene las siguientes políticas administradas.

Contenido

- AWS política gestionada: AWSSupportPlansFullAccess
- AWS política gestionada: AWSSupportPlansReadOnlyAccess
- AWS Support Planifica las actualizaciones de las políticas AWS gestionadas

AWS política gestionada: AWSSupportPlansFullAccess

AWS Support Plans utiliza la política AWSSupportPlansFullAccess AWS gestionada. La entidad de IAM usa esta política para completar las siguientes acciones de los planes de soporte en su nombre:

- Consulte el plan de soporte para su Cuenta de AWS
- Ver detalles sobre el estado de una solicitud para cambiar su plan de soporte
- Cambie el plan de soporte para su Cuenta de AWS
- Cree cronogramas de planes de apoyo para su Cuenta de AWS

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "supportplans:GetSupportPlan",
                "supportplans:GetSupportPlanUpdateStatus",
                "supportplans:StartSupportPlanUpdate",
                "supportplans:CreateSupportPlanSchedule"
            ],
            "Resource": "*"
        }
    ]
}
```

Para obtener una lista de los cambios hechos en las políticas, consulte AWS Support Planifica las actualizaciones de las políticas AWS gestionadas.

AWS política gestionada: AWSSupportPlansReadOnlyAccess

AWS Support Plans utiliza la política AWSSupportPlansReadOnlyAccess AWS gestionada. La entidad de IAM usa esta política para completar las siguientes acciones de los planes de soporte de solo lectura en su nombre:

- Consulte el plan de soporte para su Cuenta de AWS
- Ver detalles sobre el estado de una solicitud para cambiar su plan de soporte

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

Para obtener una lista de los cambios hechos en las políticas, consulte AWS Support Planifica las actualizaciones de las políticas AWS gestionadas.

AWS Support Planifica las actualizaciones de las políticas AWS gestionadas

Vea los detalles sobre las actualizaciones de las políticas AWS administradas de Support Plans desde que estos servicios comenzaron a rastrear estos cambios. Para obtener alertas automáticas sobre cambios en esta página, suscríbase a la fuente RSS en la página de Historial de documentos.

En la siguiente tabla se describen las actualizaciones importantes de las políticas administradas de los planes de Support desde el 29 de septiembre de 2022.

AWS Support

Cambio	Descripción	Fecha
AWSSupportPlansFullAccess: actualización de una política existente	Agregue la acción `CreateSupportPlanSchedule` a la política administrada `AWSSupportPlansFullAccess` .	8 de mayo de 2023

Cambio	Descripción	Fecha
Registro de cambios publicado	Registro de cambios de las políticas administradas de los planes de Support.	29 de septiembre de 2022

Administre el acceso al AWS Support Centro

Debe tener permisos para obtener acceso al Centro de asistencia y a Crear un caso de soporte.

Puede utilizar una de las siguientes opciones para obtener acceso al Centro de asistencia:

- Utilice la dirección de correo electrónico y la contraseña asociadas a su AWS cuenta. Esta identidad se denomina usuario raíz de la AWS cuenta.
- Uso AWS Identity and Access Management (IAM).

Si tiene un plan Business, Enterprise On-Ramp o Enterprise Support, también puede usar la AWS Support API para acceder AWS Support y Trusted Advisor operar mediante programación. Para obtener más información, consulte la referencia de la API de AWS Support.

> **Note**
>
> Si no puede iniciar sesión en el Centro de asistencia, puede utilizar la página Contacte con nosotros en su lugar. Puede utilizar esta página para obtener ayuda con problemas relacionados con las cuentas y la facturación.

AWS cuenta

Puede iniciar sesión AWS Management Console y acceder al Support Center con la dirección de correo electrónico y la contraseña de su AWS cuenta. Esta identidad se denomina usuario raíz de la AWS cuenta. Sin embargo, se recomienda encarecidamente no utilizar el usuario raíz para las tareas cotidianas, ni siquiera para las tareas administrativas. En su lugar, le recomendamos que utilice IAM, que le permite controlar quién puede llevar a cabo determinadas tareas en la cuenta.

AWS acciones de apoyo

Puede realizar las siguientes AWS Support acciones en la consola. También puede especificar estas AWS Support acciones en una política de IAM para permitir o denegar acciones específicas.

> **Note**
>
> Si rechaza alguna de las siguientes acciones en sus políticas de IAM, podría producirse un comportamiento no deseado en el Centro de soporte al momento de crear un caso de soporte o al interactuar con él.

Acción	Descripción
`DescribeSupportLevel`	Concede permiso para devolver el nivel de soporte para un identificador de cuenta de AWS . El AWS Support Centro lo utiliza internamente para identificar su nivel de soporte.
`InitiateCallForCase`	Otorga permiso para iniciar una llamada en AWS Support Center. AWS Support Center lo usa internamente para iniciar una llamada en tu nombre.
`InitiateChatForCase`	Concede permiso para iniciar un chat con el Centro de AWS Support . AWS Support Center lo usa internamente para iniciar un chat en tu nombre.
`RateCaseCommunication`	Otorga permiso para valorar la comunicación de un AWS Support caso.
`DescribeCaseAttributes`	Concede permiso para permitir que los servicios secundarios lean los atributos del caso de AWS Support . El AWS Support Centro lo usa internamente para etiquetar los atributos de su caso.

Acción	Descripción
`DescribeIssueTypes`	Concede permiso para devolver los tipos de errores de los casos de AWS Support . AWS Support Center lo usa internamente para obtener los tipos de problemas disponibles para su cuenta.
`SearchForCases`	Otorga permiso para devolver una lista de AWS Support casos que coincida con las entradas proporcionadas. El AWS Support Centro lo usa internamente para encontrar los casos buscados.
`PutCaseAttributes`	Otorga permiso para que los servicios secundarios adjunten atributos a AWS Support los casos. AWS Support Center lo usa internamente para agregar etiquetas operativas a sus AWS Support casos.

IAM

De forma predeterminada, los usuarios de IAM no pueden obtener acceso al Centro de asistencia. Puede utilizar IAM para crear usuarios individuales o grupos. A continuación, debe adjuntar políticas de IAM a estas entidades para que tengan permiso para realizar acciones y acceder a los recursos, como abrir casos del Support Center y usar la AWS Support API.

Después de crear los usuarios de IAM, podrá asignarles contraseñas individuales y una página de inicio de sesión específica de la cuenta. A continuación, pueden iniciar sesión en tu AWS cuenta y trabajar en el Support Center. Los usuarios de IAM que tengan AWS Support acceso pueden ver todos los casos creados para la cuenta.

Para obtener más información, consulte Iniciar sesión AWS Management Console como usuario de IAM en la Guía del usuario de IAM.

La forma más sencilla de conceder permisos es adjuntar la política AWS gestionada AWSSupportAccessal usuario, grupo o rol. AWS Support permite permisos de nivel de acción para controlar el acceso a operaciones específicas AWS Support . AWS Support no proporciona acceso

a nivel de recursos, por lo que el `Resource` elemento siempre está configurado en. * No es posible permitir ni denegar el acceso a casos de soporte específicos.

Example : Permite el acceso a todas las acciones AWS Support

La política AWS gestionada AWSSupportAccessconcede a un usuario de IAM acceso a AWS Support. Un usuario de IAM con esta política puede acceder a todas AWS Support las operaciones y recursos.

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

Para obtener más información sobre cómo adjuntar la política de `AWSSupportAccess` a sus entidades, consulte Agregar permisos de identidad de IAM (consola) en la Guía del usuario de IAM.

Example : Permita el acceso a todas las acciones excepto a la ResolveCase acción

También puede crear políticas administradas por el cliente en IAM para especificar qué acciones se deben permitir o denegar. La siguiente declaración de política permite a un usuario de IAM realizar todas las acciones AWS Support excepto resolver un caso.

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

```
}
```

Para obtener más información sobre cómo crear una política de IAM administrada por el cliente, consulte Creación de directivas de IAM (Consola) en la Guía del usuario de IAM.

Si el usuario o el grupo ya tiene una política, puede añadir la declaración AWS Support de política específica a esa política.

> **Important**
>
> - Si no puede ver los casos en el Centro de asistencia, asegúrese de que tiene los permisos necesarios. Tal vez tenga que contactar con el administrador de IAM. Para obtener más información, consulte Administración de identidad y acceso para AWS Support.

Acceso a AWS Trusted Advisor

En el AWS Management Console, un espacio de nombres de `trustedadvisor` IAM independiente controla el acceso a. Trusted Advisor En la AWS Support API, el espacio de nombres de `support` IAM controla el acceso a. Trusted Advisor Para obtener más información, consulte Gestione el acceso a AWS Trusted Advisor.

Gestione el acceso a los planes AWS Support

Temas

- Permisos para la consola de planes de Support
- Acciones de los planes de Support
- Ejemplos de políticas de IAM para planes de Support
- Resolución de problemas

Permisos para la consola de planes de Support

Para acceder a la consola de planes de Support, un usuario debe tener un conjunto mínimo de permisos. Estos permisos deben permitir al usuario enumerar y consultar los detalles sobre los recursos de los planes de Support en su Cuenta de AWS.

Puede crear una política AWS Identity and Access Management (IAM) con el `supportplans` espacio de nombres. Puede utilizar esta política para especificar permisos para acciones y recursos.

Al crear una directiva, puede especificar el espacio de nombres del servicio para permitir o denegar una acción. El espacio de nombres de los planes de Support es `supportplans`.

Puede usar políticas AWS administradas y adjuntarlas a sus entidades de IAM. Para obtener más información, consulte AWS políticas gestionadas para AWS Support los planes.

Acciones de los planes de Support

Puede llevar a cabo las siguientes acciones de los planes de Support en la consola. También puede especificar estas acciones de los planes de Support en una política de IAM para permitir o denegar acciones específicas.

Acción	Descripción
`GetSupportPlan`	Concede permiso para ver los detalles sobre el plan de soporte actual para esta Cuenta de AWS.
`GetSupportPlanUpdateStatus`	Concede permiso para ver los detalles sobre el estado de una solicitud de actualización de un plan de soporte.
`StartSupportPlanUpdate`	Concede permiso para iniciar la solicitud de actualización del plan de soporte para esta Cuenta de AWS.
`CreateSupportPlanSchedule`	Concede permiso para crear programas de planes de soporte para esta Cuenta de AWS.

Ejemplos de políticas de IAM para planes de Support

Puede usar las políticas de ejemplo siguientes para administrar el acceso a los planes de Support.

Acceso completo a los planes de Support

La siguiente política concede a los usuarios acceso completo a los planes de Support.

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

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

Acceso de solo lectura a los planes de Support

La siguiente política permite a los usuarios acceso de solo lectura a los planes de Support.

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

Denegación del acceso a planes de Support

La siguiente política no permite a los usuarios el acceso a los planes de Support.

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

Resolución de problemas

Consulte los siguientes temas para administrar el acceso al Support Plans.

Cuando intento ver o cambiar mi plan de soporte, la consola de Support Plans dice que me falta el **`GetSupportPlan`** permiso

Los usuarios de IAM deben tener los permisos necesarios para acceder a la consola de Support Plans. Puede actualizar su política de IAM para incluir el permiso que falta o utilizar una política administrada de AWS , como AWSSupportPlansFullAccess o AWSSupportPlansReadOnlyAccess. Para obtener más información, consulte AWS políticas gestionadas para AWS Support los planes.

Si no se tiene acceso para actualizar las políticas de IAM, contáctese con el administrador de su Cuenta de AWS .

Información relacionada

Para obtener más información, consulte los siguientes temas de la guía del usuario de IAM:

- Probar las políticas de IAM con el simulador de política de IAM
- Solución de problemas de mensajes de error de acceso denegado

Tengo los permisos correctos, pero sigue apareciendo el mismo error

Si Cuenta de AWS es una cuenta de miembro de la que forma parte AWS Organizations, es posible que deba actualizar la política de control de servicios (SCP). Las SCP son un tipo de política que administra los permisos en una organización.

Como Support Plans es un servicio global, las políticas que restringen las Regiones de AWS pueden impedir que las cuentas miembro vean o cambien el plan de soporte. A fin de permitir servicios globales para su organización, como IAM y Support Plans, debe agregar el servicio a la lista de exclusiones de cualquier SCP aplicable. Esto significa que las cuentas de la organización pueden acceder a estos servicios, incluso si el SCP deniega uno especificado. Región de AWS

Para agregar Support Plans como excepción, ingrese `"supportplans:*"` a la lista `"NotAction"` en la SCP.

```
"supportplans:*",
```

Es posible que la SCP aparezca como el siguiente fragmento de política.

Example : SCP que le concede a Support Plans acceso a una organización

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

```
  "Statement": [
    { "Sid":  "GRREGIONDENY",
      "Effect":  "Deny",
      "NotAction": [
        "aws-portal:*",
        "budgets:*",
        "chime:*"
        "iam:*",
        "supportplans:*",
        ....
```

Si tiene una cuenta miembro y no puede actualizar la SCP, contacte con el administrador de su Cuenta de AWS . Es posible que la cuenta de gestión tenga que actualizar la SCP para que todas las cuentas miembro puedan acceder al Support Plans.

Notas para AWS Control Tower

- Si su organización utiliza un SCP con AWS Control Tower, puede actualizar la opción Denegar acceso a en AWS función del Región de AWS control solicitado (normalmente denominado control de denegación regional).
- Si actualizas el SCP AWS Control Tower para permitirlo`supportplans`, si se corrige la desviación, se eliminará la actualización del SCP. Para obtener más información, consulta Detectar y resolver la desviación. AWS Control Tower

Información relacionada

Para obtener más información, consulte los temas siguientes:

- Políticas de control de servicio (SCP) en la Guía del usuario de AWS Organizations .
- Configuración del control de denegación de región en la Guía del usuario de AWS Control Tower
- Denegue el acceso a AWS según lo solicitado Región de AWS en la Guía AWS Control Tower del usuario

Gestione el acceso a AWS Trusted Advisor

Puede acceder AWS Trusted Advisor desde. AWS Management Console Todos Cuentas de AWS tienen acceso a un núcleo selecto de Trusted Advisor cheques. Si tiene un plan de soporte Business,

Enterprise On-Ramp o Enterprise, puede obtener acceso a todas las verificaciones. Para obtener más información, consulte AWS Trusted Advisor comprobar referencia.

Puede usar AWS Identity and Access Management (IAM) para controlar el acceso a Trusted Advisor.

Temas

Permisos para la consola de Trusted Advisor

Para acceder a la Trusted Advisor consola, el usuario debe tener un conjunto mínimo de permisos. Estos permisos deben permitir al usuario enumerar y ver detalles sobre los Trusted Advisor recursos de su propiedad Cuenta de AWS.

Puede utilizar las siguientes opciones para controlar el acceso a Trusted Advisor:

- Utilice la función de filtro de etiquetas de la Trusted Advisor consola. El usuario o el rol deben tener permisos asociados a las etiquetas.

  Puede usar políticas AWS administradas o políticas personalizadas para asignar permisos por etiquetas. Para obtener más información, consulte Control de acceso desde y hasta usuarios y roles de IAM mediante etiquetas.
- Cree una política de IAM con espacio de nombres `trustedadvisor`. Puede utilizar esta política para especificar permisos para acciones y recursos.

Al crear una directiva, puede especificar el espacio de nombres del servicio para permitir o denegar una acción. El espacio de nombres para Trusted Advisor es. `trustedadvisor` Sin embargo, no puedes usar el espacio de `trustedadvisor` nombres para permitir o denegar las operaciones de la API en la Trusted Advisor API. AWS Support Debe utilizar el espacio de nombres `support` para AWS Support en su lugar.

> **Note**
>
> Si tienes permisos para acceder a la AWS SupportAPI, el Trusted Advisor widget de la AWS Management Console muestra una vista resumida de tus Trusted Advisor resultados.

Para ver los resultados en la Trusted Advisor consola, debes tener permiso para acceder al espacio de `trustedadvisor` nombres.

Trusted Advisor acciones

Puede realizar las siguientes Trusted Advisor acciones en la consola. También puede especificar estas Trusted Advisor acciones en una política de IAM para permitir o denegar acciones específicas.

Acción	Descripción
`DescribeAccount`	Otorga permiso para ver el AWS Support plan y varias Trusted Advisor preferencias.
`DescribeAccountAccess`	Otorga permiso para ver si está Cuenta de AWS activado o desactivado Trusted Advisor.
`DescribeCheckItems`	Otorga permiso para ver los detalles de los elementos de verificación.
`DescribeCheckRefreshStatuses`	Otorga permiso para ver los estados de actualización de las verificaciones de Trusted Advisor .
`DescribeCheckSummaries`	Otorga permiso para ver los resúmenes de los Trusted Advisor cheques.
`DescribeChecks`	Otorga permiso para ver los detalles de los Trusted Advisor cheques.
`DescribeNotificationPreferences`	Otorga permiso para ver las preferencias de notificación de la cuenta de AWS .
`ExcludeCheckItems`	Otorga permiso para excluir recomendaciones para las verificaciones de Trusted Advisor .
`IncludeCheckItems`	Otorga permiso para incluir recomendaciones para las verificaciones de Trusted Advisor .

Acción	Descripción
`RefreshCheck`	Otorga permiso para actualizar un Trusted Advisor cheque.
`SetAccountAccess`	Otorga permiso Trusted Advisor para activar o desactivar la cuenta.
`UpdateNotificationPreferences`	Otorga permiso para actualizar las preferencias de notificación para Trusted Advisor.
`DescribeCheckStatusHistoryChanges`	Concede permiso para ver los resultados y los estados modificados de las comprobaciones en los últimos 30 días.

Trusted Advisor acciones para una vista organizativa

Las siguientes Trusted Advisor acciones son para la función de vista organizacional. Para obtener más información, consulte Vista organizativa para AWS Trusted Advisor.

Acción	Descripción
`DescribeOrganization`	Otorga permiso para ver si Cuenta de AWS cumple los requisitos para habilitar la función de vista organizacional.
`DescribeOrganizationAccounts`	Otorga permiso para ver las AWS cuentas vinculadas que están en la organización.
`DescribeReports`	Otorga permiso para ver los detalles de los informes de vista organizativa, como el nombre del informe, el tiempo de ejecución, la fecha de creación, el estado y el formato.
`DescribeServiceMetadata`	Otorga permiso para ver información sobre los informes de visualización de la organización, como las categorías de comprobac

Acción	Descripción
	ión Regiones de AWS, los nombres de las comprobaciones y los estados de los recursos.
`GenerateReport`	Otorga permiso para crear un informe para los Trusted Advisor cheques de su organización.
`ListAccountsForParent`	Otorga permiso para ver, en la Trusted Advisor consola, todas las cuentas de una AWS organización incluidas en una raíz o unidad organizativa (OU).
`ListOrganizationalUnitsForParent`	Otorga permiso para ver, en la Trusted Advisor consola, todas las unidades organizativas (OU) de una unidad organizativa principal o raíz.
`ListRoots`	Otorga permiso para ver, en la Trusted Advisor consola, todas las raíces definidas en una AWS organización.
`SetOrganizationAccess`	Otorga permiso para habilitar la función de visualización de la organización para Trusted Advisor.

Trusted Advisor Acciones prioritarias

Si tienes activada la Trusted Advisor prioridad en tu cuenta, puedes realizar las siguientes Trusted Advisor acciones en la consola. También puede agregar estas acciones de Trusted Advisor en una política de IAM para permitir o denegar acciones específicas. Para obtener más información, consulte Ejemplos de políticas de IAM para Trusted Advisor Priority.

> **Note**
>
> Los riesgos que aparecen en Trusted Advisor Priority son recomendaciones que su administrador técnico de cuentas (TAM) ha identificado para su cuenta. Las recomendaciones de un servicio, como un Trusted Advisor cheque, se crean automáticamente para usted. Las recomendaciones de su TAM se crean manualmente.

A continuación, su TAM envía estas recomendaciones para que aparezcan en la lista de Trusted Advisor prioridades de su cuenta.

Para obtener más información, consulte Introducción a AWS Trusted Advisor Priority.

Acción	Descripción
`DescribeRisks`	Otorga permiso para ver los riesgos en Trusted Advisor Priority.
`DescribeRisk`	Otorga permiso para ver los detalles de los riesgos en Trusted Advisor Priority.
`DescribeRiskResources`	Concede permiso para ver los recursos afectados por un riesgo en Trusted Advisor Priority
`DownloadRisk`	Otorga permiso para descargar un archivo que contiene detalles sobre el riesgo en Trusted Advisor Priority.
`UpdateRiskStatus`	Concede permiso para actualizar el estado de riesgo en Trusted Advisor Priority
`DescribeNotificationConfigurations`	Otorga permiso para obtener tus preferencias de notificación por correo electrónico para Trusted Advisor Priority.
`UpdateNotificationConfigurations`	Concede permisos para crear o actualizar las preferencias de notificación por correo electrónico para Trusted Advisor Priority.
`DeleteNotificationConfigurationForDelegatedAdmin`	Concede permiso a la cuenta de administración de la organización para eliminar las preferencias de notificación por correo electrónico de una cuenta de administrador delegado para Trusted Advisor Priority.

Trusted Advisor Participa en acciones

Si has activado Trusted Advisor Engage en tu cuenta, puedes realizar las siguientes Trusted Advisor acciones en la consola. También puede añadir estas Trusted Advisor acciones a una política de IAM para permitir o denegar acciones específicas. Para obtener más información, consulte Ejemplos de políticas de IAM para Trusted Advisor Engage.

Para obtener más información, consulte Primeros pasos con AWS Trusted Advisor Engage (vista previa).

Acción	Descripción
`CreateEngagement`	Otorga permiso para crear una participación en Trusted Advisor Engage.
`CreateEngagementAttachment`	Otorga permiso para crear un archivo adjunto de participación en Trusted Advisor Engage.
`CreateEngagementCommunication`	Otorga permiso para crear una comunicación de participación en Trusted Advisor Engage.
`GetEngagement`	Otorga permiso para ver una participación en Trusted Advisor Engage.
`GetEngagementAttachment`	Otorga permiso para ver el archivo adjunto de una participación en Engage. Trusted Advisor
`GetEngagementType`	Otorga permiso para ver un tipo de participa ción específico en Trusted Advisor Engage.
`ListEngagementCommunications`	Concede permiso para ver todas las comunicac iones de una interacción en Trusted Advisor Engage.
`ListEngagements`	Otorga permiso para ver todas las interacci ones en Trusted Advisor Engage.
`ListEngagementTypes`	Otorga permiso para ver todos los tipos de participación en Trusted Advisor Engage.

Acción	Descripción
`UpdateEngagement`	Otorga permiso para actualizar los detalles de una participación en Trusted Advisor Engage.
`UpdateEngagementStatus`	Otorga permiso para actualizar el estado de una participación en Trusted Advisor Engage.

Ejemplos de políticas de IAM

Las siguientes directivas muestran cómo permitir y denegar el acceso a Trusted Advisor. Puede utilizar una de las siguientes políticas para crear una política administrada por el cliente en la consola de IAM. Por ejemplo, puede copiar una política de ejemplo y, a continuación, pegarla en el cuadro de diálogo Pestaña JSON de la consola de IAM. A continuación, adjunte la política a su usuario, grupo o rol de IAM.

Para obtener más información sobre cómo crear una política de IAM, consulte Creación de directivas de IAM (Consola) en la Guía del usuario de IAM.

Ejemplos

- Acceso completo a Trusted Advisor
- Acceso de solo lectura a Trusted Advisor
- Denegar el acceso a Trusted Advisor
- Permitir y denegar acciones específicas
- Controle el acceso a las operaciones AWS Support de la API para Trusted Advisor
- Ejemplos de políticas de IAM para Trusted Advisor Priority
- Ejemplos de políticas de IAM para Trusted Advisor Engage

Acceso completo a Trusted Advisor

La siguiente política permite a los usuarios ver todas las Trusted Advisor comprobaciones de la Trusted Advisor consola y realizar todas las acciones correspondientes.

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

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

Acceso de solo lectura a Trusted Advisor

La siguiente política permite a los usuarios el acceso de solo lectura a la Trusted Advisor consola. Los usuarios no pueden realizar cambios, como comprobaciones de actualización o cambiar las preferencias de notificación.

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

Denegar el acceso a Trusted Advisor

La siguiente política no permite a los usuarios ver las Trusted Advisor comprobaciones de la Trusted Advisor consola ni tomar medidas al respecto.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": "trustedadvisor:*",
            "Resource": "*"
        }
```

```
    ]
}
```

Permitir y denegar acciones específicas

La siguiente política permite a los usuarios ver todas las Trusted Advisor comprobaciones de la Trusted Advisor consola, pero no les permite actualizar ninguna comprobación.

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

Controle el acceso a las operaciones AWS Support de la API para Trusted Advisor

En el AWS Management Console, un espacio de nombres de `trustedadvisor` IAM independiente controla el acceso a. Trusted Advisor No puedes usar el espacio de `trustedadvisor` nombres para permitir o denegar las operaciones de la API en la Trusted Advisor API. AWS Support En su lugar, use el espacio de nombres de `support`. Debes tener permisos de acceso a la AWS Support API para realizar llamadas Trusted Advisor mediante programación.

Por ejemplo, si desea llamar a la RefreshTrustedAdvisorCheckoperación, debe tener permisos para esta acción en la política.

Example : Permita únicamente las operaciones de la Trusted Advisor API

La siguiente política permite a los usuarios acceder a las operaciones de la AWS Support API Trusted Advisor, pero no al resto de las operaciones de la AWS Support API. Por ejemplo, los usuarios pueden utilizar la API para ver y actualizar las verificaciones. No pueden crear, ver, actualizar ni resolver AWS Support casos.

Puedes usar esta política para llamar a las operaciones de la Trusted Advisor API mediante programación, pero no puedes usarla para ver o actualizar las comprobaciones en la Trusted Advisor consola.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "support:DescribeTrustedAdvisorCheckRefreshStatuses",
                "support:DescribeTrustedAdvisorCheckResult",
                "support:DescribeTrustedAdvisorChecks",
                "support:DescribeTrustedAdvisorCheckSummaries",
                "support:RefreshTrustedAdvisorCheck",
                "trustedadvisor:Describe*"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Deny",
            "Action": [
                "support:AddAttachmentsToSet",
                "support:AddCommunicationToCase",
                "support:CreateCase",
                "support:DescribeAttachment",
                "support:DescribeCases",
                "support:DescribeCommunications",
                "support:DescribeServices",
                "support:DescribeSeverityLevels",
                "support:ResolveCase"
            ],
            "Resource": "*"
        }
    ]
}
```

Para obtener más información sobre cómo funciona IAM con AWS Support y Trusted Advisor, consulte. Acciones

Ejemplos de políticas de IAM para Trusted Advisor Priority

Puede utilizar las siguientes políticas AWS gestionadas para controlar el acceso a Trusted Advisor Priority. Para obtener más información, consulte AWS políticas gestionadas para AWS Trusted Advisor y Introducción a AWS Trusted Advisor Priority.

Ejemplos de políticas de IAM para Trusted Advisor Engage

> **Note**
>
> Trusted Advisor Engage se encuentra en una versión preliminar y actualmente no tiene políticas AWS administradas. Puede utilizar una de las siguientes políticas para crear una política administrada por el cliente en la consola de IAM.

Un ejemplo de política que otorga acceso de lectura y escritura en Trusted Advisor Engage:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "trustedadvisor:CreateEngagement*",
                "trustedadvisor:DescribeAccount*",
                "trustedadvisor:GetEngagement*",
                "trustedadvisor:ListEngagement*",
                "trustedadvisor:UpdateEngagement*"
            ],
            "Resource": "*"
        }
    ]
}
```

Un ejemplo de política que concede acceso de solo lectura en Trusted Advisor Engage:

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

```
            "Action": [
                "trustedadvisor:DescribeAccount*",
                "trustedadvisor:GetEngagement*",
                "trustedadvisor:ListEngagement*"
            ],
            "Resource": "*"
        }
    ]
}
```

Un ejemplo de política que otorga acceso de lectura y escritura en Trusted Advisor Engage y la capacidad de habilitar el acceso confiable a: Trusted Advisor

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "organizations:DescribeOrganization",
                "organizations:ListAWSServiceAccessForOrganization",
                "trustedadvisor:CreateEngagement*",
                "trustedadvisor:DescribeAccount*",
                "trustedadvisor:DescribeOrganization",
                "trustedadvisor:GetEngagement*",
                "trustedadvisor:ListEngagement*",
                "trustedadvisor:SetOrganizationAccess",
                "trustedadvisor:UpdateEngagement*"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "organizations:EnableAWSServiceAccess",
                "organizations:DisableAWSServiceAccess"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "organizations:ServicePrincipal": [
                        "reporting.trustedadvisor.amazonaws.com"
                    ]
```

```
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "arn:aws:iam::*:role/aws-service-role/
reporting.trustedadvisor.amazonaws.com/AWSServiceRoleForTrustedAdvisorReporting",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "reporting.trustedadvisor.amazonaws.com"
                }
            }
        }
    ]
}
```

Véase también

Para obtener más información sobre Trusted Advisor los permisos, consulte los siguientes recursos:

- Acciones definidas por AWS Trusted Advisor en la Guía del usuario de IAM.
- Control del acceso a la consola de Trusted Advisor

Ejemplo de políticas de control de servicios para AWS Trusted Advisor

AWS Trusted Advisor admite las políticas de control de servicios (SCP). Las SCP son políticas que se asocian a elementos de una organización para administrar los permisos dentro de esa organización. Un SCP se aplica a todas AWS las cuentas del elemento al que se adjunta el SCP. Las políticas de control de servicios (SCP) permiten un control centralizado de los máximos permisos disponibles para todas las cuentas de la organización. Pueden ayudarle a garantizar que sus AWS cuentas se ajusten a las directrices de control de acceso de su organización. Para obtener más información, consulte Políticas de control de servicios en la Guía del usuario de AWS Organizations .

Temas

- Requisitos previos
- Ejemplo de políticas de control de servicios

Requisitos previos

Para usar políticas de control de servicios, primero debe hacer lo siguiente:

- Habilitar todas las características en la organización. Para obtener más información, consulte Habilitar todas las características en la organización en la Guía del usuario de AWS Organizations .
- Habilite las SCP para utilizar en su organización. Para obtener más información, consulte Activación y desactivación de los tipos de políticas en la Guía del usuario de AWS Organizations .
- Cree las SCP que necesite. Para obtener más información acerca de la creación de SCP, consulte Creación, actualización y eliminación de políticas de control de servicios en la Guía del usuario de AWS Organizations .

Ejemplo de políticas de control de servicios

Los siguientes ejemplos le muestran cómo puede controlar varios aspectos del uso compartido de recursos en una organización.

Example : Impida que los usuarios creen o editen interacciones en Engage Trusted Advisor

La siguiente SCP impide que los usuarios creen interacciones nuevas o editen las existentes.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "trustedadvisor:CreateEngagement",
        "trustedadvisor:UpdateEngagement*"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

Example : Denegar Trusted Advisor Engage y Priority Access Trusted Advisor

El siguiente SCP impide que los usuarios accedan o realicen cualquier acción dentro de Trusted Advisor Engage y Trusted Advisor Priority.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "trustedadvisor:ListEngagement*",
        "trustedadvisor:GetEngagement*",
        "trustedadvisor:CreateEngagement*",
        "trustedadvisor:UpdateEngagement*",
        "trustedadvisor:DescribeRisk*",
        "trustedadvisor:UpdateRisk*",
        "trustedadvisor:DownloadRisk"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

Solución de problemas de AWS Support identidad y acceso

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

Temas

- No estoy autorizado a realizar el iam: PassRole
- Quiero ver mis claves de acceso
- Soy administrador y quiero permitir que otras personas accedan AWS Support
- Quiero permitir que personas ajenas a mi AWS cuenta accedan a mis recursos AWS Support

No estoy autorizado a realizar el iam: PassRole

Si recibe un error que indica que no tiene autorización para realizar la acción `iam:PassRole`, las políticas deben actualizarse a fin de permitirle pasar un rol a AWS Support.

Algunas Servicios de AWS permiten transferir una función existente a ese servicio en lugar de crear una nueva función de servicio o una función vinculada a un servicio. Para ello, debe tener permisos para transferir el rol al servicio.

En el siguiente ejemplo, el error se produce cuando un usuario de IAM denominado `marymajor` intenta utilizar la consola para realizar una acción en AWS Support. Sin embargo, la acción requiere que el servicio cuente con permisos que otorguen un rol de servicio. Mary no tiene permisos para transferir el rol al servicio.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

En este caso, las políticas de Mary se deben actualizar para permitirle realizar la acción `iam:PassRole`.

Si necesita ayuda, póngase en contacto con su administrador. AWS El administrador es la persona que le proporcionó las credenciales de inicio de sesión.

Quiero ver mis claves de acceso

Después de crear sus claves de acceso de usuario de IAM, puede ver su ID de clave de acceso en cualquier momento. Sin embargo, no puede volver a ver su clave de acceso secreta. Si pierde la clave de acceso secreta, debe crear un nuevo par de claves de acceso.

Las claves de acceso se componen de dos partes: un ID de clave de acceso (por ejemplo, `AKIAIOSFODNN7EXAMPLE`) y una clave de acceso secreta (por ejemplo, `wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY`). El ID de clave de acceso y la clave de acceso secreta se utilizan juntos, como un nombre de usuario y contraseña, para autenticar sus solicitudes. Administre sus claves de acceso con el mismo nivel de seguridad que para el nombre de usuario y la contraseña.

> **Important**
>
> No proporcione las claves de acceso a terceros, ni siquiera para que lo ayuden a buscar el ID de usuario canónico. De este modo, podrías dar a alguien acceso permanente a tu Cuenta de AWS.

Cuando crea un par de claves de acceso, se le pide que guarde el ID de clave de acceso y la clave de acceso secreta en un lugar seguro. La clave de acceso secreta solo está disponible en el momento de su creación. Si pierde la clave de acceso secreta, debe agregar nuevas claves de acceso a su usuario de IAM. Puede tener un máximo de dos claves de acceso. Si ya cuenta con dos, debe eliminar un par de claves antes de crear una nueva. Para consultar las instrucciones, consulte Administración de claves de acceso en la Guía del usuario de IAM.

Soy administrador y quiero permitir que otras personas accedan AWS Support

Para permitir el acceso de otras personas AWS Support, debe crear una entidad de IAM (usuario o rol) para la persona o aplicación a la que necesita acceso. Esta persona utilizará las credenciales de la entidad para acceder a AWS. A continuación, debe asociar una política a la entidad que le conceda los permisos correctos en AWS Support.

Para comenzar de inmediato, consulte Creación del primer grupo y usuario delegado de IAM en la Guía del usuario de IAM.

Quiero permitir que personas ajenas a mi AWS cuenta accedan a mis recursos AWS Support

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

Para más información, consulte lo siguiente:

- Para saber si AWS Support es compatible con estas funciones, consulte¿Cómo AWS Support funciona con IAM.

- Para obtener información sobre cómo proporcionar acceso a los recursos de su Cuentas de AWS propiedad, consulte Proporcionar acceso a un usuario de IAM en otro usuario de su propiedad Cuenta de AWS en la Guía del usuario de IAM.
- Para obtener información sobre cómo proporcionar acceso a tus recursos a terceros Cuentas de AWS, consulta Cómo proporcionar acceso a recursos que Cuentas de AWS son propiedad de terceros en la Guía del usuario de IAM.
- Para obtener información sobre cómo proporcionar acceso mediante una federación de identidades, consulte Proporcionar acceso a usuarios autenticados externamente (identidad federada) en la Guía del usuario de IAM.
- Para obtener información sobre la diferencia entre los roles y las políticas basadas en recursos para el acceso entre cuentas, consulte Cómo los roles de IAM difieren de las políticas basadas en recursos en la Guía del usuario de IAM.

Respuesta frente a incidencias

La respuesta a los incidentes AWS Support es una AWS responsabilidad. AWS tiene una política y un programa formales y documentados que rigen la respuesta a los incidentes. Para obtener más información, consulte el documento técnico Introducción a la respuesta a los incidentes de AWS seguridad.

Utilice las siguientes opciones para informarse sobre problemas operativos:

- Consulte los problemas AWS operativos con un amplio impacto en el AWS Service Health Dashboard. Por ejemplo, eventos que afectan a un servicio o región que no es específico de su cuenta.
- Vea los problemas operativos de las cuentas individuales en AWS Health Dashboard. Por ejemplo, eventos que afectan a los servicios o recursos de su cuenta. Para obtener más información, consulte Cómo empezar a trabajar con AWS Health Dashboard en la Guía del usuario de AWS Health .

Inicio de sesión y supervisión, AWS Support y AWS Trusted Advisor

La supervisión es una parte importante del mantenimiento de la confiabilidad, la disponibilidad y el rendimiento de las demás AWS soluciones AWS Support AWS Trusted Advisor y de las demás. AWS

proporciona las siguientes herramientas de supervisión para observar AWS Support e AWS Trusted Advisor informar cuando algo va mal y tomar las medidas necesarias:

- Amazon CloudWatch monitorea tus AWS recursos y las aplicaciones en las que AWS ejecutas en tiempo real. Puede recopilar métricas y realizar un seguimiento de las métricas, crear paneles personalizados y definir alarmas que le advierten o que toman medidas cuando una métrica determinada alcanza el umbral que se especifique. Por ejemplo, puede CloudWatch hacer un seguimiento del uso de la CPU u otras métricas de sus instancias de Amazon Elastic Compute Cloud (Amazon EC2) y lanzar nuevas instancias automáticamente cuando sea necesario. Para obtener más información, consulta la Guía del CloudWatch usuario de Amazon.
- Amazon EventBridge ofrece un flujo casi en tiempo real de los eventos del sistema que describen los cambios en AWS los recursos. EventBridge permite la computación automatizada basada en eventos, ya que puede escribir reglas que vigilen ciertos eventos y activen acciones automatizadas en otros AWS servicios cuando estos eventos ocurren. Para obtener más información, consulta la Guía del EventBridge usuario de Amazon.
- AWS CloudTrailcaptura las llamadas a la API y los eventos relacionados realizados por su AWS cuenta o en su nombre y envía los archivos de registro a un depósito de Amazon Simple Storage Service (Amazon S3) que especifique. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron. Para obtener más información, consulte la Guía del usuario de AWS CloudTrail.

Para obtener más información, consulte Supervisar y registrar para AWS Support y Supervisar y registrar para AWS Trusted Advisor.

Validación de conformidad para AWS Support

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 Support

La infraestructura AWS global se basa en AWS regiones y zonas de disponibilidad. AWS Las regiones 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 las zonas sin interrupciones. Las zonas de disponibilidad tienen una mayor disponibilidad, tolerancia a errores y escalabilidad que las infraestructuras tradicionales de uno o varios centros de datos.

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

Seguridad de la infraestructura en AWS Support

Como servicio gestionado, AWS Support está protegido por los procedimientos de seguridad de la red AWS global que se describen en el documento técnico Amazon Web Services: descripción general de los procesos de seguridad.

Utiliza las llamadas a la API AWS publicadas para acceder a AWS Support través de la red. Los clientes deben ser compatibles con la seguridad de la capa de transporte (TLS) 1.0 o una versión posterior. Recomendamos TLS 1.2 o una versión posterior. Los clientes también deben ser compatibles con conjuntos de cifrado con confidencialidad directa total (PFS) tales como Ephemeral Diffie-Hellman (DHE) o Elliptic Curve Ephemeral Diffie-Hellman (ECDHE). 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 Support

Para AWS Trusted Advisor, se AWS encarga de las tareas de seguridad básicas, como la aplicación de parches al sistema operativo (SO) huésped y a las bases de datos, la configuración del firewall y la recuperación ante desastres.

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.

Ejemplos de código para AWS Support usar los AWS SDK

Los siguientes ejemplos de código muestran cómo usarlo AWS Support con un kit de desarrollo de AWS software (SDK).

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las funciones de servicio individuales, es posible ver las acciones en contexto en los escenarios relacionados y en los ejemplos entre servicios.

Los escenarios son ejemplos de código que muestran cómo llevar a cabo una tarea específica llamando a varias funciones dentro del mismo servicio.

Para obtener una lista completa de las guías para desarrolladores del AWS SDK y ejemplos de código, consulteAWS Support Utilizándolo con un AWS SDK. En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

Introducción

Hola AWS Support

En los siguientes ejemplos de código se muestra cómo empezar a utilizar AWS Glue.

.NET

AWS SDK for .NET

> **Note**
>
> Hay más información GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
using Amazon.AWSSupport;
using Microsoft.Extensions.DependencyInjection;
using Microsoft.Extensions.Hosting;

public static class HelloSupport
{
    static async Task Main(string[] args)
    {
```

```
        // Use the AWS .NET Core Setup package to set up dependency injection for
 the AWS Support service.
        // Use your AWS profile name, or leave it blank to use the default
 profile.
        // You must have one of the following AWS Support plans: Business,
 Enterprise On-Ramp, or Enterprise. Otherwise, an exception will be thrown.
        using var host = Host.CreateDefaultBuilder(args)
            .ConfigureServices((_, services) =>
                services.AddAWSService<IAmazonAWSSupport>()
            ).Build();

        // Now the client is available for injection.
        var supportClient =
 host.Services.GetRequiredService<IAmazonAWSSupport>();

        // You can use await and any of the async methods to get a response.
        var response = await supportClient.DescribeServicesAsync();
        Console.WriteLine($"\tHello AWS Support! There are
 {response.Services.Count} services available.");
    }
}
```

- Para obtener más información sobre la API, consulta DescribeServicesla Referencia AWS SDK for .NET de la API.

Java

SDK para Java 2.x

> **Note**
>
> Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.support.SupportClient;
import software.amazon.awssdk.services.support.model.Category;
import software.amazon.awssdk.services.support.model.DescribeServicesRequest;
import software.amazon.awssdk.services.support.model.DescribeServicesResponse;
```

```
import software.amazon.awssdk.services.support.model.Service;
import software.amazon.awssdk.services.support.model.SupportException;
import java.util.ArrayList;
import java.util.List;

/**
 * Before running this Java (v2) code example, set up your development
 * environment, including your credentials.
 *
 * For more information, see the following documentation topic:
 *
 * https://docs.aws.amazon.com/sdk-for-java/latest/developer-guide/get-
started.html
 *
 * In addition, you must have the AWS Business Support Plan to use the AWS
 * Support Java API. For more information, see:
 *
 * https://aws.amazon.com/premiumsupport/plans/
 *
 * This Java example performs the following task:
 *
 * 1. Gets and displays available services.
 *
 *
 * NOTE: To see multiple operations, see SupportScenario.
 */

public class HelloSupport {
    public static void main(String[] args) {
        Region region = Region.US_WEST_2;
        SupportClient supportClient = SupportClient.builder()
                .region(region)
                .build();

        System.out.println("***** Step 1. Get and display available services.");
        displayServices(supportClient);
    }

    // Return a List that contains a Service name and Category name.
    public static void displayServices(SupportClient supportClient) {
        try {
            DescribeServicesRequest servicesRequest =
 DescribeServicesRequest.builder()
                    .language("en")
```

```
                    .build();

            DescribeServicesResponse response =
 supportClient.describeServices(servicesRequest);
            List<Service> services = response.services();

            System.out.println("Get the first 10 services");
            int index = 1;
            for (Service service : services) {
                if (index == 11)
                    break;

                System.out.println("The Service name is: " + service.name());

                // Display the Categories for this service.
                List<Category> categories = service.categories();
                for (Category cat : categories) {
                    System.out.println("The category name is: " + cat.name());
                }
                index++;
            }

        } catch (SupportException e) {
            System.out.println(e.getLocalizedMessage());
            System.exit(1);
        }
    }
}
```

- Para obtener más información sobre la API, consulta DescribeServicesla Referencia AWS SDK for Java 2.x de la API.

JavaScript

SDK para JavaScript (v3)

> **Note**
>
> Hay más información. GitHub Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

Invoque ‘main()’ para ejecutar el ejemplo.

```
import {
  DescribeServicesCommand,
  SupportClient,
} from "@aws-sdk/client-support";

// Change the value of 'region' to your preferred AWS Region.
const client = new SupportClient({ region: "us-east-1" });

const getServiceCount = async () => {
  try {
    const { services } = await client.send(new DescribeServicesCommand({}));
    return services.length;
  } catch (err) {
    if (err.name === "SubscriptionRequiredException") {
      throw new Error(
        "You must be subscribed to the AWS Support plan to use this feature.",
      );
    } else {
      throw err;
    }
  }
};

export const main = async () => {
  try {
    const count = await getServiceCount();
    console.log(`Hello, AWS Support! There are ${count} services available.`);
  } catch (err) {
    console.error("Failed to get service count: ", err.message);
  }
};
```

- Para obtener más información sobre la API, consulta DescribeServicesla Referencia AWS SDK for JavaScript de la API.

Kotlin

SDK para Kotlin

> **Note**
>
> Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
/**
Before running this Kotlin code example, set up your development environment,
including your credentials.

For more information, see the following documentation topic:
https://docs.aws.amazon.com/sdk-for-kotlin/latest/developer-guide/setup.html

In addition, you must have the AWS Business Support Plan to use the AWS Support
 Java API. For more information, see:

https://aws.amazon.com/premiumsupport/plans/

This Kotlin example performs the following task:

1. Gets and displays available services.
 */

suspend fun main() {
    displaySomeServices()
}

// Return a List that contains a Service name and Category name.
suspend fun displaySomeServices() {
    val servicesRequest =
        DescribeServicesRequest {
            language = "en"
        }

    SupportClient { region = "us-west-2" }.use { supportClient ->
        val response = supportClient.describeServices(servicesRequest)
        println("Get the first 10 services")
```

```
        var index = 1

        response.services?.forEach { service ->
            if (index == 11) {
                return@forEach
            }

            println("The Service name is: " + service.name)

            // Get the categories for this service.
            service.categories?.forEach { cat ->
                println("The category name is ${cat.name}")
                index++
            }
        }
    }
}
```

- Para obtener más información sobre la API, consulta DescribeServicesla referencia sobre el AWS SDK para la API de Kotlin.

Python

SDK para Python (Boto3)

> **Note**
>
> Hay más información al respecto. GitHub Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
import logging
import boto3
from botocore.exceptions import ClientError

logger = logging.getLogger(__name__)


def hello_support(support_client):
```

```
    """
    Use the AWS SDK for Python (Boto3) to create an AWS Support client and count
    the available services in your account.
    This example uses the default settings specified in your shared credentials
    and config files.

    :param support_client: A Boto3 Support Client object.
    """
    try:
        print("Hello, AWS Support! Let's count the available Support services:")
        response = support_client.describe_services()
        print(f"There are {len(response['services'])} services available.")
    except ClientError as err:
        if err.response["Error"]["Code"] == "SubscriptionRequiredException":
            logger.info(
                "You must have a Business, Enterprise On-Ramp, or Enterprise
 Support "
                "plan to use the AWS Support API. \n\tPlease upgrade your
 subscription to run these "
                "examples."
            )
        else:
            logger.error(
                "Couldn't count services. Here's why: %s: %s",
                err.response["Error"]["Code"],
                err.response["Error"]["Message"],
            )
            raise


if __name__ == "__main__":
    hello_support(boto3.client("support"))
```

- Para obtener más información sobre la API, consulta DescribeServicesla AWS Referencia de API de SDK for Python (Boto3).

Ejemplos de código

- Acciones para usar los SDK AWS SupportAWS
  - Úselo AddAttachmentsToSet con un AWS SDK o CLI
  - Úselo AddCommunicationToCase con un AWS SDK o CLI

- Úselo CreateCase con un AWS SDK o CLI
- Úselo DescribeAttachment con un AWS SDK o CLI
- Úselo DescribeCases con un AWS SDK o CLI
- Úselo DescribeCommunications con un AWS SDK o CLI
- Úselo DescribeServices con un AWS SDK o CLI
- Úselo DescribeSeverityLevels con un AWS SDK o CLI
- Úselo DescribeTrustedAdvisorCheckRefreshStatuses con un AWS SDK o CLI
- Úselo DescribeTrustedAdvisorCheckResult con un AWS SDK o CLI
- Úselo DescribeTrustedAdvisorCheckSummaries con un AWS SDK o CLI
- Úselo DescribeTrustedAdvisorChecks con un AWS SDK o CLI
- Úselo RefreshTrustedAdvisorCheck con un AWS SDK o CLI
- Úselo ResolveCase con un AWS SDK o CLI
- Escenarios de AWS Support uso de AWS los SDK
  - Comience con AWS Support los casos con un AWS SDK

Acciones para usar los SDK AWS SupportAWS

Los siguientes ejemplos de código muestran cómo realizar AWS Support acciones individuales con los AWS SDK. Estos extractos se denominan AWS Support API y son fragmentos de código de programas más grandes que deben ejecutarse en su contexto. Cada ejemplo incluye un enlace a GitHub, donde puede encontrar instrucciones para configurar y ejecutar el código.

Los siguientes ejemplos incluyen solo las acciones que se utilizan con mayor frecuencia. Para ver una lista completa, consulte la Referencia de la API de AWS Support.

Ejemplos

- Úselo AddAttachmentsToSet con un AWS SDK o CLI
- Úselo AddCommunicationToCase con un AWS SDK o CLI
- Úselo CreateCase con un AWS SDK o CLI
- Úselo DescribeAttachment con un AWS SDK o CLI
- Úselo DescribeCases con un AWS SDK o CLI
- Úselo DescribeCommunications con un AWS SDK o CLI
- Úselo DescribeServices con un AWS SDK o CLI

- Úselo DescribeSeverityLevels con un AWS SDK o CLI
- Úselo DescribeTrustedAdvisorCheckRefreshStatuses con un AWS SDK o CLI
- Úselo DescribeTrustedAdvisorCheckResult con un AWS SDK o CLI
- Úselo DescribeTrustedAdvisorCheckSummaries con un AWS SDK o CLI
- Úselo DescribeTrustedAdvisorChecks con un AWS SDK o CLI
- Úselo RefreshTrustedAdvisorCheck con un AWS SDK o CLI
- Úselo ResolveCase con un AWS SDK o CLI

Úselo **`AddAttachmentsToSet`** con un AWS SDK o CLI

En los siguientes ejemplos de código, se muestra cómo utilizar `AddAttachmentsToSet`.

Los ejemplos de acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Puede ver esta acción en contexto en el siguiente ejemplo de código:

- Introducción a los casos

.NET

AWS SDK for .NET

> **Note**
>
> Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
   /// <summary>
   /// Add an attachment to a set, or create a new attachment set if one does
not exist.
   /// </summary>
   /// <param name="data">The data for the attachment.</param>
   /// <param name="fileName">The file name for the attachment.</param>
   /// <param name="attachmentSetId">Optional setId for the attachment. Creates
a new attachment set if empty.</param>
   /// <returns>The setId of the attachment.</returns>
```

```
    public async Task<string> AddAttachmentToSet(MemoryStream data, string
 fileName, string? attachmentSetId = null)
    {
        var response = await _amazonSupport.AddAttachmentsToSetAsync(
            new AddAttachmentsToSetRequest
            {
                AttachmentSetId = attachmentSetId,
                Attachments = new List<Attachment>
                {
                    new Attachment
                    {
                        Data = data,
                        FileName = fileName
                    }
                }
            });
        return response.AttachmentSetId;
    }
```

- Para obtener más información sobre la API, consulta AddAttachmentsToSetla Referencia AWS SDK for .NET de la API.

CLI

AWS CLI

Para añadir un adjunto a un conjunto

En el siguiente `add-attachments-to-set` ejemplo, se agrega una imagen a un conjunto que, a continuación, puede especificar para un caso de soporte en su AWS cuenta.

```
aws support add-attachments-to-set \
    --attachment-set-id "as-2f5a6faa2a4a1e600-mu-nk5xQlBr70-
G1cUos5LZkd38KOAHZa9BMDVzNEXAMPLE" \
    --attachments fileName=troubleshoot-screenshot.png,data=base64-encoded-string
```

Salida:

```
{
```

```
    "attachmentSetId": "as-2f5a6faa2a4a1e600-mu-nk5xQlBr70-
G1cUos5LZkd38KOAHZa9BMDVzNEXAMPLE",
    "expiryTime": "2020-05-14T17:04:40.790+0000"
}
```

Para obtener más información, consulte Administración de casos en la Guía del usuario de soporte de AWS .

- Para obtener más información sobre la API, consulta AddAttachmentsToSetla Referencia de AWS CLI comandos.

Java

SDK para Java 2.x

> **Note**
>
> Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
   public static String addAttachment(SupportClient supportClient, String
fileAttachment) {
       try {
           File myFile = new File(fileAttachment);
           InputStream sourceStream = new FileInputStream(myFile);
           SdkBytes sourceBytes = SdkBytes.fromInputStream(sourceStream);

           Attachment attachment = Attachment.builder()
                   .fileName(myFile.getName())
                   .data(sourceBytes)
                   .build();

           AddAttachmentsToSetRequest setRequest =
AddAttachmentsToSetRequest.builder()
                   .attachments(attachment)
                   .build();

           AddAttachmentsToSetResponse response =
supportClient.addAttachmentsToSet(setRequest);
           return response.attachmentSetId();
```

```
        } catch (SupportException | FileNotFoundException e) {
            System.out.println(e.getLocalizedMessage());
            System.exit(1);
        }
        return "";
    }
```

- Para obtener más información sobre la API, consulta AddAttachmentsToSetla Referencia AWS SDK for Java 2.x de la API.

JavaScript

SDK para JavaScript (v3)

> **Note**
>
> Hay más información. GitHub Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
import { AddAttachmentsToSetCommand } from "@aws-sdk/client-support";

import { client } from "../libs/client.js";

export const main = async () => {
  try {
    // Create a new attachment set or add attachments to an existing set.
    // Provide an 'attachmentSetId' value to add attachments to an existing set.
    // Use AddCommunicationToCase or CreateCase to associate an attachment set
 with a support case.
    const response = await client.send(
      new AddAttachmentsToSetCommand({
        // You can add up to three attachments per set. The size limit is 5 MB
 per attachment.
        attachments: [
          {
            fileName: "example.txt",
            data: new TextEncoder().encode("some example text"),
          },
        ],
```

```
      }),
    );
    // Use this ID in AddCommunicationToCase or CreateCase.
    console.log(response.attachmentSetId);
    return response;
  } catch (err) {
    console.error(err);
  }
};
```

- Para obtener más información sobre la API, consulta AddAttachmentsToSetla Referencia AWS SDK for JavaScript de la API.

Kotlin

SDK para Kotlin

> **Note**
>
> Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
suspend fun addAttachment(fileAttachment: String): String? {
    val myFile = File(fileAttachment)
    val sourceBytes = (File(fileAttachment).readBytes())
    val attachmentVal =
        Attachment {
            fileName = myFile.name
            data = sourceBytes
        }

    val setRequest =
        AddAttachmentsToSetRequest {
            attachments = listOf(attachmentVal)
        }

    SupportClient { region = "us-west-2" }.use { supportClient ->
        val response = supportClient.addAttachmentsToSet(setRequest)
        return response.attachmentSetId
```

```
    }
}
```

- Para obtener más información sobre la API, consulta AddAttachmentsToSetla referencia sobre el AWS SDK para la API de Kotlin.

Python

SDK para Python (Boto3)

> **Note**
>
> Hay más información al respecto. GitHub Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
class SupportWrapper:
    """Encapsulates Support actions."""

    def __init__(self, support_client):
        """
        :param support_client: A Boto3 Support client.
        """
        self.support_client = support_client

    @classmethod
    def from_client(cls):
        """
        Instantiates this class from a Boto3 client.
        """
        support_client = boto3.client("support")
        return cls(support_client)


    def add_attachment_to_set(self):
        """
        Add an attachment to a set, or create a new attachment set if one does
 not exist.

        :return: The attachment set ID.
```

```
        """
        try:
            response = self.support_client.add_attachments_to_set(
                attachments=[
                    {
                        "fileName": "attachment_file.txt",
                        "data": b"This is a sample file for attachment to a
support case.",
                    }
                ]
            )
            new_set_id = response["attachmentSetId"]
        except ClientError as err:
            if err.response["Error"]["Code"] == "SubscriptionRequiredException":
                logger.info(
                    "You must have a Business, Enterprise On-Ramp, or Enterprise
Support "
                    "plan to use the AWS Support API. \n\tPlease upgrade your
subscription to run these "
                    "examples."
                )
            else:
                logger.error(
                    "Couldn't add attachment. Here's why: %s: %s",
                    err.response["Error"]["Code"],
                    err.response["Error"]["Message"],
                )
                raise
        else:
            return new_set_id
```

- Para obtener más información sobre la API, consulta AddAttachmentsToSetla AWS Referencia de API de SDK for Python (Boto3).

Para obtener una lista completa de guías para desarrolladores del AWS SDK y ejemplos de código, consulte. AWS Support Utilizándolo con un AWS SDK En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

Úselo **AddCommunicationToCase** con un AWS SDK o CLI

En los siguientes ejemplos de código, se muestra cómo utilizar `AddCommunicationToCase`.

Los ejemplos de acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Puede ver esta acción en contexto en el siguiente ejemplo de código:

- Introducción a los casos

.NET

AWS SDK for .NET

> **Note**
>
> Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
    /// <summary>
    /// Add communication to a case, including optional attachment set ID and CC
 email addresses.
    /// </summary>
    /// <param name="caseId">Id for the support case.</param>
    /// <param name="body">Body text of the communication.</param>
    /// <param name="attachmentSetId">Optional Id for an attachment set.</param>
    /// <param name="ccEmailAddresses">Optional list of CC email addresses.</
param>
    /// <returns>True if successful.</returns>
    public async Task<bool> AddCommunicationToCase(string caseId, string body,
        string? attachmentSetId = null, List<string>? ccEmailAddresses = null)
    {
        var response = await _amazonSupport.AddCommunicationToCaseAsync(
            new AddCommunicationToCaseRequest()
            {
                CaseId = caseId,
                CommunicationBody = body,
                AttachmentSetId = attachmentSetId,
                CcEmailAddresses = ccEmailAddresses
            });
```

```
        return response.Result;
    }
```

- Para obtener más información sobre la API, consulta AddCommunicationToCasela Referencia AWS SDK for .NET de la API.

CLI

AWS CLI

Para añadir una comunicación a un caso

En el siguiente `add-communication-to-case` ejemplo, se agregan comunicaciones a un caso de soporte de tu AWS cuenta.

```
aws support add-communication-to-case \
    --case-id "case-12345678910-2013-c4c1d2bf33c5cf47" \
    --communication-body "I'm attaching a set of images to this case." \
    --cc-email-addresses "myemail@example.com" \
    --attachment-set-id "as-2f5a6faa2a4a1e600-mu-nk5xQlBr70-
G1cUos5LZkd38KOAHZa9BMDVzNEXAMPLE"
```

Salida:

```
{
    "result": true
}
```

Para obtener más información, consulte Administración de casos en la Guía del usuario de soporte de AWS .

- Para obtener información sobre la API, consulta AddCommunicationToCasela Referencia de AWS CLI comandos.

Java

SDK para Java 2.x

> **Note**
>
> Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
   public static void addAttachSupportCase(SupportClient supportClient, String
caseId, String attachmentSetId) {
       try {
           AddCommunicationToCaseRequest caseRequest =
AddCommunicationToCaseRequest.builder()
                   .caseId(caseId)
                   .attachmentSetId(attachmentSetId)
                   .communicationBody("Please refer to attachment for details.")
                   .build();

           AddCommunicationToCaseResponse response =
supportClient.addCommunicationToCase(caseRequest);
           if (response.result())
               System.out.println("You have successfully added a communication
to an AWS Support case");
           else
               System.out.println("There was an error adding the communication
to an AWS Support case");

       } catch (SupportException e) {
           System.out.println(e.getLocalizedMessage());
           System.exit(1);
       }
   }
```

- Para obtener más información sobre la API, consulta AddCommunicationToCasela Referencia AWS SDK for Java 2.x de la API.

JavaScript

SDK para JavaScript (v3)

> **Note**
>
> Hay más información. GitHub Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
import { AddCommunicationToCaseCommand } from "@aws-sdk/client-support";

import { client } from "../libs/client.js";

export const main = async () => {
  let attachmentSetId;

  try {
    // Add a communication to a case.
    const response = await client.send(
      new AddCommunicationToCaseCommand({
        communicationBody: "Adding an attachment.",
        // Set value to an existing support case id.
        caseId: "CASE_ID",
        // Optional. Set value to an existing attachment set id to add
 attachments to the case.
        attachmentSetId,
      }),
    );
    console.log(response);
    return response;
  } catch (err) {
    console.error(err);
  }
};
```

- Para obtener más información sobre la API, consulta AddCommunicationToCasela Referencia AWS SDK for JavaScript de la API.

Kotlin

SDK para Kotlin

> **Note**
>
> Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
suspend fun addAttachSupportCase(
    caseIdVal: String?,
    attachmentSetIdVal: String?
) {
    val caseRequest =
        AddCommunicationToCaseRequest {
            caseId = caseIdVal
            attachmentSetId = attachmentSetIdVal
            communicationBody = "Please refer to attachment for details."
        }

    SupportClient { region = "us-west-2" }.use { supportClient ->
        val response = supportClient.addCommunicationToCase(caseRequest)
        if (response.result) {
            println("You have successfully added a communication to an AWS
 Support case")
        } else {
            println("There was an error adding the communication to an AWS
 Support case")
        }
    }
}
```

- Para obtener más información sobre la API, consulta AddCommunicationToCasela referencia sobre el AWS SDK para la API de Kotlin.

PowerShell

Herramientas para PowerShell

Ejemplo 1: agrega el cuerpo de una comunicación de correo electrónico al caso especificado.

```
Add-ASACommunicationToCase -CaseId "case-12345678910-2013-c4c1d2bf33c5cf47" -
CommunicationBody "Some text about the case"
```

Ejemplo 2: agrega el cuerpo de una comunicación de correo electrónico a las mayúsculas y minúsculas especificadas más una o más direcciones de correo electrónico contenidas en la línea CC del correo electrónico.

```
Add-ASACommunicationToCase -CaseId "case-12345678910-2013-c4c1d2bf33c5cf47" -
CcEmailAddress @("email1@address.com", "email2@address.com") -CommunicationBody
 "Some text about the case"
```

- Para obtener información sobre la API, consulte AddCommunicationToCasela referencia de AWS Tools for PowerShell cmdlets.

Python

SDK para Python (Boto3)

> **Note**
>
> Hay más información al respecto. GitHub Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
class SupportWrapper:
    """Encapsulates Support actions."""

    def __init__(self, support_client):
        """
        :param support_client: A Boto3 Support client.
        """
        self.support_client = support_client

    @classmethod
```

```
    def from_client(cls):
        """
        Instantiates this class from a Boto3 client.
        """
        support_client = boto3.client("support")
        return cls(support_client)


    def add_communication_to_case(self, attachment_set_id, case_id):
        """
        Add a communication and an attachment set to a case.

        :param attachment_set_id: The ID of an existing attachment set.
        :param case_id: The ID of the case.
        """
        try:
            self.support_client.add_communication_to_case(
                caseId=case_id,
                communicationBody="This is an example communication added to a
support case.",
                attachmentSetId=attachment_set_id,
            )
        except ClientError as err:
            if err.response["Error"]["Code"] == "SubscriptionRequiredException":
                logger.info(
                    "You must have a Business, Enterprise On-Ramp, or Enterprise
Support "
                    "plan to use the AWS Support API. \n\tPlease upgrade your
subscription to run these "
                    "examples."
                )
            else:
                logger.error(
                    "Couldn't add communication. Here's why: %s: %s",
                    err.response["Error"]["Code"],
                    err.response["Error"]["Message"],
                )
                raise
```

- Para obtener más información sobre la API, consulta AddCommunicationToCasela AWS Referencia de API de SDK for Python (Boto3).

Para obtener una lista completa de guías para desarrolladores del AWS SDK y ejemplos de código, consulte. AWS Support Utilizándolo con un AWS SDK En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

Úselo **`CreateCase`** con un AWS SDK o CLI

En los siguientes ejemplos de código, se muestra cómo utilizar `CreateCase`.

Los ejemplos de acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Puede ver esta acción en contexto en el siguiente ejemplo de código:

- Introducción a los casos

.NET

AWS SDK for .NET

> **Note**
>
> Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
   /// <summary>
   /// Create a new support case.
   /// </summary>
   /// <param name="serviceCode">Service code for the new case.</param>
   /// <param name="categoryCode">Category for the new case.</param>
   /// <param name="severityCode">Severity code for the new case.</param>
   /// <param name="subject">Subject of the new case.</param>
   /// <param name="body">Body text of the new case.</param>
   /// <param name="language">Optional language support for your case.
   /// Currently Chinese (“zh”), English ("en"), Japanese ("ja") and Korean
(“ko”) are supported.</param>
   /// <param name="attachmentSetId">Optional Id for an attachment set for the
new case.</param>
   /// <param name="issueType">Optional issue type for the new case. Options are
"customer-service" or "technical".</param>
   /// <returns>The caseId of the new support case.</returns>
```

```
    public async Task<string> CreateCase(string serviceCode, string categoryCode,
 string severityCode, string subject,
        string body, string language = "en", string? attachmentSetId = null,
 string issueType = "customer-service")
    {
        var response = await _amazonSupport.CreateCaseAsync(
            new CreateCaseRequest()
            {
                ServiceCode = serviceCode,
                CategoryCode = categoryCode,
                SeverityCode = severityCode,
                Subject = subject,
                Language = language,
                AttachmentSetId = attachmentSetId,
                IssueType = issueType,
                CommunicationBody = body
            });
        return response.CaseId;
    }
```

- Para obtener más información sobre la API, consulta CreateCasela Referencia AWS SDK for .NET de la API.

CLI

AWS CLI

Creación de un caso

En el siguiente `create-case` ejemplo, se crea un caso de soporte para tu AWS cuenta.

```
aws support create-case \
    --category-code "using-aws" \
    --cc-email-addresses "myemail@example.com" \
    --communication-body "I want to learn more about an AWS service." \
    --issue-type "technical" \
    --language "en" \
    --service-code "general-info" \
    --severity-code "low" \
    --subject "Question about my account"
```

Salida:

```
{
    "caseId": "case-12345678910-2013-c4c1d2bf33c5cf47"
}
```

Para obtener más información, consulte Administración de casos en la Guía del usuario de soporte de AWS .

- Para obtener más información sobre la API, consulta CreateCasela Referencia de AWS CLI comandos.

Java

SDK para Java 2.x

> **Note**
>
> Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
   public static String createSupportCase(SupportClient supportClient,
List<String> sevCatList, String sevLevel) {
       try {
           String serviceCode = sevCatList.get(0);
           String caseCat = sevCatList.get(1);
           CreateCaseRequest caseRequest = CreateCaseRequest.builder()
                   .categoryCode(caseCat.toLowerCase())
                   .serviceCode(serviceCode.toLowerCase())
                   .severityCode(sevLevel.toLowerCase())
                   .communicationBody("Test issue with " +
serviceCode.toLowerCase())
                   .subject("Test case, please ignore")
                   .language("en")
                   .issueType("technical")
                   .build();

           CreateCaseResponse response = supportClient.createCase(caseRequest);
           return response.caseId();
```

```
        } catch (SupportException e) {
            System.out.println(e.getLocalizedMessage());
            System.exit(1);
        }
        return "";
    }
```

- Para obtener más información sobre la API, consulta CreateCasela Referencia AWS SDK for Java 2.x de la API.

JavaScript

SDK para JavaScript (v3)

> **Note**
>
> Hay más información. GitHub Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
import { CreateCaseCommand } from "@aws-sdk/client-support";

import { client } from "../libs/client.js";

export const main = async () => {
  try {
    // Create a new case and log the case id.
    // Important: This creates a real support case in your account.
    const response = await client.send(
      new CreateCaseCommand({
        // The subject line of the case.
        subject: "IGNORE: Test case",
        // Use DescribeServices to find available service codes for each service.
        serviceCode: "service-quicksight-end-user",
        // Use DescribeSecurityLevels to find available severity codes for your
 support plan.
        severityCode: "low",
        // Use DescribeServices to find available category codes for each
 service.
        categoryCode: "end-user-support",
```

```
        // The main description of the support case.
        communicationBody: "This is a test. Please ignore.",
      }),
    );
    console.log(response.caseId);
    return response;
  } catch (err) {
    console.error(err);
  }
};
```

- Para obtener más información sobre la API, consulta CreateCasela Referencia AWS SDK for JavaScript de la API.

Kotlin

SDK para Kotlin

> **Note**
>
> Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
suspend fun createSupportCase(
    sevCatListVal: List<String>,
    sevLevelVal: String
): String? {
    val serCode = sevCatListVal[0]
    val caseCategory = sevCatListVal[1]
    val caseRequest =
        CreateCaseRequest {
            categoryCode = caseCategory.lowercase(Locale.getDefault())
            serviceCode = serCode.lowercase(Locale.getDefault())
            severityCode = sevLevelVal.lowercase(Locale.getDefault())
            communicationBody = "Test issue with
 ${serCode.lowercase(Locale.getDefault())}"
            subject = "Test case, please ignore"
            language = "en"
            issueType = "technical"
```

```
        }

    SupportClient { region = "us-west-2" }.use { supportClient ->
        val response = supportClient.createCase(caseRequest)
        return response.caseId
    }
}
```

- Para obtener más información sobre la API, consulta CreateCasela referencia sobre el AWS SDK para la API de Kotlin.

PowerShell

Herramientas para PowerShell

Ejemplo 1: Crea un nuevo caso en el AWS Support Center. Los valores de los CategoryCode parámetros - ServiceCode y - se pueden obtener mediante el cmdlet Get-AsaService. El valor del SeverityCode parámetro - se puede obtener mediante el cmdlet Get-ASA. SeverityLevel El valor del IssueType parámetro - puede ser «servicio al cliente» o «técnico». Si tiene éxito, se AWS mostrará el número de caso de Support. De forma predeterminada, las mayúsculas y minúsculas se gestionarán en inglés. Para usar japonés, añada el parámetro «ja» en el idioma. Los CommunicationBody parámetros -ServiceCode, -CategoryCode, -Subject y - son obligatorios.

```
New-ASACase -ServiceCode "amazon-cloudfront" -CategoryCode "APIs" -SeverityCode
 "low" -Subject "subject text" -CommunicationBody "description of the case" -
CcEmailAddress @("email1@domain.com", "email2@domain.com") -IssueType "technical"
```

- Para obtener más información sobre la API, consulte la referencia CreateCasedel AWS Tools for PowerShell cmdlet.

Python

SDK para Python (Boto3)

> **Note**
>
> Hay más información al respecto. GitHub Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
class SupportWrapper:
    """Encapsulates Support actions."""

    def __init__(self, support_client):
        """
        :param support_client: A Boto3 Support client.
        """
        self.support_client = support_client

    @classmethod
    def from_client(cls):
        """
        Instantiates this class from a Boto3 client.
        """
        support_client = boto3.client("support")
        return cls(support_client)


    def create_case(self, service, category, severity):
        """
        Create a new support case.

        :param service: The service to use for the new case.
        :param category: The category to use for the new case.
        :param severity: The severity to use for the new case.
        :return: The caseId of the new case.
        """
        try:
            response = self.support_client.create_case(
                subject="Example case for testing, ignore.",
                serviceCode=service["code"],
                severityCode=severity["code"],
```

```
                categoryCode=category["code"],
                communicationBody="Example support case body.",
                language="en",
                issueType="customer-service",
            )
            case_id = response["caseId"]
        except ClientError as err:
            if err.response["Error"]["Code"] == "SubscriptionRequiredException":
                logger.info(
                    "You must have a Business, Enterprise On-Ramp, or Enterprise
Support "
                    "plan to use the AWS Support API. \n\tPlease upgrade your
subscription to run these "
                    "examples."
                )
            else:
                logger.error(
                    "Couldn't create case. Here's why: %s: %s",
                    err.response["Error"]["Code"],
                    err.response["Error"]["Message"],
                )
                raise
        else:
            return case_id
```

- Para obtener más información sobre la API, consulta CreateCasela AWS Referencia de API de SDK for Python (Boto3).

Para obtener una lista completa de guías para desarrolladores del AWS SDK y ejemplos de código, consulte. AWS Support Utilizándolo con un AWS SDK En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

Úselo **`DescribeAttachment`** con un AWS SDK o CLI

En los siguientes ejemplos de código, se muestra cómo utilizar `DescribeAttachment`.

Los ejemplos de acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Puede ver esta acción en contexto en el siguiente ejemplo de código:

- Introducción a los casos

.NET

AWS SDK for .NET

> **Note**
>
> Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
    /// <summary>
    /// Get description of a specific attachment.
    /// </summary>
    /// <param name="attachmentId">Id of the attachment, usually fetched by
describing the communications of a case.</param>
    /// <returns>The attachment object.</returns>
    public async Task<Attachment> DescribeAttachment(string attachmentId)
    {
        var response = await _amazonSupport.DescribeAttachmentAsync(
            new DescribeAttachmentRequest()
            {
                AttachmentId = attachmentId
            });
        return response.Attachment;
    }
```

- Para obtener más información sobre la API, consulta DescribeAttachmentla Referencia AWS SDK for .NET de la API.

CLI

AWS CLI

Descripción de un archivo adjunto

El siguiente ejemplo de `describe-attachment` devuelve información sobre el archivo adjunto con el ID especificado.

```
aws support describe-attachment \
    --attachment-id "attachment-KBnjRNrePd9D6Jx0-Mm00xZuDEaL2JAj_0-
gJv9qqDooTipsz3V1Nb19rCfkZneeQeDPgp8X1iVJyHH7UuhZDdNeqGoduZsPrAhyMakqlc60-
iJjL5HqyYGiT1FG8EXAMPLE"
```

Salida:

```
{
    "attachment": {
        "fileName": "troubleshoot-screenshot.png",
        "data": "base64-blob"
    }
}
```

Para obtener más información, consulte Administración de casos en la Guía del usuario de soporte de AWS .

- Para obtener más información sobre la API, consulta DescribeAttachmentla Referencia de AWS CLI comandos.

Java

SDK para Java 2.x

> **Note**
>
> Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
   public static void describeAttachment(SupportClient supportClient, String
attachId) {
       try {
           DescribeAttachmentRequest attachmentRequest =
DescribeAttachmentRequest.builder()
                   .attachmentId(attachId)
                   .build();

           DescribeAttachmentResponse response =
supportClient.describeAttachment(attachmentRequest);
```

```
            System.out.println("The name of the file is " +
 response.attachment().fileName());

        } catch (SupportException e) {
            System.out.println(e.getLocalizedMessage());
            System.exit(1);
        }
    }
```

- Para obtener más información sobre la API, consulta DescribeAttachmentla Referencia AWS SDK for Java 2.x de la API.

JavaScript

SDK para JavaScript (v3)

> **Note**
>
> Hay más información. GitHub Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
import { DescribeAttachmentCommand } from "@aws-sdk/client-support";

import { client } from "../libs/client.js";

export const main = async () => {
  try {
    // Get the metadata and content of an attachment.
    const response = await client.send(
      new DescribeAttachmentCommand({
        // Set value to an existing attachment id.
        // Use DescribeCommunications or DescribeCases to find an attachment id.
        attachmentId: "ATTACHMENT_ID",
      }),
    );
    console.log(response.attachment?.fileName);
    return response;
  } catch (err) {
    console.error(err);
```

```
  }
};
```

- Para obtener más información sobre la API, consulta DescribeAttachmentla Referencia AWS SDK for JavaScript de la API.

Kotlin

SDK para Kotlin

> **Note**
>
> Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
suspend fun describeAttachment(attachId: String?) {
    val attachmentRequest =
        DescribeAttachmentRequest {
            attachmentId = attachId
        }

    SupportClient { region = "us-west-2" }.use { supportClient ->
        val response = supportClient.describeAttachment(attachmentRequest)
        println("The name of the file is ${response.attachment?.fileName}")
    }
}
```

- Para obtener más información sobre la API, consulta DescribeAttachmentla referencia sobre el AWS SDK para la API de Kotlin.

Python

SDK para Python (Boto3)

> **Note**
>
> Hay más información al respecto. GitHub Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
class SupportWrapper:
    """Encapsulates Support actions."""

    def __init__(self, support_client):
        """
        :param support_client: A Boto3 Support client.
        """
        self.support_client = support_client

    @classmethod
    def from_client(cls):
        """
        Instantiates this class from a Boto3 client.
        """
        support_client = boto3.client("support")
        return cls(support_client)


    def describe_attachment(self, attachment_id):
        """
        Get information about an attachment by its attachmentID.

        :param attachment_id: The ID of the attachment.
        :return: The name of the attached file.
        """
        try:
            response = self.support_client.describe_attachment(
                attachmentId=attachment_id
            )
            attached_file = response["attachment"]["fileName"]
        except ClientError as err:
            if err.response["Error"]["Code"] == "SubscriptionRequiredException":
```

```
                logger.info(
                    "You must have a Business, Enterprise On-Ramp, or Enterprise
Support "
                    "plan to use the AWS Support API. \n\tPlease upgrade your
subscription to run these "
                    "examples."
                )
            else:
                logger.error(
                    "Couldn't get attachment description. Here's why: %s: %s",
                    err.response["Error"]["Code"],
                    err.response["Error"]["Message"],
                )
                raise
        else:
            return attached_file


```

- Para obtener más información sobre la API, consulta DescribeAttachmentla AWS Referencia de API de SDK for Python (Boto3).

Para obtener una lista completa de guías para desarrolladores del AWS SDK y ejemplos de código, consulte. AWS Support Utilizándolo con un AWS SDK En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

Úselo **`DescribeCases`** con un AWS SDK o CLI

En los siguientes ejemplos de código, se muestra cómo utilizar `DescribeCases`.

Los ejemplos de acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Puede ver esta acción en contexto en el siguiente ejemplo de código:

- Introducción a los casos

.NET

AWS SDK for .NET

> **Note**
>
> Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
    /// <summary>
    /// Get case details for a list of case ids, optionally with date filters.
    /// </summary>
    /// <param name="caseIds">The list of case IDs.</param>
    /// <param name="displayId">Optional display ID.</param>
    /// <param name="includeCommunication">True to include communication.
 Defaults to true.</param>
    /// <param name="includeResolvedCases">True to include resolved cases.
 Defaults to false.</param>
    /// <param name="afterTime">The optional start date for a filtered search.</
param>
    /// <param name="beforeTime">The optional end date for a filtered search.</
param>
    /// <param name="language">Optional language support for your case.
    /// Currently Chinese (“zh”), English ("en"), Japanese ("ja") and Korean
 (“ko”) are supported.</param>
    /// <returns>A list of CaseDetails.</returns>
    public async Task<List<CaseDetails>> DescribeCases(List<string> caseIds,
 string? displayId = null, bool includeCommunication = true,
        bool includeResolvedCases = false, DateTime? afterTime = null, DateTime?
 beforeTime = null,
        string language = "en")
    {
        var results = new List<CaseDetails>();
        var paginateCases = _amazonSupport.Paginators.DescribeCases(
            new DescribeCasesRequest()
            {
                CaseIdList = caseIds,
                DisplayId = displayId,
                IncludeCommunications = includeCommunication,
                IncludeResolvedCases = includeResolvedCases,
```

```
                AfterTime = afterTime?.ToString("s"),
                BeforeTime = beforeTime?.ToString("s"),
                Language = language
            });
        // Get the entire list using the paginator.
        await foreach (var cases in paginateCases.Cases)
        {
            results.Add(cases);
        }
        return results;
    }
```

- Para obtener más información sobre la API, consulta DescribeCasesla Referencia AWS SDK for .NET de la API.

CLI

AWS CLI

Descripción de un caso

El siguiente `describe-cases` ejemplo devuelve información sobre el caso de soporte especificado en tu AWS cuenta.

```
aws support describe-cases \
    --display-id "1234567890" \
    --after-time "2020-03-23T21:31:47.774Z" \
    --include-resolved-cases \
    --language "en" \
    --no-include-communications \
    --max-item 1
```

Salida:

```
{
    "cases": [
        {
            "status": "resolved",
            "ccEmailAddresses": [],
```

```
            "timeCreated": "2020-03-23T21:31:47.774Z",
            "caseId": "case-12345678910-2013-c4c1d2bf33c5cf47",
            "severityCode": "low",
            "language": "en",
            "categoryCode": "using-aws",
            "serviceCode": "general-info",
            "submittedBy": "myemail@example.com",
            "displayId": "1234567890",
            "subject": "Question about my account"
        }
    ]
}
```

Para obtener más información, consulte Administración de casos en la Guía del usuario de soporte de AWS .

- Para obtener información sobre la API, consulta DescribeCasesla Referencia de AWS CLI comandos.

Java

SDK para Java 2.x

> **Note**
>
> Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
    public static void getOpenCase(SupportClient supportClient) {
        try {
            // Specify the start and end time.
            Instant now = Instant.now();
            java.time.LocalDate.now();
            Instant yesterday = now.minus(1, ChronoUnit.DAYS);

            DescribeCasesRequest describeCasesRequest =
DescribeCasesRequest.builder()
                    .maxResults(20)
                    .afterTime(yesterday.toString())
                    .beforeTime(now.toString())
                    .build();
```

```
            DescribeCasesResponse response =
 supportClient.describeCases(describeCasesRequest);
            List<CaseDetails> cases = response.cases();
            for (CaseDetails sinCase : cases) {
                System.out.println("The case status is " + sinCase.status());
                System.out.println("The case Id is " + sinCase.caseId());
                System.out.println("The case subject is " + sinCase.subject());
            }

        } catch (SupportException e) {
            System.out.println(e.getLocalizedMessage());
            System.exit(1);
        }
    }
```

- Para obtener más información sobre la API, consulta DescribeCasesla Referencia AWS SDK for Java 2.x de la API.

JavaScript

SDK para JavaScript (v3)

> **Note**
>
> Hay más información. GitHub Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
import { DescribeCasesCommand } from "@aws-sdk/client-support";

import { client } from "../libs/client.js";

export const main = async () => {
  try {
    // Get all of the unresolved cases in your account.
    // Filter or expand results by providing parameters to the
 DescribeCasesCommand. Refer
    // to the TypeScript definition and the API doc for more information on
 possible parameters.
```

```
    // https://docs.aws.amazon.com/AWSJavaScriptSDK/v3/latest/clients/client-
support/interfaces/describecasescommandinput.html
    const response = await client.send(new DescribeCasesCommand({}));
    const caseIds = response.cases.map((supportCase) => supportCase.caseId);
    console.log(caseIds);
    return response;
  } catch (err) {
    console.error(err);
  }
};
```

- Para obtener más información sobre la API, consulta DescribeCasesla Referencia AWS SDK for JavaScript de la API.

Kotlin

SDK para Kotlin

> **Note**
>
> Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
suspend fun getOpenCase() {
    // Specify the start and end time.
    val now = Instant.now()
    LocalDate.now()
    val yesterday = now.minus(1, ChronoUnit.DAYS)
    val describeCasesRequest =
        DescribeCasesRequest {
            maxResults = 20
            afterTime = yesterday.toString()
            beforeTime = now.toString()
        }

    SupportClient { region = "us-west-2" }.use { supportClient ->
        val response = supportClient.describeCases(describeCasesRequest)
        response.cases?.forEach { sinCase ->
            println("The case status is ${sinCase.status}")
```

```
            println("The case Id is ${sinCase.caseId}")
            println("The case subject is ${sinCase.subject}")
        }
    }
}
```

- Para obtener más información sobre la API, consulta DescribeCaseslа referencia sobre el AWS SDK para la API de Kotlin.

PowerShell

Herramientas para PowerShell

Ejemplo 1: Devuelve los detalles de todos los casos de soporte.

```
Get-ASACase
```

Ejemplo 2: Devuelve los detalles de todos los casos de soporte desde la fecha y hora especificadas.

```
Get-ASACase -AfterTime "2013-09-10T03:06Z"
```

Ejemplo 3: Devuelve los detalles de los primeros 10 casos de soporte, incluidos los que se han resuelto.

```
Get-ASACase -MaxResult 10 -IncludeResolvedCases $true
```

Ejemplo 4: devuelve los detalles del único caso de soporte especificado.

```
Get-ASACase -CaseIdList "case-12345678910-2013-c4c1d2bf33c5cf47"
```

Ejemplo 5: Devuelve los detalles de los casos de soporte especificados.

```
Get-ASACase -CaseIdList @("case-12345678910-2013-c4c1d2bf33c5cf47",
 "case-18929034710-2011-c4fdeabf33c5cf47")
```

Ejemplo 6: devuelve todos los casos de soporte mediante la paginación manual. Los estuches se recuperan en lotes de 20.

```
$nextToken = $null
do {
  Get-ASACase -NextToken $nextToken -MaxResult 20
  $nextToken = $AWSHistory.LastServiceResponse.NextToken
} while ($nextToken -ne $null)
```

- Para obtener más información sobre la API, consulte la referencia DescribeCasesde AWS Tools for PowerShell cmdlets.

Python

SDK para Python (Boto3)

> **Note**
>
> Hay más información al respecto. GitHub Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
class SupportWrapper:
    """Encapsulates Support actions."""

    def __init__(self, support_client):
        """
        :param support_client: A Boto3 Support client.
        """
        self.support_client = support_client

    @classmethod
    def from_client(cls):
        """
        Instantiates this class from a Boto3 client.
        """
        support_client = boto3.client("support")
        return cls(support_client)


    def describe_cases(self, after_time, before_time, resolved):
        """
        Describe support cases over a period of time, optionally filtering
        by status.
```

```
        :param after_time: The start time to include for cases.
        :param before_time: The end time to include for cases.
        :param resolved: True to include resolved cases in the results,
            otherwise results are open cases.
        :return: The final status of the case.
        """
        try:
            cases = []
            paginator = self.support_client.get_paginator("describe_cases")
            for page in paginator.paginate(
                afterTime=after_time,
                beforeTime=before_time,
                includeResolvedCases=resolved,
                language="en",
            ):
                cases += page["cases"]
        except ClientError as err:
            if err.response["Error"]["Code"] == "SubscriptionRequiredException":
                logger.info(
                    "You must have a Business, Enterprise On-Ramp, or Enterprise
Support "
                    "plan to use the AWS Support API. \n\tPlease upgrade your
subscription to run these "
                    "examples."
                )
            else:
                logger.error(
                    "Couldn't describe cases. Here's why: %s: %s",
                    err.response["Error"]["Code"],
                    err.response["Error"]["Message"],
                )
                raise
        else:
            if resolved:
                cases = filter(lambda case: case["status"] == "resolved", cases)
            return cases
```

- Para obtener más información sobre la API, consulta DescribeCasesla AWS Referencia de API de SDK for Python (Boto3).

Para obtener una lista completa de guías para desarrolladores del AWS SDK y ejemplos de código, consulte. AWS Support Utilizándolo con un AWS SDK En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

Úselo **`DescribeCommunications`** con un AWS SDK o CLI

En los siguientes ejemplos de código, se muestra cómo utilizar `DescribeCommunications`.

Los ejemplos de acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Puede ver esta acción en contexto en el siguiente ejemplo de código:

- Introducción a los casos

.NET

AWS SDK for .NET

> **Note**
>
> Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
    /// <summary>
    /// Describe the communications for a case, optionally with a date filter.
    /// </summary>
    /// <param name="caseId">The ID of the support case.</param>
    /// <param name="afterTime">The optional start date for a filtered search.</
param>
    /// <param name="beforeTime">The optional end date for a filtered search.</
param>
    /// <returns>The list of communications for the case.</returns>
    public async Task<List<Communication>> DescribeCommunications(string caseId,
 DateTime? afterTime = null, DateTime? beforeTime = null)
    {
        var results = new List<Communication>();
        var paginateCommunications =
 _amazonSupport.Paginators.DescribeCommunications(
            new DescribeCommunicationsRequest()
            {
```

```
                CaseId = caseId,
                AfterTime = afterTime?.ToString("s"),
                BeforeTime = beforeTime?.ToString("s")
            });
        // Get the entire list using the paginator.
        await foreach (var communications in
 paginateCommunications.Communications)
        {
            results.Add(communications);
        }
        return results;
    }
```

- Para obtener más información sobre la API, consulta DescribeCommunicationsla Referencia AWS SDK for .NET de la API.

CLI

AWS CLI

Descripción de la última comunicación de un caso

En el siguiente `describe-communications` ejemplo, se devuelve la última comunicación del caso de soporte especificado en tu AWS cuenta.

```
aws support describe-communications \
    --case-id "case-12345678910-2013-c4c1d2bf33c5cf47" \
    --after-time "2020-03-23T21:31:47.774Z" \
    --max-item 1
```

Salida:

```
{
    "communications": [
        {
            "body": "I want to learn more about an AWS service.",
            "attachmentSet": [],
            "caseId": "case-12345678910-2013-c4c1d2bf33c5cf47",
            "timeCreated": "2020-05-12T23:12:35.000Z",
            "submittedBy": "Amazon Web Services"
```

```
        }
    ],
    "NextToken":
 "eyJuZXh0VG9rZW4iOiBudWxsLCAiYm90b190cnVuY2F0ZV9hbW91bnQEXAMPLE=="
}
```

Para obtener más información, consulte Administración de casos en la Guía del usuario de soporte de AWS .

- Para obtener información sobre la API, consulta DescribeCommunicationsla Referencia de AWS CLI comandos.

Java

SDK para Java 2.x

> **Note**
>
> Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
   public static String listCommunications(SupportClient supportClient, String
caseId) {
       try {
           String attachId = null;
           DescribeCommunicationsRequest communicationsRequest =
DescribeCommunicationsRequest.builder()
                   .caseId(caseId)
                   .maxResults(10)
                   .build();

           DescribeCommunicationsResponse response =
supportClient.describeCommunications(communicationsRequest);
           List<Communication> communications = response.communications();
           for (Communication comm : communications) {
               System.out.println("the body is: " + comm.body());

               // Get the attachment id value.
               List<AttachmentDetails> attachments = comm.attachmentSet();
               for (AttachmentDetails detail : attachments) {
                   attachId = detail.attachmentId();
```

```
                }
            }
            return attachId;

        } catch (SupportException e) {
            System.out.println(e.getLocalizedMessage());
            System.exit(1);
        }
        return "";
    }
```

- Para obtener más información sobre la API, consulta DescribeCommunicationsla Referencia AWS SDK for Java 2.x de la API.

JavaScript

SDK para JavaScript (v3)

> **Note**
>
> Hay más información. GitHub Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
import { DescribeCommunicationsCommand } from "@aws-sdk/client-support";

import { client } from "../libs/client.js";

export const main = async () => {
  try {
    // Get all communications for the support case.
    // Filter results by providing parameters to the
 DescribeCommunicationsCommand. Refer
    // to the TypeScript definition and the API doc for more information on
 possible parameters.
    // https://docs.aws.amazon.com/AWSJavaScriptSDK/v3/latest/clients/client-
support/interfaces/describecommunicationscommandinput.html
    const response = await client.send(
      new DescribeCommunicationsCommand({
        // Set value to an existing case id.
```

```
        caseId: "CASE_ID",
      }),
    );
    const text = response.communications.map((item) => item.body).join("\n");
    console.log(text);
    return response;
  } catch (err) {
    console.error(err);
  }
};
```

- Para obtener más información sobre la API, consulta DescribeCommunicationsla Referencia AWS SDK for JavaScript de la API.

Kotlin

SDK para Kotlin

> **Note**
>
> Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
suspend fun listCommunications(caseIdVal: String?): String? {
    val communicationsRequest =
        DescribeCommunicationsRequest {
            caseId = caseIdVal
            maxResults = 10
        }

    SupportClient { region = "us-west-2" }.use { supportClient ->
        val response =
 supportClient.describeCommunications(communicationsRequest)
        response.communications?.forEach { comm ->
            println("the body is: " + comm.body)
            comm.attachmentSet?.forEach { detail ->
                return detail.attachmentId
            }
        }
```

```
    }
    return ""
}
```

- Para obtener más información sobre la API, consulta DescribeCommunicationsla referencia sobre el AWS SDK para la API de Kotlin.

PowerShell

Herramientas para PowerShell

Ejemplo 1: devuelve todas las comunicaciones del caso especificado.

```
Get-ASACommunication -CaseId "case-12345678910-2013-c4c1d2bf33c5cf47"
```

Ejemplo 2: devuelve todas las comunicaciones desde la medianoche (UTC) del 1 de enero de 2012 para el caso especificado.

```
Get-ASACommunication -CaseId "case-12345678910-2013-c4c1d2bf33c5cf47" -AfterTime
 "2012-01-10T00:00Z"
```

Ejemplo 3: devuelve todas las comunicaciones desde la medianoche (UTC) del 1 de enero de 2012, en el caso especificado, mediante la búsqueda manual. Las comunicaciones se recuperan en lotes de 20.

```
$nextToken = $null
do {
  Get-ASACommunication -CaseId "case-12345678910-2013-c4c1d2bf33c5cf47" -
NextToken $nextToken -MaxResult 20
  $nextToken = $AWSHistory.LastServiceResponse.NextToken
} while ($nextToken -ne $null)
```

- Para obtener más información sobre la API, consulte la referencia DescribeCommunicationsde AWS Tools for PowerShell cmdlets.

Python

SDK para Python (Boto3)

> **Note**
>
> Hay más información al respecto. GitHub Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
class SupportWrapper:
    """Encapsulates Support actions."""

    def __init__(self, support_client):
        """
        :param support_client: A Boto3 Support client.
        """
        self.support_client = support_client

    @classmethod
    def from_client(cls):
        """
        Instantiates this class from a Boto3 client.
        """
        support_client = boto3.client("support")
        return cls(support_client)


    def describe_all_case_communications(self, case_id):
        """
        Describe all the communications for a case using a paginator.

        :param case_id: The ID of the case.
        :return: The communications for the case.
        """
        try:
            communications = []
            paginator =
 self.support_client.get_paginator("describe_communications")
            for page in paginator.paginate(caseId=case_id):
                communications += page["communications"]
        except ClientError as err:
```

```
            if err.response["Error"]["Code"] == "SubscriptionRequiredException":
                logger.info(
                    "You must have a Business, Enterprise On-Ramp, or Enterprise
Support "
                    "plan to use the AWS Support API. \n\tPlease upgrade your
subscription to run these "
                    "examples."
                )
            else:
                logger.error(
                    "Couldn't describe communications. Here's why: %s: %s",
                    err.response["Error"]["Code"],
                    err.response["Error"]["Message"],
                )
                raise
        else:
            return communications
```

- Para obtener más información sobre la API, consulta DescribeCommunicationsla AWS Referencia de API de SDK for Python (Boto3).

Para obtener una lista completa de guías para desarrolladores del AWS SDK y ejemplos de código, consulte. AWS Support Utilizándolo con un AWS SDK En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

Úselo **`DescribeServices`** con un AWS SDK o CLI

En los siguientes ejemplos de código, se muestra cómo utilizar `DescribeServices`.

Los ejemplos de acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Puede ver esta acción en contexto en el siguiente ejemplo de código:

- Introducción a los casos

.NET

AWS SDK for .NET

> **Note**
>
> Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
    /// <summary>
    /// Get the descriptions of AWS services.
    /// </summary>
    /// <param name="name">Optional language for services.
    /// Currently Chinese (“zh”), English ("en"), Japanese ("ja") and Korean
(“ko”) are supported.</param>
    /// <returns>The list of AWS service descriptions.</returns>
    public async Task<List<Service>> DescribeServices(string language = "en")
    {
        var response = await _amazonSupport.DescribeServicesAsync(
            new DescribeServicesRequest()
            {
                Language = language
            });
        return response.Services;
    }
```

- Para obtener más información sobre la API, consulta DescribeServicesla Referencia AWS SDK for .NET de la API.

CLI

AWS CLI

Para enumerar AWS los servicios y las categorías de servicios

En el siguiente ejemplo de `describe-services` se enumeran las categorías de servicios disponibles para solicitar información general.

```
aws support describe-services \
    --service-code-list "general-info"
```

Salida:

```
{
    "services": [
        {
            "code": "general-info",
            "name": "General Info and Getting Started",
            "categories": [
                {
                    "code": "charges",
                    "name": "How Will I Be Charged?"
                },
                {
                    "code": "gdpr-queries",
                    "name": "Data Privacy Query"
                },
                {
                    "code": "reserved-instances",
                    "name": "Reserved Instances"
                },
                {
                    "code": "resource",
                    "name": "Where is my Resource?"
                },
                {
                    "code": "using-aws",
                    "name": "Using AWS & Services"
                },
                {
                    "code": "free-tier",
                    "name": "Free Tier"
                },
                {
                    "code": "security-and-compliance",
                    "name": "Security & Compliance"
                },
                {
                    "code": "account-structure",
                    "name": "Account Structure"
                }
```

```
            ]
        }
    ]
}
```

Para obtener más información, consulte Administración de casos en la Guía del usuario de soporte de AWS .

- Para obtener más información sobre la API, consulte DescribeServicesla Referencia de AWS CLI comandos.

Java

SDK para Java 2.x

> **Note**
>
> Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
   // Return a List that contains a Service name and Category name.
   public static List<String> displayServices(SupportClient supportClient) {
       try {
           DescribeServicesRequest servicesRequest =
DescribeServicesRequest.builder()
                   .language("en")
                   .build();

           DescribeServicesResponse response =
supportClient.describeServices(servicesRequest);
           String serviceCode = null;
           String catName = null;
           List<String> sevCatList = new ArrayList<>();
           List<Service> services = response.services();

           System.out.println("Get the first 10 services");
           int index = 1;
           for (Service service : services) {
               if (index == 11)
                   break;
```

```
                System.out.println("The Service name is: " + service.name());
                if (service.name().compareTo("Account") == 0)
                    serviceCode = service.code();

                // Get the Categories for this service.
                List<Category> categories = service.categories();
                for (Category cat : categories) {
                    System.out.println("The category name is: " + cat.name());
                    if (cat.name().compareTo("Security") == 0)
                        catName = cat.name();
                }
                index++;
            }

            // Push the two values to the list.
            sevCatList.add(serviceCode);
            sevCatList.add(catName);
            return sevCatList;

        } catch (SupportException e) {
            System.out.println(e.getLocalizedMessage());
            System.exit(1);
        }
        return null;
    }
```

- Para obtener más información sobre la API, consulta DescribeServicesla Referencia AWS SDK for Java 2.x de la API.

Kotlin

SDK para Kotlin

> **Note**
>
> Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
// Return a List that contains a Service name and Category name.
```

```
suspend fun displayServices(): List<String> {
    var serviceCode = ""
    var catName = ""
    val sevCatList = mutableListOf<String>()
    val servicesRequest =
        DescribeServicesRequest {
            language = "en"
        }

    SupportClient { region = "us-west-2" }.use { supportClient ->
        val response = supportClient.describeServices(servicesRequest)
        println("Get the first 10 services")
        var index = 1

        response.services?.forEach { service ->
            if (index == 11) {
                return@forEach
            }

            println("The Service name is ${service.name}")
            if (service.name == "Account") {
                serviceCode = service.code.toString()
            }

            // Get the categories for this service.
            service.categories?.forEach { cat ->
                println("The category name is ${cat.name}")
                if (cat.name == "Security") {
                    catName = cat.name!!
                }
            }
            index++
        }
    }

    // Push the two values to the list.
    serviceCode.let { sevCatList.add(it) }
    catName.let { sevCatList.add(it) }
    return sevCatList
}
```

- Para obtener más información sobre la API, consulta DescribeServicesla referencia sobre el AWS SDK para la API de Kotlin.

PowerShell

Herramientas para PowerShell

Ejemplo 1: Devuelve todos los códigos, nombres y categorías de servicio disponibles.

```
Get-ASAService
```

Ejemplo 2: devuelve el nombre y las categorías del servicio con el código especificado.

```
Get-ASAService -ServiceCodeList "amazon-cloudfront"
```

Ejemplo 3: Devuelve el nombre y las categorías de los códigos de servicio especificados.

```
Get-ASAService -ServiceCodeList @("amazon-cloudfront", "amazon-cloudwatch")
```

Ejemplo 4: Devuelve el nombre y las categorías (en japonés) de los códigos de servicio especificados. Actualmente, se admiten los códigos de idioma inglés («en») y japonés («ja»).

```
Get-ASAService -ServiceCodeList @("amazon-cloudfront", "amazon-cloudwatch") -
Language "ja"
```

- Para obtener más información sobre la API, consulte DescribeServicesla Referencia de AWS Tools for PowerShell cmdlets.

Python

SDK para Python (Boto3)

> **Note**
>
> Hay más información al respecto. GitHub Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
class SupportWrapper:
```

```
    """Encapsulates Support actions."""

    def __init__(self, support_client):
        """
        :param support_client: A Boto3 Support client.
        """
        self.support_client = support_client

    @classmethod
    def from_client(cls):
        """
        Instantiates this class from a Boto3 client.
        """
        support_client = boto3.client("support")
        return cls(support_client)


    def describe_services(self, language):
        """
        Get the descriptions of AWS services available for support for a
language.

        :param language: The language for support services.
        Currently, only "en" (English) and "ja" (Japanese) are supported.
        :return: The list of AWS service descriptions.
        """
        try:
            response = self.support_client.describe_services(language=language)
            services = response["services"]
        except ClientError as err:
            if err.response["Error"]["Code"] == "SubscriptionRequiredException":
                logger.info(
                    "You must have a Business, Enterprise On-Ramp, or Enterprise
Support "
                    "plan to use the AWS Support API. \n\tPlease upgrade your
subscription to run these "
                    "examples."
                )
            else:
                logger.error(
                    "Couldn't get Support services for language %s. Here's why:
%s: %s",
                    language,
                    err.response["Error"]["Code"],
```

```
                err.response["Error"]["Message"],
            )
            raise
    else:
        return services
```

- Para obtener más información sobre la API, consulta DescribeServicesla AWS Referencia de API de SDK for Python (Boto3).

Para obtener una lista completa de guías para desarrolladores del AWS SDK y ejemplos de código, consulte. AWS Support Utilizándolo con un AWS SDK En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

Úselo **`DescribeSeverityLevels`** con un AWS SDK o CLI

En los siguientes ejemplos de código, se muestra cómo utilizar `DescribeSeverityLevels`.

Los ejemplos de acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Puede ver esta acción en contexto en el siguiente ejemplo de código:

- Introducción a los casos

.NET

AWS SDK for .NET

> **Note**
>
> Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
/// <summary>
/// Get the descriptions of support severity levels.
/// </summary>
/// <param name="name">Optional language for severity levels.
```

```
    /// Currently Chinese (“zh”), English ("en"), Japanese ("ja") and Korean
 (“ko”) are supported.</param>
    /// <returns>The list of support severity levels.</returns>
    public async Task<List<SeverityLevel>> DescribeSeverityLevels(string language
 = "en")
    {
        var response = await _amazonSupport.DescribeSeverityLevelsAsync(
            new DescribeSeverityLevelsRequest()
            {
                Language = language
            });
        return response.SeverityLevels;
    }
```

- Para obtener información detallada sobre la API, consulta la DescribeSeveritysección Niveles in AWS SDK for .NET API Reference.

CLI

AWS CLI

Creación de una lista de los niveles de gravedad disponibles

En el siguiente ejemplo de `describe-severity-levels` se enumeran los niveles de gravedad disponibles para un caso de soporte.

```
aws support describe-severity-levels
```

Salida:

```
{
    "severityLevels": [
        {
            "code": "low",
            "name": "Low"
        },
        {
            "code": "normal",
            "name": "Normal"
        },
```

```
        {
            "code": "high",
            "name": "High"
        },
        {
            "code": "urgent",
            "name": "Urgent"
        },
        {
            "code": "critical",
            "name": "Critical"
        }
    ]
}
```

Para obtener más información, consulte Elección de la gravedad en la Guía del usuario de soporte de AWS .

- Para obtener más información sobre la API, consulta la DescribeSeveritysección Niveles in AWS CLI Command Reference.

Java

SDK para Java 2.x

> **Note**
>
> Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
    public static String displaySevLevels(SupportClient supportClient) {
        try {
            DescribeSeverityLevelsRequest severityLevelsRequest =
DescribeSeverityLevelsRequest.builder()
                    .language("en")
                    .build();

            DescribeSeverityLevelsResponse response =
supportClient.describeSeverityLevels(severityLevelsRequest);
            List<SeverityLevel> severityLevels = response.severityLevels();
            String levelName = null;
```

```
            for (SeverityLevel sevLevel : severityLevels) {
                System.out.println("The severity level name is: " +
 sevLevel.name());
                if (sevLevel.name().compareTo("High") == 0)
                    levelName = sevLevel.name();
            }
            return levelName;

        } catch (SupportException e) {
            System.out.println(e.getLocalizedMessage());
            System.exit(1);
        }
        return "";
    }
```

- Para obtener información detallada sobre la API, consulta la DescribeSeveritysección Niveles in AWS SDK for Java 2.x API Reference.

JavaScript

SDK para JavaScript (v3)

> **Note**
>
> Hay más información. GitHub Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
import { DescribeSeverityLevelsCommand } from "@aws-sdk/client-support";

import { client } from "../libs/client.js";

export const main = async () => {
  try {
    // Get the list of severity levels.
    // The available values depend on the support plan for the account.
    const response = await client.send(new DescribeSeverityLevelsCommand({}));
    console.log(response.severityLevels);
    return response;
  } catch (err) {
```

```
    console.error(err);
  }
};
```

- Para obtener información detallada sobre la API, consulta la DescribeSeveritysección Niveles in AWS SDK for JavaScript API Reference.

Kotlin

SDK para Kotlin

> **Note**
>
> Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
suspend fun displaySevLevels(): String {
    var levelName = ""
    val severityLevelsRequest =
        DescribeSeverityLevelsRequest {
            language = "en"
        }

    SupportClient { region = "us-west-2" }.use { supportClient ->
        val response =
 supportClient.describeSeverityLevels(severityLevelsRequest)
        response.severityLevels?.forEach { sevLevel ->
            println("The severity level name is: ${sevLevel.name}")
            if (sevLevel.name == "High") {
                levelName = sevLevel.name!!
            }
        }
        return levelName
    }
}
```

- Para obtener más información sobre la API, consulta la referencia sobre DescribeSeveritylos nivelesAWS del SDK para la API de Kotlin.

PowerShell

Herramientas para PowerShell

Ejemplo 1: Devuelve la lista de niveles de gravedad que se pueden asignar a un caso de AWS Support.

```
Get-ASASeverityLevel
```

Ejemplo 2: Devuelve la lista de niveles de gravedad que se pueden asignar a un caso de AWS Support. Los nombres de los niveles se devuelven en japonés.

```
Get-ASASeverityLevel -Language "ja"
```

- Para obtener información sobre la API, consulte DescribeSeverityLevels in AWS Tools for PowerShell Cmdlet Reference.

Python

SDK para Python (Boto3)

> **Note**
>
> Hay más información al respecto. GitHub Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
class SupportWrapper:
    """Encapsulates Support actions."""

    def __init__(self, support_client):
        """
        :param support_client: A Boto3 Support client.
        """
        self.support_client = support_client

    @classmethod
    def from_client(cls):
        """
        Instantiates this class from a Boto3 client.
```

```
        """
        support_client = boto3.client("support")
        return cls(support_client)


    def describe_severity_levels(self, language):
        """
        Get the descriptions of available severity levels for support cases for a
language.

        :param language: The language for support severity levels.
        Currently, only "en" (English) and "ja" (Japanese) are supported.
        :return: The list of severity levels.
        """
        try:
            response =
self.support_client.describe_severity_levels(language=language)
            severity_levels = response["severityLevels"]
        except ClientError as err:
            if err.response["Error"]["Code"] == "SubscriptionRequiredException":
                logger.info(
                    "You must have a Business, Enterprise On-Ramp, or Enterprise
Support "
                    "plan to use the AWS Support API. \n\tPlease upgrade your
subscription to run these "
                    "examples."
                )
            else:
                logger.error(
                    "Couldn't get severity levels for language %s. Here's why:
%s: %s",
                    language,
                    err.response["Error"]["Code"],
                    err.response["Error"]["Message"],
                )
                raise
        else:
            return severity_levels
```

- Para obtener más información sobre la API, consulta DescribeSeverityNiveles in AWS SDK for Python (Boto3) API Reference.

Para obtener una lista completa de guías para desarrolladores del AWS SDK y ejemplos de código, consulte. AWS Support Utilizándolo con un AWS SDK En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

Úselo **`DescribeTrustedAdvisorCheckRefreshStatuses`** con un AWS SDK o CLI

En los siguientes ejemplos de código, se muestra cómo utilizar `DescribeTrustedAdvisorCheckRefreshStatuses`.

CLI

AWS CLI

Para enumerar los estados de actualización de las comprobaciones de AWS Trusted Advisor

El siguiente `describe-trusted-advisor-check-refresh-statuses` ejemplo muestra los estados de actualización de dos comprobaciones de Trusted Advisor: Amazon S3 Bucket Permissions e IAM Use.

```
aws support describe-trusted-advisor-check-refresh-statuses \
    --check-id "Pfx0RwqBli" "zXCkfM1nI3"
```

Salida:

```
{
    "statuses": [
        {
            "checkId": "Pfx0RwqBli",
            "status": "none",
            "millisUntilNextRefreshable": 0
        },
        {
            "checkId": "zXCkfM1nI3",
            "status": "none",
            "millisUntilNextRefreshable": 0
        }
    ]
}
```

Para obtener más información, consulte AWS Trusted Advisor en la Guía del usuario de AWS Support.

- Para obtener más información sobre la API, consulte DescribeTrustedAdvisorCheckRefreshStatuseslа Referencia de AWS CLI comandos.

PowerShell

Herramientas para PowerShell

Ejemplo 1: Devuelve el estado actual de las solicitudes de actualización para las comprobaciones especificadas. Request-ASA se TrustedAdvisorCheckRefresh puede utilizar para solicitar que se actualice la información de estado de las comprobaciones.

```
Get-ASATrustedAdvisorCheckRefreshStatus -CheckId @("checkid1", "checkid2")
```

- Para obtener más información sobre la API, consulte la referencia de DescribeTrustedAdvisorCheckRefreshStatusescmdlets AWS Tools for PowerShell .

Para obtener una lista completa de guías para desarrolladores del AWS SDK y ejemplos de código, consulte. AWS Support Utilizándolo con un AWS SDK En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

Úselo **`DescribeTrustedAdvisorCheckResult`** con un AWS SDK o CLI

En los siguientes ejemplos de código, se muestra cómo utilizar `DescribeTrustedAdvisorCheckResult`.

CLI

AWS CLI

Para enumerar los resultados de una comprobación de AWS Trusted Advisor

El siguiente `describe-trusted-advisor-check-result` ejemplo muestra los resultados de la comprobación de uso de IAM.

```
aws support describe-trusted-advisor-check-result \
    --check-id "zXCkfM1nI3"
```

Salida:

```
{
    "result": {
        "checkId": "zXCkfM1nI3",
        "timestamp": "2020-05-13T21:38:05Z",
        "status": "ok",
        "resourcesSummary": {
            "resourcesProcessed": 1,
            "resourcesFlagged": 0,
            "resourcesIgnored": 0,
            "resourcesSuppressed": 0
        },
        "categorySpecificSummary": {
            "costOptimizing": {
                "estimatedMonthlySavings": 0.0,
                "estimatedPercentMonthlySavings": 0.0
            }
        },
        "flaggedResources": [
            {
                "status": "ok",
                "resourceId": "47DEQpj8HBSa-_TImW-5JCeuQeRkm5NMpJWZEXAMPLE",
                "isSuppressed": false
            }
        ]
    }
}
```

Para obtener más información, consulte AWS Trusted Advisor en la Guía del usuario de AWS Support.

- Para obtener más información sobre la API, consulte DescribeTrustedAdvisorCheckResult in AWS CLI Command Reference.

PowerShell

Herramientas para PowerShell

Ejemplo 1: Devuelve los resultados de una comprobación de Trusted Advisor. La lista de comprobaciones de Trusted Advisor disponibles se puede obtener mediante Get-ASA TrustedAdvisor Checks. El resultado es el estado general de la comprobación, la fecha y hora

en la que se ejecutó por última vez y el identificador único de la comprobación específica. Para que los resultados se muestren en japonés, añada el parámetro «ja» de -Language.

```
Get-ASATrustedAdvisorCheckResult -CheckId "checkid1"
```

- Para obtener información sobre la API, consulte DescribeTrustedAdvisorCheckResult in AWS Tools for PowerShell Cmdlet Reference.

Para obtener una lista completa de guías para desarrolladores del AWS SDK y ejemplos de código, consulte. AWS Support Utilizándolo con un AWS SDK En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

Úselo **`DescribeTrustedAdvisorCheckSummaries`** con un AWS SDK o CLI

En los siguientes ejemplos de código, se muestra cómo utilizar `DescribeTrustedAdvisorCheckSummaries`.

CLI

AWS CLI

Para enumerar los resúmenes de las comprobaciones de AWS Trusted Advisor

El siguiente `describe-trusted-advisor-check-summaries` ejemplo muestra los resultados de dos comprobaciones de Trusted Advisor: Amazon S3 Bucket Permissions e IAM Use.

```
aws support describe-trusted-advisor-check-summaries \
    --check-ids "Pfx0RwqBli" "zXCkfM1nI3"
```

Salida:

```
{
    "summaries": [
        {
            "checkId": "Pfx0RwqBli",
            "timestamp": "2020-05-13T21:38:12Z",
```

```
            "status": "ok",
            "hasFlaggedResources": true,
            "resourcesSummary": {
                "resourcesProcessed": 44,
                "resourcesFlagged": 0,
                "resourcesIgnored": 0,
                "resourcesSuppressed": 0
            },
            "categorySpecificSummary": {
                "costOptimizing": {
                    "estimatedMonthlySavings": 0.0,
                    "estimatedPercentMonthlySavings": 0.0
                }
            }
        },
        {
            "checkId": "zXCkfM1nI3",
            "timestamp": "2020-05-13T21:38:05Z",
            "status": "ok",
            "hasFlaggedResources": true,
            "resourcesSummary": {
                "resourcesProcessed": 1,
                "resourcesFlagged": 0,
                "resourcesIgnored": 0,
                "resourcesSuppressed": 0
            },
            "categorySpecificSummary": {
                "costOptimizing": {
                    "estimatedMonthlySavings": 0.0,
                    "estimatedPercentMonthlySavings": 0.0
                }
            }
        }
    ]
}
```


Para obtener más información, consulte AWS Trusted Advisor en la Guía del usuario de AWS Support.

- Para obtener más información sobre la API, consulte DescribeTrustedAdvisorChecklos resúmenes en la referencia de AWS CLI comandos.

PowerShell

Herramientas para PowerShell

Ejemplo 1: Devuelve el resumen más reciente de la comprobación de Trusted Advisor especificada.

```
Get-ASATrustedAdvisorCheckSummary -CheckId "checkid1"
```

Ejemplo 2: Devuelve los resúmenes más recientes de las comprobaciones de Trusted Advisor especificadas.

```
Get-ASATrustedAdvisorCheckSummary -CheckId @("checkid1", "checkid2")
```

- Para obtener más información sobre la API, consulte los DescribeTrustedAdvisorCheckresúmenes en la referencia de los AWS Tools for PowerShell cmdlets.

Para obtener una lista completa de guías para desarrolladores del AWS SDK y ejemplos de código, consulte. AWS Support Utilizándolo con un AWS SDK En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

Úselo **`DescribeTrustedAdvisorChecks`** con un AWS SDK o CLI

En los siguientes ejemplos de código, se muestra cómo utilizar `DescribeTrustedAdvisorChecks`.

CLI

AWS CLI

Para enumerar las comprobaciones AWS de Trusted Advisor disponibles

El siguiente `describe-trusted-advisor-checks` ejemplo muestra los cheques de Trusted Advisor disponibles en su AWS cuenta. Esta información incluye el nombre, el identificador, la descripción, la categoría y los metadatos del cheque. Tenga en cuenta que el resultado está abreviado para facilitar la lectura.

```
aws support describe-trusted-advisor-checks \
    --language "en"
```

Salida:

```
{
    "checks": [
        {
            "id": "zXCkfM1nI3",
            "name": "IAM Use",
            "description": "Checks for your use of AWS Identity and Access
 Management (IAM). You can use IAM to create users, groups, and roles in
 AWS, and you can use permissions to control access to AWS resources. \n<br>
\n<br>\n<b>Alert Criteria</b><br>\nYellow: No IAM users have been created
 for this account.\n<br>\n<br>\n<b>Recommended Action</b><br>\nCreate one or
 more IAM users and groups in your account. You can then create additional
 users whose permissions are limited to perform specific tasks in your AWS
 environment. For more information, see <a href=\"https://docs.aws.amazon.com/
IAM/latest/UserGuide/IAMGettingStarted.html\" target=\"_blank\">Getting
 Started</a>. \n<br><br>\n<b>Additional Resources</b><br>\n<a href=\"https://
docs.aws.amazon.com/IAM/latest/UserGuide/IAM_Introduction.html\" target=\"_blank
\">What Is IAM?</a>",
            "category": "security",
            "metadata": []
        }
    ]
}
```

Para obtener más información, consulte AWS Trusted Advisor en la Guía del usuario de AWS Support.

- Para obtener más información sobre la API, consulte DescribeTrustedAdvisorChecksla Referencia de AWS CLI comandos.

PowerShell

Herramientas para PowerShell

Ejemplo 1: Devuelve la colección de cheques de Trusted Advisor. Debe especificar el parámetro de idioma, que puede aceptar «en» para la salida en inglés o «ja» para la salida en japonés.

```
Get-ASATrustedAdvisorCheck -Language "en"
```

- Para obtener más información sobre la API, consulte DescribeTrustedAdvisorChecksla referencia de AWS Tools for PowerShell cmdlets.

Para obtener una lista completa de guías para desarrolladores del AWS SDK y ejemplos de código, consulte. AWS Support Utilizándolo con un AWS SDK En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

Úselo **`RefreshTrustedAdvisorCheck`** con un AWS SDK o CLI

En los siguientes ejemplos de código, se muestra cómo utilizar `RefreshTrustedAdvisorCheck`.

CLI

AWS CLI

Para actualizar una comprobación AWS de Trusted Advisor

En el siguiente `refresh-trusted-advisor-check` ejemplo, se actualiza la comprobación de Amazon S3 Bucket Permissions Trusted Advisor de su AWS cuenta.

```
aws support refresh-trusted-advisor-check \
    --check-id "Pfx0RwqBli"
```

Salida:

```
{
    "status": {
        "checkId": "Pfx0RwqBli",
        "status": "enqueued",
        "millisUntilNextRefreshable": 3599992
    }
}
```

Para obtener más información, consulte AWS Trusted Advisor en la Guía del usuario de AWS Support.

- Para obtener más información sobre la API, consulte RefreshTrustedAdvisorCheckla Referencia de AWS CLI comandos.

PowerShell

Herramientas para PowerShell

Ejemplo 1: Solicita una actualización para la comprobación de Trusted Advisor especificada.

```
Request-ASATrustedAdvisorCheckRefresh -CheckId "checkid1"
```

- Para obtener más información sobre la API, consulte RefreshTrustedAdvisorChecklа referencia del AWS Tools for PowerShell cmdlet.

Para obtener una lista completa de guías para desarrolladores del AWS SDK y ejemplos de código, consulte. AWS Support Utilizándolo con un AWS SDK En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

Úselo **`ResolveCase`** con un AWS SDK o CLI

En los siguientes ejemplos de código, se muestra cómo utilizar `ResolveCase`.

Los ejemplos de acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Puede ver esta acción en contexto en el siguiente ejemplo de código:

- Introducción a los casos

.NET

AWS SDK for .NET

> **Note**
>
> Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
/// <summary>
/// Resolve a support case by caseId.
/// </summary>
```

```
    /// <param name="caseId">Id for the support case.</param>
    /// <returns>The final status of the case after resolving.</returns>
    public async Task<string> ResolveCase(string caseId)
    {
        var response = await _amazonSupport.ResolveCaseAsync(
            new ResolveCaseRequest()
            {
                CaseId = caseId
            });
        return response.FinalCaseStatus;
    }
```

- Para obtener más información sobre la API, consulta ResolveCasela Referencia AWS SDK for .NET de la API.

CLI

AWS CLI

Resolución de un caso de soporte

El siguiente `resolve-case` ejemplo resuelve un caso de soporte en tu AWS cuenta.

```
aws support resolve-case \
    --case-id "case-12345678910-2013-c4c1d2bf33c5cf47"
```

Salida:

```
{
    "finalCaseStatus": "resolved",
    "initialCaseStatus": "work-in-progress"
}
```

Para obtener más información, consulte Administración de casos en la Guía del usuario de soporte de AWS .

- Para obtener más información sobre la API, consulta ResolveCasela Referencia de AWS CLI comandos.

Java

SDK para Java 2.x

> **Note**
>
> Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
   public static void resolveSupportCase(SupportClient supportClient, String
caseId) {
       try {
           ResolveCaseRequest caseRequest = ResolveCaseRequest.builder()
                   .caseId(caseId)
                   .build();

           ResolveCaseResponse response =
supportClient.resolveCase(caseRequest);
           System.out.println("The status of case " + caseId + " is " +
response.finalCaseStatus());

       } catch (SupportException e) {
           System.out.println(e.getLocalizedMessage());
           System.exit(1);
       }
   }
```

- Para obtener más información sobre la API, consulta ResolveCasela Referencia AWS SDK for Java 2.x de la API.

JavaScript

SDK para JavaScript (v3)

> **Note**
>
> Hay más información. GitHub Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
import { ResolveCaseCommand } from "@aws-sdk/client-support";

import { client } from "../libs/client.js";

const main = async () => {
  try {
    const response = await client.send(
      new ResolveCaseCommand({
        caseId: "CASE_ID",
      }),
    );

    console.log(response.finalCaseStatus);
    return response;
  } catch (err) {
    console.error(err);
  }
};
```

- Para obtener más información sobre la API, consulta ResolveCasela Referencia AWS SDK for JavaScript de la API.

Kotlin

SDK para Kotlin

> **Note**
>
> Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
suspend fun resolveSupportCase(caseIdVal: String) {
    val caseRequest =
        ResolveCaseRequest {
            caseId = caseIdVal
        }
    SupportClient { region = "us-west-2" }.use { supportClient ->
        val response = supportClient.resolveCase(caseRequest)
        println("The status of case $caseIdVal is ${response.finalCaseStatus}")
```

```
    }
}
```

- Para obtener más información sobre la API, consulta ResolveCasela referencia sobre el AWS SDK para la API de Kotlin.

PowerShell

Herramientas para PowerShell

Ejemplo 1: devuelve el estado inicial del caso especificado y el estado actual una vez finalizada la llamada para resolverlo.

```
Resolve-ASACase -CaseId "case-12345678910-2013-c4c1d2bf33c5cf47"
```

- Para obtener más información sobre la API, consulte ResolveCasela referencia del AWS Tools for PowerShell cmdlet.

Python

SDK para Python (Boto3)

> **Note**
>
> Hay más información al respecto. GitHub Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
class SupportWrapper:
    """Encapsulates Support actions."""

    def __init__(self, support_client):
        """
        :param support_client: A Boto3 Support client.
        """
        self.support_client = support_client

    @classmethod
```

```
    def from_client(cls):
        """
        Instantiates this class from a Boto3 client.
        """
        support_client = boto3.client("support")
        return cls(support_client)


    def resolve_case(self, case_id):
        """
        Resolve a support case by its caseId.

        :param case_id: The ID of the case to resolve.
        :return: The final status of the case.
        """
        try:
            response = self.support_client.resolve_case(caseId=case_id)
            final_status = response["finalCaseStatus"]
        except ClientError as err:
            if err.response["Error"]["Code"] == "SubscriptionRequiredException":
                logger.info(
                    "You must have a Business, Enterprise On-Ramp, or Enterprise
Support "
                    "plan to use the AWS Support API. \n\tPlease upgrade your
subscription to run these "
                    "examples."
                )
            else:
                logger.error(
                    "Couldn't resolve case. Here's why: %s: %s",
                    err.response["Error"]["Code"],
                    err.response["Error"]["Message"],
                )
                raise
        else:
            return final_status
```

- Para obtener más información sobre la API, consulta ResolveCasela AWS Referencia de API de SDK for Python (Boto3).

Para obtener una lista completa de guías para desarrolladores del AWS SDK y ejemplos de código, consulte. AWS Support Utilizándolo con un AWS SDK En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

Escenarios de AWS Support uso de AWS los SDK

Los siguientes ejemplos de código muestran cómo implementar escenarios comunes AWS Support con los AWS SDK. Estos escenarios muestran cómo realizar tareas específicas mediante la llamada a varias funciones internas AWS Support. Cada escenario incluye un enlace a GitHub, donde puede encontrar instrucciones sobre cómo configurar y ejecutar el código.

Ejemplos

- Comience con AWS Support los casos con un AWS SDK

Comience con AWS Support los casos con un AWS SDK

En el siguiente ejemplo de código, se muestra cómo:

- Obtenga y muestre los servicios disponibles y los niveles de gravedad de los casos.
- Cree un caso de asistencia mediante un servicio, una categoría y un nivel de gravedad seleccionados.
- Obtenga y muestre una lista de casos abiertos para el día actual.
- Añada una serie de archivos adjuntos y una comunicación al nuevo caso.
- Describa el nuevo archivo adjunto y la comunicación del caso.
- Resuelva el caso.
- Obtenga y muestre una lista de casos resueltos para el día actual.

.NET

AWS SDK for .NET

> **Note**
>
> Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

Ejecutar un escenario interactivo en un símbolo del sistema.

```
/// <summary>
/// Hello AWS Support example.
/// </summary>
public static class SupportCaseScenario
{
    /*
    Before running this .NET code example, set up your development environment,
 including your credentials.
    To use the AWS Support API, you must have one of the following AWS Support
 plans: Business, Enterprise On-Ramp, or Enterprise.

    This .NET example performs the following tasks:
    1.  Get and display services. Select a service from the list.
    2.  Select a category from the selected service.
    3.  Get and display severity levels and select a severity level from the
 list.
    4.  Create a support case using the selected service, category, and severity
 level.
    5.  Get and display a list of open support cases for the current day.
    6.  Create an attachment set with a sample text file to add to the case.
    7.  Add a communication with the attachment to the support case.
    8.  List the communications of the support case.
    9.  Describe the attachment set.
    10. Resolve the support case.
    11. Get a list of resolved cases for the current day.
   */

    private static SupportWrapper _supportWrapper = null!;

    static async Task Main(string[] args)
    {
        // Set up dependency injection for the AWS Support service.
        // Use your AWS profile name, or leave it blank to use the default
 profile.
        using var host = Host.CreateDefaultBuilder(args)
            .ConfigureLogging(logging =>
                logging.AddFilter("System", LogLevel.Debug)
                    .AddFilter<DebugLoggerProvider>("Microsoft",
 LogLevel.Information)
                    .AddFilter<ConsoleLoggerProvider>("Microsoft",
 LogLevel.Trace))
```

```
            .ConfigureServices((_, services) =>
                services.AddAWSService<IAmazonAWSSupport>(new AWSOptions()
{ Profile = "default" })
                    .AddTransient<SupportWrapper>()
            )
            .Build();

        var logger = LoggerFactory.Create(builder =>
        {
            builder.AddConsole();
        }).CreateLogger(typeof(SupportCaseScenario));

        _supportWrapper = host.Services.GetRequiredService<SupportWrapper>();

        Console.WriteLine(new string('-', 80));
        Console.WriteLine("Welcome to the AWS Support case example scenario.");
        Console.WriteLine(new string('-', 80));

        try
        {
            var apiSupported = await _supportWrapper.VerifySubscription();
            if (!apiSupported)
            {
                logger.LogError("You must have a Business, Enterprise On-Ramp, or
Enterprise Support " +
                                "plan to use the AWS Support API. \n\tPlease
upgrade your subscription to run these examples.");
                return;
            }

            var service = await DisplayAndSelectServices();

            var category = DisplayAndSelectCategories(service);

            var severityLevel = await DisplayAndSelectSeverity();

            var caseId = await CreateSupportCase(service, category,
severityLevel);

            await DescribeTodayOpenCases();

            var attachmentSetId = await CreateAttachmentSet();

            await AddCommunicationToCase(attachmentSetId, caseId);
```

```
            var attachmentId = await ListCommunicationsForCase(caseId);

            await DescribeCaseAttachment(attachmentId);

            await ResolveCase(caseId);

            await DescribeTodayResolvedCases();

            Console.WriteLine(new string('-', 80));
            Console.WriteLine("AWS Support case example scenario complete.");
            Console.WriteLine(new string('-', 80));
        }
        catch (Exception ex)
        {
            logger.LogError(ex, "There was a problem executing the scenario.");
        }
    }

    /// <summary>
    /// List some available services from AWS Support, and select a service for
the example.
    /// </summary>
    /// <returns>The selected service.</returns>
    private static async Task<Service> DisplayAndSelectServices()
    {
        Console.WriteLine(new string('-', 80));
        var services = await _supportWrapper.DescribeServices();
        Console.WriteLine($"AWS Support client returned {services.Count}
services.");

        Console.WriteLine($"1. Displaying first 10 services:");
        for (int i = 0; i < 10 && i < services.Count; i++)
        {
            Console.WriteLine($"\t{i + 1}. {services[i].Name}");
        }

        var choiceNumber = 0;
        while (choiceNumber < 1 || choiceNumber > services.Count)
        {
            Console.WriteLine(
                "Select an example support service by entering a number from the
preceding list:");
            var choice = Console.ReadLine();
```

```
            Int32.TryParse(choice, out choiceNumber);
        }
        Console.WriteLine(new string('-', 80));

        return services[choiceNumber - 1];
    }

    /// <summary>
    /// List the available categories for a service and select a category for the
example.
    /// </summary>
    /// <param name="service">Service to use for displaying categories.</param>
    /// <returns>The selected category.</returns>
    private static Category DisplayAndSelectCategories(Service service)
    {
        Console.WriteLine(new string('-', 80));

        Console.WriteLine($"2. Available support categories for Service
\"{service.Name}\":");
        for (int i = 0; i < service.Categories.Count; i++)
        {
            Console.WriteLine($"\t{i + 1}. {service.Categories[i].Name}");
        }

        var choiceNumber = 0;
        while (choiceNumber < 1 || choiceNumber > service.Categories.Count)
        {
            Console.WriteLine(
                "Select an example support category by entering a number from the
preceding list:");
            var choice = Console.ReadLine();
            Int32.TryParse(choice, out choiceNumber);
        }

        Console.WriteLine(new string('-', 80));

        return service.Categories[choiceNumber - 1];
    }

    /// <summary>
    /// List available severity levels from AWS Support, and select a level for
the example.
    /// </summary>
    /// <returns>The selected severity level.</returns>
```

```
    private static async Task<SeverityLevel> DisplayAndSelectSeverity()
    {
        Console.WriteLine(new string('-', 80));
        var severityLevels = await _supportWrapper.DescribeSeverityLevels();

        Console.WriteLine($"3. Get and display available severity levels:");
        for (int i = 0; i < 10 && i < severityLevels.Count; i++)
        {
            Console.WriteLine($"\t{i + 1}. {severityLevels[i].Name}");
        }

        var choiceNumber = 0;
        while (choiceNumber < 1 || choiceNumber > severityLevels.Count)
        {
            Console.WriteLine(
                "Select an example severity level by entering a number from the
preceding list:");
            var choice = Console.ReadLine();
            Int32.TryParse(choice, out choiceNumber);
        }
        Console.WriteLine(new string('-', 80));

        return severityLevels[choiceNumber - 1];
    }

    /// <summary>
    /// Create an example support case.
    /// </summary>
    /// <param name="service">Service to use for the new case.</param>
    /// <param name="category">Category to use for the new case.</param>
    /// <param name="severity">Severity to use for the new case.</param>
    /// <returns>The caseId of the new support case.</returns>
    private static async Task<string> CreateSupportCase(Service service,
        Category category, SeverityLevel severity)
    {
        Console.WriteLine(new string('-', 80));
        Console.WriteLine($"4. Create an example support case" +
                          $" with the following settings:" +
                          $" \n\tService: {service.Name}, Category:
{category.Name} " +
                          $"and Severity Level: {severity.Name}.");
        var caseId = await _supportWrapper.CreateCase(service.Code,
category.Code, severity.Code,
```

```
            "Example case for testing, ignore.", "This is my example support
case.");

        Console.WriteLine($"\tNew case created with ID {caseId}");

        Console.WriteLine(new string('-', 80));

        return caseId;
    }

    /// <summary>
    /// List open cases for the current day.
    /// </summary>
    /// <returns>Async task.</returns>
    private static async Task DescribeTodayOpenCases()
    {
        Console.WriteLine($"5. List the open support cases for the current
day.");
        // Describe the cases. If it is empty, try again and allow time for the
new case to appear.
        List<CaseDetails> currentOpenCases = null!;
        while (currentOpenCases == null || currentOpenCases.Count == 0)
        {
            Thread.Sleep(1000);
            currentOpenCases = await _supportWrapper.DescribeCases(
                new List<string>(),
                null,
                false,
                false,
                DateTime.UtcNow.Date,
                DateTime.UtcNow);
        }

        foreach (var openCase in currentOpenCases)
        {
            Console.WriteLine($"\tCase: {openCase.CaseId} created
{openCase.TimeCreated}");
        }

        Console.WriteLine(new string('-', 80));
    }

    /// <summary>
    /// Create an attachment set for a support case.
```

```
    /// </summary>
    /// <returns>The attachment set id.</returns>
    private static async Task<string> CreateAttachmentSet()
    {
        Console.WriteLine(new string('-', 80));
        Console.WriteLine($"6. Create an attachment set for a support case.");
        var fileName = "example_attachment.txt";

        // Create the file if it does not already exist.
        if (!File.Exists(fileName))
        {
            await using StreamWriter sw = File.CreateText(fileName);
            await sw.WriteLineAsync(
                "This is a sample file for attachment to a support case.");
        }

        await using var ms = new MemoryStream(await
 File.ReadAllBytesAsync(fileName));

        var attachmentSetId = await _supportWrapper.AddAttachmentToSet(
            ms,
            fileName);

        Console.WriteLine($"\tNew attachment set created with id: \n
\t{attachmentSetId.Substring(0, 65)}...");

        Console.WriteLine(new string('-', 80));

        return attachmentSetId;
    }

    /// <summary>
    /// Add an attachment set and communication to a case.
    /// </summary>
    /// <param name="attachmentSetId">Id of the attachment set.</param>
    /// <param name="caseId">Id of the case to receive the attachment set.</
param>
    /// <returns>Async task.</returns>
    private static async Task AddCommunicationToCase(string attachmentSetId,
 string caseId)
    {
        Console.WriteLine(new string('-', 80));
        Console.WriteLine($"7. Add attachment set and communication to
 {caseId}.");
```

```
        await _supportWrapper.AddCommunicationToCase(
            caseId,
            "This is an example communication added to a support case.",
            attachmentSetId);

        Console.WriteLine($"\tNew attachment set and communication added to
{caseId}");

        Console.WriteLine(new string('-', 80));
    }

    /// <summary>
    /// List the communications for a case.
    /// </summary>
    /// <param name="caseId">Id of the case to describe.</param>
    /// <returns>An attachment id.</returns>
    private static async Task<string> ListCommunicationsForCase(string caseId)
    {
        Console.WriteLine(new string('-', 80));
        Console.WriteLine($"8. List communications for case {caseId}.");

        var communications = await
_supportWrapper.DescribeCommunications(caseId);
        var attachmentId = "";
        foreach (var communication in communications)
        {
            Console.WriteLine(
                $"\tCommunication created on: {communication.TimeCreated} has
{communication.AttachmentSet.Count} attachments.");
            if (communication.AttachmentSet.Any())
            {
                attachmentId = communication.AttachmentSet.First().AttachmentId;
            }
        }

        Console.WriteLine(new string('-', 80));
        return attachmentId;
    }

    /// <summary>
    /// Describe an attachment by id.
    /// </summary>
    /// <param name="attachmentId">Id of the attachment to describe.</param>
```

```
    /// <returns>Async task.</returns>
    private static async Task DescribeCaseAttachment(string attachmentId)
    {
        Console.WriteLine(new string('-', 80));
        Console.WriteLine($"9. Describe the attachment set.");

        var attachment = await _supportWrapper.DescribeAttachment(attachmentId);
        var data = Encoding.ASCII.GetString(attachment.Data.ToArray());
        Console.WriteLine($"\tAttachment includes {attachment.FileName} with
data: \n\t{data}");

        Console.WriteLine(new string('-', 80));
    }

    /// <summary>
    /// Resolve the support case.
    /// </summary>
    /// <param name="caseId">Id of the case to resolve.</param>
    /// <returns>Async task.</returns>
    private static async Task ResolveCase(string caseId)
    {
        Console.WriteLine(new string('-', 80));
        Console.WriteLine($"10. Resolve case {caseId}.");

        var status = await _supportWrapper.ResolveCase(caseId);
        Console.WriteLine($"\tCase {caseId} has final status {status}");

        Console.WriteLine(new string('-', 80));
    }

    /// <summary>
    /// List resolved cases for the current day.
    /// </summary>
    /// <returns>Async Task.</returns>
    private static async Task DescribeTodayResolvedCases()
    {
        Console.WriteLine(new string('-', 80));
        Console.WriteLine($"11. List the resolved support cases for the current
day.");
        var currentCases = await _supportWrapper.DescribeCases(
            new List<string>(),
            null,
            false,
            true,
```

```
            DateTime.UtcNow.Date,
            DateTime.UtcNow);

        foreach (var currentCase in currentCases)
        {
            if (currentCase.Status == "resolved")
            {
                Console.WriteLine(
                    $"\tCase: {currentCase.CaseId}: status
 {currentCase.Status}");
            }
        }

        Console.WriteLine(new string('-', 80));
    }
}
```

Métodos envoltorios utilizados por el escenario para AWS Support las acciones.

```
/// <summary>
/// Wrapper methods to use AWS Support for working with support cases.
/// </summary>
public class SupportWrapper
{
    private readonly IAmazonAWSSupport _amazonSupport;
    public SupportWrapper(IAmazonAWSSupport amazonSupport)
    {
        _amazonSupport = amazonSupport;
    }


    /// <summary>
    /// Get the descriptions of AWS services.
    /// </summary>
    /// <param name="name">Optional language for services.
    /// Currently Chinese (“zh”), English ("en"), Japanese ("ja") and Korean
 (“ko”) are supported.</param>
    /// <returns>The list of AWS service descriptions.</returns>
    public async Task<List<Service>> DescribeServices(string language = "en")
    {
        var response = await _amazonSupport.DescribeServicesAsync(
```

```
            new DescribeServicesRequest()
            {
                Language = language
            });
        return response.Services;
    }



    /// <summary>
    /// Get the descriptions of support severity levels.
    /// </summary>
    /// <param name="name">Optional language for severity levels.
    /// Currently Chinese (“zh”), English ("en"), Japanese ("ja") and Korean
(“ko”) are supported.</param>
    /// <returns>The list of support severity levels.</returns>
    public async Task<List<SeverityLevel>> DescribeSeverityLevels(string language
= "en")
    {
        var response = await _amazonSupport.DescribeSeverityLevelsAsync(
            new DescribeSeverityLevelsRequest()
            {
                Language = language
            });
        return response.SeverityLevels;
    }



    /// <summary>
    /// Create a new support case.
    /// </summary>
    /// <param name="serviceCode">Service code for the new case.</param>
    /// <param name="categoryCode">Category for the new case.</param>
    /// <param name="severityCode">Severity code for the new case.</param>
    /// <param name="subject">Subject of the new case.</param>
    /// <param name="body">Body text of the new case.</param>
    /// <param name="language">Optional language support for your case.
    /// Currently Chinese (“zh”), English ("en"), Japanese ("ja") and Korean
(“ko”) are supported.</param>
    /// <param name="attachmentSetId">Optional Id for an attachment set for the
new case.</param>
    /// <param name="issueType">Optional issue type for the new case. Options are
"customer-service" or "technical".</param>
```

```
   /// <returns>The caseId of the new support case.</returns>
   public async Task<string> CreateCase(string serviceCode, string categoryCode,
string severityCode, string subject,
       string body, string language = "en", string? attachmentSetId = null,
string issueType = "customer-service")
   {
       var response = await _amazonSupport.CreateCaseAsync(
           new CreateCaseRequest()
           {
               ServiceCode = serviceCode,
               CategoryCode = categoryCode,
               SeverityCode = severityCode,
               Subject = subject,
               Language = language,
               AttachmentSetId = attachmentSetId,
               IssueType = issueType,
               CommunicationBody = body
           });
       return response.CaseId;
   }



   /// <summary>
   /// Add an attachment to a set, or create a new attachment set if one does
not exist.
   /// </summary>
   /// <param name="data">The data for the attachment.</param>
   /// <param name="fileName">The file name for the attachment.</param>
   /// <param name="attachmentSetId">Optional setId for the attachment. Creates
a new attachment set if empty.</param>
   /// <returns>The setId of the attachment.</returns>
   public async Task<string> AddAttachmentToSet(MemoryStream data, string
fileName, string? attachmentSetId = null)
   {
       var response = await _amazonSupport.AddAttachmentsToSetAsync(
           new AddAttachmentsToSetRequest
           {
               AttachmentSetId = attachmentSetId,
               Attachments = new List<Attachment>
               {
                   new Attachment
                   {
                       Data = data,
```

```
                        FileName = fileName
                    }
                }
            });
        return response.AttachmentSetId;
    }



    /// <summary>
    /// Get description of a specific attachment.
    /// </summary>
    /// <param name="attachmentId">Id of the attachment, usually fetched by
 describing the communications of a case.</param>
    /// <returns>The attachment object.</returns>
    public async Task<Attachment> DescribeAttachment(string attachmentId)
    {
        var response = await _amazonSupport.DescribeAttachmentAsync(
            new DescribeAttachmentRequest()
            {
                AttachmentId = attachmentId
            });
        return response.Attachment;
    }



    /// <summary>
    /// Add communication to a case, including optional attachment set ID and CC
 email addresses.
    /// </summary>
    /// <param name="caseId">Id for the support case.</param>
    /// <param name="body">Body text of the communication.</param>
    /// <param name="attachmentSetId">Optional Id for an attachment set.</param>
    /// <param name="ccEmailAddresses">Optional list of CC email addresses.</
param>
    /// <returns>True if successful.</returns>
    public async Task<bool> AddCommunicationToCase(string caseId, string body,
        string? attachmentSetId = null, List<string>? ccEmailAddresses = null)
    {
        var response = await _amazonSupport.AddCommunicationToCaseAsync(
            new AddCommunicationToCaseRequest()
            {
                CaseId = caseId,
```

```
                CommunicationBody = body,
                AttachmentSetId = attachmentSetId,
                CcEmailAddresses = ccEmailAddresses
            });
        return response.Result;
    }



    /// <summary>
    /// Describe the communications for a case, optionally with a date filter.
    /// </summary>
    /// <param name="caseId">The ID of the support case.</param>
    /// <param name="afterTime">The optional start date for a filtered search.</
param>
    /// <param name="beforeTime">The optional end date for a filtered search.</
param>
    /// <returns>The list of communications for the case.</returns>
    public async Task<List<Communication>> DescribeCommunications(string caseId,
 DateTime? afterTime = null, DateTime? beforeTime = null)
    {
        var results = new List<Communication>();
        var paginateCommunications =
 _amazonSupport.Paginators.DescribeCommunications(
            new DescribeCommunicationsRequest()
            {
                CaseId = caseId,
                AfterTime = afterTime?.ToString("s"),
                BeforeTime = beforeTime?.ToString("s")
            });
        // Get the entire list using the paginator.
        await foreach (var communications in
 paginateCommunications.Communications)
        {
            results.Add(communications);
        }
        return results;
    }



    /// <summary>
    /// Get case details for a list of case ids, optionally with date filters.
    /// </summary>
```

```
    /// <param name="caseIds">The list of case IDs.</param>
    /// <param name="displayId">Optional display ID.</param>
    /// <param name="includeCommunication">True to include communication.
 Defaults to true.</param>
    /// <param name="includeResolvedCases">True to include resolved cases.
 Defaults to false.</param>
    /// <param name="afterTime">The optional start date for a filtered search.</
param>
    /// <param name="beforeTime">The optional end date for a filtered search.</
param>
    /// <param name="language">Optional language support for your case.
    /// Currently Chinese (“zh”), English ("en"), Japanese ("ja") and Korean
 (“ko”) are supported.</param>
    /// <returns>A list of CaseDetails.</returns>
    public async Task<List<CaseDetails>> DescribeCases(List<string> caseIds,
 string? displayId = null, bool includeCommunication = true,
        bool includeResolvedCases = false, DateTime? afterTime = null, DateTime?
 beforeTime = null,
        string language = "en")
    {
        var results = new List<CaseDetails>();
        var paginateCases = _amazonSupport.Paginators.DescribeCases(
            new DescribeCasesRequest()
            {
                CaseIdList = caseIds,
                DisplayId = displayId,
                IncludeCommunications = includeCommunication,
                IncludeResolvedCases = includeResolvedCases,
                AfterTime = afterTime?.ToString("s"),
                BeforeTime = beforeTime?.ToString("s"),
                Language = language
            });
        // Get the entire list using the paginator.
        await foreach (var cases in paginateCases.Cases)
        {
            results.Add(cases);
        }
        return results;
    }



    /// <summary>
    /// Resolve a support case by caseId.
```

```
    /// </summary>
    /// <param name="caseId">Id for the support case.</param>
    /// <returns>The final status of the case after resolving.</returns>
    public async Task<string> ResolveCase(string caseId)
    {
        var response = await _amazonSupport.ResolveCaseAsync(
            new ResolveCaseRequest()
            {
                CaseId = caseId
            });
        return response.FinalCaseStatus;
    }


    /// <summary>
    /// Verify the support level for AWS Support API access.
    /// </summary>
    /// <returns>True if the subscription level supports API access.</returns>
    public async Task<bool> VerifySubscription()
    {
        try
        {
            var response = await _amazonSupport.DescribeServicesAsync(
                new DescribeServicesRequest()
                {
                    Language = "en"
                });
            return response.HttpStatusCode == HttpStatusCode.OK;
        }
        catch (Amazon.AWSSupport.AmazonAWSSupportException ex)
        {
            if (ex.ErrorCode == "SubscriptionRequiredException")
            {
                return false;
            }
            else throw;
        }
    }
}
```

- Para obtener información sobre la API, consulte los siguientes temas en la Referencia de la API de AWS SDK for .NET .

- AddAttachmentsToSet
- AddCommunicationToCase
- CreateCase
- DescribeAttachment
- DescribeCases
- DescribeCommunications
- DescribeServices
- DescribeSeverityNiveles
- ResolveCase

Java

SDK para Java 2.x

> **Note**
>
> Hay más en marcha GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

Ejecute varias AWS Support operaciones.

```
import software.amazon.awssdk.core.SdkBytes;
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.support.SupportClient;
import software.amazon.awssdk.services.support.model.AddAttachmentsToSetResponse;
import
 software.amazon.awssdk.services.support.model.AddCommunicationToCaseRequest;
import
 software.amazon.awssdk.services.support.model.AddCommunicationToCaseResponse;
import software.amazon.awssdk.services.support.model.Attachment;
import software.amazon.awssdk.services.support.model.AttachmentDetails;
import software.amazon.awssdk.services.support.model.CaseDetails;
import software.amazon.awssdk.services.support.model.Category;
import software.amazon.awssdk.services.support.model.Communication;
import software.amazon.awssdk.services.support.model.CreateCaseRequest;
import software.amazon.awssdk.services.support.model.CreateCaseResponse;
import software.amazon.awssdk.services.support.model.DescribeAttachmentRequest;
```

```
import software.amazon.awssdk.services.support.model.DescribeAttachmentResponse;
import software.amazon.awssdk.services.support.model.DescribeCasesRequest;
import software.amazon.awssdk.services.support.model.DescribeCasesResponse;
import
 software.amazon.awssdk.services.support.model.DescribeCommunicationsRequest;
import
 software.amazon.awssdk.services.support.model.DescribeCommunicationsResponse;
import software.amazon.awssdk.services.support.model.DescribeServicesRequest;
import software.amazon.awssdk.services.support.model.DescribeServicesResponse;
import
 software.amazon.awssdk.services.support.model.DescribeSeverityLevelsRequest;
import
 software.amazon.awssdk.services.support.model.DescribeSeverityLevelsResponse;
import software.amazon.awssdk.services.support.model.ResolveCaseRequest;
import software.amazon.awssdk.services.support.model.ResolveCaseResponse;
import software.amazon.awssdk.services.support.model.Service;
import software.amazon.awssdk.services.support.model.SeverityLevel;
import software.amazon.awssdk.services.support.model.SupportException;
import software.amazon.awssdk.services.support.model.AddAttachmentsToSetRequest;
import java.io.File;
import java.io.FileInputStream;
import java.io.FileNotFoundException;
import java.io.InputStream;
import java.time.Instant;
import java.time.temporal.ChronoUnit;
import java.util.ArrayList;
import java.util.List;

/**
 * Before running this Java (v2) code example, set up your development
 * environment, including your credentials.
 *
 * For more information, see the following documentation topic:
 *
 * https://docs.aws.amazon.com/sdk-for-java/latest/developer-guide/get-
started.html
 *
 * In addition, you must have the AWS Business Support Plan to use the AWS
 * Support Java API. For more information, see:
 *
 * https://aws.amazon.com/premiumsupport/plans/
 *
 * This Java example performs the following tasks:
 *
```

```
 * 1. Gets and displays available services.
 * 2. Gets and displays severity levels.
 * 3. Creates a support case by using the selected service, category, and
 * severity level.
 * 4. Gets a list of open cases for the current day.
 * 5. Creates an attachment set with a generated file.
 * 6. Adds a communication with the attachment to the support case.
 * 7. Lists the communications of the support case.
 * 8. Describes the attachment set included with the communication.
 * 9. Resolves the support case.
 * 10. Gets a list of resolved cases for the current day.
 */
public class SupportScenario {

    public static final String DASHES = new String(new char[80]).replace("\0",
 "-");

    public static void main(String[] args) {
        final String usage = """

                Usage:
                    <fileAttachment>Where:
                    fileAttachment - The file can be a simple saved .txt file to
 use as an email attachment.\s
                """;

        if (args.length != 1) {
            System.out.println(usage);
            System.exit(1);
        }

        String fileAttachment = args[0];
        Region region = Region.US_WEST_2;
        SupportClient supportClient = SupportClient.builder()
                .region(region)
                .build();

        System.out.println(DASHES);
        System.out.println("***** Welcome to the AWS Support case example
 scenario.");
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("1. Get and display available services.");
```

```
        List<String> sevCatList = displayServices(supportClient);
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("2. Get and display Support severity levels.");
        String sevLevel = displaySevLevels(supportClient);
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("3. Create a support case using the selected service,
category, and severity level.");
        String caseId = createSupportCase(supportClient, sevCatList, sevLevel);
        if (caseId.compareTo("") == 0) {
            System.out.println("A support case was not successfully created!");
            System.exit(1);
        } else
            System.out.println("Support case " + caseId + " was successfully
created!");
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("4. Get open support cases.");
        getOpenCase(supportClient);
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("5. Create an attachment set with a generated file to
add to the case.");
        String attachmentSetId = addAttachment(supportClient, fileAttachment);
        System.out.println("The Attachment Set id value is" + attachmentSetId);
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("6. Add communication with the attachment to the
support case.");
        addAttachSupportCase(supportClient, caseId, attachmentSetId);
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("7. List the communications of the support case.");
        String attachId = listCommunications(supportClient, caseId);
        System.out.println("The Attachment id value is" + attachId);
        System.out.println(DASHES);
```

```
        System.out.println(DASHES);
        System.out.println("8. Describe the attachment set included with the
communication.");
        describeAttachment(supportClient, attachId);
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("9. Resolve the support case.");
        resolveSupportCase(supportClient, caseId);
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("10. Get a list of resolved cases for the current
day.");
        getResolvedCase(supportClient);
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("***** This Scenario has successfully completed");
        System.out.println(DASHES);
    }

    public static void getResolvedCase(SupportClient supportClient) {
        try {
            // Specify the start and end time.
            Instant now = Instant.now();
            java.time.LocalDate.now();
            Instant yesterday = now.minus(1, ChronoUnit.DAYS);

            DescribeCasesRequest describeCasesRequest =
DescribeCasesRequest.builder()
                    .maxResults(30)
                    .afterTime(yesterday.toString())
                    .beforeTime(now.toString())
                    .includeResolvedCases(true)
                    .build();

            DescribeCasesResponse response =
supportClient.describeCases(describeCasesRequest);
            List<CaseDetails> cases = response.cases();
            for (CaseDetails sinCase : cases) {
                if (sinCase.status().compareTo("resolved") == 0)
                    System.out.println("The case status is " + sinCase.status());
            }
```

```
        } catch (SupportException e) {
            System.out.println(e.getLocalizedMessage());
            System.exit(1);
        }
    }

    public static void resolveSupportCase(SupportClient supportClient, String
caseId) {
        try {
            ResolveCaseRequest caseRequest = ResolveCaseRequest.builder()
                    .caseId(caseId)
                    .build();

            ResolveCaseResponse response =
supportClient.resolveCase(caseRequest);
            System.out.println("The status of case " + caseId + " is " +
response.finalCaseStatus());

        } catch (SupportException e) {
            System.out.println(e.getLocalizedMessage());
            System.exit(1);
        }
    }

    public static void describeAttachment(SupportClient supportClient, String
attachId) {
        try {
            DescribeAttachmentRequest attachmentRequest =
DescribeAttachmentRequest.builder()
                    .attachmentId(attachId)
                    .build();

            DescribeAttachmentResponse response =
supportClient.describeAttachment(attachmentRequest);
            System.out.println("The name of the file is " +
response.attachment().fileName());

        } catch (SupportException e) {
            System.out.println(e.getLocalizedMessage());
            System.exit(1);
        }
    }
```

```
   public static String listCommunications(SupportClient supportClient, String
caseId) {
       try {
           String attachId = null;
           DescribeCommunicationsRequest communicationsRequest =
DescribeCommunicationsRequest.builder()
                   .caseId(caseId)
                   .maxResults(10)
                   .build();

           DescribeCommunicationsResponse response =
supportClient.describeCommunications(communicationsRequest);
           List<Communication> communications = response.communications();
           for (Communication comm : communications) {
               System.out.println("the body is: " + comm.body());

               // Get the attachment id value.
               List<AttachmentDetails> attachments = comm.attachmentSet();
               for (AttachmentDetails detail : attachments) {
                   attachId = detail.attachmentId();
               }
           }
           return attachId;

       } catch (SupportException e) {
           System.out.println(e.getLocalizedMessage());
           System.exit(1);
       }
       return "";
   }

   public static void addAttachSupportCase(SupportClient supportClient, String
caseId, String attachmentSetId) {
       try {
           AddCommunicationToCaseRequest caseRequest =
AddCommunicationToCaseRequest.builder()
                   .caseId(caseId)
                   .attachmentSetId(attachmentSetId)
                   .communicationBody("Please refer to attachment for details.")
                   .build();

           AddCommunicationToCaseResponse response =
supportClient.addCommunicationToCase(caseRequest);
           if (response.result())
```

```
                System.out.println("You have successfully added a communication
to an AWS Support case");
            else
                System.out.println("There was an error adding the communication
to an AWS Support case");

        } catch (SupportException e) {
            System.out.println(e.getLocalizedMessage());
            System.exit(1);
        }
    }

    public static String addAttachment(SupportClient supportClient, String
fileAttachment) {
        try {
            File myFile = new File(fileAttachment);
            InputStream sourceStream = new FileInputStream(myFile);
            SdkBytes sourceBytes = SdkBytes.fromInputStream(sourceStream);

            Attachment attachment = Attachment.builder()
                    .fileName(myFile.getName())
                    .data(sourceBytes)
                    .build();

            AddAttachmentsToSetRequest setRequest =
AddAttachmentsToSetRequest.builder()
                    .attachments(attachment)
                    .build();

            AddAttachmentsToSetResponse response =
supportClient.addAttachmentsToSet(setRequest);
            return response.attachmentSetId();

        } catch (SupportException | FileNotFoundException e) {
            System.out.println(e.getLocalizedMessage());
            System.exit(1);
        }
        return "";
    }

    public static void getOpenCase(SupportClient supportClient) {
        try {
            // Specify the start and end time.
            Instant now = Instant.now();
```

```
            java.time.LocalDate.now();
            Instant yesterday = now.minus(1, ChronoUnit.DAYS);

            DescribeCasesRequest describeCasesRequest =
DescribeCasesRequest.builder()
                    .maxResults(20)
                    .afterTime(yesterday.toString())
                    .beforeTime(now.toString())
                    .build();

            DescribeCasesResponse response =
supportClient.describeCases(describeCasesRequest);
            List<CaseDetails> cases = response.cases();
            for (CaseDetails sinCase : cases) {
                System.out.println("The case status is " + sinCase.status());
                System.out.println("The case Id is " + sinCase.caseId());
                System.out.println("The case subject is " + sinCase.subject());
            }

        } catch (SupportException e) {
            System.out.println(e.getLocalizedMessage());
            System.exit(1);
        }
    }

    public static String createSupportCase(SupportClient supportClient,
List<String> sevCatList, String sevLevel) {
        try {
            String serviceCode = sevCatList.get(0);
            String caseCat = sevCatList.get(1);
            CreateCaseRequest caseRequest = CreateCaseRequest.builder()
                    .categoryCode(caseCat.toLowerCase())
                    .serviceCode(serviceCode.toLowerCase())
                    .severityCode(sevLevel.toLowerCase())
                    .communicationBody("Test issue with " +
serviceCode.toLowerCase())
                    .subject("Test case, please ignore")
                    .language("en")
                    .issueType("technical")
                    .build();

            CreateCaseResponse response = supportClient.createCase(caseRequest);
            return response.caseId();
```

```
        } catch (SupportException e) {
            System.out.println(e.getLocalizedMessage());
            System.exit(1);
        }
        return "";
    }

    public static String displaySevLevels(SupportClient supportClient) {
        try {
            DescribeSeverityLevelsRequest severityLevelsRequest =
DescribeSeverityLevelsRequest.builder()
                    .language("en")
                    .build();

            DescribeSeverityLevelsResponse response =
supportClient.describeSeverityLevels(severityLevelsRequest);
            List<SeverityLevel> severityLevels = response.severityLevels();
            String levelName = null;
            for (SeverityLevel sevLevel : severityLevels) {
                System.out.println("The severity level name is: " +
sevLevel.name());
                if (sevLevel.name().compareTo("High") == 0)
                    levelName = sevLevel.name();
            }
            return levelName;

        } catch (SupportException e) {
            System.out.println(e.getLocalizedMessage());
            System.exit(1);
        }
        return "";
    }

    // Return a List that contains a Service name and Category name.
    public static List<String> displayServices(SupportClient supportClient) {
        try {
            DescribeServicesRequest servicesRequest =
DescribeServicesRequest.builder()
                    .language("en")
                    .build();

            DescribeServicesResponse response =
supportClient.describeServices(servicesRequest);
            String serviceCode = null;
```

```
            String catName = null;
            List<String> sevCatList = new ArrayList<>();
            List<Service> services = response.services();

            System.out.println("Get the first 10 services");
            int index = 1;
            for (Service service : services) {
                if (index == 11)
                    break;

                System.out.println("The Service name is: " + service.name());
                if (service.name().compareTo("Account") == 0)
                    serviceCode = service.code();

                // Get the Categories for this service.
                List<Category> categories = service.categories();
                for (Category cat : categories) {
                    System.out.println("The category name is: " + cat.name());
                    if (cat.name().compareTo("Security") == 0)
                        catName = cat.name();
                }
                index++;
            }

            // Push the two values to the list.
            sevCatList.add(serviceCode);
            sevCatList.add(catName);
            return sevCatList;

        } catch (SupportException e) {
            System.out.println(e.getLocalizedMessage());
            System.exit(1);
        }
        return null;
    }
}
```

- Para obtener información sobre la API, consulte los siguientes temas en la Referencia de la API de AWS SDK for Java 2.x .
  - AddAttachmentsToSet
  - AddCommunicationToCase

- CreateCase
- DescribeAttachment
- DescribeCases
- DescribeCommunications
- DescribeServices
- DescribeSeverityNiveles
- ResolveCase

JavaScript

SDK para JavaScript (v3)

> **Note**
>
> Hay más información. GitHub Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

Ejecute un escenario interactivo en el terminal.

```
import {
  AddAttachmentsToSetCommand,
  AddCommunicationToCaseCommand,
  CreateCaseCommand,
  DescribeAttachmentCommand,
  DescribeCasesCommand,
  DescribeCommunicationsCommand,
  DescribeServicesCommand,
  DescribeSeverityLevelsCommand,
  ResolveCaseCommand,
  SupportClient,
} from "@aws-sdk/client-support";
import * as inquirer from "@inquirer/prompts";
import { retry } from "@aws-doc-sdk-examples/lib/utils/util-timers.js";

const wrapText = (text, char = "=") => {
  const rule = char.repeat(80);
  return `${rule}\n    ${text}\n${rule}\n`;
};
```

```
const client = new SupportClient({ region: "us-east-1" });

// Verify that the account has a Support plan.
export const verifyAccount = async () => {
  const command = new DescribeServicesCommand({});

  try {
    await client.send(command);
  } catch (err) {
    if (err.name === "SubscriptionRequiredException") {
      throw new Error(
        "You must be subscribed to the AWS Support plan to use this feature.",
      );
    } else {
      throw err;
    }
  }
};

/**
 * Select a service from the list returned from DescribeServices.
 */
export const getService = async () => {
  const { services } = await client.send(new DescribeServicesCommand({}));
  const selectedService = await inquirer.select({
    message:
      "Select a service. Your support case will be created for this service. The
 list of services is truncated for readability.",
    choices: services.slice(0, 10).map((s) => ({ name: s.name, value: s })),
  });
  return selectedService;
};

/**
 * @param {{ categories: import('@aws-sdk/client-support').Category[]}} service
 */
export const getCategory = async (service) => {
  const selectedCategory = await inquirer.select({
    message: "Select a category.",
    choices: service.categories.map((c) => ({ name: c.name, value: c })),
  });
  return selectedCategory;
};
```

```
// Get the available severity levels for the account.
export const getSeverityLevel = async () => {
  const command = new DescribeSeverityLevelsCommand({});
  const { severityLevels } = await client.send(command);
  const selectedSeverityLevel = await inquirer.select({
    message: "Select a severity level.",
    choices: severityLevels.map((s) => ({ name: s.name, value: s })),
  });
  return selectedSeverityLevel;
};

/**
 * Create a new support case
 * @param {{
 *  selectedService: import('@aws-sdk/client-support').Service
 *  selectedCategory: import('@aws-sdk/client-support').Category
 *  selectedSeverityLevel: import('@aws-sdk/client-support').SeverityLevel
 * }} selections
 * @returns
 */
export const createCase = async ({
  selectedService,
  selectedCategory,
  selectedSeverityLevel,
}) => {
  const command = new CreateCaseCommand({
    subject: "IGNORE: Test case",
    communicationBody: "This is a test. Please ignore.",
    serviceCode: selectedService.code,
    categoryCode: selectedCategory.code,
    severityCode: selectedSeverityLevel.code,
  });
  const { caseId } = await client.send(command);
  return caseId;
};

// Get a list of open support cases created today.
export const getTodaysOpenCases = async () => {
  const d = new Date();
  const startOfToday = new Date(d.getFullYear(), d.getMonth(), d.getDate());
  const command = new DescribeCasesCommand({
    includeCommunications: false,
    afterTime: startOfToday.toISOString(),
```

```
  });

  const { cases } = await client.send(command);

  if (cases.length === 0) {
    throw new Error(
      "Unexpected number of cases. Expected more than 0 open cases.",
    );
  }
  return cases;
};

// Create an attachment set.
export const createAttachmentSet = async () => {
  const command = new AddAttachmentsToSetCommand({
    attachments: [
      {
        fileName: "example.txt",
        data: new TextEncoder().encode("some example text"),
      },
    ],
  });
  const { attachmentSetId } = await client.send(command);
  return attachmentSetId;
};

export const linkAttachmentSetToCase = async (attachmentSetId, caseId) => {
  const command = new AddCommunicationToCaseCommand({
    attachmentSetId,
    caseId,
    communicationBody: "Adding attachment set to case.",
  });
  await client.send(command);
};

// Get all communications for a support case.
export const getCommunications = async (caseId) => {
  const command = new DescribeCommunicationsCommand({
    caseId,
  });
  const { communications } = await client.send(command);
  return communications;
};
```

```
/**
 * @param {import('@aws-sdk/client-support').Communication[]} communications
 */
export const getFirstAttachment = (communications) => {
  const firstCommWithAttachment = communications.find(
    (c) => c.attachmentSet.length > 0,
  );
  return firstCommWithAttachment?.attachmentSet[0].attachmentId;
};

// Get an attachment.
export const getAttachment = async (attachmentId) => {
  const command = new DescribeAttachmentCommand({
    attachmentId,
  });
  const { attachment } = await client.send(command);
  return attachment;
};

// Resolve the case matching the given case ID.
export const resolveCase = async (caseId) => {
  const shouldResolve = await inquirer.confirm({
    message: `Do you want to resolve ${caseId}?`,
  });

  if (shouldResolve) {
    const command = new ResolveCaseCommand({
      caseId: caseId,
    });

    await client.send(command);
    return true;
  }
  return false;
};

/**
 * Find a specific case in the list of provided cases by case ID.
 * If the case is not found, and the results are paginated, continue
 * paging through the results.
 * @param {{
 *   caseId: string,
 *   cases: import('@aws-sdk/client-support').CaseDetails[]
 *   nextToken: string
```

```
 * }} options
 * @returns
 */
export const findCase = async ({ caseId, cases, nextToken }) => {
  const foundCase = cases.find((c) => c.caseId === caseId);

  if (foundCase) {
    return foundCase;
  }

  if (nextToken) {
    const response = await client.send(
      new DescribeCasesCommand({
        nextToken,
        includeResolvedCases: true,
      }),
    );
    return findCase({
      caseId,
      cases: response.cases,
      nextToken: response.nextToken,
    });
  }

  throw new Error(`${caseId} not found.`);
};

// Get all cases created today.
export const getTodaysResolvedCases = async (caseIdToWaitFor) => {
  const d = new Date("2023-01-18");
  const startOfToday = new Date(d.getFullYear(), d.getMonth(), d.getDate());
  const command = new DescribeCasesCommand({
    includeCommunications: false,
    afterTime: startOfToday.toISOString(),
    includeResolvedCases: true,
  });
  const { cases, nextToken } = await client.send(command);
  await findCase({ cases, caseId: caseIdToWaitFor, nextToken });
  return cases.filter((c) => c.status === "resolved");
};

const main = async () => {
  let caseId;
  try {
```

```
    console.log(wrapText("Welcome to the AWS Support basic usage scenario."));

    // Verify that the account is subscribed to support.
    await verifyAccount();

    // Provided a truncated list of services and prompt the user to select one.
    const selectedService = await getService();

    // Provided the categories for the selected service and prompt the user to
select one.
    const selectedCategory = await getCategory(selectedService);

    // Provide the severity available severity levels for the account and prompt
the user to select one.
    const selectedSeverityLevel = await getSeverityLevel();

    // Create a support case.
    console.log("\nCreating a support case.");
    caseId = await createCase({
      selectedService,
      selectedCategory,
      selectedSeverityLevel,
    });
    console.log(`Support case created: ${caseId}`);

    // Display a list of open support cases created today.
    const todaysOpenCases = await retry(
      { intervalInMs: 1000, maxRetries: 15 },
      getTodaysOpenCases,
    );
    console.log(
      `\nOpen support cases created today: ${todaysOpenCases.length}`,
    );
    console.log(todaysOpenCases.map((c) => `${c.caseId}`).join("\n"));

    // Create an attachment set.
    console.log("\nCreating an attachment set.");
    const attachmentSetId = await createAttachmentSet();
    console.log(`Attachment set created: ${attachmentSetId}`);

    // Add the attachment set to the support case.
    console.log(`\nAdding attachment set to ${caseId}`);
    await linkAttachmentSetToCase(attachmentSetId, caseId);
    console.log(`Attachment set added to ${caseId}`);
```

```
    // List the communications for a support case.
    console.log(`\nListing communications for ${caseId}`);
    const communications = await getCommunications(caseId);
    console.log(
      communications
        .map(
          (c) =>
            `Communication created on ${c.timeCreated}. Has
 ${c.attachmentSet.length} attachments.`,
        )
        .join("\n"),
    );

    // Describe the first attachment.
    console.log(`\nDescribing attachment ${attachmentSetId}`);
    const attachmentId = getFirstAttachment(communications);
    const attachment = await getAttachment(attachmentId);
    console.log(
      `Attachment is the file '${
        attachment.fileName
      }' with data: \n${new TextDecoder().decode(attachment.data)}`,
    );

    // Confirm that the support case should be resolved.
    const isResolved = await resolveCase(caseId);
    if (isResolved) {
      // List the resolved cases and include the one previously created.
      // Resolved cases can take a while to appear.
      console.log(
        "\nWaiting for case status to be marked as resolved. This can take some
 time.",
      );
      const resolvedCases = await retry(
        { intervalInMs: 20000, maxRetries: 15 },
        () => getTodaysResolvedCases(caseId),
      );
      console.log("Resolved cases:");
      console.log(resolvedCases.map((c) => c.caseId).join("\n"));
    }
  } catch (err) {
    console.error(err);
  }
};
```

- Para obtener información sobre la API, consulte los siguientes temas en la referencia de la API de AWS SDK for JavaScript .
  - AddAttachmentsToSet
  - AddCommunicationToCase
  - CreateCase
  - DescribeAttachment
  - DescribeCases
  - DescribeCommunications
  - DescribeServices
  - DescribeSeverityNiveles
  - ResolveCase

Kotlin

SDK para Kotlin

> **Note**
>
> Hay más en marcha GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
/**
Before running this Kotlin code example, set up your development environment,
including your credentials.

For more information, see the following documentation topic:

https://docs.aws.amazon.com/sdk-for-kotlin/latest/developer-guide/setup.html
In addition, you must have the AWS Business Support Plan to use the AWS Support
 Java API. For more information, see:

https://aws.amazon.com/premiumsupport/plans/
```

```
This Kotlin example performs the following tasks:
1. Gets and displays available services.
2. Gets and displays severity levels.
3. Creates a support case by using the selected service, category, and severity
 level.
4. Gets a list of open cases for the current day.
5. Creates an attachment set with a generated file.
6. Adds a communication with the attachment to the support case.
7. Lists the communications of the support case.
8. Describes the attachment set included with the communication.
9. Resolves the support case.
10. Gets a list of resolved cases for the current day.
*/

suspend fun main(args: Array<String>) {
    val usage = """
    Usage:
        <fileAttachment>
    Where:
         fileAttachment - The file can be a simple saved .txt file to use as an
 email attachment.
    """

    if (args.size != 1) {
        println(usage)
        exitProcess(0)
    }

    val fileAttachment = args[0]
    println("***** Welcome to the AWS Support case example scenario.")
    println("***** Step 1. Get and display available services.")
    val sevCatList = displayServices()

    println("***** Step 2. Get and display Support severity levels.")
    val sevLevel = displaySevLevels()

    println("***** Step 3. Create a support case using the selected service,
 category, and severity level.")
    val caseIdVal = createSupportCase(sevCatList, sevLevel)
    if (caseIdVal != null) {
        println("Support case $caseIdVal was successfully created!")
    } else {
        println("A support case was not successfully created!")
        exitProcess(1)
```

```
    }

    println("***** Step 4. Get open support cases.")
    getOpenCase()

    println("***** Step 5. Create an attachment set with a generated file to add
 to the case.")
    val attachmentSetId = addAttachment(fileAttachment)
    println("The Attachment Set id value is $attachmentSetId")

    println("***** Step 6. Add communication with the attachment to the support
 case.")
    addAttachSupportCase(caseIdVal, attachmentSetId)

    println("***** Step 7. List the communications of the support case.")
    val attachId = listCommunications(caseIdVal)
    println("The Attachment id value is $attachId")

    println("***** Step 8. Describe the attachment set included with the
 communication.")
    describeAttachment(attachId)

    println("***** Step 9. Resolve the support case.")
    resolveSupportCase(caseIdVal)

    println("***** Step 10. Get a list of resolved cases for the current day.")
    getResolvedCase()
    println("***** This Scenario has successfully completed")
}

suspend fun getResolvedCase() {
    // Specify the start and end time.
    val now = Instant.now()
    LocalDate.now()
    val yesterday = now.minus(1, ChronoUnit.DAYS)
    val describeCasesRequest =
        DescribeCasesRequest {
            maxResults = 30
            afterTime = yesterday.toString()
            beforeTime = now.toString()
            includeResolvedCases = true
        }

    SupportClient { region = "us-west-2" }.use { supportClient ->
```

```
        val response = supportClient.describeCases(describeCasesRequest)
        response.cases?.forEach { sinCase ->
            println("The case status is ${sinCase.status}")
            println("The case Id is ${sinCase.caseId}")
            println("The case subject is ${sinCase.subject}")
        }
    }
}

suspend fun resolveSupportCase(caseIdVal: String) {
    val caseRequest =
        ResolveCaseRequest {
            caseId = caseIdVal
        }
    SupportClient { region = "us-west-2" }.use { supportClient ->
        val response = supportClient.resolveCase(caseRequest)
        println("The status of case $caseIdVal is ${response.finalCaseStatus}")
    }
}

suspend fun describeAttachment(attachId: String?) {
    val attachmentRequest =
        DescribeAttachmentRequest {
            attachmentId = attachId
        }

    SupportClient { region = "us-west-2" }.use { supportClient ->
        val response = supportClient.describeAttachment(attachmentRequest)
        println("The name of the file is ${response.attachment?.fileName}")
    }
}

suspend fun listCommunications(caseIdVal: String?): String? {
    val communicationsRequest =
        DescribeCommunicationsRequest {
            caseId = caseIdVal
            maxResults = 10
        }

    SupportClient { region = "us-west-2" }.use { supportClient ->
        val response =
 supportClient.describeCommunications(communicationsRequest)
        response.communications?.forEach { comm ->
            println("the body is: " + comm.body)
```

```
            comm.attachmentSet?.forEach { detail ->
                return detail.attachmentId
            }
        }
    }
    return ""
}

suspend fun addAttachSupportCase(
    caseIdVal: String?,
    attachmentSetIdVal: String?
) {
    val caseRequest =
        AddCommunicationToCaseRequest {
            caseId = caseIdVal
            attachmentSetId = attachmentSetIdVal
            communicationBody = "Please refer to attachment for details."
        }

    SupportClient { region = "us-west-2" }.use { supportClient ->
        val response = supportClient.addCommunicationToCase(caseRequest)
        if (response.result) {
            println("You have successfully added a communication to an AWS
 Support case")
        } else {
            println("There was an error adding the communication to an AWS
 Support case")
        }
    }
}

suspend fun addAttachment(fileAttachment: String): String? {
    val myFile = File(fileAttachment)
    val sourceBytes = (File(fileAttachment).readBytes())
    val attachmentVal =
        Attachment {
            fileName = myFile.name
            data = sourceBytes
        }

    val setRequest =
        AddAttachmentsToSetRequest {
            attachments = listOf(attachmentVal)
        }
```

```
    SupportClient { region = "us-west-2" }.use { supportClient ->
        val response = supportClient.addAttachmentsToSet(setRequest)
        return response.attachmentSetId
    }
}

suspend fun getOpenCase() {
    // Specify the start and end time.
    val now = Instant.now()
    LocalDate.now()
    val yesterday = now.minus(1, ChronoUnit.DAYS)
    val describeCasesRequest =
        DescribeCasesRequest {
            maxResults = 20
            afterTime = yesterday.toString()
            beforeTime = now.toString()
        }

    SupportClient { region = "us-west-2" }.use { supportClient ->
        val response = supportClient.describeCases(describeCasesRequest)
        response.cases?.forEach { sinCase ->
            println("The case status is ${sinCase.status}")
            println("The case Id is ${sinCase.caseId}")
            println("The case subject is ${sinCase.subject}")
        }
    }
}

suspend fun createSupportCase(
    sevCatListVal: List<String>,
    sevLevelVal: String
): String? {
    val serCode = sevCatListVal[0]
    val caseCategory = sevCatListVal[1]
    val caseRequest =
        CreateCaseRequest {
            categoryCode = caseCategory.lowercase(Locale.getDefault())
            serviceCode = serCode.lowercase(Locale.getDefault())
            severityCode = sevLevelVal.lowercase(Locale.getDefault())
            communicationBody = "Test issue with
 ${serCode.lowercase(Locale.getDefault())}"
            subject = "Test case, please ignore"
            language = "en"
```

```
            issueType = "technical"
        }

    SupportClient { region = "us-west-2" }.use { supportClient ->
        val response = supportClient.createCase(caseRequest)
        return response.caseId
    }
}

suspend fun displaySevLevels(): String {
    var levelName = ""
    val severityLevelsRequest =
        DescribeSeverityLevelsRequest {
            language = "en"
        }

    SupportClient { region = "us-west-2" }.use { supportClient ->
        val response =
 supportClient.describeSeverityLevels(severityLevelsRequest)
        response.severityLevels?.forEach { sevLevel ->
            println("The severity level name is: ${sevLevel.name}")
            if (sevLevel.name == "High") {
                levelName = sevLevel.name!!
            }
        }
        return levelName
    }
}

// Return a List that contains a Service name and Category name.
suspend fun displayServices(): List<String> {
    var serviceCode = ""
    var catName = ""
    val sevCatList = mutableListOf<String>()
    val servicesRequest =
        DescribeServicesRequest {
            language = "en"
        }

    SupportClient { region = "us-west-2" }.use { supportClient ->
        val response = supportClient.describeServices(servicesRequest)
        println("Get the first 10 services")
        var index = 1
```

```
        response.services?.forEach { service ->
            if (index == 11) {
                return@forEach
            }

            println("The Service name is ${service.name}")
            if (service.name == "Account") {
                serviceCode = service.code.toString()
            }

            // Get the categories for this service.
            service.categories?.forEach { cat ->
                println("The category name is ${cat.name}")
                if (cat.name == "Security") {
                    catName = cat.name!!
                }
            }
            index++
        }
    }

    // Push the two values to the list.
    serviceCode.let { sevCatList.add(it) }
    catName.let { sevCatList.add(it) }
    return sevCatList
}
```

- Para obtener información acerca de la API, consulte los siguientes temas en la Referencia de la API de AWS SDK para Kotlin.
  - AddAttachmentsToSet
  - AddCommunicationToCase
  - CreateCase
  - DescribeAttachment
  - DescribeCases
  - DescribeCommunications
  - DescribeServices
  - DescribeSeverityNiveles
  - ResolveCase

Python

SDK para Python (Boto3)

> **Note**
>
> Hay más en marcha GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

Ejecutar un escenario interactivo en un símbolo del sistema.

```
class SupportCasesScenario:
    """Runs an interactive scenario that shows how to get started using AWS
 Support."""

    def __init__(self, support_wrapper):
        """
        :param support_wrapper: An object that wraps AWS Support actions.
        """
        self.support_wrapper = support_wrapper

    def display_and_select_service(self):
        """
        Lists support services and prompts the user to select one.

        :return: The support service selected by the user.
        """
        print("-" * 88)
        services_list = self.support_wrapper.describe_services("en")
        print(f"AWS Support client returned {len(services_list)} services.")
        print("Displaying first 10 services:")

        service_choices = [svc["name"] for svc in services_list[:10]]
        selected_index = q.choose(
            "Select an example support service by entering a number from the
 preceding list:",
            service_choices,
        )
        selected_service = services_list[selected_index]
        print("-" * 88)
        return selected_service
```

```
    def display_and_select_category(self, service):
        """
        Lists categories for a support service and prompts the user to select
one.

        :param service: The service of the categories.
        :return: The selected category.
        """
        print("-" * 88)
        print(
            f"Available support categories for Service {service['name']}
{len(service['categories'])}:"
        )
        categories_choices = [category["name"] for category in
service["categories"]]
        selected_index = q.choose(
            "Select an example support category by entering a number from the
preceding list:",
            categories_choices,
        )
        selected_category = service["categories"][selected_index]
        print("-" * 88)
        return selected_category

    def display_and_select_severity(self):
        """
        Lists available severity levels and prompts the user to select one.

        :return: The selected severity level.
        """
        print("-" * 88)
        severity_levels_list =
self.support_wrapper.describe_severity_levels("en")
        print(f"Available severity levels:")
        severity_choices = [level["name"] for level in severity_levels_list]
        selected_index = q.choose(
            "Select an example severity level by entering a number from the
preceding list:",
            severity_choices,
        )
        selected_severity = severity_levels_list[selected_index]
        print("-" * 88)
        return selected_severity
```

```
    def create_example_case(self, service, category, severity_level):
        """
        Creates an example support case with the user's selections.

        :param service: The service for the new case.
        :param category: The category for the new case.
        :param severity_level: The severity level for the new case.
        :return: The caseId of the new support case.
        """
        print("-" * 88)
        print(f"Creating new case for service {service['name']}.")
        case_id = self.support_wrapper.create_case(service, category,
severity_level)
        print(f"\tNew case created with ID {case_id}.")
        print("-" * 88)
        return case_id

    def list_open_cases(self):
        """
        List the open cases for the current day.
        """
        print("-" * 88)
        print("Let's list the open cases for the current day.")
        start_time = str(datetime.utcnow().date())
        end_time = str(datetime.utcnow().date() + timedelta(days=1))
        open_cases = self.support_wrapper.describe_cases(start_time, end_time,
False)
        for case in open_cases:
            print(f"\tCase: {case['caseId']}: status {case['status']}.")
        print("-" * 88)

    def create_attachment_set(self):
        """
        Create an attachment set with a sample file.

        :return: The attachment set ID of the new attachment set.
        """
        print("-" * 88)
        print("Creating attachment set with a sample file.")
        attachment_set_id = self.support_wrapper.add_attachment_to_set()
        print(f"\tNew attachment set created with ID {attachment_set_id}.")
        print("-" * 88)
        return attachment_set_id
```

```
    def add_communication(self, case_id, attachment_set_id):
        """
        Add a communication with an attachment set to the case.

        :param case_id: The ID of the case for the communication.
        :param attachment_set_id: The ID of the attachment set to
        add to the communication.
        """
        print("-" * 88)
        print(f"Adding a communication and attachment set to the case.")
        self.support_wrapper.add_communication_to_case(attachment_set_id,
case_id)
        print(
            f"Added a communication and attachment set {attachment_set_id} to the
case {case_id}."
        )
        print("-" * 88)

    def list_communications(self, case_id):
        """
        List the communications associated with a case.

        :param case_id: The ID of the case.
        :return: The attachment ID of an attachment.
        """
        print("-" * 88)
        print("Let's list the communications for our case.")
        attachment_id = ""
        communications =
self.support_wrapper.describe_all_case_communications(case_id)
        for communication in communications:
            print(
                f"\tCommunication created on {communication['timeCreated']} "
                f"has {len(communication['attachmentSet'])} attachments."
            )
            if len(communication["attachmentSet"]) > 0:
                attachment_id = communication["attachmentSet"][0]["attachmentId"]
        print("-" * 88)
        return attachment_id

    def describe_case_attachment(self, attachment_id):
        """
        Describe an attachment associated with a case.
```

```
        :param attachment_id: The ID of the attachment.
        """
        print("-" * 88)
        print("Let's list the communications for our case.")
        attached_file = self.support_wrapper.describe_attachment(attachment_id)
        print(f"\tAttachment includes file {attached_file}.")
        print("-" * 88)

    def resolve_case(self, case_id):
        """
        Shows how to resolve an AWS Support case by its ID.

        :param case_id: The ID of the case to resolve.
        """
        print("-" * 88)
        print(f"Resolving case with ID {case_id}.")
        case_status = self.support_wrapper.resolve_case(case_id)
        print(f"\tFinal case status is {case_status}.")
        print("-" * 88)

    def list_resolved_cases(self):
        """
        List the resolved cases for the current day.
        """
        print("-" * 88)
        print("Let's list the resolved cases for the current day.")
        start_time = str(datetime.utcnow().date())
        end_time = str(datetime.utcnow().date() + timedelta(days=1))
        resolved_cases = self.support_wrapper.describe_cases(start_time,
end_time, True)
        for case in resolved_cases:
            print(f"\tCase: {case['caseId']}: status {case['status']}.")
        print("-" * 88)

    def run_scenario(self):
        logging.basicConfig(level=logging.INFO, format="%(levelname)s:
%(message)s")

        print("-" * 88)
        print("Welcome to the AWS Support get started with support cases demo.")
        print("-" * 88)

        selected_service = self.display_and_select_service()
        selected_category = self.display_and_select_category(selected_service)
```

```
        selected_severity = self.display_and_select_severity()
        new_case_id = self.create_example_case(
            selected_service, selected_category, selected_severity
        )
        wait(10)
        self.list_open_cases()
        new_attachment_set_id = self.create_attachment_set()
        self.add_communication(new_case_id, new_attachment_set_id)
        new_attachment_id = self.list_communications(new_case_id)
        self.describe_case_attachment(new_attachment_id)
        self.resolve_case(new_case_id)
        wait(10)
        self.list_resolved_cases()

        print("\nThanks for watching!")
        print("-" * 88)


if __name__ == "__main__":
    try:
        scenario = SupportCasesScenario(SupportWrapper.from_client())
        scenario.run_scenario()
    except Exception:
        logging.exception("Something went wrong with the demo.")
```

Defina una clase que incluya acciones de soporte al cliente.

```
class SupportWrapper:
    """Encapsulates Support actions."""

    def __init__(self, support_client):
        """
        :param support_client: A Boto3 Support client.
        """
        self.support_client = support_client

    @classmethod
    def from_client(cls):
        """
        Instantiates this class from a Boto3 client.
        """
        support_client = boto3.client("support")
```

```
        return cls(support_client)


    def describe_services(self, language):
        """
        Get the descriptions of AWS services available for support for a
language.

        :param language: The language for support services.
        Currently, only "en" (English) and "ja" (Japanese) are supported.
        :return: The list of AWS service descriptions.
        """
        try:
            response = self.support_client.describe_services(language=language)
            services = response["services"]
        except ClientError as err:
            if err.response["Error"]["Code"] == "SubscriptionRequiredException":
                logger.info(
                    "You must have a Business, Enterprise On-Ramp, or Enterprise
Support "
                    "plan to use the AWS Support API. \n\tPlease upgrade your
subscription to run these "
                    "examples."
                )
            else:
                logger.error(
                    "Couldn't get Support services for language %s. Here's why:
%s: %s",
                    language,
                    err.response["Error"]["Code"],
                    err.response["Error"]["Message"],
                )
                raise
        else:
            return services


    def describe_severity_levels(self, language):
        """
        Get the descriptions of available severity levels for support cases for a
language.

        :param language: The language for support severity levels.
        Currently, only "en" (English) and "ja" (Japanese) are supported.
```

```
        :return: The list of severity levels.
        """
        try:
            response =
self.support_client.describe_severity_levels(language=language)
            severity_levels = response["severityLevels"]
        except ClientError as err:
            if err.response["Error"]["Code"] == "SubscriptionRequiredException":
                logger.info(
                    "You must have a Business, Enterprise On-Ramp, or Enterprise
Support "
                    "plan to use the AWS Support API. \n\tPlease upgrade your
subscription to run these "
                    "examples."
                )
            else:
                logger.error(
                    "Couldn't get severity levels for language %s. Here's why:
%s: %s",
                    language,
                    err.response["Error"]["Code"],
                    err.response["Error"]["Message"],
                )
                raise
        else:
            return severity_levels


    def create_case(self, service, category, severity):
        """
        Create a new support case.

        :param service: The service to use for the new case.
        :param category: The category to use for the new case.
        :param severity: The severity to use for the new case.
        :return: The caseId of the new case.
        """
        try:
            response = self.support_client.create_case(
                subject="Example case for testing, ignore.",
                serviceCode=service["code"],
                severityCode=severity["code"],
                categoryCode=category["code"],
                communicationBody="Example support case body.",
```

```
                language="en",
                issueType="customer-service",
            )
            case_id = response["caseId"]
        except ClientError as err:
            if err.response["Error"]["Code"] == "SubscriptionRequiredException":
                logger.info(
                    "You must have a Business, Enterprise On-Ramp, or Enterprise
Support "
                    "plan to use the AWS Support API. \n\tPlease upgrade your
subscription to run these "
                    "examples."
                )
            else:
                logger.error(
                    "Couldn't create case. Here's why: %s: %s",
                    err.response["Error"]["Code"],
                    err.response["Error"]["Message"],
                )
                raise
        else:
            return case_id


    def add_attachment_to_set(self):
        """
        Add an attachment to a set, or create a new attachment set if one does
not exist.

        :return: The attachment set ID.
        """
        try:
            response = self.support_client.add_attachments_to_set(
                attachments=[
                    {
                        "fileName": "attachment_file.txt",
                        "data": b"This is a sample file for attachment to a
support case.",
                    }
                ]
            )
            new_set_id = response["attachmentSetId"]
        except ClientError as err:
            if err.response["Error"]["Code"] == "SubscriptionRequiredException":
```

```
                logger.info(
                    "You must have a Business, Enterprise On-Ramp, or Enterprise
Support "
                    "plan to use the AWS Support API. \n\tPlease upgrade your
subscription to run these "
                    "examples."
                )
            else:
                logger.error(
                    "Couldn't add attachment. Here's why: %s: %s",
                    err.response["Error"]["Code"],
                    err.response["Error"]["Message"],
                )
                raise
        else:
            return new_set_id


    def add_communication_to_case(self, attachment_set_id, case_id):
        """
        Add a communication and an attachment set to a case.

        :param attachment_set_id: The ID of an existing attachment set.
        :param case_id: The ID of the case.
        """
        try:
            self.support_client.add_communication_to_case(
                caseId=case_id,
                communicationBody="This is an example communication added to a
support case.",
                attachmentSetId=attachment_set_id,
            )
        except ClientError as err:
            if err.response["Error"]["Code"] == "SubscriptionRequiredException":
                logger.info(
                    "You must have a Business, Enterprise On-Ramp, or Enterprise
Support "
                    "plan to use the AWS Support API. \n\tPlease upgrade your
subscription to run these "
                    "examples."
                )
            else:
                logger.error(
                    "Couldn't add communication. Here's why: %s: %s",
```

```
                    err.response["Error"]["Code"],
                    err.response["Error"]["Message"],
                )
                raise


    def describe_all_case_communications(self, case_id):
        """
        Describe all the communications for a case using a paginator.

        :param case_id: The ID of the case.
        :return: The communications for the case.
        """
        try:
            communications = []
            paginator =
self.support_client.get_paginator("describe_communications")
            for page in paginator.paginate(caseId=case_id):
                communications += page["communications"]
        except ClientError as err:
            if err.response["Error"]["Code"] == "SubscriptionRequiredException":
                logger.info(
                    "You must have a Business, Enterprise On-Ramp, or Enterprise
Support "
                    "plan to use the AWS Support API. \n\tPlease upgrade your
subscription to run these "
                    "examples."
                )
            else:
                logger.error(
                    "Couldn't describe communications. Here's why: %s: %s",
                    err.response["Error"]["Code"],
                    err.response["Error"]["Message"],
                )
                raise
        else:
            return communications


    def describe_attachment(self, attachment_id):
        """
        Get information about an attachment by its attachmentID.

        :param attachment_id: The ID of the attachment.
```

```
        :return: The name of the attached file.
        """
        try:
            response = self.support_client.describe_attachment(
                attachmentId=attachment_id
            )
            attached_file = response["attachment"]["fileName"]
        except ClientError as err:
            if err.response["Error"]["Code"] == "SubscriptionRequiredException":
                logger.info(
                    "You must have a Business, Enterprise On-Ramp, or Enterprise
Support "
                    "plan to use the AWS Support API. \n\tPlease upgrade your
subscription to run these "
                    "examples."
                )
            else:
                logger.error(
                    "Couldn't get attachment description. Here's why: %s: %s",
                    err.response["Error"]["Code"],
                    err.response["Error"]["Message"],
                )
                raise
        else:
            return attached_file


    def resolve_case(self, case_id):
        """
        Resolve a support case by its caseId.

        :param case_id: The ID of the case to resolve.
        :return: The final status of the case.
        """
        try:
            response = self.support_client.resolve_case(caseId=case_id)
            final_status = response["finalCaseStatus"]
        except ClientError as err:
            if err.response["Error"]["Code"] == "SubscriptionRequiredException":
                logger.info(
                    "You must have a Business, Enterprise On-Ramp, or Enterprise
Support "
                    "plan to use the AWS Support API. \n\tPlease upgrade your
subscription to run these "
```

```
                    "examples."
                )
            else:
                logger.error(
                    "Couldn't resolve case. Here's why: %s: %s",
                    err.response["Error"]["Code"],
                    err.response["Error"]["Message"],
                )
                raise
        else:
            return final_status


    def describe_cases(self, after_time, before_time, resolved):
        """
        Describe support cases over a period of time, optionally filtering
        by status.

        :param after_time: The start time to include for cases.
        :param before_time: The end time to include for cases.
        :param resolved: True to include resolved cases in the results,
            otherwise results are open cases.
        :return: The final status of the case.
        """
        try:
            cases = []
            paginator = self.support_client.get_paginator("describe_cases")
            for page in paginator.paginate(
                afterTime=after_time,
                beforeTime=before_time,
                includeResolvedCases=resolved,
                language="en",
            ):
                cases += page["cases"]
        except ClientError as err:
            if err.response["Error"]["Code"] == "SubscriptionRequiredException":
                logger.info(
                    "You must have a Business, Enterprise On-Ramp, or Enterprise
Support "
                    "plan to use the AWS Support API. \n\tPlease upgrade your
subscription to run these "
                    "examples."
                )
            else:
```

```
                logger.error(
                    "Couldn't describe cases. Here's why: %s: %s",
                    err.response["Error"]["Code"],
                    err.response["Error"]["Message"],
                )
                raise
        else:
            if resolved:
                cases = filter(lambda case: case["status"] == "resolved", cases)
            return cases
```

- Para obtener información sobre la API, consulte los siguientes temas en la Referencia de la API de AWS SDK para Python (Boto3).
  - AddAttachmentsToSet
  - AddCommunicationToCase
  - CreateCase
  - DescribeAttachment
  - DescribeCases
  - DescribeCommunications
  - DescribeServices
  - DescribeSeverityNiveles
  - ResolveCase

Para obtener una lista completa de guías para desarrolladores del AWS SDK y ejemplos de código, consulteAWS Support Utilizándolo con un AWS SDK. En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

Supervisar y registrar para AWS Support

La supervisión es una parte importante del mantenimiento de la fiabilidad, la disponibilidad y el rendimiento de AWS Support y de sus otras soluciones de AWS. AWS ofrece las siguientes herramientas de supervisión para vigilar AWS Support, informar cuando algo no va bien y tomar medidas automáticamente cuando proceda:

- Amazon EventBridge proporciona una transmisión de una secuencia de eventos de sistema casi en tiempo real que describen cambios en los recursos de AWS. EventBridge habilita la computación basada en eventos automatizada, para que pueda escribir reglas que vigilan determinados eventos y desencadenan acciones automatizadas en otros servicios de AWS cuando estos eventos se producen. Para obtener más información, consulte la Guía del usuario de Amazon EventBridge.
- AWS CloudTrail captura llamadas a la API y eventos relacionados efectuados por su cuenta de AWS o en su nombre, y entrega los archivos de registro al bucket de Amazon S3 que se haya especificado. También pueden identificar qué usuarios y cuentas llamaron a AWS, la dirección IP de origen de las llamadas y el momento en que se hicieron. Para obtener más información, consulte la Guía del usuario de AWS CloudTrail.

Temas

Supervisión de AWS Support casos con Amazon EventBridge

Puedes usar Amazon EventBridge para detectar los cambios en tus AWS Support casos y reaccionar ante ellos. A continuación, en función de las reglas que cree, EventBridge invoca una o más acciones objetivo cuando un evento coincide con los valores que especifique en una regla.

Dependiendo del tipo de evento, puede enviar notificaciones, capturar información sobre el evento, tomar medidas correctivas, iniciar eventos o adoptar otras acciones. Por ejemplo: puede recibir notificaciones cada vez que se produzcan las acciones siguientes en su cuenta:

- Creación de un caso de soporte

- Agregar correspondencia de un caso a un caso de soporte existente
- Resolución de un caso de soporte
- Volver a abrir un caso de soporte

> **Note**
>
> AWS Support entrega eventos de la mejor forma posible. No siempre se garantiza que los eventos se entreguen a EventBridge.

Creación de una regla de EventBridge para los casos de AWS Support.

Puede crear una EventBridge regla para recibir notificaciones de los eventos de los AWS Support casos. La regla supervisará las actualizaciones de los casos de soporte de su cuenta, incluidas las acciones que usted, sus usuarios de IAM o los agentes de soporte realizan. Antes de crear reglas de eventos para AWS Support, haga lo siguiente:

- Familiarícese con los eventos, las reglas y los objetivos en EventBridge. Para obtener más información, consulta ¿Qué es Amazon EventBridge? en la Guía del EventBridge usuario de Amazon.
- Crear el destino que se va a usar en su regla de eventos. Por ejemplo, puede crear un tema de Amazon Simple Notification Service (Amazon SNS) de modo que cada vez que se actualice un caso de soporte, reciba un mensaje de texto o un correo electrónico. Para más información, consulte Destinos de EventBridge.

> **Note**
>
> AWS Support es un servicio global. Para recibir actualizaciones de los casos de soporte, puede utilizar una de las siguientes regiones: este de EE. UU. (Norte de Virginia), oeste de EE. UU. (Oregón) o Europa (Irlanda).

Para crear una EventBridge regla para los eventos de AWS Support casos

1. Abre la EventBridge consola de Amazon en https://console.aws.amazon.com/events/.

2. Si aún no lo ha hecho, use el Selector de regiones en la esquina superior derecha de la página y elija Este de EE. UU. (Norte de Virginia).
3. En el panel de navegación, seleccione Reglas.
4. Elija Create rule (Crear regla).
5. En la página Crear detalles de la regla, ingrese un nombre y una descripción para su regla.
6. Mantenga los valores predeterminados para Event bus (Bus de eventos) y Rules type (Tipo de regla) y luego seleccione Next (Siguiente).
7. En la página Crear un patrón de eventos, en Origen del evento, selecciona AWSeventos o eventos EventBridge asociados.
8. En Event pattern (Patrón de eventos), mantenga el valor predeterminado de Servicios de AWS.
9. En Servicio de AWS, elija Support (Soporte).
10. Para Event type (Tipo de evento), elija Support Case Update (Actualización de casos de soporte).
11. Seleccione Siguiente.
12. En la sección Select targets (Seleccionar objetivos), elija el destino que haya creado para esta regla y, a continuación, configure las opciones adicionales necesarias para dicho tipo. Por ejemplo, si elige Amazon SNS, asegúrese de que el tema de SNS esté configurado correctamente para que se le notifique por correo electrónico o SMS.
13. Seleccione Siguiente.
14. (Opcional) En la página Add tags (Agregar etiquetas) agregue etiquetas a su clave y, a continuación, elija Next (Siguiente).
15. En la página Review and create (Revisar y crear), revise la configuración de las reglas para asegurarse de que se ajustan a los requisitos de supervisión de eventos.
16. Elija Crear regla. Su regla se controlará ahora para eventos de casos AWS Support y, a continuación, envíelos al destino que especificó.

Notas

- Cuando reciba un evento, puede utilizar el parámetro `origin` para determinar si usted o un agente AWS Support agregaron una correspondencia de caso a un caso de soporte. El valor de `origin` puede ser `CUSTOMER` o `AWS`.

En la actualidad, solo eventos para la acción `AddCommunicationToCase` tendrán este valor.

- Para obtener más información sobre la creación de patrones de eventos, consulta Patrones de eventos en la Guía del EventBridge usuario de Amazon.
- También puede crear otra regla para la AWS API Call (Llamada a la API) mediante el tipo de evento CloudTrail. Esta regla supervisará los registros de AWS CloudTrail para Llamadas a la API AWS Support en su cuenta.

Eventos AWS Support de ejemplo

Los siguientes eventos se crean cuando se producen acciones de soporte en su cuenta.

Example : Crear un caso de soporte

El siguiente evento se crea cuando se crea un caso de soporte.

```
{
    "version": "0",
    "id": "3433df007-9285-55a3-f6d1-536944be45d7",
    "detail-type": "Support Case Update",
    "source": "aws.support",
    "account": "111122223333",
    "time": "2022-02-21T15:51:19Z",
    "region": "us-east-1",
    "resources": [],
    "detail": {
        "case-id": "case-111122223333-muen-2022-7118885805350839",
        "display-id": "1234563851",
        "communication-id": "",
        "event-name": "CreateCase",
        "origin": ""
    }
}
```

Example : caso de soporte de actualización

El siguiente evento se crea cuando AWS Support responde a un caso de soporte.

```
{
```

```
    "version": "0",
    "id": "f90cb8cb-32be-1c91-c0ba-d50b4ca5e51b",
    "detail-type": "Support Case Update",
    "source": "aws.support",
    "account": "111122223333",
    "time": "2022-02-21T15:51:31Z",
    "region": "us-east-1",
    "resources": [],
    "detail": {
        "case-id": "case-111122223333-muen-2022-7118885805350839",
        "display-id": "1234563851",
        "communication-id": "ekko:us-east-1:12345678-268a-424b-be08-54613cab84d2",
        "event-name": "AddCommunicationToCase",
        "origin": "AWS"
    }
}
```


Example : resolver un caso de soporte

El siguiente evento se crea cuando se resuelve un caso de soporte.


```
{
    "version": "0",
    "id": "1aa4458d-556f-732e-ddc1-4a5b2fbd14a5",
    "detail-type": "Support Case Update",
    "source": "aws.support",
    "account": "111122223333",
    "time": "2022-02-21T15:51:31Z",
    "region": "us-east-1",
    "resources": [],
    "detail": {
        "case-id": "case-111122223333-muen-2022-7118885805350839",
        "display-id": "1234563851",
        "communication-id": "",
        "event-name": "ResolveCase",
        "origin": ""
    }
}
```


Example : volver a abrir un caso de soporte

El siguiente evento se crea cuando se vuelve a abrir un caso de soporte.

```
{
    "version": "0",
    "id": "3bb9d8fe-6089-ad27-9508-804209b233ad",
    "detail-type": "Support Case Update",
    "source": "aws.support",
    "account": "111122223333",
    "time": "2022-02-21T15:47:19Z",
    "region": "us-east-1",
    "resources": [],
    "detail": {
        "case-id": "case-111122223333-muen-2021-27f40618fe0303ea",
        "display-id": "1234563851",
        "communication-id": "",
        "event-name": "ReopenCase",
        "origin": ""
    }
}
```

Véase también

Para obtener más información sobre cómo utilizarlos EventBridge conAWS Support, consulta los siguientes recursos:

- Cómo automatizar la AWS Support API con Amazon EventBridge
- AWS Supportnotificador de actividad de casos en GitHub

Registrar llamadas a la API de AWS Support con AWS CloudTrail

AWS Support 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 Support. CloudTrail captura las llamadas a la API de AWS Support como eventos. Las llamadas capturadas incluyen las llamadas desde la consola de AWS Support y las llamadas desde el código a las operaciones de la API de AWS Support.

Si crea un registro de seguimiento, puede habilitar la entrega continua de eventos de CloudTrail a un bucket de Amazon Simple Storage Service (Amazon S3), incluidos los eventos para AWS Support. 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 Support, la dirección IP desde la que se realizó, quién la realizó y cuándo, etc.

Para obtener más información acerca de CloudTrail, incluso cómo configurarlo y habilitarlo, consulte la Guía del usuario de AWS CloudTrail.

Información de AWS Support en CloudTrail

CloudTrail se habilita en su cuenta de AWS cuando la crea. Cuando se produce una actividad de eventos compatible en AWS Support, la actividad se registra en un evento de CloudTrail junto con otros eventos de servicios de AWS en Event history (Historial de eventos). Puede ver, buscar y descargar los últimos eventos de la cuenta de AWS. Para obtener más información, consulte Visualización de 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 Support, cree un registro de seguimiento. Un registro de seguimiento permite a CloudTrail enviar archivos de registro a un bucket de Amazon S3. De manera predeterminada, cuando se crea un registro de seguimiento en la consola, el registro de seguimiento se aplica a todas las regiones de AWS. El registro de seguimiento registra los eventos de todas las regiones de la partición de AWS y envía los archivos de registro al bucket de Amazon S3 especificado. También es posible configurar otros servicios de AWS para analizar en profundidad y actuar en función de los datos de eventos recopilados en los registros de CloudTrail. Para 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 operaciones de API de AWS Support y se documentan en la Referencia de la API de AWS Support.

Por ejemplo, las llamadas a las operaciones `CreateCase`, `DescribeCases` y `ResolveCase` generan entradas en los archivos de registro de CloudTrail.

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

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

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

También puede agregar archivos de registro de AWS Support desde varias regiones de AWS y varias cuentas de AWS en un solo bucket de Amazon S3.

Información de AWS Trusted Advisor en el registro de CloudTrail

Trusted Advisor es un servicio de AWS Support que puede utilizar para verificar la cuenta de AWS para buscar formas de ahorrar costos, mejorar la seguridad y optimizar la cuenta.

CloudTrail registra todas las operaciones de API de Trusted Advisor y se documentan en la Referencia de la API de AWS Support.

Por ejemplo, las llamadas a las operaciones `DescribeTrustedAdvisorCheckRefreshStatuses`, `DescribeTrustedAdvisorCheckResult` y `RefreshTrustedAdvisorCheck` generan entradas en los archivos de registro de CloudTrail.

> **Note**
>
> CloudTrail también registra las acciones de la consola de Trusted Advisor. Consulte Registrar las acciones de la AWS Trusted Advisor consola con AWS CloudTrail.

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

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 única solicitud desde cualquier origen. Incluye información acerca de la operación solicitada, la fecha y la hora de la operación, 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.

Example : entrada de registro para CreateCase

En el siguiente ejemplo, se muestra una entrada del registro de CloudTrail para la operación CreateCase.


```
{
   "Records": [
      {
         "eventVersion": "1.04",
         "userIdentity": {
            "type": "IAMUser",
            "principalId": "AIDACKCEVSQ6C2EXAMPLE",
            "arn": "arn:aws:iam::111122223333:user/janedoe",
            "accountId": "111122223333",
            "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
            "userName": "janedoe",
            "sessionContext": {
               "attributes": {
                  "mfaAuthenticated": "false",
                  "creationDate": "2016-04-13T17:51:37Z"
               }
            },
            "invokedBy": "signin.amazonaws.com"
         },
         "eventTime": "2016-04-13T18:05:53Z",
         "eventSource": "support.amazonaws.com",
         "eventName": "CreateCase",
         "awsRegion": "us-east-1",
         "sourceIPAddress": "198.51.100.15",
         "userAgent": "signin.amazonaws.com",
         "requestParameters": {
            "severityCode": "low",
            "categoryCode": "other",
            "language": "en",
            "serviceCode": "support-api",
            "issueType": "technical"
         },
         "responseElements": {
            "caseId": "case-111122223333-muen-2016-c3f2077e504940f2"
         },
         "requestID": "58c257ef-01a2-11e6-be2a-01c031063738",
         "eventID": "5aa34bfc-ad5b-4fb1-8a55-2277c86e746a",
         "eventType": "AwsApiCall",
         "recipientAccountId": "111122223333"
```

```
      }
   ],
   ...
}
```

Example : entrada de registro para RefreshTrustedAdvisorCheck

En el siguiente ejemplo, se muestra una entrada del registro de CloudTrail para la operación RefreshTrustedAdvisorCheck.

```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::111122223333:user/Admin",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "Admin"
    },
    "eventTime": "2020-10-21T16:34:13Z",
    "eventSource": "support.amazonaws.com",
    "eventName": "RefreshTrustedAdvisorCheck",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "72.21.198.67",
    "userAgent": "signin.amazonaws.com",
    "requestParameters": {
        "checkId": "Pfx0RwqBli"
    },
    "responseElements": null,
    "requestID": "4c4d5fc8-c403-4f82-9544-41f820e0fa01",
    "eventID": "2f4630ac-5c27-4f0d-b93f-63742d6fc85e",
    "eventType": "AwsApiCall",
    "recipientAccountId": "111122223333"
}
```

Registro de llamadas a la API de la aplicación AWS Support en Slack mediante AWS CloudTrail

La aplicación AWS Support en Slack está integrada con AWS CloudTrail. CloudTrail proporciona un registro de las acciones que lleva a cabo un usuario, un rol o un Servicio de AWS en la aplicación

AWS Support. Para crear este registro, CloudTrail captura todas las llamadas a la API pública de la aplicación AWS Support como eventos. Estas llamadas capturadas incluyen aquellas desde la consola de la aplicación AWS Support y las llamadas de código a las operaciones de la API pública de la aplicación AWS Support. Si crea un registro de seguimiento, puede habilitar la entrega continua de eventos de CloudTrail a un bucket de Amazon S3. Estos incluyen eventos de la aplicación AWS Support. Si no configura un registro de seguimiento, puede ver los eventos más recientes de la consola de CloudTrail en el Historial de eventos. Puede usar la información que recopila CloudTrail para determinar la solicitud que se hizo a la aplicación AWS Support. También puede identificar la dirección IP desde la que se hizo la llamada, quién hizo dicha solicitud, cuándo se hizo y detalles adicionales.

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

Información de la aplicación AWS Support en CloudTrail

Cuando crea su Cuenta de AWS, se activa CloudTrail en la cuenta. Cuando se produce una actividad de API pública en la aplicación AWS Support, dicha actividad se registra en un evento de CloudTrail junto con otros eventos de servicios de AWS en Event history (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 los eventos de su Cuenta de AWS, incluidos los eventos de AWS Support, cree un registro de seguimiento. 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 los datos del evento recopilados en los registros de CloudTrail y tomar medidas en función de los datos. Para obtener más información, consulte lo siguiente:

- 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 públicas de la aplicación AWS Support. Estas acciones también se documentan en la referencia de la API de la aplicación AWS Support en Slack. Por ejemplo, las llamadas a las acciones `CreateSlackChannelConfiguration`, `GetAccountAlias` y `UpdateSlackChannelConfiguration` generan entradas en los archivos de registros 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 credenciales de usuario AWS Identity and Access Management (IAM) o credenciales de usuario raíz.
- Si la solicitud se realizó con credenciales de seguridad temporales de un rol o fue un usuario federado.
- Si la solicitud la realizó otro Servicio de AWS.

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

Descripción de las entradas de archivos de registro de la aplicación AWS Support

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 son un seguimiento ordenado de las pilas de llamadas a la API pública. Esto significa que los registros no aparecen en ningún orden específico.

Example : ejemplo de registro de **`CreateSlackChannelConfiguration`**

En el siguiente ejemplo, se muestra una entrada de registro de CloudTrail de la operación CreateSlackChannelConfiguration.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE:JaneDoe",
        "arn": "arn:aws:sts::111122223333:assumed-role/Administrator/JaneDoe",
```

```
        "accountId": "111122223333",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AIDACKCEVSQ6C2EXAMPLE",
                "arn": "arn:aws:iam::111122223333:role/Administrator",
                "accountId": "111122223333",
                "userName": "Administrator"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2022-02-26T01:37:57Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2022-02-26T01:48:20Z",
    "eventSource": "supportapp.amazonaws.com",
    "eventName": "CreateSlackChannelConfiguration",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "205.251.233.183",
    "userAgent": "aws-cli/1.3.23 Python/2.7.6 Linux/2.6.18-164.el5",
    "requestParameters": {
        "notifyOnCreateOrReopenCase": true,
        "teamId": "T012ABCDEFG",
        "notifyOnAddCorrespondenceToCase": true,
        "notifyOnCaseSeverity": "all",
        "channelName": "troubleshooting-channel",
        "notifyOnResolveCase": true,
        "channelId": "C01234A5BCD",
        "channelRoleArn": "arn:aws:iam::111122223333:role/AWSSupportAppRole"
    },
    "responseElements": null,
    "requestID": "d06df6ca-c233-4ffb-bbff-63470c5dc255",
    "eventID": "0898ce29-a396-444a-899d-b068f390c361",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```

Example : ejemplo de registro de **`ListSlackChannelConfigurations`**

En el siguiente ejemplo, se muestra una entrada de registro de CloudTrail de la operación ListSlackChannelConfigurations.


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE:AWSSupportAppRole",
        "arn": "arn:aws:sts::111122223333:assumed-role/AWSSupportAppRole",
        "accountId": "111122223333",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AIDACKCEVSQ6C2EXAMPLE",
                "arn": "arn:aws:iam::111122223333:role/AWSSupportAppRole",
                "accountId": "111122223333",
                "userName": "AWSSupportAppRole"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2022-03-01T20:06:32Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2022-03-01T20:06:46Z",
    "eventSource": "supportapp.amazonaws.com",
    "eventName": "ListSlackChannelConfigurations",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "72.21.217.131",
    "userAgent": "aws-cli/1.3.23 Python/2.7.6 Linux/2.6.18-164.el5",
    "requestParameters": null,
    "responseElements": null,
    "requestID": "20f81d63-31c5-4351-bd02-9eda7f76e7b8",
    "eventID": "70acb7fe-3f84-47cd-8c28-cc148ad06d21",
    "readOnly": true,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
```

```
}
```

Example : ejemplo de registro de **`GetAccountAlias`**

En el siguiente ejemplo, se muestra una entrada de registro de CloudTrail de la operación GetAccountAlias.


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE:devdsk",
        "arn": "arn:aws:sts::111122223333:assumed-role/AWSSupportAppRole/devdsk",
        "accountId": "111122223333",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AIDACKCEVSQ6C2EXAMPLE",
                "arn": "arn:aws:iam::111122223333:role/AWSSupportAppRole",
                "accountId": "111122223333",
                "userName": "AWSSupportAppRole"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2022-03-01T20:31:27Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2022-03-01T20:31:47Z",
    "eventSource": "supportapp.amazonaws.com",
    "eventName": "GetAccountAlias",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "72.21.217.142",
    "userAgent": "aws-cli/1.3.23 Python/2.7.6 Linux/2.6.18-164.el5",
    "requestParameters": null,
    "responseElements": null,
    "requestID": "a225966c-0906-408b-b8dd-f246665e6758",
    "eventID": "79ebba8d-3285-4023-831a-64af7de8d4ad",
    "readOnly": true,
    "eventType": "AwsApiCall",
    "managementEvent": true,
```

```
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```

Supervisión y registro de planes de AWS Support

La supervisión es una parte importante del mantenimiento de la fiabilidad, la disponibilidad y el rendimiento de los planes de Support y de otras soluciones de AWS. AWS ofrece las siguientes herramientas de supervisión para vigilar los planes de Support, informar cuando algo no va bien y tomar medidas automáticamente cuando proceda:

- AWS CloudTrail captura llamadas a la API y eventos relacionados efectuados por su cuenta de AWS o en su nombre, y entrega los archivos de registro al bucket de Amazon S3 que se haya especificado. También pueden identificar qué usuarios y cuentas llamaron a AWS, la dirección IP de origen de las llamadas y el momento en que se hicieron. Para obtener más información, consulte la Guía del usuario de AWS CloudTrail.

Temas

Registro de llamadas de la API de planes de AWS Support con AWS CloudTrail

Los planes de AWS Support se integran con AWS CloudTrail, un servicio que proporciona un registro de las acciones que lleva a cabo un usuario, un rol o un Servicio de AWS. CloudTrail captura las llamadas a la API de planes de AWS Support como eventos. Las llamadas capturadas incluyen las llamadas desde la consola de planes de AWS Support y las llamadas desde el código a las operaciones de la API de planes de AWS Support.

Si crea un registro de seguimiento, puede habilitar la entrega continua de eventos de CloudTrail a un bucket de Amazon Simple Storage Service (Amazon S3), incluidos los eventos para los planes de AWS Support. 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 que recopila CloudTrail, puede determinar la solicitud que se hizo a los planes de AWS Support, la dirección IP desde la que se hizo dicha solicitud, quién la hizo y cuándo, además de información adicional.

Para obtener más información acerca de CloudTrail, incluso cómo configurarlo y habilitarlo, consulte la Guía del usuario de AWS CloudTrail.

Información de planes de AWS Support en CloudTrail

CloudTrail se habilita en su Cuenta de AWS cuando la crea. Cuando se produce una actividad de eventos compatible en los planes de AWS Support, la actividad se registra en un evento de CloudTrail junto con otros eventos de Servicio de AWS en Event history (Historial de eventos). Puede ver, buscar y descargar los últimos eventos de la cuenta de . Para obtener más información, consulte Visualización de eventos con el historial de eventos de CloudTrail.

Para mantener un registro continuo de los eventos de su cuenta, incluidos los eventos de los planes de AWS Support, 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 lo siguiente:

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

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

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

También puede agregar archivos de registro de los planes de AWS Support desde varias cuentas y Regiones de AWS en un solo bucket de Amazon S3.

Descripción de las entradas de archivos de registro de los planes de AWS Support

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 única solicitud desde cualquier origen. Incluye información acerca de la operación solicitada, la fecha y la hora de la operación, 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.

Example : entrada de registro de **`GetSupportPlan`**

En el siguiente ejemplo, se muestra una entrada de registro de CloudTrail de la operación `GetSupportPlan`.


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:sts::111122223333:user/janedoe",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AIDACKCEVSQ6C2EXAMPLE",
                "arn": "arn:aws:iam::111122223333:role/Admin",
                "accountId": "111122223333",
                "userName": "Admin"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2022-06-29T16:30:04Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2022-06-29T16:39:11Z",
    "eventSource": "supportplans.amazonaws.com",
    "eventName": "GetSupportPlan",
    "awsRegion": "us-west-2",
```

```
    "sourceIPAddress": "205.251.233.183",
    "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:91.0) Gecko/20100101
 Firefox/91.0",
    "requestParameters": null,
    "responseElements": null,
    "requestID": "7665c39a-d6bf-4d0d-8010-2f59740b8ecb",
    "eventID": "b711bc30-16a5-4579-8f0d-9ada8fe6d1ce",
    "readOnly": true,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```

Example : entrada de registro de **`GetSupportPlanUpdateStatus`**

En el siguiente ejemplo, se muestra una entrada de registro de CloudTrail de la operación `GetSupportPlanUpdateStatus`.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:sts::111122223333:user/janedoe",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AIDACKCEVSQ6C2EXAMPLE",
                "arn": "arn:aws:iam::111122223333:role/Admin",
                "accountId": "111122223333",
                "userName": "Admin"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2022-06-29T16:30:04Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2022-06-29T16:39:02Z",
```

```
    "eventSource": "supportplans.amazonaws.com",
    "eventName": "GetSupportPlanUpdateStatus",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "205.251.233.183",
    "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:91.0) Gecko/20100101
 Firefox/91.0",
    "requestParameters": {
        "supportPlanUpdateArn":
 "arn:aws:supportplans::111122223333:supportplanupdate/7f03b7a233a0e87ebc79e56d4d2bcaf19e976c37
    },
    "responseElements": null,
    "requestID": "75e5c767-8703-4ed3-b01e-4dda28020322",
    "eventID": "28d1c0e3-ccb6-4fd1-8793-65be010114cc",
    "readOnly": true,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```

Example : entrada de registro de **`StartSupportPlanUpdate`**

En el siguiente ejemplo, se muestra una entrada de registro de CloudTrail de la operación `StartSupportPlanUpdate`.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:sts::111122223333:user/janedoe",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AIDACKCEVSQ6C2EXAMPLE",
                "arn": "arn:aws:iam::111122223333:role/Admin",
                "accountId": "111122223333",
                "userName": "Admin"
            },
            "webIdFederationData": {},
            "attributes": {
```

```
                "creationDate": "2022-06-29T16:30:04Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2022-06-29T16:38:55Z",
    "eventSource": "supportplans.amazonaws.com",
    "eventName": "StartSupportPlanUpdate",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "205.251.233.183",
    "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:91.0) Gecko/20100101
 Firefox/91.0",
    "requestParameters": {
        "clientToken": "98add111-dcc9-464d-8722-438d697fe242",
        "update": {
            "supportLevel": "BASIC"
        }
    },
    "responseElements": {
        "Access-Control-Expose-Headers": "x-amzn-RequestId,x-amzn-ErrorType,x-amzn-
ErrorMessage,Date",
        "supportPlanUpdateArn":
 "arn:aws:supportplans::111122223333:supportplanupdate/7f03b7a233a0e87ebc79e56d4d2bcaf19e976c37
    },
    "requestID": "e5ff9382-5fb8-4764-9993-0f33fb0b1e17",
    "eventID": "5dba89f8-2e5b-42b9-9b8f-395580c52962",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```

Example : entrada de registro de **`CreateSupportPlanSchedule`**

En el siguiente ejemplo, se muestra una entrada de registro de CloudTrail de la operación `CreateSupportPlanSchedule`.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
```

```
        "arn": "arn:aws:sts::111122223333:user/janedoe",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AIDACKCEVSQ6C2EXAMPLE",
                "arn": "arn:aws:iam::111122223333:role/Admin",
                "accountId": "111122223333",
                "userName": "Admin"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-05-09T16:30:04Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-05-09T16:30:04Z",
    "eventSource": "supportplans.amazonaws.com",
    "eventName": "CreateSupportPlanSchedule",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "205.251.233.183",
    "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:91.0) Gecko/20100101
 Firefox/91.0",
    "requestParameters": {
        "clientToken": "b998de5e-ad1c-4448-90db-2bf86d6d9e9a",
        "scheduleCreationDetails": {
            "startLevel": "BUSINESS",
            "startOffer": "TrialPlan7FB93B",
            "startTimestamp": "2023-06-03T17:23:56.109Z",
            "endLevel": "BUSINESS",
            "endOffer": "StandardPlan2074BB",
            "endTimestamp": "2023-09-03T17:23:55.109Z"
        }
    },
    "responseElements": {
        "Access-Control-Expose-Headers": "x-amzn-RequestId,x-amzn-ErrorType,x-amzn-
ErrorMessage,Date",
        "supportPlanUpdateArn":
 "arn:aws:supportplans::111122223333:supportplanschedule/
b9a9a4336a3974950a6e670f7dab79b77a4b104db548a0d57050ce4544721d4b"
    },
    "requestID": "150450b8-e61a-4b15-93a8-c3b557a1ca48",
```

```
    "eventID": "a2a1ba44-610d-4dc8-bf16-29f1635b57a9",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```

Registro de cambios en su plan de AWS Support

Important

A partir del 3 de agosto de 2022, las siguientes operaciones serán obsoletas y no aparecerán en los nuevos registros de CloudTrail. Para ver una lista de las operaciones admitidas, consulte Descripción de las entradas de archivos de registro de los planes de AWS Support.

- `DescribeSupportLevelSummary`: esta acción aparece en el registro al abrir la página Planes de soporte.
- `UpdateProbationAutoCancellation`: tras registrarse en Developer Support o en Business Support e intentar cancelar alguno de estos planes en un plazo de 30 días, su plan se cancelará automáticamente al final de dicho periodo. Esta acción aparece en el registro cuando elige Opt-out of automatic cancellation (Anular cancelación automática) en el banner que aparece en la página Planes de soporte. Con esta acción se reanudará su plan Developer Support o Business Support.
- `UpdateSupportLevel`: esta acción aparece en el registro al cambiar el plan de soporte.

Note

El campo `eventSource` tiene el espacio de nombres `support-subscription.amazonaws.com` para estas acciones.

Example : entrada de registro para DescribeSupportLevelSummary

En el ejemplo siguiente se muestra una entrada de registro de CloudTrail para la acción `DescribeSupportLevelSummary`.

```
{
```

```
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "Root",
    "principalId": "111122223333",
    "arn": "arn:aws:iam::111122223333:root",
    "accountId": "111122223333",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {},
      "webIdFederationData": {},
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2021-01-07T22:08:05Z"
      }
    }
  },
  "eventTime": "2021-01-07T22:08:07Z",
  "eventSource": "support-subscription.amazonaws.com",
  "eventName": "DescribeSupportLevelSummary",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "100.127.8.67",
  "userAgent": "AWS-SupportPlansConsole, aws-internal/3",
  "requestParameters": {
    "lang": "en"
  },
  "responseElements": null,
  "requestID": "b423b84d-829b-4090-a239-2b639b123abc",
  "eventID": "e1eeda0e-d77c-487b-a7e5-4014f7123abc",
  "readOnly": true,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "eventCategory": "Management",
  "recipientAccountId": "111122223333"
}
```


Example : entrada de registro para UpdateProbationAutoCancelation

En el ejemplo siguiente se muestra una entrada de registro de CloudTrail para la acción `UpdateProbationAutoCancellation`.


```
{
  "eventVersion": "1.08",
  "userIdentity": {
```

```
    "type": "Root",
    "principalId": "111122223333",
    "arn": "arn:aws:iam::111122223333:root",
    "accountId": "111122223333",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE"
  },
  "eventTime": "2021-01-07T23:28:43Z",
  "eventSource": "support-subscription.amazonaws.com",
  "eventName": "UpdateProbationAutoCancellation",
  "awsRegion": "us-east-1", "sourceIPAddress": "100.127.8.67",
  "userAgent": "AWS-SupportPlansConsole, aws-internal/3",
  "requestParameters": {
    "lang": "en"
  },
  "responseElements": null,
  "requestID": "5492206a-e200-4c33-9fcf-4162d4123abc",
  "eventID": "f4a58c09-0bb0-4ba2-a8d3-df6909123abc",
  "readOnly": false,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "eventCategory": "Management",
  "recipientAccountId": "111122223333"
}
```

Example : entrada de registro para UpdateUpportLevel

En el siguiente ejemplo, se muestra una entrada de registro de CloudTrail de la acción `UpdateSupportLevel` para cambiar al plan Developer Support.

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "Root",
    "principalId": "111122223333",
    "arn": "arn:aws:iam::111122223333:root",
    "accountId": "111122223333",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {},
      "webIdFederationData": {},
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2021-01-07T22:08:05Z"
```

```
      }
    }
  },
  "eventTime": "2021-01-07T22:08:43Z",
  "eventSource": "support-subscription.amazonaws.com",
  "eventName": "UpdateSupportLevel",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "100.127.8.247",
  "userAgent": "AWS-SupportPlansConsole, aws-internal/3",
  "requestParameters": {
    "supportLevel": "new_developer"
  },
  "responseElements": {
    "aispl": false,
    "supportLevel": "new_developer"
  },
  "requestID": "5df3da3a-61cd-4a3c-8f41-e5276b123abc",
  "eventID": "c69fb149-c206-47ce-8766-8df6ec123abc",
  "readOnly": false,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "eventCategory": "Management",
  "recipientAccountId": "111122223333"
}
```

Supervisar y registrar para AWS Trusted Advisor

La supervisión es una parte importante del mantenimiento de la fiabilidad, la disponibilidad y el rendimiento de Trusted Advisor y de sus otras soluciones de AWS. AWS ofrece las siguientes herramientas de supervisión para vigilar Trusted Advisor, informar cuando algo no va bien y tomar medidas automáticamente cuando proceda:

- Amazon EventBridge proporciona una transmisión de una secuencia de eventos de sistema casi en tiempo real que describen cambios en los recursos de AWS. EventBridge habilita la informática basada en eventos automatizada, para que pueda escribir reglas que vigilan determinados eventos y desencadenan acciones automatizadas en otros servicios de AWS cuando estos eventos se producen.

  Por ejemplo, Trusted Advisor proporciona la verificación de Permisos de bucket de Amazon S3. Esta comprobación identifica si tiene buckets que tienen permisos de acceso abierto o permiten el acceso a cualquier usuario de AWS autenticado. Si cambia un permiso de bucket, el estado cambia para la verificación de Trusted Advisor. EventBridge detecta este evento y, a continuación, le envía una notificación para que pueda tomar medidas. Para obtener más información, consulte la Guía del usuario de Amazon EventBridge.
- Las verificaciones de AWS Trusted Advisor identifican formas de reducir los costos, aumentar el rendimiento y mejorar la seguridad de su cuenta de AWS. Puede utilizar EventBridge para supervisar el estado de las verificaciones de Trusted Advisor. A continuación, puede utilizar Amazon CloudWatch para crear alarmas a partir de métricas de Trusted Advisor. Estas alarmas le notifican cuando cambia el estado de una comprobación de Trusted Advisor, como un recurso actualizado o una cuota de servicio alcanzada.
- AWS CloudTrail captura llamadas a la API y eventos relacionados efectuados por su cuenta de AWS o en su nombre, y entrega los archivos de registro al bucket de Amazon S3 que se haya especificado. También pueden identificar qué usuarios y cuentas llamaron a AWS, la dirección IP de origen de las llamadas y el momento en que se hicieron. Para obtener más información, consulte la Guía del usuario de AWS CloudTrail.

Temas

- Registrar las acciones de la AWS Trusted Advisor consola con AWS CloudTrail

Supervisión de los resultados de los AWS Trusted Advisor controles con Amazon EventBridge

Puede utilizarla EventBridge para detectar cuándo sus comprobaciones Trusted Advisor cambian de estado. A continuación, en función de las reglas que cree, EventBridge invoca una o más acciones de destino cuando el estado cambia a un valor que especifique en una regla.

En función del tipo de cambio de estado, puede enviar notificaciones, capturar información de estado, tomar medidas correctivas, iniciar eventos o adoptar otras medidas. Por ejemplo: puede especificar los siguientes tipos de destino si una verificación cambia de estado de ningún problema detectado (verde) a acción recomendada (rojo).

- Utilice una función de AWS Lambda para pasar una notificación a un canal de Slack.
- Envíe datos acerca de la verificación a un Amazon Kinesis stream para permitir una supervisión completa y en tiempo real del estado.
- Envía un tema de Amazon Simple Notification Service a su correo electrónico.
- Recibe una notificación con una acción de CloudWatch alarma de Amazon.

Para obtener más información sobre cómo utilizar EventBridge las funciones Lambda para automatizar las respuestasTrusted Advisor, consulte las Trusted Advisorherramientas en. GitHub

Notas

- Trusted Advisor entrega eventos de la mejor forma posible. No siempre se garantiza que los eventos se entreguen a EventBridge.
- Para crear una regla para las comprobaciones de Trusted Advisor, debe contar con un plan AWS Support Business, Enterprise On-Ramp o Enterprise. Para más información, consulte ¿Cambiar AWS Support los planes.
- Como Trusted Advisor es un servicio global, todos los eventos se emiten EventBridge en la región EE.UU. Este (Norte de Virginia).

Siga este procedimiento para crear una EventBridge regla paraTrusted Advisor. Antes de crear reglas de eventos, haga lo siguiente:

- Familiarícese con los eventos, las reglas y los objetivos de EventBridge. Para obtener más información, consulta ¿Qué es Amazon EventBridge? en la Guía del EventBridge usuario de Amazon.
- Cree el destino que utilizará en su regla de evento.

Para crear una EventBridge regla para Trusted Advisor

1. Abre la EventBridge consola de Amazon en https://console.aws.amazon.com/events/.
2. Para cambiar la región, utilice el Region selector (Selector de regiones) ubicado en la esquina superior derecha de la página y elija Este de EE. UU. (Norte de Virginia).
3. En el panel de navegación, seleccione Reglas.
4. Elija Create rule (Crear regla).
5. En la página Crear detalles de la regla, ingrese un nombre y una descripción para su regla.
6. Mantenga los valores predeterminados para Event bus (Bus de eventos) y Rules type (Tipo de regla) y luego seleccione Next (Siguiente).
7. En la página Crear un patrón de eventos, en Origen del evento, selecciona AWSeventos o eventos EventBridge asociados.
8. En Event pattern (Patrón de eventos), mantenga el valor predeterminado de Servicios de AWS.
9. En Servicio de AWS, elija Trusted Advisor.
10. ParaEvent type (Tipo de evento), elija Check Item Refresh Status (Verificar estado de actualización de elementos).
11. Elija una de las siguientes opciones para los verificar los estados:
    - Elija Cualquier estado para crear una regla que supervise cualquier cambio de estado.
    - Elija Estado(s) específico(s) y, a continuación, elija los valores que desea que supervise su regla.
        - ERROR: Trusted Advisor recomienda una acción para la verificación.
        - INFO: Trusted Advisor no puede determinar el estado de la verificación.
        - OK: Trusted Advisor no detecta ningún problema para la verificación.
        - WARN: Trusted Advisor detecta un posible problema para la verificación y recomienda la investigación.

12. Elija una de las siguientes opciones para sus verificaciones:
    - Elija Cualquier verificación.
    - Elija Verificaciones específicas y, a continuación, elija uno o más nombres de verificación de la lista.
13. Elija una de las siguientes opciones para los recursos de AWS:
    - Elija Cualquier ID de recurso para crear una regla que supervise todos los recursos.
    - Elija ID de recursos específicos por ARN y, a continuación, ingrese los nombres de recurso de Amazon (ARN) que desee.
14. Seleccione Siguiente.
15. En la página Select target(s) (Seleccionar destinos), elija el tipo de destino que haya preparado para usarlo con esta regla y luego configure las opciones adicionales que requiera dicho tipo. Por ejemplo: puede enviar el evento a una cola de Amazon SQS o a un tema de Amazon SNS.
16. Seleccione Siguiente.
17. (Opcional) En la página Add tags (Agregar etiquetas) agregue etiquetas a su clave y, a continuación, elija Next (Siguiente).
18. En la página Review and create (Revisar y crear), revise la configuración de las reglas para asegurarse de que se ajustan a los requisitos de supervisión de eventos.
19. Elija Crear regla. Su regla supervisará ahora la verificación de Trusted Advisor y, a continuación, enviará el evento al destino que especificó.

Creación de alarmas de Amazon CloudWatch para supervisar las métricas de AWS Trusted Advisor

Cuando AWS Trusted Advisor actualiza sus cheques, Trusted Advisor publica métricas sobre los resultados de las verificaciones en CloudWatch. Puede ver las métricas en CloudWatch. También puede crear alarmas para detectar cambios de estado en verificaciones de Trusted Advisor y cambios de estado de los recursos, y el uso de cuotas de servicio (anteriormente denominadas límites). Por ejemplo, puede crear una alarma para llevar a cabo un seguimiento de los cambios de estado de las verificaciones de la categoría Service Limits. La alarma le notificará cuando alcance o supere una cuota de servicio para su cuenta de AWS.

Siga este procedimiento para crear una alarma de CloudWatch para una métrica específica de Trusted Advisor.

Temas

Requisitos previos

Antes de crear alarmas de CloudWatch para las métricas de Trusted Advisor, revise la siguiente información:

- Comprenda cómo CloudWatch utiliza métricas y alarmas. Para obtener más información, consulte Cómo funciona CloudWatch en la Guía del usuario de Amazon CloudWatch.
- Use la consola de Trusted Advisor o la API de AWS Support para actualizar sus verificaciones y obtener los resultados de las verificaciones más recientes. Para obtener más información, consulte Actualizar resultados de verificaciones.

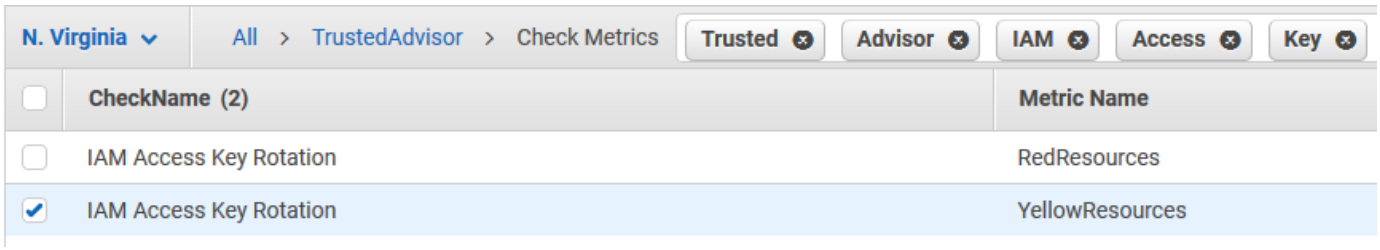
Si desea crear una alarma de CloudWatch para una métrica de Trusted Advisor

1. Abra la consola de CloudWatch en https://console.aws.amazon.com/cloudwatch/.
2. Use el Selector de región y elija la región EE. UU. Este (Norte de Virginia) de AWS.
3. En el panel de navegación, elija Alarms.
4. Elija Create alarm (Crear alarma).
5. Elija Select Metric (Seleccionar métrica).
6. Para Métricas, ingrese uno o varios valores de dimensión para filtrar la lista de métricas. Por ejemplo, puede ingresar el nombre de la métrica ServiceLimitUsage o la dimensión, como el nombre de verificación de Trusted Advisor.

   > **Tip**
   >
   > - Puede buscar **`Trusted Advisor`** para enumerar todas las métricas del servicio.
   > - Para ver una lista de las métricas y nombres de dimensiones disponibles, consulte Métricas y dimensiones de Trusted Advisor.

7. En la tabla de resultados, active la casilla de la fila que contiene la métrica.

En el siguiente ejemplo, el nombre de la verificación es Rotación de clave de acceso de IAM y el nombre de la métrica es YellowResources.

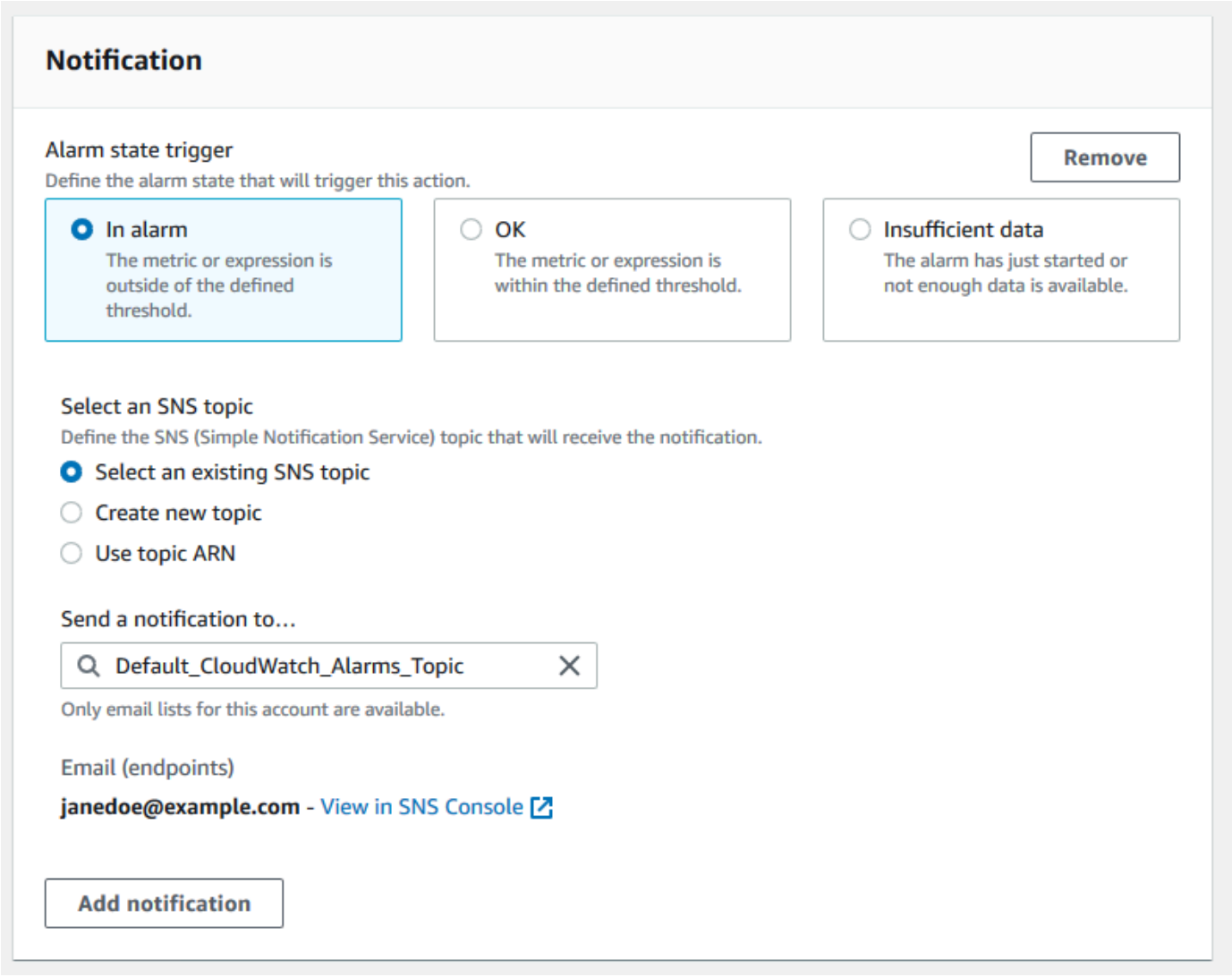


8. Elija Select Metric (Seleccionar métrica).
9. En la página Especificar métrica y condiciones, verifique que el nombre de métrica y el CheckName que eligió aparezcan en la página.
10. Para Period (Periodo), puede especificar el tiempo que desea que se inicie la alarma cuando cambie el estado de la verificación, como 5 minutos.
11. En Condiciones, elija Estático y, a continuación, especifique la condición de alarma de cuándo debe iniciarse la alarma.

    Por ejemplo, si elige Greater/Equal >=threshold (Mayor o igual que umbral) e ingresa **1** para el valor de umbral, esto significa que la alarma se iniciará cuando Trusted Advisor detecte al menos una clave de acceso de IAM que no se ha rotado en los últimos 90 días.

    > **Notas**
    >
    > - En las métricas GreenChecks, RedChecks, YellowChecks, RedResources y YellowResources, puede especificar un umbral que sea un número entero mayor o igual a cero.
    > - Trusted Advisor no envía métricas para GreenResources, que son recursos para los que Trusted Advisor no ha detectado ningún problema.

12. Elija Next (Siguiente).
13. En la página Configure actions (Configuración de acciones), para Alarm state trigger (Desencadenador de estado de alarma), elija In alarm (En alarma).
14. Para Select an SNS topic (Seleccione un tema de SNS), elija un tema existente de Amazon Simple Notification Service (Amazon SNS) o cree uno.



15. Elija Next (Siguiente).
16. En Name and description (Nombre y descripción), ingrese un nombre y una descripción para la alarma.
17. Elija Next (Siguiente).
18. En la página Preview and create (Vista previa y crear), revise los detalles de la alarma y, a continuación, elija Create alarm (Crear alarma).

    Cuando el estado de la verificación Rotación de clave de acceso de IAM cambie a rojo durante 5 minutos, la alarma enviará una notificación a su tema de SNS.

Example : notificación por correo electrónico para una alarma de CloudWatch

El siguiente mensaje de correo electrónico muestra que una alarma detectó un cambio en la verificación de Rotación de clave de acceso de IAM.

```
You are receiving this email because your Amazon CloudWatch Alarm
 "IAMAcessKeyRotationCheckAlarm" in the US East (N. Virginia) region has entered the
 ALARM state,
because "Threshold Crossed: 1 out of the last 1 datapoints [9.0 (26/03/21 22:44:00)]
 was greater than or equal to the threshold (1.0) (minimum 1 datapoint for OK -> ALARM
 transition)." at "Friday 26 March, 2021 22:49:42 UTC".

View this alarm in the AWS Management Console:
https://us-east-1.console.aws.amazon.com/cloudwatch/home?region=us-
east-1#s=Alarms&alarm=IAMAcessKeyRotationCheckAlarm

Alarm Details:
- Name:                       IAMAcessKeyRotationCheckAlarm
- Description:                This alarm starts when one or more AWS access keys in my
 AWS account have not been rotated in the last 90 days.
- State Change:               INSUFFICIENT_DATA -> ALARM
- Reason for State Change:    Threshold Crossed: 1 out of the last 1 datapoints [9.0
 (26/03/21 22:44:00)] was greater than or equal to the threshold (1.0) (minimum 1
 datapoint for OK -> ALARM transition).
- Timestamp:                  Friday 26 March, 2021 22:49:42 UTC
- AWS Account:                123456789012
- Alarm Arn:                  arn:aws:cloudwatch:us-
east-1:123456789012:alarm:IAMAcessKeyRotationCheckAlarm

Threshold:
- The alarm is in the ALARM state when the metric is GreaterThanOrEqualToThreshold 1.0
 for 300 seconds.

Monitored Metric:
- MetricNamespace:                    AWS/TrustedAdvisor
- MetricName:                         RedResources
- Dimensions:                         [CheckName = IAM Access Key Rotation]
- Period:                             300 seconds
- Statistic:                          Average
- Unit:                               not specified
- TreatMissingData:                   missing


State Change Actions:
```

```
- OK:
- ALARM: [arn:aws:sns:us-east-1:123456789012:Default_CloudWatch_Alarms_Topic]
- INSUFFICIENT_DATA:
```

Métricas de CloudWatch para Trusted Advisor

Puede usar la consola de CloudWatch o la AWS Command Line Interface (AWS CLI) para encontrar las métricas disponibles para Trusted Advisor.

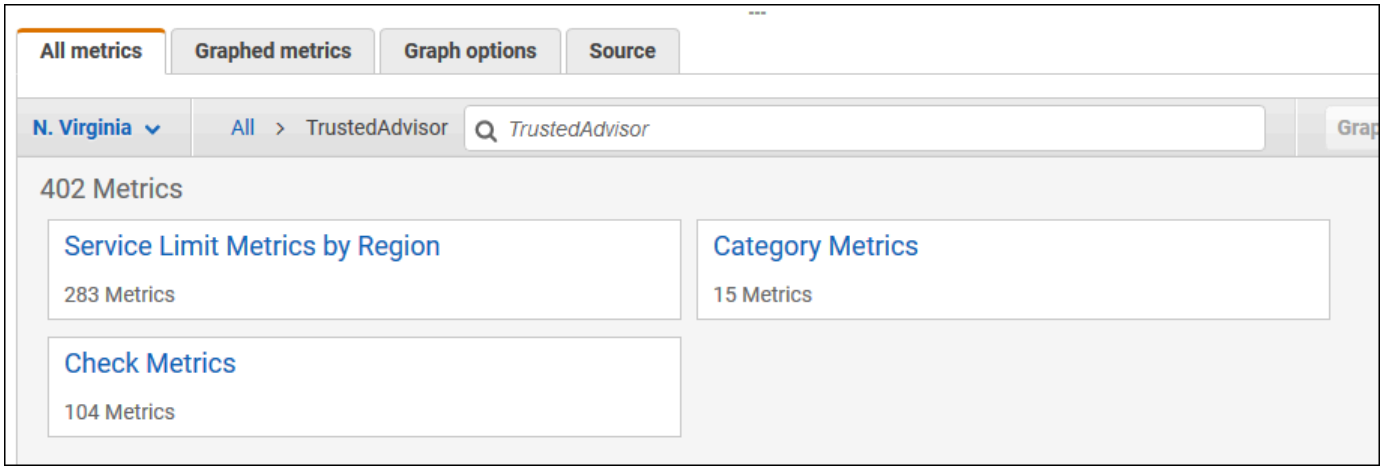
Para obtener una lista de los espacios de nombres, métricas y dimensiones de todos los servicios que publican métricas, consulte Servicios de AWS que publican métricas de CloudWatch en la Guía del usuario de Amazon CloudWatch.

Ver métricas de Trusted Advisor (consola)

Puede iniciar sesión en la consola de CloudWatch y ver las métricas disponibles para Trusted Advisor.

Para ver las métricas de Trusted Advisor disponibles (consola)

1. Abra la consola de CloudWatch en https://console.aws.amazon.com/cloudwatch/.
2. Utilice el Selector de región y elija la región EE. UU. Este (Norte de Virginia) de AWS.
3. En el panel de navegación, seleccione Metrics (Métricas).
4. Ingrese un espacio de nombres de métrica, como **`TrustedAdvisor`**.
5. Elija una dimensión de métrica, como Métricas de verificación.



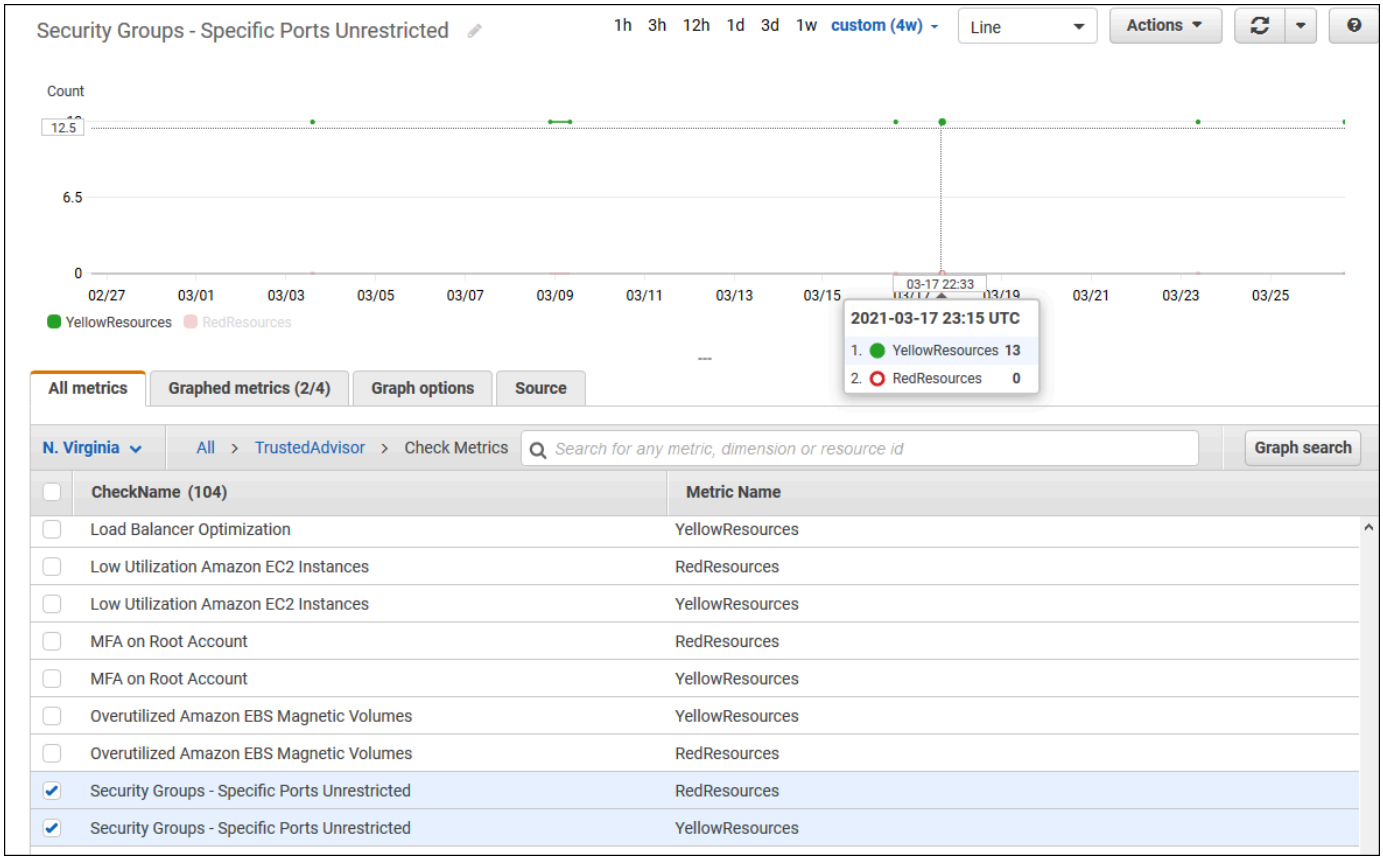
6. La pestaña All metrics (Todas las métricas) muestra las métricas para dicha dimensión en el espacio de nombres. Puede hacer lo siguiente:

a. Para ordenar la tabla, elija el encabezado de columna.

b. Para representar gráficamente una métrica, active la casilla de verificación situada junto a ella. Para seleccionar todas las métricas, seleccione la casilla de verificación en la fila de encabezado de la tabla.

c. Para filtrar por métrica, elija el nombre de la métrica y, a continuación, elija Add to search (Añadir a la búsqueda).

En el siguiente ejemplo, se muestran los resultados de la verificación Grupos de seguridad: puertos específicos sin restricciones. La verificación identifica 13 recursos que están en amarillo. Trusted Advisor recomienda investigar las verificaciones en amarillo.



7. (Opcional) Para agregar este gráfico a un panel de CloudWatch, elija Actions (Acciones) y, a continuación, Add to dashboard (Agregar al panel).

Para obtener más información sobre cómo crear un gráfico para ver sus métricas, consulte Representar una métrica gráficamente en la Guía del usuario de Amazon CloudWatch.

Ver las métricas de Trusted Advisor (CLI)

Puede utilizar el comando list-metrics de AWS CLI para ver las métricas disponibles para Trusted Advisor.

Example : muestra todas las métricas de Trusted Advisor

En el siguiente ejemplo se especifica el espacio de nombres `AWS/TrustedAdvisor` para ver todas las métricas para Trusted Advisor.

```
aws cloudwatch list-metrics --namespace AWS/TrustedAdvisor
```

El resultado puede tener el siguiente aspecto.

```
{
    "Metrics": [
        {
            "Namespace": "AWS/TrustedAdvisor",
            "Dimensions": [
                {
                    "Name": "ServiceName",
                    "Value": "EBS"
                },
                {
                    "Name": "ServiceLimit",
                    "Value": "Magnetic (standard) volume storage (TiB)"
                },
                {
                    "Name": "Region",
                    "Value": "ap-northeast-2"
                }
            ],
            "MetricName": "ServiceLimitUsage"
        },
        {
            "Namespace": "AWS/TrustedAdvisor",
            "Dimensions": [
                {
                    "Name": "CheckName",
                    "Value": "Overutilized Amazon EBS Magnetic Volumes"
                }
            ],
            "MetricName": "YellowResources"
```

```
        },
        {
            "Namespace": "AWS/TrustedAdvisor",
            "Dimensions": [
                {
                    "Name": "ServiceName",
                    "Value": "EBS"
                },
                {
                    "Name": "ServiceLimit",
                    "Value": "Provisioned IOPS"
                },
                {
                    "Name": "Region",
                    "Value": "eu-west-1"
                }
            ],
            "MetricName": "ServiceLimitUsage"
        },
        {
            "Namespace": "AWS/TrustedAdvisor",
            "Dimensions": [
                {
                    "Name": "ServiceName",
                    "Value": "EBS"
                },
                {
                    "Name": "ServiceLimit",
                    "Value": "Provisioned IOPS"
                },
                {
                    "Name": "Region",
                    "Value": "ap-south-1"
                }
            ],
            "MetricName": "ServiceLimitUsage"
        },
    ...
  ]
}
```

Example : muestra todas las métricas de una dimensión

El siguiente ejemplo especifica el espacio de nombres `AWS/TrustedAdvisor` y la dimensión `Region` para ver las métricas disponibles para una región de AWS especificada.

```
aws cloudwatch list-metrics --namespace AWS/TrustedAdvisor --dimensions
 Name=Region,Value=us-east-1
```

El resultado puede tener el siguiente aspecto.

```
{
    "Metrics": [
        {
            "Namespace": "AWS/TrustedAdvisor",
            "Dimensions": [
                {
                    "Name": "ServiceName",
                    "Value": "SES"
                },
                {
                    "Name": "ServiceLimit",
                    "Value": "Daily sending quota"
                },
                {
                    "Name": "Region",
                    "Value": "us-east-1"
                }
            ],
            "MetricName": "ServiceLimitUsage"
        },
        {
            "Namespace": "AWS/TrustedAdvisor",
            "Dimensions": [
                {
                    "Name": "ServiceName",
                    "Value": "AutoScaling"
                },
                {
                    "Name": "ServiceLimit",
                    "Value": "Launch configurations"
                },
                {
                    "Name": "Region",
```

```
                    "Value": "us-east-1"
                }
            ],
            "MetricName": "ServiceLimitUsage"
        },
        {
            "Namespace": "AWS/TrustedAdvisor",
            "Dimensions": [
                {
                    "Name": "ServiceName",
                    "Value": "CloudFormation"
                },
                {
                    "Name": "ServiceLimit",
                    "Value": "Stacks"
                },
                {
                    "Name": "Region",
                    "Value": "us-east-1"
                }
            ],
            "MetricName": "ServiceLimitUsage"
        },
    ...
  ]
}
```

Example : lista de métricas para un nombre de métrica específico

El siguiente ejemplo especifica el espacio de nombres de `AWS/TrustedAdvisor` y un nombre de métrica de `RedResources` para ver los resultados únicamente de la métrica especificada.

```
aws cloudwatch list-metrics --namespace AWS/TrustedAdvisor --metric-name RedResources
```

El resultado puede tener el siguiente aspecto.

```
{
    "Metrics": [
        {
            "Namespace": "AWS/TrustedAdvisor",
            "Dimensions": [
                {
                    "Name": "CheckName",
```

```
                    "Value": "Amazon RDS Security Group Access Risk"
                }
            ],
            "MetricName": "RedResources"
        },
        {
            "Namespace": "AWS/TrustedAdvisor",
            "Dimensions": [
                {
                    "Name": "CheckName",
                    "Value": "Exposed Access Keys"
                }
            ],
            "MetricName": "RedResources"
        },
        {
            "Namespace": "AWS/TrustedAdvisor",
            "Dimensions": [
                {
                    "Name": "CheckName",
                    "Value": "Large Number of Rules in an EC2 Security Group"
                }
            ],
            "MetricName": "RedResources"
        },
        {
            "Namespace": "AWS/TrustedAdvisor",
            "Dimensions": [
                {
                    "Name": "CheckName",
                    "Value": "Auto Scaling Group Health Check"
                }
            ],
            "MetricName": "RedResources"
        },
    ...
  ]
}
```

Métricas y dimensiones de Trusted Advisor

Consulte las siguientes tablas para conocer las métricas y dimensiones de Trusted Advisor que puede utilizar para sus alarmas y gráficos de CloudWatch.

Métricas de nivel de verificación de Trusted Advisor

Puede utilizar las siguientes métricas para verificaciones de Trusted Advisor.

Métrica	Descripción
`RedResources`	El número de recursos que están en un estado rojo (acción recomendada).
`YellowResources`	El número de recursos que están en un estado amarillo (investigación recomendada).

Métricas de nivel de categoría de Trusted Advisor

Puede utilizar las siguientes métricas para categorías de Trusted Advisor.

Métrica	Descripción
`GreenChecks`	El número de verificaciones de Trusted Advisor que están en estado verde (no se han detectado problemas).
`RedChecks`	El número de verificaciones de Trusted Advisor que están en estado rojo (acción recomendada).
`YellowChecks`	El número de verificaciones de Trusted Advisor que están en estado amarillo (investigación recomendada).

Métricas de nivel de cuota de servicio de Trusted Advisor

Puede utilizar las siguientes métricas para cuotas de Servicio de AWS.

Métrica	Descripción
`ServiceLimitUsage`	El porcentaje de uso de recursos frente a una cuota de servicio (anteriormente denominadas límites).

Dimensiones de las métricas de nivel de verificación

Puede utilizar la siguiente dimensión para verificaciones de Trusted Advisor.

Dimensión	Descripción
`CheckName`	El nombre de la verificación de Trusted Advisor. Puede encontrar todos los nombres de verificación en la consola de Trusted Advisor o AWS Trusted Advisor comprobar referencia.

Dimensiones de las métricas de nivel de categoría

Puede utilizar la siguiente dimensión para categorías de verificación de Trusted Advisor.

Dimensión	Descripción
`Category`	El nombre de una categoría de comprobación de Trusted Advisor. Puede encontrar todas las categorías de verificación en la consola de Trusted Advisor o la página Ver categorías de verificación.

Dimensiones de las métricas de cuota de servicio

Puede utilizar las siguientes dimensiones para métricas de cuotas de servicio de Trusted Advisor.

Dimensión	Descripción
`Region`	La Región de AWS para una cuota de servicio.
`ServiceName`	Nombre del elemento Servicio de AWS.
`ServiceLimit`	El nombre de la cuota de servicio. Para más información acerca de las cuotas de servicio, consulte Cuotas de Servicio de AWS en Referencia general de AWS.

Registrar las acciones de la AWS Trusted Advisor consola con AWS CloudTrail

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

Para obtener más información CloudTrail, incluido cómo configurarla y habilitarla, consulta la Guía del AWS CloudTrail usuario.

Trusted Advisor información en CloudTrail

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

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

- Descripción general de la creación de un sendero
- CloudTrail Integraciones y servicios compatibles
- Configuración de las notificaciones de Amazon SNS para CloudTrail

- Recibir archivos de CloudTrail registro de varias regiones y recibir archivos de CloudTrail registro de varias cuentas

Trusted Advisor permite registrar un subconjunto de las acciones de la Trusted Advisor consola como eventos en los archivos de CloudTrail registro. CloudTrail registra las siguientes acciones:

- BatchUpdateRecommendationResourceExclusion
- CreateEngagement
- CreateEngagementAttachment
- CreateEngagementCommunication
- CreateExcelReport
- DescribeAccount
- DescribeAccountAccess
- DescribeCheckItems
- DescribeCheckRefreshStatuses
- DescribeCheckSummaries
- DescribeChecks
- DescribeNotificationPreferences
- DescribeOrganization
- DescribeOrganizationAccounts
- DescribeReports
- DescribeServiceMetadata
- ExcludeCheckItems
- GenerateReport
- GetEngagement
- GetEngagementAttachment
- GetEngagementType
- GetExcelReport
- GetOrganizationRecommendation
- GetRecommendation
- IncludeCheckItems

- ListAccountsForParent
- ListChecks
- ListEngagementCommunications
- ListEngagementTypes
- ListEngagements
- ListOrganizationRecommendationAccounts
- ListOrganizationRecommendationResources
- ListOrganizationRecommendations
- ListOrganizationalUnitsForParent
- ListRecommendationResources
- ListRecommendations
- ListRoots
- RefreshCheck
- SetAccountAccess
- SetOrganizationAccess
- UpdateEngagement
- UpdateEngagementStatus
- UpdateNotificationPreferences
- UpdateOrganizationRecommendationLifecycle
- UpdateRecommendationLifecycle

Para obtener una lista completa de las acciones de la Trusted Advisor consola, consulteTrusted Advisor acciones.

> **Note**
>
> CloudTrail también registra las operaciones de la Trusted Advisor API en la referencia AWS Support de la API. Para obtener más información, consulte Registrar llamadas a la API de AWS Support con AWS CloudTrail.

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

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

Para obtener más información, consulte el elemento CloudTrail UserIdentity.

Ejemplo: Trusted Advisor entradas de archivos de registro

Un rastro es una configuración que permite la entrega de eventos como archivos de registro a un bucket de Amazon S3 que especifique. CloudTrail Los archivos de registro contienen una o más entradas de registro. Un evento representa una solicitud única de cualquier fuente e incluye información sobre la acción solicitada, la fecha y la hora de la acción, los parámetros de la solicitud, etc. CloudTrail Los archivos de registro no son un registro ordenado de las llamadas a la API pública, por lo que no aparecen en ningún orden específico.

Example : entrada de registro para RefreshCheck

El siguiente ejemplo muestra una entrada de CloudTrail registro que demuestra la `RefreshCheck` acción de la comprobación de versiones (IDR365s2Qddf) del bucket de Amazon S3.


```
{
        "eventVersion":"1.04",
        "userIdentity":{
        "type":"IAMUser",
        "principalId":"AIDACKCEVSQ6C2EXAMPLE",
        "arn":"arn:aws:iam::123456789012:user/janedoe",
        "accountId":"123456789012",
        "accessKeyId":"AKIAIOSFODNN7EXAMPLE",
        "userName":"janedoe",
        "sessionContext":{
        "attributes":{
        "mfaAuthenticated":"false",
        "creationDate":"2020-10-21T22:06:18Z"
        }
        }
        },
        "eventTime":"2020-10-21T22:06:33Z",
        "eventSource":"trustedadvisor.amazonaws.com",
        "eventName":"RefreshCheck",
```

```
        "awsRegion":"us-east-1",
        "sourceIPAddress":"100.127.34.136",
        "userAgent":"signin.amazonaws.com",
        "requestParameters":{
        "checkId":"R365s2Qddf"
        },
        "responseElements":{
        "status":{
        "checkId":"R365s2Qddf",
        "status":"enqueued",
        "millisUntilNextRefreshable":3599993
        }
        },
        "requestID":"d23ec729-8995-494c-8054-dedeaEXAMPLE",
        "eventID":"a49d5202-560f-4a4e-b38a-02f1cEXAMPLE",
        "eventType":"AwsApiCall",
        "recipientAccountId":"123456789012"
        }
```


Example : Entrada de registro para UpdateNotificationPreferences

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


```
{
        "eventVersion":"1.04",
        "userIdentity":{
        "type":"IAMUser",
        "principalId":"AIDACKCEVSQ6C2EXAMPLE",
        "arn":"arn:aws:iam::123456789012:user/janedoe",
        "accountId":"123456789012",
        "accessKeyId":"AKIAIOSFODNN7EXAMPLE",
        "userName":"janedoe",
        "sessionContext":{
        "attributes":{
        "mfaAuthenticated":"false",
        "creationDate":"2020-10-21T22:06:18Z"
        }
        }
        },
        "eventTime":"2020-10-21T22:09:49Z",
        "eventSource":"trustedadvisor.amazonaws.com",
```

```
        "eventName":"UpdateNotificationPreferences",
        "awsRegion":"us-east-1",
        "sourceIPAddress":"100.127.34.167",
        "userAgent":"signin.amazonaws.com",
        "requestParameters":{
        "contacts":[
        {
        "id":"billing",
        "type":"email",
        "active":false
        },
        {
        "id":"operational",
        "type":"email",
        "active":false
        },
        {
        "id":"security",
        "type":"email",
        "active":false
        }
        ],
        "language":"en"
        },
        "responseElements":null,
        "requestID":"695295f3-c81c-486e-9404-fa148EXAMPLE",
        "eventID":"5f923d8c-d210-4037-bd32-997c6EXAMPLE",
        "eventType":"AwsApiCall",
        "recipientAccountId":"123456789012"
        }
```


Example : entrada de registro para GenerateReport

El siguiente ejemplo muestra una entrada de CloudTrail registro que demuestra la `GenerateReport` acción. Esta acción crea un informe para su organización de AWS .


```
{
        "eventVersion":"1.04",
        "userIdentity":{
        "type":"IAMUser",
        "principalId":"AIDACKCEVSQ6C2EXAMPLE",
        "arn":"arn:aws:iam::123456789012:user/janedoe",
```

```
        "accountId":"123456789012",
        "accessKeyId":"AKIAIOSFODNN7EXAMPLE",
        "userName":"janedoe",
        "sessionContext":{
        "attributes":{
        "mfaAuthenticated":"false",
        "creationDate":"2020-11-03T13:03:10Z"
        }
        }
        },
        "eventTime":"2020-11-03T13:04:29Z",
        "eventSource":"trustedadvisor.amazonaws.com",
        "eventName":"GenerateReport",
        "awsRegion":"us-east-1",
        "sourceIPAddress":"100.127.36.171",
        "userAgent":"signin.amazonaws.com",
        "requestParameters":{
        "refresh":false,
        "includeSuppressedResources":false,
        "language":"en",
        "format":"JSON",
        "name":"organizational-view-report",
        "preference":{
        "accounts":[

        ],
        "organizationalUnitIds":[
        "r-j134"
        ],
        "preferenceName":"organizational-view-report",
        "format":"json",
        "language":"en"
        }
        },
        "responseElements":{
        "status":"ENQUEUED"
        },
        "requestID":"bb866dc1-60af-47fd-a660-21498EXAMPLE",
        "eventID":"2606c89d-c107-47bd-a7c6-ec92fEXAMPLE",
        "eventType":"AwsApiCall",
        "recipientAccountId":"123456789012"
        }
```

Recursos para la resolución de problemas

Para obtener respuestas a las preguntas sobre resolución de problemas comunes, consulte el Centro de conocimientos de AWS Support.

Para Windows, Amazon EC2 ofrece EC2Rescue, que los clientes pueden utilizar para examinar sus instancias de Windows con el fin de identificar problemas comunes, recopilar archivos de registro y AWS Support solucionar sus problemas. También puede utilizar EC2Rescue para analizar los volúmenes de arranque de las instancias no funcionales. Para obtener más información, consulte ¿Cómo puedo utilizar EC2Rescue para solucionar y resolver problemas comunes en mi instancia EC2 Windows?

Solución de problemas específicos del servicio

La mayoría de Servicio de AWS la documentación contiene temas de solución de problemas que pueden ayudarle a empezar antes de ponerse en contacto con usted. AWS Support La siguiente tabla proporciona enlaces a temas de resolución de problemas, organizados por servicio.

> **Note**
>
> La siguiente tabla proporciona una lista de los servicios más comunes. Para buscar otros temas de solución de problemas, utilice el cuadro de texto de búsqueda de la página de inicio de la AWS documentación.

Servicio	Enlace
Amazon Web Services	Solución de errores de la versión 4 de AWS Signature
Amazon API Gateway	Solución de problemas con las API HTTP
Amazon AppStream	Solución de problemas de Amazon AppStream
Amazon Athena	Solución de problemas en Athena
Amazon Aurora MySQL	Solución de problemas de Amazon Aurora

Servicio	Enlace
PostgreSQL de Amazon Aurora	Solución de problemas de Amazon Aurora
Amazon EC2 Auto Scaling	Solución de problemas de Auto Scaling
AWS Certificate Manager (ACM)	Solución de problemas
AWS CloudFormation	Solución de problemas de AWS CloudFormation
Amazon CloudFront	Solución de problemas | Solución de problemas con distribuciones de RTMP
AWS CloudHSM	Solución de problemas
Amazon CloudSearch	Solución de problemas de Amazon CloudSearch
AWS CodeDeploy	Solución de problemas de AWS CodeDeploy
Amazon CloudWatch	Solución de problemas de
AWS Database Migration Service	Solución de problemas de migración en AWS Database Migration Service
AWS Data Pipeline	Solución de problemas
AWS Direct Connect	Solución de problemas de AWS Direct Connect
AWS Directory Service	Solución de problemas AWS Directory Service de administración
Amazon DynamoDB	Solución de problemas | Solución de problemas de establecimiento de conexiones SSL/TLS
AWS Elastic Beanstalk	Solución de problemas

Servicio	Enlace
Amazon Elastic Compute Cloud (Amazon EC2)	Solución de problemas de instancias | Solución de problemas de instancias de Windows | Solución de problemas con VM Import/Export | Solución de errores de solicitudes de API | Solución de problemas con AWS Management Pack | Solución de problemas con AWS Systems Manager para Microsoft SCVMM | Diagnóstico de AWS para Microsoft Windows Server
Amazon Elastic Container Service (Amazon ECS)	Solución de problemas de Amazon ECS
Amazon Elastic Kubernetes Service (Amazon EKS)	Solución de problemas de Amazon EKS
Elastic Load Balancing	Solución de problemas con balanceadores de carga de aplicación | Solución de problemas del balanceador de carga clásico
Amazon ElastiCache para Memcached	Solución de problemas de aplicaciones
Amazon ElastiCache para Redis	Solución de problemas de aplicaciones
Amazon EMR	Solución de problemas de un clúster
AWS Flow Framework	Solución de problemas y sugerencias de depuración
AWS Glue	Solución de problemas AWS Glue
AWS Glue DataBrew	Solución de problemas de identidades y accesos en AWS Glue DataBrew
AWS GovCloud (US)	Solución de problemas
AWS Identity and Access Management (IAM)	Solución de problemas de IAM
Amazon Keyspaces (para Apache Cassandra)	Solución de problemas de Amazon Keyspaces (para Apache Cassandra)

Servicio	Enlace
Amazon Kinesis Data Streams	Solución de problemas de productores de Amazon Kinesis Data Streams | Solución de problemas de consumidores de Amazon Kinesis Data Streams
Amazon Managed Service para Apache Flink	Solución de problemas de rendimiento | Solución de problemas de Amazon Managed Service para Apache Flink para aplicaciones SQL
Amazon Data Firehose	Solución de problemas de Amazon Data Firehose
AWS Lambda	AWS Lambda Funciones de resolución de problemas y supervisión con CloudWatch
OpenSearch Servicio Amazon	Solución de problemas de Amazon OpenSearch Service
AWS OpsWorks	Guía de depuración y solución de problemas
Amazon Personalize	Solución de problemas
Amazon QLDB	Solución de problemas de Amazon QLDB
Amazon QuickSight	Solución de problemas de Amazon QuickSight | Solución de errores de filas omitidas
AWS Resource Access Manager (AWS RAM)	Solución de problemas con AWS RAM
Amazon Redshift	Solución de problemas de consultas | Solución de problemas de cargas de datos | Solución de problemas de conexión en Amazon Redshift | Solución de problemas de registros de auditoría en Amazon Redshift Spectrum | Solución de problemas de consultas en Amazon Redshift Spectrum
Amazon Relational Database Service (Amazon RDS)	Solución de problemas | Solución de problemas de aplicaciones en Amazon RDS | Solución de problemas de bases de datos para Amazon RDS Custom
Amazon Route 53	Solución de problemas de Amazon Route 53

Servicio	Enlace
Amazon SageMaker	Solucionar errores | Solución de problemas de Amazon Studio SageMaker
Amazon Silk	Solución de problemas
Amazon Simple Email Service (Amazon SES)	Solución de problemas de Amazon SES
Amazon Simple Storage Service (Amazon S3)	Solución de problemas
Amazon Simple Workflow Service (Amazon SWF)	AWS marco de flujo para Java: consejos de solución de problemas y depuración | marco de AWS flujo para Ruby: solución de problemas y depuración de flujos de trabajo
AWS Storage Gateway	Solución de problemas de la gateway
AWS Systems Manager	Solución de problemas de Agente SSM
Amazon Virtual Private Cloud (Amazon VPC)	Solución de problemas
AWS Virtual Private Network (AWS VPN)	Solución de problemas del dispositivo de puerta de enlace de cliente
AWS WAF	Probando y ajustando sus protecciones AWS WAF
Amazon WorkMail	Solución de problemas de la aplicación WorkMail web Amazon
Amazon WorkSpaces	Solución de problemas de Amazon WorkSpaces | Solución de problemas de WorkSpaces clientes de Amazon

Historial de documentos

En la siguiente tabla se describen los cambios importantes en la documentación desde la última versión del AWS Support servicio.

- AWS Support Versión de API: 2013-04-15
- AWS Support Versión de la API de la aplicación: 20 de agosto de 2021

En la siguiente tabla se describen las actualizaciones importantes de la AWS Trusted Advisor documentación AWS Support y, a partir del 10 de mayo de 2021. Puede suscribirse a una fuente RSS para recibir notificaciones sobre actualizaciones.

Cambio	Descripción	Fecha
Documentación actualizada para AWSTrustedAdvisorServiceRolePolicy	Se agregaron nuevas acciones de IAM access-analyzer:ListAnalyzers cloudwatch:ListMetrics dax:DescribeClusters ec2:DescribeNatGateways ,ec2:DescribeRouteTables ,,ec2:DescribeVpcEndpoints ,ec2:GetManagedPrefixListEntries , elasticloadbalancing:DescribeTargetHealth iam:ListSAMLProviders , kafka:DescribeClusterV2 network-firewall:ListFirewalls network-f	11 de junio de 2024

	`irewall:DescribeFirewall` y `sqs:GetQueueAttributes` para incorporar nuevos cheques. Para obtener más información, consulte Políticas administradas de AWS : AWSTrustedAdvisorServiceRolePolicy.	
Se agregó documentación para las recomendaciones AWS Support	Se agregó documentación para AWS Support las recomendaciones.	22 de mayo de 2024
Se eliminaron 5 AWS Trusted Advisor cheques de la documentación	Se eliminaron 5 AWS Trusted Advisor comprobaciones que ahora están en desuso. Para obtener más información, consulte el registro de cambios de las AWS Trusted Advisor comprobaciones.	15 de mayo de 2024
Se agregó 1 nuevo control AWS Trusted Advisor de seguridad a la documentación	Se agregó 1 nuevo control AWS Trusted Advisor de seguridad a la documentación. Para obtener más información, consulte el registro de cambios de las AWS Trusted Advisor comprobaciones.	15 de mayo de 2024
Se eliminaron 3 comprobaciones de tolerancia a errores de la documentación	Se eliminaron 3 comprobaciones de tolerancia a errores que ahora están en desuso. Para obtener más información, consulte el registro de cambios para ver las AWS Trusted Advisor comprobaciones.	25 de abril de 2024

Documentación actualizada sobre la tolerancia a errores y los controles de seguridad	Se ha añadido 1 nueva comprobación de toleranci a a fallos. Se actualizaron 1 tolerancia a fallas y 1 control de seguridad. Para obtener más información, consulte el registro de cambios de las AWS Trusted Advisor comprobaciones.	29 de marzo de 2024
Documentación actualizada para `AWSSupportServiceRolePolicy`	Se han agregado nuevos permisos para proporcionar servicios administrativos, de facturación y de soporte para el rol vinculado al servicio. Para obtener más información, consulte Políticas administradas de AWS : AWSSupportServiceRolePolicy.	22 de marzo de 2024
Documentación actualizada del AWS Support plan	Actualizaciones de las características de AWS Support los planes. Para obtener más información, consulte AWS Support los planes.	11 de marzo de 2024
Documentación actualizada para Trusted Advisor	Se ha añadido 1 comprobac ión de tolerancia a fallos. Para obtener más informaci ón, consulte el registro de cambios para ver las AWS Trusted Advisor comprobac iones.	29 de febrero de 2024

Documentación actualizada para Trusted Advisor	Se ha añadido 1 comprobación de tolerancia a fallos. Para obtener más información, consulte el registro de cambios para ver las AWS Trusted Advisor comprobaciones.	31 de enero de 2024
Documentación actualizada para `AWSTrustedAdvisorServiceRolePolicy`	Se agregaron nuevas acciones de IAM `cloudtrail:GetTrail` `cloudtrail:ListTrails` `cloudtrail:GetEventSelectors` ,`outposts:GetOutpost` , `outposts:ListAssets` y `outposts:ListOutposts` para incorporar nuevos cheques. Para obtener más información, consulte Políticas administradas de AWS : AWSTrustedAdvisorServiceRolePolicy.	18 de enero de 2024
Documentación actualizada para `AWSSupportServiceRolePolicy`	Se han agregado nuevos permisos para proporcionar servicios administrativos, de facturación y de soporte para el rol vinculado al servicio. Para obtener más información, consulte Políticas administradas de AWS : AWSSupportServiceRolePolicy.	17 de enero de 2024

Documentación actualizada para Trusted Advisor	Se actualizó 1 comprobación de tolerancia a fallos para modificar el título y la descripción. Para obtener más información, consulte el registro de cambios para ver las AWS Trusted Advisor comprobaciones.	8 de enero de 2024
Documentación actualizada para Trusted Advisor	Se actualizó 1 control de seguridad para reflejar el cambio en el período de obsolescencia. Para obtener más información, consulta el registro de cambios para ver las AWS Trusted Advisor comprobaciones.	21 de diciembre de 2023
Documentación actualizada para Trusted Advisor	Se agregaron 2 controles de seguridad y 2 controles de rendimiento. Para obtener más información, consulte el registro de cambios de las AWS Trusted Advisor comprobaciones.	20 de diciembre de 2023
Documentación actualizada para Trusted Advisor	Se agregó 1 control de seguridad. Para obtener más información, consulta el registro de cambios de las AWS Trusted Advisor comprobaciones.	15 de diciembre de 2023

Documentación actualizada de Trusted Advisor Engage	Se actualizó la documentación de Trusted Advisor Engage con cambios en la opción de notificación por correo electrónico.	14 de diciembre de 2023
Documentación actualizada de Trusted Advisor Engage	Se actualizó la documentación de Trusted Advisor Engage con cambios en las contratac iones programadas.	11 de diciembre de 2023
Documentación actualizada para Trusted Advisor	Se agregaron 2 nuevas comprobaciones de toleranci a a fallas y 1 verificación de optimización de costos. Para obtener más informaci ón, consulte el registro de cambios para ver las AWS Trusted Advisor comprobac iones.	7 de diciembre de 2023
Documentación actualizada para `AWSSupportServiceR olePolicy`	Se han agregado nuevos permisos para proporcionar servicios administrativos, de facturación y de soporte para el rol vinculado al servicio. Para obtener más información, consulte Políticas administr adas de AWS : AWSSuppor tServiceRolePolicy.	6 de diciembre de 2023

Se actualizaron las políticas AWS gestionadas para Trusted Advisor	Se actualizaron `AWSTrustedAdvisorPriorityFullAccess` y `AWSTrustedAdvisorPriorityReadOnlyAccess` AWS gestionaron las políticas para incluir los identificadores de las declaraciones. Para más información, consulte Políticas administradas de AWS para AWS Trusted Advisor.	6 de diciembre de 2023
Documentación actualizada para Trusted Advisor	Se han añadido 3 nuevas comprobaciones de tolerancia a fallos. Para obtener más información, consulte el registro de cambios para ver las AWS Trusted Advisor comprobaciones.	17 de noviembre de 2023
Documentación actualizada para Trusted Advisor	Se han añadido 37 cheques nuevos para Amazon RDS. Para obtener más información, consulte el registro de cambios de las AWS Trusted Advisor comprobaciones.	15 de noviembre de 2023

Documentación actualizada para AWSTrustedAdvisorServiceRolePolicy	Se han añadido nuevas acciones ec2:DescribeRegions de IAM ecs:DescribeTaskDefinition y se ecs:ListTaskDefinitions han incorporado nuevos cheques. s3:GetLifecycleConfiguration Para obtener más información, consulte Políticas administradas de AWS : AWSTrustedAdvisorServiceRolePolicy.	9 de noviembre de 2023
Documentación actualizada para AWSSupportServiceRolePolicy	Se han agregado nuevos permisos para proporcionar servicios administrativos, de facturación y de soporte para el rol vinculado al servicio. Para obtener más información, consulte Políticas administradas de AWS : AWSSupportServiceRolePolicy.	27 de octubre de 2023
Documentación actualizada para Trusted Advisor	Se agregaron 64 nuevos cheques integrados desde AWS Config. Para obtener más información, consulte el registro de cambios de las AWS Trusted Advisor comprobaciones.	26 de octubre de 2023

Documentación actualizada para Trusted Advisor	Se han añadido seis nuevas comprobaciones de tolerancia a fallos Trusted Advisor. Para obtener más información, consulte el registro de cambios para ver las AWS Trusted Advisor comprobaciones.	12 de octubre de 2023
Documentación actualizada para `AWSTrustedAdvisorServiceRolePolicy`	Se agregaron las nuevas acciones de IAM `route53resolver:ListResolverEndpoints`, `route53resolver:ListResolverEndpointIpAddresses`, `ec2:DescribeSubnets`, `kafka:ListClustersV2` y `kafka:ListNodes` para incorporar comprobaciones de resiliencia nuevas. Para obtener más información, consulte Políticas administradas de AWS : AWSTrustedAdvisorServiceRolePolicy.	14 de septiembre de 2023
Documentación actualizada para `AWSSupportServiceRolePolicy`	Se han agregado nuevos permisos para proporcionar servicios administrativos, de facturación y de soporte para el rol vinculado al servicio. Para obtener más información, consulte Políticas administradas de AWS : AWSSupportServiceRolePolicy.	28 de agosto de 2023

Documentación actualizada para Trusted Advisor	Se agregó 1 nueva verificación de límites de servicio AWS Lambda. Para obtener más información, consulta el registro de cambios para ver las AWS Trusted Advisor comprobaciones.	17 de agosto de 2023
Documentación actualizada para Trusted Advisor	Se agregó 1 nueva comprobación de tolerancia a fallos para Lambda. Para obtener más información, consulte el registro de cambios para ver las AWS Trusted Advisor comprobaciones.	3 de agosto de 2023
Documentación actualizada de Trusted Advisor Engage	Se actualizó la documentación de Trusted Advisor Engage con cambios en los formularios para la creación y edición de interacciones. Se agregó una página con ejemplos de políticas de control de servicios para AWS Trusted Advisor.	27 de julio de 2023
Documentación actualizada para `AWSSupportServiceRolePolicy`	Se han agregado nuevos permisos para proporcionar servicios administrativos, de facturación y de soporte para el rol vinculado al servicio. Para obtener más información, consulte Políticas administradas de AWS : AWSSupportServiceRolePolicy.	26 de junio de 2023

Documentación actualizada para Trusted Advisor	Se agregaron dos nuevas comprobaciones de tolerancia a fallos para Amazon MQ. Se agregó una nueva comprobación de tolerancia a errores y una nueva comprobación de rendimiento para Amazon Elastic File System. Para obtener más información, consulte el registro de cambios para ver las AWS Trusted Advisor comprobaciones.	1 de junio de 2023
Documentación actualizada para Trusted Advisor	Se agregaron dos nuevas comprobaciones de tolerancia a fallos para NAT Gateway. Para obtener más información, consulte el registro de cambios para ver las AWS Trusted Advisor comprobaciones.	16 de mayo de 2023
Documentación actualizada de los AWS Support planes	Se agregaron un nuevo permiso y CloudTrail documentación para la creación de los cronogramas de los planes de soporte. Para obtener más información, consulte Administrar el acceso a AWS Support los planes, AWS administrar las políticas de AWS Support los planes y Registrar las llamadas a la API de AWS Support los planes con ellos AWS CloudTrail.	8 de mayo de 2023

Documentación actualizada para `AWSSupportServiceRolePolicy`	Se han agregado nuevos permisos para proporcionar servicios administrativos, de facturación y de soporte para el rol vinculado al servicio. Para obtener más información, consulte Políticas administradas de AWS : AWSSupportServiceRolePolicy.	2 de mayo de 2023
Documentación actualizada para Trusted Advisor Engage y Trusted Advisor Priority	Se han aclarado los requisitos previos para Trusted Advisor Engage y Trusted Advisor Priority. Se agregó un ejemplo de la política de IAM con la capacidad de usar Trusted Advisor Engage y permitir un acceso confiable a Trusted Advisor.	28 de abril de 2023
Documentación actualizada para Trusted Advisor	Se agregaron dos nuevas comprobaciones de tolerancia a errores para AWS Resilience Hub Incident Manager. Para obtener más información, consulte el registro de cambios para ver las AWS Trusted Advisor comprobaciones.	27 de abril de 2023

Se agregó documentación para Trusted Advisor Engage	Puede usar AWS Trusted Advisor Engage para aprovechar al máximo sus AWS Support planes, ya que le permite ver, solicitar y realizar un seguimiento de todas sus interacciones proactivas y comunicarse con su Cuenta de AWS equipo sobre las interacciones en curso. Para obtener más información, consulte Introducción a AWS Trusted Advisor Engage.	6 de abril de 2023
Documentación actualizada para Trusted Advisor	Se agregaron dos nuevas comprobaciones de tolerancia a fallos para Amazon ECS. Para obtener más información, consulte el registro de cambios para ver las AWS Trusted Advisor comprobaciones.	30 de marzo de 2023
Documentación actualizada para `AWSSupportServiceRolePolicy`	Se han agregado nuevos permisos para proporcionar servicios administrativos, de facturación y de soporte para el rol vinculado al servicio. Para obtener más información, consulte Políticas administradas de AWS : AWSSupportServiceRolePolicy.	16 de marzo de 2023

Se agregó documentación para Trusted Advisor Priority	Se actualizó la consola Trusted Advisor Priority: • Los botones Confirmar y Descartar han reemplaza do a los botones Aceptar y Rechazar. • No es necesario ingresar el cargo ni el nombre para confirmar, resolver, descartar o reabrir recomendaciones. Para obtener más informaci ón, consulta Cómo empezar a usar Trusted Advisor Priority.	16 de febrero de 2023
Ejemplos de código actualiza dos para AWS Support	Se agregaron ejemplos de código.NET, Java y Kotlin que muestran cómo usarlos AWS Support con un kit de desarroll o de AWS software (SDK). Para obtener más información, consulta Ejemplos de código para AWS Support usar los AWS SDK.	16 de enero de 2023
Documentación actualizada para `AWSSupportServiceR olePolicy`	Se han agregado nuevos permisos para proporcionar servicios administrativos, de facturación y de soporte para el rol vinculado al servicio. Para obtener más información, consulte Políticas administr adas de AWS : AWSSuppor tServiceRolePolicy.	10 de enero de 2023

Documentación actualizada de la aplicación AWS Support	Puede buscar casos de soporte en Slack mediante las opciones de filtro o buscando por ID de caso. Para más información, consulte Búsqueda de casos de soporte en Slack.	29 de diciembre de 2022
Documentación actualizada de la AWS Support aplicación	También puede usar Terraform para crear sus recursos para la AWS Support aplicación. Para obtener más información, consulte Crear recursos de AWS Support aplicaciones mediante Terraform.	22 de diciembre de 2022
Documentación actualizada para Trusted Advisor	Se agregaron tres nuevas comprobaciones de tolerancia a errores para Amazon MemoryDB ElastiCache, Amazon y. AWS CloudHSM Para obtener más información, consulte el registro de cambios para AWS Trusted Advisor ver las comprobaciones.	15 de diciembre de 2022

Documentación actualizada de la AWS Support aplicación en Slack	Ahora puede solicitar soporte por chat en vivo para las siguientes opciones: • Casos de soporte de cuentas y facturación. • Soporte en japonés para casos de soporte técnico. • Para más información, consulte Creación de casos de soporte en un canal de Slack.	14 de diciembre de 2022
Documentación actualizada para AWS Support	Se agregó documentación sobre los nuevos puntos finales de la AWS Support API. Para más información, consulte Sobre la API de AWS Support.	14 de diciembre de 2022
Se agregó documentación sobre las AWS CloudForm ation plantillas que se usarán en la AWS Support aplicación en Slack	Puedes usar CloudForm ation plantillas para crear espacios de trabajo y canales de configuración de Slack para ello. Cuentas de AWS AWS Organizations Para obtener más información, consulta Cómo crear recursos de AWS Support aplicaciones con. AWS CloudFormation	5 de diciembre de 2022

Documentación actualizada para Trusted Advisor	Se agregaron dos nuevas comprobaciones de tolerancia a errores para AWS Resilience Hub. Para obtener más información, consulte el registro de cambios para ver las AWS Trusted Advisor comprobaciones.	17 de noviembre de 2022
Se agregó documentación para sus AWS Security Hub hallazgos en Trusted Advisor	Los hallazgos de los controles de Security Hub se eliminan Trusted Advisor más rápido. Para obtener más información, consulte el registro de cambios para ver las AWS Trusted Advisor comprobaciones.	17 de noviembre de 2022
Documentación actualizada para AWS Trusted Advisor	Se agregó documentación para Trusted Advisor las recomendaciones. Para obtener más información, consulte el registro de cambios para ver las AWS Trusted Advisor comprobaciones.	16 de noviembre de 2022
Documentación actualizada de la AWS Support aplicación en Slack	Se agregó documentación para la compatibilidad con el idioma japonés. Para más información, consulte Creación de casos de soporte en un canal de Slack.	11 de noviembre de 2022

Documentación actualizada de los planes AWS Support	Se agregó información de solución de problemas para permitir el acceso de Support Plans en una organización. Para más información, consulte Solución de problemas.	9 de noviembre de 2022
Documentación actualizada de la AWS Support aplicación en Slack	Se agregó documentación para los permisos `supportapp` . Para obtener más información, consulta los permisos necesarios para que la AWS Support aplicación se conecte a Slack.	1 de noviembre de 2022
Documentación actualizada de la AWS Support aplicación en Slack	Puede usar la operación de la API `RegisterSlackWorkspaceForOrganization` para registrar un espacio de trabajo de Slack para su Cuenta de AWS. Para llamar a esta API, su cuenta debe formar parte de una organización de AWS Organizations. Para obtener más información, consulte Aplicación AWS Support en Referencia de la API en Slack.	19 de octubre de 2022

Documentación actualizada para `AWSSupportServiceRolePolicy`	Se han agregado nuevos permisos para proporcionar servicios administrativos, de facturación y de soporte para el rol vinculado al servicio. Para obtener más información, consulte Políticas administradas de AWS : AWSSupportServiceRolePolicy.	4 de octubre de 2022
Documentación actualizada para los planes de Support	Ahora puedes usar AWS Identity and Access Management (IAM) para gestionar los permisos y cambiar tu plan de soporte. Cuenta de AWS Para obtener más información, consulte los temas siguientes: • Administrar el acceso a los planes AWS Support • AWS políticas gestionadas para AWS Support los planes • Cambiar AWS Support los planes • Registrar las llamadas a la API de AWS Support Plans con AWS CloudTrail	29 de septiembre de 2022

Documentación actualizada de la AWS Support aplicación en Slack	Se agregó documentación sobre cómo configurar un canal público o privado para usarlo con la AWS Support aplicación. Para obtener más información, consulte Configuring a Slack channel (Configuración de un canal de Slack).	22 de septiembre de 2022
Documentación actualizada para AWS Support	Se agregó una nueva sección sobre seguridad para sus casos de soporte. Para obtener más información, consulte Seguridad para sus AWS Support casos.	9 de septiembre de 2022
Documentación actualizada para Trusted Advisor	Se agregó una nueva comprobación de seguridad para Amazon EC2. Para obtener más información, consulte el registro de cambios para ver las AWS Trusted Advisor comprobaciones.	1 de septiembre de 2022

Documentación actualizada de la AWS Support aplicación en Slack	Consulte los siguientes temas: Puedes usar la AWS Support aplicación para gestionar tus casos de asistencia, solicitar aumentos de la cuota de servicio y chatear con los agentes de asistencia directamente en tus canales de Slack. Para obtener más información, consulte la documentación sobre la aplicación AWS Support en Slack. Puedes adjuntar políticas AWS gestionadas a tus funciones de IAM para usar la AWS Support aplicación. Para obtener más informaci ón, consulta las políticas AWS gestionadas de la AWS Support aplicación en Slack. Nueva referencia de API para la AWS Support aplicación. Consulte la referencia de la API de la aplicación AWS Support.	24 de agosto de 2022

Documentación actualizada para `AWSSupportServiceRolePolicy`	Se han agregado nuevos permisos para proporcionar servicios administrativos, de facturación y de soporte para el rol vinculado al servicio. Para obtener más información, consulte Políticas administradas de AWS : AWSSupportServiceRolePolicy.	17 de agosto de 2022
Se agregó documentación para Trusted Advisor Priority	Trusted Advisor Priority añade compatibilidad con las siguientes funciones: • Administradores delegados • Notificaciones diarias y semanales por correo electrónico de resúmenes de recomendaciones • Reapertura de recomendaciones resueltas o rechazadas • AWS políticas gestionadas Para obtener más información, consulte Cómo empezar con Trusted Advisor Priority.	17 de agosto de 2022
Documentación actualizada para Trusted Advisor	Se ha actualizado la página de preferencias de la Trusted Advisor consola. Para obtener más información, consulte Primeros pasos con AWS Trusted Advisor.	15 de julio de 2022

Documentación actualizada para Trusted Advisor	Se actualizaron las comprobaciones para que se incluya la siguiente información: • Criterios de alerta • Acción recomendada • Recursos adicionales • Columnas de informes Para obtener más información, consulte Referencia de verificaciones de AWS Trusted Advisor.	7 de julio de 2022
Documentación actualizada para AWS Support	Se agregó documentación que explica cómo administrar los casos de soporte. • Actualización de un caso de soporte existente • Solución de problemas	28 de junio de 2022
Documentación actualizada para `AWSSupportServiceRolePolicy`	Se actualizaron permisos para proporcionar servicios administrativos, de facturación y de soporte para el rol vinculado al servicio. Para obtener más información, consulte Políticas administradas de AWS : AWSSupportServiceRolePolicy.	23 de junio de 2022

Documentación actualizada para Trusted Advisor	Trusted Advisor admite controles estándar de seguridad adicionales de AWS Foundational Security Best Practices que provienen de AWS Security Hub. Para obtener más informaci ón, consulte el registro de cambios para ver las AWS Trusted Advisor comprobac iones.	23 de junio de 2022
Documentación actualizada para Trusted Advisor	Se agregó información acerca de cómo solicitar el aumento de la cuota de servicio. Para obtener más información, consulte Límites de servicio.	21 de junio de 2022
Documentación actualizada para AWS Support	La experiencia de creación de casos se ha actualiza do en la consola del Centro de asistencia. Para obtener más información, consulte Creación de casos de soporte y administración de casos.	18 de mayo de 2022
Documentación actualizada para Trusted Advisor	Se han añadido cuatro comprobaciones para Amazon EBS y AWS Lambda. Para obtener más información, consulte Optar por añadir Trusted Advisor cheques. AWS Compute Optimizer	4 de mayo de 2022

Documentación actualizada para `AWSSupportServiceRolePolicy`	Se han agregado nuevos permisos para proporcionar servicios administrativos, de facturación y de soporte para el rol vinculado al servicio. Para obtener más información, consulte Políticas administradas de AWS : AWSSupportServiceRolePolicy.	27 de abril de 2022
Documentación actualizada para la comprobación de las claves de acceso expuestas	Se actualiza ahora esta comprobación automáticamente. Para obtener más información, consulte el registro de cambios de AWS Trusted Advisor cheques.	25 de abril de 2022
Documentación actualizada para Trusted Advisor	Se actualizan las AWS Direct Connect comprobaciones de la categoría de tolerancia a fallos. Para obtener más información, consulte el registro de cambios para ver las AWS Trusted Advisor comprobaciones.	29 de marzo de 2022
Documentación actualizada para `AWSSupportServiceRolePolicy`	Se han agregado nuevos permisos para proporcionar servicios administrativos, de facturación y de soporte para el rol vinculado al servicio. Para obtener más información, consulte Políticas administradas de AWS : AWSSupportServiceRolePolicy.	14 de marzo de 2022

Se agregó documentación para Trusted Advisor Priority	Puede usar Trusted Advisor Priority para ver una lista de recomendaciones priorizadas de su administrador técnico de cuentas (TAM). Para obtener más información, consulte Cómo empezar a usar Trusted Advisor Priority.	28 de febrero de 2022
Documentación actualizada sobre el uso de Amazon EventBridge para Trusted Advisor	Puedes crear una EventBridge regla para supervisar los cambios en tus Trusted Advisor cheques. Para obtener más información, consulte Supervisar los resultados de las AWS Trusted Advisor comprobaciones con EventBridge.	21 de febrero de 2022
Nueva documentación sobre el uso de Amazon EventBridge para supervisar AWS Support los casos	Puedes crear una EventBridge regla para supervisar y recibir notificaciones sobre tus casos de soporte. Para obtener más información, consulte Supervisar AWS Support los casos con EventBridge.	21 de febrero de 2022
Documentación actualizada para `AWSSupportServiceRolePolicy`	Se han agregado nuevos permisos para proporcionar servicios administrativos, de facturación y de soporte para el rol vinculado al servicio. Para obtener más información, consulte Políticas administradas de AWS : AWSSupportServiceRolePolicy.	17 de febrero de 2022

Se agregó documentación para la integración con AWS Security Hub	En la Trusted Advisor consola, ahora puede ver los resultados de los controles de Security Hub que forman parte del estándar de seguridad AWS Foundational Security Best Practices. Para obtener más información, consulte Visualización de AWS Security Hub los controles de la AWS Trusted Advisor consola.	18 de enero de 2022
Documentación actualizada para Trusted Advisor	Se han agregado tres verificaciones nuevas para las instancias de Amazon EC2 que ejecutan Microsoft SQL Server. • Consolidación de las instancias de Amazon EC2 para Microsoft SQL Server • Instancias de Amazon EC2 con exceso de aprovisionamiento para Microsoft SQL Server • Instancias de Amazon EC2 con fin del soporte para Microsoft SQL Server Para obtener más información, consulte Referencia de verificaciones de AWS Trusted Advisor.	20 de diciembre de 2021

Documentación actualizada para Trusted Advisor	Trusted Advisor se agregaron cuatro nuevas comprobaciones para AWS Well-Architected • Problemas de alto riesgo de AWS Well-Architected para la optimización de costos • Problemas de alto riesgo de AWS Well-Architected para el rendimiento • Problemas de alto riesgo de AWS Well-Architected para la seguridad • Problemas de alto riesgo de AWS Well-Architected para la fiabilidad Para obtener más información, consulte Referencia de verificaciones de AWS Trusted Advisor.	20 de diciembre de 2021
Documentación actualizada	Si tienes un plan Enterprise On-Ramp Support, tienes acceso a todas las Trusted Advisor comprobaciones y a la AWS Support API.	24 de noviembre de 2021
Documentación actualizada para Trusted Advisor	Trusted Advisor se agregaron dos nuevos cheques para Amazon Comprehend. Para obtener más información, consulte Referencia de verificaciones de AWS Trusted Advisor.	29 de septiembre de 2021

Documentación actualizada para Trusted Advisor	Se actualizó el nombre del cheque Amazon OpenSearch Service Reserved Instance Optimization. Para obtener más información, consulte el registro de cambios de las AWS Trusted Advisor comprobaciones.	8 de septiembre de 2021
Documentación actualizada para las Trusted Advisor comprobaciones	Se ha añadido un tema de referencia para todas las Trusted Advisor comprobaciones. Para obtener más información, consulte Referencia de verificaciones de AWS Trusted Advisor.	1 de septiembre de 2021
Documentación actualizada para las políticas Trusted Advisor gestionadas	Documentación actualizada de las políticas Trusted Advisor gestionadas. Para obtener más información, consulte las políticas AWS administradas para AWS Support y AWS Trusted Advisor.	10 de agosto de 2021
Documentación actualizada para Trusted Advisor	Documentación actualizada para la Trusted Advisor consola. Para obtener más información, consulte Comenzar con AWS Trusted Advisor.	16 de julio de 2021

Documentación actualizada para la creación de AWS Support casos	Se agregó documentación acerca de cómo crear un caso de soporte relacionado para casos cerrados permanentemente. Para obtener más información, consulte Reapertura de un caso cerrado y Creación de un caso relacionado.	8 de junio de 2021
Documentación actualizada para Trusted Advisor	Trusted Advisor agregó dos nuevos cheques para el almacenamiento por volumen de Amazon Elastic Block Store (Amazon EBS). Para obtener más información, consulte el registro de cambios de las AWS Trusted Advisor comprobaciones.	8 de junio de 2021
Documentación actualizada	Se han actualizado los temas siguientes: • Procedimientos actualizados y contenido agregado al tema Creación de CloudWatch alarmas de Amazon para monitorear AWS Trusted Advisor las métricas • Se agregaron las cuotas de servicio para la sección AWS Support de API	12 de mayo de 2021

Actualizaciones anteriores

Cambio	Descripción	Fecha
Documentación actualizada para Trusted Advisor	Se ha agregado documentación para filtrar, actualizar y descargar los resultados de las verificaciones. Para obtener más información, consulte las siguientes secciones: • Filtrar sus verificaciones • Actualizar resultados de verificaciones • Descargar los resultados de la verificación	16 de marzo de 2021
Documentación actualizada sobre las políticas AWS gestionadas	Se agregó información sobre la política `AWSSupportServiceRolePolicy` AWS gestionada. Para obtener más información, consulte Uso de roles vinculados a servicios de AWS Support.	16 de marzo de 2021
Se agregaron comprobaciones para AWS Lambda	Se agregaron cuatro AWS Trusted Advisor comprobaciones de Lambda en el. Registro de cambios para AWS Trusted Advisor	8 de marzo de 2021
Se han actualizado las verificaciones de límite de servicio de Amazon Elastic Block Store	Se actualizaron cinco AWS Trusted Advisor comprobaciones para Amazon EBS en elRegistro de cambios para AWS Trusted Advisor.	5 de marzo de 2021
Documentación actualizada para el registro CloudTrail	CloudTrail admite el registro de las acciones de la consola cuando cambias de AWS Support plan. Para obtener más información, consulte Registro de cambios en su plan de AWS Support.	9 de febrero de 2021

Cambio	Descripción	Fecha
Documentación actualizada para Trusted Advisor	Se ha actualizado el tema Comience con Recommendations de Trusted Advisor.	29 de enero de 2021
Documentación actualizada para los Trusted Advisor informes	Se agregó una Solución de problemas sección para usar Trusted Advisor los informes con otros AWS servicios.	4 de diciembre de 2020
Se agregó AWS Trusted Advisor soporte para el AWS CloudTrail registro	CloudTrail admite el registro de un subconjunto de acciones de la Trusted Advisor consola. Para obtener más información, consulte Registrar las acciones de la AWS Trusted Advisor consola con AWS CloudTrail.	23 de noviembre de 2020
Se ha agregado un tema de registro de cambios.	Vea los cambios en las AWS Trusted Advisor comprobaciones y las categorías en. Registro de cambios para AWS Trusted Advisor	18 de noviembre de 2020
Se ha agregado compatibilidad con las unidades organizativas.	Ahora puede crear informes para las Trusted Advisor comprobaciones de las unidades organizativas (OU). Para obtener más información, consulte Crear informes de vista organizativa.	17 de noviembre de 2020
Se actualizó el registro con AWS CloudTrail el tema	Se agregó un ejemplo de entrada de registro para una operación de Trusted Advisor API. Consulte Información de AWS Trusted Advisor en el registro de CloudTrail.	22 de octubre de 2020
Se agregaron AWS Support cuotas	Se ha agregado información sobre las cuotas y restricciones actuales de AWS Support. Consulte los puntos de enlace y las cuotas AWS Support en Referencia general de AWS.	4 de agosto de 2020

Cambio	Descripción	Fecha
Vista organizativa de AWS Trusted Advisor	Ahora puede crear informes para los Trusted Advisor cheques de las cuentas que forman parte de AWS Organizations. Consulte Vista organizativa para AWS Trusted Advisor.	17 de julio de 2020
Seguridad y AWS Support	Se ha actualizado información sobre considera ciones de seguridad al usar AWS Support y Trusted Advisor. Consulte Seguridad en AWS Support	5 de mayo de 2020
Seguridad y AWS Support	Se ha agregado información sobre las consideraciones de seguridad cuando se utiliza AWS Support.	10 de enero de 2020
Trusted Advisor Utilización como servicio web	Se agregaron instrucciones actualizadas para actualizar Trusted Advisor los datos después de obtener la lista de Trusted Advisor comprobaciones.	1 de noviembre de 2018
Uso de roles vinculados a servicios	Se ha agregado una nueva sección.	11 de julio de 2018
Introducción: solución de problemas	Se han agregado enlaces de resolución de problemas para Route 53 y AWS Certificate Manager.	1 de septiembre de 2017
Ejemplo de administr ación de casos: Creación de un caso	Se ha añadido una nota sobre el cuadro CC para usuarios que tienen el plan de soporte Basic.	1 de agosto de 2017
Supervisión de los resultados de las Trusted Advisor comprobaciones mediante CloudWatch eventos	Se ha agregado una nueva sección.	18 de noviembre de 2016

Cambio	Descripción	Fecha
Administración de casos	Actualizados los nombres de niveles de gravedad de casos.	27 de octubre de 2016
Registrar AWS Support llamadas con AWS CloudTrail	Se ha agregado una nueva sección.	21 de abril de 2016
Introducción: solución de problemas	Se han añadido más enlaces de resolución de problemas.	19 de mayo de 2015
Introducción: solución de problemas	Se han añadido más enlaces de resolución de problemas.	18 de noviembre de 2014
Introducción: Administración de casos	Se actualizó para reflejar Service Catalog en la AWS Management Console.	30 de octubre de 2014
Programando la vida de un AWS Support caso	Se ha añadido información sobre nuevos elementos de API para añadir archivos adjuntos a casos y para omitir comunicaciones de casos al recuperar el historial de casos.	16 de julio de 2014
Acceder AWS Support	Se han eliminado contactos de soporte designados como método de acceso.	28 de mayo de 2014
Introducción	Se ha añadido la sección Introducción.	13 de diciembre de 2013
Publicación inicial	Lanzamiento AWS Support de un nuevo servicio.	30 de abril de 2013

Glosario de AWS

Para ver la terminología más reciente de AWS, consulte el Glosario de AWS en la Referencia de Glosario de AWS.

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.