



Guía del usuario de

AWS Support



Versión de API 2026-06-08

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

AWS Support: Guía del usuario de

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

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

Table of Contents

Comience con AWS Support	1
AI-enhanced solución de problemas en Support Center Console	2
Configura los permisos para utilizar la AI-enhanced solución de problemas	5
Cree una interacción de soporte	9
Cree un caso de soporte a partir de una interacción de soporte	12
Vea las interacciones de soporte	17
Resolución de problemas	17
Reuniones virtuales con AWS Support	18
Únase a una reunión virtual	19
Seguridad y privacidad durante la reunión virtual	19
Permisos de IAM necesarios para las reuniones virtuales	20
Solución de problemas de reuniones virtuales	21
Administración de casos	21
Descripción del problema	22
Elegir un nivel de gravedad inicial	22
Descripción AWS Support tiempos de respuesta	26
Cambiar el nivel de gravedad de un caso de soporte	27
Solicite un aumento de la cuota de servicio.	30
Método tradicional: crear casos de soporte y gestión de casos	32
Creación de un caso de soporte	33
Descripción del problema	35
Elegir un nivel de gravedad inicial	36
Descripción AWS Support tiempos de respuesta	38
Cambiar el nivel de gravedad de un caso de soporte	39
Ejemplo: Crear un caso de soporte para cuentas y facturación	42
Experiencia tradicional: actualice, resuelva y vuelva a abrir sus casos	48
Trabajando con AWS SDK	54
Usando Agente de AWS DevOps	56
Elegibilidad y créditos del plan	56
Habilitando Agente de AWS DevOps	57
Recursos creados	58
Eliminando Agente de AWS DevOps	62
Seguridad	62
Obtener ayuda	63

Acerca de la API de la consola del centro de soporte	64
Añadir políticas de IAM para las operaciones de la API de la consola del centro de soporte	64
Pruebas de las llamadas a la API de la consola del centro de soporte	67
Acerca de la AWS Support API	69
Administración de casos de soporte	70
AWS Trusted Advisor	71
Puntos de conexión	71
Support en AWS SDKs	72
AWS Support Planes	73
Características de AWS Support Planes	74
¿Qué es? AWS Operaciones unificadas	76
AWS Precios de operaciones unificadas	76
Ventajas de las operaciones unificadas	77
Equipo de operaciones unificado	78
Ciclo de vida de las operaciones unificadas	80
Cómo empezar con las operaciones unificadas	84
Cambio AWS Support Planes	91
Información relacionada	93
Configure las notificaciones de caducidad del plan promocional	93
Ver las notificaciones del plan promocional	94
On-Ramp Fin del soporte para desarrolladores, empresas y empresas	94
Desarrollador Soporte planifique el fin del soporte	95
Usuarios Soporte planifique el fin del soporte	95
On-Ramp Fin del soporte empresarial	95
AWS Trusted Advisor	96
Comience con Trusted Advisor las recomendaciones	98
Inicie sesión en la Trusted Advisor consola	99
Ver categorías de verificación	101
Ver verificaciones específicas	102
Filtrar sus verificaciones	104
Actualizar resultados de verificaciones	105
Descargar los resultados de la verificación	106
Vista organizativa	107
Preferencias	107
Comience con la Trusted Advisor API	109
Uso de Trusted Advisor como un servicio web	111

Obtener la lista de comprobaciones de Trusted Advisor disponibles	111
Actualizar la lista de comprobaciones de Trusted Advisor disponibles	112
Sondear una comprobación de Trusted Advisor para cambios de estado	112
Solicitar un resultado de comprobación de Trusted Advisor	115
Mostrar detalles de una verificación de Trusted Advisor	116
Vista organizativa de AWS Trusted Advisor	116
Requisitos previos	117
Habilitar la vista organizativa	118
Actualiza Trusted Advisor los cheques	119
Crear informes de vista organizativa	120
Ver el resumen del informe	124
Descargar un informe de vista organizativa	125
Desactivar la vista organizativa	131
Uso de políticas de IAM para permitir el acceso a la vista organizativa	132
Uso de otros AWS servicios para ver Trusted Advisor informes	135
Vea Trusted Advisor los cheques impulsados por AWS Config	145
Resolución de problemas	147
Vea los controles CSPM de su Security Hub en Trusted Advisor	148
Requisitos previos	149
Vea las conclusiones sobre el CSPM de Security Hub	150
Actualice sus hallazgos sobre el CSPM de Security Hub	152
Desactivar Security Hub CSPM desde Trusted Advisor	153
Resolución de problemas	153
Optar AWS Compute Optimizer por recibir Trusted Advisor cheques	157
Información relacionada	158
Comience con AWS Trusted Advisor Priority	158
Requisitos previos	160
Habilitar Trusted Advisor la prioridad	160
Ver recomendaciones priorizadas	160
Confirmación de una recomendación	163
Descartar una recomendación	166
Resolver una recomendación	168
Reapertura de una recomendación	170
Descargar detalles de las recomendaciones	172
Registro de administradores delegados	173
Anulación del registro de administradores delegados	173

Administra las notificaciones Trusted Advisor prioritarias	174
Deshabilita Trusted Advisor la prioridad	175
Trusted Advisor comprobar la referencia	175
Optimización de costos	177
Desempeño	241
Seguridad	296
Tolerancia a errores	348
Límites de los servicios	474
Excelencia operativa	494
Registro de cambios para AWS Trusted Advisor	541
Actualizaciones más antiguas	548
Nueva verificación: las copias de seguridad de Amazon RDS no están habilitadas	549
Nuevo cheque: AWS CloudTrail Registro de eventos de administración	550
Se actualizó la verificación de recursos del grupo de escalado automático	550
Se actualizó la verificación de acceso externo de IAM Access Analyzer.	551
Se agregó una verificación nueva.	551
Se actualizaron tres verificaciones	551
Se agregaron cuatro verificaciones	551
Se actualizaron tres verificaciones	552
Se agregaron nueve nuevas verificaciones	552
Se actualizó un control de seguridad y se agregó un control de seguridad	552
Se actualizaron seis controles de seguridad	553
Se actualizó una verificación de tolerancia a errores	553
Se actualizaron nueve verificaciones	553
Se eliminaron cinco verificaciones y se agregó una verificación	554
Se eliminaron verificaciones de tolerancia a errores	554
Nueva comprobación de tolerancia a errores	554
Se actualizó una verificación de tolerancia a errores y un control de seguridad	555
Nueva comprobación de tolerancia a errores	555
Verificación de tolerancia a errores actualizada	555
Controles de seguridad actualizados	555
Nuevas verificaciones de seguridad y rendimiento	555
Nuevo control de seguridad	556
Nuevas verificaciones de tolerancia a errores y de optimización de costos.	556
Nuevas comprobaciones de tolerancia a errores	556
Nuevas verificaciones para Amazon RDS	557

New AWS Trusted Advisor API	557
Trusted Advisor eliminación de cheques	557
Integración de AWS Config se registra en Trusted Advisor	558
Nuevas comprobaciones de tolerancia a errores	558
Nueva comprobación de límites de servicio	558
Nueva comprobación de tolerancia a errores	559
Nuevas comprobaciones de tolerancia a errores y de rendimiento	559
Nuevas comprobaciones de tolerancia a errores	559
Nuevas comprobaciones de tolerancia a errores	559
Expansión regional de las comprobaciones de tolerancia a errores de Amazon ECS	560
Nuevas comprobaciones de tolerancia a errores	560
Nuevas comprobaciones de tolerancia a errores	556
Actualizaciones de la Trusted Advisor integración con AWS Security Hub CSPM	561
Nuevas comprobaciones de tolerancia a errores para AWS Resilience Hub	556
Actualice a la Trusted Advisor consola	562
Nuevas comprobaciones para Amazon EC2	562
Se agregaron comprobaciones CSPM de Security Hub a Trusted Advisor	562
Se agregaron cheques de AWS Compute Optimizer	563
Actualizaciones de la comprobación de las claves de acceso expuestas	563
La actualización comprueba si AWS Direct Connect	564
AWS Security Hub CSPM controles agregados a la AWS Trusted Advisor consola	565
Nuevas comprobaciones para Amazon EC2 y AWS Well-Architected	566
Nombre de cheque actualizado para Amazon OpenSearch Service	566
Se han agregado verificaciones de almacenamiento de volúmenes de Amazon Elastic Block Store	567
Se agregaron cheques para AWS Lambda	567
Trusted Advisor comprobar la eliminación	568
Se han actualizado verificaciones de Amazon Elastic Block Store	568
Trusted Advisor eliminación de cheques	569
Trusted Advisor eliminación de cheques	570
Aplicación AWS Support en Slack	571
Requisitos previos	572
Gestione el acceso al widget de AWS Support la aplicación	573
Gestione el acceso a la AWS Support aplicación	574
Autorización de un espacio de trabajo de Slack	580
Autorización de varias cuentas	583

Configurar un canal de Slack	585
Actualización de la configuración del canal de Slack	590
Creación de casos de soporte en Slack	591
Responder a casos de soporte en Slack	597
Únase a una sesión de chat en vivo con AWS Support	599
Buscar casos de soporte en Slack	605
Utilice los resultados de búsqueda	607
Resolución de casos de soporte en Slack	609
Reapertura de casos de soporte en Slack	609
Elimina una configuración de canales de Slack de la aplicación AWS Support	610
Elimina una configuración de espacio de trabajo de Slack de la aplicación AWS Support	611
AWS Support Comandos de la aplicación en Slack	612
Comandos del canal de Slack	612
Comandos del canal de chat en vivo	613
Vea las correspondencias de la AWS Support aplicación en el AWS Support Center Console .	613
Crea AWS CloudFormation recursos para la AWS Support aplicación en Slack	614
AWS Support Aplicación y CloudFormation plantillas	615
Creación de recursos de configuración de Slack para su organización	615
Obtenga más información sobre CloudFormation	621
Cree recursos de AWS Support aplicaciones mediante Terraform	621
Seguridad	623
Protección de datos	624
Seguridad para casos de soporte	625
Identity and Access Management	626
Público	626
Autenticación con identidades	627
Administración del acceso con políticas	628
Cómo AWS Support funciona con IAM	629
Identity-based ejemplos de políticas	631
Cómo utilizar roles vinculados a servicios	634
AWS políticas gestionadas	642
Gestione el acceso a AWS Support Center	734
Gestione el acceso a AWS Support Planes	742
Gestione el acceso a AWS Trusted Advisor	746
Resolución de problemas	756
Respuesta a incidentes	759

Inicio de sesión y supervisión AWS Support and AWS Trusted Advisor	759
Validación de conformidad	760
Resiliencia	760
Seguridad de la infraestructura	761
Configuración y análisis de vulnerabilidades	761
Ejemplos de código	762
Conceptos básicos	763
Hola Soporte	764
Conceptos básicos	771
Acciones	829
Escenarios	905
Cómo empezar con Support	906
Supervisar y registrar para Soporte	915
Integrándose en AWS Support EDAs	915
EventBridge ¿ AWS Support Cómo direcciona los eventos	916
AWS Support eventos	916
Creación de patrones de eventos	917
Evento Actualización de caso de soporte	918
Registrar llamadas a la AWS Support API con AWS CloudTrail	922
AWS Support información en CloudTrail	922
AWS Trusted Advisor información al iniciar CloudTrail sesión	923
Descripción de las entradas de los archivos de AWS Support registro	924
Registrar las llamadas a AWS Support la API de la aplicación con CloudTrail	926
AWS Support Información sobre la aplicación en CloudTrail	926
Descripción de las entradas del archivo de registro de la AWS Support aplicación	928
Supervisión y registro de planes de Support	932
Registrar las llamadas a la API de AWS Support Plans con AWS CloudTrail	932
AWS Support La información del plan se encuentra en CloudTrail	933
Descripción de las entradas del archivo de registro de AWS Support Plans	934
Registrar las acciones de la consola para los cambios en tu Soporte plan	940
Supervisar y registrar para Trusted Advisor	944
Supervisar los resultados de los Trusted Advisor controles con EventBridge	945
Crear CloudWatch alarmas para monitorear Trusted Advisor las métricas	948
Requisitos previos	949
CloudWatch métricas para Trusted Advisor	953
Trusted Advisor métricas y dimensiones	959

- Registrar las acciones de la AWS Trusted Advisor consola con AWS CloudTrail 960
 - Trusted Advisor información en CloudTrail 961
 - Ejemplo: Trusted Advisor entradas de archivos de registro 964
- Recursos para la resolución de problemas 968
 - Solución de problemas específicos del servicio 968
- Historial de revisión 973
 - Actualizaciones anteriores 1024
- mxxviii

Introducción al AWS Support

AWS Support ofrece una gama de planes que brindan acceso a herramientas y experiencia que respaldan el éxito y la salud operativa de sus AWS soluciones. Todos los planes de soporte ofrecen acceso ininterrumpido al servicio de atención al cliente, a la AWS 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.

Important

Aviso de fin de soporte: el soporte para desarrolladores se suspenderá el 1 de enero de 2027. Los clientes con soporte para desarrolladores pueden seguir usando su plan actual o optar por actualizarse a Business Support+ en cualquier momento antes del 1 de enero de 2027. Business Support+ ofrece AI-powered asistencia que comprende el contexto de sus operaciones, con 24/7 acceso a AWS expertos a un precio 29/month mínimo de \$ por cuenta. Para obtener más información, consulta los detalles del [plan Business Support+](#)

Aviso de fin de soporte: el soporte empresarial se suspenderá el 1 de enero de 2027. Los clientes con Business Support pueden seguir usando su plan actual o optar por actualizarse a Business Support+ en cualquier momento antes del 1 de enero de 2027. Business Support + ofrece AI-powered asistencia que comprende el contexto de sus operaciones, con 24/7 acceso a AWS expertos a un precio 29/month mínimo de \$ por cuenta. Para obtener más información, consulta los detalles del [plan Business Support+](#)

Aviso de fin de soporte: el 1 de enero de 2027, AWS se suspenderá Enterprise. On-Ramp A lo largo de 2026, On-Ramp los clientes empresariales pasarán automáticamente a AWS Enterprise Support durante la renovación del contrato o en lotes periódicos. Los clientes recibirán una notificación por correo electrónico un mes antes de la actualización. No hay que hacer nada más. Enterprise Support proporciona una asignación de TAM designada, tiempos de respuesta de 15 minutos y Respuesta frente a incidencias de seguridad de AWS está disponible sin costo adicional, todo a un precio mínimo inferior de 5000\$ (reducido de 15 000\$). Para obtener más información, consulte los detalles del [Soporte plan AWS Enterprise](#). Para obtener más información, consulte [On-Ramp Fin del soporte para desarrolladores, empresas y empresas](#).

Developer Support, Business Support y Enterprise On-Ramp seguirán estando disponibles en la AWS GovCloud (US) región.

Notas

- Si desea crear una Soporte interacción que utilice la AI-generated solución de problemas para resolver su problema y, si lo desea, crear un caso de soporte, consulte [AI-enhanced solución de problemas en la consola del Support Center](#).
- Para obtener más información sobre los distintos AWS Support planes, consulte [Comparar AWS Support planes](#) y [Cambio AWS Support Planes](#).
- Los planes de soporte ofrecen diferentes tiempos de respuesta para sus casos. Consulte [Elegir un nivel de gravedad inicial para el caso de soporte](#) y [Descripción AWS Support tiempos de respuesta](#).

Temas

- [AI-enhanced solución de problemas en la consola del Support Center](#)
- [Reuniones virtuales con AWS Support](#)
- [Administración de casos](#)
- [Solicite un aumento de la cuota de servicio.](#)
- [Experiencia heredada: creación de casos de soporte y administración de casos](#)
- [Utilización AWS Support con un AWS SDK](#)

AI-enhanced solución de problemas en la consola del Support Center

AI-enhanced se admiten capacidades de solución de problemas que le ayudan a resolver los problemas de forma más rápida y eficiente Regiones de AWS. Si tiene un plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puede utilizar las funciones de la consola del Support Center para solucionar problemas técnicos, así como problemas de cuenta y facturación. Si tiene un Soporte plan Basic, puede utilizar las funciones de la consola del Support Center para solucionar problemas generales y obtener ayuda con problemas de cuenta y facturación. El uso AI-enhanced de la solución de problemas optimiza la experiencia de soporte al utilizar el reconocimiento contextual y el diagnóstico automatizado para ofrecer soluciones específicas para su AWS entorno.

AI-enhanced la solución de problemas en la consola del Support Center es compatible con lo siguiente Regiones de AWS:

- Región Este de EE. UU. (Norte de Virginia)
- Región del este de EE. UU. (Ohio)
- Región de Europa (Irlanda)

 Note

Si opera en una consola Región de AWS que no admite AI-enhanced las capacidades de la consola del Support Center, utilizará el método tradicional de administración de casos. Para obtener más información, consulte [Experiencia heredada: creación de casos de soporte y administración de casos](#).

Al acceder a la consola del Support Center, puede introducir la descripción del problema en lenguaje natural, importar las conversaciones relevantes de Amazon Q, recibir una guía generativa de solución de problemas de IA y optar por crear un caso de soporte con campos rellenados previamente, si es necesario.

Puede proporcionar información contextual sobre su entorno y su problema para recibir soluciones personalizadas durante todo el proceso de resolución de problemas.

AI-enhanced la solución de problemas en la AWS Support consola ofrece las siguientes ventajas clave:

- Resolución de problemas más rápida: obtenga respuestas inmediatas y soluciones relevantes tan pronto como describa su problema.
- Preservación del contexto: importe sus conversaciones anteriores de Amazon Q para mantener el contexto de la solución de problemas.
- Creación de casos simplificada: utilice un lenguaje natural para describir los problemas en lugar de navegar por varios campos del formulario.
- Seguimiento inteligente: reciba preguntas de seguimiento relevantes en función de su entorno específico AWS .
- AI-powered orientación sobre problemas técnicos, de facturación y de cuentas: la AI-enhanced solución de problemas proporciona recomendaciones contextuales sobre todos los tipos de

problemas admitidos. Para las preguntas sobre cuentas y facturación, la AI-enhanced solución de problemas muestra las respuestas pertinentes, te guía por las soluciones más comunes y te ayuda a navegar por la configuración de la cuenta. En el caso de los problemas técnicos, analiza el contexto de su entorno, formula preguntas de seguimiento específicas y proporciona una guía paso a paso para la solución de problemas basada en las AWS mejores prácticas, lo que le ayuda a resolver los problemas sin necesidad de crear un caso de soporte.

- Investigación autónoma de problemas operativos: en el caso de problemas operativos como la degradación del rendimiento, el aumento de las tasas de error o las regresiones posteriores a la implementación, los clientes pueden recurrir a los servicios de observabilidad de su cuenta [Agente de AWS DevOps](#) para consultar de forma autónoma los servicios de observabilidad de su cuenta, identificar la causa raíz y generar un plan de mitigación, transmitiendo el progreso directamente en su interacción de soporte. La primera vez que lo utilice, la consola del Support Center le solicitará su consentimiento explícito para activar el DevOps agente. Para obtener más información, consulta [Cómo usarlo Agente de AWS DevOps con tu AWS Support plan](#).

Para obtener una lista completa de las capacidades disponibles en su plan Support, consulte [Comparar AWS Support planes](#).

Notas

- Para cambiar el plan de soporte, consulte [Cambio AWS Support Planes](#).
- Para cerrar una cuenta, consulte [Cerrar una cuenta](#) en la Guía del AWS Billing usuario.
- Para encontrar temas comunes de solución de problemas Servicios de AWS, consulte [Recursos 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](#)

Important

Antes de iniciar una interacción de soporte o crear un caso de soporte, compruebe si hay eventos que afecten a los recursos de su cuenta visitando su Panel de estado dirección [https://phd.aws.amazon.com/phd/home #/](https://phd.aws.amazon.com/phd/home#/). Puedes comprobar cualquier Servicio de AWS problema en el panel de control, aunque es posible que se produzca un ligero retraso en la publicación de los incidentes. Si no estás seguro de si hay un incidente activo, abre un caso de soporte.

Temas

- [Configura los permisos para utilizar la AI-enhanced solución de problemas](#)
- [Cree una interacción de soporte](#)
- [Cree un caso de soporte a partir de una interacción de soporte](#)
- [Vea las interacciones de soporte](#)
- [Resolución de problemas](#)

Configura los permisos para utilizar la AI-enhanced solución de problemas

Para acceder a las funciones AI-enhanced de solución de problemas en Support Center, necesita AWS Identity and Access Management permisos específicos. En esta sección se describen los permisos de IAM necesarios y se explica cómo configurarlos para que pueda utilizar plenamente estas capacidades.

AI-enhanced la solución de problemas requiere permisos que van más allá de la administración tradicional de casos de soporte. Los permisos necesarios se dividen en cuatro categorías:

- Permisos de interacción de soporte: habilite el nuevo flujo de trabajo basado en interacciones en Support Center.
- AI-powered permisos de clasificación: permiten el acceso a las funciones de clasificación de AI-powered problemas.
- Permisos de integración de Amazon Q: habilita la importación de conversaciones desde Amazon Q Developer.
- Agente de AWS DevOps permisos: permite que el DevOps agente investigue las operaciones durante una interacción de soporte.

Estos permisos complementan los AWS Support permisos existentes y no los sustituyen.

Puedes configurar los permisos para AI-enhanced solucionar problemas de dos maneras:

[Opción 1: utilizar la política AWS gestionada \(recomendada\)](#). Adjunte la política AWSSupportAccess gestionada a sus usuarios o roles. Esta política incluye todos los permisos necesarios y se actualiza automáticamente cuando se lanzan nuevas Soporte funciones.

[Opción 2: cree una política personalizada con los permisos mínimos necesarios](#). Este enfoque le brinda más control, pero requiere actualizaciones manuales cuando se agregan nuevas funciones.

Opción 1: utilice la AWS política gestionada (recomendada)

Si actualmente tiene la política AWSSupportAccess gestionada adjunta, no se requieren permisos adicionales. Sin embargo, para seguir utilizando las funciones incluidas en la [API de Support Center Console](#), debe añadir las operaciones de Support Center Console a sus políticas de IAM antes del 2 de noviembre de 2026, si aún no las tiene. Para ello, actualice la política AWS Support gestionada para incluir las `support-console:*` acciones. Para obtener más información, consulte [Añadir políticas de IAM para las operaciones de la API de la consola del centro de soporte](#).

Opción 2: cree una política personalizada con los permisos mínimos necesarios

Puede permitir explícitamente incluir acciones específicas en una lista en lugar de utilizar caracteres comodín. Los siguientes son los permisos necesarios para las interacciones de soporte, la creación y la administración de casos:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "support:AddAttachmentsToSet",
        "support:AddCommunicationToCase",
        "support:CreateCase",
        "support:DescribeAttachment",
        "support:DescribeCaseAttributes",
        "support:DescribeCases",
        "support:DescribeCommunication",
```

```

    "support:DescribeCommunications",
    "support:DescribeCreateCaseOptions",
    "support:DescribeIssueTypes",
    "support:DescribeServices",
    "support:DescribeSeverityLevels",
    "support:DescribeSupportedLanguages",
    "support:DescribeSupportLevel",
    "support:GetInteraction",
    "support:InitiateCallForCase",
    "support:ListInteractionEntries",
    "support:ListInteractions",
    "support:InitiateChatForCase",
    "support:PutCaseAttributes",
    "support:ResolveCase",
    "support:ResolveInteraction",
    "support:SearchForCases",
    "support:StartInteraction",
    "support:UpdateInteraction",
    "support-console:GetAccountState",
    "support-console:GetAccountGovCloudEnabled",
    "support-console:GetCaseDraft",
    "support-console:CreateCaseDraft",
    "support-console>DeleteCaseDraft",
    "support-console:GetBanner",
    "support-console:DescribeDynamicHelp",
    "support-console:CreateContact",
  ],
  "Resource": "*"
}
]
}

```

Para Agente de AWS DevOps los permisos que requiere su identidad de IAM, adjunte las siguientes políticas AWS gestionadas:

- **AIDevOpsAgentFullAccess.** Proporciona acceso completo a las acciones de administración de DevOps agentes.
- **AIDevOpsAgentAccessPolicy.** Necesario para crear el espacio de agentes.
- **AIDevOpsOperatorAppAccessPolicy.** Necesario para habilitar el acceso a la aplicación Operator.

Para ver la lista completa de acciones, consulte los [permisos de IAM del DevOps agente](#) en la Guía del Agente de AWS DevOps usuario.

Su identidad de IAM debe `iam:PassRole` figurar en las `DevOpsAgentRole-WebappAdmin` funciones `DevOpsAgentRole-AgentSpace` y funciones para que la consola del Support Center pueda transferir estas funciones al DevOps agente al crearlas en su nombre durante la primera configuración. Para las investigaciones sobre los clústeres de Amazon Elastic Kubernetes Service, también es `eks:DescribeAccessEntry` necesaria `eks:CreateAccessEntry` su identidad de IAM y que la consola del Support Center `eks:AssociateAccessPolicy` pueda crear la entrada de acceso de solo lectura en el clúster de destino. Para obtener más información sobre las entradas de acceso, consulte [Otorgar a los usuarios de IAM acceso a Kubernetes con entradas de acceso de Amazon EKS](#) en la Guía del usuario de Amazon Elastic Kubernetes Service.

Note

El uso de una política personalizada requiere un mantenimiento continuo a medida que se lanzan nuevas funciones. AWS Support Para obtener más información sobre las operaciones de la API de Support Center Console, consulte [Añadir políticas de IAM para las operaciones de la API de la consola del centro de soporte](#). Para obtener más información sobre cada una de las operaciones de la Soporte API, consulte [Gestione el acceso a AWS Support Center](#).

Permisos necesarios para la integración de Amazon Q

Para utilizar la función de importación de conversaciones de Amazon Q en Support Center, las identidades de IAM necesitan permisos para las siguientes acciones de los desarrolladores de Amazon Q:

- `q:StartConversation`: Inicie una nueva conversación con Amazon Q.
- `q:SendMessage`: Envía mensajes dentro de una conversación.
- `q:GetConversation`: Recupera los detalles de la conversación. Esta acción es necesaria para acceder a la consola.
- `q:ListConversations`: Muestra las conversaciones disponibles. Esta acción es necesaria para el acceso a la consola y la integración del Support Center.

La integración de Amazon Q con Support Center Console requiere específicamente el `q:ListConversations` permiso para mostrar tus conversaciones recientes para importarlas. Para

obtener instrucciones detalladas sobre la configuración de los permisos de Amazon Q Developer, consulte la [referencia de permisos de Amazon Q Developer](#) y [Gestione el acceso a Amazon Q Developer con políticas](#).

Aplicar los permisos necesarios para las interacciones de soporte

Para aplicar permisos a sus usuarios de IAM, siga estos pasos:

1. Inicie sesión en la consola de IAM Consola de administración de AWS y ábrala en. <https://console.aws.amazon.com/iam/>
2. En el panel de navegación, seleccione Políticas y, a continuación, elija Crear política.
3. Seleccione la pestaña JSON y pegue uno de los documentos de política mencionados en las secciones anteriores.
4. Seleccione Siguiente: Etiquetas y, a continuación, Siguiente: Revisar.
5. Introduzca un nombre de política como, por ejemplo, SupportConsoleInteractionsAccess y proporcione una descripción que explique el propósito de la política.
6. Elija Crear política.
7. Adjunte la política a sus usuarios, grupos o funciones de IAM que necesiten acceder al Support Center.

Si ya tiene adjuntos a una política AWSSupportAccess gestionada, adjunte la política personalizada complementaria a la política gestionada.

Cree una interacción de soporte

Una interacción de apoyo es la forma en que comienza su participación AWS Support. Primero debes describir tu problema en un lenguaje natural y recibir asistencia personalizada para ti mediante la AI-enhanced solución de problemas. Tu interacción inicial puede incluir preguntas aclaratorias, soluciones contextuales y resolución automática de problemas, sin necesidad de crear un caso de soporte. Estas interacciones pueden resolver los problemas de forma independiente o servir de base para un caso de soporte que recurra a un ingeniero humano, si es necesario.

Soporte las interacciones difieren de los casos de soporte en que los casos de soporte incluyen la colaboración con un ingeniero de soporte en la nube. Puede optar por generar automáticamente un caso de soporte en función de una interacción de soporte previa. El caso de soporte mantiene todo el contexto de la interacción de soporte inicial e incluye AI-generated información adicional para

ayudar al ingeniero de soporte de la nube a resolver su problema. Esta poderosa combinación de AI-enhanced solución de problemas y asistencia de los ingenieros de AWS Cloud Support puede conducir a una resolución de problemas más rápida y a reducir el tiempo de inactividad.

Notas

- Para volver al método tradicional de administración de casos, seleccione Use the old experience en el banner situado en la parte superior de la consola del Support Center. Para obtener más información, consulte [Experiencia heredada: creación de casos de soporte y administración de casos](#).
- Puede iniciar sesión en la consola del Support Center como usuario AWS Identity and Access Management (IAM). Para obtener más información, consulte [Gestione el acceso a AWS Support Center](#).
- Si no puede iniciar sesión en la consola del Support Center y crear un caso de soporte, puede utilizar la página de [contacto](#) en su lugar. Puede utilizar esta página para obtener ayuda con problemas relacionados con las cuentas y la facturación.

Para iniciar una interacción de soporte, complete los siguientes pasos:

1. Inicie sesión en la [AWS Support Center Console](#).

Tip

En Consola de administración de AWS, también puede elegir el icono del signo de interrogación



y, a continuación, elegir Support Center.

2. Dispone de varias opciones para iniciar su interacción de soporte:
 - Introduzca los detalles sobre los problemas con los que necesita ayuda. Así es como se inicia una nueva interacción de soporte. Introduzca información detallada sobre el problema y cualquier paso de solución de problemas que ya haya tomado.
 - Continúe con una interacción de soporte existente: elija una de las interacciones de soporte recientes que se muestran en la sección Describa su problema o continúe con ella. En esta sección se muestran las dos interacciones de soporte más recientes. Acceda a la sección

Visualización de interacciones de soporte anteriores para ver otras interacciones de soporte anteriores.

- Usa una transcripción de Amazon Q: selecciona el icono de Amazon Q en el campo de texto para ver una lista de las conversaciones recientes de Amazon Q. Región de AWS Se muestran las cinco conversaciones más recientes de AWS GovCloud (US-East). O bien, elige una de las interacciones recientes de Amazon Q que se muestran en la sección Describe tu problema o continúa con. Al seleccionar una conversación, se genera un resumen de esa conversación y se añade al cuadro de texto. Si seleccionas una conversación de Amazon Q, verás un aviso legal sobre la accesibilidad de Región de AWS los usuarios.
3. Selecciona el icono Enviar en la parte inferior derecha del campo de texto.
 4. AWS Support La solución generativa AI-powered de problemas analiza su consulta junto con su AWS entorno específico. Es posible que se le pida que proporcione información adicional para facilitar el análisis. Si aparece una solicitud de información adicional, introduzca los datos solicitados y, a continuación, pulse Enviar. Si no conoces o no tienes acceso a la información solicitada, puedes saltarte este paso y, en su lugar, recibir una respuesta orientativa general. La respuesta a una guía general no es específica de su AWS entorno.

En el caso de problemas operativos, como la degradación del rendimiento, el aumento de las tasas de error o las regresiones posteriores [Agente de AWS DevOps](#) la implementación, la AI-enhanced solución de problemas puede requerir una investigación autónoma del entorno. DevOps El agente consulta los servicios de observabilidad de tu cuenta (Amazon CloudWatch AWS CloudTrail, AWS X-Ray, AWS Config, y otros) para identificar la causa raíz y proponer un plan de mitigación. Si su cuenta aún no tiene el DevOps agente configurado, se le pedirá que apruebe la creación de los recursos necesarios antes de que comience la investigación. El progreso se refleja directamente en tu interacción de soporte.

Cuando se complete el análisis, verá un resumen de los hallazgos, junto con las medidas correctivas. En el caso de las investigaciones sobre los DevOps agentes, el resumen incluye los síntomas, la causa raíz, las deficiencias en la investigación y un plan de mitigación. Para ver las fuentes utilizadas en los pasos de análisis y corrección, seleccione Fuentes.

5. Si necesita más ayuda, puede completar una de las siguientes opciones:
 - Continúe con el AI-assisted soporte: para refinar aún más el AI-assisted análisis y generar una nueva respuesta, elija Agregar más detalles para obtener una mejor respuesta. Introduzca la información en el campo Detalles adicionales y, a continuación, seleccione Enviar. Tenga en cuenta que esta opción proporciona un contexto adicional para el problema original. Si

necesita introducir el contexto de una nueva edición, seleccione **Iniciar una nueva interacción** en la parte superior o inferior de la pantalla.

- **Crear un caso de soporte:** para crear un caso de soporte con AWS Support, selecciona **Crear un caso**. Esta opción inicia el flujo de trabajo de creación de casos. Muchos de los detalles del caso se rellenan automáticamente en función de su interacción con el servicio de asistencia. Puede cambiar esta información según sea necesario. Su interacción de soporte, incluidos los detalles de cualquier paso de resolución proporcionado, se agrega al caso de soporte. Para obtener más información sobre cómo crear un caso de soporte, consulte [Cree un caso de soporte a partir de una interacción de soporte](#).

En cualquier momento de la interacción de asistencia, puedes usar los íconos del pulgar hacia arriba y el pulgar hacia abajo para enviar comentarios sobre tu experiencia.

Cree un caso de soporte a partir de una interacción de soporte

Al seleccionar **Crear caso** durante la interacción de soporte, se crea un caso de soporte para usted con muchos de los detalles del caso, como el asunto, la descripción, el tipo de caso, el servicio, la categoría y el nivel de gravedad. Puede cambiar esta información según sea necesario. Asegúrese de revisar esta información para comprobar su precisión. Para obtener información sobre cómo elegir un nivel de gravedad para su caso, consulte [Elegir un nivel de gravedad inicial para un caso de apoyo](#).

Important

Antes de crear un caso de soporte, visita tu página para comprobar si hay algún suceso que afecte a los recursos de tu cuenta [Panel de estado](#). Puedes verificar cualquier Servicio de AWS problema en el panel de control. Es posible que se produzca un ligero retraso en la publicación de los incidentes. Si no estás seguro de si hay un incidente activo, abre un caso de soporte.

Tras seleccionar **Crear caso**, introduce o verifica la siguiente información:

1. Verifique el asunto de este caso de soporte. El tema es una breve sinopsis de lo que trata su interacción de apoyo.
2. Verifica la descripción. La consulta inicial aparece en el campo Descripción. Modifique esta información según sea necesario. 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.

3. (Opcional) Elija 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.
4. En Tipo de caso, elija una de las siguientes opciones:
 - Cuenta y facturación
 - Técnico
 - Cuotas de servicio. Solo puede solicitar ciertos tipos de aumentos de la cuota de servicio desde la consola Support Center. Para obtener más información, consulte [Solicite un aumento de la cuota de servicio](#).

 Note

Si tienes un Soporte plan básico, no puedes crear un caso de soporte técnico.

5. Verifica el servicio, la categoría y la gravedad.
6. En la sección de preferencias de comunicación, indique cómo AWS desea comunicarse con usted. Puede elegir una de las siguientes opciones:
 - a. Correo electrónico: reciba una respuesta a su correo electrónico.
 - b. 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
 - c. Chat: inicie un chat en vivo con un agente de soporte. Si no puede conectarse a un chat, consulte [Resolución de problemas](#).

(Opcional) Si tiene un plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puede introducir hasta 10 direcciones de correo electrónico adicionales en los 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 la dirección de correo electrónico y la contraseña de su cuenta raíz, no es necesario que la incluya.

Note

Si tiene el plan de soporte Basic, la opción Additional contacts (Contactos adicionales) no está disponible. Sin embargo, el contacto de operaciones especificado en la sección Contactos alternativos de la página Mi cuenta recibe copias de la correspondencia del caso, pero solo para los tipos de cuenta y facturación específicos del caso.

7. Cuando esté listo para enviar el caso de soporte, seleccione Enviar. Se le dirigirá a la página de detalles del caso, donde podrá ver los detalles del caso, la interacción con el soporte y la correspondencia entre los casos.

Seleccione Detalles del caso para ver la información sobre su caso, como los archivos adjuntos o el nivel de gravedad. Seleccione Interacciones de soporte para ver las interacciones de soporte asociadas a este caso.

Mejores prácticas y tiempos de respuesta previstos para los casos de Enterprise Support

Antes de crear un caso de soporte, visite su página para comprobar si hay algún suceso que afecte a los recursos de su cuenta [Panel de estado](#). Puedes verificar cualquier Servicio de AWS problema en el panel de control. Es posible que se produzca un ligero retraso en la publicación de los incidentes. Si no estás seguro de si hay un incidente activo, abre un caso de soporte.

Al crear tu caso de soporte, asegúrate de elegir el nivel de gravedad correcto y de proporcionar la mayor cantidad de información posible. Para obtener más información sobre el tipo de información que debe proporcionarse, consulte la siguiente sección de prácticas recomendadas para casos de Enterprise Support.

Utilice la siguiente matriz para ayudarlo a identificar la gravedad correcta.

AWS ITIL Case Severity Matrix				
Urgency				
		Low	Medium	High
Impact	Low	Low	Normal	High
	Medium	Normal	High	Urgent
	High	High	Urgent	Critical

Para casos críticos o urgentes, asegúrese de dejar sus datos de contacto para que podamos ponernos en contacto con usted si es necesario.

Note

La forma más rápida de obtener ayuda es utilizar el método de contacto por chat o teléfono.

Temas

- Tiempos de respuesta objetivos para casos de Enterprise Support
- Mejores prácticas de Enterprise Support
- Ruta de escalación de Enterprise Support

Tiempos de respuesta objetivos para casos de Enterprise Support

El siguiente gráfico muestra los tiempos de AWS Support respuesta esperados para los diferentes niveles de gravedad de los casos.

ITIL Priority	Severity Level	How to Raise		Examples for reference
Critical	Business Critical System Down		15 minutes	Major outage; loss of entire enterprise or customer base. Has potential for large revenue loss or business risk.
Urgent	Production System Down		1 hour	Business significantly impacted, where important functions or applications aren't available.
High	Production System Impaired		4 hours	Critical functions of your applications are impaired or degraded.
Normal	System Impaired		12 hours	Non-critical applications are behaving abnormally; time-sensitive development question.
Low	General Guidance		24 hours	General development/ service questions or want to submit feature request.

Mejores prácticas de casos de Enterprise Support

Envíe su caso de soporte con el nivel de gravedad adecuado.

- El nivel de gravedad adecuado ayuda a garantizar que su caso sea visible en todas partes AWS y permite que el TAM gestione el problema.
- Envíe solo un caso por cada evento o problema.
- Asegúrese de plantear los casos de la forma correcta Cuenta de AWS.

Proporcione la mayor cantidad de información detallada posible, respondiendo a las preguntas relevantes que se proporcionan en la siguiente lista:

- **Quién:** ¿Quién hizo qué? ¿Quién está afectado? ¿Quién debería estar informado? ¿Con quién has hablado ya?
- **Qué:** Qué pasó, exactamente. ¿Cuál es el radio del impacto o de la explosión? ¿Qué es lo que ya has intentado para resolver el problema?
- **Cuándo:** ¿Cuándo ocurrió o ocurrirá (fecha, hora, zona horaria)? ¿Cuándo necesita una respuesta antes?
- **Dónde:** zona de disponibilidad Región de AWS, identificadores específicos de instancia o recurso y otros identificadores.
- **Por qué:** ¿Por qué abre este caso (información, aumento del límite, análisis de eventos o RCA, interrupción)?
- **Cómo:** incluye información sobre cómo reproducir el problema, cómo agravarlo y cómo ponernos en contacto contigo.

 Note

Puedes cambiar la gravedad de tu caso de soporte después de crearlo. Para obtener información, consulte [Cambiar el nivel de gravedad de su caso de soporte](#).

Enterprise Support, sistema crítico para la empresa o de producción inactivo

- Para los Business-critical casos de caída del sistema o de producción, utilice el chat o el teléfono y asegúrese de que haya personas disponibles en su organización para resolver el caso.
- Describa claramente el problema, incluyendo lo que ha intentado, lo que espera y el contexto. Resuma el impacto empresarial.
- Proporcione (o comience a capturar) tantas métricas, tiempos y síntomas como pueda. Más datos se traduce en un diagnóstico más rápido.
- Proporcione un puente para conferencias. Al resolver un problema de inactividad Business-critical del sistema, proporcione un puente de conferencia para que los equipos de soporte se unan para ayudar a solucionar el problema. Como los problemas de desconexión del Business-critical sistema son una pérdida de producción, lo mejor es que todos hablen por teléfono y elaboren un plan de acción común para resolverlo.

- Asegúrese de incluir toda la actividad relacionada con el evento en el caso de soporte (actualización desde la consola, no por correo electrónico). La opción de teléfono es buena para las comunicaciones en tiempo real; sin embargo, asegúrate de registrar las actualizaciones y los resultados en el caso de soporte.

Ruta de escalación de Enterprise Support

Puede seguir el siguiente proceso paso a paso cuando se enfrente a un problema.

1. Compruebe Panel de estado si cree que el problema podría estar relacionado con un Servicio de AWS funcionamiento anormal.
2. Evalúe la información del caso tal como se describe en la sección Support Case Best Practices anterior.
3. Seleccione la gravedad adecuada y utilice el teléfono o el chat si necesita una respuesta rápida.
4. Póngase en contacto con su TAM si necesita ayuda adicional o si no recibe la respuesta esperada.

Vea las interacciones de soporte

Las interacciones pasadas con AWS Support se guardan durante 10 años. Puede ver las interacciones pasadas desde su Soporte panel de control seleccionando el icono de lista. Luego, elige la interacción que desees ver. Aparecen los detalles de la AWS Support interacción. Si eliges crear un caso de soporte a partir de una interacción, la interacción ya no aparecerá en tu lista de interacciones anteriores. La interacción ahora se muestra en la página de detalles del caso de soporte asociado.

Puede añadir detalles adicionales a la interacción para generar una nueva respuesta. O bien, puede elegir crear un Soporte caso a partir de la interacción seleccionando Crear un caso en la pantalla de detalles de la AWS Support interacción.

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 obtener 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

Para AWS GovCloud (US), el punto final es `*.connect-fips.us-east-1.amazonaws.com`.

- El firewall admite conexiones de socket web.

Si sigues sin poder conectarte a la ventana de chat, comunícate AWS Support mediante las opciones de contacto por correo electrónico o teléfono.

Reuniones virtuales con AWS Support

Las reuniones virtuales le permiten conectarse con los AWS Support ingenieros a través de videollamadas con funciones de pantalla compartida. Esta función le ayuda a resolver problemas técnicos complejos que requieren una demostración visual o una colaboración en tiempo real.

Cuando un ingeniero de soporte determine que su caso requiere asistencia visual, puede iniciar una reunión virtual. Recibirá una invitación a una reunión en la página de detalles de su caso en el

AWS Support Center. Tras aceptar la invitación, se unirá a una videollamada segura en la que podrá compartir su pantalla y colaborar con el ingeniero de soporte.

Las reuniones virtuales se integran con Connect Customer y utilizan la tecnología WebRTC para ofrecer videoconferencias seguras basadas en el navegador sin necesidad de instalar software adicional.

[Las reuniones virtuales solo están disponibles en el anuncio. Regiones de AWS](#)

Temas

- [Únase a una reunión virtual](#)
- [Seguridad y privacidad durante la reunión virtual](#)
- [Permisos de IAM necesarios para las reuniones virtuales](#)
- [Solución de problemas de reuniones virtuales](#)

Únase a una reunión virtual

Las reuniones virtuales las inicia el AWS Support ingeniero que le ayuda con su caso de soporte. Para unirse a una reunión virtual, complete los siguientes pasos.

1. Cuando un ingeniero de soporte inicia una reunión virtual, verá una invitación a la reunión en la página de detalles del caso de su caso de soporte. Para unirse a la reunión, seleccione Unirse a la reunión virtual para aceptar la invitación.

Las invitaciones a las reuniones caducan a los 10 minutos. Si no se une dentro de este plazo, solicite una nueva reunión a su ingeniero de soporte.

2. Otorgue permisos de navegador para acceder a la cámara y al micrófono cuando se le solicite.

La reunión virtual se abre en una ventana nueva y ya está conectado con el ingeniero de soporte. Puede silenciar y volver a silenciar el micrófono o desconectarse de la reunión mediante los botones de la parte inferior de la pantalla.

Seguridad y privacidad durante la reunión virtual

Las reuniones virtuales utilizan los mismos mecanismos de autenticación y autorización que otras AWS Support operaciones. Las siguientes medidas de seguridad protegen sus reuniones:

- Validación de la titularidad de los casos: solo puede unirse a las reuniones de los casos que le pertenezcan Cuenta de AWS.
- AWS Identity and Access Management Control de acceso basado en (IAM): debe tener los permisos de IAM adecuados para unirse a las reuniones virtuales.
- Conexiones cifradas: todos los datos de las reuniones se transmiten a través de conexiones WebRTC cifradas.
- Registro de auditoría: todas las actividades de las reuniones se registran con AWS CloudTrail fines de cumplimiento y auditoría.

 Important

Las reuniones virtuales se graban con fines de garantía de calidad y formación. No comparta información confidencial, como contraseñas o claves de acceso, durante la reunión.

Permisos de IAM necesarios para las reuniones virtuales

Para unirse a las reuniones virtuales, su usuario o rol de IAM debe tener el siguiente permiso:

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

Para obtener más información sobre AWS Support los permisos, consulte [Gestione el acceso a AWS Support Center](#).

Solución de problemas de reuniones virtuales

No puedo ver la invitación a la reunión.

Compruebe que su ingeniero de soporte haya iniciado la reunión. Actualice la página de detalles del caso. Si la invitación sigue sin aparecer, ponte en contacto con tu ingeniero de soporte a través de la correspondencia sobre el caso.

La invitación a la reunión ha caducado.

Las invitaciones a reuniones caducan a los 10 minutos por motivos de seguridad. Solicite una nueva invitación a una reunión a su ingeniero de soporte.

Tengo problemas de conexión.

Compruebe la conexión a Internet. Asegúrese de que la configuración de seguridad de su red o firewall permita el tráfico WebRTC. Intente utilizar un navegador o una conexión de red diferentes.

Recibo un error de autorización.

Compruebe que su usuario o rol de IAM tenga permisos para la acción `support:InitiateLiveContactForCase`.

Administración de casos

Note

Para volver al método tradicional de administración de casos, seleccione *Use the old experience* en el banner situado en la parte superior de la consola del Support Center. Para obtener más información, consulte [Experiencia heredada: creación de casos de soporte y administración de casos](#).

En el Consola de administración de AWS, puede crear tres tipos de casos de clientes en Soporte:

- 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 Basic Support, no puede crear un caso de soporte técnico.

Notas

- Para cambiar el plan de soporte, consulte [Cambio AWS Support 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, consulte [Recursos 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](#)

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.

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

Elegir un nivel de gravedad inicial para el caso de soporte

Al crear un caso de soporte, asegúrese de definir la gravedad correcta y de proporcionar la mayor cantidad de información posible.

Es posible que desee crear un caso de soporte con la máxima gravedad que permita su plan de soporte. Sin embargo, se recomienda que elija la máxima gravedad solo para los casos que no puedan solucionarse o que afecten directamente a las aplicaciones de producción. Para obtener información sobre cómo crear sus servicios de manera que la pérdida de un solo recurso no afecte a sus aplicaciones, consulte el paper AWS técnico [Building Fault-Tolerant Applications on](#).

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

 Notas

- Si tiene un plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puede reasignar el nivel de gravedad de los casos de soporte para reflejar los cambios en la urgencia y el impacto empresarial. Por ejemplo, puede cambiar su caso de soporte, de Tener problemas con el sistema a Tener problemas con el sistema de producción. Cuando cambias la gravedad del caso, AWS Support recibe una notificación y distribuye el caso de acuerdo con el nuevo nivel de gravedad. Para obtener más información, consulte [Cambiar el nivel de gravedad de su caso de soporte](#).
- Si tienes un Soporte plan básico, no podrás cambiar el nivel de gravedad de un caso de soporte después de crearlo. Si tu situación cambia, trabaja con el Soporte agente.
- Para obtener más información sobre el nivel de gravedad, consulte la [Referencia de la API de AWS Support](#).

Gravedad	Código del nivel de gravedad	First-res ponse hora	Descripción y plan de soporte
General guidance	low	24 horas	Tiene una pregunta de desarrollo general o quiere solicitar una característica. (plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations)
System impaired	normal	12 horas	Non-critical las funciones de su aplicación se comportan de forma anormal o tiene una pregunta de desarrollo urgente. (plan AWS

Gravedad	Código del nivel de gravedad	First-response hora	Descripción y plan de soporte
			Business Support+, AWS Enterprise Support o AWS Unified Operations)
Production system impaired	high	4 horas	Las funciones importantes de su aplicación se han deteriorado o degradado. (plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations)
Production system down	urgent	1 hora	Su negocio se ve afectado significativamente . Funciones importantes de su aplicación no están disponibles. (plan AWS Business Support +, AWS Enterprise Support o AWS Unified Operations)

Gravedad	Código del nivel de gravedad	First-response hora	Descripción y plan de soporte
Business-critical sistema inactivo	critical	• AWS Business Support +: menos de 30 minutos • AWS Enterprise Support: menos de 15 minutos • AWS Operaciones unificadas: 5 minutos a cargo de un ingeniero de gestión de incidentes	Su empresa está en riesgo. Funciones críticas de su aplicación no están disponibles.

Descripción AWS Support tiempos de respuesta

AWS Support hace todos los esfuerzos razonables para responder a su solicitud inicial dentro del plazo indicado. Para obtener información sobre el alcance del soporte de cada Soporte plan, consulte [AWS Support las características](#).

Si tiene un plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, tiene acceso ininterrumpido al soporte técnico.

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 servicio de atención al cliente para casos de soporte no técnico, el soporte en japonés está disponible durante el horario laboral en Japón, definido como 09:00 a.m. a 6:00 p.m., hora estándar de Japón (GMT+9), excepto festivos y fines de semana.
- Si tiene un plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, el soporte técnico está disponible durante todo el día, todos los días en japonés.

Si eliges el chino como idioma de contacto preferido para los casos de asistencia, es posible que la asistencia en chino esté 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 AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, el soporte técnico está disponible durante todo el día, todos los días 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 AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, el soporte técnico está disponible durante todo el día, todos los días en coreano.

Si elige el turco como idioma de contacto preferido para los casos de asistencia, es posible que la asistencia en turco esté disponible de la siguiente manera:

- Si necesitas atención al cliente para casos de asistencia no técnica, la asistencia en turco está disponible durante el horario laboral de Turquía, de 09:00 a 18:00 (GMT+3), excepto festivos y fines de semana.
- Si tiene un plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, el soporte técnico está disponible durante todo el día, todos los días en inglés.

Cambiar el nivel de gravedad de su caso de soporte

Si tiene un plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puede reasignar el nivel de gravedad de los casos de soporte para reflejar los cambios en la urgencia y el impacto empresarial. Por ejemplo, puede cambiar su caso de soporte, de Tener problemas con el sistema a Tener problemas con el sistema de producción. Cuando cambias la gravedad del caso, AWS Support recibe una notificación y atiende el caso de acuerdo con el nuevo nivel de gravedad.

Note

Los casos de cuentas o facturación en japonés (JP), de solicitud de aumento de Service Quotas (SQIR) y los casos de cuentas o facturación en turco (TR) creados en estos idiomas tienen una gravedad predeterminada y no se pueden cambiar.

Para cambiar la gravedad de un caso de asistencia, siga los siguientes pasos:

1. Inicie sesión en la [AWS Support Center Console](#).

Tip

En Consola de administración de AWS, también puede elegir el icono del signo de interrogación



y, a continuación, elegir Support Center.

2. Seleccione el caso para el que desee cambiar el nivel de gravedad.
3. En Detalles del caso, seleccione el icono del lápiz situado junto al campo de gravedad, como se muestra en el siguiente ejemplo.

Case details

Subject	
Case ID	
Created	2025-04-24T08:49:10.815Z
Case type	Technical

Status	Unassigned
Severity	General guidance
Category	-
Language	Portuguese

4. En Gravedad, elija el nuevo nivel de gravedad entre las siguientes opciones:
 - General guidance
 - System impaired
 - Production system impaired
 - Production system down
 - Business-critical sistema inactivo
5. En Motivo del cambio de gravedad de un caso, elija entre las opciones disponibles por las que va a cambiar la gravedad del caso.
6. (Opcional) En Cuéntenos más, introduzca información adicional sobre este cambio.
7. Realice una de las siguientes acciones:
 - Si quiere reducir la gravedad de los casos de soporte o si va a elevarlos de la guía general a Tener problemas con el sistema o Tener problemas con el sistema de producción, seleccione Actualizar.
 - Si está aumentando la gravedad de la caída del sistema de producción o la caída del Business-critical sistema, utilice una de las opciones de la sección Métodos de contacto para interactuar y AWS Support, a continuación, seleccione Actualizar. El siguiente ejemplo muestra las opciones disponibles en la sección Métodos de contacto.

Change case severity ✕

Severity

Production system down ▼

Reason for case severity change

- ▼

Tell us more - optional

Tell us more about the reason for the escalation

Contact methods [Info](#)

For high severity issues we recommend using our live contact mechanisms

Web ☐
We'll respond by email and Support Center.

Chat(Recommended) ☒
Chat online with a representative.

Phone(Recommended) ☐
We'll call you back at your number.

[Cancel](#) [Update](#)

Note

- Si cambias la gravedad de tu caso de soporte a un sistema de producción Business-critical inactivo o inactivo, debes esperar 60 minutos antes de poder volver a cambiar la gravedad.
- Si tu caso de soporte está actualmente configurado para que el Business-critical sistema esté inactivo, se te pedirá que inicies un contacto directo con él AWS Support en lugar de asignarle una gravedad mayor.
- Si va a aumentar el nivel de gravedad del caso de soporte después de haberlo aumentado al menos una vez, es posible que se encuentre con un período de espera. Por ejemplo, si cambia la gravedad de Tener problemas con el sistema a Tener problemas con el sistema de producción a las 6:00 de la mañana, entonces el caso de soporte estará por debajo del nivel de 4 horas de primera respuesta para el nivel de gravedad Tener problemas con el sistema de producción. En este escenario, puede volver a actualizar el nivel de gravedad a las 10:00 de la mañana, una vez transcurrido el período de 4 horas. Para ver una lista de los tiempos de primera respuesta para cada nivel de gravedad, consulte la tabla de [Descripción AWS Support tiempos de respuesta](#).

Solicite un aumento de la cuota de servicio.

Puede solicitar aumentos de las cuotas de servicio (anteriormente denominadas límites) para satisfacer sus requisitos de carga de trabajo.

Utilice el servicio Service Quotas para solicitar aumentos directamente para sus servicios. Para obtener más información, consulte la siguiente documentación sobre :

- [¿Qué es Service Quotas?](#) en la Guía del usuario de Service Quotas.
- [Solicitud de aumento de cuota](#) en la Guía del usuario de Service Quotas

En este momento, Service Quotas no admite cuotas de servicio Servicios de AWS en general Regiones de AWS. Si Región de AWS está disponible Servicio de AWS o no en la [consola de Service Quotas](#), complete los siguientes pasos para crear un caso de soporte para solicitar el aumento de cuota:

1. Inicie sesión en la [AWS Support Center Console](#).

Tip

En Consola de administración de AWS, también puede elegir el icono del signo de interrogación



y, a continuación, elegir Support Center.

2. En la página de interacciones de Support, introduzca los detalles sobre este aumento del límite de servicio. Cuando se le solicite, elija Crear un caso. Muchos de los campos del Soporte caso se rellenarán previamente con el texto que ingresó durante la interacción. Puede editar estos campos según sea necesario. Para obtener información adicional sobre la creación de una interacción de soporte, consulte [Cree una interacción de soporte](#).
3. Para el tipo de caso, seleccione Cuotas de servicio.
4. En Servicio, selecciona Aumentar el límite de servicio.
5. En Categoría, selecciona de la lista el tipo de aumento que vas a solicitar. Aquí solo se muestran las solicitudes de aumento del límite de servicio disponibles en Support Center. Para otros tipos de solicitudes de límite de servicio, consulte [Solicitar un aumento de cuota](#) en la Guía del usuario de Service Quotas.

6. (Opcional) En el menú desplegable Idioma de contacto preferido, selecciona el idioma que deseas AWS Support usar cuando te comuniques contigo.
7. Para la región, selecciona el Región de AWS lugar en el que deseas solicitar el aumento.

 Note

Región de AWS la selección no está disponible si seleccionó General como categoría.

8. (Opcional) Para solicitar varios aumentos de límites, seleccione Añadir otro límite y, a continuación, elija otra Región de AWS.
9. Introduzca una descripción para este aumento o varios aumentos de la cuota de servicio. Si es necesario, puede adjuntar archivos.
10. Elija Siguiente paso: Resuelva ahora o póngase en contacto con nosotros.
11. En Opciones de contacto, elija 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:
 - Country/Region
 - Número de teléfono
 - (Opcional) Extensión
12. Cuando estés listo para enviar el caso de soporte, selecciona Enviar. Se le dirigirá a la página de detalles del caso, donde podrá ver los detalles del caso, la interacción con el soporte y la correspondencia entre los casos.

Seleccione Detalles del caso para ver la información sobre su caso, como los archivos adjuntos o el nivel de gravedad. Seleccione Interacciones de soporte para ver las interacciones de soporte asociadas a este caso.

Experiencia heredada: creación de casos de soporte y administración de casos

Important

Para volver al método tradicional de administración de casos, seleccione **Use the old experience** en el banner situado en la parte superior de la consola del Support Center.

En el Consola de administración de AWS, puede crear tres tipos de casos de clientes en Soporte:

- 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 Basic Support, no puede crear un caso de soporte técnico.

Notas

- Para cambiar el plan de soporte, consulte [Cambio AWS Support 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, consulte [Recursos 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 Consola de administración de AWS.

Notas

- Puede iniciar sesión en Support Center como usuario AWS Identity and Access Management (IAM). Para obtener más información, consulte [Gestione el acceso a AWS Support Center](#).
- 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 Consola de administración de AWS, también puede elegir el icono del signo de interrogación



y, a continuación, elegir Support Center.

2. Seleccione Crear caso.
3. Elija una de las siguientes opciones:
 - Cuenta y facturación
 - Técnico
 - Para aumentar la cuota de servicios, elija ¿Busca aumentos del límite de servicio? y siga las instrucciones para [Solicite un aumento de la cuota 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:
 - Consola de administración de AWS
 - 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 AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, aparece la opción 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.

Elegir un nivel de gravedad inicial para el caso de soporte

Es posible que desee crear un caso de soporte con la máxima gravedad que permita su plan de soporte. Sin embargo, se recomienda que elija la máxima gravedad solo para los casos que no puedan solucionarse o que afecten directamente a las aplicaciones de producción. Para obtener información sobre cómo crear sus servicios de manera que la pérdida de un solo recurso no afecte a sus aplicaciones, consulte el paper AWS técnico [Building Fault-Tolerant Applications on](#).

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

 Notas

- Si tiene Enterprise Support o un On-Ramp plan Enterprise, puede reasignar el nivel de gravedad de su caso de soporte para reflejar los cambios en la urgencia y el impacto empresarial. Por ejemplo, puede cambiar su caso de soporte, de Tener problemas con el sistema a Tener problemas con el sistema de producción. Al cambiar la gravedad del caso, AWS Support recibe una notificación y distribuye el caso de acuerdo con el nuevo nivel de gravedad. Para obtener más información, consulte [Cambiar el nivel de gravedad de su caso de soporte](#).
- Si no tienes soporte empresarial ni un On-Ramp plan empresarial, no puedes cambiar el nivel de gravedad de un caso de soporte después de crearlo. Si tu situación cambia, trabaja con el Soporte agente para tu 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	First-response hora	Descripción y plan de soporte
General guidance	low	24 horas	Tiene una pregunta de desarrollo general o quiere solicitar una característica. (*Plan

Gravedad	Código del nivel de gravedad	First-response hora	Descripción y plan de soporte
			para desarrolladores, AWS Business Support +, Enterprise AWS Support o AWS Unified Operations)
System impaired	normal	12 horas	Non-critical las funciones de su aplicación se comportan de forma anormal o tiene una pregunta de desarrollo urgente. (*Plan para desarrolladores, AWS Business Support +, Enterprise AWS Support o AWS Unified Operations)
Production system impaired	high	4 horas	Las funciones importantes de su aplicación se han deteriorado o degradado. (plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations)
Production system down	urgent	1 hora	Su negocio se ve afectado significativamente . Funciones importantes de su aplicación no están disponibles. (plan AWS Business Support +, AWS Enterprise Support o AWS Unified Operations)
Business-critical sistema inactivo	critical	15 minutos	Su empresa está en riesgo. Hay funciones críticas de su aplicación que no están disponibles (plan de soporte Enterprise). Tenga en cuenta que son 30 minutos para el plan Enterprise On-Ramp Support.

Descripción AWS Support tiempos de respuesta

AWS Support hace todos los esfuerzos razonables para responder a su solicitud inicial dentro del plazo indicado. Para obtener información sobre el alcance del soporte de cada Soporte plan, consulte [AWS Support las características](#).

Si tiene un plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, tiene acceso ininterrumpido al soporte técnico. *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 Consola de administración de AWS.

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 AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, el soporte técnico está disponible durante todo el día, todos los días 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 AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, el soporte técnico está disponible durante todo el día, todos los días 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 AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, el soporte técnico está disponible durante todo el día, todos los días en coreano.

Cambiar el nivel de gravedad de su caso de soporte

Si tiene Enterprise Support o un On-Ramp plan Enterprise, puede reasignar el nivel de gravedad de su caso de soporte para reflejar los cambios en la urgencia y el impacto empresarial. Por ejemplo, puede cambiar su caso de soporte, de Tener problemas con el sistema a Tener problemas con el sistema de producción. Al cambiar la gravedad del caso, AWS Support recibe una notificación y atiende el caso de acuerdo con el nuevo nivel de gravedad.

Note

Los casos de cuentas o facturación en japonés (JP), de solicitud de aumento de Service Quotas (SQIR) y los casos de cuentas o facturación en turco (TR) creados en estos idiomas tienen una gravedad predeterminada y no se pueden cambiar.

Para cambiar la gravedad de un caso de asistencia, siga los siguientes pasos:

1. Inicie sesión en la [AWS Support Center Console](#).

Tip

En Consola de administración de AWS, también puede elegir el icono del signo de interrogación



y, a continuación, elegir Support Center.

2. Seleccione el caso para el que desee cambiar el nivel de gravedad.
3. En Detalles del caso, seleccione el icono del lápiz situado junto al campo de gravedad, como se muestra en el siguiente ejemplo.

4. En Gravedad, elija el nuevo nivel de gravedad entre las siguientes opciones:
 - General guidance
 - System impaired
 - Production system impaired
 - Production system down
 - Business-critical sistema inactivo
5. En Motivo del cambio de gravedad de un caso, elija entre las opciones disponibles por las que va a cambiar la gravedad del caso.
6. (Opcional) En Cuéntenos más, introduzca información adicional sobre este cambio.
7. Realice una de las siguientes acciones:
 - Si quiere reducir la gravedad de los casos de soporte o si va a elevarlos de la guía general a Tener problemas con el sistema o Tener problemas con el sistema de producción, seleccione Actualizar.

- Si está aumentando la gravedad de la caída del sistema de producción o la caída del Business-critical sistema, utilice una de las opciones de la sección Métodos de contacto para interactuar y AWS Support, a continuación, seleccione Actualizar. El siguiente ejemplo muestra las opciones disponibles en la sección Métodos de contacto.

The screenshot shows a 'Change case severity' dialog box. It has a title bar with a close button (X). The 'Severity' dropdown is set to 'Production system down'. The 'Reason for case severity change' dropdown is set to '-'. Below this is a text area labeled 'Tell us more - optional' with the placeholder text 'Tell us more about the reason for the escalation'. Underneath is a section titled 'Contact methods' with an 'Info' link. A blue banner states 'For high severity issues we recommend using our live contact mechanisms'. There are three radio button options: 'Web' (We'll respond by email and Support Center.), 'Chat(Recommended)' (Chat online with a representative.), and 'Phone(Recommended)' (We'll call you back at your number.). The 'Chat' option is selected. At the bottom right are 'Cancel' and 'Update' buttons.

Note

- Si cambias la gravedad de tu caso de soporte a un sistema de producción Business-critical inactivo o inactivo, debes esperar 60 minutos antes de poder volver a cambiar la gravedad.
- Si tu caso de soporte está actualmente configurado para que el Business-critical sistema esté inactivo, se te pedirá que inicies un contacto directo con él AWS Support en lugar de asignarle una gravedad mayor.
- Si va a aumentar el nivel de gravedad del caso de soporte después de haberlo aumentado al menos una vez, es posible que se encuentre con un período de espera. Por ejemplo, si cambia la gravedad de Tener problemas con el sistema a Tener problemas con el sistema de producción a las 6:00 de la mañana, entonces el caso de soporte estará por debajo del nivel de 4 horas de primera respuesta para el nivel de gravedad Tener problemas con el sistema de producción. En este escenario, puede volver a actualizar el nivel de gravedad a las 10:00 de la mañana, una vez transcurrido el período de 4 horas. Para ver una lista

de los tiempos de primera respuesta para cada nivel de gravedad, consulte la tabla de [Descripción AWS Support tiempos de respuesta](#).

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.



Hello!

We're here to help.

Account: 123456789012 • Support plan: Basic • [Change](#) 

How can we help?

Choose the related issue for your case.

1

☒ Account and billing

[Looking for Service limit increase?](#)

☐ Technical

2

Service

Billing ▼

3

Category

Other Billing Questions ▼

4

Severity [Info](#)

General question ▼

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 Enterprise On-Ramp o Enterprise Support pueden elegir el Business-critical sistema inactivo (respuesta de 15 minutos para Enterprise Support y 30 minutos para Enterprise On-Ramp).

Los tiempos de respuesta corresponden 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 obtener más información, consulte [Elegir un nivel de gravedad inicial para el caso de soporte](#).

 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.

Additional information

Describe your issue

✔ Case draft saved

1 Subject

I have an issue with my bill

Maximum 250 characters (222 remaining)

Description

Don't share any sensitive information in case correspondences, such as credentials, credit cards, signed URLs, or personally identifiable information.

[Learn more](#) 

2

I found a charge on my bill for unused resources.

Maximum 5000 characters (4951 remaining)

3

 **Attach files**

Up to 3 attachments, each less than 5MB



Description Guidance

Provide a detailed description of your issue. If you have a question about a charge, provide the date, amount, or any other details about the charge.

Cancel

Previous

Next step: Solve now or contact us

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 usted proporciona a Soporte. Para algunas combinaciones de servicio y categoría, aparece un mensaje con información relacionada. Utilice estos enlaces para ayudar a resolver el problema. Para obtener 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.

Hello! We're here to help.
Account: 123456789012 • Support plan: Basic • [Change](#)

How can we help?
[Account and billing](#), [Billing](#),
[Dispute a Charge](#), [General ...](#)

Additional information
[I have an issue in my account](#)

Solve now or contact us

Solve now | **Contact us**

Preferred contact language

English

Q |

English ✓

中文

한국어

日本語

☐ Phone
We'll call you back at your number.

☐ Chat
Chat online with a representative.

Cancel Previous **Submit**

Case draft saved

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 AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, el soporte técnico está disponible 24/7 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 AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, el soporte técnico está disponible 24/7 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 AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, el soporte técnico está disponible 24/7 en coreano.

Experiencia tradicional: 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 se actualice su caso, recibirá un correo electrónico con la correspondencia y un enlace al caso en Support Center. 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 que presentó el caso de soporte. Si inicia sesión como usuario AWS Identity and Access Management (IAM), debe tener los permisos necesarios para ver los casos de soporte. Para obtener más información, consulte [Gestione el acceso a AWS Support Center](#).
- Si no respondes al caso en unos días, lo AWS Support resolverá 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](#)
- [Resolución de un caso de soporte](#)

- [Reapertura de un caso resuelto](#)
- [Creación de un caso relacionado](#)
- [Historial de casos](#)

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.

Note

Si tiene un plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puede reasignar el nivel de gravedad de los casos de soporte para reflejar los cambios en la urgencia y el impacto empresarial. Si no tiene uno de estos planes de soporte, no podrá actualizar la gravedad de su caso. Para obtener más información, consulte [Elegir un nivel de gravedad inicial para el caso de soporte](#) y [Cambiar el nivel de gravedad de su caso de soporte](#).

Para actualizar un caso de soporte existente

1. Inicie sesión en la [AWS Support Center Console](#).

Tip

En Consola de administración de AWS, también puede elegir el icono del signo de interrogación



y, a continuación, elegir Support Center.

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. Seleccione 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 la [AWS Support Center Console](#).

 Tip

En Consola de administración de AWS, también puede elegir el icono del signo de interrogación



y, a continuación, elegir Support Center.

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 has AWS Support resuelto tu caso, puedes utilizar el enlace de comentarios para proporcionar más información sobre tu experiencia con él 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.

Please let us know if we helped resolve your issue:

If YES, click here:

<https://console.aws.amazon.com/support/feedback?eventId=1234567890&language=en&questionnaireId=Support-HMD-Yes> 

If NO, click here:

<https://console.aws.amazon.com/support/feedback?eventId=1234567890&language=en&questionnaireId=Support-HMD-No> 

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 la [AWS Support Center Console](#).

Tip

En Consola de administración de AWS, también puede elegir el icono del signo de interrogación



y, a continuación, elegir Support Center.

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 la [AWS Support Center Console](#).

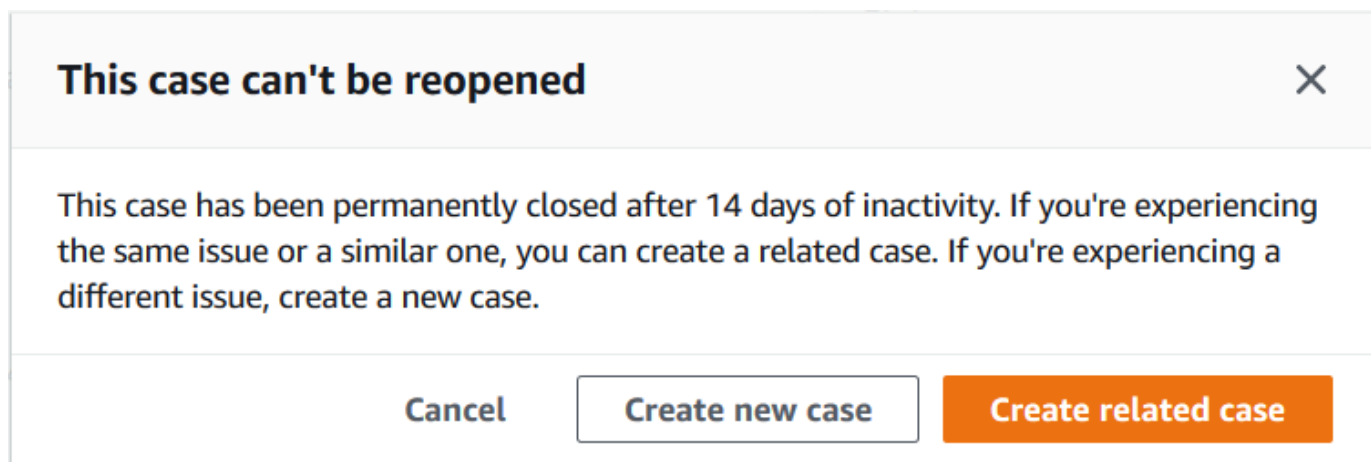
i Tip

En Consola de administración de AWS, también puede elegir el icono del signo de interrogación



y, a continuación, elegir Support Center.

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](#).

i 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.

Case ID 234567891 [Info](#) Resolve case

Case details

Subject Same issue is happening for my Amazon EC2 instances	Status Unassigned
Case ID 234567891	Severity General question
Created 2021-04-21T20:30:23.945Z	Category General Info and Getting Started
Case type Account	Additional contacts johndoe@example.com
Opened by janedoe@example.com	

Related cases

Subject	Case ID
Problem with EC2 instances	1234567890

Correspondence Reply

Jane Doe Wed Apr 21 2021 13:30:23 GMT-0700 (Pacific Daylight Time)	I keep getting an error for my EC2 instances. What do you recommend that I do to fix it?

Historial de casos

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

Utilización AWS Support 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 para C++	AWS SDK para C++ ejemplos de código
AWS CLI	AWS CLI ejemplos de código
AWS SDK para Go	AWS SDK para Go ejemplos de código
AWS SDK para Java	AWS SDK para Java ejemplos de código
AWS SDK para JavaScript	AWS SDK para JavaScript ejemplos de código
AWS SDK para Kotlin	AWS SDK para Kotlin ejemplos de código
AWS SDK para .NET	AWS SDK para .NET ejemplos de código
AWS SDK para PHP	AWS SDK para PHP ejemplos de código
Herramientas de AWS para PowerShell	Herramientas de AWS para PowerShell ejemplos de código
AWS SDK para Python (Boto3)	AWS SDK para Python (Boto3) ejemplos de código
AWS SDK para Ruby	AWS SDK para 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.

Utilización Agente de AWS DevOps con tu AWS Support plan

Agente de AWS DevOps es un compañero de equipo de AI-powered operaciones que investiga los incidentes, recomienda mejoras preventivas y se encarga de las tareas de SRE bajo demanda en todas sus instalaciones. Cuenta de AWS Si su cuenta pertenece a un Soporte plan que cumpla con los requisitos, puede habilitarla Agente de AWS DevOps directamente desde la consola del Support Center. Para obtener una descripción general de lo que hace el agente, consulte [Acerca de Agente de AWS DevOps](#) nosotros en la Guía del Agente de AWS DevOps usuario.

Temas

- [Requisitos y créditos del plan](#)
- [Habilitación Agente de AWS DevOps desde tu AWS Support Center Console](#)
- [Recursos creados para Agente de AWS DevOps activado desde AWS Support](#)
- [Eliminación Agente de AWS DevOps](#)
- [Seguridad para Agente de AWS DevOps activado desde AWS Support](#)
- [Obtener ayuda con Agente de AWS DevOps activado desde AWS Support](#)

Requisitos y créditos del plan

Puede activarlo Agente de AWS DevOps desde la consola del Support Center si su cuenta está en uno de los siguientes planes:

- AWS Soporte empresarial +
- AWS Enterprise Support
- AWS Operaciones unificadas

Cada plan incluye una asignación mensual de créditos de Agente de AWS DevOps uso. Las nuevas activaciones incluyen un período de crédito gratuito de 2 meses. Después de eso, tu plan proporciona créditos mensuales continuos para Agente de AWS DevOps el uso. Para ver tu asignación y uso actuales, consulta tus detalles de facturación en la AWS Billing consola.

Habilitación Agente de AWS DevOps desde tu AWS Support Center Console

La activación Agente de AWS DevOps desde la consola Support Center crea un espacio para agentes y los recursos AWS Identity and Access Management (IAM) que necesitan el agente y la aplicación web del operador. La activación se realiza en la región EE.UU. Este (Norte de Virginia) (us-east-1).

Para habilitar Agente de AWS DevOps

1. Inicie sesión en la [AWS Support Center Console](#).
2. Navegue hasta la página de administración de su Soporte plan.
3. En la Agente de AWS DevOps tarjeta, selecciona Activar.
4. En el cuadro de diálogo de activación, revise la descripción, elija Activar DevOps agente y, a continuación, seleccione Guardar.

La activación incluye las cuatro fases siguientes:

- Configuración de los permisos de supervisión
- Crear el espacio de agentes
- Configurar el acceso del operador
- Conectar el agente a su Cuenta de AWS

Cuando se complete la activación, podrá abrir la aplicación Agente de AWS DevOps web desde el enlace del mensaje de confirmación o en cualquier momento desde el Consola de administración de AWS.

Para obtener una explicación detallada de lo que hace el agente en su cuenta, los datos que almacena y el acceso a IAM que tiene, consulte [Qué Agente de AWS DevOps hace la activación en su cuenta Cuenta de AWS en](#) la Guía del Agente de AWS DevOps usuario. Para obtener una descripción general de la postura de seguridad del agente, consulte [Agente de AWS DevOps Seguridad](#) en la Guía del Agente de AWS DevOps usuario.

Recursos creados para Agente de AWS DevOps activado desde AWS Support

La activación desde la consola Support Center crea los siguientes recursos en us-east-1.

ACCOUNT_ID Sustitúyala por tu Cuenta de AWS ID de 12 dígitos. El sufijo del WebappAdmin rol es un identificador de 12 caracteres derivado del espacio del agente.

Los recursos se crean cuando se habilita Agente de AWS DevOps desde la consola Support Center

Servicio de AWS	Tipo de recurso	Nombre del recurso	Ámbito de confianza	Permisos concedidos
Agente de AWS DevOps	Espacio de agente	DevOpsAgentSpace	No aplicable	Contenedor para la asociación de cuentas, la configuración de la aplicación web del operador y los datos que el agente genera mientras está en funcionamiento.
AWS Identity and Access Management (IAM)	Rol	DevOpsAgentRole-AgentSpace- ACCOUNT_ID	Cuenta aidevops.amazonaws.com con la confianza <code>aws:SourceAccount</code> y <code>aws:SourceArn</code> las condiciones que limitan la función a los espacios de agente en su propia cuenta (protección de agente confuso).	Otorga al agente los permisos de investigación de solo lectura Servicios de AWS que necesita para investigar los recursos de tu cuenta. Los permisos provienen del archivo AWS administrado AIDevOpsAgentAccessPolicy adjunto en el momento de la activación. Para

Servicio de AWS	Tipo de recurso	Nombre del recurso	Ámbito de confianza	Permisos concedidos
				ver la lista completa, consulte AIDevOpsAgentAccessPolicy la Guía del Agente de AWS DevOps usuario. También se adjunta la AIDevOpsAllowAwsSupportActionsPolicy - <i>ACCOUNT_ID</i> política gestionada por el cliente.

Servicio de AWS	Tipo de recurso	Nombre del recurso	Ámbito de confianza	Permisos concedidos
AWS Identity and Access Management (IAM)	Rol	DevOpsAgentRole-WebAppAdmin - <i>suffix</i>	La política de confianza se aplica a un espacio de agente específico, por lo que solo la aplicación web del operador de ese espacio de agentes puede asumirla.	Otorga al operador de la aplicación web los permisos que necesita para el chat, el diario, las recomendaciones y Soporte la integración. Los permisos provienen de la parte AWS administrada <code>AIDevOpsOperatorAppAccessPolicy</code> . Para ver la lista completa, consulte AIDevOpsOperatorAppAccessPolicy la Guía del Agente de AWS DevOps usuario.

Servicio de AWS	Tipo de recurso	Nombre del recurso	Ámbito de confianza	Permisos concedidos
AWS Identity and Access Management (IAM)	Customer-managed política	AIDevOpsAllowAWSSupportActionsPolicy - <i>ACCOUNT_ID</i>	Adscrito al DevOpsAgentRole-AgentSpace- <i>ACCOUNT_ID</i> rol.	Concesión <code>esiam:CreateServiceLinkedRole</code> , asignadas al rol ARN <code>()</code> vinculado al servicio de AWS Resource Explorer. <code>arn:aws:iam::<i>ACCOUNT_ID</i>:role/aws-service-role/resource-explorer-2.amazonaws.com/AWSServiceRoleForResourceExplorer</code> Este permiso permite al agente crear el rol vinculado al servicio de AWS Resource Explorer en su nombre si aún no existe, de modo que el agente puede usar AWS Resource Explorer para descubrir la topología.

La activación de la consola Support Center no crea recursos en ninguna otra Región de AWS.

Eliminación Agente de AWS DevOps

Para eliminar los recursos que se crearon al habilitarlos Agente de AWS DevOps desde la consola del Support Center, consulte [Eliminar un espacio de agente](#) en la Guía del Agente de AWS DevOps usuario. Los procedimientos incluyen la eliminación del espacio de agentes, las dos funciones de IAM y cualquier política gestionada por el cliente que comience con ella. AIDevOps El procedimiento también explica cómo volver a activarlo Agente de AWS DevOps más adelante y qué hay que tener en cuenta al hacerlo.

Note

Las políticas AWS administradas asociadas a las funciones (AIDevOpsAgentAccessPolicyyAIDevOpsOperatorAppAccessPolicy) de IAM se separan, pero no se eliminan, ya que estas políticas son propiedad de. AWS

Cuando siga ese procedimiento, tenga en cuenta que los nombres de sus recursos aparecen en [Recursos creados para Agente de AWS DevOps activado desde AWS Support](#) la lista y están todos incluidos. us-east-1

Seguridad para Agente de AWS DevOps activado desde AWS Support

Agente de AWS DevOps proporciona los siguientes controles de seguridad:

- Los espacios de los agentes son el límite de seguridad principal. Cada espacio de agentes está aislado en uno solo Cuenta de AWS.
- Los datos se cifran en reposo con claves AWS gestionadas y se cifran en tránsito.
- La actividad de los agentes se captura en un diario de agentes inmutable y en AWS CloudTrail (). CloudTrail
- Agente de AWS DevOps aplica las protecciones de límites de cuentas, escritura limitada e inyección rápida.

[Para conocer todos los aspectos de seguridad, incluidos el procesamiento regional, la seguridad de la integración, la conectividad de la red y el modelo de responsabilidad compartida, consulte la sección Seguridad en la Guía del usuario.](#)[Agente de AWS DevOps Agente de AWS DevOps](#)

Obtener ayuda con Agente de AWS DevOps activado desde AWS Support

Si tienes preguntas sobre tu Soporte plan o tus créditos de Agente de AWS DevOps uso o si deseas informar de problemas relacionados con la activación o la desactivación que no puedas resolver a través de la Guía del Agente de AWS DevOps usuario, [ponte en contacto con nosotros AWS Support](#).

Acerca de la API de la consola del centro de soporte

La API de la consola del centro de soporte mejora la experiencia con dicha consola. Entre los ejemplos de la funcionalidad que proporciona la API de la consola del centro de soporte se incluyen los siguientes:

- La posibilidad de crear y actualizar un borrador de su caso de soporte
- La posibilidad de que la consola del centro de soporte muestre el estado actual de su cuenta
- La capacidad de la consola del centro de soporte de mostrar ayuda dinámica para el servicio y la categoría seleccionados

Para obtener una lista completa de las acciones que proporciona la API de la consola del centro de soporte, consulte la tabla de [Añadir políticas de IAM para las operaciones de la API de la consola del centro de soporte](#).

Important

Para seguir utilizando las funciones incluidas en la API de Support Center Console, debe añadir las operaciones de Support Center Console a sus AWS Identity and Access Management políticas antes del 16 de noviembre de 2026. Tras crear las políticas de IAM, actualice la política AWS Support gestionada para incluir las `support-console:*` acciones. Para obtener más información, consulte [Añadir políticas de IAM para las operaciones de la API de la consola del centro de soporte](#).

Temas

- [Añadir políticas de IAM para las operaciones de la API de la consola del centro de soporte](#)
- [Pruebas de las llamadas a la API de la consola del centro de soporte](#)

Añadir políticas de IAM para las operaciones de la API de la consola del centro de soporte

Antes del 16 de noviembre de 2026, debe crear AWS Identity and Access Management políticas para las operaciones de la API de Support Center Console. Si no crea estas políticas antes del 16 de noviembre de 2026, recibirá `AccessDenied` errores.

Para añadir estas operaciones a sus políticas de IAM, consulte [Crear políticas de IAM \(consola\)](#) en la Guía del usuario de AWS Identity and Access Management .

En la siguiente tabla se resumen las operaciones de la consola.

 **Note**

Estas son operaciones solo para la consola. No están disponibles para su uso en el AWS SDK ni en el AWS CLI.

Operación	Nivel de acceso	Description (Descripción)
GetAccountState	LEER	Concede permiso a la consola para mostrar el estado actual de la cuenta.
GetAccountGovCloudEnabled	LEER	Otorga permiso para determinar si tu cuenta está GovCloud habilitada.
GetCaseDraft	LEER	Concede permiso a la consola para mostrar el borrador del caso que creó anteriormente.
CreateCaseDraft	ESCRIBIR	Concede permiso para crear o actualizar el borrador de caso para el tipo de caso determinado.
DeleteCaseDraft	ESCRIBIR	Concede permiso para eliminar el borrador de caso para el tipo de caso determinado.
GetBanner	LEER	Otorga permiso a la consola para mostrar el Soporte banner que se muestra

Operación	Nivel de acceso	Description (Descripción)
		durante los eventos que afectan a los clientes.
DescribeDynamicHelp	LEER	Concede permiso a la consola para mostrar los recursos de ayuda dinámica para el servicio y la categoría seleccionados.
CreateContact	ESCRIBIR	Concede permiso a la consola para crear un contacto autenticado para el tipo de contacto seleccionado.
CheckSubscription	LEER	Concede permiso a la consola para verificar si su cuenta tiene acceso al producto seleccionado.
GetQuestionnaire	LEER	Concede permiso a la consola para mostrar el cuestionario de comentarios de los clientes.
SaveFeedback	ESCRIBIR	Concede permiso para guardar los comentarios del cuestionario.

Note

Si tiene una configuración de VPN personalizada, asegúrese de configurar su VPN para que reenvíe correctamente la dirección IP de su cliente al punto final de la API de Support Center Console. Cuando utilice una VPN con AWS Identity and Access Management políticas que incluyan [aws: SourceIp conditions](#), la dirección IP del cliente especificada en su política de IAM debe reenviarse al punto final de la API, no a la dirección IP de la VPN. Si la VPN reenvía su propia dirección IP en lugar de la dirección IP del cliente, la autorización podría

fallar porque la dirección IP no coincide con la `aws:SourceIp` condición de su política de IAM. La siguiente tabla proporciona los puntos finales de la API de Support Center Console por Región de AWS.

Región de AWS	Punto de conexión de la API de la consola del centro de soporte
<code>https://api.us-east-1.prod.support-console.support.aws.dev</code>	Este de EE. UU. (Norte de Virginia)
<code>https://api.us-west-2.prod.support-console.support.aws.dev</code>	Oeste de EE. UU. (Oregón)
<code>https://api.eu-west-1.prod.support-console.support.aws.dev</code>	Europa (Irlanda)

Pruebas de las llamadas a la API de la consola del centro de soporte

Para validar que sus políticas de IAM estén configuradas correctamente para las operaciones de la API de Support Center Console, abra [AWS Support Center Console](#) para generar llamadas recientes a la API.

Para comprobar si faltan permisos de IAM, complete los siguientes pasos:

1. Inicie sesión en Consola de administración de AWS y abra la CloudTrail consola en <https://console.aws.amazon.com/cloudtrail>.
2. Consulta el Región de AWS menú desplegable para asegurarte de que te encuentras en la región EE.UU. Este (Virginia del Norte).
3. En el panel de navegación, elija Historial de eventos.
4. Filtra por fuente de eventos `support-console.amazonaws.com`.

5. Haga coincidir los nombres de los eventos con la lista de `support-console:*` operaciones de (por ejemplo,). [Añadir políticas de IAM para las operaciones de la API de la consola del centro de soporte](#) `GetAccountState`
6. Abra los eventos coincidentes y busque un `additionalEventData` campo que contenga una `authZHeader` entrada. Si está presente, a tu política de IAM le falta el permiso que aparece en esa entrada.
7. Añada el `support-console` permiso específico a su política de IAM. Puede conceder acceso a todas las operaciones utilizando `support-console:*` o seleccionar operaciones individuales para un control detallado. Para obtener una lista completa de las operaciones, consulte la [Añadir políticas de IAM para las operaciones de la API de la consola del centro de soporte](#).
8. Para comprobar la corrección, vuelve a visitar para generar nuevas llamadas AWS Support Center Console a la API y, a continuación, repite los pasos 1 a 6. Asegúrese de que los nuevos eventos ya no contengan ningún campo. `additionalEventData`

Acerca de la AWS Support API

Important

Aviso de fin de soporte: el soporte para desarrolladores se suspenderá el 1 de enero de 2027. Los clientes con soporte para desarrolladores pueden seguir usando su plan actual o optar por actualizarse a Business Support+ en cualquier momento antes del 1 de enero de 2027. Business Support+ ofrece asistencia basada en inteligencia artificial que comprende el contexto de sus operaciones, con acceso a AWS expertos las 24 horas del día, los 7 días de la semana, a un precio mínimo de 29 USD al mes por cuenta. Para obtener más información, consulta los detalles del [plan Business Support+](#)

Aviso de fin de soporte: el soporte empresarial se suspenderá el 1 de enero de 2027. Los clientes con Business Support pueden seguir usando su plan actual o optar por actualizarse a Business Support+ en cualquier momento antes del 1 de enero de 2027. Business Support + ofrece asistencia basada en inteligencia artificial que comprende el contexto de sus operaciones, con acceso a AWS expertos las 24 horas del día, los 7 días de la semana, a un precio mínimo de 29 USD al mes por cuenta. Para obtener más información, consulta los detalles del [plan Business Support+](#)

Aviso de fin de soporte: el 1 de enero de 2027, Enterprise AWS On-Ramp dejará de funcionar. A lo largo de 2026, los clientes de Enterprise On-Ramp pasarán automáticamente a AWS Enterprise Support durante la renovación del contrato o en lotes periódicos. Los clientes recibirán una notificación por correo electrónico un mes antes de la actualización. No hay que hacer nada más. Enterprise Support proporciona una asignación de TAM designada, tiempos de respuesta de 15 minutos y Respuesta frente a incidencias de seguridad de AWS está disponible sin costo adicional, todo a un precio mínimo inferior de 5000\$ (reducido de 15 000\$). Para obtener más información, consulte los detalles del [Soporte plan AWS Enterprise](#). Para obtener más información, consulte [On-Ramp Fin del soporte para desarrolladores, empresas y empresas](#).

Developer Support, Business Support y Enterprise On-Ramp seguirán estando disponibles en la AWS GovCloud (US) región.

La AWS Support API proporciona acceso a algunas de las funciones del [AWS Support Center](#).

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

Debe tener un plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations para usar la AWS Support API. Para obtener más información, consulte [Soporte](#).

Para obtener más información sobre las operaciones y los tipos de datos que proporciona Soporte, consulte la [referencia de la AWS Support API](#).

Temas

- [Administración de casos de soporte](#)
- [AWS Trusted Advisor](#)
- [Puntos de conexión](#)
- [Support en AWS SDKs](#)

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 respaldar las operaciones de administración de casos. Para obtener más información, consulte [Registrar llamadas a la AWS Support API con AWS CloudTrail](#).

Para ver ejemplos de código que muestran cómo gestionar todo el ciclo de vida de un caso de soporte, consulta [Ejemplos de código para su Soporte uso AWS SDKs](#).

AWS Trusted Advisor

Puede utilizar las Trusted Advisor operaciones para realizar las siguientes tareas:

- Obtenga los nombres e identificadores de las Trusted Advisor comprobaciones
- Solicita que se Trusted Advisor compruebe tu AWS cuenta y tus recursos
- Obtenga resúmenes e información detallada de los resultados de sus Trusted Advisor comprobaciones
- Actualice sus cheques Trusted Advisor
- Obtenga el estado de cada Trusted Advisor cheque

La AWS Support API admite el CloudTrail registro de Trusted Advisor las operaciones. Para obtener más información, consulte [AWS Trusted Advisor información al iniciar CloudTrail sesión](#).

Puedes usar Amazon CloudWatch Events para supervisar los cambios en los resultados de tus comprobaciones Trusted Advisor. Para obtener más información, consulte [Supervisión de los resultados de los AWS Trusted Advisor controles con Amazon EventBridge](#).

Para ver un ejemplo de código Java que muestra cómo utilizar las Trusted Advisor operaciones, consulte [Uso de Trusted Advisor como un servicio web](#).

Puntos de conexión

Soporte 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.

Puedes usar los siguientes puntos de conexión para la Soporte API:

- 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 [CreateCase](#) operación 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 [ResolveCase](#) operación para resolverlo.
- Para llamar a las AWS Trusted Advisor operaciones de la AWS Support API, debes usar el punto final de EE. UU. Este (Virginia del Norte). Actualmente, los puntos finales de EE. UU. Oeste (Oregón) y Europa (Irlanda) no admiten Trusted Advisor las operaciones.

Para obtener más información sobre los AWS puntos finales, consulte los [AWS Support puntos finales y las cuotas](#) en. Referencia general de Amazon Web Services

Support en AWS SDKs

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

Para obtener una lista de los idiomas compatibles con la AWS Support API, elija un nombre de operación, por ejemplo [CreateCase](#), y en la sección [Vea también](#), elija el idioma que prefiera.

AWS Support Planes

AWS ofrece los siguientes AWS Support planes entre los que puede elegir en función de las necesidades de su empresa.

- Basic
- AWS Soporte empresarial +
- AWS Enterprise Support
- AWS Operaciones unificadas

Important

Aviso de fin de soporte: el soporte para desarrolladores se suspenderá el 1 de enero de 2027. Los clientes con soporte para desarrolladores pueden seguir usando su plan actual o optar por actualizarse a Business Support+ en cualquier momento antes del 1 de enero de 2027. Business Support+ ofrece AI-powered asistencia que comprende el contexto de sus operaciones, con 24/7 acceso a AWS expertos a un precio 29/month mínimo de \$ por cuenta. Para obtener más información, consulta los detalles del [plan Business Support+](#)

Aviso de fin de soporte: el soporte empresarial se suspenderá el 1 de enero de 2027. Los clientes con Business Support pueden seguir usando su plan actual o optar por actualizarse a Business Support+ en cualquier momento antes del 1 de enero de 2027. Business Support + ofrece AI-powered asistencia que comprende el contexto de sus operaciones, con 24/7 acceso a AWS expertos a un precio 29/month mínimo de \$ por cuenta. Para obtener más información, consulta los detalles del [plan Business Support+](#)

Aviso de fin de soporte: el 1 de enero de 2027, AWS se suspenderá Enterprise. On-Ramp A lo largo de 2026, On-Ramp los clientes empresariales pasarán automáticamente a AWS Enterprise Support durante la renovación del contrato o en lotes periódicos. Los clientes recibirán una notificación por correo electrónico un mes antes de la actualización. No hay que hacer nada más. Enterprise Support proporciona una asignación de TAM designada, tiempos de respuesta de 15 minutos y Respuesta frente a incidencias de seguridad de AWS está disponible sin costo adicional, todo a un precio mínimo inferior de 5000\$ (reducido de 15 000\$). Para obtener más información, consulte los detalles del [Soporte plan AWS Enterprise](#). Para obtener más información, consulte [On-Ramp Fin del soporte para desarrolladores, empresas y empresas](#).

Developer Support, Business Support y Enterprise On-Ramp seguirán estando disponibles en la AWS GovCloud (US) región.

Temas

- [Características de AWS Support Planes](#)
- [¿Qué es? AWS Operaciones unificadas](#)
- [Cambio AWS Support Planes](#)
- [Configure las notificaciones de caducidad del plan promocional](#)
- [On-Ramp Fin del soporte para desarrolladores, empresas y empresas](#)

Características de AWS Support Planes

Basic Support ofrece asistencia para preguntas sobre cuentas y facturación y para aumentar la cuota de servicio. Los otros planes ofrecen diversos casos de soporte técnico, con pagos mensuales 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:

- One-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 Business Support+ tienen acceso a estas funciones adicionales:

- Respuestas contextuales y en tiempo real a través de la IA generativa.
- Acceso por teléfono, web y chat las 24 horas del día, los 7 días de la semana a los ingenieros de Cloud Support.
- Interacción humana en menos de 30 minutos para casos críticos de funcionamiento del sistema empresarial.
- Más de 500 comprobaciones con [AWS Trusted Advisor](#).

- 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 .
- Third-party soporte de software: ayuda con los sistemas operativos y la configuración de las instancias de Amazon Elastic Compute Cloud (Amazon EC2). Además, ayude a mejorar el rendimiento de los componentes de software de terceros más populares en AWS.
- Admite un número ilimitado de casos de soporte que cualquier usuario con [permisos](#) puede abrirlos.

Los clientes con un plan Enterprise Support tienen todos los beneficios disponibles con el plan AWS Business Support+, además de los siguientes beneficios adicionales:

- Un administrador técnico de cuentas (TAM) designado.
- Respuesta de hasta 15 minutos a casos críticos para la producción.
- Acceda a [Respuesta frente a incidencias de seguridad de AWS](#) un servicio que le ayuda a prepararse, responder y recibir orientación rápidamente para recuperarse de los incidentes de seguridad. Esto incluye incidentes como la toma de control de cuentas, las filtraciones de datos y los ataques de ransomware.
- Revisiones empresariales estratégicas con AWS expertos.
- Acceso a la gestión de eventos de AWS Countdown. AWS Countdown proporciona TAM-led apoyo especializado para ayudarlo a tener éxito durante los eventos empresariales críticos.

Los clientes con un plan de operaciones AWS unificadas tienen acceso a los siguientes beneficios. Para obtener más información sobre el plan de operaciones AWS unificadas, incluidos los detalles de incorporación y la información de introducción, consulte [¿Qué es? AWS Operaciones unificadas](#).

- 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.
- Gestión de eventos de infraestructura: Short-term póngase en contacto con AWS Support usted para obtener una comprensión profunda de su caso de uso. Después del análisis, proporcione orientación arquitectónica y de escalado para un evento.
- Diseñe un administrador AWS técnico de cuentas (TAM) y un ingeniero especialista en dominios (DSE) para sus aplicaciones y casos de uso específicos.
- Una suscripción periódica a [AWS Countdown Premium](#).

- Revisiones críticas de la carga de trabajo y manuales y procedimientos operativos personalizados.

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.

 Note

Si trabaja con un AWS socio y desea obtener más información sobre Partner-led Support, consulte [AWS Partner-Led Support](#)

¿Qué es? AWS Operaciones unificadas

AWS Unified Operations combina experiencia comprobada con AI-powered conocimientos para ayudar a reducir los riesgos operativos y de seguridad, resolver los problemas con mayor rapidez y ayudarlo a diseñar soluciones en la nube más resilientes desde el principio, lo que acelera sus iniciativas de nube más críticas. AWS Los especialistas designados actúan como una extensión de su equipo a través de sus canales de colaboración preferidos: revisan las cargas de trabajo, proporcionan orientación estratégica y optimizan el rendimiento a través de un profundo conocimiento contextual. Con 24/7 la supervisión de la seguridad y el rendimiento, detectamos y mitigamos los incidentes de forma temprana y, al mismo tiempo, reducimos el volumen de alertas. Una respuesta de cinco minutos y adaptada al contexto para los incidentes críticos reduce aún más el tiempo de resolución y ayuda a mantener el máximo rendimiento operativo.

AWS Precios de operaciones unificadas

AWS Los precios de Unified Operations se basan en sus requisitos específicos y en la complejidad de la carga de trabajo. Para obtener información detallada sobre los precios, consulte los [precios del AWS Support plan](#).

Contenido

- [Ventajas de las operaciones unificadas](#)
- [Equipo de operaciones unificado](#)
 - [Gestor técnico de cuentas](#)
 - [Ingeniero especialista en dominios](#)

- [Especialista sénior en facturación y cuentas](#)
- [Ingeniero de gestión de incidentes](#)
- [Ingeniero de migraciones y eventos](#)
- [AWS Equipo de respuesta a incidentes del cliente](#)
- [Ingeniero de soporte especializado](#)
- [Ciclo de vida de las operaciones unificadas](#)
 - [Incorporación previa a las operaciones unificadas](#)
 - [Incorporación de operaciones unificadas](#)
 - [Planificación unificada de operaciones Pre-event o migración](#)
 - [Evento de operaciones unificadas: migración o transición](#)
 - [Operaciones unificadas: puesto Go-live o evento](#)
 - [Gestión unificada de incidentes de carga de trabajo de operaciones](#)
 - [Operaciones unificadas: después del incidente](#)
 - [Operaciones unificadas: mejora continua](#)
- [Cómo empezar con las operaciones unificadas](#)
 - [Introducción a las operaciones unificadas: requisitos previos](#)
 - [Primeros pasos en las operaciones unificadas: incorpore alarmas críticas para una gestión rápida de los incidentes](#)
 - [Primeros pasos en las operaciones unificadas: cómo solicitar una respuesta a un incidente en 5 minutos](#)
 - [Primeros pasos de las operaciones unificadas: planifique la cobertura del dominio](#)
 - [Primeros pasos en las operaciones unificadas: incorpore su cuenta a una gestión proactiva de los incidentes de seguridad](#)
 - [Primeros pasos de operaciones unificadas: AWS expectativas de usted](#)
 - [Primeros pasos en las operaciones unificadas: lo que puede esperar de AWS](#)

Ventajas de las operaciones unificadas

Las operaciones unificadas ofrecen varios beneficios clave.

- [AWS Expertos designados: su AWS equipo incluye administradores técnicos de cuentas \(TAM\) designados, un ingeniero especialista en AWS dominios y un especialista sénior en facturación y](#)

cuentas. Tu AWS equipo se integra con tus herramientas de colaboración, como Slack o Microsoft Teams.

- **Asesoramiento técnico exhaustivo:** tu AWS equipo te ayuda a reforzar tu capacidad de recuperación mediante análisis exhaustivos sobre aplicaciones específicas, evaluaciones de preparación, soporte para pruebas guiadas y manuales personalizados adaptados a tu entorno. Su AWS equipo proporciona una gestión financiera centrada en la carga de trabajo y alinea los costes de forma estratégica con sus objetivos empresariales.
- **Soporte para migraciones, eventos y lanzamientos:** acelere sus migraciones críticas a la nube y los eventos empresariales con AWS ingenieros designados que ayudan a mitigar los riesgos de forma proactiva y lo guían desde la planificación hasta la ejecución. Real-time asistencia para eventos programados, aumento de la velocidad de migración y lanzamientos exitosos.
- **Supervisión proactiva de la carga de trabajo las 24 horas del día, los 7 días de la semana:** incorpore alarmas a nivel de aplicaciones e infraestructura desde sus herramientas existentes AWS y de terceros para detectar las señales de advertencia tempranas e impulsar la mitigación proactiva junto con su equipo.
- **Póngase en contacto con los administradores de AWS incidentes en un plazo de 5 minutos para resolver los problemas de inactividad del sistema críticos para la empresa:** reciba asistencia proactiva de los ingenieros de gestión de incidentes en menos de 5 minutos si se producen alarmas, alertas de carga de trabajo o problemas de inactividad del sistema críticos para la empresa.
- **Context-specific respuesta a cada caso:** acceda a ingenieros de soporte sensibles al contexto para impulsar la resolución de incidentes. Guías y guías de respuesta a incidentes personalizados para sus flujos de trabajo, lo que agiliza el diagnóstico y la resolución de problemas en función de sus necesidades empresariales específicas.
- **Asesoramiento y asistencia en materia de seguridad:** supervisión proactiva de los eventos de seguridad mediante una clasificación e investigación automatizadas, además de 24/7 acceso al equipo de respuesta a incidentes del AWS cliente para prepararse, responder y recuperarse de los eventos de seguridad que se produzcan en su entorno. AWS

Equipo de operaciones unificado

AWS Unified Operations reúne a un equipo designado de expertos especializados que trabajan en conjunto para respaldar su transición a la nube. Cada función está cuidadosamente diseñada para proporcionar una cobertura integral de las dimensiones técnicas, financieras, operativas y de seguridad de su entorno de nube. Desde la orientación estratégica hasta el soporte técnico, desde la

optimización financiera hasta la respuesta rápida a los incidentes, estos expertos actúan como una extensión de su equipo y están disponibles 24/7 para garantizar que sus operaciones en la nube se ejecuten de manera eficiente y segura.

Contenido

- [Gestor técnico de cuentas](#)
- [Ingeniero especialista en dominios](#)
- [Especialista sénior en facturación y cuentas](#)
- [Ingeniero de gestión de incidentes](#)
- [Ingeniero de migraciones y eventos](#)
- [AWS Equipo de respuesta a incidentes del cliente](#)
- [Ingeniero de soporte especializado](#)

Gestor técnico de cuentas

El administrador técnico de cuentas (TAM), su estrategia de nube designado, organiza el compromiso general e impulsa los resultados empresariales. Los TAM lideran la planificación estratégica, realizan revisiones empresariales trimestrales, proporcionan orientación sobre resiliencia y coordinan los equipos especializados para garantizar el éxito de sus iniciativas en la nube. Son su principal punto de contacto para las escalaciones y las decisiones estratégicas.

Ingeniero especialista en dominios

Un ingeniero especialista en dominios (DSE) es un experto técnico que comprende a fondo su arquitectura de carga de trabajo específica y Servicios de AWS. Los DSE realizan revisiones críticas de las cargas de trabajo, crean documentación técnica, desarrollan guías de solución de problemas y ofrecen consultas técnicas continuas. Analizan los incidentes para evitar que se repitan y mantienen un intercambio de conocimientos a nivel mundial para garantizar que la calidad del soporte sea constante.

Especialista sénior en facturación y cuentas

Su especialista sénior en facturación y cuentas (SBAS) es un experto designado en optimización financiera que ayuda a equilibrar el rendimiento con los costos. Administran las estrategias de optimización de costos, supervisan las carteras de instancias reservadas y planes de ahorro, realizan revisiones de las empresas financieras y proporcionan análisis detallados de los gastos para maximizar la eficiencia de sus inversiones en la nube.

Ingeniero de gestión de incidentes

Los ingenieros de gestión de incidentes (IME) son especialistas en respuesta rápida que coordinan la resolución de incidentes críticos. Los IME proporcionan tiempos de respuesta de 5 minutos, organizan los equipos técnicos durante los incidentes y gestionan las comunicaciones con las partes interesadas. Durante los incidentes activos, los IME realizan evaluaciones en tiempo real de la gestión de los incidentes y la eficacia de la respuesta y, previa solicitud, documentan la secuencia de los eventos, las decisiones tomadas y los resultados inmediatos. Observan y evalúan la ejecución de los protocolos de respuesta, la coordinación del equipo y la aplicación de las estrategias existentes mientras el incidente aún se está desarrollando.

Ingeniero de migraciones y eventos

On-demand expertos que guían las transiciones críticas, como los lanzamientos y las migraciones. Validan las arquitecturas, crean planes de ejecución detallados, proporcionan supervisión en tiempo real durante los eventos y realizan análisis posteriores a los eventos para captar lo aprendido y optimizar las operaciones futuras.

AWS Equipo de respuesta a incidentes del cliente

El equipo de respuesta a incidentes del AWS cliente (CIRT) está formado por expertos en seguridad que brindan asistencia 24/7 especializada en casos de seguridad. Supervisan los hallazgos de seguridad, proporcionan una respuesta guiada a los pocos minutos de la detección y mejoran las capacidades de las operaciones de seguridad mediante el apoyo de expertos en la investigación y la orientación sobre las mejores prácticas.

Ingeniero de soporte especializado

Los ingenieros de soporte especializados (SSE) son expertos técnicos con gran experiencia que utilizan herramientas contextuales avanzadas para ofrecer soluciones de soporte precisas. Aprovechan AI-powered los sistemas y un profundo conocimiento técnico para comprender rápidamente su entorno y resolver desafíos técnicos complejos.

Ciclo de vida de las operaciones unificadas

El plan Unified Operations Support contiene diferentes fases, desde la preincorporación hasta la mejora continua, que le ayudan a aprovechar al máximo su entorno de nube. En este tema se tratan los puntos clave de cada fase.

Contenido

- [Incorporación previa a las operaciones unificadas](#)
- [Incorporación de operaciones unificadas](#)
- [Planificación unificada de operaciones Pre-event o migración](#)
- [Evento de operaciones unificadas: migración o transición](#)
- [Operaciones unificadas: puesto Go-live o evento](#)
- [Gestión unificada de incidentes de carga de trabajo de operaciones](#)
- [Operaciones unificadas: después del incidente](#)
- [Operaciones unificadas: mejora continua](#)

Incorporación previa a las operaciones unificadas

Durante las fases previas a la incorporación, AWS recopila la información sobre usted necesaria para iniciar el proceso de incorporación, incluida la siguiente información:

Descubrimiento del entorno y validación técnica

- Comprensión de la arquitectura de su carga de trabajo y de sus claves Servicios de AWS.
- Sus necesidades de planificación futuras, como la migración o los eventos.
- Pre-requisitos, como una lista de sus Cuentas de AWS y Regiones de AWS.
- Sus necesidades empresariales específicas.

Incorporación de operaciones unificadas

Inicio de la incorporación

- Conozca al equipo (cliente y recursos AWS asignados).

Taller de incorporación

- Identifique las cargas de trabajo críticas.
- Realice una revisión profunda de la arquitectura de las cargas de trabajo.
- Revise las funciones y responsabilidades (revisión por parte del RACI, AWS así como sus funciones y responsabilidades).
- Revise los flujos de trabajo de gestión de incidentes y cambios (ITSM).
- Protocolo de comunicación: herramientas y procesos, ruta de escalamiento, horarios de guardia

- Identifique y defina las alarmas críticas (en Amazon CloudWatch, su APM de terceros o una herramienta de monitoreo personalizada).
- Cree manuales para las alarmas críticas.

Incorporación de servicios

- Tu Cuenta de AWS incorporación a. Respuesta frente a incidencias de seguridad de AWS
- Incorporación de alarmas críticas para una gestión rápida de incidentes.

Planificación unificada de operaciones Pre-event o migración

Pre-event o la planificación de la migración en AWS Unified Operations incluye los siguientes elementos clave.

- Recopilación de contexto: descubrimiento y arquitectura de la carga de trabajo.
- Revisión de la preparación operativa (ORR): evaluación sistemática basada en las AWS mejores prácticas y manuales para identificar posibles problemas antes de que afecten al evento.
- Evaluaciones de riesgos: identifique, enumere los posibles riesgos y planifique su mitigación.
- Revise los eventos: asegure el soporte para eventos de transición o migración.

Evento de operaciones unificadas: migración o transición

La migración o transición de eventos en Unified Operations incluye los siguientes elementos clave.

- Real-time puente hacia la resolución: AWS los expertos se unen a sus canales de comunicación para supervisar los eventos y resolver los problemas durante los períodos comerciales críticos.
- 24/7 soporte integral: asistencia de Round-the-clock expertos con orientación inmediata para satisfacer las necesidades de ampliación de los recursos.
- AWS ingeniería: trabaje directamente con ingenieros que entiendan su negocio y le ofrezcan soluciones personalizadas.

Operaciones unificadas: puesto Go-live o evento

El proceso posterior a la puesta en marcha o posterior al evento en Unified Operations incluye los siguientes elementos clave:

- Spin-down recursos de participación y específicos para eventos.
- Realice revisiones de eventos.
- Actualice los manuales y la documentación en función de lo aprendido.
- Realice retrospectivas para identificar las áreas de mejora.

Gestión unificada de incidentes de carga de trabajo de operaciones

La gestión de incidentes de carga de trabajo incluye los siguientes elementos clave:

- AWS Support creación de casos.
- Colaboración con usted y con un ingeniero de gestión de AWS incidentes (IME) para gestionar los incidentes teniendo en cuenta el contexto.
- Unirse a una llamada puente sobre incidentes o crearla.
- Monitorización de la Servicio de AWS salud y de los eventos a gran escala (LSE).
- Recuperación rápida de aplicaciones o cargas de trabajo críticas.

Operaciones unificadas: después del incidente

Post-incident El análisis de los incidentes críticos lo lleva a cabo el ingeniero especialista de dominio (DSE) asignado. Tras la resolución, el DSE adopta un enfoque analítico más amplio y lleva a cabo un análisis exhaustivo de la causa raíz para identificar cualquier laguna en los procesos o en las herramientas. El DSE transforma los conocimientos en mejoras prácticas mediante la actualización de los manuales de respuesta, la recomendación de medidas preventivas y la sugerencia de mejoras arquitectónicas para ayudar a prevenir incidentes similares en el futuro.

Operaciones unificadas: mejora continua

La mejora continua incluye los siguientes elementos clave:

- Actualice las revisiones de la carga de trabajo crítica y proponga recomendaciones AWS específicas para cada servicio y directrices sobre resiliencia.
- Revise los casos antiguos y nuevos de forma continua y proporcione guías de solución de problemas técnicos identificados.
- Aplique las lecciones y supervise las implementaciones y las pruebas.
- Analice los problemas técnicos, las configuraciones, los proyectos e hitos pasados y futuros.

- Revise los planes de implementación de nuevas funciones con evaluaciones de riesgos y optimizaciones del rendimiento.
- Realice una revisión empresarial mensual o trimestral (MBR/QBR).

Cómo empezar con las operaciones unificadas

En este tema se describen los pasos para incorporarse a AWS Unified Operations.

Contenido

- [Introducción a las operaciones unificadas: requisitos previos](#)
- [Primeros pasos en las operaciones unificadas: incorpore alarmas críticas para una gestión rápida de los incidentes](#)
- [Primeros pasos en las operaciones unificadas: cómo solicitar una respuesta a un incidente en 5 minutos](#)
- [Primeros pasos de las operaciones unificadas: planifique la cobertura del dominio](#)
- [Primeros pasos en las operaciones unificadas: incorpore su cuenta a una gestión proactiva de los incidentes de seguridad](#)
- [Primeros pasos de operaciones unificadas: AWS expectativas de usted](#)
- [Primeros pasos en las operaciones unificadas: lo que puede esperar de AWS](#)

Introducción a las operaciones unificadas: requisitos previos

Se requieren los siguientes elementos para incorporarse a AWS Unified Operations

Un firmado AWS Contrato de operaciones unificadas. Para obtener más información, póngase en contacto con su AWS representante de ventas.

- Identificó las necesidades empresariales, como la migración, la modernización, los eventos, el tiempo de actividad previsto, etc.
- Una lista de sus cargas de trabajo.
- Una lista suya Cuentas de AWS y de las asociadas Regiones de AWS.
- Identificó a las partes interesadas de los equipos de aplicaciones, arquitectura, operaciones y seguridad.

Primeros pasos en las operaciones unificadas: incorpore alarmas críticas para una gestión rápida de los incidentes

Para poder notificarle rápidamente los incidentes críticos, complete los siguientes pasos para incorporar sus alarmas a la detección y respuesta a AWS incidentes

1. Defina y configure sus alarmas críticas para una gestión rápida de los incidentes. Para obtener información detallada, consulte [Definir y configurar las alarmas en la detección y respuesta a incidentes](#) en la Guía del usuario de detección y respuesta a incidentes.
 - a. Para conocer los pasos para configurar las alarmas con Amazon CloudWatch, consulta [Definir y configurar alarmas en Detección y respuesta a incidentes](#) en la Guía del usuario de detección y respuesta a incidentes. Para obtener AWS recomendaciones sobre los tipos de alarmas críticas para varios tipos Servicios de AWS, consulte [Detección y respuesta a incidentes \(IDR\)](#). Póngase en contacto con su equipo de operaciones AWS unificadas si AWS desea automatizar la creación de AWS alarmas críticas para sus AWS recursos etiquetados.
 - b. Para redirigir o ingerir alarmas críticas de herramientas de APM de terceros con [EventBridge integración directa con Amazon](#), como DataDog, etc. NewRelic, consulte [Ingesta de alarmas de APM que tienen integración directa con Amazon EventBridge](#) en la Guía del usuario de detección y respuesta a AWS incidentes. Debe implementar un conjunto de AWS recursos (AWS Lambda y reglas del bus de EventBridge eventos de Amazon) para transformar y redirigir su alarma (evento) a la detección y respuesta a AWS incidentes. Su equipo de operaciones AWS unificadas puede ayudarlo a proporcionar la CloudFormation plantilla para instalar estos recursos.
 - c. Redirige o ingiere alarmas críticas desde tu herramienta de monitorización personalizada a través de una herramienta de APM de terceros que no tenga una integración directa con Amazon. EventBridge Para obtener más información, consulta [Cómo usar webhooks para ingerir alarmas de APM sin una integración directa con Amazon EventBridge](#) en la Guía del usuario de detección y respuesta a AWS incidentes. Debe implementar un conjunto de AWS recursos (AWS Lambda funciones de API Gateway y reglas de bus de EventBridge eventos de Amazon) para transformar y redirigir su alarma (evento) a AWS Incident Detection and Response. Su equipo de operaciones AWS unificadas puede ayudarlo a proporcionar la CloudFormation plantilla para instalar estos recursos.
2. Proporcione los detalles de la arquitectura de la carga de trabajo, la información del punto de contacto y la información preliminar sobre las acciones de mitigación en caso de alarmas críticas. Para ello, siga los pasos que se describen a continuación:

- Descargue y complete el [cuestionario de incorporación de cargas de trabajo de detección y respuesta a AWS incidentes](#) para cada carga de trabajo o aplicación crítica y el [cuestionario de incorporación de alarmas relacionado con](#) cada carga de trabajo única.

La información de estos cuestionarios ayuda al AWS equipo a elaborar un manual de corrección de incidentes. Este manual permite tomar las medidas adecuadas para solucionar y corregir rápidamente las alarmas críticas antes de que provoquen un tiempo de inactividad empresarial. Para ver ejemplos y ejemplos de información, consulte los [cuestionarios sobre la incorporación de la carga de trabajo y la ingesta de alarmas en](#) la sección Detección y respuesta a incidentes. AWS

3. Proporcione acceso para incorporar sus alarmas críticas a la detección y respuesta a AWS incidentes
 - a. Implemente la función `AWSServiceRoleForHealth_EventProcessor` vinculada al servicio (SLR) en la Cuenta de AWS gestión de la carga de trabajo crítica para que el equipo de gestión de AWS incidentes la supervise. Para obtener más información, consulte [Proporcionar acceso para la ingesta de alertas a la detección y respuesta a AWS incidentes](#).

 Note

Para ayudarle a incorporar una cámara réflex de gran tamaño Cuentas de AWS, AWS podemos proporcionarle un AWS Command Line Interface script que agilice el aprovisionamiento de esta cámara réflex.

- b. (Opcional) Si tus alarmas están en Amazon CloudWatch, asegúrate de que el AWS Identity and Access Management usuario o rol que se utiliza para las pruebas de alarmas (antes de la puesta en marcha) tenga el permiso de `cloudwatch:SetAlarmState` IAM en el Cuenta de AWS que se ejecuta la carga de trabajo crítica. Esto es necesario para probar las alarmas (el día del partido) tras la incorporación. Para obtener más información, consulte [Probar las cargas de trabajo integradas en AWS Detección](#) y respuesta a incidentes.
4. Cree un AWS Support caso para suscribir una carga de trabajo para una gestión rápida de los incidentes. Tenga en cuenta que Cuenta de AWS está habilitada automáticamente para la gestión rápida de incidentes entrantes, lo que significa que puede enviar un caso a la cola de detección y respuesta a incidentes de Unified Operations a través de la consola del Support Center AWS Command Line Interface, el o el AWS SDK para tomar medidas rápidas. AWS Para supervisar y crear incidentes de forma proactiva con un AWS Support caso saliente, cree un

AWS Support caso para su carga de trabajo crítica. Para ello, siga los pasos que se describen a continuación:

- a. Inicie sesión en [AWS Support Center Console](#), seleccione Crear caso y, a continuación, seleccione Soporte técnico.
- b. En Servicio, selecciona Detección y respuesta a incidentes.
- c. En Categoría, seleccione Incorporar una nueva carga de trabajo.
- d. En Gravedad, selecciona Guía general.
- e. Adjunte los cuestionarios de carga de trabajo y alarma que completó en el paso anterior.

Primeros pasos en las operaciones unificadas: cómo solicitar una respuesta a un incidente en 5 minutos

AWS Unified Operations ofrece una respuesta a incidentes en 5 minutos para sus incidentes críticos. Para solicitar una respuesta entrante de 5 minutos, puede [crear un caso de soporte a partir de una interacción de soporte](#) o utilizar el [método de creación de casos de soporte tradicional](#). Al crear su caso, asegúrese de introducir la siguiente información para garantizar que su caso reciba una respuesta en un plazo de 5 minutos:

Note

Utilice este método independientemente de si utiliza la supervisión proactiva o no, o si se producen incidentes antes de que se complete la configuración de la alarma.

1. En Tipo de caso, elija Técnico.
2. En Servicio, selecciona el AWS servicio afectado.
3. En Categoría, elige la opción que mejor se adapte a tu problema.
4. En Gravedad, selecciona Business-critical Sistema inactivo.
5. En la descripción, incluya la siguiente información
 - a. Información técnica
 - Nombre de carga de trabajo
 - ARN (s) de los AWS recursos afectados
 - b. Información empresarial

- Descripción del impacto en el negocio
- (Opcional) Detalles del puente con el cliente

Note

La eficacia de la resolución depende del contexto disponible. Las cargas de trabajo integradas con alarmas se benefician del acceso inmediato a información completa sobre las cargas de trabajo, mientras que las cargas de trabajo no integradas comienzan con los datos sobre el estado del servicio y la información proporcionada por el cliente.

Primeros pasos de las operaciones unificadas: planifique la cobertura del dominio

AWS Unified Operations proporciona experiencia especializada a través de un enfoque de cobertura basado en el dominio. Cada dominio cuenta con el apoyo de un equipo de especialistas en AWS dominios que proporcionan los siguientes servicios:

- Experiencia especializada adaptada a sus áreas tecnológicas específicas.
- Cobertura continua con disponibilidad a través de sus herramientas de colaboración preferidas (Slack o Microsoft Teams) durante los días hábiles.
- Asesoramiento proactivo sobre la arquitectura, las mejores prácticas y las oportunidades de optimización.
- Respuesta mejorada a los incidentes mediante un profundo conocimiento del campo y familiaridad con las cargas de trabajo.
- Una experiencia uniforme mantenida por un equipo coordinado y no por individuos.

Este enfoque de cobertura de dominios permite a los AWS especialistas mantener un profundo conocimiento de sus cargas de trabajo críticas y, al mismo tiempo, brindar un soporte integral en toda su gama de tecnologías.

Para seleccionar los dominios, las organizaciones mantienen la autoridad de decisión entre una selección de 23 AWS dominios y tienen en cuenta los siguientes factores a la hora de decidir:

- Cargas de trabajo críticas de Servicios de AWS ejecución principales
- Servicio de AWS Dependencias críticas (como Amazon EC2, Amazon EKS o Amazon RDS)

- Los próximos eventos importantes que requieren una cobertura de soporte ininterrumpida (migraciones, lanzamientos) están planificados en un plazo de 3 a 6 meses

Esta información, combinada con la orientación de su gerente técnico de cuentas, permite alinear con precisión la experiencia en el campo con las necesidades específicas de su organización, lo que le ayuda a mantener un soporte óptimo para las cargas de trabajo de misión crítica.

Primeros pasos en las operaciones unificadas: incorpore su cuenta a una gestión proactiva de los incidentes de seguridad

Las operaciones unificadas le permiten prepararse, responder y recuperarse rápidamente de los incidentes de seguridad, como la apropiación de cuentas, las filtraciones de datos y los ataques de ransomware. Respuesta frente a incidencias de seguridad de AWS Respuesta frente a incidencias de seguridad de AWS clasifica los hallazgos, intensifica los eventos y gestiona los casos críticos, al tiempo que proporciona acceso al equipo de respuesta a incidentes del AWS cliente (CIRT) para investigar los recursos afectados. Este acceso le ayuda a mitigar y resolver de forma eficaz los incidentes de seguridad, minimizando el impacto en sus operaciones. Para incorporar esta función de servicio, complete los siguientes pasos:

1. Cree un formulario centralizado Cuenta de AWS Respuesta frente a incidencias de seguridad de AWS. Esto se Cuenta de AWS usará para configurar todos los demás Cuentas de AWS que desee monitorear, para administrar su equipo de respuesta a incidentes y para crear y ver los eventos de seguridad. Le recomendamos que alinee esta cuenta con la cuenta que utiliza para otros servicios de seguridad, como Amazon GuardDuty y AWS Security Hub CSPM. Puedes usar una cuenta [AWS Organizations](#) de administración o una cuenta de administrador AWS Organizations delegado como cuenta de membresía de Security Incident Response. Para obtener más información, consulte [Seleccionar una cuenta de membresía](#) en la Guía del Respuesta frente a incidencias de seguridad de AWS usuario.
 - a. Elija los detalles básicos de la membresía. Para obtener más información, consulte [Configurar los detalles de la membresía](#) en la Guía del Respuesta frente a incidencias de seguridad de AWS usuario.
 - b. Elija con qué desea asociar las cuentas AWS Organizations. Para obtener más información, consulte [Asociar cuentas a AWS Organizations](#) en la Guía del Respuesta frente a incidencias de seguridad de AWS usuario.
 - c. (Opcional) Si lo desea, puede habilitar el flujo de trabajo de respuesta proactiva y clasificación de alertas para que su organización pueda monitorear e investigar las alertas

generadas por Amazon GuardDuty y las AWS Security Hub CSPM integraciones. Para obtener más información, consulte [Configurar flujos de trabajo de respuesta proactiva y clasificación de alertas](#) en la Guía del Respuesta frente a incidencias de seguridad de AWS usuario.

2. (Opcional) Habilite la contención proactiva de un posible incidente de seguridad. AWS puede realizar acciones de contención para mitigar rápidamente el impacto, como aislar los hosts comprometidos o rotar las credenciales. Para activar esta función, primero debe conceder los permisos necesarios al servicio. Para ello, despliega un [Step Functions StackSet](#).

Primeros pasos de operaciones unificadas: AWS expectativas de usted

Para que las operaciones unificadas ofrezcan el máximo valor, recomendamos el siguiente enfoque de colaboración:

Compromiso del equipo

- Identifique a expertos en la materia de su equipo para que colaboren con AWS los ingenieros durante la incorporación y la participación continua.
- Participe en las llamadas de descubrimiento iniciales y en las reuniones posteriores para compartir los detalles de la arquitectura y los requisitos operativos.
- Establezca puntos de contacto periódicos para revisar las actualizaciones de la arquitectura o los cambios en la carga de trabajo.

Integración operativa

- Configure las alarmas críticas en su cuenta para permitir una gestión eficaz de los incidentes.
- Implemente las medidas de acción recomendadas por los AWS especialistas,
- Participe en los ejercicios del día del partido para validar los procesos de respuesta a los incidentes.

Este marco de colaboración lo ayuda a maximizar el valor de las operaciones unificadas, alcanzar sus objetivos de tiempo de actividad, mitigar los riesgos operativos y recibir un soporte integral para sus cargas de trabajo de misión crítica.

Primeros pasos en las operaciones unificadas: lo que puede esperar de AWS

Cuando se incorpore a Unified Operations, puede esperar lo siguiente AWS.

- Proporcione un equipo de AWS expertos designados con una amplia experiencia técnica en el ámbito y los servicios de su carga de trabajo.
- Ofrezca orientación proactiva, optimización continua y recomendaciones de mejora continua para mejorar el rendimiento y la resiliencia de las cargas de trabajo y acelerar el proceso de migración y modernización.
- Ayude a brindar una respuesta rápida a los incidentes, con ingenieros sensibles al contexto que contratan en un plazo de 5 minutos después de plantear un caso de soporte crítico para la empresa.

Note

La eficacia de la resolución depende del contexto disponible. Las cargas de trabajo integradas con alarmas se benefician del acceso inmediato a información completa sobre las cargas de trabajo, mientras que las cargas de trabajo no integradas comienzan con los datos sobre el estado del servicio y la información proporcionada por el cliente.

- Ofrezca un soporte integral durante todo el ciclo de vida de la aplicación, desde el diseño y la migración hasta el lanzamiento de la producción y las operaciones a largo plazo.
- Supervise de forma proactiva las amenazas a la seguridad con la clasificación automática, lo que reduce los falsos positivos y aumenta los incidentes para posibles incidentes de seguridad.
- Ayude a solucionar problemas y a mitigar de forma conjunta el incidente de seguridad que AWS haya identificado.

Cambio AWS Support Planes

Puede usar la consola de AWS Support planes para cambiar el plan de soporte para su Cuenta de AWS. Para cambiar su plan de soporte, debe tener permisos AWS Identity and Access Management (de IAM). Para obtener más información, consulte [Gestione el acceso a AWS Support Planes](#) y [AWS políticas gestionadas para AWS Support 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) Para comparar los planes de asistencia, en la página AWS Support Planes, selecciona Comparar todos los Soporte planes y funciones.

3. (Opcional) Para ver los costos estimados de un plan de soporte, elija la calculadora de precios. En la calculadora de precios, seleccione un nivel de soporte, introduzca una estimación de cuánto espera gastar AWS cada mes y, a continuación, seleccione Calcular.
4. Para reducir su plan Enterprise Support, póngase en contacto con su administrador técnico de cuentas (TAM).

Para bajar de categoría tu plan Business Support+, en la página Administrar [planes de soporte](#), selecciona Revisar la reducción de categoría en la sección Plan básico Soporte .

Para actualizar a un plan AWS Enterprise Support o AWS Unified Operations, elija Contactar con el departamento de ventas.

Para actualizar a un plan AWS Business Support+ desde Basic Soporte, complete los siguientes pasos:

- a. Selecciona Comenzar en la sección AWS Business Support+.
- b. Si está incorporado AWS Organizations y tiene activado el modo con todas las funciones, puede suscribir a toda su organización a Business Support+. Para obtener información sobre el modo con todas las funciones, consulte [Habilitar todas las funciones para una organización](#) en la Guía del usuario. AWS Organizations Para inscribirse a nivel de organización, seleccione el botón de opción Mi organización. Revisa los [detalles y los precios del plan](#) y, a continuación, marca la casilla para aceptar las condiciones de la suscripción. Solo la cuenta de administración de su organización puede suscribir a toda la organización.

O bien, para inscribirse a nivel de cuenta, selecciona el botón de opción Mi cuenta y, a continuación, marca la casilla para aceptar las condiciones de la suscripción.

- c. Selecciona Confirmar la actualización para completar la suscripción al plan AWS Business Support+.

 Note

Después de suscribir a toda la organización a AWS Business Support+, todas las cuentas nuevas que se creen en esa organización se suscriben automáticamente a AWS Business Support+. Si una cuenta que anteriormente estaba suscrita a AWS Business Support+ a nivel de organización abandona la organización, esa cuenta pasa al plan de soporte básico.

 Note

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](#).

Información relacionada

[Para obtener más información sobre los planes, consulta las preguntas frecuentes AWS Support .AWS Support](#) 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 .

Configure las notificaciones de caducidad del plan promocional

Puede utilizar [AWS User Notifications](#) para configurar las notificaciones que le informen cuando finalice el período promocional de su plan de soporte. Puedes suscribirte para recibir notificaciones por correo electrónico, en el AWS Console Mobile Application canal de chat o en otros canales de chat de tu elección.

Configure las notificaciones de caducidad del plan de soporte promocional

1. Abra las notificaciones de usuario en [Consola de administración de AWS](#):
 - a. Elija el icono de campana, en la barra de navegación.
 - b. Seleccione el centro de notificaciones.
 - c. En el panel de navegación, elija Configuración de notificaciones.
 - d. Elija Crear configuración de notificación.
 - e. Seleccione al menos un Centro de configuración. Para obtener más información, consulte [Almacenamiento, procesamiento y replicación de notificaciones mediante centros de notificaciones en AWS User Notifications](#).
2. En Regla de eventos, introduzca la siguiente información:
 - En Nombre del Servicio de AWS , escriba Planes de soporte.
 - En Tipo de evento, introduzca Caducidad de la promoción del plan de soporte.

- En el caso de las regiones, selecciona la fuente Regiones de AWS en la que deseas recibir las notificaciones. Para esta opción, seleccione Este de EE. UU. (Norte de Virginia), Este de EE. UU. (Ohio), Oeste de EE. UU. (Norte de California) y Oeste de EE. UU. (Oregón).
3. Configure los ajustes de agregación para reducir la frecuencia de las notificaciones. Se recomienda configurar la agregación en Recibir en un plazo de 5 minutos.
 4. Configure los canales de entrega en los que desea recibir notificaciones. Si no seleccionas un canal de entrega, puedes ver las notificaciones seleccionando el icono de la campana en la barra de Consola de administración de AWS navegación.

Para obtener instrucciones detalladas sobre cómo crear notificaciones configuradas por el usuario, consulta el [paso 1: crear una configuración de notificaciones en la Guía del AWS User Notifications usuario](#).

Ver las notificaciones del plan promocional

Sus notificaciones se envían al canal de entrega que eligió durante la configuración. También puede ver las notificaciones cuando selecciona el icono de campana de la barra de navegación de la consola. El icono de la campana muestra una insignia roja cuando hay nuevas notificaciones disponibles.

Para obtener más información sobre la visualización de las notificaciones, consulte [Paso 2: Visualización de las notificaciones](#) en la Guía del usuario de AWS User Notifications .

On-Ramp Fin del soporte para desarrolladores, empresas y empresas

Para obtener información sobre la transición a un nuevo plan, consulte la siguiente información específica de su plan y las [AWS Support Preguntas frecuentes](#).

Note

Developer Support, Business Support y Enterprise On-Ramp seguirán estando disponibles en la AWS GovCloud (US) región.

Desarrollador Soporte planifique el fin del soporte

Aviso de fin de soporte: el soporte para desarrolladores se suspenderá el 1 de enero de 2027. Los clientes con soporte para desarrolladores pueden seguir usando su plan actual o optar por actualizarse a Business Support+ en cualquier momento antes del 1 de enero de 2027. Business Support+ ofrece AI-powered asistencia que comprende el contexto de sus operaciones, con 24/7 acceso a AWS expertos a un precio 29/month mínimo de \$ por cuenta. Para obtener más información, consulta los [detalles del plan Business Support+](#).

Usuarios Soporte planifique el fin del soporte

Aviso de fin de soporte: el soporte empresarial se suspenderá el 1 de enero de 2027. Los clientes con Business Support pueden seguir usando su plan actual o optar por actualizarse a Business Support+ en cualquier momento antes del 1 de enero de 2027. Business Support+ ofrece AI-powered asistencia que comprende el contexto de sus operaciones, con 24/7 acceso a AWS expertos a un precio 29/month mínimo de \$ por cuenta. Para obtener más información, consulta los detalles del [plan Business Support+](#)

On-Ramp Fin del soporte empresarial

Aviso de fin de soporte: el 1 de enero de 2027, AWS se suspenderá Enterprise. On-Ramp A lo largo de 2026, On-Ramp los clientes empresariales pasarán automáticamente a AWS Enterprise Support durante la renovación del contrato o en lotes periódicos. Los clientes recibirán una notificación por correo electrónico un mes antes de la actualización. No hay que hacer nada más. Enterprise Support proporciona una asignación de TAM designada, tiempos de respuesta de 15 minutos y Respuesta frente a incidencias de seguridad de AWS está disponible sin costo adicional, todo a un precio mínimo inferior de 5000\$ (reducido de 15 000\$). Para obtener más información, consulte los detalles del [Soporte plan AWS Enterprise](#).

AWS Trusted Advisor

Important

Aviso de fin de soporte: el soporte para desarrolladores se suspenderá el 1 de enero de 2027. Los clientes con soporte para desarrolladores pueden seguir usando su plan actual o optar por actualizarse a Business Support+ en cualquier momento antes del 1 de enero de 2027. Business Support+ ofrece asistencia basada en inteligencia artificial que comprende el contexto de sus operaciones, con acceso a AWS expertos las 24 horas del día, los 7 días de la semana, a un precio mínimo de 29 USD al mes por cuenta. Para obtener más información, consulta los detalles del [plan Business Support+](#)

Aviso de fin de soporte: el soporte empresarial se suspenderá el 1 de enero de 2027. Los clientes con Business Support pueden seguir usando su plan actual o optar por actualizarse a Business Support+ en cualquier momento antes del 1 de enero de 2027. Business Support+ ofrece asistencia basada en inteligencia artificial que comprende el contexto de sus operaciones, con acceso a AWS expertos las 24 horas del día, los 7 días de la semana, a un precio mínimo de 29 USD al mes por cuenta. Para obtener más información, consulta los detalles del [plan Business Support+](#)

Aviso de fin de soporte: el 1 de enero de 2027, Enterprise AWS On-Ramp dejará de funcionar. A lo largo de 2026, los clientes de Enterprise On-Ramp pasarán automáticamente a AWS Enterprise Support durante la renovación del contrato o en lotes periódicos. Los clientes recibirán una notificación por correo electrónico un mes antes de la actualización. No hay que hacer nada más. Enterprise Support proporciona una asignación de TAM designada, tiempos de respuesta de 15 minutos y Respuesta frente a incidencias de seguridad de AWS está disponible sin costo adicional, todo a un precio mínimo inferior de 5000\$ (reducido de 15 000\$). Para obtener más información, consulte los detalles del [Soporte plan AWS Enterprise](#). Para obtener más información, consulte [On-Ramp Fin del soporte para desarrolladores, empresas y empresas](#).

Developer Support, Business Support y Enterprise On-Ramp seguirán estando disponibles en la AWS GovCloud (US) región.

Trusted Advisor se basa en las mejores prácticas aprendidas al prestar servicio 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.

AWS Trusted Advisor los cheques están disponibles para los clientes con un plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations.

Si tiene un plan Basic o Developer Support, puede utilizar la Trusted Advisor consola para acceder a todas las comprobaciones de la categoría Límites de servicio y a [determinadas comprobaciones](#) de las categorías de Seguridad y Tolerancia a fallos. En los planes Basic y Developer Support no están disponibles las actualizaciones automáticas de las verificaciones. Debe actualizar manualmente las Trusted Advisor comprobaciones de la categoría Seguridad. Para actualizar una verificación de manera manual, se debe hacer lo siguiente:

Si tiene un plan Basic Support, puede utilizar la Trusted Advisor consola para acceder a todas las comprobaciones de la categoría Límites de servicio y a [determinadas comprobaciones](#) de las categorías de Seguridad y Tolerancia a fallos. En los planes Basic y Developer Support no están disponibles las actualizaciones automáticas de las verificaciones. Debe actualizar manualmente las Trusted Advisor comprobaciones de la categoría Seguridad. Para actualizar una verificación de manera manual, se debe hacer lo siguiente:

1. Inicia sesión en la Trusted Advisor consola de <https://console.aws.amazon.com/trustedadvisor/tu casa>.
2. Seleccione el botón Actualizar en la verificación que se desee actualizar.

Si tiene un plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puede 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 Consola de administración de AWS. Para obtener más información sobre cómo controlar el acceso a la Trusted Advisor consola, consulte [Gestione el acceso a AWS Trusted Advisor](#).

Para obtener más información, consulte [Trusted Advisor](#).

Temas

- [Comience con Trusted Advisor las recomendaciones](#)
- [Comience con la Trusted Advisor API](#)
- [Uso de Trusted Advisor como un servicio web](#)

- [Vista organizativa de AWS Trusted Advisor](#)
- [Ver AWS Trusted Advisor cheques impulsados por AWS Config](#)
- [Visualización de AWS Security Hub CSPM los controles en AWS Trusted Advisor](#)
- [Optar AWS Compute Optimizer por recibir Trusted Advisor cheques](#)
- [Comience con AWS Trusted Advisor Priority](#)
- [AWS Trusted Advisor comprobar referencia](#)
- [Registro de cambios para AWS Trusted Advisor](#)

Comience con Trusted Advisor las recomendaciones

Important

Aviso de fin de soporte: el soporte para desarrolladores se suspenderá el 1 de enero de 2027. Los clientes con soporte para desarrolladores pueden seguir usando su plan actual o optar por actualizarse a Business Support+ en cualquier momento antes del 1 de enero de 2027. Business Support+ ofrece AI-powered asistencia que comprende el contexto de sus operaciones, con 24/7 acceso a AWS expertos a un precio 29/month mínimo de \$ por cuenta. Para obtener más información, consulta los detalles del [plan Business Support+](#)

Aviso de fin de soporte: el soporte empresarial se suspenderá el 1 de enero de 2027. Los clientes con Business Support pueden seguir usando su plan actual o optar por actualizarse a Business Support+ en cualquier momento antes del 1 de enero de 2027. Business Support + ofrece AI-powered asistencia que comprende el contexto de sus operaciones, con 24/7 acceso a AWS expertos a un precio 29/month mínimo de \$ por cuenta. Para obtener más información, consulta los detalles del [plan Business Support+](#)

Aviso de fin de soporte: el 1 de enero de 2027, AWS se suspenderá Enterprise. On-Ramp A lo largo de 2026, On-Ramp los clientes de Enterprise pasarán automáticamente a AWS Enterprise Support durante la renovación del contrato o en lotes periódicos. Los clientes recibirán una notificación por correo electrónico un mes antes de la actualización. No hay que hacer nada más. Enterprise Support proporciona una asignación de TAM designada, tiempos de respuesta de 15 minutos y Respuesta frente a incidencias de seguridad de AWS está disponible sin costo adicional, todo a un precio mínimo inferior de 5000\$ (reducido de 15 000\$). Para obtener más información, consulte los detalles del [Soporte plan AWS Enterprise](#). Para obtener más información, consulte [On-Ramp Fin del soporte para desarrolladores, empresas y empresas](#).

Developer Support, Business Support y Enterprise On-Ramp seguirán estando disponibles en la AWS GovCloud (US) región.

Puedes usar la página de Trusted Advisor recomendaciones de la Trusted Advisor consola para revisar los resultados de las 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](#)
- [Ver categorías de verificación](#)
- [Ver verificaciones específicas](#)
- [Filtrar sus verificaciones](#)
- [Actualizar resultados de verificaciones](#)
- [Descargar los resultados de la verificación](#)
- [Vista organizativa](#)
- [Preferencias](#)

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 Recommendations 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.

Trusted Advisor > Recommendations

Trusted Advisor Recommendations

Refresh all checks

Download all checks

Use this page to get an overview of the check results in your AWS account. Choose a check name or category to view the recommended actions or potential issues that Trusted Advisor has identified. Each check provides more information about how to address any issues. You can also download a summary of all check results. [Learn more](#)

Checks summary

42

Action recommended

Info

Security	30
Performance	1
Fault tolerance	9
Cost optimization	1
Service limits	1

127

Investigation recommended

Info

Fault tolerance	29
Performance	9
Operational Excellence	12
Cost optimization	14
Security	63

28

Checks with excluded items

Info

Security	11
Cost optimization	11
Service limits	1
Performance	2
Fault tolerance	3

Potential monthly savings

\$7,082.26

Trusted Advisor has identified 18 cost optimization checks that can save you money. For example, you might have unused resources in your AWS account that can be deleted. Choose a cost optimization check to view the recommendations.

View all cost optimization checks

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.
- Para cada verificación, elija el icono de actualización
 para actualizar esta verificación.
 - 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.

Cost optimization Refresh all checks Download all checks

Choose a check name to see recommendations for ways to help save money for your AWS account. Trusted Advisor might recommend that you delete unused and idle resources, or use reserved capacity.

Overview

Potential monthly savings \$7,082.26	 1 Action recommended Info	 14 Investigation recommended Info	 10 No problems detected Info	 11 Checks with excluded items Info

Cost optimization checks

Filter by tag key [Learn more about using tags](#)

Tag Key Tag Value Reset Apply filter

Search by keyword [Info](#) Source View

All sources < 1 2 >

▶  **Amazon Comprehend Underutilized Endpoints**

Checks the throughput configuration of your endpoints.

Last updated: 2 hours ago  

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.

▼

 Low Utilization Amazon EC2 Instances

Last updated: 14 hours ago  

Checks the Amazon Elastic Compute Cloud (Amazon EC2) instances that were running at any time during the last 14 days and alerts you if the daily CPU utilization was 10% or less and network I/O was 5 MB or less on 4 or more days. Running instances generate hourly usage charges. Although some scenarios can result in low utilization by design, you can often lower your costs by managing the number and size of your instances.

Estimated monthly savings are calculated by using the current usage rate for On-Demand Instances and the estimated number of days the instance might be underutilized. Actual savings will vary if you are using Reserved Instances or Spot Instances, or if the instance is not running for a full day. To get daily utilization data, download the report for this check.

Alert Criteria

Yellow: An instance had 10% or less daily average CPU utilization and 5 MB or less network I/O on at least 4 of the previous 14 days.

Recommended Action

Consider stopping or terminating instances that have low utilization, or scale the number of instances by using Auto Scaling. For more information, see [Stop and Start Your Instance](#), [Terminate Your Instance](#), and [What is Auto Scaling?](#)

Additional Resources

[Monitoring Amazon EC2](#)
[Instance Metadata and User Data](#)
[Amazon CloudWatch Developer Guide](#)
[Auto Scaling Developer Guide](#)

Low Utilization Amazon EC2 Instances (38)

Exclude & Refresh

Included items ▼

38 of 39 Amazon EC2 instances have low average daily utilization. Monthly savings of up to \$713.23 might be available by minimizing underutilized instances. 1 items have been excluded.

< 1 2 > 

Region/AZ ▼	Instance ID ▼	Instance Name ▼	Instance Type ▼	Estimated Monthly Savings ▼	CPU Utilization 14-Day Average ▼
ca-central-1b	i-0f818268643c7ae32		t2.micro	\$9.22	0.1%
ca-central-1a	i-06c233a11aa626588		t2.micro	\$9.22	0.1%

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 de 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 tiene un plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, actualiza Trusted Advisor automáticamente los cheques de su 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, seleccione 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-Architected alto 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 CSPM habilitaste tu cuenta, no podrás usar la Trusted Advisor consola para actualizar los controles CSPM de Security Hub. Para obtener más información, consulte [Actualice sus hallazgos sobre el CSPM de Security Hub](#).

Descargar los resultados de la verificación

Puedes descargar los resultados de las comprobaciones para obtener una visión general de tu Trusted Advisor cuenta. 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

Puede configurar la función de visualización de la organización para crear un informe para todas las cuentas de los miembros de su AWS organización. Para obtener más información, consulte [Vista organizativa de 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 función [Vista organizativa de AWS Trusted Advisor](#) y [Trusted Advisor Priority](#).

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 [Administra las notificaciones Trusted Advisor prioritarias](#).

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 Administración de facturación y costos de AWS 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 de 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 con la Trusted Advisor API

Important

Aviso de fin de soporte: el soporte para desarrolladores se suspenderá el 1 de enero de 2027. Los clientes con soporte para desarrolladores pueden seguir usando su plan actual o optar por actualizarse a Business Support+ en cualquier momento antes del 1 de enero de 2027. Business Support+ ofrece asistencia basada en inteligencia artificial que comprende el contexto de sus operaciones, con acceso a AWS expertos las 24 horas del día, los 7 días de la semana, a un precio mínimo de 29 USD al mes por cuenta. Para obtener más información, consulta los detalles del [plan Business Support+](#)

Aviso de fin de soporte: el soporte empresarial se suspenderá el 1 de enero de 2027. Los clientes con Business Support pueden seguir usando su plan actual o optar por actualizarse a Business Support+ en cualquier momento antes del 1 de enero de 2027. Business Support+ ofrece asistencia basada en inteligencia artificial que comprende el contexto de sus operaciones, con acceso a AWS expertos las 24 horas del día, los 7 días de la semana, a un precio mínimo de 29 USD al mes por cuenta. Para obtener más información, consulta los detalles del [plan Business Support+](#)

Aviso de fin de soporte: el 1 de enero de 2027, Enterprise AWS On-Ramp dejará de funcionar. A lo largo de 2026, los clientes de Enterprise On-Ramp pasarán automáticamente a AWS Enterprise Support durante la renovación del contrato o en lotes periódicos. Los clientes recibirán una notificación por correo electrónico un mes antes de la actualización. No hay que hacer nada más. Enterprise Support proporciona una asignación de TAM designada, tiempos de respuesta de 15 minutos y Respuesta frente a incidencias de seguridad de AWS está disponible sin costo adicional, todo a un precio mínimo inferior de 5000\$ (reducido de 15 000\$). Para obtener más información, consulte los detalles del [Soporte plan AWS Enterprise](#). Para obtener más información, consulte [On-Ramp Fin del soporte para desarrolladores, empresas y empresas](#).

Developer Support, Business Support y Enterprise On-Ramp seguirán estando disponibles en la AWS GovCloud (US) región.

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 AWS Business Support+, AWS Enterprise Support o AWS Unified Operations para usar la Trusted Advisor API.
- Si llamas a la AWS Trusted Advisor API desde una cuenta que no tiene un plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, 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 puede actualizar el ciclo de vida de las recomendaciones. Para administrar recomendaciones, utilice las siguientes operaciones de API.

- Usa las operaciones [ListChecksListRecommendationsGetRecommendation](#), y [ListRecommendationResources](#) API para ver las recomendaciones y las cuentas y los recursos correspondientes.
- Usa la operación [UpdateRecommendationLifecycle](#) API para actualizar el ciclo de vida de una recomendación gestionada por Trusted Advisor Priority.
- Usa la operación de la [BatchUpdateRecommendationResourceExclusion](#) API para incluir o excluir uno o más recursos de tus Trusted Advisor resultados.
- Las llamadas [ListOrganizationRecommendationsGetOrganizationRecommendation](#), [ListOrganizationRecommendationResourcesListOrganizationRecommendationAccounts](#), y a la [UpdateOrganizationRecommendationLifecycle](#) API solo admiten las recomendaciones gestionadas por Trusted Advisor Priority. Estas recomendaciones también se denominan recomendaciones

priorizadas. Puede ver y administrar 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 información acerca de la autenticación de solicitudes, [consulte Proceso de firma Signature Version 4](#).

Uso de Trusted Advisor como un servicio web

El servicio de AWS Support le permite escribir aplicaciones que interactúan con [AWS Trusted Advisor](#). En este tema se muestra cómo obtener una lista de comprobaciones de Trusted Advisor, 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

- [Obtener la lista de comprobaciones de Trusted Advisor disponibles](#)
- [Actualizar la lista de comprobaciones de Trusted Advisor disponibles](#)
- [Sondear una comprobación de Trusted Advisor para cambios de estado](#)
- [Solicitar un resultado de comprobación de Trusted Advisor](#)
- [Mostrar detalles de una verificación de Trusted Advisor](#)

Obtener la lista de comprobaciones de Trusted Advisor disponibles

El siguiente fragmento de código Java crea una instancia de un cliente de Soporte que se puede utilizar para llamar a todas las operaciones de la API de Trusted Advisor. A continuación, el código obtiene la lista de verificaciones de Trusted Advisor y sus valores CheckId correspondientes llamando a la operación de la API [DescribeTrustedAdvisorChecks](#). 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());
    }
}
```

Actualizar la lista de comprobaciones de Trusted Advisor disponibles

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

```
// 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());
}
```

Sondear una comprobación de Trusted Advisor para cambios de estado

Después de enviar la solicitud para ejecutar una verificación de Trusted Advisor para generar los datos de estado más recientes, se utiliza la operación de la API [DescribeTrustedAdvisorChecks](#) para solicitar el progreso de la ejecución de la verificación y saber cuándo están listos los nuevos datos para la verificación.

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 demuestra otros usos diversos del servicio de Trusted Advisor:

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.
}

```


Solicitar un resultado de comprobación de Trusted Advisor

Una vez que seleccione la verificación para consultar los resultados detallados, puede enviar una solicitud a través de la operación de la API [DescribeTrustedAdvisorChecks](#).

Tip

Los nombres y las descripciones de las verificaciones de Trusted Advisor 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 API [DescribeTrustedAdvisorChecks](#) para obtener el ID de verificación.

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: la solicitud de un resultado de comprobación de Trusted Advisor no genera datos de resultados actualizados.

Mostrar detalles de una verificación de Trusted Advisor

El siguiente fragmento de código de Java se itera a través de la instancia `DescribeTrustedAdvisorCheckResultResult` devuelta en la sección anterior para obtener una lista de recursos etiquetados mediante la comprobación de 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 de AWS Trusted Advisor

Important

Aviso de fin de soporte: el soporte para desarrolladores se suspenderá el 1 de enero de 2027. Los clientes con soporte para desarrolladores pueden seguir usando su plan actual o optar por actualizarse a Business Support+ en cualquier momento antes del 1 de enero de 2027. Business Support+ ofrece AI-powered asistencia que comprende el contexto de sus operaciones, con 24/7 acceso a AWS expertos a un precio 29/month mínimo de \$ por cuenta. Para obtener más información, consulta los detalles del [plan Business Support+](#)

Aviso de fin de soporte: el soporte empresarial se suspenderá el 1 de enero de 2027. Los clientes con Business Support pueden seguir usando su plan actual o optar por actualizarse a Business Support+ en cualquier momento antes del 1 de enero de 2027. Business Support + ofrece AI-powered asistencia que comprende el contexto de sus operaciones, con 24/7 acceso a AWS expertos a un precio 29/month mínimo de \$ por cuenta. Para obtener más información, consulta los detalles del [plan Business Support+](#)

Aviso de fin de soporte: el 1 de enero de 2027, AWS se suspenderá Enterprise. On-Ramp A lo largo de 2026, On-Ramp los clientes de Enterprise pasarán automáticamente a AWS Enterprise Support durante la renovación del contrato o en lotes periódicos. Los clientes recibirán una notificación por correo electrónico un mes antes de la actualización. No hay que hacer nada más. Enterprise Support proporciona una asignación de TAM designada, tiempos de respuesta de 15 minutos y Respuesta frente a incidencias de seguridad de AWS

está disponible sin costo adicional, todo a un precio mínimo inferior de 5000\$ (reducido de 15 000\$). Para obtener más información, consulte los detalles del [Soporte plan AWS Enterprise](#). Para obtener más información, consulte [On-Ramp Fin del soporte para desarrolladores, empresas y empresas](#).

Developer Support, Business Support y Enterprise On-Ramp seguirán estando disponibles en la AWS GovCloud (US) región.

La vista organizativa le permite ver los Trusted Advisor cheques de todas las cuentas de su cuenta [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 comprobación de uso de IAM o si ha recomendado acciones para los buckets de Amazon Simple Storage Service (Amazon S3) con la comprobación de permisos de buckets de Amazon S3.

Temas

- [Requisitos previos](#)
- [Habilitar la vista organizativa](#)
- [Actualiza Trusted Advisor los cheques](#)
- [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 AWS servicios para ver Trusted Advisor informes](#)

Requisitos previos

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

- Sus cuentas deben formar parte de una [AWS Organizations](#).

- 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 AWS Business Support+, AWS Enterprise Support o AWS Unified Operations. Puede encontrar su plan de soporte en el AWS Support Centro o en la página de [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 está activado 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. Esta función incluye los permisos Trusted Advisor necesarios para llamar a Organizations en tu nombre. Este rol vinculado al servicio está bloqueado y no puede eliminarlo manualmente. Para obtener más información, consulte [Utilizar funciones vinculadas al servicio para Trusted Advisor](#).

La vista organizativa se activa desde la Trusted Advisor consola.

Para habilitar la vista organizativa

1. Inicie sesión como administrador en la cuenta de administración de la organización y abra la AWS Trusted Advisor consola en <https://console.aws.amazon.com/trustedadvisor>.
2. En el panel de navegación, en Preferences (Preferencias), elija Your organization (Su organización).
3. En Habilitar el acceso de confianza con AWS Organizations, activa 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 AWS Support plan determina qué Trusted Advisor checks están disponibles para una cuenta.

Actualiza Trusted Advisor los cheques

Antes de crear un informe para su organización, le recomendamos que actualice los estados de los Trusted Advisor checks. 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 AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, actualiza Trusted Advisor automáticamente los cheques de su cuenta semanalmente.

 Note

Si tiene cuentas en su organización que tienen un plan de soporte básico o para desarrolladores, el usuario de esas cuentas debe iniciar sesión en la Trusted Advisor consola para actualizar los cheques. No puede actualizar las verificaciones de todas las cuentas desde la cuenta de administración de la organización.

Para actualizar las Trusted Advisor comprobaciones

1. Navegue hasta la AWS Trusted Advisor consola 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 [RefreshTrustedAdvisorCheck](#) de la API.

- 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 en la cuenta de administración de la organización y abra la AWS Trusted Advisor consola 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 de AWS categorías de comprobaciones, las comprobaciones y los estados de los recursos. 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 Región, especifique Regiones de AWS o elija Todos.
 - 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. Para AWS Organizations, selecciona las unidades organizativas (OU) que deseas 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. Seleccione 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)

Report filters

Choose the filter options for your report.

Report name

Trusted-Advisor-report

The report name can be up to 100 characters and can't start with a hyphen. Valid characters: A-Z, a-z, 0-9, and - (hyphen)

Format

JSON

Region

Choose Region

us-east-1 X us-east-2 X us-west-1 X

Check category

Choose category

Security X Performance X

Checks

Choose check names

Resource status

Choose status

All X

En el siguiente ejemplo, el informe incluye la unidad organizativa del equipo de soporte y una AWS cuenta que forman parte de la organización.

AWS organization

You can select the organizational units (OUs) and individual AWS accounts to include in your report.

Organizational structure

▼

Root

r-xa9c

▶

instance-management

ou-xa9c-example1

▼

support-team

ou-xa9c-example2

Jane Doe

111122223333 | janedoe@example.com

Mateo Jackson

444455556666 | mateojackson@example.com

▶

security-team

ou-xa9c-example3

Ana Carolina Silva

777788889999 | anacarolinasilva@example.com

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.

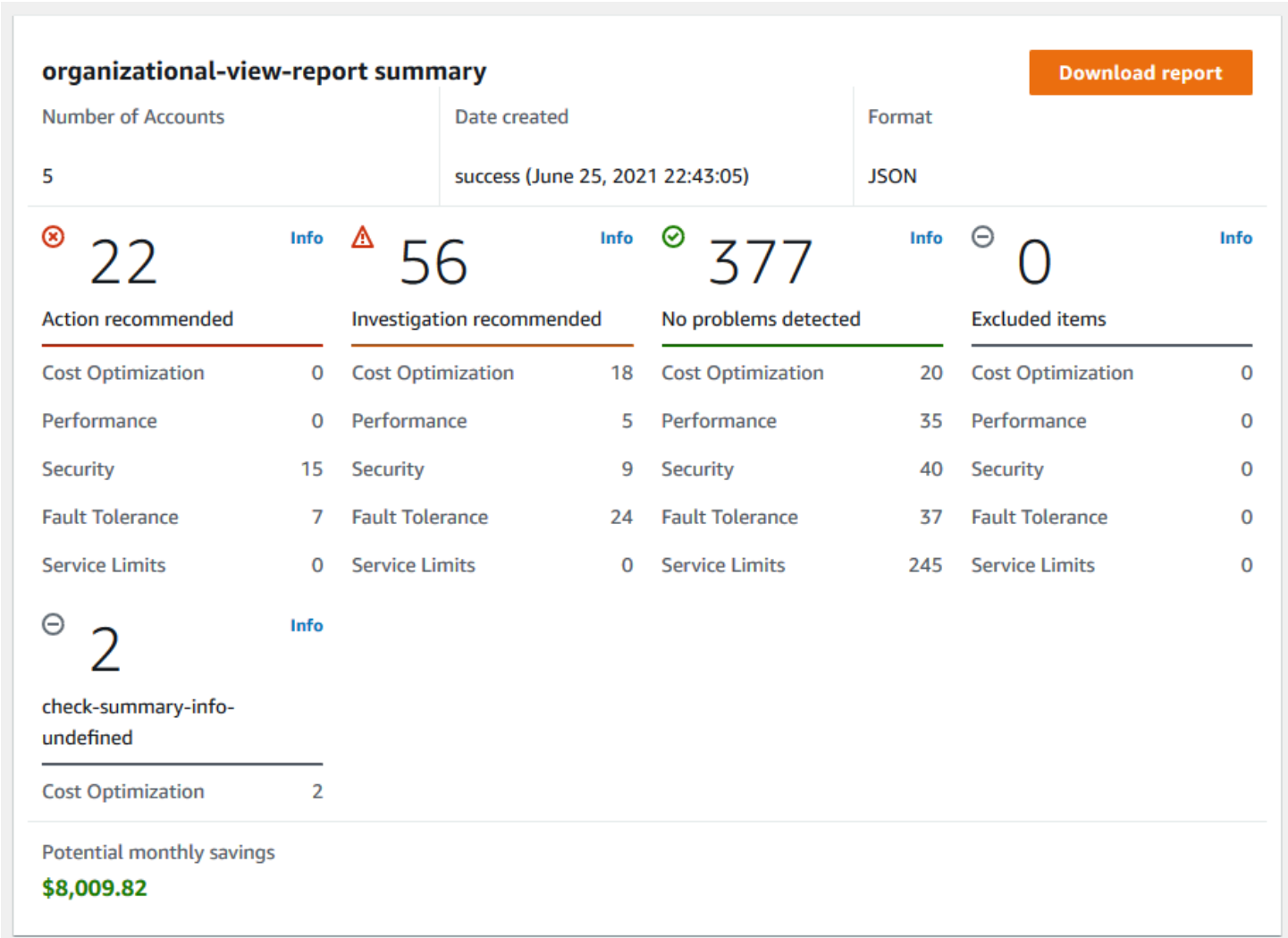
Ver el resumen del informe

Cuando el informe esté listo, podrás ver el resumen del informe desde la Trusted Advisor consola. 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 en la cuenta de administración de la organización y abra la AWS Trusted Advisor consola 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

Cuando el informe esté listo, descárguelo de la Trusted Advisor consola. 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 en la cuenta de administración de la organización y abra la AWS Trusted Advisor consola 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.

Organizational View

With AWS organizations, you can create reports for check results across all AWS accounts within an organization. This provides you a centralized view for all AWS Trusted Advisor checks. You can also view and download reports on this page. Use this report to identify issues and take action for accounts in your organization. [Learn more](#) .

Reports (50)

Create report

Download report

	Report name	Date generated	Status	Format
☐	all-regions-check-report	June 15, 2021 18:43:42	Success	JSON
☐	json-us-east-1-region-only	June 14, 2021 20:54:29	Success	JSON
☐	security-checks-only-all-accounts	June 10, 2021 03:33:59	Success	JSON

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 colores para comprobar los resultados:

- Green— Trusted Advisor no detecta ningún problema en la comprobación.
- Yellow— Trusted Advisor detecta un posible problema con el cheque.
- Red— Trusted Advisor detecta un error y recomienda una acción para la comprobación.
- Blue— no Trusted Advisor puede determinar el estado de la comprobación.

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 identificador del Trusted Advisor cheque
- El ID del recurso
- Marca de tiempo del informe
- El nombre completo del Trusted Advisor cheque
- La categoría del Trusted Advisor cheque
- 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	vioZmlba45kf2JWle_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	Llc4zRaUSiIGRSImqaMa5V	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-_TlmW-5J0	1.58983E+12	IAM Password Policy	Security
7.77789E+11	H7lgTzjTYb	1xHQ5ovV8bS0H1Z-t7Kbik	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 básico o para desarrolladores inician sesión en la Trusted Advisor consola por primera vez. Si tienes un plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, los usuarios pueden tardar hasta una semana en ver los resultados de la comprobación desde el registro de la cuenta. Para obtener más información, consulte [Actualiza Trusted Advisor los cheques](#).
- 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 usar una interfaz SQL con un AWS servicio como Amazon Athena para ejecutar consultas en sus informes. También puede usar Amazon Quick para crear paneles y visualizar sus datos. Para obtener más información, consulte [Uso de otros AWS servicios para ver Trusted Advisor informes](#).

Desactivar la vista organizativa

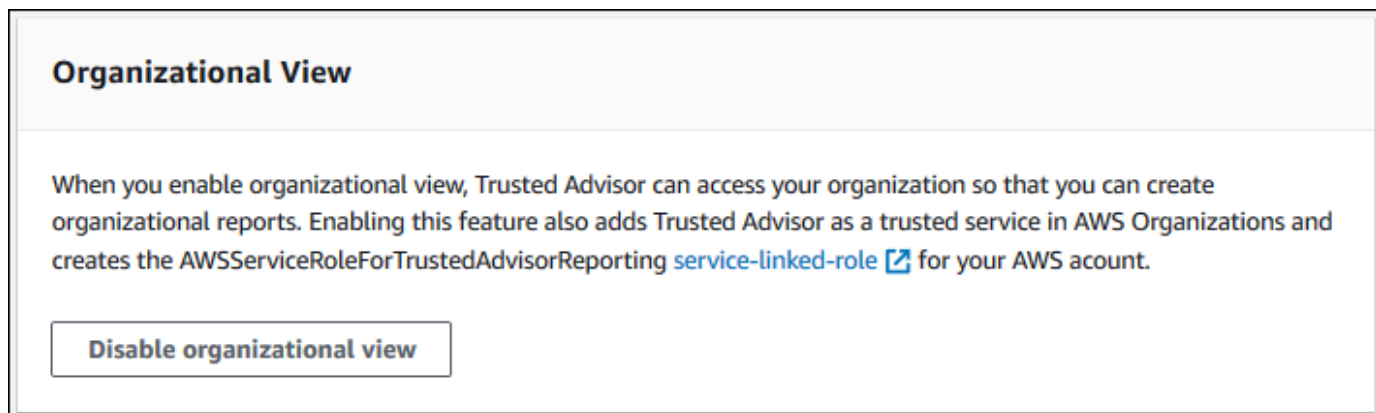
Siga este procedimiento para desactivar la vista organizativa. Debe iniciar sesión con la cuenta de administración de la organización o asumir un rol con los permisos necesarios para desactivar esta característica. No puede desactivar esta característica desde otra cuenta de la organización.

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 deshabilitar la vista organizativa de Trusted Advisor

1. Inicie sesión en la cuenta de administración de la organización y abra la AWS Trusted Advisor consola 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).



Tras deshabilitar la vista organizativa, ya Trusted Advisor no agrega cheques de otras AWS cuentas de la organización. Sin embargo, el rol `AWSServiceRoleForTrustedAdvisorReporting` vinculado al servicio permanece en la cuenta de administración de la organización hasta que lo

elimines a través de la consola de IAM, la API de IAM o (). AWS Command Line Interface AWS CLI
Para obtener más información, consulte [Eliminación de un rol vinculado a servicios](#) en la Guía del usuario de IAM.

Note

Puedes usar otros AWS servicios para consultar y visualizar tus datos para los informes de visualización de la organización. 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 AWS servicios para ver Trusted Advisor informes](#)

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

Puedes usar las siguientes políticas AWS Identity and Access Management (de IAM) para permitir que los usuarios o los roles de tu cuenta accedan a la vista organizacional 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

JSON

```
{
  "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 el acceso de solo lectura a la vista de la organización para. Trusted Advisor Un usuario con estos permisos solo puede ver y descargar informes existentes.

JSON

```
{
  "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 lo has activado AWS CloudTrail en tu cuenta, las siguientes funciones pueden aparecer en tus entradas de registro:

- `AWSServiceRoleForTrustedAdvisorReporting`— El rol vinculado al servicio que se Trusted Advisor utiliza para acceder a las cuentas de su organización.
- `AWSServiceRoleForTrustedAdvisor`— El rol vinculado al servicio que se Trusted Advisor utiliza para acceder a los servicios de su organización.

Para obtener más información acerca de los roles vinculados a servicios, consulte [Utilizar funciones vinculadas al servicio para Trusted Advisor](#).

Uso de otros AWS servicios para ver Trusted Advisor informes

Siga este tutorial para cargar y ver sus datos mediante otros AWS servicios. En este tema, crearás un bucket de Amazon Simple Storage Service (Amazon S3) para almacenar tu informe y CloudFormation una plantilla para crear recursos en tu cuenta. Luego, puede usar Amazon Athena para analizar o ejecutar consultas para su informe o Quick para visualizar esos datos en un panel de control.

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 AWS Identity and Access Management (IAM) con permisos de administrador.
- Utilice EE. UU. Este (Virginia del Norte) Región de AWS para configurar rápidamente sus AWS servicios y recursos.
- Cree una cuenta rápida. Para obtener más información, consulte [Introducción al análisis de datos en Quick](#) en la Guía rápida del usuario de Amazon.

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 Consola de administración de AWS 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 *bucket-name* página, selecciona Crear carpeta, escribe el nombre **folder1**, a continuación, selecciona 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.

Cree sus recursos con AWS CloudFormation

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

Para crear sus recursos con CloudFormation

1. Descarga el [trusted-advisor-reports-templatearchivo.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 CloudFormation consola 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 Specify 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, selecciona la casilla de verificación Acepto que CloudFormation podría crear recursos de IAM.
15. Seleccione Creación de 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.

Trusted-Advisor-reports				Delete	Update	Stack actions ▼
Stack info	Events	Resources	Outputs	Parameters	Template	Change sets
Resources (12)						
Search resources						
Logical ID ▲	Physical ID ▼	Type ▼	Status ▼			
AWSPutS3TANotification	2020/05/27/[\$LATEST]5bfd3cb8b29a4b85bc0f8d861EXAMPLE1	Custom::AWSPutS3TANotification	✔ CREATE_COMPLETE			
AWSS3TAEvtLambdaPermission	Trusted-Advisor-reports-AWSS3TAEvtLambdaPermission-10KT2EXAMPLE1	AWS::Lambda::Permission	✔ CREATE_COMPLETE			
AWSS3TALambdaExecutor	Trusted-Advisor-reports-AWSS3TALambdaExecutor-1BJCOEXAMPLE1	AWS::IAM::Role	✔ CREATE_COMPLETE			
AWSS3TANotification	Trusted-Advisor-reports-AWSS3TANotification-15J3KEXAMPLE1	AWS::Lambda::Function	✔ CREATE_COMPLETE			
AWStartTACrawler	2020/05/27/[\$LATEST]66726149d3d64a1f9242cdccEXAMPLE1	Custom::AWStartTACrawler	✔ CREATE_COMPLETE			
AWSTACrawler	AWSTACrawler	AWS::Glue::Crawler	✔ CREATE_COMPLETE			

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.

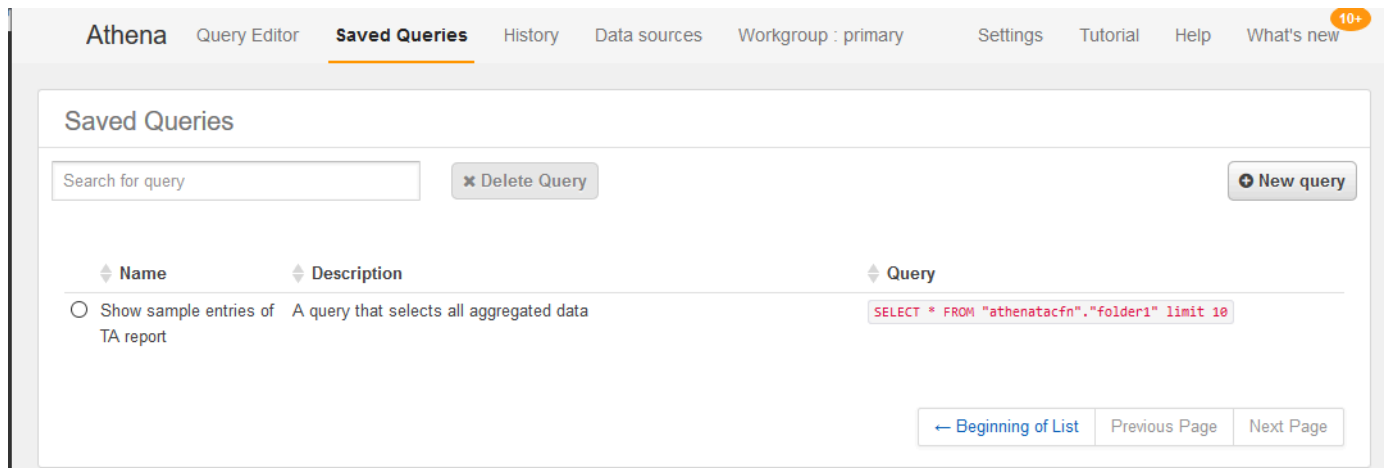
Notas

- 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 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 Ejecutar consulta. Aparecerán los resultados de la consulta.

Example: Consulta de Athena

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

New query 1

✔ Show sample ent... ✕ +

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

2

Run query

Save as

Create ▾

(Run time: 0.83 seconds, Data scanned: 94.75 KB)

Format query

Clear

Use Ctrl + Enter to run query, Ctrl + Space to autocomplete

Results

	volume type ▾	checkname ▾	accountid ▾	category ▾	issuppressed ▾	snapshot
1	General purpose(SSD)	Underutilized Amazon EBS Volumes	123456789012	Cost Optimizing	false	snap-0d4
2	General purpose(SSD)	Underutilized Amazon EBS Volumes	123456789012	Cost Optimizing	false	snap-06b
3	General purpose(SSD)	Underutilized Amazon EBS Volumes	123456789012	Cost Optimizing	false	
4	General purpose(SSD)	Underutilized Amazon EBS Volumes	123456789012	Cost Optimizing	false	
5	General purpose(SSD)	Underutilized Amazon EBS Volumes	123456789012	Cost Optimizing	false	snap-0ef4
6	General purpose(SSD)	Underutilized Amazon EBS Volumes	123456789012	Cost Optimizing	false	snap-0a5
7	General purpose(SSD)	Underutilized Amazon EBS Volumes	123456789012	Cost Optimizing	false	snap-078
8	General purpose(SSD)	Underutilized Amazon EBS Volumes	123456789012	Cost Optimizing	false	
9	General purpose(SSD)	Underutilized Amazon EBS Volumes	123456789012	Cost Optimizing	false	snap-0ff6!
10	General purpose(SSD)	Underutilized Amazon EBS Volumes	123456789012	Cost Optimizing	false	

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

Cree un panel de control en Quick

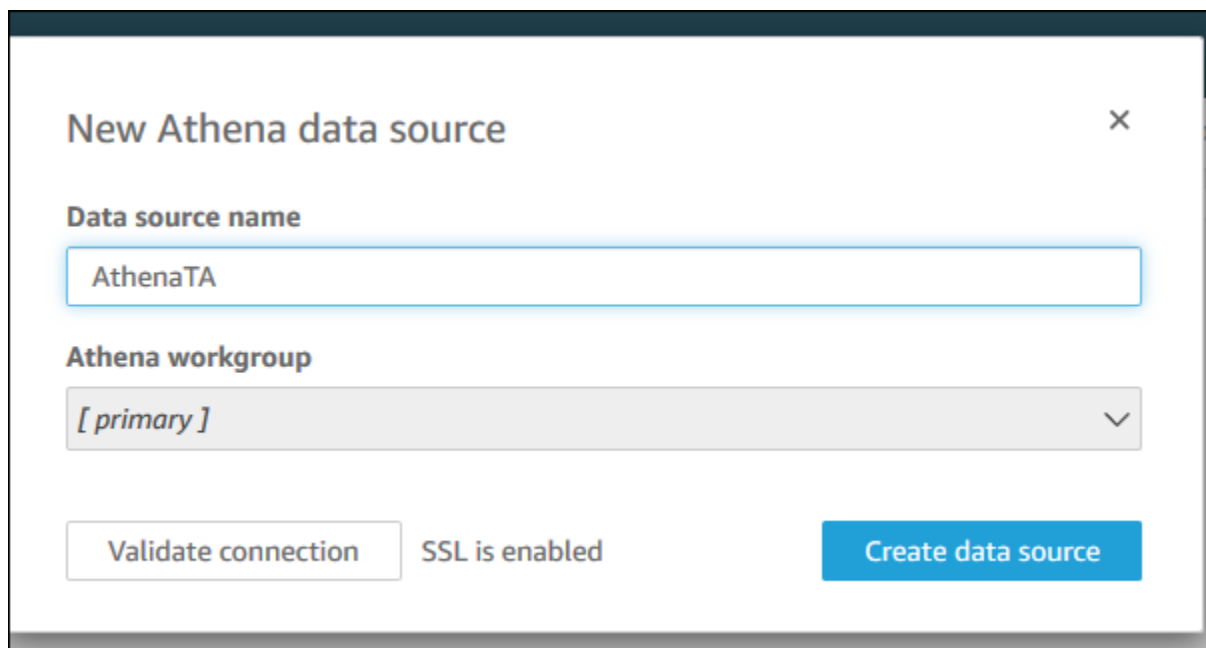
También puedes configurar Quick para que puedas ver tus datos en un panel y visualizar la información de tu informe.

Note

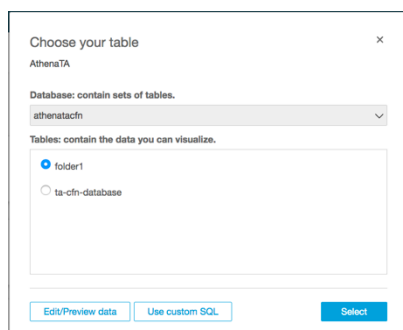
Debe usar la región EE. UU. Este (Norte de Virginia).

Para crear un panel en Quick

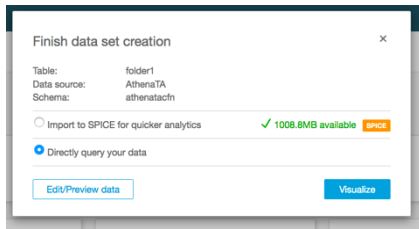
1. Ve a la consola Quick e inicia sesión en tu [cuenta](#).
2. Elija New analysis (Análisis nuevo), New dataset (Nuevo conjunto de datos) y haga clic en Athena.
3. En el cuadro de diálogo New Athena data source (Nuevo origen de datos de Athena), ingrese un nombre del origen de datos, como AthenaTA y 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).

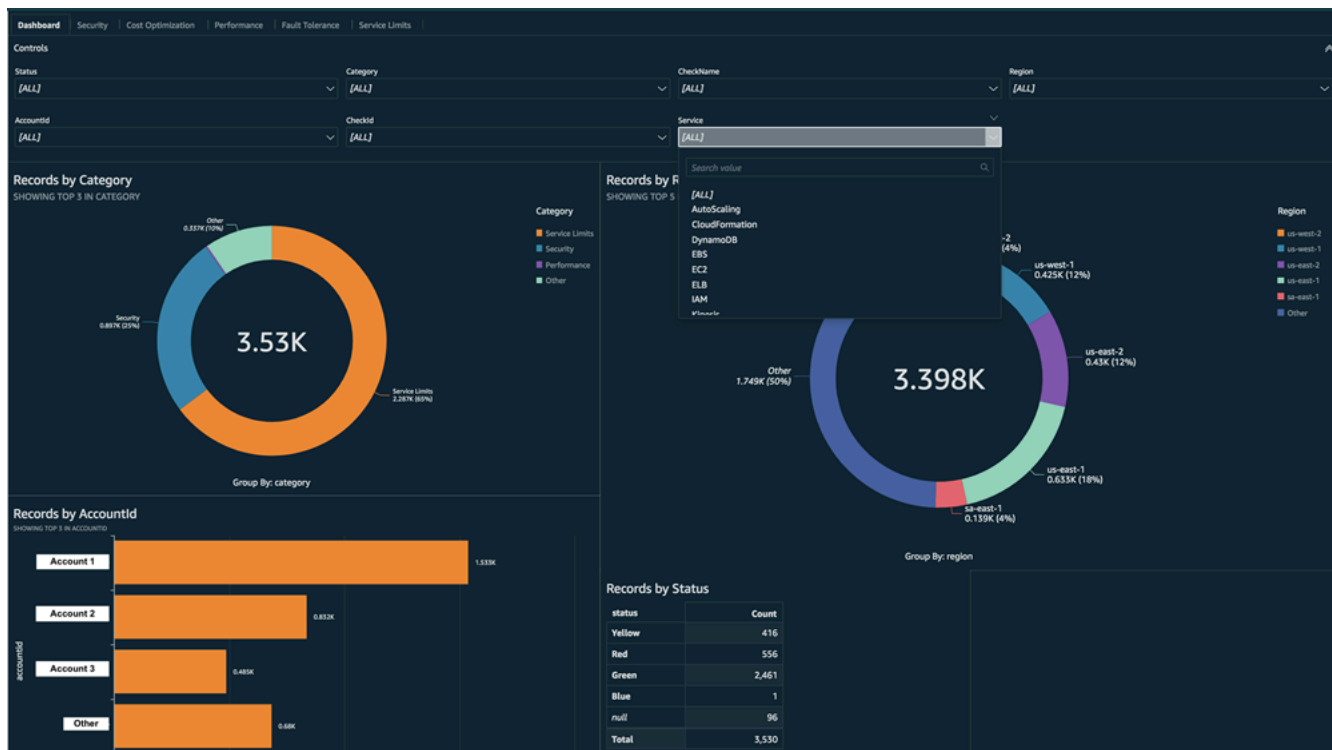


Ahora puede crear un panel de control en Quick. Para obtener más información, consulte [Trabajar con paneles](#) de control en la Guía rápida del usuario de Amazon.

Example: Panel de control rápido

El siguiente panel de ejemplo muestra información sobre las Trusted Advisor comprobaciones, como la siguiente:

- Cuenta afectada IDs
- Resumen por AWS regiones
- 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 Quick pueda usar Athena. Para obtener más información, consulte [No puedo conectarme a Amazon Athena](#) en la Guía rápida del usuario de Amazon.

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.

Resolución 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 función de visualización de la organización no actualiza automáticamente las Trusted Advisor comprobaciones de la 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 [Actualiza Trusted Advisor los cheques](#).

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

Puedes usar la AWS Glue consola para ver el esquema e identificar rápidamente si tienes columnas duplicadas en tu informe.

Para buscar columnas duplicadas

1. Abra la AWS Glue consola 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 Tablas.
4. Elija el nombre de la carpeta, por ejemplo *folder1*, y, a continuación, en Esquema, consulte los valores del 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 Trusted Advisor los cheques de las cuentas de su organización. Consulte [Actualizar Trusted Advisor los cheques](#).
2. Crea y descarga otro informe JSON en la Trusted Advisor consola. Consulte [Crear informes de vista organizativa](#). En este tutorial debe utilizar un archivo JSON.
3. Inicie sesión en la consola de Amazon S3 Consola de administración de AWS y ábrala 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 AWS Trusted Advisor cheques impulsados por AWS Config

Important

Aviso de fin de soporte: el soporte para desarrolladores se suspenderá el 1 de enero de 2027. Los clientes con soporte para desarrolladores pueden seguir usando su plan actual o optar por actualizarse a Business Support+ en cualquier momento antes del 1 de enero de 2027. Business Support+ ofrece asistencia basada en inteligencia artificial que comprende el contexto de sus operaciones, con acceso a AWS expertos las 24 horas del día, los 7 días de

la semana, a un precio mínimo de 29 USD al mes por cuenta. Para obtener más información, consulta los detalles del [plan Business Support+](#)

Aviso de fin de soporte: el soporte empresarial se suspenderá el 1 de enero de 2027. Los clientes con Business Support pueden seguir usando su plan actual o optar por actualizarse a Business Support+ en cualquier momento antes del 1 de enero de 2027. Business Support + ofrece asistencia basada en inteligencia artificial que comprende el contexto de sus operaciones, con acceso a AWS expertos las 24 horas del día, los 7 días de la semana, a un precio mínimo de 29 USD al mes por cuenta. Para obtener más información, consulta los detalles del [plan Business Support+](#)

Aviso de fin de soporte: el 1 de enero de 2027, Enterprise AWS On-Ramp dejará de funcionar. A lo largo de 2026, los clientes de Enterprise On-Ramp pasarán automáticamente a AWS Enterprise Support durante la renovación del contrato o en lotes periódicos. Los clientes recibirán una notificación por correo electrónico un mes antes de la actualización. No hay que hacer nada más. Enterprise Support proporciona una asignación de TAM designada, tiempos de respuesta de 15 minutos y Respuesta frente a incidencias de seguridad de AWS está disponible sin costo adicional, todo a un precio mínimo inferior de 5000\$ (reducido de 15 000\$). Para obtener más información, consulte los detalles del [Soporte plan AWS Enterprise](#). Para obtener más información, consulte [On-Ramp Fin del soporte para desarrolladores, empresas y empresas](#).

Developer Support, Business Support y Enterprise On-Ramp seguirán estando disponibles en la AWS GovCloud (US) región.

AWS Config es un servicio que evalúa, audita y evalúa continuamente las configuraciones de sus recursos para adaptarlas a las configuraciones deseadas. AWS Config proporciona reglas gestionadas, que son comprobaciones de conformidad predefinidas y personalizables que se AWS Config utilizan para evaluar si sus AWS recursos cumplen con las mejores prácticas habituales.

La AWS Config consola le guía a través de la configuración y activación de las reglas administradas. También puedes usar AWS Command Line Interface (AWS CLI) o la AWS Config API 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 sobre la activación AWS Config, consulta la [Guía para AWS Config desarrolladores](#).

AWS Config Las reglas gestionadas impulsan un conjunto de Trusted Advisor comprobaciones en todas las categorías. Al activar determinadas reglas gestionadas, las Trusted Advisor comprobaciones correspondientes se activan automáticamente. Para ver qué Trusted Advisor comprobaciones funcionan con reglas AWS Config administradas específicas, consulte [AWS Trusted Advisor comprobar referencia](#).

Los cheques AWS Config automatizados están disponibles para los clientes con un plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations. Si habilita uno de estos AWS Support planes AWS Config y lo tiene, verá automáticamente las recomendaciones basadas en las correspondientes reglas AWS Config gestionadas implementadas.

 Note

Los resultados de estas comprobaciones se actualizan automáticamente en función de las actualizaciones de las reglas gestionadas provocadas por cambios. AWS Config No se permiten las solicitudes de actualización. Actualmente, no se pueden excluir recursos de estas comprobaciones.

Resolución de problemas

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

Contenido

- [Acabo de activar la grabación y gestionar las reglas AWS Config, pero no veo las comprobaciones correspondientes. Trusted Advisor](#)
- [He implementado la misma regla AWS Config administrada dos veces, ¿qué verá? Trusted Advisor](#)
- [He desactivado la grabación AWS Config en una AWS región. ¿Qué verá en Trusted Advisor?](#)

Acabo de activar la grabación y gestionar las reglas AWS Config, pero no veo las comprobaciones correspondientes. Trusted Advisor

Una vez que la AWS Config regla genera los resultados de la evaluación, los verá prácticamente Trusted Advisor en tiempo real. Si tiene problemas con esta característica, cree un caso de soporte técnico en el [Centro de AWS Support](#).

He implementado la misma regla AWS Config administrada dos veces, ¿qué veré? Trusted Advisor

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

He desactivado la grabación AWS Config en una AWS región. ¿Qué veré en Trusted Advisor?

Si has desactivado el registro de recursos AWS Config en una AWS región, ya Trusted Advisor no recibirá los datos de las correspondientes reglas gestionadas y comprobaciones en esa región. Los resultados de las reglas gestionadas existentes permanecen AWS Config activos y activos Trusted Advisor hasta que AWS Config caducan, según la política de retención de registradores. Si eliminas una regla gestionada, los datos de Trusted Advisor comprobación normalmente se eliminan prácticamente en tiempo real.

Visualización de AWS Security Hub CSPM los controles en AWS Trusted Advisor

Después de AWS Security Hub CSPM activarlos Cuenta de AWS, podrá ver sus controles de seguridad y sus resultados en la Trusted Advisor consola. Puede usar los controles CSPM de Security Hub para identificar las vulnerabilidades de seguridad en su cuenta de la misma manera que puede usar Trusted Advisor las comprobaciones. Puede ver el estado de la comprobación, la lista de recursos afectados y, a continuación, seguir las recomendaciones de CSPM de Security Hub para solucionar sus problemas de seguridad. Puede utilizar esta función para encontrar las recomendaciones de seguridad de Trusted Advisor un Security Hub CSPM en una ubicación cómoda.

Notas

- Desde Trusted Advisor, puede ver 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 CSPM .

Para obtener más información sobre las categorías CSPM de Security Hub, consulte Categorías de [control](#).

- Trusted Advisor El Security Hub CSPM incorporado controla hasta el 26 de septiembre de 2024. Los controles lanzados después del 26 de septiembre de 2024 aún no están integrados. Trusted Advisor Puede encontrar los controles publicados después de esa fecha en el registro [CSPM de Security Hub](#).

Temas

- [Requisitos previos](#)
- [Vea las conclusiones sobre el CSPM de Security Hub](#)
- [Actualice sus hallazgos sobre el CSPM de Security Hub](#)
- [Desactivar Security Hub CSPM desde Trusted Advisor](#)
- [Resolución de problemas](#)

Requisitos previos

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

- Debe tener un plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations para poder utilizar esta función. Puede encontrar su plan de soporte en [AWS Support Center](#) o en la página [Planes de soporte](#). Para obtener más información, consulte [Comparar AWS Support planes](#).
- Debe habilitar el registro de recursos AWS Config para lo Regiones de AWS que desee para los controles CSPM de Security Hub. Para obtener más información, consulte [Habilitación y configuración de AWS Config](#).
- Debe habilitar Security Hub CSPM y seleccionar el estándar de seguridad AWS Foundational Security Best Practices v1.0.0. Si aún no lo ha hecho, consulte [Configuración de AWS Security Hub CSPM](#) en la Guía del usuario de AWS Security Hub CSPM .

 Note

Si ya ha completado los requisitos previos, puede ir a [Vea las conclusiones sobre el CSPM de Security Hub](#).

AWS Organizations Acerca de las cuentas

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. No es necesario contactar con las cuentas de los miembros individuales Soporte para habilitar esta función. Sin embargo, las cuentas de los miembros de su organización deben habilitar el CSPM de Security Hub si quieren ver sus hallazgos en él. Trusted Advisor

Si desea desactivar esta integración para una cuenta miembro específica, consulte [Desactive esta función para las cuentas AWS Organizations](#).

Vea las conclusiones sobre el CSPM de Security Hub

Después de habilitar el CSPM de Security Hub en su cuenta, las conclusiones sobre el CSPM de Security Hub pueden tardar hasta 24 horas en aparecer en la página de seguridad de la consola. Trusted Advisor

Para ver las conclusiones sobre el CSPM 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, puede optar por filtrar AWS Security Hub CSPM los controles CSPM de Security Hub.

3. Elija el nombre del control CSPM 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 CSPM. Para los controles CSPM de Security Hub, puede encontrar el ID del control.
- **Alert Criteria (Criterios de alerta):** indica el estado del control. Por ejemplo, si Security Hub CSPM detecta un problema importante, el estado puede ser Rojo: Crítico o Alto.
- **Acción recomendada:** utilice el enlace de documentación CSPM de Security Hub para encontrar los pasos recomendados para solucionar el problema.
- **Recursos de Security Hub CSPM:** puede encontrar los recursos de su cuenta en los que Security Hub CSPM ha detectado un problema.

Notas

- Los resultados de estas comprobaciones se actualizan automáticamente al menos una vez al día y no se admiten solicitudes de actualización. Puede que los cambios tarden unas horas en aparecer. Puede usar la Trusted Advisor consola para excluir los recursos de las comprobaciones que se actualizan automáticamente. Puedes usar la [BatchUpdateRecommendationResourceExclusion](#) API para excluir los recursos de cualquier comprobación, excepto los recursos de recomendación Trusted Advisor prioritaria.
- La función de vista organizacional admite esta integración con Security Hub CSPM. Puede ver los resultados de los controles CSPM de su Security Hub en toda la organización y, a continuación, crear y descargar informes. Para obtener más información, consulte [Vista organizativa de AWS Trusted Advisor](#).

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

El siguiente es un ejemplo de búsqueda de un control CSPM de Security Hub en la Trusted Advisor consola.

IAM root user access key should not exist

Last updated: an hour ago

Checks if the root user access key is available.

Source
[AWS Security Hub](#)
 Security Hub control ID: IAM.4

Alert Criteria
 Red: Critical or High. Security Hub control failed.

Recommended Action
 Follow the [Security Hub documentation](#) to fix the issue.

IAM root user access key should not exist (1)

Exclude & Refresh

Included items ▼

1 of 1 resources failed this Security Hub control.

<

1

>

☐	Status ▼	Region ▼	Resource ▼	Last Updated Time ▼
☐		us-east-1	AWS:::Account:123456789012	2021-12-12T19:56:26.305Z

Actualice sus hallazgos sobre el CSPM de Security Hub

Después de habilitar un estándar de seguridad, Security Hub CSPM puede tardar hasta dos horas en encontrar información sobre sus recursos. Luego, esos datos pueden tardar hasta 24 horas en aparecer en la Trusted Advisor consola. Si ha activado recientemente el estándar de seguridad AWS Foundational Security Best Practices v1.0.0, vuelva a comprobar la Trusted Advisor consola más adelante.

Note

- El programa de actualización de cada control CSPM de Security Hub es periódico o se desencadena por cambios. Actualmente, no puedes usar la Trusted Advisor consola o la AWS Support API para actualizar los controles CSPM de Security Hub. Para obtener más información, consulte [Programación para ejecución de controles de seguridad](#).
- Los resultados de estas comprobaciones se actualizan automáticamente al menos una vez al día y no se admiten solicitudes de actualización. Puede que los cambios tarden unas horas en aparecer. Puede usar la Trusted Advisor consola para excluir los recursos de las comprobaciones que se actualizan automáticamente. Puedes usar la [BatchUpdateRecommendationResourceExclusion](#) API para excluir los recursos de

cualquier comprobación, excepto los recursos de recomendación Trusted Advisor prioritaria.

Desactivar Security Hub CSPM desde Trusted Advisor

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

Para deshabilitar la integración de Security Hub (CSPM)

1. Póngase en contacto con el Security Hub CSPM [AWS Support](#) y solicite que se deshabilite su integración. Trusted Advisor

Tras AWS Support deshabilitar esta función, el Security Hub CSPM ya no envía datos a Trusted Advisor. Se eliminarán los datos de CSPM de su Security Hub. Trusted Advisor

2. Si desea volver a habilitar esta integración, contacte a [AWS Support](#).

Desactive esta función para las cuentas AWS Organizations

Si ya ha completado el procedimiento anterior para una cuenta de administración, la integración de Security Hub CSPM se elimina automáticamente de todas las cuentas de los miembros de su organización. Las cuentas miembro individuales de la organización no necesitan contactar a AWS Support por separado.

Si es miembro de una cuenta de una organización, puede ponerse en contacto con nosotros Soporte para eliminar esta función únicamente de su cuenta.

Resolución de problemas

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

Contenido

- [No veo los resultados del CSPM de Security Hub en la consola Trusted Advisor](#)
- [He configurado Security Hub \(CSPM\) y AWS Config correctamente, pero aún faltan mis resultados](#)

- [Quiero deshabilitar controles CSPM específicos de Security Hub](#)
- [Quiero encontrar mis recursos de CSPM de Security Hub excluidos](#)
- [Quiero activar o desactivar esta función para una cuenta de miembro que pertenece a una organización AWS](#)
- [Veo varios Regiones de AWS para el mismo recurso afectado en una comprobación de CSPM de Security Hub](#)
- [He desactivado Security Hub \(CSPM\) o AWS Config en una región](#)
- [Mi control está archivado en Security Hub \(CSPM\), pero sigo viendo los resultados en Trusted Advisor](#)
- [Sigo sin poder ver las conclusiones sobre el CSPM de Security Hub](#)

No veo los resultados del CSPM de Security Hub en la consola Trusted Advisor

Asegúrese de haber completado los siguientes pasos:

- Tiene un plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations.
- Ha activado el registro de recursos AWS Config en la misma región que Security Hub CSPM.
- Ha activado Security Hub CSPM y ha seleccionado el estándar de seguridad AWS Foundational Security Best Practices v1.0.0.
- Los nuevos controles de Security Hub CSPM se añaden a los registros en un Trusted Advisor plazo de dos a cuatro semanas. Consulte la [nota](#).

Para obtener más información, consulte la [Requisitos previos](#).

He configurado Security Hub (CSPM) y AWS Config correctamente, pero aún faltan mis resultados

Security Hub CSPM puede tardar hasta dos horas en encontrar información sobre sus recursos. Luego, esos datos pueden tardar hasta 24 horas en aparecer en la Trusted Advisor consola. Vuelva a verificar la consola de Trusted Advisor más tarde.

 Notas

- Solo aparecerán las conclusiones sobre los controles incluidos en el estándar de seguridad AWS Foundational Security Best Practices, Trusted Advisor excepto en el caso de los controles que tengan la categoría: Recuperación > Resiliencia.
- Si hay un problema de servicio con el Security Hub CSPM o el Security Hub CSPM no está disponible, tus hallazgos pueden tardar hasta 24 horas en aparecer. Trusted Advisor Vuelva a verificar la consola de Trusted Advisor más tarde.

Quiero deshabilitar controles CSPM específicos de Security Hub

Security Hub CSPM envía sus datos automáticamente. Trusted Advisor Si inhabilitas un control CSPM de Security Hub o ya no tienes recursos para ese control, tus resultados no aparecerán en. Trusted Advisor

Puede iniciar sesión en la [consola CSPM de Security Hub](#) y comprobar si el control está activado o desactivado.

Si deshabilita un control CSPM de Security Hub o deshabilita todos los controles del estándar de seguridad AWS Foundational Security Best Practices, sus hallazgos se archivarán 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 sus hallazgos, se eliminan de. Trusted Advisor

Para obtener más información, consulte los temas siguientes:

- [Deshabilitación y habilitación de controles individuales](#)
- [Deshabilitación o habilitación de un estándar de seguridad](#)

Quiero encontrar mis recursos de CSPM de Security Hub excluidos

Desde la Trusted Advisor consola, puede elegir el nombre de control CSPM de Security Hub y, a continuación, elegir la opción Elementos excluidos. Esta opción muestra todos los recursos que están suprimidos en Security Hub CSPM.

Si el estado de flujo de trabajo de un recurso se establece en SUPPRESSED, ese recurso es un elemento excluido en Trusted Advisor. No puede suprimir los recursos CSPM de Security Hub de

la Trusted Advisor consola. Para ello, utilice la consola [CSPM de Security Hub](#). Para obtener más información, consulte [Establecimiento del estado de flujo de trabajo de los hallazgos](#).

Quiero activar o desactivar esta función para una cuenta de miembro que pertenece a una organización 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 varios Regiones de AWS para el mismo recurso afectado en una comprobación de CSPM de Security Hub

Algunos Servicios de AWS son globales y no son específicas 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).

En las comprobaciones CSPM 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 CSPM 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 (CSPM) o AWS Config en una región

Si detiene el registro de recursos con el Security Hub CSPM AWS Config o lo deshabilita en una Región de AWS, Trusted Advisor dejará de recibir datos de ningún control de esa región. Trusted Advisor elimina los hallazgos de CSPM 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 [Desactivar Security Hub CSPM](#).

Para deshabilitar esta característica de la cuenta, consulte [Desactivar Security Hub CSPM desde Trusted Advisor](#).

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

Cuando el RecordState estado cambia a «ARCHIVEDPara un hallazgo», Trusted Advisor elimina el hallazgo de ese control CSPM de Security Hub de su cuenta. Es posible que sigas viendo el hallazgo entre Trusted Advisor 7 y 9 días antes de que se elimine. Este plazo es el máximo esfuerzo y no está garantizado.

Sigo sin poder ver las conclusiones sobre el CSPM 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 al menos una vez al día y no se admiten solicitudes de actualización. Puede que los cambios tarden unas horas en aparecer. Puede usar la Trusted Advisor consola para excluir los recursos de las comprobaciones que se actualizan automáticamente. Puede utilizar la [BatchUpdateRecommendationResourceExclusion](#) API para excluir los recursos de cualquier comprobación, excepto los recursos de recomendación prioritaria de Trusted Advisor.
- Trusted Advisor ya tiene los cheques Amazon EBS Volumes subutilizados y Amazon EBS Magnetic Volumes sobreutilizados.

Tras optar por Compute Optimizer, te recomendamos que utilices las nuevas comprobaciones de volúmenes sobreaprovisionados de Amazon EBS y de volúmenes insuficientemente aprovisionados de Amazon EBS en su lugar.

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
- [Solicitar modificaciones a los volúmenes de Amazon EBS](#) en la Guía del usuario de Amazon EC2

Comience con AWS Trusted Advisor Priority

Trusted Advisor Priority le ayuda a proteger y optimizar sus prácticas AWS recomendadas Cuenta de AWS para que las siga. Con Trusted Advisor Priority, tu Cuenta de AWS equipo puede supervisar tu

cuenta de forma proactiva y crear recomendaciones priorizadas cuando identifiquen oportunidades para ti.

Por ejemplo, el equipo de su cuenta puede identificar si el usuario raíz de su AWS cuenta 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 activa en la página de Trusted Advisor prioridad de la consola. Trusted Advisor A continuación, debe seguir las recomendaciones para resolver el asunto en cuestión.

Trusted Advisor Las recomendaciones prioritarias provienen de estas dos fuentes:

- Servicios de AWS — Servicios como Trusted Advisor AWS Security Hub CSPM, y AWS Well-Architected crean recomendaciones automáticamente. El equipo de su cuenta comparte estas recomendaciones con usted para que aparezcan en Trusted Advisor Priority.
- Equipo de cuentas: el equipo de cuentas puede crear recomendaciones manuales.

Trusted Advisor Priority te ayuda a centrarte 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 buscar recomendaciones para todas las cuentas de los miembros de su organización.

Temas

- [Requisitos previos](#)
- [Habilitar Trusted Advisor la prioridad](#)
- [Ver recomendaciones priorizadas](#)
- [Confirmación de una recomendación](#)
- [Descartar una recomendación](#)
- [Resolver una recomendación](#)
- [Reapertura de una recomendación](#)
- [Descargar detalles de las recomendaciones](#)
- [Registro de administradores delegados](#)
- [Anulación del registro de administradores delegados](#)
- [Administra las notificaciones Trusted Advisor prioritarias](#)

- [Deshabilita Trusted Advisor la prioridad](#)

Requisitos previos

Debe cumplir los siguientes requisitos para usar Trusted Advisor Priority:

- Debe tener un plan AWS Enterprise Support o AWS Unified Operations.
- 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 haber habilitado el acceso confiable a Trusted Advisor. Para habilitar el acceso de confianza, inicie sesión con la cuenta de administración. Abre la página [Tu organización](#) en la Trusted Advisor consola.
- Debe iniciar sesión en su AWS cuenta para ver las recomendaciones Trusted Advisor prioritarias para su cuenta.
- 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 AWS Identity and Access Management (de IAM) para acceder a Trusted Advisor Priority. Para obtener información sobre cómo controlar el acceso a Trusted Advisor Priority, consulte [Gestione el acceso a AWS Trusted Advisor](#) y [AWS políticas gestionadas para AWS Trusted Advisor](#).

Habilitar Trusted Advisor la prioridad

Solicite a su equipo de cuentas que habilite esta característica. Debe tener un plan de operaciones AWS unificado y ser el propietario de la cuenta de administración de su organización. Si en la página de Trusted Advisor prioridad de la consola se indica que necesita un acceso de confianza AWS Organizations, seleccione Habilitar el acceso de confianza con AWS Organizations. Para obtener más información, consulte la sección [Requisitos previos](#).

Ver recomendaciones priorizadas

Cuando el equipo de tu cuenta te active la Trusted Advisor prioridad, podrás ver las recomendaciones más recientes para tu AWS cuenta.

Ver sus recomendaciones priorizadas

1. Inicia sesión en la Trusted Advisor consola de <https://console.aws.amazon.com/trustedadvisor/tu casa>.

2. En la página Trusted Advisor Priority, podrá ver los siguientes elementos:

Si utilizas una cuenta AWS Organizations de administración o de administrador delegado, cambia 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 su Cuenta de AWS equipo o de 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 AWS

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

 Note

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

1. Inicie sesión en la Trusted Advisor consola de <https://console.aws.amazon.com/trustedadvisor/su casa>.
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 tu Cuenta de AWS equipo o de 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 Trusted Advisor prioritarias

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.

Trusted Advisor > Priority

Trusted Advisor Priority [Info](#)

You can use this page to find critical recommendations, trends, and activities for your organization.

My organization | My account

Select an account from your organization

All accounts

Action needed

Pending response
15

In progress
27

Overview

Dismissed in the last 90 days
5

Resolved in the last 90 days
22

No update in 30+ days
10

Average time to resolve
46 days

Active | Closed

Active prioritized recommendations (42)

Your AWS account team has prioritized the following recommendations for your organization. Choose a recommendation to learn more.

Search

Recommendations	Status	Source	Category	Age (days)
Low Utilization Amazon EC2 Instances test	Pending response	AWS Trusted Advisor	Cost optimization	33 day(s) Shared on: Jun 20, 2023
RDS DB instances should have deletion protection enabled	Pending response	AWS Security Hub	Security	20 day(s) Shared on: Jul 3, 2023

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. Inicia sesión en la Trusted Advisor consola de <https://console.aws.amazon.com/trustedadvisor/tu casa>.

2. Si utilizas una cuenta AWS Organizations de administración o de administrador delegado, cambia 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 Activas de la página de Trusted Advisor prioridades.

8. Realice las acciones recomendadas para resolver la recomendación. Para obtener 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.

Trusted Advisor > Priority > Low Utilization Amazon EC2 Instances - Production accounts

My organization

My account

Low Utilization Amazon EC2 Instances - Production accounts

Copy recommendation link

Download

Acknowledge

Dismiss

Details

Affected resources

Overview

Source AWS Trusted Advisor	Category Cost optimization	Age 33 day(s) Shared on: Jun 20, 2023	Status Pending response
Shared by person@amazon.com			

Details

Description

Checks the Amazon Elastic Compute Cloud (Amazon EC2) instances that were running at any time during the last 14 days and alerts you if the daily CPU utilization was 10% or less and network I/O was 5 MB or less on 4 or more days. Running instances generate hourly usage charges. Although some scenarios can result in low utilization by design, you can often lower your costs by managing the number and size of your instances.

Estimated monthly savings are calculated by using the current usage rate for On-Demand Instances and the estimated number of days the instance might be underutilized. Actual savings will vary if you are using Reserved Instances or Spot Instances, or if the instance is not running for a full day. To get daily utilization data, download the report for this check.

Alert Criteria

Yellow: An instance had 10% or less daily average CPU utilization and 5 MB or less network I/O on at least 4 of the previous 14 days.

Recommended Action

Consider stopping or terminating instances that have low utilization, or scale the number of instances by using Auto Scaling. For more information, see [Stop and Start Your Instance](#), [Terminate Your Instance](#), and [What Is Auto Scaling?](#)

Additional Resources

[Monitoring Amazon EC2](#)
[Instance Metadata and User Data](#)
[Amazon CloudWatch Developer Guide](#)
[Auto Scaling Developer Guide](#)

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

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. Inicia sesión en la Trusted Advisor consola de <https://console.aws.amazon.com/trustedadvisor/tu casa>.
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 obtener 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.

Trusted Advisor > Priority > Low Utilization Amazon EC2 Instances - Production accounts

My organization My account

Low Utilization Amazon EC2 Instances - Production accounts

Copy recommendation link Download Acknowledge Dismiss

Details Affected accounts Affected resources

Overview

Source	Category	Age	Status
AWS Trusted Advisor	Cost optimization	0 day(s) Shared on: Jul 10, 2023	Pending response

Shared by
person@amazon.com

Status Summary

This is a summary of the status of this recommendation across all your accounts

- 1 account Pending response
- 1 account In progress

Details

Description

Checks the Amazon Elastic Compute Cloud (Amazon EC2) instances that were running at any time during the last 14 days and alerts you if the daily CPU utilization was 10% or less and network I/O was 5 MB or less on 4 or more days. Running instances generate hourly usage charges. Although some scenarios can result in low utilization by design, you can often lower your costs by managing the number and size of your instances.

Estimated monthly savings are calculated by using the current usage rate for On-Demand Instances and the estimated number of days the instance might be underutilized. Actual savings will vary if you are using Reserved Instances or Spot Instances, or if the instance is not running for a full day. To get daily utilization data, download the report for this check.

Alert Criteria

Yellow: An instance had 10% or less daily average CPU utilization and 5 MB or less network I/O on at least 4 of the previous 14 days.

Recommended Action

Consider stopping or terminating instances that have low utilization, or scale the number of instances by using Auto Scaling. For more information, see [Stop and Start Your Instance](#), [Terminate Your Instance](#), and [What is Auto Scaling?](#)

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 tienes una prueba Cuenta de AWS que piensas eliminar, no necesitas seguir las acciones recomendadas.

Para descartar una recomendación

1. Inicia sesión en la Trusted Advisor consola de <https://console.aws.amazon.com/trustedadvisor/tu casa>.
2. Si utilizas una cuenta AWS Organizations de administración o de administrador delegado, cambia 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 Cerrada de la página de Trusted Advisor prioridades.

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

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

1. [Inicia sesión en la Trusted Advisor consola de tu casa](https://console.aws.amazon.com/trustedadvisor/)<https://console.aws.amazon.com/trustedadvisor/>.
2. En la página de Trusted Advisor prioridades, asegúrate 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 Cerrado de la página de Trusted Advisor prioridad.

 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 a tu equipo de cuentas que has rechazado la recomendación.

Example: Rechaza una recomendación de Priority Trusted Advisor

El siguiente ejemplo muestra cómo se puede descartar una recomendación.

Dismiss recommendation

 Please note: This action will apply to all accounts affected by this recommendation

Choose a reason for why you're dismissing this recommendation

The affected AWS account was temporarily created for an event

Note - optional

These are test accounts that we will delete soon

CancelDismiss

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 reabirla. Si desea volver a revisar la recomendación más adelante, consulte [Descartar una recomendación](#).

Para resolver una recomendación

1. Inicia sesión en la Trusted Advisor consola de <https://console.aws.amazon.com/trustedadvisor/tu casa>.

2. En la página de Trusted Advisor prioridades, asegúrate de estar en la pestaña Mi organización.
3. En la página Trusted Advisor Priority, seleccione la recomendación y, a continuación, elija Resuelve (Resolver).
4. En el cuadro de diálogo Resolver recomendación, seleccione Resolver. Las recomendaciones resueltas aparecen en la pestaña Cerrado de la página de Trusted Advisor prioridades. Trusted Advisor Priority notifica a tu equipo de cuentas que has resuelto la recomendación.

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

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

 Note

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

1. Inicia sesión en la Trusted Advisor consola de <https://console.aws.amazon.com/trustedadvisor/tu casa>.
2. Si utilizas una cuenta AWS Organizations de administración o de administrador delegado, ve 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 Cerrado de la página de Trusted Advisor prioridades. Trusted Advisor Priority notifica a tu equipo de cuentas que has resuelto la recomendación.

Example: Recomendación manual de Priority Trusted Advisor

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

Trusted Advisor > Priority > Low Utilization Amazon EC2 Instances - Production accounts

My organization My account

Low Utilization Amazon EC2 Instances - Production accounts

Copy recommendation link Download

Details Affected accounts Affected resources

Overview

Source AWS Trusted Advisor	Category Cost optimization	Age 0 day(s) Shared on: Jul 10, 2023	Status Resolved
Shared by person@amazon.com	Resolved on Jul 10, 2023		

Status Summary

This is a summary of the status of this recommendation across all your accounts

2 accounts Resolved

Reapertura de una recomendación

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

Para reabrir una recomendación

1. Inicia sesión en la Trusted Advisor consola de <https://console.aws.amazon.com/trustedadvisor/tu casa>.
2. Si utilizas una cuenta AWS Organizations de administración o de administrador delegado, cambia 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 tu organización AWS

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

 Note

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

1. [Inicia sesión en la Trusted Advisor consola de tu casa](https://console.aws.amazon.com/trustedadvisor/)<https://console.aws.amazon.com/trustedadvisor/>.
2. En la página de Trusted Advisor prioridades, asegúrate 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: Vuelva a abrir una recomendación de Priority Trusted Advisor

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

Reopen recommendation ✕

 Please note: This action will apply to all accounts affected by this recommendation

Reason for reopening

I need to address this recommendation for my organization

Cancel Reopen

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. Inicia sesión en la Trusted Advisor consola de <https://console.aws.amazon.com/trustedadvisor/tu casa>.
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 administrador delegado pueden revisar, reconocer, resolver, descartar y volver a abrir las recomendaciones en Priority. Trusted Advisor

Después de registrar una cuenta, debe conceder al administrador delegado los AWS Identity and Access Management permisos necesarios para acceder a Priority. Trusted Advisor 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.

Registro de un administrador delegado de

1. Inicie sesión en la Trusted Advisor consola de <https://console.aws.amazon.com/trustedadvisor/su casa> como 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 sean administradores delegados no recibirán notificaciones por correo electrónico de Trusted Advisor Priority.

Anulación del registro de un administrador delegado de

1. Inicia sesión en la Trusted Advisor consola de <https://console.aws.amazon.com/trustedadvisor/tu casa> como 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).

Administra las notificaciones Trusted Advisor prioritarias

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

Si has registrado las cuentas de los miembros como administradores delegados, estos también pueden configurar sus cuentas para recibir notificaciones Trusted Advisor prioritarias por correo electrónico.

Trusted Advisor Las notificaciones prioritarias por correo electrónico no incluyen los resultados de las comprobaciones de las cuentas individuales y son independientes de la notificación semanal de las Trusted Advisor recomendaciones. Para obtener más información, consulte [Configurar las preferencias de notificación](#).

Note

Solo la cuenta de administración o el administrador delegado pueden configurar las notificaciones Trusted Advisor prioritarias por correo electrónico.

Para gestionar tus notificaciones Trusted Advisor prioritarias

1. Inicia sesión en la Trusted Advisor consola de <https://console.aws.amazon.com/trustedadvisor/tu casa> como una cuenta de administración o de administrador delegado.
2. En el panel de navegación, en Preferences (Preferencias), elija Notifications (Notificaciones).
3. En Prioridad, 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. Puedes añadir y eliminar contactos desde la página de [configuración de la cuenta](#) de la Administración de facturación y costos de AWS 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 `noreply@notifications.trustedadvisor.us-west-2.amazonaws.com` dirección. Es posible que tenga que comprobar que su cliente de correo electrónico no identifique estos correos electrónicos como spam.

Deshabilita Trusted Advisor la prioridad

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

Si inhabilitas la Trusted Advisor prioridad y la vuelves a activar más adelante, podrás seguir viendo las recomendaciones que el equipo de tu cuenta te envió antes de deshabilitar la Trusted Advisor prioridad.

AWS Trusted Advisor comprobar referencia

 Important

Aviso de fin de soporte: el soporte para desarrolladores se suspenderá el 1 de enero de 2027. Los clientes con soporte para desarrolladores pueden seguir usando su plan actual o optar por actualizarse a Business Support+ en cualquier momento antes del 1 de enero de 2027. Business Support+ ofrece asistencia basada en inteligencia artificial que comprende el contexto de sus operaciones, con acceso a AWS expertos las 24 horas del día, los 7 días de la semana, a un precio mínimo de 29 USD al mes por cuenta. Para obtener más información, consulta los detalles del [plan Business Support+](#)

Aviso de fin de soporte: el soporte empresarial se suspenderá el 1 de enero de 2027. Los clientes con Business Support pueden seguir usando su plan actual o optar por actualizarse a Business Support+ en cualquier momento antes del 1 de enero de 2027. Business Support+ ofrece asistencia basada en inteligencia artificial que comprende el contexto de sus operaciones, con acceso a AWS expertos las 24 horas del día, los 7 días de la semana, a un precio mínimo de 29 USD al mes por cuenta. Para obtener más información, consulta los detalles del [plan Business Support+](#)

Aviso de fin de soporte: el 1 de enero de 2027, Enterprise AWS On-Ramp dejará de funcionar. A lo largo de 2026, los clientes de Enterprise On-Ramp pasarán automáticamente a AWS Enterprise Support durante la renovación del contrato o en lotes periódicos. Los clientes recibirán una notificación por correo electrónico un mes antes de la actualización. No hay que hacer nada más. Enterprise Support proporciona una asignación de TAM designada, tiempos de respuesta de 15 minutos y Respuesta frente a incidencias de seguridad de AWS está disponible sin costo adicional, todo a un precio mínimo inferior de 5000\$ (reducido de 15 000\$). Para obtener más información, consulte los detalles del [Soporte plan AWS Enterprise](#). Para obtener más información, consulte [On-Ramp Fin del soporte para desarrolladores, empresas y empresas](#).

Developer Support, Business Support y Enterprise On-Ramp seguirán estando disponibles en la AWS GovCloud (US) región.

Puede ver todos los nombres y descripciones de los Trusted Advisor cheques IDs 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 tienes un plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, también puedes usar la [AWS Trusted Advisor API](#) y el AWS Command Line Interface (AWS CLI) para acceder a tus cheques. Para obtener más información, consulte los temas siguientes:

- [Comience con la Trusted Advisor API](#)
- [AWS Trusted Advisor Referencia de la API](#)

Note

Si tienes un plan Basic Support o Developer Support, puedes usar la Trusted Advisor consola para acceder a todas las comprobaciones de la [Límites de los servicios](#) categoría y a las siguientes comprobaciones de las categorías Security y Fault Tolerance:

- [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](#)
- [AWS STS uso global de puntos finales en Regiones de AWS](#)

Categorías de verificación

- [Optimización de costos](#)
- [Desempeño](#)
- [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

- [Cuenta de AWS no forma parte de AWS Organizations](#)
- [Recomendaciones de optimización de costos de Amazon Aurora para el almacenamiento en clústeres de bases de datos](#)
- [Puntos de conexión infrautilizados de Amazon Comprehend](#)
- [Recomendaciones de compra de capacidad reservada de Amazon DynamoDB](#)
- [Recomendaciones de optimización de costos de Amazon EBS para volúmenes](#)
- [Volúmenes con exceso de aprovisionamiento de Amazon EBS](#)
- [Recomendaciones de optimización de costos de Amazon EC2 para grupos de Amazon EC2 Auto Scaling](#)
- [Recomendaciones de optimización de costos de Amazon EC2 para instancias](#)
- [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](#)
- [Vencimiento del arrendamiento de la instancia reservada de Amazon EC2](#)
- [Optimización de instancias reservadas de Amazon EC2](#)
- [Repositorio de Amazon ECR sin política de ciclo de vida configurada](#)
- [Recomendaciones de compra de nodos ElastiCache reservados de Amazon](#)
- [AWS Fargate recomendaciones de optimización de costes para Amazon ECS](#)
- [Recomendaciones de compra de nodos reservados de Amazon MemoryDB](#)
- [Recomendaciones de compra de instancias reservadas de Amazon OpenSearch Service](#)
- [Recomendaciones de optimización de costos de Amazon RDS para instancias de base de datos](#)
- [Recomendaciones de optimización de costos de Amazon RDS para el almacenamiento de instancias de base de datos](#)
- [Instancias de bases de datos inactivas de Amazon RDS](#)
- [Recomendaciones de compra de instancias reservadas de Amazon RDS](#)
- [Recomendaciones de compra de nodos reservados de Amazon Redshift](#)
- [Conjuntos de registros de recursos de latencia en Amazon Route 53](#)
- [Política de ciclo de vida del bucket de Amazon S3 configurada](#)
- [Configuración de anulación de carga multiparte incompleta de Amazon S3](#)
- [Buckets habilitados para versiones de Amazon S3 sin políticas de ciclo de vida configuradas](#)
- [AWS Lambda recomendaciones de optimización de costes para las funciones](#)
- [AWS Lambda funciones con tiempos de espera excesivos](#)
- [AWS Lambda funciones con altas tasas de error](#)
- [AWS Lambda funciones sobreaprovisionadas para el tamaño de la memoria](#)
- [AWS Recomendaciones de compra de Savings Plans para computación](#)
- [AWS Recomendaciones de compra de Savings Plans para Amazon SageMaker AI](#)
- [Problemas de alto riesgo de AWS Well-Architected para la optimización de costos](#)
- [Balanceadores de carga inactivos](#)
- [Puertas de enlace NAT inactivas](#)
- [Inactivo AWS Network Firewall](#)
- [Puntos de conexión de interfaz de VPC inactivos](#)

- [Puntos de conexión inactivos del equilibrador de carga de la puerta de enlace](#)
- [Puertas de enlace NAT inactivas](#)
- [Utilización baja de instancias de Amazon EC2](#)
- [Direcciones IP elásticas no asociadas](#)
- [Volúmenes de Amazon EBS infrautilizados](#)
- [Underutilized Amazon Redshift Clusters](#)

Cuenta de AWS no forma parte de AWS Organizations

Description (Descripción)

Comprueba si una Cuenta de AWS forma parte de AWS Organizations la cuenta de gestión correspondiente.

AWS Organizations es un servicio de administración de cuentas para consolidar varias AWS cuentas en una organización gestionada 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 `MasterAccountId` parámetro de las reglas. AWS Config

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.

Para los clientes del plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puede usar la [BatchUpdateRecommendationResourceExclusionAPI](#) para incluir o excluir uno o más recursos de sus Trusted Advisor resultados.

ID de la verificación

c18d2gz127

origen

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

Criterios de alerta

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

Acción recomendada

Agrega esta AWS cuenta como parte de AWS Organizations.

Para obtener más información, consulte [Tutorial: Creación y configuración de una organización](#).

Columnas de informes

- Status
- Region
- Recurso
- AWS Config Regla
- Parámetros de entrada
- Hora de la última actualización

Recomendaciones de optimización de costos de Amazon Aurora para el almacenamiento en clústeres de bases de datos

Description (Descripción)

Verifica las configuraciones de almacenamiento y los patrones de uso de los clústeres de bases de datos de Amazon Aurora para ofrecer recomendaciones sobre posibles ahorros de costos.

Para cada recurso, Trusted Advisor muestra solo la principal acción recomendada de Centro de optimización de costes de AWS.

Para usar esta verificación, debe iniciar sesión en el [Centro de optimización de costos](#) y en [AWS Compute Optimizer](#).

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.

Para los clientes del plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puede usar la [BatchUpdateRecommendationResourceExclusionAPI](#) para incluir o excluir uno o más recursos de sus Trusted Advisor resultados.

ID de la verificación

c1z7kmr17n

origen

Centro de optimización de costes de AWS

Criterios de alerta

Amarillo: el Centro de optimización de costos ha identificado una acción de ahorro de costos para el almacenamiento en un clúster de base de datos de Aurora.

Acción recomendada

Considere la posibilidad de implementar la recomendación. La recomendación es uno de los tipos de recomendaciones que se enumeran en la sección [Estrategias de optimización de costos](#) de la Guía del usuario de AWS Cost Management . Para obtener más información sobre la implementación de estas recomendaciones, consulte el manual de [optimización de costos de los servicios](#) de administración financiera en la AWS nube (CFM).

Utilice las recomendaciones detalladas AWS Compute Optimizer para comprender el posible impacto de estos cambios en los costes y el rendimiento.

Recursos adicionales

- [Visualización de las recomendaciones para las bases de datos de Aurora y RDS](#)
- [Recomendaciones para Amazon Aurora](#)
- [Configuración de Amazon Aurora](#)

Columnas de informes

- Status
- Region
- Resource ID (ID de recurso)
- Acción recomendada
- Resumen de recursos actuales
- Resumen de recursos recomendados

- Costo mensual estimado
- Ahorros mensuales estimados
- Marca temporal de la última actualización

Puntos de conexión infrautilizados de Amazon Comprehend

Description (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 infrautilizado. 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

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.

Para los clientes del plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puede usar la [BatchUpdateRecommendationResourceExclusionAPI](#) para incluir o excluir uno o más recursos de sus Trusted Advisor resultados.

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

Recomendaciones de compra de capacidad reservada de Amazon DynamoDB

Description (Descripción)

Verifica sus patrones de uso de Amazon DynamoDB y ofrece recomendaciones para posibles ahorros de costos mediante la compra de capacidad reservada.

Esta verificación genera recomendaciones en el [ámbito del pagador para la cuenta del pagador y en el ámbito vinculado para una cuenta vinculada](#).

Trusted Advisor muestra solo la principal acción recomendada de Centro de optimización de costes de AWS.

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.

Para los clientes del plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puede usar la [BatchUpdateRecommendationResourceExclusion](#) API para incluir o excluir uno o más recursos de sus Trusted Advisor resultados.

ID de la verificación

c1z7kmr15n

origen

Centro de optimización de costes de AWS

Criterios de alerta

Amarillo: el Centro de optimización de costos ha identificado una acción de ahorro de costos para DynamoDB en la cuenta.

Acción recomendada

Considere la posibilidad [de implementar la recomendación](#). Para obtener más información sobre la implementación de estas recomendaciones, consulte el manual de [optimización de costos de los servicios](#) de administración financiera en la AWS nube (CFM).

Recursos adicionales

- [Capacidad reservada de DynamoDB](#)
- [Acceder a las recomendaciones de reservas](#)
- [Capacidad reservada de Amazon DynamoDB](#)

Columnas de informes

- Status
- Region
- Resumen de recursos recomendados
- Costo mensual estimado
- Ahorros mensuales estimados
- Marca temporal de la última actualización

Recomendaciones de optimización de costos de Amazon EBS para volúmenes

Description (Descripción)

Verifica las configuraciones de volumen y los patrones de uso de Amazon EBS para ofrecer recomendaciones sobre posibles ahorros de costos.

Para cada recurso, Trusted Advisor muestra solo la principal acción recomendada de Centro de optimización de costes de AWS.

Para usar esta verificación, debe iniciar sesión en el [Centro de optimización de costos](#) y en [AWS Compute Optimizer](#).

 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.

Para los clientes del plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puede usar la [BatchUpdateRecommendationResourceExclusion](#) API para incluir o excluir uno o más recursos de sus Trusted Advisor resultados.

ID de la verificación

c1z7kmr02n

origen

Centro de optimización de costes de AWS

Criterios de alerta

Amarillo: el Centro de optimización de costos ha identificado una acción de ahorro de costos para el volumen de EBS.

Acción recomendada

Considere la posibilidad de implementar la recomendación. La recomendación es uno de los tipos de recomendaciones que se enumeran en la sección [Estrategias de optimización de costos](#) de la Guía del usuario de AWS Cost Management . Para obtener más información sobre la implementación de estas recomendaciones, consulte el manual de [optimización de costos de los servicios](#) de administración financiera en la AWS nube (CFM).

Utilice las recomendaciones detalladas AWS Compute Optimizer para comprender el posible impacto de estos cambios en los costes y el rendimiento.

Recursos adicionales

- [Visualización de las recomendaciones de volumen de Amazon EBS](#)
- [Métricas de volumen de EBS](#)
- [Amazon EBS volume types](#)
- [Solicitar modificaciones de volumen de Amazon EBS](#)

Columnas de informes

- Status

- Region
- Resource ID (ID de recurso)
- Acción recomendada
- Resumen de recursos actuales
- Resumen de recursos recomendados
- Costo mensual estimado
- Ahorros mensuales estimados
- Marca temporal de la última actualización

Volúmenes con exceso de aprovisionamiento de Amazon EBS

Description (Descripción)

Note

Esta es una verificación heredada. Se recomienda usar la nueva verificación (ID de verificación: [c1z7kmr02n](#)) que ofrece recomendaciones personalizadas adicionales.

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 varían 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.

Para los clientes del plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puede usar la [BatchUpdateRecommendationResourceExclusionAPI](#) para incluir o excluir uno o más recursos de sus Trusted Advisor resultados.

ID de la verificación

C0r6dfpM03

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 mejores prácticas. 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
- Region
- 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

Recomendaciones de optimización de costos de Amazon EC2 para grupos de Amazon EC2 Auto Scaling

Description (Descripción)

Verifica las configuraciones de grupo y los patrones de utilización de Amazon EC2 Auto Scaling para ofrecer recomendaciones sobre posibles ahorros de costos.

Para cada recurso, Trusted Advisor muestra solo la acción más recomendada de. Centro de optimización de costes de AWS

Para usar esta verificación, debe iniciar sesión en el [Centro de optimización de costos](#) y en [AWS Compute Optimizer](#).

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.

Para los clientes del plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puede usar la [BatchUpdateRecommendationResourceExclusion](#) API para incluir o excluir uno o más recursos de sus Trusted Advisor resultados.

ID de la verificación

c1z7kmr01n

origen

Centro de optimización de costes de AWS

Criterios de alerta

Amarillo: el Centro de optimización de costos ha identificado una acción de ahorro de costos para el grupo Amazon EC2 Auto Scaling.

Acción recomendada

Considere la posibilidad de implementar la recomendación. La recomendación es uno de los tipos de recomendaciones que se enumeran en la sección [Estrategias de optimización de costos](#) de la Guía del usuario de AWS Cost Management . Para obtener más información sobre la implementación de estas recomendaciones, consulte el manual de [optimización de costos de los servicios](#) de administración financiera en la AWS nube (CFM).

Utilice las recomendaciones detalladas AWS Compute Optimizer para comprender el posible impacto de estos cambios en los costes y el rendimiento.

Recursos adicionales

- [Visualización de recomendaciones para el volumen de Amazon EC2 Auto Scaling](#)
- [Grupos de Amazon EC2 Auto Scaling](#)
- [¿Qué es Amazon EC2 Auto Scaling?](#)

Columnas de informes

- Status
- Region
- Resource ID (ID de recurso)
- Acción recomendada
- Resumen de recursos actuales
- Resumen de recursos recomendados
- Costo mensual estimado
- Ahorros mensuales estimados
- Marca temporal de la última actualización

Recomendaciones de optimización de costos de Amazon EC2 para instancias

Description (Descripción)

Verifica las configuraciones y los patrones de uso de las instancias de Amazon EC2 para ofrecer recomendaciones sobre posibles ahorros de costos.

Para cada recurso, Trusted Advisor muestra solo la principal acción recomendada de Centro de optimización de costes de AWS.

Para usar esta verificación, debe iniciar sesión en el [Centro de optimización de costos](#) y en [AWS Compute Optimizer](#).

 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.

Para los clientes del plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puede usar la [BatchUpdateRecommendationResourceExclusionAPI](#) para incluir o excluir uno o más recursos de sus Trusted Advisor resultados.

ID de la verificación

c1z7kmr00n

origen

Centro de optimización de costes de AWS

Criterios de alerta

Amarillo: el Centro de optimización de costos ha identificado una acción de ahorro de costos para la instancia EC2.

Acción recomendada

Considere la posibilidad de implementar la recomendación. La recomendación es uno de los tipos de recomendaciones que se enumeran en la sección [Estrategias de optimización de costos](#) de la Guía del usuario de AWS Cost Management . Para obtener más información sobre la implementación de estas recomendaciones, consulte el manual de [optimización de costos de los servicios](#) de administración financiera en la AWS nube (CFM).

Utilice las recomendaciones detalladas AWS Compute Optimizer para comprender el posible impacto de estos cambios en los costes y el rendimiento.

Recursos adicionales

- [Visualización de las recomendaciones de instancias de EC2](#)

- [Métricas de instancias EC2](#)
- [Cambios en el tipo de instancia de Amazon EC2](#)

Columnas de informes

- Status
- Region
- Resource ID (ID de recurso)
- Acción recomendada
- Resumen de recursos actuales
- Resumen de recursos recomendados
- Costo mensual estimado
- Ahorros mensuales estimados
- Marca temporal de la última actualización

Consolidación de las instancias de Amazon EC2 para Microsoft SQL Server

Description (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, pagas 4 licencias de vCPU aunque una instancia solo tenga 1 o 2 v. CPUs. Puede consolidar instancias de SQL Server más pequeñas para 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.

Para los clientes del plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puede usar la [BatchUpdateRecommendationResourceExclusionAPI](#) para incluir o excluir uno o más recursos de sus Trusted Advisor resultados.

ID de la verificación

Qsdfp3A4L2

Criterios de alerta

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

Acción recomendada

Considere la posibilidad de consolidar cargas de trabajo de SQL Server más pequeñas en instancias con al menos cuatro v. CPUs

Recursos adicionales

- [Microsoft SQL Server en AWS](#)
- [Licencias de Microsoft en AWS](#)
- [Guía de licencias de Microsoft SQL Server](#)

Columnas de informes

- Status
- Region
- 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

Description (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 la edición SQL Server Standard puede utilizar hasta 48 vCPUs. Una instancia con SQL Server Web puede utilizar hasta 32 vCPUs. Esta comprobación 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 v CPUs que puede usar 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.

Para los clientes del plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puede usar la [BatchUpdateRecommendationResourceExclusionAPI](#) para incluir o excluir uno o más recursos de sus Trusted Advisor resultados.

ID de la verificación

Qsdfp3A4L1

Criterios de alerta

- Rojo: una instancia con la edición SQL Server Standard tiene más de 48 versiones. CPUs
- Rojo: una instancia con la edición web de SQL Server tiene más de 32 versionesCPUs.

Acción recomendada

En el caso de la edición SQL Server Standard, considere la posibilidad de cambiar a una instancia de la misma familia de instancias con 48 vCPUs. Para la edición Web de SQL Server, considere la posibilidad de cambiar a una instancia de la misma familia de instancias con 32 vCPUs. Si consume mucha memoria, considere la posibilidad de cambiar a instancias R5 optimizadas para memoria.

Recursos adicionales

- [Microsoft SQL Server en AWS](#)
- Puede utilizar [Launch Wizard](#) para simplificar la implementación de SQL Server en EC2.

Columnas de informes

- Status
- Region
- 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

Description (Descripción)

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

Puede especificar el valor de número de días permitido en AllowedDayslos AWS Config parámetros.

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.

Para los clientes del plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puede usar la [BatchUpdateRecommendationResourceExclusion](#) API para incluir o excluir uno o más recursos de sus Trusted Advisor resultados.

ID de la verificación

c18d2gz150

origen

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

Vencimiento del arrendamiento de la instancia reservada de Amazon EC2

Description (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

Description (Descripción)

Una parte importante del uso AWS implica equilibrar la compra de instancias reservadas (RI) con el uso de instancias bajo demanda. Esta comprobación proporciona recomendaciones que RIs ayudarán a reducir los costes derivados del 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 una parte por adelantado RIs puede ayudar a reducir los costos.

Acción recomendada

Consulte la página de [Cost Explorer](#) para obtener recomendaciones más detalladas y personalizadas. Además, consulta la [guía de compra](#) para saber cómo comprar RIs y las opciones disponibles.

Recursos adicionales

- Puede encontrar información sobre RIs cómo pueden ahorrarle dinero [aquí](#).
- Para obtener más información sobre esta recomendación, consulte las [preguntas de comprobación de la optimización de instancias reservadas](#) en el Trusted Advisor FAQs.

Columnas de informes

- Region
- Tipo de instancia
- Plataforma
- Número recomendado RIs de compra
- Utilización media prevista de IR
- Ahorros estimados con recomendaciones (mensual)
- Costo inicial de RIs
- Costos estimados de RIs (mensuales)
- 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

Description (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

origen

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
- Region
- Recurso

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

Recomendaciones de compra de nodos ElastiCache reservados de Amazon

Description (Descripción)

Comprueba tus patrones de ElastiCache uso de Amazon para ofrecerte recomendaciones sobre posibles ahorros de costes mediante la compra de nodos reservados.

Esta verificación genera recomendaciones en el [ámbito del pagador para la cuenta del pagador y en el ámbito vinculado para una cuenta vinculada](#).

Trusted Advisor muestra solo las principales acciones recomendadas entre Centro de optimización de costes de AWS.

Para usar esta verificación, debe iniciar sesión en el [Centro de optimización de 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.

Para los clientes del plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puede usar la [BatchUpdateRecommendationResourceExclusion](#) API para incluir o excluir uno o más recursos de sus Trusted Advisor resultados.

ID de la verificación

c1z7kmr13n

origen

Centro de optimización de costes de AWS

Criterios de alerta

Amarillo: la cuenta tiene una acción de ahorro de costes identificada por Cost Optimization Hub for Amazon ElastiCache.

Acción recomendada

Considere [implementar la recomendación](#) Para obtener más información sobre la implementación de estas recomendaciones, consulte el [manual de optimización de costos de los servicios](#) de administración financiera en la AWS nube (CFM).

Recursos adicionales

- [Nodos reservados](#)
- [Acceder a las recomendaciones de reserva](#)
- [Nodos ElastiCache reservados de Amazon](#)

Columnas de informes

- Status
- Region
- Resumen de recursos recomendados
- Costo mensual estimado
- Ahorros mensuales estimados
- Marca temporal de la última actualización

AWS Fargate recomendaciones de optimización de costes para Amazon ECS

Description (Descripción)

Comprueba las configuraciones y AWS Fargate los patrones de uso de Amazon ECS para ofrecer recomendaciones sobre posibles ahorros de costes.

Para cada recurso, Trusted Advisor muestra solo la acción más recomendada entre Centro de optimización de costes de AWS.

Para usar esta verificación, debe iniciar sesión en el [Centro de optimización de costos](#) y en [AWS Compute Optimizer](#).

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.

Para los clientes del plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puede usar la [BatchUpdateRecommendationResourceExclusionAPI](#) para incluir o excluir uno o más recursos de sus Trusted Advisor resultados.

ID de la verificación

c1z7kmr06n

origen

Centro de optimización de costes de AWS

Criterios de alerta

Amarillo: los servicios de Amazon ECS AWS Fargate tienen una acción de ahorro de costes identificada por Cost Optimization Hub.

Acción recomendada

Considere la posibilidad de implementar la recomendación. La recomendación es uno de los tipos de recomendaciones que se enumeran en la sección [Estrategias de optimización de costos](#) de la Guía del usuario de AWS Cost Management . Para obtener más información sobre la implementación de estas recomendaciones, consulte el manual de optimización de [costos de los servicios](#) de administración financiera en la AWS nube (CFM).

Utilice las recomendaciones detalladas AWS Compute Optimizer para comprender el posible impacto de estos cambios en los costes y el rendimiento.

Recursos adicionales

- [Visualización de los servicios de Amazon ECS según las recomendaciones de Fargate](#)
- [Métricas de los servicios de Amazon ECS en Fargate](#)
- [AWS Fargate para Amazon ECS](#)
- [Actualización de un servicio de Amazon ECS mediante la consola](#)

Columnas de informes

- Status
- Region
- Resource ID (ID de recurso)
- Acción recomendada

- Resumen de recursos actuales
- Resumen de recursos recomendados
- Costo mensual estimado
- Ahorros mensuales estimados
- Marca temporal de la última actualización

Recomendaciones de compra de nodos reservados de Amazon MemoryDB

Description (Descripción)

Verifica los patrones de uso de Amazon MemoryDB para ofrecer recomendaciones sobre posibles ahorros de costos mediante la compra de nodos reservados.

Esta verificación genera recomendaciones en el [ámbito del pagador para la cuenta del pagador y en el ámbito vinculado para una cuenta vinculada](#).

Para cada recurso, Trusted Advisor muestra solo la principal acción recomendada de Centro de optimización de costes de AWS.

Para usar esta verificación, debe iniciar sesión en el [Centro de optimización de 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.

Para los clientes del plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puede usar la [BatchUpdateRecommendationResourceExclusionAPI](#) para incluir o excluir uno o más recursos de sus Trusted Advisor resultados.

ID de la verificación

c1z7kmr16n

origen

Centro de optimización de costes de AWS

Criterios de alerta

Amarillo: el Centro de optimización de costos ha identificado una acción de ahorro de costos para MemoryDB en la cuenta.

Acción recomendada

Considere la posibilidad [de implementar la recomendación](#). Para obtener más información sobre la implementación de estas recomendaciones, consulte el manual de [optimización de costos de los servicios](#) de administración financiera en la AWS nube (CFM).

Recursos adicionales

- [Nodos reservados de MemoryDB](#)
- [Acceder a las recomendaciones de reserva](#)
- [Trabajar con nodos reservados](#)

Columnas de informes

- Status
- Region
- Resumen de recursos recomendados
- Costo mensual estimado
- Ahorros mensuales estimados
- Marca temporal de la última actualización

Recomendaciones de compra de instancias reservadas de Amazon OpenSearch Service

Description (Descripción)

Comprueba tus patrones de uso de Amazon OpenSearch Service para ofrecerte recomendaciones sobre posibles ahorros de costes mediante la compra de instancias reservadas (RI).

Esta verificación genera recomendaciones en el [ámbito del pagador para la cuenta del pagador y en el ámbito vinculado para una cuenta vinculada](#).

Trusted Advisor muestra solo la principal acción recomendada de Centro de optimización de costes de AWS.

Para usar esta verificación, debe iniciar sesión en el [Centro de optimización de 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.

Para los clientes del plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puede usar la [BatchUpdateRecommendationResourceExclusion](#) API para incluir o excluir uno o más recursos de sus Trusted Advisor resultados.

ID de la verificación

c1z7kmr14n

origen

Centro de optimización de costes de AWS

Criterios de alerta

Amarillo: la cuenta tiene una acción de ahorro de costes identificada por Cost Optimization Hub for Amazon OpenSearch Service.

Acción recomendada

Considere la posibilidad [de implementar la recomendación](#). Para obtener más información sobre la implementación de estas recomendaciones, consulta el [manual de optimización de costos del servicio](#) de administración financiera en la AWS nube (CFM).

Recursos adicionales

- [Instancias reservadas en Amazon OpenSearch Service](#)
- [Acceder a las recomendaciones de reservas](#)
- [Compra de instancias reservadas \(AWS CLI\)](#)

Columnas de informes

- Status
- Region
- Resumen de recursos recomendados
- Costo mensual estimado
- Ahorros mensuales estimados
- Marca temporal de la última actualización

Recomendaciones de optimización de costos de Amazon RDS para instancias de base de datos

Description (Descripción)

Verifica las configuraciones y los patrones de uso de las instancias de base de datos de Amazon RDS para ofrecer recomendaciones sobre posibles ahorros de costos.

Para cada recurso, Trusted Advisor muestra solo la principal acción recomendada de Centro de optimización de costes de AWS.

Para usar esta verificación, debe iniciar sesión en el [Centro de optimización de costos](#) y en [AWS Compute Optimizer](#).

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.

Para los clientes del plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puede usar la [BatchUpdateRecommendationResourceExclusion](#) API para incluir o excluir uno o más recursos de sus Trusted Advisor resultados.

ID de la verificación

c1z7kmr03n

origen

Centro de optimización de costes de AWS

Criterios de alerta

Amarillo: el Centro de optimización de costos ha identificado una acción de ahorro de costos para la instancia de base de datos de RDS.

Acción recomendada

Considere la posibilidad de implementar la recomendación. La recomendación es uno de los tipos de recomendaciones que se enumeran en la sección [Estrategias de optimización de costos](#) de la Guía del usuario de AWS Cost Management . Para obtener más información sobre la

implementación de estas recomendaciones, consulte el manual de [optimización de costos de los servicios](#) de administración financiera en la AWS nube (CFM).

Utilice las recomendaciones detalladas AWS Compute Optimizer para comprender el posible impacto de estos cambios en los costes y el rendimiento.

Recursos adicionales

- [Visualización de las recomendaciones para la bases de datos de RDS](#)
- [Métricas de la base de datos de RDS](#)
- [Clases de instancia de base de datos](#)
- [Modificación de una instancia de base de datos de Amazon RDS](#)

Columnas de informes

- Status
- Region
- Resource ID (ID de recurso)
- Acción recomendada
- Resumen de recursos actuales
- Resumen de recursos recomendados
- Costo mensual estimado
- Ahorros mensuales estimados
- Marca temporal de la última actualización

Recomendaciones de optimización de costos de Amazon RDS para el almacenamiento de instancias de base de datos

Description (Descripción)

Verifica las configuraciones de almacenamiento y los patrones de uso de las instancias de base de datos de Amazon RDS para ofrecer recomendaciones sobre posibles ahorros de costos.

Para cada recurso, Trusted Advisor muestra solo la principal acción recomendada de Centro de optimización de costes de AWS.

Para usar esta verificación, debe iniciar sesión en el [Centro de optimización de costos](#) y en [AWS Compute Optimizer](#).

 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.

Para los clientes del plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puede usar la [BatchUpdateRecommendationResourceExclusion](#) API para incluir o excluir uno o más recursos de sus Trusted Advisor resultados.

ID de la verificación

c1z7kmr04n

origen

Centro de optimización de costes de AWS

Criterios de alerta

Amarillo: el Centro de optimización de costos ha identificado una acción de ahorro de costos para el almacenamiento de bases de datos de RDS.

Acción recomendada

Considere la posibilidad de implementar la recomendación. La recomendación es uno de los tipos de recomendaciones que se enumeran en la sección [Estrategias de optimización de costos](#) de la Guía del usuario de AWS Cost Management . Para obtener más información sobre la implementación de estas recomendaciones, consulte el manual de [optimización de costos de los servicios](#) de administración financiera en la AWS nube (CFM).

Utilice las recomendaciones detalladas AWS Compute Optimizer para comprender el posible impacto de estos cambios en los costes y el rendimiento.

Recursos adicionales

- [Visualización de las recomendaciones para la bases de datos de RDS](#)
- [Almacenamiento de instancias de base de datos de Amazon RDS](#)

Columnas de informes

- Status
- Region
- Resource ID (ID de recurso)

- Acción recomendada
- Resumen de recursos actuales
- Resumen de recursos recomendados
- Costo mensual estimado
- Ahorros mensuales estimados
- Marca temporal de la última actualización

Instancias de bases de datos inactivas de Amazon RDS

Description (Descripción)

Note

Esta es una verificación heredada. Se recomienda usar la nueva verificación (ID de verificación: [c1z7kmr03n](#)) que ofrece recomendaciones personalizadas adicionales.

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.

Note

Esta verificación indica los recursos alertados según los criterios y el número total de recursos evaluados, incluidos los recursos OK. La tabla de recursos muestra solo los recursos marcados.

ID de la verificación

Ti39ha1fu8

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

- Region
- 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)

Recomendaciones de compra de instancias reservadas de Amazon RDS

Description (Descripción)

Verifica sus patrones de uso de Amazon RDS para ofrecer recomendaciones sobre posibles ahorros de costos mediante la compra de instancias reservadas (RI).

Esta verificación genera recomendaciones en el [ámbito del pagador para la cuenta del pagador y en el ámbito vinculado para una cuenta vinculada](#).

Trusted Advisor muestra solo las principales acciones recomendadas de Centro de optimización de costes de AWS.

Para usar esta verificación, debe iniciar sesión en el [Centro de optimización de 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.

Para los clientes del plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puede usar la [BatchUpdateRecommendationResourceExclusion](#) API para incluir o excluir uno o más recursos de sus Trusted Advisor resultados.

ID de la verificación

c1z7kmr11n

origen

Centro de optimización de costes de AWS

Criterios de alerta

Amarillo: el Centro de optimización de costos ha identificado una acción de ahorro de costos para el volumen de EBS.

Acción recomendada

Considere la posibilidad [de implementar la recomendación](#). Para obtener más información sobre la implementación de estas recomendaciones, consulte el manual de [optimización de costos de los servicios](#) de administración financiera en la AWS nube (CFM).

Recursos adicionales

- [Instancia de base de datos reservada para Amazon RDS](#)
- [Acceder a las recomendaciones de reservas](#)
- [Compra de instancias de base de datos reservadas para Amazon RDS](#)

Columnas de informes

- Status
- Region
- Resumen de recursos recomendados
- Costo mensual estimado

- Ahorros mensuales estimados
- Marca temporal de la última actualización

Recomendaciones de compra de nodos reservados de Amazon Redshift

Description (Descripción)

Verifica sus patrones de uso de Amazon Redshift para ofrecer recomendaciones sobre posibles ahorros de costos mediante la compra de nodos reservados.

Esta verificación genera recomendaciones en el [ámbito del pagador para la cuenta del pagador y en el ámbito vinculado para una cuenta vinculada](#).

Trusted Advisor muestra solo la principal acción recomendada de Centro de optimización de costes de AWS.

Para usar esta verificación, debe iniciar sesión en el [Centro de optimización de 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.

Para los clientes del plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puede usar la [BatchUpdateRecommendationResourceExclusionAPI](#) para incluir o excluir uno o más recursos de sus Trusted Advisor resultados.

ID de la verificación

c1z7kmr12n

origen

Centro de optimización de costes de AWS

Criterios de alerta

Amarillo: el Centro de optimización de costos ha identificado una acción de ahorro de costos para Amazon Redshift en la cuenta.

Acción recomendada

Considere la posibilidad [de implementar la recomendación](#). Para obtener más información sobre la implementación de estas recomendaciones, consulte el manual de [optimización de costos de los servicios](#) de administración financiera en la AWS nube (CFM).

Recursos adicionales

- [Nodos reservados](#)
- [Acceder a las recomendaciones de reserva](#)
- [Comprar un nodo reservado](#)

Columnas de informes

- Status
- Region
- Resumen de recursos recomendados
- Costo mensual estimado
- Ahorros mensuales estimados
- Marca temporal de la última actualización

Conjuntos de registros de recursos de latencia en Amazon Route 53

Description (Descripción)

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

Para permitir que Amazon Route 53 dirija las consultas a la red Región de AWS con la latencia de red más baja, debe crear conjuntos de registros de recursos de latencia para un nombre de dominio concreto (como example.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 por AWS los servicios no aparecerán en los resultados de la comprobación.

 Note

Esta verificación indica los recursos que están marcados según los criterios y el número total de recursos evaluados, incluidos los recursos de OK. La tabla de recursos muestra solo los recursos marcados.

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 solo tiene recursos en una Región de AWS, considere la posibilidad de crear recursos en más de una Región de AWS y definir conjuntos de registros de recursos de latencia para cada una de ellas; consulte [Enrutamiento basado en la latencia](#).

Si no quiere usar varias Regiones de AWS, debe usar un conjunto de registros de recursos simple. 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

Description (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 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 verificación mediante los parámetros de sus AWS Config reglas

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.

Para los clientes del plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puede usar la [BatchUpdateRecommendationResourceExclusion](#) API para incluir o excluir uno o más recursos de sus Trusted Advisor resultados.

ID de la verificación

c18d2gz100

origen

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
- Region
- Recurso
- AWS Config Regla
- Parámetros de entrada

Configuración de anulación de carga multiparte incompleta de Amazon S3

Description (Descripción)

Verifica 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 de manera automática una o más veces, y no se permiten las solicitudes de actualización. Puede que los cambios tarden unas horas en aparecer. Puede que los cambios tarden unas horas en aparecer. Para

los clientes de Business, Enterprise On-Ramp o Enterprise Support, pueden usar la BatchUpdateRecommendationResourceExclusion API para incluir o excluir uno o más recursos de sus Trusted Advisor resultados.

ID de la verificación

c1cj39rr6v

Criterios de alerta

Amarillo: el bucket de configuración del ciclo de vida no contiene una regla de ciclo de vida que anule todas las cargas multiparte que permanezcan incompletas después de 7 días.

Acción recomendada

Revise 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. [Aquí](#) encontrará las instrucciones para crear una regla de ciclo de vida. Se recomienda que se aplique a todos los objetos del bucket. Si necesita aplicar otras acciones de ciclo de vida a objetos seleccionados del bucket, puede 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

[Creación de una configuración del ciclo de vida](#)

[Detección y eliminación de cargas incompletas multiparte para reducir los costos 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
- Region
- Nombre del bucket

- ARN de bucket
- Regla de ciclo de vida para eliminar las MPU incompletas
- Días después de la iniciación
- Hora de la última actualización

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

Description (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 desea comprobar mediante los parámetros bucketNames de sus 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.

Para los clientes del plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puede usar la [BatchUpdateRecommendationResourceExclusion](#) API para incluir o excluir uno o más recursos de sus Trusted Advisor resultados.

ID de la verificación

c18d2gz171

origen

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

AWS Lambda recomendaciones de optimización de costes para las funciones

Description (Descripción)

Comprueba AWS Lambda las configuraciones y los patrones de uso para ofrecer recomendaciones sobre posibles ahorros de costes.

Para cada recurso, Trusted Advisor muestra solo la acción más recomendada entre Centro de optimización de costes de AWS.

Para usar esta verificación, debe iniciar sesión en el [Centro de optimización de costos](#) y en [AWS Compute Optimizer](#).

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.

Para los clientes del plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puede usar la [BatchUpdateRecommendationResourceExclusionAPI](#) para incluir o excluir uno o más recursos de sus Trusted Advisor resultados.

ID de la verificación

c1z7kmr05n

origen

Centro de optimización de costes de AWS

Criterios de alerta

Amarillo: el Centro de optimización de costos ha identificado una acción de ahorro de costos para la función de Lambda.

Acción recomendada

Considere la posibilidad de implementar la recomendación. La recomendación es uno de los tipos de recomendaciones que se enumeran en la sección [Estrategias de optimización de costos](#) de la Guía del usuario de AWS Cost Management . Para obtener más información sobre la implementación de estas recomendaciones, consulte el manual de [optimización de costos de los servicios](#) de administración financiera en la AWS nube (CFM).

Utilice las recomendaciones detalladas AWS Compute Optimizer para comprender el posible impacto de estos cambios en los costes y el rendimiento.

Recursos adicionales

- [Visualización de las recomendaciones de funciones Lambda](#)
- [Métricas de función de Lambda](#)
- [Configuración de funciones AWS Lambda](#)

Columnas de informes

- Status
- Region
- Resource ID (ID de recurso)
- Acción recomendada
- Resumen de recursos actuales

- Resumen de recursos recomendados
- Costo mensual estimado
- Ahorros mensuales estimados
- Marca temporal de la última actualización

AWS Lambda funciones con tiempos de espera excesivos

Description (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.

Para los clientes del plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puede usar la [BatchUpdateRecommendationResourceExclusionAPI](#) para incluir o excluir uno o más recursos de sus Trusted Advisor resultados.

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 AWS SDK 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](#)
- [Se usa con AWS LambdaAWS X-Ray](#)
- [Acceder a CloudWatch los registros de Amazon para AWS Lambda](#)
- [Ejemplo de aplicación de procesador de errores para AWS Lambda](#)

Columnas de informes

- Status
- Region
- 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

AWS Lambda funciones con altas tasas de error

Description (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.

Para los clientes del plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puede usar la [BatchUpdateRecommendationResourceExclusionAPI](#) para incluir o excluir uno o más recursos de sus Trusted Advisor resultados.

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 que ofrecen los socios. 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](#)
- [Ejemplo de procesador de errores: aplicación para AWS Lambda](#)

Columnas de informes

- Status
- Region
- 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
- Invocaciones diarias actuales
- Tasa de errores diarios actual
- *Promedio de invocaciones diarias
- Hora de la última actualización

AWS Lambda funciones sobreaprovisionadas para el tamaño de la memoria

Description (Descripción)

Note

Esta es una verificación heredada. Se recomienda usar la nueva verificación (ID de verificación: [c1z7kmr05n](#)) que ofrece recomendaciones personalizadas adicionales.

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 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.

Para los clientes del plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puede usar la [BatchUpdateRecommendationResourceExclusionAPI](#) para incluir o excluir uno o más recursos de sus Trusted Advisor resultados.

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

- Region
- 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

AWS Recomendaciones de compra de Savings Plans para computación

Description (Descripción)

Comprueba sus patrones de uso AWS informático en Amazon EC2 AWS Lambda y proporciona recomendaciones AWS Fargate de compra de Savings Plans. Con estas recomendaciones, puede 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.

Esta verificación genera recomendaciones en el [ámbito del pagador para la cuenta del pagador y en el ámbito vinculado para una cuenta vinculada](#).

Trusted Advisor muestra solo las principales acciones recomendadas entre Centro de optimización de costes de AWS.

Para usar esta verificación, debe iniciar sesión en el [Centro de optimización de 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.

Para los clientes del plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puede usar la [BatchUpdateRecommendationResourceExclusion](#) API para incluir o excluir uno o más recursos de sus Trusted Advisor resultados.

ID de la verificación

c1z7kmr09n

origen

Centro de optimización de costes de AWS

Criterios de alerta

Amarillo: el Centro de optimización de costos ha identificado una acción de ahorro de costos para los recursos de computación en la cuenta.

Acción recomendada

Considere la posibilidad [de implementar la recomendación](#). Para obtener más información sobre la implementación de estas recomendaciones, consulte el manual de [optimización de costos de los servicios](#) de administración financiera en la AWS nube (CFM).

Recursos adicionales

- [¿Qué son los Savings Plans?](#)
- [Tipos de Savings Plans](#)
- [Purchasing Savings Plans](#)

Columnas de informes

- Status
- Region
- Resumen de recursos recomendados
- Costo mensual estimado
- Ahorros mensuales estimados
- Marca temporal de la última actualización

AWS Recomendaciones de compra de Savings Plans para Amazon SageMaker AI

Description (Descripción)

Comprueba el uso que haces de Amazon SageMaker AI y proporciona recomendaciones de compra de Savings Plans. Con estas recomendaciones, puede 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.

Esta verificación genera recomendaciones en el [ámbito del pagador para la cuenta del pagador y en el ámbito vinculado para una cuenta vinculada](#).

Trusted Advisor muestra solo las principales acciones recomendadas entre Centro de optimización de costes de AWS.

Para usar esta verificación, debe iniciar sesión en el [Centro de optimización de 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.

Para los clientes del plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puede usar la [BatchUpdateRecommendationResourceExclusion](#) API para incluir o excluir uno o más recursos de sus Trusted Advisor resultados.

ID de la verificación

c1z7kmr08n

origen

Centro de optimización de costes de AWS

Criterios de alerta

Amarillo: la cuenta tiene una acción de ahorro de costes identificada por Cost Optimization Hub for Amazon SageMaker AI.

Acción recomendada

Considere la posibilidad [de implementar la recomendación](#). Para obtener más información sobre la implementación de estas recomendaciones, consulte el [manual de optimización de costos del servicio](#) de administración financiera en la AWS nube (CFM).

Recursos adicionales

- [¿Qué son los Savings Plans?](#)
- [Tipos de Savings Plans](#)
- [Purchasing Savings Plans](#)

Columnas de informes

- Status
- Region
- Resumen de recursos recomendados
- Costo mensual estimado
- Ahorros mensuales estimados
- Marca temporal de la última actualización

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

Description (Descripción)

Comprueba si hay problemas de alto riesgo (HRIs) para sus cargas de trabajo en el pilar de la optimización de costes. 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.

Para los clientes del plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puede usar la [BatchUpdateRecommendationResourceExclusion](#) API para incluir o excluir uno o más recursos de sus Trusted Advisor resultados.

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 detectó ningún problema activo de alto riesgo en el pilar de optimización de costes 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
- Region
- 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
- Número de identificados HRIs para la optimización de costos
- Número de HRIs 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

Description (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).

 Note

Esta verificación indica los recursos que están marcados según los criterios y el número total de recursos evaluados, incluidos los recursos de OK. La tabla de recursos muestra solo los recursos marcados.

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

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

Puertas de enlace NAT inactivas

Description (Descripción)

Comprueba las configuraciones y los patrones de uso de las puertas de enlace NAT para identificar las puertas de enlace NAT inactivas o infrautilizadas que podrían ser aptas para la optimización de costes.

Para cada recurso, Trusted Advisor muestra solo la acción más recomendada entre. Centro de optimización de costes de AWS

Para usar esta verificación, debe iniciar sesión en el [Centro de optimización de costos](#) y en [AWS Compute Optimizer](#).

ID de la verificación

c1z7kmr18n

origen

Centro de optimización de costes de AWS

Criterios de alerta

Amarillo: la pasarela NAT tiene una acción de ahorro de costes identificada por Cost Optimization Hub.

Acción recomendada

Considere implementar la recomendación de eliminar la puerta de enlace NAT inactiva. Para obtener más información sobre la implementación de esta recomendación, consulte el [manual de optimización de costos de los servicios](#) de administración financiera en la AWS nube.

Recursos adicionales

- [Visualización de las recomendaciones sobre recursos inactivos](#)
- [Trabaje con pasarelas NAT](#)
- [Gateways NAT](#)

Columnas de informes

- Status
- Region
- Resource ID (ID de recurso)
- Acción recomendada

- Resumen de recursos actuales
- Resumen de recursos recomendados
- Costo mensual estimado
- Ahorros mensuales estimados
- Fecha y hora de la última actualización

Inactivo AWS Network Firewall

Description (Descripción)

Comprueba sus AWS Network Firewall puntos finales y le avisa cuando el Network Firewall parece estar inactivo.

Se considera que un firewall de red está inactivo si ninguno de sus puntos de conexión ha procesado datos en los últimos 30 días. Los puntos de conexión del firewall de red generan cargos por hora. Esta verificación le avisa de que el firewall de red no ha procesado ningún dato en los últimos 30 días. Se recomienda eliminar los firewalls de red no utilizados o actualizar la arquitectura.

ID de la verificación

c2v1fg0bfbw

Criterios de alerta

- Amarillo: el firewall de red ha procesado 0 bytes en los últimos 30 días.
- Verde: el firewall de red ha procesado más de 0 bytes en los últimos 30 días.

Acción recomendada

Si el firewall de red no se ha utilizado en los últimos 30 días, considere la posibilidad de eliminarlo.

Si se utiliza Transit Gateway para la comunicación entre VPC, considere la posibilidad de implementar sus firewalls de red en una arquitectura de inspección de red centralizada. Esto puede reducir los costos por hora de los firewalls de red inactivos.

Recursos adicionales

[Precios de AWS Network Firewall](#)

[Inspeccione los modelos de despliegue con AWS Network Firewall](#)

Columnas de informes

- Status
- Region
- ARN de firewall de red
- ID de VPC
- Subredes
- TotalBytesProcessed
- Hora de la última actualización

Puntos de conexión de interfaz de VPC inactivos

Description (Descripción)

Verifica los puntos de conexión de la interfaz de VPC y le avisa cuando parecen estar inactivos. Un punto de conexión de la interfaz de VPC se considera inactivo si no ha procesado datos en los últimos 30 días. Los puntos de conexión de la interfaz de VPC generan cargos por hora y costos de procesamiento de datos. Esta verificación le alerta sobre los puntos de conexión de la interfaz de VPC con 0 datos procesados en los últimos 30 días. Se recomienda eliminar los puntos de conexión de la interfaz de VPC no utilizados o actualizar la arquitectura.

ID de la verificación

c2v1fg0jp6

Criterios de alerta

- Amarillo: el punto de conexión de la interfaz de VPC ha procesado 0 bytes en los últimos 30 días.
- Verde: el punto de conexión de la interfaz de VPC ha procesado más de 0 bytes en los últimos 30 días.

Acción recomendada

Si el punto de conexión de la interfaz de VPC no se ha utilizado en los últimos 30 días, considere la posibilidad de eliminarlo de la interfaz de VPC.

Si se utiliza Transit Gateway para la comunicación entre VPC, considere la posibilidad de implementar los puntos de conexión de la interfaz de VPC en una arquitectura centralizada para reducir los cargos por hora en los puntos de conexión inactivos de la interfaz de VPC.

Recursos adicionales

- [AWS PrivateLink Precios](#)
- [Acceso centralizado a puntos de conexión privados de VPC](#)

Columnas de informes

- Status
- Region
- ID de punto de conexión de VPC
- ID de VPC
- ID de subred
- Nombre del servicio
- TotalBytesProcessed
- Hora de la última actualización

Puntos de conexión inactivos del equilibrador de carga de la puerta de enlace

Description (Descripción)

Verifica los puntos de conexión del equilibrador de carga de puerta de enlace y avisa cuando parecen estar inactivos. Se considera que un punto de conexión del equilibrador de carga de puerta de enlace está infrautilizado si no ha procesado datos en los últimos 30 días. Los puntos de conexión del equilibrador de carga de puerta de enlace generan cargos por hora y por procesamiento de datos. Esta verificación le alerta sobre los puntos de conexión del equilibrador de carga en la puerta de enlace con 0 datos procesados en los últimos 30 días. Le recomendamos que elimine los puntos de conexión del equilibrador de carga de puerta de enlace que no utilice o que actualice su arquitectura.

ID de la verificación

c2v1fg0k35

Criterios de alerta

- Amarillo: el punto de conexión del equilibrador de carga de puerta de enlace ha procesado 0 bytes en los últimos 30 días
- Verde: el punto de conexión del equilibrador de carga de la puerta de enlace ha procesado más de 0 bytes en los últimos 30 días

Acción recomendada

Si el punto de conexión del equilibrador de carga de puerta de enlace no se ha utilizado en los últimos 30 días, considere la posibilidad de eliminar el punto de conexión de VPC.

Si se utiliza Transit Gateway para la comunicación entre VPC, considere la posibilidad de implementar los puntos de conexión del equilibrador de carga de la puerta de enlace en una arquitectura centralizada de inspección de red para reducir los cargos por hora en los puntos de conexión del equilibrador de carga de la puerta de enlace.

Recursos adicionales

[Precios de AWS PrivateLink](#)

[Arquitectura de inspección centralizada con AWS Gateway Load Balancer y AWS Transit Gateway](#)

Columnas de informes

- Status
- Region
- ID de punto de conexión de VPC
- ID de VPC
- ID de subred
- Nombre del servicio
- TotalBytesProcessed
- Hora de la última actualización

Puertas de enlace NAT inactivas

Description (Descripción)

Verifica si las puertas de enlace NAT están inactivas. Una puerta de enlace NAT se considera inactiva si no se ha procesado ningún dato (0 bytes) en los últimos 30 días. Las puertas de enlace NAT generan cargos por hora y por procesamiento de datos.

ID de la verificación

c2v1fg022t

Criterios de alerta

- **Amarillo:** la puerta de enlace NAT ha procesado 0 bytes en los últimos 30 días
- **Verde:** la puerta de enlace NAT procesó más de 0 bytes en los últimos 30 días

Acción recomendada

Considere la posibilidad de eliminar todas las puertas de enlace NAT que no se hayan utilizado en los últimos 30 días y que no sean necesarias para el acceso a redes externas fuera de la VPC.

Si se utiliza una Transit Gateway para la comunicación entre VPC, considere la posibilidad de implementar una puerta de enlace NAT centralizada para la salida a la arquitectura de Internet. Esto puede reducir el costo por hora de las puertas de enlace NAT inactivas.

Recursos adicionales

[Precios de puertas de enlace NAT](#)

[Salida centralizada a Internet](#)

Columnas de informes

- Status
- Region
- ID de puerta de enlace NAT
- ID de subred
- ID de VPC
- TotalBytesFromDest
- TotalBytesFromSrc
- TotalBytes
- Hora de la última actualización

Utilización baja de instancias de Amazon EC2

Description (Descripción)

Note

Esta es una verificación heredada. Se recomienda usar la nueva verificación (ID de verificación: [c1z7kmr00n](#)) que ofrece recomendaciones personalizadas adicionales.

Verifica las instancias de Amazon Elastic Compute Cloud (Amazon EC2) que han estado en ejecución en cualquier momento durante los últimos 14 días. Esta comprobación le avisa si la utilización diaria de la CPU fue del 10% o inferior y la red I/O fue de 5 MB o menos 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.

 Note

Esta verificación indica los recursos que están marcados según los criterios y el número total de recursos evaluados, incluidos los recursos de OK. La tabla de recursos muestra solo los recursos marcados.

ID de la verificación

Qch7DwouX1

Criterios de alerta

Amarillo: una instancia tuvo un uso medio diario de CPU del 10% o menos y una red I/O de 5 MB o menos durante 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 I/O 14 días de red
- Cantidad de días de baja utilización

Direcciones IP elásticas no asociadas

Description (Descripción)

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

EIPs son direcciones IP estáticas diseñadas para la computación en nube dinámica. A diferencia de las direcciones IP estáticas tradicionales, EIPs oculta el error de una instancia o zona de disponibilidad reasignando 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.

Note

Esta verificación indica los recursos que están marcados según los criterios y el número total de recursos evaluados, incluidos los recursos de OK. La tabla de recursos muestra solo los recursos marcados.

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

- Region
- Dirección IP

Volúmenes de Amazon EBS infrautilizados

Description (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.

Note

Esta verificación indica los recursos que están marcados según los criterios y el número total de recursos evaluados, incluidos los recursos de OK. La tabla de recursos muestra solo los recursos marcados.

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

- Region
- 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 optó por ello en su cuenta AWS Compute Optimizer, le recomendamos que utilice en su lugar la comprobación de volúmenes sobreaaprovisionados de Amazon EBS. Para obtener más información, consulte [Optar AWS Compute Optimizer por recibir Trusted Advisor cheques](#).

Underutilized Amazon Redshift Clusters

Description (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
- Region
- Clúster
- Tipo de instancia
- Motivo
- Ahorros mensuales estimados

Desempeño

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

- [El clúster de base de datos Amazon Aurora está insuficientemente aprovisionado 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 autovacuum de Amazon RDS está desactivado](#)
- [Los clústeres de base de datos de Amazon RDS solo admiten un volumen de hasta 64 TiB](#)
- [Instancias de bases de datos de Amazon RDS en los clústeres con clases de instancia heterogéneas](#)
- [Instancias de bases de datos de Amazon RDS en los clústeres con tamaños de instancia heterogéneos](#)
- [Los parámetros de la memoria de la 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 con 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](#)
- [Volumen magnético Amazon RDS en uso](#)
- [Los grupos de parámetros de Amazon RDS no utilizan páginas de gran tamaño](#)
- [El parámetro del caché de consultas de Amazon RDS está activado](#)
- [Es necesaria la actualización de la clase de instancia de los recursos de Amazon RDS](#)
- [Es necesario actualizar las versiones principales de los recursos de Amazon RDS](#)
- [Los recursos de Amazon RDS utilizan una edición del motor al final del soporte con licencia incluida](#)

- [Conjuntos de registros de recursos de alias en Amazon Route 53](#)
- [AWS Lambda funciones insuficientemente aprovisionadas 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](#)
- [Instancias de Amazon EC2 de alta utilización de CPU](#)

El clúster de base de datos Amazon Aurora está insuficientemente aprovisionado para la carga de trabajo de lectura

Description (Descripción)

Verifica 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

Yellow:

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,

Acción recomendada

Se recomienda que ajuste las consultas para disminuir la carga de la base de datos o que agregue 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 escritor del clúster. La configuración actual tiene al menos una instancia de base de datos con una carga de base de datos continuamente alta, causada en el mayor número de casos por 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 de conexión del lector para conexiones de solo lectura. Este punto de conexión 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 de conexión del lector dirige estas declaraciones a las réplicas de lectura de Aurora y reduce la carga en la instancia principal. El punto de conexión 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
- Region
- Recurso
- Aumento de la lectura (recuento) de la base de datos
- Período de la última detección
- Hora de la última actualización

El escalado automático de Amazon DynamoDB no está habilitado

Description (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 las comprobaciones 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.

Para los clientes del plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puede usar la [BatchUpdateRecommendationResourceExclusion](#) API para incluir o excluir uno o más recursos de sus Trusted Advisor resultados.

ID de la verificación

c18d2gz136

origen

AWS Config Regla gestionada: dynamodb-autoscaling-enabled

Criterios de alerta

Amarillo: el escalado automático no está activado para los índices secundarios globales de and/or las tablas de DynamoDB.

Acción recomendada

A menos que ya disponga de un mecanismo para escalar automáticamente el rendimiento aprovisionado de su tabla and/or de DynamoDB (los índices secundarios globales) en función de sus requisitos de carga de trabajo, considere activar el escalado automático para sus tablas de Amazon DynamoDB.

Para obtener más información, consulte [Uso de Consola de administración de AWS with DynamoDB auto scalingp](#).

Recursos adicionales

[Administración automática de la capacidad de rendimiento con el escalado automático de DynamoDB](#)

Columnas de informes

- Status
- Region
- Recurso

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

La optimización de Amazon EBS no está habilitada

Description (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 Amazon EBS I/O. This optimization provides the best performance for your Amazon EBS volumes by minimizing contention between Amazon EBS I/O y otro tráfico 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.

Para los clientes del plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puede usar la [BatchUpdateRecommendationResourceExclusionAPI](#) para incluir o excluir uno o más recursos de sus Trusted Advisor resultados.

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
- Region
- 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

Description (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

Description (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.

Para los clientes del plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puede usar la [BatchUpdateRecommendationResourceExclusionAPI](#) para incluir o excluir uno o más recursos de sus Trusted Advisor resultados.

ID de la verificación

C0r6dfpM04

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
- Region
- 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

Description (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.

Para los clientes del plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puede usar la [BatchUpdateRecommendationResourceExclusion](#) API para incluir o excluir uno o más recursos de sus Trusted Advisor resultados.

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

Optimización del rendimiento de Amazon EC2 a EBS

Description (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
- Region
- ID de instancia
- Tipo de instancia
- Tiempo cerca del máximo

El tipo de virtualización de EC2 es paravirtual

Description (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 la HVM y a la disponibilidad de controladores fotovoltáicos para la HVM AMIs, que han cerrado la brecha de rendimiento que existía históricamente entre los huéspedes de sistemas fotovoltáicos y de HVM. Es importante tener en cuenta que los tipos de instancias de la generación actual no son compatibles con la energía fotovoltáica. AMIs 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.

Para los clientes del plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puede usar la [BatchUpdateRecommendationResourceExclusionAPI](#) para incluir o excluir uno o más recursos de sus Trusted Advisor resultados.

ID de la verificación

c18d2gz148

origen

AWS Config Regla gestionada: 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
- Region
- Recurso
- AWS Config Regla
- Parámetros de entrada
- Hora de la última actualización

Límite máximo de memoria de Amazon ECS

Description (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.

Para los clientes del plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puede usar la [BatchUpdateRecommendationResourceExclusionAPI](#) para incluir o excluir uno o más recursos de sus Trusted Advisor resultados.

ID de la verificación

c18d2gz176

origen

AWS Config Regla gestionada: -hard-limit ecs-task-definition-memory

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

Optimización del modo de rendimiento de Amazon EFS

Description (Descripción)

Verifica si el sistema de archivos de Amazon EFS del cliente está configurado actualmente para utilizar el modo de rendimiento por ráfagas. El rendimiento en ráfagas de Amazon EFS utiliza «créditos» para un rendimiento superior al rendimiento de referencia (50 por KiB/s GiB). Una vez agotados los créditos, el rendimiento se limita hasta alcanzar el rendimiento básico, lo que puede provocar lentitud, errores en las aplicaciones y tiempos de espera para los usuarios. Para obtener más información sobre el modo por ráfagas, consulte [Modo de rendimiento](#) en la Guía del usuario de Amazon EFS

ID de la verificación

c1dfprch02

Criterios de alerta

- Amarillo: el sistema de archivos utiliza el modo de rendimiento por ráfaga.

Acción recomendada

Si sus créditos de rendimiento por ráfagas son bajos o están agotados, considere la posibilidad de cambiar al modo de rendimiento elástico o aprovisionado para ofrecer a sus usuarios y aplicaciones el rendimiento deseado. Con el rendimiento aprovisionado puede establecer el rendimiento requerido de su carga de trabajo y pagar por la cantidad de rendimiento habilitada para el sistema de archivos. Si no está seguro de cuáles son sus requisitos de rendimiento, se puede utilizar el modo de rendimiento elástico, en el que el rendimiento se escala de forma elástica con la carga de trabajo y solo paga por lo que utiliza, medido en función del total de datos transferidos. Puede actualizar la configuración del sistema de archivos para cambiar entre los modos de rendimiento en cualquier momento. Para obtener más información sobre precios del rendimiento, consulte [Precios de Amazon EFS](#). Puede calcular también sus costos con [Calculadora de precios de AWS](#).

Recursos adicionales

- [Rendimiento en ráfaga](#)
- [Precios de Amazon EFS](#)
- [Calculadora de precios de AWS](#)

Columnas de informes

- Status
- Region
- ID del sistema de archivos de EFS
- Modo de rendimiento
- Hora de la última actualización

El parámetro autovacuum de Amazon RDS está desactivado

Description (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.

Para los clientes del plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puede usar la [BatchUpdateRecommendationResourceExclusion](#) API para incluir o excluir uno o más recursos de sus Trusted Advisor resultados.

 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 autovacuum desactivado.

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 autovacuum. 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 autovacuum está desactivado, 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 [Understanding autovacuum in Amazon RDS for PostgreSQL environments](#).

Columnas de informes

- Status
- Region
- Recurso
- Nombre del parámetro
- Valores recomendados
- Hora de la última actualización

Los clústeres de base de datos de Amazon RDS solo admiten un volumen de hasta 64 TiB

Description (Descripción)

Sus clústeres de base de datos admiten volúmenes de hasta 64 TiB. Las versiones más recientes del motor admiten volúmenes de hasta 128 TiB. Le recomendamos que actualice la versión del 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.

Para los clientes del plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puede usar la [BatchUpdateRecommendationResourceExclusion](#) API para incluir o excluir uno o más recursos de sus Trusted Advisor resultados.

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 solo admiten un volumen 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 escalar verticalmente 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 [Límites de tamaño de Amazon Aurora](#).

Columnas de informes

- Status
- Region
- Recurso
- Nombre del motor
- Versión del motor actual
- Valores recomendados
- Hora de la última actualización

Instancias de bases de datos de Amazon RDS en los clústeres con clases de instancia heterogéneas

Description (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.

Para los clientes del plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puede usar la [BatchUpdateRecommendationResourceExclusion](#) API para incluir o excluir uno o más recursos de sus Trusted Advisor resultados.

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

Rojos: clústeres de base de datos tienen instancias de bases de datos con clases de instancia 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 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 lector pasa a ser una instancia de base de datos de escritor. 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 en su clúster de base de datos.

Para obtener más información, consulte [Réplicas de Aurora](#).

Columnas de informes

- Status
- Region
- Recurso
- Valores recomendados
- Nombre del motor
- Hora de la última actualización

Instancias de bases de datos de Amazon RDS en los clústeres con tamaños de instancia heterogéneos

Description (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.

Para los clientes del plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puede usar la [BatchUpdateRecommendationResourceExclusionAPI](#) para incluir o excluir uno o más recursos de sus Trusted Advisor resultados.

 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: instancias de bases de datos en los clústeres 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 lector pasa a ser una instancia de base de datos de escritor. 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 en su clúster de base de datos.

Para obtener más información, consulte [Réplicas de Aurora](#).

Columnas de informes

- Status
- Region
- Recurso
- Valores recomendados
- Nombre del motor
- Hora de la última actualización

Los parámetros de la memoria de la base de datos de Amazon RDS difieren de los predeterminados

Description (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.

Para los clientes del plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puede usar la [BatchUpdateRecommendationResourceExclusion](#) API para incluir o excluir uno o más recursos de sus Trusted Advisor resultados.

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 se diferencian 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
- Region
- Recurso
- Nombre del parámetro
- Valores recomendados
- Hora de la última actualización

El parámetro enable_indexonlyscan de Amazon RDS está desactivado

Description (Descripción)

El planificador u optimizador de consultas no puede usar el plan de análisis de solo índice si está desactivado.

Se recomienda que establezca 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.

Para los clientes del plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puede usar la [BatchUpdateRecommendationResourceExclusionAPI](#) para incluir o excluir uno o más recursos de sus Trusted Advisor resultados.

 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 costo 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
- Region
- Recurso
- Nombre del parámetro
- Valores recomendados
- Hora de la última actualización

El parámetro enable_indexscan de Amazon RDS está desactivado

Description (Descripción)

El planificador u optimizador de consultas no puede usar el plan de análisis de índice si está desactivado.

Es recomendable que establezca 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.

Para los clientes del plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puede usar la [BatchUpdateRecommendationResourceExclusion](#) API para incluir o excluir uno o más recursos de sus Trusted Advisor resultados.

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 costo 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
- Region
- Recurso
- Nombre del parámetro
- Valores recomendados
- Hora de la última actualización

El parámetro general_logging de Amazon RDS está activado

Description (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, activar el registro general aumenta la cantidad de I/O operaciones y el espacio de almacenamiento asignado, lo que puede provocar contención y una degradación del rendimiento.

Compruebe sus requisitos para el uso del registro general. Se recomienda que establezca 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.

Para los clientes del plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puede usar la [BatchUpdateRecommendationResourceExclusionAPI](#) para incluir o excluir uno o más recursos de sus Trusted Advisor resultados.

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 `general_logging` activado.

Acción recomendada

Compruebe sus requisitos para el uso del registro general. Si no es obligatorio, se recomienda que establezca 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 usuarios se conectan o desconectan y los registros contienen todas las instrucciones SQL recibidas 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 ha enviado al servidor de la base de datos.

Para obtener más información, consulte [Overview of RDS for MySQL database logs](#).

Columnas de informes

- Status
- Region
- Recurso
- Nombre del parámetro
- Valores recomendados
- Hora de la última actualización

Parámetro `InnoDB_Change_Buffering` de Amazon RDS con un valor inferior al óptimo

Description (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.

Para los clientes del plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puede usar la [BatchUpdateRecommendationResourceExclusion](#) API para incluir o excluir uno o más recursos de sus Trusted Advisor resultados.

 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

Establezca 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
- Region
- Recurso
- Nombre del parámetro
- Valores recomendados
- Hora de la última actualización

El parámetro innodb_open_files de Amazon RDS es bajo

Description (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 que establezca 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.

Para los clientes del plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puede usar la [BatchUpdateRecommendationResourceExclusionAPI](#) para incluir o excluir uno o más recursos de sus Trusted Advisor resultados.

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 para 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 todos los archivos de registro y los archivos de espacio de tablas del sistema abiertos 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
- Region
- Recurso
- Nombre del parámetro
- Valores recomendados
- Hora de la última actualización

El parámetro innodb_stats_persistent de Amazon RDS está desactivado

Description (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.

Para los clientes del plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puede usar la [BatchUpdateRecommendationResourceExclusionAPI](#) para incluir o excluir uno o más recursos de sus Trusted Advisor resultados.

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
- Region
- Recurso
- Nombre del parámetro
- Valores recomendados
- Hora de la última actualización

Instancia de Amazon RDS con aprovisionamiento insuficiente para la capacidad del sistema

Description (Descripción)

Verifica 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

Yellow:

Out-of-memory muertes: cuando un proceso en el host de la base de datos se detiene debido a una reducción de memoria a nivel del sistema operativo, el contador de cancelaciones 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 una mayor memoria asignada. Cuando la instancia se ejecuta con poca memoria, el rendimiento de la base de datos se ve afectado.

Recursos adicionales

Out-of-memory se detectaron muertes: el núcleo 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
- Region
- Recurso
- Out-of-memory muertes (contar)
- Intercambio excesivo (recuento)
- Período de la última detección

- Hora de la última actualización

Volumen magnético Amazon RDS en uso

Description (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.

Para los clientes del plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puede usar la [BatchUpdateRecommendationResourceExclusionAPI](#) para incluir o excluir uno o más recursos de sus Trusted Advisor resultados.

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 el 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 IOPS aprovisionadas. Estos tipos de almacenamiento ofrecen un rendimiento superior y uniforme y opciones de tamaño de almacenamiento mejoradas.

Para obtener más información, consulte [Volumen de generaciones anteriores](#).

Columnas de informes

- Status
- Region
- Recurso
- Valores recomendados
- Nombre del motor
- Hora de la última actualización

Los grupos de parámetros de Amazon RDS no utilizan páginas de gran tamaño

Description (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 `ONLY` en el grupo de parámetros de base de datos 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.

Para los clientes del plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puede usar la [BatchUpdateRecommendationResourceExclusion](#) API para incluir o excluir uno o más recursos de sus Trusted Advisor resultados.

 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 ONLY en sus grupos de parámetros de base de datos.

Recursos adicionales

Para obtener más información, consulte [Cómo activar una HugePages instancia de RDS para Oracle](#).

Columnas de informes

- Status
- Region
- Recurso
- Nombre del parámetro
- Valores recomendados
- Hora de la última actualización

El parámetro del caché de consultas de Amazon RDS está activado

Description (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.

Para los clientes del plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puede usar la [BatchUpdateRecommendationResourceExclusionAPI](#) para incluir o excluir uno o más recursos de sus Trusted Advisor resultados.

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

Establezca el valor del parámetro `query_cache_type` en 0 en el grupo de parámetros de su 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
- Region
- Recurso
- Nombre del parámetro
- Valores recomendados
- Hora de la última actualización

Es necesaria la actualización de la clase de instancia de los recursos de Amazon RDS

Description (Descripción)

Su base de datos se ejecuta en una clase de instancia de base de datos de generación anterior. Hemos sustituido las clases de instancia de base de datos de una generación anterior por clases de instancia de base de datos con mejor costo, 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.

Para los clientes del plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puede usar la [BatchUpdateRecommendationResourceExclusionAPI](#) para incluir o excluir uno o más recursos de sus Trusted Advisor resultados.

 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 la clase de instancia de base de datos de fin de soporte.

Acción recomendada

Actualizar a la clase de instancia de bases de datos más reciente.

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
- Region
- Recurso
- Clase de instancia de base de datos
- Valores recomendados
- Nombre del motor
- Hora de la última actualización

Es necesario actualizar las versiones principales de los recursos de Amazon RDS

Description (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.

Para los clientes del plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puede usar la [BatchUpdateRecommendationResourceExclusion](#) API para incluir o excluir uno o más recursos de sus Trusted Advisor resultados.

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 lanzadas pueden incluir correcciones de errores, mejoras de seguridad y otras mejoras para 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 blue/green implementación.

Para obtener más información, consulte los siguientes recursos:

- [Upgrading a DB instance engine version](#)
- [Actualizaciones de Amazon Aurora](#)
- [Uso de Amazon RDS Blue/Green Deployments para actualizaciones de bases de datos](#)

Columnas de informes

- Status
- Region
- Recurso
- Nombre del motor
- Versión actual del motor
- Valores recomendados
- Hora de la última actualización

Los recursos de Amazon RDS utilizan una edición del motor al final del soporte con licencia incluida

Description (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.

Para los clientes del plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puede usar la [BatchUpdateRecommendationResourceExclusionAPI](#) para incluir o excluir uno o más recursos de sus Trusted Advisor resultados.

 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 una edición del motor al final del soporte 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 [Actualizaciones de versiones principales de Oracle](#).

Columnas de informes

- Status
- Region
- Recurso
- Nombre del motor

- Versión del motor actual
- Valores recomendados
- Nombre del motor
- Hora de la última actualización

Conjuntos de registros de recursos de alias en Amazon Route 53

Description (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.

Note

Esta verificación indica los recursos que están marcados según los criterios y el número total de recursos evaluados, incluidos los recursos de OK. La tabla de recursos muestra solo los recursos marcados.

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

AWS Lambda funciones insuficientemente aprovisionadas para el tamaño de la memoria

Description (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.

Para los clientes del plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puede usar la [BatchUpdateRecommendationResourceExclusionAPI](#) para incluir o excluir uno o más recursos de sus Trusted Advisor resultados.

ID de la verificación

C0r6dfpM06

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
- Region
- 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

Description (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 de simultaneidad reservado mínimo y máximo mediante los `ConcurrencyLimitHigh` y `ConcurrencyLimitLow` parámetros 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.

Para los clientes del plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puede usar la [BatchUpdateRecommendationResourceExclusion](#) API para incluir o excluir uno o más recursos de sus Trusted Advisor resultados.

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

Problemas de alto riesgo de AWS Well-Architected para el rendimiento

Description (Descripción)

Comprueba si hay problemas de alto riesgo (HRIs) para sus cargas de trabajo en el pilar del 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.

Para los clientes del plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puede usar la [BatchUpdateRecommendationResourceExclusionAPI](#) para incluir o excluir uno o más recursos de sus Trusted Advisor resultados.

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
- Region
- 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
- Número de identificados HRIs para el rendimiento
- Número de resultados HRIs 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

Description (Descripción)

Note

Esta comprobación se aplica a las CloudFront distribuciones clásicas de Amazon.

Comprueba que el DNS esté correctamente configurado en CloudFront las distribuciones clásicas de Amazon que utilizan nombres de dominio alternativos (CNAMEs).

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 \(CNAMEs\)](#).

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

Description (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.

 Note

Esta verificación indica los recursos que están marcados según los criterios y el número total de recursos evaluados, incluidos los recursos de OK. La tabla de recursos muestra solo los recursos marcados.

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

Considera usarlo CloudFront 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
- Region
- 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

Description (Descripción)

Note

Esta comprobación se aplica a las CloudFront distribuciones clásicas de Amazon.

Comprueba los encabezados de las solicitudes HTTP que recibe CloudFront actualmente del cliente y los reenvía a tu 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

- [Incrementar la proporción de solicitudes que atienden las cachés de periferia de CloudFront](#)
- [CloudFront Informes de estadísticas en 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

Instancias de Amazon EC2 de alta utilización de CPU

Description (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.

Note

Esta verificación indica los recursos que están marcados según los criterios y el número total de recursos evaluados, incluidos los recursos de OK. La tabla de recursos muestra solo los recursos marcados.

ID de la verificación

ZRxQ1Psb6c

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 ha activado Security Hub CSPM para usted Cuenta de AWS, puede ver los resultados en la Trusted Advisor consola. Para obtener información, consulte [Visualización de AWS Security Hub CSPM los controles 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 CSPM .

Nombres de la verificación

- [Grupo de seguridad del equilibrador de carga de aplicación](#)
- [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](#)
- [Instancias de Amazon EC2 con final del soporte estándar con Ubuntu LTS](#)
- [Los clientes de Amazon EFS no utilizan el cifrado de datos en tránsito](#)

- [Instantáneas públicas de Amazon EBS](#)
- [El cifrado de almacenamiento de Amazon RDS Aurora está desactivado](#)
- [Debe efectuarse una actualización menor de la versión del motor de 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 de S3](#)
- [Marco de políticas de remitentes y conjuntos de registros de recursos MX de Amazon Route 53](#)
- [Permisos de bucket de Amazon S3](#)
- [Conexiones de emparejamiento de Amazon VPC con la resolución de DNS deshabilitada](#)
- [Protocolo de cifrado de grupos de destino del equilibrador de carga de aplicación](#)
- [AWS Backup Almacene sin una Resource-based política para evitar la eliminación de los puntos de recuperación](#)
- [AWS CloudTrail Registro de eventos de administración](#)
- [AWS Lambda Funciones que utilizan tiempos de ejecución obsoletos](#)
- [AWS Well-Architected problemas de seguridad de alto riesgo](#)
- [CloudFront Certificados SSL personalizados en la tienda de certificados de IAM](#)
- [CloudFront Certificado SSL en el servidor de origen](#)
- [Seguridad del agente de escucha de ELB](#)
- [Grupos de seguridad del equilibrador de carga clásico](#)
- [Exposed Access Keys](#)
- [Rotación de claves de acceso de IAM](#)
- [Acceso externo de IAM Access Analyzer](#)
- [Política de contraseñas de IAM](#)
- [Proveedor de identidades IAM SAML 2.0](#)
- [MFA en la cuenta raíz](#)
- [Clave de acceso de usuario raíz](#)
- [Grupos de seguridad: puertos específicos sin restricciones](#)

- [Grupos de seguridad: acceso sin restricciones](#)

Grupo de seguridad del equilibrador de carga de aplicación

Description (Descripción)

Verifica los grupos de seguridad adjuntos al equilibrador de carga de aplicación y sus destinos de Amazon EC2. Los grupos de seguridad del equilibrador de carga de aplicación solo deben permitir los puertos entrantes que estén configurados en un oyente. Los grupos de seguridad de un destino no deben aceptar conexiones directas desde Internet en el mismo puerto en el que el destino recibe el tráfico del equilibrador de carga.

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 equilibrador de carga o permite acceso directo a los objetivos.

Esta verificación excluye los siguientes grupos:

- Grupos de destino que no están asociados a direcciones IP o instancias EC2.
- Reglas de grupo de seguridad para el tráfico de IPv6

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.

Para los clientes del plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puede usar la [BatchUpdateRecommendationResourceExclusionAPI](#) para incluir o excluir uno o más recursos de sus Trusted Advisor resultados.

ID de la verificación

8604e947f2

Criterios de alerta

- Red: Target tiene una IP pública y un grupo de seguridad que permite las conexiones entrantes en el puerto de control de destino desde cualquier lugar (0.0.0). 0/0).
- Rojo: Target tiene una IP pública y un grupo de seguridad que permite las conexiones entrantes en el puerto de tráfico desde cualquier lugar (0.0.0). 0/0).

- Rojo: Application Load Balancer tiene habilitada la autenticación y Target permite conexiones entrantes en el puerto de tráfico desde cualquier lugar (0.0.0. 0/0).
- Amarillo: el grupo de seguridad de Target permite las conexiones entrantes en el puerto de tráfico desde cualquier lugar (0.0.0. 0/0).
- Amarillo: el grupo de seguridad de Target permite las conexiones entrantes en el puerto de control de destino desde cualquier lugar (0.0.0. 0/0).
- Amarillo: el grupo de seguridad del equilibrador de carga de aplicación permite las conexiones entrantes en puertos que no tienen un oyente correspondiente.
- Amarillo: el grupo de seguridad de Target permite las conexiones entrantes en el puerto de control de destino desde un grupo de seguridad que no está conectado a Application Load Balancer.
- Verde: el grupo de seguridad Application Load Balancer solo permite conexiones entrantes en los puertos que coinciden con un listener.

Acción recomendada

Para mejorar la seguridad, asegúrese de que sus grupos de seguridad solo permitan los flujos de tráfico necesarios:

- Los grupos de seguridad del equilibrador de carga de aplicación solo deben permitir las conexiones entrantes para los mismos puertos que estén configurados en un oyente.
- Utilice grupos de seguridad exclusivos para los destinos y los equilibradores de carga.
- Los grupos de seguridad de destino deberían permitir las conexiones en el puerto de tráfico únicamente desde los equilibradores de carga a los que estén asociados.
- Los grupos de seguridad de destino deberían permitir las conexiones en el puerto de control de destino únicamente desde los balanceadores de carga a los que estén asociados.

Recursos adicionales

- [Controlar el tráfico hacia los recursos de AWS mediante grupos de seguridad](#)
- [Grupos de seguridad para el equilibrador de carga de aplicación](#)

Columnas de informes

- Status
- Region
- Grupo de destinos
- Nombre de ALB
- ID de SG de ALB

- ID de SG de destino
- Autenticación habilitada
- Hora de la última actualización

Período de retención de Amazon CloudWatch Log Group

Description (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 `MinRetentionTime` parámetros `LogGroupName`s 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.

Para los clientes del plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puede usar la [BatchUpdateRecommendationResourceExclusion](#) API para incluir o excluir uno o más recursos de sus Trusted Advisor resultados.

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

Instancias de Amazon EC2 con fin del soporte para Microsoft SQL Server

Description (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.

Para los clientes del plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puede usar la [BatchUpdateRecommendationResourceExclusionAPI](#) para incluir o excluir uno o más recursos de sus Trusted Advisor resultados.

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 su SQL Server en Amazon EC2, considere el Programa de End-of-Support migración (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
- Region

- 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

Description (Descripción)

Esta verificación le avisa si a las versiones de Microsoft Windows Server les queda poco tiempo de soporte o si dicho soporte ya se ha vencido. Cada versión de Windows Server ofrece 10 años de soporte, que incluyen 5 años de soporte general y 5 años de soporte ampliado. Una vez que se llega al final del soporte, la versión de Windows Server no recibirá actualizaciones de seguridad periódicas. La ejecución de aplicaciones con versiones de Windows Server no compatibles puede suponer riesgos de seguridad o conformidad.

Note

Esta verificación genera resultados en función de la AMI utilizada para lanzar la instancia de EC2. Es posible que el sistema operativo de la instancia actual sea diferente de su AMI de lanzamiento. Por ejemplo, si lanzó una instancia desde una AMI de Windows Server 2016 y, posteriormente, la actualizó a Windows Server 2019, la AMI de lanzamiento no cambiará.

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.

Para los clientes del plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puede usar la [BatchUpdateRecommendationResourceExclusion](#) API para incluir o excluir uno o más recursos de sus Trusted Advisor resultados.

ID de la verificación

Qsdfp3A4L4

Criterios de alerta

- Rojo: una instancia de EC2 se ejecuta en una versión de Windows Server que ha llegado al final del soporte (Windows Server 2003, 2003 R2, 2008 y 2008 R2).
- Amarillo: una instancia de EC2 tiene una versión de Windows Server que llegará al final del soporte 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](#).

Realice los siguientes pasos:

- Actualización de la versión de Windows Server
- Detener e iniciar la actualización
- Si utiliza EC2Config, migre a EC2Launch

Columnas de informes

- Status
- Region
- ID de instancia
- Versión de Windows Server
- Ciclo de soporte
- Fin del soporte
- Hora de la última actualización

Instancias de Amazon EC2 con final del soporte estándar con Ubuntu LTS

Description (Descripción)

Esta verificación le avisa si a las versiones les queda poco tiempo de soporte o si dicho soporte ya se ha vencido. Es importante tomar medidas, ya sea migrando al siguiente LTS o

actualizándolo a Ubuntu Pro. Una vez que se llega al final del soporte, sus máquinas 18.04 LTS no recibirán actualizaciones de seguridad. Con una suscripción a Ubuntu Pro, su implementación de Ubuntu 18.04 LTS podrá recibir mantenimiento de seguridad ampliado (ESM) hasta 2028. Las vulnerabilidades de seguridad que no se hayan reparado exponen los sistemas a los piratas informáticos y corren el riesgo de sufrir una violación grave.

Note

Los resultados de esta verificación se actualizan de manera automática al menos una vez por día, y no se permiten las solicitudes de actualización. Puede que los cambios tarden unas horas en aparecer.

Para los clientes del plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puede usar la [BatchUpdateRecommendationResourceExclusionAPI](#) para incluir o excluir uno o más recursos de sus Trusted Advisor resultados.

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](#), visite la consola de AWS License Manager y siga los pasos que se mencionan en la [guía del usuario de AWS License Manager](#). También puede 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, contáctese con [Soporte](#).

Columnas de informes

- Status
- Region
- 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 el cifrado de datos en tránsito

Description (Descripción)

Verifica si el sistema de archivos de Amazon EFS está montado mediante cifrado de datos en tránsito. AWS recomienda que los clientes utilicen el cifrado de datos en tránsito para todos los flujos de datos a fin de 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 el cifrado de datos en tránsito.

Verde: todos los clientes NFS de su sistema de archivos Amazon EFS utilizan la configuración de montaje recomendada que proporciona cifrado de datos en tránsito.

Acción recomendada

Para aprovechar la característica de cifrado de datos en tránsito de Amazon EFS, le recomendamos que vuelva a montar el sistema de archivos con 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 estas características de TLS de forma predeterminada. Si utiliza una distribución de Linux no compatible (consulte [Distribuciones compatibles](#) en la Guía del usuario de Amazon Elastic File System), se recomienda 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
- Region
- ID del sistema de archivos de EFS
- Zonas de disponibilidad con conexiones no cifradas
- Hora de la última actualización

Instantáneas públicas de Amazon EBS

Description (Descripción)

Verifica la configuración de permisos de las instantáneas de volumen de Amazon Elastic Block Store (Amazon EBS) y le avisa si hay alguna instantánea accesible de manera pública.

Al hacer pública una instantánea, concedes a todas las 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. Tenga en cuenta que si ha activado la opción Bloquear el acceso público en el modo 'bloquear todo lo que se comparte', las instantáneas públicas no serán de acceso público y no aparecerán en los resultados de esta verificación.

 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 desea conceder permisos. Para obtener más información, consulte [Compartir una instantánea de Amazon EBS](#). Utilice el bloqueo del acceso público de instantáneas de EBS para controlar la configuración que permite el acceso público a los 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
- Region
- ID de volumen
- ID de instantánea
- Description (Descripción)

El cifrado de almacenamiento de Amazon RDS Aurora está desactivado

Description (Descripción)

Amazon RDS admite el cifrado en reposo para todos los motores de bases de datos mediante las claves que administra en 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 de Aurora, entonces, 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.

Para los clientes del plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puede usar la [BatchUpdateRecommendationResourceExclusionAPI](#) para incluir o excluir uno o más recursos de sus Trusted Advisor resultados.

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 de 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 en un clúster de base de datos cifrado. Sin embargo, sí es posible restaurar una instantánea sin cifrar 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
- Region
- Recurso
- Nombre del motor
- Hora de la última actualización

Debe efectuarse una actualización menor de la versión del motor de Amazon RDS

Description (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.

Para los clientes del plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puede usar la [BatchUpdateRecommendationResourceExclusionAPI](#) para incluir o excluir uno o más recursos de sus Trusted Advisor resultados.

 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

Amarillo: los recursos de su base de datos de Amazon no están ejecutando la última versión secundaria del motor de base de datos.

Acción recomendada

Actualice a la última versión del motor.

Recursos adicionales

Le recomendamos que su base de datos esté actualizada con la última versión secundaria del motor de base de datos, ya que incluirá las últimas correcciones de seguridad y funcionalidad. Las actualizaciones de versiones secundarias del motor de base de datos contienen solo los cambios 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
- Region
- Recurso
- Nombre del motor
- Versión del motor actual
- Valores recomendados
- Hora de la última actualización

Instantáneas públicas de Amazon RDS

Description (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.

Cuando hace pública una instantánea, permite a todos los usuarios Cuentas de AWS y a todos los usuarios acceder 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
- Region
- Instancia de base de datos o ID de clúster
- ID de instantánea

Amazon RDS Security Group Access Risk

Description (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.

Note

Esta verificación evalúa únicamente los grupos de seguridad que están conectados a instancias de Amazon RDS que se ejecutan fuera de una [Amazon VPC](#).

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.
- **Rojo:** una regla de grupo de seguridad de base de datos otorga acceso global (el sufijo de la regla CIDR es /0).
- **Verde:** un grupo de seguridad de base de datos no incluye reglas permisivas.

Acción recomendada

EC2-Classic se retiró el 15 de agosto de 2022. Se recomienda trasladar las instancias de Amazon RDS a una VPC y utilizar grupos de seguridad de Amazon EC2. Para obtener más información sobre cómo mover una instancia de base de datos a una VPC, consulte [Mover una instancia de base de datos que no está en una VPC a una VPC](#).

Si no se pueden migrar sus instancias de Amazon RDS a una VPC, 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 [AuthorizeDBSecurityGroupIngress](#) API o la Consola de administración de AWS. Para obtener más información, consulte [Trabajo con grupos de seguridad de base de datos](#).

Recursos adicionales

- [Grupos de seguridad de Amazon RDS](#)
- [Enrutamiento sin clase Inter-Domain](#)
- [Lista de números de puertos TCP y UDP](#)

Columnas de informes

- Status
- Region
- Nombre de grupo de seguridad RDS
- Regla de entrada
- Motivo

El cifrado de almacenamiento de Amazon RDS está desactivado

Description (Descripción)

Amazon RDS admite el cifrado en reposo para todos los motores de bases de datos mediante las claves que administra en 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, se debe restaurar una copia cifrada de la instantánea descifrada de la instancia 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.

Para los clientes del plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puede usar la [BatchUpdateRecommendationResourceExclusionAPI](#) para incluir o excluir uno o más recursos de sus Trusted Advisor resultados.

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

Solo se puede cifrar una instancia de base de datos al crearla. 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 recursos de Amazon RDS](#)
- [Copiar una instantánea de base de datos](#)

Columnas de informes

- Status
- Region
- Recurso
- Nombre del motor
- Hora de la última actualización

Registros CNAME no coincidentes de Amazon Route 53 que apuntan directamente a buckets de S3

Description (Descripción)

Verifica las zonas alojadas de Amazon Route 53 con registros CNAME que apuntan directamente a los nombres de host del bucket de Amazon S3 y le avisa 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 del bucket de S3 no coinciden.

Verde: no se han encontrado registros CNAME que no coinciden en su zona alojada de Amazon Route 53.

Acción recomendada

Al apuntar registros CNAME a nombres de host del bucket de S3, debe asegurarse de que existe un bucket coincidente para cualquier registro CNAME o alias que configure. De este modo, evita el riesgo de que los registros CNAME sean falsificados. También evita que cualquier AWS usuario no autorizado aloje contenido web defectuoso o malintencionado en su 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
- ARN de zona alojada
- Registros CNAME coincidentes
- Registros CNAME no coincidentes
- Hora de la última actualización

Marco de políticas de remitentes y conjuntos de registros de recursos MX de Amazon Route 53

Description (Descripción)

Para cada registro MX, verifica un registro TXT asociado que contenga un valor SPF válido. El valor del registro TXT debe comenzar con "v=spf1". Los tipos de registro SPF están obsoletos por el Internet Engineering Task Force (IETF). Con Route 53, se recomienda utilizar un registro TXT en lugar de un registro SPF. Trusted Advisor muestra esta marca en verde cuando un registro MX tiene al menos un registro TXT asociado con un valor SPF válido.

Note

Esta verificación indica los recursos que están marcados según los criterios y el número total de recursos evaluados, incluidos los recursos de OK. La tabla de recursos muestra solo los recursos marcados.

ID de la verificación

c9D319e7sG

Criterios de alerta

- Verde: un conjunto de registros de recursos MX tiene un registro de recursos TXT que contiene un valor SPF válido.
- Amarillo: un conjunto de registros de recursos MX tiene un registro de recursos TXT o SPF que contiene un valor SPF válido.
- Rojo: un conjunto de registros de recursos MX no tiene un registro de recursos TXT o SPF que contiene 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

- [Tipo de registro MX](#)
- [Tipo de registro SPF](#)

- [Guía de re:Post](#)
- [RFC 7208](#)

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

Description (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

Pfx0RwqB1i

Criterios de alerta

- Rojo: la ACL del bucket permite el acceso a la lista o el Upload/Delete acceso para todos o cualquier AWS usuario autenticado y la configuración de bloqueo del acceso público no está habilitada.
- Rojo: una política de compartimentos permite el acceso público y la configuración de Bloquear el acceso público no está habilitada.
- Rojo: Trusted Advisor no tiene permiso para comprobar la política o la política no se ha podido evaluar por otros motivos.
- Amarillo: una política de grupos permite el acceso público, pero la configuración Restringir grupos públicos está activada y restringe el acceso solo a los usuarios autorizados de esa cuenta.

- **Amarillo:** el compartimento es compatible, pero no tiene habilitada la protección de bloqueo total del acceso público.
- **Verde:** el depósito es compatible y tiene habilitada la protección de acceso público por bloqueo total.

 Note

Las concesiones de ACL públicas no se evalúan cuando está activado Bloquear el acceso público Ignorar las ACL públicas.

Acción recomendada

Si un bucket permite el acceso abierto, determine si este tipo de acceso es realmente necesario. Por ejemplo, para alojar un sitio web estático, puede utilizar Amazon CloudFront para ofrecer el contenido alojado en Amazon S3. Consulte [Restringir el acceso a un origen de Amazon S3](#) en la Guía para CloudFront desarrolladores de Amazon. Cuando sea posible, 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](#)

[Establecer la configuración del bloqueo del acceso público para sus buckets 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 lo permite Upload/Delete
- La política permite el acceso

Conexiones de emparejamiento de Amazon VPC con la resolución de DNS deshabilitada

Description (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.

Para los clientes del plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puede usar la [BatchUpdateRecommendationResourceExclusion](#) API para incluir o excluir uno o más recursos de sus Trusted Advisor resultados.

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

Protocolo de cifrado de grupos de destino del equilibrador de carga de aplicación

Description (Descripción)

Verifica que los grupos de destino del equilibrador de carga de aplicación (ALB) utilizan el protocolo HTTPS para cifrar la comunicación en tránsito para los tipos de instancia o IP de destino de backend. Las solicitudes HTTPS entre el ALB y los destinos de backend ayudan a mantener la confidencialidad de los datos en tránsito.

ID de la verificación

c2v1fg0p1w

Criterios de alerta

- Amarillo: grupo de destino del equilibrador de carga de aplicación que utiliza HTTP.
- Verde: grupo de destino del equilibrador de carga de aplicación que utiliza HTTPS.

Acción recomendada

Configure los tipos de instancia o IP de destino de backend para que admitan el acceso HTTPS y cambie el grupo de destino para usar el protocolo HTTPS para cifrar la comunicación entre los tipos de instancia o IP de ALB y de destino backend.

Recursos adicionales

[Imponga el cifrado en tránsito](#)

[Tipos de destino del equilibrador de carga de aplicación](#)

[Configuración de enrutamiento del equilibrador de carga de aplicación](#)

[Protección de datos en Elastic Load Balancing](#)

Columnas de informes

- Status
- Region
- Arn de ALB
- Nombre de ALB
- ID de VPC de ALB
- ARN del grupo de destino
- Nombre de grupo de destino
- Protocolo del grupo de destino
- Hora de la última actualización

AWS Backup Almacene sin una Resource-based política para evitar la eliminación de los puntos de recuperación

Description (Descripción)

Comprueba si AWS Backup los almacenes tienen una política asociada basada en los recursos 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.

Para los clientes del plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puede usar la [BatchUpdateRecommendationResourceExclusion](#) API para incluir o excluir uno o más recursos de sus Trusted Advisor resultados.

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 para evitar 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 los permisos de copia de seguridad: DeleteRecoveryPoint, copia de seguridad: UpdateRecoveryPointLifecycle y copia de seguridad: PutBackupVaultAccessPolicy

Para obtener más información, consulte [Configuración de políticas de acceso en almacenes de copias de seguridad](#).

Columnas de informes

- Status
- Region
- Recurso
- AWS Config Regla

- Parámetros de entrada
- Hora de la última actualización

AWS CloudTrail Registro de eventos de administración

Description (Descripción)

Comprueba el uso de AWS CloudTrail. CloudTrail proporciona una mayor visibilidad de la actividad en su Cuenta de AWS. Para ello, registra información sobre las llamadas a la AWS API que se realizan 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 de AWS (la opción predeterminada cuando se crea un nuevo registro de seguimiento), este aparecerá varias veces en el informe de Trusted Advisor.

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.

Para los clientes del plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puede usar la [BatchUpdateRecommendationResourceExclusion](#) API para incluir o excluir uno o más recursos de sus Trusted Advisor resultados.

ID de la verificación

c25hn9x03v

Criterios de alerta

- Rojo: no se crea ningún rastro para ningún rastro o el registro no está activado para ningún rastro. Región de AWS
- Amarillo: CloudTrail está activado, pero todos los senderos indican errores en la entrega de los registros.

- Verde: CloudTrail está activado y no se informa de ningún error en la entrega de registros.

Acción recomendada

Para crear un registro de seguimiento o iniciar el registro desde la consola, abra 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, entonces verifique 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](#)
- [Crear una ruta para una organización](#)

Columnas de informes

- Status
- Region
- Registro habilitado
- Error de entrega informado
- Hora de la última actualización

AWS Lambda Funciones que utilizan tiempos de ejecución obsoletos

Description (Descripción)

Verifica las funciones de Lambda cuya versión \$LATEST está configurada para utilizar un tiempo de ejecución que pronto estará o que ya está obsoleto. Los tiempos de ejecución obsoletos no pueden 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.

Para los clientes del plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puede usar la [BatchUpdateRecommendationResourceExclusionAPI](#) para incluir o excluir uno o más recursos de sus Trusted Advisor resultados.

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 utilizar un tiempo de ejecución que ya está obsoleto.
- Amarillo: la versión \$LATEST de la función se ejecuta en un tiempo de ejecución que está a punto de quedar obsoleto. Las funciones se incluyen al menos 180 días antes de la fecha de caducidad del tiempo de ejecución.

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
- Region
- ARN de función
- Tiempo de ejecución
- Días hasta la obsolescencia
- Fecha de obsolescencia
- Promedio de invocaciones diarias

- Hora de la última actualización

AWS Well-Architected problemas de seguridad de alto riesgo

Description (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.

Para los clientes del plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puede usar la [BatchUpdateRecommendationResourceExclusionAPI](#) para incluir o excluir uno o más recursos de sus Trusted Advisor resultados.

ID de la verificación

Wxdfp4B1L3

Criterios de alerta

- Rojo: se identificó al menos un problema activo de alto riesgo en el pilar de seguridad AWS Well-Architected.
- Verde: no se detectó ningún problema activo de alto riesgo en el pilar de seguridad durante 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 [AWS Well-Architected](#) herramienta para revisar sus respuestas y tomar medidas para resolver los problemas activos.

Columnas de informes

- Status

- Region
- 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

CloudFront Certificados SSL personalizados en la tienda de certificados de IAM

Description (Descripción)

Note

Esta comprobación se aplica a las CloudFront distribuciones clásicas de Amazon.

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. La mayoría de los navegadores web, como Chrome SHA-1 y Firefox, están dejando de lado los certificados cifrados mediante el algoritmo de hash.

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](#).

 Note

Esta verificación indica los recursos que están marcados según los criterios y el número total de recursos evaluados, incluidos los recursos de OK. La tabla de recursos muestra solo los recursos marcados.

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: se cifró un certificado SSL personalizado mediante el algoritmo SHA-1 de hash.
- 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

Recomendamos usarlo AWS Certificate Manager para aprovisionar, administrar e implementar los certificados de servidor. Con ACM, puede solicitar un certificado nuevo o implementar un ACM existente o un certificado externo en los AWS recursos. Los certificados que proporciona ACM son gratuitos y pueden renovarse automáticamente. Para obtener más información sobre ACM, consulte la [Guía del usuario de AWS Certificate Manager](#). Para comprobar si el Regiones de AWS ACM es compatible, consulte los [AWS Certificate Manager puntos finales](#) y las cuotas en. Referencia general de AWS

Renueve certificados caducados o que estén a punto de caducar. Para obtener más información sobre la renovación de un certificado, consulte [Administración de certificados de servidor](#) en IAM.

Sustituya un certificado que se haya cifrado mediante el algoritmo de SHA-1 hash por un certificado que se haya cifrado mediante el SHA-256 algoritmo de hash.

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](#)

[Importar certificados](#)

[AWS Certificate Manager Guía del usuario](#)

Columnas de informes

- Status
- ID de distribución
- Nombre de dominio de distribución
- Nombre del certificado
- Motivo

CloudFront Certificado SSL en el servidor de origen

Description (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 cifraban mediante el algoritmo SHA-1 de hash están quedando 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

Note

Esta verificación indica los recursos que están marcados según los criterios y el número total de recursos evaluados, incluidos los recursos de OK. La tabla de recursos muestra solo los recursos marcados.

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 SHA-1 de hash.
- 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.

Sustituya un certificado que se cifró mediante el algoritmo de SHA-1 hash por un certificado cifrado mediante el algoritmo de SHA-256 hash.

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

Description (Descripción)

Verifica si hay equilibradores de carga clásicos con oyentes que no utilicen configuraciones de seguridad recomendadas para la comunicación cifrada. AWS recomienda utilizar un protocolo

seguro (HTTPS o SSL), políticas de seguridad actualizadas, así como cifrados y protocolos seguros. Cuando se utiliza un protocolo seguro para una conexión frontend (del cliente al equilibrador de carga), las solicitudes se cifran entre los clientes y el equilibrador de carga, lo que crea un entorno más seguro. Esto crea un entorno más seguro. Elastic Load Balancing proporciona políticas de seguridad predefinidas con cifrados y protocolos que se adhieren a las prácticas recomendadas de seguridad de AWS. 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

- Rojo: un equilibrador de carga no tiene oyentes configurados con un protocolo seguro (HTTPS).
- Amarillo: un oyente HTTPS del equilibrador de cargas está configurado con una política de seguridad que contiene un cifrado débil.
- Amarillo: un oyente HTTPS del equilibrador de cargas no está configurado con la política de seguridad recomendada.
- Verde: un equilibrador de cargas tiene al menos un oyente de HTTPS y todos los oyentes de HTTPS están configurados con la política recomendada.

Acción recomendada

Si es necesario que el tráfico al equilibrador de carga sea seguro, utilice el protocolo HTTPS o SSL para la conexión frontend.

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
- Region
- Nombre del equilibrador de carga
- Puerto del equilibrador de carga
- Motivo

Grupos de seguridad del equilibrador de carga clásico

Description (Descripción)

Verifica si hay equilibradores 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 equilibrador de carga.

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.
- 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 oyente del 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](#)
- [Migre su Classic Load Balancer](#)
- [Configuración del equilibrador de carga clásico](#)

Columnas de informes

- Status
- Region
- Nombre del equilibrador de carga
- ID de grupos de seguridad
- Motivo

Exposed Access Keys

Description (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 tu cuenta de cargos excesivos, limita AWS temporalmente tu 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.

 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.

Para los clientes del plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puede usar la [BatchUpdateRecommendationResourceExclusion](#) API para incluir o excluir uno o más recursos de sus Trusted Advisor resultados.

Si se muestra 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

12Fnkp18Y5

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 [Consola de administración de AWS](#) 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

Description (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

Acceso externo de IAM Access Analyzer

Description (Descripción)

Verifica si existe el acceso externo de IAM Access Analyzer a nivel de cuenta.

Los analizadores de acceso externo de IAM Access Analyzer ayudan a identificar los recursos de su organización en sus cuentas que se comparten con una entidad externa. A continuación, el analizador crea un panel centralizado con los resultados. Una vez activado el nuevo analizador en la consola de IAM, los equipos de seguridad pueden priorizar las cuentas que van a revisar en

función de los permisos excesivos. Un analizador de acceso externo genera resultados sobre el acceso público y el acceso entre cuentas a los recursos, y se proporciona sin costo adicional.

ID de la verificación

07602fcad6

Criterios de alerta

- Rojo: el acceso externo del analizador no está activado a nivel de cuenta.
- Verde: el acceso externo del analizador está activado a nivel de cuenta.

Acción recomendada

La creación de un analizador de acceso externo por cuenta ayuda a los equipos de seguridad a priorizar qué cuentas revisar en función de los permisos excesivos. Para obtener más información, consulte [Introducción a los resultados de AWS Identity and Access Management Access Analyzer](#).

Además, es una buena práctica utilizar el analizador de acceso no utilizado, una característica de pago que simplifica la inspección del acceso no utilizado para orientarle hacia el nivel de privilegio mínimo. Para más información, consulte [Identifying unused access granted to IAM users and roles](#).

Recursos adicionales

- [Uso de AWS Identity and Access Management Access Analyzer](#)
- [Actualizaciones de IAM Access Analyzer: busque el acceso no utilizado y compruebe las políticas antes de la implementación](#)

Columnas de informes

- Status
- Region
- Arn del analizador de acceso externo de la cuenta
- Arn del analizador de acceso externo de la organización
- Hora de la última actualización

Política de contraseñas de IAM

Description (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

Yw2K9puPz1

Criterios de alerta

- Verde: hay una política de contraseñas habilitada con los requisitos de contenido recomendados habilitados.
- Amarillo: hay una política de contraseñas habilitada, pero al menos un requisito del contenido no está habilitado.

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](#).

Para acceder a Consola de administración de AWS, los usuarios de IAM necesitan contraseñas. Como práctica recomendada, AWS recomienda encarecidamente que, en lugar de crear usuarios de IAM, utilice la federación. La federación permite a los usuarios utilizar sus credenciales corporativas existentes para iniciar sesión en Consola de administración de AWS. Utilice IAM Identity Center para crear o federar el usuario y, a continuación, asuma un rol de IAM en una cuenta.

Para obtener más información sobre los proveedores de identidad y la federación, consulte [Proveedores de identidad y federación](#) en la Guía del usuario de IAM. Para obtener más información sobre IAM Identity Center, consulte la [Guía del usuario de IAM Identity Center](#).

Recursos adicionales

[Administración de contraseñas](#)

Columnas de informes

- Política de contraseñas
- Mayúsculas
- Minúsculas
- Número
- Non-alphanumeric

Proveedor de identidades IAM SAML 2.0

Description (Descripción)

Verifica si la Cuenta de AWS está configurada para el acceso a través de un proveedor de identidad (IdP) compatible con SAML 2.0. Asegúrese de seguir las prácticas recomendadas al centralizar las identidades y configurar los usuarios en un proveedor de [identidades externo](#) o [AWS IAM Identity Center](#).

ID de la verificación

c2v1fg0p86

Criterios de alerta

- Amarillo: esta cuenta no está configurada para obtener acceso a través de un proveedor de identidad (IdP) compatible con SAML 2.0.
- Verde: esta cuenta está configurada para acceder a través de un proveedor de identidad (IdP) compatible con SAML 2.0.

Acción recomendada

Active IAM Identity Center para Cuenta de AWS. Para obtener más información, consulte [Habilitación de IAM Identity Center](#). Tras activar el IAM Identity Center, se podrán realizar tareas habituales, como crear un conjunto de permisos y asignar el acceso a los grupos del centro de identidad. Para obtener más información, consulte [Tareas comunes](#).

Se recomienda administrar los usuarios humanos en el IAM Identity Center. Sin embargo, puede activar el acceso de usuario federado con IAM para usuarios humanos a corto plazo para implementaciones a pequeña escala. Para obtener más información, consulte [Federación SAML 2.0..](#)

Recursos adicionales

[¿Qué es IAM Identity Center?](#)

[¿Qué es IAM?](#)

Columnas de informes

- Status
- ID de Cuenta de AWS
- Hora de la última actualización

MFA en la cuenta raíz

Description (Descripción)

Verifica las credenciales del usuario raíz de una cuenta 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 Consola de administración de AWS sitios web asociados.

Note

En el caso AWS Organizations de su cuenta de administración, se AWS requiere una autenticación multifactor (MFA) para el usuario raíz al acceder a. Consola de administración de AWS

Para sus cuentas de AWS Organizations miembros, le recomendamos que administre de forma centralizada las credenciales raíz mediante. AWS Identity and Access Management Las credenciales de usuario raíz de la cuenta de miembro se pueden eliminar de forma centralizada, lo que quita la necesidad de administrar la MFA en las credenciales de los usuarios raíz. Para obtener más información, consulte [Prácticas recomendadas para cuentas de miembro](#) en la Guía del usuario de AWS Organizations .

ID de la verificación

7DAFEemoDos

Criterios de alerta

- Rojo: la MFA no está habilitada en la cuenta raíz.
- Verde: no existen credenciales de usuario raíz (contraseña raíz) o la MFA está activada para la cuenta.

Acción recomendada

Si se trata de una cuenta de miembro AWS Organizations: inicie sesión en su cuenta de administración, habilite la función de administración del acceso raíz en IAM y elimine las credenciales de usuario raíz de esta cuenta de miembro. Consulte [Centralización del acceso raíz para las cuentas de miembros](#).

Si se trata de una cuenta independiente o de administración, inicie sesión en su cuenta raíz y active un dispositivo de MFA. AWS Organizations Para obtener más información, consulte [Comprobar el estado y la AWS Multi-factor autenticación de la MFA](#) en IAM

Recursos adicionales

- [Administración de forma centralizada el acceso raíz a las cuentas de los miembros](#)
- [AWS Multi-factor autenticación en IAM](#)
- [Multi-factor autenticación para el usuario Cuenta de AWS root](#)

Clave de acceso de usuario raíz

Description (Descripción)

Comprueba si la clave de acceso del usuario raíz está presente. Se recomienda encarecidamente no crear pares de claves de acceso para el usuario raíz. Dado que [solo unas pocas tareas requieren el usuario raíz](#) y, por lo general, las realiza con poca frecuencia, le recomendamos iniciar sesión en la Consola de administración de AWS para realizar las tareas de usuario raíz. Antes de crear claves de acceso, revise las [alternativas a las claves de acceso a largo plazo](#).

ID de la verificación

c2v1fg0f4h

Criterios de alerta

- Rojo: la clave de acceso del usuario raíz está presente
- Verde: la clave de acceso del usuario raíz no está presente

Acción recomendada

Elimine las claves de acceso para el usuario raíz. Consulte [Eliminación de claves de acceso para el usuario raíz](#). Esta tarea debe realizarla el usuario raíz. No puede realizar estos pasos como usuario o rol de IAM.

Recursos adicionales

- [Tareas que requieren credenciales de usuario root](#)
- [Restablecer una contraseña de usuario root perdida u olvidada](#)

Columnas de informes

- Status
- ID de cuenta
- Hora de la última actualización

Grupos de seguridad: puertos específicos sin restricciones

Description (Descripción)

Comprueba 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 oportunidades de actividades maliciosas (piratería, ataques de denegación de servicio, 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 excluir. Para obtener más información, consulte las [Preguntas frecuentes sobre Trusted Advisor](#).

 Note

Esta verificación indica los recursos que están marcados según los criterios y el número total de recursos evaluados, incluidos los recursos de OK. La tabla de recursos muestra solo los recursos marcados.

ID de la verificación

HCP4007jGY

Criterios de alerta

- Verde: el grupo de seguridad proporciona acceso sin restricciones en los puertos 80, 25, 443 o 465.
- Rojo: Security Group proporciona acceso sin restricciones a los puertos 20, 21, 22, 1433, 1434, 3306, 3389, 4333, 5432 o 5500.
- Amarillo: el grupo de seguridad proporciona acceso sin restricciones a cualquier otro puerto.

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.

Revise y elimine los grupos de seguridad no utilizados. Se puede utilizar AWS Firewall Manager para configurar y gestionar de forma centralizada los grupos de seguridad a escala. Para obtener más información, consulte la [AWS Firewall Manager documentación](#). Cuentas de AWS

Considere utilizar Systems Manager Sessions Manager para el acceso SSH (puerto 22) y RDP (puerto 3389) a las instancias de EC2. Con el administrador de sesiones, puede acceder a las instancias de EC2 sin habilitar los puertos 22 y 3389 en el grupo de seguridad.

Recursos adicionales

- [Grupos de seguridad de Amazon EC2](#)
- [Lista de números de puertos TCP y UDP](#)

- [Enrutamiento sin clase Inter-Domain](#)
- [Trabajar con el administrador de sesiones](#)
- [AWS Firewall Manager](#)

Columnas de informes

- Status
- Region
- Nombre de grupo de seguridad
- ID de grupo de seguridad
- Protocolo
- Del puerto
- Al puerto
- Asociación

Grupos de seguridad: acceso sin restricciones

Description (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 oportunidades de actividades maliciosas (piratería, ataques de denegación de servicio, 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 creados por AWS Directory Service se marcan en rojo o amarillo, pero no representan un riesgo para la seguridad y se pueden excluir. Para obtener más información, consulte las [Preguntas frecuentes sobre Trusted Advisor](#).

 Note

Esta verificación indica los recursos que están marcados según los criterios y el número total de recursos evaluados, incluidos los recursos de OK. La tabla de recursos muestra solo los recursos marcados.

ID de la verificación

1iG5NDGVre

Criterios de alerta

- Verde: una regla del grupo de seguridad tiene una dirección IP de origen con un sufijo /0 para los puertos 25, 80 o 443.
- Amarillo: 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 y el grupo de seguridad está adjunto a un recurso.
- 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 y el grupo de seguridad no está adjunto a un recurso.

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.

Revise y elimine los grupos de seguridad no utilizados. Se puede utilizar AWS Firewall Manager para configurar y gestionar de forma centralizada los grupos de seguridad a escala. Para obtener más información, consulte la [AWS Firewall Manager documentación](#). Cuentas de AWS

Considere utilizar Systems Manager Sessions Manager para el acceso SSH (puerto 22) y RDP (puerto 3389) a las instancias de EC2. Con el administrador de sesiones, puede acceder a las instancias de EC2 sin habilitar los puertos 22 y 3389 en el grupo de seguridad.

Recursos adicionales

- [Grupos de seguridad de Amazon EC2](#)
- [Enrutamiento sin clase Inter-Domain](#)
- [Trabajar con el administrador de sesiones](#)

- [AWS Firewall Manager](#)

Columnas de informes

- Status
- Region
- Nombre de grupo de seguridad
- ID de grupo de seguridad
- Protocolo
- Del puerto
- Al puerto
- Rango de IP
- Asociación

Tolerancia a errores

Puede utilizar las siguientes verificaciones para la categoría de tolerancia a errores.

Nombres de la verificación

- [Multi-AZ de ALB](#)
- [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 Single-AZ de Amazon DocumentDB](#)
- [Recuperación de Amazon DynamoDB Point-in-time](#)
- [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 AZs varios o no cumple con el número mínimo de AZs](#)
- [Balance de zona de disponibilidad de Amazon EC2](#)
- [El monitoreo detallado de Amazon EC2 no está habilitado](#)
- [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 objetivo de montaje de Amazon EFS](#)
- [Amazon EFS no está en el AWS Backup plan](#)
- [Clústeres ElastiCache Multi-AZ de Amazon](#)
- [ElastiCache \(Redis OSS\) Clusters Automatic Backup](#)
- [Clústeres Multi-AZ Amazon MemoryDB](#)
- [Los agentes de Amazon MSK alojan demasiadas particiones](#)
- [Clústeres multi-AZ de Amazon MSK](#)
- [Dominios OpenSearch de Amazon Service con menos de tres nodos de datos](#)
- [Copias de seguridad de Amazon RDS](#)
- [Las copias de seguridad de Amazon RDS no están habilitadas](#)
- [Los clústeres de base de datos de Amazon RDS tienen una instancia de base de datos](#)
- [Clústeres de base de datos de Amazon RDS con todas las instancias en la misma zona de disponibilidad](#)
- [Clústeres de base de datos de Amazon RDS con todas las instancias de lector 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 del almacenamiento](#)
- [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 table](#)
- [La configuración del parámetro innodb_default_row_format de Amazon RDS no es segura](#)

- [El parámetro innodb_flush_log_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 de escritura](#)
- [El recurso de copias de seguridad automatizadas de Amazon RDS está desactivado](#)
- [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](#)
- [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](#)
- [Auto Scaling disponible IPs en subredes](#)
- [Comprobación de estado de grupos de Auto Scaling](#)
- [Recursos de grupos de Auto Scaling](#)
- [AWS CloudHSM clústeres que ejecutan instancias de HSM en una única zona de disponibilidad](#)
- [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](#)
- [AWS Lambda Funciones habilitadas para VPC sin redundancia Multi-AZ](#)
- [AWS Outposts Despliegue en un solo rack](#)

- [AWS Resilience Hub Verificación de componentes de la aplicación](#)
- [AWS Resilience Hub política incumplida](#)
- [AWS Resilience Hub puntajes de resiliencia](#)
- [AWS Resilience Hub edad de evaluación](#)
- [AWS Site-to-Site VPN tiene al menos un túnel en estado INACTIVO](#)
- [AWS STS uso global de puntos finales en Regiones de AWS](#)
- [Problemas de alto riesgo de AWS Well-Architected para la fiabilidad](#)
- [Classic Load Balancer no tiene configurados múltiples AZs](#)
- [Drenaje de conexiones de ELB](#)
- [Desequilibrio de objetivos del ELB](#)
- [GWLB: independencia de la zona de disponibilidad del punto de conexión](#)
- [Optimización del balanceador de carga](#)
- [Independencia de la zona de disponibilidad de la puerta de enlace de NAT](#)
- [Independencia de las zonas de disponibilidad del punto de conexión del firewall de red](#)
- [Firewall de red multi-AZ](#)
- [Equilibrador de carga cruzado del equilibrador de carga de red](#)
- [NLB: recurso con acceso a Internet en una subred privada](#)
- [Multi-AZ de NLB](#)
- [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 múltiples AZs](#)
- [Redundancia de túnel de VPN](#)
- [Redundancia de la zona de disponibilidad de ActiveMQ](#)
- [Redundancia de la zona de disponibilidad de RabbitMQ](#)

Multi-AZ de ALB

Description (Descripción)

Verifica si los equilibradores 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 su balanceador de carga AZs en varios lugares 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.

Para los clientes del plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puede usar la [BatchUpdateRecommendationResourceExclusionAPI](#) para incluir o excluir uno o más recursos de sus Trusted Advisor resultados.

ID de la verificación

c1dfprch08

Criterios de alerta

Amarillo: ALB está en una única zona de disponibilidad.

Verde: ALB tiene dos o más. AZs

Acción recomendada

Asegúrese de que el equilibrador 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
- Region
- Nombre de ALB

- Regla de ALB
- ARN de ALB
- Número de AZs
- Hora de la última actualización

La característica de búsqueda de datos anteriores del clúster de Amazon Aurora MySQL no está habilitada

Description (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 `BacktrackWindowInHours` parámetro de las AWS Config reglas.

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.

Para los clientes del plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puede usar la [BatchUpdateRecommendationResourceExclusionAPI](#) para incluir o excluir uno o más recursos de sus Trusted Advisor resultados.

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

Accesibilidad de instancias de base de datos de Amazon Aurora

Description (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

`xuy7H1avt1`

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
- Region
- Clúster
- Instancias de bases de datos públicas
- Instancias de bases de datos privadas
- Motivo

Conmutación por error CloudFront de Amazon Origin

Description (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.

Para los clientes del plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puede usar la [BatchUpdateRecommendationResourceExclusionAPI](#) para incluir o excluir uno o más recursos de sus Trusted Advisor resultados.

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

Riesgo de acceso a los puntos de enlace de Amazon Comprehend

Description (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.

Para los clientes del plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puede usar la [BatchUpdateRecommendationResourceExclusionAPI](#) para incluir o excluir uno o más recursos de sus Trusted Advisor resultados.

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 la política clave se modificó y desea seguir utilizando el punto final, le recomendamos que actualice la política AWS KMS clave. Para obtener más información, consulte [Changing a key policy](#).

Recursos adicionales

[AWS KMS Permisos](#)

Columnas de informes

- Status
- Region
- ARN de punto de conexión
- ARN de modelo
- KMS KeyId

- Hora de la última actualización

Clústeres Single-AZ de Amazon DocumentDB

Description (Descripción)

Verifica si hay clústeres de Amazon DocumentDB configurados como Single-AZ

La ejecución de cargas de trabajo de Amazon DocumentDB en una arquitectura de 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 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.

Para los clientes del plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puede usar la [BatchUpdateRecommendationResourceExclusionAPI](#) para incluir o excluir uno o más recursos de sus Trusted Advisor resultados.

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 la aplicación requiere 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
- Region
- 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 DynamoDB Point-in-time

Description (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 [Point-in-time recuperación 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.

Para los clientes del plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puede usar la [BatchUpdateRecommendationResourceExclusion](#) API para incluir o excluir uno o más recursos de sus Trusted Advisor resultados.

ID de la verificación

c18d2gz138

origen

AWS Config Managed Rule: dynamodb-pitr-enabled

Criterios de alerta

Amarillo: Point-in-time la recuperación 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 [Point-in-time Recuperación: Cómo funciona.](#)

Recursos adicionales

[Point-in-time recuperación para DynamoDB](#)

Columnas de informes

- Status
- Region
- 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

Description (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.

Para los clientes del plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puede usar la [BatchUpdateRecommendationResourceExclusionAPI](#) para incluir o excluir uno o más recursos de sus Trusted Advisor resultados.

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

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

Amazon EBS no está incluido en el plan AWS Backup

Description (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.

Para los clientes del plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puede usar la [BatchUpdateRecommendationResourceExclusionAPI](#) para incluir o excluir uno o más recursos de sus Trusted Advisor resultados.

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

Instantáneas de Amazon EBS

Description (Descripción)

Verifica la antigüedad de las instantáneas de los volúmenes de Amazon EBS (disponibles o en uso). Pueden producirse errores aunque los volúmenes de Amazon EBS estén replicados. Las instantáneas se conservan en Amazon S3 para un almacenamiento y point-in-time una recuperación duraderos.

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](#).

Para automatizar la creación de instantáneas de EBS, puede utilizar [AWS Backup](#) o [Amazon Data Lifecycle Manager](#).

Recursos adicionales

[Amazon Elastic Block Store \(Amazon EBS\)](#)

[Instantáneas de Amazon EBS](#)

[AWS Backup](#)

[Gestionador de vida útil de datos de Amazon](#)

Columnas de informes

- Status
- Region
- 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

Description (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 Amazon 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 [Agregar comprobaciones de estado del equilibrador de carga elástico](#).

 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.

Para los clientes del plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puede usar la [BatchUpdateRecommendationResourceExclusionAPI](#) para incluir o excluir uno o más recursos de sus Trusted Advisor resultados.

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
- Region
- 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

Description (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.

Para los clientes del plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puede usar la [BatchUpdateRecommendationResourceExclusion](#) API para incluir o excluir uno o más recursos de sus Trusted Advisor resultados.

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

Amazon EC2 Auto Scaling no se implementa en AZs varios o no cumple con el número mínimo de AZs

Description (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 `minAvailabilityZones` parámetro 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 Amazon EC2 Auto Scaling no tiene AZs varios configurados o no cumple con el número mínimo especificado AZs .

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

Balance de zona de disponibilidad de Amazon EC2

Description (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](#)
- [Grupos de ubicación para sus instancias de Amazon EC2](#)
- [Tipos de instancias de Amazon EC2](#)

Columnas de informes

- Status
- Region
- Instancias de zona a
- Instancias de zona b
- Instancias de zona c
- Instancias de zona e
- Instancias de zona f
- Motivo

El monitoreo detallado de Amazon EC2 no está habilitado

Description (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.

Para los clientes del plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puede usar la [BatchUpdateRecommendationResourceExclusionAPI](#) para incluir o excluir uno o más recursos de sus Trusted Advisor resultados.

ID de la verificación

AWS Config c18d2gz144

origen

AWS Config Regla gestionada: 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
- Region
- Recurso
- AWS Config Regla
- Parámetros de entrada
- Hora de la última actualización

Amazon ECS AWS registra el controlador en modo de bloqueo

Description (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.

Esta verificación no tiene en cuenta los ajustes de configuración del controlador a nivel de 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.

Para los clientes del plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puede usar la [BatchUpdateRecommendationResourceExclusionAPI](#) para incluir o excluir uno o más recursos de sus Trusted Advisor resultados.

ID de la verificación

c1dvkm4z6b

Criterios de alerta

Amarillo: el modo de parámetro de configuración de registro del controlador awslogs está configurado en modo de bloqueo.

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 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 [Evitar la pérdida de registros con el modo sin bloqueo en el controlador de AWS registros del contenedor de registros](#).

Recursos adicionales

[Uso del controlador de registro de AWS Logs](#)

[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 de registros](#)

Columnas de informes

- Status
- Region
- ARN de definición de tarea
- Nombres de definición de contenedor
- Hora de la última actualización

Servicio de Amazon ECS con una única zona de disponibilidad

Description (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 AZs los mismos. Región de AWS Al lanzar instancias en varias instancias AZs en la misma región, puede ayudar a proteger sus aplicaciones frente a un único punto de fallo.

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.

Para los clientes del plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puede usar la [BatchUpdateRecommendationResourceExclusionAPI](#) para incluir o excluir uno o más recursos de sus Trusted Advisor resultados.

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 sitios diferentes AZs.

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
- Region
- Nombre del Name/ECS servicio de clúster de ECS
- Número de zonas de disponibilidad
- Hora de la última actualización

Estrategia de ubicación multi-AZ de Amazon ECS

Description (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.

Para los clientes del plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puede usar la [BatchUpdateRecommendationResourceExclusionAPI](#) para incluir o excluir uno o más recursos de sus Trusted Advisor resultados.

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 varios AZs. 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
- Region
- Nombre del Name/ECS servicio de clúster de ECS

- La estrategia de distribución de tareas ha sido habilitada y aplicada correctamente
- Hora de la última actualización

Redundancia sin objetivo de montaje de Amazon EFS

Description (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.

Para los clientes del plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puede usar la [BatchUpdateRecommendationResourceExclusionAPI](#) para incluir o excluir uno o más recursos de sus Trusted Advisor resultados.

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
- Region
- ID del sistema de archivos de EFS
- Número de puntos de montaje
- Número de AZs
- Hora de la última actualización

Amazon EFS no está en el AWS Backup plan

Description (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: los sistemas de archivos Amazon EFS no están incluidos 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
- Region
- Recurso
- AWS Config Regla
- Parámetros de entrada
- Hora de la última actualización

Clústeres ElastiCache Multi-AZ de Amazon

Description (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 AZs mejoran la disponibilidad de los ElastiCache clústeres al replicar de forma asíncrona en réplicas de solo lectura en una zona de disponibilidad diferente. Cuando se lleva a cabo el mantenimiento planificado del clúster o si un nodo principal no está disponible, ElastiCache 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.

Para los clientes del plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puede usar la [BatchUpdateRecommendationResourceExclusionAPI](#) para incluir o excluir uno o más recursos de sus Trusted Advisor resultados.

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 \(Redis OSS\) con Multi-AZ](#).

Columnas de informes

- Status
- Region
- Nombre del clúster
- Hora de la última actualización

ElastiCache (Redis OSS) Clusters Automatic Backup

Description (Descripción)

Comprueba si los clústeres de Amazon ElastiCache (Redis OSS) 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 `snapshotRetentionPeriod` parámetros de sus AWS Config reglas.

Para obtener más información, consulte [Backup and restore for ElastiCache \(Redis OSS\)](#).

 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.

Para los clientes del plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puede usar la [BatchUpdateRecommendationResourceExclusion](#) API para incluir o excluir uno o más recursos de sus Trusted Advisor resultados.

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 (Redis OSS) 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 (Redis OSS) 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 for ElastiCache \(Redis OSS\)](#).

Recursos adicionales

Para obtener más información, consulte [Programar copias de seguridad automáticas](#).

Columnas de informes

- Status
- Region
- Nombre del clúster
- Hora de la última actualización

Clústeres Multi-AZ Amazon MemoryDB

Description (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 varios nodos AZs mejoran la disponibilidad de los clústeres de MemoryDB mediante la replicación asíncrona en réplicas de solo lectura en una zona de disponibilidad 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.

Para los clientes del plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puede usar la [BatchUpdateRecommendationResourceExclusionAPI](#) para incluir o excluir uno o más recursos de sus Trusted Advisor resultados.

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
- Region
- Nombre del clúster
- Hora de la última actualización

Los agentes de Amazon MSK alojan demasiadas particiones

Description (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
- Region
- ARN del clúster
- ID del agente
- Recuento de particiones

Clústeres multi-AZ de Amazon MSK

Description (Descripción)

Comprueba el número de zonas de disponibilidad (AZs) del clúster aprovisionado de Amazon MSK. El clúster Amazon MSK está formado por varios agentes que trabajan juntos y distribuyen los datos y la carga. La producción podría interrumpirse durante el mantenimiento o por problemas de intermediación en un clúster 2-AZ.

ID de la verificación

90046ff5b5

Criterios de alerta

- Amarillo: el clúster de Amazon MSK se aprovisiona con agentes en solo dos AZs
- Verde: el clúster de Amazon MSK se aprovisiona con agentes de tres o más AZs

Acción recomendada

Para aumentar la disponibilidad del clúster, puede crear otro clúster en una configuración de 3 AZs . A continuación, se migra el clúster existente al nuevo clúster que se creó. Puede utilizar la replicación de Amazon MSK para esta migración.

Recursos adicionales

[Alta disponibilidad de Amazon MSK](#)

[Migración a Amazon MSK](#)

Columnas de informes

- Status
- Region
- Clúster de MSK (ARN)

- Número de AZs
- Hora de la última actualización

Dominios OpenSearch de Amazon Service con menos de tres nodos de datos

Description (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.

Para los clientes del plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puede usar la [BatchUpdateRecommendationResourceExclusionAPI](#) para incluir o excluir uno o más recursos de sus Trusted Advisor resultados.

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

Copias de seguridad de Amazon RDS

Description (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.

Note

Esta verificación indica los recursos que están marcados según los criterios y el número total de recursos evaluados, incluidos los recursos de OK. La tabla de recursos muestra solo los recursos marcados.

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
- Backup Retention Period

Las copias de seguridad de Amazon RDS no están habilitadas

Description (Descripción)

Verifica si una instancia de Amazon RDS está habilitada con copias de seguridad automatizadas mediante Amazon RDS o con copias de seguridad continuas de AWS Backup. Las copias de seguridad continuas reducen el riesgo de pérdida inesperada de datos y permiten la point-in-time recuperación.

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.

Para los clientes del plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puede usar la [BatchUpdateRecommendationResourceExclusionAPI](#) para incluir o excluir uno o más recursos de sus Trusted Advisor resultados.

ID de la verificación

44fde09ab5

Criterios de alerta

- Rojo: la instancia no tiene habilitada la copia de seguridad automática en Amazon RDS ni la copia de seguridad continua en AWS Backup.
- Rojo: las versiones de MySQL anteriores a 5.6 no admiten copias de seguridad automatizadas ni continuas. Para ofrecer resiliencia, primero actualice la versión de la base de datos y, a continuación, habilite la copia de seguridad automática o continua.
- Verde: la instancia tiene habilitada la copia de seguridad automática en Amazon RDS.
- Verde: la instancia tiene habilitada la copia de seguridad continua. AWS Backup

Acción recomendada

Asegúrese de que las instancias de Amazon RDS tengan configurada la copia de seguridad automática, ya sea mediante la configuración de un período de retención superior a 0 en Amazon RDS o la creación de un plan de copia de seguridad continua con AWS Backup.

Recursos adicionales

- [Introducción a Amazon RDS](#)
- [Administrar copias de seguridad automatizadas](#)
- [Introducción a las copias de seguridad](#)
- [Respaldos y point-in-time restauración continuos \(PITR\)](#)
- [AWS Backup disponibilidad de funciones](#)

Columnas de informes

- Status
- Region
- DB Instance Identifier
- ARN de una instancia de base de datos
- Tipo de implementación

- Tipo de copia de seguridad
- Motivo
- Hora de la última actualización

Los clústeres de base de datos de Amazon RDS tienen una instancia de base de datos

Description (Descripción)

Agregue al menos otra instancia de base de datos más 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.

Para los clientes del plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puede usar la [BatchUpdateRecommendationResourceExclusionAPI](#) para incluir o excluir uno o más recursos de sus Trusted Advisor resultados.

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

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
- Region
- Recurso
- Nombre del motor
- Clase de instancia de base de datos
- Hora de la última actualización

Clústeres de base de datos de Amazon RDS con todas las instancias en la misma zona de disponibilidad

Description (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.

Para los clientes del plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puede usar la [BatchUpdateRecommendationResourceExclusionAPI](#) para incluir o excluir uno o más recursos de sus Trusted Advisor resultados.

 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

c1qf5bt007

Criterios de alerta

Amarillo: los clústeres de base 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 que agregue las instancias de base de datos a varias zonas de disponibilidad en un clúster de base de datos. Agregar las instancias de base de datos a varias zonas de disponibilidad mejora la disponibilidad de su clúster de base de datos.

Para obtener más información, consulte [Alta disponibilidad para Amazon Aurora](#).

Columnas de informes

- Status
- Region

- Recurso
- Nombre del motor
- Hora de la última actualización

Clústeres de base de datos de Amazon RDS con todas las instancias de lector en la misma zona de disponibilidad

Description (Descripción)

El clúster de base de datos dispone de todas las instancias de lector en la misma zona de disponibilidad. Se recomienda distribuir las instancias de lector entre varias zonas de disponibilidad en su clúster de base de datos.

Esta 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.

Para los clientes del plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puede usar la [BatchUpdateRecommendationResourceExclusion](#) API para incluir o excluir uno o más recursos de sus Trusted Advisor resultados.

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

c1qf5bt018

Criterios de alerta

Rojo: los clústeres de base de datos disponen de las instancias de lector en la misma zona de disponibilidad.

Acción recomendada

Distribuya las instancias de lector entre varias zonas de disponibilidad.

Recursos adicionales

Las zonas de disponibilidad (AZs) son ubicaciones distintas entre sí para proporcionar aislamiento en caso de interrupciones en cada AWS región. Le recomendamos que distribuya la instancia principal y las instancias de lectura de su clúster de base de datos entre varias AZs para mejorar la disponibilidad de su clúster de base de datos. Puede crear un clúster Multi-AZ mediante la API Consola de administración de AWS 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
- Region
- 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

Description (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.

Para los clientes del plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puede usar la [BatchUpdateRecommendationResourceExclusion](#) API para incluir o excluir uno o más recursos de sus Trusted Advisor resultados.

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
- Region
- 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 del almacenamiento

Description (Descripción)

El escalado automático de Amazon RDS no está activado en su instancia de base de datos. El escalado automático del almacenamiento de RDS escala automáticamente la capacidad de almacenamiento cuando hay un aumento del tamaño de la carga de trabajo de la base de datos, 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.

Para los clientes del plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puede usar la [BatchUpdateRecommendationResourceExclusion](#) API para incluir o excluir uno o más recursos de sus Trusted Advisor resultados.

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

c1qf5bt013

Criterios de alerta

Rojos: las instancias de base de datos no tienen habilitado el escalado automático.

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 cuando aumenta el tamaño de la carga de trabajo de la base de datos, sin tiempo de inactividad. El escalado automático del almacenamiento monitorea el uso del almacenamiento y escala automáticamente la capacidad cuando el uso se acerca a la capacidad de almacenamiento aprovisionada. También se puede establecer un límite máximo en el almacenamiento que Amazon RDS puede asignar en la instancia de base de datos. No existe un costo adicional por el escalado automático de almacenamiento. Solo tiene que pagar por los recursos de Amazon RDS que se asignan a la instancia de base de datos. Le recomendamos que active el escalado automático 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
- Region
- Recurso

- Valores recomendados
- Nombre del motor
- Hora de la última actualización

Instancias de base de datos de Amazon RDS que no utilizan la implementación multi-AZ

Description (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.

Para los clientes del plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puede usar la [BatchUpdateRecommendationResourceExclusion](#) API para incluir o excluir uno o más recursos de sus Trusted Advisor resultados.

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

c1qf5bt019

Crterios de alerta

Amarillo: instancias de base de datos que no utilizan la implementación multi-AZ

Acción recomendada

Configure multi-AZ para las instancias de base de datos afectadas.

Recursos adicionales

En una implementación de Amazon RDS Multi-AZ, Amazon RDS crea automáticamente una instancia de base de datos principal y replica sincrónicamente los datos en una instancia en espera en una zona de disponibilidad diferente. Cuando detecta un error, Amazon RDS conmuta por error automáticamente a una instancia en espera sin intervención manual.

Para obtener más información, consulte [Precios](#).

Columnas de informes

- Status
- Region
- Recurso
- Nombre del motor
- Hora de la última actualización

Amazon RDS DiskQueueDepth

Description (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

Crterios 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 read/write estas características.

Columnas de informes

- Status
- Region
- ARN de una instancia de base de datos
- DiskQueueDepth Métrica

Amazon RDS FreeStorageSpace

Description (Descripción)

Comprueba si la FreeStorageSpace CloudWatch métrica de una instancia de base de datos de RDS ha disminuido por debajo de un umbral razonable desde el punto de vista operativo.

ID de la verificación

Cmsvnj8db2

Criterios de alerta

- Rojo: FreeStorageSpace tiene menos del 10% de la capacidad total
- Amarillo: FreeStorageSpace se encuentra entre el 10% y el 20% de la capacidad total
- Verde: FreeStorageSpace representa más del 20% de la capacidad total

Acción recomendada

Escale el espacio de almacenamiento de la instancia de base de datos de RDS que se está quedando sin almacenamiento gratis mediante la consola de administración de Amazon RDS, la API de Amazon RDS o la Interfaz de la línea de comandos de AWS.

Columnas de informes

- Status
- Region
- ARN de una instancia de base de datos

- FreeStorageSpace Métrico (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 table

Description (Descripción)

Cuando log_output se establece en TABLE, se utiliza más espacio de almacenamiento que cuando log_output se establece en FILE. Se recomienda que establezca el parámetro en FILE para evitar que se alcance 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.

Para los clientes del plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puede usar la [BatchUpdateRecommendationResourceExclusionAPI](#) para incluir o excluir uno o más recursos de sus Trusted Advisor resultados.

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

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 el grupo de parámetros de su base de datos.

Recursos adicionales

Para obtener más información, consulte [Archivos de registro de la base de datos de MySQL](#).

Columnas de informes

- Status
- Region
- Recurso
- Nombre del parámetro
- Valores recomendados
- Hora de la última actualización

La configuración del parámetro `innodb_default_row_format` de Amazon RDS no es segura

Description (Descripción)

Su 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 valor `row_format` establecido en `COMPACT` o `REDUNDANT` será inaccesible e irrecuperable si 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.

Para los clientes del plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puede usar la [BatchUpdateRecommendationResourceExclusionAPI](#) para incluir o excluir uno o más recursos de sus Trusted Advisor resultados.

 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

c1qf5bt036

Criterios de alerta

Rojo: los grupos de parámetros de base de datos tienen una configuración no segura 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 podrá obtener acceso ni recuperar estas tablas.

Para obtener más información, consulte [Cambios enMySQL 8.0.26 \(2021-07-20, disponibilidad general\)n](#), en el sitio web de documentación de MySQL.

Columnas de informes

- Status

- Region
- Recurso
- Nombre del parámetro
- Valores recomendados
- Hora de la última actualización

El parámetro `innodb_flush_log_log_at_trx_commit` de Amazon RDS no es 1

Description (Descripción)

El valor del parámetro `innodb_flush_log_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 que establezca el parámetro `innodb_flush_log_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.

Para los clientes del plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puede usar la [BatchUpdateRecommendationResourceExclusion](#) API para incluir o excluir uno o más recursos de sus Trusted Advisor resultados.

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

c1qf5bt030

Criterios de alerta

Amarillo: los grupos de parámetros de base de datos tienen `innodb_flush_log_log_at_trx_commit` establecido en un valor distinto de 1.

Acción recomendada

Establezca el valor del parámetro `innodb_flush_log_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. En función del valor establecido en 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 cada transacción confirmada y se guardan en el disco una vez por segundo. Los datos se mueven desde el 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

- Region
- Recurso
- Nombre del parámetro
- Valores recomendados
- Hora de la última actualización

El parámetro `max_user_connections` de Amazon RDS es bajo

Description (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 aumentar el parámetro `max_user_connections` a 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.

Para los clientes del plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puede usar la [BatchUpdateRecommendationResourceExclusionAPI](#) para incluir o excluir uno o más recursos de sus Trusted Advisor resultados.

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

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 en los 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
- Region
- Recurso
- Nombre del parámetro
- Valores recomendados
- Hora de la última actualización

Amazon RDS Multi-AZ

Description (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.

 Note

Esta verificación indica los recursos que están marcados según los criterios y el número total de recursos evaluados, incluidos los recursos de OK. La tabla de recursos muestra solo los recursos marcados.

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

Description (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 la 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.

Para los clientes del plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puede usar la [BatchUpdateRecommendationResourceExclusionAPI](#) para incluir o excluir uno o más recursos de sus Trusted Advisor resultados.

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

Las réplicas de lectura de Amazon RDS están abiertas en modo de escritura

Description (Descripción)

Su instancia de base de datos tiene la réplica de lectura en modo de escritura, lo que permite actualizaciones de los clientes.

Se recomienda configurar el parámetro `read_only` para que las réplicas leídas no estén en `TrueIfReplicaModeWritable`.

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.

Para los clientes del plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puede usar la [BatchUpdateRecommendationResourceExclusionAPI](#) para incluir o excluir uno o más recursos de sus Trusted Advisor resultados.

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

c1qf5bt035

Criterios de alerta

Amarillo: los grupos de parámetros de base de datos activan el modo de escritura permitida para las réplicas de lectura.

Acción recomendada

Establezca el valor del parámetro `read_only` en `TruelfReplica`

Recursos adicionales

El parámetro `read_only` controla el permiso de escritura de los clientes en una instancia de base de datos. El valor predeterminado para este parámetro es `TruelfReplica`. Para una instancia de réplica, `TruelfReplica` establece el valor `read_only` en `ON` (1) y desactiva cualquier actividad de escritura de los clientes. master/writer Por ejemplo, `TruelfReplica` 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 de escritura permitida, 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 [“Best practices for configuring parameters for Amazon RDS for MySQL, part 2: Parameters related to replication”](#) en el sitio web de documentación de MySQL.

Columnas de informes

- Status
- Region
- Recurso
- Nombre del parámetro
- Valores recomendados
- Hora de la última actualización

El recurso de copias de seguridad automatizadas de Amazon RDS está desactivado

Description (Descripción)

Las copias de seguridad automatizadas están deshabilitadas en los recursos de la base de datos. Las copias de seguridad automatizadas permiten la point-in-time recuperación 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.

Para los clientes del plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puede usar la [BatchUpdateRecommendationResourceExclusion](#) API para incluir o excluir uno o más recursos de sus Trusted Advisor resultados.

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

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. Se recomienda activar las copias de seguridad automatizadas. Al activar las copias de seguridad automatizadas para una instancia de base de datos, Amazon RDS realiza de manera automática 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. Obtiene almacenamiento de copia de seguridad hasta el tamaño de almacenamiento de su instancia de base de datos sin costo adicional.

Para obtener más información, consulte los siguientes recursos:

- [Permitir copias de seguridad automatizadas](#)
- [Desmistificar los costos de almacenamiento de las copias de seguridad de Amazon RDS](#)

Columnas de informes

- Status
- Region
- Recurso
- Valores recomendados
- Nombre del motor
- Hora de la última actualización

El parámetro sync_binlog de Amazon RDS está desactivado

Description (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 que establezca 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.

Para los clientes del plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puede usar la [BatchUpdateRecommendationResourceExclusionAPI](#) para incluir o excluir uno o más recursos de sus Trusted Advisor resultados.

 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

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 la forma en que 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 [“Best practices for configuring parameters for Amazon RDS for MySQL, part 2: Parameters related to replication”](#).

Columnas de informes

- Status
- Region
- Recurso
- Nombre del parámetro
- Valores recomendados
- Hora de la última actualización

El clúster de base de datos de RDS no tiene habilitada la replicación Multi-AZ

Description (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.

Para los clientes del plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puede usar la [BatchUpdateRecommendationResourceExclusion](#) API para incluir o excluir uno o más recursos de sus Trusted Advisor resultados.

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

Instancia de reserva Multi-AZ de RDS no habilitada

Description (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.

Para los clientes del plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puede usar la [BatchUpdateRecommendationResourceExclusion](#) API para incluir o excluir uno o más recursos de sus Trusted Advisor resultados.

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

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

Amazon RDS ReplicaLag

Description (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 durante 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 que recientemente se han replicado instancias de copias de seguridad antiguas y a que estas replaced/launched réplicas requieran un tiempo considerable para «ponerse al día» con la instancia de base de datos principal y con las transacciones en tiempo real. 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... lo que provoca ReplicaLag retrasos ocasionales day/month/etc. Su equipo debería investigar qué posible causa raíz ha contribuido a que la base de datos esté ReplicaLag 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.

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
- Region
- ARN de una instancia de base de datos
- ReplicaLag Métrica

El parámetro synchronous_commit de Amazon RDS está desactivado

Description (Descripción)

Cuando el parámetro synchronous_commit está desactivado, es posible que se pierdan datos si la base de datos se bloquea. La durabilidad de la base de datos está en riesgo.

Le recomendamos que active 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.

Para los clientes del plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puede usar la [BatchUpdateRecommendationResourceExclusion](#) API para incluir o excluir uno o más recursos de sus Trusted Advisor resultados.

 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

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 la 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 una 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 la base de datos de MySQL](#).

Columnas de informes

- Status
- Region
- Recurso
- Nombre del parámetro

- Valores recomendados
- Hora de la última actualización

Instantánea automática de clúster de Amazon Redshift

Description (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 RA3 nodos.

Puede especificar el período de retención mínimo y máximo que desee mediante el `MaxRetentionPeriod` parámetro `MinRetentionPeriod` 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.

Para los clientes del plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puede usar la [BatchUpdateRecommendationResourceExclusionAPI](#) para incluir o excluir uno o más recursos de sus Trusted Advisor resultados.

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

Comprobaciones de estado eliminadas de Amazon Route 53

Description (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.

 Note

Esta verificación indica los recursos que están marcados según los criterios y el número total de recursos evaluados, incluidos los recursos de OK. La tabla de recursos muestra solo los recursos marcados.

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

Description (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.

 Note

Esta verificación indica los recursos que están marcados según los criterios y el número total de recursos evaluados, incluidos los recursos de OK. La tabla de recursos muestra solo los recursos marcados.

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

Description (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 largo, los solucionadores de DNS tardan más tiempo en solicitar registros de DNS actualizados, lo que puede causar retrasos innecesarios en el redireccionamiento del tráfico (p. ej., cuando la conmutación por error de DNS detecta y responde a una falla de uno de sus puntos de conexión). Esta verificación solo examina los registros con una política de conmutación por error o si hay una comprobación de estado asociada.

Las zonas alojadas creadas por AWS los servicios no aparecerán en los resultados de la comprobación.

Note

Esta verificación indica los recursos que están marcados según los criterios y el número total de recursos evaluados, incluidos los recursos de OK. La tabla de recursos muestra solo los recursos marcados.

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.
- **Verde:** un registro de recursos no tiene una política de conmutación por error o tiene una política de conmutación por error con un TTL inferior a 60.

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

Description (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 ## normalmente representan 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.

 Note

Esta verificación indica los recursos que están marcados según los criterios y el número total de recursos evaluados, incluidos los recursos de OK. La tabla de recursos muestra solo los recursos marcados.

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

Description (Descripción)

Comprueba si la configuración del servicio tiene direcciones IP especificadas en al menos dos zonas de disponibilidad (AZs) para garantizar la redundancia. Una zona de disponibilidad es

una ubicación diferente que queda aislada en caso de error en otras zonas. Al especificar varias direcciones IP AZs en la misma región, puede ayudar a proteger sus aplicaciones frente a 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 AZs

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
- Region
- ARN de recurso
- Número de AZs

La replicación de bucket de Amazon S3 no está habilitada

Description (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.

Para los clientes del plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puede usar la [BatchUpdateRecommendationResourceExclusionAPI](#) para incluir o excluir uno o más recursos de sus Trusted Advisor resultados.

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

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

Amazon S3 Bucket Versioning

Description (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 habilitado el control de versiones para el bucket.
- Amarillo: no se ha habilitado el control de versiones para el bucket.
- Amarillo: el control de versiones está suspendido para el bucket.
- Amarillo: Trusted Advisor no tiene acceso para validar el control de versiones.

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
- Region
- 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

Description (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 `minAvailabilityZones` parámetros 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.

Para los clientes del plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puede usar la [BatchUpdateRecommendationResourceExclusion](#) API para incluir o excluir uno o más recursos de sus Trusted Advisor resultados.

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

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

Auto Scaling disponible IPs en subredes

Description (Descripción)

Comprueba que haya suficiente disponibilidad IPs en las subredes de destino. Tener suficiente IPs disponibilidad para su uso ayudaría cuando Auto Scaling Group 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
- Region
- ARN de recurso
- Número máximo de instancias que se pueden crear
- Número de instancias disponibles

Comprobación de estado de grupos de Auto Scaling

Description (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

CLOG40CD08

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
- Region
- Nombre del grupo de escalado automático
- Equilibrador de carga asociado
- Comprobación de estado

Recursos de grupos de Auto Scaling

Description (Descripción)

Verifica la disponibilidad de los recursos asociados con las configuraciones de lanzamiento, las plantillas de lanzamiento y los grupos de escalado automático.

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 configuraciones/launch las plantillas de lanzamiento que apuntan a recursos no disponibles no funcionan según lo previsto.

Note

Esta verificación indica los recursos que están marcados según los criterios y el número total de recursos evaluados, incluidos los recursos de OK. La tabla de recursos muestra solo los recursos marcados.

ID de la verificación

8CNsS11I5v

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.
- Rojo: una plantilla 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 asícielo 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 configuración de lanzamiento o una versión de plantilla de lanzamiento mediante una AMI válida y asóciela a un grupo de escalado automático. Para obtener información sobre cómo crear una nueva configuración de lanzamiento, consulte [Crear una configuración de lanzamiento](#) en la Guía usuario de Amazon EC2 Auto Scaling. Para obtener información acerca de cómo crear una plantilla de lanzamiento, consulte [Crear un grupo de escalado automático](#) en la Guía del usuario de Amazon EC2 Auto Scaling.

 Note

Por motivos de seguridad, los resultados de la comprobación no incluyen ningún recurso al que se haga referencia mediante AWS Systems Manager los parámetros de la plantilla de lanzamiento.

Si sus plantillas de lanzamiento incluyen un AWS Systems Manager parámetro que incluye un ID de Amazon Machine Image (AMI), revise la plantilla de lanzamiento para asegurarse de que los parámetros hacen referencia a un ID de AMI válido o realice los cambios adecuados en el almacén de AWS Systems Manager parámetros. Para obtener más información, consulte [Usar AWS Systems Manager parámetros en lugar de AMI IDs](#) en la Guía del usuario de Amazon EC2 Auto Scaling.

Recursos adicionales

- [Solución de problemas de Auto Scaling: Amazon EC2 AMIs](#)
- [Solución de problemas de Auto Scaling: configuración del equilibrador de carga](#)
- [Guía del usuario de Amazon EC2 Auto Scaling](#)
- [Utilice AWS Systems Manager parámetros en lugar de AMI IDs](#)

Columnas de informes

- Status
- Region
- Nombre del grupo de escalado automático
- Tipo de lanzamiento
- Tipo de recurso
- Nombre del recurso

AWS CloudHSM clústeres que ejecutan instancias de HSM en una única zona de disponibilidad

Description (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.

Para los clientes del plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puede usar la [BatchUpdateRecommendationResourceExclusionAPI](#) para incluir o excluir uno o más recursos de sus Trusted Advisor resultados.

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

[Prácticas recomendadas para AWS CloudHSM](#)

Columnas de informes

- Status
- Region

- ID del clúster
- Número de instancias de HSM
- Hora de la última actualización

Direct Connect Resiliencia de ubicación

Description (Descripción)

Comprueba la resistencia del Direct Connect utilizado para conectar su entorno local a cada puerta de enlace de Direct Connect o puerta de enlace privada virtual.

Esta verificación 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 la 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 que se conecte al menos a dos ubicaciones distintas de Direct Connect. Para obtener más información, consulte [Recomendaciones de resiliencia de Direct Connect](#).

Recursos adicionales

[Direct Connect Recomendaciones de resiliencia](#)

[Direct Connect Prueba de conmutación por error](#)

Columnas de informes

- Status
- Region
- 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

Description (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.

Para los clientes del plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puede usar la [BatchUpdateRecommendationResourceExclusion](#) API para incluir o excluir uno o más recursos de sus Trusted Advisor resultados.

ID de la verificación

c18d2gz182

origen

AWS Config Managed Rule: `lambda-dlq-check`

Criterios de alerta

Amarillo: AWS Lambda la función no tiene configurada una 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

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

AWS Lambda Sobre los destinos de los eventos de falla

Description (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.

Para los clientes del plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puede usar la [BatchUpdateRecommendationResourceExclusionAPI](#) para incluir o excluir uno o más recursos de sus Trusted Advisor resultados.

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
- Region
- La característica con la versión que está marcada.
- Porcentaje de solicitudes asíncronas caídas en el día actual
- Solicitudes asíncronas del día actual
- Porcentaje promedio diario de solicitudes asíncronas caídas
- Promedio de solicitudes asíncronas diarias
- Hora de la última actualización

AWS Lambda Funciones habilitadas para VPC sin redundancia Multi-AZ

Description (Descripción)

Verifica la versión \$LATEST de las funciones de Lambda habilitadas para VPC que son vulnerables a la interrupción del servicio en una única zona de disponibilidad. Es una práctica recomendada conectar las funciones habilitadas para VPC con múltiples zonas de disponibilidad para obtener 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.

Para los clientes del plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puede usar la [BatchUpdateRecommendationResourceExclusionAPI](#) para incluir o excluir uno o más recursos de sus Trusted Advisor resultados.

ID de la verificación

L4dfs2Q4C6

Criterios de alerta

Amarillo: la versión \$LATEST de una función de Lambda habilitada para VPC se conecta a subredes en 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
- Region
- ARN de función
- ID de VPC
- Promedio de invocaciones diarias
- Hora de la última actualización

AWS Outposts Despliegue en un solo rack

Description (Descripción)

Verifica el saldo de bastidores de Outpost. Esto evalúa si las instancias de Outpost de un cliente están implementadas en varios bastidores de Outpost o en un solo bastidor de Outpost. Un único rack de Outposts crea un único punto de fallo para los problemas relacionados con un único bastidor (por ejemplo, fallos medioambientales). Estos escenarios se pueden mitigar con la implementación de Outposts en varios bastidores.

ID de la verificación

c243hjzrhn

Criterios de alerta

- Amarillo: su Outpost está implementado en un solo bastidor
- Verde: su Outpost está implementado en varios bastidores.

Acción recomendada

Si ejecuta cargas de trabajo de producción AWS Outposts, se recomienda utilizar la siguiente arquitectura resiliente. Un único AWS Outposts rack crea un único punto de fallo. Considere la posibilidad de añadir un segundo AWS Outposts rack a esa ubicación con capacidad suficiente para un evento de conmutación por error y, a continuación, distribuir las cargas de trabajo entre los racks.

Recursos adicionales

[Modo de fallo 4: racks o centros de datos](#)

Columnas de informes

- Status
- ARN de recurso
- AZ
- Número de bastidores
- Hora de la última actualización

AWS Resilience Hub Verificación de componentes de la aplicación

Description (Descripción)

Comprueba si un componente de la aplicación (AppComponent) de la aplicación es irrecuperable. Si un 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

RH23stm04

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
- Region
- Nombre de la aplicación
- AppComponent Nombre
- Hora de la última actualización

AWS Resilience Hub política incumplida

Description (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

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.

Para los clientes del plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puede usar la [BatchUpdateRecommendationResourceExclusion](#) API para incluir o excluir uno o más recursos de sus Trusted Advisor resultados.

ID de la verificación

RH23stm02

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
- Region
- Nombre de la aplicación
- Hora de la última actualización

AWS Resilience Hub puntajes de resiliencia

Description (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 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.

Para los clientes del plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puede usar la [BatchUpdateRecommendationResourceExclusion](#) API para incluir o excluir uno o más recursos de sus Trusted Advisor resultados.

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
- Region
- Nombre de la aplicación
- Puntuación de resiliencia de la aplicación

- Hora de la última actualización

AWS Resilience Hub edad de evaluación

Description (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.

Para los clientes del plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puede usar la [BatchUpdateRecommendationResourceExclusionAPI](#) para incluir o excluir uno o más recursos de sus Trusted Advisor resultados.

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
- Region
- 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

Description (Descripción)

Comprueba el número de túneles que están activos para cada uno de tus AWS Site-to-Site VPNs.

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, consulta [¿Qué es AWS Site-to-Site una 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.

Para los clientes del plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puede usar la [BatchUpdateRecommendationResourceExclusion](#) API para incluir o excluir uno o más recursos de sus Trusted Advisor resultados.

ID de la verificación

c18d2gz123

origen

AWS Config Managed Rule: vpc-vpn-2-tunnels-up

Criterios de alerta

Amarillo: una Site-to-Site VPN tiene al menos un túnel 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
- Region
- Recurso
- AWS Config Regla
- Parámetros de entrada
- Hora de la última actualización

AWS STS uso global de puntos finales en Regiones de AWS

Description (Descripción)

Esta comprobación identifica un riesgo de resiliencia cuando AWS las cargas de trabajo realizan llamadas entre regiones al punto final global de STS en la región de EE. UU. Este (Virginia del Norte). AWS Las cargas de trabajo que realizan solicitudes entre regiones al punto final global de STS en EE. UU. Este (Virginia del Norte) podrían verse afectadas negativamente si se ve afectada la conectividad con el punto final de STS de EE. UU. Este (Virginia del Norte).

En abril de 2025, AWS mejoró el punto final global para que atendiera automáticamente las llamadas a los puntos finales globales de STS en la misma región en la que se encuentran sus cargas de trabajo AWS, y todas ellas están Regiones de AWS activadas de forma predeterminada. Sin embargo, algunas cargas de trabajo, como las que se ejecutan en regiones de suscripción o las que no utilizan servidores DNS de Amazon, no se benefician de la reducción de la latencia y el [aislamiento de errores](#) que se ofrecen como parte de esta mejora. Para estas cargas de trabajo, las solicitudes de puntos de conexión globales de STS se atienden en la región

Este de EE. UU. (Norte de Virginia), lo que supone un riesgo de resiliencia para la aplicación y aumenta la latencia de las solicitudes de STS.

 Note

Los resultados de esta comprobación se actualizan automáticamente varias veces al día, y cada vez corresponde a los últimos 15 días. No se permiten las solicitudes de actualización. Por lo tanto, los cambios pueden tardar hasta 15 días en aparecer en los resultados de la Trusted Advisor comprobación.

Para los clientes de Business, Enterprise On-Ramp o Enterprise Support, pueden usar la [BatchUpdateRecommendationResourceExclusion](#) API para incluir o excluir uno o más recursos de sus Trusted Advisor resultados.

ID de la verificación

c15m0mg1d3

Criterios de alerta

Rojo: las cargas de trabajo realizan llamadas entre regiones al punto final AWS STS global de la región EE.UU. Este (Norte de Virginia).

Acción recomendada

Para mejorar la resiliencia y el rendimiento de sus cargas de trabajo, le recomendamos que migre del punto de conexión global de STS al punto de conexión regional de STS. Al usar un punto final regional, puede usarlo AWS STS en la misma región que sus cargas de trabajo.

La siguiente es una lista de los directores AWS Identity and Access Management (IAM) que realizan llamadas entre regiones al punto final AWS STS global de la región EE.UU. Este (Virginia del Norte). Si sigue los pasos de la entrada del blog [Cómo usar los AWS STS puntos de enlace regionales, puede volver a](#) configurar sus cargas de trabajo para que utilicen el punto de conexión STS regional.

Status	ARN de la entidad principal	Tipo de entidad principal de IAM	Action	Hora de la última actualización	Región de origen
Red	arn:aws:iam::999999999999:role/example	Rol	AssumeRole	2025-01-01T08:00.000Z	ca-west-1
Red	arn:aws:iam: :123456789012:user/JohnDoe	Usuario	GetCallerIdentity	2025-01-01T08:00.000Z	ca-west-1
Red	arn:aws:sts::123456789012:federated-user/<Name>	Usuario federado	GetCallerIdentity	2025-01-01T08:00.000Z	eu-west-2
Red	arn:aws:iam::123456789012:root	Raíz	AssumeRole	2025-01-01T08:00.000Z	il-central-1
Red	arn:aws:sts: :0123456789012:supuesto-0123456789 ejemplo role/aws:ec2-instance/i	Rol de identidad de instancia de EC2	GetCallerIdentity	2025-01-01T08:00.000Z	us-west-1

Recursos adicionales

- [Administrar AWS STS en un Región de AWS](#)

- [AWS STS Puntos de conexión regionales](#)

Columnas de informes

- Status
- ARN de la entidad principal
- Action
- Tipo de elemento principal
- Región de origen
- Hora de la última actualización

Problemas de alto riesgo de AWS Well-Architected para la fiabilidad

Description (Descripción)

Comprueba si hay problemas de alto riesgo (HRIs) para sus cargas de trabajo en el pilar de la 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.

Para los clientes del plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puede usar la [BatchUpdateRecommendationResourceExclusionAPI](#) para incluir o excluir uno o más recursos de sus Trusted Advisor resultados.

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
- Region
- 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
- Número de HRIs identificables en cuanto a confiabilidad
- Número de valores HRIs resueltos en cuanto a confiabilidad
- Cantidad de preguntas contestadas para la fiabilidad
- Cantidad total de preguntas en el pilar de fiabilidad
- Hora de la última actualización

Classic Load Balancer no tiene configurados múltiples AZs

Description (Descripción)

Comprueba si Classic Load Balancer abarca varias zonas de disponibilidad (). AZs

Un equilibrador de carga distribuye el tráfico entrante de aplicaciones en varias instancias de Amazon EC2 en varias zonas de disponibilidad. De forma predeterminada, el equilibrador de carga distribuye equitativamente el tráfico entre las zonas de disponibilidad que se habilitan para el equilibrador 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 `minAvailabilityZones` parámetro 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.

Para los clientes del plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puede usar la [BatchUpdateRecommendationResourceExclusion](#) API para incluir o excluir uno o más recursos de sus Trusted Advisor resultados.

ID de la verificación

c18d2gz154

origen

AWS Config Managed Rule: clb-multiple-az

Criterios de alerta

Amarillo: Classic Load Balancer no tiene la configuración Multi-AZ o no cumple con el número mínimo especificado. AZs

Acción recomendada

Asegúrese de que sus equilibradores de carga clásicos tengan configuradas varias zonas de disponibilidad. Distribuya el balanceador de carga en varios AZs para asegurarse de que su aplicación tiene una alta disponibilidad.

Para obtener más información, consulte [Tutorial: crear un equilibrador de carga clásico](#).

Columnas de informes

- Status
- Region
- Recurso

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

Drenaje de conexiones de ELB

Description (Descripción)

Verifica si hay equilibradores de carga clásicos que no tienen habilitado el drenaje de conexiones.

Cuando el drenaje de conexiones no está habilitado y se anula el registro de una instancia de Amazon EC2 desde un equilibrador de carga clásico, el equilibrador de carga detiene el enrutamiento del tráfico a dicha instancia y cierra la conexión. Cuando se habilita el drenaje de conexiones, el equilibrador de carga clásico 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 clásico.
- Amarillo: el drenaje de conexiones está habilitado para un equilibrador de carga clásico.

Acción recomendada

Habilite el drenaje de conexiones para el equilibrador de carga clásico. 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
- Region
- Nombre del equilibrador de carga
- Motivo

Desequilibrio de objetivos del ELB

Description (Descripción)

Comprueba la distribución objetivo de los grupos objetivo en las zonas de disponibilidad (AZs) para Application Load Balancer (ALB), Network Load Balancer (NLB) y Gateway Load Balancer (GWLB).

Esta comprobación excluye lo siguiente:

- Equilibradores de carga configurados con una sola zona de disponibilidad (AZ).
- Equilibradores de carga en los que la diferencia en el número de objetivos entre el más poblado y el menos poblado es igual o inferior a 1. AZs
- Grupos de destinatarios con objetivos basados en IP en los que el AvailabilityZone atributo está establecido en «todos».

ID de la verificación

b92b83d667

Criterios de alerta

- Rojo: una única zona de disponibilidad representa más del 66 % de la capacidad del equilibrador de carga.
- Amarillo: una única zona de disponibilidad representa más del 50 % de la capacidad del equilibrador de carga.
- Verde: No AZs representa más del 50% de la capacidad del balanceador de carga.

Acción recomendada

Para mejorar la resiliencia, asegúrate de que tus grupos de objetivos tengan el mismo número de objetivos en todos AZs los grupos.

Recursos adicionales

[Grupos de destino para los Equilibradores de carga de aplicación](#)

[Registre los objetivos con su grupo objetivo de Application Load Balancer](#)

Columnas de informes

- Status
- Region

- Nombre del equilibrador de carga
- Tipo de equilibrador de carga
- ARN del grupo de destino (arn)
- Diferencia entre los objetivos registrados AZs
- Hora de la última actualización

GWLB: independencia de la zona de disponibilidad del punto de conexión

Description (Descripción)

Verifica si los puntos de conexión del equilibrador de carga de puerta de enlace (GWLB) están configurados como destino de ruta desde otra zona de disponibilidad (AZ).

Los puntos de conexión del equilibrador de carga de la puerta de enlace reenvían el tráfico de la red a los dispositivos de firewall que se encuentran detrás de un equilibrador de carga de la puerta de enlace para su inspección. Cada punto de conexión del equilibrador de carga de puerta de enlace funciona dentro de una zona de disponibilidad designada y se crea con redundancia únicamente en esa zona de disponibilidad. Por lo tanto, cualquier recurso de una zona de disponibilidad determinada debe utilizar un punto de conexión del equilibrador de carga de la puerta de enlace en la misma zona de disponibilidad. Esto garantiza que cualquier posible interrupción de un punto de conexión del equilibrador de carga de la puerta de enlace o de su zona de disponibilidad no afecte a los recursos de otra zona de disponibilidad.

ID de la verificación

528d6f5ee7

Criterios de alerta

- Rojo: el tráfico de la subred en una zona de disponibilidad se enruta a través de un punto de conexión del equilibrador de carga de una puerta de enlace en una zona de disponibilidad diferente.
- Verde: el tráfico de la subred en una zona de disponibilidad se enruta a través de un punto de conexión del equilibrador de carga de una puerta de enlace en la misma zona de disponibilidad.

Acción recomendada

Verifique la zona de disponibilidad de su subred y configure su tabla de enrutamiento para enrutar el tráfico a través de un punto de conexión del equilibrador de carga de la puerta de enlace en la misma zona de disponibilidad.

Si no hay ningún punto de conexión del equilibrador de carga de puerta de enlace en la zona de disponibilidad, cree uno nuevo y, a continuación, dirija el tráfico de la subred a través de él.

Si tiene la misma tabla de enrutamiento asociada a subredes de diferentes subredes AZs, mantenga esta tabla de enrutamiento asociada a las subredes que residen en la misma zona de disponibilidad que el punto final de Gateway Load Balancer. Para las subredes de la otra zona de disponibilidad, puede asociar una tabla de enrutamiento independiente con una ruta a un punto de conexión del equilibrador de carga de la puerta de enlace en esta zona de disponibilidad.

Se recomienda que elija un período de mantenimiento para los cambios de arquitectura en Amazon VPC.

Recursos adicionales

- [Independencia de la zona de disponibilidad](#)
- [Configuración del enrutamiento para el punto de conexión del equilibrador de carga de la puerta de enlace](#)
- [AWS Well-Architected Tool - Utilice arquitecturas de mamparo para limitar el alcance del impacto](#)

Columnas de informes

- Status
- Region
- Lista de identificadores de subredes entre zonas de disponibilidad
- ID del punto de conexión del equilibrador de carga de puerta de enlace
- ID de la subred del punto de conexión del equilibrador de carga de puerta de enlace
- Zonas de disponibilidad de la subred de puntos de conexión de VPC
- Hora de la última actualización

Optimización del balanceador de carga

Description (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
- Region
- Nombre del equilibrador de carga
- N.º 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

Description (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.

Para los clientes del plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puede usar la [BatchUpdateRecommendationResourceExclusion](#) API para incluir o excluir uno o más recursos de sus Trusted Advisor resultados.

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 distintas subredes AZs, mantenga esta tabla de enrutamiento asociada a las subredes que residen en la misma zona de disponibilidad que la puerta de enlace de NAT y, para las subredes de la otra zona de disponibilidad, asocie una tabla de enrutamiento independiente a una ruta a una puerta de enlace de 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
- Region
- 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

Independencia de las zonas de disponibilidad del punto de conexión del firewall de red

Description (Descripción)

Comprueba si sus AWS Network Firewall puntos de conexión están configurados como un destino de ruta desde otra zona de disponibilidad (AZ).

Los puntos de conexión del firewall de red reenvían el tráfico de red a un firewall de red para su inspección. Cada punto de conexión del firewall de red funciona dentro de una zona de disponibilidad designada y se crea con redundancia únicamente en esa zona de disponibilidad. Los recursos de una zona de disponibilidad determinada deben utilizar un punto de conexión del firewall de red en la misma zona de disponibilidad. Esto garantiza que cualquier posible interrupción de un punto de conexión del firewall de red o de su zona de disponibilidad no afecte a los recursos de otra zona de disponibilidad. El tráfico de red que se origina en otra zona de disponibilidad para inspeccionar el tráfico implica cargos por la transferencia de datos entre zonas de disponibilidad. Se recomienda asegurarse de que todos los recursos de una zona de disponibilidad específica utilicen un firewall de red en la misma zona de disponibilidad para evitar cargos por datos entre zonas de disponibilidad.

ID de la verificación

7040ea389a

Criterios de alerta

- **Amarillo:** el tráfico de una subred en una zona de disponibilidad se enruta a través de un punto de conexión del firewall de red en una zona de disponibilidad diferente.
- **Verde:** el tráfico de una subred en una zona de disponibilidad se enruta a través de un punto de conexión del firewall de red en la misma zona de disponibilidad.

Acción recomendada

Verifique la zona de disponibilidad de la subred y dirija el tráfico a través de un punto de conexión del firewall de red en la misma zona de disponibilidad.

Si no hay ningún punto de conexión del firewall de red en la zona de disponibilidad, cree un nuevo firewall de red y dirija el tráfico de la subred a través de él.

Si la misma tabla de enrutamiento está asociada a varias subredes en diferentes subredes AZs, mantenga esta tabla de enrutamiento asociada a las subredes que residen en la misma zona de disponibilidad que el punto final de Network Firewall. Para las subredes de otras AZs, asocie una

tabla de enrutamiento independiente a una ruta a un punto final de Network Firewall en esa zona de disponibilidad.

Se recomienda que elija un período de mantenimiento para los cambios de arquitectura en Amazon VPC.

Recursos adicionales

[Transferencia de datos dentro de la misma Región de AWS](#)

[Comprensión de los cargos por transferencia de datos](#)

[Independencia de la zona de disponibilidad](#)

[Pasos de alto nivel para implementar un firewall](#)

[Creación de un firewall](#)

[AWS Well-Architected Tool - Utilice arquitecturas de mamparo para limitar el alcance del impacto](#)

Columnas de informes

- Status
- Region
- ID de punto de conexión de firewall de red
- ARN de firewall de red
- Subred de puntos de conexión de firewall de red
- Zona de disponibilidad del punto de conexión del firewall de red
- Lista de subredes entre zonas de disponibilidad
- Hora de la última actualización

Firewall de red multi-AZ

Description (Descripción)

Verifica si los firewalls de red están configurados para usar más de una zona de disponibilidad (AZ) como puntos de conexión de firewall.

Una zona de disponibilidad es una ubicación diferente que queda aislada en caso de error en otras zonas. Si el punto final del Network Firewall se implementa solo en 1 AZ, puede tratarse

de un único punto de error y afectar las cargas de trabajo de otros usuarios que AZs utilizan el Network Firewall para inspeccionar el tráfico. Se recomienda configurar los firewalls de red AZs en varios servidores de la misma región para mejorar la disponibilidad de la carga de trabajo.

ID de la verificación

c2v1fg0gqd

Criterios de alerta

- Amarillo: el punto de conexión de firewall de red está implementado en 1 zona de disponibilidad.
- Verde: los puntos finales de Network Firewall están desplegados en al menos dos AZs.

Acción recomendada

Asegúrese de que su Network Firewall esté configurado con al menos dos AZs para las cargas de trabajo de producción.

Recursos adicionales

[Configuración de subred de VPC para AWS Network Firewall](#)

[Creación de un firewall](#)

[Zona de disponibilidad](#)

[AWS Well-Architected Tool - Implemente la carga de trabajo en varias ubicaciones](#)

[Dispositivo en una VPC de servicios compartidos](#)

Columnas de informes

- Status
- Region
- ARN de firewall de red
- ID de VPC
- Subredes de firewall de red
- Subredes de Network Firewall AZs
- Hora de la última actualización

Equilibrador de carga cruzado del equilibrador de carga de red

Description (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.

Para los clientes del plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puede usar la [BatchUpdateRecommendationResourceExclusion](#) API para incluir o excluir uno o más recursos de sus Trusted Advisor resultados.

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

NLB: recurso con acceso a Internet en una subred privada

Description (Descripción)

Verifica si un equilibrador de carga de red (NLB) expuesto a Internet está configurado con una subred privada. Se debe configurar un equilibrador de carga de red (NLB) expuesto a Internet en las subredes públicas para recibir tráfico. Una subred pública es una subred que tiene una ruta directa a una [puerta de enlace de 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.

Para los clientes del plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puede usar la [BatchUpdateRecommendationResourceExclusionAPI](#) para incluir o excluir uno o más recursos de sus Trusted Advisor resultados.

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 acceso a Internet

Acción recomendada

Compruebe que las subredes configuradas en un equilibrador de carga con acceso a Internet son públicas. Una subred pública es una subred que tiene una ruta directa a una [puerta de enlace de Internet](#). Utilice una de las siguientes opciones:

- Cree un equilibrador de carga nuevo y seleccione una subred diferente con una ruta directa a una puerta de enlace de Internet.
- Cambie la subred que actualmente está conectada al equilibrador de cargas de privada a pública. Para ello, cambie su tabla de enrutamiento y [asocie una puerta de enlace de Internet](#).

Recursos adicionales

- [Configurar un equilibrador de carga y un oyente](#)
- [Subredes para su VPC](#)
- [Asocie una puerta de enlace a una tabla de enrutamiento](#)

Columnas de informes

- Status
- Region
- Arn de NLB
- Nombre de NLB
- ID de subred
- Esquema de NLB
- Tipo de subred
- Hora de la última actualización

Multi-AZ de NLB

Description (Descripción)

Verifica si los equilibradores 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 su balanceador de carga AZs en varios 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.

Para los clientes del plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puede usar la [BatchUpdateRecommendationResourceExclusionAPI](#) para incluir o excluir uno o más recursos de sus Trusted Advisor resultados.

ID de la verificación

c1dfprch09

Criterios de alerta

Amarillo: NLB está en una única zona de disponibilidad.

Verde: NLB tiene dos o más. AZs

Acción recomendada

Asegúrese de que el equilibrador 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
- Region
- Número de AZs
- ARN de NLB
- Nombre de NLB
- Hora de la última actualización

Número de Regiones de AWS en un conjunto de réplicas de Incident Manager

Description (Descripción)

Comprueba que la configuración de un conjunto de replicación de Incident Manager utiliza más de una 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 en la 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.

Para los clientes del plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puede usar la [BatchUpdateRecommendationResourceExclusionAPI](#) para incluir o excluir uno o más recursos de sus Trusted Advisor resultados.

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

Description (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 su servicio entre varios AZs, limita el radio de alcance de una falla en una 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.

Para los clientes del plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puede usar la [BatchUpdateRecommendationResourceExclusionAPI](#) para incluir o excluir uno o más recursos de sus Trusted Advisor resultados.

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
- Region
- ID de VPC
- Hora de la última actualización

Interfaz de VPC: interfaces de red de punto final en múltiples AZs

Description (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 una AZs misma región. AWS Seleccione subredes en varias AZs al crear puntos finales de interfaz para ayudar a proteger sus aplicaciones frente a un único punto de fallo.

Note

Actualmente, esta verificación solo incluye los puntos de conexión 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.

Para los clientes del plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puede usar la [BatchUpdateRecommendationResourceExclusionAPI](#) para incluir o excluir uno o más recursos de sus Trusted Advisor resultados.

ID de la verificación

c1dfprch10

Criterios de alerta

Amarillo: el punto de conexión de VPC está en una única zona de disponibilidad.

Verde: el punto final de la VPC está en al menos dos. AZs

Acción recomendada

Asegúrese de que el punto de conexión 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 :

- [Acceso y Servicio de AWS uso de un punto final de VPC de interfaz](#)
- [La dirección IP privada de la interfaz de red del punto de conexión](#)
- [AWS PrivateLink conceptos](#)
- [Regiones y zonas de disponibilidad](#)

Columnas de informes

- Status
- Region
- ID de punto de conexión de VPC
- Es multi-AZ
- Hora de la última actualización

Redundancia de túnel de VPN

Description (Descripción)

Comprueba el número de túneles que están activos para cada uno de sus Site-to-Site VPNs.

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 usuario de Site-to-Site VPN de AWS](#).

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 El [dispositivo de puerta de enlace del cliente](#) o [Eliminar una conexión Site-to-Site VPN](#).

Recursos adicionales

- [AWS Site-to-Site Guía del usuario de VPN](#)
- [Cree una puerta de enlace de destino](#)

Columnas de informes

- Status
- Region
- ID de VPN
- VPC
- Puerta de enlace privada virtual
- Gateway de cliente
- Túneles activos
- Motivo

Redundancia de la zona de disponibilidad de ActiveMQ

Description (Descripción)

Comprueba que Amazon MQ para agentes ActiveMQ esté configurado para una alta disponibilidad con un active/standby agente 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.

Para los clientes del plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puede usar la [BatchUpdateRecommendationResourceExclusion](#) API para incluir o excluir uno o más recursos de sus Trusted Advisor resultados.

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 active/standby de despliegue.

Recursos adicionales

- [Creación de un agente ActiveMQ](#)

Columnas de informes

- Status
- Region
- 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

Description (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.

Para los clientes del plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puede usar la [BatchUpdateRecommendationResourceExclusionAPI](#) para incluir o excluir uno o más recursos de sus Trusted Advisor resultados.

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

- Region
- 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: no Trusted Advisor ha podido recuperar la utilización o los límites de 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 \(io1\) de IOPS aprovisionadas \(SSD\) 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-Classical](#)
- [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

Description (Descripción)

Verifica si el uso supera el 80 % de la cuota de grupos de Auto Scaling.

ID de la verificación

fw7HH017J9

Recursos adicionales

[Cuotas de Auto Scaling](#)

Configuraciones de lanzamiento de Auto Scaling

Description (Descripción)

Verifica si el uso supera el 80 % de la cuota de configuraciones de lanzamiento de Auto Scaling.

ID de la verificación

aw7HH017J9

Recursos adicionales

[Cuotas de Auto Scaling](#)

CloudFormation Pilas

Description (Descripción)

Comprueba si el uso supera el 80% de la cuota de CloudFormation pilas.

ID de la verificación

gW7HH017J9

Recursos adicionales

[CloudFormation cuotas](#)

Capacidad de lectura de DynamoDB

Description (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

Description (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

Description (Descripción)

Verifica si el uso supera el 80 % de la cuota de instantáneas activas de EBS.

ID de la verificación

eI7KK017J9

Recursos adicionales

[Límites de Amazon EBS](#)

Almacenamiento de volúmenes de HDD en frío (sc1) de EBS

Description (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

Description (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

dH7RR016J9

Recursos adicionales

[Límites de Amazon EBS](#)

Almacenamiento de volúmenes de SSD de uso general (gp3) de EBS

Description (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

dH7RR016J3

Recursos adicionales

[Límites de Amazon EBS](#)

Almacenamiento de volúmenes magnéticos (estándar) de EBS

Description (Descripción)

Verifica si el uso supera el 80 % de la cuota de almacenamiento de volúmenes magnéticos (estándar) de EBS.

ID de la verificación

cG7HH017J9

Recursos adicionales

[Límites de Amazon EBS](#)

IOPS agregadas de volúmenes (io1) de IOPS aprovisionadas (SSD) de EBS

Description (Descripción)

Verifica el uso que supera el 80 % de la cuota de IOPS agregadas de volúmenes (io1) de IOPS aprovisionadas (SSD) de EBS.

ID de la verificación

tV7YY017J9

Recursos adicionales

[Límites de Amazon EBS](#)

Almacenamiento de volúmenes de SSD de IOPS provisionadas (io1) de EBS

Description (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

gI7MM017J9

Recursos adicionales

[Límites de Amazon EBS](#)

Almacenamiento de volúmenes de SSD de IOPS provisionadas (io2) de EBS

Description (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

gI7MM017J2

Recursos adicionales

[Límites de Amazon EBS](#)

Almacenamiento de volúmenes de HDD con rendimiento optimizado (st1) de EBS

Description (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

wH7DD013J9

Recursos adicionales

[Límites de Amazon EBS](#)

Instancias bajo demanda de EC2

Description (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

Description (Descripción)

Verifica si el uso supera el 80 % de la cuota de asignación de instancias reservadas de EC2.

ID de la verificación

iH7PP017J9

Recursos adicionales

[Cuotas de Amazon EC2](#)

Direcciones IP elásticas de EC2-Classic

Description (Descripción)

Verifica si el uso supera el 80 % de la cuota de direcciones IP elásticas de EC2-Classic.

ID de la verificación

aW9HH018J6

Recursos adicionales

[Cuotas de Amazon EC2](#)

Dirección IP elástica de EC2-VPC

Description (Descripción)

Verifica si el uso supera el 80 % de la cuota de direcciones IP elásticas de EC2-VPC.

ID de la verificación

1N7RR017J9

Recursos adicionales

[Cuotas de IP elásticas de VPC](#)

Application Load Balancers de ELB

Description (Descripción)

Verifica si el uso supera el 80 % de la cuota de Application Load Balancers de ELB.

ID de la verificación

EM8b3yLRTx

Recursos adicionales

[Cuotas de Elastic Load Balancing](#)

Classic Load Balancers de ELB

Description (Descripción)

Verifica si el uso supera el 80 % de la cuota de Classic Load Balancers de ELB.

ID de la verificación

iK700017J9

Recursos adicionales

[Cuotas de Elastic Load Balancing](#)

Network Load Balancers de ELB

Description (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

Description (Descripción)

Verifica si el uso supera el 80 % de la cuota de grupo de IAM.

ID de la verificación

sU7XX017J9

Recursos adicionales

[Cuotas de IAM](#)

Perfiles de instancias de IAM

Description (Descripción)

Verifica si el uso supera el 80 % de la cuota de perfiles de instancias de IAM.

ID de la verificación

n07SS017J9

Recursos adicionales

[Cuotas de IAM](#)

Políticas de IAM

Description (Descripción)

Verifica si el uso supera el 80 % de la cuota de políticas de IAM.

ID de la verificación

pR7UU017J9

Recursos adicionales

[Cuotas de IAM](#)

Roles de IAM

Description (Descripción)

Verifica si el uso supera el 80 % de la cuota de roles de IAM.

ID de la verificación

oQ7TT017J9

Recursos adicionales

[Cuotas de IAM](#)

Certificados de servidor de IAM

Description (Descripción)

Verifica si el uso supera el 80 % de la cuota de certificados de servidor de IAM.

ID de la verificación

rT7WW017J9

Recursos adicionales

[Cuotas de IAM](#)

Usuarios de IAM

Description (Descripción)

Verifica si el uso supera el 80 % de la cuota de usuarios de IAM.

ID de la verificación

qS7VV017J9

Recursos adicionales

[Cuotas de IAM](#)

Particiones de Kinesis por región

Description (Descripción)

Verifica si el uso supera el 80 % de cuota de particiones de Kinesis por región.

ID de la verificación

bW7HH017J9

Recursos adicionales

[Cuotas de Kinesis](#)

Uso del almacenamiento de código de Lambda

Description (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.

Para los clientes del plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puede usar la [BatchUpdateRecommendationResourceExclusion](#) API para incluir o excluir uno o más recursos de sus Trusted Advisor resultados.

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 del almacenamiento del código de la función se expresa MegaBytes con 2 decimales.
- La cantidad de versiones de la función

- Hora de la última actualización

Grupos de parámetros de clústeres de RDS

Description (Descripción)

Verifica si el uso supera el 80 % de la cuota de grupos de parámetros de clústeres de RDS.

ID de la verificación

jt1IM03qZM

Recursos adicionales

[Cuotas de Amazon RDS](#)

Roles de clústeres de RDS

Description (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

Description (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

Description (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

Description (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

Description (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

Description (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

gfZAn3W7w1

Recursos adicionales

[Cuotas de Amazon RDS](#)

Suscripciones de eventos de RDS

Description (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

Description (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

Description (Descripción)

Verifica si el uso supera el 80 % de la cuota de grupos de opciones de RDS.

ID de la verificación

3Njm0DJQ09

Recursos adicionales

[Cuotas de Amazon RDS](#)

Réplicas de lectura por maestro de RDS

Description (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

Description (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

Description (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

Description (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

Description (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

Description (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

Description (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

Description (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

Description (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

Description (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

Description (Descripción)

Verifica si el uso supera el 80 % de la cuota de envío diaria de Amazon SES.

ID de la verificación

hJ7NN017J9

Recursos adicionales

[Cuotas de Amazon SES](#)

VPC

Description (Descripción)

Verifica si el uso supera el 80 % de la cuota de VPC.

ID de la verificación

jL7PP017J9

Recursos adicionales

[Cuotas de VPC](#)

Gateways de Internet de VPC

Description (Descripción)

Verifica si el uso supera el 80 % de la cuota de gateways de Internet de VPC.

ID de la verificación

kM7QQ017J9

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](#)
- [Amazon API Gateway REST APIs sin rastreo de rayos X activado](#)
- [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 bases de datos de Amazon RDS en los clústeres con grupos de parámetros heterogéneos](#)
- [La monitorización mejorada de Amazon RDS está desactivada](#)
- [La información de rendimiento de Amazon RDS está desactivada](#)
- [El parámetro track_counts de Amazon RDS está desactivado](#)
- [Registro de auditoría de clústeres de Amazon Redshift](#)
- [Registros de acceso de Amazon S3 habilitados](#)
- [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](#)
- [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

Description (Descripción)

Comprueba si Amazon API Gateway tiene CloudWatch los registros activados en el nivel de registro deseado.

Active el CloudWatch registro de los métodos de API REST o las rutas de WebSocket API en Amazon API Gateway para recopilar los registros de ejecución en CloudWatch los registros de las solicitudes que reciba APIs. 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.

Para los clientes del plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puede usar la [BatchUpdateRecommendationResourceExclusionAPI](#) para incluir o excluir uno o más recursos de sus Trusted Advisor resultados.

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 para su Amazon API Gateway [REST APIs](#) o [WebSocket APIs](#) 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
- Region
- Recurso
- AWS Config Regla
- Parámetros de entrada
- Hora de la última actualización

Amazon API Gateway REST APIs sin rastreo de rayos X activado

Description (Descripción)

Comprueba si Amazon API Gateway REST APIs tiene activado AWS X-Ray el rastreo.

Activa el rastreo de X-Ray en tu REST APIs para permitir que API Gateway muestree las solicitudes de invocación de API con información de rastreo. Esto le permite aprovechar para rastrear y analizar las solicitudes AWS X-Ray a medida que viajan a través de su REST de API Gateway APIs hacia los servicios descendentes.

Para obtener más información, consulte [Rastrear las solicitudes de los usuarios a REST APIs 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.

Para los clientes del plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puede usar la [BatchUpdateRecommendationResourceExclusionAPI](#) para incluir o excluir uno o más recursos de sus Trusted Advisor resultados.

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

Activa el rastreo de X-Ray para tu REST de API Gateway. APIs

Para obtener más información, consulte [Configuración AWS X-Ray con API Gateway REST APIs](#).

Recursos adicionales

- [Rastreo de las solicitudes de los usuarios a REST APIs mediante X-Ray](#)
- [¿Qué es? AWS X-Ray](#)

Columnas de informes

- Status
- Region
- Recurso
- AWS Config Regla
- Parámetros de entrada
- Hora de la última actualización

Registro de CloudFront acceso a Amazon configurado

Description (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.

Para los clientes del plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puede usar la [BatchUpdateRecommendationResourceExclusion](#) API para incluir o excluir uno o más recursos de sus Trusted Advisor resultados.

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

La acción CloudWatch de alarma de Amazon está desactivada

Description (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.

Para los clientes del plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puede usar la [BatchUpdateRecommendationResourceExclusion](#) API para incluir o excluir uno o más recursos de sus Trusted Advisor resultados.

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, elimínala para evitar incurrir en costes innecesarios.

Para obtener más información, consulta [enable-alarm-actions](#) la referencia de AWS CLI comandos y [func \(*CloudWatch\) EnableAlarmActions](#) en la referencia de la API de AWS SDK for Go.

Columnas de informes

- Status
- Region
- Recurso
- AWS Config Regla
- Parámetros de entrada
- Hora de la última actualización

Instancia de Amazon EC2 no gestionada por AWS Systems Manager

Description (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.

Para los clientes del plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puede usar la [BatchUpdateRecommendationResourceExclusion](#) API para incluir o excluir uno o más recursos de sus Trusted Advisor resultados.

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

Repositorio de Amazon ECR con la inmutabilidad de etiquetas desactivada

Description (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.

Para los clientes del plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puede usar la [BatchUpdateRecommendationResourceExclusion](#) API para incluir o excluir uno o más recursos de sus Trusted Advisor resultados.

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

Desactivación de la información de contenedores en clústeres de Amazon ECS

Description (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.

Para los clientes del plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puede usar la [BatchUpdateRecommendationResourceExclusion](#) API para incluir o excluir uno o más recursos de sus Trusted Advisor resultados.

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

El registro de tareas de Amazon ECS no está habilitado

Description (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.

Para los clientes del plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puede usar la [BatchUpdateRecommendationResourceExclusionAPI](#) para incluir o excluir uno o más recursos de sus Trusted Advisor resultados.

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
- Region
- Recurso
- AWS Config Regla

- Parámetros de entrada
- Hora de la última actualización

El registro OpenSearch de Amazon Service CloudWatch no está configurado

Description (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 [Supervisión 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.

Para los clientes del plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puede usar la [BatchUpdateRecommendationResourceExclusionAPI](#) para incluir o excluir uno o más recursos de sus Trusted Advisor resultados.

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

Instancias de bases de datos de Amazon RDS en los clústeres con grupos de parámetros heterogéneos

Description (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.

Para los clientes del plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puede usar la [BatchUpdateRecommendationResourceExclusion](#) API para incluir o excluir uno o más recursos de sus Trusted Advisor resultados.

 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

c1qf5bt010

Criterios de alerta

Amarillo: clústeres de base de datos tienen instancias de bases 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
- Region
- Recurso
- Valores recomendados
- Nombre del motor

- Hora de la última actualización

La monitorización mejorada de Amazon RDS está desactivada

Description (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.

Para los clientes del plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puede usar la [BatchUpdateRecommendationResourceExclusionAPI](#) para incluir o excluir uno o más recursos de sus Trusted Advisor resultados.

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

c1qf5bt004

Criterios de alerta

Amarillo: los recursos de Amazon RDS no tienen activado el monitoreo mejorado.

Acción recomendada

Active la monitorización mejorada

Recursos adicionales

El monitoreo mejorado de Amazon RDS proporciona visibilidad adicional del estado de sus instancias de base de datos. Le recomendamos que active el monitoreo mejorado. Cuando la opción de monitoreo mejorado 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
- Region
- Recurso
- Valores recomendados
- Nombre del motor
- Hora de la última actualización

La información de rendimiento de Amazon RDS está desactivada

Description (Descripción)

La información de rendimiento de Amazon RDS monitorea la carga de la instancia de base de datos para ayudarle a analizar y solucionar los problemas de rendimiento de la base 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.

Para los clientes del plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puede usar la [BatchUpdateRecommendationResourceExclusion](#) API para incluir o excluir uno o más recursos de sus Trusted Advisor resultados.

 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

c1qf5bt012

Criterios de alerta

Amarillo: los recursos de Amazon RDS no tienen la información de rendimiento activada.

Acción recomendada

Activar Información de rendimiento.

Recursos adicionales

La información de rendimiento utiliza un método de recopilación de datos ligero que no afecta al rendimiento de las aplicaciones. La información de rendimiento le ayuda a evaluar rápidamente la carga de la base de datos.

Para obtener más información, consulte [Supervisión de la carga de base de datos con información de rendimiento en Amazon RDS](#).

Columnas de informes

- Status
- Region
- Recurso
- Valores recomendados
- Nombre del motor
- Hora de la última actualización

El parámetro track_counts de Amazon RDS está desactivado

Description (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 que establezca 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.

Para los clientes del plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puede usar la [BatchUpdateRecommendationResourceExclusionAPI](#) para incluir o excluir uno o más recursos de sus Trusted Advisor resultados.

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

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, desactiva 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 [Run-time Statistics for PostgreSQL](#) en la documentación de PostgreSQL.

Columnas de informes

- Status
- Region
- Recurso
- Valor del parámetro
- Valores recomendados
- Hora de la última actualización

Registro de auditoría de clústeres de Amazon Redshift

Description (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.

Para los clientes del plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puede usar la [BatchUpdateRecommendationResourceExclusionAPI](#) para incluir o excluir uno o más recursos de sus Trusted Advisor resultados.

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

Registros de acceso de Amazon S3 habilitados

Description (Descripción)

Verifica la configuración de registro de los buckets de Amazon Simple Storage Service.

La activación del registro de acceso al servidor proporciona registros de acceso detallados por hora a un bucket de Amazon S3 específico. Los registros de acceso contienen detalles de la solicitud, incluidos el tipo, los recursos especificados y la fecha y hora de procesamiento. El registro está desactivado de forma predeterminada. Los clientes deben activar el registro de acceso para realizar auditorías de seguridad o analizar el comportamiento de los usuarios y los patrones de uso.

Cuando el registro está activado inicialmente, la configuración se valida automáticamente. No obstante, las modificaciones futuras pueden dar lugar a errores de registro. Tenga en cuenta que, actualmente, esta comprobación no examina los permisos de escritura en el bucket de Amazon S3.

ID de la verificación

c1fd6b9614

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.
- Verde: el bucket tiene habilitado el registro de acceso al servidor, el destino ya existe y los permisos para escribir en el destino también

Acción recomendada

Active el registro de acceso al servidor para todos los buckets de Amazon S3 relevantes. Los registros de acceso al servidor proporcionan un registro de auditoría que se puede utilizar para comprender los patrones de acceso a los buckets e investigar actividades sospechosas. La activación del registro en todos los buckets aplicables mejorará la visibilidad de los eventos de acceso en su entorno de Amazon S3. 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](#).

Recursos adicionales

[Trabajar 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
- Region
- ARN de recurso
- Nombre del bucket
- Nombre del destino
- El destino existe
- Mismo propietario
- Escritura habilitada
- Motivo
- Hora de la última actualización

Amazon S3 no tiene habilitadas las notificaciones de eventos

Description (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.

Para los clientes del plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puede usar la [BatchUpdateRecommendationResourceExclusion](#) API para incluir o excluir uno o más recursos de sus Trusted Advisor resultados.

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
- Region
- 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

Description (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.

Para los clientes del plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puede usar la [BatchUpdateRecommendationResourceExclusionAPI](#) para incluir o excluir uno o más recursos de sus Trusted Advisor resultados.

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

Amazon VPC sin registros de flujo

Description (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.

Para los clientes del plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puede usar la [BatchUpdateRecommendationResourceExclusionAPI](#) para incluir o excluir uno o más recursos de sus Trusted Advisor resultados.

ID de la verificación

c18d2gz122

origen

AWS Config Managed Rule: vpc-flow-logs-enabled

Criterios de alerta

Amarillo: VPCs no tienen registros de flujo de Amazon VPC.

Acción recomendada

Cree registros de flujo de VPC para cada uno de sus VPCs

Para obtener más información, consulte [Creación de un registro de flujo](#)

Columnas de informes

- Status
- Region
- 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

Description (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.

Para los clientes del plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puede usar la [BatchUpdateRecommendationResourceExclusionAPI](#) para incluir o excluir uno o más recursos de sus Trusted Advisor resultados.

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
- Region
- Recurso
- AWS Config Regla
- Parámetros de entrada

- Hora de la última actualización

CloudFormation Notificación de pila

Description (Descripción)

Comprueba si todas tus CloudFormation pilas utilizan Amazon SNS para recibir notificaciones cuando se produce un evento.

Puede configurar esta comprobación para buscar un tema específico de Amazon SNS ARNs mediante los parámetros de sus AWS Config reglas.

Para obtener más información, consulte [Configuración de las opciones de 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.

Para los clientes del plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puede usar la [BatchUpdateRecommendationResourceExclusionAPI](#) para incluir o excluir uno o más recursos de sus Trusted Advisor resultados.

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 CloudFormation stacks no están activadas.

Acción recomendada

Asegúrese de que sus 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
- Region
- 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

Description (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.

Para los clientes del plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puede usar la [BatchUpdateRecommendationResourceExclusion](#) API para incluir o excluir uno o más recursos de sus Trusted Advisor resultados.

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

AWS CodeBuild Registro de proyectos

Description (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 `cloudWatchGroupNames` 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.

Para los clientes del plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puede usar la [BatchUpdateRecommendationResourceExclusion](#) API para incluir o excluir uno o más recursos de sus Trusted Advisor resultados.

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

AWS CodeDeploy Reversión automática y monitor activados

Description (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.

Para los clientes del plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puede usar la [BatchUpdateRecommendationResourceExclusionAPI](#) para incluir o excluir uno o más recursos de sus Trusted Advisor resultados.

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

AWS CodeDeploy Lambda utiliza all-at-once la configuración de implementación

Description (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.

Para los clientes del plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puede usar la [BatchUpdateRecommendationResourceExclusionAPI](#) para incluir o excluir uno o más recursos de sus Trusted Advisor resultados.

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

AWS Elastic Beanstalk Los informes de salud mejorados no están configurados

Description (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.

Para los clientes del plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puede usar la [BatchUpdateRecommendationResourceExclusion](#) API para incluir o excluir uno o más recursos de sus Trusted Advisor resultados.

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

AWS Elastic Beanstalk con las actualizaciones de plataforma gestionadas deshabilitadas

Description (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 UpdateLevel parámetros 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.

Para los clientes del plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puede usar la [BatchUpdateRecommendationResourceExclusionAPI](#) para incluir o excluir uno o más recursos de sus Trusted Advisor resultados.

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

AWS Fargate la versión de la plataforma no es la más reciente

Description (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.

Para los clientes del plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puede usar la [BatchUpdateRecommendationResourceExclusionAPI](#) para incluir o excluir uno o más recursos de sus Trusted Advisor resultados.

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
- Region
- 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

Description (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.

Para los clientes del plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puede usar la [BatchUpdateRecommendationResourceExclusion](#) API para incluir o excluir uno o más recursos de sus Trusted Advisor resultados.

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 NON_COMPLIANT.

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

CloudTrail las rutas no están configuradas con Amazon CloudWatch Logs

Description (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.

Para los clientes del plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puede usar la [BatchUpdateRecommendationResourceExclusionAPI](#) para incluir o excluir uno o más recursos de sus Trusted Advisor resultados.

ID de la verificación

c18d2gz164

origen

AWS Config Managed Rule: cloud-trail-cloud-watch-logs-enabled

Criterios de alerta

Amarillo: no AWS CloudTrail está configurada con la integración de CloudWatch Logs.

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
- Region
- 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

Description (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.

Para los clientes del plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puede usar la [BatchUpdateRecommendationResourceExclusionAPI](#) para incluir o excluir uno o más recursos de sus Trusted Advisor resultados.

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
- Region
- 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

Description (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.

Para los clientes del plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puede usar la [BatchUpdateRecommendationResourceExclusion](#) API para incluir o excluir uno o más recursos de sus Trusted Advisor resultados.

Recursos adicionales

[Protección contra eliminación para clústeres de Aurora](#)

Columnas de informes

- Status
- Region
- 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

Description (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.

Para los clientes del plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, puede usar la [BatchUpdateRecommendationResourceExclusion](#) API para incluir o excluir uno o más recursos de sus Trusted Advisor resultados.

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
- Region
- 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 obsoletas no aparecerán en los resultados de las comprobaciones. Si utilizas una comprobación obsoleta, como especificar el ID de la comprobación en una operación de AWS Support API o en tu código, recibirás errores en las llamadas a la API. Elimine estas verificaciones para evitar errores.

Para obtener más información sobre las verificaciones disponibles, consulte [AWS Trusted Advisor comprobar referencia](#).

Fecha de modificación	Nombre de la verificación	Descripción del cambio
19 de febrero de 2026	Nuevas pasarelas NAT inactivas	Se agregó una nueva verificación para identificar las

Fecha de modificación	Nombre de la verificación	Descripción del cambio
		pasarelas NAT inactivas o infrautilizadas que podrían ser aptas para la optimización de costos.
9 de enero de 2026	Se dejaron de utilizar 5 comprobaciones de optimización de Trusted Advisor costes	Quedaron en desuso las siguientes comprobaciones: • Savings Plan - Vz2c2w1srf • Optimización de instancias reservadas de Amazon Relational Database Service (RDS) - 1QazxSW23E • Optimización de nodos reservados de Amazon Redshift: 1qw23er45t • Optimización de nodos ElastiCache reservados de Amazon - H3L1oth3re • Optimización de instancias reservadas OpenSearch de Amazon Service: 7ujm6yhn5t
18 de diciembre de 2025	Se actualizó el control de versiones de Amazon S3 Bucket	Se agregó un nuevo criterio de alerta: • Amarillo: Trusted Advisor no tiene acceso para validar el control de versiones
17 de diciembre de 2025	Permisos de bucket de Amazon S3 actualizados	Se actualizó la sección de criterios de alerta.

Fecha de modificación	Nombre de la verificación	Descripción del cambio
21 de noviembre de 2025	Grupo de seguridad actualizado de Application Load Balancer	Se actualizaron las alertas y recomendaciones del grupo de seguridad Application Load Balancer.
17 de noviembre de 2025	Se actualizó AWS STS el uso global de los terminales en toda la descripción del Regiones de AWS cheque	Se actualizó el uso AWS STS global de los puntos finales en la descripción de las Regiones de AWS comprobaciones para aclarar cuándo se actualizan los resultados de las comprobaciones.
15 de octubre de 2025	Se actualizaron las descripciones de varias verificaciones	Se agregó una nota a las múltiples descripciones de verificaciones para indicar que en la verificación se informan todos los recursos marcados según los criterios y el número total de recursos evaluados, incluidos los recursos de OK. La tabla de recursos muestra solo los recursos marcados.
10 de octubre de 2025	Se actualizó la referencia de verificaciones	Se actualizó la referencia de verificación para mostrar todas las verificaciones disponibles.
11 de septiembre de 2025	L4dfs2q4c5: funciones que utilizan tiempos de ejecución obsoletos AWS Lambda	Se actualizó el criterio de alerta amarilla para indicar que se incluyen los tiempos de ejecución obsoletos en un intervalo mínimo de 180.

Fecha de modificación	Nombre de la verificación	Descripción del cambio
19 de agosto de 2025	Pfx0RwqBli: Permisos de bucket de Amazon S3	Criterios de alerta actualizados: Trusted Advisor no tiene permiso para verificar la política o la ACL, o bien la política o la ACL no se han podido evaluar por otros motivos. Se ha cambiado de amarillo a rojo.
22 de julio de 2025	- VjaFugJ9h0: Registro AWS CloudTrail - BueAdJ7NrP: Registro de buckets de Amazon S3	Estas verificaciones están en desuso.
3 de julio de 2025	Pfx0RwqBli: Permisos de bucket de Amazon S3	Los criterios de alerta se actualizaron para reflejar todos los criterios amarillos y rojos.
3 de julio de 2025	c1dfprch15: instancias de Amazon EC2 con final del soporte estándar con Ubuntu LTS	Se actualizó la nota para indicar que esta verificación se actualiza al menos una vez al día.
02 de julio de 2025	c1dvkm4z6b: controlador de Amazon ECS AWSLogs en modo de bloqueo	Amazon ECS cambió la configuración predeterminada del modo de parámetros de configuración de registro del controlador awslogs de blocking a non-blocking. La descripción de estado amarillo se ha actualizado para reflejar este cambio.

Fecha de modificación	Nombre de la verificación	Descripción del cambio
02 de julio de 2025	7DAFEemoDos: MFA en la cuenta raíz	Se agregó información que indica que las credenciales de usuario raíz de la cuenta de miembro se pueden eliminar de forma centralizada, lo que quita la necesidad de administrar la MFA en las credenciales de los usuarios raíz.
9 de junio de 2025	c1z7kmr17n: recomendaciones de optimización de costos de Amazon Aurora para el almacenamiento en clústeres de bases de datos	Nuevas verificaciones
9 de junio de 2025	c15m0mgld3: uso global de terminales en todo el mundo AWS STSRegiones de AWS	Verificación actualizada: esta verificación ya está disponible para todos los planes. AWS Support
2 de junio de 2025	c15m0mgld3: uso global de terminales en todos AWS STSRegiones de AWS	Nuevas verificaciones

Fecha de modificación	Nombre de la verificación	Descripción del cambio
30 de mayo de 2025	• c1z7kmr15n: Recomendaciones de compra de capacidad reservada de Amazon DynamoDB • c1z7kmr02n: Recomendaciones de optimización de costos de Amazon EBS para volúmenes • c1z7kmr01n: Recomendaciones de optimización de costos de Amazon EC2 para grupos de Amazon EC2 Auto Scaling • c1z7kmr00n: Recomendaciones de optimización de costos de Amazon EC2 para instancias • c1z7kmr13n: Recomendaciones de compra de nodos ElastiCache reservados de Amazon • c1z7kmr16n: Recomendaciones de compra de nodos reservados de Amazon MemoryDB • c1z7kmr14n: Recomendaciones de compra de instancias reservadas de Amazon OpenSearch Service • c1z7kmr04n: Recomendaciones de optimización de costos de Amazon RDS	Verificaciones nuevas del centro de optimización de costos

Fecha de modificación	Nombre de la verificación	Descripción del cambio
	para el almacenamiento de instancias de base de datos • c1z7kmr03n: Recomendaciones de optimización de costos de Amazon RDS para instancias de base de datos • c1z7kmr11n: Recomendaciones de compra de instancias reservadas de Amazon RDS • c1z7kmr12n: Recomendaciones de compra de nodos reservados de Amazon Redshift • c1z7kmr06n: AWS Fargate recomendaciones de optimización de costes para Amazon ECS • c1z7kmr05n: AWS Lambda recomendaciones de optimización de costes para las funciones • c1z7kmr08n: AWS Recomendaciones de compra de Savings Plans para Amazon SageMaker AI • c1z7kmr09n: AWS Recomendaciones de compra de Savings Plans para computación	

Fecha de modificación	Nombre de la verificación	Descripción del cambio
30 de abril de 2025	N420c450f2: Nombres CloudFront de dominio alternativos N425c450f2: certificados SSL personalizados en el almacén de certificados de IAM CloudFront	Se ha añadido una nota que indica que esta comprobación se aplica a CloudFront las distribuciones clásicas de Amazon.
30 de abril de 2025	N415c450f2: CloudFront reenvío de encabezados y porcentaje de aciertos de caché	Se ha añadido una nota que indica que esta comprobación se aplica a CloudFront las distribuciones clásicas de Amazon.
2 de abril de 2025	c1dfprch02: optimización del modo de rendimiento de Amazon EFS	La descripción de esta verificación ha cambiado. Para más información, consulte Instancias de Amazon EC2 con final de la compatibilidad con Microsoft Windows Server
02 de abril de 2025	Qsdfp3A4L4: instancias de Amazon EC2 con final de la compatibilidad con Microsoft Windows Server	La descripción de esta verificación ha cambiado. Para obtener más información, consulte Optimización del modo de rendimiento de Amazon EFS

Actualizaciones más antiguas

Las siguientes AWS Security Hub CSPM comprobaciones están en desuso:

Nombre de la verificación	ID de la verificación
S3.10 - Los depósitos de uso general de S3 con el control de versiones activado deben tener configuraciones de ciclo de vida	Hs4Ma3G211
S3.11 - Los depósitos de uso general de S3 deben tener habilitadas las notificaciones de eventos	Hs4Ma3G212
CodeBuild.5 - los entornos de CodeBuild proyecto no deberían tener habilitado el modo privilegiado	Hs4Ma3G218
CloudFormation.1 - las CloudFormation pilas deben estar integradas con Amazon Simple Notification Service (SNS)	Hs4Ma3G245
SNS.2 - Debe habilitarse el registro del estado de entrega de los mensajes de notificación enviados a un tema	Hs4Ma3G263
Athena.1 - Los grupos de trabajo de Athena deben estar cifrados en reposo	Hs4Ma3G294

Nueva verificación: las copias de seguridad de Amazon RDS no están habilitadas

Trusted Advisor agregó el siguiente cheque el 23 de diciembre de 2024.

Nombre de la verificación	Categoría de verificación	ID de la verificación
Las copias de seguridad de Amazon RDS no están habilitadas	Tolerancia a errores	44fde09ab5

Verifica si una instancia de Amazon RDS está habilitada con copias de seguridad automatizadas mediante Amazon RDS o con copias de seguridad continuas de AWS Backup. Las copias de seguridad continuas reducen el riesgo de pérdidas de datos inesperadas y permiten la recuperación a un momento dado.

Para obtener más información, consulte [Las copias de seguridad de Amazon RDS no están habilitadas](#).

Nuevo cheque: AWS CloudTrail Registro de eventos de administración

Trusted Advisor agregó la siguiente verificación el 23 de diciembre de 2024.

Nombre de la verificación	Categoría de verificación	ID de la verificación
AWS CloudTrail Registro de eventos de administración	Seguridad	c25hn9x03v

Comprueba el uso de AWS CloudTrail.

Para obtener más información, consulte [AWS CloudTrail Registro de eventos de administración](#).

Se actualizó la verificación de recursos del grupo de escalado automático

Trusted Advisor actualizó la siguiente verificación el 23 de diciembre de 2024.

Nombre de la verificación	Categoría de verificación	ID de la verificación
Recursos de grupos de Auto Scaling	Tolerancia a errores	8CNsS11I5v

La descripción de esta verificación se actualizó para incluir las configuraciones y plantillas de lanzamiento.

Se agregó un nuevo criterio de alerta, Red: A launch template is associated with a deleted Amazon Machine Image (AMI)..

Para obtener más información, consulte [Recursos de grupos de Auto Scaling](#).

Se actualizó la verificación de acceso externo de IAM Access Analyzer.

Trusted Advisor actualizó la siguiente verificación el 23 de diciembre de 2024.

Nombre de la verificación	Categoría de verificación	ID de la verificación
Acceso externo de IAM Access Analyzer	Seguridad	07602fcad6

La descripción de esta verificación se actualizó para indicar que analiza el acceso a IAM a nivel de cuenta. Para obtener más información, consulte [Acceso externo de IAM Access Analyzer](#).

Se agregó una verificación nueva.

Trusted Advisor agregó 1 cheque nuevo el 22 de noviembre de 2024:

- 8604e947f2: [grupo de seguridad del equilibrador de carga de aplicación](#)

Se actualizaron tres verificaciones

Trusted Advisor actualizó 3 controles el 7 de noviembre de 2024:

- b92b83d667: [desequilibrio entre los destinos de ELB](#)
- 8 CNsIII5v - [Recursos de Auto Scaling Group](#)
- wuy7G1zxql: [equilibrio de zona de disponibilidad de Amazon EC2](#)

Se agregaron cuatro verificaciones

Trusted Advisor se agregaron 4 nuevos controles el 11 de octubre de 2024:

- 07602fcad6: IAM Access Analyzer: acceso externo
- 528d6f5ee7: GWLB: zona de disponibilidad de punto de conexión
- c2vlfq0jp6: puntos de conexión de interfaz de VPC inactivos
- c2vlfq0k35: puntos de conexión inactivos del equilibrador de carga de la puerta de enlace

Se actualizaron tres verificaciones

Trusted Advisor actualizó 3 controles el 2 de octubre de 2024:

- El identificador de verificación 7040ea389a pasó del pilar de optimización de costos al pilar de tolerancia a errores
- ID de cheque actualizado: 7 DAFEmoDos
- ID de verificación actualizado CMSvNJ8db2

Se agregaron nueve nuevas verificaciones

Trusted Advisor se agregaron 9 cheques nuevos el 23 de agosto de 2024:

- c2vlfg0p86: [IAM]: proveedor de identidades SAML 2.0
- 7040ea389a - Transferencia de datos de terminales de Network Firewall Cross-AZ
- c2vlfg0bfbw: firewall de red de baja utilización
- c2vlfg0gqgd - Network Firewall Multi-AZ
- c2vlfg0p1w: protocolo de cifrado de grupos de destino del equilibrador de carga de aplicación
- c2vlfg022t: [Puerta de enlace NAT]: recurso infrautilizado
- c243hjzrhn: implementación en un solo AWS Outposts rack
- b92b83d667: desequilibrio entre los destinos de ELB
- 90046ff5b5: La disponibilidad de MSK está limitada a dos zonas

Para obtener más información, consulte la [AWS Trusted Advisor comprobar referencia](#).

Se actualizó un control de seguridad y se agregó un control de seguridad

Trusted Advisor se actualizaron 1 comprobaciones de excelencia operativa el 22 de agosto de 2024:

- c1fd6b96l4

Trusted Advisor se agregaron 1 control de seguridad el 22 de agosto de 2024:

- c2vlfg0f4h

Para obtener más información, consulte la [AWS Trusted Advisor comprobar referencia](#).

Se actualizaron seis controles de seguridad

Trusted Advisor actualizó 6 controles de seguridad el 20 de agosto de 2024:

- en NauJis YIT
- c9D319e7sG
- a2sEc6ILx
- HCP4007jGY
- 1iG5NDGVre
- Yw2K9puPzl

Para obtener más información, consulte la [AWS Trusted Advisor comprobar referencia](#).

Se actualizó una verificación de tolerancia a errores

Trusted Advisor actualizó 1 control de tolerancia a fallos y 1 de seguridad el 12 de agosto de 2024:

- Redundancia de túnel de VPN
- Debe efectuarse una actualización menor de la versión del motor de Amazon RDS

Para obtener más información, consulte la [AWS Trusted Advisor comprobar referencia](#).

Se actualizaron nueve verificaciones

Trusted Advisor actualizó las 9 comprobaciones el 21 de julio de 2024:

- 7q GXsKIUw
- ZRxQIPsb6c
- N425c450f2
- 7 DAFEmoDos
- Pfx0RwqBli
- H7lgTzjTYb
- C056F80cR3
- Yw2K9puPzl

- xSqX82fQu

Para obtener más información, consulte la [AWS Trusted Advisor comprobar referencia](#).

Se eliminaron cinco verificaciones y se agregó una verificación

Trusted Advisor dejó de utilizar 3 controles de tolerancia a errores, 1 control de rendimiento y 1 control de seguridad el 15 de mayo de 2024:

- Uso de IAM
- Equilibrio de carga ELB Cross-Zone
- 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 agregó 1 nuevo control de seguridad el 15 de mayo de 2024:

- Habilitación del registro de acceso al servidor de Amazon S3.

Para obtener más información, consulte la [AWS Trusted Advisor comprobar referencia](#).

Se eliminaron verificaciones de tolerancia a errores

Trusted Advisor quedó obsoleta la comprobación de tolerancia a tres fallos el 25 de abril de 2024:

- Direct Connect Redundancia de conexión
- Direct Connect Redundancia de ubicación
- Direct Connect Redundancia de interfaz virtual

Para obtener más información, consulte la [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: Internet-facing recurso en una subred privada

Para obtener más información, consulte la [AWS Trusted Advisor comprobar referencia](#).

Se actualizó una verificación de tolerancia a errores y un control de seguridad

Trusted Advisor se añadió 1 nueva comprobación de tolerancia a fallos y se modificaron 1 comprobación de tolerancia a fallos y 1 comprobación de seguridad existentes el 28 de marzo de 2024:

- Se agregó AWS Resilience Hub la verificación de componentes de la aplicación
- AWS Lambda VPC-enabled Funciones actualizadas sin Multi-AZ redundancia
- AWS Lambda Funciones actualizadas que utilizan tiempos de ejecución obsoletos

Para obtener más información, consulte la [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:

- Direct Connect Resiliencia de ubicación

Para obtener más información, consulte la [AWS Trusted Advisor comprobar referencia](#).

Verificación de tolerancia a errores actualizada

Trusted Advisor modificó 1 control de tolerancia a fallos el 8 de enero de 2024:

- El parámetro innodb_flush_log_log_at_trx_commit de Amazon RDS no es 1

Para obtener más información, consulte la [AWS Trusted Advisor comprobar referencia](#).

Controles de seguridad actualizados

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 la [AWS Trusted Advisor comprobar referencia](#).

Nuevas verificaciones de seguridad y rendimiento

Trusted Advisor se agregaron 2 nuevas comprobaciones de seguridad y 2 nuevas comprobaciones de rendimiento el 20 de diciembre de 2023:

- Los clientes de Amazon EFS no utilizan el cifrado de datos en tránsito
- El clúster de base de datos Amazon Aurora está insuficientemente aprovisionado para la carga de trabajo de lectura
- Instancia de Amazon RDS con aprovisionamiento insuficiente para la capacidad del sistema
- Instancias de Amazon EC2 con final del soporte estándar con Ubuntu LTS

Para obtener más información, consulte la [AWS Trusted Advisor comprobar referencia](#).

Nuevo control 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 buckets de S3

Para obtener más información, consulte la [AWS Trusted Advisor comprobar referencia](#).

Nuevas verificaciones de tolerancia a errores y de optimización de costos.

Trusted Advisor se agregaron 2 nuevas comprobaciones de tolerancia a fallos y 1 nueva comprobación de optimización de costes el 7 de diciembre de 2023:

- Clústeres de Amazon DocumentDB Single-AZ
- Configuración de anulación de carga multiparte incompleta de Amazon S3
- Amazon ECS AWS registra el controlador en modo de bloqueo

Para obtener más información, consulte la [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
- Interfaces de red de punto de conexión de interfaz de VPC en varias zonas de disponibilidad

Para obtener más información, consulte la [AWS Trusted Advisor comprobar referencia](#).

Nuevas verificaciones para Amazon RDS

Trusted Advisor añadió 37 cheques nuevos para Amazon RDS el 15 de noviembre de 2023.

Para obtener más información, consulte la [AWS Trusted Advisor comprobar referencia](#).

New AWS Trusted Advisor API

AWS Trusted Advisor presenta nuevas API que le permiten acceder mediante programación a las comprobaciones de mejores prácticas, las recomendaciones y las recomendaciones priorizadas de 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 gran escala. Disponibles para los clientes de Business On-Ramp, Enterprise 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 información de soporte.

Trusted Advisor Las API generalmente 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 API de AWS Trusted Advisor](#).

Trusted Advisor eliminación de cheques

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 instancias de 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 a origen	Seguridad	Hs4Ma3G195

Integración de AWS Config se registra en Trusted Advisor

Trusted Advisor se agregaron 64 cheques nuevos activados AWS Config el 30 de octubre de 2023.

Para obtener más información, consulte la [Ver AWS Trusted Advisor cheques impulsados por 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 [Desempeño](#).

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 Multi-AZ colocación 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 las siguientes comprobaciones el 30 de marzo de 2023.

- Servicio de Amazon ECS con una única zona de disponibilidad
- Estrategia de Multi-AZ colocación de Amazon ECS

Para obtener más información, consulte la categoría [Tolerancia a errores](#).

Nuevas comprobaciones de tolerancia a errores

Trusted Advisor agregó las siguientes comprobaciones el 15 de diciembre de 2022.

- AWS CloudHSM clústeres que ejecutan instancias de HSM en una única zona de disponibilidad
- ElastiCache Multi-AZ Clústeres de Amazon
- AmazonClústeres de MemoryDB Multi-AZ

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](#)

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 CSPM

Trusted Advisor realizó la siguiente actualización el 17 de noviembre de 2022.

Si inhabilita Security Hub CSPM o AWS Config para un Región de AWS, Trusted Advisor ahora elimina los hallazgos de control correspondientes en un Región de AWS plazo de 7 a 9 días. Anteriormente, el plazo para eliminar los datos de CSPM de Security Hub Trusted Advisor era de 90 días.

Para más información, consulte las siguientes secciones del tema [Resolución de problemas](#):

- [He desactivado Security Hub \(CSPM\) o AWS Config en una región](#)
- [Mi control está archivado en Security Hub \(CSPM\), pero sigo viendo los resultados en Trusted Advisor](#)

Nuevas comprobaciones de tolerancia a errores para AWS Resilience Hub

Trusted Advisor agregó las siguientes comprobaciones el 17 de noviembre de 2022.

- AWS Resilience Hub política incumplida
- AWS Resilience Hub puntuaciones 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 obtener más información, consulte la categoría [Tolerancia a errores](#).

Actualice a la Trusted Advisor consola

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 Soporte API como de costumbre.

Para obtener más información, consulte [Comience con Trusted Advisor las recomendaciones](#).

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 CSPM de Security Hub a Trusted Advisor

A partir del 23 de junio de 2022, Trusted Advisor solo es compatible con los controles CSPM de Security Hub disponibles hasta el 7 de abril de 2022. Esta versión es compatible con 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 AWS Security Hub CSPM los controles 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 CSPM .

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 costos	C0r6dfpM03
Volúmenes con falta de aprovisionamiento de Amazon EBS	Desempeño	C0r6dfpM04
AWS Lambda funciones sobrep provisionadas para el tamaño de la memoria	Optimización de costos	C0r6dfpM05
AWS Lambda funciones insuficientemente aprovisionadas para el tamaño de la memoria	Desempeño	C0r6dfpM06

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	12Fnkp18Y5

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



).

La actualización comprueba si 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 CSPM controles agregados a la AWS Trusted Advisor consola

AWS Trusted Advisor añadió 111 controles CSPM de Security Hub a la categoría Seguridad el 18 de enero de 2022.

Puede ver sus hallazgos sobre los controles CSPM 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 AWS Security Hub CSPM los controles en AWS Trusted Advisor](#).

Nuevas comprobaciones para Amazon EC2 y AWS Well-Architected

Trusted Advisor añadió 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 actualizó 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 instancia s reservadas de Amazon OpenSearch Service	Optimización de costos	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 [Crear CloudWatch alarmas de Amazon para monitorear AWS Trusted Advisor las métricas](#).

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	dH7RR016J3
Almacenamiento de volúmenes de SSD de IOPS provisionadas (io2) de EBS	Límites de los servicios	gI7MM017J2

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 costos	L4dfs2Q3C3
AWS Lambda Funciones con altas tasas de error	Optimización de costos	L4dfs2Q3C2
AWS Lambda Funciones que utilizan tiempos de ejecución obsoletos	Seguridad	L4dfs2Q4C5
AWS Lambda VPC-enabled Funciones 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	aW9HH018J6

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 [Crear CloudWatch alarmas de Amazon para monitorear AWS Trusted Advisor las métricas](#).

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	Límites de los servicios	dH7RR016J9	Almacenamiento de volúmenes de SSD

Nombre de la verificación	Categoría de verificación	ID de la verificación	CloudWatch Métrica actualizada para ServiceLimit
uso general (gp2) de EBS			de uso general (gp2) (TiB)
Almacenamiento de volúmenes magnéticos (estándar) de EBS	Límites de los servicios	cG7HH017J9	Almacenamiento de volúmenes magnéticos (estándar) (TiB)
Almacenamiento de volúmenes de SSD de IOPS provisionadas (io1) de EBS	Límites de los servicios	gI7MM017J9	Almacenamiento IOPS provisionadas (SSD) (TiB)
Almacenamiento de volúmenes de HDD con rendimiento optimizado (st1) de EBS	Límites de los servicios	wH7DD013J9	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	V77i0L1Bqz

Verificaciones eliminadas el 18 de noviembre de 2020	Categoría de verificación	ID de la verificación
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
Versión del controlador de PV para instancias de Windows de EC2	Tolerancia a errores	Wnwm9I15bG
Volúmenes activos de EBS	Límites de los servicios	fH7LL017J9

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	Desempeño	eW7HH017J9

Aplicación AWS Support en Slack

Puede usar la aplicación AWS Support para administrar sus casos de soporte de AWS en Slack. Puede invitar a los miembros de su equipo a los canales de chat, responder a las actualizaciones de los casos y chatear directamente con los agentes de soporte. Puede usar la aplicación AWS Support para administrar sus casos de soporte rápido en Slack.

Para utilizar la aplicación AWS Support, haga lo siguiente:

- Crear, actualizar, buscar y resolver casos de soporte en los canales de Slack
- Adjuntar archivos en casos de soporte
- 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 asistencia en la aplicación AWS Support, el caso también se actualiza en la 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, y soporte técnico.

Temas

- [Requisitos previos](#)
- [Autorización de un espacio de trabajo de Slack](#)
- [Configuración de un canal de Slack](#)
- [Creación de casos de soporte en un canal de Slack](#)
- [Respuesta a casos de soporte en Slack](#)
- [Únase a una sesión de chat en vivo con Soporte](#)
- [Búsqueda de casos de soporte en Slack](#)

- [Resolución de un caso de soporte en Slack](#)
- [Reapertura de un caso de soporte en Slack](#)
- [Eliminar la configuración de un canal de Slack de la aplicación AWS Support](#)
- [Eliminar una configuración de espacio de trabajo de Slack de la aplicación AWS Support](#)
- [AWS Support Comandos de la aplicación en Slack](#)
- [Vea las correspondencias de la AWS Support aplicación en el AWS Support Center Console](#)
- [Cómo crear una AWS Support aplicación en los recursos de Slack con AWS CloudFormation](#)

Requisitos previos

Debes cumplir los siguientes requisitos para usar la AWS Support aplicación en Slack:

- Tiene un plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations. 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 AWS Support planes](#).
- 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](#).
- Inicia sesión Cuenta de AWS como usuario o rol AWS Identity and Access Management (de IAM) con los permisos necesarios. Para obtener más información, consulte [Administrar el acceso al widget de AWS Support la aplicación](#).
- Deberá crear un rol de IAM que tenga los permisos necesarios para llevar a cabo acciones en su nombre. La AWS Support aplicación utiliza esta función para realizar llamadas a la API a diferentes servicios. Para obtener más información, consulte [Administrar el acceso a la AWS Support aplicación](#).

Temas

- [Administrar el acceso al widget de AWS Support la aplicación](#)
- [Administrar el acceso a la AWS Support aplicación](#)

Administrar el acceso al widget de AWS Support la aplicación

Puede adjuntar una política AWS Identity and Access Management (IAM) para conceder a un usuario de IAM permiso para configurar el widget de la AWS Support aplicación en el. 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 puedes iniciar sesión como usuario root en tu cuenta Cuenta de AWS, pero no te recomendamos que lo hagas. 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.

JSON

```
{
  "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 AWS Support aplicación a Slack

La AWS Support aplicación incluye acciones que solo requieren permisos y que no se corresponden directamente con una operación de la API. Estas acciones se indican en la [Referencia de autorización de servicio](#) con [solo permiso].

La AWS Support aplicación utiliza las siguientes acciones de la API para conectarse a Slack y, a continuación, muestra tus 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 la API no están incluidas en el AWS CLI y. AWS SDKs

Administrar el acceso a la AWS Support aplicación

Una vez que tengas permisos para acceder al widget de la AWS Support aplicación, también debes crear un rol AWS Identity and Access Management (de IAM). Esta función realiza acciones de otras Servicios de AWS por ti, como la AWS Support API 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 solicitas un chat en directo con un agente de asistencia y eliges un nuevo canal privado como canal de chat en directo preferido, la AWS Support aplicación 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 cambias la función de IAM o la política de IAM, los cambios se aplicarán al canal de Slack que hayas configurado y a todos los nuevos canales de Slack de chat en directo que la AWS Support aplicación cree para ti.

Siga estos procedimientos para crear su política y rol de IAM.

Temas

- [Usa una política AWS gestionada o crea una política gestionada por el cliente](#)
- [Creación de un rol de IAM](#)
- [Resolución de problemas](#)

Usa una política AWS gestionada o crea una política gestionada por el cliente

Para conceder los permisos a su función, puede utilizar una política AWS gestionada o una política gestionada 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 AWS Support aplicación. No es necesario actualizar las políticas manualmente. Para obtener más información, consulte [AWS políticas gestionadas para AWS Support 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 gestionada por el cliente para la AWS Support aplicación

1. Inicie sesión en la consola de IAM Consola de administración de AWS y ábrala en <https://console.aws.amazon.com/iam/>.
2. En el panel de navegación, seleccione Políticas.
3. Elija 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 Siguiente: etiquetas.
7. (Opcional) Puede usar etiquetas como pares clave-valor para agregar metadatos a la política.
8. Elija 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 necesarios para realizar todas las acciones necesarias para la AWS Support aplicación. Después de configurar un canal de Slack con el rol, todos los usuarios de su canal tendrán los mismos permisos.

Note

Para obtener una lista de las políticas AWS administradas, consulte [AWS políticas gestionadas para AWS Support Aplicación en Slack](#).

Puede actualizar la política para eliminar un permiso de la AWS Support aplicación.

JSON

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

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 condición para AWS Identity and Access Management](#)

Creación de 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 AWS Support aplicación

1. Inicie sesión en la consola de IAM Consola de administración de AWS y ábrala en <https://console.aws.amazon.com/iam/>.
2. En el panel de navegación, seleccione Roles y luego seleccione Crear rol.
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 AWS gestionada o elegir una política gestionada por el cliente que haya creado, por ejemplo, *AWSSupportAppRolePolicy* A continuación, seleccione la casilla situada junto a la política.
7. Elija Siguiente: etiquetas.
8. (Opcional) Puede usar etiquetas como valores clave-valor para agregar metadatos al rol.
9. Elija 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 Crear rol. 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 [Crear un rol para un AWS servicio](#) en la Guía del usuario de IAM.

Resolución de problemas

Consulte los siguientes temas para gestionar el acceso a la AWS Support aplicación.

Contenido

- [Quiero restringir acciones específicas a usuarios específicos de mi canal de Slack](#)
- [Cuando configuro un canal de Slack, no veo el rol de IAM que he creado](#)
- [A mi rol de IAM le falta un permiso](#)
- [Un error de Slack indica que mi rol de IAM no es válido](#)
- [La AWS Support aplicación dice que me falta un rol de IAM para Service Quotas](#)

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 usuario del canal tiene acceso de lectura o escritura a tus casos de soporte, tenga o no un Cuenta de AWS usuario de IAM.

Recomendamos que siga las siguientes prácticas recomendadas:

- Configura los 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 Aplicación en Slack](#).

Cuando configuro un canal de Slack, no veo el rol de IAM que he creado

Si tu función de IAM no aparece en la función de IAM de la lista de AWS Support aplicaciones, significa que la función no tiene a la AWS Support aplicación como entidad de confianza o que la función se ha eliminado. Puede actualizar el rol actual o crear otro. Consulte [Creación de 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 AWS Support aplicación asume esta función para realizar estas acciones en tu nombre.

Si recibe un error sobre la falta de un permiso de la AWS Support aplicación, compruebe que la política asociada a su función cuente con el permiso necesario.

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 AWS Support Center Console en 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 AWS Support aplicación dice 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. Luego, puedes usar la AWS Support aplicación para solicitar aumentos de cuota 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 [Política de IAM de ejemplo](#) permite a la AWS Support aplicación crear el rol Service Quotas por usted.

```
{
  "Effect": "Allow",
  "Action": "iam:CreateServiceLinkedRole",
  "Resource": "*",
  "Condition": {
    "StringEquals": {"iam:AWSServiceName": "servicequotas.amazonaws.com"}
  }
}
```

Si eliminas el rol de IAM que configuraste para tu canal, debes crearlo manualmente o actualizar la política de IAM para que la AWS Support aplicación pueda crear uno para ti.

Autorización de un espacio de trabajo de Slack

Una vez que autorices tu espacio de trabajo y des permiso a la AWS Support aplicación para acceder a él, necesitarás un rol AWS Identity and Access Management (de IAM) para ti. Cuenta de AWS La AWS Support aplicación utiliza esta función para llamar a las operaciones de la API [AWS](#)

[Supporty](#) a [Service Quotas](#) en su nombre. Por ejemplo, la AWS Support aplicación usa el rol para llamar a la CreateCase operación y crear un caso de soporte para ti en Slack.

Notas

- El canal de Slack hereda los permisos del rol de IAM. Todos los usuarios del canal de Slack tienen los mismos permisos que se especifican en la política de IAM asociada al rol. Por ejemplo, si su política de IAM concede 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 ven 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 tienes varias Cuentas de AWS, debes 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 tu 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 que solicita permiso para acceder a la página de your-workspace-name Slack, selecciona Permitir.

 Note

Si no puedes permitir que Slack acceda a tu espacio de trabajo, asegúrate de tener los permisos de tu administrador de Slack para añadir la AWS Support aplicación 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, tu número de Cuenta de AWS identificación aparece como nombre de cuenta en tu 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 AWS Support aplicación usa este nombre para identificar tu cuenta en el canal de Slack. Puede actualizar este nombre en cualquier momento.

Edit account name ✕

Choose an account name that you can easily recognize in Slack. This name won't appear in your AWS account settings.

Account name

aws-administrator-account

Maximum 30 characters (5 remaining)

Example Usage:

Account name being used by Support Slack App Bot

- **AWS account:** aws-administrator-account (ID: 123456789012)

Cancel Save

Su espacio de trabajo y el nombre de la cuenta aparecen en la página Slack configuration (Configuración de Slack).

Slack configuration

Workspaces

Delete Authorize workspace Add multiple accounts ↺

Workspace

troubleshooting

Account name

Delete Edit

Name used in Slack

aws-administrator-account

Autorización de varias cuentas

Si tu cuenta pertenece a una organización de AWS Organizations, puedes autorizar a varias Cuentas de AWS para que usen el mismo espacio de trabajo de Slack. Puedes usar AWS CloudFormation plantillas para automatizar este proceso o puedes configurar manualmente cada cuenta mediante la API de la AWS Support aplicación.

Usa AWS CloudFormation plantillas

Puedes usar [AWS CloudFormationTerraform](#) para crear los recursos de tu AWS Support aplicación en varias cuentas. Este es el enfoque recomendado para gestionar varias cuentas a gran escala.

Para obtener más información, consulte [Cómo crear una AWS Support aplicación en los recursos de Slack con AWS CloudFormation](#).

Usa la API de AWS Support la aplicación

Si prefieres no usar AWS CloudFormation plantillas, puedes autorizar manualmente varias cuentas mediante la API de la AWS Support aplicación. Completa los siguientes pasos para cada cuenta de miembro que quieras añadir al espacio de trabajo de Slack.

Para autorizar manualmente varias cuentas

1. En la cuenta de administración (la cuenta en la que creaste el espacio de trabajo de Slack), autoriza el espacio de trabajo de Slack. Para obtener más información, consulta el procedimiento en [Autorización de un espacio de trabajo de Slack](#)
2. En cada cuenta de miembro, llama a la operación de [RegisterSlackWorkspaceForOrganization](#)API para registrar el espacio de trabajo de Slack de esa cuenta.

Esta operación añade la cuenta del miembro al espacio de trabajo de Slack que fue autorizada por la cuenta de administración.

3. En cada cuenta de miembro, crea un rol de IAM con los permisos necesarios para la AWS Support aplicación. Para obtener más información, consulte [Administrar el acceso a la AWS Support aplicación](#).
4. En cada cuenta de miembro, llama a la operación de la [CreateSlackChannelConfiguration](#)API para configurar un canal de Slack para esa cuenta.

Esta operación asocia el canal de Slack a la cuenta del miembro y especifica la función de IAM que la AWS Support aplicación utiliza para las llamadas AWS Support y las operaciones de Service Quotas.

 Note

Cada cuenta de miembro debe formar parte de la misma organización que la cuenta de AWS Organizations administración que autorizó el espacio de trabajo de Slack.

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 .

En el canal en el que invites y AWS Support añadas la aplicación, puedes crear y buscar casos y recibir notificaciones de casos. Este canal muestra actualizaciones de casos, incluidos los creados recientemente o los resueltos, correspondencias agregadas y detalles de casos compartidos.

El canal de Slack hereda los permisos del rol de IAM. Todos los usuarios del canal de Slack tienen los mismos permisos que se especifican en la política de IAM asociada al rol. Por ejemplo, si su política de IAM concede 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 ven los casos de soporte.

Puedes añadir hasta 20 canales por canal Cuenta de AWS. Cada canal de Slack admite hasta 100 Cuentas de AWS. Esto significa que solo 100 cuentas pueden agregar el mismo canal de Slack a la aplicación AWS Support . Para minimizar las distracciones, se recomienda añadir solo las cuentas necesarias para administrar los casos de soporte de su organización.

Cada uno Cuenta de AWS debe configurar un canal de Slack por separado en la AWS Support aplicación. De esta forma, la AWS Support aplicación puede acceder a los casos de soporte que Cuenta de AWS contiene. Si otro miembro Cuenta de AWS de tu organización ya ha invitado a la AWS Support aplicación a ese canal de Slack, continúa con el 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 Cuenta de AWS puede usar la AWS Support aplicación. La

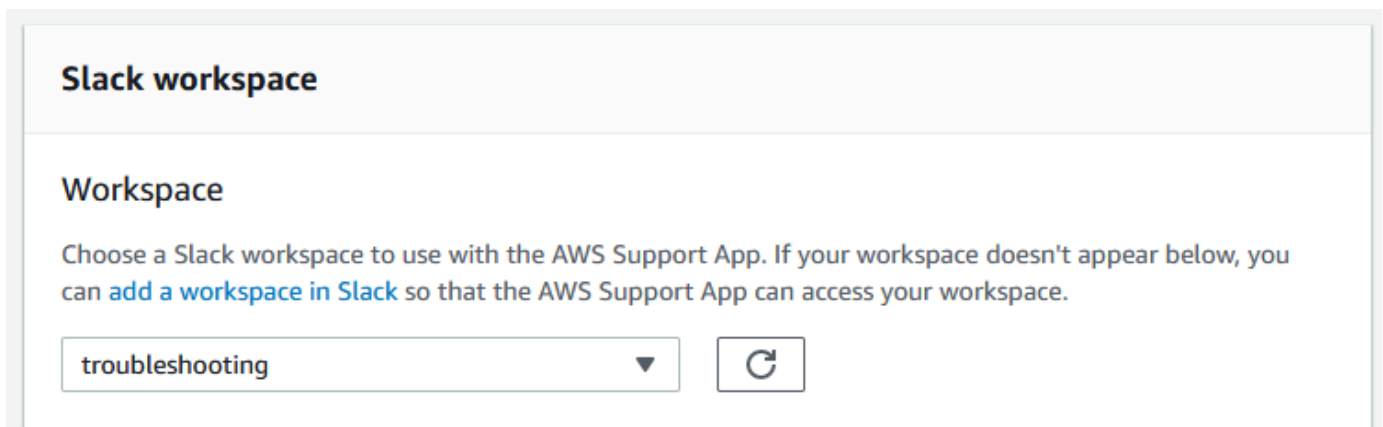
AWS Support aplicación muestra un mensaje de error si intentas configurar el mismo canal de Slack para otro espacio de trabajo.

Para configurar un canal de Slack

1. Desde tu aplicación de Slack, elige el canal de Slack que quieres usar con la aplicación. AWS Support
2. Completa los siguientes pasos para invitar a la AWS Support aplicación a tu canal:
 - a. Abra el menú contextual (haga clic con el botón derecho) en el nombre de canal y elija Ver detalles del canal.
 - b. Seleccione la pestaña Integraciones y, a continuación, seleccione Añadir una aplicación.
 - c. Para buscar la aplicación, ingrese aplicación AWS Support .
 - d. 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.
 - Privado: en el ID del canal, introduce el ID o la URL del canal de Slack al que has invitado a la AWS Support aplicación.

 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 tu canal es el valor que aparece.

C01234A5BCD

7. En Nombre de la configuración del canal, introduce un nombre que identifique fácilmente la configuración de tu canal de Slack para la AWS Support aplicación. Este nombre solo aparece en la tuya 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.

▼ Slack channel

Channel Type

- ☐ Public
Choose a public channel from the list.
- ☒ Private
A channel member must invite a user to join or view.

Channel ID

Channel configuration name

Choose a name that you can easily identify. You can change the name at any time.



Tip

Tip To find the channel ID, right-click your channel name in Slack, choose **Copy** and then choose **Copy link**. Your channel ID is the value that looks like **C01234A5BCD**.

8. En Permisos, en la sección «Función de IAM» de la AWS Support aplicación en Slack, elige una función que hayas creado para la aplicación. AWS Support En la lista solo aparecen los roles en los que la AWS Support aplicación es una entidad de confianza.

▼ Permissions

IAM role for the AWS Support App

Choosing another IAM role for this Slack channel configuration can affect the permissions for any chat channels created from this troubleshooting channel. You can verify that your role has the required permissions. [Learn more](#)



 Note

Si no ha creado ningún rol o no lo ve en la lista, consulte [Administrar el acceso a la AWS Support aplicación](#).

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 [Elegir un nivel de gravedad inicial para el caso de soporte](#).
 - 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.

▼ Notifications

Additional case notifications
Choose when to get notified for cases created and updated.

☒ All cases

☐ High-severity cases

☐ None

Notification types
Get notified for the following types of cases that are created.

☒ New and reopened cases

☒ Case correspondences

☒ Resolved cases

Note: You will receive notifications in your Slack channel for all case updates for this account.

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 **channelName** página, puedes realizar las siguientes tareas:
 - Elegir Rename (Renombrar) para actualizar el nombre de la configuración de su canal. Este nombre solo aparece en tu página Cuenta de AWS y no aparecerá en Slack.
 - Selecciona Eliminar para eliminar la configuración del canal de la AWS Support aplicación. Consulte [Eliminar 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. Proporciona detalles, como la forma en que utilizas un Servicio de AWS y los pasos de solución de problemas que has seguido.

aws **Create a support case**

Step 1 of 3

You can create a case with AWS Support for technical and account-related issues.

AWS account

dev-ops-production (ID:123456789012)

Subject

AWS resources issue

Description

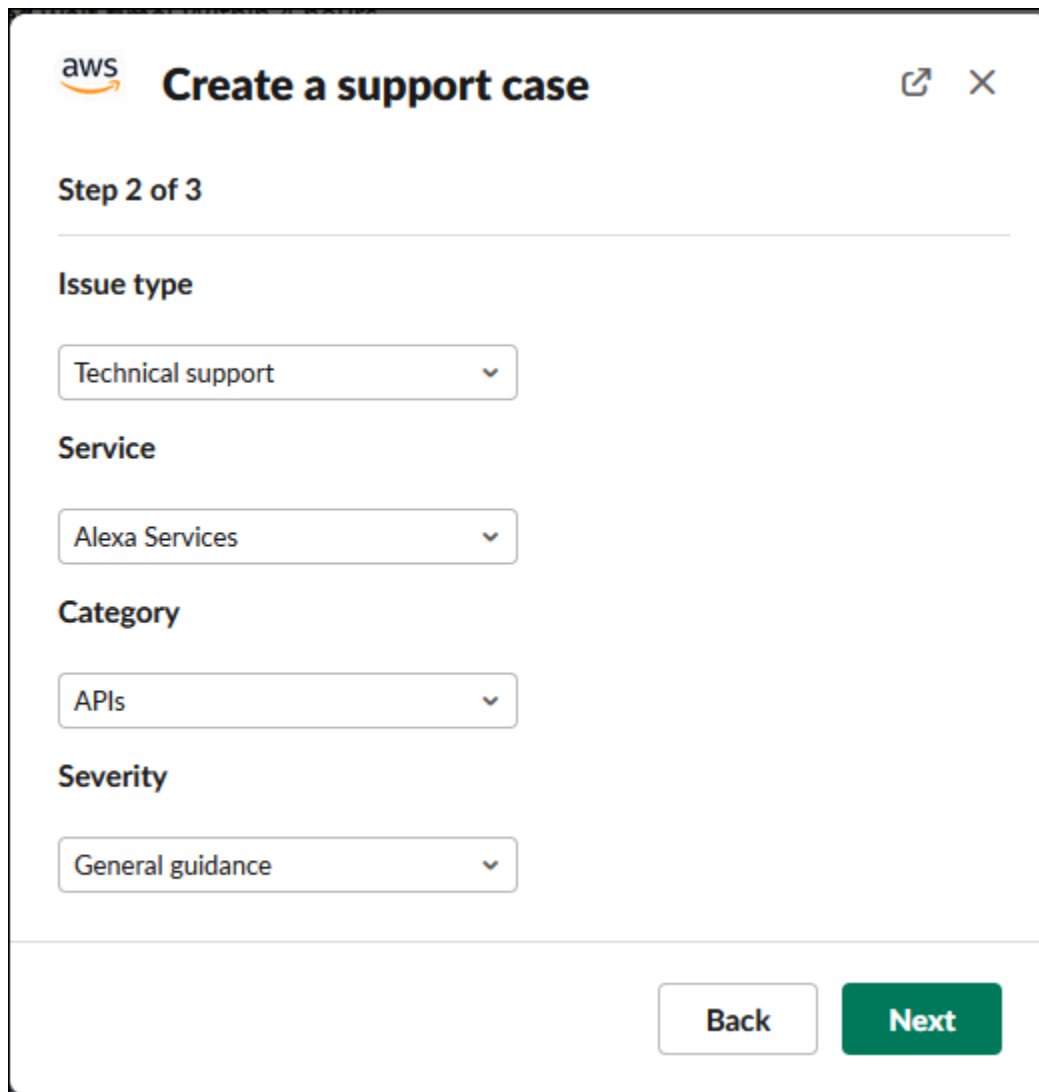
I can't find my resource in my AWS account. 2457

Note: You can add attachments after step 3 when you confirm the case.

Cancel Next

3. Elija 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.



The screenshot shows the 'Create a support case' interface in the AWS Support console. It is titled 'Step 2 of 3'. The form contains four dropdown menus: 'Issue type' set to 'Technical support', 'Service' set to 'Alexa Services', 'Category' set to 'APIs', and 'Severity' set to 'General guidance'. At the bottom right, there are two buttons: 'Back' and 'Next'.

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.

 **Create a support case** ×

Step 3 of 3

Contact language

English ▼

Contact method

☒ Live chat in Slack

☐ Email and Slack notifications

Live chat channel preference

New private channel ▼

 A new channel will be created for your live chat session, and anyone who is invited to the channel can see previous chat history.

Additional chat members (optional)

Add chat members

You will be added to the live chat automatically.

Back

Review

- a. Si elige Chat en vivo en Slack, elija Canal privado nuevo o Canal actual como Canal de chat en vivo de preferencia. El nuevo canal privado creará un canal privado independiente para que puedas chatear con el AWS Support agente, y el canal actual utilizará un hilo en el canal actual para que puedas charlar con el AWS Support agente.
- b. (Opcional) Si elige Live chat in Slack (Chat en vivo en Slack), puede ingresar los nombres de otros miembros de Slack. En el caso del nuevo canal privado, la AWS Support aplicación te añadirá automáticamente a ti y a los miembros seleccionados al nuevo canal. En el canal actual, la AWS Support aplicación te etiquetará automáticamente a ti y a los miembros seleccionados en el hilo de chat cuando el AWS Support agente 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 inicias una nueva sesión de chat en directo para un caso de asistencia existente, la AWS Support aplicación utilizará el mismo canal o hilo de chat que se utilizó en un chat en directo anterior. La AWS Support aplicación también utiliza la misma preferencia de canal de chat en directo 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 Revisar.
9. En el canal de Slack, revise los detalles del caso. Se 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

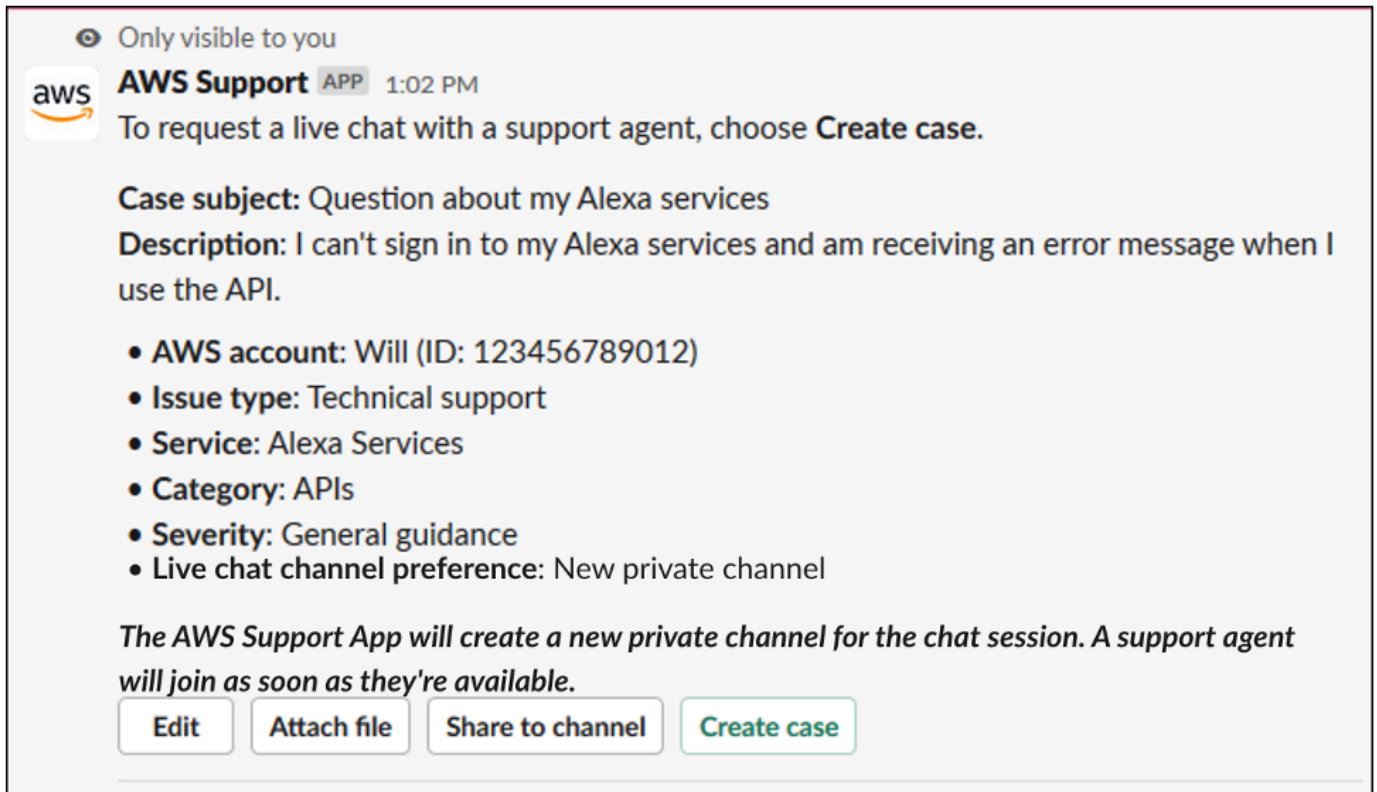
- Puede adjuntar hasta tres archivos. Cada archivo puede ser de hasta 5 MB.

- 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.



Only visible to you

 **AWS Support** APP 1:02 PM

To request a live chat with a support agent, choose **Create case**.

Case subject: Question about my Alexa services

Description: I can't sign in to my Alexa services and am receiving an error message when I use the API.

- **AWS account:** Will (ID: 123456789012)
- **Issue type:** Technical support
- **Service:** Alexa Services
- **Category:** APIs
- **Severity:** General guidance
- **Live chat channel preference:** New private channel

The AWS Support App will create a new private channel for the chat session. A support agent will join as soon as they're available.

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 Resolver 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 puedes utilizarla AWS Support Center Console para responder a los agentes de asistencia. Para obtener más información, consulte [Experiencia tradicional: actualización, resolución y reapertura de su caso](#).
- No puede añadir correspondencias a los casos desde los canales de chat creados por la AWS Support aplicación. 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

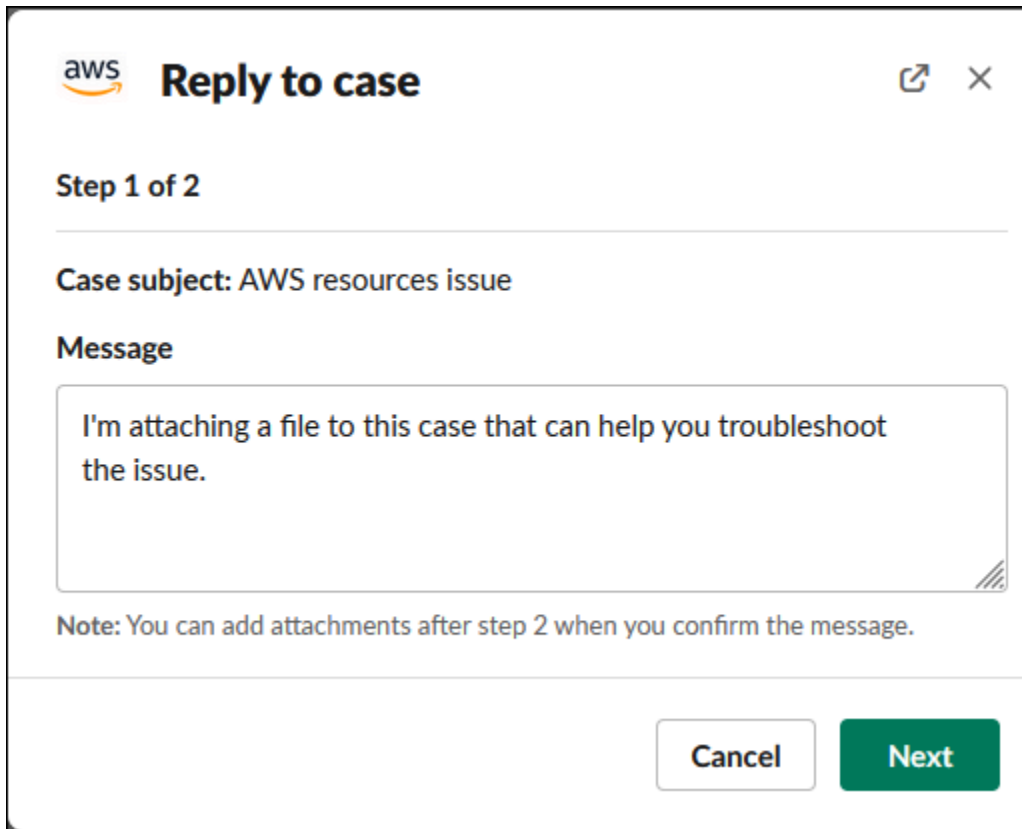
1. En su canal de Slack, elija el caso al que quiere responder. Puede ingresar `/awssupport search` para encontrar su caso de soporte.
2. Elija See details (Ver detalles) junto al caso que quiere revisar.
3. En la parte inferior de los detalles del caso, elija Reply (Responder).

Share to channel

Reply

Resolve case

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 Siguiente.



The screenshot shows a modal dialog titled "aws Reply to case" with a close button (X) and a share icon. It is labeled "Step 1 of 2". The "Case subject" is "AWS resources issue". The "Message" field contains the text: "I'm attaching a file to this case that can help you troubleshoot the issue." Below the message field is a note: "Note: You can add attachments after step 2 when you confirm the message." At the bottom right are "Cancel" and "Next" buttons.

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 Revisar. 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

 Only visible to you

 **AWS Support** APP 10:53 AM

To respond to this case, review and then choose **Send message**.

Case subject: AWS resources issue
Message: I'm attaching a file to this case that can help you troubleshoot the issue.

We will contact you by email and Slack notifications within 24 hours.

Additional contacts to notify: None

Edit Attach file Share to channel Send message

Attachments: error-log

Delete files

✓ You successfully attached 1 file. Choose **Create case** within 1 hour to include the file with your case.

Únase a una sesión de chat en vivo con Soporte

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 que solo se agreguen usuarios que requieran acceso a sus casos de soporte. Cualquier miembro de un canal o un hilo de chat también puede participar en un chat activo.

Note

Los canales y los hilos de chat en vivo también reciben notificaciones cuando se agregue una correspondencia al caso fuera de la sesión de chat en vivo. Esto ocurre antes, durante y después de una sesión de chat, de modo que puede utilizar un canal o un hilo de chat para

monitorear todas las actualizaciones relacionadas con un caso. Si eliges usar un nuevo canal de chat, usa el canal de configuración al que invitaste a la AWS Support aplicación para responder a estas correspondencias.

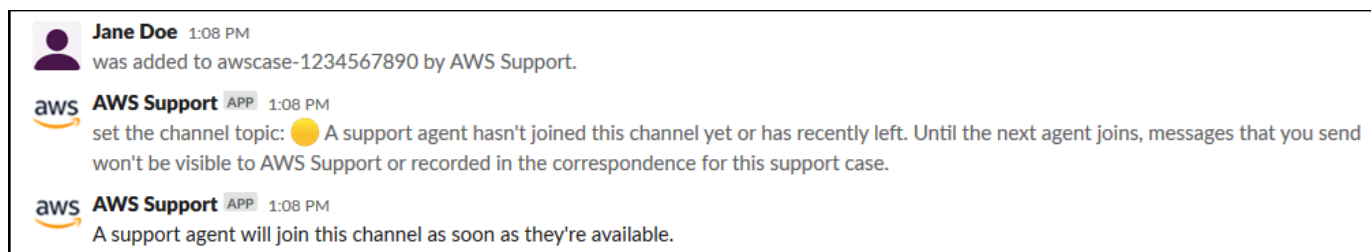
Para unirse a una sesión de chat en vivo Soporte en un canal nuevo

1. En la aplicación de Slack, navega hasta el canal que la AWS Support aplicación cree para ti. El nombre del canal incluye el identificador de tu caso de asistencia, 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 soporte no se una al canal, el agente no verá los mensajes en el chat y los mensajes no aparecerán en la correspondencia de su 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 tus archivos y el registro de chat en la correspondencia que recibas sobre el caso.

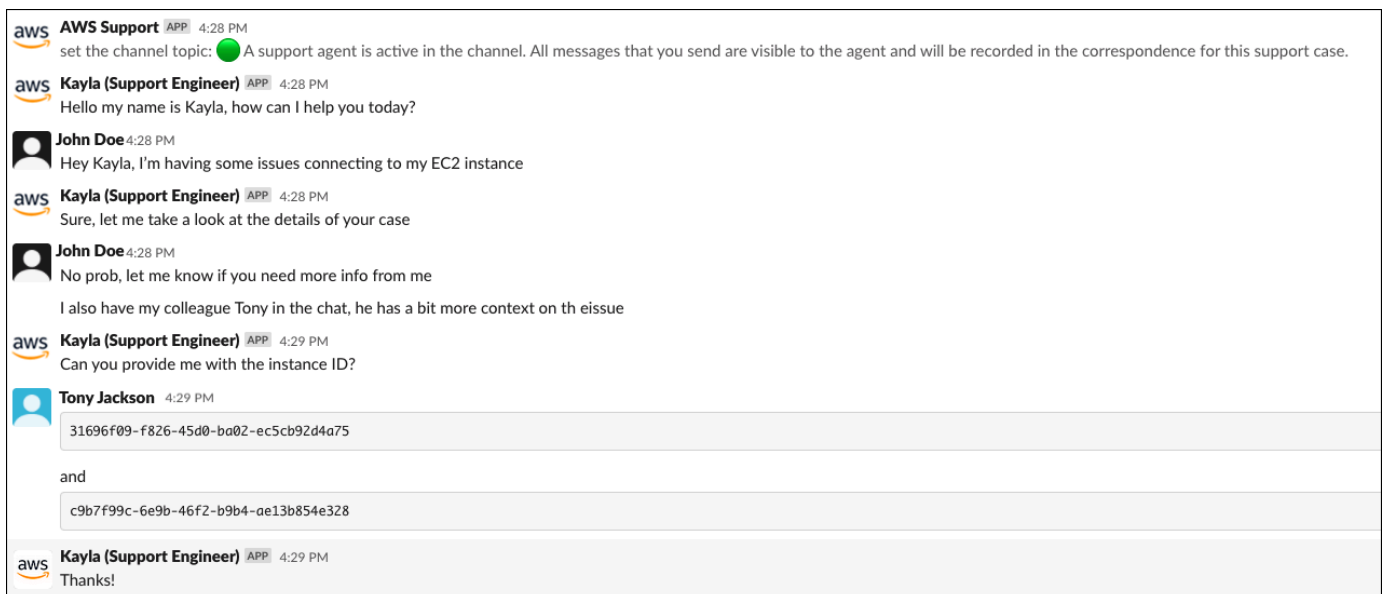
 Note

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).



aws **AWS Support** APP 4:28 PM
set the channel topic:  A support agent is active in the channel. All messages that you send are visible to the agent and will be recorded in the correspondence for this support case.

aws **Kayla (Support Engineer)** APP 4:28 PM
Hello my name is Kayla, how can I help you today?

 **John Doe** 4:28 PM
Hey Kayla, I'm having some issues connecting to my EC2 instance

aws **Kayla (Support Engineer)** APP 4:28 PM
Sure, let me take a look at the details of your case

 **John Doe** 4:28 PM
No prob, let me know if you need more info from me
I also have my colleague Tony in the chat, he has a bit more context on th eissue

aws **Kayla (Support Engineer)** APP 4:29 PM
Can you provide me with the instance ID?

 **Tony Jackson** 4:29 PM
31696f09-f826-45d0-ba02-ec5cb92d4a75
and
c9b7f99c-6e9b-46f2-b9b4-ae13b854e328

aws **Kayla (Support Engineer)** APP 4:29 PM
Thanks!

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.



 **AWS Support** APP 2:33 PM

This is a live chat channel for the following case.

Case subject: Cannot connect to ec2 instance (Case ID: 6887208841)

Description: The ec2 instance i-09f00da444 was unable to lookup our dns region. We had full access yesterday. Now we get "Access denied" message.

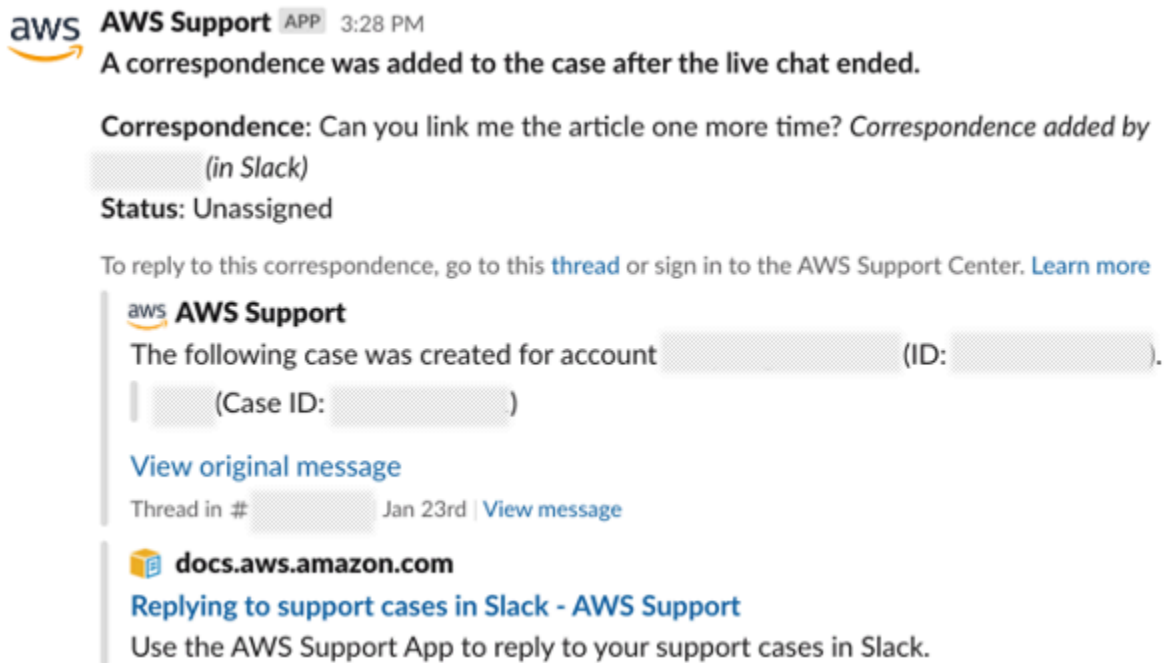
Case created by Jane Doe (in Slack)

- **Status:** Unassigned
- **Created:** 02/16/2021, 2:33PM PST
- **AWS account:** Instance Management (ID: 111122223333)
- **Issue type:** Technical support
- **Service:** Elastic Compute Cloud (EC2-Linux)
- **Category:** SSH Issue
- **Severity:** Production system impaired

End chat Resolve case

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 Soporte 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 enviados a este canal fuera del hilo de chat nunca se ven Soporte, ni siquiera cuando el chat está activo.

Thread aws-support-communications**AWS Support** APP < 1 minute ago

The following case was created for account [REDACTED].

Question about my Alexa services (Case ID: [REDACTED])

A support agent hasn't joined this chat session yet or has recently left

[Get updates](#)[See details](#)[End chat](#)[Reply](#)[Resolve case](#)

7 replies

**AWS Support** APP < 1 minute ago

@Jane Doe requested a chat for this case.

Question about my Alexa services (Case ID: [REDACTED])**AWS Support** APP < 1 minute ago

A support agent will join this chat session as soon as they're available.

**Tip:** Editing and deleting messages is not supported during the chat session. Support agents will still see original messages.

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 está activo 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.

Thread  aws-support-communications

 **AWS Support** APP < 1 minute ago

The following case was created for account .

Question about my Alexa services (Case ID: )

 A support agent hasn't joined this chat session yet or has recently left

[Get updates](#) [See details](#) [End chat](#) [Reply](#) [Resolve case](#)

7 replies

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.

👁 Only visible to you

 **AWS Support** APP 1:07 PM

Search for cases created by account **aws-administrator-account** (ID: 123456789012).

I want to search for cases by:

☒ Filter options

☐ Case ID

Date range:

Case status:

Case created in:

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 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.

 Only visible to you

 **AWS Support** APP 1:51 PM

3 results found for cases created from 10/01/2022 to 12/28/2022 with AWS account aws-administrator-account (ID:123456789012).

Case subject: Can't retrieve info about my certificate (Case ID: 1234567890)

Created: 10/25/2022, 10:30 PM UTC

Status: Resolved

[See details](#)

Case subject: Question about my AWS account bill (Case ID: 4445556660)

Created: 10/14/2022, 7:35 PM UTC

Status: Resolved

[See details](#)

Case subject: Technical support for EC2 instances (Case ID: 9087654321)

Created: 10/13/2022, 2:28 PM UTC

Status: In progress

[See details](#)

[Edit Search](#) [Share to channel](#)

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).

 Only visible to you

This case was created on 10/14/2022, 10:30 PM UTC.

Case subject: Question about my AWS account bill (Case ID: 4445556660)

Description: I have a question about a charge for my last statement

- **Status:** Resolved
- **AWS account:** aws-administrator-account (ID: 123456789012)
- **Issue type:** Account and billing support
- **Service:** Academy
- **Category:** Account/Lab access issue
- **Severity:** General question
- **Language:** English

Correspondence:

Amazon Web Services, 10/25/2022, 10:30 PM UTC

This case has been resolved. Please contact us again if you need further assistance.

Share to channel

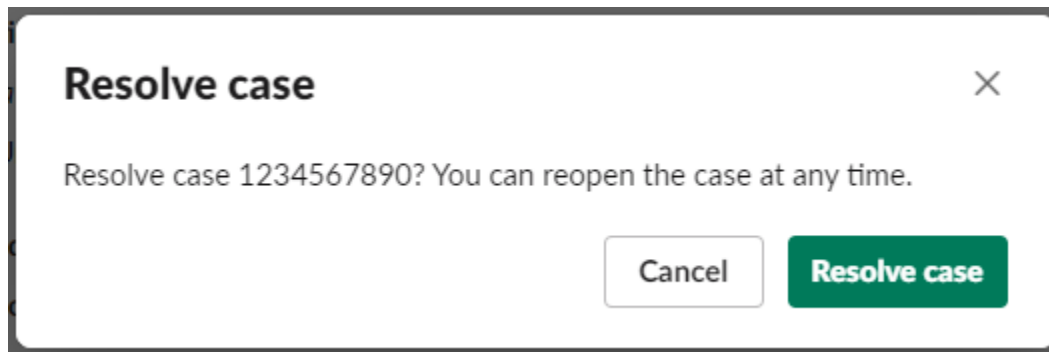
Reopen case

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 Resolver 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.

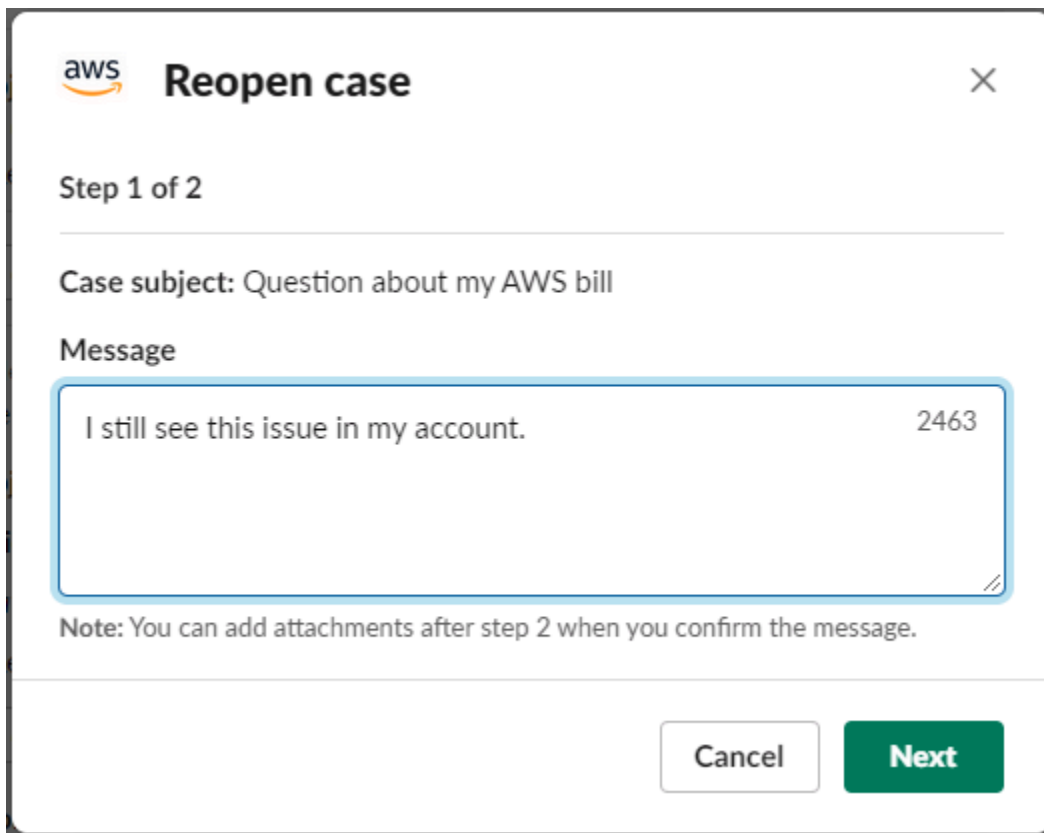


Reapertura de un caso de soporte en Slack

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 Siguiente.



aws Reopen case X

Step 1 of 2

Case subject: Question about my AWS bill

Message

I still see this issue in my account. 2463

Note: You can add attachments after step 2 when you confirm the message.

Cancel Next

6. (Opcional) Ingrese contactos adicionales.
7. Elija Revisar.
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.

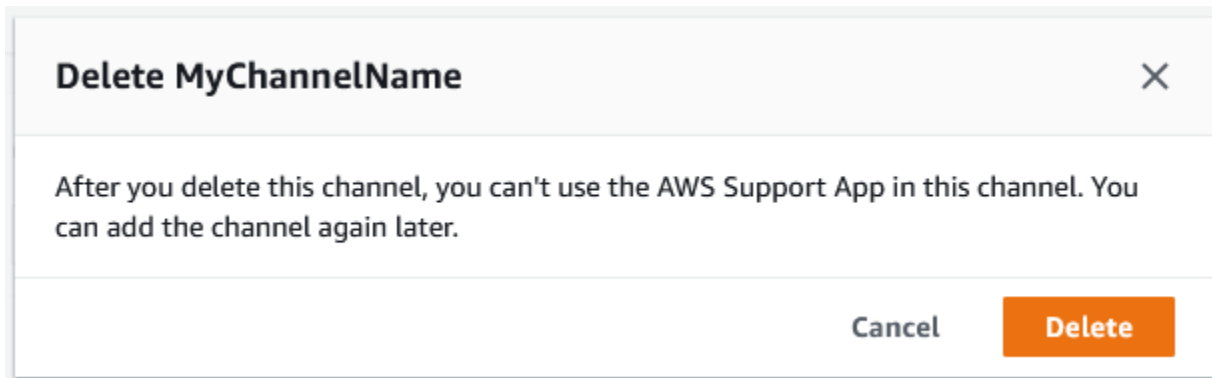
Eliminar la configuración de un canal de Slack de la aplicación AWS Support

Puedes eliminar la configuración de un canal de la AWS Support aplicación si no la necesitas. Esta acción solo elimina el canal de la AWS Support aplicación y del 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 añadir este canal a la AWS Support aplicación más adelante.



Eliminar una configuración de espacio de trabajo de Slack de la aplicación AWS Support

Puedes eliminar una configuración de espacio de trabajo de la AWS Support aplicación si no la necesitas. Esta acción solo elimina el espacio de trabajo de la AWS Support aplicación y del AWS Support Center Console. Su espacio de trabajo no se elimina de Slack.

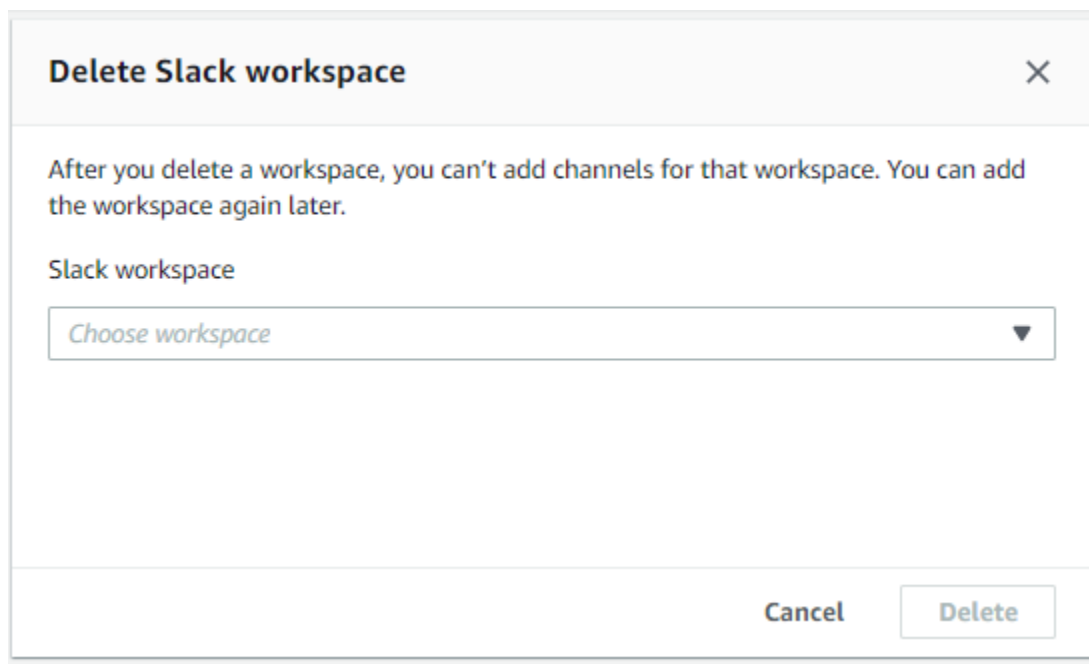
Puede agregar hasta 5 espacios de trabajo en su Cuenta de AWS. Si ya alcanzó esta cuota, debe eliminar un espacio de trabajo de Slack antes de agregar otro.

Note

Si ha agregado canales de este espacio de trabajo a la AWS Support aplicación, primero debe eliminar estos canales antes de poder eliminar el espacio de trabajo. Consulte [Eliminar 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). Puedes Cuenta de AWS volver a añadir el espacio de trabajo a tu cuenta más adelante.



AWS Support Comandos de la aplicación 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. Puedes buscar casos de asistencia para aquellos Cuentas de AWS que configuraron la AWS Support aplicación 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 AWS Support aplicación crea para ti si eliges un nuevo canal para chatear Soporte. Los canales de chat incluyen el identificador de tu caso de asistencia, como *aws-case-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.

Vea las correspondencias de la AWS Support aplicación en el 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.

Correspondence	
MyIAMRole (Role) Thu Feb 24 2022 09:09:33 GMT-0800 (Pacific Standard Time)	I am having difficulty retrieving information about my certificates. _Case created by JaneDoe (in Slack)_

Cómo crear una AWS Support aplicación en los recursos de Slack con AWS CloudFormation

AWS Support La aplicación de Slack viene integrada con AWS CloudFormation un servicio que te ayuda a modelar y configurar tus AWS recursos para que puedas dedicar menos tiempo a crear y gestionar tus recursos e infraestructura. Creas una plantilla que describe todos los AWS recursos que desees (como los tuyos AccountAlias y los tuyos SlackChannelConfiguration), y los CloudFormation aprovisiona y configura automáticamente.

Cuando la utilices CloudFormation, podrás reutilizar la plantilla para configurar los recursos de la AWS Support aplicación de forma coherente y repetida. Describa sus recursos una vez y, a continuación, aprovisiona los mismos recursos una y otra vez en varias Cuentas de AWS regiones.

AWS Support Aplicación y CloudFormation plantillas

Para aprovisionar y configurar recursos para AWS Support la aplicación y los servicios relacionados, debe conocer [CloudFormation las plantillas](#). Las plantillas son archivos de texto con formato JSON o YAML. Estas plantillas describen los recursos que desea aprovisionar en sus CloudFormation pilas. Si no estás familiarizado con JSON o YAML, puedes usar CloudFormation Designer para ayudarte a empezar con CloudFormation las plantillas. Para obtener más información, consulta [¿Qué es CloudFormation Designer?](#) en la Guía AWS CloudFormation del usuario.

AWS Support La aplicación permite crear tu AccountAlias propio y SlackChannelConfiguration en CloudFormation. Para obtener más información, incluidos ejemplos de plantillas JSON y YAML para SlackChannelConfiguration los recursos AccountAlias y los recursos, consulta la [referencia sobre los tipos de recursos de la AWS Support aplicación](#) en la Guía del AWS CloudFormation usuario.

Creación de recursos de configuración de Slack para su organización

Puedes usar CloudFormation plantillas para crear los recursos que necesitas para la AWS Support aplicación. 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, puedes usar una plantilla para crear la misma configuración de espacio de trabajo de Slack para todas las cuentas de la organización, pero luego usar plantillas independientes para crear diferentes configuraciones de canales de Slack para unidades organizativas Cuentas de AWS o específicas ()OUs. 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.

Puedes elegir si quieres usar CloudFormation plantillas o no. Si no utiliza plantillas de CloudFormation , puede completar los siguientes pasos manuales en su lugar:

- Cree los recursos de la AWS Support aplicación en AWS Support Center Console.
- Llame a la operación de la API [RegisterSlackWorkspaceForOrganization](#) para registrar un espacio de trabajo de Slack para su cuenta. La CloudFormation pila llama a esta operación de API por ti.
- Cree un rol de IAM con los permisos necesarios para cada cuenta de miembro.
- Llama a la operación de la [CreateSlackChannelConfiguration](#)API para configurar un canal de Slack para cada cuenta de miembro.

Para ver los pasos manuales detallados, consulta [Autorización de varias cuentas](#).

Siga estos procedimientos para cargar la CloudFormation plantilla en su organización. Puede utilizar las plantillas de ejemplo de la [página de referencia del tipo de origen de la aplicación AWS Support](#).

Las plantillas indican CloudFormation que hay que crear 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 `AWSSupportAppFullAccess` AWS gestionada.

Contenido

- [Actualiza tus CloudFormation plantillas para Slack](#)
- [Cree una pila para la cuenta de administración](#)
- [Creación de un conjunto de pilas para su organización](#)

Actualiza tus CloudFormation plantillas 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 AccountAlias recurso identifica de forma exclusiva a un Cuenta de AWS usuario en la AWS Support aplicación. 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 tus CloudFormation plantillas de Slack

1. Si eres la cuenta de administración de una organización, debes autorizar manualmente un espacio de trabajo de Slack para tu cuenta antes de que las cuentas de tus miembros puedan usarlo 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 el espacio de trabajo y el canal IDs, abre tu 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/T012ABCDEFGH/C01234A5BCD`, T012ABCDEFGH 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 necesitas subir la plantilla de configuración del canal de Slack, a menos que también estés configurando la cuenta de administración para usar la AWS Support aplicación.

Para crear una pila para la cuenta de administración

1. Inicia sesión Consola de administración de AWS como cuenta de administración de tu organización.
2. Abre la CloudFormation consola en <https://console.aws.amazon.com/cloudformation>.
3. Si aún no lo ha hecho, en el selector de regiones, elija una de las siguientes opciones: 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 CloudFormation](#).

Una vez que haya creado CloudFormation correctamente la pila, puede usar 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 usar conjuntos de pilas para crear la pila para toda la organización o especificar la OUs 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 Consola de administración de AWS la cuenta de administración de su organización.
2. Abre la CloudFormation consola en <https://console.aws.amazon.com/cloudformation>.
3. Si aún no lo ha hecho, en el selector de regiones, elija el mismo Región de AWS que utilizó en el procedimiento anterior.
4. En el panel de navegación, elija StackSets.
5. Seleccione 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 Especificar StackSet detalles, introduzca un nombre de pila, por ejemplo **support-app-slack-workspace**, introduzca una descripción y, a continuación, seleccione Siguiente.
10. En la página Configurar StackSet opciones, mantenga las opciones predeterminadas y, a continuación, seleccione 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 el caso de los objetivos de despliegue, elija si desea crear la pila para toda la organización o para una organización específica OUs. Si elige una OU, introduzca el ID de la OU.
13. En Especificar regiones, introduzca solo una de las siguientes opciones 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)

 Notas:

- Para agilizar el flujo de trabajo, le recomendamos que utilice el mismo Región de AWS que eligió en el paso 3.
- Elegir más de uno Región de AWS puede provocar conflictos a la hora de crear la pila.

14. En las opciones de despliegue y en la opción Tolerancia a errores (opcional), introduzca el número de cuentas en las que las pilas pueden fallar antes de que CloudFormation se 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 la operación CloudFormation falle 9 veces, al menos una cuenta se ejecutará correctamente.
15. Elija 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 AWS administrada. Este rol tiene los permisos necesarios para acceder a otros servicios en su nombre. Para obtener más información, consulte [Administrar el acceso a la AWS Support aplicación](#).

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](#).

Una vez CloudFormation creadas las pilas, cada cuenta de miembro puede iniciar sesión en la consola del Support Center y encontrar sus espacios de trabajo y canales de Slack configurados.

Luego, pueden usar la AWS Support aplicación para sus. 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.

Obtenga más información sobre CloudFormation

Para obtener más información CloudFormation, consulte los siguientes recursos:

- [AWS CloudFormation](#)
- [AWS CloudFormation Guía del usuario](#)
- [CloudFormation Referencia de la API](#)
- [AWS CloudFormation Guía del usuario de la interfaz de línea de comandos](#)

Cree recursos de AWS Support aplicaciones mediante Terraform

También puede usar [Terraform](#) para crear los recursos de la AWS Support aplicación para su. Cuenta de AWS Terraform es una infrastructure-as-code herramienta que puede utilizar para sus aplicaciones en la nube. Puede usar Terraform para crear recursos de AWS Support aplicaciones en lugar de implementar una CloudFormation pila en una cuenta.

Después de instalar Terraform, puede especificar los recursos de la AWS Support aplicación 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 CloudFormation pilas, no puede usar Terraform para crear los recursos de la AWS Support aplicación para una unidad organizativa 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 [Registrar AWS Support las llamadas a la API de Slack mediante AWS CloudTrail](#).

Más información

Para más información sobre Terraform, consulte los siguientes temas:

- [Instalación de Terraform](#)
- [Tutorial de Terraform: Cree una 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 <https://aws.amazon.com/compliance/shared-responsibility-model/> describe estos conceptos 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. Third-party los auditores prueban y verifican periódicamente la eficacia de nuestra seguridad como parte de los programas de [AWS cumplimiento, los programas](#) 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 lo Servicio de AWS que utilice. También es responsable de otros factores, incluida la confidencialidad de los datos, los requisitos de la empresa y la legislación y la normativa aplicables.

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

Temas

- [Protección de datos en AWS Support](#)
- [Seguridad para su AWS Support fundas](#)
- [Administración de identidad y acceso para AWS Support](#)
- [Respuesta a incidentes](#)
- [Inicio de sesión y supervisión AWS Support and AWS Trusted Advisor](#)
- [Validación de conformidad para AWS Support](#)
- [Resiliencia en AWS Support](#)
- [Seguridad de la infraestructura en AWS Support](#)
- [Análisis de configuración y vulnerabilidad en Soporte](#)

Protección de datos en AWS Support

El [modelo de responsabilidad compartida](#) de AWS se aplica a la protección de datos en Soporte. Como se describe en este modelo, AWS es responsable de proteger la infraestructura global que ejecuta todos los Nube de AWS. Eres responsable de mantener el control sobre el contenido alojado en esta infraestructura. También eres responsable de las tareas de administración y configuración de seguridad para los Servicios de AWS que utiliza. Para obtener más información sobre la privacidad de los datos, consulte las [Preguntas frecuentes sobre privacidad de datos](#) y los . Para obtener más información sobre la protección de datos en Europa, consulte el [Centro del Reglamento General de Protección de Datos \(RGPD\)](#).

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

- Utiliza la autenticación multifactor (MFA) en cada cuenta.
- Se utiliza SSL/TLS para comunicarse con AWS los recursos. Exigimos TLS 1.2 y recomendamos TLS 1.3.
- Configure la API y el registro de actividad de los usuarios con AWS CloudTrail. Para obtener información sobre el uso de CloudTrail senderos para capturar AWS actividades, consulte [Cómo trabajar con CloudTrail senderos](#) en la Guía del AWS CloudTrail usuario.
- Utilice soluciones de AWS cifrado, junto con todos los controles de seguridad predeterminados Servicios de AWS.
- Utiliza servicios de seguridad administrados avanzados, como Amazon Macie, que lo ayuden a detectar y proteger la información confidencial almacenada en Amazon S3.
- Si necesita módulos criptográficos validados por FIPS 140-3 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 \(FIPS\) 140-3](#).

Se recomienda encarecidamente no introducir nunca información confidencial o sensible, como por ejemplo, direcciones de correo electrónico de clientes, en etiquetas o campos de formato libre, tales como el campo Nombre. Esto incluye cuando trabaja AWS Support o Servicios de AWS utiliza la consola, la API o los SDK. AWS CLI AWS Cualquier dato que introduzca en etiquetas o campos

de formato libre utilizados para los nombres se pueden 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.

 Important

En la correspondencia de los casos, no comparta información confidencial, como credenciales, datos de tarjetas de crédito, URL firmadas o información de identificación personal.

Seguridad para su AWS Support fundas

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. Puedes ver los detalles del caso hasta 24 meses después de su creación. Para obtener más información, consulta [DescribeCases](#) en la AWS Support Referencia de la API de .
- Sus casos de soporte siguen la [Validación de la conformidad en AWS Support](#).
- Cuando creas un caso de soporte, AWS no tendrá acceso 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. Soporte La IAM es una Servicio de AWS opción que puede utilizar sin coste adicional.

Temas

- [Público](#)
- [Autenticación con identidades](#)
- [Administración del acceso con políticas](#)
- [Cómo AWS Support funciona con IAM](#)
- [AWS Support ejemplos de políticas basadas en identidades](#)
- [Cómo utilizar roles vinculados a servicios](#)
- [AWS políticas gestionadas para AWS Support](#)
- [Gestione el acceso a AWS Support Center](#)
- [Gestione el acceso a AWS Support Planes](#)
- [Gestione el acceso a AWS Trusted Advisor](#)
- [Resolución de problemas AWS Support identidad y acceso](#)

Público

La forma de usar AWS Identity and Access Management (IAM) varía según la función que desempeñes:

- Usuario del servicio: solicite permisos al administrador si no puede acceder a las características (consulte [Resolución de problemas AWS Support identidad y acceso](#)).

- Administrador del servicio: determine el acceso de los usuarios y envíe las solicitudes de permiso (consulte [Cómo AWS Support funciona con IAM](#)).
- Administrador de IAM: escribe las políticas para administrar el acceso (consulte [AWS Support ejemplos de políticas basadas en identidades](#)).

Autenticación con identidades

La autenticación es la forma en que inicias sesión AWS con tus credenciales de identidad. Debe autenticarse como usuario de Usuario raíz de la cuenta de AWS IAM o asumir una función de IAM.

Puede iniciar sesión como una identidad federada con las credenciales de una fuente de identidad, como AWS IAM Identity Center (IAM Identity Center), la autenticación de inicio de sesión único o las credenciales. Google/Facebook Para obtener más información sobre el inicio de sesión, consulte [Cómo iniciar sesión en la Cuenta de AWS](#) en la Guía del usuario de AWS Sign-In .

Para el acceso programático, AWS proporciona un SDK y una CLI para firmar criptográficamente las solicitudes. Para obtener más información, consulte [AWS Signature Version 4 para solicitudes de API](#) en la Guía del usuario de IAM.

AWS usuario raíz de la cuenta

Al crear una Cuenta de AWS, se comienza con una identidad de inicio de sesión denominada usuario Cuenta de AWS raíz, que tiene acceso completo a todos los Servicios de AWS recursos. Se recomienda encarecidamente que no utilice el usuario raíz para las tareas diarias. Para ver la lista completa de las tareas que requieren credenciales de 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 con permisos específicos para una sola persona o aplicación. Recomendamos el uso de credenciales temporales en lugar de usuarios de IAM con credenciales de larga duración. Para obtener más información, consulte [Exigir a los usuarios humanos que utilicen la federación con un proveedor de identidad para acceder AWS mediante credenciales temporales](#) en la Guía del usuario de IAM.

Un [grupo de IAM](#) especifica un conjunto de usuarios de IAM y facilita la administración de los permisos para grupos grandes de usuarios. Para obtener más información, consulte [Casos de uso para usuarios de IAM](#) en la Guía del usuario de IAM.

Roles de IAM

Un [Rol de IAM](#) es una identidad con permisos específicos que proporciona credenciales temporales. Puede asumir un rol [cambiando de un rol de usuario a uno de IAM \(consola\)](#) o llamando a una AWS CLI operación de AWS API. Para obtener más información, consulte [Métodos para asumir un rol](#) en la Guía del usuario de IAM.

Los roles de IAM son útiles para el acceso de usuario federado, los permisos de usuario de IAM temporales, el acceso entre cuentas, el acceso entre servicios y las aplicaciones que se ejecutan en Amazon EC2. Para obtener más información, consulte [Acceso a recursos entre cuentas en IAM](#) en la Guía del usuario de IAM.

Administración del acceso con políticas

AWS Para controlar el acceso, puede crear políticas y adjuntarlas a AWS identidades o recursos. Una política define los permisos cuando están asociados a una identidad o un recurso. AWS evalúa estas políticas cuando un director hace una solicitud. La mayoría de las políticas se almacenan AWS como documentos JSON. Para obtener más información sobre los documentos de políticas de JSON, consulte [Información general de políticas de JSON](#) en la Guía del usuario de IAM.

Mediante las políticas, los administradores especifican quién tiene acceso a qué, definiendo qué entidad principal puede realizar acciones sobre qué recursos y en qué condiciones.

De forma predeterminada, los usuarios y los roles no tienen permisos. Un administrador de IAM crea políticas de IAM y las agrega a roles, que los usuarios pueden asumir posteriormente. Las políticas de IAM definen permisos independientemente del método que se utilice para realizar la operación.

Identity-based políticas

Identity-based las políticas son documentos de política de permisos de JSON que se adjuntan a una identidad (usuario, grupo o rol). Estas políticas controlan qué acciones pueden realizar las identidades, en qué recursos y en qué condiciones. Para obtener más información sobre cómo crear una política basada en la identidad, consulte [Definición de permisos de IAM personalizados con políticas administradas por el cliente](#) en la Guía del usuario de IAM.

Identity-based las políticas pueden ser políticas integradas (integradas directamente en una sola identidad) o políticas administradas (políticas independientes asociadas a varias identidades). Para obtener información sobre cómo elegir entre políticas administradas e insertadas, consulte [Selección entre políticas administradas y políticas insertadas](#) en la Guía del usuario de IAM.

Otros tipos de políticas

AWS admite tipos de políticas adicionales que pueden establecer los permisos máximos que conceden los tipos de políticas más comunes:

- Límites de permisos: establecen los permisos máximos que una política basada en identidad puede conceder a una entidad de IAM. Para obtener más información, consulte [Límites de permisos para las entidades de IAM](#) en la Guía del usuario de IAM.
- Políticas de control de servicios (SCP): especifican los permisos máximos para una organización o unidad organizativa en AWS Organizations. Para obtener más información, consulte [Políticas de control de servicios](#) en la Guía del usuario de AWS Organizations .
- Políticas de control de recursos (RCP): definen los permisos máximos disponibles para los recursos de las cuentas. Para obtener más información, consulte [Políticas de control de recursos \(RCP\)](#) en la Guía del usuario de AWS Organizations .
- Políticas de sesión: políticas avanzadas que se pasan como parámetro cuando se crea una sesión temporal para un rol o un usuario federado. Para obtener 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 se AWS determina 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 Soporte, debe comprender las funciones de IAM disponibles para su uso. SoportePara obtener una visión general de cómo funcionan con IAM Soporte 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 Soporte usar IAM, consulte Administrar el acceso para. Soporte](#)

Temas

- [Soporte políticas basadas en identidad](#)

- [Soporte Roles de IAM](#)

Soporte políticas basadas en identidad

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

Las acciones políticas Soporte 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`. Soporte 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 Soporte acciones, consulte las [acciones definidas por AWS Support](#) en la Guía del usuario de IAM.

Ejemplos

Para ver ejemplos de políticas Soporte basadas en la identidad, consulte. [AWS Support ejemplos de políticas basadas en identidades](#)

Soporte Roles de IAM

Un [rol de IAM](#) es una entidad de tu AWS cuenta que tiene permisos específicos.

Usar credenciales temporales con Soporte

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 [AssumeRole](#) o [GetFederationToken](#).

Soporte admite el uso de credenciales temporales.

Service-linked roles

[Service-linked los roles](#) permiten a los AWS servicios acceder a los recursos de otros servicios para completar una acción en su nombre. Service-linked los roles aparecen en su 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.

Soporte admite funciones vinculadas al servicio. Para obtener más información sobre la creación o la administración de funciones Soporte vinculadas a servicios, consulte. [Uso de roles vinculados al servicio para 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.

Soporte admite funciones de servicio.

AWS Support ejemplos de políticas basadas en identidades

De forma predeterminada, los usuarios y los roles de IAM no tienen permiso para crear, ver ni modificar recursos de Soporte . Tampoco pueden realizar tareas con la API Consola de

administración de 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](#)
- [Uso de Soporte consola](#)
- [Permitir a los usuarios consultar sus propios permisos](#)

Prácticas recomendadas relativas a políticas

Identity-based las políticas son muy poderosas. Determinan si alguien puede crear Soporte 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 Soporte 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.

Uso de Soporte consola

Para acceder a la AWS Support consola, debe tener un conjunto mínimo de permisos. Estos permisos deben permitirle enumerar y ver detalles sobre los Soporte 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 Soporte 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:ListGroupsWithUser",
        "iam:ListAttachedUserPolicies",
```

```

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

```

Cómo utilizar 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. Soporte Trusted Advisor En cada caso, el rol vinculado a un servicio es un rol predefinido. Esta función incluye todos los permisos Soporte 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 Soporte y. Trusted Advisor

Temas

- [Uso de roles vinculados al servicio para AWS Support](#)
- [Utilizar funciones vinculadas al servicio para Trusted Advisor](#)

Uso de roles vinculados al servicio para 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, Soporte 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. Soporte Esta función vinculada al servicio está predefinida e incluye los permisos necesarios para llamar a otros AWS servicios Soporte 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 Soporte acceder a los metadatos de los recursos, no a los datos de los clientes. Solo Soporte 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 de la [GetExecutionHistory](#) llamada a la AWS Step Functions API no están visibles para Soporte. 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 [Utilizar funciones vinculadas al servicio para 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 Soporte cabo en su nombre. Para obtener más información al respecto CloudTrail, consulte la [Guía AWS CloudTrail del usuario](#).

Service-linked permisos de rol para Soporte

Este rol usa la política `AWSSupportServiceRolePolicy` AWS administrada. 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: Soporte 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 Soporte 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: Soporte 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](#).

Creación de un rol vinculado a un servicio de Soporte

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 Soporte 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 Soporte

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 Soporte 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.

Los clientes que se hayan incorporado a un Soporte plan Enterprise AWS Organizations y que lo tengan pueden eliminar el rol vinculado al `AWSServiceRoleForSupport` servicio. La eliminación de este rol restringe el acceso de los AWS Support ingenieros a tus recursos, lo que limita su capacidad para realizar acciones en tu nombre. Para obtener más información o para solicitar la eliminación del rol `AWSServiceRoleForSupport` vinculado al servicio, póngase en contacto con su administrador técnico de cuentas (TAM).

Para obtener más información sobre el rol de `AWSServiceRoleForSupport` o sus usos, póngase en contacto con [Soporte](#).

Utilizar funciones vinculadas al servicio para 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 Service-linked los roles vienen predefinidos Trusted Advisor e incluyen todos los permisos que el servicio necesita para llamar a otros AWS servicios en su nombre. 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 al servicio para AWS Support](#).

Para obtener más información sobre otros servicios que admiten los roles vinculados a servicios, consulte [Servicios de AWS que funcionan con IAM](#). Busca los servicios cuyo texto sea Sí en la Service-linked column de funciones. Elija una opción Sí con un enlace para ver la documentación acerca del rol vinculado al servicio en cuestión.

Temas

- [Service-linked permisos de rol para 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 un servicio de Trusted Advisor](#)
- [Eliminación de un rol vinculado a un servicio de Trusted Advisor](#)

Service-linked permisos de rol para Trusted Advisor

Trusted Advisor utiliza dos funciones vinculadas a un 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. Este rol 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 de 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: Permita que una entidad de IAM edite la descripción del rol vinculado al 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 utilizar una política AWS gestionada, por ejemplo [AdministratorAccess](#), para proporcionar acceso 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 Consola de administración de AWS, 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 un servicio 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 . Cuando lo inhabilitas Trusted Advisor, deshabilitas todas las funciones del servicio, incluidos el procesamiento y las notificaciones 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 Consola de administración de AWS y navegue hasta la Trusted Advisor consola en <https://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 por AWS](#) en la Guía del usuario de IAM.

Temas

- [AWS políticas gestionadas para AWS Support](#)
- [AWS políticas gestionadas para AWS Support Aplicación en Slack](#)
- [AWS políticas gestionadas para AWS Trusted Advisor](#)
- [AWS políticas gestionadas para AWS Support planes](#)
- [AWS políticas gestionadas para AWS Partner-Led Support](#)

AWS políticas gestionadas para AWS Support

AWS Support tiene las siguientes políticas gestionadas.

Contenido

- [AWS política gestionada: AWSSupportAccess](#)
- [AWS política gestionada: AWSSupportServiceRolePolicy](#)
- [AWS Support actualizaciones de AWS políticas administradas](#)
- [Cambios de permisos para AWSSupportServiceRolePolicy](#)

AWS política gestionada: AWSSupportAccess

AWS Support utiliza la política [AWSSupportAccess](#) AWS gestionada. Esta política gestiona el ciclo de vida de los casos de soporte a través de la Soporte API. La funcionalidad mejorada AWS Support Center Console se proporciona a través del servicio de API de la consola de soporte. Puede asociar esta política a sus entidades de IAM. Para obtener más información, consulte [Service-linked permisos de rol para Soporte](#).

Para ver los permisos de esta política, consulte [AWSSupportAccess](#) en la Referencia de la política administrada de AWS .

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 [Service-linked permisos de rol para Soporte](#).

Para ver los permisos de esta política, consulte [AWSSupportServiceRolePolicy](#) en la Referencia de la política administrada de AWS .

Para obtener una lista de los cambios en la política, consulte [AWS Support actualizaciones de AWS políticas administradas](#) y [Cambios de permisos para AWSSupportServiceRolePolicy](#).

AWS Support actualizaciones de AWS políticas administradas

Vea 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 revisión](#).

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 146 permisos nuevos a los siguientes 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 Managed Workflows for Apache Airflow Serverless: para depurar problemas relacionados con Amazon Managed Workflows for Apache Airflow Serverless.	21 de abril de 2026

Cambio	Descripción	Fecha
	• AWS Backup: para depurar problemas relacionados con el AWS Backup. • Amazon Bedrock Agent Core: para depurar problemas relacionados con Amazon Bedrock Agent Core. • Amazon Connect Campaigns: para solucionar problemas relacionados con Amazon Connect Campaigns. • AWS Torre de Control: para depurar problemas relacionados con la Torre AWS de Control. • AWS Device Farm: para depurar problemas relacionados con AWS Device Farm. • Amazon EC2: para depurar problemas relacionados con Amazon EC2. • Amazon ECS: para depurar problemas relacionados con Amazon ECS. • Amazon EKS: para depurar problemas relacionados con Amazon EKS. • AWS Lambda: para depurar problemas relacionados con Lambda. AWS	

Cambio	Descripción	Fecha
	• Amazon Macie: para depurar problemas relacionados con Amazon Macie. • Amazon Route 53 Recovery Control Config: para depurar problemas relacionados con Amazon Route 53 Recovery Control Config. • Amazon Route 53 Recovery Readiness: para depurar problemas relacionados con Amazon Route 53 Recovery Readiness. • Amazon Route 53 Resolver: para depurar problemas relacionados con Amazon Route 53 Resolver. • Amazon Route 53 Global Resolver: para depurar problemas relacionados con Amazon Route 53 Global Resolver. • Amazon S3 en Outposts: para depurar problemas relacionados con Amazon S3 en Outposts. • AWS Security Hub: para depurar problemas relacionados con AWS Security Hub. • Amazon Simple Email Service: para depurar	

Cambio	Descripción	Fecha
	problemas relaciona dos con Amazon Simple Email Service. • Amazon Pinpoint SMS Voice: para depurar problemas relacionados con Amazon Pinpoint SMS Voice. • AWS Systems Manager for SAP: para depurar problemas relacionados con AWS Systems Manager for SAP. • Amazon WorkSpaces : para solucionar problemas relacionados con Amazon WorkSpaces.	

Cambio	Descripción	Fecha
AWSSupportServiceRolePolicy : actualización de una política actual	Se agregaron 105 permisos nuevos a los siguientes 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 Bedrock: para solucionar problemas relacionados con Amazon Bedrock. • Amazon Braket: para solucionar problemas relacionados con Amazon Braket. • Connect Customer: para depurar problemas relacionados con Connect Customer. • Amazon Aurora DSQL: para solucionar problemas relacionados con Amazon Aurora DSQL. • AWS Compute Optimizer — Para depurar problemas relacionados con AWS Compute Optimizer • Connect Customer: para depurar problemas relacionados con Connect Customer.	29 de enero de 2026

Cambio	Descripción	Fecha
	• Amazon EBS: para depurar problemas relacionados con Amazon EBS. • Amazon EC2: para solucionar problemas relacionados con Amazon EC2. • Amazon EKS: para depurar problemas relacionados con Amazon EKS. • AWS Elastic Beanstalk — Para depurar problemas relacionados con. AWS Elastic Beanstalk • AWS Glue — Para solucionar problemas relacionados con. AWS Glue • AWS IoT Greengrass — Para depurar problemas relacionados con. AWS IoT Greengrass • Facturación de AWS — Para depurar problemas relacionados con. Facturación de AWS • Amazon Kinesis Video Streams: para solucionar problemas relacionados con Amazon Kinesis Video Streams. • AWS License Manager — Para depurar problemas	

Cambio	Descripción	Fecha
	relacionados con. AWS License Manager • Amazon MemoryDB: para solucionar problemas relacionados con Amazon MemoryDB. • Multi-party aprobación: para depurar problemas relacionados con la aprobación. Multi-party • Amazon MQ: para solucionar problemas relacionados con Amazon MQ. • Oracle Database@AWS : para solucionar problemas relacionados con Oracle Database@.AWS • AWS Criptografía de pagos: para depurar problemas relacionados con la criptografía de pagos. AWS • Amazon RDS: para depurar problemas relacionados con Amazon RDS. • AWS Configuración de impuestos: para solucionar problemas relacionados con la configuración de impuestos. AWS	

Cambio	Descripción	Fecha
AWSSupportServiceRolePolicy : actualización de una política actual	Se agregaron 145 permisos nuevos a los siguientes 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 Amplify — Para solucionar problemas relacionados con. AWS Amplify • AWS AppSync — Para depurar problemas relacionados con. AWS AppSync • AWS Outposts — Para depurar problemas relacionados con. AWS Outposts • AWS Salas limpias: para solucionar problemas relacionados con las salas AWS limpias. • AWS Compute Optimizer — Para depurar problemas relacionados con. AWS Compute Optimizer • Connect Customer: para depurar problemas relacionados con Connect Customer.	8 de diciembre de 2025

Cambio	Descripción	Fecha
	• Amazon DynamoDB: para depurar problemas relacionados con Amazon DynamoDB. • Amazon EMR: para solucionar problemas relacionados con Amazon EMR. • Amazon Location Service: para solucionar problemas relacionados con Amazon Location Service. • Amazon GuardDuty : para solucionar problemas relacionados con Amazon GuardDuty. • AWS Network Firewall — Para depurar problemas relacionados con. AWS Network Firewall • AWS HealthOmics — Para solucionar problemas relacionados con. AWS HealthOmics • AWS Organizations — Para depurar problemas relacionados con. AWS Organizations • Amazon S3: para depurar problemas relacionados con Amazon S3. • Amazon S3 Tables: para depurar problemas	

Cambio	Descripción	Fecha
	relacionados con las tablas de Amazon S3. • Amazon S3 Vectors: para depurar problemas relacionados con Amazon S3 Vectors. • Amazon SageMaker AI: para solucionar problemas relacionados con Amazon SageMaker AI. • AWS Security Hub CSPM — Para solucionar problemas relacionados con. AWS Security Hub CSPM • Amazon SES: para depurar problemas relacionados con Amazon SES. • AWS Signer — Para depurar problemas relacionados con. AWS Signer • AWS STS — Para solucionar problemas relacionados con. AWS STS	

Cambio	Descripción	Fecha
AWSSupportServiceRolePolicy : actualización de una política actual	Se agregaron 125 permisos nuevos a los siguientes servicios para realizar acciones que ayuden a solucionar los problemas de los clientes relacionados con la facturación, el soporte administrativo y el soporte técnico: • Inteligencia artificial para operaciones de TI (AIOps): para depurar problemas relacionados con la inteligencia artificial para operaciones de TI (AIOps). • AWS Backup gateway — Para solucionar problemas relacionados con. AWS Backup gateway • CloudFormation — Para depurar problemas relacionados con. CloudFormation • Amazon Cognito Identity: para depurar problemas relacionados con Amazon Cognito Identity. • Amazon Cognito: para solucionar problemas relacionados con Amazon Cognito. • AWS Backup — Para depurar problemas	30 de septiembre de 2025

Cambio	Descripción	Fecha
	relacionados con. AWS Backup • Directory Service — Para depurar problemas relacionados con. Directory Service • Amazon EC2: para depurar problemas relacionados con Amazon EC2. • AWS FIS — Para solucionar problemas relacionados con. AWS FIS • Amazon FSx: para solucionar problemas relacionados con Amazon FSx. • AWS Global Accelerator — Para depurar problemas relacionados con. AWS Global Accelerator • AWS Identity Store: para depurar problemas relacionados con AWS Identity Store. • Facturación de AWS — Para depurar problemas relacionados con. Facturación de AWS • AWS Lake Formation — Para solucionar problemas relacionados con. AWS Lake Formation	

Cambio	Descripción	Fecha
	• AWS Network Firewall — Para depurar problemas relacionados con. AWS Network Firewall • Oracle Database@AWS : para solucionar problemas relacionados con Oracle Database@.AWS • Amazon S3: para depurar problemas relacionados con Amazon S3. • Amazon SES: para solucionar problemas relacionados con Amazon SES. • AWS IAM Identity Center — Para solucionar problemas relacionados con. AWS IAM Identity Center	
AWSSupportAccess : actualización de una política actual	Se agregaron permisos para la API de la consola de soporte a la política gestionada a AWSSupportAccess.	18 de julio de 2025

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: • CloudFormation — Para depurar problemas relacionados CloudFormation con. • AWS Config — Para solucionar problemas relacionados con. AWS Config • Amazon OpenSearch Service: para depurar problemas relacionados con Amazon OpenSearch Service. • AWS Glue — Para depurar problemas relacionados con. AWS Glue • AWS IAM: para solucionar problemas relacionados con IAM. AWS • Amazon Pinpoint: para solucionar problemas relacionados con Amazon Pinpoint. • AWS Outposts — Para depurar problemas	15 de julio de 2025

Cambio	Descripción	Fecha
	relacionados con. AWS Outposts • AWS STS — Para depurar problemas relacionados con. AWS STS Para obtener más información, consulte Cambios de permisos para AWSSupportServiceRolePolicy.	

Cambio	Descripción	Fecha
AWSSupportServiceRolePolicy : actualización de una política actual	Se agregaron 257 permisos nuevos a los siguientes servicios para realizar acciones que ayuden a solucionar los problemas de los clientes relacionados con la facturación, el soporte administrativo y el soporte técnico: • AWS App Runner — Para depurar problemas relacionados con. AWS App Runner • AWS AppSync — Para solucionar problemas relacionados con. AWS AppSync • AWS Batch — Para depurar problemas relacionados con. AWS Batch • Amazon Bedrock: para solucionar problemas relacionados con Amazon Bedrock. • Amazon CloudFront : para solucionar problemas relacionados con Amazon CloudFront. • AWS CodePipeline — Para solucionar problemas relacionados con. AWS CodePipeline	17 de junio de 2025

Cambio	Descripción	Fecha
	• AWS Config — Para solucionar problemas relacionados con. AWS Config • Connect Customer: para depurar problemas relacionados con Connect Customer. • AWS DataSync — Para depurar problemas relacionados con. AWS DataSync • Direct Connect — Para solucionar problemas relacionados con. Direct Connect • Amazon EC2: para solucionar problemas relacionados con el servicio Amazon EC2. • AWS Servicio de inyección de fallas: para depurar problemas relacionados con el servicio de inyección de AWS fallas. • AWS Firewall Manager — Para solucionar problemas relacionados con. AWS Firewall Manager • AWS Glue — Para depurar problemas relacionados con. AWS Glue	

Cambio	Descripción	Fecha
	• Amazon GuardDuty : para solucionar problemas relacionados con Amazon GuardDuty. • Generador de imágenes de EC2: para solucionar problemas relacionados con el generador de imágenes de EC2. • AWS IoT — Para solucionar problemas relacionados con. AWS IoT • AWS IoT FleetWise — Para depurar problemas relacionados con. AWS IoT FleetWise • Amazon CloudWatch Logs: para depurar problemas relacionados con Amazon CloudWatch Logs. • AWS Elemental MediaLive — Para depurar problemas relacionados con. AWS Elemental MediaLive • Network Flow Monitor: para solucionar problemas relacionados con Network Flow Monitor • AWS Network Manager — Para solucionar problemas relacionados con. AWS Network Manager	

Cambio	Descripción	Fecha
	• Servicio de administración CloudWatch de Amazon Observability: para solucionar problemas relacionados con el Servicio de administración de Amazon CloudWatch Observability. • AWS Servicio de computación paralela: para depurar problemas relacionados con el AWS servicio de computación paralela. • Amazon Redshift sin servidor: para solucionar problemas relacionados con el servicio Amazon Redshift sin servidor. • Amazon Redshift: para solucionar problemas relacionados con Amazon Redshift. • AWS Resilience Hub — Para depurar problemas relacionados con. AWS Resilience Hub • AWS Identity and Access Management Roles Anywhere: para depurar problemas relacionados con los roles de AWS Identity and Access Management Anywhere.	

Cambio	Descripción	Fecha
	• Amazon S3 en Outposts: para solucionar problemas relacionados con Amazon S3 en Outposts. • Amazon S3: para solucionar problemas relacionados con Amazon S3. • Tablas de Amazon S3: para solucionar problemas relacionados con las tablas de Amazon S3. • Amazon SageMaker AI: para depurar problemas relacionados con la SageMaker IA de Amazon. • AWS Security Hub CSPM — Para depurar problemas relacionados con. AWS Security Hub CSPM • Amazon SQS: para depurar problemas relacionados con Amazon SQS. • Administrador de incidentes de AWS Systems Manager — Para solucionar problemas relacionados con. Administrador de incidentes de AWS Systems Manager • AWS Systems Manager Configuración rápida: para depurar problemas relacionados con la	

Cambio	Descripción	Fecha
	configuración AWS Systems Manager rápida. • AWS Systems Manager — Para depurar problemas relacionados con. AWS Systems Manager • Amazon WorkSpaces Thin Client: para solucionar problemas relacionados con Amazon WorkSpaces Thin Client. • Amazon Timestream: para depurar problemas relacionados con Amazon Timestream. • AWS Telco Network Builder: para solucionar problemas relacionados con el AWS Telco Network Builder. • AWS Transfer Family — Para depurar problemas relacionados con. AWS Transfer Family • Amazon VPC Lattice: para solucionar problemas relacionados con Amazon VPC Lattice.	

Cambio	Descripción	Fecha
AWSSupportServiceRolePolicy : actualización de una política actual	Se agregaron 88 permisos nuevos a los siguientes servicios para realizar acciones que ayuden a solucionar los problemas de los clientes relacionados con la facturación, el soporte administrativo y el soporte técnico: • Amazon Bedrock: para solucionar problemas relacionados con Amazon Bedrock. • Connect Customer: para depurar problemas relacionados con Connect Customer. • Amazon DataZone : para solucionar problemas relacionados con Amazon DataZone. • Amazon EC2: para solucionar problemas relacionados con el servicio Amazon EC2. • Amazon EKS: para depurar problemas relacionados con Amazon EKS. • AWS Glue — Para solucionar problemas relacionados con. AWS Glue	25 de noviembre de 2024

Cambio	Descripción	Fecha
	• Amazon Managed Service para Apache Flink: para solucionar problemas relacionados con Amazon Managed Service para Apache Flink. • AWS Lambda — Para depurar problemas relacionados con. AWS Lambda	

Cambio	Descripción	Fecha
AWSSupportServiceRolePolicy : actualización de una política actual	Se agregaron 79 permisos nuevos a los siguientes 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 OpenSearch Serverless: para solucionar problemas relacionados con Amazon OpenSearch Serverless. • AWS AppConfig — Para depurar problemas relacionados con AWS AppConfig • Application Signals: para depurar problemas relacionados con Application Signals. • Amazon Athena: para solucionar problemas relacionados con Amazon Athena. • Amazon CloudWatch : para solucionar problemas relacionados con Amazon CloudWatch. • Amazon DynamoDB: para solucionar problemas	8 de octubre de 2024

Cambio	Descripción	Fecha
	relacionados con Amazon DynamoDB. • Amazon EC2: para solucionar problemas relacionados con el servicio Amazon EC2. • AWS IoT — Para depurar problemas relacionados con. AWS IoT • AWS Lambda — Para solucionar problemas relacionados con. AWS Lambda • AWS Launch Wizard — Para solucionar problemas relacionados con. AWS Launch Wizard • AWS Security Hub CSPM — Para depurar problemas relacionados con. AWS Security Hub CSPM • Amazon WorkSpaces : para solucionar problemas relacionados con Amazon WorkSpaces.	

Cambio	Descripción	Fecha
AWSSupportServiceRolePolicy : actualización de una política actual	Se agregaron 79 permisos nuevos a los siguientes servicios para realizar acciones que ayuden a solucionar los problemas de los clientes relacionados con la facturación, el soporte administrativo y el soporte técnico: • Cuenta de AWS — Para solucionar problemas relacionados con. Cuenta de AWS • AWS Auto Scaling — Para depurar problemas relacionados con. AWS Auto Scaling • Amazon Bedrock: para depurar problemas relacionados con Amazon Bedrock. • AWS CodeConnections — Para solucionar problemas relacionados con. AWS CodeConnections • AWS Deadline Cloud: para depurar problemas relacionados con AWS Deadline Cloud. • Amazon Elastic Kubernetes Service: para solucionar problemas relacionados con	5 de agosto de 2024

Cambio	Descripción	Fecha
	Amazon Elastic Kubernetes Service. • Elastic Load Balancing: para solucionar problemas relacionados con Elastic Load Balancing. • AWS Nivel gratuito: para depurar problemas relacionados con el nivel AWS gratuito. • Amazon Inspector: para solucionar problemas relacionados con Amazon Inspector. • Amazon OpenSearch Ingestion: para solucionar problemas relacionados con Amazon OpenSearch Ingestion. • Amazon WorkSpaces : para solucionar problemas relacionados con Amazon WorkSpaces. • AWS X-Ray — Para depurar problemas relacionados con. AWS X-Ray	

Cambio	Descripción	Fecha
AWSSupportServiceRolePolicy : actualización de una política actual	Se agregaron 17 permisos nuevos a los siguientes 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 para Apache Kafka: para depurar problemas relacionados con Amazon Managed Streaming para Apache Kafka. • Amazon Managed Service para Prometheus: para solucionar problemas relacionados con Amazon Managed Service para Prometheus.	22 de marzo de 2024

Cambio	Descripción	Fecha
AWSSupportServiceRolePolicy : actualización de una política actual	Se agregaron 63 permisos nuevos a los siguientes 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 Image Builder. • Amazon Inspector2: para solucionar problemas relacionados con Amazon Inspector2. • Amazon Inspector Scan: para solucionar problemas relacionados con 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 siguientes 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 AI: para solucionar problemas relacionados con el servicio Amazon SageMaker AI. • Amazon AppStream : para solucionar 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 solucionar problemas relacionados con el servicio Amazon Redshift sin servidor. • Amazon ElastiCache : para solucionar problemas	6 de diciembre de 2023

Cambio	Descripción	Fecha
	relacionados con Amazon ElastiCache. • Amazon Comprehend: para solucionar problemas relacionados con Amazon Comprehend. • Amazon EC2: para solucionar problemas relacionados con el servicio 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 relacionados con el AWS Health Servicio.	

Cambio	Descripción	Fecha
	• Connect Customer: para depurar problemas relacionados con Connect Customer. • AWS Snowball Edge — Para solucionar problemas relacionados con. AWS Snowball Edge • AWS Health Imaging: para solucionar problemas relacionados con AWS Health Imaging.	

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 solucionar problemas relacionados con Amazon AppStream. • AWS WAF — Para depurar problemas relacionados con el firewall de aplicaciones AWS web. • Connect Customer: para solucionar problemas relacionados con Connect Customer. • 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 relacionados 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 Quick: para depurar problemas relacionados con Amazon Quick. • 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 AI: para depurar problemas relacionados con Amazon SageMaker AI.	

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 solucionar problemas relacionados 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 Transform MGN — Para solucionar problemas relacionados con MGN. • AWS Salas limpias: para depurar problemas relacionados con las salas limpias; AWS • AWS Systems Manager para SAP: para solucionar problemas relacionados con AWS Systems Manager con SAP. • Amazon VPC Lattice: para depurar problemas relacionados con Amazon VPC Lattice.	16 de marzo de 2023

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 Servers: para solucionar problemas relacionados con Amazon GameLift Servers. • 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 Transform MGN — 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 AWS Mainframe Modernization con. • AWS Outposts — Para ayudar a AWS Support	4 de octubre de 2022

Cambio	Descripción	Fecha
	obtener una lista de servidores 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 configuraciones de resolución que AWS Support permitan comprobar el comportamiento 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 Soporte 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 Plans. • 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 Transform MGN — Para admitir la replicación sin agentes en la MGN. • AWS CloudFormation — Realizar diagnósticos sobre 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. • Amazon FSx: permite ver la descripción de las instantáneas de Amazon FSx.	17 de febrero de 2022

Cambio	Descripción	Fecha
	• 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 configuraciones 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 información, consulte Cambios de permisos para AWSSupportServiceRolePolicy.	
Registro de cambios publicado	Registro de cambios de las políticas AWS Support gestionadas.	17 de febrero de 2022

Cambios de permisos para AWSSupportServiceRolePolicy

Se agregaron la AWSSupportServiceRolePolicy mayoría de los permisos 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	
	s3.GetBucketInventoryConfiguration	s3:GetInventoryConfiguration
	s3.ListBucketInventoryConfiguration	
	s3.GetBucketLifecycleConfiguration	s3:GetLifecycleConfiguration

Date	Nombre de operación de la API	Permisos de IAM necesarios
	s3.GetBucketMetric sConfiguration	s3:GetMetricsConfi guration
	s3.ListBucketMetri csConfiguration	
	s3.GetBucketReplic ation	s3:GetReplicationC onfiguration
	s3.HeadBucket	s3:ListBucket
	s3.ListObjects	
	s3.ListBuckets	s3:ListAllMyBuckets
	s3.ListMultipartUp loads	s3:ListBucketMulti partUploads
	s3.ListObjectVersi ons	s3:ListBucketVersi ons
	s3.ListParts	s3:ListMultipartUp loadParts
Se agregaron permisos el 15 de julio de 2025	cloudcontrolapi:Ge tResource	cloudformation:Get Resource
	cloudcontrolapi:Li stResources	cloudformation:Lis tResources

AWS políticas gestionadas para AWS Support Aplicación en Slack

Note

Para acceder y ver los casos de soporte en el AWS Support Center Console, consulte [Gestione el acceso a AWS Support Center](#).

AWS Support La aplicación tiene las siguientes políticas administradas.

Contenido

- [AWS política gestionada: AWSSupportAppFullAccess](#)
- [AWS política gestionada: AWSSupportAppReadOnlyAccess](#)
- [AWS Support La aplicación se actualiza a AWS políticas administradas](#)

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 [Aplicación AWS Support en Slack](#).

Para ver los permisos de esta política, consulte [AWSSupportAppFullAccess](#) en la Referencia de la política administrada de AWS .

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.

Para obtener más información, consulte [Administrar el acceso a la AWS Support aplicación](#).

AWS política gestionada: AWSSupportAppReadOnlyAccess

La [AWSSupportAppReadOnlyAccess](#) política otorga permisos que permiten a la entidad realizar acciones de AWS Support aplicación de solo lectura. Para obtener más información, consulte [Aplicación AWS Support en Slack](#).

Para ver los permisos de esta política, consulte [AWSSupportAppReadOnlyAccess](#) en la Referencia de la política administrada de AWS .

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.

AWS Support La aplicación se actualiza a AWS políticas administradas

Consulta los detalles sobre las actualizaciones de las políticas AWS gestionadas de AWS Support la aplicación desde que este servicio comenzó a rastrear estos cambios. Para obtener alertas automáticas sobre cambios en esta página, suscríbese a la fuente RSS en la página de [Historial de revisión](#).

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 App

Cambio	Descripción	Fecha
AWSSupportAppFullAccess y 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.	19 de agosto de 2022

Cambio	Descripción	Fecha
	Para obtener más información, consulte Administrar el acceso a la AWS Support aplicación .	
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](#)
- [AWS política gestionada: AWSTrustedAdvisorServiceRolePolicy](#)
- [AWS política gestionada: AWSTrustedAdvisorReportingServiceRolePolicy](#)
- [Trusted Advisor actualizaciones de AWS políticas administradas](#)

AWS política gestionada: AWSTrustedAdvisorPriorityFullAccess

La [AWSTrustedAdvisorPriorityFullAccess](#) política 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.

JSON

```
{
  "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 [AWSTrustedAdvisorPriorityReadOnlyAccess](#) política 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 los Servicios de AWS que ha habilitado para usar Organizations.
- Enumera los administradores delegados por prioridad Trusted Advisor

JSON

```
{
  "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"
          ]
        }
      }
    }
  ]
}
```

```
}
```

AWS política gestionada: 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 [Utilizar funciones vinculadas al servicio para 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 AWS Network Firewall los recursos

- `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 recursos de Amazon ECS
- `outposts`— Obtiene recursos AWS Outposts

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "TrustedAdvisorServiceRolePermissions",
      "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:DescribeListeners",
"elasticloadbalancing:DescribeRules",
"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 [Utilizar funciones vinculadas al servicio para 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

JSON

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

Trusted Advisor actualizaciones de AWS políticas administradas

Vea los detalles sobre las actualizaciones de las políticas AWS AWS Support administradas Trusted Advisor 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 revisión](#).

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 se agregaron nuevas acciones para conceder los <code>ecs:ListTaskDefinitionFamilies</code> permisos <code>ecs:ListClusters</code> <code>ecs:ListTasks</code> <code>ecs:DescribeTasks</code> , y.	14 de mayo de 2026
AWSTrustedAdvisorServiceRolePolicy Actualización de una política existente.	Trusted Advisor se agregaron nuevas acciones para conceder los <code>elasticloadbalancing:DescribeRules</code> permisos <code>elasticloadbalancing:DescribeListeners</code> , y.	30 de octubre de 2024
AWSTrustedAdvisorServiceRolePolicy Actualización de una política existente.	Trusted Advisor agregó nuevas acciones para conceder los <code>sqs:GetQueueAttributes</code> permisos <code>access-analyzer:ListAnalyzers</code> <code>cloudwatch:ListMetrics</code> <code>dax:DescribeClusters</code> <code>ec2:DescribeNatGateways</code> <code>ec2:DescribeRouteTables</code> <code>ec2:DescribeVpcEndpoints</code> , <code>ec2:GetManagedPrefixListEnt</code>	11 de junio de 2024

Cambio	Descripción	Fecha
	ries elasticlo adbalanci ng:DescribeTargetH ealth ,iam:ListS AMLProviders ,, kafka:DescribeClus terV2 network-f irewall:ListFirewa lls network-f irewall:DescribeFi rewall y.	
AWSTrustedAdvisorServiceRolePolicy Actualización de una política existente.	Trusted Advisor agregó nuevas acciones para conceder cloudtrail:GetTrail cloudtrail:ListTrails cloudtrail:GetEventSelectors outposts:GetOutpost los outposts:ListOutposts permisos outposts:ListAssets y.	18 de enero de 2024
AWSTrustedAdvisorPriorityFullAccess Actualización de una política existente.	Trusted Advisor actualizó la política AWSTrustedAdvisorPriorityFullAccess AWS gestionada para incluir los ID de las declaraciones.	6 de diciembre de 2023

Cambio	Descripción	Fecha
AWSTrustedAdvisorPriorityReadOnlyAccess Actualización de una política existente.	Trusted Advisor actualizó la política AWSTrustedAdvisorPriorityReadOnlyAccess AWS gestionada para incluir los ID de los estados de cuenta.	6 de diciembre de 2023
AWSTrustedAdvisorServiceRolePolicy : actualización de una política actual	Trusted Advisor agregó nuevas acciones para conceder los <code>ecs:ListTaskDefinitions</code> permisos <code>ec2:DescribeRegions</code> <code>s3:GetLifecycleConfiguration</code> <code>ecs:DescribeTaskDefinition</code> y.	9 de noviembre de 2023
AWSTrustedAdvisorServiceRolePolicy : actualización de una política actual	Trusted Advisor agregó nuevas acciones <code>route53resolver:ListResolverEndpoints</code> de IAM <code>route53resolver:ListResolverEndpointIpAddresses</code> <code>kafka:ListClustersV2</code> e <code>ec2:DescribeSubnets</code> <code>kafka:ListNodes</code> incorporó nuevas comprobaciones de resiliencia.	14 de septiembre de 2023

Cambio	Descripción	Fecha
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 el 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 <code>GetAccountPublicAccessBlock</code> permisos <code>DescribeTargetGroups</code> y. El permiso <code>DescribeTargetGroup</code> 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 <code>GetAccountPublicAccessBlock</code> 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 planes

AWS Support Plans tiene las siguientes políticas administradas.

Contenido

- [AWS política gestionada: AWSSupportPlansFullAccess](#)
- [AWS política gestionada: AWSSupportPlansReadOnlyAccess](#)
- [AWS Support Planifica actualizaciones para AWS políticas administradas](#)

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
- Consulte una lista de todos los modificadores del plan de soporte para su Cuenta de AWS

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "supportplans:GetSupportPlan",
        "supportplans:GetSupportPlanUpdateStatus",
        "supportplans:StartSupportPlanUpdate",
        "supportplans:CreateSupportPlanSchedule",
        "supportplans:ListSupportPlanModifiers"
      ],
      "Resource": "*"
    }
  ]
}
```

Para obtener una lista de los cambios hechos en las políticas, consulte [AWS Support Planifica actualizaciones para AWS políticas administradas](#).

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
- Vea una lista de todos los modificadores del plan de soporte para su Cuenta de AWS

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "supportplans:GetSupportPlan",
        "supportplans:GetSupportPlanUpdateStatus",
        "supportplans:ListSupportPlanModifiers"
      ],
      "Resource": "*"
    }
  ]
}
```

Para obtener una lista de los cambios hechos en las políticas, consulte [AWS Support Planifica actualizaciones para AWS políticas administradas](#).

AWS Support Planifica actualizaciones para AWS políticas administradas

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 revisión](#).

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
AWSSupportPlansReadOnlyAccess : actualización de una política existente AWSSupportPlansFullAccess : actualización de una política existente	Añada la acción <code>ListSupportPlanModifiers</code> a las políticas administradas <code>AWSSupportPlansFullAccess</code> y <code>AWSSupportPlansReadOnlyAccess</code> .	9 de septiembre de 2024
AWSSupportPlansFullAccess : actualización de una política existente	Agregue la acción <code>CreateSupportPlanSchedule</code> a la política administrada <code>AWSSupportPlansFullAccess</code> .	8 de mayo de 2023
Registro de cambios publicado	Registro de cambios de las políticas administradas de los planes de Support.	29 de septiembre de 2022

AWS políticas gestionadas para AWS Partner-Led Support

Una política AWS gestionada 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 por AWS](#) en la Guía del usuario de IAM.

AWS política gestionada: `AWSPartnerLedSupportReadOnlyAccess`

Puede asociar `AWSPartnerLedSupportReadOnlyAccess` a los usuarios, grupos y roles.

Esta política se puede utilizar para conceder acceso de solo lectura a las API que pueden leer los metadatos de los servicios de tu AWS cuenta. Puede utilizar esta política para proporcionar a sus socios del AWS Partner-Led Support Program acceso a los servicios especificados en la siguiente sección de detalles de permisos.

 Important

Aunque `AWSPartnerLedSupportReadOnlyAccess` se trata de una política gestionada proporcionada por AWS, usted es responsable de revisar los servicios y permisos que se incluyen en la política para comprobar que cumplen sus requisitos de soporte específicos. No dé por sentado que esta política gestionada incluye automáticamente todos los existentes o nuevos Servicios de AWS. Es posible que tenga que crear y mantener políticas personalizadas adicionales para cubrir los servicios que están fuera del ámbito de esta política administrada.

Detalles de los permisos

Esta política incluye los siguientes permisos.

- `acm`: permite que las entidades principales solucionen los casos de soporte técnico relacionados con AWS Certificate Manager
- `acm-pca`: permite que las entidades principales solucionen los casos de soporte técnico relacionados con AWS Private Certificate Authority
- `apigateway`: permite que las entidades principales solucionen los casos de soporte técnico relacionados con Amazon API Gateway.

- **athena**: permite que las entidades principales solucionen los casos de soporte técnico relacionados con Amazon Athena.
- **backup**: permite que las entidades principales solucionen los casos de soporte técnico relacionados con AWS Backup
- **backup-gateway**— Permitir que los directores solucionen los casos de soporte técnico relacionados con AWS Backup Gateway.
- **cloudformation**: permite que las entidades principales solucionen los casos de soporte técnico relacionados con AWS CloudFormation
- **cloudfront**— Permitir que los directores solucionen los casos de soporte técnico relacionados con Amazon. CloudFront
- **cloudtrail**: permite que las entidades principales solucionen los casos de soporte técnico relacionados con AWS CloudTrail
- **cloudwatch**— Permitir que los directores solucionen los casos de soporte técnico relacionados con Amazon. CloudWatch
- **codepipeline**: permite que las entidades principales solucionen los casos de soporte técnico relacionados con AWS CodePipeline
- **cognito-identity**: permite que las entidades principales solucionen los casos de soporte técnico relacionados con Amazon Cognito Identity.
- **cognito-idp**: permite que las entidades principales solucionen los casos de soporte técnico relacionados con los grupos de usuario de Amazon Cognito.
- **cognito-sync**: permite que las entidades principales solucionen los casos de soporte técnico relacionados con Amazon Cognito Sync.
- **connect**— Permita que los directores solucionen los casos de soporte técnico relacionados con los clientes de Amazon Connect.
- **directconnect**: permite que las entidades principales solucionen los casos de soporte técnico relacionados con AWS Direct Connect
- **dms**: permite que las entidades principales solucionen los casos de soporte técnico relacionados con AWS Database Migration Service
- **ds**: permite que las entidades principales solucionen los casos de soporte técnico relacionados con AWS Directory Service
- **ec2**: permite que las entidades principales solucionen los casos de soporte técnico relacionados con Amazon Elastic Compute Cloud. Esto incluye las categorías de soporte técnico en EC2 (Windows y Linux), nube privada virtual (VPC) y VPC.

- `ecs`: permite que las entidades principales solucionen los casos de soporte técnico relacionados con Amazon Elastic Container Service.
- `eks`: permite que las entidades principales solucionen los casos de soporte técnico relacionados con Amazon Elastic Kubernetes Service.
- `elasticache`— Permitir que los directores solucionen los casos de soporte técnico relacionados con Amazon. ElastiCache
- `elasticbeanstalk`: permite que las entidades principales solucionen los casos de soporte técnico relacionados con AWS Elastic Beanstalk
- `elasticfilesystem`: permite que las entidades principales solucionen los casos de soporte técnico relacionados con Amazon Elastic File System.
- `elasticloadbalancing`: permite que las entidades principales solucionen los casos de soporte técnico relacionados con Elastic Load Balancing.
- `emr-containers`: permite que las entidades principales solucionen los casos de soporte técnico relacionados con Amazon EMR en EKS.
- `emr-serverless`: permite que las entidades principales solucionen los casos de soporte técnico relacionados con Amazon EMR sin servidor.
- `es`— Permitir a los directores solucionar los casos de soporte técnico relacionados con Amazon OpenSearch Service. Esto incluye categorías de soporte técnico, como OpenSearch Service Managed Cluster.
- `events`— Permitir que los directores solucionen los casos de soporte técnico relacionados con Amazon. EventBridge
- `fsx`: permite que las entidades principales solucionen los casos de soporte técnico relacionados con Amazon FSx. Esto incluye categorías de soporte técnico como FSX para Windows File Server.
- `glue`: permite que las entidades principales solucionen los casos de soporte técnico relacionados con AWS Glue
- `guardduty`— Permitir que los directores solucionen los casos de soporte técnico relacionados con Amazon. GuardDuty
- `iam`: permite que las entidades principales solucionen los casos de soporte técnico relacionados con AWS Identity and Access Management
- `kafka`: permite que las entidades principales solucionen los casos de soporte técnico relacionados con Amazon Managed Streaming para Apache Kafka.
- `kafkaconnect`: permite que las entidades principales solucionen los casos de soporte técnico relacionados con Amazon Managed Streaming para Apache Kafka Connect.

- `lambda`: permite que las entidades principales solucionen los casos de soporte técnico relacionados con AWS Lambda
- `logs`— Permite que los directores solucionen los casos de soporte técnico relacionados con Amazon CloudWatch Logs.
- `medialive`: permite que las entidades principales solucionen los casos de soporte técnico relacionados con AWS Elemental MediaLive
- `mobiletargeting`: permite que las entidades principales solucionen los casos de soporte técnico relacionados con Amazon Pinpoint.
- `pipes`— Permite que los directores solucionen los casos de soporte técnico relacionados con Amazon EventBridge Pipes.
- `polly`: permite que las entidades principales solucionen los casos de soporte técnico relacionados con Amazon Polly.
- `quicksight`— Permite que los directores solucionen los casos de soporte técnico relacionados con Amazon Quick.
- `rds`: permite que las entidades principales solucionen los casos de soporte técnico relacionados con el servicio de base de datos relacional de Amazon. Esto incluye categorías de soporte técnico como: Relational Database Service (Aurora - MySQL-Compatible), Relational Database Service (Aurora - PostgreSQL-c), Relational Database Service (PostgreSQL), Relational Database Service (SQL Server), Relational Database Service (MySQL) y Relational Database Service (Oracle).
- `redshift`: permite que las entidades principales solucionen los casos de soporte técnico relacionados con Amazon Redshift.
- `redshift-data`: permite que las entidades principales solucionen los casos de soporte técnico relacionados con la API de datos de Amazon Redshift.
- `redshift-serverless`: permite que las entidades principales solucionen los casos de soporte técnico relacionados con Amazon Redshift sin servidor.
- `route53`: permite que las entidades principales solucionen los casos de soporte técnico relacionados con Amazon Route 53.
- `route53domains`: permite que las entidades principales solucionen los casos de soporte técnico relacionados con los dominios de Amazon Route 53.
- `route53-recovery-cluster`: permite que las entidades principales solucionen los casos de soporte técnico relacionados con el clúster de recuperación de Amazon Route 53.
- `route53-recovery-control-config`: permite que las entidades principales solucionen los casos de soporte técnico relacionados con los controles de recuperación de Amazon Route 53.

- `route53-recovery-readiness`: permite que las entidades principales solucionen los casos de soporte técnico relacionados con la preparación de recuperación de Amazon Route 53.
- `route53resolver`: permite que las entidades principales solucionen los casos de soporte técnico relacionados con Amazon Route 53 Resolver.
- `s3`: permite que las entidades principales solucionen los casos de soporte técnico relacionados con Amazon Simple Storage Service.
- `s3express`: permite que las entidades principales solucionen los casos de soporte técnico relacionados con Amazon S3 Express.
- `sagemaker`— Permite que los directores solucionen los casos de soporte técnico relacionados con Amazon SageMaker AI.
- `scheduler`— Permite que los directores solucionen los casos de soporte técnico relacionados con Amazon EventBridge Scheduler.
- `servicequotas`: permite que las entidades principales solucionen los casos de soporte técnico relacionados con Service Quotas.
- `ses`: permite que las entidades principales solucionen los casos de soporte técnico relacionados con el servicio de correo electrónico de Amazon Simple.
- `sns`: permite que las entidades principales solucionen los casos de soporte técnico relacionados con el servicio de notificaciones de Amazon Simple.
- `ssm`: permite que las entidades principales solucionen los casos de soporte técnico relacionados con AWS Systems Manager
- `ssm-contacts`— Permite que los directores solucionen los casos de soporte técnico relacionados con los contactos. Administrador de incidentes de AWS Systems Manager
- `ssm-incidents`: permite que las entidades principales solucionen los casos de soporte técnico relacionados con Administrador de incidentes de AWS Systems Manager
- `ssm-sap`— Permite que los directores solucionen los casos de soporte técnico relacionados con SAP. AWS Systems Manager
- `swf`: permite que las entidades principales solucionen los casos de soporte técnico relacionados con el servicio de flujo de trabajo de Amazon Simple.
- `vpc-lattice`: permite que las entidades principales solucionen los casos de soporte técnico relacionados con Amazon VPC Lattice. Esto incluye categorías de soporte técnico como VPC - Transit Gateway.
- `waf`: permite que las entidades principales solucionen los casos de soporte técnico relacionados con AWS WAF

- `waf-regional`— Permita que los directores solucionen los casos de soporte técnico relacionados con la región. AWS WAF
- `wafv2`— Permitir que los directores solucionen los casos de soporte técnico relacionados con la versión 2. AWS WAF
- `workspaces`— Permitir que los directores solucionen los casos de soporte técnico relacionados con Amazon. WorkSpaces Esto incluye categorías de soporte técnico como Workspaces (Windows).
- `workspaces-web`— Permitir a los directores solucionar los casos de soporte técnico relacionados con Amazon WorkSpaces Secure Browser. Esto incluye categorías de soporte técnico como Workspaces (Windows).

Para ver los permisos de esta política, consulte [AWSPartnerLedSupportReadOnlyAccess](#) en la Referencia de la política administrada de AWS .

AWS Partner-Led Support actualiza a AWS políticas administradas

Consulte los detalles sobre las actualizaciones de las políticas AWS gestionadas de AWS Partner-Led Support desde que este servicio comenzó a realizar el seguimiento de estos cambios. Para recibir alertas automáticas sobre los cambios en esta página, suscríbase a la fuente RSS de la página del historial del documento de AWS Partner-Led Support.

Cambio	Descripción	Fecha
AWSPartnerLedSupportReadOnlyAccess : política nueva	Se agregó una nueva política AWS administrada que contiene permisos que pueden leer los metadatos de los servicios de su AWS cuenta.	22 de noviembre de 2024
AWS Partner-Led Support comenzó a rastrear los cambios	AWS Partner-Led Support comenzó a realizar un seguimiento de los cambios en sus políticas AWS gestionadas.	22 de noviembre de 2024

Gestione el acceso a AWS Support Center

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:

- Uso AWS Identity and Access Management (IAM).
- Usa la dirección de correo electrónico y la contraseña asociadas a tu AWS cuenta. Esta identidad se denomina usuario raíz de la AWS cuenta (no se recomienda).

Si tiene un plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations, también puede usar la [Soporte API](#) para acceder Soporte 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.

Para obtener información sobre las operaciones de la API de Support Center Console y cómo añadirlas a sus políticas de IAM, consulte [Añadir políticas de IAM para las operaciones de la API de la consola del centro de soporte](#).

AWS cuenta (no se recomienda)

Puede iniciar sesión en el Support Center Consola de administración de AWS y acceder al mismo 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 Soporte acciones en la consola. También puede especificar estas Soporte acciones en una política de IAM para permitir o denegar acciones específicas.

 Note

El rechazo de alguna de las siguientes acciones en sus políticas de IAM, podría producirse un comportamiento no deseado en el Centro de soporte en el momento de crear un caso de soporte o al interactuar con él.

Action	Description (Descripción)
AddAttachmentsToSet	Concede permiso para agregar uno o más archivos adjuntos a un conjunto de archivos adjuntos. Un conjunto de archivos adjuntos es un contenedor temporal para los archivos adjuntos que se añaden a un caso o a una comunicación entre casos. El conjunto estará disponible durante 1 hora después de su creación. El tiempo de caducidad devuelto en la respuesta es cuando el conjunto caduca.
AddCommunicationToCase	Otorga permiso para añadir comunicaciones adicionales con el cliente a un Soporte caso, incluido un conjunto de direcciones de correo electrónico para copiarlas en la comunicación.
CreateCase	Concede permiso para crear un caso.
DescribeAttachment	Concede permiso para recuperar un adjunto en un caso.
DescribeCaseAttributes	Concede permiso para permitir que los servicios secundarios lean los atributos del caso de Soporte . *El Soporte Centro lo usa internamente para etiquetar los atributos del caso.

Action	Description (Descripción)
DescribeCases	Otorga permiso para devolver una lista de Soporte casos que coincida con uno o varios identificadores de caso.
DescribeCommunication	Otorga permiso para obtener una sola comunicación y los archivos adjuntos de un solo AWS Soporte caso.
DescribeCommunications	Otorga permiso para devolver las comunicaciones y los archivos adjuntos en uno o más Soporte casos.
DescribeCreateCaseOptions	Otorga permiso para devolver una lista de CreateCaseOption tipos junto con los horarios admitidos correspondientes y la disponibilidad de idiomas.
DescribeIssueTypes	Concede permiso para devolver los tipos de errores de los casos de Soporte . El Soporte Centro lo usa internamente para obtener los tipos de problemas disponibles para su cuenta.
DescribeServices	Otorga permiso para devolver la lista actual de AWS servicios y una lista de categorías de servicios para cada servicio. A continuación, se utilizan los nombres y las categorías de los servicios para crear un caso. Cada AWS servicio tiene su propio conjunto de categorías.
DescribeSeverityLevels	Otorga permiso para devolver la lista de niveles de gravedad que puede asignar a un Soporte caso.
DescribeSupportedLanguages	Concede permiso para devolver una lista de idiomas compatibles con un CategoryCode, IssueType y ServiceCode especificados.

Action	Description (Descripción)
<code>DescribeSupportLevel</code>	Otorga permiso para devolver el nivel de soporte de un identificador de AWS cuenta. El Soporte Centro lo usa internamente para identificar su nivel de soporte.
<code>DescribeTrustedAdvisorCheckRefreshStatuses</code>	Otorga permiso para devolver el estado de actualización de las AWS Trusted Advisor comprobaciones que tienen los ID de comprobación especificados.
<code>DescribeTrustedAdvisorCheckResult</code>	Otorga permiso para devolver los resultados de la AWS Trusted Advisor comprobación que tiene el identificador de comprobación especificado.
<code>DescribeTrustedAdvisorChecks</code>	Otorga permiso para devolver información sobre todos los AWS Trusted Advisor cheques disponibles, incluidos el nombre, el identificador, la categoría, la descripción y los metadatos.
<code>DescribeTrustedAdvisorCheckSummaries</code>	Otorga permiso para devolver los resultados de los resúmenes de las AWS Trusted Advisor comprobaciones correspondientes a los identificadores de comprobación que haya especificado.
<code>GetInteraction</code>	Concede permiso para recuperar detalles sobre una interacción específica mediante su identificador único. El Soporte Centro lo utiliza internamente para recuperar recomendaciones personalizadas.

Action	Description (Descripción)
InitiateCallForCase	Otorga permiso para iniciar una llamada en Soporte Center. Soporte Center lo usa internamente para iniciar una llamada en tu nombre.
ListInteractionEntries	Otorga permiso para recuperar una lista de entradas de una interacción específica, incluidos mensajes, actualizaciones de estado u otros puntos de datos relevantes. Soporte Center lo utiliza internamente para realizar un seguimiento detallado de una interacción.
ListInteractions	Otorga permiso para recuperar una lista de interacciones, posiblemente con filtros o paginación. Soporte Center lo usa internamente para administrar y obtener una visión general de múltiples interacciones.
InitiateChatForCase	Concede permiso para iniciar un chat con el Centro de Soporte . Soporte Center lo usa internamente para iniciar un chat en tu nombre.
PutCaseAttributes	Otorga permiso para que los servicios secundarios adjunten atributos a Soporte los casos. Soporte Center lo usa internamente para agregar etiquetas operativas a sus Soporte casos.
RateCaseCommunication	Otorga permiso para calificar la comunicación de un Soporte caso.
RefreshTrustedAdvisorCheck	Otorga permiso para actualizar el AWS Trusted Advisor cheque que especifique mediante el identificador del cheque.
ResolveCase	Otorga permiso para resolver un Soporte caso.

Action	Description (Descripción)
ResolveInteraction	Otorga permiso para marcar una interacción como resuelta mediante su identificador único, lo que indica que el problema se ha abordado por completo y no requiere ninguna otra acción. Una vez resuelta, el estado de la interacción pasa a ser CERRADA y todos los usuarios de la misma cuenta pueden acceder a ella.
SearchForCases	Otorga permiso para devolver una lista de Soporte casos que coincide con las entradas indicadas. El Soporte Centro lo usa internamente para encontrar los casos buscados.
StartInteraction	Concede permiso para iniciar una nueva interacción y recibir asistencia personalizada para la solución de problemas técnicos y de la cuenta. Soporte Center lo usa internamente para iniciar el proceso de solución de problemas.
UpdateInteraction	Concede permiso para actualizar una interacción específica mediante su identificador único con otro mensaje. Soporte Center lo usa internamente para actualizar el proceso de solución de problemas.

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 Soporte 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 su Support Center

Cuenta de AWS y trabajar en él. 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 Consola de administración de AWS como usuario de IAM en la Guía del usuario](#) de IAM.

La forma más sencilla de conceder permisos es adjuntar la política AWS gestionada [AWSSupportAccess](#) al 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: Permitir el acceso a todos Soporte actions

La política AWS gestionada [AWSSupportAccess](#) concede a un usuario de IAM acceso a Soporte. Un usuario de IAM con esta política puede acceder a todas AWS Support las operaciones y recursos.

JSON

```
{
  "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 Soporte excepto resolver un caso.

JSON

```
{
  "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 Consola de administración de AWS, un espacio de nombres de `trustedadvisor` IAM independiente controla el acceso a Trusted Advisor. En la Soporte 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 AWS Support Planes

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 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.

Action	Description (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.

Action	Description (Descripción)
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.
ListSupportPlanModifiers	Concede permiso para ver una lista de todos los modificadores del plan 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.

JSON

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

Read-only acceso a Support Plans

La siguiente política permite a los usuarios acceso de solo lectura a los planes de Support.

JSON

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

Denegación del acceso a planes de Support

La siguiente política no permite a los usuarios el acceso a los planes de Support.

JSON

```
{
  "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 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 que forma parte de ella 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 permitirlosupportplans, 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. Consola de administración de AWS Todos Cuentas de AWS tienen acceso a un núcleo selecto de [Trusted Advisor cheques](#). Si tiene un plan AWS Business

Support+, AWS Enterprise Support o AWS Unified Operations, puede acceder a todos los controles. 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 Trusted Advisor consola](#)
- [Trusted Advisor actions](#)
- [Ejemplos de políticas de IAM](#)
- [Véase también](#)

Permisos para Trusted Advisor consola

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. Soporte Debe utilizar el espacio de nombres `support` para Soporte en su lugar.

Note

Si tienes permisos para acceder a la [AWS Support API](#), el Trusted Advisor widget de la Consola de administración de AWS 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 actions

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.

Action	Description (Descripción)
<code>DescribeAccount</code>	Otorga permiso para ver el Soporte plan y varias Trusted Advisor preferencias.
<code>DescribeAccountAccess</code>	Otorga permiso para ver si está Cuenta de AWS activado o desactivado Trusted Advisor.
<code>DescribeCheckItems</code>	Otorga permiso para ver los detalles de los elementos de verificación.
<code>DescribeCheckRefreshStatuses</code>	Otorga permiso para ver los estados de actualización de las verificaciones de Trusted Advisor .
<code>DescribeCheckSummaries</code>	Otorga permiso para ver los resúmenes de los Trusted Advisor cheques.
<code>DescribeChecks</code>	Otorga permiso para ver los detalles de los Trusted Advisor cheques.
<code>DescribeNotificationPreferences</code>	Otorga permiso para ver las preferencias de notificación de la cuenta de AWS .
<code>ExcludeCheckItems</code>	Otorga permiso para excluir recomendaciones para las verificaciones de Trusted Advisor .
<code>IncludeCheckItems</code>	Otorga permiso para incluir recomendaciones para las verificaciones de Trusted Advisor .

Action	Description (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 de AWS Trusted Advisor](#).

Action	Description (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

Action	Description (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 que estén 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 \(Prioridad\)](#).

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 [Comience con AWS Trusted Advisor Priority](#).

Action	Description (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.

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](#)
- [Read-only acceso a Trusted Advisor](#)
- [Denegar el acceso a Trusted Advisor](#)
- [Permitir y denegar acciones específicas](#)
- [Controle el acceso al Soporte Operaciones de API para Trusted Advisor](#)
- [Ejemplos de políticas de IAM para Trusted Advisor Priority \(Prioridad\)](#)

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.

JSON

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

Read-only acceso 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.

JSON

```
{
  "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.

JSON

```
{
  "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.

JSON

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

Controle el acceso al Soporte Operaciones de API para Trusted Advisor

En el Consola de administración de AWS, 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. Soporte En su lugar, use el espacio de nombres de `support`. Debes tener permisos de acceso a la Soporte API para realizar llamadas Trusted Advisor mediante programación.

Por ejemplo, si desea llamar a la [RefreshTrustedAdvisorCheck](#) operación, debe tener permisos para esta acción en la política.

Example: Permitir Trusted Advisor Solo operaciones de API

La siguiente política permite a los usuarios acceder a las operaciones de la Soporte API Trusted Advisor, pero no al resto de las operaciones de la Soporte 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.

JSON

```
{
  "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 Soporte y Trusted Advisor, consulte.

[Acciones](#)

Ejemplos de políticas de IAM para Trusted Advisor Priority (Prioridad)

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 [Comience con AWS Trusted Advisor Priority](#).

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](#)

Resolución de problemas 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 Soporte 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 Soporte](#)
- [Quiero permitir que personas ajenas a mi AWS cuenta para acceder a mi Soporte recursos](#)

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 Soporte.

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 la función 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 Soporte. 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 AWS administrador. 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 Soporte

Para permitir el acceso de otras personas Soporte, debes conceder permiso a las personas o aplicaciones que necesitan acceso. Si usa AWS IAM Identity Center para administrar las personas y las aplicaciones, debe asignar conjuntos de permisos a los usuarios o grupos para definir su nivel de acceso. Los conjuntos de permisos crean políticas de IAM y las asignan a los roles de IAM asociados a la persona o aplicación de forma automática. Para obtener más información, consulte la sección [Conjuntos de permisos](#) en la Guía del usuario de AWS IAM Identity Center .

Si no utiliza IAM Identity Center, debe crear entidades de IAM (usuarios o roles) para las personas o aplicaciones que necesitan acceso. A continuación, debe asociar una política a la entidad que le conceda los permisos correctos en Soporte. Una vez concedidos los permisos, proporcione las credenciales al usuario o al desarrollador de la aplicación. Utilizarán esas credenciales para acceder a AWS. Para obtener más información sobre la creación de usuarios, grupos, políticas y permisos de IAM, consulte [Identities de IAM](#) y [Políticas y permisos en IAM](#) en la Guía del usuario de IAM.

Quiero permitir que personas ajenas a mi AWS cuenta para acceder a mi Soporte recursos

Se puede crear un rol que los usuarios de otras cuentas o las personas externas a la organización puedan utilizar para acceder a sus recursos. Se 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 obtener más información, consulte lo siguiente:

- Para saber si Soporte 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 conocer sobre la diferencia entre las políticas basadas en roles y en recursos para el acceso entre cuentas, consulte [Acceso a recursos entre cuentas en IAM](#) en la Guía del usuario de IAM.

Respuesta a incidentes

La respuesta a los incidentes Soporte 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 la [Guía técnica de Respuesta frente a incidencias de seguridad de AWS](#).

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 [Panel de estado](#). Por ejemplo, eventos que afectan a los servicios o recursos de su cuenta. Para obtener más información, consulte [Cómo empezar a trabajar con Panel de estado](#) en la Guía del usuario de AWS Health .

Inicio de sesión y supervisión AWS Support and 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 CloudTrail captura 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. Para obtener más información sobre su responsabilidad de conformidad al utilizarlos Servicios de AWS, consulte [AWS la documentación de seguridad](#).

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 Soporte 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 admitir conjuntos de cifrado con perfecto secreto directo (PFS), como Ephemeral (DHE) o Elliptic Curve Ephemeral Diffie-Hellman (ECDHE). Diffie-Hellman La mayoría de los sistemas modernos como Java 7 y posteriores son compatibles con estos modos.

Además, las solicitudes deben estar firmadas mediante un ID de clave de acceso y una clave de acceso secreta que esté asociada a una entidad principal de IAM. También puedes utilizar [AWS Security Token Service](#) (AWS STS) para generar credenciales de seguridad temporales para firmar solicitudes.

Análisis de configuración y vulnerabilidad en Soporte

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 Soporte usar los AWS SDK

Los siguientes ejemplos de código muestran cómo usarlo Soporte con un kit de desarrollo de AWS software (SDK).

Los conceptos básicos son ejemplos de código que muestran cómo realizar las operaciones esenciales dentro de un servicio.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las distintas funciones de servicio, es posible ver las acciones en contexto en los escenarios relacionados.

Los escenarios son ejemplos de código que muestran cómo llevar a cabo una tarea específica a través de llamadas a varias funciones dentro del servicio o combinado con otros Servicios de AWS.

Para obtener una lista completa de las guías para desarrolladores del AWS SDK y ejemplos de código, consulte [Utilización AWS Support con un AWS SDK](#). En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

Ejemplos de código

- [Ejemplos básicos de Soporte uso de los AWS SDK](#)
 - [¿Hola Soporte](#)
 - [Aprenda los conceptos básicos del Soporte uso de un AWS SDK](#)
 - [Acciones para Soporte usar los AWS SDK](#)
 - [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](#)
 - [Utilizar DescribeTrustedAdvisorCheckRefreshStatuses con una CLI](#)
 - [Utilizar DescribeTrustedAdvisorCheckResult con una CLI](#)
 - [Utilizar DescribeTrustedAdvisorCheckSummaries con una CLI](#)

- [Utilizar DescribeTrustedAdvisorChecks con una CLI](#)
- [Utilizar RefreshTrustedAdvisorCheck con una CLI](#)
- [Úselo ResolveCase con un AWS SDK o CLI](#)
- [Escenarios de Soporte uso de AWS los SDK](#)
 - [Cómo empezar con Support](#)

Ejemplos básicos de Soporte uso de los AWS SDK

Los siguientes ejemplos de código muestran cómo utilizar los aspectos básicos de AWS Support los AWS SDK.

Ejemplos

- [¿Hola Soporte](#)
- [Aprenda los conceptos básicos del Soporte uso de un AWS SDK](#)
- [Acciones para Soporte usar los AWS SDK](#)
 - [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](#)
 - [Utilizar DescribeTrustedAdvisorCheckRefreshStatuses con una CLI](#)
 - [Utilizar DescribeTrustedAdvisorCheckResult con una CLI](#)
 - [Utilizar DescribeTrustedAdvisorCheckSummaries con una CLI](#)
 - [Utilizar DescribeTrustedAdvisorChecks con una CLI](#)
 - [Utilizar RefreshTrustedAdvisorCheck con una CLI](#)
 - [Úselo ResolveCase con un AWS SDK o CLI](#)

¿Hola Soporte

En los siguientes ejemplos de código se muestra cómo empezar a utilizar Soporte.

.NET

SDK para .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](#).

```
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($"{response.Services.Count} services available.");
    }
}
```

```
}  
}
```

- Para obtener más información sobre la API, consulta [DescribeServices](#) la Referencia AWS SDK para .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 [DescribeServices](#) la 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](#).

Invoke '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.",
            );
        }
    }
}

```

```
    );  
  }  
  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 [DescribeServices](#) la Referencia AWS SDK para 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.fromEnvironment { 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 [DescribeServices](#) la 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 [DescribeServices](#) la 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. [Utilización AWS Support con un AWS SDK](#) En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

Aprenda los conceptos básicos del Soporte uso de 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

SDK para .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($"3. Get and display available severity levels:");
        for (int i = 0; i < 10 && i < severityLevels.Count; i++)
        {
            Console.WriteLine($"  {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(
                $"{currentCase.CaseId}: status
{currentCase.Status}");
        }
    }

    Console.WriteLine(new string('-', 80));
}
}
```

Métodos envoltorios utilizados por el escenario para Soporte 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 detalles sobre la API, consulte los siguientes temas en la Referencia de la API de AWS SDK para .NET .
 - [AddAttachmentsToSet](#)
 - [AddCommunicationToCase](#)
 - [CreateCase](#)
 - [DescribeAttachment](#)
 - [DescribeCases](#)
 - [DescribeCommunications](#)
 - [DescribeServices](#)
 - [DescribeSeverityLevels](#)
 - [ResolveCase](#)

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](#).

Ejecute varias Soporte 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 = "C:\\AWS\\test.txt" ; //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 detalles 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](#)
 - [DescribeSeverityLevels](#)
 - [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.",
        );
      }
      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 getTodayOpenCases = async () => {
  const d = new Date();
  const startOfDay = new Date(d.getFullYear(), d.getMonth(), d.getDate());
  const command = new DescribeCasesCommand({
    includeCommunications: false,
    afterTime: startOfDay.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 detalles sobre la API, consulte los siguientes temas en la Referencia de la API de AWS SDK para JavaScript .
 - [AddAttachmentsToSet](#)
 - [AddCommunicationToCase](#)
 - [CreateCase](#)
 - [DescribeAttachment](#)
 - [DescribeCases](#)
 - [DescribeCommunications](#)
 - [DescribeServices](#)
 - [DescribeSeverityLevels](#)
 - [ResolveCase](#)

Kotlin

SDK para Kotlin

Note

Hay más información 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.fromEnvironment { 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.fromEnvironment { 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.fromEnvironment { 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.fromEnvironment { 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.fromEnvironment { 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.fromEnvironment { 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.fromEnvironment { 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.fromEnvironment { 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.fromEnvironment { 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.fromEnvironment { 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 detalles sobre la API, consulte los siguientes temas en la Referencia de la API de AWS SDK para Kotlin.
 - [AddAttachmentsToSet](#)
 - [AddCommunicationToCase](#)
 - [CreateCase](#)

- [DescribeAttachment](#)
- [DescribeCases](#)
- [DescribeCommunications](#)
- [DescribeServices](#)
- [DescribeSeverityLevels](#)
- [ResolveCase](#)

Python

SDK para Python (Boto3)

Note

Hay más información 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_scenari0(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_scenari0()
    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](#)
 - [DescribeSeverityLevels](#)
 - [ResolveCase](#)

Para obtener una lista completa de guías para desarrolladores del AWS SDK y ejemplos de código, consulte [Utilización AWS Support con un AWS SDK](#). En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

Acciones para Soporte usar los AWS SDK

Los siguientes ejemplos de código muestran cómo realizar Soporte acciones individuales con los AWS SDK. Cada ejemplo incluye un enlace a GitHub, donde puede encontrar instrucciones para configurar y ejecutar el código.

Estos extractos se denominan Soporte API y son fragmentos de código de programas más grandes que deben ejecutarse en su contexto. Puede ver las acciones en contexto en [Escenarios de Soporte uso de AWS los SDK](#).

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](#)
- [Utilizar DescribeTrustedAdvisorCheckRefreshStatuses con una CLI](#)
- [Utilizar DescribeTrustedAdvisorCheckResult con una CLI](#)
- [Utilizar DescribeTrustedAdvisorCheckSummaries con una CLI](#)
- [Utilizar DescribeTrustedAdvisorChecks con una CLI](#)
- [Utilizar RefreshTrustedAdvisorCheck con una CLI](#)
- [Úselo ResolveCase con un AWS SDK o CLI](#)

Úselo **AddAttachmentsToSet** con un AWS SDK o CLI

Los siguientes ejemplos de código muestran 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:

- [Conceptos básicos](#)

.NET

SDK para .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 [AddAttachmentsToSet](#) la Referencia AWS SDK para .NET de la API.

CLI

AWS CLI

Para añadir un archivo adjunto a un conjunto

En el siguiente add-attachments-to-set ejemplo, se agrega una imagen a un conjunto que, a continuación, puedes especificar para un caso de soporte en tu AWS cuenta.

```

aws support add-attachments-to-set \
  --attachment-set-id "as-2f5a6faa2a4a1e600-mu-nk5xQ1Br70-
  G1cUos5LZkd38K0AHZa9BMDVzNEXAMPLE" \
  --attachments fileName=troubleshoot-screenshot.png,data=base64-encoded-string

```

Salida:

```

{
  "attachmentSetId": "as-2f5a6faa2a4a1e600-mu-nk5xQ1Br70-
  G1cUos5LZkd38K0AHZa9BMDVzNEXAMPLE",
  "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 información sobre la API, consulta [AddAttachmentsToSet](#) la 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 [AddAttachmentsToSet](#) la 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 [AddAttachmentsToSet](#) la Referencia AWS SDK para 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.fromEnvironment { region = "us-west-2" }.use { supportClient ->
        val response = supportClient.addAttachmentsToSet(setRequest)
        return response.attachmentSetId
    }
}
```

- Para obtener más información sobre la API, consulta [AddAttachmentsToSet](#) la 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 [AddAttachmentsToSet](#) la 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. [Utilización AWS Support 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

Los siguientes ejemplos de código muestran 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 los siguientes ejemplos de código:

- [Conceptos básicos](#)
- [Cómo empezar con Support](#)

.NET

SDK para .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 [AddCommunicationToCase](#) la Referencia AWS SDK para .NET de la API.

CLI

AWS CLI

Para agregar una comunicación a un caso

En el siguiente `add-communication-to-case` ejemplo, se añaden 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-  
G1cUos5LZkd38K0AHZa9BMDVzNEXAMPLE"
```

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 [AddCommunicationToCase](#) la 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 [AddCommunicationToCase](#) la 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 para 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.fromEnvironment { 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 [AddCommunicationToCase](#) la referencia sobre el AWS SDK para la API de Kotlin.

PowerShell

Herramientas para la versión PowerShell 4

Ejemplo 1: Añade el cuerpo de una comunicación por correo electrónico al caso especificado.

```
Add-ASACommunicationToCase -CaseId "case-12345678910-2013-c4c1d2bf33c5cf47" -
CommunicationBody "Some text about the case"
```

Ejemplo 2: Añade el cuerpo de una comunicación por correo electrónico al caso especificado más una o varias direcciones de correo electrónico o más incluidas 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 más información sobre la API, consulte [AddCommunicationToCase](#) [Herramientas de AWS para PowerShell](#) Cmdlet Reference (V4).

Herramientas para la versión 5 PowerShell

Ejemplo 1: Añade el cuerpo de una comunicación por correo electrónico al caso especificado.

```
Add-ASACommunicationToCase -CaseId "case-12345678910-2013-c4c1d2bf33c5cf47" -
CommunicationBody "Some text about the case"
```

Ejemplo 2: Añade el cuerpo de una comunicación por correo electrónico al caso especificado más una o varias direcciones de correo electrónico o más incluidas 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 más información sobre la API, consulte [AddCommunicationToCase](#) la referencia de Herramientas de AWS para PowerShell cmdlets (V5).

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 [AddCommunicationToCase](#) la 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 [Utilización AWS Support 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

Los siguientes ejemplos de código muestran 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 los siguientes ejemplos de código:

- [Conceptos básicos](#)
- [Cómo empezar con Support](#)

.NET

SDK para .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 [CreateCase](#) la Referencia AWS SDK para .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 [CreateCase](#) la 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 [CreateCase](#) la 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 [CreateCase](#) la Referencia AWS SDK para 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.fromEnvironment { region = "us-west-2" }.use { supportClient ->
    val response = supportClient.createCase(caseRequest)
    return response.caseId
}
}
```

- Para obtener más información sobre la API, consulta [CreateCase](#) la referencia sobre el AWS SDK para la API de Kotlin.

PowerShell

Herramientas para la versión PowerShell 4

Ejemplo 1: Crea un nuevo caso en el AWS Support Center. Los valores de los CategoryCode parámetros - ServiceCode y - se pueden obtener mediante el Get-ASAService cmdlet. El valor del SeverityCode parámetro - se puede obtener mediante el Get-ASASeverityLevel cmdlet. El valor del IssueType parámetro - puede ser «servicio al cliente» o «técnico». Si tiene éxito, se AWS mostrará el número de caso de Support. Por defecto, el caso se gestiona en inglés, pero si desea usarlo en japonés, añada el parámetro -Language "ja". Los CommunicationBody parámetros -ServiceCode, -CategoryCode, -Asunto 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 información sobre la API, consulte [CreateCase Herramientas de AWS para PowerShell](#) Cmdlet Reference (V4).

Herramientas para la versión 5 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 Get-ASAService cmdlet. El valor del SeverityCode parámetro - se puede obtener mediante el Get-ASASeverityLevel cmdlet. El valor del IssueType parámetro - puede ser «servicio al cliente» o «técnico». Si tiene éxito, se AWS mostrará el número de caso de Support. Por defecto, el caso se gestiona en inglés, pero si desea usarlo en japonés, añada el parámetro -Language "ja". Los CommunicationBody parámetros -ServiceCode, -CategoryCode, -Asunto 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 información sobre la API, consulte [CreateCase Herramientas de AWS para PowerShell](#) Cmdlet Reference (V5).

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 [CreateCase](#) la 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. [Utilización AWS Support 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

Los siguientes ejemplos de código muestran 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:

- [Conceptos básicos](#)

.NET

SDK para .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 [DescribeAttachment](#) la Referencia AWS SDK para .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-
gJv9qqDooTipsz3V1Nb19rCfkZneeQeDPgp8X1iVJyHH7UuhZDdNeqGoduZsPrAhyMakq1c60-
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 [DescribeAttachment](#) la 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 [DescribeAttachment](#) la 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.
            })
        );
    } catch (error) {
        console.error(error);
    }
}
```

```
// 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 [DescribeAttachment](#) la Referencia AWS SDK para 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.fromEnvironment { 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 [DescribeAttachment](#) la 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 [DescribeAttachment](#) la 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. [Utilización AWS Support 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

Los siguientes ejemplos de código muestran 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 los siguientes ejemplos de código:

- [Conceptos básicos](#)
- [Cómo empezar con Support](#)

.NET

SDK para .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 [DescribeCases](#) la Referencia AWS SDK para .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 [DescribeCases](#) la 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 [DescribeCases](#) la 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 [DescribeCases](#) la Referencia AWS SDK para 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.fromEnvironment { 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 [DescribeCases](#) la referencia sobre el AWS SDK para la API de Kotlin.

PowerShell

Herramientas para la versión PowerShell 4

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")
```

- Para obtener más información sobre la API, consulte [DescribeCases Herramientas de AWS para PowerShell](#) Cmdlet Reference (V4).

Herramientas para la versión 5 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\")
```

- Para obtener más información sobre la API, consulte [DescribeCases](#) la referencia de Herramientas de AWS para PowerShell cmdlets (V5).

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 [DescribeCases](#) la 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. [Utilización AWS Support 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

Los siguientes ejemplos de código muestran 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 los siguientes ejemplos de código:

- [Conceptos básicos](#)
- [Cómo empezar con Support](#)

.NET

SDK para .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 [DescribeCommunications](#) la Referencia AWS SDK para .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":
    "eyJ1ZXh0VG9rZW4iOiBudWxsLCAiYm90b190cnVuY2F0ZV9hbW91bnQEXAMPLE=="
}
```

Para obtener más información, consulte [Administración de casos](#) en la Guía del usuario de soporte de AWS .

- Para obtener información sobre la API, consulta [DescribeCommunications](#) la 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 [DescribeCommunications](#) la 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 [DescribeCommunications](#) la Referencia AWS SDK para 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.fromEnvironment { 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 [DescribeCommunications](#) la referencia sobre el AWS SDK para la API de Kotlin.

PowerShell

Herramientas para la versión PowerShell 4

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 (horario UTC) del 1 de enero de 2012 para el caso especificado.

```
Get-ASACommunication -CaseId "case-12345678910-2013-c4c1d2bf33c5cf47" -AfterTime  
"2012-01-10T00:00Z"
```

- Para obtener más información sobre la API, consulte [DescribeCommunications](#) [Herramientas de AWS para PowerShell](#) Cmdlet Reference (V4).

Herramientas para la versión 5 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 (horario UTC) del 1 de enero de 2012 para el caso especificado.

```
Get-ASACommunication -CaseId "case-12345678910-2013-c4c1d2bf33c5cf47" -AfterTime  
"2012-01-10T00:00Z"
```

- Para obtener más información sobre la API, consulte [DescribeCommunications](#) la referencia de Herramientas de AWS para PowerShell cmdlets (V5).

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 [DescribeCommunications](#) la 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. [Utilización AWS Support 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

Los siguientes ejemplos de código muestran 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 los siguientes ejemplos de código:

- [Conceptos básicos](#)
- [Cómo empezar con Support](#)

.NET

SDK para .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 [DescribeServices](#) la Referencia AWS SDK para .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 [DescribeServices](#) la 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 [DescribeServices](#) la 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.fromEnvironment { 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 [DescribeServices](#) la referencia sobre el AWS SDK para la API de Kotlin.

PowerShell

Herramientas para la versión PowerShell 4

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 [DescribeServices Herramientas de AWS para PowerShell](#) Cmdlet Reference (V4).

Herramientas para la versión 5 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 [DescribeServices](#) la referencia de Herramientas de AWS para PowerShell cmdlets (V5).

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 [DescribeServices](#) la 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. [Utilización AWS Support 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

Los siguientes ejemplos de código muestran 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 los siguientes ejemplos de código:

- [Conceptos básicos](#)
- [Cómo empezar con Support](#)

.NET

SDK para .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 más información sobre la API, consulta [DescribeSeverityLevels](#) la Referencia AWS SDK para .NET de la API.

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 [DescribeSeverityLevels](#) la 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 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 más información sobre la API, consulta [DescribeSeverityLevels](#) la 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 { 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 más información sobre la API, consulta [DescribeSeverityLevels](#) la Referencia AWS SDK para 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 displaySevLevels(): String {
    var levelName = ""
    val severityLevelsRequest =
        DescribeSeverityLevelsRequest {
            language = "en"
        }

    SupportClient.fromEnvironment { 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 [DescribeSeverityLevels](#) la referencia sobre el AWS SDK para la API de Kotlin.

PowerShell

Herramientas para la versión PowerShell 4

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 más información sobre la API, consulte [DescribeSeverityLevels Herramientas de AWS para PowerShell](#) Cmdlet Reference (V4).

Herramientas para la versión 5 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 más información sobre la API, consulte [DescribeSeverityLevels Herramientas de AWS para PowerShell](#) Cmdlet Reference (V5).

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 [DescribeSeverityLevels](#) la 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 [Utilización AWS Support con un AWS SDK](#). En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

Utilizar **DescribeTrustedAdvisorCheckRefreshStatuses** con una CLI

Los siguientes ejemplos de código muestran cómo utilizar `DescribeTrustedAdvisorCheckRefreshStatuses`.

CLI

AWS CLI

Para enumerar los estados de actualización de las comprobaciones de AWS Trusted Advisor

En el siguiente ejemplo de `describe-trusted-advisor-check-refresh-statuses`, se muestran los estados de actualización de dos comprobaciones de Trusted Advisor: Permisos de bucket de Amazon S3 y Uso de IAM.

```
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 [DescribeTrustedAdvisorCheckRefreshStatuses](#) la Referencia de AWS CLI comandos.

PowerShell

Herramientas para la PowerShell versión 4

Ejemplo 1: devuelve el estado actual de las solicitudes de actualización para las comprobaciones especificadas. Request-ASATrustedAdvisorCheckRefresh se 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 [DescribeTrustedAdvisorCheckRefreshStatuses](#) la referencia de Herramientas de AWS para PowerShell cmdlets (V4).

Herramientas para la versión 5 PowerShell

Ejemplo 1: devuelve el estado actual de las solicitudes de actualización para las comprobaciones especificadas. Request-ASATrustedAdvisorCheckRefresh se 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 [DescribeTrustedAdvisorCheckRefreshStatuses Herramientas de AWS para PowerShell](#) Cmdlet Reference (V5).

Para obtener una lista completa de guías para desarrolladores del AWS SDK y ejemplos de código, consulte. [Utilización AWS Support con un AWS SDK](#) En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

Utilizar **DescribeTrustedAdvisorCheckResult** con una CLI

Los siguientes ejemplos de código muestran cómo utilizar `DescribeTrustedAdvisorCheckResult`.

CLI

AWS CLI

Para enumerar los resultados de una comprobación de AWS Trusted Advisor

En el siguiente ejemplo de `describe-trusted-advisor-check-result`, se muestran 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](#) la Referencia de AWS CLI comandos.

PowerShell

Herramientas para la PowerShell versión 4

Ejemplo 1: Devuelve los resultados de una comprobación de Trusted Advisor. La lista de comprobaciones de Trusted Advisor disponibles se puede obtener utilizando Get-ASATrustedAdvisorChecks. El resultado contiene 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. Si desea que los resultados se muestren en japonés, añada el parámetro -Language "ja".

```
Get-ASATrustedAdvisorCheckResult -CheckId "checkid1"
```

- Para obtener más información sobre la API, consulte [DescribeTrustedAdvisorCheckResult](#) la referencia de Herramientas de AWS para PowerShell cmdlets (V4).

Herramientas para la versión 5 PowerShell

Ejemplo 1: Devuelve los resultados de una comprobación de Trusted Advisor. La lista de comprobaciones de Trusted Advisor disponibles se puede obtener utilizando Get-ASATrustedAdvisorChecks. El resultado contiene 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. Si desea que los resultados se muestren en japonés, añada el parámetro -Language "ja".

```
Get-ASATrustedAdvisorCheckResult -CheckId "checkid1"
```

- Para obtener más información sobre la API, consulte [DescribeTrustedAdvisorCheckResult](#) [Herramientas de AWS para PowerShell](#) Cmdlet Reference (V5).

Para obtener una lista completa de guías para desarrolladores del AWS SDK y ejemplos de código, consulte. [Utilización AWS Support con un AWS SDK](#) En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

Utilizar **DescribeTrustedAdvisorCheckSummaries** con una CLI

Los siguientes ejemplos de código muestran cómo utilizar `DescribeTrustedAdvisorCheckSummaries`.

CLI

AWS CLI

Para enumerar los resúmenes de las comprobaciones de AWS Trusted Advisor

En el siguiente ejemplo de `describe-trusted-advisor-check-summaries`, se muestran los resultados de dos comprobaciones de Trusted Advisor: Permisos de bucket de Amazon S3 y Uso de IAM.

```
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 [DescribeTrustedAdvisorCheckSummaries](#) la Referencia de AWS CLI comandos.

PowerShell

Herramientas para la PowerShell versión 4

Ejemplo 1: Devuelve el resumen más reciente de la comprobación especificada de Trusted Advisor.

```
Get-ASATrustedAdvisorCheckSummary -CheckId "checkid1"
```

Ejemplo 2: Devuelve los resúmenes más recientes de las comprobaciones especificadas de Trusted Advisor.

```
Get-ASATrustedAdvisorCheckSummary -CheckId @("checkid1", "checkid2")
```

- Para obtener más información sobre la API, consulte [DescribeTrustedAdvisorCheckSummaries Herramientas de AWS para PowerShell Cmdlet Reference \(V4\)](#).

Herramientas para la versión 5 PowerShell

Ejemplo 1: Devuelve el resumen más reciente de la comprobación especificada de Trusted Advisor.

```
Get-ASATrustedAdvisorCheckSummary -CheckId "checkid1"
```

Ejemplo 2: Devuelve los resúmenes más recientes de las comprobaciones especificadas de Trusted Advisor.

```
Get-ASATrustedAdvisorCheckSummary -CheckId @("checkid1", "checkid2")
```

- Para obtener más información sobre la API, consulte [DescribeTrustedAdvisorCheckSummaries](#) la referencia de Herramientas de AWS para PowerShell cmdlets (V5).

Para obtener una lista completa de guías para desarrolladores del AWS SDK y ejemplos de código, consulte. [Utilización AWS Support con un AWS SDK](#) En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

Utilizar **DescribeTrustedAdvisorChecks** con una CLI

Los siguientes ejemplos de código muestran 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 ID, la descripción, la categoría y los metadatos del cheque. Tenga en cuenta que el resultado se abrevia para que se pueda leer.

```
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 [DescribeTrustedAdvisorChecks](#) la Referencia de AWS CLI comandos.

PowerShell

Herramientas para la PowerShell versión 4

Ejemplo 1: Devuelve la colección de comprobaciones de Trusted Advisor. Debe especificar el parámetro Language, 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 [DescribeTrustedAdvisorChecks](#) [Herramientas de AWS para PowerShell](#) Cmdlet Reference (V4).

Herramientas para la versión 5 PowerShell

Ejemplo 1: Devuelve la colección de comprobaciones de Trusted Advisor. Debe especificar el parámetro Language, 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 [DescribeTrustedAdvisorChecks](#) la referencia de Herramientas de AWS para PowerShell cmdlets (V5).

Para obtener una lista completa de guías para desarrolladores del AWS SDK y ejemplos de código, consulte. [Utilización AWS Support con un AWS SDK](#) En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

Utilizar **RefreshTrustedAdvisorCheck** con una CLI

Los siguientes ejemplos de código muestran 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 [RefreshTrustedAdvisorCheck](#) la Referencia de AWS CLI comandos.

PowerShell

Herramientas para la PowerShell versión 4

Ejemplo 1: Solicita una actualización para la comprobación especificada de Trusted Advisor.

```
Request-ASATrustedAdvisorCheckRefresh -CheckId "checkid1"
```

- Para obtener más información sobre la API, consulte [RefreshTrustedAdvisorCheck](#) [Herramientas de AWS para PowerShell](#) Cmdlet Reference (V4).

Herramientas para la versión 5 PowerShell

Ejemplo 1: Solicita una actualización para la comprobación especificada de Trusted Advisor.

```
Request-ASATrustedAdvisorCheckRefresh -CheckId "checkid1"
```

- Para obtener más información sobre la API, consulte [RefreshTrustedAdvisorCheck](#) la referencia de Herramientas de AWS para PowerShell cmdlets (V5).

Para obtener una lista completa de guías para desarrolladores del AWS SDK y ejemplos de código, consulte. [Utilización AWS Support 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

Los siguientes ejemplos de código muestran 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 los siguientes ejemplos de código:

- [Conceptos básicos](#)

- [Cómo empezar con Support](#)

.NET

SDK para .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 [ResolveCase](#) la Referencia AWS SDK para .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 información sobre la API, consulta [ResolveCase](#) la 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 [ResolveCase](#) la 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 [ResolveCase](#) la Referencia AWS SDK para 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.fromEnvironment { 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 [ResolveCase](#) la referencia sobre el AWS SDK para la API de Kotlin.

PowerShell

Herramientas para la versión PowerShell 4

Ejemplo 1: Devuelve el estado inicial del caso especificado y su estado actual una vez que se completa la llamada para resolverlo.

```
Resolve-ASACase -CaseId "case-12345678910-2013-c4c1d2bf33c5cf47"
```

- Para obtener más información sobre la API, consulte [ResolveCase Herramientas de AWS para PowerShell](#) Cmdlet Reference (V4).

Herramientas para la versión 5 PowerShell

Ejemplo 1: Devuelve el estado inicial del caso especificado y su estado actual una vez que se completa la llamada para resolverlo.

```
Resolve-ASACase -CaseId "case-12345678910-2013-c4c1d2bf33c5cf47"
```

- Para obtener más información sobre la API, consulte [ResolveCase](#) la referencia de Herramientas de AWS para PowerShell cmdlets (V5).

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 [ResolveCase](#) la 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. [Utilización AWS Support 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 Soporte uso de AWS los SDK

Los siguientes ejemplos de código muestran cómo implementar escenarios comunes Soporte con los AWS SDK. Estos escenarios muestran cómo realizar tareas específicas mediante la invocación de varias funciones integradas Soporte o combinadas con otras Servicios de AWS. En cada escenario se incluye un enlace al código fuente completo, con instrucciones de configuración y ejecución del código.

Los escenarios requieren un nivel intermedio de experiencia para entender las acciones de servicio en su contexto.

Ejemplos

- [Cómo empezar con Support](#)

Cómo empezar con Support

En el siguiente ejemplo de código, se muestra cómo:

- Compruebe los servicios disponibles y los niveles de gravedad
- Creación de un caso de soporte
- Agregue comunicaciones a un caso

Bash

AWS CLI con el script Bash

Note

Hay más información. GitHub Encuentre el ejemplo completo y obtenga información sobre cómo configurarlo y ejecutarlo en el repositorio de [Tutoriales para desarrolladores de ejemplo](#).

```
#!/bin/bash

# AWS Support CLI Tutorial Script
# This script demonstrates how to use AWS Support API through AWS CLI

set -euo pipefail

# Security: Validate script location and permissions
SCRIPT_DIR="$(cd "$(dirname "${BASH_SOURCE[0]}")" && pwd)"
readonly SCRIPT_DIR

# Security: Use secure temporary directory
readonly TEMP_DIR="$(mktemp -d)" || { echo "Failed to create temp directory";
  exit 1; }
trap "rm -rf '$TEMP_DIR'" EXIT

# Set up logging with secure permissions
```



```
LOG_FILE="${TEMP_DIR}/aws-support-tutorial.log"
touch "$LOG_FILE"
chmod 600 "$LOG_FILE"

# Security: Validate AWS CLI is available
if ! command -v aws &> /dev/null; then
    echo "ERROR: AWS CLI is not installed or not in PATH" >&2
    exit 1
fi

# Security: Check AWS credentials are configured
if ! aws sts get-caller-identity &> /dev/null; then
    echo "ERROR: AWS credentials are not properly configured" >&2
    exit 1
fi

{
    echo "Starting AWS Support Tutorial at $(date)"
    echo "Script: $0"
    echo "User: $(whoami)"
    echo "---"
} >> "$LOG_FILE"

# Function to log commands and their outputs securely
log_cmd() {
    local cmd="$1"
    echo "$(date): Running command" >> "$LOG_FILE"
    # Don't echo the actual command to prevent credential leakage
    eval "$cmd" 2>&1 | tee -a "$LOG_FILE"
    return ${PIPESTATUS[0]}
}

# Function to check for errors in command output
check_error() {
    local cmd_output="$1"
    local cmd_status="$2"
    local error_msg="$3"
    local is_fatal="${4:-true}"

    if [[ $cmd_status -ne 0 || "$cmd_output" =~ [Ee][Rr][Rr][Oo][Rr] ]]; then
        echo "ERROR: $error_msg" | tee -a "$LOG_FILE"
        echo "Command returned status: $cmd_status" >> "$LOG_FILE"

        # Check for subscription error
```

```

        if [[ "$cmd_output" =~ "SubscriptionRequiredException" ]]; then
            {
                echo ""
                echo "=====
Support plan."
                echo "IMPORTANT: This account does not have the required AWS
Support plan"
                echo "You need a Business, Enterprise On-Ramp, or Enterprise
Support plan"
                echo "to use the AWS Support API."
                echo ""
                echo "This script will now demonstrate the commands that would be
run"
                echo "if you had the appropriate support plan, but will not
execute them."
                echo "=====
            } | tee -a "$LOG_FILE"

            DEMO_MODE=true
            return 0
        fi

        if [[ "$is_fatal" == "true" ]]; then
            cleanup_resources
            exit 1
        fi
    fi
}

# Function to clean up resources
cleanup_resources() {
    echo "Cleaning up resources..." | tee -a "$LOG_FILE"
    echo "No persistent resources were created that need cleanup." | tee -a
"$LOG_FILE"
}

# Function to run a command in demo mode
demo_cmd() {
    local cmd="$1"
    local description="$2"

    {
        echo ""
        echo "DEMO: $description"
        echo "Command that would be executed:"
    }

```

```

        echo " [Command hidden for security]"
        echo ""
    } | tee -a "$LOG_FILE"
}

# Function to safely extract JSON values
extract_json_value() {
    local json_output="$1"
    local key="$2"

    echo "$json_output" | grep -o "\"$key\": \"[^\"]*\"" | head -1 | cut -d'"' -
f4 || echo ""
}

# Array to track created resources
declare -a CREATED_RESOURCES

# Initialize demo mode flag
DEMO_MODE=false

# Security: Validate input parameters
if [[ $# -gt 0 ]]; then
    echo "ERROR: This script does not accept parameters" >&2
    exit 1
fi

{
    echo "====="
    echo "AWS Support CLI Tutorial"
    echo "====="
    echo "This script demonstrates how to use AWS Support API"
    echo "Note: You must have a Business, Enterprise On-Ramp,"
    echo "or Enterprise Support plan to use the AWS Support API."
    echo "====="
    echo ""
} | tee -a "$LOG_FILE"

# Step 1: Check available services
echo "Step 1: Checking available AWS Support services..." | tee -a "$LOG_FILE"
SERVICES_OUTPUT=$(log_cmd "aws support describe-services --language en" 2>&1) ||
SERVICES_OUTPUT=""
check_error "$SERVICES_OUTPUT" $? "Failed to retrieve AWS Support services"

# If we're in demo mode, set default values

```

```

if [[ "$DEMO_MODE" == "true" ]]; then
    SERVICE_CODE="general-info"
    echo "Using demo service code: $SERVICE_CODE" | tee -a "$LOG_FILE"
else
    # Extract a service code for demonstration using safer method
    SERVICE_CODE=$(extract_json_value "$SERVICES_OUTPUT" "code") ||
SERVICE_CODE=""
    if [[ -z "$SERVICE_CODE" ]]; then
        SERVICE_CODE="general-info"
        echo "Using default service code: $SERVICE_CODE" | tee -a "$LOG_FILE"
    else
        echo "Found service code: $SERVICE_CODE" | tee -a "$LOG_FILE"
    fi
fi

# Step 2: Check available severity levels
echo "Step 2: Checking available severity levels..." | tee -a "$LOG_FILE"
if [[ "$DEMO_MODE" == "true" ]]; then
    demo_cmd "aws support describe-severity-levels --language en" "Check
available severity levels"
    SEVERITY_CODE="low"
    echo "Using demo severity code: $SEVERITY_CODE" | tee -a "$LOG_FILE"
else
    SEVERITY_OUTPUT=$(log_cmd "aws support describe-severity-levels --language
en" 2>&1) || SEVERITY_OUTPUT=""
    check_error "$SEVERITY_OUTPUT" $? "Failed to retrieve severity levels"

    SEVERITY_CODE=$(extract_json_value "$SEVERITY_OUTPUT" "code") ||
SEVERITY_CODE=""
    if [[ -z "$SEVERITY_CODE" ]]; then
        SEVERITY_CODE="low"
        echo "Using default severity code: $SEVERITY_CODE" | tee -a "$LOG_FILE"
    else
        echo "Found severity code: $SEVERITY_CODE" | tee -a "$LOG_FILE"
    fi
fi

# Step 3: Create a test support case
{
    echo ""
    echo "=====
echo "SUPPORT CASE CREATION"
    echo "=====
} | tee -a "$LOG_FILE"

```

```
if [[ "$DEMO_MODE" == "true" ]]; then
{
    echo "DEMO MODE: The following steps would create and manage a support
case"
    echo "if you had a Business, Enterprise On-Ramp, or Enterprise Support
plan."
    echo ""
} | tee -a "$LOG_FILE"

USER_EMAIL="example@example.com"

demo_cmd "aws support create-case" "Create a support case"

CASE_ID="case-12345678910-2013-c4c1d2bf33c5cf47"
echo "Demo case ID: $CASE_ID" | tee -a "$LOG_FILE"

demo_cmd "aws support describe-cases" "List support cases"
demo_cmd "aws support add-communication-to-case" "Add communication to case"
demo_cmd "aws support describe-communications" "View case communications"
demo_cmd "aws support resolve-case" "Resolve the support case"

else
    echo "Creating a test support case..." | tee -a "$LOG_FILE"

    USER_EMAIL="example@example.com"
    CC_EMAIL_PARAM="--cc-email-addresses $USER_EMAIL"

    # Create the case
    CASE_OUTPUT=$(log_cmd "aws support create-case --subject 'AWS CLI Tutorial
Test Case' --service-code '$SERVICE_CODE' --category-code 'using-aws' --
communication-body 'This is a test case created as part of an AWS CLI tutorial.'
--severity-code '$SEVERITY_CODE' --language 'en' $CC_EMAIL_PARAM" 2>&1) ||
CASE_OUTPUT=""

    check_error "$CASE_OUTPUT" $? "Failed to create support case"

    # Extract the case ID safely
    CASE_ID=$(extract_json_value "$CASE_OUTPUT" "caseId") || CASE_ID=""

    if [[ -n "$CASE_ID" ]]; then
        echo "Successfully created support case with ID: $CASE_ID" | tee -a
"$LOG_FILE"
        CREATED_RESOURCES+=("Support Case: $CASE_ID")
    fi
fi
```

```

# Step 4: List the case we just created
echo "" | tee -a "$LOG_FILE"
echo "Step 4: Listing the support case we just created..." | tee -a
"$LOG_FILE"
CASES_OUTPUT=$(log_cmd "aws support describe-cases --case-id-
list '$CASE_ID' --include-resolved-cases false --language 'en'" 2>&1) ||
CASES_OUTPUT=""

check_error "$CASES_OUTPUT" $? "Failed to retrieve case details"

# Step 5: Add a communication to the case
echo "" | tee -a "$LOG_FILE"
echo "Step 5: Adding a communication to the support case..." | tee -a
"$LOG_FILE"
COMM_OUTPUT=$(log_cmd "aws support add-communication-to-case --case-id
'$CASE_ID' --communication-body 'This is an additional communication for the
test case.' $CC_EMAIL_PARAM" 2>&1) || COMM_OUTPUT=""

check_error "$COMM_OUTPUT" $? "Failed to add communication to case"

# Step 6: View communications for the case
echo "" | tee -a "$LOG_FILE"
echo "Step 6: Viewing communications for the support case..." | tee -a
"$LOG_FILE"
COMMS_OUTPUT=$(log_cmd "aws support describe-communications --case-id
'$CASE_ID' --language 'en'" 2>&1) || COMMS_OUTPUT=""

check_error "$COMMS_OUTPUT" $? "Failed to retrieve case communications"

# Step 7: Resolve the case
{
    echo ""
    echo "=====
    echo "CASE RESOLUTION"
    echo "=====
    echo "Resolving the support case..."
} | tee -a "$LOG_FILE"

RESOLVE_OUTPUT=$(log_cmd "aws support resolve-case --case-id '$CASE_ID'"
2>&1) || RESOLVE_OUTPUT=""

check_error "$RESOLVE_OUTPUT" $? "Failed to resolve case"
echo "Successfully resolved support case: $CASE_ID" | tee -a "$LOG_FILE"

```

```

        else
            echo "Could not extract case ID from the response." | tee -a "$LOG_FILE"
        fi
    fi

# Display summary of created resources
{
    echo ""
    echo "=====
    echo "TUTORIAL SUMMARY"
    echo "=====
} | tee -a "$LOG_FILE"

if [[ "$DEMO_MODE" == "true" ]]; then
{
    echo "This was a demonstration in DEMO MODE."
    echo "No actual AWS Support cases were created."
    echo "To use the AWS Support API, you need a Business, Enterprise On-
Ramp,"
    echo "or Enterprise Support plan."
} | tee -a "$LOG_FILE"
else
{
    echo "Resources created during this tutorial:"
    if [[ ${#CREATED_RESOURCES[@]} -eq 0 ]]; then
        echo "No resources were created."
    else
        for resource in "${CREATED_RESOURCES[@]}"; do
            echo "- $resource"
        done
    fi
} | tee -a "$LOG_FILE"
fi

{
    echo ""
    echo "Tutorial completed successfully!"
    echo "Log file: $LOG_FILE"
    echo "=====
} | tee -a "$LOG_FILE"

# Display log file path to user

```

```
echo "Log file: $LOG_FILE"
```

- Para obtener información sobre la API, consulte los siguientes temas en la Referencia de comandos de AWS CLI .
 - [AddCommunicationToCase](#)
 - [CreateCase](#)
 - [DescribeCases](#)
 - [DescribeCommunications](#)
 - [DescribeServices](#)
 - [DescribeSeverityLevels](#)
 - [ResolveCase](#)

Para obtener una lista completa de guías para desarrolladores del AWS SDK y ejemplos de código, consulte [Utilización AWS Support 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 Soporte y de sus otras soluciones de AWS. AWS ofrece las siguientes herramientas de supervisión para vigilar Soporte, 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 puede identificar qué usuarios y cuentas llamaron a AWS, la dirección IP de origen de las llamadas y el momento en que se hicieron. Para más información, consulte la [Guía del usuario de AWS CloudTrail](#).

Temas

- [Integración AWS Support en aplicaciones basadas en eventos mediante Amazon EventBridge](#)
- [Registrar llamadas a la AWS Support API con AWS CloudTrail](#)
- [Registrar AWS Support las llamadas a la API de Slack mediante AWS CloudTrail](#)

Integración AWS Support en aplicaciones basadas en eventos mediante Amazon EventBridge

Puede AWS Support incorporarlas en aplicaciones basadas en eventos (EDAs) que utilizan los eventos que se producen AWS Support para comunicarse entre los componentes de la aplicación e iniciar procesos posteriores.

Por ejemplo, puede recibir una notificación cada vez que se produzcan los siguientes AWS Support eventos en su cuenta:

- Se crea, resuelve o vuelve a abrir un caso de soporte

- Se agrega una correspondencia a un caso de soporte existente

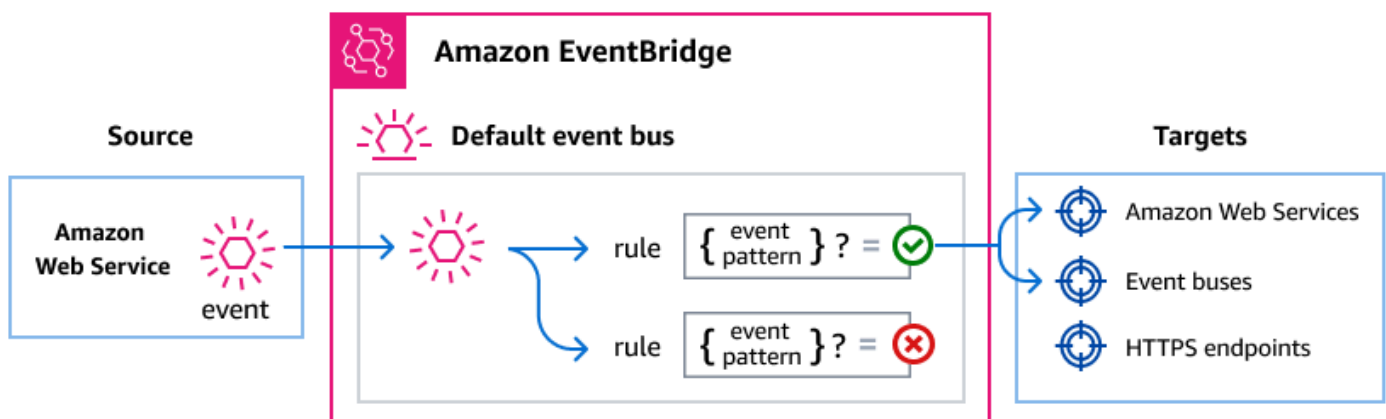
Para ello, utiliza Amazon EventBridge para enrutar eventos desde AWS Support otros componentes de software. Amazon EventBridge es un servicio sin servidor que utiliza eventos para conectar los componentes de la aplicación entre sí, lo que facilita la integración de AWS servicios, por ejemplo, en arquitecturas basadas AWS Support en eventos sin código ni operaciones adicionales.

EventBridge ¿ AWS Support Cómo direcciona los eventos

Así es como EventBridge funciona con AWS Support los eventos:

Como ocurre con muchos AWS servicios, AWS Support genera y envía eventos al bus de eventos EventBridge predeterminado. Un bus de eventos es un enrutador que recibe eventos y los envía a destinos u objetivos, que se especifican. Los objetivos pueden incluir otros AWS servicios, aplicaciones personalizadas y aplicaciones de socios de SaaS.

EventBridge enruta los eventos de acuerdo con las reglas que usted crea en el bus de eventos. Para cada regla, se debe especificar un filtro o patrón de eventos para seleccionar solo los eventos que desee. Cada vez que se envía un evento al bus de eventos, lo EventBridge compara con cada regla. Si el evento coincide con la regla, lo EventBridge enruta a los objetivos especificados.



AWS Support eventos

AWS Support envía automáticamente los siguientes eventos al bus de EventBridge eventos predeterminado.

Tipo de detalle del evento	Description (Descripción)
Actualización de caso de soporte	Representa un cambio en un caso de soporte.

Estructura de evento

Todos los eventos de AWS los servicios contienen dos tipos de datos:

- Un conjunto común de campos que contiene metadatos sobre el evento, como el AWS servicio que lo origina, la hora en que se generó el evento, la cuenta y la región en las que tuvo lugar el evento, etc. Para ver las definiciones de estos campos generales, consulte [Estructura de eventos](#) en la referencia de Amazon EventBridge Events.
- Un campo `detail` que contiene los datos específicos de ese evento en particular.

AWS Support entrega de eventos a través de AWS CloudTrail

AWS los servicios pueden enviar los eventos directamente al bus de eventos EventBridge predeterminado. Además, también AWS CloudTrail envía eventos que se originan en EventBridge numerosos AWS servicios. Estos eventos pueden incluir llamadas a la API, inicios de sesión y acciones en la consola, eventos de servicio e CloudTrail Insights. Para obtener más información, consulte [los eventos AWS de servicio que se ofrecen AWS CloudTrail](#) en la Guía del EventBridge usuario.

Para obtener una lista de AWS Support los eventos enviados a EventBridge, consulte el AWS Support tema de la [Referencia de EventBridge eventos](#).

Crear patrones de eventos que coincidan con AWS Support los eventos

Los patrones de eventos son filtros que especifican los datos que deben tener los eventos que desea seleccionar.

Cada patrón de eventos es un objeto JSON que contiene:

- Un atributo `source` que identifica el servicio que envía el evento. En el AWS Support caso de los eventos, la fuente es `aws.support`.
- (Opcional): un atributo `detail-type` que contiene una matriz de los nombres de eventos que deben coincidir.

- (Opcional): un atributo `detail` que contiene cualquier otro dato de evento con el que coincidir.

Por ejemplo, el siguiente patrón de eventos seleccionaría todos los eventos de Actualización de un caso de soporte de AWS Support:

```
{
  "source": ["aws.support"],
  "detail-type": ["Support Case Update"]
}
```

Para ser más específico en la selección de eventos, se pueden incluir valores en el propio evento. Por ejemplo, el siguiente patrón de eventos coincide con los eventos de Actualización de caso de soporte que representan la reapertura de un caso:

```
{
  "source": ["aws.support"],
  "detail-type": ["Support Case Update"],
  "detail": {
    "event-name": "ReopenCase"
  }
}
```

Para obtener más información sobre la escritura de los patrones de eventos, consulte [Patrones de eventos](#) en la Guía del usuario de EventBridge .

Véase también

Para obtener más información sobre cómo usarlo EventBridge con AWS Support, consulta los siguientes recursos:

- [Cómo automatizar la AWS Support API con Amazon EventBridge](#)
- [AWS Support notificador de actividad de casos](#) en GitHub

Evento Actualización de caso de soporte

A continuación, se muestran los campos de detalle del evento `Support Case Update`.

Los `detail-type` campos `source` y se incluyen a continuación porque contienen valores específicos para los AWS Support eventos. Para ver las definiciones de los demás campos de

metadatos que se incluyen en todos los eventos, consulte [Estructura de eventos](#) en la referencia de Amazon EventBridge Events.

```
{
  . . . ,
  "detail-type": "Support Case Update",
  "source": "aws.support",
  . . . ,
  "detail": {
    "case-id" : "string",
    "display-id" : "string",
    "communication-id" : "string",
    "event-name" : "string",
    "origin" : "string"
  }
}
```

detail-type

Identifica el tipo de evento.

Para este evento, este valor es Support Case Update.

source

Identifica el servicio que generó el evento. Para AWS Support los eventos, este valor es `aws.support`.

detail

Un objeto JSON que contiene información sobre el evento. El servicio que genera el evento determina el contenido de este campo.

Para este evento, estos datos incluyen lo siguiente:

case-id

El identificador del caso de soporte. El identificador de caso es una cadena alfanumérica con el siguiente formato: `case-12345678910-2013-c4c1d2bf33c5cf47`.

display-id

El identificador del caso en las páginas del AWS Support Centro.

communication-id

El identificador de la comunicación.

event-name

Valores válidos: CreateCase | AddCommunicationToCase | ResolveCase | ReopenCase

Especifica el tipo de evento de caso de soporte.

origin

Valores válidos: AWS | CUSTOMER

Especifica si usted o un AWS Support agente agregaron la correspondencia de un caso a un caso de soporte.

Actualmente, solo los eventos con un event-name de AddCommunicationToCase tendrán este valor.

Example Ejemplo de evento de actualización de caso de soporte: caso de soporte creado

```
{
  "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 Ejemplo de evento Support Case Update: AWS Support respuestas 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 Ejemplo de evento de actualización de caso de soporte: caso de soporte resuelto

```

{
  "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 Ejemplo de evento de actualización de caso de soporte: caso de soporte reabierto

```

{
  "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": ""
  }
}
```

Registrar llamadas a la AWS Support API con AWS CloudTrail

AWS Support está integrado con AWS CloudTrail un servicio que proporciona un registro de las acciones realizadas por un usuario, un rol o un AWS servicio en AWS Support. CloudTrail captura las llamadas a la API AWS Support como eventos. Las llamadas capturadas incluyen llamadas desde la AWS Support consola y llamadas en código a las operaciones de la AWS Support API.

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 AWS Support. 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 el destinatario de la solicitud AWS Support, la dirección IP desde la que 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](#).

AWS Support información en CloudTrail

CloudTrail está habilitada en su AWS cuenta al crear la cuenta. Cuando se produce una actividad de eventos admitida AWS Support, 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 tu cuenta AWS Support, 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:

- [Introducción a la creación de registros de seguimiento](#)
- [CloudTrail servicios e integraciones compatibles](#)
- [Configuración de las notificaciones de Amazon SNS para CloudTrail](#)
- [Recepción de archivos de registros de CloudTrail desde varias regiones](#) y [Recepción de archivos de registro de CloudTrail de varias cuentas](#)

Todas las operaciones de la AWS Support API se registran CloudTrail y se documentan en la [referencia de la AWS Support API](#).

Por ejemplo, las llamadas a las CreateCase ResolveCase operaciones DescribeCases y generan entradas en los archivos de CloudTrail registro.

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 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 userIdentity de CloudTrail](#) .

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

AWS Trusted Advisor información al iniciar CloudTrail sesión

Trusted Advisor es un AWS Support servicio que puede utilizar para comprobar su AWS cuenta y encontrar formas de ahorrar costes, mejorar la seguridad y optimizar su cuenta.

Todas las operaciones de la Trusted Advisor API se registran CloudTrail y se documentan en la [Referencia de la AWS Support API](#).

Por ejemplo, las llamadas a las `DescribeTrustedAdvisorCheckRefreshStatuses` `RefreshTrustedAdvisorCheck` operaciones `DescribeTrustedAdvisorCheckResult` y generan entradas en los archivos de CloudTrail registro.

 Note

CloudTrail también registra las acciones Trusted Advisor de la consola. Consulte [Registrar las acciones de la AWS Trusted Advisor consola con AWS CloudTrail](#).

Descripción de las entradas de los archivos de AWS Support registro

Un rastro es una configuración que permite la entrega de eventos como archivos de registro a un bucket de Amazon S3 que usted especifique. CloudTrail Los archivos de registro contienen una o más entradas de registro. Un evento representa una 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 ordenado de las llamadas a las API públicas, por lo que no aparecen en ningún orden específico.

Example: entrada de registro para `CreateCase`

El siguiente ejemplo muestra una entrada de CloudTrail registro para la [CreateCase](#) operación.

```
{
  "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

El siguiente ejemplo muestra una entrada de CloudTrail registro para la [RefreshTrustedAdvisorCheck](#) operación.

```

{
  "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"
}
```

Registrar AWS Support las llamadas a la API de Slack mediante AWS CloudTrail

La AWS Support aplicación de Slack está integrada con. AWS CloudTrail CloudTrail proporciona un registro de las acciones realizadas por un usuario, un rol o una persona Servicio de AWS en la AWS Support aplicación. Para crear este registro, CloudTrail captura todas las llamadas públicas a la API de AWS Support la aplicación como eventos. Estas llamadas capturadas incluyen las llamadas desde la consola de la AWS Support aplicación y las llamadas en código a las operaciones de la API pública de la AWS Support aplicación. Si crea una ruta, puede habilitar la entrega continua de CloudTrail eventos a un bucket de Amazon S3. Entre ellos se incluyen los eventos de AWS Support la aplicación. Si no configuras una ruta, podrás ver los eventos más recientes en la CloudTrail consola, en el historial de eventos. Puedes usar la información CloudTrail recopilada para determinar cuál es la solicitud que se hizo a AWS Support App. 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 CloudTrail, consulta la [Guía AWS CloudTrail del usuario](#).

AWS Support Información sobre la aplicación en CloudTrail

Cuando creas la tuya Cuenta de AWS, se activa CloudTrail en la cuenta. Cuando se produce una actividad de API pública en la AWS Support aplicación, 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 Cuenta de AWS. Para obtener más información, consulte [Visualización de eventos con el historial de CloudTrail eventos](#).

Para tener un registro continuo de los eventos en tu Cuenta de AWS, incluidos los eventos de AWS Support la aplicación, crea una ruta. 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. Además, puede configurar otros Servicios de AWS para que analicen más a fondo los datos de eventos recopilados en CloudTrail los registros y actúen 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](#)

CloudTrail registra todas las acciones de AWS Support la aplicación pública. Estas acciones también se documentan en la [referencia de la API de la aplicación AWS Support en Slack](#). Por ejemplo, las llamadas a las `CreateSlackChannelConfiguration` `UpdateSlackChannelConfiguration` acciones `GetAccountAlias` y las llamadas generan entradas en los archivos de CloudTrail registro.

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 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 Servicio de AWS.

Para obtener más información, consulte el [elemento `userIdentity` de CloudTrail](#).

Descripción de las entradas del archivo de registro de la AWS Support aplicación

Un rastro es una configuración que permite la entrega de eventos como archivos de registro a un bucket de Amazon S3 que usted especifique. CloudTrail Los archivos de registro contienen una o más entradas de registro. Un evento representa una solicitud única de cualquier fuente e incluye información sobre la acción solicitada, la fecha y la hora de la acción, los parámetros de la solicitud, etc. CloudTrail Los archivos de registro no son un seguimiento ordenado de las 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 CloudTrail registro de la [CreateSlackChannelConfiguration](#) operación.

```
{
  "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 CloudTrail registro de la [ListSlackChannelConfigurations](#) operación.

```

{
  "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 CloudTrail registro de la [GetAccountAlias](#) operación.

```

{
    "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 puede 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 llamadas a la API de AWS Support Plans con AWS CloudTrail](#)

Registrar las llamadas a la API de AWS Support Plans con AWS CloudTrail

AWS Support Plans está integrado con AWS CloudTrail un servicio que proporciona un registro de las acciones realizadas por un usuario, un rol o una persona Servicio de AWS. CloudTrail captura las llamadas a la API de AWS Support los planes como eventos. Las llamadas capturadas incluyen llamadas desde la consola de AWS Support Plans y llamadas en código a las operaciones de la API de AWS Support Plans.

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 los planes. 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 Plans, 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 La información del plan se encuentra en CloudTrail

CloudTrail está habilitada en tu cuenta Cuenta de AWS al crear la cuenta. Cuando se produce una actividad de eventos admitida en AWS Support los planes, esa actividad se registra en un CloudTrail evento junto con otros Servicio de AWS eventos en el historial de eventos. Se puede ver, buscar y descargar los últimos eventos de la cuenta de . Para obtener más información, consulta [Cómo ver eventos con el historial de CloudTrail eventos](#).

Para tener un registro continuo de los eventos de tu cuenta, incluidos los eventos de AWS Support los planes, crea una ruta. Un rastro permite CloudTrail entregar archivos de registro a un bucket de Amazon S3. De forma predeterminada, cuando se crea un registro de seguimiento en la consola, el registro de seguimiento se aplica a todas las Regiones de AWS. La ruta registra los eventos de todas las regiones de la AWS partición y envía los archivos de registro al bucket de Amazon S3 que especifique. Además, puede configurar otros Servicios de AWS para que analicen más a fondo los datos de eventos recopilados en los CloudTrail registros y actúen 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](#)
- [Recepción de archivos de registros de CloudTrail desde varias regiones](#) y [Recepción de archivos de registro de CloudTrail de varias cuentas](#)

Todas las operaciones AWS Support de la API de los planes se registran mediante 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 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 Servicio de AWS.

Para obtener más información, consulte el [elemento userIdentity de CloudTrail](#) .

También puede agrupar los archivos de registro de AWS Support planes de varias Regiones de AWS y múltiples cuentas en un único bucket de Amazon S3.

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

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 ordenado de las llamadas a las API públicas, por lo que no aparecen en ningún orden específico.

Example: entrada de registro de GetSupportPlan

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

```
{
  "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

El siguiente ejemplo muestra una entrada de CloudTrail registro para la GetSupportPlanUpdateStatus operación.

```

{
  "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

El siguiente ejemplo muestra una entrada de CloudTrail registro para la StartSupportPlanUpdate operación.

```

{
    "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

El siguiente ejemplo muestra una entrada de CloudTrail registro para la CreateSupportPlanSchedule operación.

```

{
  "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:supportplansschedule/
b9a9a4336a3974950a6e670f7dab79b77a4b104db548a0d57050ce4544721d4b"
    },
    "requestID": "150450b8-e61a-4b15-93a8-c3b557a1ca48",
    "eventID": "a2a1ba44-610d-4dc8-bf16-29f1635b57a9",

```



```
"readOnly": false,
"eventType": "AwsApiCall",
"managementEvent": true,
"recipientAccountId": "111122223333",
"eventCategory": "Management"
}
```

Example: entrada de registro de ListSupportPlanModifiers

El siguiente ejemplo muestra una entrada de CloudTrail registro para la ListSupportPlanModifiers operación.

```
{
  "eventVersion": "1.09",
  "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:sts::111122223333:user/janedoe",
        "accountId": "111122223333",
        "userName": "Admin"
      },
      "attributes": {
        "creationDate": "2024-08-15T15:44:43Z",
        "mfaAuthenticated": "false"
      }
    }
  },
  "eventTime": "2024-08-15T16:29:59Z",
  "eventSource": "supportplans.amazonaws.com",
  "eventName": "ListSupportPlanModifiers",
  "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"
}
```

Registrar los cambios en su Soporte plan

Important

A partir del 3 de agosto de 2022, las siguientes operaciones quedarán obsoletas y no aparecerán en CloudTrail los nuevos registros. Para ver una lista de las operaciones admitidas, consulte [Descripción de las entradas del archivo de registro de AWS Support Plans](#).

- `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 reanuda 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 siguiente ejemplo, se muestra una entrada de CloudTrail registro para la `DescribeSupportLevelSummary` acción.

```
{
  "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 UpdateProbationAutoCancellation

En el siguiente ejemplo, se muestra una entrada de CloudTrail registro para la UpdateProbationAutoCancellation acción.

```
{
  "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 UpdateSupportLevel

El siguiente ejemplo muestra una entrada de CloudTrail registro para que la UpdateSupportLevel acción cambie a 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 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 puede 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 los resultados de los AWS Trusted Advisor controles con Amazon EventBridge](#)
- [Crear CloudWatch alarmas de Amazon para monitorear AWS Trusted Advisor las métricas](#)
- [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

Important

Aviso de fin de soporte: el soporte para desarrolladores se suspenderá el 1 de enero de 2027. Los clientes con soporte para desarrolladores pueden seguir usando su plan actual o optar por actualizarse a Business Support+ en cualquier momento antes del 1 de enero de 2027. Business Support+ ofrece asistencia basada en inteligencia artificial que comprende el contexto de sus operaciones, con acceso a AWS expertos las 24 horas del día, los 7 días de la semana, a un precio mínimo de 29 USD al mes por cuenta. Para obtener más información, consulta los detalles del [plan Business Support+](#)

Aviso de fin de soporte: el soporte empresarial se suspenderá el 1 de enero de 2027. Los clientes con Business Support pueden seguir usando su plan actual o optar por actualizarse a Business Support+ en cualquier momento antes del 1 de enero de 2027. Business Support + ofrece asistencia basada en inteligencia artificial que comprende el contexto de sus operaciones, con acceso a AWS expertos las 24 horas del día, los 7 días de la semana, a un precio mínimo de 29 USD al mes por cuenta. Para obtener más información, consulta los detalles del [plan Business Support+](#)

Aviso de fin de soporte: el 1 de enero de 2027, Enterprise AWS On-Ramp dejará de funcionar. A lo largo de 2026, los clientes de Enterprise On-Ramp pasarán automáticamente a AWS Enterprise Support durante la renovación del contrato o en lotes periódicos. Los clientes recibirán una notificación por correo electrónico un mes antes de la actualización. No hay que hacer nada más. Enterprise Support proporciona una asignación de TAM designada, tiempos de respuesta de 15 minutos y Respuesta frente a incidencias de seguridad de AWS está disponible sin costo adicional, todo a un precio mínimo inferior de 5000\$ (reducido de 15 000\$). Para obtener más información, consulte los detalles del [Soporte plan AWS Enterprise](#). Para obtener más información, consulte [On-Ramp Fin del soporte para desarrolladores, empresas y empresas](#).

Developer Support, Business Support y Enterprise On-Ramp seguirán estando disponibles en la AWS GovCloud (US) región.

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).

- Usa una AWS Lambda función 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 respuestas Trusted Advisor, consulte las [Trusted Advisor herramientas](#) en GitHub

Notas

- Trusted Advisor ofrece eventos en función del mejor esfuerzo posible. No siempre se garantiza que los eventos se entreguen a EventBridge.
- Debe tener un plan AWS Business Support+, AWS Enterprise Support o AWS Unified Operations para crear una regla para las Trusted Advisor comprobaciones. Para obtener más información, consulte [Cambio AWS Support Planes](#).
-
- Como Trusted Advisor es un servicio global, todos los eventos se emiten EventBridge en la región de EE. UU. Este (Virginia del Norte).

Siga este procedimiento para crear una EventBridge regla para Trusted 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. Abra 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, elige AWS eventos 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. Para Event 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 comprobación.
 - INFORMACIÓN: no Trusted Advisor se puede determinar el estado de la comprobación.
 - OK: Trusted Advisor no detecta ningún problema con la comprobación.
 - ADVERTENCIA: Trusted Advisor detecta un posible problema en la comprobación y recomienda que se investigue.
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 de AWS recursos:
 - Elija Cualquier ID de recurso para crear una regla que supervise todos los recursos.

- Elija los ID de recursos específicos por ARN y, a continuación, introduzca los nombres de los recursos de Amazon (ARNs) que desee.
14. Elija 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. Elija 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 ahora supervisará las Trusted Advisor comprobaciones y, a continuación, enviará el evento al destino que especificó.

Crear CloudWatch alarmas de Amazon para monitorear AWS Trusted Advisor las métricas

Cuando AWS Trusted Advisor actualiza las comprobaciones, Trusted Advisor publica las métricas sobre los resultados de las comprobaciones en CloudWatch. Puede consultar las métricas en CloudWatch. También puede crear alarmas para detectar los cambios de estado de las Trusted Advisor comprobaciones y los cambios de estado de los recursos, así como el uso de las cuotas de servicio (antes denominadas límites).

Siga este procedimiento para crear una CloudWatch alarma para una Trusted Advisor métrica específica.

Temas

- [Requisitos previos](#)
- [CloudWatch métricas para Trusted Advisor](#)
- [Trusted Advisor métricas y dimensiones](#)

Requisitos previos

Antes de crear CloudWatch alarmas para Trusted Advisor las métricas, revise la siguiente información:

- Comprenda cómo se CloudWatch utilizan las métricas y las alarmas. Para obtener más información, consulta [Cómo CloudWatch funciona](#) en la Guía del CloudWatch usuario de Amazon.
- Usa la Trusted Advisor consola o la AWS Support API para actualizar tus comprobaciones y obtener los resultados más recientes. Para obtener más información, consulte [Actualizar resultados de verificaciones](#).

Para crear una CloudWatch alarma para Trusted Advisor las métricas

1. Abra la CloudWatch consola en <https://console.aws.amazon.com/cloudwatch/>.
2. Utilice el selector de regiones y elija la región EE.UU. Este (Norte de Virginia) AWS .
3. En el panel de navegación, elija Alarmas.
4. Elija Crear alarma.
5. Elija Seleccionar métrica.
6. Para Métricas, ingrese uno o varios valores de dimensión para filtrar la lista de métricas. Por ejemplo, puede introducir el nombre de la métrica ServiceLimitUsageo la dimensión, como el nombre del Trusted Advisor cheque.

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 [Trusted Advisor métricas y dimensiones](#).

7. En la tabla de resultados, active la casilla de la fila que contiene la métrica.

En el siguiente ejemplo, el nombre de la comprobación es IAM Access Key Rotation y el nombre de la métrica es YellowResources.

N. Virginia ▾	All > TrustedAdvisor > Check Metrics	Trusted ✕	Advisor ✕	IAM ✕	Access ✕	Key ✕
☐	CheckName (2)	Metric Name				
☐	IAM Access Key Rotation	RedResources				
☒	IAM Access Key Rotation	YellowResources				

8. Elija Seleccionar métrica.
9. En la página Especificar la métrica y las condiciones, compruebe que el nombre de la métrica y la CheckName que ha elegido aparecen 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 $\geq$ 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

- Para las YellowResources métricas GreenChecksRedChecksYellowChecks, RedResources, y, puede especificar un umbral que sea cualquier número entero mayor o igual a cero.
- Trusted Advisor no envía métricas para GreenResources, que son recursos para los que no Trusted Advisor ha detectado ningún problema.

12. Elija 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.

Notification

Alarm state trigger
Define the alarm state that will trigger this action.

☒ **In alarm**
The metric or expression is outside of the defined threshold.

☐ **OK**
The metric or expression is within the defined threshold.

☐ **Insufficient data**
The alarm has just started or not enough data is available.

Remove

Select an SNS topic
Define the SNS (Simple Notification Service) topic that will receive the notification.

☒ **Select an existing SNS topic**

☐ Create new topic

☐ Use topic ARN

Send a notification to...

X

Only email lists for this account are available.

Email (endpoints)
janedoe@example.com - [View in SNS Console](#)

Add notification

15. Elija Siguiente.
16. En Name and description (Nombre y descripción), ingrese un nombre y una descripción para la alarma.
17. Elija 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 de una CloudWatch alarma

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 "IAMAccessKeyRotationCheckAlarm" 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 Consola de administración de AWS:
<https://us-east-1.console.aws.amazon.com/cloudwatch/home?region=us-east-1#s=Alarms&alarm=IAMAccessKeyRotationCheckAlarm>

Alarm Details:

- Name: IAMAccessKeyRotationCheckAlarm
- 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:IAMAccessKeyRotationCheckAlarm

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:

CloudWatch métricas para Trusted Advisor

Puedes usar la CloudWatch consola o el AWS Command Line Interface (AWS CLI) para buscar las métricas disponibles Trusted Advisor.

Para obtener una lista de los espacios de nombres, las métricas y las dimensiones de todos los servicios que publican métricas, consulta los [AWS servicios que publican CloudWatch métricas](#) en la Guía CloudWatch del usuario de Amazon.

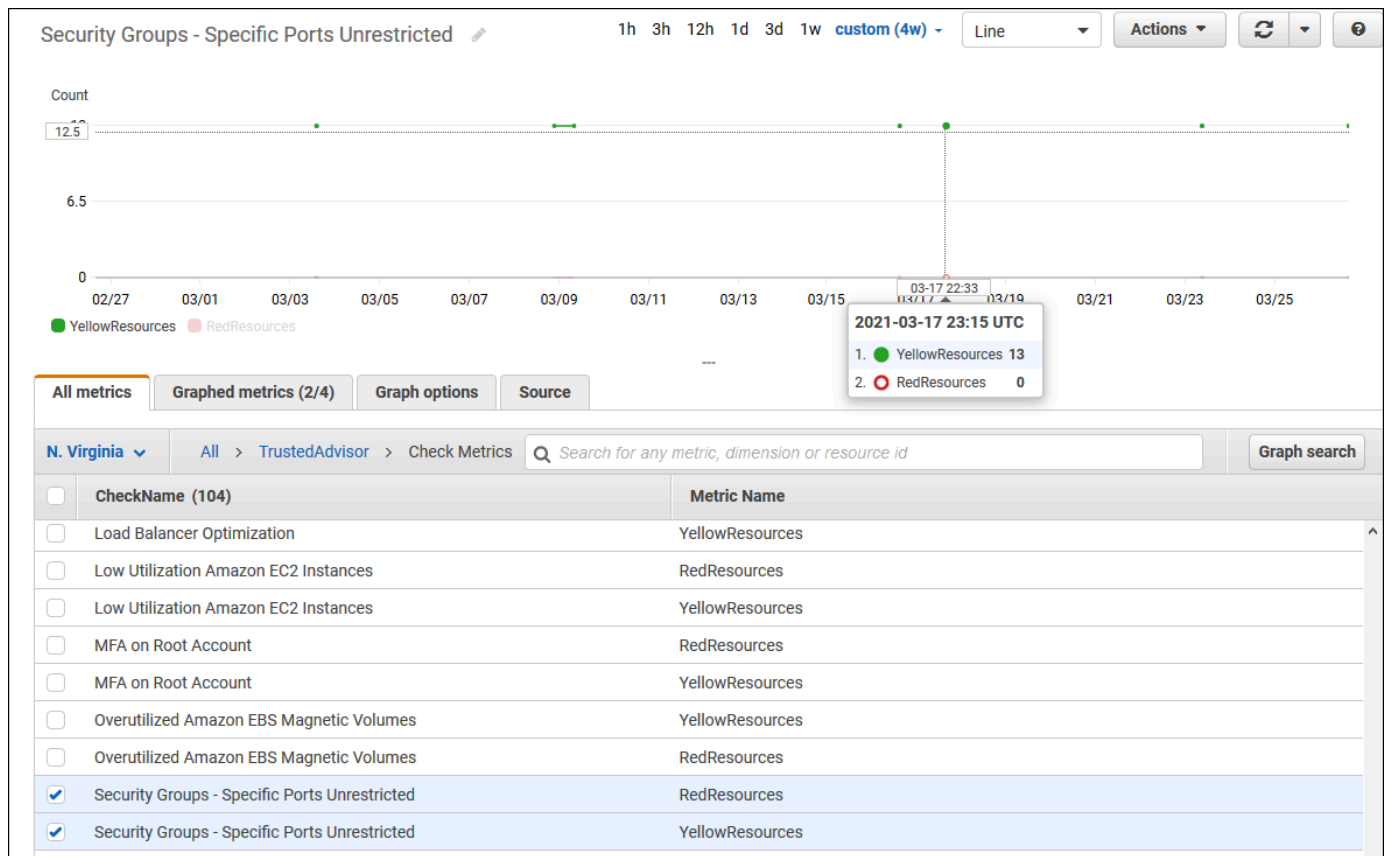
Ver Trusted Advisor las métricas (consola)

Puedes iniciar sesión en la CloudWatch consola y ver las métricas disponibles para Trusted Advisor.

Para ver Trusted Advisor las métricas disponibles (consola)

1. Abra la CloudWatch consola en <https://console.aws.amazon.com/cloudwatch/>.
2. Utilice el selector de regiones y elija la región EE.UU. Este (Norte de Virginia) AWS .
3. En el panel de navegación, seleccione 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. Se 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 marca identifica 13 recursos que son de color amarillo. Trusted Advisor recomienda que investigue los cheques amarillos.



7. (Opcional) Para agregar este gráfico a un CloudWatch panel, elija Acciones y, a continuación, elija Agregar al panel.

Para obtener más información sobre cómo crear un gráfico para ver tus métricas, consulta [Cómo graficar una métrica](#) en la Guía del CloudWatch usuario de Amazon.

Ver Trusted Advisor métricas (CLI)

Puede usar el AWS CLI comando [list-metrics](#) para ver las métricas disponibles de Trusted Advisor

Example: Enumere todas las métricas de Trusted Advisor

En el siguiente ejemplo, se especifica el espacio de AWS/TrustedAdvisor nombres para el que se van a ver todas las métricas. 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"
  },
  ...
]
```

Trusted Advisor métricas y dimensiones

Consulte las siguientes tablas para ver las Trusted Advisor métricas y dimensiones que puede usar para sus CloudWatch alarmas y gráficos.

Trusted Advisor métricas a nivel de comprobación

Puede utilizar las siguientes métricas para las Trusted Advisor comprobaciones.

Métrica	Description (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).

Trusted Advisor métricas a nivel de cuota de servicio

Puedes usar las siguientes métricas para Servicio de AWS las cuotas.

Métrica	Description (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 usar la siguiente dimensión para las Trusted Advisor comprobaciones.

Dimensión	Description (Descripción)
CheckName	El nombre del Trusted Advisor cheque. Puede encontrar todos los nombres de verificación en la consola de Trusted Advisor o AWS Trusted Advisor comprobar referencia .

Dimensiones de las métricas de cuota de servicio

Puede usar las siguientes dimensiones para las métricas Trusted Advisor de cuota de servicio.

Dimensión	Description (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 para eventos 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 el destinatario de la solicitud Trusted Advisor, la dirección IP desde la que 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 obtener más información, consulte los siguientes temas:

- [Introducción a la creación de registros de seguimiento](#)
- [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, consulte [Trusted Advisor actions](#).

 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 AWS Support API con AWS 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 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 usted especifique. CloudTrail Los archivos de registro contienen una o más entradas de registro. Un evento representa una solicitud única de cualquier fuente e incluye información sobre la acción solicitada, la fecha y la hora de la acción, los parámetros de la solicitud, etc. CloudTrail Los archivos de registro no son un registro ordenado de las 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](#).

En el caso de las instancias Amazon EC2 de Windows, puede utilizar EC2 Rescue para examinarlas y así identificar problemas comunes, recopilar archivos de registro y Soporte solucionar sus problemas. También puede usar EC2 Rescue para analizar los volúmenes de arranque de instancias que no funcionan. 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 AWS Support usted. 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	Link
Amazon Web Services	Solución de errores de la versión 4 de AWS Signature
Amazon API Gateway	Solución de problemas con HTTP APIs
Amazon AppStream	Solución de problemas de Amazon AppStream
Amazon Athena	Solución de problemas en Athena
Amazon Aurora MySQL	Solución de problemas de Amazon Aurora
PostgreSQL de Amazon Aurora	Solución de problemas de Amazon Aurora

Servicio	Link
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 SSL/TLS conexión
AWS Elastic Beanstalk	Solución de problemas
Amazon Elastic Compute Cloud (Amazon EC2)	Solución de problemas de instancias Solución de problemas de instancias de Windows Solución de problemas de VM Import/Export Solución de errores de solicitudes de API
Amazon Elastic Container Service (Amazon ECS)	Solución de problemas de Amazon ECS

Servicio	Link
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 (Memcached)	Solución de problemas de aplicaciones
Amazon ElastiCache (Redis OSS)	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)
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 en Amazon Data Firehose

Servicio	Link
AWS Lambda	AWS Lambda Funciones de resolución de problemas y supervisión con CloudWatch
OpenSearch Servicio Amazon	Solución de problemas de Amazon OpenSearch Service
Amazon Personalize	Solución de problemas
Amazon Quick	Solución de problemas de Amazon Quick 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
Amazon SageMaker AI	Solucionar errores Solución de problemas de Amazon SageMaker AI Studio
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

Servicio	Link
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 (Site-to-Site 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 revisión

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
Nuevo: ¿Se puede usar Agente de AWS DevOps con su AWS Support plan	Se agregó documentación para Agente de AWS DevOps habilitarla AWS Support Center Console si tu cuenta está en un Soporte plan que cumpla con los requisitos. Para obtener más información, consulta Cómo usarlo Agente de AWS DevOps con tu AWS Support plan .	8 de junio de 2026
Nuevo: Agente de AWS DevOps integración con la AI-enhanced solución de problemas	Se agregó documentación para la Agente de AWS DevOps integración con la AI-enhanced solución de problemas en la consola del Support Center, incluidas las capacidades de investigación autónoma de problemas operativos, los permisos de IAM necesarios y los detalles de las políticas administradas.	8 de junio de 2026

Para obtener más información, consulte la [AI-enhanced solución de problemas en la consola del Support Center](#).

[Procedimiento actualizado para solicitar una respuesta a un incidente en 5 minutos](#)

Se corrigió el paso de categoría en el procedimiento para solicitar una respuesta a un incidente de 5 minutos para las operaciones AWS unificadas. Para obtener más información, consulte [Cómo solicitar una respuesta a un incidente de 5 minutos](#).

18 de mayo de 2026

[Documentación actualizada para AWSTrustedAdvisorServiceRolePolicy](#)

Se agregaron nuevas acciones `ecs:ListClusters` de IAM y se `ecs:ListTaskDefinitionFamilies` incorporaron nuevos cheques. `ecs:ListTasks` `ecs:DescribeTasks` Para obtener más información, consulte [Políticas administradas de AWS : AWSTrustedAdvisorServiceRolePolicy](#).

14 de mayo de 2026

[Pasos actualizados para probar las llamadas a la API de Support Center Console](#)

Se actualizó el procedimiento para probar las llamadas a la API de Support Center Console a fin de incluir pasos para identificar los permisos de IAM faltantes mediante AWS CloudTrail. Para obtener más información, consulte [Probar las llamadas a la API de Support Center Console](#).

8 de mayo de 2026

[Fecha límite actualizada para las políticas de IAM de la API de Support Center Console](#)

Se actualizó la fecha límite del 2 de noviembre de 2026 al 16 de noviembre de 2026 para añadir las operaciones de Support Center Console a las políticas de IAM. Para obtener más información, consulte [Añadir políticas de IAM para las operaciones de la API de Support Center Console](#).

8 de mayo de 2026

[Procedimiento actualizado para solicitar una respuesta a un incidente en 5 minutos](#)

Se actualizó el procedimiento para solicitar una respuesta a incidentes en 5 minutos para las Operaciones AWS Unificadas. Para obtener más información, consulte [Cómo solicitar una respuesta a un incidente en 5 minutos](#).

4 de mayo de 2026

[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](#).

21 de abril de 2026

[Se agregó información de soporte en turco](#)

Se agregó información sobre la disponibilidad del soporte en turco para los casos de soporte. Para obtener más información, consulta [Cómo entender los tiempos de AWS Support respuesta](#).

14 de abril de 2026

[Fecha límite actualizada para las políticas de IAM de la API de Support Center Console](#)

Se actualizó la fecha límite del 1 de junio de 2026 al 2 de noviembre de 2026 para añadir las operaciones de Support Center Console a las políticas de IAM. Para obtener más información, consulte [Añadir políticas de IAM para las operaciones de la API de Support Center Console](#).

27 de marzo de 2026

[Se actualizó el cargo del equipo de Operaciones AWS Unificadas](#)

Se actualizó el título de especialista en migración a ingeniero de migraciónes y eventos en la sección del equipo de operaciones unificadas. Para obtener más información, consulte Ingeniero de [migraciones y eventos](#).

19 de marzo de 2026

[Documentación de AWS Support la aplicación actualizada para autorizar varias cuentas](#)

Se actualizaron los pasos manuales para autorizar varias cuentas sin usar CloudFormation plantillas. Para obtener más información, consulta [Autorizar varias cuentas](#) y [Crear recursos con CloudFormation](#).

27 de febrero de 2026

[Nueva comprobación de las pasarelas NAT inactivas](#)

Se agregó una nueva verificación para identificar las pasarelas NAT inactivas o infrautilizadas que podrían ser aptas para la optimización de costos. Para obtener más información, consulte el [registro de cambios de las comprobaciones AWS Trusted Advisor](#).

19 de febrero de 2026

[Actualizado: Gestiona el acceso al AWS Support Centro](#)

Se agregó una referencia al tema de operaciones de la API de Support Center Console para ayudar a los clientes a encontrar información sobre operaciones adicionales para sus políticas. Para obtener más información, consulte [Administrar el acceso al AWS Support Centro](#).

13 de febrero de 2026

[Nota actualizada en Añadir políticas de IAM para las operaciones de la API de Support Center Console](#)

Se actualizó la nota sobre el uso de una configuración de VPN personalizada. Para obtener más información, consulte [Añadir políticas de IAM para las operaciones de la API de Support Center Console](#).

11 de febrero de 2026

[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](#).

29 de enero de 2026

[Se agregaron las mejores prácticas y los tiempos de respuesta previstos para los casos de Enterprise Support en Crear un caso de soporte a partir de una interacción de soporte](#)

Se agregó una nueva sección desplegable que detalla las mejores prácticas para los clientes de Enterprise Support a la hora de crear casos para AWS Support. Para obtener más información, consulte [Crear un caso de soporte a partir de una interacción de soporte](#).

12 de enero de 2026

[Se dejaron de utilizar 5 comprobaciones de optimización de Trusted Advisor costes](#)

Para obtener más información, consulte el [registro de cambios para ver las AWS Trusted Advisor comprobaciones](#).

9 de enero de 2026

[AWS Support Planes de cambio actualizados](#)

Se ha añadido una nota en la que se detalla lo que ocurre si se añade o elimina una cuenta de una organización que está inscrita en AWS Business Support+. Para obtener más información, consulta [Cambiar AWS Support planes](#).

8 de enero de 2026

[Nueva sección: configure los permisos para utilizar la AI-enhanced solución de problemas](#)

Se agregó una nueva sección en la que se describe cómo configurar los permisos necesarios para la AI-enhanced solución de problemas en Service Catalog. Para obtener más información, consulte [Configurar los permisos para utilizar la AI-enhanced solución de problemas](#).

22 de diciembre de 2025

Referencia de Trusted Advisor cheque actualizada	Para obtener más información, consulte el registro de cambios para ver las AWS Trusted Advisor comprobaciones .	18 de diciembre de 2025
Referencia de Trusted Advisor verificación actualizada	Para obtener más información, consulte el registro de cambios para ver las AWS Trusted Advisor comprobaciones .	17 de diciembre de 2025
Se agregó información sobre las reuniones virtuales con AWS Support	Para obtener más información, consulte Reuniones virtuales con AWS Support .	9 de diciembre de 2025
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 .	8 de diciembre de 2025
Se agregó información sobre los nuevos AWS Support planes	Para obtener más información, consulte AWS Support Planes .	2 de diciembre de 2025
Se agregó información sobre la AI-enhanced solución de problemas	Para obtener más información, consulte la AI-enhanced solución de problemas en Support Center Console .	2 de diciembre de 2025
Se agregó información: una nueva sección para Operaciones AWS Unificadas	Para obtener más información, consulte Qué son las operaciones AWS unificadas .	2 de diciembre de 2025

[Se agregó una descripción para las API de Support Assistant](#)

Se agregaron acciones de AWS Support API para Support Assistant: ListInteractions, y ResolveInteraction en [Administrar el acceso al AWS Support Centro](#).

2 de diciembre de 2025

[Referencia de Trusted Advisor cheque actualizada](#)

Para obtener más información, consulte el [registro de cambios para ver las AWS Trusted Advisor comprobaciones](#).

21 de noviembre de 2025

[Referencia de Trusted Advisor cheque actualizada](#)

Para obtener más información, consulte el [registro de cambios para ver las AWS Trusted Advisor comprobaciones](#).

17 de noviembre de 2025

[Se actualizó la edición y eliminación de un rol vinculado a un servicio para Soporte](#)

Los clientes que se hayan incorporado a AWS Organizations un plan Enterprise Support pueden eliminar el rol vinculado al AWSServiceRoleForSupport servicio. Para obtener más información, consulte [Edición y eliminación de un rol vinculado al servicio de Soporte](#).

31 de octubre de 2025

[Referencia de Trusted Advisor cheque actualizada](#)

Para obtener más información, consulte el [registro de cambios para ver las AWS Trusted Advisor comprobaciones](#).

15 de octubre de 2025

[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](#).

30 de septiembre de 2025

[Nuevo tema](#)

Se agregó un tema nuevo con información sobre cómo activar las notificaciones de caducidad de los planes promocionales. Para obtener más información, consulte [Configurar las notificaciones de caducidad de los planes promocionales](#).

12 de septiembre de 2025

[Trusted Advisor Cheque actualizado](#)

Para obtener más información, consulte el [registro de cambios para ver las AWS Trusted Advisor comprobaciones](#).

11 de septiembre de 2025

[Se actualizó Pruebas de las llamadas a la API de la consola del centro de soporte](#)

Se actualizó el paso 3 para indicar la fuente correcta del evento, support-console.amazonaws.com. Para obtener más información, consulte [Pruebas de las llamadas a la API de la consola del centro de soporte](#).

2 de septiembre de 2025

AWS Support Planes cambiantes actualizados	Se han actualizado los pasos para mejorar o reducir tu AWS Support suscripción. Para obtener más información, consulta Cómo cambiar AWS Support los planes .	27 de agosto de 2025
Trusted Advisor Cheque actualizado	Para obtener más información, consulte el registro de cambios para ver las AWS Trusted Advisor comprobaciones .	19 de agosto de 2025
Se ha eliminado la sección Trusted Advisor Engage	Se ha eliminado la sección Comenzar AWS Trusted Advisor a usar Engage (vista previa).	7 de agosto de 2025
Se ha actualizado la forma de añadir la AWS Support aplicación a un canal de Slack	Para obtener más información, consulte Configuración de un canal de Slack .	6 de agosto de 2025
Dos verificaciones están en desuso	Para obtener más información, consulta el registro de cambios para ver las AWS Trusted Advisor comprobaciones .	22 de julio de 2025
Políticas gestionadas actualizadas: AWSSupportAccess	Para obtener más información, consulte AWS Support las actualizaciones de las políticas AWS gestionadas .	18 de julio de 2025

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 .	15 de julio de 2025
Verificación actualizada: las instancias de Amazon EC2 con Ubuntu LTS han dejado de tener soporte estándar	Para obtener más información, consulta el registro de cambios para ver las AWS Trusted Advisor comprobaciones .	3 de julio de 2025
Trusted Advisor Comprobación actualizada: permisos de bucket de Amazon S3	Para obtener más información, consulte el registro de cambios para ver las AWS Trusted Advisor comprobaciones .	3 de julio de 2025
Verificación actualizada: MFA en la cuenta raíz	Para obtener más información, consulta el registro de cambios para ver las AWS Trusted Advisor comprobaciones .	2 de julio de 2025
Comprobación actualizada: Amazon ECS AWS registra el controlador en modo de bloqueo.	Para obtener más información, consulte el registro de cambios para ver las AWS Trusted Advisor comprobaciones .	2 de julio de 2025

[Se actualizó Solicite un aumento de la cuota de servicio.](#)

Se agregó información sobre cómo crear una solicitud de aumento de la cuota de servicio si la consola Service Quotas admite Servicio de AWS o Región de AWS no. Para obtener más información, consulte [Solicite un aumento de la cuota de servicio.](#)

2 de julio de 2025

[Ya no se admite la creación de una solicitud de aumento de la cuota de servicio en la consola del centro de soporte.](#)

Para obtener más información, consulte [Creación de un aumento de cuota de servicio.](#)

23 de junio de 2025

[Se agregó una descripción para UpdateInteraction en la Soporte API](#)

Se agregó AWS Soporte la descripción de UpdateInteraction las acciones de la API en [Administrar el acceso al AWS Support Centro.](#)

23 de junio de 2025

[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 junio de 2025

[Nueva sección: Acerca de la API de la consola del centro de soporte](#)

La API de la consola del centro de soporte mejora la experiencia con dicha consola. Para obtener más información, consulte [Acerca de la API de la consola del centro de soporte](#).

16 de junio de 2025

[Se actualizó la introducción AWS Trusted Advisor del capítulo para reflejar que los planes Basic y Developer Support no admiten la actualización automática de comprobaciones. Se deben actualizar manualmente los controles de seguridad para ver el estado de los controles más recientes.](#)

Para obtener más información, consulte [AWS Trusted Advisor](#).

11 de junio de 2025

[Comprobación actualizada: el uso AWS STS global de terminales en todos los niveles del plan ya Regiones de AWS está disponible en todos los niveles del AWS Support plan.](#)

Para obtener más información, consulta el [registro de cambios para ver las AWS Trusted Advisor comprobaciones](#).

9 de junio de 2025

[Nueva verificación: recomendaciones de optimización de costos de Amazon Aurora para el almacenamiento en clústeres de bases de datos](#)

Para obtener más información, consulta el [registro de cambios para ver las AWS Trusted Advisor comprobaciones](#).

9 de junio de 2025

Nueva comprobación: uso AWS STS global de terminales en todas partes Regiones de AWS	Para obtener más información, consulte el registro de cambios para ver las AWS Trusted Advisor comprobaciones .	2 de junio de 2025
15 Centro de optimización de costes de AWS cheques nuevos se suman a Trusted Advisor	Para obtener más información, consulte el registro de cambios para ver las AWS Trusted Advisor comprobaciones .	30 de mayo de 2025
Se actualizaron tres Trusted Advisor comprobaciones	Para obtener más información, consulta el registro de cambios para ver las AWS Trusted Advisor comprobaciones .	21 de mayo de 2025
Nueva característica: actualización de la gravedad de los casos de soporte	Para obtener más información, consulte la sección Cambiar el nivel de gravedad de un caso de soporte Creación de casos de soporte y administración de casos .	21 de mayo de 2025
Hora actualizada en la que puede ver los detalles del AWS Support caso.	Para obtener más información, consulta Seguridad para tus AWS Support casos .	29 de abril de 2025
Se actualizaron dos Trusted Advisor comprobaciones	Para obtener más información, consulte el registro de cambios para ver las AWS Trusted Advisor comprobaciones .	2 de abril de 2025

[Se agregó una descripción para la Soporte API](#)

Se agregó una descripción de las acciones de la AWS Soporte API en [Administrar el acceso al AWS Support Centro](#).

7 de marzo de 2025

[Se han dejado de utilizar 6 comprobaciones AWS Security Hub CSPM](#)

Para obtener más información, consulte el [registro de cambios para ver las AWS Trusted Advisor comprobaciones](#).

5 de marzo de 2025

[Se eliminaron las referencias a las métricas a nivel de categoría para Trusted Advisor](#)

Category-level las métricas de Trusted Advisor están en desuso. Las referencias a las métricas a nivel de categoría se eliminan de la sección Creación de [CloudWatch alarmas de Amazon para monitorizar AWS Trusted Advisor](#) las métricas.

27 de enero de 2025

[Documentación actualizada para Trusted Advisor](#)

Se agregaron dos nuevas comprobaciones: AWS CloudTrail Management Events Logging y Amazon RDS Continuous Backups Not Enabled. Para obtener más información, consulte el [registro de cambios para ver las AWS Trusted Advisor comprobaciones](#).

23 de diciembre de 2024

[Documentación actualizada para Trusted Advisor](#)

Se actualizaron los recursos de grupo de escalado automático. Para obtener más información, consulte [el registro de cambios de las AWS Trusted Advisor comprobaciones](#).

23 de diciembre de 2024

[Documentación actualizada para Trusted Advisor](#)

Se actualizó la verificación de acceso externo de IAM Access Analyzer. Para obtener más información, consulte [el registro de cambios de las AWS Trusted Advisor comprobaciones](#).

23 de diciembre 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](#).

25 de noviembre de 2024

[Documentación actualizada para Trusted Advisor](#)

Se agregó 1 Trusted Advisor cheque nuevo. Para obtener más información, consulta [el registro de cambios de las AWS Trusted Advisor comprobaciones](#).

22 de noviembre de 2024

[Se agregó documentación para las políticas AWS administradas de AWS Partner-Led Support](#)

Se agregó documentación para una nueva política AWS administrada `AWSPartnerLedSupportReadOnlyAccess` . Para obtener más información, consulte [políticas AWS gestionadas de AWS Partner-Led Support](#).

22 de noviembre de 2024

[Documentación actualizada para Trusted Advisor](#)

Se actualizaron 3 Trusted Advisor controles. Para obtener más información, consulte [el registro de cambios de las AWS Trusted Advisor comprobaciones](#).

7 de noviembre de 2024

[Documentación actualizada de los AWS Support planes](#)

Se agregó un nuevo ejemplo de registro de la `ListSupportPlanModifiers` operación a la AWS CloudTrail página de [llamadas a la API Logging Soporte Plans](#).

6 de noviembre de 2024

[Documentación actualizada para `AWSTrustedAdvisorServiceRolePolicy`](#)

Se agregaron nuevas acciones de IAM `elasticloadbalancing:DescribeListeners` y `elasticloadbalancing:DescribeRules` , para incorporar un nuevo control de seguridad. Para obtener más información, consulte [Políticas administradas de AWS : `AWSTrustedAdvisorServiceRolePolicy`](#).

30 de octubre de 2024

[Documentación actualizada para Trusted Advisor](#)

Se agregaron 4 Trusted Advisor cheques nuevos. Para obtener más información, consulte [el registro de cambios de las AWS Trusted Advisor comprobaciones](#).

11 de octubre 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](#).

8 de octubre de 2024

[Documentación actualizada para Trusted Advisor](#)

Se movió una verificación de optimización de costos al pilar de tolerancia a errores. Se actualizó un control de seguridad y un control de tolerancia a errores. Para obtener más información, consulte [el registro de cambios de las AWS Trusted Advisor comprobaciones](#).

2 de octubre de 2024

[Se actualizó la sección AWS Trusted Advisor Engage](#)

Se actualizó la sección AWS Trusted Advisor Engage para hacer referencia a AWS Countdown. Para obtener más información, consulte Comenzar a usar AWS Trusted Advisor Engage (versión preliminar).

16 de septiembre de 2024

[Documentación actualizada de los AWS Support planes](#)

Se agregó un nuevo permiso y CloudTrail documentación para ver una lista de modificadores del plan de soporte. Para obtener más información, consulte [Administrar el acceso a AWS Support los planes, AWS administrar las políticas de los AWS Support planes y Registrar las llamadas a la API de AWS Support los planes con AWS CloudTrail ellos.](#)

9 de septiembre de 2024

[Documentación actualizada para Trusted Advisor](#)

Trusted Advisor se agregaron 9 nuevos cheques el 23 de agosto. Para obtener más información, consulte [el registro de cambios de AWS Trusted Advisor cheques.](#)

23 de agosto de 2024

[Documentación actualizada para Trusted Advisor](#)

Se actualizó 1 control de excelencia Trusted Advisor operativa y se agregó 1 nuevo control Trusted Advisor de seguridad. Para obtener más información, consulte [el registro de cambios de las AWS Trusted Advisor comprobaciones.](#)

22 de agosto de 2024

[Documentación actualizada para Trusted Advisor](#)

Se actualizaron 6 controles Trusted Advisor de seguridad. Para obtener más información, consulta [el registro de cambios de las AWS Trusted Advisor comprobaciones.](#)

20 de agosto de 2024

[Documentación actualizada
para Trusted Advisor](#)

Se actualizaron 2 Trusted Advisor controles. Para obtener más información, consulte [el registro de cambios de las AWS Trusted Advisor comprobaciones](#).

12 de agosto 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](#).

5 de agosto de 2024

[Documentación actualizada
para Trusted Advisor](#)

Se actualizaron 9 Trusted Advisor cheques. Para obtener más información, consulte [el registro de cambios de las AWS Trusted Advisor comprobaciones](#).

21 de julio de 2024

[Documentación actualizada
para AWSTrustedAdvisorS
erviceRolePolicy](#)

11 de junio de 2024

Se agregaron las 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-firewall:DescribeFirewall y sqs:GetQueueAttributes para incorporar verificaciones nuevas. Para obtener más información, consulte [Políticas administradas de AWS : AWSTrustedAdvisorServiceRolePolicy](#).

<u>Se eliminaron 5 AWS Trusted Advisor cheques de la documentación</u>	Se eliminaron 5 AWS Trusted Advisor comprobaciones que ahora están en desuso. Para obtener más información, consulte el <u>registro de cambios de las AWS Trusted Advisor comprobaciones</u> .	15 de mayo de 2024
<u>Se agregó 1 nuevo control AWS Trusted Advisor de seguridad a la documentación</u>	Se agregó 1 nuevo control AWS Trusted Advisor de seguridad a la documentación. Para obtener más información, consulte <u>el registro de cambios de las AWS Trusted Advisor comprobaciones</u> .	15 de mayo de 2024
<u>Se eliminaron tres verificaciones de tolerancia a errores de la documentación</u>	Se eliminaron tres verificaciones de tolerancia a errores que ahora se encuentran obsoletas. Para obtener más información, consulte <u>el registro de cambios de las AWS Trusted Advisor comprobaciones</u> .	25 de abril de 2024
<u>Se actualizó la documentación sobre la tolerancia a errores y los controles de seguridad</u>	Se agregó una nueva verificación de tolerancia a errores. Se actualizó un control de tolerancia a errores y un control de seguridad. Para obtener más información, consulte <u>el registro de cambios de las AWS Trusted Advisor comprobaciones</u> .	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 Soporte plan](#)

Actualizaciones de las características de Soporte los planes. Para más información, consulte [Planes de Soporte](#).

11 de marzo de 2024

[Documentación actualizada para Trusted Advisor](#)

Se agregó una verificación de tolerancia a errores. Para obtener más información, consulte [el registro de cambios de las AWS Trusted Advisor comprobaciones](#).

29 de febrero de 2024

[Documentación actualizada para Trusted Advisor](#)

Se agregó una verificación de tolerancia a errores. Para obtener más información, consulte [el registro de cambios de las AWS Trusted Advisor comprobaciones](#).

31 de enero de 2024

[Documentación actualizada para AWSTrustedAdvisorServiceRolePolicy](#)

Se agregaron las nuevas acciones de IAM `cloudtrail:GetTrail` , `cloudtrail:ListTrails` , `cloudtrail:GetEventSelectors` , `outposts:GetOutpost` , `outposts:ListAssets` y `outposts:ListOutposts` para incorporar verificaciones nuevas. 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 una verificación de tolerancia a errores para modificar el título y la descripción. Para obtener más información, consulte [el registro de cambios de las AWS Trusted Advisor comprobaciones](#).

8 de enero de 2024

[Documentación actualizada para Trusted Advisor](#)

Se actualizó un control de seguridad para reflejar el cambio en el período de obsolescencia. Para obtener más información, consulte [el registro de cambios de las AWS Trusted Advisor comprobaciones](#).

21 de diciembre de 2023

[Documentación actualizada para Trusted Advisor](#)

Se agregaron dos controles de seguridad y dos 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 un control de seguridad. Para obtener más información, consulte [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 contrataciones programadas.

11 de diciembre de 2023

[Documentación actualizada
para Trusted Advisor](#)

Se agregaron dos nuevas verificaciones de tolerancia a errores y una verificación de optimización de costos. Para obtener más información, consulte [el registro de cambios de las AWS Trusted Advisor comprobaciones](#).

7 de diciembre 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](#).

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 ID 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 agregaron tres nuevas verificaciones de tolerancia a errores. Para obtener más información, consulte [el registro de cambios de las AWS Trusted Advisor comprobaciones](#).

17 de noviembre de 2023

[Documentación actualizada para Trusted Advisor](#)

Se agregaron 37 nuevas verificaciones 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 agregaron nuevas acciones de IAM `ec2:DescribeRegions`, `s3:GetLifecycleConfiguration`, `ecs:DescribeTaskDefinition` y `ecs:ListTaskDefinitions` para incorporar verificaciones nuevas. 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:ListResolveEndpoints , route53resolver:ListResolveEndpointIpAddresses , 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 crear y editar las 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 Resiliency 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 [Comenzar a usar Engage](#).
AWS Trusted Advisor

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:

16 de febrero de 2023

- Los botones Confirmar y Descartar han reemplazado 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 información, consulta [Cómo empezar a usar Trusted Advisor Priority](#).

[Ejemplos de código actualizados para Soporte](#)

Se agregaron ejemplos de código.NET, Java y Kotlin que muestran cómo usarlos Soporte con un kit de desarrollo de AWS software (SDK). Para obtener más información, consulta [Ejemplos de código para Soporte usar los AWS SDK](#).

16 de enero 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](#).

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:

14 de diciembre de 2022

- 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](#).

[Documentación actualizada para AWS Support](#)

Se agregó documentación sobre los nuevos puntos finales de la Soporte API. Para más información, consulte [Sobre la API de AWS Support](#).

14 de diciembre de 2022

[Se agregó documentación sobre las CloudFormation plantillas que se usarán en la AWS Support aplicación en Slack](#)

Puedes usar CloudFormation plantillas para crear espacios de trabajo y canales de configuración de Slack para ello. Cuentas de 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 Resiliencia 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 CSPM hallazgos en Trusted Advisor](#)

Los hallazgos de los controles CSPM de Security Hub se eliminan Trusted Advisor más rápido. Para obtener más información, consulte el [registro de cambios para AWS Trusted Advisor](#) ver las 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:

29 de septiembre de 2022

- [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](#)

[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 [Configuración 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: 24 de agosto de 2022

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 información, 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](#).

[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:

17 de agosto de 2022

- 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](#).

[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](#).

[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](#)

[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](#).

[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 CSPM. Para obtener más información, consulte el [registro de cambios para ver las AWS Trusted Advisor comprobaciones](#).

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 actualizado 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 para usar Amazon EventBridge para monitorear AWS Support casos](#)

Puedes crear una EventBridge regla para supervisar y recibir notificaciones sobre tus casos de soporte. Para obtener más información, consulte [Supervisar Soporte 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 CSPM](#)

En la Trusted Advisor consola, ahora puede ver los resultados de los controles CSPM 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 CSPM los controles](#) de la consola. AWS Trusted Advisor

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.

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

Para obtener más información, consulte [Referencia de verificaciones de AWS Trusted Advisor](#).

[Documentación actualizada para Trusted Advisor](#)

Trusted Advisor se agregaron cuatro nuevas comprobaciones para AWS Well-Architected

20 de diciembre de 2021

- 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](#).

[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 agregó 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 Soporte 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:

12 de mayo de 2021

- 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](#)

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 al servicio para 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 el Registro 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 Registrar los cambios en su Soporte plan .	9 de febrero de 2021
Documentación actualizada para Trusted Advisor	Se ha actualizado el tema Comience con Trusted Advisor las recomendaciones .	29 de enero de 2021

Cambio	Descripción	Fecha
Documentación actualizada para los Trusted Advisor informes	Se agregó una Resolución 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 AWS Trusted Advisor información al iniciar CloudTrail sesión .	22 de octubre de 2020
Se agregaron AWS Support cuotas	Se ha agregado información sobre las cuotas y restricciones actuales de Soporte. Consulte los puntos de enlace y las cuotas Soporte en Referencia general de AWS.	4 de agosto de 2020
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 de AWS Trusted Advisor .	17 de julio de 2020

Cambio	Descripción	Fecha
Seguridad y AWS Support	Se ha actualizado información sobre consideraciones 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 Service-linked roles	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 administración 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 con CloudWatch eventos	Se ha agregado una nueva sección.	18 de noviembre de 2016
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

Cambio	Descripción	Fecha
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 Consola de administración de AWS.	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

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.