aws

Guía del usuario de

Administrador de incidentes de

Administrador de incidentes de: Guía del usuario de

Table of Contents

Administrador de incidentes de AWS Systems Manager ya no está abierto a nuevos clientes. Los clientes existentes pueden seguir utilizando el servicio con normalidad. Para obtener más información, consulte Cambio en la disponibilidad de Administrador de incidentes de AWS Systems Manager.

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

¿Qué es Administrador de incidentes de AWS Systems Manager?

Incident Manager, una herramienta incluida AWS Systems Manager, está diseñada para ayudarlo a mitigar los incidentes que afecten a sus aplicaciones alojadas y a recuperarse de ellos AWS.

En este contexto AWS, un incidente es cualquier interrupción o reducción no planificada de la calidad de los servicios que puede tener un impacto significativo en las operaciones comerciales. Por lo tanto, es esencial que las organizaciones establezcan una estrategia de respuesta de mitigación y recuperación eficaz ante incidentes e implementen acciones para prevenirlos en el futuro.

Para ayudar a reducir el tiempo de resolución de incidentes, Incident Manager:

- Proporciona planes automatizados que involucra de manera eficiente a las personas responsables de responder a los incidentes.
- Proporciona datos relevantes para la solución de problemas.
- Habilita acciones de respuesta automatizadas mediante manuales de procedimientos de automatización predefinidos.
- Proporciona métodos para colaborar y comunicar con todas las partes interesadas.

Las características y los flujos de trabajo integrados en Incident Manager se basan en las prácticas recomendadas de respuesta a incidentes que Amazon ha venido desarrollando casi desde su creación. Incident Manager se integra con Amazon CloudWatch AWS CloudTrail, AWS Systems Manager, y Amazon EventBridge. Servicios de AWS

Componentes y características principales

En esta sección se describen las características de Incident Manager que usted utiliza para configurar sus planes de respuesta a incidentes.

Plan de respuesta

Un plan de respuesta funciona como una plantilla que define lo que se debe establecer al producirse un incidente. Incluye información como:

- Quién debe responder al producirse un incidente.

- La respuesta automatizada establecida para mitigar el incidente.
- La herramienta de colaboración que los respondedores deben utilizar para comunicar y recibir notificaciones automáticas sobre el incidente.

Detección de incidentes

Puede configurar CloudWatch las alarmas de Amazon y EventBridge los eventos de Amazon para crear incidentes cuando se detecten condiciones o cambios que afecten a sus AWS recursos.

Soporte de automatización de manuales de procedimientos

Puede iniciar manuales de procedimientos de automatización desde Incident Manager para automatizar su respuesta crítica a los incidentes y proporcionar pasos detallados a los respondedores iniciales.

Participación y escalada

Un plan de participación especifica a quiénes se debe enviar una notificación para cada incidente único. Puede especificar contactos individuales que haya añadido a Incident Manager o especificar un horario de guardia que haya creado en Incident Manager. Los planes de participación también especifican una ruta de escalada para ayudar a garantizar la visibilidad entre las partes interesadas y la participación activa durante el proceso de respuesta a incidentes.

Horarios de guardia

Un horario de guardia en Incident Manager consta de una o más rotaciones que usted crea para el horario. Para cada rotación, puede incluir hasta 30 contactos. El horario de guardia, al añadirlo a un plan de escalada o de respuesta, define a quién se notifica al producirse un incidente que requiera la intervención de un respondedor. Los horarios de guardia le permiten asegurarse de que dispone de una cobertura completa, redundante e ininterrumpida (24/7) según sea necesario para su respuesta a incidentes.

Colaboración activa

El personal de respuesta a incidentes responde activamente a los incidentes mediante la integración con Amazon Q Developer en el cliente de aplicaciones de chat. Amazon Q Developer en aplicaciones de chat admite la creación de canales de chat para Incident Manager que utilizan Slack, Microsoft Teams, o Amazon Chime. Los socorristas pueden comunicarse directamente entre sí, recibir notificaciones automáticas sobre los incidentes y... Slack y Microsoft Teams—ejecute directamente algunas operaciones de la interfaz de línea de comandos (CLI) de Incident Manager.

Diagnóstico de incidentes

El personal de respuesta puede ver la up-to-date información en la consola de Incident Manager durante un incidente. En función de los cambios en la información, los respondedores pueden crear elementos de seguimiento y corregirlos mediante manuales de procedimientos de automatización.

Resultados de otros servicios

Para apoyar el diagnóstico de incidentes de los respondedores, puede habilitar la característica Resultados en Incident Manager. Los resultados son información sobre AWS CodeDeploy las implementaciones y las actualizaciones de la AWS CloudFormation pila que se produjeron alrededor del momento de un incidente y que implicaron uno o más recursos probablemente relacionados con el incidente. Disponer de esta información reduce el tiempo necesario para evaluar las causas potenciales, lo que puede reducir el tiempo medio de recuperación (MTTR) de un incidente.

Análisis post-incidente

Una vez resuelto un incidente, utilice un análisis post-incidente para identificar mejoras en su respuesta a incidentes, incluyendo el tiempo de detección y mitigación. Un análisis también puede ayudarle a comprender la causa raíz de los incidentes. Incident Manager crea elementos de acción de seguimiento recomendados que puede utilizar para mejorar su respuesta a los incidentes.

Beneficios del uso de Incident Manager

Obtenga información sobre los beneficios que brinda Incident Manager en sus operaciones de detección y respuesta a incidentes.

En esta sección se describen los beneficios que su organización puede obtener al implementar un plan de respuesta con Incident Manager.

Diagnóstico de problemas de manera eficaz e inmediata

CloudWatch Las alarmas de Amazon y EventBridge los eventos de Amazon que configure pueden crear incidentes automáticamente cuando se produzca una interrupción no planificada o una reducción de la calidad de sus servicios.

CloudWatch las alarmas detectan e informan cuando se producen cambios en el valor de la métrica o expresión en relación con un umbral durante varios períodos de tiempo. EventBridge los eventos

se crean como resultado de un cambio en un entorno, una aplicación o un servicio que se haya especificado en una EventBridge regla. Al crear una alarma o un evento, puede especificar una acción para que se cree un incidente en Incident Manager y el plan de respuesta apropiado para facilitar el afrontamiento, la escalada y la mitigación del incidente.

El administrador de incidentes permite recopilar y rastrear automáticamente las métricas relacionadas con un incidente mediante el uso de CloudWatch métricas. Además de las métricas automatizadas que se generan para el incidente cuando se crea mediante una CloudWatch alarma, puede añadir métricas manualmente en tiempo real para proporcionar contexto y datos adicionales a los responsables de un incidente.

Utilice la línea temporal de incidentes de Incident Manager para mostrar los puntos de interés en orden cronológico. Los respondedores también pueden utilizar la línea temporal para añadir eventos personalizados que describan lo que hicieron o lo que ocurrió. Los puntos de interés automatizados incluyen:

- Una CloudWatch alarma o EventBridge regla crea un incidente.
- Las métricas de los incidentes se comunican a Incident Manager.
- Los respondedores participan.
- Los pasos del manual de procedimientos se completan con éxito.

Participación eficaz

Incident Manager reúne a los respondedores de incidentes mediante el uso de contactos, horarios de guardia, planes de escalada y canales de chat. Usted define los contactos individuales directamente en Incident Manager y especifica las preferencias de contacto (correo electrónico, SMS o voz). Usted añade contactos a las rotaciones de los planes de guardia para determinar quién está encargado de atender las incidencias durante un periodo determinado. Al utilizar los contactos definidos y los horarios de guardia, usted crea planes de escalada para involucrar a los respondedores necesarios en el momento adecuado durante un incidente.

Colaboración en tiempo real

La comunicación durante un incidente es el elemento clave para una resolución más rápida. Uso de un Amazon Q Developer en un cliente de aplicaciones de chat configurado para usar Slack, Microsoft Teams, o Amazon Chime, puedes reunir a los socorristas en su canal de chat conectado preferido, donde interactúan directamente con el incidente y entre sí. Incident Manager también muestra las

acciones en tiempo real de los respondedores de incidentes en el canal de chat, proporcionando contexto a los demás.

Automatización del restablecimiento del servicio

Incident Manager permite a sus respondedores centrarse en las tareas clave necesarias para resolver un incidente mediante el uso de manuales de procedimientos automatizados. En Incident Manager, los manuales de procedimientos son una serie de acciones predefinidas para resolver un incidente. Combinan la potencia de las tareas automatizadas con pasos manuales según sea necesario, lo que da a los respondedores más disponibilidad para analizar y responder al impacto.

Prevención de futuros incidentes

Mediante el análisis post-incidente de Incident Manager, su equipo puede desarrollar planes de respuesta más sólidos y efectuar cambios en todas sus aplicaciones para prevenir futuros incidentes y tiempos de inactividad. El análisis post-incidente también permite el aprendizaje iterativo y la mejora de los manuales de procedimientos, los planes de respuesta y las métricas.

Servicios relacionados

Incident Manager se integra con varios servicios Servicios de AWS y herramientas de otros fabricantes para ayudarle a detectar y resolver incidentes, así como a interactuar indirectamente con sus operaciones de API y gestionar la infraestructura. Para obtener más información, consulte Integraciones de productos y servicios con Incident Manager.

Acceso a Incident Manager

Puede acceder a Incident Manager de cualquiera de las siguientes formas:

- La consola de Incident Manager
- AWS CLI: Para obtener información general, consulte Introducción a la AWS CLI en la Guía del usuario de AWS Command Line Interface . Para obtener información sobre los comandos de CLI para Incident Manager, consulte ssm-incidents y ssm-contactsen la Referencia de AWS CLI comandos.
- API de Incident Manager: Para obtener más información, consulte la Referencia de la API de Administrador de incidentes de AWS Systems Manager.
- AWS SDKs— Para obtener más información, consulte Herramientas sobre las que construir AWS.

Regiones y cuotas de Incident Manager

Incident Manager no es compatible con todos los sistemas Regiones de AWS compatibles con Systems Manager.

Para obtener información sobre regiones y cuotas de Incident Manager, consulte Puntos de conexión y cuotas de Administrador de incidentes de AWS Systems Manager en Referencia general de Amazon Web Services.

Precios de Incident Manager

El uso de Incident Manager tiene un costo. Para obtener más información, consulte Precios de AWS Systems Manager.

> **Note**
>
> El resto Servicios de AWS del AWS contenido y el contenido de terceros que estén disponibles en relación con este servicio pueden estar sujetos a cargos separados y regirse por condiciones adicionales.

Para obtener una descripción general de Trusted Advisor un servicio que le ayuda a optimizar los costos, la seguridad y el rendimiento de su AWS entorno, consulte AWS Trusted Advisorla Guía del AWS Support usuario.

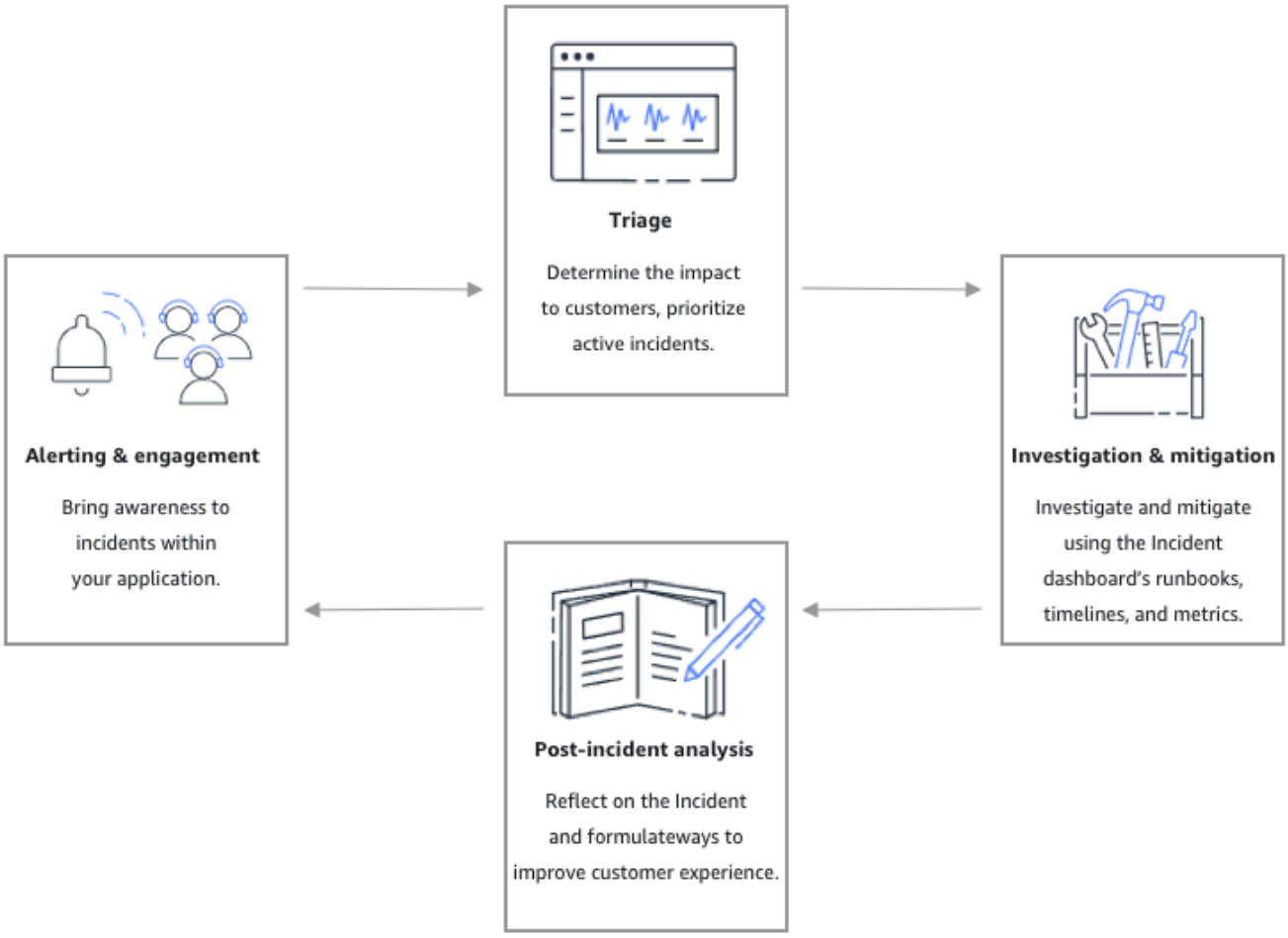
Ciclo de vida del incidente en Incident Manager

Administrador de incidentes de AWS Systems Manager proporciona un step-by-step marco basado en las mejores prácticas para identificar incidentes y reaccionar ante ellos, como las interrupciones del servicio o las amenazas a la seguridad. El objetivo principal de Incident Manager es ayudar a restablecer la normalidad de los servicios o aplicaciones afectados lo antes posible mediante una solución completa de administración del ciclo de vida de los incidentes.

Como se muestra en la siguiente ilustración, Incident Manager proporciona herramientas y mejores prácticas para cada fase del ciclo de vida de los incidentes:

- Alerta e intervención
- Triaje

- Investigación y mitigación
- Análisis post-incidente



Alerta e intervención

La fase de alerta e intervención del ciclo de vida del incidente se centra en dar a conocer los incidentes dentro de sus aplicaciones y servicios. Esta fase comienza antes de que se detecte un incidente y requiere un profundo conocimiento de sus aplicaciones. Puedes usar CloudWatchlas métricas de Amazon para monitorear los datos sobre el rendimiento de tus aplicaciones o usar Amazon EventBridge para agregar alertas de diferentes fuentes, aplicaciones y servicios. Después de haber configurado el monitoreo de sus aplicaciones, puede comenzar a alertar sobre las métricas que se desvían de la norma histórica. Para obtener más información sobre las prácticas recomendadas de monitoreo, consulte Supervisión.

Para apoyar el diagnóstico de incidentes de los respondedores, puede habilitar la característica Resultados en Incident Manager. Los resultados son información sobre AWS CodeDeploy las implementaciones y las actualizaciones de la AWS CloudFormation pila que se produjeron en torno al momento de un incidente. Disponer de esta información reduce el tiempo necesario para evaluar las causas potenciales, lo que puede reducir el tiempo medio de recuperación (MTTR) de un incidente.

Ahora que está monitoreando los incidentes en sus aplicaciones, puede definir un plan de respuesta a incidentes a fin de utilizarlo durante un incidente. Para obtener más información sobre la creación de planes de respuesta, consulte Creación y configuración de planes de respuesta en Incident Manager. EventBridge Los eventos o CloudWatch alarmas de Amazon pueden crear automáticamente un incidente utilizando planes de respuesta como plantilla. Para obtener más información sobre la creación de incidentes, consulte Crear incidentes de forma automática o manual en Incident Manager.

Los planes de respuesta lanzan planes de escalada y planes de participación relacionados para atraer a los primeros respondedores al incidente. Para obtener más información sobre la creación de planes de escalada, consulte Creación de un plan de escalada. Simultáneamente, Amazon Q Developer en las aplicaciones de chat notifica a los socorristas mediante un canal de chat que los dirige a la página de detalles del incidente. Mediante el canal de chat y los detalles del incidente, el equipo puede comunicar y clasificar un incidente. Para obtener más información sobre la configuración de canales de chat en Incident Manager, consulte Tarea 2: Crear un canal de chat en Amazon Q Developer en aplicaciones de chat.

Triaje

El triaje es cuando los primeros respondedores intentan determinar el impacto para los clientes. La vista de detalles del incidente en la consola de Incident Manager proporciona a los respondedores líneas temporales y métricas para ayudarles a evaluar el incidente. La evaluación del impacto de un incidente también sienta las bases para el tiempo de respuesta, la resolución y la comunicación del incidente. Los respondedores priorizan los incidentes utilizando clasificaciones de impacto del 1 (Crítico) al 5 (Sin impacto).

Su organización puede definir el alcance exacto de cada clasificación de impacto como prefiera. En la tabla siguiente se ofrecen ejemplos de cómo podría definirse normalmente cada nivel de impacto.

Código del impacto	Nombre del impacto	Ejemplo de alcance definido
1	`Critical`	Fallo total de una aplicación que repercute en la mayoría de los clientes.
2	`High`	Fallo total de una aplicació n que repercute en un subconjunto de clientes.
3	`Medium`	Fallo parcial de una aplicación que repercute en los clientes.
4	`Low`	Fallos intermitentes que tienen un impacto limitado en los clientes.
5	`No Impact`	Los clientes no se ven actualmente afectados, pero es necesario tomar medidas urgentes para evitar el impacto.

Investigación y mitigación

La vista de detalles del incidente proporciona a su equipo manuales de procedimientos, líneas temporales y métricas. Para obtener información sobre cómo puede trabajar con un incidente, consulte Visualización de los detalles del incidente en la consola.

Los manuales de procedimientos suelen proporcionar pasos de investigación y pueden extraer datos o intentar soluciones de uso común de forma automática. Los manuales de procedimientos también proporcionan pasos claros y repetibles que su equipo ha encontrado útiles para mitigar incidentes. La pestaña “Manual de procedimientos” se centra en el paso actual del manual de procedimientos y muestra los pasos pasados y futuros.

Incident Manager se integra con Systems Manager Automation para crear manuales de procedimientos. Utilice los manuales de procedimientos para realizar cualquiera de las siguientes acciones:

- Gestione las instancias y los recursos AWS
- Ejecutar scripts de forma automática
- Administre CloudFormation los recursos

Para obtener más información sobre los tipos de acciones admitidos, consulte Referencia de acciones de Systems Manager Automation en la Guía del usuario de AWS Systems Manager .

La pestaña Línea temporal muestra las acciones que se han realizado. La línea temporal registra cada acción con una marca de tiempo y detalles creados automáticamente. Para añadir eventos personalizados a la línea temporal, consulte la sección Plazo en la página Detalles del incidente de esta guía del usuario.

La pestaña Diagnóstico muestra métricas introducidas tanto de forma automática como manual. Esta vista proporciona información valiosa sobre las actividades de su aplicación durante un incidente.

La pestaña Participaciones le permite añadir contactos adicionales al incidente y ayuda a proporcionar los recursos para que el contacto implicado se ponga al día rápidamente una vez involucrado en el incidente. Los contactos se comprometen a través de planes de escalada o planes de participación personal definidos.

Mediante un canal de chat, puede interactuar directamente con su incidente y con otros respondedores de su equipo. Al utilizar Amazon Q Developer en las aplicaciones de chat, puede configurar los canales de chat en. Slack, Microsoft Teamsy Amazon Chime. In Slack y Microsoft Teams canales, los socorristas pueden interactuar con los incidentes directamente desde el canal de chat mediante una serie de `ssm-incidents` comandos. Para obtener más información, consulte Interacción a través del canal de chat.

Análisis post-incidente

Incident Manager proporciona un marco para reflexionar sobre un incidente, tomar las medidas necesarias para evitar que se repita en el futuro y mejorar las actividades de respuesta a incidentes en general. Las mejoras pueden incluir:

- Cambios en las aplicaciones implicadas en un incidente. Su equipo puede utilizar este tiempo para mejorar el sistema y hacerlo más tolerante a los fallos.
- Cambios en un plan de respuesta a incidentes. Tómese el tiempo necesario para incorporar las lecciones aprendidas.

- Cambios en los manuales de procedimientos. Su equipo puede profundizar en los pasos necesarios para la resolución y en los pasos que usted puede automatizar.
- Cambios en las alertas. Tras un incidente, su equipo podría haber observado puntos críticos en las métricas que puede utilizar para alertar con antelación al equipo sobre un incidente.

Incident Manager facilita estas mejoras potenciales a través de un conjunto de preguntas de análisis post-incidente y elementos de acción junto con la línea temporal del incidente. Para obtener más información sobre la mejora a través del análisis, consulte Realización de un análisis post-incidente en Incident Manager.

Administrador de incidentes de AWS Systems Manager cambio de disponibilidad

Tras considerarlo detenidamente, AWS ha tomado la decisión de dejar de aceptar nuevos clientes en AWS Systems Manager Incident Manager a partir del 7 de noviembre de 2025 y, en adelante, no añadirá nuevas funciones o capacidades a Incident Manager. AWS seguirá invirtiendo en la seguridad y la disponibilidad de Incident Manager, y los clientes actuales de Incident Manager podrán seguir utilizando el servicio con normalidad en las cuentas en las que Incident Manager ya esté activado.

Como Incident Manager ya no añadirá nuevas funciones o capacidades, es importante que comprenda sus alternativas para la gestión de incidentes. Para obtener más información sobre las alternativas, consulteGuías de migración.

Al migrar de Incident Manager a una solución alternativa, recomendamos exportar los datos del incidente para analizarlos o archivarlos con más detalle. Para obtener más información, consulte Exportación de datos de Incident Manager.

Una vez que se complete la migración, también le recomendamos que elimine los recursos restantes de Incident Manager para evitar que se sigan cobrando cargos. Para obtener más información, consulte Limpieza de los recursos del administrador de incidentes.

Para obtener asistencia adicional, puede ponerse en contacto con su administrador técnico de cuentas o crear un caso de soporte en el Centro de soporte del Consola de administración de AWS.

Guías de migración

Como ya no se Administrador de incidentes de AWS Systems Manager añadirán nuevas funciones o capacidades, es importante que comprenda sus alternativas para la gestión de incidentes. En esta sección se proporcionan guías de migración que le ayudarán a pasar de Incident Manager a soluciones alternativas.

Para gestionar los problemas operativos de su AWS infraestructura, le recomendamos que utilice AWS Systems Manager OpsCenter. Para obtener capacidades automatizadas de localización y respuesta, recomendamos las soluciones ofrecidas por nuestros socios de la red de AWS socios. AWS Los arquitectos de soluciones y los gestores técnicos de cuentas podrán guiarlo hacia la opción más adecuada en función de sus requisitos específicos.

También puede consultar las siguientes guías de migración para integrarlas con las soluciones de los socios:

- Migración a AWS Systems Manager OpsCenter
- Migración a Jira Service Management
- Migración a ServiceNow
- Migración a PagerDuty

Migración a AWS Systems Manager OpsCenter

Esta guía le ayuda a comprender las principales diferencias entre Incident Manager y OpsCenter a decidir si OpsCenter se ajusta a sus necesidades operativas, y le proporciona formas de migrar OpsCenter desde AWS Systems Manager Incident Manager.

AWS Systems Manager OpsCenter, una capacidad de AWS Systems Manager, proporciona una ubicación central donde los ingenieros de operaciones y los profesionales de TI pueden ver, investigar y resolver las tareas operativas (OpsItems) relacionadas con los AWS recursos. OpsCenter está diseñado para reducir el tiempo medio de resolución (MTTR) de los problemas que afectan AWS a los recursos. OpsCenter agrega y estandariza OpsItems todos los servicios y, al mismo tiempo, proporciona datos de investigación contextual sobre cada uno de los recursos relacionados OpsItem y relacionados OpsItems. OpsCenter se integra con Systems Manager Automation, lo que le permite utilizar los manuales de automatización para investigar y resolver problemas. Puede ver los informes resumidos generados automáticamente OpsItems por estado y fuente. También puede utilizar la función multicuenta para gestionar OpsCenter de forma centralizada todas las cuentas. OpsItems

> **Note**
>
> Hay cargos asociados con el OpsCenter uso. Consulte la página de AWS Systems Manager precios para obtener más información.

Similar a Incident Manager, OpsCenter tiene integraciones con Amazon CloudWatch y Amazon EventBridge. Esto significa que puede configurar estos servicios para que creen automáticamente una entrada OpsCenter cuando una CloudWatch alarma entre OpsItem en `ALARM` estado o cuando EventBridge procese un evento desde cualquiera Servicio de AWS que publique eventos. La configuración de CloudWatch alarmas y EventBridge eventos para que se creen automáticamente

OpsItems le permite diagnosticar y solucionar problemas rápidamente con AWS los recursos de una única consola.

Comprender las diferencias

AWS Systems Manager Incident Manager ofrece funciones de respuesta a incidentes que incluyen planes de respuesta automatizados, participación y escalamiento del personal de respuesta, gestión de la rotación de guardia, automatización de manuales, integración de operaciones de chat (Slack, Microsoft Teams, Amazon Chime) y análisis posterior al incidente. Estas funciones ayudan a las organizaciones a coordinar y resolver los incidentes críticos y urgentes que afectan a las aplicaciones alojadas. AWS

Por el contrario, AWS Systems Manager OpsCenter se centra en gestionar los elementos de trabajo operativos (OpsItems) para cuestiones day-to-day operativas como las alertas de seguridad, la degradación del rendimiento, los fallos de recursos, las notificaciones de estado y los cambios de estado. OpsCenter se integra con AWS los recursos de Amazon CloudWatch y Amazon EventBridge, lo que permite OpsItem la creación y la corrección automatizadas mediante manuales de automatización de Systems Manager. OpsCenter permite la administración de varias cuentas OpsItems dentro de una región, lo que permite a los equipos de operaciones ver, investigar y resolver los problemas en varias cuentas. AWS Sin embargo, OpsCenter no incluye las funciones de radiobúsqueda o rotación de llamadas.

Las principales diferencias entre estos dos AWS servicios radican en su enfoque y alcance. Incident Manager está diseñado para responder a incidentes críticos y urgentes, mientras que OpsCenter está orientado a la gestión de tareas operativas y elementos de trabajo más amplios.

En la siguiente tabla se comparan las capacidades clave de Incident Manager y OpsCenter. Utilice esta comparación para decidir si OpsCenter se ajusta a sus necesidades operativas.

Característica/capacidad	Administrador de incidentes de AWS Systems Manager	AWS Systems Manager OpsCenter
Propósito principal	Coordinación y respuesta ante incidentes críticos y urgentes	Day-to-day gestión operativa de los elementos de trabajo
Casos de uso	Incidentes que afectan a las aplicaciones; brechas de seguridad; interrupciones del	Alertas de seguridad; degradación del rendimiento; fallos de recursos; notificac

Característica/capacidad	Administrador de incidentes de AWS Systems Manager	AWS Systems Manager OpsCenter
	servicio; fallas críticas del sistema	iones de salud; cambios de estado
Paginación automatizada	Sí, paginación integrada y participación del personal de respuesta	No: requiere la integraci ón de terceros (PagerDuty, ServiceNow, Jira)
Gestión de la rotación de guardia	Sí, horarios y rotación nativos de guardia	No: no se admite
Políticas de escalamiento	Sí, cadenas de escalamiento automatizadas	No: se requiere un escalamie nto manual
Integración de Chat-Ops	Sí: Slack, Microsoft Teams, Amazon Chime	Limitado: se requiere una integración manual
Runbook Automation	Sí, ejecución automatizada mediante planes de respuesta	Sí: ejecución manual de los manuales de automatización de Systems Manager
Administración entre cuentas	Sí, intercambio de incidentes entre cuentas	Sí, OpsItem administración de varias cuentas dentro de una región

Opciones de migración

Si ya tiene CloudWatch alarmas y EventBridge reglas integradas en Incident Manager, tendrá que actualizarlas para poder integrarlas. OpsCenter Puede migrar mediante uno de los siguientes enfoques:

Migración automatizada mediante manuales

Utilice los manuales de automatización de Systems Manager para migrar automáticamente sus CloudWatch alarmas y EventBridge reglas de Incident Manager a OpsCenter. Este enfoque incluye copias de seguridad, flujos de trabajo de aprobación configurables y registros detallados. Puede optar por solicitar la aprobación manual antes de la migración u omitir el paso de

aprobación para las migraciones automatizadas a gran escala. Para obtener step-by-step instrucciones, consultethe section called “Uso de manuales de migración para OpsCenter”.

Integración manual

Configure manualmente CloudWatch las alarmas y EventBridge las reglas con las que desee integrarlas OpsCenter. Para obtener instrucciones, consulte Configuración de CloudWatch alarmas para crear OpsItems y Configuración EventBridge para crear OpsItems en la Guía del usuario de Systems Manager.

Recursos relacionados

- AWS Systems Manager OpsCenter Guía del usuario
- the section called “Exportación de datos de Incident Manager”
- the section called “Limpieza de los recursos del administrador de incidentes”

Uso de manuales de migración para OpsCenter

En esta guía se proporcionan step-by-step instrucciones para migrar las CloudWatch alarmas y las EventBridge reglas de Amazon de AWS Systems Manager Incident Manager a AWS Systems Manager OpsCenter utilizar guías de migración automatizadas.

Para obtener una descripción general de OpsCenter las capacidades y comprender las diferencias entre Incident Manager y OpsCenter, consulte. the section called “Migración a AWS Systems Manager OpsCenter”

Información general sobre la migración

El proceso de migración utiliza los manuales de automatización de Systems Manager para integrar sus CloudWatch alarmas y EventBridge reglas existentes. OpsCenter El proceso consta de los pasos siguientes:

- Implemente la infraestructura: implemente la CloudFormation pila para crear los recursos necesarios para los manuales de migración.
- Migre las CloudWatch alarmas y EventBridge las reglas: ejecute los manuales de automatización a los que desee migrar sus recursos. OpsCenter
- Limpie los recursos: si lo desea, elimine el conjunto de replicación y otros recursos de Incident Manager.

> **Note**
>
> Los manuales admiten la migración de un solo par de cuenta-región. Si tiene recursos en varias cuentas o regiones, debe ejecutar la migración por separado para cada combinación de cuentas y regiones.

Paso 1: Implemente la plantilla CloudFormation

Implemente la CloudFormation plantilla para crear el rol de IAM, el bucket de Amazon S3 y el tema de Amazon SNS requeridos en los manuales de migración.

Permisos de IAM necesarios

Para implementar esta CloudFormation plantilla, necesita permisos de IAM para las operaciones de CloudFormation pila (`cloudformation:CreateStack`,`cloudformation:DescribeStacks`), la administración de roles de IAM (`iam:CreateRole`,,`iam:PassRole`) `iam:PutRolePolicyiam:AttachRolePolicy`, la creación y configuración de buckets de Amazon S3 (`s3:CreateBucket`,`s3:PutBucket*`) y las operaciones temáticas de Amazon SNS `sns:CreateTopic` (`sns:Subscribe`,,). `sns:SetTopicAttributes`

Para obtener información completa sobre los CloudFormation permisos, consulte la referencia sobre CloudFormation los permisos en la Guía del CloudFormation usuario.

Para implementar la CloudFormation plantilla mediante la consola

1. Descargue y extraiga el archivo AWS- IncidentManager - MigrationResources .zip que contiene la `AWS-IncidentManager-MigrationResources.yaml` plantilla.
2. Abra la CloudFormation consola en https://console.aws.amazon.com/cloudformation.
3. Seleccione Crear pila.
4. En la sección Specify template (Especificar plantilla) seleccione Upload a template file (Cargar un archivo de plantilla).
5. Elija Elegir archivo y, a continuación, seleccione el `AWS-IncidentManager-MigrationResources.yaml` archivo.
6. Elija Siguiente.
7. En la página Especificar los detalles de la pila, introduzca lo siguiente:
   - Nombre de pila: introduzca un nombre (por ejemplo,`im-migration-infrastructure`)

- ApprovalEmail- Introduzca la dirección de correo electrónico para recibir las notificaciones de aprobación (solo se utiliza cuando el parámetro RequireManualApproval runbook está establecido en true).
- IsPrimaryMigrationRegion- Elige `true` si esta es la primera región de tu cuenta en la que vas a implementar la pila; de lo contrario, elige `false`

8. Elija Siguiente.
9. En la página Configurar opciones de pila, elija Siguiente.
10. En la página de revisión, desplázate hacia abajo y selecciona Reconozco que CloudFormation podría crear recursos de IAM con nombres personalizados.
11. Seleccione Enviar.

CloudFormation muestra el `CREATE_IN_PROGRESS` estado. El estado cambia a `CREATE_COMPLETE` cuando la pila está lista.

> **Note**
>
> Si tiene CloudWatch alarmas o EventBridge reglas en varias regiones, implemente esta CloudFormation pila en cada región en la que desee realizar la migración.
> Para despliegues con varias cuentas en AWS Organizations, usa dos: CloudFormation StackSets
>
> - Principal StackSet: se establece en True IsPrimaryMigrationRegion para una región por cuenta
> - Secundario StackSet: se establece en falso IsPrimaryMigrationRegion para todas las demás regiones
>
> Para obtener instrucciones, consulte Utilización CloudFormation StackSets en la Guía CloudFormation del usuario.

Para implementar la CloudFormation plantilla mediante el AWS CLI

Para la primera región de tu cuenta, usa el siguiente comando:

```
aws cloudformation create-stack \
    --stack-name im-migration-infrastructure \
    --template-body file://AWS-IncidentManager-MigrationResources.yaml \
    --parameters ParameterKey=ApprovalEmail,ParameterValue=your-email@example.com \
    ParameterKey=IsPrimaryMigrationRegion,ParameterValue=true \
    --capabilities CAPABILITY_NAMED_IAM \
    --region us-east-1
```

Para regiones adicionales de la misma cuenta, establézcalo `IsPrimaryMigrationRegion` en`false`:

```
aws cloudformation create-stack \
    --stack-name im-migration-infrastructure \
    --template-body file://AWS-IncidentManager-MigrationResources.yaml \
    --parameters ParameterKey=ApprovalEmail,ParameterValue=your-email@example.com \
    ParameterKey=IsPrimaryMigrationRegion,ParameterValue=false \
    --capabilities CAPABILITY_NAMED_IAM \
    --region us-west-2
```

Para verificar el estado de la pila:

```
aws cloudformation describe-stacks \
    --stack-name im-migration-infrastructure \
    --query 'Stacks[0].StackStatus' \
    --output text
```

Espere a que vuelva el comando `CREATE_COMPLETE` antes de continuar con el siguiente paso.

Paso 2: migrar CloudWatch las alarmas y EventBridge las reglas

Utilice los manuales de automatización de Systems Manager para migrar sus CloudWatch alarmas y EventBridge reglas de Incident Manager a OpsCenter.

Cuadernos de migración

- AWS- MigrateIncidentManagerCloudWatchAlarms

- AWS- MigrateIncidentManagerEventBridgeRules

Para obtener más información sobre lo que hacen estos manuales de ejecución, incluidas las descripciones detalladas de los pasos, los parámetros de entrada y los resultados, consulte la documentación del manual de ejecución.

Cómo funcionan los manuales de ejecución

Ambos manuales de migración siguen el mismo flujo de trabajo:

- Detección y procesamiento por lotes: descubre todas las CloudWatch alarmas o EventBridge reglas configuradas con las acciones del plan de respuesta de Incident Manager y las organiza en lotes configurables.
- Aprobación manual (opcional): de forma predeterminada, se requiere una aprobación explícita antes de continuar con la migración, con un tiempo de espera de 24 horas. Se envía una notificación de Amazon SNS a la dirección de correo electrónico especificada durante CloudFormation la implementación. Se hace una copia de seguridad de todas las configuraciones en Amazon S3 y se guarda la lista completa de los recursos que se van a migrar para su revisión manual. Este paso se puede omitir si se establece en RequireManualApproval false.
- Backup y migración: si la aprobación manual se establece en True, espera la aprobación y, a continuación, realiza una copia de seguridad de cada configuración en Amazon S3 y realiza la migración. Si se establece en false, pasa directamente a la copia de seguridad y la migración.

Parámetros de entrada

Ambos manuales de ejecución requieren los siguientes parámetros:

AutomationAssumeRole (Obligatorio)

El ARN del `IM-Migration-Automation-Role` creado por la CloudFormation pila.

ApproverArn (Obligatorio)

El ARN del rol o usuario de IAM que puede revisar y aprobar la migración.

S3 BucketName (obligatorio)

El nombre del bucket de Amazon S3 creado por la CloudFormation pila.

SNSTopicArn (obligatorio)

El ARN del tema de Amazon SNS creado por la pila. CloudFormation

MaxNumberOfAlarmsToMigrate o MaxNumberOfRulesToMigrate (opcional)

El número máximo de recursos que se van a migrar en una sola ejecución. Valores válidos: 1, 5, 10, 50, 100, 500, 5000, 10000, 25000, 50000. Predeterminado: 10000.

BatchSize (Opcional)

La cantidad de recursos que se van a procesar en cada lote. Valores válidos: 25, 50, 100, 200, 250, 300, 350, 400, 450, 500. Valor predeterminado: 100. El manual de ejecución admite un máximo de 100 × BatchSize recursos por ejecución.

RequireManualApproval (Opcional)

Valor booleano para controlar si se requiere la aprobación manual antes de la migración. Si se establece en true (predeterminado), recibirá un correo electrónico de notificación de Amazon SNS con la ubicación de Amazon S3 de la lista de recursos y un enlace a la consola de ejecución de la automatización para aprobarla, denegarla o cancelarla. Si se establece en false, el runbook continúa automáticamente después de detectarlo y hacer una copia de seguridad. Valores válidos: verdadero, falso. Valor predeterminado: verdadero.

Para migrar mediante la consola

1. Abra la consola de Systems Manager en https://console.aws.amazon.com/systems-manager.
2. En el panel de navegación, elija automatización.
3. Busque el nombre (o) del runbook. `AWS-MigrateIncidentManagerCloudWatchAlarms` `AWS-MigrateIncidentManagerEventBridgeRules`
4. Elija Ejecutar automatización.
5. Introduzca los valores de los parámetros de las salidas de la CloudFormation pila.
6. (Opcional) RequireManualApproval`false`Configúrelo si desea omitir el paso de aprobación manual.
7. Elija Ejecutar.
8. Si `RequireManualApproval` se establece en true (predeterminado), recibirá una notificación por correo electrónico cuando la ejecución esté pendiente de revisión manual. El correo electrónico contiene un enlace de aprobación a la página de la consola de ejecución de la automatización. Revise la lista de recursos del bucket de Amazon S3 y, a continuación, apruebe, deniegue o cancele en un plazo de 24 horas desde el enlace del correo electrónico o desde la página de la consola. La migración solo se lleva a cabo después de la aprobación. Si se establece en falso, la migración se realiza automáticamente después de la copia de seguridad.

9. Espere a que el estado de ejecución cambie a Éxito.

Para migrar mediante el AWS CLI

Para CloudWatch las alarmas:

```
aws ssm start-automation-execution \
    --document-name "AWS-MigrateIncidentManagerCloudWatchAlarms" \
    --parameters '{
        "AutomationAssumeRole": ["arn:aws:iam::123456789012:role/IM-Migration-
Automation-Role"],
        "ApproverArn": ["arn:aws:iam::123456789012:role/Admin"],
        "S3BucketName": ["im-migration-logs-123456789012-us-east-1"],
        "SNSTopicArn": ["arn:aws:sns:us-east-1:123456789012:Automation-IM-Migration-
Approvals"],
        "RequireManualApproval": ["false"]
    }' \
    --region us-east-1
```

Para EventBridge las reglas:

```
aws ssm start-automation-execution \
    --document-name "AWS-MigrateIncidentManagerEventBridgeRules" \
    --parameters '{
        "AutomationAssumeRole": ["arn:aws:iam::123456789012:role/IM-Migration-
Automation-Role"],
        "ApproverArn": ["arn:aws:iam::123456789012:role/Admin"],
        "S3BucketName": ["im-migration-logs-123456789012-us-east-1"],
        "SNSTopicArn": ["arn:aws:sns:us-east-1:123456789012:Automation-IM-Migration-
Approvals"],
        "RequireManualApproval": ["false"]
    }' \
    --region us-east-1
```

Para revisar la lista de recursos en Amazon S3:

```
# For CloudWatch alarms
aws s3 cp s3://im-migration-logs-123456789012-us-east-1/review/CloudWatch/
review_CW_alarms_to_migrate_123456789012_us-east-1.json ./

# For EventBridge rules
aws s3 cp s3://im-migration-logs-123456789012-us-east-1/review/EventBridge/
review_EB_rules_to_migrate_123456789012_us-east-1.json ./
```

Si RequireManualApproval se establece en true, revise la lista de recursos y apruebe la migración haciendo clic en el enlace de aprobación que aparece en la notificación por correo electrónico o en la página de la consola de ejecución de la automatización. Si se establece en falso, la migración se realiza automáticamente tras la copia de seguridad.

Paso 3: Verifica la migración

Tras completar la migración, compruebe que los recursos funcionan correctamente:

- Active una alarma o un evento de prueba: active una de las CloudWatch alarmas o EventBridge reglas migradas para generar una notificación de prueba.
- Confirme OpsItem la creación: compruebe que OpsItem se crea automáticamente una OpsCenter cuando se activa la alarma o el evento.
- Valide el mapa de gravedad: compruebe que el nivel de gravedad de la configuración original de Incident Manager se conserva correctamente en el OpsItem. (Aplicable solo a CloudWatch las alarmas).

Paso 4: Limpiar los recursos de Incident Manager

Tras migrar correctamente las CloudWatch alarmas y EventBridge las reglas, si lo desea, puede limpiar los recursos de Incident Manager para desconectarlos por completo del servicio.

Para obtener instrucciones detalladas sobre cómo eliminar el conjunto de réplicas, los planes de respuesta, los contactos, los manuales de instrucciones y otros recursos de Incident Manager, consulte. the section called “Limpieza de los recursos del administrador de incidentes”

Eliminar CloudFormation pilas (opcional)

Puede eliminar las CloudFormation pilas para eliminar la función de IAM, el tema de Amazon SNS y el bucket de Amazon S3 creados para la migración.

> **Important**
>
> El depósito de Amazon S3 que contiene las copias de seguridad de todos los recursos migrados debe vaciarse antes de eliminar la pila. CloudFormation no puede eliminar los buckets de Amazon S3 que contienen objetos.

Para eliminar la pila CloudFormation

```
aws cloudformation delete-stack --stack-name <your-stack-name>
```

Supervisión y solución de problemas

CloudWatch Registros: las actividades de migración se registran en los CloudWatch registros:

- CloudWatch alarmas: `/aws/ssm/incidentmanager/cwmigration`
- EventBridge reglas: `/aws/ssm/incidentmanager/ebmigration`

Estructura de backup de Amazon S3: se hace una copia de seguridad de todas las configuraciones en Amazon S3 antes de la migración:

```
migration-logs-{AccountId}-{Region}/
### backups/
#   ### CloudWatch/
#   #   ### {AccountId}/
#   #       ### {Region}/
#   #           ### {AlarmName}_backup.json
#   ### EventBridge/
#       ### {AccountId}/
#           ### {Region}/
#               ### {RuleName}_backup.json
### review/
    ### CloudWatch/
    #   ### review_CW_alarms_to_migrate_{AccountId}_{Region}.json
    ### EventBridge/
        ### review_EB_rules_to_migrate_{AccountId}_{Region}.json
```

Problemas comunes:

- No se ha recibido la notificación de Amazon SNS (cuando RequireManualApproval es cierto): compruebe la suscripción al tema de Amazon SNS:

```
aws sns list-subscriptions-by-topic --topic-arn <sns-topic-arn>
```

- Fallos de migración parciales: consulte CloudWatch los registros para ver los mensajes de error detallados y vuelva a intentar la automatización con un tamaño de lote reducido.

Procedimiento de reversión:

Si necesita revertir la migración:

- Recupere copias de seguridad de Amazon S3:

```
aws s3 sync s3://im-migration-logs-123456789012-us-east-1/backups/ ./backups/
```

- Restaure los recursos:

```
# For CloudWatch alarms
aws cloudwatch put-metric-alarm --cli-input-json file://backups/
CloudWatch/123456789012/us-east-1/MyAlarm_backup.json

# For EventBridge rules
aws events put-targets --rule MyRule --targets file://backups/
EventBridge/123456789012/us-east-1/MyRule_backup.json
```

Preguntas frecuentes

P: ¿Qué ocurre si se agota el tiempo de espera de la automatización durante la aprobación?

R: La automatización caduca después de 24 horas si no se recibe la aprobación. Puede reiniciar la automatización con los mismos parámetros.

P: ¿Puedo migrar los recursos de una región a otra?

R: No. Cada región debe migrarse por separado mediante ejecuciones de automatización específicas de la región.

P: ¿Cuánto tarda la migración?

R: El tiempo de migración depende de la cantidad de recursos:

- Aproximadamente 100 alarmas/reglas: de 5 a 10 minutos
- ~1000 alarmas/reglas: 30-60 minutos
- ~10000 alarmas/reglas: de 2 a 4 horas

P: ¿Se conserva la gravedad tras la migración a? OpsCenter

R: Sí. La gravedad configurada en los niveles de impacto del plan de respuesta de Incident Manager se conserva y se asigna automáticamente a los niveles de OpsCenter gravedad adecuados durante la migración de las CloudWatch alarmas. Esto no se aplica a EventBridge las reglas.

P: ¿Se me cobrará por ejecutar los manuales de automatización?

R: No. Los manuales de automatización de la migración no incurren en cargos de ejecución. Sin embargo, el OpsCenter uso después de la migración generará cargos. Para obtener más información, consulte la documentación de precios de Systems Manager.

Recursos relacionados

- the section called “Migración a AWS Systems Manager OpsCenter”
- AWS Systems Manager OpsCenter Guía del usuario
- Automatización de Systems Manager
- the section called “Exportación de datos de Incident Manager”
- the section called “Limpieza de los recursos del administrador de incidentes”

Migración a Jira Service Management

Jira Service Management (JSM) es una solución de administración de servicios de TI (ITSM) que ayuda a los equipos a recibir, rastrear, gestionar y resolver las solicitudes de los empleados y los clientes a través de varios canales, como el correo electrónico, el chat, los centros de ayuda y los

widgets. Basado en la plataforma Jira, Jira Service Management permite a los equipos de toda la organización, desde el área de desarrollo hasta la de TI y RRHH, recibir solicitudes, responder a alertas e incidentes, implementar cambios, realizar un seguimiento de los activos, dar a conocer el conocimiento y automatizar los flujos de trabajo. Jira Service Management incluye funciones de gestión de incidentes, como la programación de llamadas, las alertas, la gestión de incidentes graves, la gestión de cambios y funciones post mortem (PIR) impecables diseñadas para los DevOps flujos de trabajo, que aprovechan los CI/CD procesos existentes y la automatización para reducir el esfuerzo manual.

Jira Service Management se integra con Amazon CloudWatch y Amazon EventBridge, lo que te permite crear automáticamente alertas de Jira Service Management cuando CloudWatch las alarmas entran en `ALARM` estado o cuando EventBridge procesa eventos de cualquiera Servicio de AWS que publique eventos. La configuración de CloudWatch las alarmas y EventBridge los eventos para crear automáticamente alertas de Jira Service Management te permite diagnosticar y solucionar los problemas rápidamente con AWS los recursos de una única plataforma. Jira Service Management actúa como despachador y notifica a las personas adecuadas a través de varios canales (correo electrónico, SMS, llamadas telefónicas, notificaciones push a dispositivos móviles) en función de los horarios de llamadas y las políticas de escalamiento.

Si ya tienes integradas CloudWatch Alarms and EventBridge Rules Administrador de incidentes de AWS Systems Manager, te recomendamos que actualices esas integraciones y utilices Jira Service Management en su lugar. La documentación oficial de Atlassian proporciona instrucciones detalladas para integrar Jira Service Management e integrarlo con CloudWatch Jira Service Management. EventBridge

Además de la creación automática de alertas, Jira Service Management ofrece una serie de funciones para agilizar la gestión de incidentes, como la programación de llamadas, las políticas de escalamiento y las reglas de automatización. Los clientes pueden consultar la siguiente documentación de Atlassian para obtener más información sobre la configuración de estas capacidades:

- Descubra las alertas y la función de guardia
- Cree horarios de guardia
- Cree políticas de escalamiento
- Configure equipos y personas
- Configure los métodos de contacto
- Configure las reglas de notificación

- Configura las notificaciones por SMS y voz
- Configure las reglas de automatización
- Configure y gestione a las partes interesadas en los incidentes

Si necesitas asistencia adicional, puedes ponerte en contacto con tu director técnico de cuentas o con un representante de ventas de Atlassian para obtener más información.

Migración a ServiceNow

ServiceNow La gestión de incidentes es un módulo central de ITSM diseñado para restablecer las operaciones normales del servicio tras interrupciones no planificadas y, al mismo tiempo, minimizar el impacto empresarial. Al igual que ServiceNow Incident Manager, Incident Management proporciona un sistema estructurado y automatizado para ver, investigar y resolver los incidentes de TI, con funciones como la priorización automatizada y los procesos de escalamiento integrados.

El módulo ServiceNow Service Operations con gestión de incidentes y gestión de eventos se integra con Amazon CloudWatch, lo que le permite crear automáticamente ServiceNow eventos/alertas e incidentes cuando CloudWatch las alarmas entran en estado. `ALARM` La configuración de CloudWatch alarmas para crear ServiceNow incidentes automáticamente con WebHook to AIOps Event Management te permite diagnosticar y solucionar los problemas rápidamente con AWS los recursos de una única plataforma.

Si ya tiene CloudWatch alarmas integradas Administrador de incidentes de AWS Systems Manager, le recomendamos que actualice esas integraciones para utilizar en su lugar la plataforma de gestión de ServiceNow incidentes e inteligencia de AIOps eventos. La ServiceNow documentación oficial proporciona instrucciones detalladas para la integración ServiceNow con Amazon CloudWatch.

Además de la creación automática de incidentes, la gestión de ServiceNow incidentes ofrece una gama de funciones para mejorar la gestión de incidentes, como la gestión de la comunicación de incidentes, la programación de llamadas, las políticas de escalamiento y más. Los clientes pueden consultar la siguiente ServiceNow documentación para obtener detalles sobre la configuración de estas capacidades:

- Documentación de gestión de incidentes
- Gestión de la fiabilidad del servicio
- Gestión de comunicaciones y contactos en caso de incidentes
- Horarios de guardia

- Proceso de escalamiento

Para obtener asistencia adicional, puede ponerse en contacto con su director técnico de cuentas o con un representante de ServiceNow ventas para obtener más información.

Migración a PagerDuty

PagerDutyes una plataforma de gestión de incidentes que ayuda a las organizaciones a detectar, responder e incluso prevenir incidentes. Al igual que Incident Manager, PagerDuty proporciona una ubicación central donde los equipos de operaciones abordan tareas críticas relacionadas con AWS los recursos, lo que reduce el impacto en los clientes.

PagerDuty se integra con Amazon CloudWatch y Amazon EventBridge, lo que le permite crear PagerDuty incidentes automáticamente cuando CloudWatch las alarmas entran en `ALARM` estado o cuando EventBridge procesa eventos desde cualquiera Servicio de AWS que publique eventos. Al configurar CloudWatch las alarmas y EventBridge los eventos para crear PagerDuty incidentes automáticamente, puede diagnosticar y solucionar rápidamente los problemas de AWS recursos desde una única plataforma.

Si ya tiene CloudWatch alarmas y EventBridge reglas integradas Administrador de incidentes de AWS Systems Manager, le recomendamos que actualice esas integraciones para PagerDuty utilizarlas en su lugar. La PagerDuty documentación oficial proporciona instrucciones detalladas para la integración PagerDuty CloudWatch y la integración PagerDuty con EventBridge.

Además de la creación automática de incidentes, PagerDuty ofrece una gama de funciones para mejorar la gestión de incidentes, como la programación de llamadas, las políticas de escalamiento y más de 700 integraciones de out-of-box plataformas. También puede personalizar las reglas de notificación, configurar las superficies de chat y aprovechar la IA y la automatización de la PagerDuty plataforma para acelerar la resolución de incidentes.

- Gestione los usuarios
- Crea equipos
- Configure los métodos de contacto
- Configure las reglas de notificación
- Configure una rotación de guardia
- Cree políticas de escalamiento

- Configura la integración de Slack
- Configura las acciones de automatización

Para obtener asistencia adicional, puede ponerse en contacto con su administrador técnico de cuentas o enviar un correo electrónico a AWS-IM-help@pagerduty.com para obtener más información.

Exportación de datos de Incident Manager

En este tema se describe cómo utilizar una secuencia de comandos de Python para exportar registros de incidentes y análisis posteriores a los incidentes desde Administrador de incidentes de AWS Systems Manager. El script exporta los datos a archivos JSON estructurados para su posterior análisis o archivado.

¿Qué puede exportar

El script exporta los siguientes datos:

- Registros completos de incidentes, que incluyen:
  - Cronología de los eventos
  - Elementos relacionados
  - Participaciones
  - Ejecuciones de automatización
  - Hallazgos de seguridad
  - Tags
- Documentos de análisis posteriores al incidente de Systems Manager

Requisitos previos

Antes de empezar, asegúrese de que tiene lo siguiente:

- Python 3.7 o posterior instalado
- AWS CLI configurado con las credenciales adecuadas
- Se instalaron los siguientes paquetes de Python:

```
pip install boto3 python-dateutil
```

Permisos de IAM necesarios

Para usar este script, asegúrese de tener los siguientes permisos:

Permisos de incidentes de Systems Manager

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ssm-incidents:ListIncidentRecords",
                "ssm-incidents:GetIncidentRecord",
                "ssm-incidents:ListTimelineEvents",
                "ssm-incidents:GetTimelineEvent",
                "ssm-incidents:ListRelatedItems",
                "ssm-incidents:ListEngagements",
                "ssm-incidents:GetEngagement",
                "ssm-incidents:BatchGetIncidentFindings",
                "ssm-incidents:ListTagsForResource"
            ],
            "Resource": "*"
        }
    ]
}
```

Permisos de Systems Manager

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ssm:ListDocuments",
                "ssm:GetDocument",
                "ssm:GetAutomationExecution"
```

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

Estructura de exportación

El script crea la siguiente estructura de directorios para los datos exportados:

```
incident_manager_export_YYYYMMDD_HHMMSS/
### incident_records/
#   ### 20250309_102129_IAD_Service_A_Lambda_High_Latency.json
#   ### 20250314_114820_SecurityFinding_SecurityHubFindings.json
#   ### ...
### post_incident_analyses/
    ### 20250310_143022_Root_Cause_Analysis_Service_A.json
    ### 20250315_091545_Security_Incident_Review.json
    ### ...
```

Ejecutar el script de exportación

Uso básico

Se proporciona el script de exportación de datos de Incident Manager`here`. Descargue el script y siga las instrucciones siguientes para ejecutarlo.

Para ejecutar el script con la configuración predeterminada:

```
python3 export-incident-manager-data.py
```

Opciones disponibles

Puede personalizar la exportación mediante estas opciones de línea de comandos:

Opción	Description (Descripción)	Predeterminado
`--region`	AWS Región	`us-east-1`
`--profile`	AWS nombre de perfil	Perfil predeterminado

Opción	Description (Descripción)	Predeterminado
`--verbose , -v`	Habilite el registro detallado	FALSO
`--limit`	Número máximo de incidentes para exportar	Sin límite
`--timeline-events-limit`	Cronología máxima de eventos por incidente	100
`--timeline-details-limit`	Cronología máxima de los detalles de los eventos por incidente	100
`--related-items-limit`	Número máximo de artículos relacionados por incidente	50
`--engagements-limit`	Número máximo de interacciones por incidente	20
`--analysis-docs-limit`	Número máximo de documentos de análisis que se pueden exportar	50

Ejemplos

Exporte desde una región específica mediante un perfil personalizado:

```
python3 export-incident-manager-data.py --region us-east-1 --profile my-aws-profile
```

Exporte con un registro detallado y límites de prueba:

```
python3 export-incident-manager-data.py --verbose --limit 5 --timeline-events-limit 10
```

Exportación con límites conservadores para conjuntos de datos grandes:

```
python3 export-incident-manager-data.py --timeline-events-limit 50 --timeline-details-limit 25
```

Estructura del archivo de salida

Estructura JSON del registro de incidentes

Cada archivo de registro de incidentes contiene la siguiente estructura:

```
{
    "incident_record": {
        // Complete incident record from get-incident-record
    },
    "incident_summary": {
        // Incident summary from list-incident-records
    },
    "incident_source_details": {
        "from_incident_record": {},
        "from_incident_summary": {},
        "enhanced_details": {
            "created_by": "arn:aws:sts::...",
            "source": "aws.ssm-incidents.custom",
            "source_analysis": {
                "source_type": "manual",
                "creation_method": "human_via_console",
                "automation_involved": false,
                "human_created": true
            }
        }
    },
    "timeline_events": {
        "detailed_events": [
            {
                "summary": {}, // From list-timeline-events
                "details": {}  // From get-timeline-event
            }
        ],
        "summary_only_events": [],
        "metadata": {
            "total_events_found": 45,
            "events_with_details": 25,
            "limits_applied": {}
        }
    },
    "related_items": {
        "items": [],
```

```
        "metadata": {}
    },
    "engagements": {
        "engagements": [],
        "metadata": {}
    },
    "automation_executions": [],
    "findings": [],
    "tags": [],
    "post_incident_analysis": {
        "analysis_reference": {},
        "metadata": {}
    },
    "export_metadata": {
        "exported_at": "2025-09-18T...",
        "region": "us-east-*",
        "incident_arn": "arn:aws:ssm-incidents::..."
    }
}
```

Análisis posterior al incidente (estructura JSON)

Cada archivo de documento de análisis contiene:

```
{
    "document_metadata": {
        // Document metadata from list-documents
    },
    "document_details": {
        "Name": "037fc5dd-cd86-49bb-9c3d-15720e78798e",
        "Content": "...", // Full JSON content
        "DocumentType": "ProblemAnalysis",
        "CreatedDate": 1234567890,
        "ReviewStatus": "APPROVED",
        "AttachmentsContent": [],
        // ... other fields from get-document
    },
    "export_metadata": {
        "exported_at": "2025-09-18T...",
        "region": "us-east-*",
        "document_name": "..."
    }
}
```

Limpieza de los recursos del administrador de incidentes

Si ya no los utiliza Administrador de incidentes de AWS Systems Manager, le recomendamos que limpie los recursos restantes de Incident Manager. Esto lo excluirá por completo del servicio y evitará que se le siga cobrando. Consulta la página de AWS Systems Manager precios para obtener más información.

Eliminar el conjunto de replicación

El conjunto de replicación es un componente clave de Incident Manager que facilita la replicación de los datos de los incidentes en varias AWS regiones. Si ya no necesita Incident Manager, debe eliminar el conjunto de replicación.

Para eliminar el conjunto de replicación:

1. Abra la AWS Systems Manager consola
2. En el panel de navegación, elija Incident Manager
3. En «Conjuntos de replicación», localice el conjunto de replicación que desee eliminar
4. Haga clic en el nombre del conjunto de replicación para abrir la página de detalles
5. En la página de detalles del conjunto de réplicas, haga clic en el botón «Eliminar»
6. En el cuadro de diálogo de confirmación, revise la información y haga clic en «Eliminar conjunto de replicación» para continuar con la eliminación

> **Note**
>
> Al eliminar el conjunto de réplicas, se eliminarán permanentemente todos los datos de incidentes almacenados en Incident Manager. Asegúrese de que ya no necesita acceder a la información histórica de ningún incidente antes de proceder a la eliminación.

Eliminar los recursos relacionados con Incident Manager

Además del conjunto de réplicas, es posible que disponga de otros recursos relacionados con Incident Manager, como planes de respuesta, contactos y manuales. Si ya no necesita estos recursos, puede considerar eliminarlos para desconectarlos por completo de Incident Manager.

Para eliminar los recursos relacionados con Incident Manager:

1. Abra la consola AWS Systems Manager
2. En el panel de navegación, elija Incident Manager
3. Navegue hasta la sección correspondiente (p. ej., «Planes de respuesta», «Contactos», «Guías») y localice los recursos que desee eliminar
4. Seleccione los recursos y haga clic en el botón «Eliminar» para eliminarlos

Configuración AWS Gestor de Sistemas Gestor de Incidentes

Recomendamos configurar AWS Systems Manager Incident Manager en la cuenta que utilice para gestionar sus operaciones. Antes de utilizar Incident Manager por primera vez, complete las siguientes tareas:

Temas

Inscríbase en una Cuenta de AWS

Para empezar AWS, necesitas un Cuenta de AWS. Para obtener información sobre cómo crear un Cuenta de AWS, consulte Cómo empezar con un Cuenta de AWS en la Guía de AWS Account Management referencia.

Rol requerido para la configuración de Incident Manager

Antes de empezar, su cuenta debe tener el permiso IAM `iam:CreateServiceLinkedRole`. Incident Manager utiliza este permiso para crear el `AWSServiceRoleforIncidentManager` en su cuenta. Para obtener más información, consulte Uso de roles vinculados a servicios para Incident Manager.

Introducción a Incident Manager

En esta sección se explica el asistente Preparación en la consola de Incident Manager. Deberá completar Preparación en la consola antes de poder utilizarla para la administración de incidentes. El asistente le guiará a través de la configuración del conjunto de réplica, al menos un contacto y un plan de escalada, y su plan de primera respuesta. Las siguientes guías le ayudarán a comprender Incident Manager y el ciclo de vida de los incidentes:

- ¿Qué es Administrador de incidentes de AWS Systems Manager?
- Ciclo de vida del incidente en Incident Manager

Requisitos previos

Si es la primera vez que utiliza Incident Manager, consulte la Configuración AWS Gestor de Sistemas Gestor de Incidentes. Le recomendamos que configure Incident Manager en la cuenta que utilice para administrar sus operaciones.

Le recomendamos que complete la configuración rápida de Systems Manager antes de iniciar el asistente Preparación de Incident Manager. Utilice Configuración rápida de Systems Manager para configurar los servicios y características de AWS de uso frecuente con las prácticas recomendadas. Incident Manager utiliza las funciones de Systems Manager para gestionar los incidentes asociados a usted Cuentas de AWS y se beneficia de tener Systems Manager configurado primero.

Asistente de preparación

La primera vez que utilice Incident Manager, puede acceder al asistente Preparación desde la página de inicio del servicio Incident Manager. Para acceder al asistente Preparación después de completar la configuración inicial, elija Preparación en la página de la lista de Incidentes.

1. Abra la consola de Incident Manager.
2. En la página de inicio del servicio Incident Manager, elija Preparación.

Configuración general

1. En Configuración general, elija Preparación.

2. Lea los términos y condiciones. Si acepta los términos y condiciones de Incident Manager, seleccione He leído y acepto los términos y condiciones de Incident Manager y, a continuación, elija Siguiente.
3. En el área Regiones, la actual Región de AWS aparece como la primera región del conjunto de réplicas. Para añadir más regiones a su conjunto de réplica, elíjalas en la lista de regiones.

   Le recomendamos que incluya al menos dos regiones. En caso de que una región no esté disponible temporalmente, las actividades relacionadas con incidentes pueden seguir dirigiéndose a la otra región.

   > **Note**
   >
   > Al crear el conjunto de réplica se crea el rol vinculado al servicio `AWSServiceRoleforIncidentManager` en su cuenta. Para obtener más información sobre este rol, consulte Uso de roles vinculados a servicios para Incident Manager.

4. Para configurar el cifrado de su conjunto de réplica, realice una de las siguientes acciones:

   > **Note**
   >
   > Todos los recursos de Incident Manager están cifrados. Para obtener más información sobre cómo se cifran sus datos, consulte Protección de los datos en Incident Manager. Para obtener más información sobre su conjunto de réplica de Incident Manager, consulte Configuración del conjunto de réplicas de Incident Manager.

   - Para usar una AWS clave propia, seleccione Usar AWS clave propia.
   - Para usar tu propia AWS KMS clave, selecciona Elegir una existente AWS KMS key. Para cada región que haya seleccionado en el paso 3, elija una AWS KMS clave o introduzca un nombre de recurso de AWS KMS Amazon (ARN).

     > **Tip**
     >
     > Si no tiene una disponible AWS KMS key, elija Crear una AWS KMS key.

5. (Opcional) En el área Etiquetas, añada una o varias etiquetas al conjunto de réplica. Una etiqueta incluye una clave y, opcionalmente, un valor.

Las etiquetas son metadatos opcionales que usted asigna a un recurso. Las etiquetas permiten clasificar los recursos de diversas maneras, por ejemplo, según la finalidad, el propietario o el entorno. Para obtener más información, consulte Etiquetado de recursos en Administración de incidentes.

6. (Opcional) En el área de acceso al servicio, para activar la función Hallazgos, selecciona la casilla Crear un rol de servicio para los hallazgos en esta cuenta.

   Un resultado es información sobre una implementación de código o un cambio en la infraestructura que se produjo alrededor del mismo momento en que se creó un incidente. Un resultado se puede examinar como una posible causa del incidente. La información sobre estas posibles causas se añade a la página Detalles del incidente del incidente. Con la información sobre estas implementaciones y cambios a mano, los respondedores no necesitan buscar manualmente esta información.

   > **Tip**
   >
   > Para ver información sobre el rol que se va a crear, selecciona Ver detalles del permiso.

7. Seleccione Crear.

   Para obtener más información sobre conjuntos de réplica y capacidad de recuperación, consulte Resiliencia en Administrador de incidentes de AWS Systems Manager.

Contactos (opcional durante la fase de preparación)

Incident Manager administra los contactos durante un incidente. Para obtener más información sobre los contactos, consulte Creación y configuración de contactos en Incident Manager.

1. Elija Crear contacto.
2. En Nombre, introduzca el nombre del contacto.
3. En Alias único, introduzca un alias para identificar a este contacto.
4. En la sección Canal del contacto, haga lo siguiente para definir cómo se involucra al contacto durante los incidentes:

   a. En Tipo, elija Correo electrónico, SMS o Voz.

   b. En Nombre del canal, introduzca un nombre único que le ayude a identificar el canal.

c. En Detalle, introduzca la dirección de correo electrónico o el número de teléfono del contacto.

   Los números de teléfono deben tener entre 9 y 15 caracteres y empezar por + seguido del prefijo del país y el número de suscriptor.

d. Para crear otro canal de contacto, selecciona Añadir canal de contacto. Recomendamos definir al menos dos canales para cada contacto.

5. En el área Plan de participación, haga lo siguiente para definir a través de qué canales se notificará al contacto y cuánto tiempo se esperará para recibir un acuse de recibo a través de cada canal.

> **Note**
>
> Recomendamos definir al menos dos canales en el plan de participación.

   a. En Nombre del canal de contacto, elija un canal que haya especificado en el área Canal de contacto.

   b. En Tiempo de participación (min), introduzca el número de minutos que se debe esperar antes de utilizar el canal de contacto.

      Le recomendamos que seleccione al menos un dispositivo al que conectarse al principio de una participación, especificando **0** (cero) minutos de tiempo de espera.

   c. Para añadir más canales de contacto al plan de participación, elija Añadir participación.

6. (Opcional) En el área Etiquetas, añada una o varias etiquetas al contacto. Una etiqueta incluye una clave y, opcionalmente, un valor.

   Las etiquetas son metadatos opcionales que usted asigna a un recurso. Las etiquetas permiten clasificar los recursos de diversas maneras, por ejemplo, según la finalidad, el propietario o el entorno. Para obtener más información, consulte Etiquetado de recursos en Administración de incidentes.

7. Para crear el registro de contactos y enviar los códigos de activación a los canales de contacto definidos, seleccione Crear.

8. (Opcional) En la página Activación del canal de contacto, introduzca el código de activación enviado a cada canal.

Puede generar nuevos códigos de activación más adelante si no puede introducirlos en este momento.

9. Para añadir contactos adicionales, elija Crear contacto y repita los pasos anteriores.

Planes de escalación (opcional durante Get Prepárate)

1. Elija Crear plan de escalada.

   Durante un incidente, un plan de escalada escala a través de sus contactos a fin de garantizar que Incident Manager implique a los respondedores correctos. Para obtener más información sobre los planes de escalada, consulte Creación de un plan de escalamiento para la participación del personal de respuesta en Incident Manager.

2. En Nombre, introduzca un nombre único para el plan de escalada.
3. En Alias, introduzca un alias único que le ayude a identificar el plan de escalada.
4. En el área Etapa 1, haga lo siguiente:

   a. Para los canales de escalación, elige los canales de contacto con los que interactuar.

   b. Si desea que un contacto pueda detener la progresión de las etapas del plan de escalada, seleccione El reconocimiento detiene la progresión del plan.

   c. Para añadir más canales a una etapa, elija Añadir canal de escalada.

5. Para crear una nueva etapa en el plan de escalada, elija Añadir etapa y añada los detalles de su etapa.
6. (Opcional) En el área Etiquetas, añada una o varias etiquetas al plan de escalada. Una etiqueta incluye una clave y, opcionalmente, un valor.

   Las etiquetas son metadatos opcionales que usted asigna a un recurso. Las etiquetas permiten clasificar los recursos de diversas maneras, por ejemplo, según la finalidad, el propietario o el entorno. Para obtener más información, consulte Etiquetado de recursos en Administración de incidentes.

7. Elija Crear plan de escalada.

Plan de respuesta

> **Note**
>
> Es posible que deba volver a la página de inicio del Administrador de incidentes y elegir Prepararse para continuar.

1. Elija Crear plan de respuesta.

   Utilice el plan de respuesta para reunir los contactos y los planes de escalada que haya creado.

   Durante este asistente de Preparación, las siguientes secciones son opcionales, en especial si es la primera vez que configura un plan de respuesta:

   - Canal de chat
   - Manuales de procedimientos
   - Participaciones
   - Integraciones de terceros

   Para obtener información sobre cómo añadir más adelante estos elementos a los planes de respuesta, consulte Preparación para incidentes en Incident Manager.
2. En Nombre, introduzca un nombre único e identificable para el plan de respuesta. El nombre se utiliza para crear el ARN del plan de respuesta o en planes de respuesta sin nombre que mostrar.
3. (Opcional) En Nombre para mostrar, introduzca un nombre que le ayude a identificar este plan de respuesta al crear incidentes.
4. En Título, introduzca un título que le ayude a identificar el tipo de incidente que se relaciona con este plan de respuesta.

   El valor que especifique se incluye en el título de cada incidente. La alarma o evento que inició el incidente también se añade al título.
5. En Impacto, seleccione el nivel de impacto que espera de los incidentes relacionados con este plan de respuesta, como **`Critical`** o **`Low`**.

6. (Opcional) En Resumen, introduzca una breve descripción que ofrezca una visión general del incidente. Incident Manager rellena automáticamente la información relevante en el resumen durante un incidente.
7. (Opcional) En Cadena de deduplicación, introduzca una cadena de deduplicación. Incident Manager utiliza esta cadena para evitar que la misma causa raíz cree varios incidentes en la misma cuenta.

   Una cadena de deduplicación es un término o frase que el sistema utiliza para buscar incidentes duplicados. Si especifica una cadena de deduplicación, Incident Manager busca incidentes abiertos que contengan la misma cadena en el campo `dedupeString` al crear el incidente. Si se detecta un duplicado, Incident Manager deduplica el incidente más reciente en el incidente existente.

   > **Note**
   >
   > De forma predeterminada, Incident Manager deduplica automáticamente varios incidentes creados por la misma CloudWatch alarma o evento de Amazon EventBridge . No es necesario que introduzca su propia cadena de deduplicación para evitar la duplicación para estos tipos de recursos.

8. (Opcional) En el área Etiquetas de incidentes, añada una o más etiquetas al plan de respuesta. Una etiqueta incluye una clave y, opcionalmente, un valor.

   Las etiquetas son metadatos opcionales que usted asigna a un recurso. Las etiquetas permiten clasificar los recursos de diversas maneras, por ejemplo, según la finalidad, el propietario o el entorno. Para obtener más información, consulte Etiquetado de recursos en Administración de incidentes.
9. Seleccione los contactos y los planes de escalada que se aplicarán al incidente en el cuadro desplegable Participaciones.
10. Elija Crear plan de respuesta.

Una vez que hayas creado un plan de respuesta, puedes asociar CloudWatch las alarmas de Amazon o EventBridge los eventos de Amazon al plan de respuesta. Esto creará automáticamente un incidente en función de una alarma o un evento. Para obtener más información, consulte Crear incidentes de forma automática o manual en Incident Manager.

Gestión de incidentes en todas Cuentas de AWS las regiones en Incident Manager

Puede configurar Incident Manager, una herramienta incluida AWS Systems Manager, para que funcione con varias cuentas Regiones de AWS y. En esta sección se describen las prácticas recomendadas, los pasos de configuración y las limitaciones conocidas entre regiones y entre cuentas.

Temas

Administración de incidentes entre regiones

Incident Manager admite la creación automatizada y manual de incidentes en múltiples Regiones de AWS. Al incorporar por primera vez Incident Manager mediante el asistente Preparación, puede especificar hasta tres Regiones de AWS para su conjunto de réplica. En el caso de los incidentes creados automáticamente por CloudWatch las alarmas o EventBridge los eventos de Amazon, Incident Manager intenta crear un incidente al mismo tiempo Región de AWS que la regla o la alarma del evento. Si Incident Manager sufre una interrupción en esa región, crea EventBridge automáticamente el incidente en otra región en la que se están replicando sus datos. CloudWatch

> **Important**
>
> Tenga en cuenta los siguientes detalles importantes.
>
> - Le recomendamos que especifique al menos dos Regiones de AWS en su conjunto de réplicas. Si no especifica al menos dos regiones, el sistema no podrá crear incidentes durante el periodo en que Incident Manager no esté disponible.
> - Los incidentes creados por una conmutación por error entre regiones no invocan los manuales de procedimientos especificados en los planes de respuesta.

Para obtener más información sobre la iniciación con Incident Manager y la especificación de regiones adicionales, consulte Introducción a Incident Manager.

Administración de incidentes entre cuentas

Incident Manager usa AWS Resource Access Manager (AWS RAM) para compartir los recursos de Incident Manager entre las cuentas de administración y de aplicaciones. En esta sección se describen las prácticas recomendadas entre cuentas, cómo configurar la funcionalidad entre cuentas y las limitaciones conocidas de funcionalidad entre cuentas en Incident Manager.

Una cuenta de administración es la cuenta desde la que se administran las operaciones. En la configuración de una organización, la cuenta de administración es propietaria de los planes de respuesta, los contactos, los planes de escalamiento, los manuales de instrucciones y otros AWS Systems Manager recursos.

Una cuenta de aplicación es la cuenta propietaria de los recursos que componen sus aplicaciones. Estos recursos pueden ser instancias de Amazon EC2, tablas de Amazon DynamoDB o cualquiera de los otros recursos que utiliza para crear aplicaciones en la Nube de AWS. Las cuentas de aplicación también son propietarias de CloudWatch las alarmas de Amazon y EventBridge los eventos de Amazon que crean incidentes en Incident Manager.

AWS RAM utiliza recursos compartidos para compartir recursos entre cuentas. Puede compartir el plan de respuesta y los recursos de contacto entre cuentas en AWS RAM. Al compartir estos recursos, las cuentas de aplicación y las cuentas de administración pueden interactuar con las participaciones y los incidentes. Al compartir un plan de respuesta se comparten todos los incidentes pasados y futuros creados mediante ese plan de respuesta. Al compartir un contacto se comparten todas las participaciones pasadas y futuras del contacto o del plan de respuesta.

Prácticas recomendadas

Observe estas prácticas recomendadas al compartir recursos de Incident Manager entre cuentas:

- Actualice regularmente el uso compartido de recursos con los planes de respuesta y los contactos.
- Revise regularmente las entidades principales del recurso compartido.
- Configure Incident Manager, los manuales de procedimientos y los canales de chat en su cuenta de administración.

Instalación y configuración de la administración de incidentes entre cuentas

Los siguientes pasos describen cómo instalar y configurar los recursos de Incident Manager y utilizarlos para la funcionalidad entre cuentas. Es posible que ya haya configurado anteriormente

algunos servicios y recursos para la funcionalidad entre cuentas. Utilice estos pasos como una lista de comprobación de los requisitos antes de iniciar su primer incidente utilizando recursos entre cuentas.

1. (Opcional) Cree organizaciones y unidades organizativas utilizando AWS Organizations. Siga los pasos del Tutorial: Creación y configuración de una organización en la Guía del usuario de AWS Organizations .
2. (Opcional) Utilice Quick Setup AWS Systems Manager, una herramienta incluida, para configurar las AWS Identity and Access Management funciones correctas que podrá utilizar al configurar sus manuales multicuentas. Para obtener más información, consulte Quick Setup de en la Guía del usuario de AWS Systems Manager .
3. Siga los pasos que se indican en Ejecución de automatizaciones en múltiples cuentas Regiones de AWS y de la Guía del AWS Systems Manager usuario para crear manuales de ejecución en los documentos de automatización de Systems Manager. Un manual de procedimientos puede ser ejecutado por una cuenta de administración o por una de sus cuentas de aplicación. Según su caso de uso, necesitará instalar la AWS CloudFormation plantilla adecuada para las funciones necesarias para crear y ver los manuales de ejecución durante un incidente.
   - Ejecución de un manual de procedimientos en la cuenta de administración. La cuenta de administración debe descargar e instalar la AWS-SystemsManager-AutomationReadOnlyRole CloudFormation plantilla. Al realizar la instalaciónAWS-SystemsManager-AutomationReadOnlyRole, especifique la cuenta IDs de todas las cuentas de la aplicación. Este rol permitirá a sus cuentas de aplicación leer el estado del manual de procedimientos desde la página de detalles del incidente. La cuenta de la aplicación debe instalar la AWS-SystemsManager-AutomationAdministrationReadOnlyRole CloudFormation plantilla. La página de detalles del incidente utiliza este rol para obtener el estado de la automatización de la cuenta de administración.
   - Ejecución de un manual de procedimientos en una cuenta de aplicación. La cuenta de administración debe descargar e instalar la AWS-SystemsManager-AutomationAdministrationReadOnlyRole CloudFormation plantilla. Este rol permite a la cuenta de administración leer el estado del manual de procedimientos en la cuenta de aplicación. La cuenta de la aplicación debe descargar e instalar la AWS-SystemsManager-AutomationReadOnlyRole CloudFormation plantilla. Al instalar `AWS-SystemsManager-AutomationReadOnlyRole`, especifique el ID de cuenta de la cuenta de administración y de otras cuentas de aplicación. La cuenta de administración y otras cuentas de aplicación asumen este rol para leer el estado del manual de procedimientos.

4. (Opcional) En cada cuenta de aplicación de la organización, descarga e instala la AWS-SystemsManager-IncidentManagerIncidentAccessServiceRole CloudFormation plantilla. Al instalar AWS-SystemsManager-IncidentManagerIncidentAccessServiceRole, especifique el ID de cuenta de la cuenta de administración. Esta función proporciona los permisos que Incident Manager necesita para acceder a la información sobre las AWS CodeDeploy implementaciones y las actualizaciones de la CloudFormation pila. Esta información se notifica como resultados de un incidente si la característica Resultados está habilitada. Para obtener más información, consulte Identificar las posibles causas de incidentes de otros servicios como «hallazgos» en Incident Manager.
5. Para configurar y crear contactos, planes de escalada, canales de chat y planes de respuesta, siga los pasos que se detallan en Preparación para incidentes en Incident Manager.
6. Añada sus contactos y recursos de planes de respuesta a su recurso compartido existente o a un nuevo recurso compartido en AWS RAM. Para obtener más información, consulte el Cómo empezar a usar AWS RAM en la Guía del usuario de AWS RAM . Agregar planes de respuesta para permitir que AWS RAM las cuentas de las aplicaciones accedan a los incidentes y a los paneles de incidentes creados con los planes de respuesta. Las cuentas de aplicación también tienen la capacidad de asociar CloudWatch alarmas y EventBridge eventos a un plan de respuesta. Al añadir los contactos y los planes de escalamiento, las cuentas de las aplicaciones pueden ver las interacciones e interactuar con los contactos desde el panel de control de incidentes. AWS RAM
7. Añada la funcionalidad multicuenta y multiregión a su consola. CloudWatch Para ver los pasos y la información, consulta la CloudWatch consola multicuentas entre regiones en la Guía CloudWatch del usuario de Amazon. La adición de esta funcionalidad garantiza que las cuentas de la aplicación y la cuenta de administración que haya creado puedan ver y editar las métricas de los paneles de control de incidentes y análisis.
8. Crea un bus de EventBridge eventos de Amazon con varias cuentas. Para ver los pasos y la información, consulta Enviar y recibir EventBridge eventos de Amazon entre AWS cuentas. A continuación, puede utilizar este bus de eventos para crear reglas de eventos que detecten incidentes en las cuentas de aplicaciones y creen incidentes en la cuenta de administración.

Limitaciones

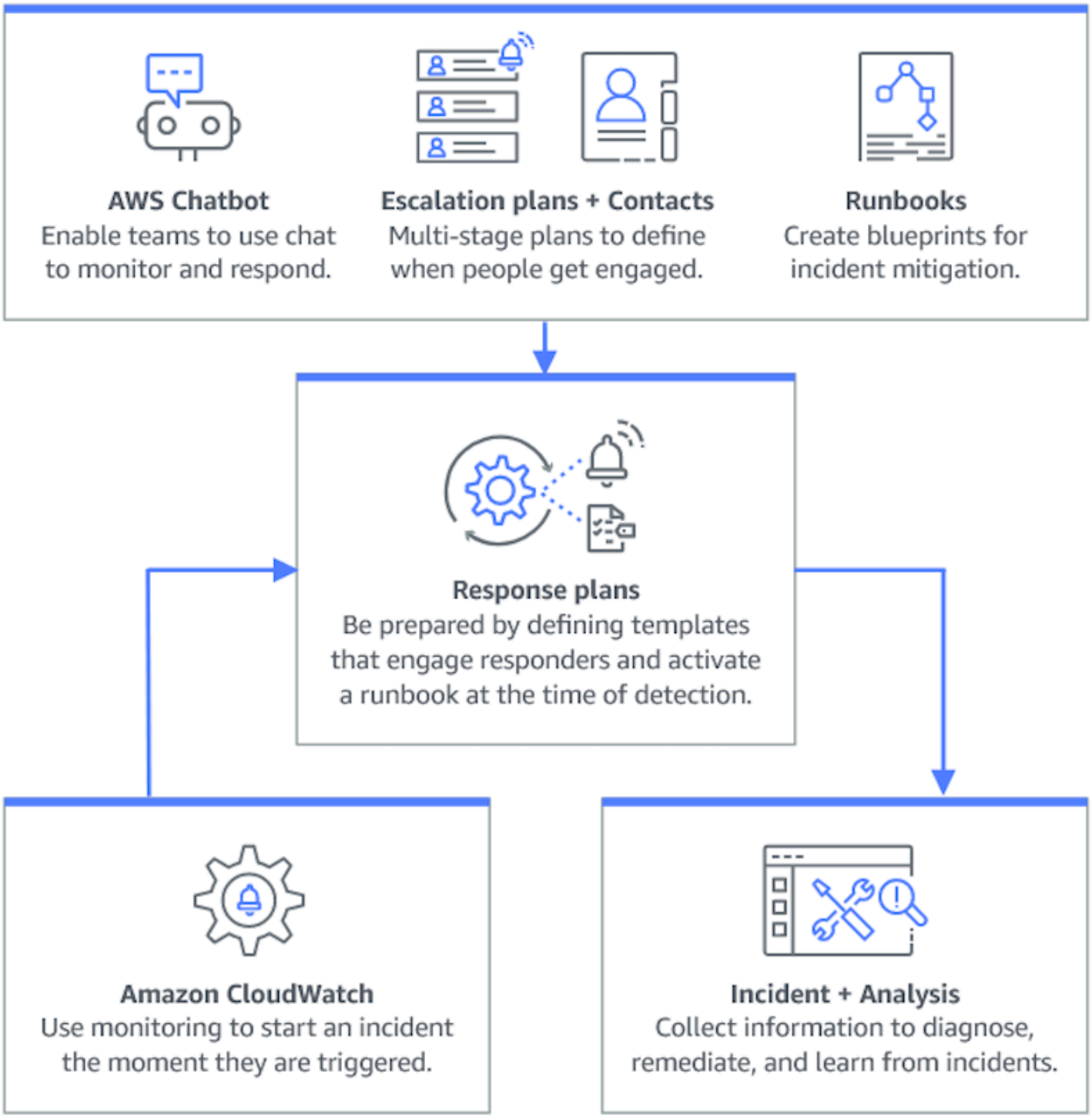
A continuación se indican las limitaciones conocidas de la funcionalidad entre cuentas de Incident Manager:

- La cuenta que crea un análisis post-incidente es la única que puede verlo y modificarlo. Si utiliza una cuenta de aplicación para crear un análisis post-incidente, solo los miembros de esa cuenta podrán verlo y modificarlo. Lo mismo ocurre si utiliza una cuenta de administración para crear un análisis post-incidente.
- Los eventos de línea temporal no se rellenan para los documentos de automatización ejecutados en cuentas de aplicación. Las actualizaciones de los documentos de automatización ejecutados en las cuentas de aplicación son visibles en la pestaña Manual de procedimientos de la incidencia.

- Los temas de Amazon Simple Notification Service no se pueden utilizar entre cuentas. Los temas de Amazon SNS se deben crear en la misma región y cuenta que el plan de respuesta en el que se utiliza. Recomendamos utilizar la cuenta de administración para crear todos los temas de SNS y planes de respuesta.
- Los planes de escalada solo se pueden crear utilizando contactos de la misma cuenta. No es posible añadir un contacto que se haya compartido con usted a un plan de escalada de su cuenta.
- Las etiquetas aplicadas a los planes de respuesta, los registros de incidentes y los contactos solo pueden verse y modificarse desde la cuenta del propietario del recurso.

Preparación para incidentes en Incident Manager

La planificación de un incidente comienza mucho antes del ciclo de vida del incidente. Como se muestra en la siguiente ilustración, antes de empezar a responder a los incidentes, hay que prepararse configurando los canales de chat, creando planes de escalamiento, especificando los contactos y determinando los manuales de automatización que se van a utilizar en la respuesta a los incidentes. A continuación, utilice un plan de respuesta que especifique cómo se lleva a cabo la supervisión y si las respuestas están automatizadas. Una vez completada la remediación, puede analizar el incidente y la respuesta al incidente para perfeccionar aún más su plan de respuesta para futuros incidentes.



Temas

- Supervisión
- Configuración de conjuntos de replicación y resultados en Incident Manager
- Creación y configuración de contactos en Incident Manager

- Gestión de las rotaciones de personal de respuesta con horarios de guardia en Incident Manager
- Creación de un plan de escalamiento para la participación del personal de respuesta en Incident Manager
- Creación e integración de canales de chat para el personal de respuesta en Incident Manager
- Integración de los manuales de automatización de Systems Manager en Incident Manager para la solución de incidentes
- Creación y configuración de planes de respuesta en Incident Manager
- Identificar las posibles causas de incidentes de otros servicios como «hallazgos» en Incident Manager

Supervisión

Supervisar el estado de las aplicaciones AWS alojadas es clave para garantizar el tiempo de actividad y el rendimiento de las aplicaciones. A la hora de determinar las soluciones de monitoreo, tenga en cuenta lo siguiente:

- Criticidad de la característica: si el sistema fallara, ¿cuán crítico sería el impacto para los usuarios intermedios?
- Comunalidad de los fallos: con qué frecuencia falla un sistema; los sistemas que requieren una intervención frecuente deben ser monitoreados de cerca.
- Aumento de la latencia: cuánto ha aumentado o disminuido el tiempo necesario para completar una tarea.
- Métricas del lado del cliente vs. métricas del lado del servidor: si existe una discrepancia entre las métricas relacionadas en el cliente y en el servidor.
- Fallos de dependencia: fallos para los que su equipo puede y debería prepararse.

Después de crear planes de respuesta, puede utilizar sus soluciones de monitoreo para hacer un seguimiento automático de los incidentes en el momento en que se produzcan en su entorno. Para obtener más información sobre el seguimiento y la creación de incidentes, consulte Visualización de los detalles del incidente en la consola de Incident Manager.

Para obtener más información sobre cómo diseñar aplicaciones y cargas de trabajo de infraestructura seguras, de alto rendimiento, resilientes y eficientes, consulte Well-Architected.AWS

Configuración de conjuntos de replicación y resultados en Incident Manager

Una vez que haya completado el asistente de preparación del administrador de incidentes, podrá gestionar determinadas opciones en la página de configuración. Estas opciones incluyen su conjunto de réplica, las etiquetas aplicadas al conjunto de réplica y la característica Resultados.

Temas

Configuración del conjunto de réplicas de Incident Manager

El conjunto de replicación de Incident Manager replica sus datos Regiones de AWS en varios para hacer lo siguiente:

- Aumente la redundancia entre regiones
- Permita que Incident Manager acceda a los recursos de diferentes regiones y reduzca la latencia para sus usuarios.
- Cifre sus datos con una clave gestionada por el cliente Clave administrada de AWS o con la suya propia.

  Todos los recursos de Incident Manager están cifrados de forma predeterminada. Para obtener más información sobre cómo se cifran sus recursos, consulte Protección de los datos en Incident Manager.

Para empezar a utilizar Incident Manager, cree primero su conjunto de réplica mediante el asistente Preparación. Para obtener más información sobre cómo prepararse en Incident Manager, consulte el Asistente de preparación.

Edición de su conjunto de réplica

Puede editar su conjunto de réplica mediante la página Configuración de Incident Manager. Puede añadir o eliminar regiones y habilitar o deshabilitar la protección de borrado del conjunto de réplica.

No puede editar la clave utilizada para cifrar sus datos. Para cambiar la clave, debe eliminar y volver a crear el conjunto de réplica.

Adición de una región

1. Abra la consola de Incident Manager y, a continuación, elija Configuración en el panel de navegación izquierdo.
2. Elija Añadir región.
3. Seleccione la Región.
4. Elija Añadir.

Eliminación de una región

1. Abra la consola de Incident Manager y, a continuación, elija Configuración en el panel de navegación izquierdo.
2. Seleccione la región que desee eliminar.
3. Elija Eliminar.
4. Escriba delete (eliminar) en el cuadro de texto y elija Eliminar.

Eliminación de su conjunto de réplica

Al eliminar la última región en su conjunto de réplica se elimina el conjunto de réplica por completo. Antes de poder eliminar la última región, desactiva la protección contra eliminación desactivándola en la página de configuración. Después de eliminar su conjunto de réplica, puede crear un nuevo conjunto de réplica utilizando el asistente Preparación.

Para eliminar una región de su conjunto de réplica, debe esperar 24 horas después de crearla. Si intenta eliminar una región de su conjunto de réplica antes de que transcurran 24 horas desde su creación, la eliminación fallará.

Al eliminar su conjunto de réplica se eliminan todos los datos de Incident Manager.

Eliminación del conjunto de réplica

1. Abra la consola de Incident Manager y, a continuación, elija Configuración en el panel de navegación izquierdo.
2. Seleccione la última región en su conjunto de réplica.

3. Elija Eliminar.
4. Escriba delete (eliminar) en el cuadro de texto y elija Eliminar.

Administración de las etiquetas de un conjunto de réplica

Las etiquetas son metadatos opcionales que usted asigna a un recurso. Utilice etiquetas para categorizar un recurso de diferentes maneras, como por ejemplo, por finalidad, propietario o entorno.

Para administrar las etiquetas de un conjunto de réplica

1. Abra la consola de Incident Manager y, a continuación, elija Configuración en el panel de navegación izquierdo.
2. En el área Etiquetas, elija Editar.
3. Para añadir una etiqueta, haga lo siguiente:
    a. Elija Añadir nueva etiqueta.
    b. Escriba una clave y un valor opcional para la etiqueta.
    c. Seleccione Save.
4. Para eliminar una etiqueta, haga lo siguiente:
    a. Debajo de la etiqueta que desee eliminar, seleccione Eliminar.
    b. Seleccione Save.

Administración de la característica Resultados

La característica Resultados ayuda a los respondedores de su organización a identificar las posibles causas raíz de los incidentes poco después de que estos comiencen. Actualmente, Incident Manager proporciona información sobre las AWS CodeDeploy implementaciones y las actualizaciones de las AWS CloudFormation pilas.

Para que los resultados sean compatibles en todas las cuentas, una vez habilitada la característica, deberá completar un paso de configuración adicional en cada cuenta de aplicación de la organización.

Para utilizar la característica, debe dejar que Incident Manager cree un rol de servicio que incluya los permisos necesarios para acceder a los datos en su nombre.

Para habilitar la característica Resultados

1. Abra la consola de Incident Manager y, a continuación, elija Configuración en el panel de navegación izquierdo.
2. En el área Resultados, elija Crear rol de servicio.
3. Revise la información sobre el rol de servicio que va a crear y, a continuación, elija Crear.

Para deshabilitar la característica Resultados

Para dejar de utilizar la característica Resultados, elimine el rol `IncidentManagerIncidentAccessServiceRole` de cada cuenta en la que se haya creado.

1. Abra la consola de IAM en https://console.aws.amazon.com/iam/.
2. En el panel de navegación izquierdo, elija Roles.
3. En el cuadro de búsqueda, escriba **`IncidentManagerIncidentAccessServiceRole`**.
4. Elija el nombre del rol y, a continuación, elija Eliminar.
5. Introduzca el nombre del rol en el cuadro de diálogo para confirmar que desea eliminarlo y, a continuación, elija Eliminar.

Creación y configuración de contactos en Incident Manager

Administrador de incidentes de AWS Systems Manager los contactos responden a los incidentes. Un contacto puede tener varios canales que Incident Manager puede involucrar durante un incidente. Puede definir el plan de participación de un contacto a fin de describir cómo y cuándo Incident Manager se relaciona con el contacto.

Temas

- Canales de contacto
- Planes de participación
- Creación de un contacto
- Importación de datos de contacto a su libreta de direcciones

Canales de contacto

Los canales de contacto son los distintos métodos que utiliza Incident Manager para interactuar con un contacto.

Incident Manager admite los siguientes canales de contacto:

- Correo electrónico
- Servicio de mensajes cortos (SMS)
- Voz

Activación del canal de contacto

Para proteger su privacidad y seguridad, Incident Manager le envía un código de activación de dispositivos al crear contactos. Para utilizar sus dispositivos durante un incidente, primero debe activarlos. Para ello, introduzca el código de activación del dispositivo en la página de creación de contactos.

Algunas características de Incident Manager incluyen funciones que envían notificaciones a un canal de contacto. Al utilizar estas características, usted da su consentimiento para que este servicio envíe notificaciones sobre interrupciones del servicio u otros eventos a los canales de contacto incluidos en el flujo de trabajo especificado. Esto incluye las notificaciones enviadas a un contacto como parte de una rotación de horario de guardia. Las notificaciones podrían enviarse por correo electrónico, mensaje SMS o llamada de voz, según se especifique en los datos de un contacto. Al utilizar estas características, usted confirma que está autorizado a añadir los canales de contacto que proporciona a Incident Manager.

Desactivación

Puede cancelar estas notificaciones en cualquier momento; para ello, elimine un dispositivo móvil como canal de contacto. Los destinatarios individuales de las notificaciones también pueden cancelar las notificaciones en cualquier momento eliminando el dispositivo de su contacto.

Para eliminar un canal de contacto de un contacto

1. Vaya a la consola de Incident Manager y elija Contactos en el panel de navegación izquierdo.
2. Seleccione el contacto con el canal de contacto que vaya a eliminar y elija Editar.
3. Elija Eliminar junto al canal de contacto que desea eliminar.

4. Elija Actualizar.

Desactivación del canal de contacto

Para desactivar un dispositivo, responda UNSUBSCRIBE. Al responder UNSUBSCRIBE, impide que Incident Manager controle su dispositivo.

Reactivación del canal de contacto

1. Responda START al mensaje de Incident Manager.
2. Vaya a la consola de Incident Manager y elija Contactos en el panel de navegación izquierdo.
3. Seleccione el contacto con el canal de contacto que vaya a eliminar y elija Editar.
4. Elija Activar dispositivos.
5. Introduzca el Código de activación enviado al dispositivo por Incident Manager.
6. Seleccione Activar.

Planes de participación

Los planes de participación definen cuándo Incident Manager utiliza los canales de contacto. Puede activar los canales de contacto varias veces en diferentes etapas desde el inicio de una intervención. Puede utilizar planes de participación en un plan de escalada o en un plan de respuesta. Para obtener más información sobre los planes de escalada, consulte Creación de un plan de escalamiento para la participación del personal de respuesta en Incident Manager.

Creación de un contacto

Para crear un contacto, siga estos pasos.

1. Abra la consola de Incident Manager y elija Contactos en el panel de navegación izquierdo.
2. Elija Crear contacto.
3. Escriba el nombre completo del contacto y proporcione un alias único e identificable.
4. Defina un Canal de contacto. Le recomendamos que disponga de dos o más tipos diferentes de canales de contacto.
    a. Elija el tipo: correo electrónico, SMS o voz.
    b. Introduzca un nombre identificable para el canal de contacto.

c. Proporcione los detalles del canal de contacto, como el correo electrónico: arosalez@example.com.

5. Para definir más de un canal de contacto, elija Añadir canal de contacto. Repita el paso 4 para cada nuevo canal de contacto añadido.
6. Defina un plan de participación.

> **Important**
>
> Para involucrar a un contacto, debe definir un plan de participación.

   a. Elija un Nombre de canal de contacto.
   b. Defina cuántos minutos desde el inicio de la participación se debe esperar hasta que Incident Manager utilice este canal de contacto.
   c. Para añadir otro canal de contacto, elija Añadir participación.
7. Una vez definido el plan de participación, seleccione Crear. Incident Manager envía un código de activación a cada uno de los canales de contacto definidos.
8. (Opcional) Para activar los canales de contacto, introduzca el código de activación que Incident Manager envió a cada canal de contacto definido.
9. (Opcional) Para enviar un nuevo código de activación, seleccione Enviar nuevo código.
10. Seleccione Finalizar.

Después de definir un contacto y activar sus canales de contacto, puede añadir contactos a los planes de escalada para formar una cadena de escalado. Para obtener más información sobre los planes de escalada, consulte Creación de un plan de escalamiento para la participación del personal de respuesta en Incident Manager. Puede añadir contactos a un plan de respuesta para lograr una participación directa. Para obtener más información sobre la creación de planes de respuesta, consulte Creación y configuración de planes de respuesta en Incident Manager.

Importación de datos de contacto a su libreta de direcciones

Al crearse un incidente, Incident Manager puede avisar a los respondedores mediante notificaciones de voz o SMS. Para garantizar que los respondedores vean que la llamada o la notificación por SMS procede de Incident Manager, recomendamos que todos los respondedores descarguen el archivo formato de tarjeta virtual (.vcf) de Incident Manager a la libreta de direcciones de sus dispositivos

móviles. El archivo está alojado en Amazon CloudFront y está disponible en la partición AWS comercial.

Para descargar el archivo .vcf de Incident Manager

1. En su dispositivo móvil, elija o introduzca la siguiente URL: https://d26vhuvd5b89k2.cloudfront.net/ aws-incident-manager .vcf.
2. Guarde o importe el archivo a la libreta de direcciones de su dispositivo móvil.

Gestión de las rotaciones de personal de respuesta con horarios de guardia en Incident Manager

Un horario de guardia en Incident Manager define a quién se notifica al producirse un incidente que requiera la intervención de un operario. Un horario de guardia consta de una o más rotaciones que usted crea para el horario. Cada rotación puede incluir hasta 30 contactos.

Después de crear un horario de guardia, puede incluirlo como una escalada en su plan de escalada. Al producirse un incidente asociado a ese plan de escalada, Incident Manager lo notifica al operador (u operadores) de guardia según el horario. Este contacto puede entonces dar reconocimiento de su participación. En su plan de escalada, puede designar uno o más horarios de guardia, así como uno o más contactos individuales, a través de múltiples etapas de escalado. Para obtener más información, consulte Creación de un plan de escalamiento para la participación del personal de respuesta en Incident Manager.

> **Tip**
>
> Como práctica recomendada, le sugerimos que añada contactos y horarios de guardia como canales de escalada en un plan de escalada. A continuación, debe elegir un plan de escalada como la participación en un plan de respuesta. Este enfoque proporciona la cobertura más completa para la respuesta a incidentes en su organización.

Cada horario de guardia admite hasta ocho rotaciones. Las rotaciones pueden superponerse o ejecutarse de forma concurrente. Esto aumenta el número de operadores notificados para responder al producirse un incidente. También puede crear rotaciones que se ejecuten consecutivamente. Esto admite escenarios como la administración de incidentes “follow-the-sun” (jornada continua) en la que tiene grupos en todo el mundo que dan soporte al mismo servicio.

Utilice los temas de esta sección como ayuda para crear y administrar horarios de guardia para sus operaciones de respuesta a incidentes.

Temas

Creación de un horario de guardia y rotaciones en Incident Manager

Cree un horario de guardia con una o varias rotaciones de contactos a los que contactar para responder a incidentes durante sus turnos.

Antes de empezar

Antes de crear un horario de guardia, asegúrese de haber creado previamente los contactos que desea añadir a las rotaciones del horario. Para obtener información, consulte Creación y configuración de contactos en Incident Manager.

Consideración de los cambios de horario de verano (DST)

Al crear una rotación, usted especifica la zona horaria global que sirve de base para las horas de cobertura de turnos y las fechas para esta rotación. Puede utilizar cualquier zona horaria definida por la Autoridad de Números Asignados en Internet (Internet Assigned Numbers Authority, IANA). Por ejemplo, `America/Los_Angeles`, `UTC` y `Asia/Seoul`. Puede añadir más de una rotación a un horario de guardia. Sin embargo, si los respondedores de cada rotación se encontrasen geográficamente en zonas horarias diferentes, tenga en cuenta cualquier cambio de horario de verano al que podría estar sujeta cada rotación.

Por ejemplo, `America/Los_Angeles` y `Europe/Dublin` observan horarios de verano diferentes. Como resultado, la diferencia horaria entre las dos zonas puede variar de 6 a 8 horas según la época del año. Por ejemplo, un horario follow-the-sun de guardia tiene una rotación en la zona `America/Los_Angeles` horaria y otra en la zona horaria. `Europe/Dublin` En este ejemplo, el horario puede contener una brecha de turnos de una hora o un solapamiento de turnos de una hora debido a los cambios por horario de verano.

Para evitar estas situaciones, le recomendamos el siguiente enfoque:

1. Utilice una única zona horaria para todas las rotaciones en un horario de guardia.
2. Calcule las horas locales al asignar respondedores fuera de esa zona horaria en particular.

Si decide asignar cada rotación a su zona horaria local, revise el horario antes que cualquier horario de verano. A continuación, ajuste los horarios de rotación de turnos según sea necesario para asegurarse de evitar brechas o solapamientos involuntarios en su cobertura de guardia antes de que entre en vigor cualquier cambio de horario de verano.

Para crear un horario de guardia

1. Abra la consola de Incident Manager.
2. En el panel de navegación izquierdo, elija Horarios de guardia.
3. Elija Crear horario de guardia.
4. En Nombre del horario, introduzca un nombre que le ayude a identificar el horario, como **`MyApp Primary On-call Schedule`**.
5. En el caso del alias de horario, introduzca un alias para este horario que sea único en el horario actual Región de AWS, por ejemplo. **`my-app-primary-on-call-schedule`**
6. (Opcional) En el área Etiquetas, aplique uno o más pares de nombre clave y valor de etiqueta al horario de guardia.

   Las etiquetas son metadatos opcionales que usted asigna a un recurso. Las etiquetas permiten clasificar los recursos de diversas maneras, por ejemplo, según la finalidad, el propietario o el entorno. Por ejemplo, puede etiquetar un horario para identificar el periodo en que se ejecuta, los tipos de operadores que contiene o el plan de escalada que admita. Para obtener más información sobre el etiquetado de recursos de Incident Manager, consulte Etiquetado de recursos en Administración de incidentes.
7. Realice a continuación la adición de una o más rotaciones al plan de guardia.

Creación de una rotación para un plan de guardia en Incident Manager

Una rotación en un programa de guardia especifica cuándo está vigente el turno. También especifica los contactos que rotan en los turnos. Puede incluir hasta ocho rotaciones en un único programa de guardia.

En una rotación puede añadir a cualquier persona que haya creado como contacto en Incident Manager. Para obtener información sobre la administración de sus contactos, consulte Creación y configuración de contactos en Incident Manager.

A medida que configura su rotación, puede ver el aspecto general del horario en un calendario de Vista previa en la parte derecha de la página.

Para crear una rotación en un horario de guardia

1. En la sección Rotación 1 de la página Crear horario de guardia, en Nombre de la rotación, introduzca un nombre que identifique la rotación, como **`00:00 - 7:59 Support`** o **`Dublin Support Group`**.
2. En Fecha de inicio, introduzca la fecha en la que se activa esta rotación en formato `YYYY/MM/DD`, como `2023/07/14`.
3. En Zona horaria, seleccione la zona horaria global que sirve de base para las horas de cobertura de turnos y las fechas que especifique para esta rotación.

   Puede utilizar cualquier zona horaria definida por la Autoridad de Números Asignados en Internet (Internet Assigned Numbers Authority, IANA). Por ejemplo: "America/Los_Angeles", "UTC", "Asia/Seoul». Para obtener más información, consulte la base de datos de zonas horarias en el sitio web de IANA.

   > **Warning**
   >
   > Puede basar cada rotación en su propia zona horaria. Sin embargo, cualquier cambio por horario de verano en las zonas horarias que seleccione puede afectar a sus ventanas de cobertura previstas. Para obtener más información, consulte Consideración de los cambios de horario de verano (DST), tratado anteriormente en este tema.

4. En Hora de inicio de la rotación, introduzca la hora a la que comienza el turno de esta rotación en formato `hh:mm` de 24 horas, como `16:00`.

   Tenga en cuenta las diferencias en la hora local para los contactos que se encuentren en zonas horarias distintas a la que ha especificado. Por ejemplo, si elige `America/Los_Angeles` como zona horaria y `00:00` como hora de inicio de la rotación, esto equivale a las 08:00 en Dublín (Irlanda) y a las 13:30 en Bombay (India).
5. En Hora de finalización de la rotación, introduzca la hora a la que finaliza el turno de esta rotación en formato `hh:mm` de 24 horas, como `23:59`.

   > **Note**
   >
   > El tiempo entre el inicio y el final de una rotación debe ser de al menos 30 minutos.

6. (Opcional) Para establecer la duración de la rotación en 24 horas, elija Cobertura de 24 horas e introduzca la hora de inicio de esta rotación en el campo Hora de inicio de la rotación. El valor de Hora de finalización de la rotación se actualiza automáticamente.

   Por ejemplo, si desea que su guardia tenga una cobertura de 24 horas con el cambio de turno a las 11 AM, seleccione Cobertura de 24 horas e introduzca **`11:00`** como hora de inicio.
7. En Días activos, seleccione los días de la semana en los que esta rotación estará activa. Por ejemplo, si su plan de guardia excluye la cobertura de fin de semana, seleccione todos los días excepto sábado y domingo.
8. Realice a continuación la Adición de contactos a la rotación.

Adición de contactos a una rotación en un horario de guardia en Incident Manager

Para cada rotación de su programa de guardia, puede añadir uno o varios contactos, hasta un total de 30. Puede elegir entre los contactos establecidos en la configuración de Incident Manager.

Al añadir un contacto a una rotación, este puede recibir notificaciones como parte de sus obligaciones de guardia. Las notificaciones pueden enviarse por correo electrónico, SMS o llamada de voz, según se especifique en los datos del contacto.

Para obtener información sobre cómo administrar los contactos y las opciones de notificación de contactos, consulte Creación y configuración de contactos en Incident Manager.

Para añadir contactos a una rotación en un programa de guardia

1. En la página Crear horario de guardia, en la sección Contactos de la rotación, elija Añadir o eliminar contactos.
2. En el cuadro de diálogo Añadir o eliminar contactos, seleccione los alias de los contactos que desee incluir en la rotación.

   El orden en que seleccione los contactos es el orden en que aparecen por primera vez en el calendario de rotación. Puede cambiar el orden de los contactos después de añadirlos.
3. Elija Confirmar.
4. Para cambiar la posición de orden de un contacto, seleccione el botón de opción correspondiente a ese usuario y utilice los botones Arriba () y Abajo

( ) para actualizar el orden de los contactos.

5. Realice a continuación la Especificación de periodicidad y duración de los turnos individuales para la rotación.

Especificación de periodicidad y duración de los turnos y adición de etiquetas a una rotación en Incident Manager

La periodicidad de los turnos especifica la frecuencia con la que los contactos de una rotación entran y salen de la guardia. Una duración de periodicidad se puede especificar en número de días, semanas o meses.

Para especificar la periodicidad y duración de los turnos y añadir etiquetas a una rotación

1. En la página Crear horario de guardia, en la sección Configuración de periodicidad de la rotación, haga lo siguiente:

   - En Tipo de periodicidad del turno, especifique si cada turno de guardia dura un número de días, semanas o meses eligiendo entre `Daily`, `Weekly` y `Monthly`.
   - En Duración del turno, introduzca cuántos días, semanas o meses dura un turno.

     Por ejemplo, si elige `Daily` e introduce **1**, el turno de guardia de cada contacto dura un día. Si elige `Weekly` e introduce **3**, el turno de guardia de cada contacto dura tres semanas.

2. (Opcional) En el área Etiquetas, aplique uno o más pares de nombre clave y valor de etiqueta a la rotación.

   Las etiquetas son metadatos opcionales que usted asigna a un recurso. Las etiquetas permiten clasificar los recursos de diversas maneras, por ejemplo, según la finalidad, el propietario o el entorno. Por ejemplo, puede etiquetar una rotación para identificar la ubicación de los contactos asignados a ella, el tipo de cobertura que debe proporcionar o el plan de escalada que respaldará. Para obtener más información sobre el etiquetado de recursos de Incident Manager, consulte Etiquetado de recursos en Administración de incidentes.

3. (Recomendado) Utilice la vista previa del calendario para asegurarse de que no haya brechas involuntarias en la cobertura de su plan de guardia.

4. Seleccione Crear.

Ahora puede añadir el horario de guardia como canal de escalada en un plan de escalada. Para obtener información, consulte Creación de un plan de escalada.

Administración de un horario de guardia existente en Incident Manager

Utilice el contenido de esta sección como ayuda para trabajar con los horarios de guardia que ya haya creado.

Temas

Visualización de detalles del horario de guardia

Puedes acceder a un at-a-glance resumen de un horario de guardia en la página Ver detalles del horario de guardia. Esta página también contiene información sobre quién está actualmente de guardia y quién lo estará a continuación. La página incluye una vista de calendario que muestra qué contactos están de guardia en un momento determinado.

Para ver los detalles de un horario de guardia

1. Abra la consola de Incident Manager.
2. En el panel de navegación izquierdo, elija Horarios de guardia.
3. En la fila del horario de guardia que desee ver, realice una de las siguientes acciones:

   - Para abrir una vista resumida del calendario, elija el alias del horario.

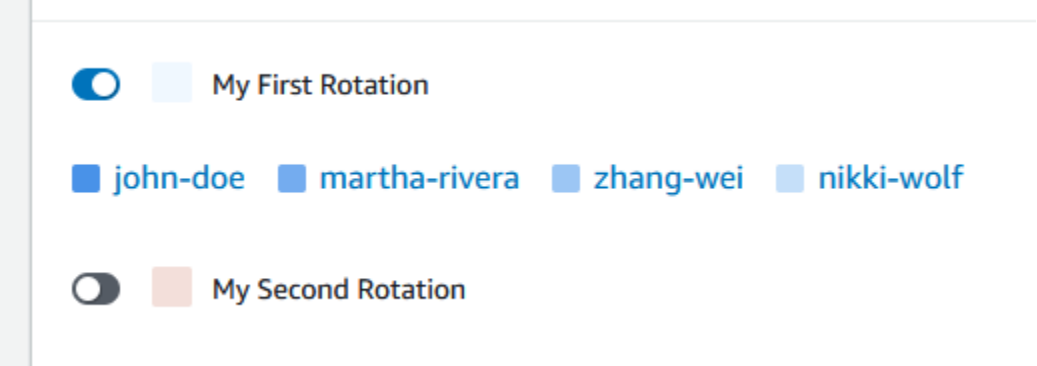
     -o bien-

     Seleccione el botón de opción de la fila y luego elija Ver.
   - Para abrir una vista de calendario del horario, elija Ver calendario

     En la vista de calendario, elija el nombre de un contacto en una fecha específica del horario para ver los detalles sobre el turno asignado o crear una anulación.

- Para activar o desactivar la visualización de una rotación específica en el calendario, selecciona la palanca situada junto al nombre de la rotación.



Edición de un horario de guardia

Puede actualizar la configuración de un horario de guardia y sus rotaciones, excepto los siguientes detalles:

- El alias del horario
- Los nombres de las rotaciones
- Las fechas de inicio de las rotaciones

Para utilizar un calendario existente como base para un nuevo calendario con la posibilidad de cambiar estos valores, puede copiar el calendario en cuestión. Para obtener información, consulte Copia de un horario de guardia.

Para editar un horario de guardia

1. Abra la consola de Incident Manager.
2. En el panel de navegación izquierdo, elija Horarios de guardia.
3. Realice una de las siguientes acciones:
   - Seleccione el botón de opción en la fila del horario de guardia que desee editar y luego elija Editar.
   - Seleccione el alias del horario de guardia para abrir la página Ver detalles del horario de guardia y luego elija Editar.
4. Realice las modificaciones necesarias en el horario de guardia y sus rotaciones. Puede cambiar las opciones de configuración de las rotaciones, como las horas de inicio y fin, los contactos y la

periodicidad. Puede añadir o eliminar rotaciones del horario según sea necesario. La vista previa del calendario refleja sus cambios a medida que los realiza.

Para obtener información sobre cómo utilizar las opciones de la página, consulte Creación de un horario de guardia y rotaciones en Incident Manager.

5. Elija Actualizar.

> **Important**
>
> Si edita un horario que contiene anulaciones, sus cambios pueden afectar a las anulaciones. Para asegurarse de que sus anulaciones permanezcan configuradas de la forma esperada, le recomendamos que revise detenidamente sus anulaciones de turnos después de actualizar el horario.

Copia de un horario de guardia

Para utilizar la configuración de un horario de guardia existente como punto de partida para un nuevo horario, puede crear una copia del horario y modificarla según sea necesario.

Para copiar un horario de guardia

1. Abra la consola de Incident Manager.
2. En el panel de navegación izquierdo, elija Horarios de guardia.
3. Seleccione el botón de opción en la fila del horario de guardia que desee copiar.
4. Elija Copiar.
5. Realice las modificaciones necesarias en el calendario y sus rotaciones. Puede cambiar, añadir o eliminar rotaciones según sea necesario.

> **Note**
>
> Al copiar un horario existente, debe especificar nuevas fechas de inicio para cada rotación. Los horarios copiados no admiten rotaciones con fechas de inicio en el pasado.

Para obtener información sobre cómo utilizar las opciones de la página, consulte Creación de un horario de guardia y rotaciones en Incident Manager.

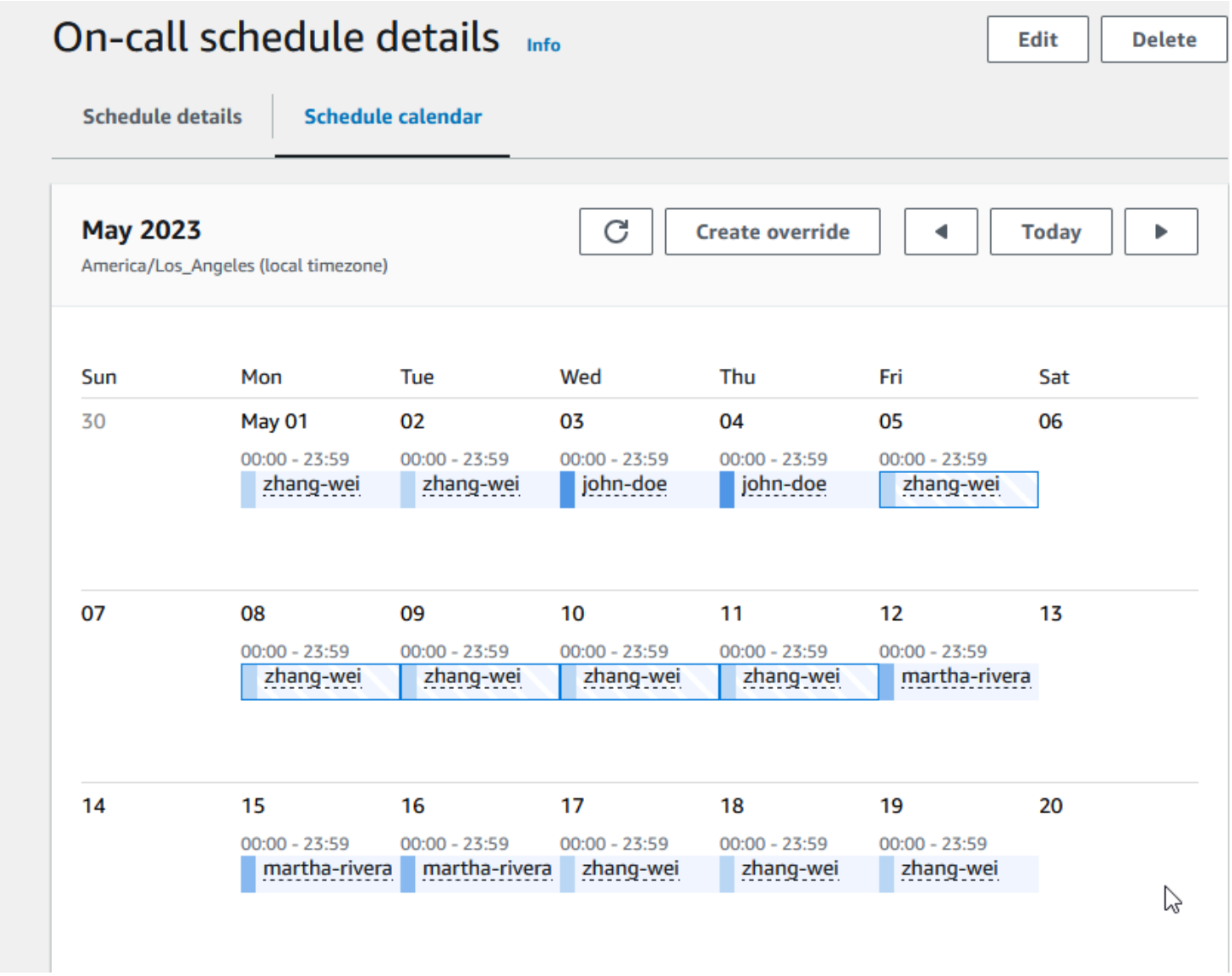
6. Elija Crear copia.

Creación de una anulación para una rotación del horario de guardia

Si necesita realizar cambios puntuales en un programa de rotación existente, puede crear una anulación. Una anulación le permite sustituir el turno de un contacto, de forma total o parcial, por otro contacto. También puede crear una anulación que abarque varios turnos.

Solo puede asignar a una anulación contactos que ya estén asignados a la rotación.

En la vista previa del calendario, los turnos anulados se muestran con un fondo con franja en vez de un fondo sólido. En la siguiente imagen se muestra que el contacto llamado Zhang Wei está de guardia en una operación de anulación. La anulación incluye partes de los turnos de John Doe y Martha Rivera, que comenzarán el 5 de mayo y finalizarán el 11 de mayo.



Para crear una anulación de un horario de guardia

1. Abra la consola de Incident Manager.
2. En el panel de navegación izquierdo, elija Horarios de guardia.
3. En la fila del horario de guardia que desee ver, realice una de las siguientes acciones:
   - Elija el alias del horario y, a continuación, la pestaña Calendario del horario.
   - Elija Ver calendario
4. Realice una de las siguientes acciones:
   - Elija Crear anulación.

- Elija el nombre de un contacto en la vista previa del calendario y, a continuación, elija Anular turno.

5. En el cuadro de diálogo Crear anulación de turno, haga lo siguiente:

> **Note**
>
> Una anulación debe tener una duración mínima de 30 minutos. Solo puede especificar una anulación para turnos que tengan lugar como máximo seis meses en el futuro.

   a. En Seleccionar rotación, seleccione el nombre de la rotación en la que desea crear una anulación.
   b. En Fecha de inicio, seleccione o introduzca la fecha en la que comienza la anulación.
   c. En Hora de inicio, introduzca la hora de inicio de la anulación en formato `hh:mm`.
   d. En Fecha de finalización, seleccione o introduzca la fecha en la que finaliza la anulación.
   e. En Hora de finalización, introduzca la hora a la que finaliza la anulación, en formato `hh:mm`.
   f. En Seleccionar contacto de anulación, seleccione el nombre del contacto de rotación que estará de guardia durante el periodo de anulación.

6. Elija Crear anulación.

Después de crear una anulación, puede identificarla por su fondo con franja. Al elegir el nombre del contacto de un turno anulado, un cuadro de información lo identifica como turno anulado. Puede elegir Eliminar anulación para eliminarla y restaurar la asignación de guardia original.

Eliminación de un horario de guardia

Cuando ya no necesite un determinado horario de guardia, puede eliminarlo de Incident Manager.

Si algún plan de escalada o de respuesta utiliza actualmente el horario de guardia como canal de escalada, deberá eliminarlo de esos planes para poder eliminar el horario.

Para eliminar un horario de guardia

1. Abra la consola de Incident Manager.
2. En el panel de navegación izquierdo, elija Horarios de guardia.
3. Seleccione el botón de opción en la fila del horario de guardia que desee eliminar.

4. Elija Eliminar.
5. En el cuadro de diálogo ¿Eliminar horario de guardia?, introduzca **`confirm`** en el cuadro de texto.
6. Elija Eliminar.

Creación de un plan de escalamiento para la participación del personal de respuesta en Incident Manager

Administrador de incidentes de AWS Systems Manager proporciona rutas de escalamiento a través de sus contactos definidos o sus horarios de guardia, conocidos colectivamente como canales de escalamiento. Puede incorporar múltiples canales de escalada a un incidente al mismo tiempo. Si los contactos designados en el canal de escalada no responden, Incident Manager escala al siguiente conjunto de contactos. También puede elegir si un plan deja de escalar una vez que un usuario reconoce la participación. Puede añadir planes de escalada a un plan de respuesta para que la escalada comience automáticamente al principio de un incidente. También puede añadir planes de escalada a un incidente activo.

Temas

Etapas

Los planes de escalada utilizan etapas en las que cada una dura un número definido de minutos. Cada etapa tiene la siguiente información:

- Duración: la cantidad de tiempo que el plan espera hasta comenzar la siguiente etapa. La primera etapa del plan de escalada comienza una vez iniciada la participación.
- Canal de escalada: un canal de escalada es un contacto único o un horario de guardia compuesto por varios contactos que rotan responsabilidades según un horario definido. El plan de escalada compromete a cada canal utilizando su plan de participación definido. Puede configurar cada canal de escalada para detener la progresión del plan de escalada antes de que continúe a la siguiente etapa. Cada etapa puede tener múltiples canales de escalada.

Para obtener información sobre la configuración de contactos individuales, consulte Creación y configuración de contactos en Incident Manager. Para obtener información sobre la creación de horarios de guardia, consulte Gestión de las rotaciones de personal de respuesta con horarios de guardia en Incident Manager.

Creación de un plan de escalada

1. Abra la consola de Incident Manager y elija Planes de escalada en el panel de navegación izquierdo.
2. Elija Crear plan de escalada.
3. En Nombre, introduzca un nombre único para el plan de escalada, como **`My Escalation Plan`**.
4. En Alias, introduzca un alias que le ayude a identificar el plan, como **`my-escalation-plan`**.
5. En Duración de la etapa, introduzca el número de minutos que debe esperar Incident Manager hasta pasar a la siguiente etapa.
6. Para el canal Escalation, elige uno o más contactos o horarios de guardia con los que interactuar durante esta etapa.
7. (Opcional) Para permitir que un contacto detenga el plan de escalada una vez que reconozca la participación, seleccione El reconocimiento detiene la progresión del plan.
8. Para añadir otro canal a esta etapa, elija Añadir canal de escalada.
9. Para añadir otra etapa al plan de escalada, elija Añadir etapa.
10. Repita los pasos 5 a 9 hasta que termine de añadir los canales de escalada y las etapas que desee para este plan de escalada.
11. (Opcional) En el área Etiquetas, aplique uno o más pares de nombre clave y valor de etiqueta al plan de escalada.

    Las etiquetas son metadatos opcionales que usted asigna a un recurso. Las etiquetas permiten clasificar los recursos de diversas maneras, por ejemplo, según la finalidad, el propietario o el entorno. Por ejemplo, puede etiquetar un plan de escalada para identificar el tipo de incidente para el cual se utilizará, los tipos de canales de escalada que contiene o el plan de escalada que admite. Para obtener más información sobre el etiquetado de recursos de Incident Manager, consulte Etiquetado de recursos en Administración de incidentes.
12. Elija Crear plan de escalada.

Creación e integración de canales de chat para el personal de respuesta en Incident Manager

El administrador de incidentes, una herramienta incluida AWS Systems Manager, permite a los socorristas comunicarse directamente a través de los canales de chat durante un incidente. Un canal de chat es una sala de chat que se configura en Amazon Q Developer en aplicaciones de chat. A continuación, conecta este canal a un plan de respuesta en Incident Manager.

Durante un incidente, los respondedores utilizan el canal de chat para comunicar entre sí sobre el incidente. Incident Manager también envía las actualizaciones y notificaciones sobre el incidente directamente al canal de chat. Envía estas notificaciones utilizando uno o varios temas de Amazon Simple Notification Service (Amazon SNS) que especifique en la configuración del canal de chat.

Amazon Q Developer en aplicaciones de chat e Incident Manager admiten los canales de chat en las siguientes aplicaciones:

- Slack
- Microsoft Teams
- Amazon Chime

El proceso de configuración de un canal de chat para utilizarlo en sus incidentes consta de tareas en tres servicios diferentes de Amazon Web Services.

Tareas

- Tarea 1: Crear o actualizar temas de Amazon SNS para su canal de chat
- Tarea 2: Crear un canal de chat en Amazon Q Developer en aplicaciones de chat
- Tarea 3: Añadir el canal de chat a un plan de respuesta en Incident Manager
- Interacción a través del canal de chat

Tarea 1: Crear o actualizar temas de Amazon SNS para su canal de chat

Amazon SNS es un servicio administrado que brinda la entrega de mensajes de los publicadores a los suscriptores (también conocidos como productores y consumidores). Los publicadores se comunican de forma asíncrona con los suscriptores mediante el envío mensajes a un tema, que es un punto de acceso lógico y un canal de comunicación. Incident Manager utiliza uno o varios

temas que usted asocia a un plan de respuesta para enviar notificaciones sobre un incidente a los respondedores del mismo.

En un plan de respuesta, puede incluir uno o varios temas de Amazon SNS en las notificaciones de incidentes. Como práctica recomendada, debe crear un tema de SNS en cada uno de los temas Región de AWS que haya agregado a su conjunto de replicación.

> **Tip**
>
> Para un flujo de trabajo de configuración más directo, le recomendamos que configure primero sus temas de Amazon SNS para utilizarlos con Incident Manager. Una vez configurados, puede crear el canal de chat.

Para crear o actualizar temas de Amazon SNS para su canal de chat

1. Siga los pasos indicados en Creación de un tema de Amazon SNS en la Guía para desarrolladores de Amazon Simple Notification Service.

   > **Note**
   >
   > Después de crear el tema, edítelo para actualizar su política de acceso.

2. Seleccione el tema que ha creado y anote o copie el nombre de recurso de Amazon (ARN) del tema, en un formato como `arn:aws:sns:us-east-2:111122223333:My_SNS_topic`.
3. Elija Editar y, a continuación, expanda la sección Política de acceso para configurar permisos de acceso adicionales más allá de los predeterminados.
4. Añada la siguiente declaración a la matriz Declaración de la política:

```
{
    "Sid": "IncidentManagerSNSPublishingPermissions",
    "Effect": "Allow",
    "Principal": {
        "Service": "ssm-incidents.amazonaws.com"
    },
    "Action": "SNS:Publish",
    "Resource": "sns-topic-arn",
    "Condition": {
        "StringEqualsIfExists": {
```

```
            "AWS:SourceAccount": "account-id"
        }
    }
}
```

Sustituya el *placeholder values* siguiente:

- *sns-topic-arn*es el nombre del recurso de Amazon (ARN) del tema que ha creado para esta región, en el formato. `arn:aws:sns:us-east-2:111122223333:My_SNS_topic`
- *account-id*es el ID del área en la Cuenta de AWS que está trabajando, por ejemplo`111122223333`.

5. Seleccione Save changes (Guardar cambios).
6. Repita el proceso en cada región incluida en su conjunto de réplica.

Tarea 2: Crear un canal de chat en Amazon Q Developer en aplicaciones de chat

Puedes crear un canal de chat en SlackMicrosoft Teams, o Amazon Chime. Solo necesita un canal de chat para cada plan de respuesta.

Para sus canales de chat, le recomendamos seguir la entidad principal de privilegio mínimo (no proporcionar a los usuarios más permisos de los necesarios para completar sus tareas). También deberías revisar periódicamente la membresía de tu desarrollador de Amazon Q en los canales de chat de las aplicaciones de chat. Las revisiones ayudan a comprobar que solo los respondedores apropiados y otras partes interesadas tengan acceso a sus canales de chat.

En Slack los canales y Microsoft Teams canales creados en Amazon Q Developer en aplicaciones de chat, el personal de respuesta a incidentes puede ejecutar varios comandos CLI de Incident Manager directamente desde la Microsoft Teams aplicación Slack o. Para obtener más información, consulte Interacción a través del canal de chat.

> **Important**
>
> Los usuarios que añada a su canal de chat deben ser los mismos contactos que figuran en su plan de escalada o de respuesta. También puede añadir usuarios adicionales a los canales de chat, como partes interesadas y observadores de incidentes.

Para obtener información general sobre Amazon Q Developer en aplicaciones de chat, consulte Qué es Amazon Q Developer en aplicaciones de chat en la Guía del administrador de Amazon Q Developer en aplicaciones de chat.

Elija entre las siguientes aplicaciones en las que crear su canal:

Slack

Los pasos indicados en este procedimiento proporcionan la configuración de permisos recomendada para permitir que todos los usuarios del canal utilicen los comandos de chat con Incident Manager. Gracias a los comandos de chat compatibles, el personal de respuesta a los incidentes puede actualizar el incidente e interactuar con él directamente desde el canal de Slack chat. Para obtener información, consulte Interacción a través del canal de chat.

Para crear un canal de chat en Slack

- Siga los pasos del tutorial: Comience con Slack la Guía del administrador de aplicaciones de chat para desarrolladores de Amazon Q e incluya lo siguiente en su configuración.
  - En el paso 10, en Configuración de roles, elija Rol del canal.
  - En el paso 10d, en Plantillas de políticas, seleccione Permisos de Incident Manager.
  - En el paso 11, en Políticas de barreras de protección del canal, en Nombre de la política, elija `AWSIncidentManagerResolverAccess`.
  - En el paso 12, en la sección Temas de SNS, haga lo siguiente:
    - Para la región 1, seleccione una Región de AWS que esté incluida en su conjunto de replicación.
    - En Temas 1, seleccione el tema de SNS que creó en esa región para utilizarlo para enviar notificaciones de incidentes al canal de chat.
    - Para cada región adicional en su conjunto de réplica, seleccione Añadir otra región y añada las regiones y los temas de SNS adicionales.

Microsoft Teams

Los pasos indicados en este procedimiento proporcionan la configuración de permisos recomendada para permitir que todos los usuarios del canal utilicen los comandos de chat con Incident Manager. Mediante los comandos de chat compatibles, los equipos de respuesta a incidentes pueden actualizar el incidente e interactuar con él directamente desde el canal de Microsoft Teams chat. Para obtener información, consulte Interacción a través del canal de chat.

Para crear un canal de chat en Microsoft Teams

- Siga los pasos del tutorial: Comience con Microsoft Teams la Guía del administrador de aplicaciones de chat para desarrolladores de Amazon Q e incluya lo siguiente en su configuración:
  - En el paso 10, en Configuración de roles, elija Rol del canal.
  - En el paso 10d, en Plantillas de políticas, seleccione Permisos de Incident Manager.
  - En el paso 11, en Políticas de barreras de protección del canal, en Nombre de la política, elija `AWSIncidentManagerResolverAccess`.
  - En el paso 12, en la sección Temas de SNS, haga lo siguiente:
    - Para la región 1, seleccione una Región de AWS que esté incluida en su conjunto de replicación.
    - En Temas 1, seleccione el tema de SNS que creó en esa región para utilizarlo para enviar notificaciones de incidentes al canal de chat.
    - Para cada región adicional en su conjunto de réplica, seleccione Añadir otra región y añada las regiones y los temas de SNS adicionales.

Amazon Chime

Para crear un canal de chat en Amazon Chime

- Siga los pasos del tutorial: Comience a utilizar Amazon Chime en la Guía del administrador de aplicaciones de chat para desarrolladores de Amazon Q e incluya lo siguiente en su configuración:
  - En el paso 11, en Plantillas de políticas, seleccione Permisos de Incident Manager.
  - En el paso 12, en la sección Temas de SNS, seleccione los temas de SNS que enviarán notificaciones al webhook de Amazon Chime:
    - Para la región 1, seleccione una Región de AWS que esté incluida en su conjunto de réplicas.
    - En Temas 1, seleccione el tema de SNS que creó en esa región para utilizarlo para enviar notificaciones de incidentes al canal de chat.
    - Para cada región adicional en su conjunto de réplica, seleccione Añadir otra región y añada las regiones y los temas de SNS adicionales.

> **Note**
>
> Amazon Chime no admite los comandos de chat, que el personal de respuesta a incidentes puede usar en los canales de Microsoft Teams chat Slack y los canales de chat.

Tarea 3: Añadir el canal de chat a un plan de respuesta en Incident Manager

Al crear o actualizar un plan de respuesta, puede añadir canales de chat para que los respondedores comuniquen y reciban actualizaciones a través de ellos.

Al seguir los pasos de Creación de un plan de respuesta, en la sección (Opcional) Especificación de un canal de chat de respuesta a incidentes, seleccione el canal que desee utilizar para los incidentes relacionados con este plan de respuesta.

Interacción a través del canal de chat

En el caso de los canales Slack internos yMicrosoft Teams, Incident Manager permite al personal de respuesta interactuar con los incidentes directamente desde el canal de chat mediante los siguientes comandos: `ssm-incidents`

- start-incident
- list-response-plan
- get-response-plan
- create-timeline-event
- delete-timeline-event
- get-incident-record
- get-timeline-event
- list-incident-records
- list-timeline-events
- list-related-items
- update-related-items
- update-incident-record

- update-timeline-event

Para ejecutar comandos en el canal de chat de un incidente activo, utilice el siguiente formato. *cli-options*Sustitúyalo por cualquier opción que desee incluir en un comando.

```
@aws ssm-incidents cli-options
```

Por ejemplo:

```
@aws ssm-incidents start-incident --response-plan-arn arn:aws:ssm-
incidents::111122223333:response-plan/test-response-plan-chat --region us-east-2
```

```
@aws ssm-incidents create-timeline-event --event-data "\"example timeline event"\" --
event-time 2023-03-31 T20:30:00.000  --event-type Custom Event --incident-record-arn
 arn:aws:ssm-incidents::111122223333:incident-record/MyResponsePlanChat/98c397e6-7c10-
aa10-9b86-f199aEXAMPLE
```

```
@aws ssm-incidents list-incident-records
```

Integración de los manuales de automatización de Systems Manager en Incident Manager para la solución de incidentes

Puede usar los manuales de AWS Systems Manager automatización, una herramienta incluida AWS Systems Manager, para automatizar las tareas comunes de aplicaciones e infraestructura en su entorno. Nube de AWS

Cada runbook define un flujo de trabajo runbook, que se compone de las acciones que Systems Manager realiza en los nodos gestionados u otros tipos de AWS recursos. Puede utilizar los manuales de procedimientos para automatizar el mantenimiento, la implementación y la corrección de sus recursos de AWS .

En Incident Manager, un manual de procedimientos dirige la respuesta y mitigación de incidentes, y usted especifica un manual de procedimientos para utilizarlo como parte de un plan de respuesta.

En sus planes de respuesta, puede elegir entre docenas de manuales de procedimientos preconfigurados para tareas automatizadas habituales, o puede crear manuales de procedimientos

personalizados. Al especificar un manual de procedimientos en la definición de un plan de respuesta, el sistema puede iniciarlo automáticamente al producirse un incidente.

> **Important**
>
> Los incidentes creados por una conmutación por error entre regiones no invocan los manuales de procedimientos especificados en los planes de respuesta.

Para obtener más información sobre Systems Manager Automation, los manuales de procedimientos y el uso de los mismos con Incident Manager, consulte los siguientes temas:

- Para añadir un manual de procedimientos a un plan de respuesta, consulte Creación y configuración de planes de respuesta en Incident Manager.
- Para obtener más información sobre los manuales de procedimientos, consulte Automatización de AWS Systems Manager en la Guía del usuario de AWS Systems Manager y la Referencia del manual de procedimientos de automatización de AWS Systems Manager.
- Para obtener información sobre el costo de uso de los manuales de procedimientos, consulte Precios de Systems Manager.
- Para obtener información sobre cómo invocar automáticamente los manuales de ejecución cuando una CloudWatch alarma o un EventBridge evento de Amazon crean un incidente, consulte el Tutorial: Uso de los manuales de ejecución de Systems Manager Automation con Incident Manager.

Temas

- Permisos de IAM necesarios para iniciar y ejecutar flujos de trabajo de manuales de procedimientos
- Uso de los parámetros del manual de procedimientos
- Definición de un manual de procedimientos
- Plantilla de manual de procedimientos de Incident Manager

Permisos de IAM necesarios para iniciar y ejecutar flujos de trabajo de manuales de procedimientos

Incident Manager requiere permisos para ejecutar manuales de procedimientos como parte de su respuesta a incidentes. Para proporcionar estos permisos, utiliza las funciones AWS Identity and Access Management (IAM), la función de servicio Runbook y la función de automatización. *AssumeRole*

El rol de servicio del manual de procedimientos es un rol de servicio obligatorio. Este rol proporciona a Incident Manager los permisos que necesita para acceder e iniciar el flujo de trabajo del manual de procedimientos.

El AssumeRole de automatización proporciona los permisos necesarios para ejecutar los comandos individuales especificados dentro del manual de procedimientos.

> **Note**
>
> Si no se especifica ningún AssumeRole, Systems Manager Automation intenta utilizar el rol de servicio del manual de procedimientos para los comandos individuales. Si no especifica un AssumeRole, debe añadir los permisos necesarios al rol de servicio del manual de procedimientos. Si no lo hace, el manual de procedimientos no podrá ejecutar esos comandos.
> Sin embargo, como práctica recomendada en materia de seguridad, recomendamos utilizar un AssumeRole separado. Con un AssumeRole separado, puede limitar los permisos necesarios que debe añadir a cada rol.

Para obtener más información sobre el AssumeRole de automatización, consulte Configuración de un rol de servicio (asumir rol) de acceso para automatizaciones en la Guía del usuario de AWS Systems Manager .

Puede crear usted mismo de forma manual cualquiera de los dos tipos de rol en la consola de IAM. También puede dejar que Incident Manager cree cualquiera de los dos por usted al crear o actualizar un plan de respuesta.

Permisos del rol de servicio del manual de procedimientos

Los permisos del rol de servicio dle manual de procedimientos se proporcionan a través de una política similar a la siguiente.

La primera declaración permite a Incident Manager iniciar la operación `StartAutomationExecution` de Systems Manager. A continuación, esta operación se ejecuta en los recursos representados por los tres formatos de nombre de recurso de Amazon (ARN).

La segunda declaración permite que el rol de servicio del manual de procedimientos asuma un rol en otra cuenta cuando ese manual de procedimientos se ejecuta en la cuenta afectada. Para obtener más información, consulte Ejecutar automatizaciones en varias cuentas Regiones de AWS y en la Guía del AWS Systems Manager usuario.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "ssm:StartAutomationExecution",
            "Resource": [
                "arn:aws:ssm:*:111122223333:document/{{DocumentName}}",
                "arn:aws:ssm:*:111122223333:automation-execution/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": "sts:AssumeRole",
            "Resource": "arn:aws:iam::*:role/AWS-SystemsManager-
AutomationExecutionRole",
            "Condition": {
                "StringEquals": {
                    "aws:CalledViaLast": "ssm.amazonaws.com"
                }
            }
        }
    ]
}
```

Permisos de automatización AssumeRole

Al crear o actualizar un plan de respuesta, puede elegir entre varias políticas AWS gestionadas para adjuntarlas a las AssumeRole que cree Incident Manager. Estas políticas proporcionan permisos

para ejecutar una serie de operaciones comunes utilizadas en los escenarios del manual de procedimientos de Incident Manager. Puede elegir una o más de estas políticas administradas para proporcionar permisos a su política `AssumeRole`. En la siguiente tabla se describen las políticas entre las que puede elegir al crear un `AssumeRole` desde la consola de Incident Manager.

Nombre de la política administrada de AWS	Descripción de la política
`AmazonSSMAutomationRole`	Concede permisos para que el servicio de Systems Manager Automation ejecute las actividades definidas en los manuales de procedimientos. Asigne esta política a los administradores y a los usuarios de confianza avanzados.
`AWSIncidentManagerResolverAccess`	Concede permiso a los usuarios para iniciar, ver y actualizar incidentes. También puede utilizarlas para crear eventos de línea temporal de clientes y elementos relacionados en el panel de control de incidentes.

Puede utilizar estas políticas administradas para conceder permisos para muchos escenarios comunes de respuesta a incidentes. Sin embargo, los permisos requeridos para las tareas específicas que necesite pueden variar. En estos casos, debe proporcionar permisos de políticas adicionales para su `AssumeRole`. Para obtener información, consulte la Referencia del manual de procedimientos de automatización de AWS Systems Manager.

Uso de los parámetros del manual de procedimientos

Cuando se añade un manual de procedimiento a un plan de respuesta, se pueden especificar los parámetros que el manual debe utilizar en tiempo de puesta en marcha. Los planes de respuesta admiten parámetros con valores tanto estáticos como dinámicos. Para los valores estáticos, se introduce el valor cuando se define el parámetro en el plan de respuesta. En el caso de los valores dinámicos, el sistema determina el valor correcto del parámetro recopilando información del incidente. Incident Manager es compatible con los siguientes parámetros dinámicos:

`Incident ARN`

Cuando Incident Manager crea un incidente, el sistema captura el nombre de recurso de Amazon (ARN) del registro de incidentes correspondiente y lo ingresa para este parámetro en el manual de procedimiento.

> **Note**
>
> Este valor solo puede asignarse a parámetros de tipo `String`. Si se asigna a un parámetro de cualquier otro tipo, el manual de procedimientos no se pone en marcha.

`Involved resources`

Cuando Incident Manager crea un incidente, el sistema captura ARNs los recursos involucrados en el incidente. A continuación, estos recursos ARNs se asignan a este parámetro en el manual de ejecución.

Acerca de los recursos asociados

El administrador de incidentes puede rellenar los valores de los parámetros ARNs del manual con los AWS recursos especificados en CloudWatch las alarmas, los EventBridge eventos y los incidentes creados manualmente. En esta sección se describen los distintos tipos de recursos que Incident Manager puede capturar ARNs al rellenar este parámetro.

CloudWatch alarmas

Cuando se crea un incidente a partir de una acción de CloudWatch alarma, Incident Manager extrae automáticamente los siguientes tipos de recursos de las métricas asociadas. A continuación, rellena los parámetros elegidos con los siguientes recursos implicados:

AWS servicio	Tipo de recurso
Amazon DynamoDB	Índices secundarios globales Transmisión Tablas
Amazon EC2	Imágenes

AWS servicio	Tipo de recurso
	instancias
AWS Lambda	Aliases de rol Versiones de funciones Funciones
Amazon Relational Database Service (Amazon RDS)	Clústeres Instancias de base de datos
Amazon Simple Storage Service (Amazon S3)	Buckets

EventBridge reglas

Cuando el sistema crea un incidente a partir de un EventBridge evento, Incident Manager rellena los parámetros elegidos con la `Resources` propiedad del evento. Para obtener más información, consulta EventBridgelos eventos de Amazon en la Guía del EventBridge usuario de Amazon.

Incidentes creados manualmente

Al crear un incidente mediante la acción de la StartIncidentAPI, Incident Manager rellena los parámetros elegidos utilizando la información de la llamada a la API. En concreto, rellena los parámetros utilizando elementos de tipo `INVOLVED_RESOURCE` que se pasan en el parámetro `relatedItems`.

> **Note**
>
> El valor `INVOLVED_RESOURCES` solo puede asignarse a parámetros de tipo `StringList`. Si se asigna a un parámetro de cualquier otro tipo, el manual de procedimientos no se pone en marcha.

Definición de un manual de procedimientos

Al crear un manual de procedimientos, puede seguir los pasos que se proporcionan aquí, o seguir la guía más detallada que se proporciona en la sección Uso de los manuales de procedimientos

de la Guía del usuario de Systems Manager. Si va a crear un manual de varias cuentas y regiones, consulte Ejecución de automatizaciones en varias cuentas Regiones de AWS y en la Guía del usuario de Systems Manager.

Definición de un manual de procedimientos

1. Abra la consola de Systems Manager en https://console.aws.amazon.com/systems-manager/.
2. En el panel de navegación, elija Documentos.
3. Elija Create automation (Crear automatización).
4. Introduzca un nombre de manual de procedimientos único e identificable.
5. Introduzca una descripción del manual de procedimientos.
6. Proporcione un rol de IAM para que el documento de automatización lo asuma. Esto permite al manual de procedimientos ejecutar comandos automáticamente. Para obtener más información, consulte Configuración de un acceso de rol de servicio para flujos de trabajo de automatización.
7. (Opcional) Añada cualquier parámetro de entrada con el que se inicie el manual de procedimientos. Puede utilizar parámetros dinámicos o estáticos al iniciar un manual de procedimientos. Los parámetros dinámicos utilizan valores del incidente en el que se inicia el manual de procedimientos. Los parámetros estáticos utilizan el valor que usted proporciona.
8. (Opcional) Añada un tipo de Objetivo.
9. (Opcional) Añada etiquetas.
10. Complete los pasos que el manual de procedimientos seguirá al ejecutarse. Cada paso requiere:
    - Un nombre.
    - Una descripción del propósito del paso.
    - La acción que se va a ejecutar durante el paso. Los manuales de procedimientos utilizan el tipo de acción Pausa para describir un paso manual.
    - (Opcional) Propiedades del comando.
11. Después de añadir todos los pasos necesarios del manual de procedimientos, elija Crear automatización.

Para habilitar la funcionalidad entre cuentas, comparta el manual de procedimientos de su cuenta de administración con todas las cuentas de la aplicación que utilicen el manual de procedimientos durante un incidente.

Uso compartido de un manual de procedimientos

1. Abra la consola de Systems Manager en https://console.aws.amazon.com/systems-manager/.
2. En el panel de navegación, elija Documentos.
3. En la lista de documentos, elija el documento que desee compartir y, a continuación, elija Ver detalles. En la pestaña Permisos, verifique que es usted el propietario del documento. Solo el propietario del documento puede compartirlo.
4. Elija Edit (Edición de).
5. Para compartir el comando públicamente, seleccione Public y, a continuación, Guardar. Para compartir el comando de forma privada, elija Privado, introduzca el Cuenta de AWS ID, elija Añadir permiso y, a continuación, seleccione Guardar.

Plantilla de manual de procedimientos de Incident Manager

Incident Manager proporciona la siguiente plantilla de manual de procedimientos para ayudar a su equipo a empezar a crear manuales de procedimientos en Systems Manager Automation. Puede utilizar esta plantilla tal cual o editarla para incluir detalles específicos de su aplicación y sus recursos.

Localización de la plantilla de manual de procedimientos de Incident Manager

1. Abra la consola de Systems Manager en https://console.aws.amazon.com/systems-manager/.
2. En el panel de navegación, elija Documentos.
3. En el área Documentos, introduzca **`AWSIncidents-`** en el campo de búsqueda para mostrar todos los manuales de procedimientos de Incident Manager.

> **Tip**
>
> Introduzca **`AWSIncidents-`** como texto libre en lugar de utilizar la opción de filtro Prefijo de nombre de documento.

Uso de una plantilla

1. Abra la consola de Systems Manager en https://console.aws.amazon.com/systems-manager/.
2. En el panel de navegación, elija Documentos.

3. Elija la plantilla que desee actualizar en la lista de documentos.
4. Elija la pestaña Contenido y, a continuación, copie el contenido del documento.
5. En el panel de navegación, elija Documentos.
6. Elija Create automation (Crear automatización).
7. Introduzca un nombre único e identificable.
8. Elija la pestaña Editor.
9. Elija Editar.
10. Pegue o introduzca los datos copiados en el área Editor de documentos.
11. Elija Create automation (Crear automatización).

`AWSIncidents-CriticalIncidentRunbookTemplate`

`AWSIncidents-CriticalIncidentRunbookTemplate` es una plantilla que proporciona el ciclo de vida de Incident Manager en pasos manuales. Estos pasos son suficientemente genéricos como para utilizarlos en la mayoría de las aplicaciones, pero también suficientemente detallados como para que los respondedores puedan iniciarse en la resolución de incidentes.

Creación y configuración de planes de respuesta en Incident Manager

Los planes de respuesta le permiten planificar cómo responder a un incidente que afecte a sus usuarios. Un plan de respuesta funciona como una plantilla que incluye información sobre a quién involucrar, la gravedad prevista del suceso, los manuales de procedimientos automáticos por iniciar y las métricas por monitorear.

Prácticas recomendadas

Puede reducir el impacto de los incidentes en sus equipos al planificarlos con antelación. Los equipos deberían tener en cuenta las siguientes prácticas recomendadas al diseñar un plan de respuesta.

- Participación racionalizada: identifique el equipo más apropiado para un incidente. Si involucra una lista de distribución demasiado amplia, o si involucra a equipos equivocados, podría causar confusión y hacer perder tiempo a los respondedores durante un incidente.
- Escalada fiable: para sus compromisos en un plan de respuesta, le recomendamos que seleccione un plan de participación en vez de contactos u horarios de guardia. El plan de participación

debe especificar los contactos individuales o los horarios de guardia (que contienen múltiples contactos rotativos) que debe involucrar durante los incidentes. Dado que los respondedores especificados en su plan de participación podrían resultar inaccesibles en ocasiones, deberá configurar respondedores de reserva en su plan de respuesta para cubrir estos escenarios. Con contactos de reserva, si los contactos principal y secundario no estuvieran disponibles o hubiera otras lagunas no planificadas en la cobertura, Incident Manager seguirá notificando el incidente a un contacto.

- Manuales de procedimientos: utilice los manuales de procedimientos para proporcionar pasos repetibles y comprensibles que reduzcan el estrés que experimenta un respondedor durante un incidente.
- Colaboración: utilice los canales de chat para agilizar la comunicación durante los incidentes. Los canales de chat ayudan a los respondedores a mantenerse al día con la información. También pueden compartir información con otros respondedores a través de estos canales.

Creación de un plan de respuesta

Utilice el siguiente procedimiento para crear un plan de respuesta y automatizar la respuesta a incidentes.

Para crear un plan de respuesta

1. Abra la consola de Incident Manager y, en el panel de navegación, elija Planes de respuesta.
2. Elija Crear plan de respuesta.
3. En Nombre, introduzca un nombre del plan de respuesta único e identificable para utilizarlo en el nombre de recurso de Amazon (ARN) para el plan de respuesta.
4. (Opcional) En Nombre para mostrar, introduzca un nombre más legible para las personas que le ayude a identificar el plan de respuesta al crear incidentes.
5. Realice a continuación la Especificación de valores predeterminados para los registros de incidentes.

Especificación de valores predeterminados para incidentes

Para ayudarle a administrar los incidentes de forma más eficaz, puede especificar valores predeterminados. Incident Manager aplica estos valores a todos los incidentes que estén asociados a un plan de respuesta.

Para especificar valores predeterminados de incidentes

1. En Título, introduzca un título para este incidente que le ayude a identificarlo en la página de inicio de Incident Manager.
2. En Impacto, elija un nivel de impacto para indicar el alcance potencial de un incidente creado a partir de este plan de respuesta, como Crítico o Bajo. Para obtener información sobre los niveles de impacto en Incident Manager, consulte Triaje.
3. (Opcional) En Resumen, introduzca un breve resumen del tipo de incidente creado a partir de este plan de respuesta.
4. (Opcional) En Cadena de deduplicación, introduzca una cadena de deduplicación. Incident Manager utiliza esta cadena para evitar que la misma causa raíz cree varios incidentes en la misma cuenta.

   Una cadena de deduplicación es un término o frase que el sistema utiliza para buscar incidentes duplicados. Si especifica una cadena de deduplicación, Incident Manager busca incidentes abiertos que contengan la misma cadena en el campo `dedupeString` al crear el incidente. Si se detecta un duplicado, Incident Manager deduplica el incidente más reciente en el incidente existente.

   > **Note**
   >
   > De forma predeterminada, Incident Manager deduplica automáticamente varios incidentes creados por la misma CloudWatch alarma o evento de Amazon EventBridge . No es necesario que introduzca su propia cadena de deduplicación para evitar la duplicación para estos tipos de recursos.

5. (Opcional) En Etiquetas de incidentes, añada claves y valores de etiqueta para asignar a los incidentes creados por este plan de respuesta.

   Debe tener el permiso `TagResource` para el recurso de registro de incidentes a fin de establecer etiquetas de incidentes dentro del plan de respuesta.
6. Realice a continuación la Especificación de un canal de chat opcional para que los respondedores comuniquen entre sí acerca de los incidentes.

(Opcional) Especificación de un canal de chat de respuesta a incidentes

Al incluir un canal de chat en un plan de respuesta, los respondedores reciben las actualizaciones del incidente a través del canal. Pueden interactuar con el incidente directamente desde el canal de chat utilizando comandos de chat.

Con Amazon Q Developer en las aplicaciones de chat, puede crear un canal para SlackMicrosoft Teams, para o para que Amazon Chime lo utilice en sus planes de respuesta. Para obtener información sobre cómo crear un canal de chat en Amazon Q Developer en aplicaciones de chat, consulte la Guía del administrador de Amazon Q Developer in chat Applications.

> **Important**
>
> Incident Manager debe tener permisos para publicar en el tema de Amazon Simple Notification Service (Amazon SNS) de un canal de chat. Sin permisos para publicar en ese tema de SNS, no podrá añadirlo al plan de respuesta. Incident Manager publica una notificación de prueba en el tema de SNS para verificar los permisos.

Para obtener más información sobre los canales de chat, consulte Creación e integración de canales de chat para el personal de respuesta en Incident Manager.

Para especificar un canal de chat de respuesta a incidentes

1. Para el canal de chat, seleccione un canal de chat para desarrolladores de Amazon Q en aplicaciones de chat donde los socorristas puedan comunicarse durante un incidente.

   > **Tip**
   >
   > Para crear un nuevo canal de chat en Amazon Q Developer en aplicaciones de chat, elija Configurar nuevo cliente de Chatbot.

2. En Temas de SNS del canal de chat, elija temas de SNS adicionales en los que publicar durante el incidente. Añadir temas de SNS en varios Regiones de AWS aumenta la redundancia en caso de que una región esté inactiva en el momento del incidente.
3. Realice a continuación la Selección de contactos, horarios de guardia y planes de escalada que se activarán durante un incidente.

(Opcional) Selección de recursos que se activarán en una respuesta a incidentes

Es importante identificar a los respondedores más apropiados al producirse un incidente. Como práctica recomendada, le sugerimos que haga lo siguiente:

1. Añada contactos y horarios de guardia como los canales de escalada en un plan de escalada.

> **Note**
>
> Actualmente, no se admite la posibilidad de añadir un contacto compartido desde otra cuenta a un plan de respuesta.

2. Elija un plan de escalada como compromiso en un plan de respuesta.

Para obtener más información sobre contactos y planes de escalada, consulte Creación y configuración de contactos en Incident Manager y Creación de un plan de escalamiento para la participación del personal de respuesta en Incident Manager.

Para seleccionar los recursos por involucrar en la respuesta a incidentes

1. En Participaciones, elija cualquier número de planes de escalada, programas de guardia y contactos individuales.
2. Como opción, realice a continuación la Especificación de un manual de procedimientos para ejecutar como parte de su mitigación de incidentes.

(Opcional) Especificación de un manual de procedimientos para mitigación de incidentes

Puede usar los manuales de AWS Systems Manager automatización, una herramienta incluida AWS Systems Manager, para automatizar las tareas comunes de aplicaciones e infraestructura en su Nube de AWS entorno.

Cada manual de procedimientos define un flujo de trabajo del manual de procedimientos. Un flujo de trabajo manual incluye las acciones que Systems Manager realiza en los nodos gestionados u otros tipos de AWS recursos. En Incident Manager, un manual de procedimientos administra la respuesta y mitigación de incidentes.

Para obtener más información sobre el uso de manuales de procedimientos en los planes de respuesta, consulte Integración de los manuales de automatización de Systems Manager en Incident Manager para la solución de incidentes.

Para especificar un manual de procedimientos para mitigación de incidentes:

1. En Manual de procedimientos, realice una de las siguientes acciones:

   - Elija Clonar manual de procedimientos de una plantilla para hacer una copia del manual de procedimientos predeterminado de Incident Manager. En Nombre, introduzca un nombre descriptivo para el nuevo manual de procedimientos.
   - Elija Seleccionar manual de procedimientos existente. Seleccione el Propietario, el Manual de procedimientos y la Versión que desee utilizar.

   > **Tip**
   >
   > Para crear un manual de procedimientos desde cero, elija Configurar nuevo manual de procedimientos.
   > Para obtener más información acerca de la creación de manuales de procedimientos, consulte Integración de los manuales de automatización de Systems Manager en Incident Manager para la solución de incidentes.

2. En el área Parámetros, introduzca los parámetros solicitados para el manual de procedimientos que haya seleccionado.

   Los parámetros disponibles son los especificados por el manual de procedimientos. Un manual de procedimientos podría requerir parámetros distintos a los de otro manual. Algunos parámetros podrían ser obligatorios y otros opcionales.

   En muchos casos, puede optar por introducir manualmente un valor estático para un parámetro, como una lista de instancias de Amazon EC2. IDs También puede permitir que Incident Manager proporcione los valores de los parámetros generados dinámicamente por un incidente.

3. (Opcional) Para AutomationAssumeRole, especifique el rol AWS Identity and Access Management (de IAM) que se va a utilizar. Este rol debe tener los permisos necesarios para ejecutar los comandos individuales especificados dentro del manual de procedimientos.

> **Note**
>
> Si no se especifica `AssumeRole`, Incident Manager intentará utilizar el rol de servicio del manual de procedimientos para ejecutar los comandos individuales especificados dentro del manual de procedimientos.

Elija una de las siguientes opciones:

- Introduzca el valor del ARN: introduzca manualmente el nombre de recurso de Amazon (ARN) de un AssumeRole, en el formato. `arn:aws:iam::`*`account-id`*`:role/`*`assume-role-name`* Por ejemplo, **`arn:aws:iam::123456789012:role/MyAssumeRole`**.
- Utilizar un rol de servicio existente: elija un rol con los permisos requeridos de una lista de roles existentes en su cuenta.
- Cree una nueva función de servicio: elija una de las políticas AWS gestionadas que desee adjuntar a la suya. AssumeRole Tras seleccionar esta opción, en Políticas administradas de AWS , elija una o más políticas en la lista.

  Puede aceptar el nombre predeterminado sugerido para el nuevo rol o introducir uno que usted elija.

  > **Note**
  >
  > Este nuevo rol de servicio del manual de procedimientos está asociado con el manual de procedimientos específico que haya seleccionado. No se puede utilizar con manuales de procedimientos diferentes. Esto se debe a que la sección de recursos de la política no admite otros manuales de procedimientos.

4. En Rol de servicio del manual de procedimientos, especifique el rol de IAM que se utilizará para proporcionar los permisos necesarios para acceder e iniciar el flujo de trabajo del manual de procedimientos en sí.

   Como mínimo, el rol debe permitir la acción `ssm:StartAutomationExecution` para su manual de procedimientos específico. Para que el manual de procedimientos funcione en todas las cuentas, el rol también debe permitir la acción `sts:AssumeRole` para el rol `AWS-SystemsManager-AutomationExecutionRole` que creó durante Gestión de incidentes en todas Cuentas de AWS las regiones en Incident Manager.

Elija una de las siguientes opciones:

- Crear nuevo rol de servicio: Incident Manager crea un rol de servicio del manual de procesimientos para usted que incluye los permisos mínimos necesarios para iniciar el flujo de trabajo del manual de procedimientos.

  En Nombre del rol, puede aceptar el nombre predeterminado sugerido o introducir uno que usted elija. Le recomendamos que utilice el nombre sugerido o que mantenga el nombre del manual de procedimientos en el nombre. Esto se debe a que la nueva AssumeRole está asociada al manual específico que ha seleccionado y es posible que no incluya los permisos necesarios para otros manuales.
- Utilizar rol de servicio existente: un rol de IAM creado previamente por usted o por Incident Manager otorga los permisos necesarios.

  En Nombre del rol, seleccione el nombre del rol existente que desee utilizar.

5. Expanda las opciones adicionales y elija una de las siguientes opciones para especificar Cuenta de AWS dónde debe ejecutarse el flujo de trabajo del manual.

   - Cuenta del propietario del plan de respuesta: inicie el flujo de trabajo del manual en la cuenta en la Cuenta de AWS que lo creó.
   - Cuenta afectada: inicie el flujo de trabajo del manual de procedimientos en la cuenta que inició o notificó el incidente.

     Elija Cuenta afectada cuando utilice Incident Manager para escenarios entre cuentas y el manual de procedimientos necesite acceder a los recursos de la cuenta afectada para corregirlos.

6. Continúe integrando opcionalmente un PagerDuty servicio en el plan de respuesta.

(Opcional) Integrar un PagerDuty servicio en el plan de respuesta

Para integrar un PagerDuty servicio en el plan de respuesta

Al integrar Incident Manager con PagerDuty, PagerDuty crea el incidente correspondiente cada vez que Incident Manager crea un incidente. El incidente PagerDuty utiliza el flujo de trabajo de

paginación y las políticas de escalamiento que usted definió allí, además de las de Incident Manager. PagerDuty adjunta los eventos de la cronología de Incident Manager como notas sobre el incidente.

1. Amplíe las integraciones de terceros y, a continuación, active la casilla Habilitar PagerDuty la integración.
2. En Seleccionar secreto, selecciona el secreto en el AWS Secrets Manager que guardas las credenciales para acceder a tu PagerDuty cuenta.

   Para obtener información sobre cómo almacenar sus PagerDuty credenciales en un secreto de Secrets Manager, consulteAlmacenar las credenciales de acceso en secreto PagerDuty AWS Secrets Manager.
3. Para el PagerDuty servicio, seleccione el servicio de su PagerDuty cuenta en el que desee crear el PagerDuty incidente.
4. Realice a continuación la Adición de etiquetas opcionales y creación del plan de respuesta.

Adición de etiquetas y creación del plan de respuesta

Para añadir etiquetas y crear el plan de respuesta

1. (Opcional) En el área Etiquetas, aplique uno o más name/value pares de claves de etiquetas al plan de respuesta.

   Las etiquetas son metadatos opcionales que usted asigna a un recurso. Con las etiquetas, puede categorizar un recurso de diferentes maneras, como por propósito, propietario o entorno. Por ejemplo, es posible que desee etiquetar un plan de respuesta para identificar el tipo de incidente que debe mitigar, los tipos de canales de escalada que contiene o el plan de escalada que se le asociará. Para obtener más información sobre el etiquetado de recursos de Incident Manager, consulte Etiquetado de recursos en Administración de incidentes.
2. Elija Crear plan de respuesta.

Identificar las posibles causas de incidentes de otros servicios como «hallazgos» en Incident Manager

En Incident Manager, un hallazgo es información sobre una AWS CodeDeploy implementación o actualización de una AWS CloudFormation pila que se produjo en torno al momento de un incidente

y que implicó uno o más recursos probablemente relacionados con el incidente. Cada resultado se puede examinar como una posible causa del incidente. La información sobre estas posibles causas se añade a la página Detalles del incidente de un incidente. Con la información sobre estas implementaciones y cambios a mano, los respondedores no necesitan buscar manualmente esta información. Esto reduce el tiempo necesario para evaluar las posibles causas, lo cual puede reducir el tiempo medio de recuperación (MTTR) de un incidente.

Actualmente, Incident Manager apoya la recopilación de resultados de dos tipos Servicios de AWS: AWS CodeDeployy AWS CloudFormation.

Los resultados son una característica opcional. Puede habilitarla en el Asistente de preparación, al incorporarse por primera vez a Incident Manager, o más tarde en la página Configuración.

Al habilitar la característica de resultados, Incident Manager crea un rol de servicio para usted. Esta función de servicio incluye los permisos necesarios para recuperar los hallazgos de CodeDeploy y CloudFormation.

Para trabajar con resultados en un escenario entre cuentas, habilite la característica en la cuenta de administración. Después de eso, cada cuenta de aplicación de una organización AWS Resource Access Manager (AWS RAM) debe crear un rol de servicio correspondiente.

Consulte los siguientes temas como ayuda para utilizar la característica Resultados.

Temas

- Habilitación y creación de un rol de servicio de resultados
- Configuración de permisos para el soporte de resultados entre cuentas

Habilitación y creación de un rol de servicio de resultados

Al habilitar la característica Resultados, Incident Manager crea un rol de servicio denominado `IncidentManagerIncidentAccessServiceRole` en su nombre. Esta función de servicio proporciona los permisos que Incident Manager necesita para recopilar información sobre las CodeDeploy implementaciones y CloudFormation apilar las actualizaciones que se produjeron en torno al momento en que se creó un incidente.

> **Note**
>
> Si utiliza Incident Manager con una organización, el rol de servicio se crea en la cuenta de administración. Para trabajar con resultados en otras cuentas de la organización, se debe

crear el rol de servicio en cada cuenta de aplicación. Para obtener información sobre el uso de una CloudFormation plantilla para crear este rol en las cuentas de la aplicación, consulte el paso 4 deInstalación y configuración de la administración de incidentes entre cuentas.

Este rol de servicio está asociado a una política AWS administrada. Para obtener información sobre los permisos de esta política, consulte AWS política gestionada: AWSIncidentManagerIncidentAccessServiceRolePolicy.

Para obtener información sobre cómo habilitar los resultados durante el proceso de incorporación a Incident Manager, consulte Introducción a Incident Manager.

Para obtener información sobre cómo habilitar los resultados una vez completado el proceso de incorporación, consulte Administración de la característica Resultados.

Configuración de permisos para el soporte de resultados entre cuentas

Para utilizar la función Findings en todas las cuentas con una organización establecida AWS RAM, cada cuenta de la aplicación debe configurar los permisos para que Incident Manager asuma la función de servicio de la cuenta de administración en su nombre.

Estos permisos se pueden configurar en una cuenta de aplicación mediante la implementación de una CloudFormation plantilla proporcionada por AWS, que crea el rol`IncidentManagerIncidentAccessServiceRole`.

Para obtener información sobre la descarga e implementación de esta plantilla en una cuenta de aplicación, consulte el paso 4 de Gestión de incidentes en todas Cuentas de AWS las regiones en Incident Manager.

Crear incidentes de forma automática o manual en Incident Manager

Incident Manager, una herramienta incluida AWS Systems Manager, le ayuda a gestionar y responder rápidamente a los incidentes. Puede configurar Amazon CloudWatch y Amazon EventBridge para que creen automáticamente incidentes en función de CloudWatch alarmas y EventBridge eventos. También puede crear incidentes manualmente en la página de la lista de incidentes o mediante la acción de la StartIncident AWS CLI API del AWS SDK. Incident Manager deduplica los incidentes creados a partir de la misma CloudWatch alarma o EventBridge evento y los convierte en el mismo incidente.

En el caso de los incidentes creados automáticamente por CloudWatch alarmas o EventBridge eventos, Incident Manager intenta crear un incidente al mismo tiempo Región de AWS que la regla o la alarma del evento. En caso de que Incident Manager no esté disponible en el conjunto de réplicas Región de AWS, CloudWatch o cree EventBridge automáticamente el incidente en una de las regiones disponibles especificadas en su conjunto de réplicas. Para obtener más información, consulte Gestión de incidentes en todas Cuentas de AWS las regiones en Incident Manager.

Cuando el sistema crea un incidente, Incident Manager recopila automáticamente información sobre los AWS recursos involucrados en el incidente y agrega esta información a la pestaña Elementos relacionados. Si ha especificado un manual de procedimientos en su plan de respuesta, cuando el sistema crea un incidente, Incident Manager puede enviar la información sobre los recursos de AWS implicados en el incidente al manual de procedimientos. El sistema puede entonces apuntar a esos recursos cuando inicie el manual de procedimientos e intente corregir el problema.

Cuando el sistema crea un incidente, también crea un elemento de trabajo operativo principal (OpsItem) en OpsCenter, un componente de Systems Manager, y lo vincula al incidente como un elemento relacionado. Puede usarlo OpsItem para realizar un seguimiento del trabajo relacionado y los análisis de futuros incidentes. Llamadas para OpsCenter incurrir en costes. Para obtener más información sobre OpsCenter los precios, consulte los precios de Systems Manager.

Important

Tenga en cuenta los siguientes detalles importantes.

- En caso de que Incident Manager no esté disponible, el sistema solo puede realizar una conmutación por error y crear incidentes en otras regiones Regiones de AWS si

ha especificado al menos dos regiones en su conjunto de replicación. Para obtener información sobre la configuración de un conjunto de réplica, consulte Introducción a Incident Manager.

- Los incidentes creados por una conmutación por error entre regiones no invocan los manuales de procedimientos especificados en los planes de respuesta.

Creación automática de incidentes mediante CloudWatch alarmas

CloudWatch utiliza sus CloudWatch métricas para avisarle sobre los cambios en su entorno y para ejecutar automáticamente la acción de iniciar el incidente. CloudWatch trabaja con Systems Manager e Incident Manager para crear un incidente a partir de una plantilla de plan de respuesta cuando una alarma pasa al estado de alarma. Esto requiere los siguientes requisitos previos:

- Incident Manager configurado y conjunto de réplica creado. Este paso crea el rol vinculado al servicio de Incident Manager en su cuenta, proporcionando los permisos necesarios.
- Plan de respuesta de Incident Manager configurado. Para obtener información sobre cómo configurar los planes de respuesta de Incident Manager, consulte Creación y configuración de planes de respuesta en Incident Manager en la sección Preparación de incidentes de esta guía.
- CloudWatch Métricas configuradas que supervisan su aplicación. Para conocer las prácticas recomendadas de monitoreo, consulte Supervisión en la sección Preparación de incidentes de esta guía.

Para crear una alarma con una acción Iniciar incidente

1. Cree una alarma en CloudWatch. Para obtener más información, consulta Uso de CloudWatch alarmas de Amazon en la Guía del CloudWatch usuario de Amazon.
2. Al elegir la acción que debe realizar la alarma, seleccione Añadir acción de Systems Manager.
3. Elija Crear incidente y seleccione el Plan de respuesta para este incidente.
4. Complete los pasos restantes de la guía del tipo de alarma seleccionada.

> **Tip**
>
> También puede añadir la acción de crear incidente a cualquier alarma existente.

Crear incidentes automáticamente con EventBridge eventos

EventBridge las reglas vigilan los patrones de eventos. Si el evento coincide con el patrón definido, Incident Manager crea un incidente utilizando el plan de respuesta elegido.

Creación de incidentes mediante eventos de socios SaaS

Puede configurarlo EventBridge para recibir eventos de aplicaciones y servicios de socios de software como servicio (SaaS), lo que permite la integración de terceros. Tras EventBridge configurarlo para recibir eventos de socios externos, puede crear reglas que coincidan con las de los socios para crear incidentes. Para ver una lista de integraciones de terceros, consulte Recepción de eventos de un socio SaaS.

Configure EventBridge para recibir eventos de una integración de SaaS.

1. Abre la EventBridge consola de Amazon en https://console.aws.amazon.com/events/.
2. En el panel de navegación, seleccione Orígenes de eventos de socios.
3. Utilice la barra de búsqueda para encontrar el socio que desee y elija Configurar para ese socio.
4. Elija Copy (Copiar) para copiar su ID de cuenta en el portapapeles.

> **Note**
>
> Para realizar la integración con Salesforce, sigue los pasos descritos en la guía del AppFlow usuario de Amazon.

5. Vaya al sitio web del socio y siga las instrucciones para crear un origen de eventos de socio. Utilice su ID de cuenta para esto. El origen de eventos que cree estará disponible solo en su cuenta.
6. Vuelva a la EventBridge consola y elija las fuentes de eventos de los socios en el panel de navegación.
7. Seleccione el botón situado junto al origen de eventos de socios y elija Associate with event bus (Asociar con bus de eventos).

Creación de una regla que se active en los eventos de un socio SaaS

1. Abre la EventBridge consola de Amazon en https://console.aws.amazon.com/events/.
2. En el panel de navegación, seleccione Reglas.

3. Elija Creación de regla.
4. Escriba un nombre y una descripción para la regla.

   Una regla no puede tener el mismo nombre que otra regla de la misma región y del mismo bus de eventos.
5. En Bus de eventos, elija el bus de eventos que corresponda a este socio.
6. En Tipo de regla, elija Regla con un patrón de evento.
7. Elija Siguiente.
8. En Fuente del evento, selecciona AWS eventos o eventos EventBridge asociados.
9. En Patrón del evento, elija Formulario de patrón de eventos.
10. Para la fuente del evento, elija EventBridgesocios
11. En Socios, elija el nombre del socio.
12. En Event type (Tipo de evento), elija All Events (Todos los eventos) o elija el tipo de evento que desea utilizar para esta regla. Si elige All Events (Todos los eventos), todos los eventos emitidos por este origen de eventos de socio coincidirán con la regla.

    Si desea personalizar el patrón del evento, elija Editar, realice los cambios y, a continuación, elija Guardar.
13. Elija Siguiente.
14. En Seleccionar un objetivo, elija Plan de respuesta de Incident Manager y, a continuación, elija un Plan de respuesta.

    > **Note**
    >
    > Al seleccionar un plan de respuesta, todos los planes de respuesta que posea y hayan sido compartidos con su cuenta aparecerán en la lista desplegable Plan de respuesta.
15. EventBridge puede crear la función de IAM necesaria para que se ejecute la regla:

    - Para crear un rol de IAM automáticamente, elija Creación de un nuevo rol para este recurso específico.
    - Para utilizar un rol de IAM que haya creado antes, elija Uso de función existente.
16. Elija Siguiente.
17. (Opcional) Introduzca una o varias etiquetas para la regla. Para obtener más información, consulta las EventBridgeetiquetas de Amazon en la Guía del EventBridge usuario de Amazon.

18. Elija Siguiente.
19. Revise su regla y, a continuación, elija Crear regla.

Creación de incidentes mediante eventos AWS de servicio

EventBridge también recibe eventos de los AWS servicios que aparecen en la sección Eventos de AWS los servicios compatibles. De forma similar a como se configuran las reglas para los socios de SaaS, puede configurarlas para AWS los servicios.

Cree una regla que se active en los eventos de un servicio AWS

1. Abre la EventBridge consola de Amazon en https://console.aws.amazon.com/events/.
2. En el panel de navegación, seleccione Reglas.
3. Elija Creación de regla.
4. Escriba un nombre y una descripción para la regla.

   Una regla no puede tener el mismo nombre que otra regla de la misma región y del mismo bus de eventos.
5. En Bus de eventos, elija Predeterminado.
6. En Tipo de regla, elija Regla con un patrón de evento.
7. Elija Siguiente.
8. En Fuente del evento, selecciona AWS eventos o eventos EventBridge asociados.
9. En Patrón del evento, elija Formulario de patrón de eventos.
10. En Origen de evento, seleccione Servicios de AWS .
11. En Nombre del servicio, elija el servicio que monitorea un incidente.
12. En Event type (Tipo de evento), elija All Events (Todos los eventos) o elija el tipo de evento que desea utilizar para esta regla. Si elige All Events (Todos los eventos), todos los eventos emitidos por este origen de eventos de socio coincidirán con la regla.

    Si desea personalizar el patrón del evento, elija Editar, realice los cambios y, a continuación, elija Guardar.
13. Elija Siguiente.
14. En Seleccionar un objetivo, elija Plan de respuesta de Incident Manager y, a continuación, elija un Plan de respuesta.

> **Note**
>
> Al seleccionar un plan de respuesta, todos los planes de respuesta que posea y hayan sido compartidos con su cuenta aparecerán en la lista desplegable Plan de respuesta.

15. EventBridge puede crear la función de IAM necesaria para que se ejecute la regla:
    - Para crear un rol de IAM automáticamente, elija Creación de un nuevo rol para este recurso específico.
    - Para utilizar un rol de IAM que haya creado antes, elija Uso de función existente.
16. Elija Siguiente.
17. (Opcional) Introduzca una o varias etiquetas para la regla. Para obtener más información, consulta las EventBridgeetiquetas de Amazon en la Guía del EventBridge usuario de Amazon.
18. Elija Siguiente.
19. Revise su regla y, a continuación, elija Crear regla.

Creación manual de incidentes

Los respondedores pueden realizar un seguimiento manual de un incidente mediante la consola de Incident Manager a través de un plan de respuesta predefinido. Efectúe los siguientes pasos para crear un incidente.

1. Abra la consola de Incident Manager.
2. Elija Iniciar incidente.
3. En Plan de respuesta, elija un plan de respuesta en la lista.
4. (Opcional) Para anular el título proporcionado por el plan de respuesta definido, introduzca un Título del incidente.
5. (Opcional) Para anular el impacto proporcionado por el plan de respuesta definido, introduzca el Impacto del incidente.

Permisos de IAM necesarios para iniciar los incidentes manualmente

Para iniciar los incidentes manualmente, los usuarios necesitan permisos para acceder a la consola de Incident Manager, ver los planes de respuesta e iniciar los incidentes. Cuando un usuario

inicia un incidente, Incident Manager utiliza sesiones de acceso directo (FAS) para realizar la `StartEngagement` llamada como parte de él`StartIncident`.

La siguiente política de IAM proporciona los permisos necesarios para iniciar los incidentes de forma manual, ver los planes de respuesta con los que se pueden crear los incidentes y ver y editar los incidentes una vez creados.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ssm-incidents:StartIncident",
                "ssm-incidents:GetResponsePlan",
                "ssm-incidents:ListResponsePlans",
                "ssm-incidents:TagResource",
                "ssm-incidents:GetIncidentRecord",
                "ssm-incidents:ListIncidentRecords",
                "ssm-incidents:UpdateIncidentRecord"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ssm-contacts:StartEngagement"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:CalledViaFirst": "ssm-incidents.amazonaws.com"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "ssm:CreateOpsItem"
            ],
```

```
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:CalledViaFirst": "ssm-incidents.amazonaws.com"
                }
            }
        }
    ]
}
```

Esta política incluye los permisos siguientes:

- ssm-incidents: StartIncident - Permite a los usuarios iniciar un incidente manualmente mediante la consola o la API. Esto crea un nuevo registro de incidentes a partir de un plan de respuesta.
- ssm-incidents: GetResponsePlan - Permite a los usuarios recuperar información sobre un plan de respuesta específico.
- ssm-incidents: ListResponsePlans - Permite a los usuarios enumerar todos los planes de respuesta de su cuenta.
- ssm-incidents: TagResource - Permite añadir etiquetas a los recursos del Incident Manager, incluidos los incidentes y los planes de respuesta.
- ssm-incidents: GetIncidentRecord - Permite a los usuarios recuperar información detallada sobre un incidente específico.
- ssm-incidents: ListIncidentRecords - Permite a los usuarios enumerar todos los incidentes de su cuenta.
- ssm-incidents: UpdateIncidentRecord - Permite a los usuarios actualizar los detalles de un incidente existente.
- ssm-contacts: StartEngagement (con condición): permite a Incident Manager iniciar interacciones con los contactos. La condición garantiza que solo se pueda llamar a través del Administrador de incidentes.
- ssm: CreateOpsItem (con condición): permite que Incident Manager cree una entrada OpsItem . OpsCenter La condición garantiza que solo se pueda llamar a ella a través del Administrador de incidentes.

La clave aws: CalledViaFirst condition garantiza que ciertos permisos (por ejemplo`StartEngagement`) solo se puedan usar cuando la solicitud llegue a través del servicio

Incident Manager. Este enfoque utiliza el FAS en lugar de funciones vinculadas al servicio, lo que evita posibles llamadas entre cuentas que podrían suponer un riesgo de seguridad.

Visualización de los detalles del incidente en la consola de Incident Manager

AWS Systems Manager Incident Manager realiza un seguimiento de sus incidentes desde el momento en que se detectan hasta su resolución y durante el análisis posterior al incidente. Puede encontrar todos los incidentes en la página Lista de incidentes de la consola de Incident Manager, con enlaces directos a los Detalles del incidente.

Temas

Visualización de la lista de incidentes en la consola

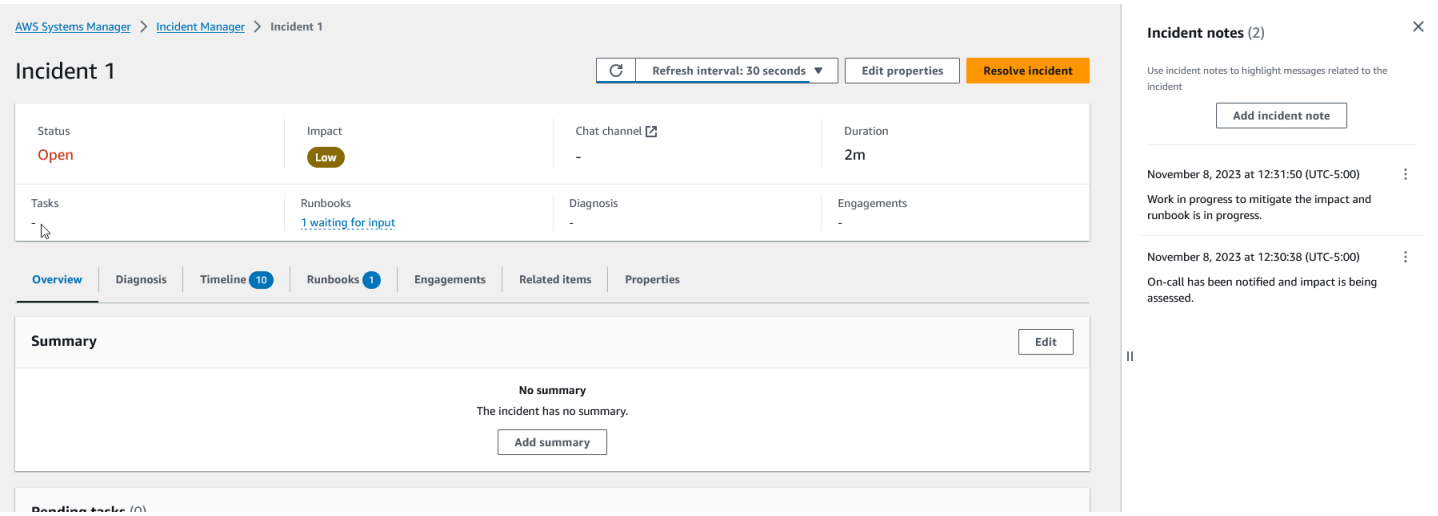
La página Lista de incidentes contiene tres secciones: Incidentes abiertos, Incidentes resueltos y Análisis. Puede hacer un seguimiento manual de los nuevos incidentes y crear análisis desde esta página. Para obtener más información sobre el seguimiento manual de un incidente, consulte Creación manual de incidentes en la sección Creación de incidentes de esta guía. Para obtener información sobre el análisis post-incidente, consulte la sección Realización de un análisis post-incidente en Incident Manager de esta guía.

Detalles del incidente muestra los Incidentes abiertos en mosaicos con el título, el impacto, la duración y el canal de chat de ese incidente. Después de resolver un incidente, este pasa a la lista Incidentes resueltos. Los Análisis se encuentran en la segunda pestaña.

Visualización de los detalles del incidente en la consola

La página Detalles del incidente proporciona información detallada y herramientas que puede utilizar para administrar un incidente. Desde esta página, puede iniciar manuales de procedimientos para mitigar un incidente, añadir notas sobre el mismo, involucrar a otros solucionadores y ver detalles del incidente como líneas temporales, métricas, propiedades y recursos relacionados.

Como se muestra en la imagen siguiente, la página de detalles del incidente incluye varias secciones: el encabezado principal, las notas del incidente y siete pestañas que contienen información y recursos adicionales. De forma predeterminada, las secciones del encabezado principal y de las notas del incidente se muestran en todas las páginas de detalles del incidente.



En este tema se explican los elementos de la página Detalles del incidente y las acciones que puede realizar desde la misma.

Banner superior

El banner superior de cada página de detalles del incidente incluye la siguiente información:

- Estado: el estado actual de un incidente, que puede ser Abierto o Resuelto.
- Impacto: el impacto del incidente en su entorno. Puede ser alto, medio y bajo. Para cambiar el impacto de un incidente, elija Editar propiedades.
- Canal de chat: un enlace para acceder al canal de chat donde puede ver las actualizaciones y notificaciones de incidentes.
- Duración: el tiempo transcurrido antes de que un respondedor resuelva el incidente.
- Manuales de procedimientos: los estados de los manuales de procedimientos asociados a este incidente. El estado puede ser esperando entrada, exitoso, o fallido. Si el estado de un manual de procedimientos es esperando entrada, puede seleccionar el manual de procedimientos para ver los detalles de la acción. Puede seleccionar fallido para ver los manuales de procedimientos que estén en estado Vencido, Fallido o Cancelado.
- Participaciones: el número total de participaciones y el estado de cada una de ellas. Al crear una participación, su estado es Participante. Una vez que reconoce la participación, el estado cambia de Participante a Reconocido. Incident Manager no admite el reconocimiento de participantes terceros. Dichos participantes permanecen en el estado Participante.

Para editar el título del incidente, el impacto y el canal de chat, elija Editar en la esquina superior derecha del banner.

Notas del incidente

La parte derecha de la pantalla muestra la sección Notas del incidente. Con las notas, puede colaborar y comunicar con otros usuarios que trabajen en un incidente. Puede explicar las mitigaciones que aplicó, una posible causa raíz que identificó o el estado actual del incidente. Como práctica recomendada, utilice la sección Notas del incidente para publicar actualizaciones de estado y acciones que usted u otras personas efectúen en un incidente. Si necesita comunicar con otros solucionadores en tiempo real, utilice el canal de chat disponible en Incident Manager.

Para añadir una nota, pulse el botón Añadir nota del incidente y, a continuación, introduzca su nota. Las notas pueden contener actualizaciones sobre el estado del incidente o cualquier otra información relevante que proporcione visibilidad a otros usuarios. De ser necesario, también puede editar o eliminar notas de incidentes.

> **Note**
>
> Cualquier usuario con permiso de IAM para ejecutar las acciones `ssm-incidents:UpdateTimelineEvent` y `ssm-incidents:DeleteTimelineEvent` puede editar y eliminar notas. Sin embargo, al compartir un incidente con otra cuenta, la política de recursos no incluye la acción `ssm-incidents:DeleteTimelineEvent`. Esto impide que el usuario con el que comparte el incidente elimine la nota. Puede ver el registro de auditoría de una nota de incidentes de Incident Manager en la consola de AWS CloudTrail .

Pestañas

La página de detalles del incidente tiene siete pestañas, lo que facilita a los respondedores la localización y visualización de la información durante un incidente. Las pestañas muestran un contador en el nombre de la pestaña, que indica el número de actualizaciones de la misma.
Para obtener más información sobre el contenido de cada pestaña, así como sobre las acciones disponibles, prosiga con la lectura.

Descripción general de

La pestaña Resumen es la página de aterrizaje para los respondedores. Contiene el resumen del incidente, una lista de eventos recientes de la línea temporal y el paso actual del manual de procedimientos.

Los respondedores utilizan el Resumen para ponerse al día sobre las acciones que se han realizado, los resultados de cualquier cambio, los posibles pasos siguientes e información sobre el impacto del incidente. Para actualizar el resumen, seleccione Editar en la esquina superior derecha de la sección Resumen.

> **Important**
>
> Si varios respondedores editasen el campo de resumen simultáneamente, el respondedor que envíe sus ediciones en último lugar sobrescribirá todas las demás entradas.

La sección Eventos recientes en la línea temporal contiene una línea temporal rellenada por Incident Manager con los cinco eventos más recientes. Utilice esta sección para conocer el estado del incidente y lo que ha ocurrido recientemente. Para ver una línea temporal completa, prosiga en la pestaña Línea temporal.

La página de resumen también muestra el Paso actual del manual de procedimientos. Este paso puede ser un paso automático que se ejecuta en su AWS entorno o puede ser un conjunto de instrucciones manuales para el personal de respuesta. Para ver el manual de procedimientos completo, incluyendo los pasos anteriores y futuros, seleccione la pestaña Manual de procedimientos.

Diagnóstico

La pestaña Diagnóstico contiene información vital sobre sus sistemas y aplicaciones alojadas en AWS , incluyendo información sobre métricas y, si están habilitados, resultados.

Uso de métricas

Incident Manager utiliza Amazon CloudWatch para rellenar las métricas y los gráficos de alarmas que se encuentran en esta pestaña. Para obtener más información sobre las prácticas recomendadas de administración de incidentes para definir alarmas y métricas, consulte Supervisión en la sección Planificación de incidentes de esta guía del usuario.

Para añadir métricas

- Seleccione Añadir en la esquina superior derecha de esta pestaña.
  - Para añadir una métrica de un panel de CloudWatch control existente, seleccione Desde un panel de CloudWatch control existente.

    a. Elija un Panel de control. Esto añade todas las métricas y alarmas que forman parte del panel de control elegido.

    b. (Opcional) También puede Seleccionar métricas desde el panel de control para ver métricas específicas.
  - Agregue una única métrica seleccionando Desde CloudWatch y pegando una fuente de métrica. Para copiar un origen de métrica

    a. Abra la CloudWatch consola en. https://console.aws.amazon.com/cloudwatch/

    b. En el panel de navegación, seleccione Métricas.

    c. En la pestaña Todas las métricas, introduzca un término de búsqueda en el campo de búsqueda, como el nombre de una métrica o el nombre de un recurso, y elija Intro.

    Por ejemplo, si busca la métrica `CPUUtilization`, verá los espacios de nombres y dimensiones asociados a esta métrica.

    d. Elija uno de los resultados de su búsqueda para ver las métricas.

    e. Elija la pestaña Origen y copie el origen.

Los gráficos de alarmas métricas solo se pueden añadir a los detalles del incidente mediante el plan de respuesta correspondiente o seleccionando Desde el CloudWatch panel de control existente al añadir una métrica.

Para eliminar métricas, seleccione Eliminar y, a continuación, elija las métricas que desee eliminar en el cuadro desplegable Métricas proporcionado.

Visualización de los resultados obtenidos de AWS CodeDeploy y CloudFormation

Una vez habilitados los resultados y configurados todos los permisos necesarios, los resultados que puedan estar relacionados con un incidente en concreto se vincularán al mismo. Los respondedores pueden ver información sobre estos resultados en la página Detalles del incidente.

Para ver los hallazgos de CodeDeploy y CloudFormation

1. Abra la consola de Incident Manager.
2. Elija el nombre de un incidente que desee investigar.
3. En la pestaña Diagnóstico, en el área Resultados, compare las horas de inicio de cualquier resultado notificado con la hora de inicio del incidente.
4. Para ver más detalles sobre un hallazgo, en la columna Referencia, elija el enlace al CloudFormation hallazgo CodeDeploy o.

Plazo

Utilice la pestaña Línea temporal para realizar un seguimiento de los eventos que se producen durante un incidente. Incident Manager rellena automáticamente los eventos de la línea temporal que identifican sucesos significativos durante el incidente. Los respondedores pueden añadir eventos personalizados basados en sucesos detectados manualmente. Durante el análisis post-incidente, la pestaña de línea temporal proporciona información valiosa sobre cómo prepararse y responder mejor a los incidentes en el futuro. Para obtener más información sobre el análisis post-incidente, consulte Realización de un análisis post-incidente en Incident Manager.

Para añadir un evento de línea temporal personalizado, seleccione Añadir. Seleccione una fecha utilizando el calendario y, a continuación, introduzca una hora. Todas las horas se muestran en su zona horaria local. Proporcione una breve descripción del evento que aparece en la línea temporal.

Para editar un evento personalizado existente, seleccione el evento en la línea temporal y elija Editar. Puede cambiar la hora, fecha y descripción de los eventos personalizados. Solo puede editar eventos personalizados.

Manuales de procedimientos

La pestaña Manuales de procedimientos de la página de detalles del incidente es donde los respondedores pueden ver los pasos del manual de procedimientos e iniciar nuevos manuales.

Para iniciar un nuevo manual de procedimientos, seleccione Iniciar manual de procedimientos en la sección Manuales de procedimientos. Utilice el campo de búsqueda para encontrar el manual de procedimientos que desea iniciar. Proporcione los Parámetros necesarios y la Versión del manual de procedimientos que desea utilizar al iniciar el manual. Los manuales de procedimientos iniciados durante un incidente desde la pestaña Manuales de procedimientos utilizan los permisos de la cuenta actualmente en sesión iniciada.

Para acceder a la definición de un manual de procedimientos en Systems Manager, seleccione el título del mismo en Manuales de procedimientos. Para navegar hasta la instancia en ejecución del manual de procedimientos en Systems Manager, elija los detalles de la ejecución en Detalles de la ejecución. Estas páginas muestran la plantilla utilizada para iniciar el manual de procedimientos y los detalles específicos de la instancia en ejecución del documento de automatización.

La sección Pasos del manual de procedimientos muestra la lista de pasos que el manual de procedimientos seleccionado realiza automáticamente o que los respondedores realizan manualmente. Los pasos se expanden a medida que se convierten en el paso actual, mostrando la información necesaria para completar el paso o detalles sobre lo que hace el paso. Los pasos automáticos del manual de procedimientos se resuelven una vez completada la automatización. Los pasos manuales requieren que los respondedores elijan Paso siguiente en la parte inferior de cada paso. Una vez completado un paso, la salida del paso aparece como un cuadro desplegable.

Para cancelar la ejecución de un manual de procedimientos, elija Cancelar manual de procedimientos. Esto detiene la ejecución del manual de procedimientos y no se completa ningún paso más en el mismo.

Participaciones

La pestaña Participaciones en detalles del incidente controla la participación de los respondedores y los equipos. Desde esta pestaña puede ver a quién se ha contactado, quién ha respondido, así como qué respondedores se van a involucrar como parte de un plan de escalada. Los respondedores pueden comprometer a otros contactos directamente desde esta pestaña. Para obtener más información sobre creación de contactos y planes de escalada, consulte las secciones Creación y configuración de contactos en Incident Manager y Creación de un plan de escalamiento para la participación del personal de respuesta en Incident Manager de esta guía.

Puede configurar planes de respuesta con contactos y planes de escalada para iniciar automáticamente la participación al principio de un incidente. Para obtener más información sobre la configuración de planes de respuesta, consulte la sección Creación y configuración de planes de respuesta en Incident Manager de esta guía.

Puede encontrar información sobre cada contacto en la tabla. Esta tabla incluye la siguiente información:

- Nombre: enlaces a la página de detalles del contacto que muestra sus métodos de contacto y su plan de participación.
- Plan de escalada: enlaces al plan de escalada que involucró al contacto.

- Origen del contacto: identifica el servicio que contrató a este contacto, como AWS Systems Manager o PagerDuty.
- Participante: muestra cuándo el plan involucró a un contacto, o cuándo involucrar a un contacto como parte de un plan de escalada.
- Reconocido: muestra si el contacto ha reconocido la participación.

Para confirmar una participación, el respondedor puede realizar una de las siguientes acciones:

- Llamada telefónica: Introduzca **1** cuando se le solicite.
- SMS: responda al mensaje con el código proporcionado o introdúzcalo en la pestaña Participaciones del incidente.
- Correo electrónico: introduzca el código proporcionado en la pestaña Participaciones del incidente.

Elementos relacionados

La pestaña Elementos relacionados se utiliza para recopilar recursos relacionados con la mitigación de incidentes. Estos recursos pueden ser ARNs enlaces a recursos externos o archivos subidos a buckets de Amazon S3. La tabla muestra un título descriptivo y un ARN, un enlace o detalles del bucket. Antes de utilizar los buckets de S3, consulte Prácticas recomendadas de seguridad de Amazon S3 en la Guía del usuario de Amazon S3.

Al cargar archivos en un bucket de Amazon S3, el control de versiones podría estar habilitado o suspendido en dicho bucket. Cuando el control de versiones está habilitado en el bucket, los archivos subidos con el mismo nombre que un archivo existente se añaden como nueva versión del archivo. Si el control de versiones está suspendido, los archivos subidos con el mismo nombre que un archivo existente sobrescriben el archivo existente. Para obtener más información sobre el control de versiones, consulte Uso del control de versiones en los buckets de S3 en la Guía del usuario de Amazon S3.

Al eliminar un elemento relacionado con un archivo, el archivo se elimina de la incidencia pero no se elimina del bucket de Amazon S3. Para obtener más información sobre cómo eliminar objetos de un bucket de Amazon S3, consulte Eliminación de objetos de Amazon S3 en la Guía del usuario de Amazon S3.

Propiedades

La pestaña Propiedades proporciona los siguientes detalles sobre el incidente.

En la sección Propiedades del incidente, puede ver lo siguiente:

- Estado: describe el estado actual del incidente. El incidente puede estar Abierto o Resuelto.
- Hora de inicio: la hora en que se creó el incidente en Incident Manager.
- Hora de resolución: la hora en que se resolvió el incidente en Incident Manager.
- Nombre de recurso de Amazon (ARN): el ARN del incidente. Utilice el ARN cuando haga referencia al incidente desde el chat o con comandos de AWS Command Line Interface (AWS CLI).
- Plan de respuesta: identifica el plan de respuesta para el incidente seleccionado. Al seleccionar el plan de respuesta se abre la página de detalles del plan de respuesta.
- Padre OpsItem: identifica al OpsItem creado como el padre del incidente. Un padre OpsItem puede tener varios incidentes relacionados y adoptar medidas de seguimiento. Al seleccionar al padre, OpsItem se abre la página de OpsItems detalles en OpsCenter.
- Análisis: identifica el análisis creado a partir de este incidente. Cree un análisis a partir de un incidente resuelto para mejorar su proceso de respuesta a incidentes. Seleccione el análisis para abrir la página de detalles del análisis.
- Propietario: la cuenta en la que se creó el incidente.

En la sección Etiquetas, puede ver y editar las claves y valores de las etiquetas asociadas al registro del incidente. Para obtener más información sobre las etiquetas en Incident Manager, consulte Etiquetado de recursos en Administración de incidentes.

Realización de un análisis post-incidente en Incident Manager

El análisis post-incidente le guía en la identificación de mejoras en su respuesta a incidentes, incluyendo el tiempo de detección y mitigación. Un análisis también puede ayudarle a comprender la causa raíz de los incidentes. Incident Manager crea elementos de acción recomendados para mejorar su respuesta ante incidentes.

Beneficios de un análisis post-incidente

- Mejora de la respuesta ante incidentes
- Comprensión de la causa raíz del problema
- Afrontamiento de las causas raíz con elementos de acción factibles
- Análisis del impacto de los incidentes
- Captación y difusión de conocimientos dentro de una organización

Para qué no se debe utilizar un análisis

Un análisis es irreprochable y no llama a las personas por su nombre.

“Independientemente de lo que descubramos, entendemos y creemos de verdad que todo el mundo hizo el mejor trabajo posible, teniendo en cuenta lo que sabía en ese momento, sus habilidades y capacidades, los recursos disponibles y la situación en cuestión”. - Norm Kerth, Retrospectivas de proyectos: Un manual para la revisión en equipo

Detalles del análisis

La página de detalles del análisis le guía en la recopilación de información, la evaluación de mejoras y la creación de elementos de acción. La página de detalles del análisis es similar a la de detalles del incidente, pero tiene algunas diferencias clave, como las métricas históricas, la línea temporal editable y las preguntas para mejorar futuros incidentes.

Descripción general

Información general es un resumen del incidente. Este resumen incluye los antecedentes, lo que ocurrió, por qué ocurrió, cómo se mitigó, la duración y los elementos de acción clave para evitar que

el incidente vuelva a ocurrir. La información general es de alto nivel. Puede explorar más detalles en la pestaña Preguntas del análisis.

Métricas

Utilice la pestaña de métricas para visualizar las métricas clave de su aplicación durante el periodo del incidente. Aquí puede añadir gráficos de métricas que tengan una o más métricas representadas en el mismo gráfico. Las métricas utilizadas durante un incidente se rellenan automáticamente en esta pestaña. Le recomendamos que añada una descripción, un título y anotaciones de los puntos temporales clave durante el incidente.

Algunos puntos temporales clave que puede tener en cuenta al analizar un gráfico de métricas:

- Cambio de implementación
- Cambio de configuración
- Hora de inicio del incidente
- Hora de la alarma
- Hora de intervención
- Hora de inicio de la mitigación
- Hora de resolución del incidente

Limitaciones

- CloudWatch las alarmas y las expresiones métricas no se importan de un incidente.
- Las métricas que se encuentren en una región que Incident Manager no admita no se importan desde el incidente.
- Las métricas en cuentas de la aplicación requieren la configuración del `CloudWatch-CrossAccountSharingRole` antes de crear el análisis. Para obtener más información sobre la función, consulte la CloudWatch consola multicuentas y regiones en la guía del CloudWatch usuario.

Plazo

Describa los puntos temporales clave en la línea temporal a medida que profundiza en la comprensión del incidente. La línea temporal de los incidentes se rellena automáticamente en esta

pestaña. Puede eliminar los puntos temporales que no sean relevantes para el análisis. También puede añadir y editar puntos temporales para describir con mayor precisión el incidente y su impacto.

Utilice la pestaña de línea temporal para responder a las preguntas que encuentre en la pestaña Preguntas sobre la respuesta al incidente.

Preguntas

Utilice las preguntas de Incident Manager para mejorar el tiempo de resolución de incidentes en su aplicación y reducir la aparición de incidentes. A medida que responda a las preguntas, actualice las pestañas Métricas y Línea temporal para mejorar su exactitud. Las preguntas se centran en estos aspectos clave de la respuesta ante incidentes:

- Detección: ¿Podría mejorar el tiempo de detección? ¿Existen actualizaciones de las métricas y alarmas que detectarían el incidente en menos tiempo?
- Diagnóstico: ¿Puede mejorar el tiempo previo al diagnóstico? ¿Existen actualizaciones para sus planes de respuesta o planes de escalada que implicarían en menos tiempo a los respondedores correctos?
- Mitigación: ¿Puede mejorar el tiempo previo a la mitigación? ¿Hay pasos del manual de procedimientos que podría añadir o mejorar?
- Prevención: ¿Puede evitar que se produzcan futuros incidentes? Para descubrir las causas fundamentales de un incidente, Amazon utiliza el enfoque de los 5 porqués en la investigación de problemas.

Acciones

Incident Manager crea elementos de acción recomendados para que los revise a medida que completa las preguntas. Puede elegir aceptar y completar estas acciones desde esta pestaña o puede descartarlas. Puede revisar los elementos de acción descartados; para ello, elija Elementos de acción descartados. Los elementos de acción son un tipo de elementos OpsItem que están vinculados al análisis y al incidente en cuestión. OpsCenter

Lista de comprobación

Antes de cerrar un análisis, utilice la lista de comprobación para revisar las acciones que un respondedor debería realizar. A medida que los respondedores completan las acciones de la lista de comprobación, el icono junto a la acción cambia de una elipse a una marca de verificación a

fin de indicar que la acción se ha completado. Si no ha completado los elementos de la lista de comprobación, Incident Manager muestra un mensaje para confirmar que el respondedor desea cerrar el análisis sin completarlo.

Plantillas de análisis

Una plantilla de análisis proporciona un conjunto de preguntas que profundizan en la causa raíz de los incidentes. Puede utilizar las respuestas a estas preguntas para mejorar el rendimiento de la aplicación y la respuesta a los incidentes.

AWS plantilla estándar

Incident Manager proporciona una plantilla estándar de preguntas basada en las mejores prácticas de respuesta a AWS incidentes y análisis de problemas, tituladaAWSIncidents-PostIncidentAnalysisTemplate.

Creación de una plantilla de análisis

Le sugerimos que utilice la plantilla de AWSIncidents-PostIncidentAnalysisTemplate predeterminada y añada preguntas o secciones adicionales que sean apropiadas para sus casos de uso. Cree plantillas de análisis basadas en la plantilla predeterminada. Utilice esta plantilla como punto de partida para crear plantillas de análisis en su cuenta de administrador. A continuación, puede duplicar sus plantillas de análisis en cada región en la que haya habilitado Incident Manager.

Creación de una plantilla de análisis

1. Invoque la acción GetDocument y utilice su parámetro Name para descargar AWSIncidents-PostIncidentAnalysisTemplate. Para obtener más información sobre la sintaxis de GetDocument, consulte Referencia de la API de Systems Manager.
2. El contenido de la respuesta contiene los bloques de construcción JSON para el análisis. Utilice los bloques de construcción de preguntas para insertar preguntas adicionales en el análisis. Le recomendamos que añada preguntas o secciones en la sección Incident questions.
3. Para crear la nueva plantilla, utilice la operación CreateDocument con el JSON actualizado del paso anterior. Debe incluir lo siguiente, donde *Analysis_Template_Name* es el nombre de su plantilla,

   - DocumentFormat: "JSON"
   - DocumentType: "ProblemAnalysisTemplate"

- `Name: "Analysis_Template_Name"`

Creación de un análisis

1. Para crear un análisis, elija Crear análisis en la página de detalles del incidente de un incidente cerrado.
2. Elija la plantilla de análisis a partir de la cual crear este análisis e introduzca un nombre descriptivo del análisis.
3. Seleccione Crear.

Impresión de un análisis de incidente formateado

Puede generar una copia de un análisis completo o incompleto formateado para impresión. También puede guardar esta copia como archivo PDF. Puede imprimir un análisis cada vez. Actualmente no se admite la impresión por lotes de múltiples análisis.

Para imprimir un análisis formateado

1. Abra la consola de Incident Manager.
2. Elija la pestaña Análisis.
3. Elija el título del análisis que desee imprimir.
4. En la esquina superior derecha de la página de detalles del análisis, elija Imprimir.
5. En el cuadro de diálogo Imprimir análisis de incidente, desactive las secciones del análisis que no desee incluir en la versión impresa. De forma predeterminada, están seleccionadas todas las secciones.
6. Elija Imprimir para abrir los controles de impresión locales de su dispositivo.
7. Elija el destino o formato de impresión. Puede elegir una impresora local o de red, o puede guardar el análisis en un archivo PDF. Realice cualquier cambio, si lo desea, en las opciones de impresión restantes y, a continuación, elija Imprimir.

> **Note**
>
> Controles de impresión locales se refiere a la interfaz de usuario proporcionada por su navegador web y dispositivo.

Destinos de impresión son aquellos configurados para su dispositivo y accesibles desde el mismo.

Tutoriales de Administración de incidentes

Estos tutoriales de AWS Systems Manager Incident Manager le ayudan a crear un sistema de gestión de incidentes más sólido. Estos tutoriales desarrollan actividades comunes llevadas a cabo durante un incidente o muestran cómo responder a determinados incidentes.

Temas

- Tutorial: Uso de los manuales de automatización de Systems Manager con Incident Manager
- Tutorial: Gestión de incidentes de seguridad en Incident Manager

Tutorial: Uso de los manuales de automatización de Systems Manager con Incident Manager

Puede usar los manuales de AWS Systems Manager automatización para simplificar las tareas comunes de mantenimiento, implementación y corrección de los servicios. AWS En este tutorial, creará un manual de procedimientos personalizado para automatizar la respuesta a un incidente en Administración de incidentes. El escenario de este tutorial implica una CloudWatch alarma de Amazon asignada a una métrica de Amazon EC2. Cuando la instancia entra en un estado que activa la alarma, Administración de incidentes realiza automáticamente las siguientes tareas:

1. Crea un incidente en Administración de incidentes.
2. Inicia un manual de procedimientos que intenta corregir el problema.
3. Publica los resultados del manual de procedimientos en la página de detalles del incidente en Administración de incidentes.

El proceso descrito en este tutorial también se puede utilizar con EventBridge eventos de Amazon y otros tipos de AWS recursos. Al automatizar su respuesta de corrección a alarmas y eventos, puede reducir el impacto de un incidente en su organización y sus recursos.

En este tutorial se describe cómo editar una CloudWatch alarma asignada a una instancia de Amazon EC2 para un plan de respuesta de Incident Manager. Si no tiene una alarma, una instancia ni un plan de respuesta configurados, le recomendamos que configure esos recursos antes de comenzar. Para obtener más información, consulte los temas siguientes:

- Uso de CloudWatch las alarmas de Amazon en la Guía del CloudWatch usuario de Amazon

- Instancias de Amazon EC2 en la Guía del usuario de Amazon EC2
- Instancias de Amazon EC2 en la Guía del usuario de Amazon EC2
- Creación y configuración de planes de respuesta en Incident Manager

> **Important**
>
> La creación de AWS recursos y el uso de los pasos de automatización habituales generarán costes. Para más información, consulte Precios de AWS.

Temas

Tarea 1: Creación del manual de procedimientos

Utilice el siguiente procedimiento para crear un manual de procedimientos en la consola de Systems Manager. Cuando se invoca desde un incidente de Administración de incidentes, el manual de procedimientos reinicia una instancia de Amazon EC2 y actualiza el incidente con información sobre la ejecución del manual de procedimientos. Antes de comenzar, verifique que tiene permiso para crear un manual de procedimientos. Para obtener más información, consulte Configuración de la automatización en la Guía del usuario de AWS Systems Manager .

> **Important**
>
> Revise los siguientes detalles importantes sobre la creación del manual de procedimientos de este tutorial:
>
> - El manual está diseñado para un incidente creado a partir de una CloudWatch fuente de alarma. Si utiliza este manual de procedimientos para otro tipo de incidentes, por ejemplo, incidentes creados manualmente, no se encontrará el evento de la línea temporal en el primer paso del manual de procedimientos y el sistema devolverá un error.

- El manual requiere que la CloudWatch alarma incluya una dimensión llamada. `InstanceId` Las alarmas para métricas de instancias de Amazon EC2 tienen esta dimensión. Si utiliza este manual con otras métricas (o con otras fuentes de incidentes, por ejemplo EventBridge), tendrá que cambiar el `JsonDecode2` paso para que coincida con los datos capturados en su escenario.
- El manual de procedimientos intenta corregir el problema que activó la alarma reiniciando la instancia de Amazon EC2. En un incidente real, es posible que no desee reiniciar la instancia. Actualice el manual de procedimientos con las acciones de corrección específicas que desea que realice el sistema.

Para obtener más información sobre la creación de manuales de procedimientos, consulte Trabajo con manuales de procedimientos en la Guía del usuario de AWS Systems Manager .

Para crear un manual de procedimientos

1. Abre la AWS Systems Manager consola en. https://console.aws.amazon.com/systems-manager/
2. En el panel de navegación, elija Documentos.
3. Elija Automatización.
4. En Nombre, introduzca un nombre descriptivo para el manual de procedimientos, como **`IncidentResponseRunbook`**.
5. Elija la pestaña Editor y después elija Edit (Editar).
6. Pegue el siguiente contenido en el editor:

```
description: This runbook attempts to restart an Amazon EC2 instance that caused an
 incident.
schemaVersion: '0.3'
parameters:
  IncidentRecordArn:
    type: String
    description: The incident
mainSteps:
  - name: ListTimelineEvents
    action: 'aws:executeAwsApi'
    outputs:
      - Selector: '$.eventSummaries[0].eventId'
        Name: eventId
        Type: String
```

```
    inputs:
      Service: ssm-incidents
      Api: ListTimelineEvents
      incidentRecordArn: '{{IncidentRecordArn}}'
      filters:
        - key: eventType
          condition:
            equals:
              stringValues:
                - SSM Incident Trigger
    description: This step retrieves the ID of the first timeline event with the
CloudWatch alarm details.
  - name: GetTimelineEvent
    action: 'aws:executeAwsApi'
    inputs:
      Service: ssm-incidents
      Api: GetTimelineEvent
      incidentRecordArn: '{{IncidentRecordArn}}'
      eventId: '{{ListTimelineEvents.eventId}}'
    outputs:
      - Name: eventData
        Selector: $.event.eventData
        Type: String
    description: This step retrieves the timeline event itself.
  - name: JsonDecode
    action: 'aws:executeScript'
    inputs:
      Runtime: python3.8
      Handler: script_handler
      Script: |-
        import json

        def script_handler(events, context):
          data = json.loads(events["eventData"])
          return data
      InputPayload:
        eventData: '{{GetTimelineEvent.eventData}}'
    outputs:
      - Name: rawData
        Selector: $.Payload.rawData
        Type: String
    description: This step parses the timeline event data.
  - name: JsonDecode2
    action: 'aws:executeScript'
```

```
    inputs:
      Runtime: python3.8
      Handler: script_handler
      Script: |-
        import json

        def script_handler(events, context):
          data = json.loads(events["rawData"])
          return data
      InputPayload:
        rawData: '{{JsonDecode.rawData}}'
    outputs:
      - Name: InstanceId
        Selector:
'$.Payload.detail.configuration.metrics[0].metricStat.metric.dimensions.InstanceId'
        Type: String
    description: This step parses the CloudWatch event data.
  - name: RestartInstance
    action: 'aws:executeAutomation'
    inputs:
      DocumentName: AWS-RestartEC2Instance
      DocumentVersion: $DEFAULT
      RuntimeParameters:
        InstanceId: '{{JsonDecode2.InstanceId}}'
    description: This step restarts the Amazon EC2 instance
```

7. Elija Create automation (Crear automatización).

Tarea 2: Creación de un rol de IAM

Utilice el siguiente tutorial para crear un rol AWS Identity and Access Management (de IAM) que dé permiso al administrador de incidentes para iniciar un manual especificado en un plan de respuesta. El manual de procedimientos de este tutorial reinicia una instancia de Amazon EC2. Especificará este rol de IAM en la siguiente tarea al conectar el manual de procedimientos a su plan de respuesta.

Creación de un rol de IAM que inicie un manual de procedimientos desde un plan de respuesta

1. Abra la consola de IAM en https://console.aws.amazon.com/iam/.
2. En el panel de navegación, seleccione Roles y luego seleccione Crear rol.
3. En Tipo de entidad de confianza, verifique que Servicio de AWS esté seleccionado.

4. En Caso de uso, en el campo Casos de uso para otros servicios de AWS , introduzca **`Incident Manager`**.
5. Elija Incident Manager y, a continuación, Siguiente.
6. En la página Añadir permisos, elija Crear política. El editor de permisos se abre en una nueva ventana o pestaña del navegador.
7. En el editor, elija la pestaña JSON.
8. Copie y pegue la siguiente política de permisos en el editor JSON. Reemplace *`account_ID`* por el ID de su Cuenta de AWS .

   JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Resource": [
                "arn:aws:ssm:*:111122223333:document/
IncidentResponseRunbook",
                "arn:aws:ssm:*::document/AWS-RestartEC2Instance",
                "arn:aws:ssm:*:111122223333:automation-execution/*"
            ],
            "Action": "ssm:StartAutomationExecution"
        },
        {
            "Effect": "Allow",
            "Resource": "arn:aws:ssm:*:*:automation-execution/*",
            "Action": "ssm:GetAutomationExecution"
        },
        {
            "Effect": "Allow",
            "Resource": "arn:aws:ssm-incidents:*:*:*",
            "Action": "ssm-incidents:*"
        },
        {
            "Effect": "Allow",
            "Resource": "arn:aws:iam::*:role/AWS-SystemsManager-
AutomationExecutionRole",
            "Action": "sts:AssumeRole"
        },
```

```
        {
            "Effect": "Allow",
            "Resource": "*",
            "Action": [
                "ec2:StopInstances",
                "ec2:DescribeInstanceStatus",
                "ec2:StartInstances"
            ]
        }
    ]
}
```

9. Elija Siguiente: etiquetas.
10. (Opcional) De ser necesario, añada etiquetas a su política.
11. Elija Siguiente: Revisar.
12. En el campo Nombre, introduzca un nombre que le ayude a identificar este rol como utilizado para este tutorial.
13. (Opcional) Introduzca una descripción en el campo Descripción.
14. Elija Crear política.
15. Regrese a la ventana o pestaña del navegador correspondiente al rol que está creando. Se visualiza la página Añadir permisos.
16. Elija el botón de actualización (situado junto al botón Crear política) y, a continuación, introduzca el nombre de la política de permisos que ha creado en el cuadro de filtro.
17. Elija la política de permisos que ha creado y, a continuación, Siguiente.
18. En la página Nombre, revisión y creación, en Nombre del rol, introduzca un nombre que le ayude a identificar este rol como utilizado para este tutorial.
19. (Opcional) Introduzca una descripción en el campo Descripción.
20. Revise los detalles del rol, añada etiquetas si fuese necesario y seleccione Crear rol.

Tarea 3: Conexión del manual de procedimientos a su plan de respuesta

Al conectar el manual de procedimientos a su plan de respuesta de Administración de incidentes, se asegura un proceso de mitigación coherente, repetible y oportuno. El manual de procedimientos también sirve como punto de partida para que los solucionadores determinen su siguiente curso de acción.

Para asignar el manual de procedimientos a su plan de respuesta

1. Abra la consola de Administración de incidentes.
2. Elija Planes de respuesta.
3. En Plan de respuesta, elija un plan de respuesta existente y seleccione Editar. Si no tiene un plan de respuesta existente, elija Crear plan de respuesta para crear uno nuevo.

   Complete los siguientes campos:

   a. En la sección Manual de procedimientos, elija Seleccionar manual de procedimientos existente.
   b. En Propietario, compruebe que Propiedad mía esté seleccionado.
   c. En Manual de procedimientos, seleccione el manual de procedimientos que creó en Tarea 1: Creación del manual de procedimientos.
   d. En Versión, elija Predeterminado en el momento de ejecución.
   e. En la sección Entradas, para el IncidentRecordArnparámetro, elija ARN de incidente.
   f. En la sección Permisos de ejecución, elija el rol de IAM que creó en Tarea 2: Creación de un rol de IAM.
4. Guarde los cambios.

Tarea 4: Asignar una CloudWatch alarma a su plan de respuesta

Utilice el siguiente procedimiento para asignar una CloudWatch alarma para una instancia de Amazon EC2 a su plan de respuesta.

Para asignar una CloudWatch alarma a su plan de respuesta

1. Abra la CloudWatch consola en https://console.aws.amazon.com/cloudwatch/.
2. En el panel de navegación, en Alarmas, elija Todas las alarmas.
3. Elija una alarma para una instancia de Amazon EC2 que desee conectar a su plan de respuesta.
4. Seleccione Acciones y, a continuación, Editar. Compruebe que la métrica tenga una dimensión denominada `InstanceId`.
5. Elija Siguiente.
6. En Asistente para configurar acciones, elija Añadir acción de Systems Manager.
7. Elija Crear incidente.

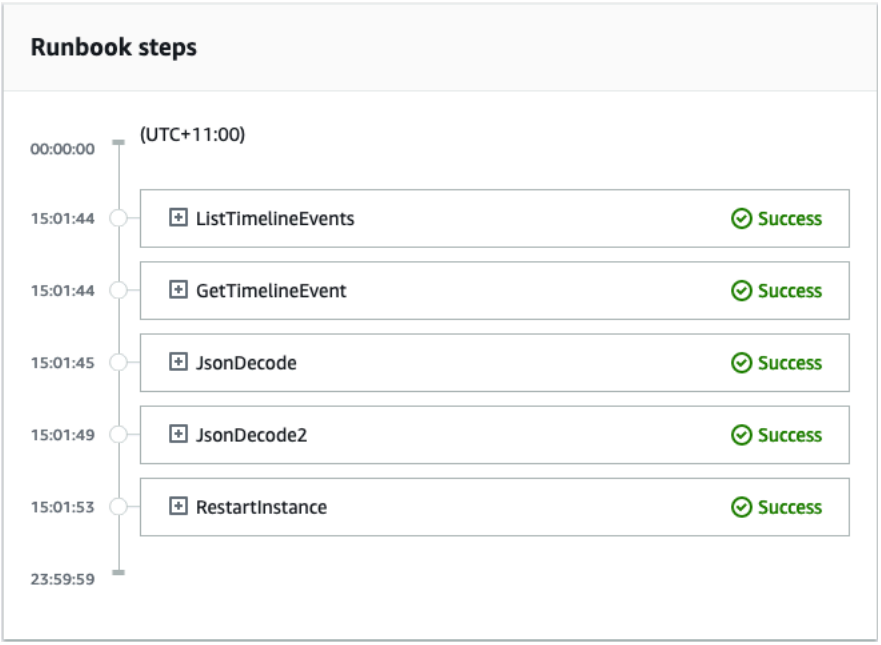
8. Elija el plan de respuesta que creó en Tarea 3: Conexión del manual de procedimientos a su plan de respuesta.
9. Elija Update alarm (Actualizar alarma).

Tarea 5: Verificación de resultados

Para comprobar que la CloudWatch alarma crea un incidente y, a continuación, procesa el manual especificado en su plan de respuesta, debe activar la alarma. Tras activar la alarma y una vez que finalice el procesamiento del manual de procedimientos, puede verificar los resultados del manual de procedimientos mediante el siguiente procedimiento. Para obtener información sobre cómo activar una alarma, consulte la set-alarm-stateReferencia de AWS CLI comandos.

1. Abra la consola de Administración de incidentes.
2. Elija el incidente creado por la CloudWatch alarma.
3. Elija la pestaña Manuales de procedimientos.
4. Vea las acciones realizadas en su instancia de Amazon EC2 en la sección Pasos del manual de procedimientos.

   La siguiente imagen muestra cómo se muestran en la consola los pasos seguidos en el manual que creó en este tutorial. Cada paso se enumera con una marca de tiempo y un mensaje de estado.



Para ver todos los detalles de la CloudWatch alarma, expanda los JsonDecodedos pasos y, a continuación, expanda la opción Salida.

> **Important**
>
> Debe sanear cualquier cambio en los recursos que haya implementado durante este tutorial y que no desee conservar. Esto incluye cambios en los recursos del administrador de incidentes, como los planes de recursos y los incidentes, los cambios en CloudWatch las alarmas y la función de IAM que creó para este tutorial.

Tutorial: Gestión de incidentes de seguridad en Incident Manager

Puede usar AWS Security Hub CSPM Amazon EventBridge e Incident Manager juntos para identificar y gestionar los incidentes de seguridad en sus aplicaciones AWS alojadas. En este tutorial se explica cómo configurar una EventBridge regla que cree un incidente en función de las conclusiones que el CSPM envía automáticamente a Security Hub.

> **Note**
>
> En este tutorial se utiliza EventBridge Security Hub CSPM. Podría incurrir en costos por el uso de estos servicios.

Requisitos previos

- Configure Security Hub CSPM. Para obtener más información, consulte Configuración AWS Security Hub CSPM.
- Cree o actualice las conclusiones en Security Hub CSPM. Para obtener más información, consulte Resultados en AWS Security Hub CSPM.
- Configure un plan de respuesta que Incident Manager utilice como plantilla al crear su incidente de seguridad. Para obtener más información, consulte Preparación para incidentes en Incident Manager.

En este tutorial, utilizamos un patrón predefinido para crear la EventBridge regla. Para crear la regla con un patrón personalizado, consulte Uso de un patrón personalizado para crear la regla en la guía del AWS Security Hub CSPM usuario.

Cree una EventBridge regla

1. Abre la EventBridge consola de Amazon en https://console.aws.amazon.com/events/.
2. En el panel de navegación, seleccione Reglas.
3. Elija Creación de regla.
4. Escriba un nombre y la descripción de la regla.

   Una regla no puede tener el mismo nombre que otra regla de la misma región y del mismo bus de eventos.
5. En Bus de eventos, elija Predeterminado.
6. En Tipo de regla, elija Regla con un patrón de evento.
7. Elija Siguiente.
8. En Fuente del evento, selecciona AWS eventos o eventos EventBridge asociados.
9. En Patrón del evento, elija Formulario de patrón de eventos.
10. En Origen de evento, seleccione Servicios de AWS .
11. Para el AWS servicio, elija Security Hub CSPM.
12. En Tipo de evento, elija Security Hub CSPM Findings - Imported.
13. De forma predeterminada, EventBridge configura el patrón de eventos sin ningún valor de filtro. Para cada atributo, se selecciona la *`attribute name`* opción Cualquiera. Actualice estos filtros para crear incidentes basados en los resultados de seguridad que más afecten a su entorno.
14. Haga clic en Next (Siguiente).
15. En Tipos de destino, seleccione Servicio de AWS .
16. En Seleccionar un objetivo, elija Plan de respuesta de Incident Manager.
17. En Plan de respuesta, elija un plan de respuesta para utilizarlo como plantilla para los incidentes creados.
18. EventBridge puede crear el rol de IAM necesario para que se ejecute la regla.

    - Para crear un rol de IAM de forma automática, elija Crear un nuevo rol para el recurso específico.
    - Para utilizar un rol de IAM que ya exista en su cuenta, elija Utilizar rol existente.

19. (Opcional) Introduzca una o varias etiquetas para la regla.
20. Elija Siguiente.
21. Revise los detalles de la regla y seleccione Creación de regla.

Ahora que ha creado esta EventBridge regla, los fallos de seguridad que coincidan con los valores de los atributos que ha definido crearán incidentes en Incident Manager. Puede clasificar, administrar, monitorear y crear análisis post-incidente a partir de estos incidentes.

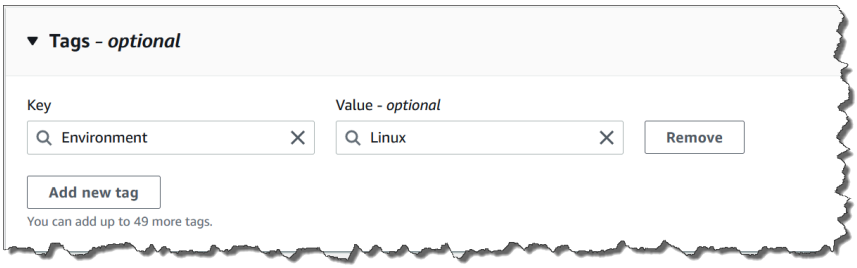
Etiquetado de recursos en Administración de incidentes

Las etiquetas son metadatos opcionales que puede asignar a los recursos de Incident Manager según lo Regiones de AWS especificado en su conjunto de replicación. Puede asignar etiquetas a planes de respuesta, registros de incidentes y contactos. También puede añadir etiquetas a los horarios y rotaciones de guardia. También puede añadir etiquetas al propio conjunto de réplica. Las etiquetas le permiten categorizar y controlar el acceso a estos recursos de diferentes maneras. Cada etiqueta está formada por una clave y un valor opcional, ambos definidos por el usuario. Le recomendamos que diseñe un conjunto de claves de etiquetas que satisfaga sus necesidades para cada tipo de recurso de Incident Manager. El uso de un conjunto coherente de claves de etiquetas le facilita la administración de estos recursos y el control del acceso a los mismos. Puede buscar y filtrar recursos en función de las etiquetas. Para obtener más información sobre cómo controlar el acceso a los recursos mediante etiquetas, consulte Controlar el acceso a AWS los recursos mediante etiquetas en la Guía del usuario de IAM.

Puede especificar etiquetas en la sección Valores predeterminados de incidentes al crear un plan de respuesta. Estas etiquetas se aplican al registro del incidente cuando se crea un incidente utilizando el plan de respuesta.

> **Note**
>
> Las etiquetas no tienen ningún significado semántico. Se interpretan estrictamente como una cadena de caracteres.

Puede añadir o eliminar etiquetas mediante la consola de Administración de incidentes. La siguiente captura de pantalla muestra el área de etiquetas de una página de consola, con campos para añadir claves y valores de etiquetas, y botones para añadir y eliminar etiquetas.



Para trabajar con etiquetas mediante programación, utilice las siguientes acciones de la API:

- TagResource

- UntagResource
- ListTagsForResource

> **Important**
>
> Las etiquetas aplicadas a los planes de respuesta, los registros de incidentes, los contactos, los horarios y rotaciones de guardia y los conjuntos de réplica pueden verse y modificarse solo desde la cuenta del propietario del recurso.

Seguridad en Administrador de incidentes de AWS Systems Manager

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

La seguridad es una responsabilidad compartida entre AWS usted y usted. El se refiere a estos conceptos como seguridad de la nube y seguridad en la nube:

- Seguridad de la nube: AWS es responsable de proteger la infraestructura que se ejecuta Servicios de AWS en la Nube de AWS. AWS también le proporciona servicios que puede utilizar de forma segura. Third-party los auditores comprueban y verifican periódicamente la eficacia de nuestra seguridad como parte de los AWS programas de de . Para obtener más información sobre los programas de cumplimiento aplicables Administrador de incidentes de AWS Systems Manager, consulte AWS Servicios incluidos en el ámbito de aplicación por programa de conformidad y AWS servicios incluidos .
- Seguridad en la nube: su responsabilidad viene determinada por el AWS servicio que utilice. 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 al utilizar Incident Manager. En los siguientes temas le mostramos cómo configurar Incident Manager para satisfacer sus objetivos de seguridad y conformidad. También aprenderá a utilizar otros Servicios de AWS que le ayuden a supervisar y proteger sus recursos de Incident Manager.

Temas

- ¿Trabajando con Administrador de incidentes de AWS Systems Manager y puntos finales de VPC de interfaz (AWS PrivateLink)
- Configuración y análisis de vulnerabilidades en Incident Manager
- Mejores prácticas de seguridad en Administrador de incidentes de AWS Systems Manager

Protección de los datos en Incident Manager

El modelo de responsabilidad compartida de AWS se aplica a la protección de datos en Administrador de incidentes de AWS Systems Manager. 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 con Incident Manager u otro tipo de administrador Servicios de AWS mediante 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.

De forma predeterminada, Incident Manager cifra los datos en tránsito mediante. SSL/TLS

Cifrado de datos

Incident Manager utiliza las claves AWS Key Management Service (AWS KMS) para cifrar los recursos de Incident Manager. Para obtener más información al respecto AWS KMS, consulte la Guía para AWS KMS desarrolladores. AWS KMS combina hardware y software seguros y de alta disponibilidad para proporcionar un sistema de administración de claves adaptado a la nube. Incident Manager cifra sus datos con la clave especificada y cifra los metadatos con una AWS clave propia. Para utilizar Incident Manager, debe configurar su conjunto de réplica, lo que incluye configurar el cifrado. Incident Manager requiere el cifrado de datos para su uso.

Puede utilizar una AWS clave propia para cifrar el conjunto de replicación o puede utilizar la clave gestionada por el cliente que creó AWS KMS para cifrar las regiones del conjunto de replicación. Incident Manager solo admite AWS KMS claves de cifrado simétricas para cifrar los datos creados en él. AWS KMS Incident Manager no admite AWS KMS claves con material de claves importado, almacenes de claves personalizados, códigos de autenticación de Hash-based mensajes (HMAC) ni ningún otro tipo de claves. Si utiliza claves administradas por el cliente, utilice la consola de AWS KMS o las API de AWS KMS para crear de forma centralizada las claves administradas por el cliente y definir las políticas de claves que controlen cómo Incident Manager puede utilizar las claves administradas por el cliente. Cuando utiliza una clave administrada por el cliente para el cifrado con Incident Manager, la clave administrada por el AWS KMS cliente debe estar en la misma región que los recursos. Para obtener más información sobre cómo configurar el cifrado de datos en Incident Manager, consulte Asistente de preparación.

El uso de claves administradas por el AWS KMS cliente conlleva cargos adicionales. Para obtener más información, consulte Conceptos de AWS KMS - Claves de KMS en la Guía para desarrolladores de AWS Key Management Service y Precios de AWS KMS.

> **Important**
>
> Si utiliza una AWS KMS key (clave KMS) para cifrar el conjunto de replicación y los datos de Incident Manager, pero más adelante decide eliminarlo, asegúrese de eliminarlo antes de deshabilitar o eliminar la clave KMS.

Para permitir que Incident Manager utilice su clave administrada por el cliente para cifrar sus datos, debe añadir las siguientes declaraciones de política a la política de claves de su clave administrada por el cliente. Para obtener más información sobre cómo configurar y cambiar la política de claves de su cuenta, consulte Uso de políticas de claves en AWS KMS en la Guía para desarrolladores de AWS Key Management Service . La política proporciona los siguientes permisos:

- Permite a Incident Manager realizar operaciones de solo lectura para encontrar la correspondiente a Incident Manager en AWS KMS key su cuenta.
- Permite a Incident Manager usar la clave KMS para crear concesiones y describir la clave, pero solo cuando actúa en nombre de los responsables de la cuenta que tienen permiso para usar Incident Manager. Si las entidades principales especificadas en la declaración de política no tienen permiso para utilizar las claves de KMS ni para utilizar Incident Manager, la llamada falla, incluso si procede del servicio de Incident Manager.

```
{
"Sid": "Allow CreateGrant through AWS Systems Manager Incident Manager",
"Effect": "Allow",
"Principal": {
  "AWS": "arn:aws:iam::111122223333:user/ssm-lead"
},
"Action": [
  "kms:CreateGrant",
  "kms:DescribeKey"
],
"Resource": "*",
"Condition": {
  "StringLike": {
    "kms:ViaService": [
      "ssm-incidents.us-east-2.amazonaws.com",
      "ssm-contacts.us-east-2.amazonaws.com"
    ]
  }
```

```
        }
      }
```

Sustituya el valor `Principal` por la entidad principal de IAM que creó su conjunto de réplica.

Incident Manager utiliza un contexto de cifrado en todas las solicitudes AWS KMS para realizar operaciones criptográficas. Puede utilizar este contexto de cifrado para identificar los eventos de CloudTrail registro en los que Incident Manager utiliza sus claves de KMS. Incident Manager utiliza el siguiente contexto de cifrado:

- `contactArn=`*`ARN of the contact or escalation plan`*

Identity and Access Management para Administrador de incidentes de AWS Systems Manager

AWS Identity and Access Management (IAM) es una herramienta Servicio de AWS que ayuda al administrador a controlar de forma segura el acceso a los AWS recursos. Los administradores de IAM controlan quién puede ser autenticado (iniciar sesión) y autorizado (tener permisos) para utilizar los recursos de Incident Manager. La IAM es una Servicio de AWS herramienta que puede utilizar sin coste adicional.

Temas

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 Administrador de incidentes de AWS Systems Manager identidad y acceso).
- Administrador del servicio: determine el acceso de los usuarios y envíe las solicitudes de permiso (consulte Cómo Administrador de incidentes de AWS Systems Manager funciona con IAM).
- Administrador de IAM: escribe las políticas para administrar el acceso (consulte Identity-based ejemplos de políticas para Administrador de incidentes de AWS Systems Manager).

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.

Cuenta de AWS usuario raíz

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 recomiendaencarecidamente que no utilice el usuario raíz para las tareas diarias. Para ver las tareas que requieren credenciales de usuario raíz, consulte Tareas que requieren credenciales de usuario raíz en la Guía del usuario de IAM.

Identidad federada

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

Una identidad federada es un usuario del directorio empresarial, del proveedor de identidades web o al Directory Service que se accede Servicios de AWS mediante credenciales de una fuente de identidad. Las identidades federadas asumen roles que proporcionan credenciales temporales.

Para una administración de acceso centralizada, se recomienda AWS IAM Identity Center. Para obtener más información, consulte ¿Qué es el Centro de identidades de IAM? en la Guía del usuario de AWS IAM Identity Center .

Usuarios y grupos de IAM

Un usuario de IAM es una identidad 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.

Resource-based políticas

Resource-based las políticas son documentos de políticas de JSON que se adjuntan a un recurso. Los ejemplos incluyen las Políticas de confianza de roles de IAM y las Políticas de bucket de Amazon S3. En los servicios que admiten políticas basadas en recursos, los administradores de servicios pueden utilizarlos para controlar el acceso a un recurso específico. Debe especificar una entidad principal en una política basada en recursos.

Resource-based las políticas son políticas en línea que se encuentran en ese servicio. No puedes usar políticas AWS gestionadas de IAM en una política basada en recursos.

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 Administrador de incidentes de AWS Systems Manager funciona con IAM

Antes de utilizar IAM para administrar el acceso a Incident Manager, infórmese de las características de IAM de que dispone para su uso con Incident Manager.

Funciones de IAM que puede utilizar con Administrador de incidentes de AWS Systems Manager

Característica de IAM	Soporte de Incident Manager
Identity-basedpolíticas	Sí
Resource-based políticas	Sí
Acciones de políticas	Sí
Recursos de políticas	Sí
Claves de condición de política	No
ACL	No

Característica de IAM	Soporte de Incident Manager
ABAC (etiquetas en políticas)	No
Credenciales temporales	Sí
Permisos de entidades principales	Sí
Roles de servicio	Sí
Service-linked roles	Sí

Para obtener una visión general de cómo funcionan Incident Manager y otros AWS servicios con la mayoría de las funciones de IAM, consulte AWS los servicios que funcionan con IAM en la Guía del usuario de IAM.

Incident Manager no admite políticas que denieguen el acceso a recursos compartidos mediante AWS RAM.

Identity-based políticas de Incident Manager

Compatibilidad con las políticas basadas en identidad: sí

Identity-based las políticas son documentos de política de permisos de JSON que puedes adjuntar a una identidad, como un usuario, un grupo de usuarios o un rol de IAM. Estas políticas controlan qué acciones pueden realizar los usuarios y los roles, en qué recursos y en qué condiciones. Para obtener más información sobre cómo crear una política basada en la identidad, consulte Definición de permisos de IAM personalizados con políticas administradas por el cliente en la Guía del usuario de IAM.

Con las políticas basadas en identidades de IAM, puede especificar las acciones y los recursos permitidos o denegados, así como las condiciones en las que se permiten o deniegan las acciones. Para obtener más información sobre los elementos que puede utilizar en una política de JSON, consulte Referencia de los elementos de la política de JSON de IAM en la Guía del usuario de IAM.

Identity-based ejemplos de políticas para Incident Manager

Para ver ejemplos de políticas basadas en identidades de Incident Manager, consulte Identity-based ejemplos de políticas para Administrador de incidentes de AWS Systems Manager.

Resource-based políticas dentro de Incident Manager

Compatibilidad con las políticas basadas en recursos: sí

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

Para habilitar el acceso entre cuentas, puede especificar toda una cuenta o entidades de IAM de otra cuenta como la entidad principal de una política en función de recursos. Para obtener más información, consulte Acceso a recursos entre cuentas en IAM en la Guía del usuario de IAM.

El servicio Incident Manager solo admite dos tipos de políticas basadas en recursos: la AWS RAM consola o la PutResourcePolicy acción, que se adjunta a un plan de respuesta o contacto. Esta política define qué entidades principales pueden realizar acciones en relación con los planes de respuesta, los contactos, los planes de escalada y los incidentes. Incident Manager utiliza políticas basadas en recursos para compartir los recursos entre las cuentas.

Incident Manager no admite políticas que denieguen el acceso a recursos compartidos mediante AWS RAM.

Para obtener información sobre cómo adjuntar una política basada en recursos a un plan de respuesta o a un contacto, consulte Gestión de incidentes en todas Cuentas de AWS las regiones en Incident Manager.

Resource-based ejemplos de políticas en Incident Manager

Para ver ejemplos de políticas basadas en recursos de Incident Manager, consulte Resource-based ejemplos de políticas para Administrador de incidentes de AWS Systems Manager.

Acciones de política de Incident Manager

Compatibilidad con las acciones de políticas: sí

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

El elemento `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.

Para ver una lista de acciones de Incident Manager, consulte Acciones definidas por Administrador de incidentes de AWS Systems Manager en la Referencia de autorización de servicios.

Las acciones de política en Incident Manager utilizan los siguientes prefijos antes de la acción:

```
ssm-incidents
ssm-contacts
```

Para especificar varias acciones en una única instrucción, sepárelas con comas.

```
"Action": [
      "ssm-incidents:GetResponsePlan",
      "ssm-contacts:GetContact"
         ]
```

Puede utilizar caracteres comodín (*) para especificar varias acciones . Por ejemplo, para especificar todas las acciones que comiencen con la palabra `Get`, incluya la siguiente acción:

```
"Action": "ssm-incidents:Get*"
```

Para ver ejemplos de políticas basadas en identidades de Incident Manager, consulte Identity-based ejemplos de políticas para Administrador de incidentes de AWS Systems Manager.

Incident Manager utiliza acciones en dos espacios de nombre diferentes, ssm-incidents y ssm-contacts. Al crear políticas para Incident Manager, asegúrese de utilizar el espacio de nombres correcto para la acción. SSM-Incidents se utiliza para el plan de respuesta y las acciones relacionadas con los incidentes. SSM-Contactsse usa para acciones relacionadas con los contactos y la participación de los contactos. Por ejemplo:

- `ssm-contacts:GetContact`

- `ssm-incidents:GetResponsePlan`

Recursos de políticas para Incident Manager

Compatibilidad con los recursos de políticas: sí

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

El elemento `Resource` de la política JSON especifica el objeto u objetos a los que se aplica la acción. Como práctica recomendada, especifique un recurso utilizando el Nombre de recurso de Amazon (ARN). En el caso de las acciones que no admiten permisos por recurso, utilice un carácter comodín (*) para indicar que la instrucción se aplica a todos los recursos.

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

Para ver una lista de los tipos de recursos de Incident Manager y sus ARN, consulte Recursos definidos por Administrador de incidentes de AWS Systems Manager en la Referencia de autorización de servicios. Para obtener información sobre las acciones con las que puede especificar el ARN de cada recurso, consulte Acciones definidas por Administrador de incidentes de AWS Systems Manager.

Para ver ejemplos de políticas basadas en identidades de Incident Manager, consulte Identity-based ejemplos de políticas para Administrador de incidentes de AWS Systems Manager.

Los recursos de Incident Manager se utilizan para crear incidentes, colaborar en los canales de chat, resolver incidentes e involucrar al personal de respuesta. Si un usuario tiene acceso a un plan de respuesta, tiene acceso a todos los incidentes creados a partir del mismo. Si un usuario tiene acceso a un contacto o a un plan de escalada puede hacer participar a un contacto (o contactos) en el plan de escalada.

Claves de condiciones de políticas para Incident Manager

Compatibilidad con claves de condición de políticas específicas del servicio: no

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

El elemento `Condition` especifica cuándo se ejecutan las instrucciones en función de criterios definidos. Puede crear expresiones condicionales que utilizan operadores de condición, tales como igual o menor que, para que la condición de la política coincida con los valores de la solicitud. Para ver todas las claves de condición AWS globales, consulte las claves de contexto de condición AWS globales en la Guía del usuario de IAM.

Listas de control de acceso (ACL) en Incident Manager

Compatibilidad con ACL: no

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

Attribute-based control de acceso (ABAC) con Incident Manager

Compatibilidad con ABAC (etiquetas en las políticas): no

Attribute-based el control de acceso (ABAC) es una estrategia de autorización que define los permisos en función de unos atributos denominados etiquetas. Puede adjuntar etiquetas a las entidades y AWS los recursos de IAM y, a continuación, diseñar políticas de ABAC para permitir las operaciones cuando la etiqueta del director coincida con la etiqueta del recurso.

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

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

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

Uso de credenciales temporales con Incident Manager

Compatibilidad con credenciales temporales: sí

Las credenciales temporales proporcionan acceso a AWS los recursos a corto plazo y se crean automáticamente cuando se utiliza la federación o se cambia de rol. AWS recomienda generar

credenciales temporales de forma dinámica en lugar de utilizar claves de acceso a largo plazo. Para obtener más información, consulte Credenciales de seguridad temporales en IAM y Servicios de AWS que funcionan con IAM en la Guía del usuario de IAM.

Cross-service permisos principales para Incident Manager

Admite sesiones de acceso directo (FAS): sí

Las sesiones de acceso directo (FAS) utilizan los permisos del operador principal que llama Servicio de AWS, junto con los de solicitud, Servicio de AWS para realizar solicitudes a los servicios descendentes. Para obtener información sobre las políticas a la hora de realizar solicitudes de FAS, consulte Sesiones de acceso directo.

Roles de servicio para Incident Manager

Compatible con roles de servicio: sí

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

> **Warning**
>
> La modificación de permisos de un rol de servicio puede interrumpir la funcionalidad de Incident Manager. Edite los roles de servicio solo cuando Incident Manager le proporcione orientación para hacerlo.

Elección de un rol de IAM en Incident Manager

Al crear un recurso de plan de respuesta en Incident Manager, debe elegir un rol para permitir que Incident Manager ejecute un documento de automatización de Systems Manager en su nombre. Si ha creado previamente un rol de servicio o un rol vinculado al servicio, Incident Manager le proporciona una lista de roles entre los que elegir. Es importante elegir un rol que permita el acceso para ejecutar sus instancias de documentos de automatización. Para obtener más información, consulte Integración de los manuales de automatización de Systems Manager en Incident Manager para la solución de incidentes. Cuando creas un canal de chat para desarrolladores de Amazon Q en aplicaciones de chat para usarlo durante un incidente, puedes seleccionar un rol de servicio que te

permita usar comandos directamente desde el chat. Para obtener más información sobre la creación de canales de chat para colaboración en incidentes, consulte Creación e integración de canales de chat para el personal de respuesta en Incident Manager. Para obtener más información sobre las políticas de IAM en aplicaciones de chat para desarrolladores de Amazon Q, consulte Administrar los permisos para ejecutar comandos con Amazon Q Developer en aplicaciones de chat en la guía del administrador de Amazon Q Developer en aplicaciones de chat.

Service-linked funciones del administrador de incidentes

Compatible con roles vinculados al servicio: sí

Un rol vinculado a un servicio es un tipo de rol de servicio que está vinculado a un. Servicio de AWS El servicio puede asumir la función de realizar una acción en su nombre. Service-linked las funciones aparecen en su nombre Cuenta de AWS y son propiedad del servicio. Un administrador de IAM puede ver, pero no editar, los permisos de los roles vinculados a servicios.

Para obtener información sobre la creación o administración de roles vinculados al servicio de Incident Manager, consulte Uso de roles vinculados a servicios para Incident Manager.

Identity-based ejemplos de políticas para Administrador de incidentes de AWS Systems Manager

De forma predeterminada, los usuarios y roles no tienen permiso para crear ni modificar recursos de Incident Manager. Un administrador de IAM puede crear políticas de IAM para conceder permisos a los usuarios para realizar acciones en los recursos que necesitan.

Para obtener información acerca de cómo crear una política basada en identidades de IAM mediante el uso de estos documentos de políticas JSON de ejemplo, consulte Creación de políticas de IAM (consola) en la Guía del usuario de IAM.

Para obtener más información sobre acciones y tipos de recursos definidos por Incident Manager, incluyendo el formato de los ARN para cada tipo de recurso, consulte Acciones, recursos y claves de condición para Administrador de incidentes de AWS Systems Manager en la Referencia de autorización de servicios.

Temas

- Prácticas recomendadas sobre las políticas
- Uso de la consola de Incident Manager
- Cómo permitir a los usuarios consultar sus propios permisos

- Acceso a un plan de respuesta

Prácticas recomendadas sobre las políticas

Identity-based las políticas determinan si alguien puede crear, acceder o eliminar los recursos de Incident Manager de su cuenta. Estas acciones pueden generar costos adicionales para su Cuenta de AWS. Siga estas directrices y recomendaciones al crear o editar políticas basadas en identidades:

- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos: para empezar a conceder permisos a sus usuarios y cargas de trabajo, utilice las políticas AWS administradas que otorgan permisos para muchos casos de uso comunes. Están disponibles en su. Cuenta de AWS Le recomendamos que reduzca aún más los permisos definiendo políticas administradas por el AWS cliente que sean específicas para sus casos de uso. Con el fin de obtener más información, consulte las políticas administradas por AWS o las políticas administradas por AWS para funciones de tarea en la Guía de usuario de IAM.
- Aplique permisos de privilegio mínimo: cuando establezca permisos con políticas de IAM, conceda solo los permisos necesarios para realizar una tarea. Para ello, debe definir las acciones que se pueden llevar a cabo en determinados recursos en condiciones específicas, también conocidos como permisos de privilegios mínimos. Con el fin de obtener más información sobre el uso de IAM para aplicar permisos, consulte Políticas y permisos en IAM en la Guía del usuario de IAM.
- Utilice condiciones en las políticas de IAM para restringir aún más el acceso: puede agregar una condición a sus políticas para limitar el acceso a las acciones y los recursos. Por ejemplo, puede escribir una condición de políticas para especificar que todas las solicitudes deben enviarse utilizando SSL. También puedes usar condiciones para conceder el acceso a las acciones del servicio si se utilizan a través de una acción específica Servicio de AWS, por ejemplo CloudFormation. Para obtener más información, consulte Elementos de la política de JSON de IAM: Condición en la Guía del usuario de IAM.
- Utiliza el analizador de acceso de IAM para validar las políticas de IAM con el fin de garantizar la seguridad y funcionalidad de los permisos: el analizador de acceso de IAM valida políticas nuevas y existentes para que respeten el lenguaje (JSON) de las políticas de IAM y las prácticas recomendadas de IAM. El analizador de acceso de IAM proporciona más de 100 verificaciones de políticas y recomendaciones procesables para ayudar a crear políticas seguras y funcionales. Para más información, consulte Validación de políticas con el Analizador de acceso de IAM en la Guía del usuario de IAM.
- Requerir autenticación multifactor (MFA): si tiene un escenario que requiere usuarios de IAM o un usuario raíz en Cuenta de AWS su cuenta, active la MFA para mayor seguridad. Para exigir la

MFA cuando se invoquen las operaciones de la API, añada condiciones de MFA a sus políticas. Para más información, consulte Acceso seguro a la API con MFA en la Guía del usuario de IAM.

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

Uso de la consola de Incident Manager

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

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, permita el acceso únicamente a las acciones que coincidan con la operación de API que intentan realizar.

Para garantizar que los usuarios y los roles puedan resolver los incidentes mediante la consola de Incident Manager, adjunte también la política `IncidentManagerResolverAccess` AWS gestionada por Incident Manager a las entidades. Para obtener más información, consulte Adición de permisos a un usuario en la Guía del usuario de IAM:

```
IncidentManagerResolverAccess
```

Cómo permitir a los usuarios consultar sus propios permisos

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

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
```

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

Acceso a un plan de respuesta

En este ejemplo, desea conceder a un usuario de IAM de su cuenta de Amazon Web Services acceso a uno de sus planes de respuesta de Incident Manager, `exampleplan`. También desea permitir al usuario que añada, actualice y elimine el plan de respuesta.

La política concede los permisos `ssm-incidents:ListResponsePlans`, `ssm-incidents:GetResponsePlan`, `ssm-incidents:UpdateResponsePlan` y `ssm-incident:ListResponsePlan` al usuario.

JSON

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

```
            "Effect":"Allow",
            "Action":[
               "ssm-incidents:ListResponsePlans"
            ],
            "Resource":"arn:aws:ssm-incidents:::*"
         },
         {
            "Sid":"ViewSpecificResponsePlanInfo",
            "Effect":"Allow",
            "Action":[
               "ssm-incidents:GetResponsePlan"
            ],
            "Resource":"arn:aws:ssm-incidents:*:111122223333:response-plan/
exampleplan"
         },
         {
            "Sid":"ManageResponsePlan",
            "Effect":"Allow",
            "Action":[
               "ssm-incidents:UpdateResponsePlan"
            ],
            "Resource":"arn:aws:ssm-incidents:*:111122223333:response-plan/
exampleplan/*"
         }
      ]
}
```

Resource-based ejemplos de políticas para Administrador de incidentes de AWS Systems Manager

Administrador de incidentes de AWS Systems Manager admite políticas de permisos basadas en recursos para los planes de respuesta y los contactos de Incident Manager.

Incident Manager no admite políticas basadas en recursos que denieguen el acceso a los recursos que se utilizan de forma compartida. AWS RAM

Para obtener información sobre cómo crear un plan de respuesta o un contacto, consulte Creación y configuración de planes de respuesta en Incident Manager y Creación y configuración de contactos en Incident Manager.

Restricción de acceso al plan de respuesta de Incident Manager por organización

El siguiente ejemplo otorga permisos a los usuarios de la organización con ID de organización `o-abc123def45` para que respondan a incidentes creados utilizando el plan de respuesta `myplan`.

El `Condition` bloque usa las `StringEquals` condiciones y la clave de `aws:PrincipalOrgID` condición, que es una clave de condición AWS Organizations específica. Para obtener más información sobre estas claves de condición, consulte Especificación de condiciones en una política.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "OrganizationAccess",
            "Effect": "Allow",
            "Principal": "*",
            "Condition": {
                "StringEquals": {
                    "aws:PrincipalOrgID": "o-abc123def45"
                }
            },
            "Action": [
                "ssm-incidents:GetResponsePlan",
                "ssm-incidents:StartIncident",
                "ssm-incidents:UpdateIncidentRecord",
                "ssm-incidents:GetIncidentRecord",
                "ssm-incidents:CreateTimelineEvent",
                "ssm-incidents:UpdateTimelineEvent",
                "ssm-incidents:GetTimelineEvent",
                "ssm-incidents:ListTimelineEvents",
                "ssm-incidents:UpdateRelatedItems",
                "ssm-incidents:ListRelatedItems"
            ],
            "Resource": [
                "arn:aws:ssm-incidents:*:111122223333:response-plan/myplan",
                "arn:aws:ssm-incidents:*:111122223333:incident-record/myplan/*"
            ]
        }
    ]
}
```

Concesión de acceso de contactos de Incident Manager a una entidad principal

El siguiente ejemplo concede permiso a la entidad principal con ARN `arn:aws:iam::999988887777:root` para crear participaciones con el contacto `mycontact`.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "PrincipalAccess",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::999988887777:root"
            },
            "Action": [
                "ssm-contacts:GetContact",
                "ssm-contacts:StartEngagement",
                "ssm-contacts:DescribeEngagement",
                "ssm-contacts:ListPagesByContact"
            ],
            "Resource": [
                "arn:aws:ssm-contacts:*:111122223333:contact/mycontact",
                "arn:aws:ssm-contacts:*:111122223333:engagement/mycontact/*"
            ]
        }
    ]
}
```

Cross-service confundido sistema de prevención adjunto en Incident Manager

El problema del suplente confuso es un problema de seguridad que se produce cuando una entidad sin permiso para realizar una acción llama a una entidad con más privilegios para que la realice. Esto puede permitir que actores malintencionados ejecuten comandos o modifiquen recursos para los que, de otro modo, no tendrían permiso de ejecución ni acceso.

En este caso AWS, la suplantación de identidad entre varios servicios puede llevar a un escenario confuso a un diputado. Cross-service la suplantación de identidad se produce cuando un servicio

(el servicio de llamadas) llama a otro servicio (el servicio al que se llama). Un actor malintencionado puede utilizar el servicio de llamadas para alterar los recursos de otro servicio mediante permisos que normalmente no tendría.

AWS proporciona a los directores de servicio acceso gestionado a los recursos de tu cuenta para ayudarte a proteger la seguridad de tus recursos. Recomendamos utilizar las claves de contexto de condición global de `aws:SourceArn` y `aws:SourceAccount` en sus políticas de recursos. Estas claves limitan los permisos que Administrador de incidentes de AWS Systems Manager otorgan otro servicio a ese recurso. Si se utilizan ambas claves de contexto de condición global, el valor `aws:SourceAccount` y la cuenta referenciada en el valor `aws:SourceArn` deben utilizar el mismo ID de cuenta cuando se utilicen en la misma declaración de política.

El valor de `aws:SourceArn` debe ser el ARN del registro del incidente afectado. Si no conoce el ARN completo del recurso o si está especificando varios recursos, utilice la clave de condición de contexto global `aws:SourceArn` con el comodín (*) para las partes desconocidas del ARN. Por ejemplo, puede establecer `aws:SourceArn` para `arn:aws:ssm-incidents::111122223333:*`.

En el siguiente ejemplo de política de confianza, utilizamos la clave de condición `aws:SourceArn` para restringir el acceso al rol de servicio en función del ARN del registro de incidentes. Solo los registros de incidentes creados a partir del recurso del plan de respuesta `myresponseplan` pueden utilizar este rol.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Principal": { "Service": "ssm-incidents.amazonaws.com" },
    "Action": "sts:AssumeRole",
    "Condition": {
      "ArnLike": {
        "aws:SourceArn": "arn:aws:ssm-incidents:*:111122223333:incident-record/
myresponseplan/*"
      }
    }
  }
}
```

Uso de roles vinculados a servicios para Incident Manager

Administrador de incidentes de AWS Systems Manager utiliza funciones vinculadas al AWS Identity and Access Management servicio (IAM). Un rol vinculado al servicio es un tipo único de rol de IAM que está vinculado directamente a Incident Manager. Service-linked Los roles están predefinidos por Incident Manager e incluyen todos los permisos que el servicio necesita para llamar a otros AWS servicios en su nombre.

Un rol vinculado a servicios facilita la configuración de Incident Manager porque no tiene que añadir manualmente los permisos necesarios. Incident Manager define los permisos de sus roles vinculados a servicios y, a menos que se defina de otro modo, solo Incident Manager puede asumir sus roles. Los permisos definidos incluyen las políticas de confianza y de permisos, y que la política de permisos no se pueda adjuntar a ninguna otra entidad de IAM.

Solo es posible eliminar un rol vinculado a un servicio después de eliminar sus recursos relacionados. Esto protege sus recursos de Incident Manager porque usted no puede eliminar inadvertidamente el permiso para acceder a los recursos.

Para obtener información acerca de otros servicios que son compatibles con roles vinculados a servicios, consulte Servicios de AWS que funcionan con IAM y busque los servicios en los que se indica Sí en la columna Service-Linked Rol vinculado a servicios. Elija una opción Sí con un enlace para ver la documentación acerca del rol vinculado al servicio en cuestión.

Service-linked permisos de rol para Incident Manager

Incident Manager utiliza el rol vinculado al servicio denominado. AWSServiceRoleforIncidentManager Esta función permite a Incident Manager gestionar los registros de incidentes del Incident Manager y los recursos relacionados en su nombre.

El rol AWSServiceRoleforIncidentManager vinculado al servicio confía en los siguientes servicios para asumir el rol:

- `ssm-incidents.amazonaws.com`

La política de permisos del rol `AWSIncidentManagerServiceRolePolicy` permite a Incident Manager realizar las siguientes acciones en los recursos especificados:

- Acción: `ssm-incidents:ListIncidentRecords` en todos los recursos relacionados con la acción.

- Acción: `ssm-incidents:CreateTimelineEvent` en todos los recursos relacionados con la acción.
- Acción: `ssm:CreateOpsItem` en todos los recursos relacionados con la acción.
- Acción: `ssm:AssociateOpsItemRelatedItem` en `all resources related to the action.`
- Acción: `ssm-contacts:StartEngagement` en todos los recursos relacionados con la acción.
- Acción: `cloudwatch:PutMetricData` en CloudWatch las métricas incluidas en los espacios de nombres y `AWS/IncidentManager` `AWS/Usage`

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. Para obtener más información, consulte los permisos de Service-Linked rol en la Guía del usuario de IAM.

Creación de un rol vinculado a servicios para Incident Manager

No necesita crear manualmente un rol vinculado a servicios. Al crear un conjunto de replicación en la Consola de administración de AWS, la API o la AWS API AWS CLI, Incident Manager crea automáticamente la función vinculada al servicio.

Si elimina este rol vinculado a servicios y necesita crearlo de nuevo, puede utilizar el mismo proceso para volver a crear el rol en su cuenta. Al crear un conjunto de réplica, Incident Manager vuelve a crear el rol vinculado a servicios por usted.

Edición de un rol vinculado a servicios para Incident Manager

Incident Manager no le permite editar el rol vinculado al AWSServiceRoleforIncidentManager servicio. Después de crear un rol vinculado a un servicio, no puede cambiarle el nombre, ya que varias entidades pueden hacer referencia a él. Sin embargo, puede editar la descripción del rol mediante IAM. Para obtener más información, consulte Edición de un Service-Linked rol en la Guía del usuario de IAM.

Eliminación de un rol vinculado a servicios para Incident Manager

Si ya no necesita usar una característica o servicio que requieran un rol vinculado a un servicio, le recomendamos que elimine dicho rol. De esta forma no conservará una entidad no utilizada que no se monitorice ni se mantenga de forma activa. Sin embargo, debe limpiar los recursos de su rol vinculado al servicio antes de eliminarlo manualmente.

Para eliminar el rol vinculado a servicios, primero debe eliminar el conjunto de réplica. Al eliminar el conjunto de réplica se eliminan todos los datos creados y almacenados en Incident Manager, incluyendo los planes de respuesta, contactos y planes de escalada. También pierde todos los incidentes creados anteriormente. Las alarmas y EventBridge reglas que indiquen la eliminación de planes de respuesta dejarán de generar un incidente al producirse una alarma o una coincidencia de reglas. Para eliminar el conjunto de réplica debe eliminar todas las regiones del conjunto.

> **Note**
>
> Si el servicio de Incident Manager utiliza el rol al momento de intentar eliminar los recursos, es posible que la eliminación falle. En tal caso, espere unos minutos e intente de nuevo la operación.

Para eliminar las regiones del conjunto de réplicas utilizado por el AWSServiceRoleforIncidentManager

1. Abra la consola de Incident Manager y seleccione Configuración en el panel de navegación izquierdo.
2. Seleccione una región en Conjunto de réplica.
3. Elija Eliminar.
4. Para confirmar la eliminación de la región, introduzca el nombre de la región y elija Eliminar.
5. Repita estos pasos hasta que haya eliminado todas las regiones de su conjunto de réplica. Al eliminar la última región, la consola le notifica que con ella elimina el conjunto de réplica.

Para eliminar manualmente el rol vinculado a servicios mediante IAM

Utilice la consola de IAM AWS CLI, la o la AWS API para eliminar la función vinculada al AWSServiceRoleforIncidentManager servicio. Para obtener más información, consulte Eliminar un Service-Linked rol en la Guía del usuario de IAM.

Regiones admitidas para los roles vinculados a servicios de Incident Manager

Incident Manager admite el uso de roles vinculados a servicios en todas las regiones en las que el servicio esté disponible. Para obtener más información, consulte AWS Regiones y puntos de conexión.

AWS políticas gestionadas para Administrador de incidentes de AWS Systems Manager

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: AWSIncidentManagerIncidentAccessServiceRolePolicy

Puede adjuntar `AWSIncidentManagerIncidentAccessServiceRolePolicy` a sus entidades de IAM. Incident Manager también asocia esta política a un rol de Incident Manager que permite a Incident Manager realizar acciones en su nombre.

Esta política otorga permisos de solo lectura que permiten a Incident Manager leer los recursos de otros Servicios de AWS para identificar los hallazgos relacionados con los incidentes en esos servicios.

Detalles de los permisos

Esta política incluye los siguientes permisos.

- `cloudformation`— Permite a los directores describir las pilas. CloudFormation Esto es necesario para que el administrador de incidentes identifique CloudFormation los eventos y los recursos relacionados con un incidente.
- `codedeploy`— Permite a los directores leer las AWS CodeDeploy implementaciones. Esto es necesario para que Incident Manager identifique CodeDeploy los despliegues y los objetivos relacionados con un incidente.
- `autoscaling`— Permite a los directores determinar si una instancia de Amazon Elastic Compute Cloud (EC2) (EC2) forma parte de un grupo de Auto Scaling. Esto es necesario para que Incident Manager pueda proporcionar resultados para las instancias de EC2 que forman parte de los grupos de Auto Scaling.

Para ver más detalles sobre la política, incluyendo la última versión del documento de política JSON, consulte AWSIncidentManagerIncidentAccessServiceRolePolicy en la Guía de referencia de políticas administradas de AWS .

AWS política gestionada: **`AWSIncidentManagerServiceRolePolicy`**

No puede asociar `AWSIncidentManagerServiceRolePolicy` a sus entidades IAM. Esta política se vincula a un rol vinculado a servicios que permite a Incident Manager realizar acciones en su nombre. Para obtener más información, consulte Uso de roles vinculados a servicios para Incident Manager.

Esta política otorga a Incident Manager permisos para enumerar incidentes, crear eventos cronológicos OpsItems, crear elementos relacionados con ellos OpsItems, asociarlos a ellos, iniciar interacciones y publicar CloudWatch métricas relacionadas con un incidente.

Detalles de los permisos

Esta política incluye los siguientes permisos.

- `ssm-incidents`: permite a las entidades principales enumerar incidentes y crear eventos de línea temporal. Resulta necesario para que los respondedores puedan colaborar durante un incidente en el panel de control de incidentes.

- `ssm`— Permite a los directores crear OpsItems y asociar elementos relacionados. Esto es necesario para crear un padre OpsItem cuando se inicia un incidente.
- `ssm-contacts`: permite a las entidades principales iniciar participaciones. Resulta necesario para que Incident Manager involucre a los contactos durante un incidente.
- `cloudwatch`— Permite a los directores publicar CloudWatch métricas. Esto es necesario para que Incident Manager publique las métricas relacionadas con un incidente y las métricas de uso.

Para ver más detalles sobre la política, incluyendo la última versión del documento de política JSON, consulte AWSIncidentManagerServiceRolePolicy en la Guía de referencia de políticas administradas de AWS .

AWS política gestionada: **`AWSIncidentManagerResolverAccess`**

Puede vincular `AWSIncidentManagerResolverAccess` a sus entidades de IAM para permitirles iniciar, ver y actualizar incidentes. Esto también les permite crear incidencias en la línea temporal del cliente y elementos relacionados en el panel de control de incidencias. También puedes adjuntar esta política a la función de desarrollador de Amazon Q en el servicio de aplicaciones de chat o directamente a tu función gestionada por el cliente asociada a cualquier canal de chat utilizado para la colaboración en caso de incidentes. Para obtener más información sobre las políticas de IAM en aplicaciones de chat para desarrolladores de Amazon Q, consulte Administrar los permisos para ejecutar comandos con Amazon Q Developer en aplicaciones de chat en la Guía del administrador de Amazon Q Developer in chat aplicaciones.

Detalles de los permisos

Esta política incluye los siguientes permisos.

- `ssm-incidents`— Permite a los directores iniciar incidentes, enumerar planes de respuesta, enumerar incidentes, actualizar incidentes, enumerar eventos cronológicos, crear eventos personalizados, actualizar eventos cronológicos personalizados, eliminar eventos cronológicos personalizados, eliminar eventos cronológicos personalizados, enumerar elementos relacionados, crear elementos relacionados y actualizar elementos relacionados.
- `ssm-contacts`— Permite a los directores iniciar interacciones con los contactos durante la creación de los incidentes.

Para ver más detalles sobre la política, incluyendo la última versión del documento de política JSON, consulte AWSIncidentManagerResolverAccess en la Guía de referencia de políticas administradas de AWS .

Incident Manager actualiza a AWS políticas administradas

Consulte los detalles sobre las actualizaciones de las políticas AWS gestionadas de Incident Manager desde que este servicio comenzó a rastrear estos cambios. Para recibir alertas automáticas sobre los cambios en esta página, suscríbase al canal RSS en la página Historial de documentos de Incident Manager.

Cambio	Descripción	Fecha
`AWSIncidentManagerResolverAccess` — Actualización de la política	Incident Manager agregó permiso para iniciar interacciones con los contactos.	20 de noviembre de 2025
`AWSIncidentManagerServiceRolePolicy` — Actualización de la política	Incident Manager agregó un nuevo permiso que le permite a Incident Manager publicar las métricas del espacio de `AWS/Usage` nombres en su cuenta.	27 de enero de 2025
AWSIncidentManagerIncidentAccessServiceRolePolicy — Actualización de la política	Incident Manager ha agregado un nuevo permiso`AWSIncidentManagerIncidentAccessServiceRolePolicy` , en apoyo de la función Findings, que le permite comprobar si una instancia EC2 forma parte de un grupo de Auto Scaling.	20 de febrero de 2024
`AWSIncidentManagerIncidentAccessServ`	Incident Manager agregó una nueva política que otorga	17 de noviembre de 2023

Cambio	Descripción	Fecha
iceRolePolicy : política nueva	permisos a Incident Manager para llamar a otras Servicios de AWS personas como parte de la gestión de un incidente.	
AWSIncidentManager ServiceRolePolicy — Actualización de la política	Incident Manager agregó un nuevo permiso que le permite a Incident Manager publicar métricas en su cuenta.	16 de diciembre de 2022
AWSIncidentManager ResolverAccess : política nueva	Incident Manager ha añadido una nueva política que permite iniciar incidente s, enumerar planes de respuesta, enumerar incidente s, actualizar incidentes, enumerar eventos de la línea temporal, crear eventos de la línea temporal personali zados, actualizar eventos de la línea temporal personali zados, eliminar eventos de la línea temporal personalizados, enumerar elementos relaciona dos, crear elementos relaciona dos y actualizar elementos relacionados.	26 de abril de 2021

Cambio	Descripción	Fecha
AWSIncidentManagerServiceRolePolicy: política nueva	Incident Manager agregó una nueva política que le otorga permisos a Incident Manager para enumerar incidentes, crear eventos cronológicos OpsItems, crear OpsItems, asociar elementos relaciona dos e iniciar interacciones relacionadas con un incidente.	26 de abril de 2021
Incident Manager comenzó a hacer el seguimiento de cambios	Incident Manager comenzó a realizar un seguimiento de los cambios en sus políticas AWS gestionadas.	26 de abril de 2021

Resolución de problemas Administrador de incidentes de AWS Systems Manager identidad y acceso

Utilice la siguiente información para diagnosticar y solucionar los problemas comunes que pudieran surgir al trabajar con Incident Manager e IAM.

Temas

- No tengo autorización para realizar una acción en Incident Manager
- No estoy autorizado a realizar tareas como: PassRole
- Deseo permitir que personas ajenas a mi cuenta de Amazon Web Services puedan acceder a mis recursos de Incident Manager

No tengo autorización para realizar una acción en Incident Manager

Si recibe un error que indica que no tiene autorización para realizar una acción, las políticas se deben actualizar para permitirle realizar la acción.

En el siguiente ejemplo, el error se produce cuando el usuario de IAM `mateojackson` intenta utilizar la consola para consultar los detalles acerca de un recurso ficticio *`my-example-widget`*, pero no tiene los permisos ficticios `ssm-incidents:`*`GetWidget`*.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform: ssm-
incidents:GetWidget on resource: my-example-widget
```

En este caso, la política del usuario `mateojackson` debe actualizarse para permitir el acceso al recurso *`my-example-widget`* mediante la acción `ssm-incidents:`*`GetWidget`*.

Si necesita ayuda, póngase en contacto con su administrador. AWS El administrador es la persona que le proporcionó las credenciales de inicio de sesión.

No estoy autorizado a realizar tareas como: PassRole

Si recibe un error que indica que no tiene autorización para realizar la acción `iam:PassRole`, se deben actualizar las políticas a fin de permitirle pasar un rol a Incident Manager.

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 llamado `marymajor` intenta utilizar la consola para realizar una acción en Incident Manager. 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.

Deseo permitir que personas ajenas a mi cuenta de Amazon Web Services puedan acceder a mis recursos de Incident Manager

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 obtener información acerca de si Incident Manager admite estas características, consulte Cómo Administrador de incidentes de AWS Systems Manager 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 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.

Uso compartido de contactos y planes de respuesta en Incident Manager

Al compartir contactos, como propietario de un contacto, puede compartir la información de contacto, los planes de escalamiento y las interacciones con otras personas Cuentas de AWS o dentro de una AWS organización.

Al compartir un plan de respuesta, como propietario del plan de respuesta, puede compartir un plan de respuesta y los incidentes relacionados con otros Cuentas de AWS o dentro de una AWS organización.

El propietario de un contacto o de un plan de respuesta puede compartir contactos y planes de respuesta con:

- Cuentas de AWS Específico dentro o fuera de su organización en AWS Organizations
- Una unidad organizativa dentro de su organización en AWS Organizations

- Toda su organización en AWS Organizations

Contenido

Requisitos previos para compartir contactos y planes de respuesta

Para compartir un contacto o un plan de respuesta con su organización o unidad organizativa en AWS Organizations:

- Debe ser propietario del recurso en su Cuenta de AWS. No puede compartir un contacto o plan de respuesta que se haya compartido con usted.
- Debe habilitar el uso compartido con AWS Organizations. Para obtener más información, consulte Habilitar el uso compartido con AWS Organizations en la Guía del usuario de AWS RAM .

Servicios relacionados

El uso compartido de contactos y planes de respuesta se integra con AWS Resource Access Manager (AWS RAM). Con AWS RAM, puede compartir sus AWS recursos con cualquiera Cuenta de AWS o mediante AWS Organizations. Puede compartir los recursos que posea creando un Uso compartido de recursos. Un uso compartido de recursos especifica los recursos que compartir y los consumidores con quienes compartirlos. Los consumidores pueden ser individuos Cuentas de AWS, unidades organizativas o toda una organización AWS Organizations.

Para obtener más información al respecto AWS RAM, consulte la Guía AWS RAM del usuario.

Uso compartido de un contacto o un plan de respuesta

Después de compartir un plan de respuesta, los consumidores tienen acceso a todos los incidentes pasados, actuales y futuros creados con el uso de ese plan de respuesta.

Después de compartir un contacto, los consumidores tienen acceso a la información de contacto, el plan de participación, los planes de escalada y las participaciones que tengan lugar durante un incidente. Los consumidores también pueden acceder a un contacto o a un plan de escalada durante un incidente.

Si forma parte de una organización AWS Organizations y está activado el uso compartido dentro de su organización, los consumidores de su organización tienen acceso automático al contacto compartido o al plan de respuesta. Caso contrario, los consumidores reciben una invitación para unirse al uso compartido del recurso y se les concede acceso al contacto o plan de respuesta compartido tras aceptar la invitación.

Puedes compartir un contacto o un plan de respuesta de tu propiedad mediante la AWS RAM consola o el AWS CLI.

> **Note**
>
> Actualmente, no se admite la posibilidad de añadir un contacto compartido desde otra cuenta a un plan de respuesta.

Para compartir un contacto o un plan de respuesta de tu propiedad mediante el AWS RAM consola

Consulte Crear un recurso compartido en la Guía del usuario de AWS RAM .

Para compartir un contacto o un plan de respuesta de tu propiedad mediante el AWS CLI

Utilice el comando create-resource-share.

Detención del uso compartido de un contacto o un plan de respuesta

Cuando el propietario de un recurso deja de compartir un contacto o un plan de respuesta con un consumidor, los contactos, planes de respuesta, planes de escalada, participaciones e incidentes dejan de aparecer en la consola del consumidor.

> **Note**
>
> El consumidor seguirá viendo los contactos, planes de respuesta, planes de escalada, participaciones e incidentes sin actualizaciones, si los ve en la consola, hasta que actualice la página o salga de ella.

Para dejar de compartir un contacto o plan de respuesta compartido de su propiedad, debe eliminarlo del recurso compartido. Puede hacerlo mediante la AWS RAM consola o el AWS CLI.

Para dejar de compartir un contacto compartido o un plan de respuesta de tu propiedad mediante el AWS RAM consola

Consulte Actualización de un recurso compartido en la Guía del usuario de AWS RAM .

Para dejar de compartir un contacto compartido o un plan de respuesta de tu propiedad mediante el AWS CLI

Utilice el comando disassociate-resource-share.

Identificación de un contacto o plan de respuesta compartidos

Los propietarios y los consumidores pueden identificar los contactos y planes de respuesta compartidos mediante la consola de Incident Manager y la AWS CLI.

Para identificar un contacto o plan de respuesta compartidos mediante la consola de Incident Manager

> **Note**
>
> Los contactos, planes de respuesta, planes de escalada, participaciones e incidentes no suelen ser identificables como recursos compartidos en la consola de Incident Manager. En aquellos lugares en los que el nombre de recurso de Amazon (ARN) sea visible, el ARN contiene el ID de cuenta del propietario.

Para identificar un contacto compartido o un plan de respuesta mediante el AWS CLI

Utilice los ListContactscomandos ListResponsePlanso. El comando devuelve los contactos y planes de respuesta que le pertenecen y aquellos que se comparten con usted. El ARN muestra el Cuenta de AWS ID del propietario del contacto o del plan de respuesta.

Permisos de los contactos y planes de respuesta compartidos

Permisos de los propietarios

Los propietarios pueden actualizar, ver, compartir, dejar de compartir y utilizar los contactos y planes de respuesta. Los contactos y planes de respuesta incluyen las participaciones y los incidentes relacionados.

Permisos de los consumidores

Los consumidores pueden utilizar y ver solo los planes de respuesta y los contactos. Los contactos y planes de respuesta incluyen las participaciones y los incidentes relacionados.

Facturación y medición

Al propietario del recurso se le factura por el recurso. No se factura a los consumidores por los recursos compartidos con ellos. Compartir un recurso no conlleva costos adicionales.

Límites de instancias

Compartir un recurso no afecta a los límites del recurso en la cuenta del propietario o del consumidor. Solo se utiliza la cuenta del propietario para calcular los límites del recurso.

Validación de conformidad para Administrador de incidentes de AWS Systems Manager

Third-party los auditores evalúan la seguridad y el cumplimiento Administrador de incidentes de AWS Systems Manager como parte de varios programas de AWS cumplimiento. Estos incluyen SOC, PCI, FedRAMP, HIPAA y otros.

Para saber si un programa de cumplimiento Servicio de AWS está dentro del ámbito de aplicación de programas de cumplimiento específicos, consulte Servicios de AWS Alcance by Compliance Servicios de AWS 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 Administrador de incidentes de AWS Systems Manager

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 Infraestructura global.AWS

Incident Manager es un servicio global-regional y actualmente no admite zonas de disponibilidad.

Además de la infraestructura AWS global, Incident Manager ofrece varias funciones para ayudarlo a satisfacer sus necesidades de respaldo y resiliencia de datos. Durante el asistente de preparación se le pedirá que configure un conjunto de réplica. Este conjunto de réplica regional garantiza que sus datos y recursos sean accesibles desde varias regiones, lo cual hace que la administración de incidentes a través de una red en la nube sea más fácil de administrar. Esta réplica también garantiza que sus datos estén seguros y sean accesibles en caso de que una de sus regiones cayese.

Para obtener más información sobre el uso del conjunto de réplica de Incident Manager, consulte Configuración del conjunto de réplicas de Incident Manager.

Seguridad de la infraestructura en Administrador de incidentes de AWS Systems Manager

Como servicio gestionado, Administrador de incidentes de AWS Systems Manager está protegido por la seguridad de la red AWS global. Para obtener información sobre los servicios AWS de seguridad y

cómo se AWS protege la infraestructura, consulte Seguridad AWS en la nube. Para diseñar su AWS entorno utilizando las mejores prácticas de seguridad de la infraestructura, consulte Protección de infraestructuras en un marco de buena AWS arquitectura basado en el pilar de la seguridad.

Utiliza las llamadas a la API AWS publicadas para acceder a Incident Manager a través de la red. Los clientes deben admitir lo siguiente:

- Seguridad de la capa de transporte (TLS). Exigimos TLS 1.2 y recomendamos TLS 1.3.
- Paquetes de cifrado con perfecto secreto directo (PFS), como el DHE (Ephemeral) o el ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). Diffie-Hellman La mayoría de los sistemas modernos como Java 7 y posteriores son compatibles con estos modos.

¿Trabajando con Administrador de incidentes de AWS Systems Manager y puntos finales de VPC de interfaz (AWS PrivateLink)

Puede establecer una conexión privada entre su VPC y crear un punto final Administrador de incidentes de AWS Systems Manager de VPC de interfaz. Puntos de conexión de tipo interfaz con tecnología de AWS PrivateLink. Con ella AWS PrivateLink, puede acceder de forma privada a las operaciones de la API de Incident Manager sin una puerta de enlace a Internet, un dispositivo NAT, una conexión VPN o Direct Connect una conexión. Las instancias de su VPC no necesitan direcciones IP públicas para comunicar con las operaciones de la API de Incident Manager. El tráfico entre su VPC e Incident Manager permanece dentro de la red de Amazon.

Cada punto de conexión de la interfaz está representado por una o más interfaces de red elásticas en las subredes.

Para obtener más información, consulte Puntos de conexión de VPC de interfaz (AWS PrivateLink) en la Guía del usuario de Amazon VPC.

Consideraciones para los puntos de conexión de VPC de Incident Manager

Antes de configurar un punto de conexión de VPC de interfaz para Incident Manager, asegúrese de revisar Propiedades y limitaciones del punto de conexión de interfaz y Cuotas de AWS PrivateLink en la Guía del usuario de Amazon VPC.

Incident Manager permite realizar llamadas a todas las acciones de su API desde su VPC. Para utilizar al completo Incident Manager, debe crear dos puntos de conexión de VPC: uno para `ssm-incidents` y otro para `ssm-contacts`.

Creación de un punto de conexión de VPC de interfaz para Incident Manager

Puede crear un punto de conexión de VPC para Incident Manager mediante la consola de Amazon VPC o la AWS Command Line Interface (AWS CLI). Para obtener más información, consulte Creación de un punto de conexión de interfaz en la Guía del usuario de Amazon VPC.

Cree un punto final de VPC para Incident Manager con los nombres de servicio compatibles con Incident Manager en su. Región de AWS Los siguientes ejemplos muestran los formatos de punto final de interfaz para puntos finales IPv4 y de doble pila.

Formatos de punto final IPv4

- `com.amazonaws.region.ssm-incidents`
- `com.amazonaws.region.ssm-contacts`

Dual-stack Formatos de punto final (IPv4 e IPv6)

- `aws.api.region.ssm-incidents`
- `aws.api.region.ssm-contacts`

Para ver una lista de los puntos de conexión compatibles en todas las regiones, consulte los puntos de conexión y las cuotas de AWS Systems Manager Incident Manager en la AWS Guía de referencia general.

Si habilita el DNS privado para el punto final de la interfaz, puede realizar solicitudes de API a Incident Manager utilizando sus nombres de DNS regionales predeterminados en ese formato. Los siguientes ejemplos muestran el formato de los nombres de DNS regionales predeterminados.

- `ssm-incidents.region.amazonaws.com`
- `ssm-contacts.region.amazonaws.com`

Para más información, consulte Acceso a un servicio a través de un punto de conexión de interfaz en la Guía del usuario de Amazon VPC.

Creación de una política de punto de conexión de VPC para Incident Manager

Puede adjuntar una política de punto de conexión a su punto de conexión de VPC que controle el acceso a Incident Manager. La política especifica la siguiente información:

- La entidad principal que puede realizar acciones.
- Las acciones que se pueden realizar.
- Los recursos sobre los que se pueden realizar estas acciones.

Para obtener más información, consulte Control del acceso a los servicios con puntos de conexión de VPC en la Guía del usuario de Amazon VPC.

Ejemplo: Política de punto de conexión de VPC para acciones de Incident Manager

A continuación, se muestra un ejemplo de una política de punto de conexión para Incident Manager. Cuando se vincula a un punto de conexión, esta política otorga acceso a las acciones de Incident Manager enumeradas para todas las entidades principales en todos los recursos.

```
{
   "Statement":[
      {
         "Principal":"*",
         "Effect":"Allow",
         "Action":[
            "ssm-contacts:ListContacts",
            "ssm-incidents:ListResponsePlans",
            "ssm-incidents:StartIncident"
         ],
         "Resource":"*"
      }
   ]
}
```

Configuración y análisis de vulnerabilidades en Incident Manager

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.

Mejores prácticas de seguridad en Administrador de incidentes de AWS Systems Manager

Administrador de incidentes de AWS Systems Manager proporciona muchas características de seguridad que debe tener en cuenta a la hora de desarrollar e implementar sus propias políticas de seguridad. Las siguientes prácticas recomendadas son directrices generales y no suponen una solución de seguridad completa. Puesto que es posible que estas prácticas recomendadas no sean adecuadas o suficientes para el entorno, plantéeselas como consideraciones útiles en lugar de como normas.

Temas

Prácticas recomendadas de seguridad preventivas para Incident Manager

Implementación del acceso a los privilegios mínimos

Al conceder permisos, usted decide quién obtiene determinados permisos en determinados recursos de Incident Manager. Habilite las acciones específicas que desea permitir en dichos recursos. Por lo tanto, conceda solo los permisos necesarios para realizar una tarea. La implementación del acceso con privilegios mínimos es esencial a la hora de reducir los riesgos de seguridad y el impacto que podrían causar los errores o los intentos malintencionados.

Las siguientes herramientas están disponibles para implementar el acceso a los privilegios mínimos:

- Controlar el acceso a AWS los recursos mediante políticas y límites de permisos para las entidades de IAM
- Políticas de control de servicios

Creación y administración de contactos

Al activar contactos, Incident Manager se pone en contacto con el dispositivo para confirmar la activación. Asegúrese de que la información del dispositivo sea correcta antes de activarlo. Esto reduce la posibilidad de que Incident Manager se ponga en contacto con un dispositivo o persona equivocados durante la activación.

Revise regularmente sus contactos y planes de escalada para asegurarse de que solo se contacte a contactos que deban ser contactados durante un incidente. Revise periódicamente los contactos a fin de eliminar información obsoleta o incorrecta. Si un contacto ya no debe ser informado al producirse un incidente, elimínelo de los planes de escalada relacionados o de Incident Manager.

Privacidad de los canales de chat

Puede hacer que sus canales de chat de incidentes sean privados para implementar el acceso de privilegio mínimo. Considere la posibilidad de utilizar un canal de chat diferente con una lista de usuarios reducida para cada plantilla del plan de respuesta. Esto garantiza que solo los respondedores correctos entren en un canal de chat que pueda contener información sensible.

Slacklos canales creados en Amazon Q Developer en aplicaciones de chat heredan los permisos del rol de IAM utilizado para configurar Amazon Q Developer en aplicaciones de chat. Esto permite a los respondedores de un Slack canal habilitado para desarrolladores de Amazon Q en aplicaciones de chat solicitar cualquier acción de la lista de permitidos, como las API de Incident Manager y la recuperación de gráficos de métricas.

Conservar AWS herramientas actualizadas

AWS publica periódicamente versiones actualizadas de herramientas y complementos que puede utilizar en sus AWS operaciones. Mantener estos recursos actualizados garantiza que los usuarios y las instancias de su cuenta tengan acceso a la funcionalidad y las características de seguridad más recientes de estas herramientas.

- AWS CLI — The AWS Command Line Interface (AWS CLI) es una herramienta de código abierto que te permite interactuar con AWS los servicios mediante comandos de tu consola de línea de comandos. Para actualizar la AWS CLI, ejecute el mismo comando utilizado para instalar la AWS CLI. Recomendamos crear una tarea programada en el equipo local que ejecute el comando apropiado para su sistema operativo al menos una vez cada dos semanas. Para obtener información sobre los comandos de instalación, consulte Instalación de la interfaz de línea de AWS comandos en la Guía del usuario de la interfaz de línea de AWS comandos.
- AWS Tools for Windows PowerShell — Las herramientas para Windows PowerShell son un conjunto de PowerShell módulos que se basan en la funcionalidad expuesta por el AWS SDK para .NET. Las herramientas para Windows le PowerShell permiten programar operaciones en sus AWS recursos desde la línea de PowerShell comandos. Periódicamente, a medida que PowerShell se publiquen versiones actualizadas de las Herramientas para Windows, debe actualizar la versión que esté ejecutando localmente. Para obtener más información, consulte Actualización

de AWS Tools for Windows PowerShell en Windows o Actualización de AWS Tools for Windows PowerShell en Linux o macOS.

Contenido relacionado

Mejores prácticas de seguridad para Systems Manager

Las mejores prácticas recomendadas de seguridad de detección para Incident Manager

Identificación y auditoría de todos sus recursos de Incident Manager

La identificación de sus activos de TI es un aspecto fundamental de seguridad y control. Identifique sus recursos de Systems Manager para evaluar su postura de seguridad y tomar medidas en las posibles áreas de debilidad. Cree grupos de recursos para sus recursos de Incident Manager. Para obtener más información, consulte ¿Qué son los grupos de recursos? en la Guía del usuario de Grupos de recursos de AWS .

Uso AWS CloudTrail

AWS CloudTrail proporciona un registro de las acciones realizadas por un usuario, un rol o un AWS servicio en Incident Manager. Con la información recopilada AWS CloudTrail, puede determinar la solicitud que se realizó a Incident Manager, la dirección IP desde la que se realizó la solicitud, quién la hizo, cuándo se realizó y detalles adicionales. Para obtener más información, consulte Registro de llamadas a la Administrador de incidentes de AWS Systems Manager API mediante AWS CloudTrail.

Supervisión AWS avisos de seguridad

Compruebe periódicamente los avisos de seguridad publicados en Trusted Advisor su nombre. Cuenta de AWS Puede hacer esto mediante programación con describe-trusted-advisor-checks.

Además, supervise activamente la dirección de correo electrónico principal registrada para cada uno de sus Cuentas de AWS miembros. AWS se pondrá en contacto con usted, utilizando esta dirección de correo electrónico, para informarle sobre los problemas de seguridad emergentes que puedan afectarle.

AWS los problemas operativos con un amplio impacto se publican en el AWS Service Health Dashboard. Los problemas operativos también se publican en las cuentas individuales a través de Panel de estado. Para obtener más información, consulte la Documentación de AWS Health.

Contenido relacionado

Amazon Web Services: información general de procesos de seguridad (documento técnico)

Cómo empezar: siga las prácticas recomendadas de seguridad al configurar sus AWS recursos (blog AWS de seguridad)

Prácticas recomendadas de IAM

Mejores prácticas de seguridad en AWS CloudTrail

Supervisión en Incident Manager

AWS Systems Manager Incident Manager se integra con los siguientes servicios que ofrecen capacidades de monitoreo y registro:

CloudWatch métricas

Utilice CloudWatch las métricas para recuperar estadísticas sobre los puntos de datos de las operaciones de AWS Systems Manager Incident Manager como un conjunto ordenado de datos de series temporales, conocidos como métricas. Utilice estas métricas para comprobar que el sistema funciona de acuerdo con lo esperado. Para obtener más información, consulte Monitorización de métricas en Incident Manager con Amazon CloudWatch.

CloudTrail logs

Se utiliza AWS CloudTrail para capturar información detallada sobre las llamadas realizadas a AWS APIs. Puede almacenar estas llamadas como archivos de registro en Amazon Simple Storage Service. Puede usar estos CloudTrail registros para determinar información como qué llamada se realizó, la dirección IP de origen de la llamada, quién hizo la llamada y cuándo se realizó la llamada. Los CloudTrail registros contienen información sobre las llamadas a las acciones de la API de Incident Manager. lPara obtener más información, consulteRegistro de llamadas a la Administrador de incidentes de AWS Systems Manager API mediante AWS CloudTrail.

Trusted Advisor

AWS Trusted Advisor puede ayudarlo a monitorear sus AWS recursos para mejorar el rendimiento, la confiabilidad, la seguridad y la rentabilidad. Hay cuatro Trusted Advisor comprobaciones disponibles para todos los usuarios; hay más de 50 comprobaciones disponibles para los usuarios con un plan de soporte empresarial o empresarial. En el caso de Incident Manager, Trusted Advisor comprueba que la configuración de un conjunto de replicación utilice más de una Región de AWS para admitir la conmutación por error y la respuesta regionales. Para obtener más información, consulte AWS Trusted Advisor en la Guía del usuario de AWS Support .

Monitorización de métricas en Incident Manager con Amazon CloudWatch

Incident Manager proporciona métricas agregadas que puedes monitorear en Amazon CloudWatch. Puede utilizar estas métricas para identificar las tendencias de los incidentes y los planes de respuesta.

Estas métricas incluyen:

- Número de incidentes creados en un determinado periodo.
- Tiempo de respuesta y resolución de esos incidentes
- Número de incidentes resueltos

Puede monitorear las métricas de Incident Manager para comprender mejor su estado operativo y tomar medidas significativas para impulsar la excelencia operativa de su respuesta a incidentes. Las métricas de Incident Manager están disponibles en todas las regiones de Incident Manager. Sus métricas estarán disponibles para consultarlas en Amazon CloudWatch en todas las regiones que especificó en su conjunto de replicaciones al incorporarse a Incident Manager. Puede ver las métricas publicadas en la región en la que se realizaron acciones para el incidente. No hay ningún cargo adicional por estas métricas.

En la CloudWatch consola, puede crear paneles con estas métricas para:

- Medir y revisar su carga de incidentes existente
- Realizar un seguimiento de si su carga de incidentes aumenta, disminuye o permanece igual
- Utilizar con mayor eficacia Incident Manager para reducir la frecuencia, la duración y el impacto de sus incidentes.

En esta página, se describen las métricas de Incident Manager disponibles en la CloudWatch consola.

> **Important**
>
> En el caso de un evento generado por un cliente, si el nombre del valor de origen en `TriggerDetails` se utiliza caracteres que no son ASCII, las métricas del evento no se incluirán en las CloudWatch métricas de Amazon, que no admite texto que no sea ASCII.

`source`solo se puede proporcionar mediante programación, por ejemplo, mediante un SDK o el. AWS CLI

Incident Manager envía las siguientes métricas a CloudWatch.

Métrica	Description (Descripción)
`NumberOfCreateIncidents`	Número de incidentes creados. Dimensiones válidas: [] (dimensión vacía), [`ResponsePlan `], [`Impact`], [`Source`], [`ResponsePlan` , `Impact`], [`ResponsePlan` , `Source`] Unidad: recuento
`NumberOfResolveIncidents`	Número de incidentes resueltos. Dimensiones válidas: [] (dimensión vacía), [`ResponsePlan `], [`Impact`], [`Source`], [`ResponsePlan` , `Impact`], [`ResponsePlan` , `Source`] Unidad: recuento
`TimeToFirstAcknowledgement`	Diferencia de tiempo entre la hora de creación del incidente y la hora en que se realizó el primer acuse de recibo del mismo. Dimensiones válidas: [] (dimensión vacía), [`ResponsePlan `], [`Impact`], [`Source`], [`ResponsePlan` , `Impact`], [`ResponsePlan` , `Source`] Unidad: segundos
`TimeToResolveIncident`	Diferencia de tiempo entre el momento en que se creó el incidente y el momento en que se resolvió.

Métrica	Description (Descripción)
	Dimensiones válidas: [] (dimensión vacía), [`ResponsePlan `], [`Impact`], [`Source`], [`ResponsePlan , Impact`], [`ResponsePlan , Source`] Unidad: segundos

Visualización de las métricas de Incident Manager en la CloudWatch consola

Para ver las métricas de Incident Manager en la CloudWatch consola

1. Abra la CloudWatch consola en https://console.aws.amazon.com/cloudwatch/.
2. En el panel de navegación, seleccione Métricas.
3. Seleccione el espacio de nombres de `IncidentManager`.
4. En la pestaña Métricas, elija una dimensión y, a continuación, elija una métrica.

Para obtener más información sobre cómo trabajar con CloudWatch métricas, consulta los siguientes temas de la Guía del CloudWatch usuario de Amazon:

- Métricas
- Uso de CloudWatch las métricas de Amazon

Dimensiones de métricas

Las métricas de Incident Manager utilizan el espacio de nombres `IncidentManager` y proporciona métricas para las siguientes dimensiones:

Dimensión	Description (Descripción)
`By Response Plan`	Visualiza las métricas agregadas por plan de respuesta.

Dimensión	Description (Descripción)
`By Impact Level`	Visualiza las métricas agregadas por el nivel de gravedad.
`By Source`	Consulta las métricas de los incidentes creados manualmente, por CloudWatch alarma o EventBridge evento.
`Across All Incidents`	Visualiza las métricas agregadas para todos los incidentes en la región de AWS actual.
`Response Plan name and Source`	Visualiza las métricas agregadas para cada combinación de plan de respuesta y origen.
`Response Plan Name and Impact Level`	Visualiza las métricas agregadas para cada combinación de plan de respuesta y nivel de gravedad.

Registro de llamadas a la Administrador de incidentes de AWS Systems Manager API mediante AWS CloudTrail

Administrador de incidentes de AWS Systems Manager está integrado con AWS CloudTrailun servicio que proporciona un registro de las acciones realizadas por un usuario, rol o un Servicio de AWS. CloudTrail captura todas las llamadas a la API de Incident Manager como eventos. Las llamadas capturadas incluyen las llamadas desde la consola de Incident Manager y las llamadas de código a las operaciones de la API de Incident Manager. Con la información recopilada CloudTrail, puede determinar la solicitud que se realizó a Incident Manager, la dirección IP desde la que se realizó la solicitud, cuándo se realizó y detalles adicionales.

Cada entrada de registro o evento contiene información sobre quién generó la solicitud. La información de identidad del usuario le ayuda a determinar lo siguiente:

- Si la solicitud se realizó con las credenciales del usuario raíz o del usuario.
- Si la solicitud se realizó en nombre de un usuario de IAM Identity Center.
- 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.

CloudTrail está activa en tu cuenta Cuenta de AWS cuando creas la cuenta y tienes acceso automáticamente al historial de CloudTrail eventos. El historial de CloudTrail eventos proporciona un registro visible, consultable, descargable e inmutable de los últimos 90 días de eventos de gestión registrados en un. Región de AWSPara obtener más información, consulte Cómo trabajar con el historial de CloudTrail eventos en la Guía del usuario.AWS CloudTrail La visualización del historial de eventos no conlleva ningún CloudTrail cargo.

Para tener un registro continuo de los eventos de Cuenta de AWS los últimos 90 días, crea un almacén de datos de eventos de senderos o CloudTraillagos.

CloudTrail senderos

Un rastro permite CloudTrail entregar archivos de registro a un bucket de Amazon S3. Todos los senderos creados con él Consola de administración de AWS son multirregionales. Puede crear un registro de seguimiento de una sola región o multirregionales mediante la AWS CLI. Se recomienda crear un sendero multirregional, ya que puedes capturar toda la actividad de tu Regiones de AWS cuenta. Si crea un registro de seguimiento de una sola región, solo podrá ver los eventos registrados en la Región de AWS del registro de seguimiento. Para obtener más información acerca de los registros de seguimiento, consulte Creación de un registro de seguimiento para su Cuenta de AWS y Creación de un registro de seguimiento para una organización en la Guía del usuario de AWS CloudTrail .

Puede enviar una copia de sus eventos de administración en curso a su bucket de Amazon S3 sin coste alguno CloudTrail mediante la creación de una ruta; sin embargo, hay cargos por almacenamiento en Amazon S3. Para obtener más información sobre CloudTrail los precios, consulte AWS CloudTrail Precios. Para obtener información acerca de los precios de Amazon S3, consulte Precios de Amazon S3.

CloudTrail Almacenes de datos de eventos en Lake

CloudTrail Lake le permite ejecutar consultas basadas en SQL en sus eventos. CloudTrail Lake convierte los eventos existentes en formato JSON basado en filas al formato Apache ORC. ORC es un formato de almacenamiento en columnas optimizado para una recuperación rápida de datos. Los eventos se agregan en almacenes de datos de eventos, que son recopilaciones inmutables de eventos en función de criterios que se seleccionan aplicando selectores de eventos avanzados. Los selectores que se aplican a un almacén de datos de eventos controlan los eventos que perduran y están disponibles para la consulta. Para obtener más información sobre

CloudTrail Lake, consulte Cómo trabajar con AWS CloudTrail Lake en la Guía del AWS CloudTrail usuario.

CloudTrail Los almacenes de datos y las consultas sobre eventos de Lake conllevan costes. Cuando crea un almacén de datos de eventos, debe elegir la opción de precios que desee utilizar para él. La opción de precios determina el costo de la incorporación y el almacenamiento de los eventos, así como el período de retención predeterminado y máximo del almacén de datos de eventos. Para obtener más información sobre CloudTrail los precios, consulte AWS CloudTrail Precios.

Eventos de gestión de incidentes de Incident Manager en CloudTrail

Los eventos de administración proporcionan información sobre las operaciones de administración que se llevan a cabo en los recursos de su empresa Cuenta de AWS. Se denominan también operaciones del plano de control. De forma predeterminada, CloudTrail registra los eventos de administración.

Administrador de incidentes de AWS Systems Manager registra todas las operaciones del plano de control de Incident Manager como eventos de gestión. Para obtener una lista de las operaciones del plano de Administrador de incidentes de AWS Systems Manager control en las que Incident Manager registra CloudTrail, consulte la referencia de la Administrador de incidentes de AWS Systems Manager API.

Ejemplos de eventos de Incident Manager

Un evento representa una solicitud única de cualquier fuente e incluye información sobre la operación de API 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 la API pública, por lo que los eventos no aparecen en ningún orden específico.

En el siguiente ejemplo, se muestra una entrada de CloudTrail registro que demuestra la `StartIncident` acción.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "1234567890abcdef0",
        "arn": "arn:aws:iam::246873129580111122223333:user/nikki_wolf",
```

```
        "accountId": "abcdef01234567890",
        "accessKeyId": "021345abcdef6789",
        "userName": "nikki_wolf"
    },
    "eventTime": "2024-04-22T23:20:10Z",
    "eventSource": "ssm-incidents.amazonaws.com",
    "eventName": "StartIncident",
    "awsRegion": "us-east-2",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "aws-cli/2.0.58 Python/3.7.4 Darwin/19.6.0 exe/x86_64 command/
ssmincidents.start-incident",
    "requestParameters": {
        "responsePlanArn": "arn:aws:ssm-incidents::555555555555:response-plan/security-
test-response-plan-non-dedupe-v1",
        "clientToken": "12345678-1111-2222-3333-abcdefghijkl"
    },
    "responseElements": {
        "incidentRecordArn": "arn:aws:ssm-incidents::444455556666:incident-record/
security-test-response-plan-non-dedupe-v1/abcdefgh-abcd-1234-1234-1234567890"
    },
    "requestID": "abcdefgh-1234-abcd-1234-1234567abcdef",
    "eventID": "12345678-1234-1234-abcd-abcdef1234567",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "eventCategory": "Management",
    "recipientAccountId": "12345678901234567"
}
```

El siguiente ejemplo muestra una entrada de CloudTrail registro que demuestra la `DeleteContactChannel` acción.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "1234567890abcdef0",
        "arn": "arn:aws:iam::246873129580111122223333:user/nikki_wolf",
        "accountId": "abcdef01234567890",
        "accessKeyId": "021345abcdef6789",
        "userName": "nikki_wolf"
    },
    "eventTime": "2024-04-08T02:27:21Z",
```

```
    "eventSource": "ssm-contacts.amazonaws.com",
    "eventName": "DeleteContactChannel",
    "awsRegion": "us-east-2",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "Apache-HttpClient/UNAVAILABLE (Java/1.8.0_282)",
    "requestParameters": {
        "contactChannelId": "arn:aws:ssm-contacts:us-west-2:555555555555:device/
bnuomysohc/abcdefgh-abcd-1234-1234-1234567890"
    },
    "responseElements": null,
    "requestID": "abcdefgh-1234-abcd-1234-1234567abcdef",
    "eventID": "12345678-1234-1234-abcd-abcdef1234567",
    "readOnly": true,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "eventCategory": "Management",
    "recipientAccountId": "12345678901234567"
}
```


Para obtener información sobre el contenido de los CloudTrail registros, consulte el contenido de los CloudTrail registros en la Guía del AWS CloudTrail usuario.

Integraciones de productos y servicios con Incident Manager

Incident Manager, una herramienta AWS Systems Manager incluida, se integra con los siguientes productos, servicios y herramientas.

Integración con Servicios de AWS

Incident Manager se integra con Servicios de AWS las herramientas que se describen en la siguiente tabla.

AWS CDK	AWS CDK Se trata de un marco de desarroll o que permite utilizar código para definir la infraestructura de la nube y utilizarlo CloudFormation para el aprovisionamiento. AWS CDK Es compatible con varios lenguajes de programación TypeScript, incluidos, JavaScript PythonJava, y C#/.Net. Para obtener información sobre el uso de AWS CDK Incident Manager, consulte las siguientes secciones de la referencia de la AWS CDK API: • Módulo de @aws-cdk/aws-ssmincidents • Módulo de @aws-cdk/aws-ssmcontacts
Amazon Q Developer en aplicaciones de chat	Amazon Q Developer en aplicaciones de chat permite DevOps a los equipos de desarrollo de software utilizar las salas de chat de los programas de mensajería para monitorear y responder a los eventos operativos en sus Nube de AWS. Al utilizar Amazon Q Developer en aplicacio nes de chat con Incident Manager, puede crear canales de chat que los socorristas puedan utilizar para supervisar y responder a los incidentes. Amazon Q Developer en

	aplicaciones de Slack chat admite salas de chat, Microsoft Teams canales y salas de chat Amazon Chime como canales de chat. Como parte de la creación de un canal de chat, también crea un tema en Amazon Simple Notification Service (Amazon SNS). Amazon SNS es un servicio administrado que realiza la entrega de mensajes de los publicadores a los suscriptores. En los planes de respuesta a incidentes, al asociar un canal de chat que haya creado con el plan, también elige uno o varios temas que haya asociado al canal de chat. Estos temas de SNS se utilizan para enviar notificaciones sobre un incidente a los respondedores del mismo. Para obtener más información, consulte Creación e integración de canales de chat para el personal de respuesta en Incident Manager.
CloudFormation	CloudFormation es un servicio que puede utilizar para crear una plantilla con todos los recursos que necesita para su aplicación y, a continuación, configurar y aprovisionar los recursos por usted. También configurará todas las dependencias, para que pueda centrarse más en su aplicación y menos en administrar los recursos. Para obtener información sobre su uso CloudFormation con Incident Manager, consulte los siguientes temas de la Guía del AWS CloudFormation usuario: • Referencia de tipo de recurso de Incident Manager • Referencia de tipo de recurso de Contactos

Amazon CloudWatch	CloudWatchsupervisa AWS los recursos y las aplicaciones en las que se ejecuta AWS en tiempo real. Puede utilizarlas CloudWatch para recopilar y realizar un seguimiento de las métricas, que son variables que puede medir para sus recursos y aplicaciones. Puede configurar CloudWatch las alarmas para crear incidentes en Incident Manager. CloudWatch trabaja con Systems Manager e Incident Manager para crear un incidente a partir de una plantilla de plan de respuesta cuando una alarma pasa al estado de alarma. Para obtener más información, consulte Creación automática de incidentes mediante CloudWatch alarmas.
Amazon Chime	Amazon Chime es un lugar de trabajo en línea que combina reuniones, chat y llamadas de negocios. Con Amazon Chime puede reunirse, chatear y realizar llamadas de negocios dentro y fuera de su organización. Puede integrar una sala de Amazon Chime en sus operaciones de Incident Manager creando un canal de chat para Amazon Chime en Amazon Q Developer en aplicaciones de chat y, a continuación, añadiendo ese canal a un plan de respuesta. Para obtener más información, consulte Creación e integración de canales de chat para el personal de respuesta en Incident Manager.

Amazon EventBridge	EventBridgees un servicio sin servidor que utiliza eventos para conectar los componentes de la aplicación, lo que le facilita la creación de aplicaciones escalables basadas en eventos. Puede configurar EventBridge reglas para detectar los patrones de eventos en sus AWS recursos y crear un incidente en Incident Manager cuando un evento coincida con un patrón que haya definido. Sus reglas pueden monitorear los patrones de eventos en docenas de aplicaciones Servicios de AWS y servicios de terceros y de terceros. Para obtener más información, consulte Crear incidentes automáticamente con EventBridge eventos.
AWS Secrets Manager	Secrets Manager le ayuda a administrar, recuperar y rotar las credenciales de las bases de datos, las credenciales de las aplicaciones, OAuth los tokens, las claves de API y otros secretos a lo largo de sus ciclos de vida. Al integrar Incident Manager con el PagerDuty servicio, crea un secreto en Secrets Manager que contiene sus PagerDuty credenciales. Para obtener más información, consulte Almacenar las credenciales de acceso en secreto PagerDuty AWS Secrets Manager.

AWS Systems Manager	Systems Manager es un centro de operaciones que puede usar para ver y controlar la infraestructura de aplicaciones y una solución de end-to-end administración segura para entornos de nube. Las siguientes herramientas de Systems Manager se integran directamente con Incident Manager: • Automatización: un manual de procedimientos de automatización define las acciones que Systems Manager realiza en sus recursos de AWS . En Incident Manager, un manual de procedimientos define una serie de pasos automatizados y manuales para resolver sus incidentes. Para obtener información sobre la creación de manuales de procedimientos de automatización para su uso con Incident Manager, consulte Integración de los manuales de automatización de Systems Manager en Incident Manager para la solución de incidentes. • OpsCenter— OpsCenter proporciona una ubicación central donde los ingenieros de operaciones y los profesionales de TI pueden gestionar las tareas operativas, denominadas OpsItems, relacionadas con AWS los recursos. Puede crear OpsItems directamente a partir de un análisis posterior al incidente para realizar un seguimiento del trabajo relacionado. Para obtener más información, consulte Realización de un análisis post-incidente en Incident Manager.

AWS Trusted Advisor	Trusted Advisores una herramienta disponible para AWS los clientes con un plan de soporte básico o para desarrolladores. Trusted Advisor inspecciona su AWS entorno y, a continuac ión, hace recomendaciones cuando existen oportunidades para ahorrar dinero, mejorar la disponibilidad y el rendimiento del sistema o ayudar a cerrar las brechas de seguridad. En el caso de Incident Manager, Trusted Advisor comprueba que la configuración de un conjunto de replicación utilice más de uno Región de AWS para admitir la conmutación por error y la respuesta regionales.

Integración a otros productos y servicios

Puede integrar o utilizar Incident Manager con los servicios de terceros que se describen en la siguiente tabla.

Jira Cloud	Con él AWS Service Management Connector , puedes integrar Incident Manager con Jira Cloud (Atlassian), una plataforma de flujo de trabajo de terceros basada en la nube. Después de configurar la integración con Jira Cloud, al crear un nuevo incidente en Incident Manager, la integración crea también el incidente en Jira Cloud. Si actualiza un incidente en Incident Manager, realiza estas actualizaciones en el incidente correspondiente en Jira Cloud. Si resuelve un incidente en Incident Manager o en Jira Cloud, la integraci ón resuelve el incidente en ambos servicios en función de las preferencias que configure.

	Para obtener más información, consulta Integración Administrador de incidentes de AWS Systems Manager (Jira Cloud) en la Guía del administrador.AWS Service Management Connector
Administración de servicios de Jira	Con ella AWS Service Management Connector , puedes integrar Incident Manager con Jira Service Management, una plataforma de flujo de trabajo de terceros basada en la nube. Después de configurar la integración con el Administrador de servicios de Jira, al crear un nuevo incidente en Incident Manager, la integración crea también el incidente en el Administrador de servicios de Jira. Si actualiza un incidente en Incident Manager, realiza estas actualizaciones en el incidente correspondiente en el Administrador de servicios de Jira. Si resuelve un incidente en Incident Manager o en el Administrador de servicios de Jira, la integración resuelve el incidente en ambos servicios en función de las preferencias que configure. Para obtener más información, consulte Configuración del administrador de servicios de Jira en la Guía del administrador de AWS Service Management Connector .

Microsoft Teams	Microsoft Teams proporciona herramientas de colaboración basadas en la nube para mensajería en equipo, audioconferencias y videoconferencias, y uso compartido de archivos. Para integrar un Microsoft Teams canal en las operaciones de Incident Manager, cree un canal de chat para Amazon Q Developer Microsoft Team en las aplicaciones de chat y, a continuación, añada ese canal a un plan de respuesta. Para obtener más información, consulte Creación e integración de canales de chat para el personal de respuesta en Incident Manager.

PagerDuty	PagerDutyes una herramienta de respuesta a incidentes que admite los flujos de trabajo de paginación y las políticas de escalamiento. Al integrar Incident Manager con PagerDuty, puede añadir un PagerDuty servicio a su plan de respuesta. Después, se crea el incidente correspondiente en PagerDuty cada vez que se crea un incidente en Incident Manager. El incidente PagerDuty utiliza el flujo de trabajo de paginación y las políticas de escalamiento que usted definió allí, además de las de Incident Manager. PagerDutyadjunta los eventos de la cronología de Incident Manager como notas sobre el incidente. Para integrar Incident Manager PagerDuty, primero debe crear un identificador secreto AWS Secrets Manager que contenga sus PagerDuty credenciales. Para obtener información sobre cómo añadir una clave de API PagerDuty REST y otros detalles necesarios a una entrada secreta AWS Secrets Manager, consulteAlmacenar las credenciales de acceso en secreto PagerDuty AWS Secrets Manager. Para obtener información sobre cómo agregar un PagerDuty servicio de su PagerDuty cuenta a un plan de respuesta en Incident Manager, consulte los pasos para integrar un PagerDuty servicio en el plan de respuesta en el temaCreación de un plan de respuesta.

ServiceNow	Con él AWS Service Management Connector, puede integrar Incident Manager con ServiceNowuna plataforma de flujo de trabajo de terceros basada en la nube. Después de configurar la integración con ServiceNow, al crear un nuevo incidente en Incident Manager, la integración ServiceNow también crea el incidente. Si actualiza un incidente en Incident Manager, este realizará estas actualizaciones en el incidente correspondiente ServiceNow. Si resuelve un incidente en Incident Manager o ServiceNow, la integración resuelve el incidente en ambos servicios en función de las preferencias que configure. Para obtener más información, consulte Integración Administrador de incidentes de AWS Systems Manager ServiceNow en la Guía AWS Service Management Connector del administrador.
Slack	Slack proporciona herramientas de colaboración basadas en la nube para mensajería en equipo, audioconferencias y videoconferencias, y uso compartido de archivos. Para integrar un Slack canal en las operaciones de Incident Manager, cree un canal de chat para Amazon Q Developer Slack en las aplicaciones de chat y, a continuación, añada ese canal a un plan de respuesta. Para obtener más información, consulte Creación e integración de canales de chat para el personal de respuesta en Incident Manager.

Terraform	HashiCorp Terraform es una herramienta de software de infraestructura como código (IaC) de código abierto que proporciona un flujo de trabajo de interfaz de la línea de comandos (CLI) para administrar varios servicios en la nube. En el caso de Incident Manager, puede utilizar Terraform para administrar o aprovisionar lo siguiente: Recursos de contactos de SSM Incident Manager • aws_ssmcontacts_contact • aws_ssmcontacts_contact_channel • aws_ssmcontacts_plan • aws_ssmcontacts_rotation Fuentes de datos de contactos SSM • aws_ssmcontacts_contact • aws_ssmcontacts_contact_channel • aws_ssmcontacts_plan • aws_ssmcontacts_rotation Recursos de Incident Manager de SSM • aws_ssmincidents_replication_set • aws_ssmincidents_response_plan Orígenes de datos de Incident Manager de SSM • aws_ssmincidents_replication_set • aws_ssmincidents_response_plan

Almacenar las credenciales de acceso en secreto PagerDuty AWS Secrets Manager

Tras activar la integración con un plan PagerDuty de respuesta, Incident Manager trabaja con él PagerDuty de las siguientes maneras:

- Incident Manager crea el incidente correspondiente PagerDuty cuando se crea un nuevo incidente en Incident Manager.
- El flujo de trabajo de paginación y las políticas de escalamiento que creó se PagerDuty utilizan en el PagerDuty entorno. Sin embargo, Incident Manager no importa la PagerDuty configuración.
- Incident Manager publica los eventos de la cronología como notas del incidente PagerDuty, con un máximo de 2000 notas.
- Puede optar por resolver automáticamente PagerDuty los incidentes al resolver el incidente relacionado en Incident Manager.

Para integrar Incident Manager con PagerDuty, primero debe crear una entrada secreta AWS Secrets Manager que contenga sus PagerDuty credenciales. Estas permiten a Incident Manager comunicarse con su PagerDuty servicio. A continuación, puede incluir un PagerDuty servicio en los planes de respuesta que cree en Incident Manager.

Este secreto que crea en el Administrador de secretos debe contener, en el formato JSON apropiado, lo siguiente:

- Una clave de API de su PagerDuty cuenta. Puede utilizar una clave API de REST de acceso general o una clave API de REST de token de usuario.
- Una dirección de correo electrónico de usuario válida de tu PagerDuty subdominio.
- La región PagerDuty de servicio en la que implementaste tu subdominio.

> **Note**
>
> Todos los servicios de un PagerDuty subdominio se implementan en la misma región de servicio.

Requisitos previos

Antes de crear el secreto en el Administrador de secretos, asegúrese de satisfacer los siguientes requisitos.

Clave de KMS

Debe cifrar el secreto que cree con una clave gestionada por el cliente que haya creado en AWS Key Management Service ()AWS KMS. Debe especificar esta clave al crear el secreto que almacena PagerDuty sus credenciales.

> **Important**
>
> Secrets Manager ofrece la opción de cifrar el secreto con un Clave administrada de AWS, pero este modo de cifrado no es compatible.

La clave administrada por el cliente debe cumplir los siguientes requisitos:

- Tipo de clave: elija Simétrica.
- Uso de la clave: elija Cifrado y descifrado.
- Regionalidad: si desea replicar su plan de respuesta en varias Regiones de AWS, asegúrese de seleccionar la clave multirregional.

Política de claves

El usuario que configure el plan de respuesta debe tener permiso para `kms:GenerateDataKey` y `kms:Decrypt` en la política basada en recursos de la clave. La entidad principal del servicio `ssm-incidents.amazonaws.com` debe tener permiso para `kms:GenerateDataKey` y `kms:Decrypt` en la política basada en recursos de la clave.

La siguiente política demuestra estos permisos. Reemplace cada *`user input placeholder`* por su propia información.

JSON

```
{
    "Version":"2012-10-17",
    "Id": "key-consolepolicy-3",
    "Statement": [
```

```
        {
            "Sid": "Enable IAM user permissions",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::111122223333:root"
            },
            "Action": "kms:*",
            "Resource": "*"
        },
        {
            "Sid": "Allow creator of response plan to use the key",
            "Effect": "Allow",
            "Principal": {
                "AWS": "IAM_ARN_of_principal_creating_response_plan"
            },
            "Action": [
                "kms:Decrypt",
                "kms:GenerateDataKey*"
            ],
            "Resource": "*"
        },
        {
            "Sid": "Allow Incident Manager to use the key",
            "Effect": "Allow",
            "Principal": {
                "Service": "ssm-incidents.amazonaws.com"
            },
            "Action": [
                "kms:Decrypt",
                "kms:GenerateDataKey*"
            ],
            "Resource": "*"
        }
    ]
}
```

Para obtener información sobre la creación de una nueva clave administrada por el cliente, consulte Creación de claves de KMS de cifrado simétricas en la Guía para desarrolladores de AWS Key Management Service . Para obtener más información sobre AWS KMS las claves, consulte AWS KMS los conceptos.

Si una clave administrada por el cliente existente cumple todos los requisitos anteriores, puede editar su política para añadir estos permisos. Para obtener información sobre la actualización de

la política de una clave administrada por el cliente, consulte Modificación de una política de clave en la Guía para desarrolladores de AWS Key Management Service .

> **Tip**
>
> Puede especificar una clave de condición para limitar aún más el acceso. Por ejemplo, la siguiente política permite el acceso a través del Administrador de secretos solo en la región este de EE. UU. (Ohio) (us-east-2):
>
> ```
> {
>     "Sid": "Enable IM Permissions",
>     "Effect": "Allow",
>     "Principal": {
>         "Service": "ssm-incidents.amazonaws.com"
>     },
>     "Action": ["kms:Decrypt", "kms:GenerateDataKey*"],
>     "Resource": "*",
>     "Condition": {
>         "StringEquals": {
>             "kms:ViaService": "secretsmanager.us-east-2.amazonaws.com"
>         }
>     }
> }
> ```

Permiso **`GetSecretValue`**

La identidad de IAM (usuario, rol o grupo) que crea el plan de respuesta debe tener el permiso de IAM `secretsmanager:GetSecretValue`.

Para almacenar las credenciales de PagerDuty acceso en AWS Secrets Manager secreto

1. Siga los pasos del paso 3a de la sección Crear un AWS Secrets Manager secreto de la Guía del AWS Secrets Manager usuario.
2. En el paso 3b, en Pares clave/valor, haga lo siguiente:
   - Elija la pestaña Texto sin formato.
   - Sustituya el contenido predeterminado del cuadro por la siguiente estructura JSON:

     ```
     {
     ```

```
    "pagerDutyToken": "pagerduty-token",
    "pagerDutyServiceRegion": "pagerduty-region",
    "pagerDutyFromEmail": "pagerduty-email"
}
```

- En el ejemplo de JSON que ha pegado, *placeholder values* sustituya el siguiente:
  - *pagerduty-token*: el valor de una clave de API de REST de acceso general o de una clave de API de REST de token de usuario de tu PagerDuty cuenta.

    Para obtener información relacionada, consulte las claves de acceso a las API en la base de PagerDuty conocimientos.
  - *pagerduty-region*: la región de servicio del centro de PagerDuty datos que aloja su PagerDuty subdominio.

    Para obtener información relacionada, consulte las regiones de servicio en la base de PagerDuty conocimientos.
  - *pagerduty-email*: la dirección de correo electrónico válida de un usuario que pertenece a su PagerDuty subdominio.

    Para obtener información relacionada, consulte Administrar usuarios en la base de PagerDuty conocimientos.

  El siguiente ejemplo muestra un secreto JSON completado que contiene las PagerDuty credenciales necesarias:

```
{
    "pagerDutyToken": "y_NbAkKc66ryYEXAMPLE",
    "pagerDutyServiceRegion": "US",
    "pagerDutyFromEmail": "JohnDoe@example.com"
}
```

3. En el paso 3c, en Clave de cifrado, elija una clave administrada por el cliente que haya creado y que cumpla los requisitos enumerados en la sección Requisitos previos anterior.
4. En el paso 4c, en Permisos de recursos, haga lo siguiente:
   - Expanda Permisos de recursos.
   - Elija Editar permisos.

- Sustituya el contenido predeterminado del cuadro de políticas por la siguiente estructura JSON:

```
{
    "Effect": "Allow",
    "Principal": {
        "Service": "ssm-incidents.amazonaws.com"
    },
    "Action": "secretsmanager:GetSecretValue",
    "Resource": "*"
}
```

- Seleccione Save.

5. En el paso 4d, en Replicar secreto, haga lo siguiente si ha replicado su plan de respuesta a más de una Región de AWS:
   - Expanda Replicar secreto.
   - En Región de AWS, seleccione la región a la que replicó su plan de respuesta.
   - En Clave de cifrado, elija una clave administrada por el cliente que haya creado en esta región o haya replicado a la misma y que cumpla los requisitos enumerados en la sección Requisitos previos.
   - Para cada uno de los adicionales Región de AWS, elige Añadir región y selecciona el nombre de la región y la clave gestionada por el cliente.
6. Complete los pasos restantes de Crear un AWS Secrets Manager secreto en la Guía del AWS Secrets Manager usuario.

Para obtener información sobre cómo agregar un PagerDuty servicio al flujo de trabajo de incidentes de Incident Manager, consulte Integrar un PagerDuty servicio en el plan de respuesta en el temaCreación de un plan de respuesta.

Información relacionada

Cómo automatizar la respuesta a los incidentes con PagerDuty y Administrador de incidentes de AWS Systems Manager (blog sobre Nube de AWS operaciones y migraciones)

Cifrado de secretos en AWS Secrets Manager en la Guía del usuario de AWS Secrets Manager

Solución de problemas AWS de Systems Manager Incident Manager

Si tiene problemas al utilizar AWS Systems Manager Incident Manager, puede utilizar la siguiente información para resolverlos de acuerdo con nuestras prácticas recomendadas. Si cualquier problema que encontrase estuviera fuera del ámbito de la siguiente información, o si persistiera después de haber intentado resolverlo, póngase en contacto con AWS Support.

Temas

Mensaje de error: **`ValidationException – We were unable to validate the AWS Secrets Manager secret`**

Problema 1: La identidad AWS Identity and Access Management (de IAM) (usuario, rol o grupo) que crea el plan de respuesta no tiene el permiso de `secretsmanager:GetSecretValue` IAM. Las identidades de IAM deben tener este permiso para validar los secretos de Secrets Manager.

- Solución: Añada el permiso `secretsmanager:GetSecretValue` que falta a la política de IAM para la identidad de IAM que crea el plan de respuesta. Para obtener más información, consulte Adición de permisos de identidad de IAM (consola) o Adición de políticas de IAM (AWS CLI) en la Guía del usuario de IAM.

Problema 2: El secreto no tiene vinculada una política basada en recursos que permita a la identidad de IAM ejecutar la acción `GetSecretValue` o la política basada en recursos deniega el permiso a la identidad.

- Solución: Cree o añada una instrucción `Allow` a la política basada en recursos del secreto que conceda permiso para `secrets:GetSecretValue` a la identidad de IAM. O bien, si utiliza una instrucción `Deny` que incluya la identidad de IAM, actualice la política para que la identidad pueda ejecutar la acción. Para obtener más información, consulte Adjuntar una política de permisos a un AWS Secrets Manager secreto en la Guía del AWS Secrets Manager usuario.

Problema 3: Los secretos no tienen vinculada una política basada en recursos que permita el acceso a la entidad principal del servicio Administración de incidentes: `ssm-incidents.amazonaws.com`.

- Solución: Cree o actualice la política basada en recursos para el secreto e incluya el siguiente permiso:

```
{
    "Effect": "Allow",
    "Principal": {
        "Service": ["ssm-incidents.amazonaws.com"]
    },
    "Action": "secretsmanager:GetSecretValue",
    "Resource": "*"
}
```

Problema 4: La clave AWS KMS key seleccionada para cifrar el secreto no es una clave administrada por el cliente o no proporciona los permisos `kms:Decrypt` de IAM ni al director de servicio de Incident Manager. `kms:GenerateDataKey*` Asimismo, la identidad de IAM que crea el plan de respuesta podría no tener el permiso de IAM `GetSecretValue`.

- Solución: Asegúrese de satisfacer los requisitos descritos en Requisitos previos en el tema Almacenar las credenciales de acceso en secreto PagerDuty AWS Secrets Manager.

Problema 5: El ID del secreto que contiene la clave de la API de REST de acceso general o la clave de la API de REST del token de usuario no es válido.

- Solución: Asegúrese de haber introducido el ID del secreto de Secrets Manager correctamente, sin espacios al final. Debe trabajar en el mismo lugar donde Región de AWS se almacena el secreto que quiere usar. No puede utilizar un secreto eliminado.

Problema 6: En raras ocasiones, el servicio Secrets Manager podría experimentar algún problema, o Administración de incidentes podría tener problemas para comunicar con él.

- Solución: Espere unos minutos y vuelva a intentarlo. Compruebe en Panel de AWS Health cualquier problema que pudiera afectar a cualquiera de los dos servicios.

Otras incidencias en la solución de problemas

Si no ha resuelto el problema con los pasos anteriores, puede encontrar más ayuda en los siguientes recursos:

- Si experimenta problemas de IAM específicos de Administración de incidentes al acceder a la consola de Administración de incidentes, consulte Resolución de problemas Administrador de incidentes de AWS Systems Manager identidad y acceso.
- Para obtener información sobre problemas generales de autenticación y autorización al acceder al Consola de administración de AWS, consulte Solución de problemas de IAM en la Guía del usuario de IAM

Historial de documentos de Incident Manager

Cambio	Descripción	Fecha
Administrador de incidentes de AWS Systems Manager documentos de migración publicados	Incident Manager ha publicado documentos de migración para ayudar a los clientes a comprender algunas de las opciones disponibles para migrar Administrador de incidentes de AWS Systems Manager. Para obtener más información, consulte Cambio en la disponibilidad de Administrador de incidentes de AWS Systems Manager.	21 de noviembre de 2025
Actualización de la política gestionada `AWSIncidentManagerResolverAccess`	Incident Manager ha actualizado la política gestionada `AWSIncidentManagerResolverAccess` para añadir ssm-contacts: StartEngagement permiso para iniciar interacciones con los contactos durante los incidentes. Para obtener más información, consulte Incident Manager actualiza las políticas gestionadas. AWS	20 de noviembre de 2025
Administrador de incidentes de AWS Systems Manager ya no está abierto a nuevos clientes.	Administrador de incidentes de AWS Systems Manager ya no está abierto a nuevos clientes. Los clientes existentes pueden seguir utilizando el servicio con normalidad. Para obtener	7 de noviembre de 2025

	más información, consulte Cambio en la disponibilidad de Administrador de incidentes de AWS Systems Manager.	
Administrador de incidentes de AWS Systems Manager dejará de estar abierto a nuevos clientes a partir del 7 de noviembre de 2025.	Administrador de incidentes de AWS Systems Manager dejará de estar abierto a nuevos clientes a partir del 7 de noviembre de 2025. Si desea utilizar Incident Manager, regístrese antes de esa fecha. Los clientes existentes pueden seguir utilizando el servicio con normalidad. Para obtener más información, consulte Cambio en la disponibilidad de Administrador de incidentes de AWS Systems Manager.	7 de octubre de 2025
Modificación de los requisitos de permiso para crear incidentes manualmente	Los permisos de IAM necesarios para que un usuario cree un incidente manualmente han cambiado y ya no utilizan un rol vinculado a un servicio. En su lugar, Incident Manager ahora utiliza sesiones de acceso directo (FAS) para realizar llamadas `ssm-contacts:StartEngagement` como parte de ellas. `ssm-incidents:StartIncident` Para obtener más información, consulte Permisos de IAM necesarios para iniciar incidentes manualmente.	10 de junio de 2025

Actualización de la política gestionada `AWSServiceRoleforIncidentManagerPolicy`	Incident Manager ha agregado un nuevo permiso `AWSServiceRoleforIncidentManagerPolicy` que le permite a Incident Manager publicar las métricas del espacio de `AWS/Usage` nombres de su cuenta. Para obtener más información, consulte las actualizaciones de Incident Manager a las políticas AWS gestionadas.	28 de enero de 2025
Actualización de la política gestionada `AWSIncidentManagerIncidentAccessServiceRolePolicy`	Incident Manager ha agregado un nuevo permiso`AWSIncidentManagerIncidentAccessServiceRolePolicy` , en apoyo de la función Findings, que le permite comprobar si una instancia EC2 forma parte de un grupo de Auto Scaling. Para obtener más información, consulte las actualizaciones de Incident Manager a las políticas AWS gestionadas.	20 de febrero de 2024

Soporte adicional de HashiCorp Terraform: rotaciones de guardia	Terraform ha ampliado su soporte para Incident Manager. Ahora puede aprovisionar o gestionar los recursos disponibles de Incident Manager con Terraform. Para obtener información sobre esta y otras integraciones de terceros con Incident Manager, consulte Integración con otros productos y servicios.	2 de febrero de 2024

Nueva función: Hallazgos de otros Servicios de AWS	Los resultados le proporcionan información sobre los cambios relacionados con las AWS CloudFormation pilas y AWS CodeDeploy las implementaciones que se produjeron aproximadamente al mismo tiempo que se creó un incidente en Incident Manager. En la consola de Incident Manager, puede ver información resumida sobre esos cambios y, en muchos casos, acceder a los enlaces a la CloudFormation o a las CodeDeploy consolas para obtener información completa sobre el cambio. Los resultados reducen el tiempo necesario para evaluar las posibles causas de los incidentes. También reducen la probabilidad de que los respondedores accedan a la cuenta o consola equivocada para investigar la causa de un incidente. Esta función también introduce una nueva política gestionada `AWSIncidentManagerIncidentAccessServiceRolePolicy`, que permite a Incident Manager leer los recursos de otras fuentes Servicios de AWS para identificar los hallazgos relacionados con	15 de noviembre de 2023

	los incidentes. Para obtener más información, consulte los temas siguientes: • Uso de los resultados • AWS política gestionada: AWSIncidentManagerIncidentAccessServiceRolePolicy	
Listas actualizadas de integraciones con Incident Manager	El tema Integraciones de productos y servicios con Incident Manager se ha ampliado a fin de enumerar y describir todas las herramientas de Servicios de AWS y de terceros que puede integrar con Incident Manager en sus operaciones de detección y respuesta a incidentes.	9 de junio de 2023

Integración con AWS Trusted Advisor	Trusted Advisor ahora comprueba que la configuración de un conjunto de replicación utilice más de uno Región de AWS para admitir la conmutación por error y la respuesta regionales. Para los incidentes creados por CloudWatch alarmas o EventBridge eventos, Incident Manager crea un incidente al Región de AWS igual que la regla de alarma o evento. Si Incident Manager no está disponible temporalmente en esa región, el sistema intenta crear un incidente en otra región dentro del conjunto de replicación. Si el conjunto de replicación incluye solo una región, el sistema no podrá crear un registro de incidentes mientras Incident Manager no esté disponible. Para evitar esta situación, Trusted Advisor informa cuando un conjunto de replicación está configurado para una sola región. Para obtener información sobre el uso de Trusted Advisor, consulte AWS Trusted Advisor en la Guía del usuario de AWS Support .	28 de abril de 2023

Úselo Microsoft Teams como canal de chat en los planes de respuesta	Gracias a la integración con Microsoft Teams un desarroll ador de Amazon Q en las aplicaciones de chat, ahora puede utilizar Microsoft Teams el canal de chat en sus planes de respuesta. Esto se suma a la compatibilidad con los canales Slack de chat de Amazon Chime. Durante un incidente, Incident Manager envía notificaciones de estado directamente a un canal de chat para mantener informado s a todos los responded ores. Los socorristas también pueden comunicarse entre sí y AWS CLI ejecutar comandos relacionados con los incidente s en la Microsoft Teams aplicación para actualizar los incidentes e interactuar con ellos. Para obtener más información, consulte Uso de los canales de chat en Incident Manager.	4 de abril de 2023

Nueva característica: Horarios de guardia	Un horario de guardia en Incident Manager define a quién se notifica al producirs e un incidente que requiera la intervención de un operario. Un horario de guardia consta de una o más rotaciones que usted crea para el horario. Cada rotación puede incluir hasta 30 contactos. Después de crear un horario de guardia, puede incluirlo como una escalada en su plan de escalada. Al producirse un incidente asociado a ese plan de escalada, Incident Manager lo notifica al operador (u operadores) de guardia según el horario. Para obtener más información, consulte Uso de los horarios de guardia en Incident Manager.	28 de marzo de 2023

Impresión de un análisis de incidentes formateado o guardado como PDF	La página de análisis de incidentes ahora incluye un botón Imprimir para generar una versión del análisis en formato de impresión. A través de los destinos de impresión configurados para su dispositivo, puede guardar el análisis del incidente como archivo PDF o enviarlo a una impresora local o de red. Para obtener más informaci ón, consulte Impresión de un análisis de incidentes formateado.	17 de enero de 2023

PagerDuty integración: Incident Manager ahora copia los eventos de la cronología de los incidentes en incidentes PagerDuty	Al activar la integración con un plan PagerDuty de respuesta, Incident Manager añade los eventos cronológicos creados a partir de ese plan al registro de incidentes correspondiente PagerDuty. PagerDuty añade los eventos de la cronología como notas sobre el incidente, hasta un máximo de 2000 notas. Para obtener más información sobre estos cambios, consulte los siguientes temas: • Guarde las credenciales de PagerDuty acceso en AWS Secrets Manager secreto • Integre un PagerDuty servicio en el plan de respuesta	15 de diciembre de 2022
Integración de Incident Manager con CloudWatch métricas.	Ahora puede publicar las métricas relacionadas con los incidentes en. CloudWatch Para obtener más información, consulte Métricas de CloudWatch. Se AWSIncidentManagerServiceRolePolicy ha incluido un permiso adicional que permite a nuestro servicio publicar métricas en tu nombre.	15 de diciembre de 2022

Se han lanzado las notas del incidente y se ha actualizado la pantalla de detalles del incidente.	Con Notas del incidente, puede colaborar y comunicar con otros usuarios que trabajen en un incidente . Además, puede ver los manuales de procedimientos y los estados de participación desde la pantalla Detalles del incidente. Para obtener más información, consulte Detalles del incidente.	16 de noviembre de 2022
Lanzamiento de Notas del incidente y actualización de la pantalla Detalles del incidente	Con Notas del incidente, puede colaborar y comunicar con otros usuarios que trabajen en un incidente . Además, puede ver los manuales de procedimientos y los estados de participación desde la pantalla Detalles del incidente. Para obtener más información, consulte Detalles del incidente.	16 de noviembre de 2022

Integre los planes de PagerDuty escalamiento y los flujos de trabajo de localización en los planes de respuesta de Incident Manager	Ahora puede integrar Incident Manager PagerDuty y añadir un PagerDuty servicio a un plan de respuesta. Tras configurar la integración, Incident Manager puede crear un incidente correspondiente PagerDuty para cada nuevo incidente creado en Incident Manager. PagerDuty utiliza el flujo de trabajo de paginación y las políticas de escalamiento que usted define en el PagerDuty entorno. Para obtener más información, consulte los temas siguientes: • Integraciones de productos y servicios con Incident Manager • Guarde las credenciales de PagerDuty acceso en secreto AWS Secrets Manager • Integre un PagerDuty servicio en el plan de respuesta del tema Creación de un plan de respuesta • Solución de problemas	16 de noviembre de 2022

Soporte de etiquetado para conjuntos de réplica	Ahora puede asignar etiquetas a su conjunto de réplica en Administrador de incidentes de AWS Systems Manager. Esto se suma al soporte existente para asignar etiquetas a los planes de respuesta, los registros de incidentes y los contactos Regiones de AWS especificados en el conjunto de replicación. Para obtener información, consulte los siguientes temas: • Asistente de preparación • Etiquetado de recursos en Incident Manager	2 de noviembre de 2022

Integración de Incident Manager con Atlassian Jira Service Management	Puedes integrar Incident Manager con Jira Service Management mediante el conector de administración de servicios para Jira AWS Service Management. Después de configurar la integración, los nuevos incidentes creados en Incident Manager crean un incidente correspondiente en Jira. Al actualizar un incidente en Incident Manager, las actualizaciones se añaden al incidente correspondiente en Jira. Si resuelve un incidente en Incident Manager o en Jira, también se resuelve el incidente correspondiente, según las preferencias configuradas. Para obtener más información, consulte Configuración de Jira Service Management en la Guía del administrador del conector de administración de servicios de AWS .	6 de octubre de 2022

Soporte de etiquetado mejorado	Incident Manager permite asignar etiquetas a los planes de respuesta, los registros de incidentes y los contactos Regiones de AWS especific ados en el conjunto de réplicas. Incident Manager también admite la asignació n automática de etiquetas a incidentes creados a partir de planes de respuesta. Para obtener más informaci ón, consulte Etiquetado de recursos de Incident Manager.	28 de junio de 2022

Integración de Incident Manager con ServiceNow	Puede integrar Incident Manager ServiceNowmediante el conector de administración de AWS servicios para ServiceNow. Tras configurar la integración, los nuevos incidentes creados en Incident Manager crean el incidente correspondiente en ServiceNow. Si actualiza un incidente en Incident Manager, las actualizaciones se añaden al incidente correspondiente en ServiceNow. Si resuelve un incidente en el Administrador de incidentes o ServiceNow, el incidente correspondiente también se resuelve, según las preferencias configuradas. Para obtener más información, consulte Integrar AWS Systems Manager Incident Manager en ServiceNow.	9 de junio de 2022

Importación de datos de contacto	Al crearse un incidente, Incident Manager puede avisar a los respondedores mediante notificaciones de voz o SMS. Para garantizar que los respondedores vean que la llamada o la notificación por SMS procede de Incident Manager, recomendamos que todos los responded ores descarguen el archivo formato de tarjeta virtual (.vcf) de Incident Manager a la libreta de direcciones de sus dispositivos móviles. Para obtener más información, consulte Importación de datos de contacto a su libreta de direcciones.	18 de mayo de 2022

Múltiples mejoras de características para mejorar la creación y corrección de incidentes	Incident Manager lanzó las siguientes mejoras de características para mejorar la creación y corrección de incidentes: • Crear incidentes automáticamente en otros Regiones de AWS: en el caso de que Incident Manager no esté disponible Región de AWS cuando Amazon CloudWatch o Amazon EventBridge creen un incidente, estos servicios ahora crean automáticamente el incidente en una de las regiones disponibles especificadas en su conjunto de replicaciones. Para obtener más información, consulte Administración de incidentes entre regiones. • Rellene automáticamente los parámetros del manual con los metadatos de los incidentes: ahora puede configurar Incident Manager para recopilar información sobre AWS los recursos derivados de los incidentes. Incident Manager puede entonces rellenar los parámetros del manual de procedimientos con la	17 de mayo de 2022

	información recopilada. Para obtener más información, consulte Tutorial: Uso de manuales de procedimientos de automatización de Systems Manager con Incident Manager. • Recopile automáticamente la información sobre los AWS recursos: cuando el sistema crea un incidente, Incident Manager ahora recopila automáticamente información sobre los AWS recursos involucrados en el incidente. A continuación, Incident Manager añade esta información a la pestaña Elementos relacionados.	
Admisión de múltiples manuales de procedimientos	Incident Manager ahora admite la ejecución de varios manuales de procedimientos durante un incidente para la página de detalles del incidente.	14 de enero de 2022

Incident Manager se lanzó en una nueva versión Regiones de AWS	Incident Manager ya está disponible en estas nuevas regiones: us-west-1, sa-east-1, ap-northeast-2, ap-south-1, ca-central-1, eu-west-2 y eu-west-3. Para obtener más información sobre regiones y cuotas de Incident Manager, consulte la Guía de referencia de Referencia general de AWS.	8 de noviembre de 2021
Reconocimiento de participación en la consola	Ahora puede reconocer las participaciones directamente desde la consola de Incident Manager.	5 de agosto de 2021
Pestaña Propiedades	Incident Manager introdujo una pestaña de propiedades en la página de detalles del incidente, que proporciona más información sobre los incidentes OpsItem, su origen y el análisis posterior al incidente.	3 de agosto de 2021
Lanzamiento de Incident Manager	Incident Manager es una consola de gestión de incidentes diseñada para ayudar a los usuarios a mitigar los incidentes que afectan a sus aplicaciones AWS alojadas y a recuperarse de ellos.	10 de mayo de 2021