aws

Guía para desarrolladores

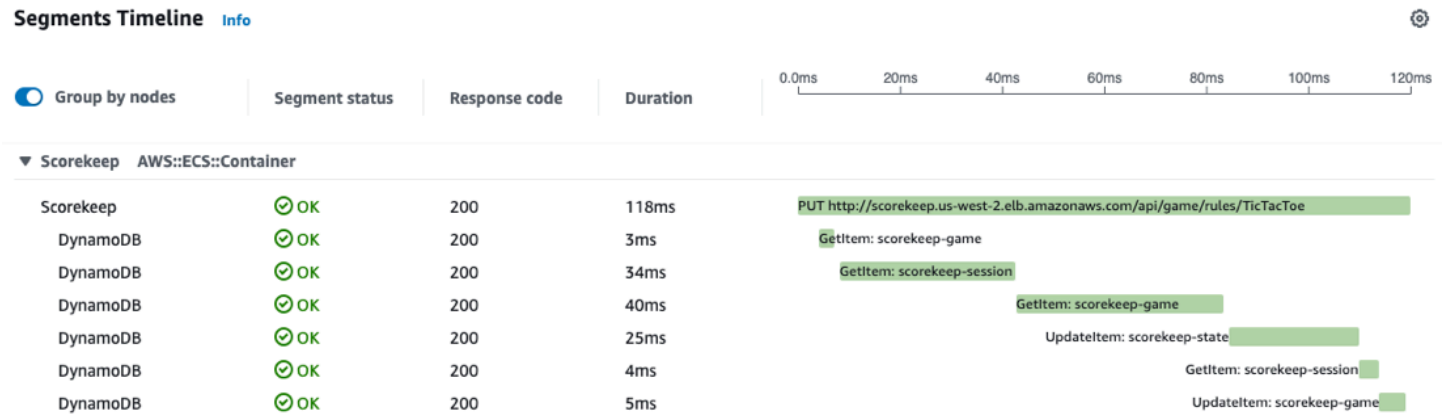
AWS X-Ray

AWS X-Ray: Guía para desarrolladores

Table of Contents

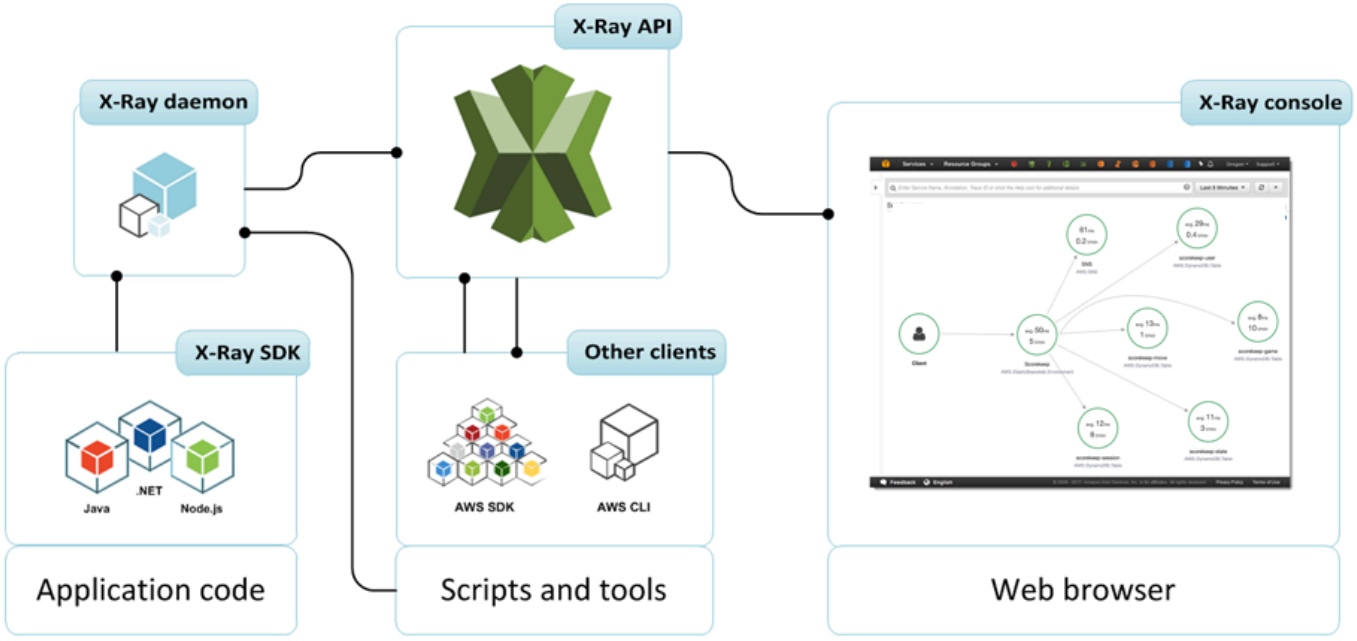
¿Qué es AWS X-Ray?

AWS X-Ray es un servicio que recopila datos sobre las solicitudes que atiende su aplicación y proporciona herramientas que puede utilizar para ver, filtrar y obtener información sobre esos datos a fin de identificar problemas y oportunidades de optimización. En el caso de cualquier solicitud rastreada hasta su aplicación, podrá consultar información detallada no solo sobre la solicitud y la respuesta, sino también sobre las llamadas que la aplicación realiza a AWS los recursos intermedios, los microservicios, las bases de datos y las API web.



AWS X-Ray recibe trazas de su aplicación, además de los usos de Servicios de AWS su aplicación que ya están integrados con X-Ray. La instrumentación de una aplicación implica el envío de datos de rastro para solicitudes entrantes y salientes y otros eventos de la aplicación junto con los metadatos de cada solicitud. Muchos escenarios de instrumentación solo requieren cambios en la configuración. Por ejemplo, puede utilizar todas las solicitudes HTTP entrantes y las llamadas posteriores Servicios de AWS que realice su aplicación Java. Existen varios SDK, agentes y herramientas que puede utilizar para instrumentar su aplicación para rastreo de X-Ray. Para obtener más información, consulte Instrumentación de su aplicación.

Servicios de AWS que están integrados con X-Ray pueden añadir encabezados de rastreo a las solicitudes entrantes, enviar datos de rastreo a X-Ray o ejecutar el daemon X-Ray. Por ejemplo, AWS Lambda puede enviar datos de rastreo sobre las solicitudes a sus funciones de Lambda y ejecutar el daemon X-Ray en los trabajadores para facilitar el uso del SDK de X-Ray.



En lugar de enviar los datos de rastro directamente a X-Ray, cada SDK cliente envía documentos de segmento JSON a un proceso del daemon que escucha el tráfico UDP. El daemon de X-Ray almacena en búfer segmentos en una cola y los carga en X-Ray en lotes. El daemon está disponible para Linux, Windows y macOS, y se incluye en AWS Lambda las plataformas AWS Elastic Beanstalk y.

X-Ray utiliza los datos de rastreo de los AWS recursos que impulsan sus aplicaciones en la nube para generar un mapa de rastreo detallado. El mapa de rastreo muestra el cliente, su servicio de front-end y los servicios de backend a los que recurre su servicio de front-end para procesar las solicitudes y conservar los datos. Utilice el mapa de rastreo para identificar los cuellos de botella, los picos de latencia y otros problemas que debe resolver para mejorar el rendimiento de sus aplicaciones.

Introducción a X-Ray

Para empezar AWS X-Ray:

- Inicie una aplicación de muestra que ya haya sido instrumentada para generar datos de rastro. En unos minutos, puede iniciar la aplicación de muestra, generar tráfico, enviar segmentos a X-Ray y ver un mapa de rastreo y los rastros en el AWS Management Console.
- Aprenda a instrumentar su aplicación, incluido el uso de los SDK de X-Ray o la AWS Distro para enviar datos de rastreo OpenTelemetry a X-Ray.
- Explore otros Servicios de AWS que están integrados en X-Ray, como el muestreo y la adición de encabezados a solicitudes entrantes, la ejecución del daemon X-Ray y el envío automático de datos de rastro a X-Ray.
- Utilice la API de X-Ray, que proporciona acceso a todas las funciones de X-Ray a través del AWS SDK o directamente a través de HTTPS. AWS Command Line Interface

AWS X-Ray conceptos

AWS X-Ray recibe datos de los servicios como segmentos. A continuación, X-Ray agrupa los segmentos que tienen una solicitud en común en rastros. X-Ray procesa los rastros para generar un gráfico de servicios, que constituye una representación visual de la aplicación.

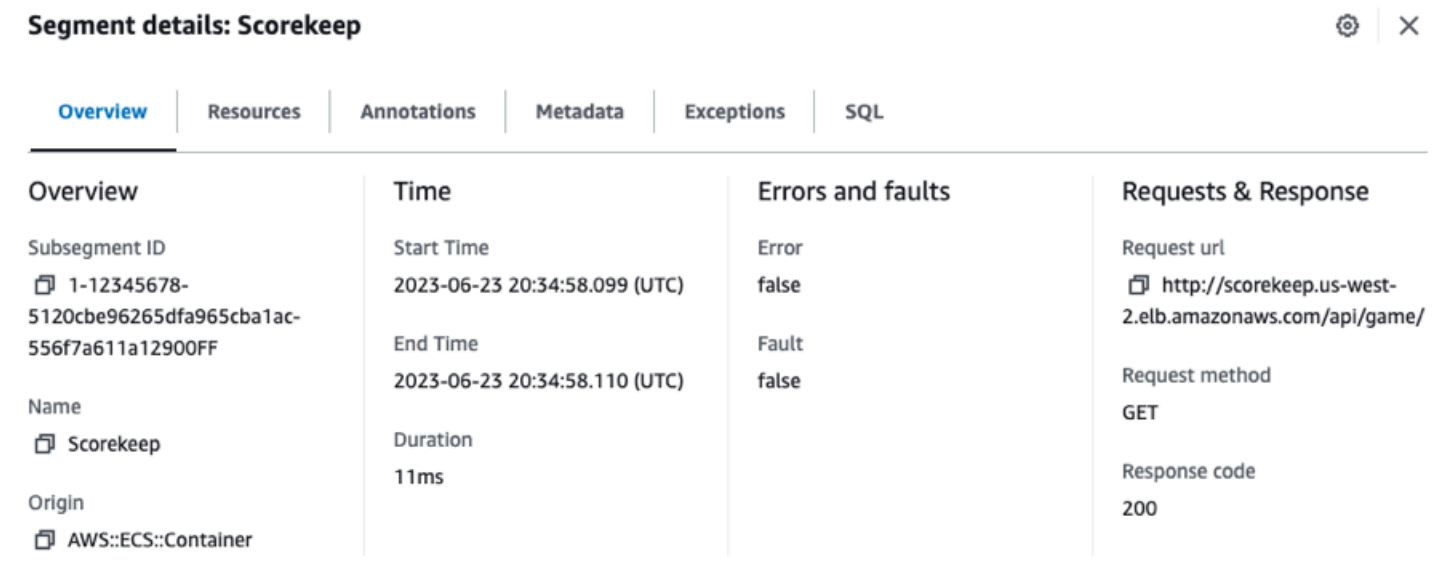
Conceptos

- Segmentos
- Subsegmentos
- Gráfico de servicios
- Rastros
- Muestreo
- Encabezado de seguimiento
- Expresiones de filtro
- Grupos
- Anotaciones y metadatos
- Errores y excepciones

Segmentos

Los recursos informáticos en los que se ejecuta la lógica de su aplicación envían datos del trabajo en forma de segmentos. Un segmento incluye el nombre del recurso, detalles de la solicitud y detalles del trabajo realizado. Por ejemplo, cuando una solicitud HTTP llega a la aplicación, puede registrar datos sobre:

- El host nombre de host, alias o dirección IP
- La solicitud: método, dirección del cliente, ruta y agente de usuario
- La respuesta: estado y contenido
- El trabajo realizado: hora de inicio y finalización y subsegmentos
- Problemas que se producen: errores, fallos y excepciones, incluida la captura automática de pilas de excepciones.



El SDK de X-Ray recopila información de los encabezados de solicitud y respuesta, el código de la aplicación y los metadatos sobre los AWS recursos en los que se ejecuta. Usted elige los datos que desea recopilar modificando la configuración o el código de la aplicación para gestionar las solicitudes entrantes, las solicitudes posteriores y AWS los clientes del SDK.

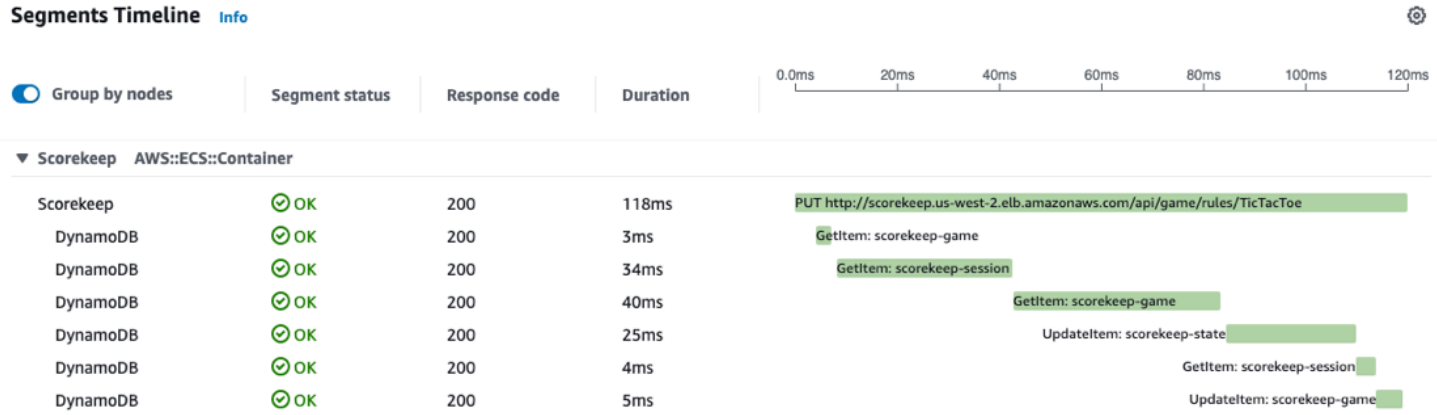
> **Solicitudes reenviadas**
>
> Si un equilibrador de carga u otro intermediario reenvía una solicitud a la aplicación, X-Ray toma la IP de cliente del encabezado `X-Forwarded-For` de la solicitud en lugar de tomar la IP de origen del paquete IP. La IP de cliente que se graba para una solicitud reenviada puede estar falsificada, por lo que no se debe confiar en ella.

Puede utilizar el SDK de X-Ray para registrar información adicional como, por ejemplo, anotaciones y metadatos. Para obtener más información sobre la estructura y la información que se registra en los segmentos y subsegmentos, consulte AWS X-Ray segmentar documentos. Los documentos de segmento pueden tener un tamaño de hasta 64 kB.

Subsegmentos

Un segmento puede desglosar los datos del trabajo realizado en subsegmentos. Los subsegments proporcionan información y detalles más precisos sobre los intervalos de las llamadas posteriores que la aplicación realizó para cumplir la solicitud original. Un subsegmento puede contener detalles adicionales sobre una llamada a una Servicio de AWS API HTTP externa o a una base de datos

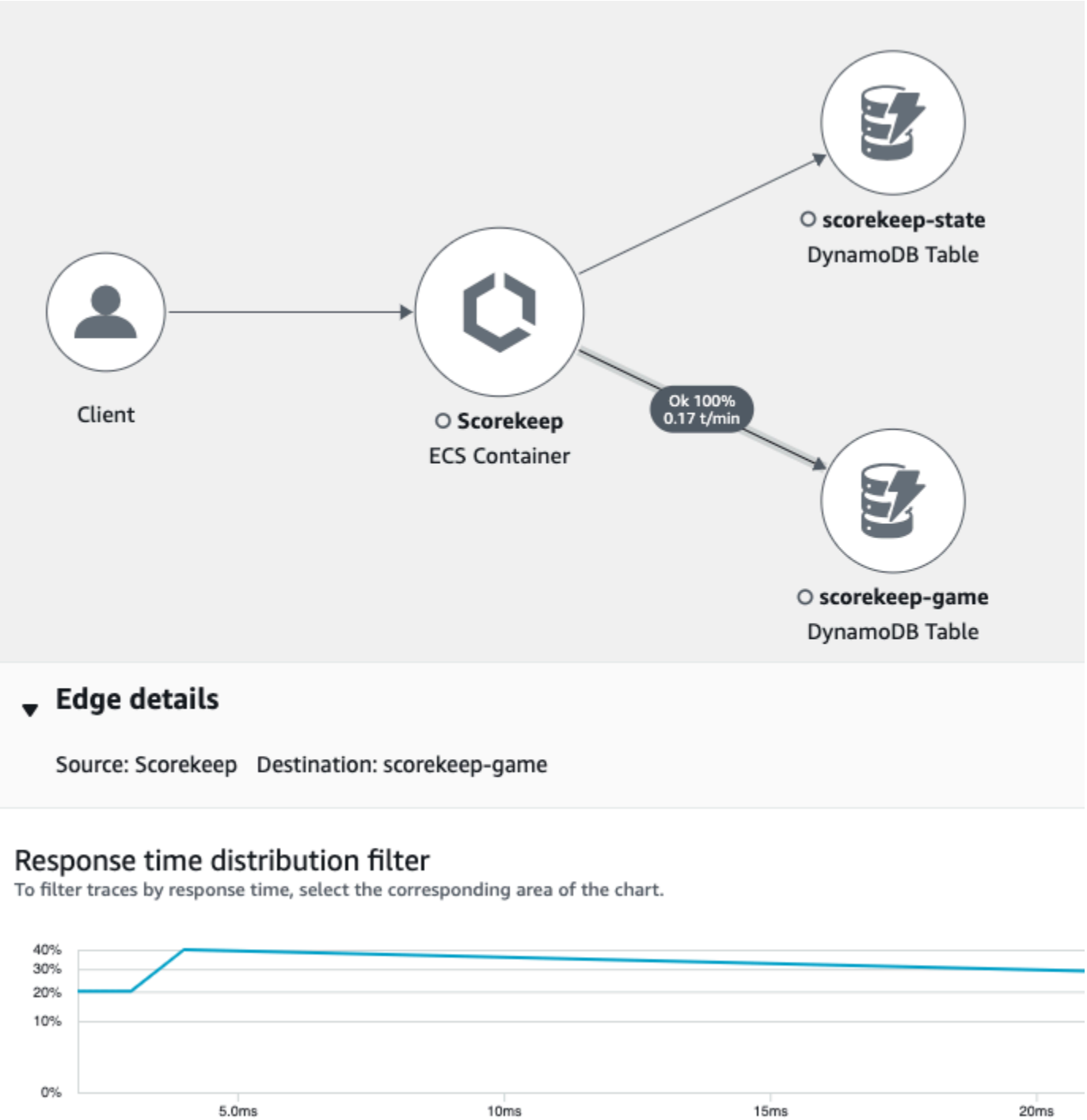
SQL. Puede incluso definir subsegmentos arbitrarios para instrumentar funciones específicas o líneas de código en su aplicación.



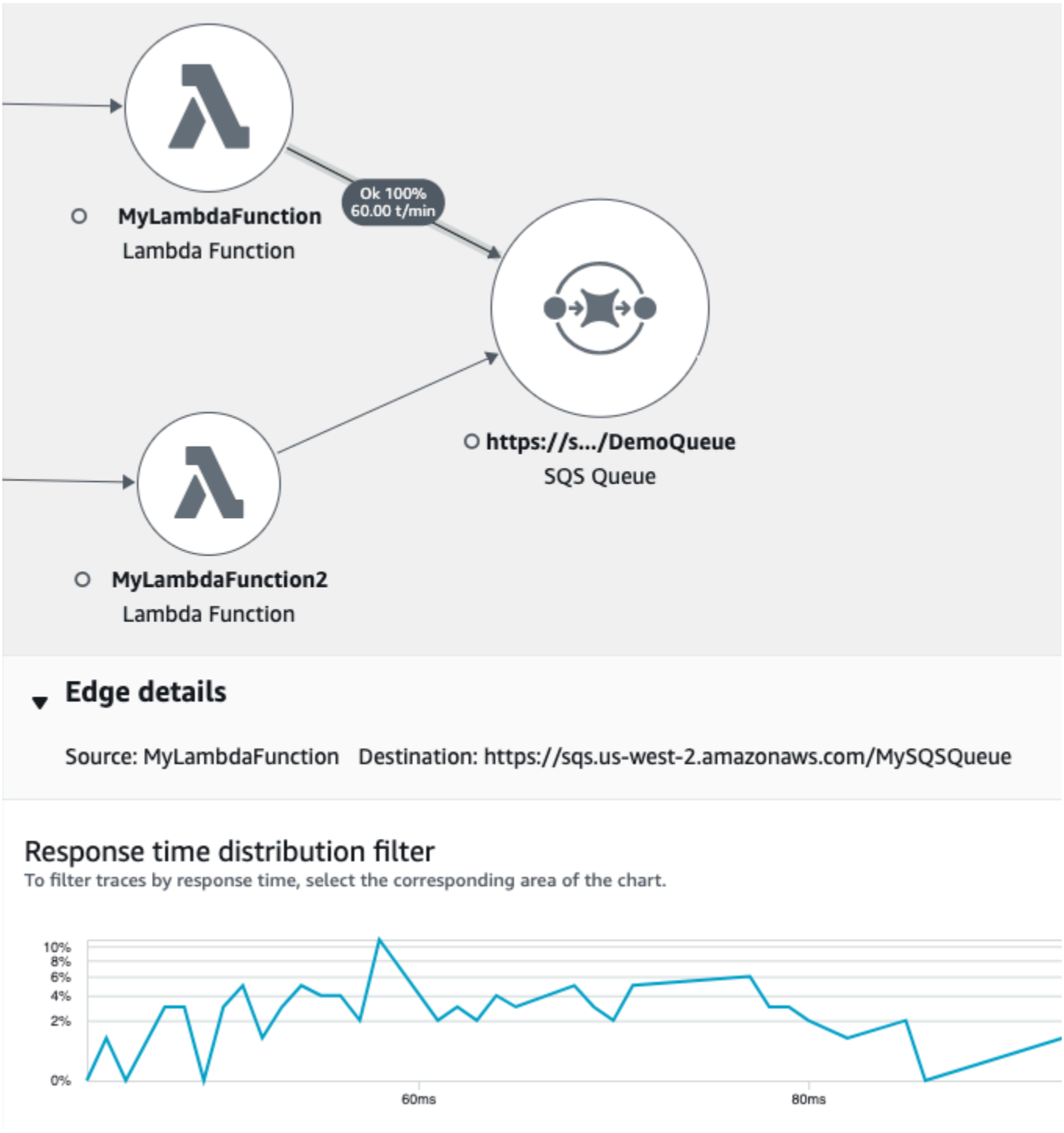
En el caso de los servicios que no envían sus propios segmentos, como Amazon DynamoDB, X-Ray utiliza subsegmentos para generar segmentos inferidos y nodos descendentes en el mapa de rastreo. Esto le permite ver todas sus dependencias posteriores, incluso si no soportan el rastreo o son externas.

Los subsegmentos representan la vista de su aplicación de una llamada posterior como cliente. Si el servicio posterior también está instrumentado, el segmento que envía sustituye al segmento inferido generado desde el subsegmento del cliente principal. El nodo en el gráfico de servicio utiliza siempre información desde el segmento del servicio, si está disponible, mientras que el límite entre los dos nodos utiliza el subsegmento del servicio ascendente.

Por ejemplo, cuando se llama a DynamoDB con un cliente de SDK AWS instrumentado, el SDK de X-Ray graba un subsegmento para esa llamada. DynamoDB no envía un segmento, por lo que el segmento inferido en el rastro, el nodo de DynamoDB en el gráfico de servicio y el borde entre su servicio y DynamoDB contienen información del subsegmento.



Si llama a otro servicio instrumentado con una aplicación instrumentada, el servicio posterior envía su propio segmento para registrar su vista de la misma llamada que el servicio ascendente registró en un subsegmento. En el gráfico de servicio, los nodos de ambos servicios contienen información de tiempo y error de los segmentos de dichos servicios, mientras que el límite entre ellos contiene información del subsegmento del servicio ascendente.



Ambos puntos de vista son útiles, ya que el servicio posterior registra precisamente cuándo comenzó y finalizó el trabajo en la solicitud y el servicio ascendente registra la latencia de ida y vuelta, incluido el tiempo que la solicitud ha pasado viajando entre los dos servicios.

Gráfico de servicios

X-Ray utiliza los datos que su aplicación envía para generar un gráfico de servicios. Cada AWS recurso que envía datos a X-Ray aparece como un servicio en el gráfico. Los límites conectan los servicios que trabajan en equipo para atender solicitudes. Los límites conectan a los clientes con la aplicación, y conectan la aplicación con los servicios y recursos posteriores que esta utiliza.

> **Nombres de servicio**
>
> El `name` de un segmento debe coincidir con el nombre de dominio o el nombre lógico del servicio que genere el segmento. Sin embargo, este requisito no se exige. Cualquier aplicación que tenga permiso para `PutTraceSegments` puede enviar segmentos con cualquier nombre.

Un gráfico de servicios es un documento JSON que contiene información acerca de los servicios y recursos que componen la aplicación. La consola de X-Ray utiliza el gráfico de servicios para generar una visualización o un mapa de servicio.

En las aplicaciones distribuidas, X-Ray combina nodos de todos los servicios que procesan solicitudes con el mismo ID de rastro en un único gráfico de servicios. El primer servicio al que llega la solicitud añade un encabezado de rastro que se propaga entre el front-end y servicios que a los llama.

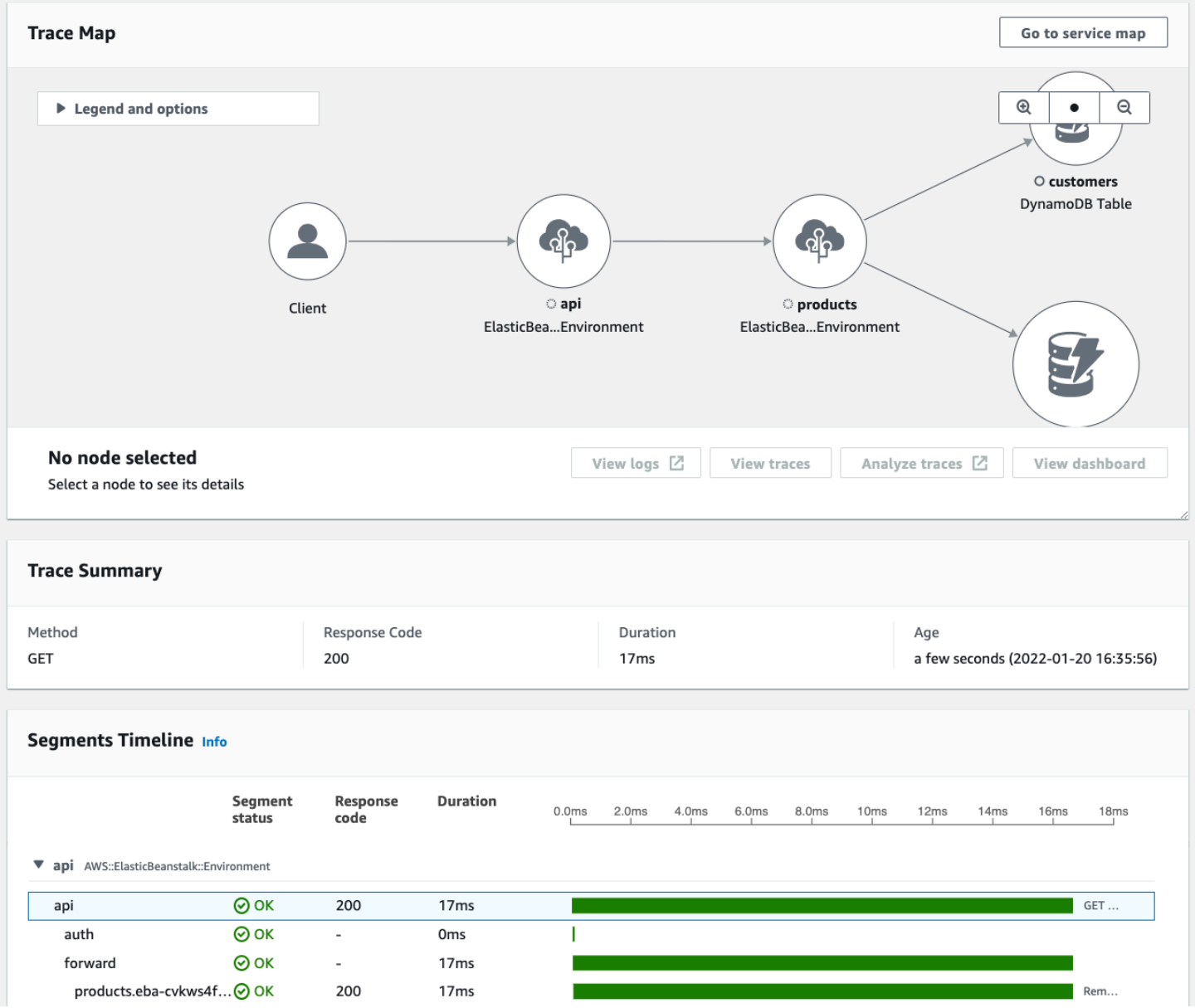
Por ejemplo, Scorekeep ejecuta una API web que llama a un microservicio (una función de AWS Lambda) para generar un nombre aleatorio usando una biblioteca Node.js. El SDK de X-Ray para Java genera el ID de rastro y lo incluye en las llamadas a Lambda. Lambda envía datos de rastreo y transfiere el ID de rastro a la función. El SDK de X-Ray para Node.js también utiliza el ID de rastro para enviar datos. Como resultado, los nodos de la API, el servicio Lambda y la función Lambda aparecen todos como nodos separados, pero conectados, en el mapa de rastreo.

Los datos del gráfico de servicio se conservan durante 30 días.

Rastros

El ID de rastro muestra la ruta que recorre una solicitud en la aplicación. Un registro de seguimiento recopila todos los segmentos que genera una solicitud. La solicitud suele ser una solicitud GET o

una solicitud POST de HTTP que viaja a través de un equilibrador de carga, llega a su código de aplicación y genera llamadas posteriores a otros servicios de AWS o API web externas. El primer servicio compatible con el que interactúa la solicitud HTTP le añade un encabezado de ID de rastro, que continúa propagándose para registrar la latencia, la disposición y otros datos que requiere la solicitud.



Consulte Precios de AWS X-Ray para obtener información sobre cómo se facturan los rastros de X-Ray. Los datos de rastro se conservan durante 30 días.

Muestreo

Para garantizar un rastreo eficaz y proporcionar una muestra representativa de las solicitudes que su aplicación atiende, el SDK de X-Ray aplica un algoritmo de muestreo para determinar qué solicitudes se rastrearán. De forma predeterminada, el SDK de X-Ray registra la primera solicitud cada segundo y el 5 % de las solicitudes adicionales.

Para evitar incurrir en cargos por servicio al empezar, la tasa de muestreo predeterminada es conservadora. Puede configurar X-Ray para modificar la regla de muestreo predeterminada y configurar reglas adicionales que aplican el muestreo en función de las propiedades del servicio o solicitud.

Por ejemplo, es posible que desee deshabilitar las solicitudes de muestreo y rastreo completo para las llamadas que modifican el estado o tratar con usuarios o transacciones. Para llamadas de solo lectura de alto volumen, como sondeo en segundo plano, comprobaciones de estado o mantenimiento de conexión, puede muestrear con un bajo índice y seguirá obteniendo datos suficientes para ver los problemas que surjan.

Para obtener más información, consulte Configuración de reglas de muestreo de .

Encabezado de seguimiento

Todas las solicitudes se rastrean hasta alcanzar un mínimo configurable, después de lo cual se rastrea un porcentaje de solicitudes para evitar un costo innecesario. La decisión de muestreo y el ID de rastro se añaden a las solicitudes HTTP en los encabezados de rastreo denominados `X-Amzn-Trace-Id`. El primer servicio integrado en X-Ray, al que llega la solicitud añade un identificador de rastreo, que es leído por el SDK de X-Ray, e incluido en la respuesta.

Example Encabezado de rastreo con ID de rastro raíz y decisión de muestreo

```
X-Amzn-Trace-Id: Root=1-5759e988-bd862e3fe1be46a994272793;Sampled=1
```

> **Seguridad del encabezado de rastreo**
>
> Un encabezado de rastreo puede provenir del SDK de X-Ray, de una Servicio de AWS o de la solicitud del cliente. Su aplicación puede eliminar el encabezado `X-Amzn-Trace-Id` en las solicitudes entrantes para evitar los problemas causados por usuarios que agregan ID de rastro o decisiones de muestreo a sus solicitudes.

El encabezado de rastreo también pueden contener un ID de segmento primario si la solicitud se originó a partir de una aplicación instrumentada. Por ejemplo, si su aplicación llama a una API web HTTP posterior con un cliente HTTP instrumentado, el SDK de X-Ray añade el ID del segmento de la solicitud original al encabezado de rastreo de la solicitud posterior. Una aplicación instrumentada que atiende la solicitud posterior puede registrar el ID del segmento primario para conectar ambas solicitudes.

Example Encabezado de rastreo con ID de rastro raíz, ID de segmento primario y decisión de muestreo

```
X-Amzn-Trace-Id: Root=1-5759e988-
bd862e3fe1be46a994272793;Parent=53995c3f42cd8ad8;Sampled=1
```

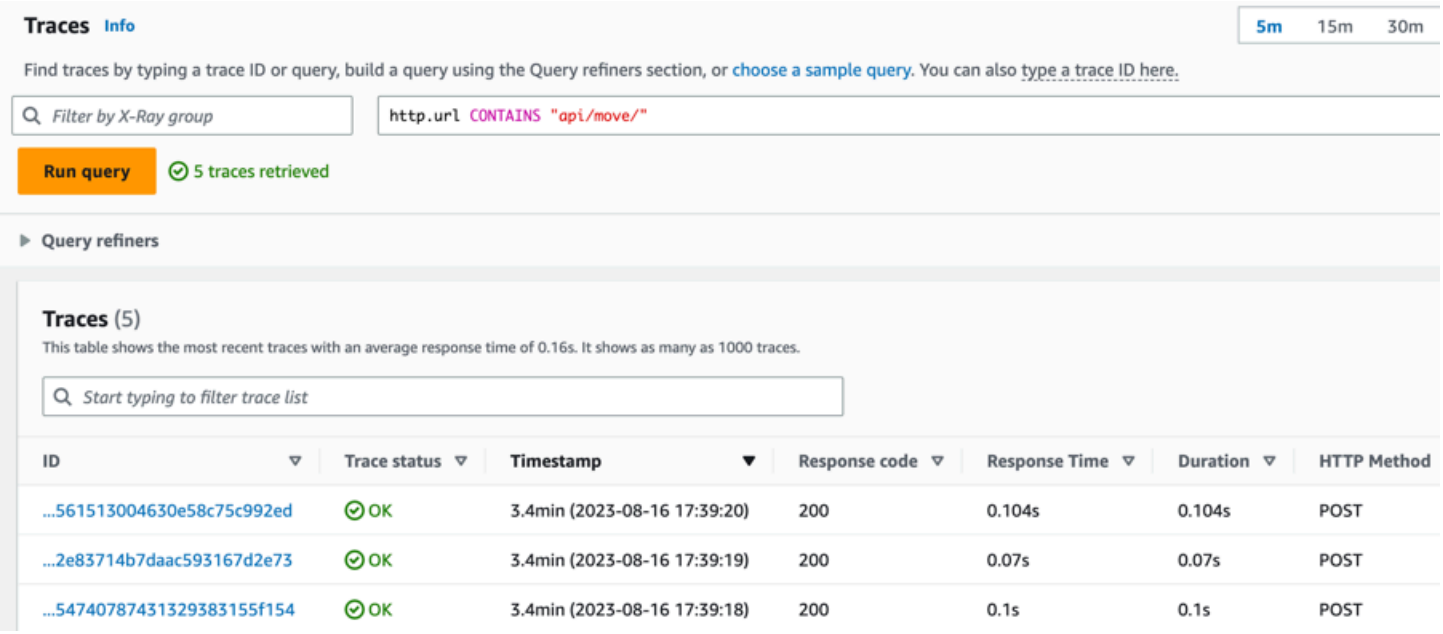
`Lineage`Lambda y Servicios de AWS otros pueden adjuntar al encabezado de seguimiento como parte de sus mecanismos de procesamiento y no deben usarse directamente.

Example Encabezado de rastreo con Lineage

```
X-Amzn-Trace-Id: Root=1-5759e988-bd862e3fe1be46a994272793;Sampled=1;Lineage=a87bd80c:1|
68fd508a:5|c512fbe3:2
```

Expresiones de filtro

Aunque se haya realizado un muestreo, una aplicación genera grandes cantidades de datos. La AWS X-Ray consola proporciona una easy-to-navigate vista del gráfico del servicio. Allí se muestra información sobre el estado y el rendimiento con la cual se puede identificar problemas y posibilidades de optimización en su aplicación. Cuando se realiza un rastreo avanzado, puede explorar en profundidad en busca de solicitudes individuales, o bien utilizar expresiones de filtro para encontrar rastros relacionados con rutas específicas o usuarios específicos.



Grupos

Como complemento de las expresiones de filtro, X-Ray también admite la característica de grupos. Mediante una expresión de filtro, puede definir los criterios para aceptar los rastros en el grupo.

Puede llamar al grupo por su nombre o por el nombre del recurso de Amazon (ARN) para generar su propio gráfico de servicios, resúmenes de seguimiento y métricas de Amazon. CloudWatch Una vez que se crea un grupo, los rastros de entrada se comparan con la expresión de filtro del grupo a medida que se almacenan en el servicio de X-Ray. Las métricas del número de rastreos que coinciden con cada criterio se publican CloudWatch cada minuto.

La actualización de la expresión de filtro de un grupo no cambia los datos que ya se han registrado. La actualización se aplica únicamente a los rastros posteriores. Esto puede dar lugar a un gráfico que combina la expresión nueva con la anterior. Para evitarlo, elimine el grupo actual y cree uno nuevo.

> **Note**
>
> Los grupos se facturan por el número de rastros recuperados que coinciden con la expresión de filtro. Para más información, consulte Precios de AWS X-Ray.

Para obtener más información acerca de los grupos, consulte Configuración de grupos.

Anotaciones y metadatos

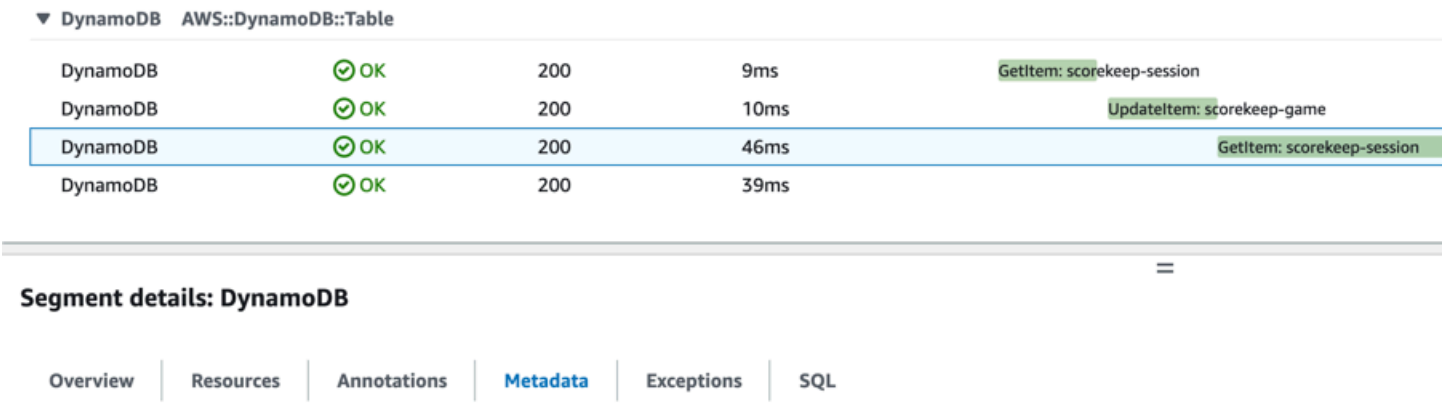
Al instrumentar la aplicación, el SDK de X-Ray registra información sobre las solicitudes entrantes y salientes, los AWS recursos utilizados y la propia aplicación. Puede añadir más información al documento de segmento, por ejemplo anotaciones y metadatos. Las anotaciones y los metadatos se agregan en el nivel de seguimiento y se pueden añadir a cualquier segmento o subsegmento.

Las anotaciones son pares de clave-valor que se indexan para usarlos en expresiones de filtro. Utilice anotaciones para registrar los datos que desee utilizar para agrupar rastros en la consola o cuando llame a la API de `GetTraceSummaries`.

X-Ray indexa hasta 50 anotaciones por rastro.

Los metadatos son pares de clave-valor con valores de cualquier tipo, por ejemplo objetos y listas, pero que no se indexan. Utilice los metadatos para registrar los datos que desee almacenar en el rastro, pero que no vaya a usar para buscar rastros.

Puede ver las anotaciones y los metadatos en la ventana de detalles del segmento o subsegmento, dentro de la página de detalles de Trace de la CloudWatch consola.



Errores y excepciones

X-Ray rastrea los errores que se producen en su código de aplicación y los errores que devuelven los servicios posteriores. Los errores se clasifican como se indica a continuación.

- **`Error`**: errores del cliente (errores de la serie 400)
- **`Fault`**: errores del servidor (errores de la serie 500)
- **`Throttle`**: errores de limitación controlada (429: demasiadas solicitudes)

Cuando se produce una excepción, mientras la aplicación está sirviendo una solicitud instrumentada, el SDK de X-Ray registra detalles sobre la excepción, incluido el rastro de pila, si está disponible. Puede ver excepciones en detalles de segmento en la consola de X-Ray.

AWS X-Ray consola

Utilice la AWS X-Ray consola para ver un mapa de los servicios y las trazas asociadas a las solicitudes que atienden sus aplicaciones, y para configurar los grupos y las reglas de muestreo que afectan a la forma en que se envían las trazas a X-Ray.

> **Note**
>
> CloudWatch ahora incluye Application Signals, que puede descubrir y monitorear sus servicios de aplicaciones, clientes, Synthetics Canaries y dependencias de servicios. Use Application Signals para ver una lista o un mapa visual de sus servicios, ver las métricas del estado en función de los objetivos de nivel de servicio (SLO) y profundizar para ver los seguimientos de X-Ray correlacionados para una solución de problemas más detallada. El mapa y CloudWatch ServiceLens el mapa del Servicio de Rayos X se han combinado en el mapa de rastreo de rayos X de la CloudWatch consola de Amazon. Abre la CloudWatch consola y selecciona Trace Map en Rastros de X-Ray en el panel de navegación izquierdo.

La página principal de la consola de X-Ray es el mapa de rastreo, que es una representación visual del gráfico de servicio JSON que X-Ray genera a partir de los datos de rastreo generados por sus aplicaciones. El mapa se compone de nodos de servicios para cada aplicación en su cuenta que atiende solicitudes, nodos cliente principales que representan los orígenes de las solicitudes, y nodos de servicios posteriores que representan los servicios web y los recursos utilizados por una aplicación mientras procesa una solicitud. Hay páginas adicionales para ver rastros y sus detalles, y para configurar grupos y reglas de muestreo.

Exploración de la consola de X-Ray

- Uso del mapa de trazas de X-Ray
- Visualización de rastros y detalles de rastros
- Uso de expresiones de filtro
- Rastreo entre cuentas
- Rastreo de aplicaciones basadas en eventos
- Uso de histogramas de latencia
- Uso de información en X-Ray
- Interacción con la consola de Analytics

- Configuración de grupos
- Configuración de reglas de muestreo de
- Enlace profundo de la consola

Uso del mapa de trazas de X-Ray

Vea el mapa de rastreo de X-Ray para identificar los servicios en los que se producen errores, las conexiones con alta latencia o los rastreos de las solicitudes que no se realizaron correctamente.

> **Note**
>
> CloudWatch ahora incluye Application Signals, que puede detectar y monitorear los servicios de sus aplicaciones, los clientes, las variables sintéticas y las dependencias de los servicios. Use Application Signals para ver una lista o un mapa visual de sus servicios, ver las métricas del estado en función de los objetivos de nivel de servicio (SLO) y profundizar para ver los seguimientos de X-Ray correlacionados para una solución de problemas más detallada.
> El mapa y CloudWatch ServiceLens el mapa del servicio de rayos X se combinan en el mapa de rastreo de rayos X de la CloudWatch consola de Amazon. Abre la CloudWatch consola y selecciona Trace Map en Rastros de X-Ray en el panel de navegación izquierdo.

Consulta del mapa de seguimiento

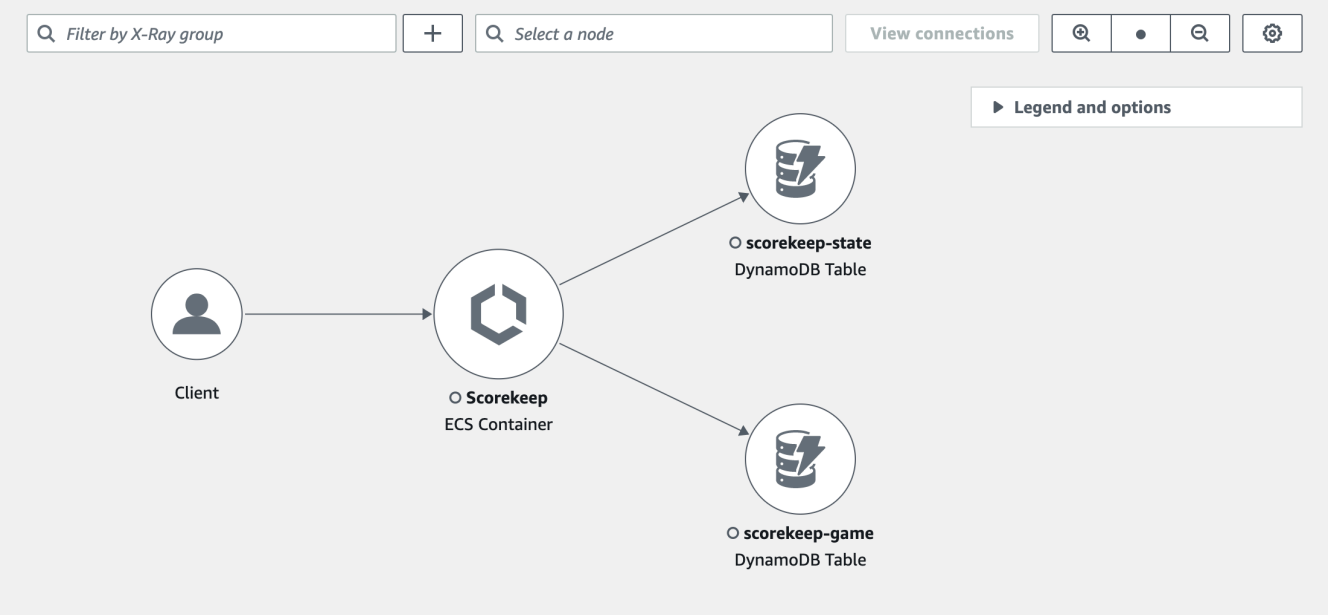
El mapa de rastreo es una representación visual de los datos de rastreo que generan sus aplicaciones. El mapa muestra nodos de servicios que atienden solicitudes, nodos cliente principales que representan los orígenes de las solicitudes, y nodos de servicios posteriores que representan los servicios web y los recursos utilizados porque utiliza una aplicación mientras procesa una solicitud.

El mapa de rastreo muestra una vista conectada de los rastreos en aplicaciones basadas en eventos que utilizan Amazon SQS y Lambda. Para obtener más información, consulte Rastreo de aplicaciones basadas en eventos. El mapa de rastreo también admite el rastreo entre cuentas, ya que muestra los nodos de varias cuentas en un solo mapa.

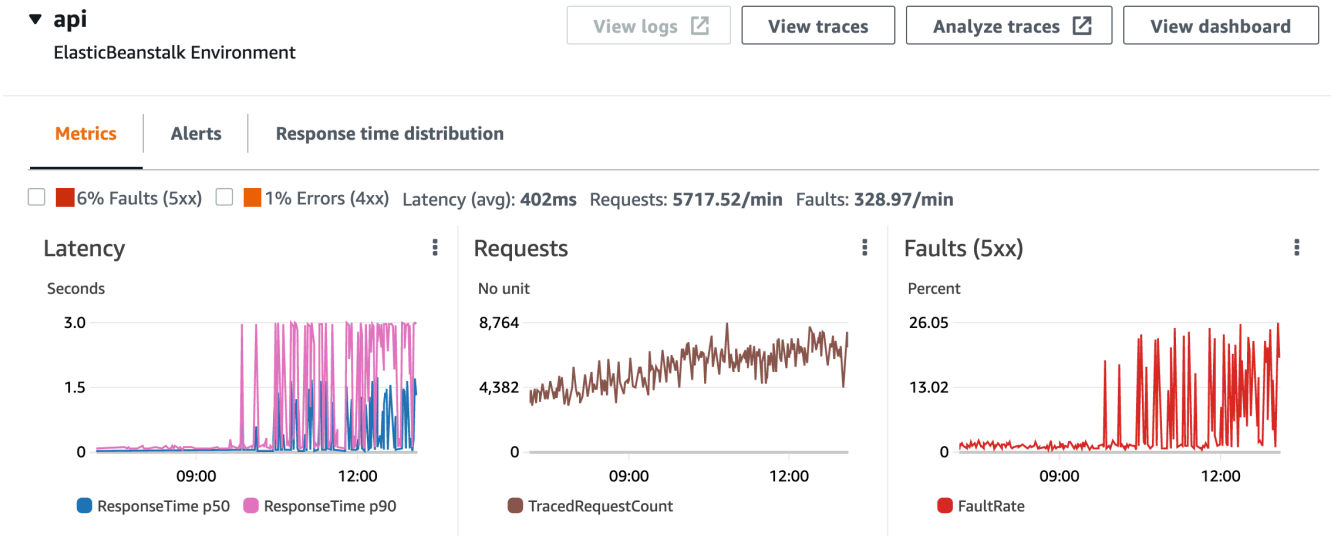
CloudWatch console

Para ver el mapa de rastreo en la consola CloudWatch

1. Abra la consola de CloudWatch . Elija Trace Map en la sección Rastros de X-Ray del panel de navegación izquierdo.



2. Seleccione un nodo de servicio para ver sus solicitudes o un límite entre dos nodos para ver las solicitudes que pasaron por esa conexión.
3. Debajo del mapa de rastreo se muestra información adicional, incluidas pestañas para métricas, alertas y distribución del tiempo de respuesta. En la pestaña Métricas, seleccione un rango dentro de cada gráfico para profundizar y ver más detalles, o elija las opciones de errores o errores para filtrar los rastreos. En la pestaña Distribución del tiempo de respuesta, seleccione un rango dentro del gráfico para filtrar los rastros por tiempo de respuesta.



4. Para ver los rastros, elija Ver rastros o, si ha aplicado un filtro, elija Ver rastros filtrados.
5. Seleccione Ver registros para ver CloudWatch los registros asociados al nodo seleccionado. No todos los nodos del mapa de rastreo admiten la visualización de registros. Consulte los CloudWatch registros de solución de problemas para obtener más información.

El mapa de rastreo indica los problemas en cada nodo delineándolo con colores:

- El rojo se usa para fallos de servidor (errores de la serie 500)
- El amarillo se usa para los errores del cliente (errores de la serie 400)
- El morado indica los errores de limitación de solicitudes (429: demasiadas solicitudes)

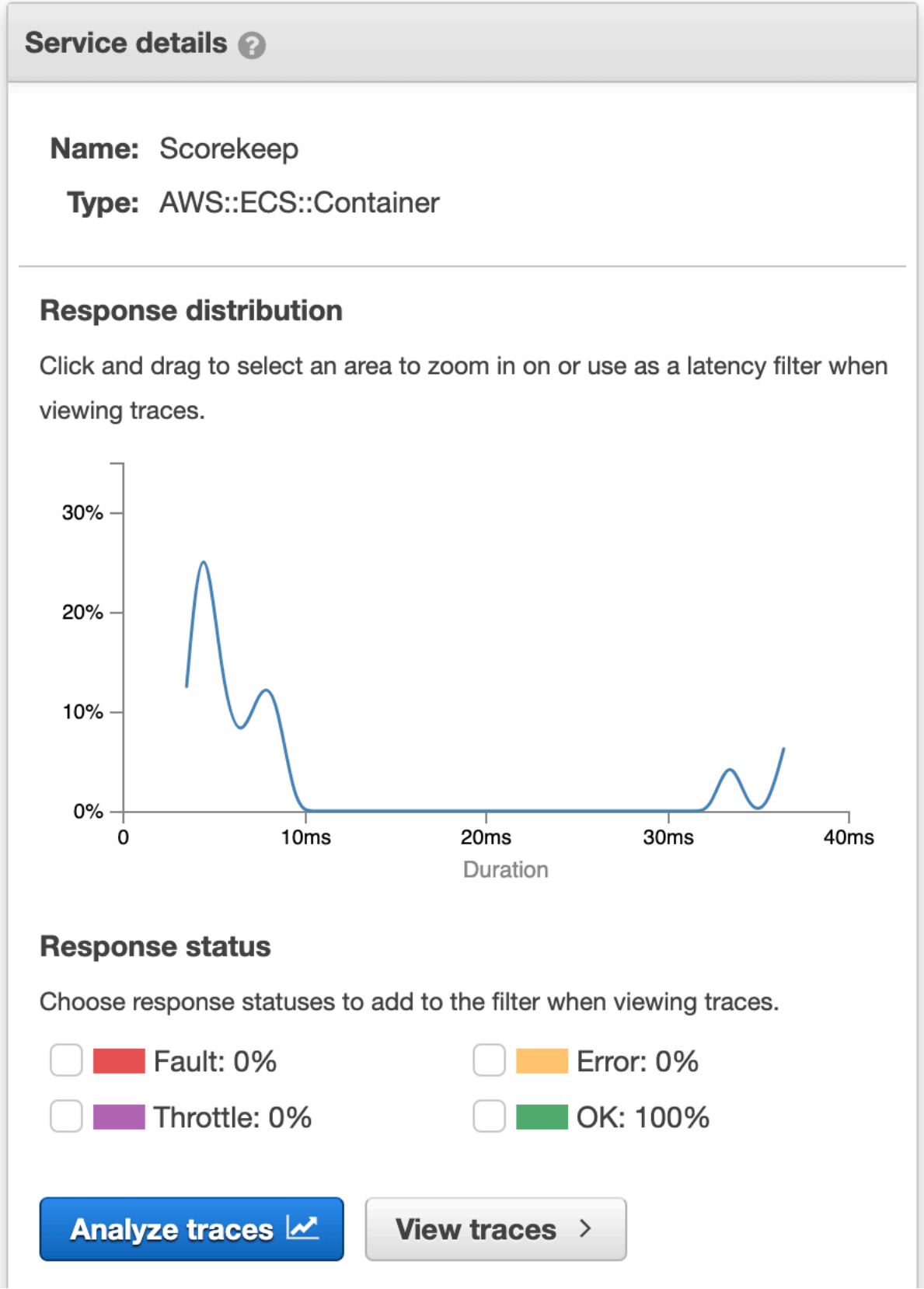
Si el mapa de rastreo es grande, usa los controles de la pantalla o el ratón para acercar y alejar el mapa y mover el mapa.

X-Ray console

Para ver el mapa del servicio

1. Abra la consola de X-Ray. El mapa de servicio se muestra de forma predeterminada. También puede elegir Service Map en el panel de navegación izquierdo.

2. Seleccione un nodo de servicio para ver sus solicitudes o un límite entre dos nodos para ver las solicitudes que pasaron por esa conexión.
3. Utilice el histograma que representa la distribución del tiempo de respuesta para filtrar los rastros por duración y seleccione los códigos de estado cuyos rastros desee ver. Después elija Ver rastros para abrir la lista de rastros con la expresión de filtro aplicada.


Service details
Name: Scorekeep
Type: AWS::ECS::Container
Response distribution
Click and drag to select an area to zoom in on or use as a latency filter when viewing traces.
30%
20%
10%
0%
0
10ms
20ms
30ms
40ms
Duration
Response status
Choose response statuses to add to the filter when viewing traces.
Fault: 0%
Error: 0%
Throttle: 0%
OK: 100%
Analyze traces
View traces

El mapa de servicio indica el estado de cada nodo mediante el uso de colores en función de la proporción de llamadas correctas y errores o fallos:

- El verde se utiliza para las llamadas realizadas con éxito
- El rojo se usa para fallos de servidor (errores de la serie 500)
- El amarillo se usa para los errores del cliente (errores de la serie 400)
- El morado indica los errores de limitación de solicitudes (429: demasiadas solicitudes)

Si el mapa de servicio es demasiado grande, utilice los controles que aparecen en pantalla o el ratón para ampliar y reducir el mapa o para moverlo por la pantalla.

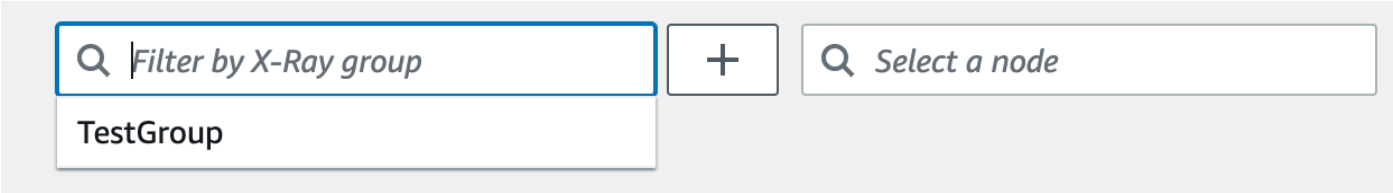
> **Note**
>
> El mapa de rastreo de X-Ray puede mostrar hasta 10 000 nodos. En raras ocasiones, en las que el número total de nodos de servicio supere este límite, es posible que reciba un error y no pueda mostrar un mapa de rastreo completo en la consola.

Filtrar el mapa de rastreo por grupo

Mediante una expresión de filtro, puede definir los criterios por los que incluir rastros en un grupo. Siga estos pasos para, a continuación, mostrar ese grupo específico en el mapa de rastreo.

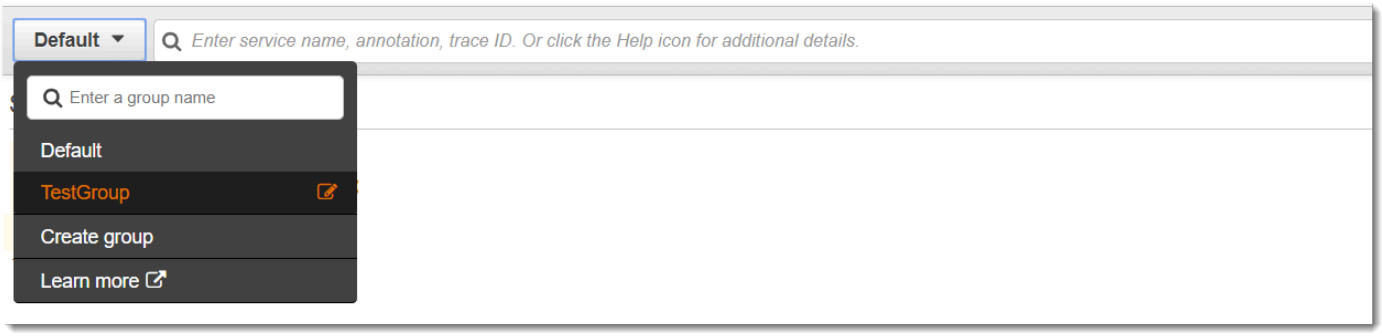
CloudWatch console

Elija un nombre de grupo en el filtro de grupo situado en la parte superior izquierda del mapa de rastreo.



X-Ray console

Elija un nombre de grupo en el menú desplegable situado a la izquierda de la barra de búsqueda.



Entonces se filtrará el mapa de servicio para mostrar los rastros que coincidan con la expresión de filtro del grupo seleccionado.

Rastrea la leyenda y las opciones del mapa

El mapa de rastreo incluye una leyenda y varias opciones para personalizar la visualización del mapa.

CloudWatch console

Seleccione el menú desplegable Leyenda y opciones en la parte superior derecha del mapa. Elija lo que se muestra dentro de los nodos, por ejemplo:

- Métricas muestra el tiempo medio de respuesta y el número de rastreos enviados por minuto durante el intervalo de tiempo elegido.
- Nodos muestra el icono de servicio dentro de cada nodo.

Seleccione otros ajustes del mapa en el panel Preferencias, al que se puede acceder mediante el icono con forma de engranaje situado en la parte superior derecha del mapa. Estos ajustes incluyen seleccionar qué métrica se utiliza para determinar el tamaño de cada nodo y qué valores controlados deben mostrarse en el mapa.

X-Ray console

Para ver la leyenda del mapa de servicio, seleccione el enlace Leyenda del mapa en la parte superior derecha del mapa. Las opciones del mapa de servicio se pueden seleccionar en la parte inferior derecha del mapa de rastreo, entre las que se incluyen:

- Iconos de servicio cambia lo que se muestra en cada nodo y muestra el icono del servicio o el tiempo medio de respuesta y el número de rastros enviados por minuto durante el intervalo de tiempo elegido.
- Tamaño de los nodos: ninguno establece el mismo tamaño para todos los nodos.
- Tamaño de los nodos: estado dimensiona los nodos en función del número de solicitudes afectadas por errores, fallos o solicitudes limitadas.
- Tamaño de los nodos: tráfico dimensiona los nodos según el número total de solicitudes.

Visualización de rastros y detalles de rastros

Utilice la página Rastros de la consola de X-Ray para encontrar rastros por URL, código de respuesta u otros datos a partir del resumen de rastros. Tras seleccionar una traza de la lista de trazas, la página de detalles de la traza muestra un mapa de los nodos de servicio que están asociados a la traza seleccionada y una cronología de los segmentos de la traza.

Consulta de registros de seguimiento

CloudWatch console

Para ver los seguimientos en la CloudWatch consola

1. Inicie sesión en la CloudWatch consola AWS Management Console y ábrala en https://console.aws.amazon.com/cloudwatch/.
2. En el panel de navegación izquierdo, elija Rastros de X-Ray y, a continuación, Traces. Puede filtrar por grupo o introducir una expresión de filtro. Esto filtra los rastros que se muestran en la sección Rastros, en la parte inferior de la página.

   Como alternativa, puede usar el mapa de servicio para navegar hasta un nodo de servicio específico y, a continuación, ver los rastros. Esto abre la página de rastreos con una consulta ya aplicada.
3. Acote su consulta en la sección Limitadores de consultas. Para filtrar los rastreos por un atributo común, elija una opción de la flecha hacia abajo situada junto a Limitar la consulta por. Las opciones incluyen:

   - Nodo: filtra los rastreos por nodo de servicio.

- ARN del recurso: filtra las trazas por un recurso asociado a una traza. Algunos ejemplos de estos recursos incluyen una instancia, una función o AWS Lambda una tabla de Amazon Elastic Compute Cloud (Amazon EC2). Amazon DynamoDB
- Usuario: filtre las trazas con un ID de usuario.
- Mensaje de causa raíz del error: filtra las trazas por la causa raíz del error.
- URL: filtra los rastreos por la ruta URL utilizada por la aplicación.
- Código de estado HTTP: filtra las trazas por el código de estado HTTP devuelto por la aplicación. Puede especificar un código de respuesta personalizado o seleccionar una de las siguientes opciones:
  - `200`— La solicitud se ha realizado correctamente.
  - `401`— La solicitud carecía de credenciales de autenticación válidas.
  - `403`— La solicitud carecía de permisos válidos.
  - `404`— El servidor no pudo encontrar el recurso solicitado.
  - `500`— El servidor detectó una condición inesperada y generó un error interno.

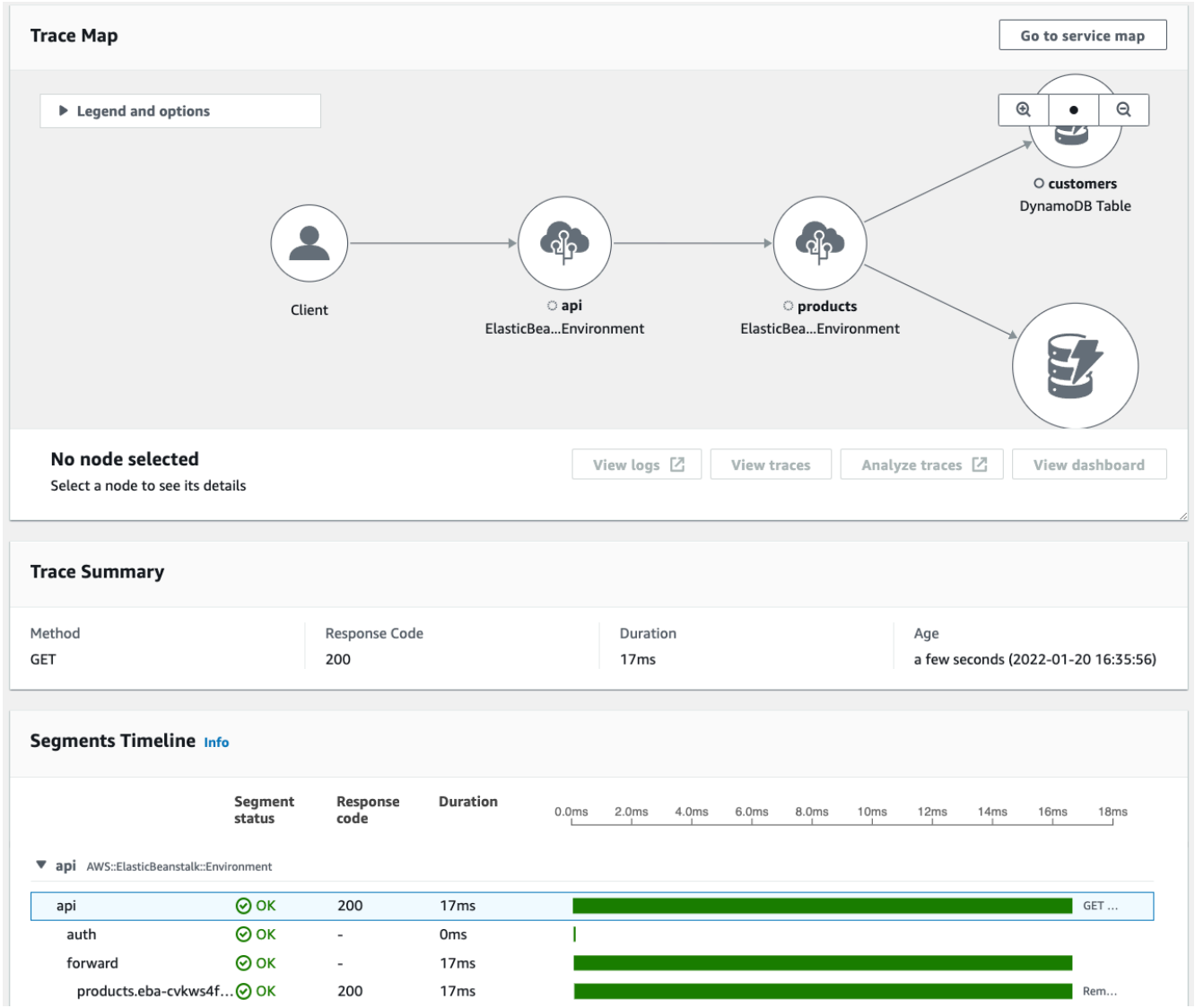
Seleccione una o más entradas y, a continuación, seleccione Añadir a la consulta para añadirlas a la expresión de filtro situada en la parte superior de la página.

4. Para buscar una única traza, introduzca un identificador de traza directamente en el campo de consulta. Puede utilizar el formato X-Ray o el formato World Wide Web Consortium (W3C). Por ejemplo, una traza que se crea con la AWS distribución para OpenTelemetry está en formato W3C.

   > **Note**
   >
   > Al consultar las trazas que se crean con un ID de traza en formato W3C, la consola muestra la traza coincidente en formato X-Ray. Por ejemplo, si realiza una consulta `4efaaf4d1e8720b39541901950019ee5` en formato W3C, la consola muestra el equivalente a X-Ray:. `1-4efaaf4d-1e8720b39541901950019ee5`

5. Seleccione Ejecutar consulta en cualquier momento para visualizar una lista de rastros coincidentes en la sección Rastros, en la parte inferior de la página.
6. Para mostrar la página de detalles del rastreo de un solo rastreo, seleccione un ID de rastreo de la lista.

La siguiente imagen muestra un mapa de rastreo que contiene los nodos de servicio asociados al rastreo y los bordes entre los nodos que representan la ruta seguida por los segmentos que componen el rastreo. Un resumen del rastreo sigue al mapa de rastreo. El resumen contiene información sobre una GET operación de ejemplo, su código de respuesta, el tiempo que tardó en ejecutarse el rastreo y la antigüedad de la solicitud. La cronología de los segmentos sigue el resumen del rastreo, que muestra la duración de los segmentos y subsegmentos del rastreo.



Si tiene una aplicación basada en eventos que utiliza Amazon SQS y Lambda, puede ver una vista conectada de los seguimientos de cada solicitud en el mapa de rastreo. En el mapa, las trazas de los productores de los mensajes están vinculadas a las trazas de AWS Lambda los consumidores y se muestran como un borde discontinuo. Para obtener más información

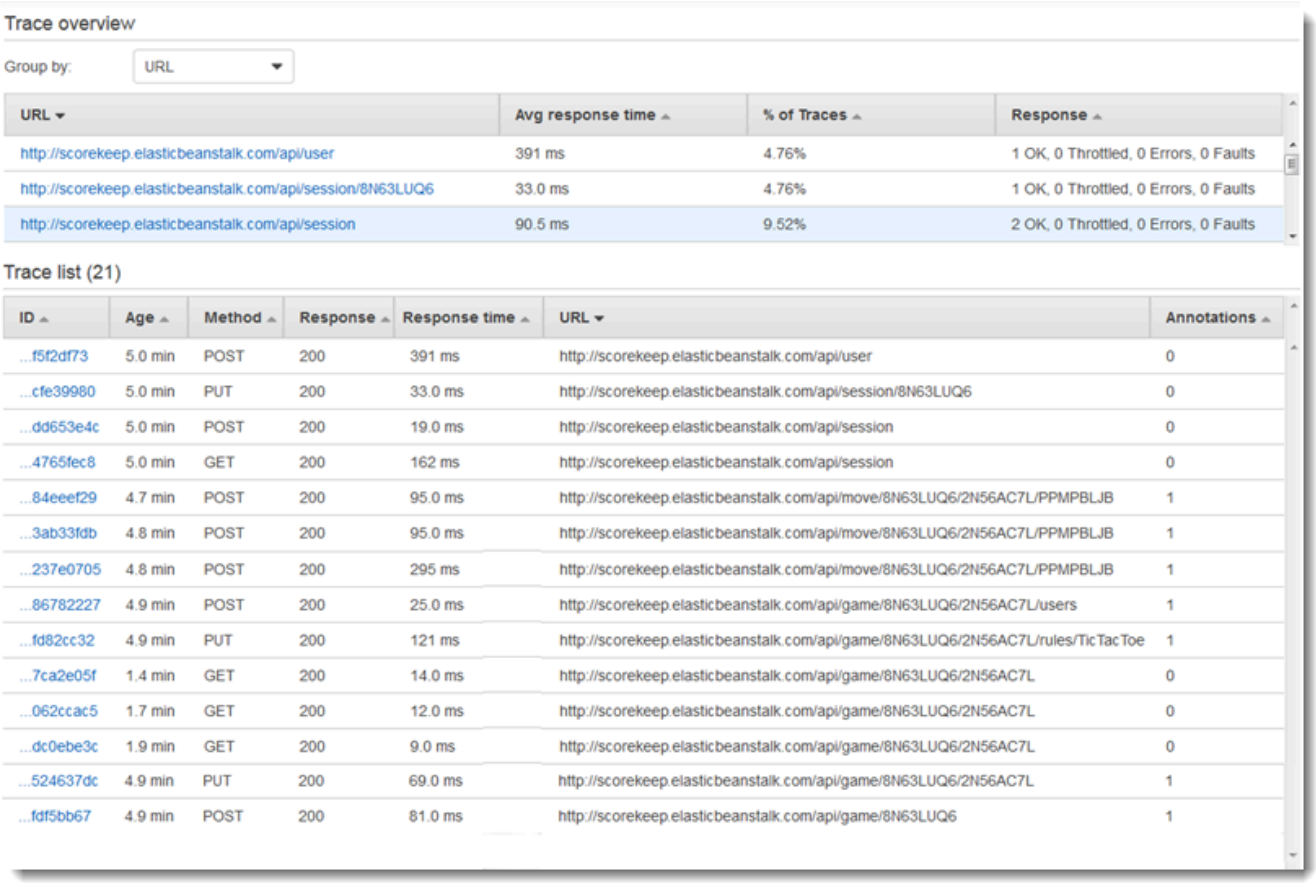
sobre las aplicaciones basadas en eventos, consulte. Rastreo de aplicaciones basadas en eventos

Las páginas Traces y de detalles de Trace también admiten el rastreo multicuenta, que permite enumerar los rastros de varias cuentas en la lista de rastreos y dentro de un único mapa de rastreo.

X-Ray console

Para ver los rastros en la consola de X-Ray

1. Abra la página Rastros de la consola de X-Ray. El panel de información general sobre el rastreo muestra una lista de rastreos agrupados por características comunes, incluidas las causas raíz de los errores, ResourceArn y. InstanceId
2. Para seleccionar una función común para ver un conjunto agrupado de rastreos, expanda la flecha hacia abajo situada junto a Agrupar por. La siguiente ilustración muestra un resumen de los rastreos agrupados por URL y una lista de los rastreos asociados. AWS X-Ray ejemplo de aplicación

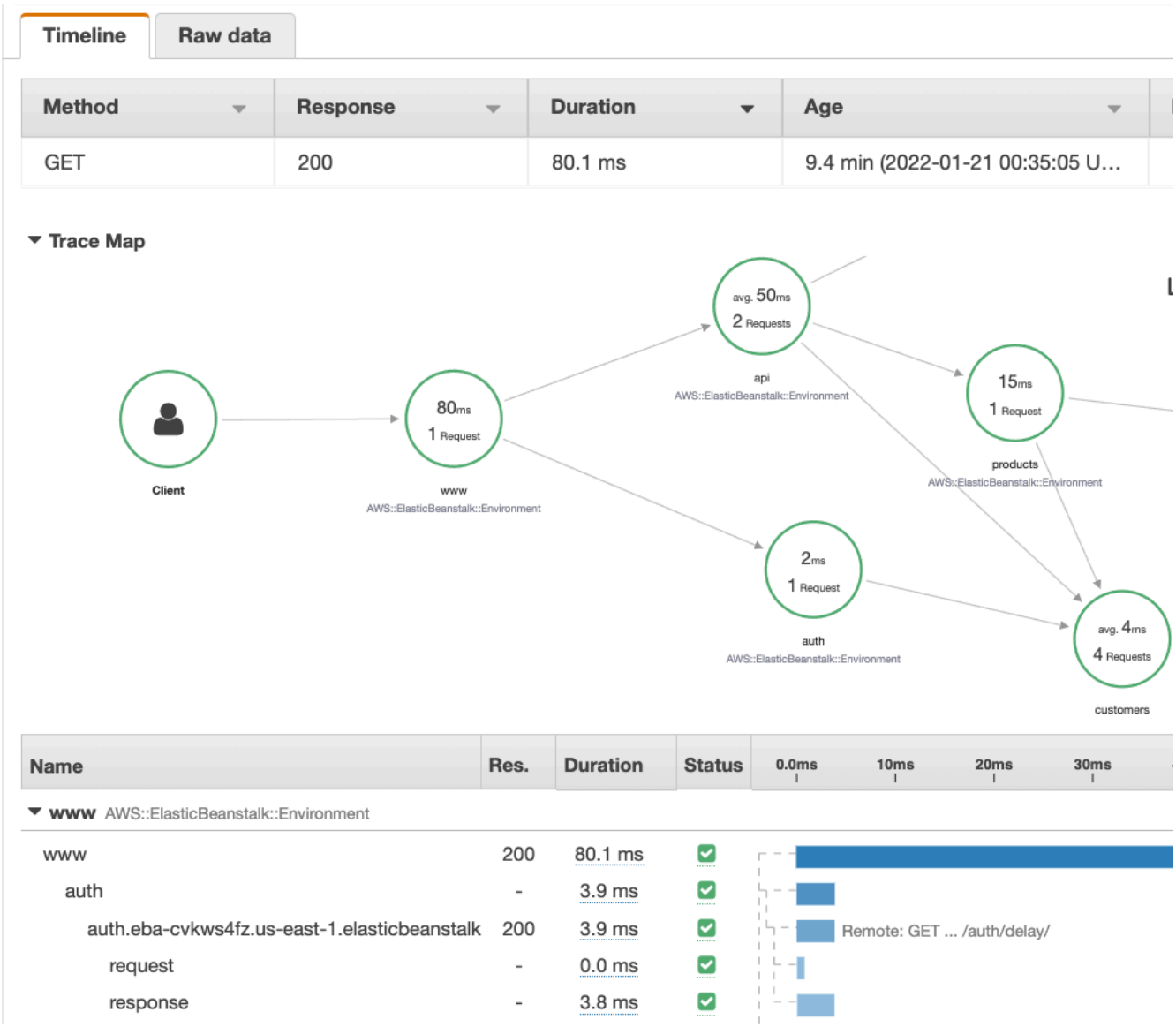


3. Elija el ID de un rastreo para verlo en la lista de rastreo. También puede elegir el mapa de servicio en el panel de navegación para ver los rastros de un nodo de servicio específico. A continuación, puede ver los rastros que están asociados a ese nodo.

   La pestaña Cronología muestra el flujo de solicitudes del rastreo e incluye lo siguiente:

   - Un mapa de la ruta de cada segmento del rastreo.
   - Cuánto tiempo tardó el segmento en llegar a un nodo del mapa de rastreo.
   - Cuántas solicitudes se realizaron al nodo del mapa de rastreo.

   La siguiente ilustración muestra un ejemplo de mapa de rastreo asociado a una `GET` solicitud realizada a una aplicación de ejemplo. Las flechas muestran la ruta que siguió cada segmento para completar la solicitud. Los nodos de servicio muestran el número de solicitudes realizadas durante la `GET` solicitud.



Para obtener más información sobre la pestaña Cronología, consulte la siguiente sección Exploración de la cronología del rastreo.

La pestaña de datos sin procesar muestra información sobre el rastreo y los segmentos y subsegmentos que lo componen, en `JSON` formato. Esta información puede incluir lo siguiente:

- Marcas temporales
- ID únicos
- Recursos asociados al segmento o subsegmento
- La fuente o el origen del segmento o subsegmento

- Información adicional sobre la solicitud a su aplicación, como la respuesta de una solicitud HTTP

Exploración de la escala de tiempo del rastro

La sección Cronología muestra una jerarquía de segmentos y subsegmentos junto a una barra horizontal que corresponde al tiempo que utilizaron para completar sus tareas. La primera entrada de la lista es el segmento, que representa todos los datos registrados por el servicio para una misma solicitud. Los subsegmentos están indentados y se enumeran a continuación del segmento. Las columnas contienen información sobre cada segmento.

CloudWatch console

En la CloudWatch consola, la cronología de los segmentos proporciona la siguiente información:

- La primera columna: muestra los segmentos y subsegmentos de la traza seleccionada.
- La columna de estado del segmento: muestra el resultado de estado de cada segmento y subsegmento.
- La columna de códigos de respuesta: muestra un código de estado de respuesta HTTP a una solicitud del navegador realizada por el segmento o subsegmento, cuando está disponible.
- La columna Duración: muestra cuánto tiempo duró el segmento o subsegmento.
- La columna Alojado en: muestra el espacio de nombres o el entorno en el que se ejecuta el segmento o subsegmento, si corresponde. Para obtener más información, consulte https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/AppSignals-StandardMetrics.html#AppSignals-StandardMetrics-Dimensions.
- La última columna: muestra las barras horizontales que corresponden a la duración del segmento o subsegmento, en relación con los demás segmentos o subsegmentos de la línea de tiempo.

Para agrupar la lista de segmentos y subsegmentos por nodo de servicio, activa Agrupar por nodos.

X-Ray console

En la página de detalles del rastreo, selecciona la pestaña Cronología para ver el cronograma de cada segmento y subsegmento que forma un rastreo.

En la consola de X-Ray, la línea de tiempo proporciona la siguiente información:

- La columna Nombre: muestra los nombres de los segmentos y subsegmentos de la traza.
- La columna Res.: muestra un código de estado de respuesta HTTP a una solicitud del navegador realizada por el segmento o subsegmento, cuando está disponible.
- La columna Duración: muestra cuánto tiempo duró el segmento o subsegmento.
- La columna Estado: muestra el resultado del estado del segmento o subsegmento.
- La última columna: muestra barras horizontales que corresponden a la duración del segmento o subsegmento, en relación con los demás segmentos o subsegmentos de la línea de tiempo.

Para ver los datos de rastreo sin procesar que la consola utiliza para generar la línea de tiempo, seleccione la pestaña Datos sin procesar. Los datos sin procesar muestran información sobre la traza y los segmentos y subsegmentos que componen la traza en `JSON` formato. Esta información puede incluir lo siguiente:

- Marcas temporales
- ID únicos
- Recursos asociados al segmento o subsegmento
- La fuente o el origen del segmento o subsegmento
- Información adicional sobre la solicitud a su aplicación, como la respuesta de una solicitud HTTP.

Cuando utilizas un AWS SDK o un SQL cliente instrumentado para realizar llamadas a recursos externos, el SDK de X-Ray graba subsegmentos automáticamente. HTTP También puedes usar el SDK de X-Ray para grabar subsegmentos personalizados para cualquier función o bloque de código. Los subsegmentos adicionales que se graban mientras un subsegmento personalizado está abierto se convierten en elementos secundarios del subsegmento personalizado.

Consulta de detalles de segmentos

En la línea de tiempo del rastreo, elija el nombre de un segmento para ver sus detalles.

El panel de detalles del segmento muestra las pestañas Descripción general, Recursos, Anotaciones, Metadatos, Excepciones y SQL. Se aplica lo siguiente:

- En Overview (Información general) se muestra información acerca de la solicitud y la respuesta. La información incluye el nombre, la hora de inicio, la hora de finalización, la duración, la URL de la solicitud, la operación de la solicitud, el código de respuesta a la solicitud y cualquier error o fallo.

- La pestaña Recursos de un segmento muestra información del SDK de X-Ray y sobre los AWS recursos que ejecutan la aplicación. Utilice los complementos Amazon EC2 o Amazon ECS para el SDK de X-Ray para registrar información de recursos específica del servicio. AWS Elastic Beanstalk Para obtener más información sobre los complementos, consulte la sección de complementos de servicio en. Configuración del SDK de X-Ray para Java
- Las pestañas restantes muestran las anotaciones, los metadatos y las excepciones que se registran para el segmento. Las excepciones se capturan automáticamente cuando se generan a partir de una solicitud instrumentada. Las anotaciones y los metadatos contienen información adicional que se graba mediante las operaciones que proporciona el SDK de X-Ray. Para añadir anotaciones o metadatos a sus segmentos, utilice el SDK de X-Ray. Para obtener más información, consulta el enlace específico del idioma que aparece en la sección Cómo equipar tu aplicación con los SDK incorporados. AWS X-Ray Instrumentación de su solicitud para AWS X-Ray

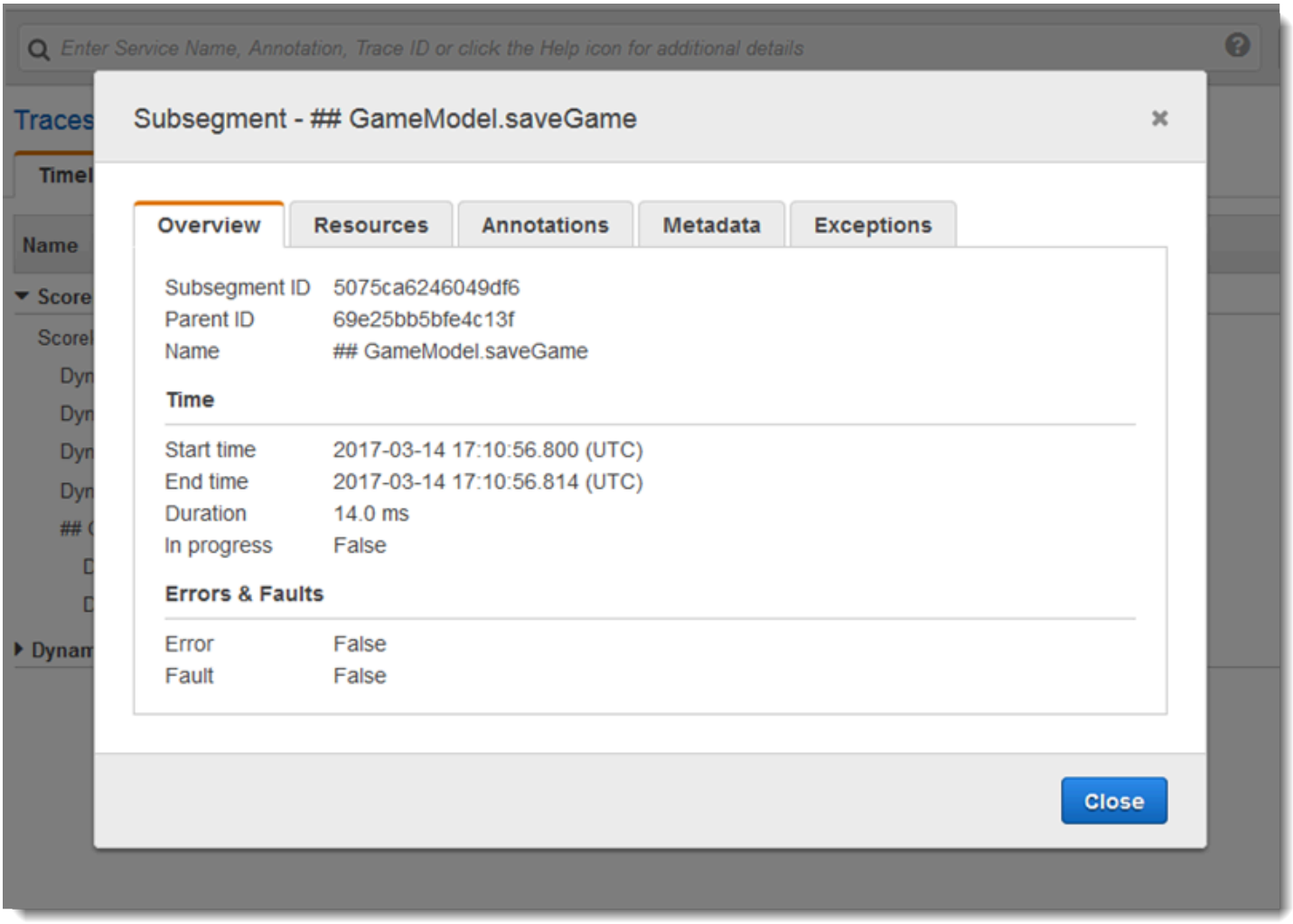
Consulta de detalles de subsegmentos

En la escala de tiempo del rastro, elija el nombre de un segmento para ver sus detalles:

- La pestaña Descripción general contiene información sobre la solicitud y la respuesta. Incluye el nombre, la hora de inicio, la hora de finalización, la duración, la solicitudURL, la operación de la solicitud, el código de respuesta a la solicitud y cualquier error o error. Para los subsegmentos generados con clientes instrumentados, la pestaña Overview (Información general) contiene información acerca de la solicitud y la respuesta desde el punto de vista de la aplicación.
- La pestaña Recursos de un subsegmento muestra detalles sobre los AWS recursos que se utilizaron para ejecutar el subsegmento. Por ejemplo, la pestaña de recursos puede incluir un ARN de AWS Lambda función, información sobre una tabla de DynamoDB, cualquier operación a la que se llame y un ID de solicitud.
- Las pestañas restantes muestran las anotaciones, los metadatos y las excepciones registradas en el subsegmento. Las excepciones se capturan automáticamente cuando se generan a partir de una solicitud instrumentada. Las anotaciones y los metadatos contienen información adicional que se graba mediante las operaciones que proporciona el SDK de X-Ray. Usa el SDK de X-Ray para añadir anotaciones o metadatos a tus segmentos. Para obtener más información, consulta el enlace específico del idioma que aparece en la sección Cómo equipar tu aplicación con los SDK incorporados. AWS X-Ray Instrumentación de su solicitud para AWS X-Ray

En los subsegmentos personalizados, la pestaña Información general muestra el nombre del subsegmento, que se puede establecer de modo que especifique el área de código o la función que registra. Para obtener más información, consulte el enlace específico del idioma que aparece en la sección Cómo instrumentar la aplicación con los SDK incluidos. AWS X-Ray [Generación de subsegmentos personalizados con el SDK de X-Ray para Java]

La siguiente imagen muestra la pestaña Descripción general de un subsegmento personalizado. El resumen contiene el identificador del subsegmento, el identificador principal, el nombre, las horas de inicio y finalización, la duración, el estado y los errores o errores.



La pestaña Metadatos de un subsegmento personalizado contiene información en JSON formato sobre los recursos utilizados por ese subsegmento.

Uso de expresiones de filtro

Use expresiones de filtro para ver un mapa de rastreo o los rastros de una solicitud, servicio, conexión entre dos servicios específicos (un borde) o solicitudes que cumplan una condición. X-Ray proporciona un lenguaje de expresiones de filtro para filtrar solicitudes, servicios y periferias teniendo en cuenta los datos presentes en los encabezados de la solicitud, el estado de la respuesta y los campos indexados en los segmentos originales.

Al elegir un periodo de tiempo de registros de seguimiento para ver en la consola de X-Ray, puede obtener más resultados que los que la consola puede mostrar. En la esquina superior derecha, la consola muestra el número de registros de seguimiento que analiza y si hay más registros de seguimiento disponibles. Puede utilizar una expresión de filtro para reducir el número de resultados a tan solo los rastros que desea encontrar.

Temas

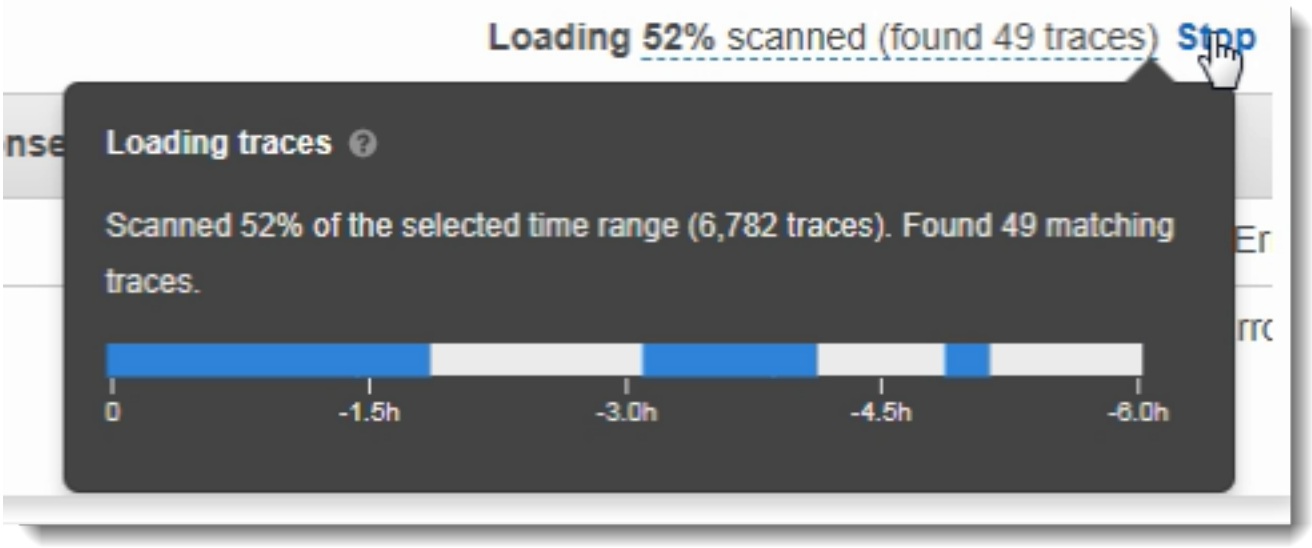
Detalles de expresión de filtro

Al elegir un nodo en el mapa de rastreo, la consola crea una expresión de filtro en función del nombre del servicio del nodo y de los tipos de error presentes en función de la selección. Para encontrar registros de seguimiento que muestren problemas de rendimiento o relacionados con solicitudes específicas, puede ajustar la expresión proporcionada por la consola, o bien crear la suya propia. Si añade anotaciones con el SDK de X-Ray, también puede filtrar en función de la presencia de una clave de anotación o el valor de una clave.

> **Note**
>
> Si elige un rango de tiempo relativo en el mapa de rastreo y elige un nodo, la consola convierte el rango de tiempo en una hora absoluta de inicio y finalización. Para asegurarse de que los registros de seguimiento del nodo aparezcan en los resultados de búsqueda y evitar los tiempos de examen cuando el nodo no estaba activo, el intervalo de tiempo solo incluye las horas a las que el nodo envió registros de seguimiento. Si desea buscar con relación a la hora actual, puede volver a un intervalo de tiempo relativo en la página de registros de seguimiento y volver a analizar.

Si sigue habiendo más resultados disponibles de los que la consola puede mostrar, la consola muestra cuántos registros de seguimiento han coincidido y el número de registros de seguimiento analizados. El porcentaje que se muestra es el porcentaje del marco temporal seleccionado que se analizó. Para asegurarse de ver todos los registros de seguimiento coincidentes representados en los resultados, filtre aún más la expresión de filtro o seleccione un marco temporal más corto.

Para obtener los resultados más recientes en primer lugar, la consola comienza a analizar al final del intervalo de tiempo y va hacia atrás. Si hay un gran número de registros de seguimiento, pero pocos resultados, la consola divide el intervalo de tiempo en porciones y las analiza en paralelo. La barra de progreso muestra las partes del intervalo de tiempo que se han analizado.



Uso de expresiones de filtro con grupos

Los grupos son una colección de registros de seguimiento que se definen mediante una expresión de filtro. Puedes usar grupos para generar gráficos de servicios adicionales y proporcionar CloudWatch métricas de Amazon.

Los grupos se identifican por su nombre o un nombre de recurso de Amazon (ARN) y contienen una expresión de filtro. El servicio compara los registros de seguimiento de entrada con la expresión y los almacena en consecuencia.

Puede crear y modificar grupos mediante el menú desplegable situado a la izquierda de la barra de búsqueda de expresiones de filtro.

> **Note**
>
> Si el servicio encuentra un error al evaluar un grupo, ese grupo deja de estar incluido en el procesamiento de los registros de seguimiento de entrada y se registra una métrica de error.

Para obtener más información acerca de los grupos, consulte Configuración de grupos.

Sintaxis de expresiones de filtro

Las expresiones de filtro pueden incluir una palabra clave, un operador único o binario y un valor para la comparación.

```
keyword operator value
```

Cada tipo de palabra clave tiene sus propios operadores. Por ejemplo, `responsetime` es una palabra clave numérica que se puede comparar con operadores relacionados con números.

Example – solicitudes con tiempo de respuesta de más de 5 segundos

```
responsetime > 5
```

Puede combinar varias expresiones en una expresión compuesta utilizando los operadores `AND` u `OR`.

Example – solicitudes con duración total de 5 a 8 segundos

```
duration >= 5 AND duration <= 8
```

Solo se detectan problemas con las palabras clave y los operadores sencillos en el nivel de registro de seguimiento. Si se produce un error posterior, pero la aplicación lo gestiona y no se muestra al usuario, este problema no se detectará al buscar con la palabra `error`.

Para encontrar registros de seguimiento con problemas posteriores, use las palabras clave complejas `service()` y `edge()`. Estas palabras clave permiten aplicar un filtro de expresión a todos los nodos posteriores, a un único nodo posterior o a un límite entre dos nodos. Para obtener un mayor nivel de detalle, puede filtrar los servicios y los bordes con la función id().

Palabras clave booleanas

Los valores de palabra clave booleana son true o false. Utilícelas para encontrar registros de seguimiento que resultaron erróneos.

Palabras clave booleanas

- `ok`: el código de estado de la respuesta fue 2XX Success.
- `error`: el código de estado de la respuesta fue 4XX Client Error.
- `throttle`: el código de estado de la respuesta fue 429 Too Many Requests.
- `fault`: el código de estado de la respuesta fue 5XX Server Error.
- `partial`: la solicitud tiene segmentos incompletos.
- `inferred`: la solicitud tiene segmentos inferidos.
- `first`: el elemento es el primero de una lista enumerada.
- `last`: el elemento es el último de una lista enumerada.
- `remote`: la entidad de causa raíz es remota.
- `root`: la solicitud es el punto de entrada o el segmento raíz de un registro de seguimiento.

Los operadores booleanos encuentran aquellos segmentos en los que la clave especificada es `true` o `false`.

Operadores booleanos

- none: la expresión es verdadera si la palabra clave es verdadera.

- `!`: la expresión es verdadera si la palabra clave es falsa.
- `=`, `!=`: compara el valor de la palabra clave con la cadena `true` o `false`. Estos operadores actúan igual que los demás, pero son más explícitos.

Example – estado de respuesta es 2XX OK

```
ok
```

Example – el estado de respuesta no es 2XX OK

```
!ok
```

Example – el estado de respuesta no es 2XX OK

```
ok = false
```

Example – el último registro de seguimiento de error enumerado tiene el nombre de error "deserialize"

```
rootcause.fault.entity { last and name = "deserialize" }
```

Example – solicitudes con segmentos remotos donde la cobertura es mayor que 0.7 y el nombre del servicio es "rastros"

```
rootcause.responsetime.entity { remote and coverage > 0.7 and name = "traces" }
```

Example : solicitudes con segmentos inferidos donde el tipo de servicio "AWS:DynamoDB"

```
rootcause.fault.service { inferred and name = traces and type = "AWS::DynamoDB" }
```

Example – solicitudes que tienen un segmento con el nombre "data-plane" como raíz.

```
service("data-plane") {root = true and fault = true}
```

Palabras clave numéricas

Utilice palabras clave numéricas para buscar solicitudes con un tiempo de respuesta, duración o estado de respuesta específico.

Palabras clave numéricas

- `responsetime`: tiempo que tardó el servidor en enviar una respuesta.
- `duration`: duración total de la solicitud, incluidas las llamadas posteriores.
- `http.status`: código de estado de respuesta.
- `index`: posición de un elemento en una lista.
- `coverage`: porcentaje decimal del tiempo de respuesta de una entidad con respecto al tiempo de respuesta del segmento raíz. Aplicable únicamente a las entidades de causa raíz de tiempo de respuesta.

Operadores numéricos

Las palabras clave numéricas usan los operadores de comparación y de igualdad estándar.

- =,`!`=: la palabra clave es igual o no a un valor numérico.
- <,<=, >,>=: la palabra clave es menor o igual a un valor numérico.

Example – el estado de respuesta no es 200 OK

```
http.status != 200
```

Example – solicitud con duración total de 5 a 8 segundos

```
duration >= 5 AND duration <= 8
```

Example – solicitudes que se completaron sin errores en menos de 3 segundos, incluidas todas las llamadas posteriores

```
ok !partial duration <3
```

Example – entidad de lista enumerada que tiene un índice mayor que 5

```
rootcause.fault.service { index > 5 }
```

Example : solicitudes en las que la última entidad tiene una cobertura superior a 0.8

```
rootcause.responsetime.entity { last and coverage > 0.8 }
```

Palabras clave de cadenas

Utilice palabras clave de cadena para encontrar registros de seguimiento con texto específico en los encabezados de solicitud o ID de usuario específicos.

Palabras clave de cadenas

- `http.url`: URL de solicitud.
- `http.method`: método de solicitud.
- `http.useragent`: cadena del agente de usuario de la solicitud.
- `http.clientip`: dirección IP del solicitante.
- `user`: valor del campo de usuario en cualquier segmento incluido en el registro de seguimiento.
- `name`: el nombre de un servicio o excepción.
- `type`: tipo de servicio.
- `message`: mensaje de excepción.
- `availabilityzone`: valor del campo availabilityzone de cualquier segmento incluido en el registro de seguimiento
- `instance.id`: valor del campo de ID de instancia de cualquier segmento incluido en el registro de seguimiento
- `resource.arn`: valor de campo ARN del recurso de cualquier segmento incluido en el registro de seguimiento

Los operadores de cadena permiten encontrar valores iguales a un texto determinado o que contienen dicho texto. Estos valores se deben escribir siempre entre comillas.

Operadores de cadena

- `=`, `!=`: la palabra clave es igual o no a un valor numérico.
- `CONTAINS`: la palabra clave contiene una cadena concreta.
- `BEGINSWITH` , `ENDSWITH`: la palabra clave comienza o termina con una cadena concreta.

Example – filtro http.url

```
http.url CONTAINS "/api/game/"
```

Para probar si un registro de seguimiento incluye un campo, independientemente de su valor, compruebe si la cadena está vacía.

Example – filtro user

Encuentre todos los registros de seguimiento con ID de usuario.

```
user CONTAINS ""
```

Example – seleccione los registros de seguimiento con una causa raíz de error que incluyan el servicio denominado "Auth"

```
rootcause.fault.service { name = "Auth" }
```

Example – seleccione los registros de seguimiento con una causa raíz de tiempo de respuesta cuyo último servicio tenga un tipo de DynamoDB

```
rootcause.responsetime.service { last and type = "AWS::DynamoDB" }
```

Example – seleccione los registros de seguimiento con una causa raíz de error cuya última excepción tenga el mensaje "access denied for account_id: 1234567890"

```
rootcause.fault.exception { last and message = "Access Denied for account_id:
 1234567890"
```

Palabras clave complejas

Utilice palabras clave complejas para buscar solicitudes basadas en nombre del servicio, nombre de borde o valor de anotación. Para servicios y límites, puede especificar una expresión de filtro adicional que se aplica al servicio o al límite. Para anotaciones, puede filtrar por el valor de una anotación con una clave específica, utilizando operadores booleanos, numéricos o de cadena.

Palabras clave complejas

- `annotation.`*`key`*: valor de anotación con campo *`key`*. Una anotación puede tener un valor booleano, numérico o de cadena, por lo que puede usar cualquiera de estos tipos de operadores de comparación. Puede utilizar esta palabra clave en combinación con la palabra clave `service` o `edge`.

- `edge(source, destination) {filter}`:conexión entre los servicios *origen* y *destino*. Las llaves opcionales pueden contener una expresión de filtro que se aplica a los segmentos de esta conexión.
- `group.name / group.arn`:l valor de la expresión de filtro de un grupo, al que se hace referencia mediante el nombre del grupo o el ARN del grupo.
- `json`: objeto de causa raíz JSON. Consulte Obtener datos de AWS X-Ray para ver los pasos para crear entidades JSON mediante programación.
- `service(name) {filter}`: servicio denominado *nombre*. Las llaves opcionales pueden contener una expresión de filtro que se aplica a los segmentos que creó el servicio.

Usa la palabra clave service para buscar los rastros de las solicitudes que lleguen a un nodo determinado del mapa de rastreo.

Los operadores de palabras clave complejas buscan segmentos en los que se haya establecido o no se haya establecido la clave especificada.

Operadores de palabras clave complejas

- none: la expresión es verdadera si la palabra clave está establecida. Si la palabra clave es de tipo booleano, se evaluará en función del valor booleano.
- `!`: la expresión es verdadera si la palabra clave no está establecida. Si la palabra clave es de tipo booleano, se evaluará en función del valor booleano.
- =,!=: compara el valor de la palabra clave.
- `edge(source, destination) {filter}`:conexión entre los servicios *origen* y *destino*. Las llaves opcionales pueden contener una expresión de filtro que se aplica a los segmentos de esta conexión.
- `annotation.key`: valor de anotación con campo *key*. Una anotación puede tener un valor booleano, numérico o de cadena, por lo que puede usar cualquiera de estos tipos de operadores de comparación. Puede utilizar esta palabra clave en combinación con la palabra clave `service` o `edge`.
- `json`: objeto de causa raíz JSON. Consulte Obtener datos de AWS X-Ray para ver los pasos para crear entidades JSON mediante programación.

Usa la palabra clave service para buscar los rastros de las solicitudes que lleguen a un nodo determinado del mapa de rastreo.

Example – filtro Service

Solicitudes que incluyen una llamada a `api.example.com` con un error (error de la serie 500).

```
service("api.example.com") { fault }
```

Puede excluir el nombre del servicio para aplicar un filtro de expresión a todos los nodos de su mapa de servicios.

Example – filtro service

Solicitudes que hayan provocado un error en cualquier parte del mapa de rastreo.

```
service() { fault }
```

La palabra clave edge aplica una expresión de filtro a una conexión entre dos nodos.

Example – filtro edge

Solicitud en la que el servicio `api.example.com` hizo una llamada a `backend.example.com` que resultó errónea.

```
edge("api.example.com", "backend.example.com") { error }
```

También puede utilizar el operador `!` con las palabras clave service y edge para excluir un servicio o un límite de los resultados de otra expresión de filtro.

Example – filtro service y de solicitud

Solicitud cuya URL comienza por `http://api.example.com/` y contiene `/v2/`, pero no llega al servicio denominado `api.example.com`.

```
http.url BEGINSWITH "http://api.example.com/" AND http.url CONTAINS "/v2/" AND !
service("api.example.com")
```

Example — filtro service y de tiempo de respuesta

Busque rastros en los que esté establecido `http url` y el tiempo de respuesta sea superior a 2 segundos.

```
http.url AND responseTime > 2
```

Para las anotaciones, puede llamar a todos los rastros en los que esté establecido `annotation.key` o utilizar los operadores de comparación que correspondan al tipo de valor.

Example – anotación con un valor de cadena

Las solicitudes con una anotación denominada `gameid` que tiene el valor de cadena `"817DL6V0"`.

```
annotation.gameid = "817DL6V0"
```

Example – la anotación está establecida

Solicitudes que tienen establecida una anotación denominada `age`.

```
annotation.age
```

Example – la anotación no está establecida

Solicitudes que no tienen establecida una anotación denominada `age`.

```
!annotation.age
```

Example – anotación con un valor numérico

Solicitudes con una edad de anotación con valor numérico mayor que 29.

```
annotation.age > 29
```

Example – anotación en combinación con service o edge

```
service { annotation.request_id = "917DL6V0" }
```

```
edge { source.annotation.request_id = "916DL6V0" }
```

```
edge { destination.annotation.request_id = "918DL6V0" }
```

Example – grupo con usuario

Solicitudes en las que los rastros cumplan los criterios del filtro de grupo `high_response_time` (p. ej.`responseTime > 3`) y el nombre del usuario sea Alice.

```
group.name = "high_response_time" AND user = "alice"
```

Example – JSON con entidad de causa raíz

Solicitudes con entidades de causa raíz coincidentes.

```
rootcause.json = #[{ "Services": [ { "Name": "GetWeatherData", "EntityPath": [{ "Name":
 "GetWeatherData" }, { "Name": "get_temperature" } ] }, { "Name": "GetTemperature",
 "EntityPath": [ { "Name": "GetTemperature" } ] } ] }]
```

función id

Cuando se proporciona un nombre de servicio a las palabras clave `service` o `edge`, se obtienen resultados de todos los nodos que tienen ese nombre. Si desea filtrar de manera más precisa, puede utilizar la función `id` para especificar un tipo de servicio, además de un nombre, para diferenciar los nodos con el mismo nombre.

Utilice la función `account.id` para especificar una cuenta concreta para el servicio cuando consulte rastros de varias cuentas de una cuenta de supervisión.

```
id(name: "service-name", type:"service::type", account.id:"account-ID")
```

Puede utilizar la función `id` en lugar de un nombre de servicio en los filtros service y edge.

```
service(id(name: "service-name", type:"service::type")) { filter }
```

```
edge(id(name: "service-one", type:"service::type"), id(name: "service-two",
 type:"service::type")) { filter }
```

Por ejemplo, AWS Lambda las funciones dan como resultado dos nodos en el mapa de rastreo: uno para la invocación de la función y otro para el servicio Lambda. Los dos nodos tienen el mismo nombre pero son de diferente tipo. Un filtro service estándar permite encontrar registros de seguimiento para ambos.

Example – filtro service

Solicitudes que incluyen un error en cualquier servicio denominado `random-name`.

```
service("function-name") { error }
```

Utilice la función `id` para limitar la búsqueda a los errores de la propia función, sin incluir los errores del servicio.

Example – filtro service con la función id

Solicitudes que incluyen un error en un servicio denominado `random-name` de tipo `AWS::Lambda::Function`.

```
service(id(name: "random-name", type: "AWS::Lambda::Function")) { error }
```

Si desea buscar nodos por tipo, también puede excluir el nombre por completo.

Example – filtro service con la función id y tipo de servicio

Solicitudes que incluyen un error en un servicio de tipo `AWS::Lambda::Function`.

```
service(id(type: "AWS::Lambda::Function")) { error }
```

Para buscar nodos para un nodo concreto Cuenta de AWS, especifique un ID de cuenta.

Example – filtro service con función id e ID de cuenta

Solicitudes que incluyen un servicio dentro de un identificador de cuenta específico `AWS::Lambda::Function`.

```
service(id(account.id: "account-id"))
```

Rastreo entre cuentas

AWS X-Ray admite la observabilidad entre cuentas, lo que le permite monitorear y solucionar problemas de las aplicaciones que abarcan varias cuentas dentro de una. Región de AWS Puede buscar, visualizar y analizar sin problemas sus métricas, registros y rastros en cualquiera de las cuentas vinculadas, como si estuviera operando en una sola cuenta. Eso le proporciona una vista completa de las solicitudes que se transfieren a varias cuentas. Puede ver los rastreos entre cuentas en el mapa de rastreo de X-Ray y en las páginas de rastreo de la CloudWatchconsola.

Los datos de observabilidad compartidos pueden incluir cualquiera de los siguientes tipos de telemetría:

- Métricas en Amazon CloudWatch
- Registrar grupos en Amazon CloudWatch Logs
- Rastros en AWS X-Ray
- Aplicaciones en Amazon CloudWatch Application Insights

Configuración de la observabilidad entre cuentas

Para activar la observabilidad entre cuentas, configure una o más cuentas de AWS monitoreo y vincúlelas con varias cuentas de origen. Una cuenta de monitoreo es una central Cuenta de AWS que puede ver e interactuar con los datos de observabilidad que se generan a partir de las cuentas de origen. Una cuenta de origen es una persona Cuenta de AWS que genera datos de observabilidad para los recursos que contiene.

Las cuentas de origen comparten sus datos de observabilidad con cuentas de supervisión. Los rastros de cada cuenta de origen se copian en un máximo de cinco cuentas de supervisión. Las copias de los rastros de las cuentas de origen en la primera cuenta de supervisión son gratuitas. Las copias de rastros enviadas a cuentas de supervisión adicionales se cargan a cada cuenta de origen, según el precio estándar. Para obtener más información, consulta AWS X-Ray los precios y los CloudWatch precios de Amazon.

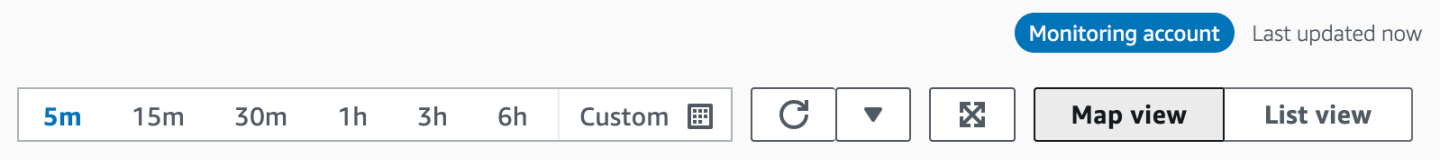
Para crear enlaces entre las cuentas de monitoreo y las cuentas de origen, usa la CloudWatch consola o los nuevos comandos de Observability Access Manager en la API AWS CLI y. Para obtener más información, consulte Observabilidad entre cuentas de CloudWatch .

> **Note**
>
> Los rastros de rayos X se facturan en el Cuenta de AWS lugar donde se reciben. Si una solicitud muestreada abarca varios servicios Cuenta de AWS, cada cuenta registra un rastreo diferente y todos los rastreos comparten el mismo identificador de rastreo. Para obtener más información sobre los precios de observabilidad entre cuentas, consulta los precios y AWS X-Ray los precios de Amazon CloudWatch .

Visualización de rastros entre cuentas

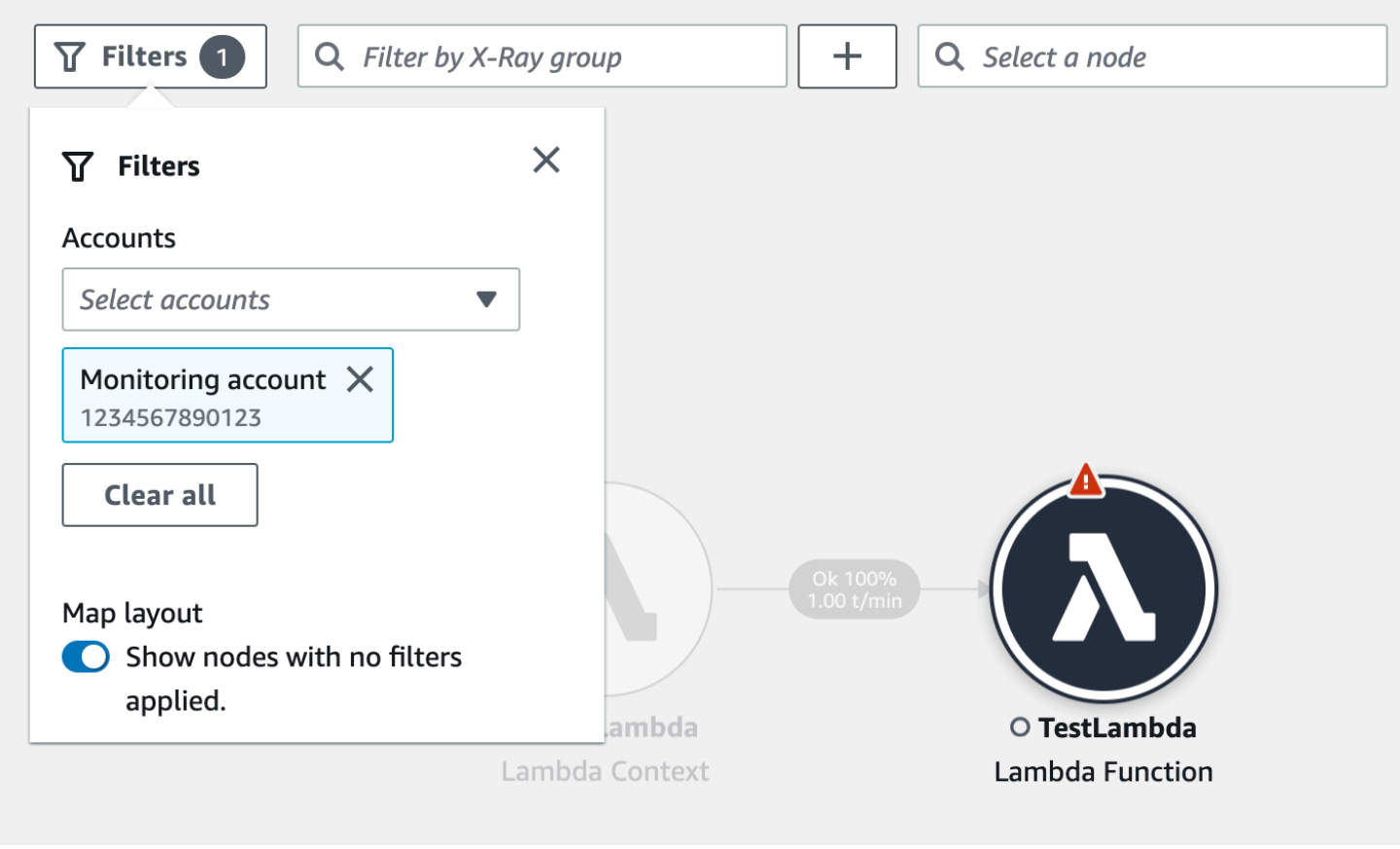
Los rastros entre cuentas se muestran en la cuenta de supervisión. Cada cuenta de origen muestra solo los rastros locales de esa cuenta específica. En las siguientes secciones se presupone que

has iniciado sesión en la cuenta de monitorización y has abierto la CloudWatch consola de Amazon. Tanto en el mapa de rastreo como en la página de rastreo, aparece una insignia de cuenta de monitoreo en la esquina superior derecha.

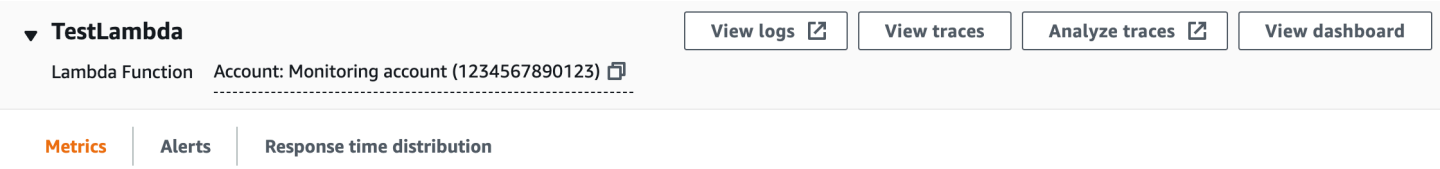


Mapa de rastreo

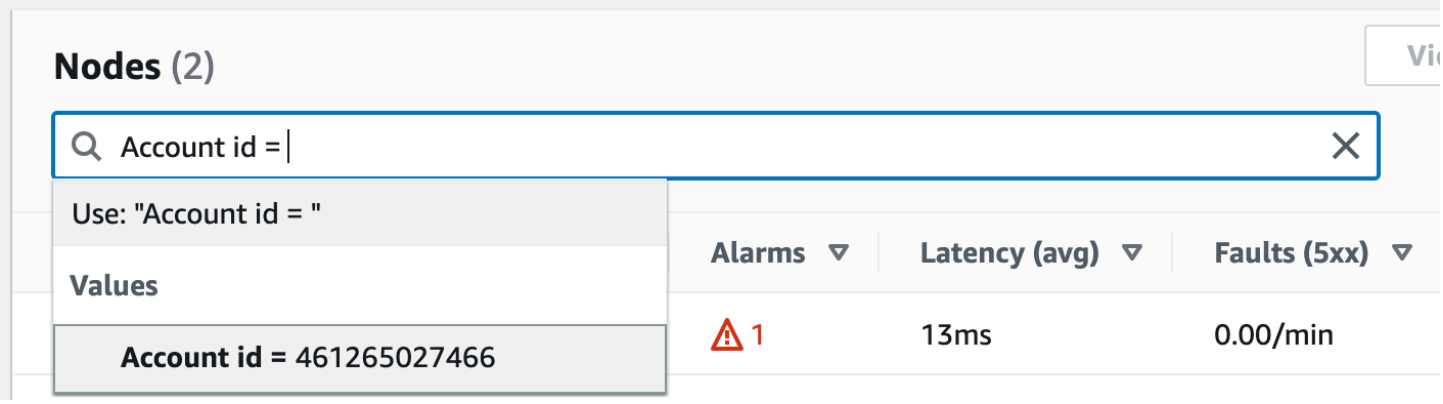
En la CloudWatch consola, elija Trace Map en Rastros de X-Ray en el panel de navegación izquierdo. De forma predeterminada, el mapa de rastreo muestra los nodos de todas las cuentas de origen que envían rastreos a la cuenta de monitoreo y los nodos de la propia cuenta de monitoreo. En el mapa de rastreo, elija Filtros en la esquina superior izquierda para filtrar el mapa de rastreo mediante el menú desplegable Cuentas. Una vez que se aplica un filtro de cuenta, los nodos de servicio de las cuentas que no coincidan con el filtro actual aparecen en color gris.



Al elegir un nodo de servicio, el panel de detalles del nodo incluye el identificador de cuenta y la etiqueta del servicio.



En la esquina superior derecha del mapa de rastreo, elija Vista de lista para ver una lista de los nodos de servicio. La lista de nodos de servicio incluye los servicios de la cuenta de supervisión y todas las cuentas de origen configuradas. Filtre la lista de nodos por Etiqueta de cuenta o por ID de cuenta seleccionándolos en el filtro de Nodos.

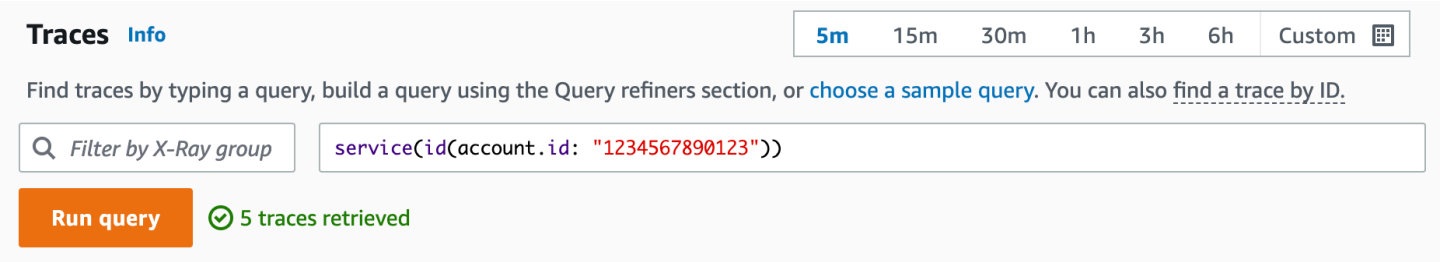


Rastros

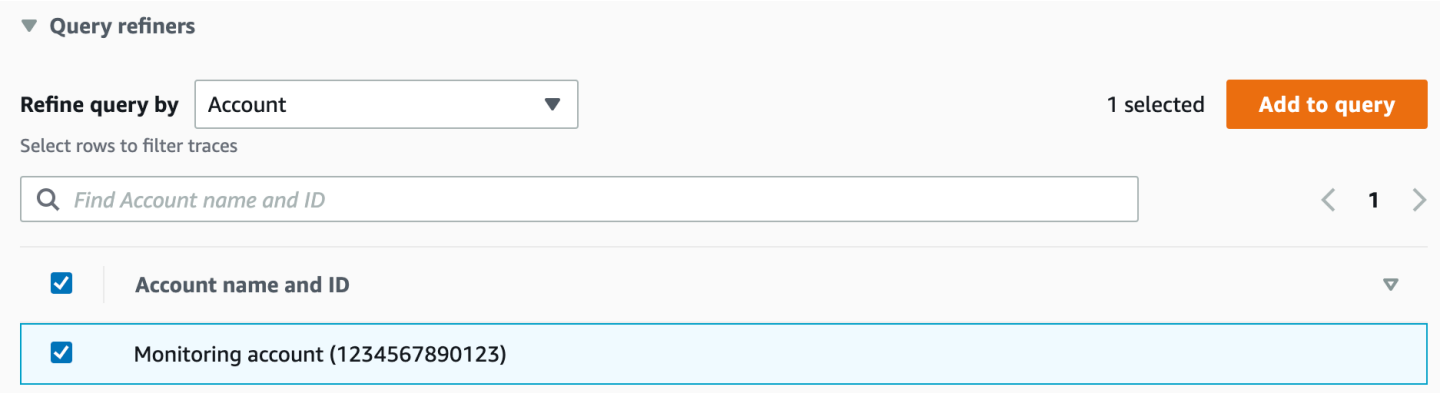
Para ver los detalles de rastreo que abarcan varias cuentas, abra la CloudWatch consola desde la cuenta de monitoreo y elija Rastros en Rastros de X-Ray en el panel de navegación izquierdo. También puede abrir esta página seleccionando un nodo en el Mapa de rastreo de rayos X y, a continuación, seleccionando Ver trazos en el panel de detalles del nodo.

La página Rastros permite realizar consultas por ID de cuenta. Para empezar, introduzca una consulta que incluya uno o más ID de cuenta. En el siguiente ejemplo se consultan rastros que hayan pasado por el ID de cuenta X o Y:

```
service(id(account.id:"X")) OR service(id(account.id:"Y"))
```



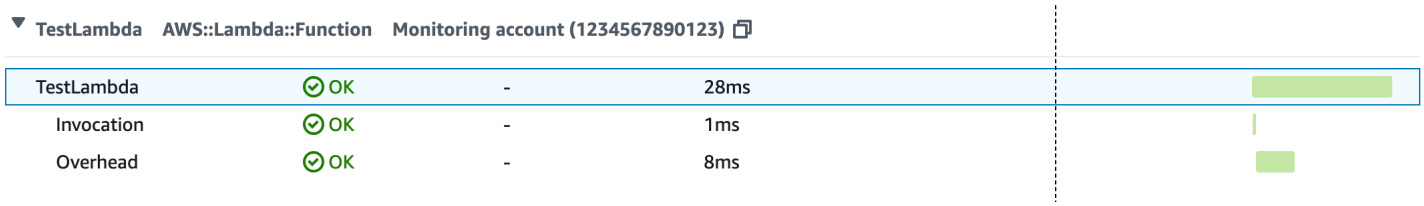
Acote su consulta por Cuenta. Seleccione una o más cuentas de la lista y elija Añadir a la consulta.



Detalles de rastros

Para ver los detalles de una rastro, selecciónelo en la lista Rastros situada en la parte inferior de la página de Rastros. Se muestran los detalles del rastreo, incluido un mapa de detalles del rastreo con los nodos de servicio de todas las cuentas por las que ha pasado el rastreo. Elija un nodo de servicio específico para ver su cuenta correspondiente.

La sección Escala de tiempo de los segmentos muestra los detalles de la cuenta de cada segmento en la escala de tiempo.



Rastreo de aplicaciones basadas en eventos

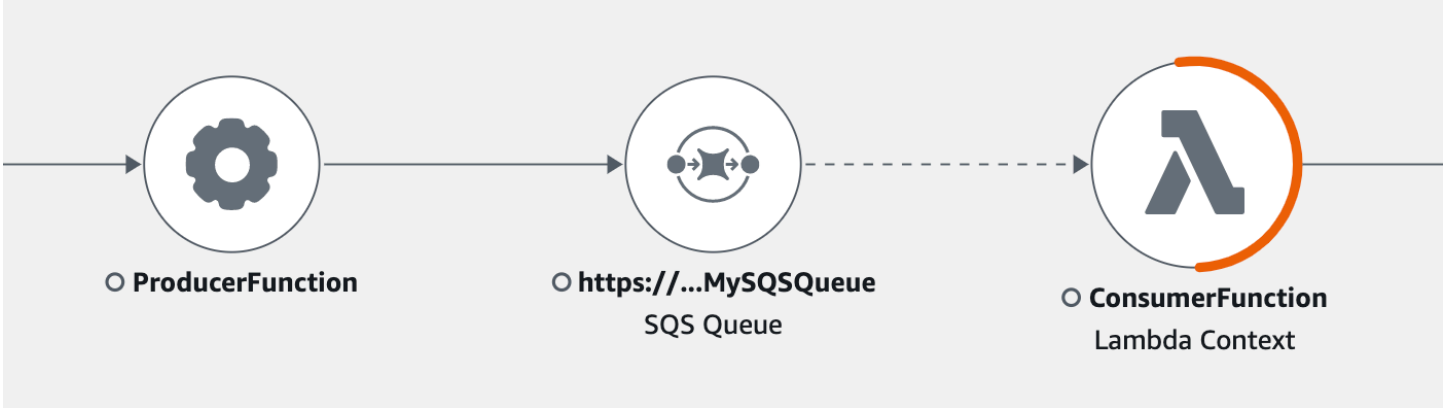
AWS X-Ray admite el seguimiento de aplicaciones basadas en eventos mediante Amazon SQS y. AWS Lambda Utilice la CloudWatch consola para ver una vista conectada de cada solicitud mientras está en cola con Amazon SQS y procesada por una o más funciones de Lambda. Las trazas de los productores de mensajes ascendentes se vinculan automáticamente a las trazas de los nodos consumidores de Lambda descendentes, lo que crea una end-to-end vista de la aplicación.

> **Note**
>
> Cada segmento de rastro se puede vincular a un máximo de 20 rastros, mientras que un rastreo puede incluir un máximo de 100 enlaces. En algunos escenarios, vincular rastros adicionales puede hacer que se exceda el tamaño máximo de documento de rastreo, lo que

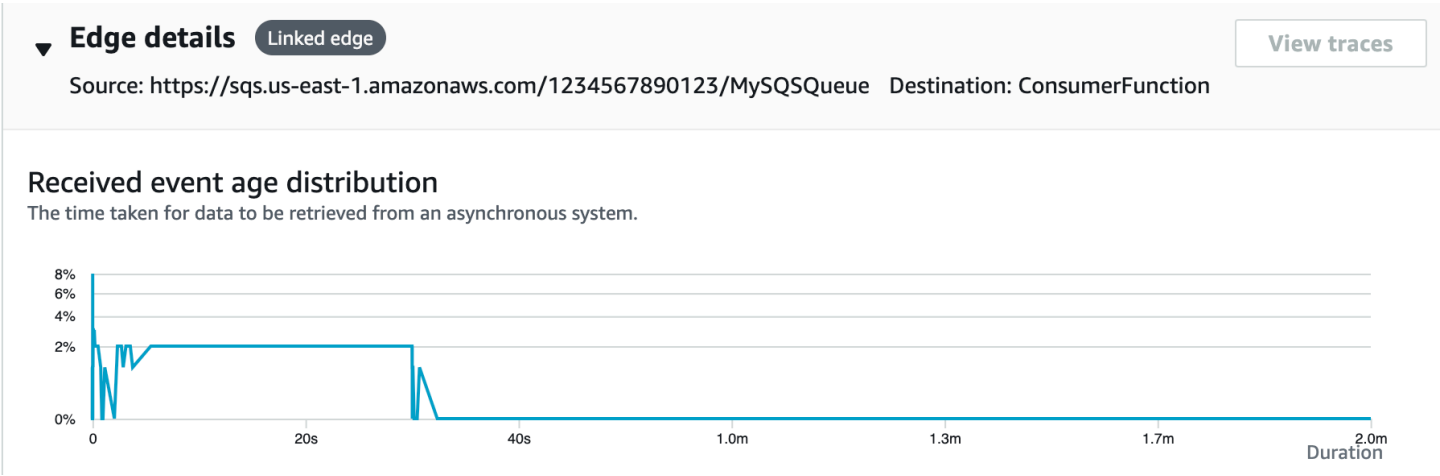
podría provocar un rastreo incompleto. Esto puede suceder, por ejemplo, cuando una función de Lambda con el rastreo habilitado envía muchos mensajes SQS a una cola en una única invocación. Si se produce este problema, hay disponible una solución de mitigación que utiliza los SDK de X-Ray. Consulte el SDK de X-Ray para Java, Node.js, Python, Go o o.NET para obtener más información.

Vea las trazas enlazadas en el mapa de trazas

Utilice la página Mapa de rastreo de la CloudWatchconsola para ver un mapa de rastreo con los rastros de los productores de mensajes que están vinculados a los rastros de los consumidores de Lambda. Estos vínculos se muestran con un borde discontinuo que conecta el nodo de Amazon SQS y los nodos de consumidores de Lambda posteriores.



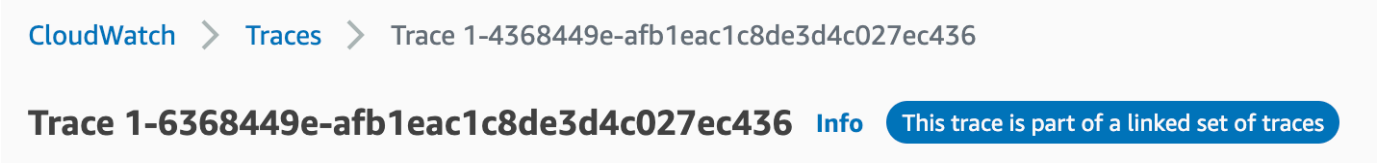
Seleccione un borde discontinuo para mostrar un histograma de antigüedad del evento recibido, que correlaciona la distribución de la antigüedad del evento cuando lo reciben los consumidores. La antigüedad se calcula cada vez que se recibe un evento.



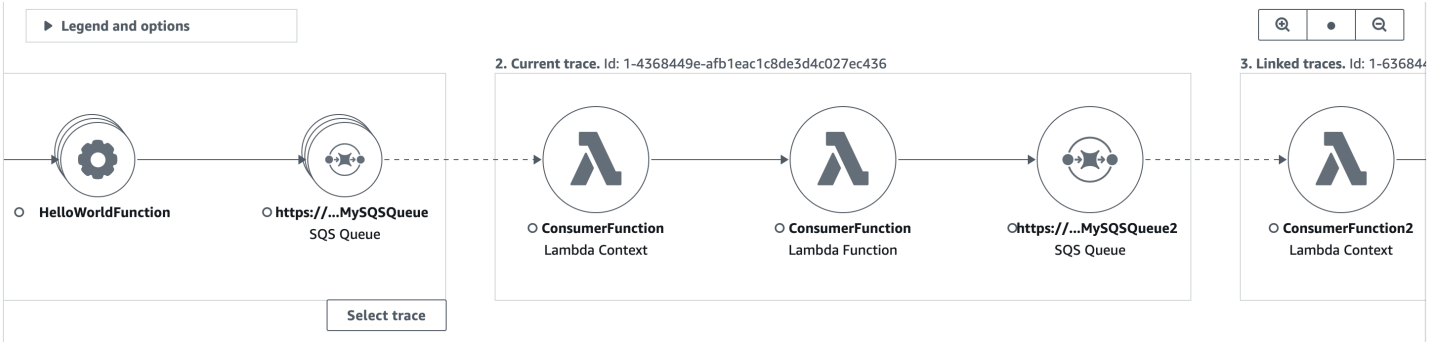
Visualización de detalles de rastreo vinculados

Vea los detalles de rastreo enviados desde un productor de mensajes, una cola de Amazon SQS o un consumidor de Lambda:

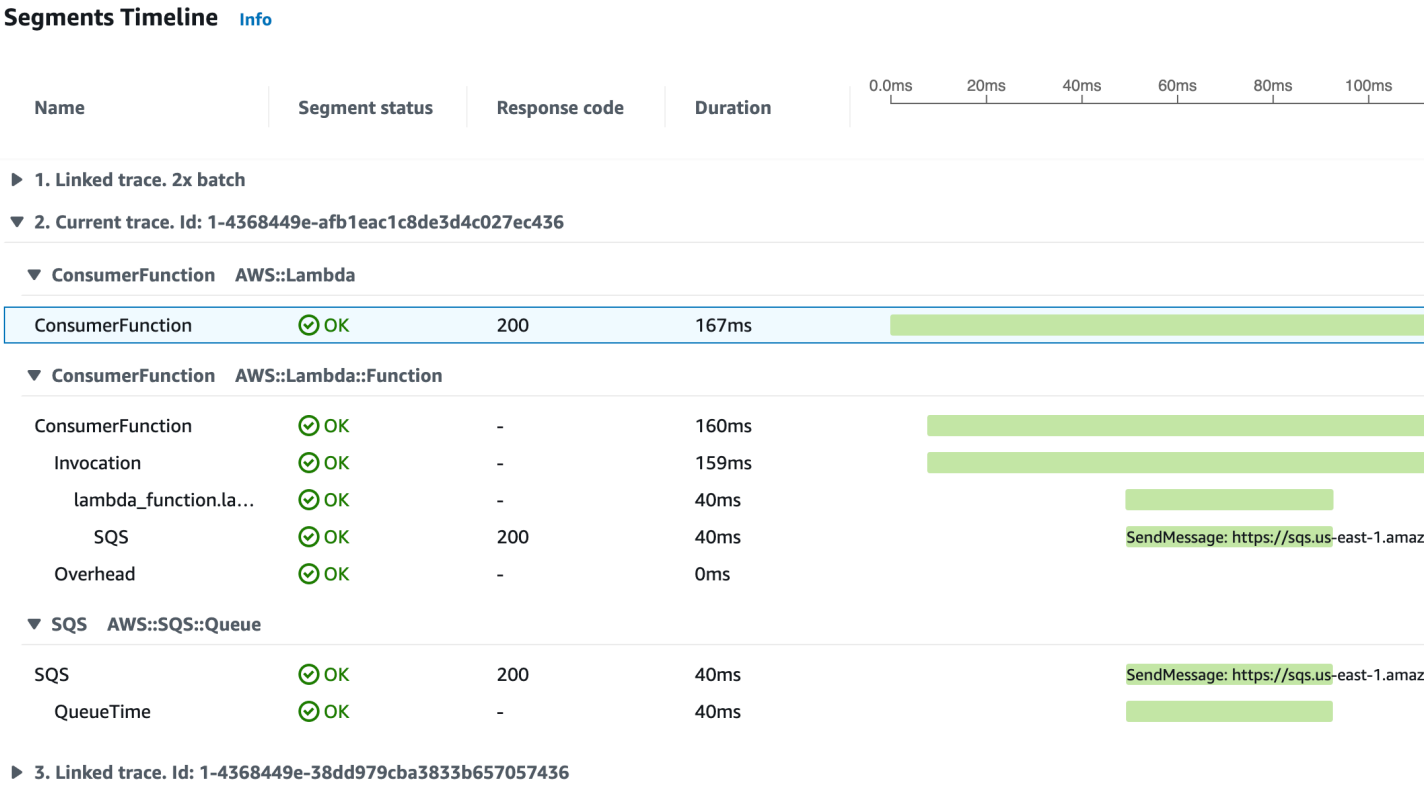
1. Utilice el mapa de rastreo para seleccionar un nodo productor de mensajes, Amazon SQS o consumidor de Lambda.
2. Seleccione Ver rastros en el panel de detalles del nodo para ver una lista de rastros. También puede navegar directamente a la página Traces de la CloudWatch consola.
3. Elija un rastro específico de la lista para abrir la página de detalles de ese rastro. La página de detalles del rastro muestra un mensaje cuando el rastro seleccionado forma parte de un conjunto de rastros vinculados.



El mapa de detalles de la traza muestra la traza actual, junto con las trazas enlazadas en sentido ascendente y descendente, cada una de las cuales se encuentra dentro de un recuadro que indica los límites de cada traza. Si el rastro actualmente seleccionado está vinculado a varios rastros precedentes o posteriores, los nodos que están dentro de los rastros vinculados precedentes o posteriores se apilan y aparece el botón Seleccionar rastro.



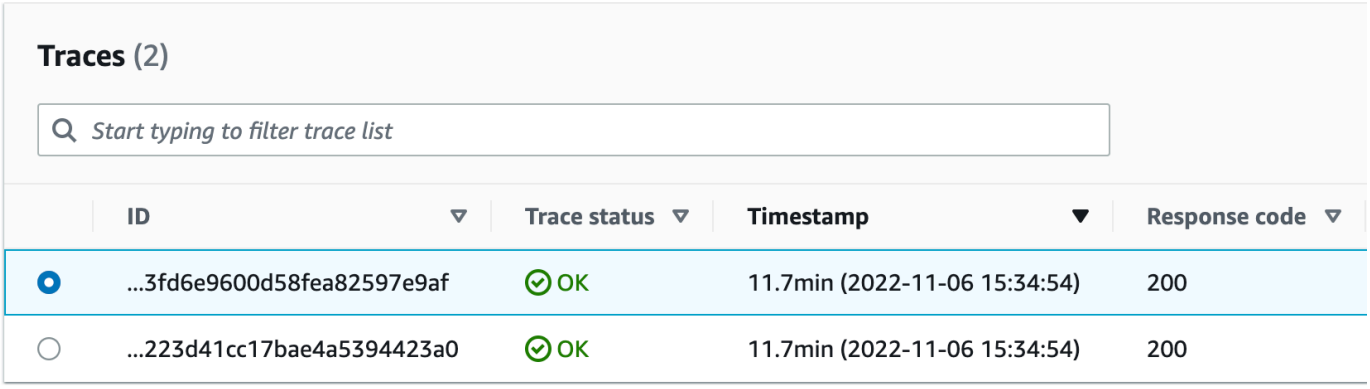
Debajo del mapa de detalles de la traza, se muestra una cronología de los segmentos de la traza, que incluye las trazas enlazadas aguas arriba y aguas abajo. Si hay varios rastros precedentes y posteriores vinculados, no se pueden mostrar los detalles de sus segmentos. Para ver los detalles del segmento de una solo rastro dentro de un conjunto de rastros vinculados, seleccione un solo rastro como se describe a continuación.



Selección de un solo rastro dentro de un conjunto de rastros vinculados

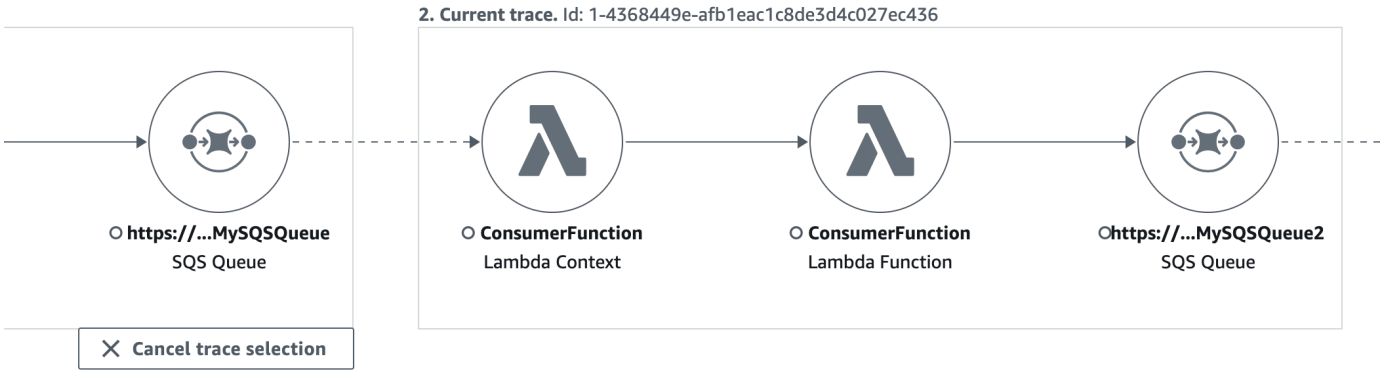
Filtre un conjunto vinculado de rastros para seleccionar un solo rastro y ver los detalles del segmento en la escala de tiempo.

1. Elija Seleccionar traza debajo de las trazas enlazadas en el mapa de detalles de la traza. Aparece una lista de rastros.



2. Seleccione el botón de radio situado junto a una traza para verla en el mapa de detalles de la traza.

3. Elija Cancelar la selección de rastro para ver todo el conjunto de rastros vinculados.



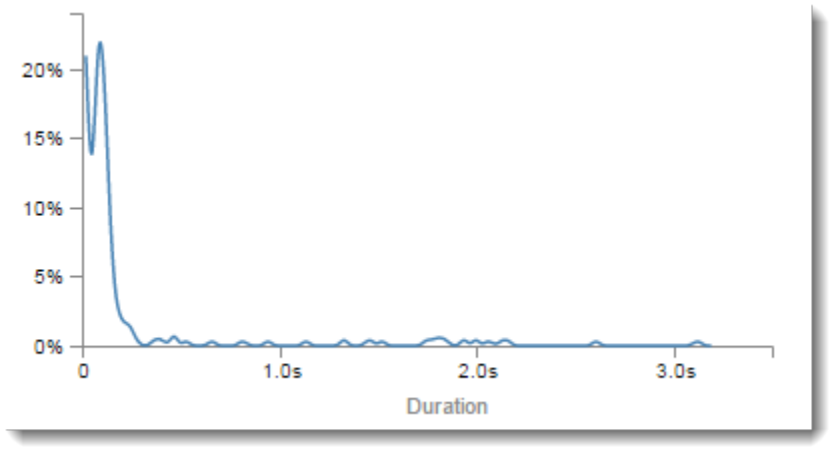
Uso de histogramas de latencia

Al seleccionar un nodo o una arista en un mapa de AWS X-Ray rastreo, la consola de X-Ray muestra un histograma de distribución de latencia.

Latencia

La latencia es el tiempo que transcurre entre el momento de iniciar una solicitud y el momento de completarla. Los histogramas muestran una distribución de las latencias. Muestran la duración en el eje x y el porcentaje de solicitudes de cada duración en el eje y.

Este histograma muestra un servicio que completa la mayor parte de las solicitudes en menos de 300 ms. Un pequeño porcentaje de solicitudes tarda hasta 2 segundos y unos cuantos casos atípicos tardan más tiempo.



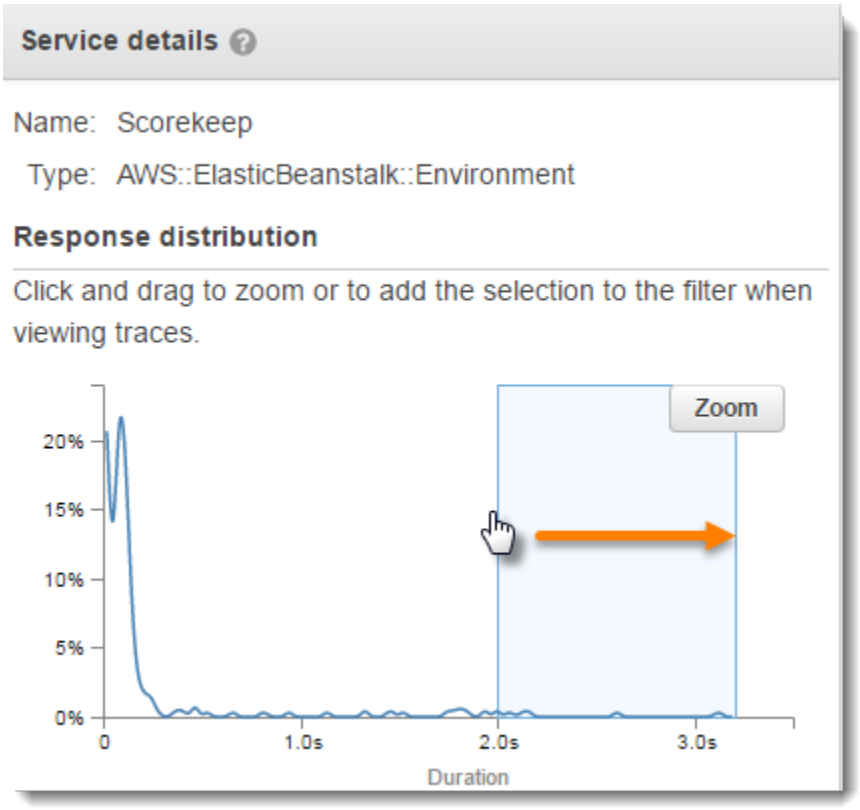
Interpretación de los detalles del servicio

Los histogramas de servicio y los histogramas de límites constituyen una representación visual de latencia desde el punto de vista de un servicio o de un solicitante.

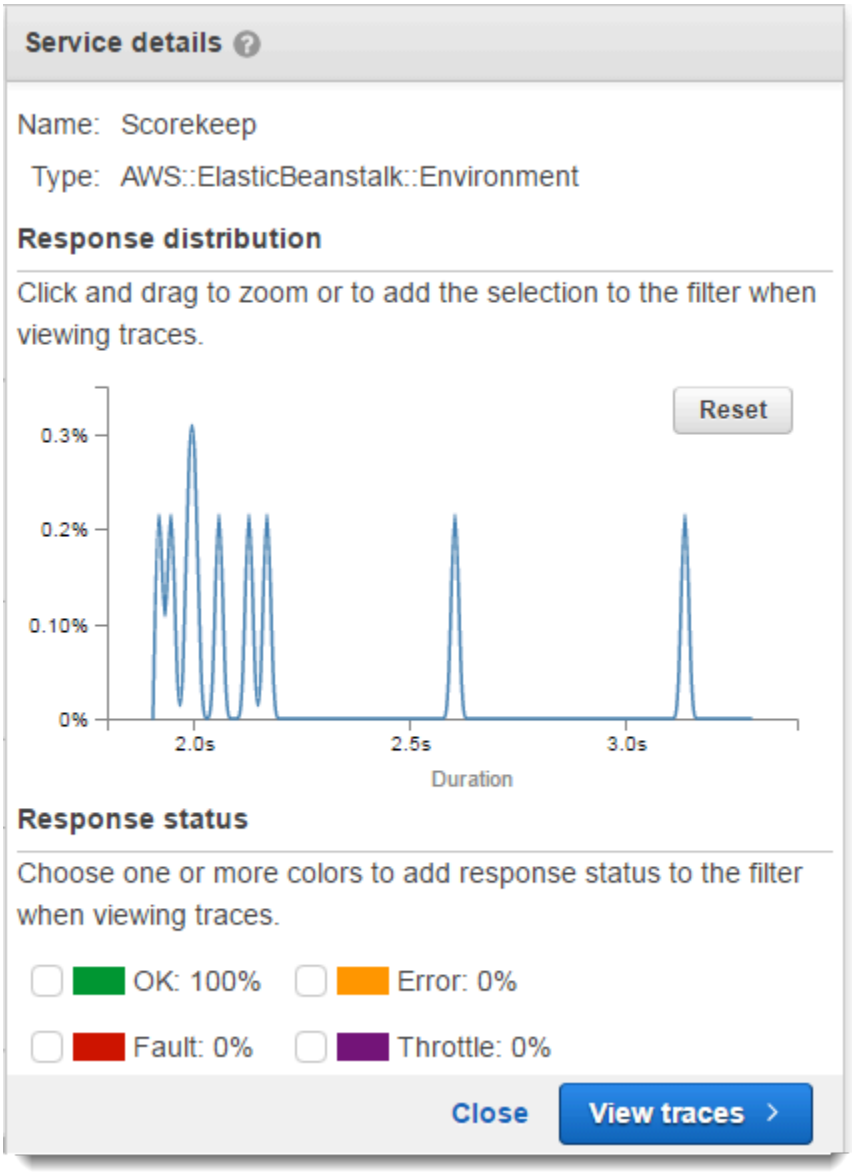
- Elija un nodo de servicio haciendo clic en el círculo. X-Ray muestra un histograma de las solicitudes que atiende el servicio. Las latencias son las que registra el servicio y no incluyen ninguna latencia de red entre el servicio y el solicitante.
- Elija un borde haciendo clic en la línea o en la punta de flecha del borde entre dos servicios. X-Ray muestra un histograma de las solicitudes del solicitante atendidas por el servicio posterior. Las latencias son las que ha registrado el solicitante e incluyen la latencia de la conexión de red entre los dos servicios.

Para interpretar el panel de histograma Service details, puede buscar los valores que más difieran de la mayoría de valores del histograma. Estos valores atípicos pueden aparecer como picos o puntas en el histograma y puede analizar los rastros de un área específica para averiguar lo que sucede.

Para ver los rastros filtrados por latencia, seleccione un intervalo en la histograma. Haga clic donde desee iniciar la selección y arrastre de izquierda a derecha para resaltar el intervalo de latencias que quiera incluir en el filtro de rastros.



Una vez seleccionado el intervalo, puede elegir Zoom (Zoom) para ver solo esa parte del histograma y retocar la selección.



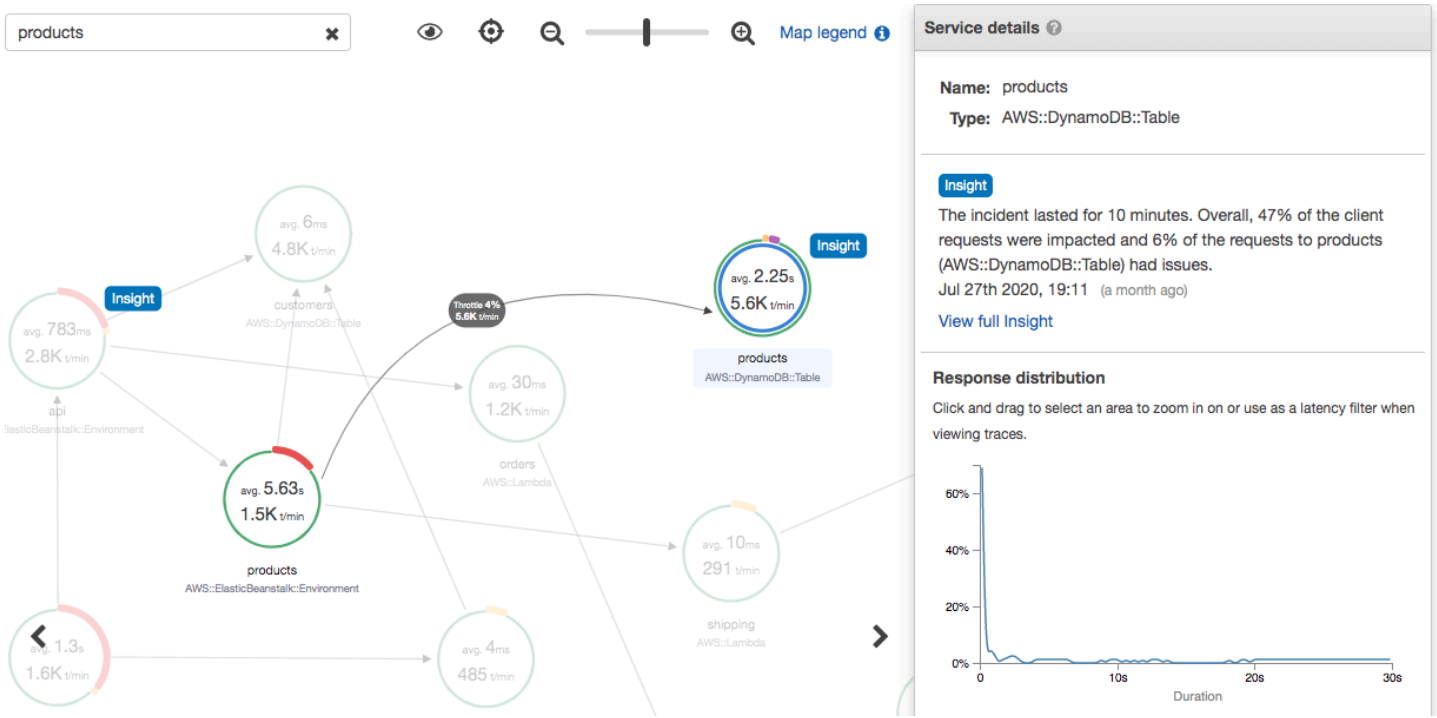
Una vez establecido el enfoque en el área que desea, elija View traces (Ver rastros).

Uso de información en X-Ray

AWS X-Ray analiza continuamente los datos de rastreo de su cuenta para identificar problemas emergentes en sus aplicaciones. Cuando las tasas de fallo superan el rango esperado, se crea una información que registra el problema y hace un seguimiento de su impacto hasta que se resuelve. Con la información, puede:

- Identificar en qué parte de su aplicación se ha producido el problema, la causa raíz del problema y el impacto asociado. El análisis de impacto que proporciona la información le permite deducir la gravedad y la prioridad de un problema.
- Reciba notificaciones a medida que el problema cambie con el tiempo. Las notificaciones de Insights se pueden integrar con tu solución de monitoreo y alertas mediante Amazon EventBridge. Esta integración le permite enviar correos electrónicos o alertas automatizados en función de la gravedad del problema.

La consola de X-Ray identifica los nodos con incidentes en curso en el mapa de rastreo. Para ver un resumen de la información, elija el nodo afectado. También puede ver y filtrar la seleccionando Información en el panel de navegación de la izquierda.



X-Ray crea información cuando detecta una anomalía en uno o más nodos del mapa de servicio. El servicio utiliza modelos estadísticos para predecir las tasas de fallo que cabe esperar de los servicios de su aplicación. En el ejemplo anterior, la anomalía es un aumento de las fallas de AWS Elastic Beanstalk. El servidor de Elastic Beanstalk agotó varias veces los tiempos de espera de llamadas a la API, lo que provocó una anomalía en los nodos posteriores.

Habilite la información en la consola de X-Ray

La información debe estar habilitada para cada grupo con el que desee utilizar las características de información. Puede activar la información desde la página Grupos.

1. Abra la consola de X-Ray.
2. Seleccione un grupo existente o cree uno nuevo seleccionando Crear grupo y, a continuación, seleccione Habilitar Información. Para obtener más información acerca de la configuración de grupos en la consola de X-Ray, consulte Configuración de grupos.
3. En el panel de navegación de la izquierda, elija Información y, luego, elija la información que desee ver.

Note

X-Ray utiliza operaciones de GetInsightImpactGraph API y GetInsightSummaries GetInsight GetInsightEvents, para recuperar datos a partir de información. Para ver información, utilice la política gestionada de AWSXrayReadOnlyAccess IAM o añada la siguiente política personalizada a su función de IAM:

```
{
   "Version": "2012-10-17",
   "Statement": [
       {
           "Effect": "Allow",
           "Action": [
               "xray:GetInsightSummaries",
               "xray:GetInsight",
               "xray:GetInsightEvents",
               "xray:GetInsightImpactGraph"
           ],
           "Resource": [
               "*"
           ]
       }
   ]
}
```

Para obtener más información, consulte Cómo AWS X-Ray funciona con IAM.

Habilitación de notificaciones de la información

Con las notificaciones de información, se crea una notificación para cada evento de información, por ejemplo, cuando se crea una información, cambia significativamente o se cierra. Los clientes pueden recibir estas notificaciones a través de EventBridge eventos de Amazon y usar reglas condicionales para realizar acciones como la notificación de SNS, la invocación de Lambda, la publicación de mensajes en una cola de SQS o cualquiera de las opciones admitidas por Target. EventBridge Las notificaciones de información se emiten en la medida de lo posible, pero no están garantizadas. Para obtener más información sobre los objetivos, consulte Amazon EventBridge Targets.

En la página Grupos puede habilitar las notificaciones de información para cualquier grupo que tenga información habilitada.

Habilitación de notificaciones para un grupo de X-Ray

1. Abra la consola de X-Ray.
2. Seleccione un grupo existente o cree uno nuevo seleccionando Crear grupo, asegúrese de que Habilitar información esté seleccionado y, a continuación, seleccione Habilitar Información. Para obtener más información acerca de la configuración de grupos en la consola de X-Ray, consulte Configuración de grupos.

Para configurar las reglas EventBridge condicionales de Amazon

1. Abre la EventBridge consola de Amazon.
2. Vaya a Reglas en la barra de navegación izquierda y elija Crear regla.
3. Escriba un nombre y una descripción para la regla.
4. Elija Patrón de eventos y, a continuación, Patrón personalizado. Proporcione un patrón que contenga `"source": [ "aws.xray" ]` y `"detail-type": [ "AWS X-Ray Insight Update" ]`. A continuación se muestran algunos ejemplos de posibles patrones.
   - Patrón de eventos que coincide con todos los eventos entrantes de información de X-Ray:

```
{
"source": [ "aws.xray" ],
"detail-type": [ "AWS X-Ray Insight Update" ]
```

```
}
```

- Patrón de eventos que coincide con un valor especificado de **`state`** y **`category`**:

```
{
"source": [ "aws.xray" ],
"detail-type": [ "AWS X-Ray Insight Update" ],
"detail": {
        "State": [ "ACTIVE" ],
        "Category": [ "FAULT" ]
  }
}
```

5. Seleccione y configure los destinos que desee invocar cuando un evento cumpla esta regla.
6. (Opcional) Proporcione etiquetas para identificar y seleccionar esta regla con mayor facilidad.
7. Seleccione Crear.

> **Note**
>
> Las notificaciones de X-Ray Insights envían eventos a Amazon EventBridge, que actualmente no admite claves gestionadas por el cliente. Para obtener más información, consulte Protección de los datos en AWS X-Ray.

Visión general acerca de la información

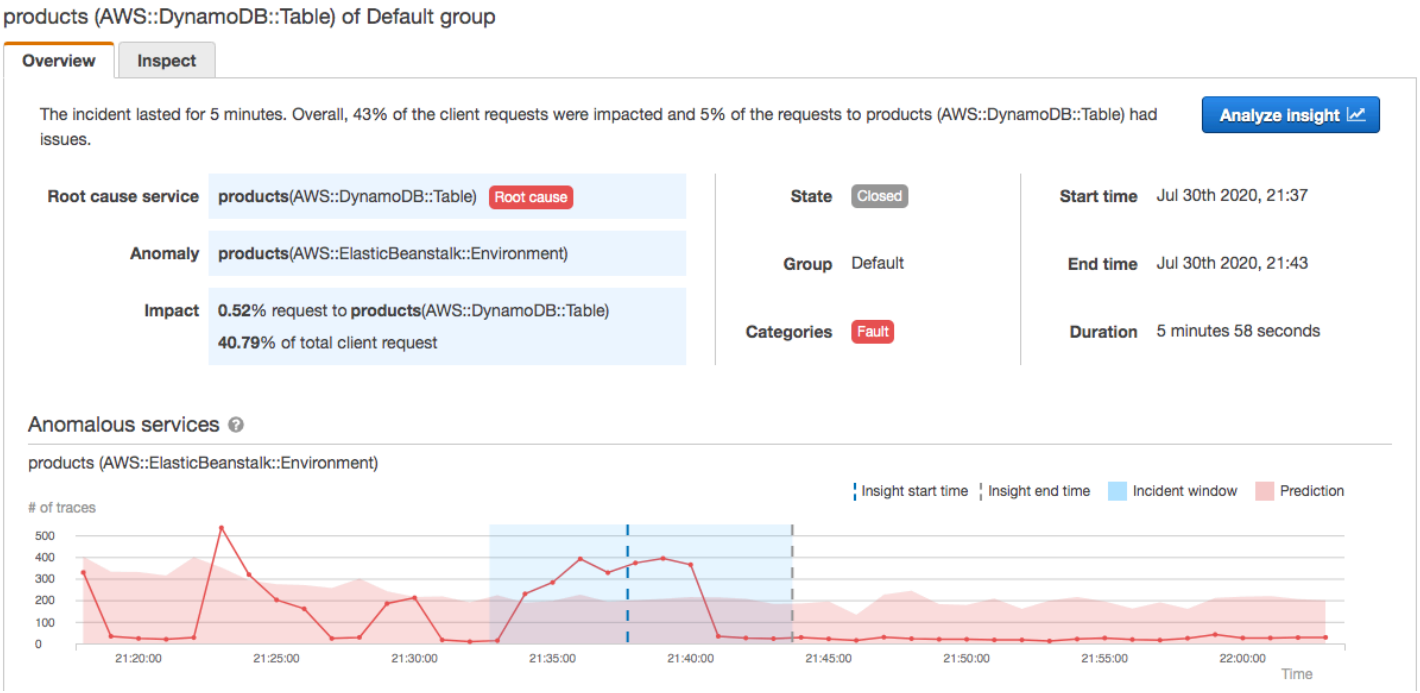
En la página de información general de una información se intenta responder a tres preguntas clave:

- ¿Cuál es el problema de fondo?
- ¿Cuál es la causa raíz?
- ¿Cuál es el impacto?

La sección Servicios anómalos muestra una escala de tiempo para cada servicio que ilustra el cambio en las tasas de fallo durante el incidente. La escala de tiempo muestra el número de rastros con fallos superpuestos en una banda continua que indica el número esperado de fallos en función de la cantidad de tráfico registrada. La duración de la información se visualiza en la ventana de

incidentes. La ventana de incidentes comienza cuando X-Ray observa que la métrica se vuelve anómala y persiste mientras la información está activa.

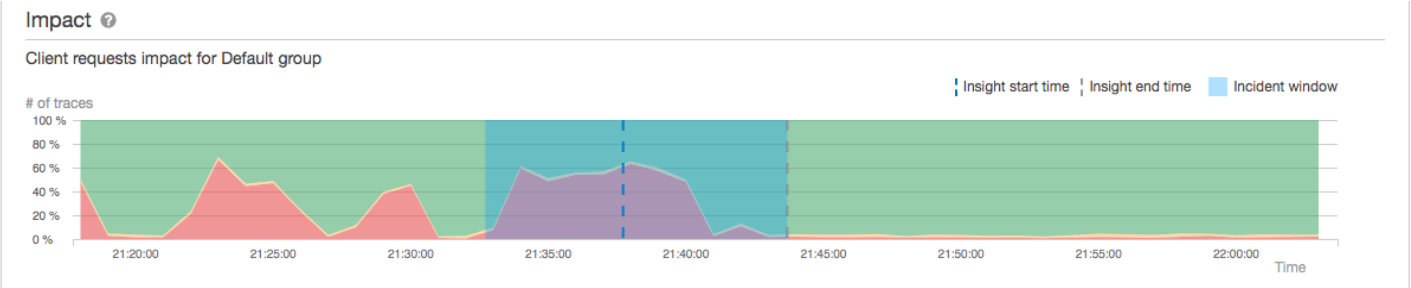
En el siguiente ejemplo se muestra un aumento en el número de fallos, lo que ha provocado un incidente:



La sección de causa raíz muestra un mapa de rastreo centrado en la causa raíz del servicio y la ruta afectada. Puede ocultar los nodos no afectados seleccionando el icono en forma de ojo en la parte superior derecha del mapa de la causa raíz. El servicio de causa raíz es el nodo posterior más alejado en el que X-Ray identificó una anomalía. Puede representar un servicio que usted instrumentó o un servicio externo al que su servicio llamó con un cliente instrumentado. Por ejemplo, si llama a Amazon DynamoDB con un cliente de SDK AWS instrumentado, si aumenta el número de errores de DynamoDB, se obtiene una idea de que DynamoDB es la causa principal.

Para investigar más a fondo la causa raíz, seleccione Ver los detalles de la causa raíz en el gráfico de la causa raíz. Puede usar la página Análisis para investigar la causa raíz y los mensajes relacionados con ella. Para obtener más información, consulte Interacción con la consola de Analytics.

Los fallos que continúan hacia arriba en el mapa pueden afectar a varios nodos y provocar múltiples anomalías. Si un fallo se transfiere hasta el usuario que realizó la solicitud, el resultado es un fallo de cliente. Se trata de un error en el nodo raíz del mapa de rastreo. El gráfico Impacto proporciona una escala de tiempo de la experiencia del cliente para todo el grupo. Esta experiencia se calcula en función de los porcentajes de los siguientes estados: fallo, error, limitación y bien.



En este ejemplo se muestra un aumento en el número de rastros con un fallo en el nodo raíz durante el momento de un incidente. Los incidentes en los servicios posteriores no siempre se corresponden con un aumento de los errores de cliente.

Al elegir Analizar información, se abre la consola de X-Ray Analytics en una ventana en la que se puede profundizar en el conjunto de rastros que han generado la información. Para obtener más información, consulte Interacción con la consola de Analytics.

Descripción del impacto

AWS X-Ray mide el impacto causado por un problema continuo como parte de la generación de información y notificaciones. El impacto se mide de dos formas:

- Impacto en el grupo de X-Ray
- Impacto en el servicio de la causa raíz

Este impacto viene determinado por el porcentaje de solicitudes que fallan o que provocan un error en un período de tiempo determinado. Este análisis de impacto le permite determinar la gravedad y la prioridad del problema en función de su situación particular. Este impacto está disponible como parte de la experiencia con la consola, además de las notificaciones de información.

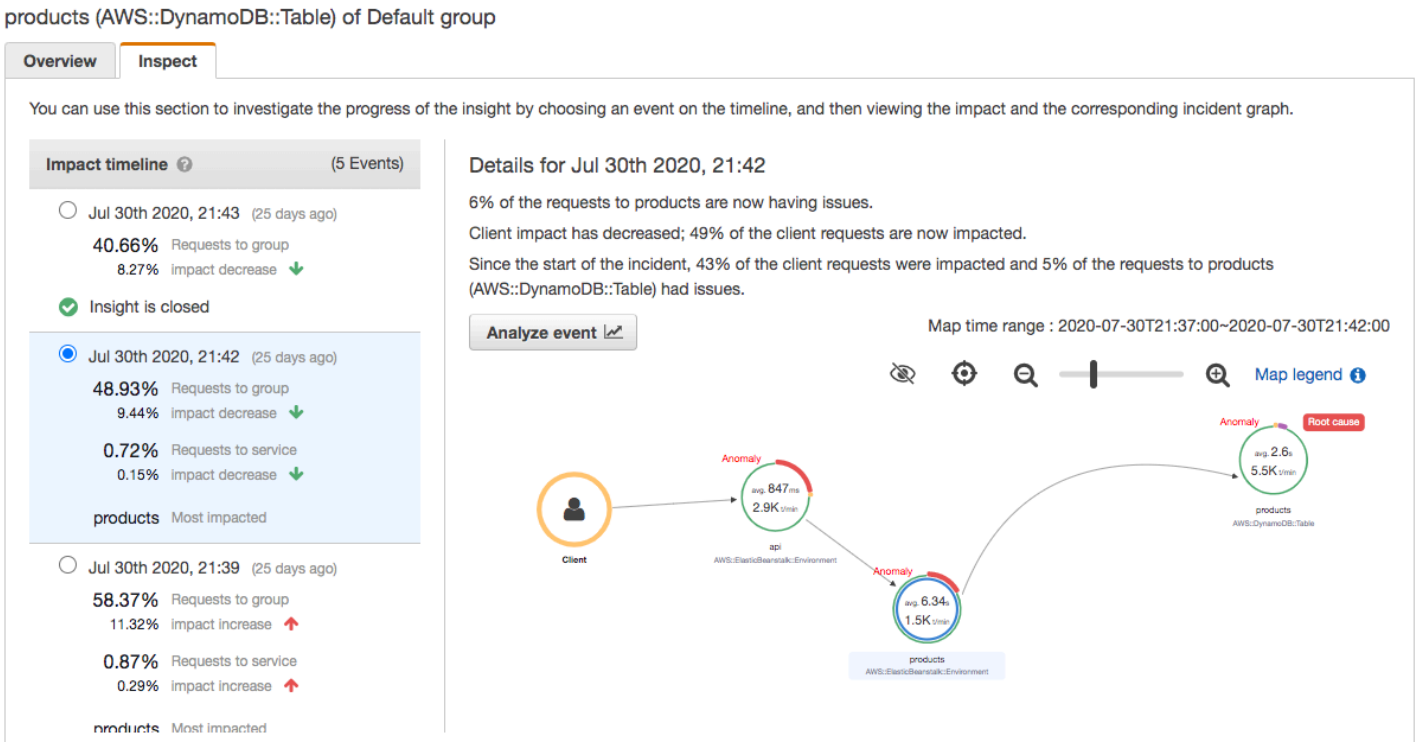
Desduplicación

AWS X-Ray insights desduplica los problemas en varios microservicios. Utiliza la detección de anomalías para determinar el servicio que es la causa principal de un problema, determina si otros servicios relacionados con él presentan un comportamiento anómalo debido a la misma causa raíz y registra el resultado como una sola información.

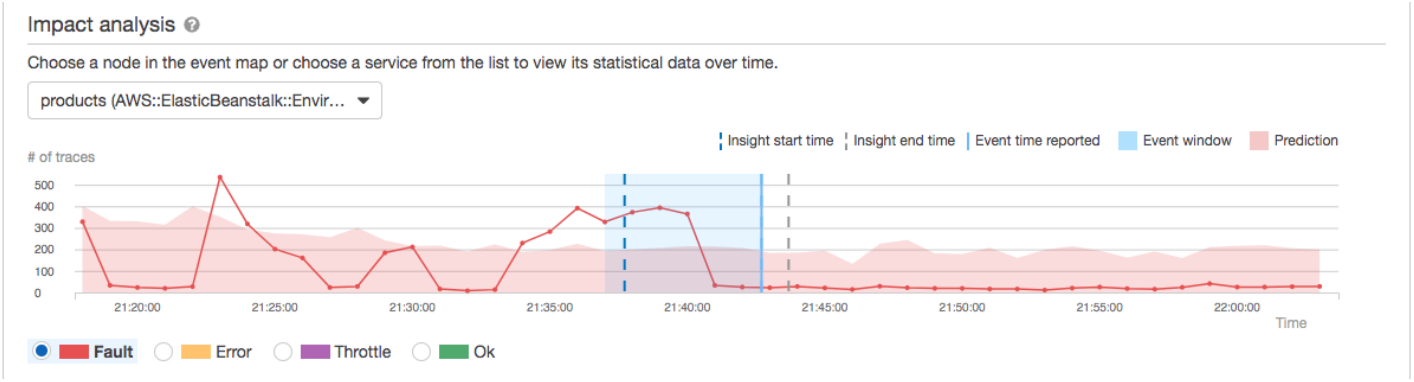
Revisión del progreso de una información

X-Ray reevalúa la información periódicamente hasta que se resuelve y registra cada cambio intermedio notable como una notificación, que se puede enviar como un evento de Amazon EventBridge . Esto le permite crear procesos y flujos de trabajo para determinar cómo ha cambiado el problema a lo largo del tiempo y tomar las medidas adecuadas, como enviar un correo electrónico o integrarlos en un sistema de alertas mediante. EventBridge

Puede revisar los eventos de los incidentes en la escala de tiempo del impacto, en la página Inspeccionar. De forma predeterminada, la escala de tiempo muestra el servicio más afectado hasta que el usuario elige un servicio diferente.



Para ver un mapa de rastreo y gráficos de un evento, elíjalo en la cronología del impacto. El mapa de rastreo muestra los servicios de su aplicación que se ven afectados por el incidente. En Análisis del impacto, los gráficos muestran las líneas de tiempo de los fallos correspondientes al nodo seleccionado y los clientes del grupo.



Para analizar en profundidad los rastros implicados en un incidente, elija Analizar evento en la página Inspeccionar. Puede utilizar la página Análisis para acotar la lista de rastros e identificar a los usuarios afectados. Para obtener más información, consulte Interacción con la consola de Analytics.

Interacción con la consola de Analytics

La consola de AWS X-Ray Analytics es una herramienta interactiva para interpretar los datos de rastreo y comprender rápidamente el rendimiento de su aplicación y sus servicios subyacentes. La consola le permite explorar, analizar y visualizar los registros de seguimiento a través de gráficos de tiempo de respuesta y series temporales.

Al realizar selecciones en la consola de Analytics, la consola crea filtros para reflejar el subconjunto seleccionado de registros de seguimiento. Puede acotar el conjunto de datos con filtros cada vez más detallados haciendo clic en los gráficos y los paneles de métricas y campos asociados al conjunto de registros de seguimiento actual.

Temas

Características de la consola

La consola de X-Ray Analytics utiliza las siguientes características principales para agrupar, filtrar, comparar y cuantificar los datos de rastreo.

Características

Característica	Descripción
Grupos	El grupo seleccionado inicial es `Default`. Para cambiar el grupo recuperado, seleccione un

Característica	Descripción
	grupo diferente en el menú que se encuentra a la derecha de la barra de búsqueda principal de expresiones de filtro. Para obtener más información sobre los grupos, consulte Uso de expresiones de filtro con grupos.
Retrieved traces (Registros de seguimiento recuperados)	De forma predeterminada, la consola de Analytics genera gráficos basados en todos los registros de seguimiento del grupo seleccion ado. Los registros de seguimiento recuperados representan todos los registros de seguimien to del conjunto de trabajo. Puede ver el número de registros de seguimiento en este icono. Las expresiones de filtro que se aplican a la barra de búsqueda principal acotan y actualizan los registros de seguimiento recuperados.
Show in charts/Hide from charts (Mostrar y ocultar de gráficos)	Un control de alternancia para comparar el grupo activo con los registros de seguimiento recuperados. Para comparar los datos relativos al grupo con los filtros activos, elija Show in charts (Mostrar en gráficos). Para eliminar esta vista de los gráficos, elija Hide from charts (Ocultar de gráficos).
Filtered trace set A (Conjunto de registros de seguimiento filtrados A)	A través de interacciones con los gráficos y las tablas, aplique filtros para crear los criterios del conjunto de rastros filtrados A. Cuando se aplican los filtros, el número de rastros aplicables y el porcentaje de rastros que se recupera se calculan en este icono. Los filtros se rellenan como etiquetas dentro del icono Filtered trace set A (Conjunto de registros de seguimiento A filtrados) y también se pueden eliminar del icono.

Característica	Descripción
Refine (Acotar)	Esta función actualiza el conjunto de registros de seguimiento recuperados en función de los filtros aplicados al conjunto de registros de seguimiento A. Al reajustar el conjunto de registros de seguimiento recuperado se actualiza el conjunto de trabajo de todos los registros de seguimiento recuperados en función de los filtros del conjunto de registros de seguimiento A. El conjunto de trabajo de registros de seguimiento recuperados es un subconjunto muestreado de todos los registros de seguimiento del grupo.
Filtered trace set B (Conjunto de registros de seguimiento filtrados B)	Cuando se crea, el conjunto de rastros filtrados B es una copia del conjunto de rastros filtrados A. Para comparar los dos conjuntos de rastros, seleccione nuevos filtros, que se aplicarán al conjunto de rastros B, mientras que el conjunto A permanece fijo. Cuando se aplican los filtros, se calcula el número de registros de seguimien to aplicables y el porcentaje de registros de seguimiento del total recuperado en este icono. Los filtros se rellenan como etiquetas dentro del icono Filtered trace set B (Conjunto de registros de seguimiento B) y también se pueden eliminar del icono.

Característica	Descripción
Response Time Root Cause Entity Paths (Rutas de entidad de causa raíz de tiempo de respuesta)	Una tabla de rutas de entidad registradas. X-ray determina qué ruta del rastro del usuario es la causa más probable del tiempo de respuesta . El formato indica una jerarquía de entidades detectadas, que termina en una causa raíz de tiempo de respuesta. Utilice estas filas para filtrar errores de tiempo de respuesta recurrentes. Para obtener más información sobre cómo personalizar un filtro de causa raíz y obtener los datos a través de la API, consulte Recuperación y reajuste de análisis de causa raíz.
Delta (�)	Una columna que se agrega a las tablas de métricas cuando los conjuntos de registros de seguimiento A y B están activos. La columna Delta calcula la diferencia porcentual de los registros de seguimiento entre el conjunto de registros de seguimiento A y el conjunto de registros de seguimiento B.

Distribución del tiempo de respuesta

La consola de X-Ray Analytics genera dos gráficos principales que ayudan al usuario a visualizar rastros: Distribución del tiempo de respuesta y Actividad de series temporales. En esta sección y las siguientes se proporcionan ejemplos de cada uno y se explican los aspectos básicos de cómo leer los gráficos.

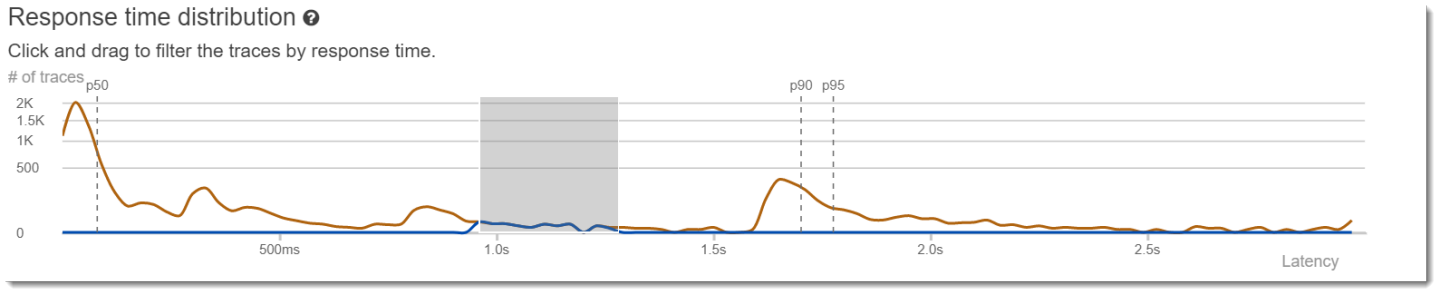
A continuación se indican los colores asociados al gráfico de líneas de tiempo de respuesta (el gráfico de series temporales utiliza la misma combinación de colores):

- Todas las trazas del grupo: gris
- Rastros recuperados: naranja
- Conjunto de rastros filtrados A: verde

- Conjunto de rastros filtrados B: azul

Example – Distribución del tiempo de respuesta

La distribución del tiempo de respuesta es un gráfico que muestra el número de registros de seguimiento con un tiempo de respuesta determinado. Haga clic y arrastre para realizar selecciones en la distribución del tiempo de respuesta. De esta forma, se selecciona y se crea un filtro del conjunto de registros de seguimiento de trabajo llamado `responseTime` para todos los registros de seguimiento de un tiempo de respuesta específico.

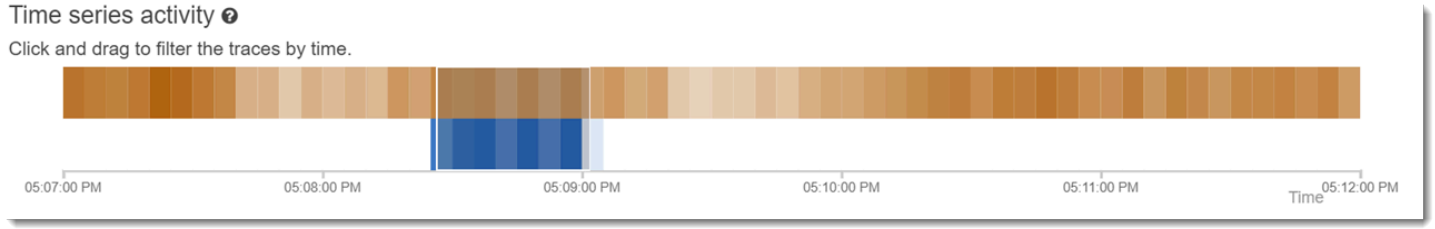


Actividad de series temporales

El gráfico de actividad de series temporales muestra el número de registros de seguimiento en un periodo de tiempo determinado. Los indicadores de color reflejan los colores del gráfico de líneas de la distribución del tiempo de respuesta. Cuanto más oscuro y opaco es el bloque de color de las series de actividad, más registros de seguimiento se representan en el momento especificado.

Example – Actividad de series temporales

Haga clic y arrastre para realizar selecciones dentro del gráfico de actividad de series temporales. De esta forma, se selecciona y se crea un filtro llamado `timerange` en el conjunto de registros de seguimiento de trabajo para todos los registros de seguimiento en un periodo de tiempo específico.



Ejemplos de flujo de trabajo

Los siguientes ejemplos muestran casos de uso comunes de la consola de X-Ray Analytics. Cada ejemplo muestra una función clave de la experiencia de la consola. En su conjunto, los ejemplos

siguen un flujo de trabajo de solución de problemas básico. Los pasos describen cómo detectar primero los nodos en mal estado y, a continuación, cómo interactuar con la consola de Analytics para generar automáticamente consultas comparativas. Una vez que haya reducido el alcance a través de las consultas, verá los detalles de los registros de seguimiento de interés para determinar qué está dañando el estado del servicio.

Observar errores en el gráfico de servicio

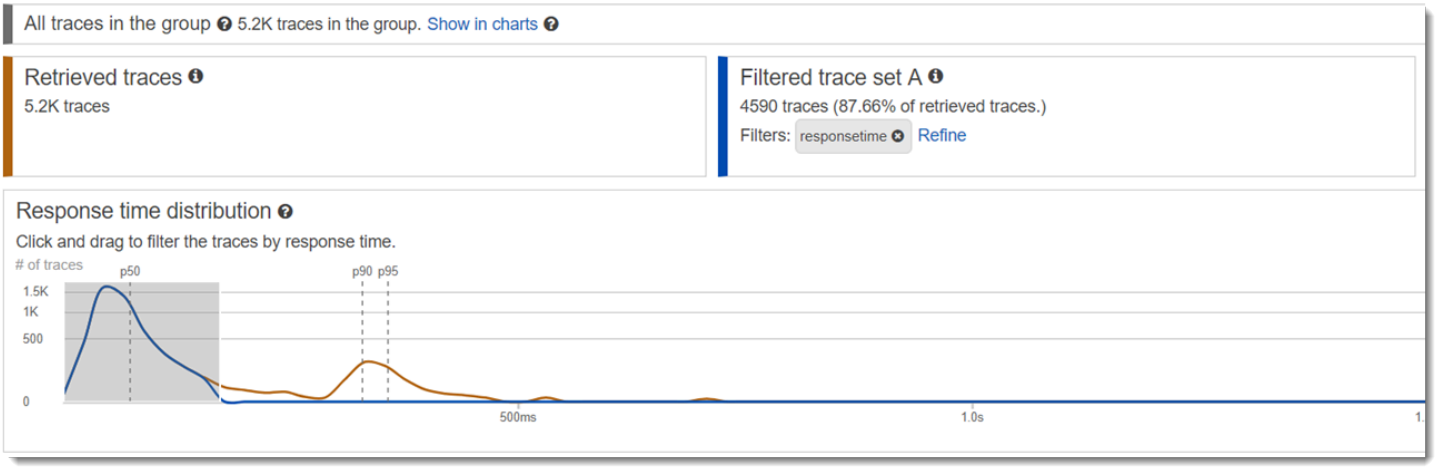
El mapa de rastreo indica el estado de cada nodo coloreándolo en función de la proporción entre llamadas correctas y errores y fallas. Cuando vea un porcentaje en rojo en el nodo, eso indica un error. Utilice la consola de X-Ray Analytics para investigar el problema.

Para obtener más información sobre cómo leer el mapa de rastreo, consulte Visualización del mapa de rastreo.

Identificar los picos de tiempo de respuesta

Mediante la distribución del tiempo de respuesta, puede observar los picos de tiempo de respuesta. Al seleccionar el pico en el tiempo de respuesta, las tablas que se encuentran debajo de los gráficos se actualizarán para mostrar las métricas asociadas, como los códigos de estado.

Al hacer clic y arrastrar, X-Ray selecciona y crea un filtro. Se muestra sombreado en gris encima de las líneas gráficas. Ahora puede arrastrar ese elemento resaltado a la izquierda o a la derecha por la distribución para actualizar su selección y filtro.



Consultar todos los registros de seguimiento marcados con un código de estado

Puede analizar los registros de seguimiento dentro del pico seleccionado mediante las tablas de métricas que se encuentran debajo de los gráficos. Al hacer clic en una fila de la tabla HTTP STATUS CODE, se crea automáticamente un filtro en el conjunto de datos de trabajo. Por ejemplo, puede ver todos los registros de seguimiento de código de estado 500. Esto crea una etiqueta de filtro en el icono del conjunto de registros de seguimiento llamado `http.status`.

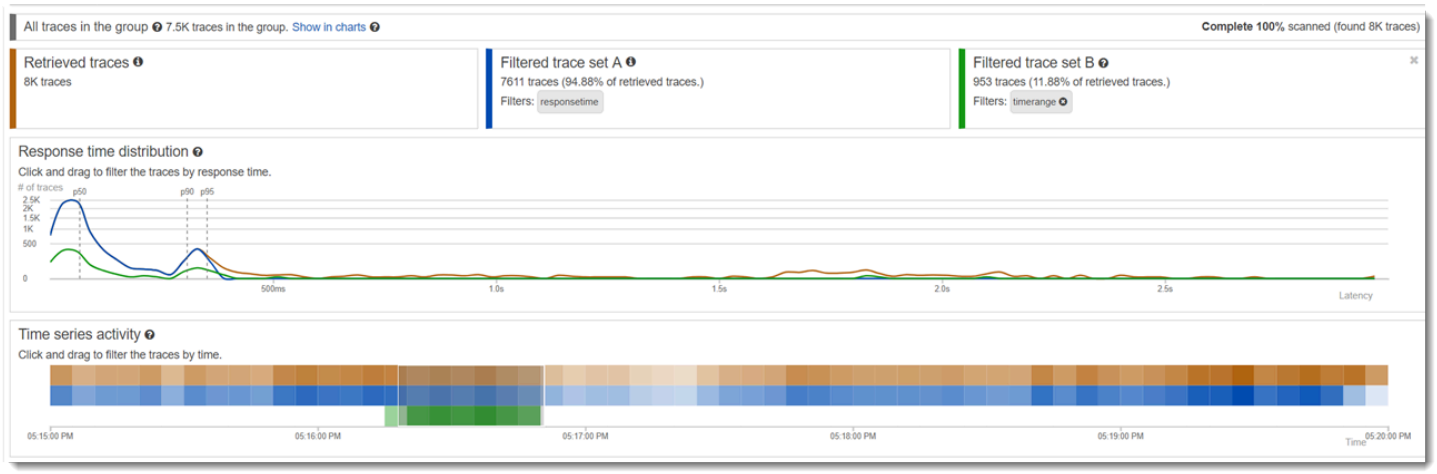
Consultar todos los elementos de un subgrupo y asociados a un usuario

Examine el conjunto de errores en función del usuario, URL, causa raíz del tiempo de respuesta u otros atributos predefinidos. Por ejemplo, para filtrar más el conjunto de registros de seguimiento con un código de estado 500, seleccione una fila de la tabla USERS. Se obtienen dos etiquetas de filtro en el icono del conjunto de registros de seguimiento: `http.status`, tal y como se designó anteriormente, y `user`.

Comparar dos conjuntos de registros de seguimiento con criterios diferentes

Compare varios usuarios y sus solicitudes POST para encontrar otras discrepancias y correlaciones. Aplique su primer conjunto de filtros. Estos filtros se definen por una línea azul en la distribución del tiempo de respuesta. A continuación, seleccione Compare (Comparar). Inicialmente, esto crea una copia de los filtros del conjunto de registros de seguimiento A.

Para continuar, defina un nuevo conjunto de filtros que se aplique al conjunto de registros de seguimiento B. Este segundo conjunto se representa mediante una línea verde. En el siguiente ejemplo se muestran diferentes líneas en función de la combinación de colores azul y verde.



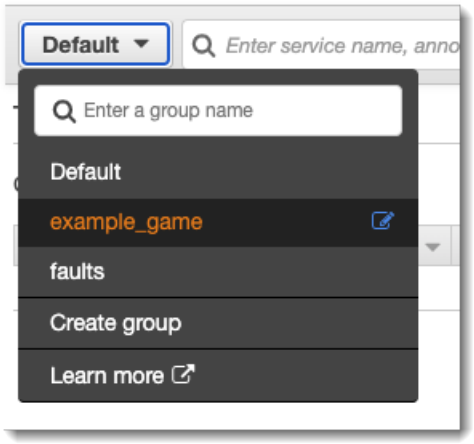
Identificar un registro de seguimiento de su interés y ver sus detalles

Cuando reduzca el alcance mediante los filtros de la consola, la lista de registros de seguimiento de debajo de las tablas de métricas le resultará más útil. La tabla de lista de registros de seguimiento combina información de URL, USER (USUARIO) y STATUS CODE (CÓDIGO DE ESTADO) en una sola consulta. Para obtener más información, seleccione una fila de esta tabla para abrir la página de detalles del registro de seguimiento y ver su escala de tiempo y sus datos sin procesar.

Configuración de grupos

Los grupos son una colección de registros de seguimiento que se definen mediante una expresión de filtro. Puedes usar grupos para generar gráficos de servicios adicionales y proporcionar CloudWatch métricas de Amazon. Puede usar la consola de AWS X-Ray o la API de X-Ray con el fin de crear y administrar grupos para sus servicios. En este tema se describe cómo crear y administrar grupos con la consola de X-Ray. Para obtener información sobre cómo administrar grupos con la API de X-Ray, consulte Grupos.

Puedes crear grupos de trazas para mapas de trazas, trazas o análisis. Al crear un grupo, el grupo pasa a estar disponible como filtro en el menú desplegable del grupo en las tres páginas: Trace Map, Traces y Analytics.



Los grupos se identifican por su nombre o un nombre de recurso de Amazon (ARN) y contienen una expresión de filtro. El servicio compara los registros de seguimiento de entrada con la expresión y los almacena en consecuencia. Para obtener más información acerca de cómo crear una expresión de filtro, consulte Uso de expresiones de filtro.

La actualización de la expresión de filtro de un grupo no cambia los datos que ya se han registrado. La actualización se aplica únicamente a los rastros posteriores. Esto puede dar lugar a un gráfico que combina la expresión nueva con la anterior. Para evitarlo, elimine el grupo actual y cree uno nuevo.

> **Note**
>
> Los grupos se facturan por el número de rastros recuperados que coinciden con la expresión de filtro. Para más información, consulte Precios de AWS X-Ray.

Temas

- Creación de un grupo
- Aplicar un grupo
- Editar un grupo
- Clonación de un grupo
- Eliminación de un grupo
- Ver las métricas de los grupos en Amazon CloudWatch

Creación de un grupo

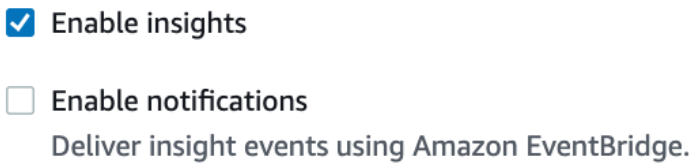
> **Note**
>
> Ahora puede configurar los grupos de X-Ray desde la CloudWatch consola de Amazon. También puede seguir utilizando la consola de X-Ray.

CloudWatch console

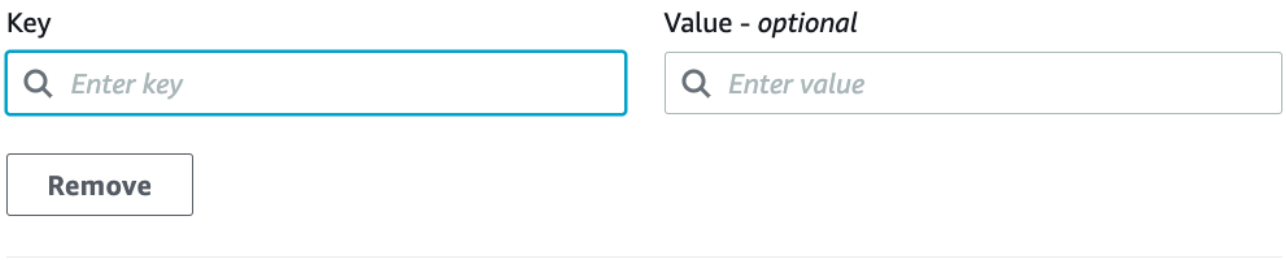
1. Inicia sesión en la CloudWatch consola AWS Management Console y ábrela en https://console.aws.amazon.com/cloudwatch/.
2. Elija Configuración en el panel de navegación izquierdo.
3. Elija Ver ajustes en Grupos dentro de la sección de Rastros de X-Ray.
4. Seleccione Crear grupo en la parte superior de la lista de grupos.
5. En la página Crear grupo escriba un nombre para el grupo. Los nombres de grupo pueden tener un máximo de 32 caracteres y solo pueden contener caracteres alfanuméricos y guiones. En los nombres de grupo se distingue entre mayúsculas y minúsculas.
6. Introduzca una expresión de filtro. Para obtener más información acerca de cómo crear una expresión de filtro, consulte Uso de expresiones de filtro. En el siguiente ejemplo, el grupo filtra los rastros de errores del servicio `api.example.com` y las solicitudes al servicio en las que el tiempo de respuesta fue superior o igual a cinco segundos.

   ```
   fault = true AND http.url CONTAINS "example/game" AND responsetime >= 5
   ```

7. En Información, habilite o deshabilite el acceso a la información para el grupo. Para obtener más detalles acerca de la información, consulte Uso de información en X-Ray.

8. En Etiquetas, elija Añadir nueva etiqueta para introducir una clave de etiqueta y, si lo desea, un valor de etiqueta. Siga añadiendo las etiquetas adicionales que desee. Cada clave de etiqueta debe ser única. Para eliminar una etiqueta, elija Eliminar debajo de cada etiqueta. Para obtener más información acerca de las etiquetas, consulte Etiquetado de reglas de muestreo y grupos de X-Ray.



9. Elija Crear grupo.

X-Ray console

1. Inicie sesión en la consola de X-Ray AWS Management Console y ábrala en https://console.aws.amazon.com/xray/home.
2. Abre la página Crear grupo desde la página Grupos del panel de navegación izquierdo o desde el menú de grupos de una de las siguientes páginas: Trace Map, Traces y Analytics.
3. En la página Crear grupo escriba un nombre para el grupo. Los nombres de grupo pueden tener un máximo de 32 caracteres y solo pueden contener caracteres alfanuméricos y guiones. En los nombres de grupo se distingue entre mayúsculas y minúsculas.
4. Introduzca una expresión de filtro. Para obtener más información acerca de cómo crear una expresión de filtro, consulte Uso de expresiones de filtro. En el siguiente ejemplo, el grupo filtra los rastros de errores del servicio `api.example.com` y las solicitudes al servicio en las que el tiempo de respuesta fue superior o igual a cinco segundos.

```
fault = true AND http.url CONTAINS "example/game" AND responsetime >= 5
```

5. En Información, habilite o deshabilite el acceso a la información para el grupo. Para obtener más detalles acerca de la información, consulte Uso de información en X-Ray.

6. En Etiquetas, introduzca una clave de etiqueta y, si lo desea, un valor de etiqueta. Al añadir una etiqueta, aparece una nueva línea para que introduzca otra etiqueta. Cada clave de etiqueta debe ser única. Para eliminar una etiqueta, elija X al final de la fila de la etiqueta. Para obtener más información acerca de las etiquetas, consulte Etiquetado de reglas de muestreo y grupos de X-Ray.

7. Elija Crear grupo.

Aplicar un grupo

CloudWatch console

1. Inicie sesión en la CloudWatch consola AWS Management Console y ábrala en https://console.aws.amazon.com/cloudwatch/.
2. Abra una de las siguientes páginas del panel de navegación, en Rastros de X-Ray:
   - Mapa de rastreo
   - Rastros
3. Introduzca un nombre de grupo en el Filtrar por grupo de X-Ray. Los datos que se muestran en la página cambian para coincidir con la expresión de filtro establecida en el grupo.

X-Ray console

1. Inicie sesión en la consola de X-Ray AWS Management Console y ábrala en https://console.aws.amazon.com/xray/home.
2. Abra una de las siguientes páginas desde el panel de navegación:
   - Mapa de rastreo
   - Rastros
   - Análisis
3. En el menú de grupos, elija el grupo que creó en la the section called “Creación de un grupo”. Los datos que se muestran en la página cambian para coincidir con la expresión de filtro establecida en el grupo.

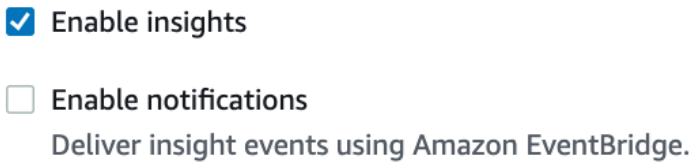
Editar un grupo

CloudWatch console

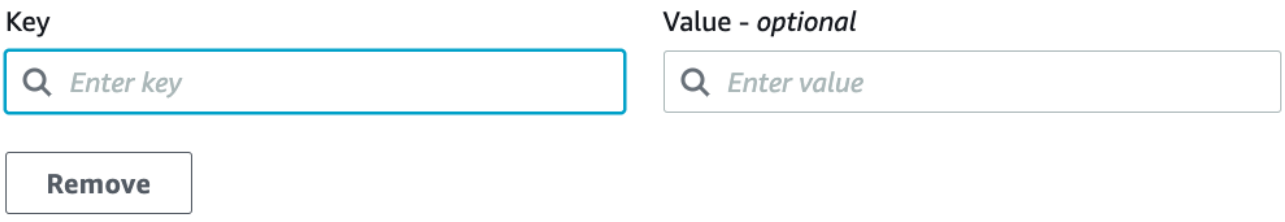
1. Inicie sesión en la CloudWatch consola AWS Management Console y ábrala en https://console.aws.amazon.com/cloudwatch/.
2. Elija Configuración en el panel de navegación izquierdo.
3. Elija Ver ajustes en Grupos dentro de la sección de Rastros de X-Ray.
4. Elija un grupo de la sección Grupos y, a continuación, elija Editar.
5. Aunque no puede cambiar el nombre de un grupo, puede actualizar la expresión de filtro. Para obtener más información acerca de cómo crear una expresión de filtro, consulte Uso de expresiones de filtro. En el siguiente ejemplo, el grupo filtra los rastros de errores del servicio `api.example.com` y las solicitudes cuya dirección URL contenga `example/game` y cuyo tiempo de respuesta fue superior o igual a cinco segundos.

   ```
   fault = true AND http.url CONTAINS "example/game" AND responsetime >= 5
   ```

6. En Información, habilite o deshabilite el acceso a la información para el grupo. Para obtener más detalles acerca de la información, consulte Uso de información en X-Ray.

7. En Etiquetas, elija Añadir nueva etiqueta para introducir una clave de etiqueta y, si lo desea, un valor de etiqueta. Siga añadiendo las etiquetas adicionales que desee. Cada clave de etiqueta debe ser única. Para eliminar una etiqueta, elija Eliminar debajo de cada etiqueta. Para obtener más información acerca de las etiquetas, consulte Etiquetado de reglas de muestreo y grupos de X-Ray.

8. Cuando haya terminado de actualizar el grupo, elija Actualizar grupo.

X-Ray console

1. Inicie sesión en la consola de X-Ray AWS Management Console y ábrala en https://console.aws.amazon.com/xray/home.
2. Siga uno de estos pasos para abrir la página Editar grupo.

   a. En la página Grupos, elija el nombre de un grupo para editarlo.

   b. En el menú de grupos de una de las páginas siguientes, elija un grupo y, a continuación, seleccione Editar.

   - Mapa de rastreo
   - Rastros
   - Análisis

3. Aunque no puede cambiar el nombre de un grupo, puede actualizar la expresión de filtro. Para obtener más información acerca de cómo crear una expresión de filtro, consulte Uso de expresiones de filtro. En el siguiente ejemplo, el grupo filtra los rastros de errores del servicio `api.example.com` y las solicitudes cuya dirección URL contenga `example/game` y cuyo tiempo de respuesta fue superior o igual a cinco segundos.

   ```
   fault = true AND http.url CONTAINS "example/game" AND responsetime >= 5
   ```

4. En Conocimientos, habilite o deshabilite los conocimientos y las notificaciones de conocimientos para el grupo. Para obtener más detalles acerca de la información, consulte Uso de información en X-Ray.

5. En Etiquetas, edite las claves y los valores de las etiquetas. Cada clave de etiqueta debe ser única. Los valores de las etiquetas son opcionales; puede eliminarlos si lo desea. Para eliminar una etiqueta, elija X al final de la fila de la etiqueta. Para obtener más información acerca de las etiquetas, consulte Etiquetado de reglas de muestreo y grupos de X-Ray.

6. Cuando haya terminado de actualizar el grupo, elija Actualizar grupo.

Clonación de un grupo

Al clonar un grupo, se crea un grupo nuevo que tiene la expresión de filtro y las etiquetas de un grupo existente. Cuando clona un grupo, el grupo nuevo tiene el mismo nombre que el grupo desde el que lo clone, con `-clone` anexado al nombre.

CloudWatch console

1. Inicie sesión en la CloudWatch consola AWS Management Console y ábrala en https://console.aws.amazon.com/cloudwatch/.
2. Elija Configuración en el panel de navegación izquierdo.
3. Elija Ver ajustes en Grupos dentro de la sección de Rastros de X-Ray.
4. Elija un grupo de la sección Grupos y, a continuación, elija Clonar.
5. En la página Crear grupo, el nombre del grupo es *`group-name`*`-clone`. Si lo desea, puede introducir un nuevo nombre para el grupo. Los nombres de grupo pueden tener un máximo de 32 caracteres y solo pueden contener caracteres alfanuméricos y guiones. En los nombres de grupo se distingue entre mayúsculas y minúsculas.
6. Puede conservar la expresión de filtro del grupo existente o, si lo desea, introducir una nueva expresión de filtro. Para obtener más información acerca de cómo crear una expresión de filtro, consulte Uso de expresiones de filtro. En el siguiente ejemplo, el grupo filtra los rastros de errores del servicio `api.example.com` y las solicitudes al servicio en las que el tiempo de respuesta fue superior o igual a cinco segundos.

   ```
   service("api.example.com") { fault = true OR responsetime >= 5 }
   ```

7. En Etiquetas, edite las claves y los valores de las etiquetas, si es necesario. Cada clave de etiqueta debe ser única. Los valores de las etiquetas son opcionales; puede eliminarlos si lo desea. Para eliminar una etiqueta, elija X al final de la fila de la etiqueta. Para obtener más información acerca de las etiquetas, consulte Etiquetado de reglas de muestreo y grupos de X-Ray.
8. Elija Crear grupo.

X-Ray console

1. Inicie sesión en la consola de X-Ray AWS Management Console y ábrala en https://console.aws.amazon.com/xray/home.
2. Abra la página Grupos desde el panel de navegación izquierdo y elija el nombre del grupo que desee clonar.
3. Seleccione Clonar grupo en el menú Acciones.
4. En la página Crear grupo, el nombre del grupo es *`group-name`*`-clone`. Si lo desea, puede introducir un nuevo nombre para el grupo. Los nombres de grupo pueden tener un máximo de 32 caracteres y solo pueden contener caracteres alfanuméricos y guiones. En los nombres de grupo se distingue entre mayúsculas y minúsculas.
5. Puede conservar la expresión de filtro del grupo existente o, si lo desea, introducir una nueva expresión de filtro. Para obtener más información acerca de cómo crear una expresión de filtro, consulte Uso de expresiones de filtro. En el siguiente ejemplo, el grupo filtra los rastros de errores del servicio `api.example.com` y las solicitudes al servicio en las que el tiempo de respuesta fue superior o igual a cinco segundos.

   ```
   service("api.example.com") { fault = true OR responsetime >= 5 }
   ```
6. En Etiquetas, edite las claves y los valores de las etiquetas, si es necesario. Cada clave de etiqueta debe ser única. Los valores de las etiquetas son opcionales; puede eliminarlos si lo desea. Para eliminar una etiqueta, elija X al final de la fila de la etiqueta. Para obtener más información acerca de las etiquetas, consulte Etiquetado de reglas de muestreo y grupos de X-Ray.
7. Elija Crear grupo.

Eliminación de un grupo

Siga los pasos de esta sección para eliminar un grupo. No se puede eliminar el grupo Predeterminado.

CloudWatch console

1. Inicie sesión en la CloudWatch consola AWS Management Console y ábrala en https://console.aws.amazon.com/cloudwatch/.
2. Elija Configuración en el panel de navegación izquierdo.

3. Elija Ver ajustes en Grupos dentro de la sección de Rastros de X-Ray.
4. Elija un grupo de la sección Grupos y, a continuación, elija Eliminar.
5. Cuando se le pida confirmación, elija Eliminar.

X-Ray console

1. Inicie sesión en la consola de X-Ray AWS Management Console y ábrala en https://console.aws.amazon.com/xray/home.
2. Abra la página Grupos desde el panel de navegación izquierdo y elija el nombre del grupo que desee eliminar.
3. En el menú Acciones, elija Eliminar.
4. Cuando se le pida confirmación, elija Eliminar.

Ver las métricas de los grupos en Amazon CloudWatch

Una vez que se crea un grupo, los rastros de entrada se comparan con la expresión de filtro del grupo a medida que se almacenan en el servicio de X-Ray. Las métricas del número de trazas que coinciden con cada criterio se publican en Amazon CloudWatch cada minuto. Al seleccionar Ver métrica en la página Editar grupo, se abre la CloudWatch consola a la página Métrica. Para obtener más información sobre cómo usar CloudWatch las métricas, consulta Uso de Amazon CloudWatch Metrics en la Guía del CloudWatch usuario de Amazon.

CloudWatch console

1. Inicie sesión en la CloudWatch consola AWS Management Console y ábrala en https://console.aws.amazon.com/cloudwatch/.
2. Elija Configuración en el panel de navegación izquierdo.
3. Elija Ver ajustes en Grupos dentro de la sección de Rastros de X-Ray.
4. Elija un grupo de la sección Grupos y, a continuación, elija Editar.
5. En la página Editar grupo, elija Ver métrica.

   La página de métricas de la CloudWatch consola se abre en una pestaña nueva.

X-Ray console

1. Inicie sesión en la consola de X-Ray AWS Management Console y ábrala en https://console.aws.amazon.com/xray/home.
2. Abra la página Grupos desde el panel de navegación izquierdo y elija el nombre del grupo cuyas métricas desee ver.
3. En la página Editar grupo, elija Ver métrica.

   La página de métricas de la CloudWatch consola se abre en una pestaña nueva.

Configuración de reglas de muestreo de

Puede usar la AWS X-Ray consola para configurar las reglas de muestreo para sus servicios. El SDK de X-Ray y los Servicios de AWS que admiten el rastreo activo con configuración de muestreo utilizan reglas de muestreo para determinar qué solicitudes registrar.

Temas

Configuración de reglas de muestreo de

Puede configurar el muestreo para los siguientes casos de uso:

- Punto de entrada de API Gateway: API Gateway admite el muestreo y el rastreo activo. Para habilitar el rastreo activo en una etapa de la API, consulte Soporte de rastreo activo de Amazon API Gateway para AWS X-Ray.
- AWS AppSync— AWS AppSync admite el muestreo y el rastreo activo. Para habilitar el rastreo activo en las AWS AppSync solicitudes, consulte Rastreo con X-Ray AWS.

- SDK de X-Ray para instrumentos en plataformas informáticas: cuando se utilizan plataformas informáticas como Amazon EC2, Amazon ECS o AWS Elastic Beanstalk, se admite el muestreo cuando la aplicación se ha equipado con el último SDK de X-Ray.

Personalización de reglas de muestreo

Al personalizar las reglas de muestreo, puede controlar la cantidad de datos que va a registrar. También puede modificar el comportamiento del muestreo sin modificar ni volver a implementar el código. Las reglas de muestreo indican al SDK de X-Ray cuántas solicitudes se van a registrar para un conjunto de criterios. De forma predeterminada, el SDK de X-Ray registra la primera solicitud cada segundo y el 5 % de las solicitudes adicionales. Una petición por segundo es el depósito. Esto garantiza que se registre al menos un registro de seguimiento cada segundo mientras el servicio atienda solicitudes. El cinco por ciento es el porcentaje al que se muestrean las solicitudes adicionales más allá del tamaño del depósito.

Puede configurar el SDK de X-Ray para leer reglas de muestreo desde un documento JSON que incluya con su código. Sin embargo, cuando ejecute varias instancias de su servicio, cada instancia realiza el muestreo de manera independiente. Esto hace que el porcentaje total de solicitudes muestreadas aumente, ya que los depósitos de todas las instancias se suman de forma efectiva. Además, para actualizar las reglas de muestreo locales, tiene que volver a implementar su código.

Al definir las reglas de muestreo en la consola de X-Ray y configurar el SDK para leer reglas desde el servicio de X-Ray, puede evitar ambos problemas. El servicio administra el depósito de cada regla y asigna cuotas a cada instancia de su servicio para distribuir el depósito de manera uniforme, en función del número de instancias que se ejecuten. El límite del depósito se calcula de acuerdo con las reglas que haya establecido. Dado que las reglas están configuradas en el servicio, puede administrar las reglas sin realizar implementaciones adicionales.

> **Note**
>
> X-Ray aplica las reglas de muestreo en la medida de lo posible y, en algunos casos, el porcentaje de muestreo efectivo puede no coincidir exactamente con las reglas de muestreo configuradas. Sin embargo, con el tiempo, el número de solicitudes muestreadas debería estar cerca del porcentaje configurado.

Ahora puede configurar las reglas de muestreo de X-Ray desde la CloudWatch consola de Amazon. También puede seguir utilizando la consola de X-Ray.

CloudWatch console

Para configurar las reglas de muestreo en la CloudWatch consola

1. Inicie sesión en la CloudWatch consola AWS Management Console y ábrala en https://console.aws.amazon.com/cloudwatch/.
2. Elija Configuración en el panel de navegación izquierdo.
3. Seleccione Ver configuración en Reglas de muestreo en la sección de Rastros de X-Ray.
4. Para crear una regla, elija Crear regla de muestreo.

   Para editar una regla, elija la regla y, a continuación, elija Editar.

   Para eliminar una regla, elija la regla y, a continuación, elija la opción Eliminar.

X-Ray console

Configuración de las reglas de muestreo en la consola de X-Ray

1. Abra la consola de X-Ray.
2. En el panel de navegación izquierdo, elija Muestreo.
3. Para crear una regla, elija Crear regla de muestreo.

   Para editar una regla, elija el nombre de una regla.

   Para eliminar una regla, elija una regla y utilice el menú Acciones para eliminarla.

Opciones de reglas de muestreo

Las siguientes opciones están disponibles para cada regla. En los valores de cadena se pueden usar caracteres comodín para buscar coincidencias de un solo carácter (?) o cero o más caracteres (*).

Opciones de reglas de muestreo

- Nombre de la regla (cadena): un nombre único para la regla.
- Prioridad (entero comprendido entre el 1 y 9999): prioridad de la regla de muestreo. Los servicios evalúan las reglas en orden ascendente de prioridad y toman una decisión de muestreo con la primera regla coincidente.

- Depósito (entero no negativo): número fijo de solicitudes coincidentes que se van a instrumentar por segundo, antes de aplicar el porcentaje fijo. Los servicios no utilizan directamente el depósito, sino que se aplica a todos los servicios que usan la regla en su conjunto.
- Porcentaje (entero comprendido entre el 0 y el 100): porcentaje de solicitudes coincidentes que se van instrumentar, una vez que se ha agotado el depósito. Al configurar una regla de muestreo en la consola, elija un porcentaje entre 0 y 100. Al configurar una regla de muestreo en un SDK de cliente mediante un documento JSON, proporcione un valor porcentual entre 0 y 1.
- Nombre del servicio (cadena): el nombre del servicio instrumentado, tal como aparece en el mapa de rastreo.
  - SDK de X-Ray: el nombre del servicio que se configura en la grabadora.
  - Amazon API Gateway: *`api-name`*/*`stage`*.
- Tipo de servicio (cadena): el tipo de servicio, tal como aparece en el mapa de rastreo. Para el SDK de X-Ray, defina el tipo de servicio aplicando el complemento adecuado:
  - `AWS::ElasticBeanstalk::Environment`— Un AWS Elastic Beanstalk entorno (complemento).
  - `AWS::EC2::Instance`: una instancia de Amazon EC2 (complemento).
  - `AWS::ECS::Container`: un contenedor de Amazon ECS (complemento).
  - `AWS::APIGateway::Stage`: una etapa de Amazon API Gateway.
  - `AWS::AppSync::GraphQLAPI` — Una solicitud AWS AppSync de API.
- Host (cadena): nombre de host del encabezado de host HTTP.
- Método HTTP (cadena): el método de la solicitud HTTP.
- Ruta URL (cadena): la ruta URL de la solicitud.
  - SDK de X-Ray: la parte de la ruta de la URL de la solicitud HTTP.
- ARN del recurso (cadena): el ARN del AWS recurso que ejecuta el servicio.
  - SDK de X-Ray: no compatible. El SDK solo puede utilizar reglas con Resource ARN (ARN de recurso) configurado en *.
  - Amazon API Gateway: el ARN de etapa.
- (Opcional) Atributos (clave y valor): atributos de segmento que se conocen cuando se toma la decisión de muestreo.
  - SDK de X-Ray: no compatible. El SDK omite las reglas que especifican atributos.
  - Amazon API Gateway: encabezados de la solicitud HTTP original.

Ejemplos de reglas de muestreo

Example – Regla predeterminada sin depósito y con un porcentaje bajo

Puede modificar el depósito predeterminado de la regla y el porcentaje. La regla predeterminada se aplica a las solicitudes que no coinciden con cualquier otra regla.

- Depósito: **`0`**
- Porcentaje: **`5`** (**`0.05`** si se configura mediante un documento JSON)

Example – Regla de depuración para rastrear todas las solicitudes para una ruta problemática

Una regla de alta prioridad aplicada temporalmente para depuración.

- Nombre de la regla: **`DEBUG - history updates`**
- Prioridad: **`1`**
- Depósito: **`1`**
- Porcentaje: **`100`** (**`1`** si se configura mediante un documento JSON)
- Nombre del servicio: **`Scorekeep`**
- Tipo de servicio: **`*`**
- Host: **`*`**
- Método HTTP: **`PUT`**
- Ruta URL: **`/history/*`**
- ARN de recurso: **`*`**

Example – Porcentaje mínimo superior para POST

- Nombre de la regla: **`POST minimum`**
- Prioridad: **`100`**
- Depósito: **`10`**
- Porcentaje: **`10`** (**`.1`** si se configura mediante un documento JSON)
- Nombre del servicio: **`*`**
- Tipo de servicio: **`*`**
- Host: **`*`**

- Método HTTP: **`POST`**
- Ruta URL: **`*`**
- ARN de recurso: **`*`**

Configuración del servicio para utilizar reglas de muestreo

El SDK de X-Ray requiere configuración adicional para utilizar reglas de muestreo que configura en la consola. Consulte el tema de configuración para su lenguaje para obtener más información sobre cómo configurar una estrategia de muestreo.

- Java: Reglas de muestreo
- Go: Reglas de muestreo
- Node.js: Reglas de muestreo
- Python: Reglas de muestreo
- Ruby: Reglas de muestreo
- .NET: Reglas de muestreo

Para API Gateway, consulte: Soporte de rastreo activo de Amazon API Gateway para AWS X-Ray.

Visualización de resultados de muestreo

La página de Muestreo de la consola de X-Ray muestra información detallada sobre cómo los servicios del usuario utilizan cada regla de muestreo.

La columna Trend (Tendencia) muestra cómo se ha utilizado la regla en los últimos minutos. Cada columna muestra las estadísticas para una ventana de 10 segundos.

Estadísticas de muestreo

- Regla coincidente total: el número de solicitudes que coincidieron con esta regla. Este número no incluye solicitudes que podrían haber coincidido con esta regla, pero coincidieron primero con una regla de prioridad más alta.
- Total muestreado: el número de solicitudes registradas.
- Muestreadas con porcentaje fijo: número de solicitudes muestreadas aplicando el porcentaje fijo de la regla.

- Muestreado con límite de depósito: el número de solicitudes muestreadas utilizando una cuota asignada por X-Ray.
- Préstamos del depósito: número de solicitudes muestreadas tomando prestado del depósito. La primera vez que un servicio hace coincidir una solicitud con una regla, X-Ray aún no le ha asignado una cuota. Sin embargo, si el depósito es al menos 1, el servicio toma prestado un rastro por segundo hasta que X-Ray asigna una cuota.

Para obtener más información acerca de cómo utilizar las estadísticas de muestreo y cómo utilizan las reglas de muestreo los servicios, consulte Using sampling rules with the X-Ray API (Uso de reglas de muestreo con la API de X-Ray).

Siguientes pasos

Puede usar la API de X-Ray para administrar reglas de muestreo. Con la API, puede crear y actualizar las reglas mediante programación de forma programada o en respuesta a alarmas o notificaciones. Consulte Configuración de las opciones de muestreo, grupos y cifrado con la API de AWS X-Ray para obtener instrucciones y ejemplos de reglas adicionales.

El SDK de X-Ray y Servicios de AWS también utilizan la API de X-Ray para leer las reglas de muestreo, informar los resultados del muestreo y obtener los objetivos de muestreo. Los servicios deben realizar un seguimiento de la frecuencia con la que se aplica cada regla, evaluar las reglas en función de la prioridad y tomar prestado del depósito cuando una solicitud coincide con una regla para la que X-Ray no ha asignado aún una cuota al servicio. Para obtener más información acerca de cómo utiliza un servicio la API para muestreo, consulte Using sampling rules with the X-Ray API (Uso de reglas de muestreo con la API de X-Ray).

Cuando el SDK de X-Ray llama a las API de muestreo, utiliza el daemon de X-Ray como proxy. Si ya utiliza el puerto de TCP 2000, puede configurar el demonio para ejecutar el proxy en un puerto diferente. Para obtener más información, consulte Configuración del AWS X-Ray daemon.

Enlace profundo de la consola

Puedes usar rutas y consultas para establecer vínculos profundos con trazas específicas o vistas filtradas de las trazas y el mapa de trazas.

Páginas de la consola

- Página principal: xray/home#/welcome

- Introducción: xray/home#/getting-started
- Mapa de rastreo: xray/home#/service-map
- Rastros: xray/home#/traces

Rastros

Puede generar enlaces a las vistas de escala de tiempo, sin procesar y mapa de los rastros individuales.

Escala de tiempo de rastros: `xray/home#/traces/`*`trace-id`*

Datos de rastreo sin procesar: `xray/home#/traces/`*`trace-id`*`/raw`

Example – datos de rastreo sin procesar

```
https://console.aws.amazon.com/xray/home#/traces/1-57f5498f-d91047849216d0f2ea3b6442/
raw
```

Expresiones de filtro

Enlazan con una lista filtrada de rastros.

Vista de rastros filtrados: `xray/home#/traces?filter=`*`filter-expression`*

Example – expresión de filtro

```
https://console.aws.amazon.com/xray/home#/traces?filter=service("api.amazon.com")
 { fault = true OR responsetime > 2.5 } AND annotation.foo = "bar"
```

Example – expresión de filtro (URL codificada)

```
https://console.aws.amazon.com/xray/home#/traces?filter=service(%22api.amazon.com
%22)%20%7B%20fault%20%3D%20true%20OR%20responsetime%20%3E%202.5%20%7D%20AND
%20annotation.foo%20%3D%20%22bar%22
```

Para obtener más información sobre las expresiones de filtro, consulte Uso de expresiones de filtro.

Intervalo de tiempo

Especifique un intervalo de tiempo o una hora de inicio y una hora de finalización en formato ISO8601. Los rangos de tiempo se indican en UTC y su duración máxima es de seis horas.

Período de tiempo: `xray/home#/page?timeRange=range-in-minutes`

Example — trazar el mapa de la última hora

```
https://console.aws.amazon.com/xray/home#/service-map?timeRange=PT1H
```

Hora de inicio y finalización: `xray/home#/page?timeRange=start~end`

Example – intervalo de tiempo con una precisión de segundos

```
https://console.aws.amazon.com/xray/home#/traces?
timeRange=2023-7-01T16:00:00~2023-7-01T22:00:00
```

Example – intervalo de tiempo con una precisión de minutos

```
https://console.aws.amazon.com/xray/home#/traces?
timeRange=2023-7-01T16:00~2023-7-01T22:00
```

Región

Especifique un enlace Región de AWS a las páginas de esa región. De lo contrario, la consola le redirige a la última región que ha visitado.

Región: `xray/home?region=region#/page`

Example — trazar un mapa en el oeste de EE. UU. (Oregón) (us-west-2)

```
https://console.aws.amazon.com/xray/home?region=us-west-2#/service-map
```

Cuando se incluye una región con otros parámetros de consulta, la consulta de región va antes de la almohadilla y las consultas específicas de X-Ray van después del nombre de página.

Example — mapa de rastreo de la última hora en el oeste de EE. UU. (Oregón) (us-west-2)

```
https://console.aws.amazon.com/xray/home?region=us-west-2#/service-map?timeRange=PT1H
```

En combinación

Example – rastros recientes con un filtro de duración

```
https://console.aws.amazon.com/xray/home#/traces?timeRange=PT15M&filter=duration%20%3E
%3D%205%20AND%20duration%20%3C%3D%208
```

Salida

- Página — Rastros
- Intervalo de tiempo: últimos 15 minutos
- Filtro: duración >= 5 Y duración <= 8

AWS X-Ray demonio

> **Note**
>
> Ahora puede usar el CloudWatch agente para recopilar métricas, registros y seguimientos de las instancias de Amazon EC2 y de los servidores locales. CloudWatch La versión 1.300025.0 del agente y posteriores puede recopilar trazas de los SDK de nuestros clientes de OpenTelemetryX-Ray y enviarlas a X-Ray. Utilizar el CloudWatch agente en lugar del Collector AWS Distro for OpenTelemetry (ADOT) o el daemon X-Ray para recopilar trazas puede ayudarle a reducir la cantidad de agentes que administra. Consulte el tema sobre los CloudWatch agentes en la Guía del CloudWatch usuario para obtener más información.

El AWS X-Ray daemon es una aplicación de software que escucha el tráfico en el puerto UDP 2000, recopila datos de segmentos sin procesar y los transmite a la API. AWS X-Ray El daemon funciona en conjunto con los AWS X-Ray SDK y debe estar en ejecución para que los datos enviados por los SDK puedan llegar al servicio X-Ray. El daemon de X-Ray es un proyecto de código abierto. Puedes seguir el proyecto y enviar las incidencias y solicitudes de cambios en: github.com/aws/ GitHub aws-xray-daemon

Activa AWS Lambda y AWS Elastic Beanstalk usa la integración de esos servicios con X-Ray para ejecutar el daemon. Lambda ejecuta el daemon automáticamente cuando se invoca una función para una solicitud de muestreo. En Elastic Beanstalk , utilice la opción de configuración `XRayEnabled` para ejecutar el daemon en las instancias de su entorno. Para obtener más información, consulte

Para ejecutar el daemon de X-Ray de forma local, local o en otro lugar, descárguelo Servicios de AWS, ejecútelo y, a continuación, dele permiso para cargar documentos segmentados en X-Ray.

Descargar el demonio

Puede descargar el daemon de Amazon S3, Amazon ECR o Docker Hub y, a continuación, ejecutarlo de forma local o instalarlo en una instancia de Amazon EC2 durante el lanzamiento.

Amazon S3

Instaladores y ejecutables del daemon de X-Ray

- Linux (ejecutable): `aws-xray-daemon-linux-3.x.zip` (sig.)

- Linux (instalador RPM): `aws-xray-daemon-3.x.rpm`
- Linux (instalador DEB): `aws-xray-daemon-3.x.deb`
- Linux (ARM64, ejecutable): `aws-xray-daemon-linux-arm64-3.x.zip` (sig.)
- Linux (ARM64, instalador RPM): `aws-xray-daemon-arm64-3.x.rpm`
- Linux (ARM64, instalador DEB): `aws-xray-daemon-arm64-3.x.deb`
- OS X (ejecutable): `aws-xray-daemon-macos-3.x.zip` (sig.)
- Windows (ejecutable): `aws-xray-daemon-windows-process-3.x.zip` (sig.)
- Windows (servicio): `aws-xray-daemon-windows-service-3.x.zip` (sig.)

Estos enlaces siempre apuntan a la última versión 3.x del daemon. Para descargar una versión específica, sustituya `3.x` por el número de versión. Por ejemplo, `2.1.0`.

Los recursos de X-Ray se replican en buckets de las regiones admitidas. Para utilizar el bucket más cercano a usted o a sus recursos de AWS , sustituya la región de los enlaces anteriores por su región.

```
https://s3.us-west-2.amazonaws.com/aws-xray-assets.us-west-2/xray-daemon/aws-xray-daemon-3.x.rpm
```

Amazon ECR

A partir de la versión 3.2.0, el daemon se encuentra en Amazon ECR. Antes de extraer una imagen, debe autenticar su cliente de Docker en el registro público de Amazon ECR.

Extraiga la etiqueta de la última versión 3.x publicada ejecutando el siguiente comando:

```
docker pull public.ecr.aws/xray/aws-xray-daemon:3.x
```

Las versiones anteriores o alfa se pueden descargar sustituyendo `3.x` por `alpha` o un número de versión específico. No es recomendable utilizar una imagen de daemon con una etiqueta alfa en un entorno de producción.

Docker Hub

El daemon se encuentra en Docker Hub. Para descargar la última versión 3.x publicada ejecutando el siguiente comando:

```
docker pull amazon/aws-xray-daemon:3.x
```

Se pueden lanzar versiones anteriores del daemon sustituyendo `3.x` por la versión deseada.

Verificación de la firma del archivo de demonio

Se incluyen los archivos signature de GPG de los recursos de demonio comprimidos en archivos ZIP. La clave pública es: `aws-xray.gpg`.

Puede utilizar la clave pública para verificar que el archivo ZIP del demonio es original y no se ha modificado. En primer lugar, importe la clave pública con GnuPG.

Para importar la clave pública

1. Descargue la clave pública.

```
$ BUCKETURL=https://s3.us-east-2.amazonaws.com/aws-xray-assets.us-east-2
$ wget $BUCKETURL/xray-daemon/aws-xray.gpg
```

2. Importe la clave pública en su llavero.

```
$ gpg --import aws-xray.gpg
gpg: /Users/me/.gnupg/trustdb.gpg: trustdb created
gpg: key 7BFE036BFE6157D3: public key "AWS X-Ray <aws-xray@amazon.com>" imported
gpg: Total number processed: 1
gpg:               imported: 1
```

Utilice la clave importada para verificar la firma del archivo ZIP del demonio.

Para verificar la firma de un archivo

1. Descargue el archivo y el archivo de firma.

```
$ BUCKETURL=https://s3.us-east-2.amazonaws.com/aws-xray-assets.us-east-2
$ wget $BUCKETURL/xray-daemon/aws-xray-daemon-linux-3.x.zip
$ wget $BUCKETURL/xray-daemon/aws-xray-daemon-linux-3.x.zip.sig
```

2. Ejecute `gpg --verify` para verificar la firma.

```
$ gpg --verify aws-xray-daemon-linux-3.x.zip.sig aws-xray-daemon-linux-3.x.zip
gpg: Signature made Wed 19 Apr 2017 05:06:31 AM UTC using RSA key ID FE6157D3
gpg: Good signature from "AWS X-Ray <aws-xray@amazon.com>"
```

```
gpg: WARNING: This key is not certified with a trusted signature!
gpg:          There is no indication that the signature belongs to the owner.
Primary key fingerprint: EA6D 9271 FBF3 6990 277F  4B87 7BFE 036B FE61 57D3
```

Tenga en cuenta la advertencia sobre confianza. Una clave solo es de confianza si la ha firmado usted o alguien en quien confíe. Esto no significa que la firma no sea válida, solo que no han verificado la clave pública.

Ejecutar el demonio

Ejecute el demonio localmente desde la línea de comandos. Utilice la opción `-o` para ejecutarlo en modo local y `-n` para configurar la región.

```
~/Downloads$ ./xray -o -n us-east-2
```

Si desea obtener instrucciones específicas para cada plataforma, consulte estos temas:

- Linux (local): Ejecución del daemon de X-Ray en Linux
- Windows (local): Ejecución de un daemon de X-Ray en Windows
- Elastic Beanstalk: Ejecución del daemon de X-Ray en AWS Elastic Beanstalk
- Amazon EC2: Ejecución del daemon de X-Ray en Amazon EC2
- Amazon ECS: Ejecución del daemon de X-Ray en Amazon ECS

Puede personalizar aún más el comportamiento del demonio utilizando las opciones de la línea de comandos o un archivo de configuración. Para obtener más información, consulte Configuración del AWS X-Ray daemon.

Permiso para el envío de datos a X-Ray desde el daemon

El daemon de X-Ray usa el AWS SDK para cargar datos de rastreo en X-Ray y necesita AWS credenciales con permiso para hacerlo.

En Amazon EC2, el daemon utiliza el rol del perfil de instancia de la instancia de manera automática. Para obtener información sobre las credenciales necesarias para ejecutar el daemon de forma local, consulte Ejecutar la aplicación de forma local.

Si especifica las credenciales en más de una ubicación (archivo de credenciales, perfil de instancia o variables de entorno), la cadena de proveedores del SDK determina qué credenciales se utilizan. Para obtener más información acerca de cómo proporcionar credenciales al SDK, consulte la sección sobre especificación de credenciales en la Guía para desarrolladores del SDK de AWS para Go.

El rol o usuario de IAM al cual pertenecen las credenciales del demonio deben tener el permiso de escribir datos en el servicio de forma automática.

- Para utilizar el daemon en Amazon EC2, cree un nuevo rol del perfil de instancia o agregue una política administrada a un rol existente.
- Para utilizar el daemon en Elastic Beanstalk, añada la política administrada al rol predeterminado del perfil de instancia de Elastic Beanstalk.
- Para ejecutar el daemon de forma local, consulte Ejecutar la aplicación de forma local.

Para obtener más información, consulte Administración de identidad y acceso para AWS X-Ray.

Registros del daemon de X-Ray

El demonio muestra información sobre la configuración y los segmentos actuales y luego la envía a AWS X-Ray.

```
2016-11-24T06:07:06Z [Info] Initializing AWS X-Ray daemon 2.1.0
2016-11-24T06:07:06Z [Info] Using memory limit of 49 MB
2016-11-24T06:07:06Z [Info] 313 segment buffers allocated
2016-11-24T06:07:08Z [Info] Successfully sent batch of 1 segments (0.123 seconds)
2016-11-24T06:07:09Z [Info] Successfully sent batch of 1 segments (0.006 seconds)
```

De forma predeterminada, el daemon envía los logs a STDOUT. Si ejecuta el demonio en segundo plano, utilice la opción de línea de comandos `--log-file` o un archivo de configuración para establecer la ruta del archivo de log. También puede definir el nivel de log y deshabilitar la rotación de logs. Para obtener instrucciones, consulte Configuración del AWS X-Ray daemon.

En Elastic Beanstalk, la plataforma establece la ubicación de los registros del daemon. Para obtener más información, consulte Ejecución del daemon de X-Ray en AWS Elastic Beanstalk.

Configuración del AWS X-Ray daemon

Puede utilizar las opciones de la línea de comandos o un archivo de configuración para personalizar el comportamiento del daemon de X-Ray. La mayoría de las opciones están disponibles con ambos métodos, pero algunas solo están disponibles en los archivos de configuración y otras solo en la línea de comandos.

Para empezar, la única opción que debe conocer es `-n` o `--region`, que se utiliza para establecer la región que el daemon utiliza para enviar los datos de rastreo a X-Ray.

```
~/xray-daemon$ ./xray -n us-east-2
```

Si no ejecuta el daemon en Amazon EC2, sino localmente, puede agregar la opción `-o` para omitir la comprobación de las credenciales del perfil de instancia, de modo que el daemon esté listo con mayor rapidez.

```
~/xray-daemon$ ./xray -o -n us-east-2
```

El resto de las opciones de la línea de comandos le permiten configurar el registro, escuchar en otro puerto, limitar la cantidad de memoria que puede utilizar el demonio o asumir un rol para enviar datos de rastreo a otra cuenta.

Puede pasar un archivo de configuración al daemon para tener acceso a las opciones avanzadas de configuración y realizar tareas como limitar el número de llamadas simultáneas a X-Ray, deshabilitar la rotación de registros, y enviar tráfico a un proxy.

Secciones

Variables de entorno admitidas

El daemon de X-Ray admite las siguientes variables de entorno:

- `AWS_REGION`: especifica la Región de AWS del punto de conexión del servicio de X-Ray.

- `HTTPS_PROXY`: especifica una dirección proxy a través de la cual el daemon puede cargar los segmentos. Se pueden utilizar un nombre de dominio DNS o una dirección IP y los números de puerto que utilizan los servidores proxy.

Uso de las opciones de la línea de comandos

Pase estas opciones al demonio cuando lo ejecute localmente o con un script de datos de usuario.

Opciones de la línea de comandos

- `-b`, `--bind`: buscan documentos de segmento en un puerto UDP diferente.

```
--bind "127.0.0.1:3000"
```

  Valor predeterminado: `2000`.

- `-t`, `--bind-tcp`: escuchan las llamadas al servicio de X-Ray en un puerto TCP diferente.

```
-bind-tcp "127.0.0.1:3000"
```

  Valor predeterminado: `2000`.

- `-c`, `--config`: cargan un archivo de configuración desde la ruta especificada.

```
--config "/home/ec2-user/xray-daemon.yaml"
```

- `-f`, `--log-file`: envían registros a ruta de archivo especificada.

```
--log-file "/var/log/xray-daemon.log"
```

- `-l`, `--log-level`: muestran el nivel de registro, desde el más detallado al menos detallado: dev, debug, info, warn, error y prod.

```
--log-level warn
```

  Valor predeterminado: `prod`.

- `-m`, `--buffer-memory`: cambian la cantidad de memoria en MB que pueden utilizar los búferes (mínimo 3).

```
--buffer-memory 50
```

Predeterminado: 1 % de memoria disponible

- `-o`, `--local-mode`: no comprueban los metadatos de la instancia de EC2.
- `-r`, `--role-arn`: asumen el rol de IAM especificado para cargar segmentos en una cuenta diferente.

```
--role-arn "arn:aws:iam::123456789012:role/xray-cross-account"
```

- `-a`, `--resource-arn` — Nombre de recurso de Amazon (ARN) del AWS recurso que ejecuta el daemon.
- `-p`, `--proxy-address` — Cargue segmentos a AWS X-Ray través de un proxy. Hay que especificar el protocolo del servidor proxy.

```
--proxy-address "http://192.0.2.0:3000"
```

- `-n`, `--region`: envían segmentos al servicio de X-Ray en una región específica.
- `-v`, `--version` — Muestra la versión AWS X-Ray del daemon.
- `-h`, `--help`: muestran la pantalla de ayuda.

Uso de un archivo de configuración

También puede utilizar un archivo con formato YAML para configurar el demonio. Transfiera el archivo de configuración al demonio mediante la opción `-c`.

```
~$ ./xray -c ~/xray-daemon.yaml
```

Configuración de las opciones de archivo

- `TotalBufferSizeMB`: tamaño máximo del búfer en MB (mínimo 3). Elija 0 para utilizar 1% de memoria del host.
- `Concurrency`— Número máximo de llamadas simultáneas AWS X-Ray para cargar documentos segmentados.
- `Region`— Enviar segmentos al AWS X-Ray servicio de una región específica.

- `Socket`: configura el enlace del daemon.
  - `UDPAddress`: cambia el puerto en el que el daemon escucha.
  - `TCPAddress`: escucha las llamadas al servicio de X-Ray en un puerto TCP diferente.
- `Logging`: configura el comportamiento de registro.
  - `LogRotation`: se establece en `false` para deshabilitar la rotación de registros.
  - `LogLevel`— Cambie el nivel de registro, del más detallado al menos detallado:`dev`,, `info` o`debug`,`prod`,`warn`,`error`. `prod` El valor predeterminado es `prod`, que equivale a `info`.
  - `LogPath`: envía los registros a la ruta de archivo especificada.
- `LocalMode`: se establece en `true` para omitir la comprobación de los metadatos de la instancia de EC2.
- `ResourceARN`— Nombre de recurso de Amazon (ARN) del AWS recurso que ejecuta el daemon.
- `RoleARN`: asume el rol de IAM especificado para cargar segmentos en una cuenta diferente.
- `ProxyAddress`— Cargue segmentos a AWS X-Ray través de un proxy.
- `Endpoint`: cambia el punto de conexión del servicio de X-Ray al que el daemon envía documentos de segmento.
- `NoVerifySSL`: desactiva la verificación del certificado TLS.
- `Version`: versión de formato del archivo de configuración del daemon. La versión del formato del archivo es un campo obligatorio.

Example Xray-daemon.yaml

Este archivo de configuración cambia el puerto de escucha del demonio a 3000, desactiva las comprobaciones de metadatos de instancias, establece el rol que se usará para cargar segmentos y cambia las opciones de región y registro.

```
Socket:
  UDPAddress: "127.0.0.1:3000"
  TCPAddress: "127.0.0.1:3000"
Region: "us-west-2"
Logging:
  LogLevel: "warn"
  LogPath: "/var/log/xray-daemon.log"
LocalMode: true
RoleARN: "arn:aws:iam::123456789012:role/xray-cross-account"
Version: 2
```

Ejecución del daemon de X-Ray localmente

Puede ejecutar el daemon de AWS X-Ray localmente en Linux, MacOS, Windows o en un contenedor de Docker. Ejecute el daemon para transmitir los datos de rastreo a X-Ray durante el desarrollo y las pruebas de una aplicación instrumentada. Descargue y extraiga el daemon mediante las instrucciones que encontrará aquí.

Al ejecutarlo localmente, el daemon puede leer las credenciales desde un archivo de credenciales del SDK de AWS (`.aws/credentials` en su directorio de usuarios) o desde las variables de entorno. Para obtener más información, consulte Permiso para el envío de datos a X-Ray desde el daemon.

El demonio escucha los datos UDP en el puerto 2000. Puede cambiar el puerto y otras opciones mediante un archivo de configuración y distintas opciones de línea de comandos. Para obtener más información, consulte Configuración del AWS X-Ray daemon.

Ejecución del daemon de X-Ray en Linux

Puede ejecutar el daemon ejecutable desde la línea de comandos. Utilice la opción `-o` para ejecutarlo en modo local y `-n` para configurar la región.

```
~/xray-daemon$ ./xray -o -n us-east-2
```

Para ejecutar el demonio en segundo plano, use &.

```
~/xray-daemon$ ./xray -o -n us-east-2 &
```

Finalice un proceso de demonio que se ejecuta en segundo plano con `pkill`.

```
~$ pkill xray
```

Ejecución del daemon de X-Ray en un contenedor de Docker

Para ejecutar el demonio localmente en un contenedor de Docker, guarde el texto siguiente en un archivo denominado `Dockerfile`. Descargue la imagen de ejemplo completa en Amazon ECR. Para obtener más información, consulte Descarga del daemon.

Example Dockerfile: Amazon Linux

```
FROM amazonlinux
```

```
RUN yum install -y unzip
RUN curl -o daemon.zip https://s3.us-east-2.amazonaws.com/aws-xray-assets.us-east-2/
xray-daemon/aws-xray-daemon-linux-3.x.zip
RUN unzip daemon.zip && cp xray /usr/bin/xray
ENTRYPOINT ["/usr/bin/xray", "-t", "0.0.0.0:2000", "-b", "0.0.0.0:2000"]
EXPOSE 2000/udp
EXPOSE 2000/tcp
```

Compile la imagen del contenedor con `docker build`.

```
~/xray-daemon$ docker build -t xray-daemon .
```

Ejecute la imagen en un contenedor con `docker run`.

```
~/xray-daemon$ docker run \
      --attach STDOUT \
      -v ~/.aws/:/root/.aws/:ro \
      --net=host \
      -e AWS_REGION=us-east-2 \
      --name xray-daemon \
      -p 2000:2000/udp \
      xray-daemon -o
```

Este comando utiliza las siguientes opciones:

- `--attach STDOUT`: ver la salida del daemon en el terminal.
- `-v ~/.aws/:/root/.aws/:ro`: asignar el acceso de solo lectura al contenedor `.aws` para que pueda leer sus credenciales del SDK de AWS.
- `AWS_REGION=`*`us-east-2`*: establecer la variable de entorno `AWS_REGION` para indicar al daemon la región que debe utilizar.
- `--net=host`: adjunte el contenedor a la red `host`. Los contenedores de la red host pueden comunicarse entre sí sin publicar puertos.
- `-p 2000:2000/udp`: asignar el puerto UDP 2000 en el equipo al mismo puerto del contenedor. Esto no es necesario para que se comuniquen los contenedores de la misma red, pero sí permite enviar segmentos al demonio desde la línea de comandos o desde una aplicación que no se ejecuta en Docker.
- `--name xray-daemon`: asignar el nombre `xray-daemon` al contenedor en lugar de generar un nombre aleatorio.

- `-o` (después del nombre de la imagen): añadir la opción `-o` al punto de entrada que ejecuta el daemon en el contenedor. Esta opción indica al daemon que se ejecute en modo local para impedirle que intente leer los metadatos de la instancia de Amazon EC2.

Para detener el demonio, utilice `docker stop`. Si realiza cambios en el archivo `Dockerfile` y crea una imagen nueva, debe eliminar el contenedor existente para poder crear otra con el mismo nombre. Utilice `docker rm` para eliminar el contenedor.

```
$ docker stop xray-daemon
$ docker rm xray-daemon
```

Ejecución de un daemon de X-Ray en Windows

Puede ejecutar el daemon ejecutable desde la línea de comandos. Utilice la opción `-o` para ejecutarlo en modo local y `-n` para configurar la región.

```
> .\xray_windows.exe -o -n us-east-2
```

Utilice un script en PowerShell para crear y ejecutar un servicio para el demonio.

Example PowerShell script: Windows

```
if ( Get-Service "AWSXRayDaemon" -ErrorAction SilentlyContinue ){
    sc.exe stop AWSXRayDaemon
    sc.exe delete AWSXRayDaemon
}
if ( Get-Item -path aws-xray-daemon -ErrorAction SilentlyContinue ) {
    Remove-Item -Recurse -Force aws-xray-daemon
}

$currentLocation = Get-Location
$zipFileName = "aws-xray-daemon-windows-service-3.x.zip"
$zipPath = "$currentLocation\$zipFileName"
$destPath = "$currentLocation\aws-xray-daemon"
$daemonPath = "$destPath\xray.exe"
$daemonLogPath = "C:\inetpub\wwwroot\xray-daemon.log"
$url = "https://s3.dualstack.us-west-2.amazonaws.com/aws-xray-assets.us-west-2/xray-
daemon/aws-xray-daemon-windows-service-3.x.zip"

Invoke-WebRequest -Uri $url -OutFile $zipPath
```

```
Add-Type -Assembly "System.IO.Compression.Filesystem"
[io.compression.zipfile]::ExtractToDirectory($zipPath, $destPath)

sc.exe create AWSXRayDaemon binPath= "$daemonPath -f $daemonLogPath"
sc.exe start AWSXRayDaemon
```

Ejecución del daemon de X-Ray en OS X

Puede ejecutar el daemon ejecutable desde la línea de comandos. Utilice la opción `-o` para ejecutarlo en modo local y `-n` para configurar la región.

```
~/xray-daemon$ ./xray_mac -o -n us-east-2
```

Para ejecutar el demonio en segundo plano, use &.

```
~/xray-daemon$ ./xray_mac -o -n us-east-2 &
```

Utilice nohup para evitar que el demonio finalice cuando se cierre la terminal.

```
~/xray-daemon$ nohup ./xray_mac &
```

Ejecución del daemon de X-Ray en AWS Elastic Beanstalk

Para retransmitir los datos de rastreo desde su aplicación a AWS X-Ray, puede ejecutar el daemon de X-Ray en instancias de Amazon EC2 de su entorno de Elastic Beanstalk. Para ver una lista de plataformas compatibles, consulte Configuración de la depuración en AWS X-Ray en la Guía para desarrolladores de AWS Elastic Beanstalk.

> **Note**
>
> El daemon utiliza el perfil de instancia del entorno para obtener permisos. Para obtener instrucciones sobre cómo añadir permisos al perfil de instancia de Elastic Beanstalk, consulte Permiso para el envío de datos a X-Ray desde el daemon.

Las plataformas de Elastic Beanstalk proporcionan una opción de configuración que puede establecer para ejecutar el daemon de forma automática. Puede habilitar el daemon en un archivo de

configuración en el código fuente o mediante la opción disponible en la consola de Elastic Beanstalk. Cuando habilita la opción de configuración, el demonio se instala en la instancia y se ejecuta como servicio.

Es posible que la versión incluida en las plataformas de Elastic Beanstalk no sea la versión más reciente. Consulte Plataformas compatibles para ver qué versión del demonio está disponible para la configuración de la plataforma que utiliza.

Elastic Beanstalk no proporciona el daemon X-Ray en la plataforma Multicontainer Docker (Amazon ECS).

Uso de la integración de X-Ray de Elastic Beanstalk para ejecutar el daemon de X-Ray

Utilice la consola para activar la integración de X-Ray o configúrela en el código fuente de la aplicación con un archivo de configuración.

Para habilitar el daemon de X-Ray en la consola de Elastic Beanstalk:

1. Abra la consola de Elastic Beanstalk.
2. Desplácese hasta la consola de administración del entorno.
3. Elija Configuration (Configuración).
4. Elija Software Settings (Configuración de software).
5. En X-Ray daemon (Demonio de X-Ray), elija Enabled (Habilitado).
6. Seleccione Apply (Aplicar).

Puede incluir un archivo de configuración en el código fuente para que la configuración sea portátil entre entornos.

Example .ebextensions/xray-daemon.config

```
option_settings:
  aws:elasticbeanstalk:xray:
    XRayEnabled: true
```

Elastic Beanstalk transfiere un archivo de configuración al daemon y envía los registros a una ubicación estándar.

En plataformas Windows Server

- Archivo de configuración: `C:\Program Files\Amazon\XRay\cfg.yaml`
- Registros: `c:\Program Files\Amazon\XRay\logs\xray-service.log`

En plataformas Linux

- Archivo de configuración: `/etc/amazon/xray/cfg.yaml`
- Registros: `/var/log/xray/xray.log`

Elastic Beanstalk proporciona herramientas para extraer registros de instancias de la AWS Management Console o de la línea de comandos. Puede indicar a Elastic Beanstalk que incluya los registros del daemon de X-Ray añadiendo una tarea con un archivo de configuración.

Example .ebextensions/xray-logs.config - Linux

```
files:
  "/opt/elasticbeanstalk/tasks/taillogs.d/xray-daemon.conf" :
    mode: "000644"
    owner: root
    group: root
    content: |
      /var/log/xray/xray.log
```

Example .ebextensions/xray-logs.config: Windows Server

```
files:
  "c:/Program Files/Amazon/ElasticBeanstalk/config/taillogs.d/xray-daemon.conf" :
    mode: "000644"
    owner: root
    group: root
    content: |
      c:\Progam Files\Amazon\XRay\logs\xray-service.log
```

Consulte la sección Consulta de los registros desde las instancias de Amazon EC2 del entorno de Elastic Beanstalk en la Guía para desarrolladores de AWS Elastic Beanstalk para obtener más información.

Descarga y ejecución del daemon de X-Ray manualmente (avanzado)

Si el daemon de X-Ray no está disponible para la configuración de la plataforma, puede descargarlo desde Amazon S3 y ejecutarlo con un archivo de configuración.

Utilice un archivo de configuración de Elastic Beanstalk para descargar y ejecutar el daemon.

Example .ebextensions/xray.config - Linux

```
commands:
  01-stop-tracing:
    command: yum remove -y xray
    ignoreErrors: true
  02-copy-tracing:
    command: curl https://s3.us-east-2.amazonaws.com/aws-xray-assets.us-east-2/xray-
daemon/aws-xray-daemon-3.x.rpm -o /home/ec2-user/xray.rpm
  03-start-tracing:
    command: yum install -y /home/ec2-user/xray.rpm

files:
  "/opt/elasticbeanstalk/tasks/taillogs.d/xray-daemon.conf" :
    mode: "000644"
    owner: root
    group: root
    content: |
      /var/log/xray/xray.log
  "/etc/amazon/xray/cfg.yaml" :
    mode: "000644"
    owner: root
    group: root
    content: |
      Logging:
        LogLevel: "debug"
      Version: 2
```

Example .ebextensions/xray.config: Windows Server

```
container_commands:
  01-execute-config-script:
    command: Powershell.exe -ExecutionPolicy Bypass -File c:\\temp\\installDaemon.ps1
    waitAfterCompletion: 0
```

```
files:
  "c:/temp/installDaemon.ps1":
    content: |
      if ( Get-Service "AWSXRayDaemon" -ErrorAction SilentlyContinue ) {
          sc.exe stop AWSXRayDaemon
          sc.exe delete AWSXRayDaemon
      }

      $targetLocation = "C:\Program Files\Amazon\XRay"
      if ((Test-Path $targetLocation) -eq 0) {
          mkdir $targetLocation
      }

      $zipFileName = "aws-xray-daemon-windows-service-3.x.zip"
      $zipPath = "$targetLocation\$zipFileName"
      $destPath = "$targetLocation\aws-xray-daemon"
      if ((Test-Path $destPath) -eq 1) {
          Remove-Item -Recurse -Force $destPath
      }

      $daemonPath = "$destPath\xray.exe"
      $daemonLogPath = "$targetLocation\xray-daemon.log"
      $url = "https://s3.dualstack.us-west-2.amazonaws.com/aws-xray-assets.us-west-2/
xray-daemon/aws-xray-daemon-windows-service-3.x.zip"

      Invoke-WebRequest -Uri $url -OutFile $zipPath
      Add-Type -Assembly "System.IO.Compression.Filesystem"
      [io.compression.zipfile]::ExtractToDirectory($zipPath, $destPath)

      New-Service -Name "AWSXRayDaemon" -StartupType Automatic -BinaryPathName
 "`"$daemonPath`" -f `"$daemonLogPath`""
      sc.exe start AWSXRayDaemon
    encoding: plain
  "c:/Program Files/Amazon/ElasticBeanstalk/config/taillogs.d/xray-daemon.conf" :
    mode: "000644"
    owner: root
    group: root
    content: |
      C:\Program Files\Amazon\XRay\xray-daemon.log
```

Estos ejemplos también añaden el archivo de registro del daemon a la tarea de registros de finalización de Elastic Beanstalk para incluirlo cuando se soliciten registros con la consola o la interfaz de línea de comandos de Elastic Beanstalk (CLI de EB).

Ejecución del daemon de X-Ray en Amazon EC2

Puede ejecutar el daemon de X-Ray en los siguientes sistemas operativos con Amazon EC2:

- Amazon Linux
- Ubuntu
- Windows Server (2012 R2 y posteriores)

Utilice un perfil de instancia para conceder permiso al daemon para cargar datos de rastreo en X-Ray. Para obtener más información, consulte Permiso para el envío de datos a X-Ray desde el daemon.

Utilice un script de datos de usuario para ejecutar el demonio de manera automática cuando inicie la instancia.

Example Script de datos de usuario: Linux

```
#!/bin/bash
curl https://s3.us-east-2.amazonaws.com/aws-xray-assets.us-east-2/xray-daemon/aws-xray-daemon-3.x.rpm -o /home/ec2-user/xray.rpm
yum install -y /home/ec2-user/xray.rpm
```

Example Script de datos de usuario: Windows Server

```
<powershell>
if ( Get-Service "AWSXRayDaemon" -ErrorAction SilentlyContinue ) {
    sc.exe stop AWSXRayDaemon
    sc.exe delete AWSXRayDaemon
}

$targetLocation = "C:\Program Files\Amazon\XRay"
if ((Test-Path $targetLocation) -eq 0) {
    mkdir $targetLocation
}

$zipFileName = "aws-xray-daemon-windows-service-3.x.zip"
$zipPath = "$targetLocation\$zipFileName"
$destPath = "$targetLocation\aws-xray-daemon"
if ((Test-Path $destPath) -eq 1) {
    Remove-Item -Recurse -Force $destPath
```

```
}

$daemonPath = "$destPath\xray.exe"
$daemonLogPath = "$targetLocation\xray-daemon.log"
$url = "https://s3.dualstack.us-west-2.amazonaws.com/aws-xray-assets.us-west-2/xray-
daemon/aws-xray-daemon-windows-service-3.x.zip"

Invoke-WebRequest -Uri $url -OutFile $zipPath
Add-Type -Assembly "System.IO.Compression.Filesystem"
[io.compression.zipfile]::ExtractToDirectory($zipPath, $destPath)

New-Service -Name "AWSXRayDaemon" -StartupType Automatic -BinaryPathName
 "`"$daemonPath`" -f `"$daemonLogPath`""
sc.exe start AWSXRayDaemon
</powershell>
```

Ejecución del daemon de X-Ray en Amazon ECS

En Amazon ECS, cree una imagen de Docker que ejecute el daemon de X-Ray, cárguelo en el repositorio de imágenes de Docker y luego impleméntelo en su clúster de Amazon ECS. Puede utilizar mapeos de puertos y la configuración del modo de red en el archivo de definición de tareas para permitir que la aplicación se comunique con el contenedor del demonio.

Uso de la imagen de Docker oficial de la

X-Ray proporciona una imagen del contenedor de Docker en Amazon ECR que puede implementar junto con la aplicación. Para obtener más información, consulte Descarga del daemon.

Example Definición de tarea

```
{
  "name": "xray-daemon",
  "image": "amazon/aws-xray-daemon",
  "cpu": 32,
  "memoryReservation": 256,
  "portMappings" : [
      {
          "hostPort": 0,
          "containerPort": 2000,
          "protocol": "udp"
```

```
        }
      ]
   }
```

Creación y compilación de una imagen de Docker

Si desea realizar una configuración personalizada, es posible que tenga que definir su propia imagen de Docker.

Añada políticas administradas al rol de tarea para conceder permiso al daemon para cargar datos de rastreo en X-Ray. Para obtener más información, consulte Permiso para el envío de datos a X-Ray desde el daemon.

Utilice uno de los siguientes Dockerfiles para crear una imagen que ejecute el demonio.

Example Dockerfile: Amazon Linux

```
FROM amazonlinux
RUN yum install -y unzip
RUN curl -o daemon.zip https://s3.us-east-2.amazonaws.com/aws-xray-assets.us-east-2/
xray-daemon/aws-xray-daemon-linux-3.x.zip
RUN unzip daemon.zip && cp xray /usr/bin/xray
ENTRYPOINT ["/usr/bin/xray", "-t", "0.0.0.0:2000", "-b", "0.0.0.0:2000"]
EXPOSE 2000/udp
EXPOSE 2000/tcp
```

> **Note**
>
> Las marcas `-t` y `-b` son necesarias para especificar una dirección de enlace que escuche el bucle invertido de un entorno con varios contenedores.

Example Dockerfile: Ubuntu

Para los derivados de Debian, tendrá que instalar certificados de una autoridad de certificación (CA) para evitar problemas al descargar el instalador.

```
FROM ubuntu:16.04
RUN apt-get update && apt-get install -y --force-yes --no-install-recommends apt-
transport-https curl ca-certificates wget && apt-get clean && apt-get autoremove && rm
 -rf /var/lib/apt/lists/*
```

```
RUN wget https://s3.us-east-2.amazonaws.com/aws-xray-assets.us-east-2/xray-daemon/aws-
xray-daemon-3.x.deb
RUN dpkg -i aws-xray-daemon-3.x.deb
ENTRYPOINT ["/usr/bin/xray", "--bind=0.0.0.0:2000", "--bind-tcp=0.0.0.0:2000"]
EXPOSE 2000/udp
EXPOSE 2000/tcp
```

En la definición de tarea, la configuración depende del modo de red que se utilice. El modo de red puente es la opción predeterminada y se puede utilizar en la VPC predeterminada. En una red en modo puente, establezca la variable de entorno `AWS_XRAY_DAEMON_ADDRESS` para indicar al SDK de X-Ray a qué puerto del contenedor se ha de hacer referencia y establezca el puerto de host. Por ejemplo, podría publicar el puerto UDP 2000 y crear un enlace desde el contenedor de la aplicación hasta el contenedor del demonio.

Example Definición de tarea

```
    {
      "name": "xray-daemon",
      "image": "123456789012.dkr.ecr.us-east-2.amazonaws.com/xray-daemon",
      "cpu": 32,
      "memoryReservation": 256,
      "portMappings" : [
          {
              "hostPort": 0,
              "containerPort": 2000,
              "protocol": "udp"
          }
       ]
    },
    {
      "name": "scorekeep-api",
      "image": "123456789012.dkr.ecr.us-east-2.amazonaws.com/scorekeep-api",
      "cpu": 192,
      "memoryReservation": 512,
      "environment": [
          { "name" : "AWS_REGION", "value" : "us-east-2" },
          { "name" : "NOTIFICATION_TOPIC", "value" : "arn:aws:sns:us-
east-2:123456789012:scorekeep-notifications" },
          { "name" : "AWS_XRAY_DAEMON_ADDRESS", "value" : "xray-daemon:2000" }
      ],
      "portMappings" : [
          {
```

```
            "hostPort": 5000,
            "containerPort": 5000
        }
      ],
      "links": [
        "xray-daemon"
      ]
    }
```

Si ejecuta el clúster en la subred privada de una VPC, puede utilizar el modo de red `awsvpc` para asociar una interfaz de red elástica (ENI) a los contenedores. De este modo, puede evitar utilizar enlaces. Omita el puerto de host en los mapeos de puertos, el enlace y la variable de entorno `AWS_XRAY_DAEMON_ADDRESS`.

Example Definición de tarea de VPC

```
{
    "family": "scorekeep",
    "networkMode":"awsvpc",
    "containerDefinitions": [
        {
          "name": "xray-daemon",
          "image": "123456789012.dkr.ecr.us-east-2.amazonaws.com/xray-daemon",
          "cpu": 32,
          "memoryReservation": 256,
          "portMappings" : [
              {
                  "containerPort": 2000,
                  "protocol": "udp"
              }
          ]
        },
        {
            "name": "scorekeep-api",
            "image": "123456789012.dkr.ecr.us-east-2.amazonaws.com/scorekeep-api",
            "cpu": 192,
            "memoryReservation": 512,
            "environment": [
                { "name" : "AWS_REGION", "value" : "us-east-2" },
                { "name" : "NOTIFICATION_TOPIC", "value" : "arn:aws:sns:us-
east-2:123456789012:scorekeep-notifications" }
            ],
            "portMappings" : [
```

```
                {
                    "containerPort": 5000
                }
            ]
        }
    ]
}
```

Configuración de las opciones de línea de comandos en la consola de Amazon ECS

Las opciones de línea de comandos anulan cualquier valor que presente algún conflicto del archivo de configuración de la imagen. Las opciones de línea de comandos se suelen utilizar para pruebas locales, pero también se pueden utilizar para mayor comodidad al establecer variables de entorno o con el fin de controlar el proceso de inicio.

Al añadir opciones de línea de comandos, se actualiza el `CMD` de Docker que se pasa al contenedor. Para obtener más información, consulte Docker run reference.

Para establecer una opción de línea de comandos

1. Abra la consola de Amazon ECS en https://console.aws.amazon.com/ecs/.
2. En la barra de navegación, seleccione la región que contiene la definición de tarea.
3. En el panel de navegación, elija Task Definitions.
4. En la página Task Definitions, seleccione la casilla situada a la izquierda de la definición de tarea que revisar y seleccione Create new revision.
5. En la página Create new revision of Task Definition (Crear nueva revisión de definición de tarea), seleccione el contenedor.
6. En la sección ENVIRONMENT (ENTORNO), añada al campo Command (Comando) la lista de opciones de línea de comandos separadas por comas.
7. Elija Actualizar.
8. Verifique la información y seleccione Create.

En el ejemplo siguiente se muestra cómo escribir una opción de línea de comandos separada por comas para la opción `RoleARN`. La opción `RoleARN` asume el rol de IAM especificado para cargar segmentos en una cuenta diferente.

Example

```
--role-arn, arn:aws:iam::123456789012:role/xray-cross-account
```

Para obtener más información sobre las opciones de línea de comandos disponibles en X-Ray, consulte Configuración del daemon de AWS X-Ray.

Instrumentación de su solicitud para AWS X-Ray

La instrumentación de una aplicación implica el envío de datos de rastro para solicitudes entrantes y salientes y otros eventos de la aplicación junto con los metadatos de cada solicitud. Hay varias opciones de instrumentación entre las que puede elegir o que puede combinar, en función de sus requisitos particulares:

- Instrumentación automática: instrumente su aplicación sin cambios de código, normalmente mediante cambios de configuración, añadiendo un agente de instrumentación automática u otros mecanismos.
- Instrumentación de biblioteca: realice cambios mínimos en el código de la aplicación para agregar instrumentación prediseñada destinada a bibliotecas o marcos específicos, como el AWS SDK, los clientes HTTP de Apache o los clientes SQL.
- Instrumentación manual: añada código de instrumentación a su aplicación en cada ubicación a la que desee enviar la información de rastro.

Existen varios SDK, agentes y herramientas que puede utilizar para instrumentar su aplicación para rastreo de X-Ray.

Temas

Instrumente su aplicación con la distribución para AWS OpenTelemetry

The AWS Distro for OpenTelemetry (ADOT) es una AWS distribución basada en el proyecto Cloud Native Computing Foundation (CNCF). OpenTelemetry OpenTelemetry proporciona un conjunto único de API, bibliotecas y agentes de código abierto para recopilar rastreos y métricas distribuidos. Este kit de herramientas es una distribución de OpenTelemetry componentes originales que incluye SDK, agentes de autoinstrumentación y recopiladores que se prueban, optimizan, protegen y respaldan. AWS

Con ADOT, los ingenieros pueden instrumentar sus aplicaciones una vez y enviar métricas y rastreos correlacionados a múltiples soluciones de AWS monitoreo CloudWatch AWS X-Ray, incluidas Amazon y Amazon OpenSearch Service.

El uso de X-Ray con ADOT requiere dos componentes: un OpenTelemetry SDK habilitado para su uso con X-Ray y una AWS Distro for OpenTelemetry Collector habilitada para su uso con X-Ray. Para obtener más información sobre el uso de la AWS distribución OpenTelemetry con AWS X-Ray y otros Servicios de AWS, consulte la documentación de la AWS distribución. OpenTelemetry

Para obtener más información sobre el soporte y el uso de idiomas, consulta AWS Observabilidad en. GitHub

> **Note**
>
> Ahora puede usar el CloudWatch agente para recopilar métricas, registros y seguimientos de las instancias de Amazon EC2 y de los servidores locales. CloudWatch La versión 1.300025.0 del agente y posteriores puede recopilar trazas de los SDK de nuestros clientes de OpenTelemetryX-Ray y enviarlas a X-Ray. Utilizar el CloudWatch agente en lugar del Collector AWS Distro for OpenTelemetry (ADOT) o el daemon X-Ray para recopilar trazas puede ayudarle a reducir la cantidad de agentes que administra. Consulte el tema sobre los CloudWatch agentes en la Guía del CloudWatch usuario para obtener más información.

ADOT incluye lo siguiente:

- AWS Distro for Go OpenTelemetry
- AWS Distro para Java OpenTelemetry
- AWS Distro para OpenTelemetry JavaScript

- AWS Distro para Python OpenTelemetry
- AWS Distro para .NET OpenTelemetry

Actualmente, ADOT admite la instrumentación automática para Java y Python. Además, ADOT permite la instrumentación automática de las funciones de AWS Lambda y sus solicitudes posteriores mediante tiempos de ejecución de Java, Node.js y Python, mediante capas Lambda gestionadas por ADOT.

Los SDK de ADOT para Java y Go admiten las reglas de muestreo centralizado de X-Ray. Si necesita soporte para las reglas de muestreo de X-Ray en otros idiomas, considere la posibilidad de usar un AWS X-Ray SDK.

> **Note**
>
> Ahora puede enviar identificadores de rastro que se ajustan a la especificación de W3C a X-Ray. De forma predeterminada, las trazas que se crean OpenTelemetry tienen un formato de ID de traza que se basa en la especificación del contexto de rastreo del W3C. Este formato es diferente del de los identificadores de rastreo que se crean con un SDK de X-Ray o mediante AWS servicios integrados con X-Ray. Para garantizar que X-Ray acepte los identificadores de rastreo en formato W3C, debe usar la versión 0.86.0 o posterior de AWS X-Ray Exporter, que se incluye en la versión 0.34.0 y posteriores de ADOT Collector. Las versiones anteriores del exportador validan las marcas de tiempo de los identificadores de rastreo, lo que puede provocar el rechazo de los identificadores de rastreo del W3C.

Instrumentación de su aplicación con SDK de AWS X-Ray

AWS X-Ray incluye un conjunto de SDK específicos para cada idioma para instrumentar su aplicación y enviar trazas a X-Ray. Cada SDK de X-Ray proporciona lo siguiente:

- Interceptadores que añadir a su código para rastrear solicitudes HTTP entrantes
- Controladores de clientes para instrumentar los clientes del AWS SDK que tu aplicación utiliza para llamar a otros Servicios de AWS
- Un cliente HTTP para instrumentar llamadas a servicios web HTTP internos y externos

Los SDK de X-Ray también admiten llamadas de instrumentación a bases de datos SQL, instrumentación automática de clientes de AWS SDK y otras funciones. En lugar de enviar los datos

de rastro directamente a X-Ray, el SDK envía documentos de segmento JSON a un proceso del daemon que escucha el tráfico UDP. El daemon de X-Ray almacena en búfer segmentos en una cola y los carga en X-Ray en lotes.

Se proporcionan los siguientes SDK específicos para cada lenguaje:

- AWS X-Ray SDK para Go
- AWS X-Ray SDK para Java
- AWS X-Ray SDK para Node.js
- AWS X-Ray SDK para Python
- AWS X-Ray SDK para .NET
- AWS X-Ray SDK para Ruby

Actualmente, X-Ray admite la instrumentación automática para Java.

Cómo elegir entre los AWS SDK Distro for OpenTelemetry y X-Ray

Los SDK de X-Ray son parte de una solución de instrumentación estrechamente integrada que ofrece AWS. El AWS Distro for OpenTelemetry forma parte de una solución industrial más amplia en la que X-Ray es solo una de las muchas soluciones de rastreo. Puede implementar el end-to-end rastreo en X-Ray utilizando cualquiera de los dos enfoques, pero es importante entender las diferencias para determinar cuál es el enfoque más útil para usted.

Le recomendamos que equipe su aplicación con la AWS Distro OpenTelemetry si necesita lo siguiente:

- La posibilidad de enviar trazas a varios backends de rastreo diferentes sin tener que volver a instrumentar el código
- Support para una gran cantidad de instrumentaciones bibliotecarias para cada idioma, mantenidas por la comunidad OpenTelemetry
- Capas de Lambda completamente administradas que empaquetan todo lo necesario para recopilar datos de telemetría sin necesidad de cambios de código al usar Java, Python o Node.js

> **Note**
>
> AWS Distro for OpenTelemetry ofrece una experiencia de inicio más sencilla para instrumentar las funciones de Lambda. Sin embargo, debido a la flexibilidad que

OpenTelemetry ofrece, la función Lambda requerirá memoria adicional y las invocaciones pueden experimentar un aumento de la latencia de arranque en frío, lo que puede generar cargos adicionales. Si está optimizando para una baja latencia y no necesita capacidades avanzadas, como destinos OpenTelemetry de back-end configurables de forma dinámica, puede utilizar el SDK de AWS X-Ray para instrumentar su aplicación.

Le recomendamos que elija un SDK de X-Ray para instrumentar su aplicación si necesita lo siguiente:

- Una solución de un solo proveedor perfectamente integrada
- Integración en reglas de muestreo centralizadas de X-Ray, incluida la capacidad de configurar las reglas de muestreo desde la consola de X-Ray y utilizarlas automáticamente en varios hosts, al utilizar Node.js, Python, Ruby o .NET

Instrumentación de su aplicación con Go

Hay dos maneras de instrumentar su Go aplicación para enviar trazas a X-Ray:

- AWS Distro for OpenTelemetry Go: una AWS distribución que proporciona un conjunto de bibliotecas de código abierto para enviar métricas y rastreos correlacionados a varias soluciones de AWS monitoreo, incluidas Amazon y Amazon OpenSearch Service CloudWatch AWS X-Ray, a través de AWS Distro for Collector. OpenTelemetry
- AWS X-Ray SDK para Go: conjunto de bibliotecas para generar y enviar trazas a X-Ray mediante el daemon X-Ray.

Para obtener más información, consulte Cómo elegir entre los AWS SDK Distro for OpenTelemetry y X-Ray.

AWS Distro para OpenTelemetry Go

Con AWS Distro para OpenTelemetry Go, puede instrumentar sus aplicaciones una vez y enviar métricas y rastros correlacionados a varias soluciones de supervisión de AWS, incluidas Amazon CloudWatch, AWS X-Ray y Amazon OpenSearch Service. El uso de X-Ray con AWS Distro para OpenTelemetry requiere dos componentes: un SDK de OpenTelemetry habilitado para usarlo con X-Ray y el AWS Distro para OpenTelemetry Collector habilitado para usarlo con X-Ray.

Para empezar, consulte la documentación de AWS Distro para OpenTelemetry Go.

Para obtener más información sobre el uso de AWS Distro para OpenTelemetry con AWS X-Ray y otros Servicios de AWS, consulte AWS Distro para OpenTelemetry o la documentación de AWS Distro para OpenTelemetry.

Para obtener información adicional sobre los lenguajes compatibles y el uso, consulte AWS Observability en GitHub.

SDK de AWS X-Ray para Go

El SDK de X-Ray para Go es un conjunto de bibliotecas para aplicaciones Go que proporcionan clases y métodos para generar y enviar datos de rastreo al daemon de X-Ray. En los datos de rastreo se incluye información sobre las solicitudes HTTP entrantes que atiende la aplicación, además de las llamadas que la aplicación realiza a servicios posteriores mediante el SDK de AWS, clientes HTTP o un conector a la base de datos SQL. También puede crear segmentos de forma manual y agregar información de depuración en anotaciones y metadatos.

Descargue el SDK desde su repositorio de GitHub con `go get`:

```
$ go get -u github.com/aws/aws-xray-sdk-go/...
```

Para las aplicaciones web, comience por utilizar la función `xray.Handler` para realizar el seguimiento de las solicitudes entrantes. El controlador de mensajes crea un segmento para cada solicitud rastreada y lo completa cuando se envía la respuesta. Mientras el segmento está abierto, puede utilizar los métodos del cliente del SDK para añadir información al segmento y crear subsegmentos para rastrear llamadas posteriores. El SDK también registra automáticamente las excepciones que produce su aplicación mientras el segmento está abierto.

En el caso de las funciones de Lambda llamadas por una aplicación o un servicio instrumentados, Lambda lee el encabezado de rastreo y rastrea automáticamente las solicitudes muestreadas. Para otras funciones, puede configurar Lambda con el fin de muestrear y rastrear las solicitudes entrantes. En cualquier caso, Lambda crea el segmento y se lo proporciona al SDK de X-Ray.

> **Note**
>
> En Lambda, el SDK de X-Ray es opcional. Si no lo usa en su función, el mapa de servicio seguirá incluyendo un nodo para el servicio de Lambda y uno para cada función de Lambda. Al añadir el SDK, puede instrumentar el código de función para añadir subsegmentos al

segmento de función registrado por Lambda. Para obtener más información, consulte AWS Lambda y AWS X-Ray.

A continuación, envuelva su cliente con una llamada a la función `AWS`. Este paso garantiza que X-Ray instrumente las llamadas a los métodos del cliente. También puede instrumentar llamadas a bases de datos SQL.

En cuanto empiece a utilizar el SDK, personalice su comportamiento configurando la grabadora y el controlador y el middleware. Puede añadir complementos para registrar los datos sobre los recursos informáticos que ejecutan su aplicación, personalizar el comportamiento de muestreo mediante la definición de reglas de muestreo y definir el nivel de log para ver más o menos información del SDK en los logs de las aplicaciones.

Registre información adicional acerca de las solicitudes y el trabajo que la aplicación realiza en anotaciones y metadatos. Las anotaciones son pares sencillos de clave-valor que se indexan para su uso con expresiones de filtro para poder buscar rastros que contengan datos específicos. Las entradas de metadatos son menos restrictivas y pueden registrar objetos y matrices completos, es decir, todo lo que se pueda serializar en JSON.

> **Anotaciones y metadatos**
>
> Las anotaciones y los metadatos son texto arbitrario que se agrega a los segmentos con el SDK de X-Ray. Las anotaciones se indexan para su uso con expresiones de filtro. Los metadatos no se indexan pero se pueden ver en el segmento sin procesar con la consola o la API de X-Ray. Cualquier persona a la que conceda acceso de lectura a X-Ray puede ver estos datos.

Cuando tenga muchos clientes instrumentados en su código, un único segmento de solicitud puede contener un gran número de subsegmentos, uno para cada llamada realizada con un cliente instrumentado. Puede organizar y agrupar los subsegmentos incluyendo las llamadas del cliente en subsegmentos personalizados. Puede crear un subsegmento personalizado para una función completa o para cualquier sección de código, y registrar los metadatos y las anotaciones en el subsegmento en lugar de escribirlo todo en el segmento principal.

Requisitos

El SDK de X-Ray para Go requiere Go 1.9 o una versión posterior.

El SDK depende de las siguientes bibliotecas durante la compilación y el tiempo de ejecución:

- SDK de AWS para Go versión 1.10.0 o más reciente

Estas dependencias se han declarado en el archivo `README.md` del SDK.

Documentación de referencia

Una vez que haya descargado el SDK, compile y aloje la documentación localmente para verla en un navegador web.

Para ver la documentación de referencia

1. Vaya al directorio `$GOPATH/src/github.com/aws/aws-xray-sdk-go` (Linux o Mac) o la carpeta `%GOPATH%\src\github.com\aws\aws-xray-sdk-go` (Windows)
2. Ejecute el comando `godoc`.

   ```
   $ godoc -http=:6060
   ```

3. Abra un navegador en `http://localhost:6060/pkg/github.com/aws/aws-xray-sdk-go/`.

Configuración del SDK de X-Ray para Go

Puede especificar la configuración del SDK de X-Ray para Go a través de variables de entorno, llamando a `Configure` con un objeto `Config` o suponiendo valores predeterminados. Las variables de entorno tienen prioridad sobre los valores `Config`, que tienen prioridad sobre cualquier valor predeterminado.

Secciones

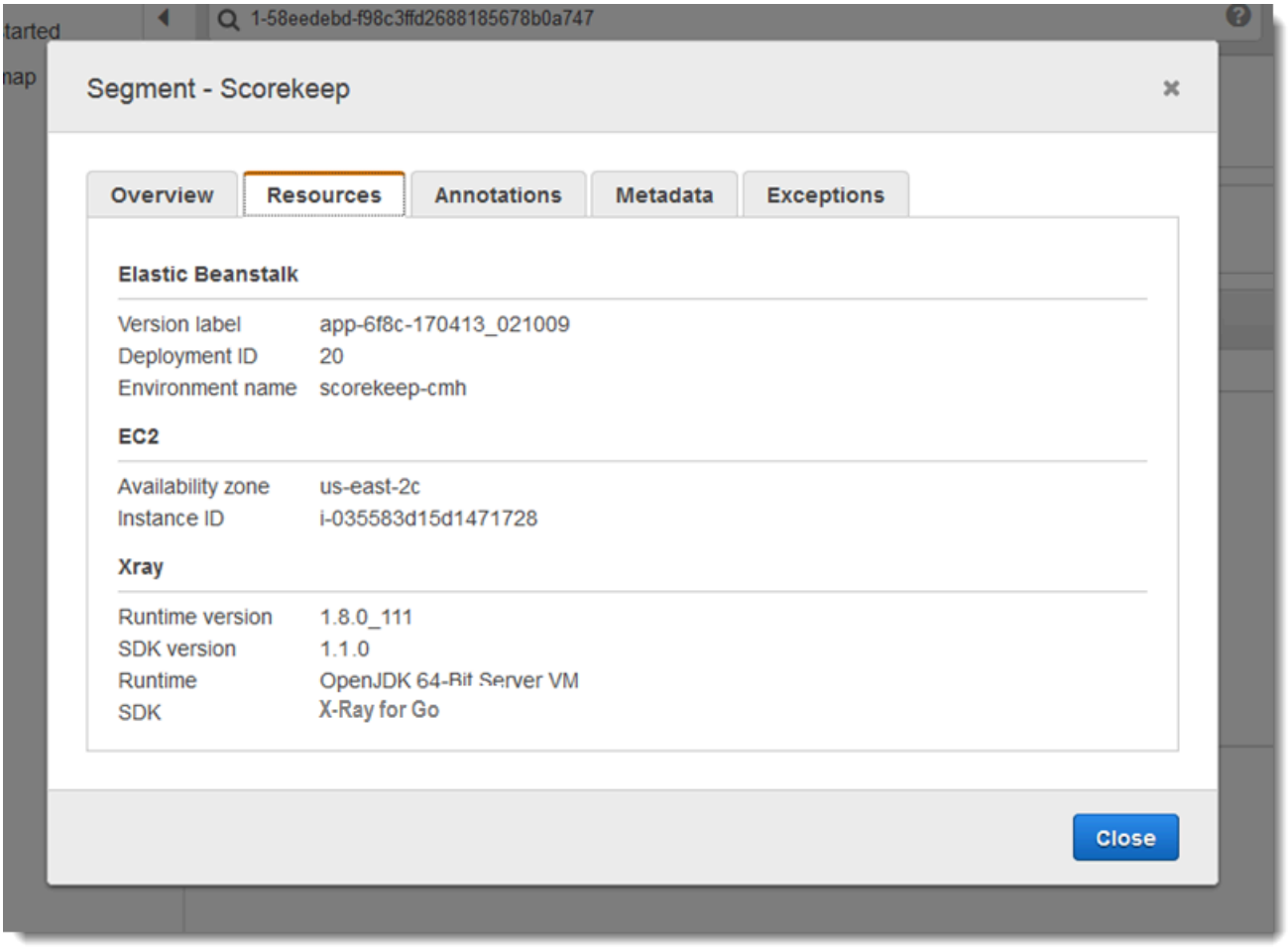
- Complementos del servicio
- Reglas de muestreo
- Registro
- Variables de entorno
- Uso de la opción configure

Complementos del servicio

Utilice `plugins` para registrar información sobre el servicio que aloja la aplicación.

Complementos

- Amazon EC2: `EC2Plugin` agrega el ID de la instancia, la zona de disponibilidad y el grupo de CloudWatch registros.
- Elastic Beanstalk: `ElasticBeanstalkPlugin` añade el nombre de entorno, la etiqueta de versión y el ID de implementación.
- Amazon ECS: `ECSPlugin` agrega el ID de contenedor.



Para utilizar un complemento, importe uno de los siguientes paquetes.

```
"github.com/aws/aws-xray-sdk-go/awsplugins/ec2"
"github.com/aws/aws-xray-sdk-go/awsplugins/ecs"
```

```
"github.com/aws/aws-xray-sdk-go/awsplugins/beanstalk"
```

Cada complemento tiene una llamada de función `Init()` explícita que lo carga.

Example ec2.Init()

```
import (
 "os"

 "github.com/aws/aws-xray-sdk-go/awsplugins/ec2"
 "github.com/aws/aws-xray-sdk-go/xray"
)

func init() {
  // conditionally load plugin
  if os.Getenv("ENVIRONMENT") == "production" {
    ec2.Init()
  }

  xray.Configure(xray.Config{
    ServiceVersion: "1.2.3",
  })
}
```

El SDK también usa la configuración del complemento para establecer el campo `origin` en el segmento. Esto indica el tipo de AWS recurso que ejecuta la aplicación. Cuando utilizas varios complementos, el SDK utiliza el siguiente orden de resolución para determinar el origen: ElasticBeanstalk > EKS > ECS > EC2.

Reglas de muestreo

El SDK utiliza las reglas de muestreo que define el usuario en la consola de X-Ray para determinar qué solicitudes registrar. La regla predeterminada rastrea la primera solicitud cada segundo y el 5 % de las solicitudes adicionales de todos los servicios que envían rastros a X-Ray. Cree reglas adicionales en la consola de X-Ray para personalizar la cantidad de datos registrados para cada una de sus aplicaciones.

El SDK aplica las reglas personalizadas en el orden en que se definen. Si una solicitud coincide con varias reglas personalizadas, el SDK solo aplica la primera regla.

> **Note**
>
> Si el SDK no puede comunicarse con X-Ray para obtener las reglas de muestreo, vuelve a una regla local predeterminada de la primera solicitud cada segundo y del 5 % de las solicitudes adicionales por host. Eso puede ocurrir si el host no tiene permiso para llamar a las API de muestreo o no puede conectarse al daemon de X-Ray, que actúa como proxy TCP para las llamadas a las API realizadas por el SDK.

También puede configurar el SDK para que cargue las reglas de muestreo desde un documento JSON. El SDK puede usar las reglas locales como respaldo para los casos en que el muestreo de X-Ray no esté disponible, o puede usar las reglas locales exclusivamente.

Example sampling-rules.json

```
{
  "version": 2,
  "rules": [
    {
      "description": "Player moves.",
      "host": "*",
      "http_method": "*",
      "url_path": "/api/move/*",
      "fixed_target": 0,
      "rate": 0.05
    }
  ],
  "default": {
    "fixed_target": 1,
    "rate": 0.1
  }
}
```

En este ejemplo se define una regla personalizada y una regla predeterminada. La regla personalizada aplica un porcentaje de muestreo del 5 % sin un número mínimo de solicitudes de rastreo para las rutas incluidas bajo `/api/move/`. La regla predeterminada rastrea la primera solicitud cada segundo y el 10 % de las solicitudes adicionales.

La desventaja de definir las reglas localmente es que el objetivo establecido lo aplica cada instancia de la grabadora de forma independiente, en lugar de ser administrado por el servicio de X-Ray. A

medida que se implementan más hosts, el porcentaje establecido se multiplica, lo que dificulta el control de la cantidad de datos registrados.

Activado AWS Lambda, no se puede modificar la frecuencia de muestreo. Si un servicio instrumentado llama a su función, Lambda registrará las llamadas que generaron solicitudes muestreadas por ese servicio. Si el rastreo activo está activado y no hay ningún encabezado de rastreo, Lambda toma la decisión de muestreo.

Para proporcionar reglas de copia de seguridad, apunte al archivo JSON de muestreo local mediante `NewCentralizedStrategyWithFilePath`.

Example main.go: regla de muestreo local

```
s, _ := sampling.NewCentralizedStrategyWithFilePath("sampling.json") // path to local
 sampling json
xray.Configure(xray.Config{SamplingStrategy: s})
```

Para utilizar solo reglas locales, apunte al archivo JSON de muestreo local mediante `NewLocalizedStrategyFromFilePath`.

Example main.go — Deshabilitar el muestreo

```
s, _ := sampling.NewLocalizedStrategyFromFilePath("sampling.json") // path to local
 sampling json
xray.Configure(xray.Config{SamplingStrategy: s})
```

Registro

> **Note**
>
> Los campos `xray.Config{}` `LogLevel` y `LogFormat` están obsoletos desde la versión 1.0.0-rc.10.

X-Ray utiliza la siguiente interfaz para el registro. El registrador predeterminado escribe en `stdout` a `LogLevelInfo` y superior.

```
type Logger interface {
 Log(level LogLevel, msg fmt.Stringer)
```

```
}

const (
 LogLevelDebug LogLevel = iota + 1
 LogLevelInfo
 LogLevelWarn
 LogLevelError
)
```

Example escribir en **`io.Writer`**

```
xray.SetLogger(xraylog.NewDefaultLogger(os.Stderr, xraylog.LogLevelError))
```

Variables de entorno

Puede usar variables de entorno con el fin de configurar el SDK de X-Ray para Go. El SDK admite las siguientes variables.

- `AWS_XRAY_CONTEXT_MISSING`: establezca esta opción en `RUNTIME_ERROR` para generar excepciones cuando el código instrumentado intente registrar datos sin que haya ningún segmento abierto.

  Valores válidos

  - `RUNTIME_ERROR`: lance una excepción de tiempo de ejecución.
  - `LOG_ERROR`: registre un error y continúe (predeterminado).
  - `IGNORE_ERROR`: ignore el error y continúe.

  Se pueden producir errores relativos a segmentos o subsegmentos inexistentes al intentar usar un cliente instrumentado en el código de inicio que se ejecuta cuando no hay ninguna solicitud abierta o en el código que inicia un nuevo subproceso.
- `AWS_XRAY_TRACING_NAME`: establezca el nombre de servicio que el SDK utiliza para los segmentos.
- `AWS_XRAY_DAEMON_ADDRESS`: establezca el host y el puerto del oyente del daemon de X-Ray. De forma predeterminada, el SDK envía los datos de rastreo a `127.0.0.1:2000`. Use esta variable si ha configurado el daemon para que escuche en un puerto diferente o si se ejecuta en un host diferente.

Las variables de entorno anulan los valores equivalentes establecidos en el código.

Uso de la opción configure

También puede configurar el SDK de X-Ray para Go con el método `Configure`. `Configure` toma un argumento, un objeto `Config`, con los siguientes campos opcionales.

DaemonAddr

Esta cadena especifica el host y el puerto del oyente del daemon de X-Ray. Si no se especifica, X-Ray utiliza el valor de la variable de entorno `AWS_XRAY_DAEMON_ADDRESS`. Si dicho valor no está establecido, utiliza "127.0.0.1:2000".

ServiceVersion

Esta cadena especifica la versión del servicio. Si no se especifica, X-Ray utiliza la cadena vacía (“”).

SamplingStrategy

Este objeto `SamplingStrategy` especifica las llamadas de aplicación a las que se realiza seguimiento. Si no se especifica, X-Ray utiliza una `LocalizedSamplingStrategy`, que adopta la estrategia tal como se define en `xray/resources/DefaultSamplingRules.json`.

StreamingStrategy

Este `StreamingStrategy` objeto especifica si se debe transmitir un segmento cuando RequiresStreamingdevuelve el valor verdadero. Si no se especifica, X-Ray utiliza un `DefaultStreamingStrategy` que transmite un segmento muestreado si el número de subsegmentos es mayor que 20.

ExceptionFormattingStrategy

Este objeto `ExceptionFormattingStrategy` especifica la forma en que desea gestionar diversas excepciones. Si no se especifica, X-Ray utiliza una `DefaultExceptionFormattingStrategy` con un `XrayError` de tipo `error`, el mensaje de error y rastro de la pila.

Instrumentación de las solicitudes HTTP entrantes con el SDK de X-Ray para Go

Puede utilizar el SDK de X-Ray para rastrear las solicitudes HTTP entrantes que su aplicación atiende en una instancia de EC2 en Amazon EC2, AWS Elastic Beanstalk o Amazon ECS.

Utilice `xray.Handler` para instrumentar las solicitudes HTTP entrantes. El SDK de X-Ray para Go implementa la interfaz `http.Handler` de la biblioteca de Go estándar en la clase `xray.Handler`

para interceptar solicitudes web. La clase `xray.Handler` envuelve el `http.Handler` proporcionado con `xray.Capture` utilizando el contexto de la solicitud, analizando los encabezados entrantes, añadiendo encabezados de respuesta si es necesario y, además, establece los campos de rastreo específicos de HTTP.

Al utilizar esta clase para gestionar solicitudes HTTP y respuestas, el SDK de X-Ray para Go crea un segmento para cada solicitud muestreada. Este segmento incluye el momento, el método y la disposición de la solicitud HTTP. La instrumentación adicional crea subsegmentos en este segmento.

> **Note**
>
> En el caso de funciones de AWS Lambda, Lambda crea un segmento para cada solicitud muestreada. Para obtener más información, consulte AWS Lambda y AWS X-Ray.

El siguiente ejemplo intercepta solicitudes en el puerto 8000 y devuelve "Hello!" como respuesta. Crea el segmento `myApp` e instrumenta llamadas a través de cualquier aplicación.

Example main.go

```
func main() {
  http.Handle("/", xray.Handler(xray.NewFixedSegmentNamer("MyApp"),
 http.HandlerFunc(func(w http.ResponseWriter, r *http.Request) {
    w.Write([]byte("Hello!"))
  })))

  http.ListenAndServe(":8000", nil)
}
```

Cada segmento tiene un nombre que identifica la aplicación en el mapa de servicio. El nombre del segmento se puede asignar de forma estática o se puede configurar el SDK para que le asigne un nombre dinámico en función del encabezado del host de la solicitud entrante. La nomenclatura dinámica permite agrupar los rastros en función del nombre de dominio de la solicitud y aplicar un nombre predeterminado si el nombre no coincide con el patrón esperado (por ejemplo, si el encabezado del host está falsificado).

> **Solicitudes reenviadas**
>
> Si un equilibrador de carga u otro intermediario reenvía una solicitud a la aplicación, X-Ray toma la IP de cliente del encabezado `X-Forwarded-For` de la solicitud en lugar de tomar la

IP de origen del paquete IP. La IP de cliente que se graba para una solicitud reenviada puede estar falsificada, por lo que no se debe confiar en ella.

Cuando se reenvía una solicitud, el SDK crea un campo adicional en el segmento para indicar que se realizó esta acción. Si el segmento contiene el campo `x_forwarded_for` configurado en `true`, el IP del cliente se obtiene a partir del encabezado `X-Forwarded-For` en la solicitud HTTP.

El controlador crea un segmento para cada solicitud entrante con un bloque `http` que contiene la siguiente información:

- Método HTTP: GET, POST, PUT, DELETE, etc.
- Dirección del cliente: la dirección IP del cliente que envió la solicitud.
- Código de respuesta: el código de respuesta HTTP para la solicitud finalizada.
- Intervalo: la hora de inicio (cuando se recibió la solicitud) y la hora de finalización (cuando se envió la respuesta).
- Agente del usuario: el `user-agent` de la solicitud.
- Longitud del contenido: la `content-length` de la respuesta.

Configuración de una estrategia de nomenclatura de segmentos

AWS X-Ray utiliza un nombre de servicio para identificar la aplicación y distinguirla del resto de aplicaciones, bases de datos, API externas y recursos de AWS utilizados por la aplicación. Cuando el SDK de X-Ray genera segmentos para las solicitudes entrantes, registra el nombre del servicio de la aplicación en el campo de nombre del segmento.

El SDK de X-Ray puede nombrar los segmentos utilizando el nombre de host en el encabezado de la solicitud HTTP. Sin embargo, este encabezado se puede falsificar, lo que podría provocar nodos inesperados en el mapa de servicio. Para evitar que el SDK nombre los segmentos de forma incorrecta debido a que las solicitudes tienen encabezados de host falsificados, debe especificar un nombre predeterminado para las solicitudes entrantes.

Si la aplicación atiende solicitudes de varios dominios, puede configurar el SDK para que utilice una estrategia de nomenclatura dinámica que refleje esto en los nombres de los segmentos. Una estrategia de nomenclatura dinámica permite al SDK usar el nombre de host para las solicitudes que coinciden con un patrón esperado y aplicar el nombre predeterminado a las solicitudes que no coincidan.

Por ejemplo, es posible que tenga una sola aplicación que atienda solicitudes a tres subdominios: `www.example.com`, `api.example.com` y `static.example.com`. Puede usar una estrategia de nomenclatura dinámica con el patrón `*.example.com` para identificar los segmentos de cada subdominio con un nombre diferente, lo que da como resultado tres nodos de servicio en el mapa de servicio. Si su aplicación recibe solicitudes con un nombre de host que no coincide con el patrón, verá un cuarto nodo en el mapa de servicio con el nombre alternativo que especifique.

Si desea utilizar el mismo nombre para todos los segmentos de solicitud, especifique el nombre de la aplicación cuando cree el controlador, tal y como se muestra en la sección anterior.

> **Note**
>
> Puede anular el nombre de servicio predeterminado que ha definido en el código mediante la `AWS_XRAY_TRACING_NAME`variable de entorno???.

Una estrategia de nomenclatura dinámica define un patrón con el que deben coincidir los nombres de host y un nombre predeterminado que se utiliza si el nombre de host de la solicitud HTTP no coincide con el patrón. Para nombrar segmentos de forma dinámica, utilice `NewDynamicSegmentNamer` para configurar el nombre predeterminado y el patrón que coincida.

Example main.go

Si el nombre de host de la solicitud coincide con el patrón `*.example.com`, utilice el nombre de host. De lo contrario, utilice `MyApp`.

```
func main() {
  http.Handle("/", xray.Handler(xray.NewDynamicSegmentNamer("MyApp", "*.example.com"),
 http.HandlerFunc(func(w http.ResponseWriter, r *http.Request) {
    w.Write([]byte("Hello!"))
  })))

  http.ListenAndServe(":8000", nil)
}
```

Rastreo de llamadas AWS del SDK con el X-Ray SDK for Go

Cuando tu aplicación realiza llamadas Servicios de AWS para almacenar datos, escribir en una cola o enviar notificaciones, el X-Ray SDK for Go rastrea las llamadas en sentido descendente en subsegmentos. El rastreo Servicios de AWS y los recursos a los que accede dentro de esos

servicios (por ejemplo, un bucket de Amazon S3 o una cola de Amazon SQS) aparecen como nodos descendentes en el mapa de rastreo de la consola X-Ray.

Para rastrear clientes del SDK de AWS, envuelva el objeto de cliente con la llamada `xray.AWS()`, tal y como se muestra en el siguiente ejemplo.

Example main.go

```
var dynamo *dynamodb.DynamoDB
func main() {
  dynamo = dynamodb.New(session.Must(session.NewSession()))
  xray.AWS(dynamo.Client)
}
```

A continuación, cuando utilice el cliente del SDK de AWS, utilice la versión `withContext` del método de llamada y transfiera el `context` desde el objeto `http.Request` transferido al handler.

Example main.go: llamada al SDK AWS

```
func listTablesWithContext(ctx context.Context) {
  output := dynamo.ListTablesWithContext(ctx, &dynamodb.ListTablesInput{})
  doSomething(output)
}
```

Para todos los servicios, puede ver el nombre de la API a la que se llama en la consola de X-Ray. Para un subconjunto de servicios, el SDK de X-Ray agrega información al segmento para proporcionar una mayor granularidad en el mapa de servicio.

Por ejemplo, cuando realiza una llamada con un cliente instrumentado de DynamoDB, el SDK agrega el nombre de tabla al segmento para las llamadas que se dirigen a una tabla. En la consola, cada tabla aparece como nodo independiente en el mapa de servicio, con un nodo genérico de DynamoDB para las llamadas que no se dirigen a una tabla.

Example Subsegmento para una llamada a DynamoDB con el fin de guardar un elemento

```
{
  "id": "24756640c0d0978a",
  "start_time": 1.480305974194E9,
  "end_time": 1.4803059742E9,
  "name": "DynamoDB",
  "namespace": "aws",
```

```
  "http": {
    "response": {
      "content_length": 60,
      "status": 200
    }
  },
  "aws": {
    "table_name": "scorekeep-user",
    "operation": "UpdateItem",
    "request_id": "UBQNSO5AEM8T4FDA4RQDEB94OVTDRVV4K4HIRGVJF66Q9ASUAAJG",
  }
}
```

Cuando accede a recursos designados, las llamadas a los siguientes servicios crean nodos adicionales en el mapa de servicio. Las llamadas que no están dirigidas a recursos concretos crean un nodo genérico en el servicio.

- Amazon DynamoDB: nombre de tabla
- Amazon Simple Storage Service: nombre de bucket y de clave
- Amazon Simple Queue Service: nombre de cola

Rastreo de llamadas a servicios web HTTP posteriores con el SDK de X-Ray para Go

Cuando la aplicación realiza llamadas a las API de HTTP público o microservicios, puede utilizar el `xray.Client` para instrumentar dichas llamadas como subsegmentos de su aplicación Go, tal y como se muestra en el siguiente ejemplo, donde http-client es un cliente HTTP.

El cliente crea una copia superficial del cliente HTTP proporcionado, tomando como valor predeterminado `http.DefaultClient`, con roundtripper envuelto con `xray.RoundTripper`.

Example

<caption>main.go: cliente HTTP</caption>

```
myClient := xray.Client(http-client)
```

<caption>main.go: rastreo de una llamada HTTP posterior con la biblioteca ctxhttp</caption>

En el siguiente ejemplo se instrumenta la llamada HTTP saliente con la biblioteca ctxhttp mediante `xray.Client`. `ctx` se puede transferir desde la llamada precedente. Eso garantiza que se utilice el

contexto de segmento existente. Por ejemplo, X-Ray no permite crear un nuevo segmento dentro de una función de Lambda, por lo que se debe utilizar el contexto de segmento de Lambda existente.

```
resp, err := ctxhttp.Get(ctx, xray.Client(nil), url)
```

Rastreo de consultas SQL con el SDK de X-Ray para Go

Para rastrear llamadas de SQL a PostgreSQL o MySQL, sustituyendo llamadas de `sql.Open` a `xray.SQLContext`, tal y como se muestra en el siguiente ejemplo. Utilice URL en lugar de cadenas de configuración si es posible.

Example main.go

```
func main() {
  db, err := xray.SQLContext("postgres", "postgres://user:password@host:port/db")
  row, err := db.QueryRowContext(ctx, "SELECT 1") // Use as normal
}
```

Generación de subsegmentos personalizados con el SDK de X-Ray para Go

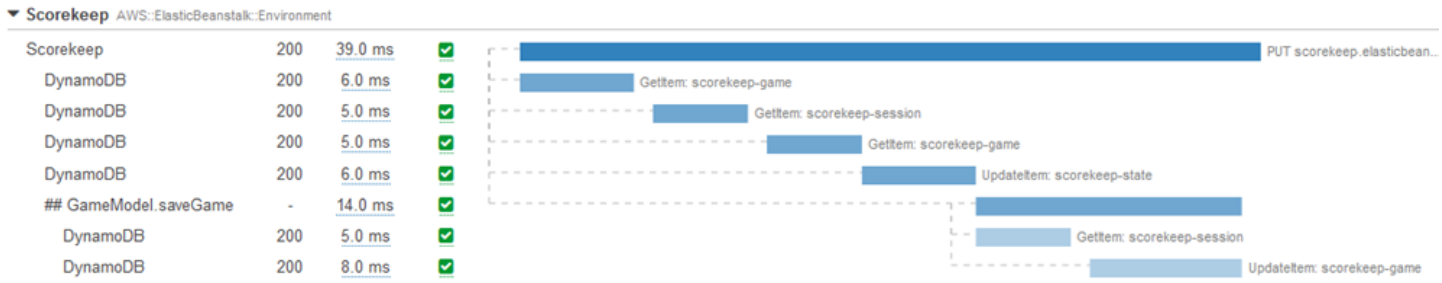
Los subsegmentos amplían el segmento de un rastro con detalles sobre el trabajo realizado para atender una solicitud. Cada vez que usted realiza una llamada con un cliente instrumentado, el SDK de X-Ray registra la información generada en un subsegmento. Puede crear subsegmentos adicionales para agrupar otros subsegmentos, medir el rendimiento de una sección de código o registrar anotaciones y metadatos.

Utilice el método `Capture` para crear un subsegmento en torno a una función.

Example main.go: subsegmento personalizado

```
func criticalSection(ctx context.Context) {
  //this is an example of a subsegment
  xray.Capture(ctx, "GameModel.saveGame", func(ctx1 context.Context) error {
    var err error

    section.Lock()
    result := someLockedResource.Go()
    section.Unlock()

    xray.AddMetadata(ctx1, "ResourceResult", result)
  })
```

En la siguiente captura de pantalla se muestra un ejemplo de cómo podría aparecer el subsegmento `saveGame` en rastreos para la aplicación `Scorekeep`.



Adición de anotaciones y metadatos a los segmentos con el SDK de X-Ray para Go

Puede usar anotaciones y metadatos para registrar información adicional sobre las solicitudes, el entorno o la aplicación. Puede añadir anotaciones y metadatos a los segmentos que crea el SDK de X-Ray o a los subsegmentos personalizados que cree usted mismo.

Las anotaciones son pares de clave-valor con valores de cadena, numéricos o booleanos. Las anotaciones se indexan para su uso con expresiones de filtro. Utilice anotaciones para registrar los datos que desee utilizar para agrupar rastros en la consola o cuando llame a la API de `GetTraceSummaries`.

Los metadatos son pares de clave-valor con valores de cualquier tipo, por ejemplo objetos y listas, pero que no se indexan para utilizarlos con expresiones de filtro. Utilice los metadatos para registrar datos adicionales que desee almacenar en el rastro, pero que no necesite usar para hacer búsquedas.

Además de anotaciones y metadatos, también puede registrar cadenas de ID de usuario en los segmentos. Los identificadores de usuario se registran en un campo aparte en segmentos y se indexan para su uso con la búsqueda.

Secciones

- Registro de anotaciones con el SDK de X-Ray para Go
- Registro de metadatos con el SDK de X-Ray para Go
- Registro de ID de usuario con el SDK de X-Ray para Go

Registro de anotaciones con el SDK de X-Ray para Go

Utilice anotaciones para registrar información sobre segmentos que desee indexar para las búsquedas.

Requisitos de anotación

- Teclas: la clave de una anotación de X-Ray puede tener hasta 500 caracteres alfanuméricos. No puede utilizar espacios ni símbolos distintos del símbolo de subrayado (_).
- Valores: el valor de una anotación de X-Ray puede tener hasta 1000 caracteres Unicode.
- Número de anotaciones: puede utilizar hasta 50 anotaciones por traza.

Para grabar anotaciones, llame a `AddAnnotation` con una cadena que contenga los metadatos que desea asociar con el segmento.

```
xray.AddAnnotation(key string, value interface{})
```

El SDK registra las anotaciones como pares de clave-valor en un objeto `annotations` del documento de segmento. Si llama dos veces a `AddAnnotation` con la misma clave, se sobrescriben los valores previamente registrados en el mismo segmento.

Para encontrar rastros que tengan anotaciones con valores específicos, utilice la palabra clave `annotations.key` en una expresión de filtro.

Registro de metadatos con el SDK de X-Ray para Go

Utilice los metadatos para registrar información sobre segmentos que no necesite indexar para las búsquedas.

Para registrar metadatos, llame a `AddMetadata` con una cadena que contenga los metadatos que desea asociar con el segmento.

```
xray.AddMetadata(key string, value interface{})
```

Registro de ID de usuario con el SDK de X-Ray para Go

Registre identificadores de usuario en segmentos de solicitud para identificar al usuario que envió la solicitud.

Para registrar identificadores de usuario

1. Obtenga una referencia al segmento actual desde `AWSXRay`.

```
import (
```

```
  "context"
  "github.com/aws/aws-xray-sdk-go/xray"
)

mySegment := xray.GetSegment(context)
```

2. Llame a `setUser` con un ID de cadena del usuario que envió la solicitud.

```
mySegment.User = "U12345"
```

Para buscar rastros de un ID de usuario, utilice la palabra clave `user` en una expresión de filtro.

Instrumentación de su aplicación con Java

Hay dos formas de instrumentar su Java aplicación para enviar trazas a X-Ray:

- AWS Distro for OpenTelemetry Java: una AWS distribución que proporciona un conjunto de bibliotecas de código abierto para enviar métricas y rastreos correlacionados a varias soluciones de AWS monitoreo, incluidas Amazon y Amazon OpenSearch Service CloudWatch AWS X-Ray, a través de AWS Distro for Collector. OpenTelemetry
- AWS X-Ray SDK para Java: conjunto de bibliotecas para generar y enviar trazas a X-Ray mediante el daemon X-Ray.

Para obtener más información, consulte Cómo elegir entre los AWS SDK Distro for OpenTelemetry y X-Ray.

AWS Distro para OpenTelemetry Java

Con AWS Distro para OpenTelemetry (ADOT) Java, puede instrumentar sus aplicaciones una vez y enviar métricas y rastros correlacionados a varias soluciones de supervisión de AWS, incluidas Amazon CloudWatch, AWS X-Ray y Amazon OpenSearch Service. El uso de X-Ray con ADOT requiere dos componentes: un SDK de OpenTelemetry habilitado para su uso con X-Ray y AWS Distro para OpenTelemetry Collector habilitado para su uso con X-Ray. ADOT Java admite la instrumentación automática, lo que permite a la aplicación del usuario enviar rastros sin cambios de código.

Para empezar, consulte la documentación de AWS Distro para OpenTelemetry Java.

Para obtener más información sobre el uso de AWS Distro para OpenTelemetry con AWS X-Ray y otros Servicios de AWS, consulte AWS Distro para OpenTelemetry o la documentación de AWS Distro para OpenTelemetry.

Para obtener información adicional sobre los lenguajes compatibles y el uso, consulte AWS Observability en GitHub.

AWS X-Ray SDK para Java

El X-Ray SDK para Java es un conjunto de bibliotecas para aplicaciones Java web que proporcionan clases y métodos para generar y enviar datos de rastreo al daemon X-Ray. Los datos de rastreo incluyen información sobre las solicitudes HTTP entrantes atendidas por la aplicación y las llamadas que la aplicación realiza a los servicios descendentes mediante el AWS SDK, los clientes HTTP o un conector de base de datos SQL. También puede crear segmentos de forma manual y agregar información de depuración en anotaciones y metadatos.

El SDK de X-Ray para Java es un proyecto de código abierto. Puedes seguir el proyecto y enviar las incidencias y solicitudes de cambios en GitHub: github.com/aws/ aws-xray-sdk-java

Comience añadiendo `AWSXRayServletFilter` como filtro de servlet para rastrear las solicitudes entrantes. Los filtros de servlets crean un segmento. Mientras el segmento está abierto, puede utilizar los métodos del cliente del SDK para añadir información al segmento y crear subsegmentos para rastrear llamadas posteriores. El SDK también registra automáticamente las excepciones que produce su aplicación mientras el segmento está abierto.

A partir de la versión 1.3, puede instrumentar una aplicación mediante la programación orientada a aspectos (AOP) de Spring. Esto significa que puedes instrumentar tu aplicación mientras está en ejecución AWS, sin añadir ningún código al tiempo de ejecución de la aplicación.

A continuación, utilice el SDK de X-Ray para Java para instrumentar a sus AWS SDK for Java clientes mediante la inclusión del submódulo SDK Instrumentor en la configuración de compilación. Cada vez que realizas una llamada a un recurso Servicio de AWS o a un servicio intermedio con un cliente instrumentado, el SDK registra la información sobre la llamada en un subsegmento. Servicios de AWS y los recursos a los que accedes desde los servicios aparecen como nodos descendentes en el mapa de rastreo para ayudarte a identificar los errores y los problemas de limitación en las conexiones individuales.

Si no quieres instrumentar todas las llamadas posteriores Servicios de AWS, puedes omitir el submódulo Instrumentor y elegir los clientes a los que quieres instrumentar. Instrumente a los clientes individuales añadiendo un `TracingHandler` a un cliente de servicio AWS del SDK.

Otros submódulos del SDK de X-Ray para Java proporcionan instrumentación para las llamadas posteriores a API de web HTTP y a bases de datos SQL. Puede utilizar las versiones de `HTTPClient` y `HTTPClientBuilder` del SDK de X-Ray para Java en el submódulo Apache HTTP para instrumentar clientes Apache HTTP. Para instrumentar consultas SQL, añada el interceptor del SDK al origen de datos.

En cuanto empiece a utilizar el SDK, personalice su comportamiento configurando la grabadora y el filtro de servlet. Puede añadir complementos para registrar los datos sobre los recursos informáticos que ejecutan su aplicación, personalizar el comportamiento de muestreo mediante la definición de reglas de muestreo y definir el nivel de log para ver más o menos información del SDK en los logs de las aplicaciones.

Registre información adicional acerca de las solicitudes y el trabajo que la aplicación realiza en anotaciones y metadatos. Las anotaciones son pares sencillos de clave-valor que se indexan para su uso con expresiones de filtro para poder buscar rastros que contengan datos específicos. Las entradas de metadatos son menos restrictivas y pueden registrar objetos y matrices completos, es decir, todo lo que se pueda serializar en JSON.

> **Anotaciones y metadatos**
>
> Las anotaciones y los metadatos son texto arbitrario que se agrega a los segmentos con el SDK de X-Ray. Las anotaciones se indexan para su uso con expresiones de filtro. Los metadatos no se indexan pero se pueden ver en el segmento sin procesar con la consola o la API de X-Ray. Cualquier persona a la que conceda acceso de lectura a X-Ray puede ver estos datos.

Si tiene un gran número de clientes instrumentados en su código, un único segmento de solicitud puede contener muchos subsegmentos, uno por cada llamada realizada con un cliente instrumentado. Puede organizar y agrupar los subsegmentos incluyendo las llamadas del cliente en subsegmentos personalizados. Puede crear un subsegmento personalizado para una función completa o para cualquier sección de código, y registrar los metadatos y las anotaciones en el subsegmento en lugar de escribirlo todo en el segmento principal.

Submódulos

Puede descargar el SDK de X-Ray para Java desde Maven. El SDK de X-Ray para Java está dividido en submódulos por caso de uso, con una factura de materiales para la administración de las versiones:

- `aws-xray-recorder-sdk-core` (obligatorio): funcionalidad básica para la creación y transmisión de segmentos. Incluye `AWSXRayServletFilter` para instrumentar solicitudes entrantes.
- `aws-xray-recorder-sdk-aws-sdk`— Instrumenta las llamadas que Servicios de AWS se realizan con AWS SDK for Java los clientes añadiendo un cliente de rastreo como gestor de solicitudes.
- `aws-xray-recorder-sdk-aws-sdk-v2`— Las llamadas de Instruments Servicios de AWS se realizan con clientes de la versión AWS SDK for Java 2.2 y versiones posteriores añadiendo un cliente de rastreo como interceptor de solicitudes.
- `aws-xray-recorder-sdk-aws-sdk-instrumentor`— Con, instrumenta a `aws-xray-recorder-sdk-aws-sdk` todos los clientes automáticamente. AWS SDK for Java
- `aws-xray-recorder-sdk-aws-sdk-v2-instrumentor`— Con`aws-xray-recorder-sdk-aws-sdk-v2`, instrumenta todos los clientes de AWS SDK for Java 2.2 y posteriores de forma automática.
- `aws-xray-recorder-sdk-apache-http`: instrumenta llamadas HTTP salientes realizadas con clientes Apache HTTP.
- `aws-xray-recorder-sdk-spring`: proporciona interceptores para las aplicaciones del marco de trabajo Spring AOP.
- `aws-xray-recorder-sdk-sql-postgres`: instrumenta llamadas salientes a la base de datos PostgreSQL realizadas con JDBC.
- `aws-xray-recorder-sdk-sql-mysql`: instrumenta llamadas salientes a la base de datos MySQL realizadas con JDBC.
- `aws-xray-recorder-sdk-bom`: proporciona una lista de materiales que puede utilizar para especificar la versión que se debe utilizar en todos los submódulos.
- `aws-xray-recorder-sdk-metrics`— Publica CloudWatch métricas de Amazon sin muestrear de tus segmentos de X-Ray recopilados.

Si utiliza Maven o Gradle para crear la aplicación, añada el SDK de X-Ray para Java a la configuración de compilación.

Para obtener documentación de referencia sobre las clases y los métodos del SDK, consulta el AWS X-Ray SDK como referencia sobre las Java API.

Requisitos

El X-Ray SDK for Java requiere Java 8 o una versión posterior, Servlet API 3, el AWS SDK y Jackson.

El SDK depende de las siguientes bibliotecas durante la compilación y el tiempo de ejecución:

- AWS SDK para la Java versión 1.11.398 o posterior
- Servlet API 3.1.0

Estas dependencias se declaran en el archivo `pom.xml` del SDK y se incluyen de forma automática si realiza la compilación con Maven o Gradle.

Si utiliza una biblioteca que se incluye en el SDK de X-Ray para Java debe utilizar la versión que se incluye. Por ejemplo, si ya depende de Jackson durante el tiempo de ejecución e incluye archivos JAR en la implementación de esa dependencia, debe eliminar dichos archivos porque el archivo JAR del SDK incluye sus propias versiones de las bibliotecas Jackson.

Administración de dependencias

El SDK de X-Ray para Java está disponible en Maven:

- Grupo: `com.amazonaws`
- Artefacto: `aws-xray-recorder-sdk-bom`
- Versión: `2.11.0`

Si utiliza Maven para compilar la aplicación, añada el SDK como dependencia en su archivo `pom.xml`.

Example pom.xml: dependencias

```
<dependencyManagement>
  <dependencies>
    <dependency>
      <groupId>com.amazonaws</groupId>
      <artifactId>aws-xray-recorder-sdk-bom</artifactId>
      <version>2.11.0</version>
      <type>pom</type>
      <scope>import</scope>
```

```
    </dependency>
  </dependencies>
</dependencyManagement>
<dependencies>
  <dependency>
    <groupId>com.amazonaws</groupId>
    <artifactId>aws-xray-recorder-sdk-core</artifactId>
  </dependency>
  <dependency>
    <groupId>com.amazonaws</groupId>
    <artifactId>aws-xray-recorder-sdk-apache-http</artifactId>
  </dependency>
  <dependency>
    <groupId>com.amazonaws</groupId>
    <artifactId>aws-xray-recorder-sdk-aws-sdk</artifactId>
  </dependency>
  <dependency>
    <groupId>com.amazonaws</groupId>
    <artifactId>aws-xray-recorder-sdk-aws-sdk-instrumentor</artifactId>
  </dependency>
  <dependency>
    <groupId>com.amazonaws</groupId>
    <artifactId>aws-xray-recorder-sdk-sql-postgres</artifactId>
  </dependency>
  <dependency>
    <groupId>com.amazonaws</groupId>
    <artifactId>aws-xray-recorder-sdk-sql-mysql</artifactId>
  </dependency>
</dependencies>
```

Si utiliza Gradle, añada el SDK como dependencia de tiempo de compilación en su archivo `build.gradle`.

Example build.gradle: dependencias

```
dependencies {
  compile("org.springframework.boot:spring-boot-starter-web")
  testCompile("org.springframework.boot:spring-boot-starter-test")
  compile("com.amazonaws:aws-java-sdk-dynamodb")
  compile("com.amazonaws:aws-xray-recorder-sdk-core")
  compile("com.amazonaws:aws-xray-recorder-sdk-aws-sdk")
  compile("com.amazonaws:aws-xray-recorder-sdk-aws-sdk-instrumentor")
  compile("com.amazonaws:aws-xray-recorder-sdk-apache-http")
```

```
  compile("com.amazonaws:aws-xray-recorder-sdk-sql-postgres")
  compile("com.amazonaws:aws-xray-recorder-sdk-sql-mysql")
  testCompile("junit:junit:4.11")
}
dependencyManagement {
    imports {
        mavenBom('com.amazonaws:aws-java-sdk-bom:1.11.39')
        mavenBom('com.amazonaws:aws-xray-recorder-sdk-bom:2.11.0')
    }
}
```

Si utiliza Elastic Beanstalk para implementar la aplicación, puede utilizar Maven o Gradle para compilar la aplicación en la instancia cada vez que realice la implementación, en lugar de compilar y cargar un archivo de gran tamaño que incluya todas sus dependencias. Consulte la aplicación de ejemplo para ver un ejemplo en el que se utiliza Gradle.

Agente de instrumentación automática de AWS X-Ray para Java

El agente de instrumentación automática de AWS X-Ray para Java es una solución de rastreo que instrumenta sus aplicaciones web Java con un mínimo esfuerzo de desarrollo. El agente permite rastrear las aplicaciones basadas en servlets y todas las solicitudes posteriores del agente realizadas con marcos y bibliotecas compatibles. Entre ellas se incluyen las solicitudes HTTP a Apache, solicitudes mediante el SDK de AWS y consultas en SQL posteriores realizadas con un controlador JDBC. El agente propaga el contexto de X-Ray, incluidos todos los segmentos y subsegmentos activos, a través de subprocesos. Todas las configuraciones y la versatilidad del SDK de X-Ray siguen disponibles con el agente para Java. Se eligieron los valores predeterminados adecuados para garantizar que el agente funcione con el mínimo esfuerzo.

Lo más adecuado para la solución del agente de X-Ray son los servidores de aplicaciones web Java de solicitud-respuesta basados en servlets. Si su aplicación utiliza un marco asíncrono o no está bien diseñada como servicio de solicitud-respuesta, la instrumentación manual con el SDK podría ser más conveniente.

Para crear el agente de X-Ray se ha utilizado el kit de herramientas Distributed Systems Comprehension o DiSCo. DisCo es un marco de código abierto para crear agentes de Java que se puede usar en sistemas distribuidos. Si bien no es necesario entender DisCO para usar el agente de X-Ray, puede obtener más información sobre el proyecto consultando su página de inicio en GitHub. El agente de X-Ray también es de código totalmente abierto. Para ver el código fuente, hacer contribuciones o indicar problemas relacionados con el agente, consulte su repositorio en GitHub.

Aplicación de muestra

La aplicación de muestra eb-java-scorekeep está adaptada para ser instrumentada con el agente de X-Ray. Esta ramificación no contiene ningún filtro de servlet ni configuración de grabadora, ya que estas funciones las realiza el agente. Para ejecutar la aplicación de forma local o utilizando recursos de AWS, siga los pasos indicados en el archivo readme de la aplicación de muestra. Las instrucciones para usar la aplicación de muestra con el fin de generar rastros de X-Ray se encuentran en el tutorial de la aplicación de muestra.

Introducción

Para empezar a utilizar el agente de instrumentación automática de X-Ray para Java en su propia aplicación, siga estos pasos.

1. Ejecute el daemon de X-Ray en su entorno. Para obtener más información, consulte Daemon de X-Ray.
2. Descargue la última distribución del agente. Descomprima el archivo y tome nota de su ubicación en el sistema de archivos. El contenido debe ser similar al siguiente.

   ```
   disco
   ### disco-java-agent.jar
   ### disco-plugins
       ### aws-xray-agent-plugin.jar
       ### disco-java-agent-aws-plugin.jar
       ### disco-java-agent-sql-plugin.jar
       ### disco-java-agent-web-plugin.jar
   ```

3. Modifique los argumentos de JVM de su aplicación para incluir lo siguiente y así habilitar el agente. Asegúrese de que el argumento `-javaagent` esté colocado delante del argumento `-jar`, si procede. El proceso de modificación de los argumentos de JVM varía en función de las herramientas y los marcos que utilice para lanzar su servidor de Java. Consulte la documentación del marco de su servidor para obtener orientación específica.

   ```
   -javaagent:/<path-to-disco>/disco-java-agent.jar=pluginPath=/<path-to-disco>/disco-plugins
   ```

4. Para especificar cómo aparece el nombre de la aplicación en la consola de X-Ray, establezca la variable de entorno `AWS_XRAY_TRACING_NAME` o la propiedad de sistema `com.amazonaws.xray.strategy.tracingName`. Si no se proporciona un nombre, se utilizará un nombre predeterminado.

5. Reinicie el servidor o el contenedor. A partir de ese momento se rastrearán las solicitudes entrantes y sus llamadas posteriores. Si no ve los resultados esperados, consulte the section called “Solución de problemas”.

Configuración

El agente de X-Ray se configura mediante un archivo JSON externo proporcionado por el usuario. De forma predeterminada, este archivo se encuentra en la raíz de la ruta de clases del usuario denominada `xray-agent.json` (por ejemplo, en su directorio `resources`). Puede configurar una ubicación personalizada para el archivo de configuración estableciendo la propiedad de sistema `com.amazonaws.xray.configFile` en la ruta absoluta del sistema de archivos del archivo de configuración.

A continuación, se muestra un ejemplo de archivo de configuración.

```
{
    "serviceName": "XRayInstrumentedService",
    "contextMissingStrategy": "LOG_ERROR",
    "daemonAddress": "127.0.0.1:2000",
    "tracingEnabled": true,
    "samplingStrategy": "CENTRAL",
    "traceIdInjectionPrefix": "prefix",
    "samplingRulesManifest": "/path/to/manifest",
    "awsServiceHandlerManifest": "/path/to/manifest",
    "awsSdkVersion": 2,
    "maxStackTraceLength": 50,
    "streamingThreshold": 100,
    "traceIdInjection": true,
    "pluginsEnabled": true,
    "collectSqlQueries": false
}
```

Especificación de la configuración

En la tabla siguiente se describen valores válidos para cada propiedad. Los nombres de las propiedades hay distinción entre mayúsculas y minúsculas, pero en sus claves no. En el caso de propiedades que las variables de entorno y las propiedades del sistema pueden anular, el orden de prioridad es siempre el siguiente: primero la variable de entorno, luego la propiedad del sistema y, por último, el archivo de configuración. Consulte Variables de entorno para obtener información sobre las propiedades que puede anular. Todos los campos son opcionales.

Nombre de la propiedad	Tipo	Valores válidos	Descripción	Variable de entorno	Propiedad del sistema	Valor predeterminado
serviceName	Cadena	Cualquier cadena	El nombre del servicio instrumentado tal como aparecerá en la consola de X-Ray.	AWS_XRAY_TRACING_NAME	com.amazonaws.xray.strategy.tracingName	XRayInstrumentedService
contextMissingStrategy	Cadena	LOG_ERROR, IGNORE_ERROR	La acción que realiza el agente cuando intenta utilizar el contexto del segmento de X-Ray, pero no hay ninguno.	AWS_XRAY_CONTEXT_MISSING	com.amazonaws.xray.strategy.contextMissingStrategy	LOG_ERROR
daemonAddress	Cadena	Dirección IP y puerto formateados o lista de direcciones TCP y UDP	La dirección que utiliza el agente para comunicarse con el	AWS_XRAY_DAEMON_ADDRESS	com.amazonaws.xray.emitter.daemonAddress	127.0.0.1:2000

Nombre de la propiedad	Tipo	Valores válidos	Descripción	Variable de entorno	Propiedad del sistema	Valor predeterminado
			daemon de X-Ray.			
tracingEnabled	Booleano	True, False	Permite la instrumentación mediante el agente de X-Ray.	AWS_XRAY_TRACING_ENABLED	com.amazonaws.xray.tracingEnabled	TRUE
samplingStrategy	Cadena	CENTRAL, LOCAL, NONE o ALL	La estrategia de muestreo que utiliza el agente. ALL captura todas las solicitudes, NONE no captura ninguna. Consulte Reglas de muestreo.	N/A	N/A	CENTRAL

Nombre de la propiedad	Tipo	Valores válidos	Descripción	Variable de entorno	Propiedad del sistema	Valor predeterminado
traceIdInjectionPrefix	Cadena	Cualquier cadena	Incluye el prefijo proporcionado antes de los ID de rastro inyectados en los registros.	N/A	N/A	Ninguno (cadena vacía)

Nombre de la propiedad	Tipo	Valores válidos	Descripción	Variable de entorno	Propiedad del sistema	Valor predeterminado
samplingRulesManifest	Cadena	Ruta de archivo absoluta	La ruta a un archivo de reglas de muestreo personalizadas que se utilizará como fuente de las reglas de muestreo para la estrategia de muestreo local o las reglas alternativas para la estrategia central.	N/A	N/A	DefaultSamplingRules.json

Nombre de la propiedad	Tipo	Valores válidos	Descripción	Variable de entorno	Propiedad del sistema	Valor predeterminado
awsServiceHandlerManifest	Cadena	Ruta de archivo absoluta	La ruta a una lista de parámetros permitidos personalizados que captura información adicional de los clientes del SDK de AWS.	N/A	N/A	DefaultOperationParameterWhitelist.json
awsSdkVersion	Entero	1, 2	Versión del SDK de AWS para Java que está utilizando. Se ignora si no se establece también `awsServiceHandlerManifest`.	N/A	N/A	2

Nombre de la propiedad	Tipo	Valores válidos	Descripción	Variable de entorno	Propiedad del sistema	Valor predeterminado
maxStackTraceLength	Entero	Enteros no negativos	El número máximo de líneas de un rastro de pila que se pueden registrar en una traza.	N/A	N/A	50
streamingThreshold	Entero	Enteros no negativos	Una vez cerrados al menos este número de subsegmentos, se transmiten al daemon fuera de banda para evitar que los fragmentos sean demasiado grandes.	N/A	N/A	100

Nombre de la propiedad	Tipo	Valores válidos	Descripción	Variable de entorno	Propiedad del sistema	Valor predeterminado
traceIdInjection	Booleano	True, False	Permite la inyección de los ID de rastro de X-Ray en los registros si también se agregan las dependencias y la configuración descritas en la configuración de registro. De lo contrario, no hace nada.	N/A	N/A	TRUE

Nombre de la propiedad	Tipo	Valores válidos	Descripción	Variable de entorno	Propiedad del sistema	Valor predeterminado
pluginsEnabled	Booleano	True, False	Habilita los complementos que registran metadatos sobre los entornos de AWS en los que está operando. Consulte Complementos de servicio.	N/A	N/A	TRUE
collectSqlQueries	Booleano	True, False	Registra cadenas de consultas SQL en subsegmentos SQL en la medida de lo posible.	N/A	N/A	FALSE

Nombre de la propiedad	Tipo	Valores válidos	Descripción	Variable de entorno	Propiedad del sistema	Valor predeterminado
contextPropagation	Booleano	True, False	Propaga automáticamente el contexto de X-Ray entre subprocesos si es verdadero. De lo contrario, utiliza Thread Local para almacenar el contexto y se requiere la propagación manual de un subproceso a otro.	N/A	N/A	TRUE

Configuración de registro

El nivel de registro del agente de X-Ray se puede configurar de la misma manera que el SDK de X-Ray para Java. Consulte Registro para obtener más información sobre la configuración del registro con el SDK de X-Ray para Java.

Instrumentación manual

Si desea realizar la instrumentación manual además de la instrumentación automática del agente, añada el SDK de X-Ray como una dependencia a su proyecto. Tenga en cuenta que los filtros de servlets personalizados del SDK que se mencionan en Rastreo de solicitudes entrantes no son compatibles con el agente de X-Ray.

> **Note**
>
> Debe usar la última versión del SDK de X-Ray para realizar la instrumentación manual y usar el agente al mismo tiempo.

Si está trabajando en un proyecto de Maven, añada las siguientes dependencias a su archivo `pom.xml`.

```
<dependencies>
  <dependency>
    <groupId>com.amazonaws</groupId>
    <artifactId>aws-xray-recorder-sdk-core</artifactId>
    <version>2.11.0</version>
  </dependency>
  </dependencies>
```

Si está trabajando en un proyecto de Gradle, añada las siguientes dependencias a su archivo `build.gradle`.

```
implementation 'com.amazonaws:aws-xray-recorder-sdk-core:2.11.0'
```

Puede agregar subsegmentos personalizados además de anotaciones, metadatos e identificadores de usuariomientras usas el agente, tal como lo haría con el SDK normal. El agente propaga automáticamente el contexto de un subproceso a otro, por lo que no deberían hacer falta soluciones provisionales para propagar el contexto cuando se trabaja con aplicaciones multiproceso.

Solución de problemas

Como el agente ofrece una instrumentación totalmente automática, puede resultar difícil identificar la causa raíz de un problema cuando se están produciendo problemas. Si el agente de X-Ray no funciona según lo esperado, revise los siguientes problemas y soluciones. El agente y el SDK de

X-Ray utilizan Jakarta Commons Logging (JCL). Para ver el resultado del registro, asegúrese de que un puente que conecte JCL con su backend de registro esté en la ruta de clases, como en el siguiente ejemplo: `log4j-jcl` o `jcl-over-slf4j`.

Problema: he habilitado el agente para Java en mi aplicación, pero no veo nada en la consola de X-Ray

¿El daemon de X-Ray se está ejecutando en la misma máquina?

Si no es así, consulte la documentación del daemon de X-Ray para configurarlo.

¿Ve un mensaje similar a "Initializing the X-Ray agent recorder" en los registros de su aplicación?

Si ha agregado correctamente el agente a la aplicación, este mensaje estará registrado en el nivel INFO cuando se inicie la aplicación, antes de que esta comience a recibir solicitudes. Si este mensaje no aparece, significa que el agente para Java no se está ejecutando con el proceso de Java. Asegúrese de haber seguido todos los pasos de configuración correctamente sin errores tipográficos.

¿Ve varios mensajes de error que digan algo así como "Suppressing AWS X-Ray context missing exception" en los registros de su aplicación?

Estos errores se producen porque el agente está intentando instrumentar las solicitudes posteriores, como las solicitudes del SDK de AWS o las consultas en SQL, pero no ha podido crear un segmento automáticamente. Si ve muchos de estos errores, es posible que el agente no sea la mejor herramienta para el uso que usted le quiere dar y, en su lugar, tal vez debería considerar la instrumentación manual con el SDK de X-Ray. Como alternativa, puedes habilitar los registros de depuración del SDK de X-Ray para ver el rastro de pila del punto donde se producen las excepciones de falta de contexto. Puede agrupar estas porciones del código con segmentos personalizados, lo que debería corregir estos errores. Para ver un ejemplo de cómo encapsular las solicitudes posteriores con segmentos personalizados, consulte el código de muestra que aparece en Instrumentación de código de inicio.

Problema: algunos de los segmentos que espero no aparecen en la consola de X-Ray

¿Su aplicación utiliza el multiproceso?

Si espera que se creen ciertos segmentos pero no aparecen en la consola, la causa pueden ser subprocesos en segundo plano en la aplicación. Si su aplicación realiza tareas mediante subprocesos en segundo plano que “se activan y se olvidan”, como realizar una llamada puntual

a una función de Lambda con el SDK de AWS o sondear periódicamente algún punto de conexión HTTP, podría confundir al agente mientras propaga el contexto de un subproceso a otro. Para comprobar que este es su problema, habilite los registros de depuración del SDK de X-Ray y mire a ver si hay mensajes como este: Not emitting segment named **<**NOMBRE **>** as it parents in-progress subsegments. Para solucionar este problema, puede intentar unir los subprocesos en segundo plano antes de que el servidor vuelva a funcionar para asegurarse de que todo el trabajo realizado en ellos queda registrado. O bien, puede establecer la configuración `contextPropagation` del agente en `false` para inhabilitar la propagación del contexto en subprocesos en segundo plano. En ese caso, tendrá que instrumentar manualmente esos subprocesos con segmentos personalizados o ignorar las excepciones de falta de contexto que generen.

¿Ha establecido reglas de muestreo?

Si aparecen segmentos aparentemente aleatorios o inesperados en la consola de X-Ray, o los segmentos que esperaba que estuvieran en la consola no están, es posible que tenga un problema de muestreo. El agente de X-Ray lleva a cabo un muestreo centralizado en todos los segmentos que crea, aplicando las reglas de la consola de X-Ray. La regla por defecto es obtener muestras en 1 segmento por segundo y, posteriormente, en el 5 % de los segmentos. Eso significa que es posible que no se obtengan muestras de los segmentos que se creen rápidamente con el agente. Para solucionar este problema, debe crear reglas de muestreo personalizadas en la consola de X-Ray para un muestreo adecuado de los segmentos deseados. Para obtener más información, consulte Configuración de reglas de muestreo.

Configuración del SDK de X-Ray para Java

El SDK de X-Ray para Java incluye una clase denominada `AWSXRay` que proporciona la grabadora global. Esto es un `TracingHandler` que puede utilizar para instrumentar su código. Puede configurar la grabadora global para que personalice el `AWSXRayServletFilter` que crea los segmentos para las llamadas HTTP entrantes.

Secciones

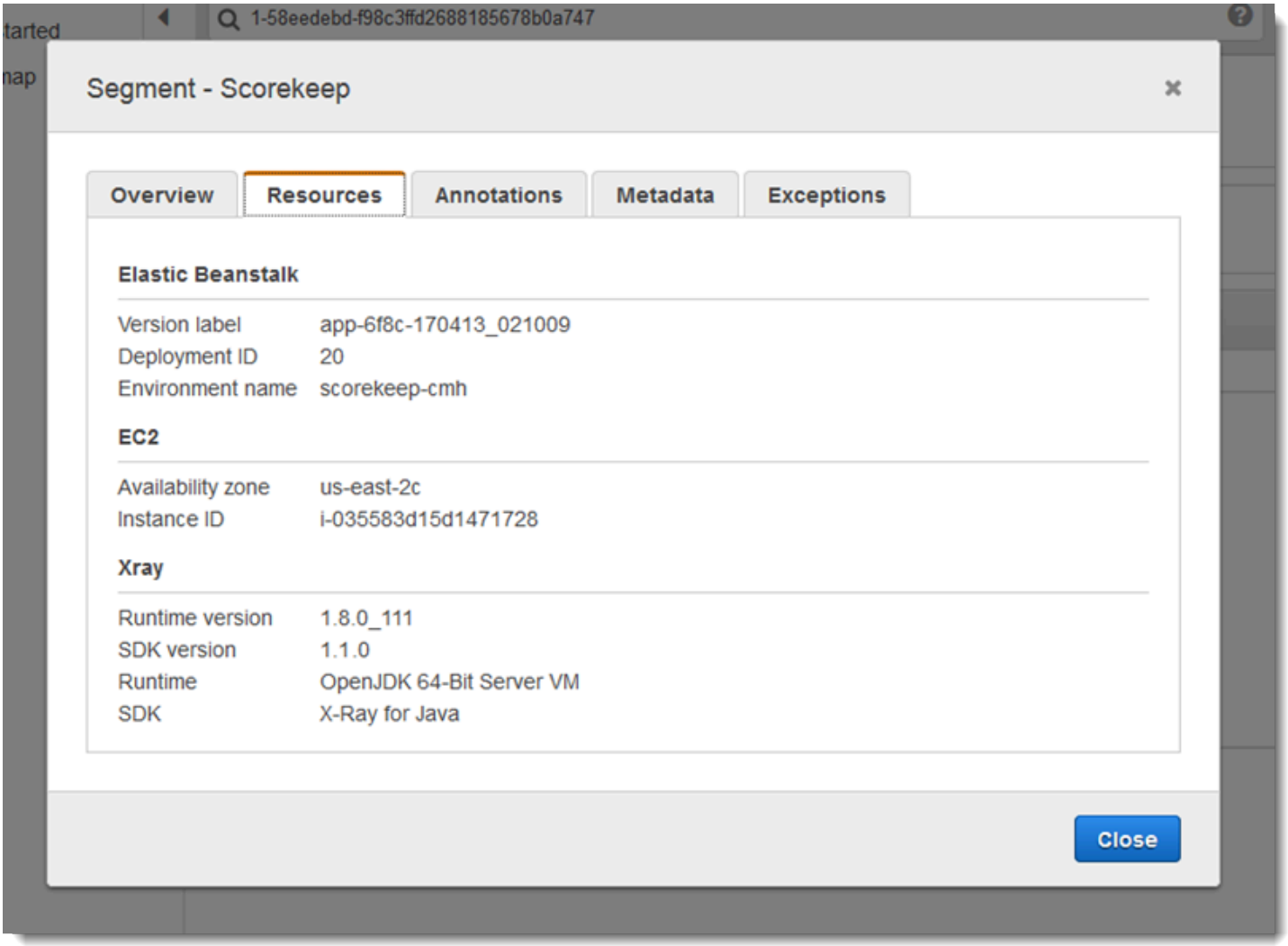
- Complementos del servicio
- Reglas de muestreo
- Registro
- Agentes de escucha de segmento
- Variables de entorno
- Propiedades del sistema

Complementos del servicio

Utilice `plugins` para registrar información sobre el servicio que aloja la aplicación.

Complementos

- Amazon EC2: `EC2Plugin` agrega el ID de la instancia, la zona de disponibilidad y el grupo de CloudWatch registros.
- Elastic Beanstalk: `ElasticBeanstalkPlugin` añade el nombre de entorno, la etiqueta de versión y el ID de implementación.
- Amazon ECS: `ECSPlugin` agrega el ID de contenedor.
- Amazon EKS: `EKSPlugin` añade el ID del contenedor, el nombre del clúster, el ID del pod y el grupo de CloudWatch registros.



Para utilizar un complemento, llame a `withPlugin` en su `AWSXRayRecorderBuilder`.

Example src/main/java/scorekeep/ .java: WebConfig grabadora

```
import com.amazonaws.xray.AWSXRay;
import com.amazonaws.xray.AWSXRayRecorderBuilder;
import com.amazonaws.xray.plugins.EC2Plugin;
import com.amazonaws.xray.plugins.ElasticBeanstalkPlugin;
import com.amazonaws.xray.strategy.sampling.LocalizedSamplingStrategy;

@Configuration
public class WebConfig {
...
  static {
    AWSXRayRecorderBuilder builder = AWSXRayRecorderBuilder.standard().withPlugin(new
 EC2Plugin()).withPlugin(new ElasticBeanstalkPlugin());

    URL ruleFile = WebConfig.class.getResource("/sampling-rules.json");
    builder.withSamplingStrategy(new LocalizedSamplingStrategy(ruleFile));

    AWSXRay.setGlobalRecorder(builder.build());
  }
}
```

El SDK también usa la configuración del complemento para establecer el campo `origin` en el segmento. Esto indica el tipo de recurso que ejecuta la aplicación. AWS Cuando utilizas varios complementos, el SDK utiliza el siguiente orden de resolución para determinar el origen: ElasticBeanstalk > EKS > ECS > EC2.

Reglas de muestreo

El SDK utiliza las reglas de muestreo que define el usuario en la consola de X-Ray para determinar qué solicitudes registrar. La regla predeterminada rastrea la primera solicitud cada segundo y el 5 % de las solicitudes adicionales de todos los servicios que envían rastros a X-Ray. Cree reglas adicionales en la consola de X-Ray para personalizar la cantidad de datos registrados para cada una de sus aplicaciones.

El SDK aplica las reglas personalizadas en el orden en que se definen. Si una solicitud coincide con varias reglas personalizadas, el SDK solo aplica la primera regla.

> **Note**
>
> Si el SDK no puede comunicarse con X-Ray para obtener las reglas de muestreo, vuelve a una regla local predeterminada de la primera solicitud cada segundo y del 5 % de las solicitudes adicionales por host. Eso puede ocurrir si el host no tiene permiso para llamar a las API de muestreo o no puede conectarse al daemon de X-Ray, que actúa como proxy TCP para las llamadas a las API realizadas por el SDK.

También puede configurar el SDK para que cargue las reglas de muestreo desde un documento JSON. El SDK puede usar las reglas locales como respaldo para los casos en que el muestreo de X-Ray no esté disponible, o puede usar las reglas locales exclusivamente.

Example sampling-rules.json

```
{
  "version": 2,
  "rules": [
    {
      "description": "Player moves.",
      "host": "*",
      "http_method": "*",
      "url_path": "/api/move/*",
      "fixed_target": 0,
      "rate": 0.05
    }
  ],
  "default": {
    "fixed_target": 1,
    "rate": 0.1
  }
}
```

En este ejemplo se define una regla personalizada y una regla predeterminada. La regla personalizada aplica un porcentaje de muestreo del 5 % sin un número mínimo de solicitudes de rastreo para las rutas incluidas bajo `/api/move/`. La regla predeterminada rastrea la primera solicitud cada segundo y el 10 % de las solicitudes adicionales.

La desventaja de definir las reglas localmente es que el objetivo establecido lo aplica cada instancia de la grabadora de forma independiente, en lugar de ser administrado por el servicio de X-Ray. A

medida que se implementan más hosts, el porcentaje establecido se multiplica, lo que dificulta el control de la cantidad de datos registrados.

Activado AWS Lambda, no se puede modificar la frecuencia de muestreo. Si un servicio instrumentado llama a su función, Lambda registrará las llamadas que generaron solicitudes muestreadas por ese servicio. Si el rastreo activo está activado y no hay ningún encabezado de rastreo, Lambda toma la decisión de muestreo.

Para proporcionar reglas de copia de seguridad en Spring, configure la grabadora global con una `CentralizedSamplingStrategy` en una clase de configuración:

Example WebConfigsrc/main/java/myapp/ .java: configuración de la grabadora

```
import com.amazonaws.xray.AWSXRay;
import com.amazonaws.xray.AWSXRayRecorderBuilder;
import com.amazonaws.xray.javax.servlet.AWSXRayServletFilter;
import com.amazonaws.xray.plugins.EC2Plugin;
import com.amazonaws.xray.strategy.sampling.LocalizedSamplingStrategy;

@Configuration
public class WebConfig {

  static {
  AWSXRayRecorderBuilder builder = AWSXRayRecorderBuilder.standard().withPlugin(new
 EC2Plugin());

  URL ruleFile = WebConfig.class.getResource("/sampling-rules.json");
  builder.withSamplingStrategy(new CentralizedSamplingStrategy(ruleFile));

  AWSXRay.setGlobalRecorder(builder.build());
}
```

Para Tomcat, añada un agente de escucha que amplíe `ServletContextListener` y registre el agente de escucha en el descriptor de la implementación.

Example src/com/myapp/web/Startup.java

```
import com.amazonaws.xray.AWSXRay;
import com.amazonaws.xray.AWSXRayRecorderBuilder;
import com.amazonaws.xray.plugins.EC2Plugin;
import com.amazonaws.xray.strategy.sampling.LocalizedSamplingStrategy;
```

```
import java.net.URL;
import javax.servlet.ServletContextEvent;
import javax.servlet.ServletContextListener;

public class Startup implements ServletContextListener {

    @Override
    public void contextInitialized(ServletContextEvent event) {
        AWSXRayRecorderBuilder builder =
 AWSXRayRecorderBuilder.standard().withPlugin(new EC2Plugin());

        URL ruleFile = Startup.class.getResource("/sampling-rules.json");
        builder.withSamplingStrategy(new CentralizedSamplingStrategy(ruleFile));

        AWSXRay.setGlobalRecorder(builder.build());
    }

    @Override
    public void contextDestroyed(ServletContextEvent event) { }
}
```

Example WEB-INF/web.xml

```
...
  <listener>
    <listener-class>com.myapp.web.Startup</listener-class>
  </listener>
```

Para utilizar reglas locales solo, reemplace la `CentralizedSamplingStrategy` por `LocalizedSamplingStrategy`.

```
builder.withSamplingStrategy(new LocalizedSamplingStrategy(ruleFile));
```

Registro

De forma predeterminada, el SDK envía mensajes de nivel de `ERROR` a los registros de la aplicación. Puede habilitar el registro a nivel de depuración en el SDK para enviar registros más detallados al archivo de registro de la aplicación. Los niveles de registro válidos son `DEBUG`, `INFO`, `WARN`, `ERROR` y `FATAL`. El nivel de registro `FATAL` silencia todos los mensajes de registro porque el SDK no registra un nivel fatal.

Example application.properties

Configure el nivel de registro con la propiedad `logging.level.com.amazonaws.xray`.

```
logging.level.com.amazonaws.xray = DEBUG
```

Utilice registros de depuración para identificar problemas como la presencia de subsegmentos sin cerrar al generar subsegmentos de forma manual.

Inyección de ID de registro de seguimiento en los registros

Para exponer el ID de seguimiento completo actual en las instrucciones del registro, puede incluir el ID en el contexto de diagnóstico asignado (MDC). Mediante la interfaz `SegmentListener`, se llama a los métodos desde la grabadora de X-Ray durante los eventos del ciclo de vida del segmento. Cuando comienza un segmento o subsegmento, el ID de seguimiento completo se incluye en el MDC con la clave `AWS-XRAY-TRACE-ID`. Cuando termina ese segmento, se elimina la clave del MDC. Esto expone el ID de registro de seguimiento a la biblioteca de registro en uso. Cuando termina un subsegmento, su ID principal se incluye en el MDC.

Example ID de seguimiento completo

El ID completo se representa como `TraceID@EntityID`

```
1-5df42873-011e96598b447dfca814c156@541b3365be3dafc3
```

Esta función funciona con aplicaciones Java equipadas con el SDK de AWS X-Ray para Java y admite las siguientes configuraciones de registro:

- API front-end SLF4J con backend Logback
- API front-end SLF4J con backend Log4J2
- API front-end Log4J2 con backend Log4J2

Consulte las siguientes pestañas para conocer las necesidades de cada front end y backend.

SLF4J Frontend

1. Agregue la siguiente dependencia de Maven a su proyecto.

```
<dependency>
    <groupId>com.amazonaws</groupId>
```

```
    <artifactId>aws-xray-recorder-sdk-slf4j</artifactId>
    <version>2.11.0</version>
</dependency>
```

2. Incluya el método `withSegmentListener` al construir la `AWSXRayRecorder`. Esto agrega una clase de `SegmentListener`, que inyecta automáticamente nuevos ID de registro de seguimiento en el MDC SLF4J.

   `SegmentListener` toma una cadena opcional como parámetro para configurar el prefijo de la instrucción de registro. El prefijo se puede configurar de las siguientes maneras:

   - Ninguno: utiliza el prefijo predeterminado `AWS-XRAY-TRACE-ID`.
   - Vacío: utiliza una cadena vacía (por ejemplo, `""`).
   - Personalizado: utiliza un prefijo personalizado tal como se define en la cadena.

   Example **`AWSXRayRecorderBuilder`** instrucción

   ```
   AWSXRayRecorderBuilder builder = AWSXRayRecorderBuilder
           .standard().withSegmentListener(new SLF4JSegmentListener("CUSTOM-
   PREFIX"));
   ```

Log4J2 front end

1. Agregue la siguiente dependencia de Maven a su proyecto.

   ```
   <dependency>
       <groupId>com.amazonaws</groupId>
       <artifactId>aws-xray-recorder-sdk-log4j</artifactId>
       <version>2.11.0</version>
   </dependency>
   ```

2. Incluya el método `withSegmentListener` al construir la `AWSXRayRecorder`. Esto agregará una clase de `SegmentListener`, que incluye automáticamente nuevos ID de seguimiento completo en el MDC SLF4J.

   `SegmentListener` toma una cadena opcional como parámetro para configurar el prefijo de la instrucción de registro. El prefijo se puede configurar de las siguientes maneras:

   - Ninguno: utiliza el prefijo predeterminado `AWS-XRAY-TRACE-ID`.

- Vacío: utiliza una cadena vacía (por ejemplo, "") y elimina el prefijo.
- Personalizado: utiliza el prefijo personalizado definido en la cadena.

Example **`AWSXRayRecorderBuilder`** instrucción

```
AWSXRayRecorderBuilder builder = AWSXRayRecorderBuilder
        .standard().withSegmentListener(new Log4JSegmentListener("CUSTOM-
PREFIX"));
```

Logback backend

Para insertar el ID de registro de seguimiento en los eventos de registro, debe modificar el `PatternLayout` del registrador, que da formato a cada instrucción de registro.

1. Busque dónde está configurado el `patternLayout`. Puede hacerlo mediante programación o a través de un archivo de configuración XML. Para obtener más información, consulte Configuración de Logback.
2. Inserte `%X{AWS-XRAY-TRACE-ID}` en cualquier lugar del `patternLayout` para insertar el ID de rastro en las futuras instrucciones de registro. `%X{}` indica que recupera un valor con la clave proporcionada del MDC. Para obtener más información sobre PatternLayouts Logback, consulte. PatternLayout

Log4J2 backend

1. Busque dónde está configurado el `patternLayout`. Puede hacerlo mediante programación o a través de un archivo de configuración escrito en XML, JSON, YAML o con las propiedades del formato.

   Para obtener más información sobre la configuración de Log4J2 ´mediante un archivo de configuración, consulte Configuración.

   Para obtener más información sobre la configuración de Log4J2 mediante programación, consulte Configuración programática.
2. Inserte `%X{AWS-XRAY-TRACE-ID}` en cualquier lugar del `PatternLayout` para insertar el ID de rastro en las futuras instrucciones de registro. `%X{}` indica que recupera un valor con la

clave proporcionada del MDC. Para obtener más información sobre PatternLayouts Log4J2, consulte Diseño de patrones.

Ejemplo de inyección de ID de registro de seguimiento

A continuación se muestra una cadena de `PatternLayout` modificada para incluir el ID de registro de seguimiento. El ID de registro de seguimiento se imprime después del nombre del subproceso (`%t`) y antes del nivel de registro (`%-5p`).

Example **`PatternLayout`** Con inyección de ID

```
%d{HH:mm:ss.SSS} [%t] %X{AWS-XRAY-TRACE-ID} %-5p %m%n
```

AWS X-Ray imprime automáticamente la clave y el ID de rastreo en la declaración de registro para facilitar el análisis. A continuación se muestra una instrucción de registro que utiliza el `PatternLayout` modificado.

Example Instrucción de registro con inyección de ID

```
2019-09-10 18:58:30.844 [nio-5000-exec-4]  AWS-XRAY-TRACE-ID:
 1-5d77f256-19f12e4eaa02e3f76c78f46a@1ce7df03252d99e1 WARN 1 - Your logging message
 here
```

El mensaje de registro en sí está alojado en el patrón `%m` y se establece al llamar al registrador.

Agentes de escucha de segmento

Los agentes de escucha de segmento son una interfaz para interceptar eventos del ciclo de vida, como el comienzo y el final de segmentos producidos por `AWSXRayRecorder`. La implementación de una función de evento de un agente de escucha de segmento es posible que sea agregar la misma anotación a todos los subsegmentos cuando se crean con `onBeginSubsegment`, registrar un mensaje después de que cada segmento se envíe al demonio mediante `afterEndSegment` o registrar consultas enviadas por los interceptores de SQL mediante `beforeEndSubsegment` para verificar si el subsegmento representa una consulta SQL, agregando metadatos adicionales si es así.

Para consultar la lista completa de funciones de `SegmentListener`, consulte la documentación del SDK de grabación de AWS X-Ray para la API de Java.

En el ejemplo siguiente se muestra cómo agregar una anotación coherente a todos los subsegmentos al crear con `onBeginSubsegment` e imprimir un mensaje de registro al final de cada segmento con `afterEndSegment`.

Example MySegmentListener.java

```
import com.amazonaws.xray.entities.Segment;
import com.amazonaws.xray.entities.Subsegment;
import com.amazonaws.xray.listeners.SegmentListener;

public class MySegmentListener implements SegmentListener {
    .....

    @Override
    public void onBeginSubsegment(Subsegment subsegment) {
        subsegment.putAnnotation("annotationKey", "annotationValue");
    }

    @Override
    public void afterEndSegment(Segment segment) {
        // Be mindful not to mutate the segment
        logger.info("Segment with ID " + segment.getId());
    }
}
```

A continuación, se hace referencia a este agente de escucha de segmento personalizado cuando se crea `AWSXRayRecorder`.

Example AWSXRayRecorderBuilder declaración

```
AWSXRayRecorderBuilder builder = AWSXRayRecorderBuilder
        .standard().withSegmentListener(new MySegmentListener());
```

Variables de entorno

Puede usar variables de entorno para configurar el SDK de X-Ray para Java. El SDK admite las siguientes variables.

- `AWS_XRAY_TRACING_NAME`: establezca el nombre de servicio que el SDK utiliza para los segmentos. Anula el nombre de servicio que se ha establecido en la estrategia de nomenclatura de segmento del filtro de servlet.

- `AWS_XRAY_DAEMON_ADDRESS`: establezca el host y el puerto del oyente del daemon de X-Ray. De forma predeterminada, el SDK utiliza `127.0.0.1:2000` tanto para los datos de rastro (UDP) como para el muestreo (TCP). Use esta variable si ha configurado el daemon para que escuche en un puerto diferente o si se ejecuta en un host diferente.

  Formato

  - El mismo puerto: *`address`*`:`*`port`*
  - Puertos diferentes: `tcp:`*`address`*`:`*`port`* `udp:`*`address`*`:`*`port`*
- `AWS_XRAY_CONTEXT_MISSING`: establezca esta opción en `RUNTIME_ERROR` para generar excepciones cuando el código instrumentado intente registrar datos sin que haya ningún segmento abierto.

  Valores válidos

  - `RUNTIME_ERROR`: lance una excepción de tiempo de ejecución.
  - `LOG_ERROR`: registre un error y continúe (predeterminado).
  - `IGNORE_ERROR`: ignore el error y continúe.

  Se pueden producir errores relativos a segmentos o subsegmentos inexistentes al intentar usar un cliente instrumentado en el código de inicio que se ejecuta cuando no hay ninguna solicitud abierta o en el código que inicia un nuevo subproceso.

Las variables de entorno anulan las propiedades de sistema equivalentes y los valores establecidos en el código.

Propiedades del sistema

Puede utilizar las propiedades del sistema como una alternativa específica de JVM para las variables de entorno. El SDK admite las propiedades siguientes:

- `com.amazonaws.xray.strategy.tracingName`: equivalente a `AWS_XRAY_TRACING_NAME`.
- `com.amazonaws.xray.emitters.daemonAddress`: equivalente a `AWS_XRAY_DAEMON_ADDRESS`.
- `com.amazonaws.xray.strategy.contextMissingStrategy`: equivalente a `AWS_XRAY_CONTEXT_MISSING`.

Si se ha establecido tanto una propiedad del sistema y como su variable de entorno equivalente, se utiliza el valor de la variable de entorno. En cualquier caso, esos valores anulan los valores establecidos en el código.

Rastreo de las solicitudes entrantes con el SDK de X-Ray para Java

Puede usar el SDK de X-Ray para rastrear las solicitudes HTTP entrantes que su aplicación sirve en una instancia EC2 de Amazon EC2 AWS Elastic Beanstalk o Amazon ECS.

Utilice un `Filter` para instrumentar las solicitudes HTTP entrantes. Cuando añade el filtro de servlet de X-Ray a su aplicación, el SDK de X-Ray para Java crea un segmento para cada solicitud muestreada. Este segmento incluye el momento, el método y la disposición de la solicitud HTTP. La instrumentación adicional crea subsegmentos en este segmento.

> **Note**
>
> Para AWS Lambda las funciones, Lambda crea un segmento para cada solicitud muestreada. Para obtener más información, consulte AWS Lambda y AWS X-Ray.

Cada segmento tiene un nombre que identifica la aplicación en el mapa de servicio. El nombre del segmento se puede asignar de forma estática o se puede configurar el SDK para que le asigne un nombre dinámico en función del encabezado del host de la solicitud entrante. La nomenclatura dinámica permite agrupar los rastros en función del nombre de dominio de la solicitud y aplicar un nombre predeterminado si el nombre no coincide con el patrón esperado (por ejemplo, si el encabezado del host está falsificado).

> **Solicitudes reenviadas**
>
> Si un equilibrador de carga u otro intermediario reenvía una solicitud a la aplicación, X-Ray toma la IP de cliente del encabezado `X-Forwarded-For` de la solicitud en lugar de tomar la IP de origen del paquete IP. La IP de cliente que se graba para una solicitud reenviada puede estar falsificada, por lo que no se debe confiar en ella.

Cuando se reenvía una solicitud, el SDK crea un campo adicional en el segmento para indicar que se realizó esta acción. Si el segmento contiene el campo `x_forwarded_for` configurado en `true`, el IP del cliente se obtiene a partir del encabezado `X-Forwarded-For` en la solicitud HTTP.

El controlador de mensajes crea un segmento para cada solicitud entrante con un bloque `http` que contiene la siguiente información:

- Método HTTP: GET, POST, PUT, DELETE, etc.
- Dirección del cliente: la dirección IP del cliente que envió la solicitud.
- Código de respuesta: el código de respuesta HTTP para la solicitud finalizada.
- Intervalo: la hora de inicio (cuando se recibió la solicitud) y la hora de finalización (cuando se envió la respuesta).
- Agente del usuario: el `user-agent` de la solicitud.
- Longitud del contenido: la `content-length` de la respuesta.

Secciones

Agregar un filtro de seguimiento a la aplicación (Tomcat)

Para Tomcat, añada un `<filter>` al archivo `web.xml` de su proyecto. Use el parámetro `fixedName` para especificar un nombre de servicio que se aplique a los segmentos creados para las solicitudes entrantes.

Example WEB-INF/web.xml - Tomcat

```
<filter>
  <filter-name>AWSXRayServletFilter</filter-name>
  <filter-class>com.amazonaws.xray.javax.servlet.AWSXRayServletFilter</filter-class>
  <init-param>
    <param-name>fixedName</param-name>
    <param-value>MyApp</param-value>
  </init-param>
</filter>
<filter-mapping>
  <filter-name>AWSXRayServletFilter</filter-name>
  <url-pattern>*</url-pattern>
</filter-mapping>
```

Agregar un filtro de seguimiento a la aplicación (Spring)

Para Spring, añada un `Filter` a la clase `WebConfig`. Pase el nombre del segmento al constructor `AWSXRayServletFilter` como cadena.

Example src/main/java/myapp/ .java - primavera WebConfig

```
package myapp;
import org.springframework.context.annotation.Configuration;
import org.springframework.context.annotation.Bean;
import javax.servlet.Filter;
import com.amazonaws.xray.javax.servlet.AWSXRayServletFilter;

@Configuration
public class WebConfig {

  @Bean
  public Filter TracingFilter() {
    return new AWSXRayServletFilter("Scorekeep");
  }
}
```

Configuración de una estrategia de nomenclatura de segmentos

AWS X-Ray utiliza un nombre de servicio para identificar la aplicación y distinguirla del resto de aplicaciones, bases de datos, API externas y recursos que utiliza la aplicación. AWS Cuando el SDK de X-Ray genera segmentos para las solicitudes entrantes, registra el nombre del servicio de la aplicación en el campo de nombre del segmento.

El SDK de X-Ray puede nombrar los segmentos utilizando el nombre de host en el encabezado de la solicitud HTTP. Sin embargo, este encabezado se puede falsificar, lo que podría provocar nodos inesperados en el mapa de servicio. Para evitar que el SDK nombre los segmentos de forma incorrecta debido a que las solicitudes tienen encabezados de host falsificados, debe especificar un nombre predeterminado para las solicitudes entrantes.

Si la aplicación atiende solicitudes de varios dominios, puede configurar el SDK para que utilice una estrategia de nomenclatura dinámica que refleje esto en los nombres de los segmentos. Una estrategia de nomenclatura dinámica permite al SDK usar el nombre de host para las solicitudes que coinciden con un patrón esperado y aplicar el nombre predeterminado a las solicitudes que no coincidan.

Por ejemplo, es posible que tenga una sola aplicación que atienda solicitudes a tres subdominios: `www.example.com`, `api.example.com` y `static.example.com`. Puede usar una estrategia de nomenclatura dinámica con el patrón `*.example.com` para identificar los segmentos de cada subdominio con un nombre diferente, lo que da como resultado tres nodos de servicio en el mapa de servicio. Si su aplicación recibe solicitudes con un nombre de host que no coincide con el patrón, verá un cuarto nodo en el mapa de servicio con el nombre alternativo que especifique.

Para utilizar el mismo nombre para todos los segmentos de solicitud, especifique el nombre de la aplicación cuando inicie el filtro de servlet, tal y como se muestra en la sección anterior. Esto tiene el mismo efecto que crear un fijo SegmentNamingStrategyllamándolo `SegmentNamingStrategy.fixed()` y pasándolo al `AWSXRayServletFilter`constructor.

> **Note**
>
> Puede anular el nombre de servicio predeterminado que ha definido en el código mediante la `AWS_XRAY_TRACING_NAME`variable de entorno???.

Una estrategia de nomenclatura dinámica define un patrón con el que deben coincidir los nombres de host y un nombre predeterminado que se utiliza si el nombre de host de la solicitud HTTP no coincide con el patrón. Para asignar nombres de forma dinámica en Tomcat, utilice `dynamicNamingRecognizedHosts` y `dynamicNamingFallbackName` para definir el patrón y el nombre predeterminado, respectivamente.

Example WEB-INF/web.xml: filtro de servlet con nomenclatura dinámica

```
<filter>
  <filter-name>AWSXRayServletFilter</filter-name>
  <filter-class>com.amazonaws.xray.javax.servlet.AWSXRayServletFilter</filter-class>
  <init-param>
    <param-name>dynamicNamingRecognizedHosts</param-name>
    <param-value>*.example.com</param-value>
  </init-param>
  <init-param>
    <param-name>dynamicNamingFallbackName</param-name>
    <param-value>MyApp</param-value>
  </init-param>
</filter>
<filter-mapping>
  <filter-name>AWSXRayServletFilter</filter-name>
```

```
  <url-pattern>*</url-pattern>
</filter-mapping>
```

Para Spring, crea una dinámica SegmentNamingStrategymediante una llamada `SegmentNamingStrategy.dynamic()` y pásala al `AWSXRayServletFilter` constructor.

Example WebConfigsrc/main/java/myapp/ .java: filtro de servlets con nomenclatura dinámica

```
package myapp;
import org.springframework.context.annotation.Configuration;
import org.springframework.context.annotation.Bean;
import javax.servlet.Filter;
import com.amazonaws.xray.javax.servlet.AWSXRayServletFilter;
import com.amazonaws.xray.strategy.SegmentNamingStrategy;

@Configuration
public class WebConfig {

  @Bean
  public Filter TracingFilter() {
    return new AWSXRayServletFilter(SegmentNamingStrategy.dynamic("MyApp",
 "*.example.com"));
  }
}
```

Rastreo de llamadas al AWS SDK con el X-Ray SDK for Java

Cuando la aplicación realiza llamadas Servicios de AWS para almacenar datos, escribir en una cola o enviar notificaciones, el X-Ray SDK for Java rastrea las llamadas en sentido descendente en subsegmentos. El rastreo Servicios de AWS y los recursos a los que accede dentro de esos servicios (por ejemplo, un bucket de Amazon S3 o una cola de Amazon SQS) aparecen como nodos descendentes en el mapa de rastreo de la consola X-Ray.

El SDK de X-Ray para Java instrumenta automáticamente todos los clientes del SDK de AWS cuando usted incluye el `aws-sdk` y un submódulo `aws-sdk-instrumentor` en su compilación. Si no incluye el submódulo Instrumentor, puede elegir instrumentar ciertos clientes a la vez que omite otros.

Para instrumentar a clientes individuales, elimine el `aws-sdk-instrumentor` submódulo de la compilación y añada `XRayClient` uno a su cliente del AWS SDK mediante el generador de clientes del servicio. `TracingHandler`

Por ejemplo, para instrumentar un cliente `AmazonDynamoDB`, transfiera un controlador de rastros a `AmazonDynamoDBClientBuilder`.

Example MyModel.java: cliente de DynamoDB

```
import com.amazonaws.xray.AWSXRay;
import com.amazonaws.xray.handlers.TracingHandler;

...
public class MyModel {
  private AmazonDynamoDB client = AmazonDynamoDBClientBuilder.standard()
        .withRegion(Regions.fromName(System.getenv("AWS_REGION")))
        .withRequestHandlers(new TracingHandler(AWSXRay.getGlobalRecorder()))
        .build();
...
```

Para todos los servicios, puede ver el nombre de la API a la que se llama en la consola de X-Ray. Para un subconjunto de servicios, el SDK de X-Ray agrega información al segmento para proporcionar una mayor granularidad en el mapa de servicio.

Por ejemplo, cuando realiza una llamada con un cliente instrumentado de DynamoDB, el SDK agrega el nombre de tabla al segmento para las llamadas que se dirigen a una tabla. En la consola, cada tabla aparece como nodo independiente en el mapa de servicio, con un nodo genérico de DynamoDB para las llamadas que no se dirigen a una tabla.

Example Subsegmento para una llamada a DynamoDB con el fin de guardar un elemento

```
{
  "id": "24756640c0d0978a",
  "start_time": 1.480305974194E9,
  "end_time": 1.4803059742E9,
  "name": "DynamoDB",
  "namespace": "aws",
  "http": {
    "response": {
      "content_length": 60,
      "status": 200
    }
  },
  "aws": {
    "table_name": "scorekeep-user",
    "operation": "UpdateItem",
```

```
    "request_id": "UBQNSO5AEM8T4FDA4RQDEB94OVTDRVV4K4HIRGVJF66Q9ASUAAJG",
  }
}
```

Cuando accede a recursos designados, las llamadas a los siguientes servicios crean nodos adicionales en el mapa de servicio. Las llamadas que no están dirigidas a recursos concretos crean un nodo genérico en el servicio.

- Amazon DynamoDB: nombre de tabla
- Amazon Simple Storage Service: nombre de bucket y de clave
- Amazon Simple Queue Service: nombre de cola

Para instrumentar las llamadas posteriores a la versión Servicios de AWS AWS SDK for Java 2.2 y versiones posteriores, puede omitir el `aws-xray-recorder-sdk-aws-sdk-v2-instrumentor` módulo de la configuración de compilación. Incluya `aws-xray-recorder-sdk-aws-sdk-v2 module` en su lugar y después instrumente los clientes por separado configurándolos con `TracingInterceptor`.

Example AWS SDK for Java 2.2 y versiones posteriores: interceptor de rastreo

```
import com.amazonaws.xray.interceptors.TracingInterceptor;
import software.amazon.awssdk.core.client.config.ClientOverrideConfiguration
import software.amazon.awssdk.services.dynamodb.DynamoDbClient;
//...
public class MyModel {
private DynamoDbClient client = DynamoDbClient.builder()
.region(Region.US_WEST_2)
.overrideConfiguration(ClientOverrideConfiguration.builder()
.addExecutionInterceptor(new TracingInterceptor())
.build()
)
.build();
//...
```

Rastreo de llamadas a servicios web HTTP posteriores con el SDK de X-Ray para Java

Cuando una aplicación realiza llamadas a microservicios o a API de HTTP públicas, se puede utilizar la versión de `HttpClient` del SDK de X-Ray para Java con el fin de instrumentar dichas llamadas y añadir la API al gráfico de servicios como un servicio posterior.

El SDK de X-Ray para Java incluye `DefaultHttpClient` `HttpClientBuilder` clases que se pueden usar en lugar de HttpComponents los equivalentes de Apache para instrumentar las llamadas HTTP salientes.

- `com.amazonaws.xray.proxies.apache.http.DefaultHttpClient` - `org.apache.http.impl.client.DefaultHttpClient`
- `com.amazonaws.xray.proxies.apache.http.HttpClientBuilder` - `org.apache.http.impl.client.HttpClientBuilder`

Estas bibliotecas se encuentran en el submódulo `aws-xray-recorder-sdk-apache-http`.

Puede sustituir las instrucciones actuales de importación con el equivalente a X-Ray para instrumentar todos los clientes, o bien utilizar el nombre completo cuando inicie un cliente para instrumentar clientes específicos.

Example HttpClientBuilder

```
import com.fasterxml.jackson.databind.ObjectMapper;
import org.apache.http.HttpEntity;
import org.apache.http.client.methods.CloseableHttpResponse;
import org.apache.http.client.methods.HttpGet;
import org.apache.http.impl.client.CloseableHttpClient;
import org.apache.http.util.EntityUtils;
import com.amazonaws.xray.proxies.apache.http.HttpClientBuilder;
...
  public String randomName() throws IOException {
    CloseableHttpClient httpclient = HttpClientBuilder.create().build();
    HttpGet httpGet = new HttpGet("http://names.example.com/api/");
    CloseableHttpResponse response = httpclient.execute(httpGet);
    try {
      HttpEntity entity = response.getEntity();
      InputStream inputStream = entity.getContent();
      ObjectMapper mapper = new ObjectMapper();
      Map<String, String> jsonMap = mapper.readValue(inputStream, Map.class);
```

```
      String name = jsonMap.get("name");
      EntityUtils.consume(entity);
      return name;
    } finally {
      response.close();
    }
  }
```

Cuando se instrumenta una llamada a una API web posterior, el del SDK de X-Ray para Java registra un subsegmento con información sobre la solicitud HTTP y la respuesta. X-Ray utiliza el subsegmento para generar un segmento inferido de la API remota.

Example Subsegmento para una llamada HTTP posterior

```
{
  "id": "004f72be19cddc2a",
  "start_time": 1484786387.131,
  "end_time": 1484786387.501,
  "name": "names.example.com",
  "namespace": "remote",
  "http": {
    "request": {
      "method": "GET",
      "url": "https://names.example.com/"
    },
    "response": {
      "content_length": -1,
      "status": 200
    }
  }
}
```

Example Segmento inferido para una llamada HTTP posterior

```
{
  "id": "168416dc2ea97781",
  "name": "names.example.com",
  "trace_id": "1-62be1272-1b71c4274f39f122afa64eab",
  "start_time": 1484786387.131,
  "end_time": 1484786387.501,
  "parent_id": "004f72be19cddc2a",
  "http": {
    "request": {
```

```
      "method": "GET",
      "url": "https://names.example.com/"
    },
    "response": {
      "content_length": -1,
      "status": 200
    }
  },
  "inferred": true
}
```

Rastreo de consultas SQL con el SDK de X-Ray para Java

Interceptores SQL

Instrumente consultas de base de datos SQL añadiendo el interceptor JDBC del SDK de X-Ray para Java a la configuración del origen de datos.

- PostgreSQL – `com.amazonaws.xray.sql.postgres.TracingInterceptor`
- MySQL – `com.amazonaws.xray.sql.mysql.TracingInterceptor`

Estos interceptadores están en los submódulos `aws-xray-recorder-sql-postgres` y `aws-xray-recorder-sql-mysql`, respectivamente. Implementan `org.apache.tomcat.jdbc.pool.JdbcInterceptor` y son compatibles con grupos de conexión Tomcat.

> **Note**
>
> Los interceptores de SQL no registran la consulta SQL en subsegmentos por motivos de seguridad.

Para Spring, añada el interceptor a un archivo de propiedades y cree el origen de datos con `DataSourceBuilder` de Spring Boot.

Example **`src/main/java/resources/application.properties`**: interceptor JDBC de PostgreSQL

```
spring.datasource.continue-on-error=true
spring.jpa.show-sql=false
```

```
spring.jpa.hibernate.ddl-auto=create-drop
spring.datasource.jdbc-interceptors=com.amazonaws.xray.sql.postgres.TracingInterceptor
spring.jpa.database-platform=org.hibernate.dialect.PostgreSQL94Dialect
```

Example **`src/main/java/myapp/WebConfig.java`**: origen de datos

```
import org.springframework.boot.autoconfigure.EnableAutoConfiguration;
import org.springframework.boot.autoconfigure.jdbc.DataSourceBuilder;
import org.springframework.boot.context.properties.ConfigurationProperties;
import org.springframework.context.annotation.Bean;
import org.springframework.context.annotation.Configuration;
import org.springframework.data.jpa.repository.config.EnableJpaRepositories;

import javax.servlet.Filter;
import javax.sql.DataSource;
import java.net.URL;

@Configuration
@EnableAutoConfiguration
@EnableJpaRepositories("myapp")
public class RdsWebConfig {

  @Bean
  @ConfigurationProperties(prefix = "spring.datasource")
  public DataSource dataSource() {
      logger.info("Initializing PostgreSQL datasource");
      return DataSourceBuilder.create()
              .driverClassName("org.postgresql.Driver")
              .url("jdbc:postgresql://" + System.getenv("RDS_HOSTNAME") + ":" +
 System.getenv("RDS_PORT") + "/ebdb")
              .username(System.getenv("RDS_USERNAME"))
              .password(System.getenv("RDS_PASSWORD"))
              .build();
  }
...
}
```

Para Tomcat, llame a `setJdbcInterceptors` en el origen de datos JDBC con una referencia a la clase del SDK de X-Ray para Java.

Example **`src/main/myapp/model.java`**: origen de datos

```
import org.apache.tomcat.jdbc.pool.DataSource;
```

```
...
DataSource source = new DataSource();
source.setUrl(url);
source.setUsername(user);
source.setPassword(password);
source.setDriverClassName("com.mysql.jdbc.Driver");
source.setJdbcInterceptors("com.amazonaws.xray.sql.mysql.TracingInterceptor;");
```

El SDK de X-Ray para Java incluye la biblioteca de origen de datos JDBC Tomcat, pero puede declararla como una dependencia para documentar su uso.

Example **`pom.xml`**: origen de datos JDBC

```
<dependency>
  <groupId>org.apache.tomcat</groupId>
  <artifactId>tomcat-jdbc</artifactId>
  <version>8.0.36</version>
  <scope>provided</scope>
</dependency>
```

Decorador de rastreo SQL nativo

- Añada `aws-xray-recorder-sdk-sql` a sus dependencias.
- Decore el origen de datos, conexión o declaración de su base de datos.

```
dataSource = TracingDataSource.decorate(dataSource)
connection = TracingConnection.decorate(connection)
statement = TracingStatement.decorateStatement(statement)
preparedStatement = TracingStatement.decoratePreparedStatement(preparedStatement,
 sql)
callableStatement = TracingStatement.decorateCallableStatement(callableStatement,
 sql)
```

Generación de subsegmentos personalizados con el SDK de X-Ray para Java

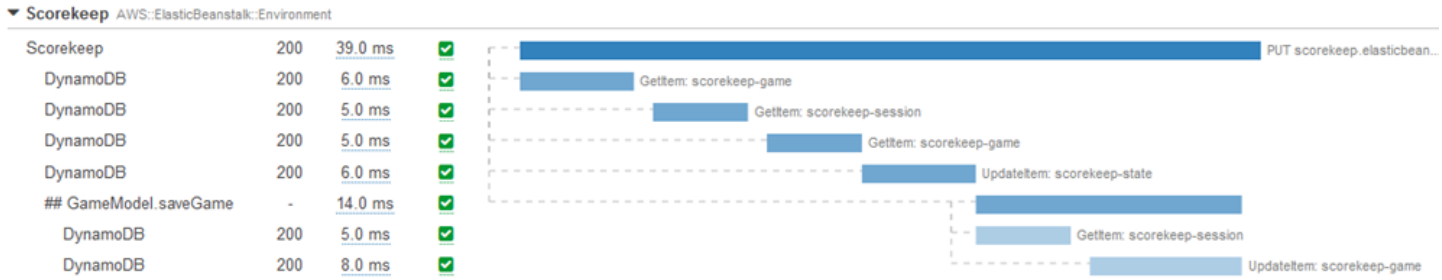
Los subsegmentos amplían el segmento de un rastro con detalles sobre el trabajo realizado para atender una solicitud. Cada vez que usted realiza una llamada con un cliente instrumentado, el SDK de X-Ray registra la información generada en un subsegmento. Puede crear subsegmentos adicionales para agrupar otros subsegmentos, medir el rendimiento de una sección de código o registrar anotaciones y metadatos.

Para administrar los subsegmentos, utilice los métodos `beginSubsegment` y `endSubsegment`.

Example GameModel.java: subsegmento personalizado

```
import com.amazonaws.xray.AWSXRay;
...
  public void saveGame(Game game) throws SessionNotFoundException {
    // wrap in subsegment
    Subsegment subsegment = AWSXRay.beginSubsegment("Save Game");
    try {
      // check session
      String sessionId = game.getSession();
      if (sessionModel.loadSession(sessionId) == null ) {
        throw new SessionNotFoundException(sessionId);
      }
      mapper.save(game);
    } catch (Exception e) {
      subsegment.addException(e);
      throw e;
    } finally {
      AWSXRay.endSubsegment();
    }
  }
```

En este ejemplo, el código del subsegmento carga la sesión del juego desde DynamoDB con un método del modelo de sesión y utiliza el mapeador de DynamoDB para AWS SDK for Java guardar la partida. Cuando se encapsula este código en un subsegmento, las llamadas a DynamoDB se convierten en elementos secundarios del subsegmento `Save Game` en la vista de rastros en la consola.



Si en el código en su subsegmentos aparecen excepciones comprobadas, envuélvalo en un bloque `try` y llame a `AWSXRay.endSubsegment()` en un bloque `finally` para garantizar que el subsegmento está siempre cerrado. Si un subsegmento no está cerrado, el segmento primario no se puede completar y no se envía a X-Ray.

En los códigos donde no aparecen excepciones comprobadas, puede transferir el código a `AWSXRay.CreateSubsegment` como una función de Lambda.

Example Función Lambda de subsegmento

```
import com.amazonaws.xray.AWSXRay;

AWSXRay.createSubsegment("getMovies", (subsegment) -> {
    // function code
});
```

Cuando crea un subsegmento dentro de un segmento o de otro subsegmento, el SDK de X-Ray para Java genera un ID para dicho subsegmento y registra la hora de inicio y la hora de finalización.

Example Subsegmentos con metadatos

```
"subsegments": [{
  "id": "6f1605cd8a07cb70",
  "start_time": 1.480305974194E9,
  "end_time": 1.4803059742E9,
  "name": "Custom subsegment for UserModel.saveUser function",
  "metadata": {
    "debug": {
      "test": "Metadata string from UserModel.saveUser"
    }
  },
```

Para la programación asíncrona y multiproceso, debe pasar manualmente el subsegmento al método `endSubsegment()` para asegurarse de que se cierra correctamente, ya que el contexto de X-Ray puede modificarse durante la ejecución asíncrona. Si un subsegmento asíncrono se cierra después de cerrar su segmento principal, este método transmitirá automáticamente todo el segmento al daemon de X-Ray.

Example Subsegmento asíncrono

```
@GetMapping("/api")
public ResponseEntity<?> api() {
  CompletableFuture.runAsync(() -> {
      Subsegment subsegment = AWSXRay.beginSubsegment("Async Work");
      try {
          Thread.sleep(3000);
```

```
        } catch (InterruptedException e) {
            subsegment.addException(e);
            throw e;
        } finally {
            AWSXRay.endSubsegment(subsegment);
        }
    });
    return ResponseEntity.ok().build();
}
```

Adición de anotaciones y metadatos a los segmentos con el SDK de X-Ray para Java

Puede usar anotaciones y metadatos para registrar información adicional sobre las solicitudes, el entorno o la aplicación. Puede añadir anotaciones y metadatos a los segmentos que crea el SDK de X-Ray o a los subsegmentos personalizados que cree usted mismo.

Las anotaciones son pares de clave-valor con valores de cadena, numéricos o booleanos. Las anotaciones se indexan para su uso con expresiones de filtro. Utilice anotaciones para registrar los datos que desee utilizar para agrupar rastros en la consola o cuando llame a la API de `GetTraceSummaries`.

Los metadatos son pares de clave-valor con valores de cualquier tipo, por ejemplo objetos y listas, pero que no se indexan para utilizarlos con expresiones de filtro. Utilice los metadatos para registrar datos adicionales que desee almacenar en el rastro, pero que no necesite usar para hacer búsquedas.

Además de anotaciones y metadatos, también puede registrar cadenas de ID de usuario en los segmentos. Los identificadores de usuario se registran en un campo aparte en segmentos y se indexan para su uso con la búsqueda.

Secciones

- Registro de anotaciones con el SDK de X-Ray para Java
- Registro de metadatos con el SDK de X-Ray para Java
- Registro de ID de usuario con el SDK de X-Ray para Java

Registro de anotaciones con el SDK de X-Ray para Java

Utilice anotaciones para registrar información sobre segmentos o subsegmentos que desee indexar para las búsquedas.

Requisitos de anotación

- Teclas: la clave de una anotación de X-Ray puede tener hasta 500 caracteres alfanuméricos. No puede utilizar espacios ni símbolos distintos del símbolo de subrayado (_).
- Valores: el valor de una anotación de X-Ray puede tener hasta 1000 caracteres Unicode.
- Número de anotaciones: puede utilizar hasta 50 anotaciones por traza.

Para registrar anotaciones

1. Obtenga una referencia al segmento o subsegmento actual desde `AWSXRay`.

   ```
   import com.amazonaws.xray.AWSXRay;
   import com.amazonaws.xray.entities.Segment;
   ...
   Segment document = AWSXRay.getCurrentSegment();
   ```

   o

   ```
   import com.amazonaws.xray.AWSXRay;
   import com.amazonaws.xray.entities.Subsegment;
   ...
   Subsegment document = AWSXRay.getCurrentSubsegment();
   ```

2. Llame a `putAnnotation` con una clave de cadena y un valor booleano, numérico o de cadena.

   ```
   document.putAnnotation("mykey", "my value");
   ```

El SDK registra las anotaciones como pares de clave-valor en un objeto `annotations` del documento de segmento. Si llama dos veces a `putAnnotation` con la misma clave, se sobrescriben los valores previamente registrados en ese segmento o subsegmento.

Para encontrar rastros que tengan anotaciones con valores específicos, utilice la palabra clave `annotations.`*`key`* en una expresión de filtro.

Example **`src/main/java/scorekeep/GameModel.java`**: anotaciones y metadatos

```
import com.amazonaws.xray.AWSXRay;
import com.amazonaws.xray.entities.Segment;
import com.amazonaws.xray.entities.Subsegment;
```

```
...
  public void saveGame(Game game) throws SessionNotFoundException {
    // wrap in subsegment
    Subsegment subsegment = AWSXRay.beginSubsegment("## GameModel.saveGame");
    try {
      // check session
      String sessionId = game.getSession();
      if (sessionModel.loadSession(sessionId) == null ) {
        throw new SessionNotFoundException(sessionId);
      }
      Segment segment = AWSXRay.getCurrentSegment();
      subsegment.putMetadata("resources", "game", game);
      segment.putAnnotation("gameid", game.getId());
      mapper.save(game);
    } catch (Exception e) {
      subsegment.addException(e);
      throw e;
    } finally {
      AWSXRay.endSubsegment();
    }
  }
```

Registro de metadatos con el SDK de X-Ray para Java

Utilice los metadatos para registrar información sobre segmentos o subsegmentos que no necesite indexar para las búsquedas. Los valores de metadatos pueden ser cadenas, números, booleanos o cualquier objeto que se pueda serializar en un objeto o matriz JSON.

Para registrar metadatos

1. Obtenga una referencia al segmento o subsegmento actual desde `AWSXRay`.

   ```
   import com.amazonaws.xray.AWSXRay;
   import com.amazonaws.xray.entities.Segment;
   ...
   Segment document = AWSXRay.getCurrentSegment();
   ```

   o

   ```
   import com.amazonaws.xray.AWSXRay;
   import com.amazonaws.xray.entities.Subsegment;
   ...
   ```

```
Subsegment document = AWSXRay.getCurrentSubsegment();
```

2. Llame a `putMetadata` con un espacio de nombres de cadena, una clave de cadena y un valor booleano, numérico, de cadena o de objeto.

   ```
   document.putMetadata("my namespace", "my key", "my value");
   ```

   o

   Llame a `putMetadata` con solo una clave y un valor.

   ```
   document.putMetadata("my key", "my value");
   ```

Si no especifica un espacio de nombres, el SDK utiliza `default`. Si llama dos veces a `putMetadata` con la misma clave, se sobrescriben los valores previamente registrados en ese segmento o subsegmento.

Example **src/main/java/scorekeep/GameModel.java**: anotaciones y metadatos

```
import com.amazonaws.xray.AWSXRay;
import com.amazonaws.xray.entities.Segment;
import com.amazonaws.xray.entities.Subsegment;
...
  public void saveGame(Game game) throws SessionNotFoundException {
    // wrap in subsegment
    Subsegment subsegment = AWSXRay.beginSubsegment("## GameModel.saveGame");
    try {
      // check session
      String sessionId = game.getSession();
      if (sessionModel.loadSession(sessionId) == null ) {
        throw new SessionNotFoundException(sessionId);
      }
      Segment segment = AWSXRay.getCurrentSegment();
      subsegment.putMetadata("resources", "game", game);
      segment.putAnnotation("gameid", game.getId());
      mapper.save(game);
    } catch (Exception e) {
      subsegment.addException(e);
      throw e;
    } finally {
      AWSXRay.endSubsegment();
```

```
    }
  }
```

Registro de ID de usuario con el SDK de X-Ray para Java

Registre identificadores de usuario en segmentos de solicitud para identificar al usuario que envió la solicitud.

Para registrar identificadores de usuario

1. Obtenga una referencia al segmento actual desde `AWSXRay`.

   ```
   import com.amazonaws.xray.AWSXRay;
   import com.amazonaws.xray.entities.Segment;
   ...
   Segment document = AWSXRay.getCurrentSegment();
   ```

2. Llame a `setUser` con un ID de cadena del usuario que envió la solicitud.

   ```
   document.setUser("U12345");
   ```

Puede llamar a `setUser` en sus controladores para registrar el ID de usuario en cuanto la aplicación empiece a procesar la solicitud. Si solo va a utilizar el segmento para establecer el ID de usuario, puede encadenar las llamadas en una sola línea.

Example src/main/java/scorekeep/ .java MoveController: ID de usuario

```
import com.amazonaws.xray.AWSXRay;
...
  @RequestMapping(value="/{userId}", method=RequestMethod.POST)
  public Move newMove(@PathVariable String sessionId, @PathVariable String
 gameId, @PathVariable String userId, @RequestBody String move) throws
 SessionNotFoundException, GameNotFoundException, StateNotFoundException,
 RulesException {
    AWSXRay.getCurrentSegment().setUser(userId);
    return moveFactory.newMove(sessionId, gameId, userId, move);
  }
```

Para buscar rastros de un ID de usuario, utilice la palabra clave `user` en una expresión de filtro.

AWS X-Ray métricas del X-Ray SDK para Java

En este tema se describen el espacio de AWS X-Ray nombres, las métricas y las dimensiones. Puedes usar el SDK de X-Ray para Java para publicar CloudWatch métricas de Amazon sin muestrear de los segmentos de X-Ray recopilados. Estas métricas se derivan de la horade inicio y finalización del segmento, y los marcadores de estado limitado, fallo y error. Utilice estas métricas de seguimiento para exponer los reintentos y los problemas de dependencia con los subsegmentos.

CloudWatch es esencialmente un repositorio de métricas. Una métrica es el concepto fundamental CloudWatch y representa un conjunto de puntos de datos ordenados en el tiempo. Usted (o Servicios de AWS) publica puntos de datos de métricas CloudWatch y recupera las estadísticas sobre esos puntos de datos como un conjunto ordenado de datos de series temporales.

Las métricas se definen de forma exclusiva mediante un nombre, un espacio de nombres y una o varias dimensiones. Cada punto de datos tiene una marca temporal y, opcionalmente, una unidad de medida. Cuando se solicitan estadísticas, el flujo de datos devuelto se identifica mediante el espacio de nombres, el nombre de la métrica y la dimensión.

Para obtener más información al respecto CloudWatch, consulta la Guía del CloudWatch usuario de Amazon.

CloudWatch Métricas de X-Ray

El espacio de nombres de `ServiceMetrics/SDK` incluye las siguientes métricas.

Métrica	Estadísticas disponibles	Descripción	Unidades
`Latency`	Media, mínima, máxima, recuento	La diferencia entre la hora de inicio y finalización. Media, mínima y máxima describen la latencia operativa. Recuento describe el recuento de llamadas.	Milisegundos
`ErrorRate`	Media, Suma	La tasa de solicitudes que fallaron con	Porcentaje

Métrica	Estadísticas disponibles	Descripción	Unidades
		un código de estado `4xx Client Error`, lo que da lugar a un error.	
`FaultRate`	Media, Suma	La tasa de seguimientos que fallaron con un código de estado `5xx Server Error`, lo que da lugar a un fallo.	Porcentaje
`ThrottleRate`	Media, Suma	La tasa de registros limitas que devuelven un código de estado `429`. Se trata de un subconjunto de la métrica `ErrorRate` .	Porcentaje
`OkRate`	Media, Suma	La tasa de solicitudes rastreadas que dan lugar a un código de estado `OK`.	Porcentaje

CloudWatch Dimensiones de X-Ray

Utilice las dimensiones de la siguiente tabla para ajustar las métricas devueltas para sus aplicaciones de Java instrumentadas de X-Ray.

Dimensión	Descripción
`ServiceType`	El tipo de servicio, por ejemplo, `AWS::EC2::Instance` o `NONE`, si no se conoce.
`ServiceName`	El nombre canónico del servicio.

Habilitar CloudWatch métricas de X-Ray

utilice el siguiente procedimiento para habilitar métricas de seguimiento en su aplicación de Java instrumentada.

Para configurar las métricas de seguimiento

1. Agregue el paquete `aws-xray-recorder-sdk-metrics` como una dependencia de Maven. Para obtener más información, consulte Submódulos del SDK de X-Ray para Java.
2. Habilite un nuevo `MetricsSegmentListener()` como parte de la compilación de la grabadora global.

   Example src/com/myapp/web/Startup.java

```
import com.amazonaws.xray.AWSXRay;
import com.amazonaws.xray.AWSXRayRecorderBuilder;
import com.amazonaws.xray.plugins.EC2Plugin;
import com.amazonaws.xray.plugins.ElasticBeanstalkPlugin;
import com.amazonaws.xray.strategy.sampling.LocalizedSamplingStrategy;

@Configuration
public class WebConfig {
...
  static {
    AWSXRayRecorderBuilder builder = AWSXRayRecorderBuilder
                                        .standard()
                                        .withPlugin(new EC2Plugin())
                                        .withPlugin(new ElasticBeanstalkPlugin())
                                        .withSegmentListener(new
 MetricsSegmentListener());

    URL ruleFile = WebConfig.class.getResource("/sampling-rules.json");
    builder.withSamplingStrategy(new LocalizedSamplingStrategy(ruleFile));

    AWSXRay.setGlobalRecorder(builder.build());
  }
}
```

3. Implemente el CloudWatch agente para recopilar métricas mediante Amazon Elastic Compute Cloud (Amazon EC2), Amazon Elastic Container Service (Amazon ECS) o Amazon Elastic Kubernetes Service (Amazon EKS):

- Para configurar Amazon EC2, consulte Implementación del CloudWatch agente y del Daemon X-Ray en Amazon EC2.
- Para configurar Amazon ECS, consulte Implementación del CloudWatch agente y del Daemon X-Ray en Amazon ECS.
- Para configurar Amazon EKS, consulte Implementación del CloudWatch agente y del Daemon X-Ray en Amazon EKS.

4. Configure el SDK para comunicarse con el CloudWatch agente. De forma predeterminada, el SDK se comunica con el CloudWatch agente en la dirección`127.0.0.1`. Puede configurar direcciones alternativas al configurar el entorno variable o la propiedad de Java en `address:port`.

   Example Variable de entorno

   ```
   AWS_XRAY_METRICS_DAEMON_ADDRESS=address:port
   ```

   Example Propiedad de Java

   ```
   com.amazonaws.xray.metrics.daemonAddress=address:port
   ```

Para validar la configuración

1. Inicie sesión en la CloudWatch consola AWS Management Console y ábrala en https://console.aws.amazon.com/cloudwatch/.
2. Abra la pestaña Metrics (Métricas) para observar el flujo de sus métricas.
3. (Opcional) En la CloudWatch consola, en la pestaña Registros, abra el grupo de `ServiceMetricsSDK` registros. Busque un flujo de registros que coincida con las métricas del host y confirme los mensajes del registro.

Transmisión de contexto de segmento entre subprocesos en una aplicación multiproceso

Cuando se crea un nuevo subproceso en la aplicación, el `AWSXRayRecorder` no mantiene una referencia al segmento o subsegmento Entity actual. Si utilizas un cliente instrumentado en el nuevo hilo, el SDK intenta escribir en un segmento que no existe, lo que provoca un. SegmentNotFoundException

Para evitar que se produzcan excepciones durante el desarrollo, puedes configurar la grabadora con una ContextMissingStrategyque le indique que registre un error en su lugar. Puede configurar la estrategia en código o configurar opciones equivalentes con una variable de entorno o una propiedad del sistema. SetContextMissingStrategy

Una forma de abordar el error consiste en utilizar un segmento nuevo llamando a beginSegment al iniciar el subproceso y a endSegment al cerrarlo. Esto funciona si está instrumentando código que no se ejecuta en respuesta a una solicitud HTTP, como código que se ejecuta cuando se inicia la aplicación.

Si utiliza varios subprocesos para gestionar las solicitudes entrantes, puede transferir el segmento o subsegmento actual al nuevo subproceso y facilitarlo a la grabadora global. De este modo, se garantiza que la información registrada en el nuevo subproceso esté asociada al mismo segmento que el resto de la información registrada sobre dicha solicitud. Una vez que el segmento esté disponible en el nuevo hilo, puede ejecutar cualquier ejecutable con acceso al contexto de ese segmento mediante el método `segment.run(() -> { ... })`.

Consulte Uso de clientes instrumentados en subprocesos de trabajo para ver un ejemplo.

Uso de X-Ray con programación asíncrona

El SDK de X-Ray para Java se puede utilizar en programas Java asíncronos con. SegmentContextExecutors SegmentContextExecutor Implementa la interfaz Executor, lo que significa que se puede transferir a todas las operaciones asíncronas de un. CompletableFuture Eso garantiza que cualquier operación asíncrona se ejecute con el segmento correcto en su contexto.

Example Ejemplo: App.java: Pasando a SegmentContextExecutor CompletableFuture

```
DynamoDbAsyncClient client = DynamoDbAsyncClient.create();

AWSXRay.beginSegment();

// ...

client.getItem(request).thenComposeAsync(response -> {
    // If we did not provide the segment context executor, this request would not be
 traced correctly.
    return client.getItem(request2);
}, SegmentContextExecutors.newSegmentContextExecutor());
```

AOP con Spring y el SDK de X-Ray para Java

En este tema se describe cómo utilizar el SDK de X-Ray y el marco de trabajo Spring para instrumentar una aplicación sin cambiar su lógica básica. Esto significa que ahora existe una forma no invasiva de instrumentar las aplicaciones que se ejecutan de forma remota. AWS

Para habilitar AOP en Spring

1. Configure Spring
2. Añada un filtro de rastreo a la aplicación.
3. Comente el código o implemente una interfaz
4. Active X-Ray en la aplicación

Configuración de Spring

Puede utilizar Maven o Gradle para configurar Spring para que utilice AOP con el fin de instrumentar la aplicación.

Si utiliza Maven para compilar la aplicación, añada la siguiente dependencia al archivo `pom.xml`.

```
<dependency>
     <groupId>com.amazonaws</groupId>
     <artifactId>aws-xray-recorder-sdk-spring</artifactId>
     <version>2.11.0</version>
</dependency>
```

Para Gradle, añada la siguiente dependencia al archivo `build.gradle`.

```
compile 'com.amazonaws:aws-xray-recorder-sdk-spring:2.11.0'
```

Configuración de Spring Boot

Además de la dependencia de Spring descrita en la sección anterior, si utiliza Spring Boot, añada la siguiente dependencia si aún no está en su classpath.

Maven:

```
<dependency>
     <groupId>org.springframework.boot</groupId>
```

```
    <artifactId>spring-boot-starter-aop</artifactId>
    <version>2.5.2</version>
</dependency>
```

Gradle:

```
compile 'org.springframework.boot:spring-boot-starter-aop:2.5.2'
```

Adición de un filtro de rastreo a la aplicación

Añada un `Filter` a su clase `WebConfig`. Pase el nombre del segmento al constructor `AWSXRayServletFilter` como cadena. Para obtener más información sobre los filtros de rastreo y la instrumentación de las solicitudes entrantes, consulte Rastreo de las solicitudes entrantes con el SDK de X-Ray para Java.

Example src/main/java/myapp/ .java - WebConfig primavera

```
package myapp;
import org.springframework.context.annotation.Configuration;
import org.springframework.context.annotation.Bean;
import javax.servlet.Filter;
import com.amazonaws.xray.javax.servlet.AWSXRayServletFilter;

@Configuration
public class WebConfig {

  @Bean
  public Filter TracingFilter() {
    return new AWSXRayServletFilter("Scorekeep");
  }
}
```

Compatibilidad con Jakarta

Spring 6 usa Jakarta en lugar de Javax para su Enterprise Edition. Para admitir este nuevo espacio de nombres, X-Ray ha creado un conjunto paralelo de clases que viven en su propio espacio de nombres de Yakarta.

Para las clases de filtro, sustituya `javax` por `jakarta`. Al configurar una estrategia de nomenclatura de segmentos, agregue `jakarta` antes del nombre de la clase de estrategia de nomenclatura, como en el siguiente ejemplo:

```
package myapp;
import org.springframework.context.annotation.Configuration;
import org.springframework.context.annotation.Bean;
import jakarta.servlet.Filter;
import com.amazonaws.xray.jakarta.servlet.AWSXRayServletFilter;
import com.amazonaws.xray.strategy.jakarta.SegmentNamingStrategy;

@Configuration
public class WebConfig {
    @Bean
    public Filter TracingFilter() {
        return new AWSXRayServletFilter(SegmentNamingStrategy.dynamic("Scorekeep"));
    }
}
```

Anotación del código o implementación de una interfaz

Las clases deben anotarse con la anotación `@XRayEnabled` o deben implementar la interfaz de `XRayTraced`. Esto indica al sistema de AOP que encapsule las funciones de la clase afectada para la instrumentación de X-Ray.

Activación de X-Ray en la aplicación

Para activar el rastreo de X-Ray en la aplicación, el código debe extender la clase abstracta `BaseAbstractXRayInterceptor` anulando los siguientes métodos.

- `generateMetadata`: esta función permite la personalización de los metadatos adjuntados al rastreo de la función actual. De forma predeterminada, el nombre de clase de la función que se ejecuta se registra en los metadatos. Puede añadir más datos si necesita más información.
- `xrayEnabledClasses`: esta función está vacía, y debe seguir así. Sirve para alojar un conjunto de puntos de unión (pointcut) que indica al interceptor los métodos que debe encapsular. Defina el pointcut especificando las clases que se han anotado con `@XRayEnabled` que se deben rastrear. La siguiente instrucción pointcut indica al interceptor que encapsule todos los beans del controlador anotados con la anotación `@XRayEnabled`.

  ```
  @Pointcut(“@within(com.amazonaws.xray.spring.aop.XRayEnabled) && bean(*Controller)”)
  ```

Si su proyecto utiliza Spring Data JPA, considere la posibilidad de ampliar desde `AbstractXRayInterceptor` en lugar de `BaseAbstractXRayInterceptor`.

Ejemplo

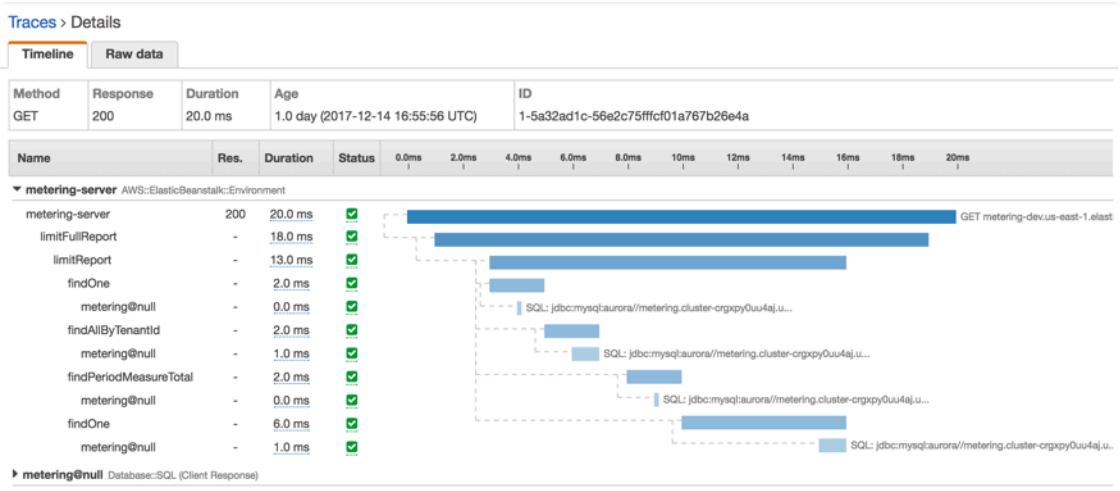
El siguiente código extiende la clase abstracta `BaseAbstractXRayInterceptor`.

```
@Aspect
@Component
public class XRayInspector extends BaseAbstractXRayInterceptor {
    @Override
    protected Map<String, Map<String, Object>> generateMetadata(ProceedingJoinPoint
 proceedingJoinPoint, Subsegment subsegment) throws Exception {
        return super.generateMetadata(proceedingJoinPoint, subsegment);
    }

  @Override
  @Pointcut("@within(com.amazonaws.xray.spring.aop.XRayEnabled) && bean(*Controller)")

  public void xrayEnabledClasses() {}

}
```

El siguiente código es una clase que X-Ray va a instrumentar.

```
@Service
@XRayEnabled
public class MyServiceImpl implements MyService {
    private final MyEntityRepository myEntityRepository;

    @Autowired
    public MyServiceImpl(MyEntityRepository myEntityRepository) {
        this.myEntityRepository = myEntityRepository;
    }

    @Transactional(readOnly = true)
    public List<MyEntity> getMyEntities(){
        try(Stream<MyEntity> entityStream = this.myEntityRepository.streamAll()){

            return entityStream.sorted().collect(Collectors.toList());
        }
    }
}
```

Si ha configurado correctamente la aplicación, debe ver la pila de llamadas completa de la aplicación, desde el controlador hasta las llamadas a los servicios, tal y como se muestra en la siguiente captura de pantalla de la consola.



Instrumentación de su aplicación con Node.js

Puede instrumentar su aplicación Node.js de dos maneras para enviar rastros a X-Ray:

- AWS Distro for OpenTelemetry JavaScript: una AWS distribución que proporciona un conjunto de bibliotecas de código abierto para enviar métricas y rastreos correlacionados a varias soluciones de AWS monitoreo, incluidas Amazon y Amazon OpenSearch Service CloudWatch AWS X-Ray, a través de AWS Distro for Collector. OpenTelemetry
- AWS X-Ray SDK para Node.js: conjunto de bibliotecas para generar y enviar trazas a X-Ray mediante el daemon X-Ray.

Para obtener más información, consulte Cómo elegir entre los AWS SDK Distro for OpenTelemetry y X-Ray.

AWS Distro para OpenTelemetry JavaScript

Con AWS Distro para OpenTelemetry (ADOT) JavaScript, puede instrumentar sus aplicaciones una vez y enviar métricas y rastros correlacionados a varias soluciones de supervisión de AWS, incluidas Amazon CloudWatch, AWS X-Ray y Amazon OpenSearch Service. El uso de X-Ray con AWS Distro para OpenTelemetry requiere dos componentes: un SDK de OpenTelemetry habilitado para usarlo con X-Ray y el AWS Distro para OpenTelemetry Collector habilitado para usarlo con X-Ray.

Para empezar, consulte la documentación de AWS Distro para OpenTelemetry JavaScript.

> **Note**
>
> ADOT JavaScript es compatible con todas las aplicaciones Node.js del lado del servidor. ADOT JavaScript no puede exportar datos a X-Ray desde los clientes del navegador.

Para obtener más información sobre el uso de AWS Distro para OpenTelemetry con AWS X-Ray y otros Servicios de AWS, consulte AWS Distro para OpenTelemetry o la documentación de AWS Distro para OpenTelemetry.

Para obtener información adicional sobre los lenguajes compatibles y el uso, consulte AWS Observability en GitHub.

AWS SDK de X-Ray para Node.js

El SDK de X-Ray para Node.js es una biblioteca para las aplicaciones web de Express y funciones de Lambda de Node.js que proporciona clases y métodos para generar y enviar datos de rastreo al daemon de X-Ray. Los datos de rastreo incluyen información sobre las solicitudes HTTP entrantes atendidas por la aplicación y las llamadas que la aplicación realiza a los servicios descendentes mediante el AWS SDK o los clientes HTTP.

> **Note**
>
> El SDK de X-Ray para Node.js es un proyecto de código abierto. Puedes seguir el proyecto y enviar las incidencias y solicitudes de cambios en GitHub: github.com/aws/ aws-xray-sdk-node

Si usa Express, empiece agregando el SDK como middleware en el servidor de aplicaciones para rastrear solicitudes entrantes. El middleware crea un segmento para cada solicitud rastreada y lo completa cuando se envía la respuesta. Mientras el segmento está abierto, puede utilizar los métodos del cliente del SDK para añadir información al segmento y crear subsegmentos para rastrear llamadas posteriores. El SDK también registra automáticamente las excepciones que produce su aplicación mientras el segmento está abierto.

En el caso de las funciones de Lambda llamadas por una aplicación o un servicio instrumentados, Lambda lee el encabezado de rastreo y rastrea automáticamente las solicitudes muestreadas. Para otras funciones, puede configurar Lambda con el fin de muestrear y rastrear las solicitudes entrantes. En cualquier caso, Lambda crea el segmento y se lo proporciona al SDK de X-Ray.

> **Note**
>
> En Lambda, el SDK de X-Ray es opcional. Si no lo usa en su función, el mapa de servicio seguirá incluyendo un nodo para el servicio de Lambda y uno para cada función de Lambda. Al añadir el SDK, puede instrumentar el código de función para añadir subsegmentos al segmento de función registrado por Lambda. Para obtener más información, consulte AWS Lambda y AWS X-Ray.

A continuación, utilice el SDK de X-Ray para Node.js a fin de instrumentar su AWS SDK para JavaScript los clientes de Node.js. Cada vez que realizas una llamada a un canal intermedio Servicio de AWS o a un recurso con un cliente instrumentado, el SDK registra la información sobre la llamada en un subsegmento. Servicios de AWS y los recursos a los que accedes desde los servicios aparecen como nodos descendentes en el mapa de rastreo para ayudarte a identificar los errores y los problemas de limitación en las conexiones individuales.

El SDK de X-Ray para Node.js también realiza la instrumentación de llamadas posteriores a API web HTTP y consultas SQL. Incluya su cliente HTTP en el método de captura del SDK para registrar información sobre las llamadas HTTP salientes. Para los clientes SQL, utilice el método de captura para el tipo de base de datos.

El middleware aplica reglas de muestreo a las solicitudes entrantes para determinar qué solicitudes se deben rastrear. Puede configurar el SDK de X-Ray para Node.js para ajustar el comportamiento del muestreo o para registrar información sobre los recursos AWS informáticos en los que se ejecuta la aplicación.

Registre información adicional acerca de las solicitudes y el trabajo que la aplicación realiza en anotaciones y metadatos. Las anotaciones son pares sencillos de clave-valor que se indexan para su uso con expresiones de filtro para poder buscar rastros que contengan datos específicos. Las entradas de metadatos son menos restrictivas y pueden registrar objetos y matrices completos, es decir, todo lo que se pueda serializar en JSON.

> **Anotaciones y metadatos**
>
> Las anotaciones y los metadatos son texto arbitrario que se agrega a los segmentos con el SDK de X-Ray. Las anotaciones se indexan para su uso con expresiones de filtro. Los metadatos no se indexan pero se pueden ver en el segmento sin procesar con la consola o

la API de X-Ray. Cualquier persona a la que conceda acceso de lectura a X-Ray puede ver estos datos.

Cuando tenga muchos clientes instrumentados en su código, un único segmento de solicitud puede contener un gran número de subsegmentos, uno para cada llamada realizada con un cliente instrumentado. Puede organizar y agrupar los subsegmentos incluyendo las llamadas del cliente en subsegmentos personalizados. Puede crear un subsegmento personalizado para una función completa o para cualquier sección de código, y registrar los metadatos y las anotaciones en el subsegmento en lugar de escribirlo todo en el segmento principal.

Para tener acceso a los documentos de referencia sobre las clases y los métodos del SDK, consulte la Referencia de la API del SDK de AWS X-Ray para Node.js.

Requisitos

El SDK de X-Ray para Node.js requiere Node.js y las siguientes bibliotecas:

- `atomic-batcher`: 1.0.2
- `cls-hooked`: 4.2.2
- `pkginfo`: 0.4.0
- `semver`: 5.3.0

El SDK obtiene estas bibliotecas cuando se instala con NPM.

Para rastrear los clientes del AWS SDK, el SDK de X-Ray para Node.js requiere una versión mínima del AWS SDK para JavaScript Node.js.

- `aws-sdk`: 2.7.15

Administración de dependencias

El SDK de X-Ray para Node.js está disponible en NPM.

- Paquete: `aws-xray-sdk`

Para el desarrollo local, instale el SDK en el directorio del proyecto con npm.

```
~/nodejs-xray$ npm install aws-xray-sdk
aws-xray-sdk@3.3.3
  ### aws-xray-sdk-core@3.3.3
  # ### @aws-sdk/service-error-classification@3.15.0
  # ### @aws-sdk/types@3.15.0
  # ### @types/cls-hooked@4.3.3
  # # ### @types/node@15.3.0
  # ### atomic-batcher@1.0.2
  # ### cls-hooked@4.2.2
  # # ### async-hook-jl@1.7.6
  # # # ### stack-chain@1.3.7
  # # ### emitter-listener@1.1.2
  # #   ### shimmer@1.2.1
  # ### semver@5.7.1
  ### aws-xray-sdk-express@3.3.3
  ### aws-xray-sdk-mysql@3.3.3
  ### aws-xray-sdk-postgres@3.3.3
```

Use la opción `--save` para guardar el SDK como una dependencia en el archivo `package.json` de la aplicación.

```
~/nodejs-xray$ npm install aws-xray-sdk --save
aws-xray-sdk@3.3.3
```

Si la aplicación tiene dependencias cuyas versiones entran en conflicto con las del SDK de X-Ray, se instalarán ambas versiones para garantizar la compatibilidad. Para obtener más detalles, consulte la documentación oficial de NPM para la resolución de dependencias.

Ejemplos de Node.js

Usa el AWS X-Ray SDK de Node.js para end-to-end ver las solicitudes a medida que se desplazan por tus aplicaciones de Node.js.

- La aplicación de ejemplo Node.js está activada GitHub.

Configuración del SDK de X-Ray para Node.js

Puede configurar el SDK de X-Ray para Node.js el uso de complementos a fin de incluir información sobre el servicio que sus aplicaciones ejecutan, modificar la conducta predeterminada de muestreo o agregar reglas de muestreo que se aplican a las solicitudes dirigidas a rutas específicas.

Secciones

Complementos del servicio

Utilice `plugins` para registrar información sobre el servicio que aloja la aplicación.

Complementos

- Amazon EC2: `EC2Plugin` agrega el ID de la instancia, la zona de disponibilidad y el grupo de CloudWatch registros.
- Elastic Beanstalk: `ElasticBeanstalkPlugin` añade el nombre de entorno, la etiqueta de versión y el ID de implementación.
- Amazon ECS: `ECSPlugin` agrega el ID de contenedor.

Para utilizar un complemento, configure el cliente del SDK de X-Ray para Node.js mediante el método `config`.

Example app.js: complementos

```
var AWSXRay = require('aws-xray-sdk');
AWSXRay.config([AWSXRay.plugins.EC2Plugin,AWSXRay.plugins.ElasticBeanstalkPlugin]);
```

El SDK también usa la configuración del complemento para establecer el campo `origin` en el segmento. Esto indica el tipo de AWS recurso que ejecuta la aplicación. Cuando utilizas varios complementos, el SDK utiliza el siguiente orden de resolución para determinar el origen: ElasticBeanstalk > EKS > ECS > EC2.

Reglas de muestreo

El SDK utiliza las reglas de muestreo que define el usuario en la consola de X-Ray para determinar qué solicitudes registrar. La regla predeterminada rastrea la primera solicitud cada segundo y el 5 % de las solicitudes adicionales de todos los servicios que envían rastros a X-Ray. Cree reglas

adicionales en la consola de X-Ray para personalizar la cantidad de datos registrados para cada una de sus aplicaciones.

El SDK aplica las reglas personalizadas en el orden en que se definen. Si una solicitud coincide con varias reglas personalizadas, el SDK solo aplica la primera regla.

> **Note**
>
> Si el SDK no puede comunicarse con X-Ray para obtener las reglas de muestreo, vuelve a una regla local predeterminada de la primera solicitud cada segundo y del 5 % de las solicitudes adicionales por host. Eso puede ocurrir si el host no tiene permiso para llamar a las API de muestreo o no puede conectarse al daemon de X-Ray, que actúa como proxy TCP para las llamadas a las API realizadas por el SDK.

También puede configurar el SDK para que cargue las reglas de muestreo desde un documento JSON. El SDK puede usar las reglas locales como respaldo para los casos en que el muestreo de X-Ray no esté disponible, o puede usar las reglas locales exclusivamente.

Example sampling-rules.json

```
{
  "version": 2,
  "rules": [
    {
      "description": "Player moves.",
      "host": "*",
      "http_method": "*",
      "url_path": "/api/move/*",
      "fixed_target": 0,
      "rate": 0.05
    }
  ],
  "default": {
    "fixed_target": 1,
    "rate": 0.1
  }
}
```

En este ejemplo se define una regla personalizada y una regla predeterminada. La regla personalizada aplica un porcentaje de muestreo del 5 % sin un número mínimo de solicitudes de

rastreo para las rutas incluidas bajo `/api/move/`. La regla predeterminada rastrea la primera solicitud cada segundo y el 10 % de las solicitudes adicionales.

La desventaja de definir las reglas localmente es que el objetivo establecido lo aplica cada instancia de la grabadora de forma independiente, en lugar de ser administrado por el servicio de X-Ray. A medida que se implementan más hosts, el porcentaje establecido se multiplica, lo que dificulta el control de la cantidad de datos registrados.

Activado AWS Lambda, no se puede modificar la frecuencia de muestreo. Si un servicio instrumentado llama a su función, Lambda registrará las llamadas que generaron solicitudes muestreadas por ese servicio. Si el rastreo activo está activado y no hay ningún encabezado de rastreo, Lambda toma la decisión de muestreo.

Para configurar reglas de respaldo, indique al SDK de X-Ray para Node.js que cargue reglas de muestreo desde un archivo con `setSamplingRules`.

Example app.js: reglas de muestreo de un archivo

```
var AWSXRay = require('aws-xray-sdk');
AWSXRay.middleware.setSamplingRules('sampling-rules.json');
```

También puede definir las reglas en código y pasarlas a `setSamplingRules` como un objeto.

Example app.js: reglas de muestreo de un objeto

```
var AWSXRay = require('aws-xray-sdk');
var rules = {
  "rules": [ { "description": "Player moves.", "service_name": "*", "http_method": "*",
 "url_path": "/api/move/*", "fixed_target": 0, "rate": 0.05 } ],
  "default": { "fixed_target": 1, "rate": 0.1 },
  "version": 1
  }

AWSXRay.middleware.setSamplingRules(rules);
```

Para utilizar solo reglas locales, llame a `disableCentralizedSampling`.

```
AWSXRay.middleware.disableCentralizedSampling()
```

Registro

Para registrar la salida del SDK, llame a `AWSXRay.setLogger(logger)`, donde `logger` es un objeto que proporciona métodos de registro estándar (`warn`, `info`, etc.).

De forma predeterminada, el SDK registrará los mensajes de error en la consola mediante los métodos estándar del objeto de la consola. El nivel de registro del registrador integrado se puede configurar mediante las variables de entorno `AWS_XRAY_DEBUG_MODE` o `AWS_XRAY_LOG_LEVEL`. Para obtener una lista de valores de nivel de registro válidos, consulte Variables de entorno.

Si desea proporcionar un formato o destino diferente para los registros, puede proporcionar al SDK su propia implementación de la interfaz del registrador, como se muestra a continuación. Se puede utilizar cualquier objeto que implemente esta interfaz. Eso significa que muchas bibliotecas de registro, por ejemplo, Winston, podrían usarse y pasarse directamente al SDK.

Example app.js: registro

```
var AWSXRay = require('aws-xray-sdk');

// Create your own logger, or instantiate one using a library.
var logger = {
  error: (message, meta) => { /* logging code */ },
  warn: (message, meta) => { /* logging code */ },
  info: (message, meta) => { /* logging code */ },
  debug: (message, meta) => { /* logging code */ }
}

AWSXRay.setLogger(logger);
AWSXRay.config([AWSXRay.plugins.EC2Plugin]);
```

Llame a `setLogger` antes de ejecutar otros métodos de configuración, con el fin de asegurarse de capturar la salida de estas operaciones.

Dirección del daemon de X-Ray

Si el daemon de X-Ray escucha en un puerto o host que no sea `127.0.0.1:2000`, puede configurar el SDK de X-Ray para Node.js con el fin de enviar datos de rastreo a otra dirección.

```
AWSXRay.setDaemonAddress('host:port');
```

Puede especificar el host por su nombre o por la dirección IPv4.

Example app.js: dirección del demonio

```
var AWSXRay = require('aws-xray-sdk');
AWSXRay.setDaemonAddress('daemonhost:8082');
```

Si ha configurado el demonio para que escuche en diferentes puertos para TCP y UDP, puede especificar ambos en la configuración de dirección del demonio.

Example app.js: dirección del demonio en puertos independientes

```
var AWSXRay = require('aws-xray-sdk');
AWSXRay.setDaemonAddress('tcp:daemonhost:8082 udp:daemonhost:8083');
```

También puede establecer la dirección del demonio utilizando la `AWS_XRAY_DAEMON_ADDRESS`variable de entorno???.

Variables de entorno

Puede usar variables de entorno para configurar el SDK de X-Ray para Node.js. El SDK admite las siguientes variables.

- `AWS_XRAY_CONTEXT_MISSING`: establezca esta opción en `RUNTIME_ERROR` para generar excepciones cuando el código instrumentado intente registrar datos sin que haya ningún segmento abierto.

  Valores válidos

  - `RUNTIME_ERROR`: lance una excepción de tiempo de ejecución.
  - `LOG_ERROR`: registre un error y continúe (predeterminado).
  - `IGNORE_ERROR`: ignore el error y continúe.

  Se pueden producir errores relativos a segmentos o subsegmentos inexistentes al intentar usar un cliente instrumentado en el código de inicio que se ejecuta cuando no hay ninguna solicitud abierta o en el código que inicia un nuevo subproceso.
- `AWS_XRAY_DAEMON_ADDRESS`: establezca el host y el puerto del oyente del daemon de X-Ray. De forma predeterminada, el SDK utiliza `127.0.0.1:2000` tanto para los datos de rastro (UDP) como para el muestreo (TCP). Use esta variable si ha configurado el daemon para que escuche en un puerto diferente o si se ejecuta en un host diferente.

Formato

- El mismo puerto: *address*:*port*
- Puertos diferentes: tcp:*address*:*port* udp:*address*:*port*

- AWS_XRAY_DEBUG_MODE: establezca este valor en TRUE para configurar el SDK de manera que envíe los registros a la consola, a nivel de debug.
- AWS_XRAY_LOG_LEVEL : establezca un nivel de registro para el registrador predeterminado. Los valores válidos son debug, info, warn, error y silent. Este valor se omite cuando AWS_XRAY_DEBUG_MODE se establece en TRUE.
- AWS_XRAY_TRACING_NAME: establezca el nombre de servicio que el SDK utiliza para los segmentos. Anula el nombre de segmento que se ha establecido en el middleware de Express.

Rastreo de las solicitudes entrantes con el SDK de X-Ray para Node.js

Puede usar el SDK de X-Ray para Node.js para rastrear las solicitudes HTTP entrantes que sus aplicaciones Express y Restify sirven en una instancia EC2 en Amazon EC2 o Amazon AWS Elastic Beanstalk ECS.

El SDK de X-Ray para Node.js proporciona middleware para aplicaciones que utilizan los marcos de trabajo Express y Restify. Cuando añade el middleware de X-Ray a su aplicación, el SDK de X-Ray para Node.js crea un segmento para cada solicitud muestreada. Este segmento incluye el momento, el método y la disposición de la solicitud HTTP. La instrumentación adicional crea subsegmentos en este segmento.

> **Note**
>
> En el AWS Lambda caso de las funciones, Lambda crea un segmento para cada solicitud muestreada. Para obtener más información, consulte AWS Lambda y AWS X-Ray.

Cada segmento tiene un nombre que identifica la aplicación en el mapa de servicio. El nombre del segmento se puede asignar de forma estática o se puede configurar el SDK para que le asigne un nombre dinámico en función del encabezado del host de la solicitud entrante. La nomenclatura dinámica permite agrupar los rastros en función del nombre de dominio de la solicitud y aplicar un nombre predeterminado si el nombre no coincide con el patrón esperado (por ejemplo, si el encabezado del host está falsificado).

> **Solicitudes reenviadas**
>
> Si un equilibrador de carga u otro intermediario reenvía una solicitud a la aplicación, X-Ray toma la IP de cliente del encabezado `X-Forwarded-For` de la solicitud en lugar de tomar la IP de origen del paquete IP. La IP de cliente que se graba para una solicitud reenviada puede estar falsificada, por lo que no se debe confiar en ella.

Cuando se reenvía una solicitud, el SDK crea un campo adicional en el segmento para indicar que se realizó esta acción. Si el segmento contiene el campo `x_forwarded_for` configurado en `true`, el IP del cliente se obtiene a partir del encabezado `X-Forwarded-For` en la solicitud HTTP.

El controlador de mensajes crea un segmento para cada solicitud entrante con un bloque `http` que contiene la siguiente información:

- Método HTTP: GET, POST, PUT, DELETE, etc.
- Dirección del cliente: la dirección IP del cliente que envió la solicitud.
- Código de respuesta: el código de respuesta HTTP para la solicitud finalizada.
- Intervalo: la hora de inicio (cuando se recibió la solicitud) y la hora de finalización (cuando se envió la respuesta).
- Agente del usuario: el `user-agent` de la solicitud.
- Longitud del contenido: la `content-length` de la respuesta.

Secciones

Seguimiento de solicitudes entrantes con Express

Para usar el middleware Express, inicie el cliente del SDK y utilice el middleware que devolvió la función `express.openSegment` antes de definir las rutas que desea usar.

Example app.js - Express

```
var app = express();
```

```
var AWSXRay = require('aws-xray-sdk');
app.use(AWSXRay.express.openSegment('MyApp'));

app.get('/', function (req, res) {
  res.render('index');
});

app.use(AWSXRay.express.closeSegment());
```

Después de definir las rutas, utilice el resultado de `express.closeSegment` tal como se muestra para poder solucionar los errores que el SDK de X-Ray para Node.js haya devuelto.

Seguimiento de solicitudes entrantes con Restify

Para utilizar el middleware Restify, inicialice el cliente del SDK y ejecute `enable`. Indique su servidor de Restify y el nombre de segmento.

Example app.js: restify

```
var AWSXRay = require('aws-xray-sdk');
var AWSXRayRestify = require('aws-xray-sdk-restify');

var restify = require('restify');
var server = restify.createServer();
AWSXRayRestify.enable(server, 'MyApp'));

server.get('/', function (req, res) {
  res.render('index');
});
```

Configuración de una estrategia de nomenclatura de segmentos

AWS X-Ray utiliza un nombre de servicio para identificar la aplicación y distinguirla del resto de aplicaciones, bases de datos, API externas y AWS recursos que utiliza la aplicación. Cuando el SDK de X-Ray genera segmentos para las solicitudes entrantes, registra el nombre del servicio de la aplicación en el campo de nombre del segmento.

El SDK de X-Ray puede nombrar los segmentos utilizando el nombre de host en el encabezado de la solicitud HTTP. Sin embargo, este encabezado se puede falsificar, lo que podría provocar nodos inesperados en el mapa de servicio. Para evitar que el SDK nombre los segmentos de forma

incorrecta debido a que las solicitudes tienen encabezados de host falsificados, debe especificar un nombre predeterminado para las solicitudes entrantes.

Si la aplicación atiende solicitudes de varios dominios, puede configurar el SDK para que utilice una estrategia de nomenclatura dinámica que refleje esto en los nombres de los segmentos. Una estrategia de nomenclatura dinámica permite al SDK usar el nombre de host para las solicitudes que coinciden con un patrón esperado y aplicar el nombre predeterminado a las solicitudes que no coincidan.

Por ejemplo, es posible que tenga una sola aplicación que atienda solicitudes a tres subdominios: `www.example.com`, `api.example.com` y `static.example.com`. Puede usar una estrategia de nomenclatura dinámica con el patrón `*.example.com` para identificar los segmentos de cada subdominio con un nombre diferente, lo que da como resultado tres nodos de servicio en el mapa de servicio. Si su aplicación recibe solicitudes con un nombre de host que no coincide con el patrón, verá un cuarto nodo en el mapa de servicio con el nombre alternativo que especifique.

Si desea utilizar el mismo nombre para todos los segmentos de solicitud, especifique el nombre de la aplicación cuando inicie el middleware, tal y como se muestra en las secciones anteriores.

> **Note**
>
> Puede anular el nombre de servicio predeterminado que ha definido en el código mediante la `AWS_XRAY_TRACING_NAME`variable de entorno???.

Una estrategia de nomenclatura dinámica define un patrón con el que deben coincidir los nombres de host y un nombre predeterminado que se utiliza si el nombre de host de la solicitud HTTP no coincide con el patrón. Para nombrar los segmentos dinámicamente, use `AWSXRay.middleware.enableDynamicNaming`.

Example app.js: nombres de segmentos dinámicos

Si el nombre de host de la solicitud coincide con el patrón `*.example.com`, utilice el nombre de host. De lo contrario, utilice `MyApp`.

```
var app = express();

var AWSXRay = require('aws-xray-sdk');
app.use(AWSXRay.express.openSegment('MyApp'));
AWSXRay.middleware.enableDynamicNaming('*.example.com');
```

```
app.get('/', function (req, res) {
  res.render('index');
});

app.use(AWSXRay.express.closeSegment());
```

Rastreo de llamadas al AWS SDK con el SDK de X-Ray para Node.js

Cuando la aplicación realiza llamadas Servicios de AWS para almacenar datos, escribir en una cola o enviar notificaciones, el SDK de X-Ray para Node.js rastrea las llamadas en sentido descendente en subsegmentos. El Servicios de AWS rastreo y los recursos a los que accede dentro de esos servicios (por ejemplo, un bucket de Amazon S3 o una cola de Amazon SQS) aparecen como nodos descendentes en el mapa de rastreo de la consola X-Ray.

Clientes del AWS SDK de instrumentos que se crean mediante la AWS SDK for JavaScript V2 o la V3.AWS SDK for JavaScript Cada versión AWS del SDK proporciona diferentes métodos para instrumentar AWS los clientes del SDK.

> **Note**
>
> Actualmente, el AWS X-Ray SDK para Node.js devuelve menos información de segmentos al instrumentar los clientes de la AWS SDK for JavaScript V3, en comparación con la instrumentación de los clientes de la V2. Por ejemplo, los subsegmentos que representan llamadas a DynamoDB no devolverán el nombre de la tabla. Si necesita esta información de segmento en sus trazas, considere la posibilidad de utilizar la V2. AWS SDK for JavaScript

AWS SDK for JavaScript V2

Puede instrumentar todos los clientes AWS del SDK V2 empaquetando la sentencia `aws-sdk` require en una llamada a`AWSXRay.captureAWS`.

Example app.js: instrumentación con el SDK de AWS

```
const AWS = AWSXRay.captureAWS(require('aws-sdk'));
```

Para instrumentar a clientes individuales, incluye tu cliente del AWS SDK en una llamada a`AWSXRay.captureAWSClient`. Por ejemplo, para instrumentar un cliente de `AmazonDynamoDB`:

Example app.js - Instrumentación de clientes de DynamoDB

```
    const AWSXRay = require('aws-xray-sdk');
...
    const ddb = AWSXRay.captureAWSClient(new AWS.DynamoDB());
```

> **Warning**
>
> No use `captureAWS` y `captureAWSClient` conjuntamente. Esto dará lugar a subsegmentos duplicados.

Si quieres usar TypeScriptmódulos ECMAScript (ESM) para cargar tu JavaScript código, usa el siguiente ejemplo para importar bibliotecas:

Example app.js: instrumentación del SDK AWS

```
import * as AWS from 'aws-sdk';
import * as AWSXRay from 'aws-xray-sdk';
```

Para instrumentar ESM AWS a todos los clientes, utilice el siguiente código:

Example app.js: instrumentación AWS del SDK

```
import * as AWS from 'aws-sdk';
import * as AWSXRay from 'aws-xray-sdk';
const XRAY_AWS = AWSXRay.captureAWS(AWS);
const ddb = new XRAY_AWS.DynamoDB();
```

Para todos los servicios, puede ver el nombre de la API a la que se llama en la consola de X-Ray. Para un subconjunto de servicios, el SDK de X-Ray agrega información al segmento para proporcionar una mayor granularidad en el mapa de servicio.

Por ejemplo, cuando realiza una llamada con un cliente instrumentado de DynamoDB, el SDK agrega el nombre de tabla al segmento para las llamadas que se dirigen a una tabla. En la consola, cada tabla aparece como nodo independiente en el mapa de servicio, con un nodo genérico de DynamoDB para las llamadas que no se dirigen a una tabla.

Example Subsegmento para una llamada a DynamoDB con el fin de guardar un elemento

```
{
```

```
  "id": "24756640c0d0978a",
  "start_time": 1.480305974194E9,
  "end_time": 1.4803059742E9,
  "name": "DynamoDB",
  "namespace": "aws",
  "http": {
    "response": {
      "content_length": 60,
      "status": 200
    }
  },
  "aws": {
    "table_name": "scorekeep-user",
    "operation": "UpdateItem",
    "request_id": "UBQNSO5AEM8T4FDA4RQDEB94OVTDRVV4K4HIRGVJF66Q9ASUAAJG",
  }
}
```

Cuando accede a recursos designados, las llamadas a los siguientes servicios crean nodos adicionales en el mapa de servicio. Las llamadas que no están dirigidas a recursos concretos crean un nodo genérico en el servicio.

- Amazon DynamoDB: nombre de tabla
- Amazon Simple Storage Service: nombre de bucket y de clave
- Amazon Simple Queue Service: nombre de cola

AWS SDK for JavaScript V3

La AWS SDK for JavaScript V3 es modular, por lo que su código solo carga los módulos que necesita. Por este motivo, no es posible instrumentar todos los clientes AWS del SDK, ya que la V3 no admite este método. `captureAWS`

Si quieres usar TypeScript los módulos ECMAScript (ESM) para cargar tu JavaScript código, puedes usar el siguiente ejemplo para importar bibliotecas:

```
import * as AWS from 'aws-sdk';
import * as AWSXRay from 'aws-xray-sdk';
```

Instrumente cada cliente AWS del SDK mediante el método. `AWSXRay.captureAWSv3Client` Por ejemplo, para instrumentar un cliente de `AmazonDynamoDB`:

Example app.js: instrumentación de clientes de DynamoDB mediante la V3 del SDK para Javascript

```
    const AWSXRay = require('aws-xray-sdk');
    const { DynamoDBClient } = require("@aws-sdk/client-dynamodb");
...
    const ddb = AWSXRay.captureAWSv3Client(new DynamoDBClient({ region:
 "region" }));
```

Cuando se utiliza la AWS SDK for JavaScript V3, actualmente no se devuelven metadatos como el nombre de la tabla, el nombre del bucket y la clave o el nombre de la cola y, por lo tanto, el mapa de rastreo no contendrá nodos discretos para cada recurso nombrado, como ocurre cuando se instrumentan los clientes del AWS SDK mediante la V2. AWS SDK for JavaScript

Example Subsegmento para una llamada a DynamoDB para guardar un elemento, cuando se utiliza la V3 AWS SDK for JavaScript

```
{
  "id": "24756640c0d0978a",
  "start_time": 1.480305974194E9,
  "end_time": 1.4803059742E9,
  "name": "DynamoDB",
  "namespace": "aws",
  "http": {
    "response": {
      "content_length": 60,
      "status": 200
    }
  },
  "aws": {
    "operation": "UpdateItem",
    "request_id": "UBQNSO5AEM8T4FDA4RQDEB94OVTDRVV4K4HIRGVJF66Q9ASUAAJG",
  }
}
```

Rastreo de llamadas a servicios web HTTP posteriores utilizando el SDK de X-Ray para Node.js

Cuando su aplicación realiza llamadas a microservicios o a API de HTTP públicas, puede utilizar el cliente del SDK de X-Ray para Node.js para instrumentar dichas llamadas y añadir la API al gráfico de servicios como un servicios posterior.

Pase su cliente `http` o `https` al método `captureHTTPs` del SDK de X-Ray para Node.js con el fin de rastrear llamadas salientes.

> **Note**
>
> Las llamadas que utilizan bibliotecas de solicitudes HTTP de terceros, como Axios o Superagent, son compatibles a través de la API `captureHTTPsGlobal()` y se seguirán rastreando cuando utilicen el módulo `http` nativo.

Example app.js: cliente HTTP

```
var AWSXRay = require('aws-xray-sdk');
var http = AWSXRay.captureHTTPs(require('http'));
```

Para habilitar el rastreo en todos los clientes HTTP, llame a `captureHTTPsGlobal` antes de cargar `http`.

Example app.js: cliente HTTP (global)

```
var AWSXRay = require('aws-xray-sdk');
AWSXRay.captureHTTPsGlobal(require('http'));
var http = require('http');
```

Cuando se instrumenta una llamada a una API web posterior, el SDK de X-Ray para Node.js registra un subsegmento que contiene información acerca de la solicitud HTTP y la respuesta. X-Ray utiliza el subsegmento para generar un segmento inferido de la API remota.

Example Subsegmento para una llamada HTTP posterior

```
{
```

```
  "id": "004f72be19cddc2a",
  "start_time": 1484786387.131,
  "end_time": 1484786387.501,
  "name": "names.example.com",
  "namespace": "remote",
  "http": {
    "request": {
      "method": "GET",
      "url": "https://names.example.com/"
    },
    "response": {
      "content_length": -1,
      "status": 200
    }
  }
}
```

Example Segmento inferido para una llamada HTTP posterior

```
{
  "id": "168416dc2ea97781",
  "name": "names.example.com",
  "trace_id": "1-62be1272-1b71c4274f39f122afa64eab",
  "start_time": 1484786387.131,
  "end_time": 1484786387.501,
  "parent_id": "004f72be19cddc2a",
  "http": {
    "request": {
      "method": "GET",
      "url": "https://names.example.com/"
    },
    "response": {
      "content_length": -1,
      "status": 200
    }
  },
  "inferred": true
}
```

Rastreo de consultas SQL con el SDK de X-Ray para Node.js

Instrumente las consultas de base de datos SQL incluyendo su cliente SQL en el método del cliente de SDK de X-Ray para Node.js correspondiente.

- PostgreSQL – `AWSXRay.capturePostgres()`

```
var AWSXRay = require('aws-xray-sdk');
var pg = AWSXRay.capturePostgres(require('pg'));
var client = new pg.Client();
```

- MySQL – `AWSXRay.captureMySQL()`

```
var AWSXRay = require('aws-xray-sdk');
var mysql = AWSXRay.captureMySQL(require('mysql'));
...
var connection = mysql.createConnection(config);
```

Cuando usa un cliente instrumentado para realizar consultas SQL, el SDK de X-Ray para Node.js registra información acerca de la conexión y consultas en un subsegmento.

Inclusión de datos adicionales en subsegmentos SQL

Puede agregar información adicional a los subsegmentos generados para consultas SQL, siempre que se asigne a un campo SQL con permiso. Por ejemplo, para registrar la cadena de consultas SQL saneada en un subsegmento, puede agregarla directamente al objeto SQL del subsegmento.

Example Asignar SQL al subsegmento

```
    const queryString = 'SELECT * FROM MyTable';
connection.query(queryString, ...);

// Retrieve the most recently created subsegment
const subs = AWSXRay.getSegment().subsegments;

if (subs & & subs.length > 0) {
  var sqlSub = subs[subs.length - 1];
  sqlSub.sql.sanitized_query = queryString;
}
```

Para obtener una lista completa de campos SQL con permiso, consulte Consultas SQL en la Guía para desarrolladores de AWS X-Ray .

Generación de subsegmentos personalizados con el SDK de X-Ray para Node.js

Los subsegmentos amplían el segmento de un rastro con detalles sobre el trabajo realizado para atender una solicitud. Cada vez que usted realiza una llamada con un cliente instrumentado, el SDK de X-Ray registra la información generada en un subsegmento. Puede crear subsegmentos adicionales para agrupar otros subsegmentos, medir el rendimiento de una sección de código o registrar anotaciones y metadatos.

Subsegmentos Express personalizados

Para crear un subsegmento personalizado para una función que realiza llamadas a servicios posteriores, utilice la función `captureAsyncFunc`.

Example app.js: subsegmentos personalizados Express

```
var AWSXRay = require('aws-xray-sdk');

app.use(AWSXRay.express.openSegment('MyApp'));

app.get('/', function (req, res) {
  var host = 'api.example.com';

  AWSXRay.captureAsyncFunc('send', function(subsegment) {
    sendRequest(host, function() {
      console.log('rendering!');
      res.render('index');
      subsegment.close();
    });
  });
});

app.use(AWSXRay.express.closeSegment());

function sendRequest(host, cb) {
  var options = {
    host: host,
    path: '/',
  };

  var callback = function(response) {
    var str = '';

    response.on('data', function (chunk) {
```

```
      str += chunk;
    });

    response.on('end', function () {
      cb();
    });
  }

  http.request(options, callback).end();
};
```

En este ejemplo, la aplicación crea un subsegmento personalizado denominado `send` para realizar llamadas a la función `sendRequest`. `captureAsyncFunc` transfiere un subsegmento que debe cerrar dentro de la función de devolución de llamada cuando se completen las llamadas asíncronas que realiza.

Para las funciones síncronas, puede utilizar la función `captureFunc`, la cual cierra de forma automática el subsegmento en cuanto el bloque de funciones termina de ejecutarse.

Cuando crea un subsegmento dentro de un segmento o de otro subsegmento, el SDK de X-Ray para Node.js genera un ID para dicho subsegmento y registra la hora de inicio y la hora de finalización.

Example Subsegmentos con metadatos

```
"subsegments": [{
  "id": "6f1605cd8a07cb70",
  "start_time": 1.480305974194E9,
  "end_time": 1.4803059742E9,
  "name": "Custom subsegment for UserModel.saveUser function",
  "metadata": {
    "debug": {
      "test": "Metadata string from UserModel.saveUser"
    }
  },
```

Subsegmentos personalizados de Lambda

El SDK está configurado para crear automáticamente un segmento de fachada de marcador de posición cuando detecta que se está ejecutando en Lambda. Para crear un subsegmento básico, que creará un único `AWS::Lambda::Function` nodo en el mapa de trazas de X-Ray, llame al segmento de fachada y reutilícelo. Si crea manualmente un nuevo segmento con un nuevo ID

(mientras comparte el ID de registro de seguimiento, el ID principal y la decisión de muestreo) podrá enviar un nuevo segmento.

Example app.js - subsegmentos personalizados manuales

```
const segment = AWSXRay.getSegment(); //returns the facade segment
const subsegment = segment.addNewSubsegment('subseg');
...
subsegment.close();
//the segment is closed by the SDK automatically
```

Adición de anotaciones y metadatos a los segmentos con el SDK de X-Ray para Node.js

Puede usar anotaciones y metadatos para registrar información adicional sobre las solicitudes, el entorno o la aplicación. Puede añadir anotaciones y metadatos a los segmentos que crea el SDK de X-Ray o a los subsegmentos personalizados que cree usted mismo.

Las anotaciones son pares de clave-valor con valores de cadena, numéricos o booleanos. Las anotaciones se indexan para su uso con expresiones de filtro. Utilice anotaciones para registrar los datos que desee utilizar para agrupar rastros en la consola o cuando llame a la API de `GetTraceSummaries`.

Los metadatos son pares de clave-valor con valores de cualquier tipo, por ejemplo objetos y listas, pero que no se indexan para utilizarlos con expresiones de filtro. Utilice los metadatos para registrar datos adicionales que desee almacenar en el rastro, pero que no necesite usar para hacer búsquedas.

Además de anotaciones y metadatos, también puede registrar cadenas de ID de usuario en los segmentos. Los identificadores de usuario se registran en un campo aparte en segmentos y se indexan para su uso con la búsqueda.

Secciones

- Registro de anotaciones con el SDK de X-Ray para Node.js
- Registro de metadatos con el SDK de X-Ray para Node.js
- Registro de ID de usuario con el SDK de X-Ray para Node.js

Registro de anotaciones con el SDK de X-Ray para Node.js

Utilice anotaciones para registrar información sobre segmentos o subsegmentos que desee indexar para las búsquedas.

Requisitos de anotación

- Teclas: la clave de una anotación de X-Ray puede tener hasta 500 caracteres alfanuméricos. No puede utilizar espacios ni símbolos distintos del símbolo de subrayado (_).
- Valores: el valor de una anotación de X-Ray puede tener hasta 1000 caracteres Unicode.
- Número de anotaciones: puede utilizar hasta 50 anotaciones por traza.

Para registrar anotaciones

1. Obtenga una referencia al segmento o subsegmento actual.

```
var AWSXRay = require('aws-xray-sdk');
...
var document = AWSXRay.getSegment();
```

2. Llame a `addAnnotation` con una clave de cadena y un valor booleano, numérico o de cadena.

```
document.addAnnotation("mykey", "my value");
```

El SDK registra las anotaciones como pares de clave-valor en un objeto `annotations` del documento de segmento. Si llama dos veces a `addAnnotation` con la misma clave, se sobrescriben los valores previamente registrados en ese segmento o subsegmento.

Para encontrar rastros que tengan anotaciones con valores específicos, utilice la palabra clave `annotations.key` en una expresión de filtro.

Example app.js: anotaciones

```
var AWS = require('aws-sdk');
var AWSXRay = require('aws-xray-sdk');
var ddb = AWSXRay.captureAWSClient(new AWS.DynamoDB());
...
app.post('/signup', function(req, res) {
    var item = {
```

```
        'email': {'S': req.body.email},
        'name': {'S': req.body.name},
        'preview': {'S': req.body.previewAccess},
        'theme': {'S': req.body.theme}
    };

    var seg = AWSXRay.getSegment();
    seg.addAnnotation('theme', req.body.theme);

    ddb.putItem({
      'TableName': ddbTable,
      'Item': item,
      'Expected': { email: { Exists: false } }
  }, function(err, data) {
...
```

Registro de metadatos con el SDK de X-Ray para Node.js

Utilice los metadatos para registrar información sobre segmentos o subsegmentos que no necesite indexar para las búsquedas. Los valores de metadatos pueden ser cadenas, números, booleanos o cualquier otro objeto que se pueda serializar en un objeto o matriz JSON.

Para registrar metadatos

1. Obtenga una referencia al segmento o subsegmento actual.

   ```
   var AWSXRay = require('aws-xray-sdk');
   ...
   var document = AWSXRay.getSegment();
   ```

2. Llame a `addMetadata` con una clave de cadena, un valor booleano, numérico, de cadena o de objeto y un espacio de nombres de cadena.

   ```
   document.addMetadata("my key", "my value", "my namespace");
   ```

   o

   Llame a `addMetadata` con solo una clave y un valor.

   ```
   document.addMetadata("my key", "my value");
   ```

Si no especifica un espacio de nombres, el SDK utiliza `default`. Si llama dos veces a `addMetadata` con la misma clave, se sobrescriben los valores previamente registrados en ese segmento o subsegmento.

Registro de ID de usuario con el SDK de X-Ray para Node.js

Registre identificadores de usuario en segmentos de solicitud para identificar al usuario que envió la solicitud. Esta operación no es compatible con AWS Lambda las funciones porque los segmentos de los entornos Lambda son inmutables. La llamada `setUser` solo se puede efectuar con segmentos, no con subsegmentos.

Para registrar identificadores de usuario

1. Obtenga una referencia al segmento o subsegmento actual.

```
var AWSXRay = require('aws-xray-sdk');
...
var document = AWSXRay.getSegment();
```

2. Llame a `setUser()` con un ID de cadena del usuario que envió la solicitud.

```
var user = 'john123';

AWSXRay.getSegment().setUser(user);
```

Puede llamar a `setUser` para registrar el ID de usuario en cuanto la aplicación rápida comience a procesar una solicitud. Si va a utilizar el segmento únicamente para establecer el ID de usuario, puede encadenar las llamadas en una sola línea.

Example app.js: ID de usuario

```
var AWS = require('aws-sdk');
var AWSXRay = require('aws-xray-sdk');
var uuidv4 = require('uuid/v4');
var ddb = AWSXRay.captureAWSClient(new AWS.DynamoDB());
...
    app.post('/signup', function(req, res) {
    var userId = uuidv4();
    var item = {
        'userId': {'S': userId},
```

```
        'email': {'S': req.body.email},
        'name': {'S': req.body.name}
    };

    var seg = AWSXRay.getSegment().setUser(userId);

    ddb.putItem({
      'TableName': ddbTable,
      'Item': item,
      'Expected': { email: { Exists: false } }
  }, function(err, data) {
...
```

Para buscar rastros de un ID de usuario, utilice la palabra clave `user` en una expresión de filtro.

Instrumentación de su aplicación con Python

Hay dos formas de instrumentar su Python aplicación para enviar trazas a X-Ray:

- AWS Distro for OpenTelemetry Python: una AWS distribución que proporciona un conjunto de bibliotecas de código abierto para enviar métricas y rastreos correlacionados a varias soluciones de AWS monitoreo, incluidas Amazon y Amazon OpenSearch Service CloudWatch AWS X-Ray, a través de AWS Distro for Collector. OpenTelemetry
- AWS X-Ray SDK para Python: conjunto de bibliotecas para generar y enviar trazas a X-Ray mediante el daemon X-Ray.

Para obtener más información, consulte Cómo elegir entre los AWS SDK Distro for OpenTelemetry y X-Ray.

AWS Distro para OpenTelemetry Python

Con AWS Distro for OpenTelemetry (ADOT)Python, puede instrumentar sus aplicaciones una vez y enviar métricas y rastreos correlacionados a varias soluciones de AWS monitoreo CloudWatch, incluidas Amazon AWS X-Ray y Amazon Service. OpenSearch El uso de X-Ray con ADOT requiere dos componentes: un OpenTelemetry SDK habilitado para su uso con X-Ray y una AWS Distro for OpenTelemetry Collector habilitada para su uso con X-Ray. ADOT Python incluye soporte de instrumentación automática, lo que permite a su aplicación enviar trazas sin cambios de código.

Para empezar, consulta la documentación en la AWS Distro. OpenTelemetry Python

Para obtener más información sobre el uso de la AWS distribución OpenTelemetry con AWS X-Ray y otros Servicios de AWS, consulta la sección AWS Distro for OpenTelemetry o la AWS Distro para ver la documentación. OpenTelemetry

Para obtener más información sobre el soporte y el uso de idiomas, consulta AWS Observabilidad en. GitHub

AWS X-Ray SDK para Python

El SDK de X-Ray para Python es una biblioteca para aplicaciones Python web que proporciona clases y métodos para generar y enviar datos de rastreo al daemon de X-Ray. Los datos de rastreo incluyen información sobre las solicitudes HTTP entrantes atendidas por la aplicación y las llamadas que la aplicación realiza a los servicios descendentes mediante el AWS SDK, los clientes HTTP o un conector de base de datos SQL. También puede crear segmentos de forma manual y agregar información de depuración en anotaciones y metadatos.

Puede descargar el SDK con `pip`.

```
$ pip install aws-xray-sdk
```

> **Note**
>
> El SDK de X-Ray para Python es un proyecto de código abierto. Puedes seguir el proyecto y enviar las incidencias y solicitudes de cambios en GitHub: github.com/aws/ aws-xray-sdk-python

Si usa Django o Flask, empiece agregando el middleware del SDK a la aplicación para rastrear las solicitudes entrantes. El middleware crea un segmento para cada solicitud rastreada y lo completa cuando se envía la respuesta. Mientras el segmento está abierto, puede utilizar los métodos del cliente del SDK para añadir información al segmento y crear subsegmentos para rastrear llamadas posteriores. El SDK también registra automáticamente las excepciones que produce su aplicación mientras el segmento está abierto. Para otras aplicaciones, puede crear segmentos manualmente.

En el caso de las funciones de Lambda llamadas por una aplicación o un servicio instrumentados, Lambda lee el encabezado de rastreo y rastrea automáticamente las solicitudes muestreadas. Para otras funciones, puede configurar Lambda con el fin de muestrear y rastrear las solicitudes entrantes. En cualquier caso, Lambda crea el segmento y se lo proporciona al SDK de X-Ray.

> **Note**
>
> En Lambda, el SDK de X-Ray es opcional. Si no lo usa en su función, el mapa de servicio seguirá incluyendo un nodo para el servicio de Lambda y uno para cada función de Lambda. Al añadir el SDK, puede instrumentar el código de función para añadir subsegmentos al segmento de función registrado por Lambda. Para obtener más información, consulte AWS Lambda y AWS X-Ray.

Consulte Entorno de trabajo para ver un ejemplo de Python función instrumentada en Lambda.

A continuación, utilice el SDK de X-Ray para Python con el fin de instrumentar llamadas posteriores aplicando parches a las bibliotecas de su aplicación. El SDK admite las siguientes bibliotecas.

Bibliotecas compatibles

- `botocore`, `boto3` — Clientes de instrumentos AWS SDK for Python (Boto) .
- `pynamodb`: instrumente la versión de PynamoDB del cliente de Amazon DynamoDB.
- `aiobotocore`, `aioboto3`: instrumente las versiones integradas en asyncio de los clientes del SDK para Python.
- `requests`, `aiohttp`: instrumente clientes HTTP de alto nivel.
- `httplib`, `http.client`: instrumente los clientes HTTP de bajo nivel y las bibliotecas de más alto nivel que los utilizan.
- `sqlite3`: instrumente los clientes de SQLite.
- `mysql-connector-python`: instrumente los clientes de MySQL.
- `pg8000`: instrumente la interfaz PostgreSQL Pure-Python.
- `psycopg2`: instrumente el adaptador de base de datos PostgreSQL.
- `pymongo`: instrumente clientes de MongoDB.
- `pymysql`— Clientes basados en Instrument PyMy SQL y MariaDB.

Cada vez que la aplicación realiza llamadas a AWS una base de datos SQL u otros servicios HTTP, el SDK registra la información sobre la llamada en un subsegmento. Servicios de AWS y los recursos a los que accedes desde los servicios aparecen como nodos descendentes en el mapa de rastreo para ayudarte a identificar los errores y los problemas de limitación en las conexiones individuales.

En cuanto empiece a utilizar el SDK, personalice su comportamiento configurando la grabadora y el controlador y el middleware. Puede añadir complementos para registrar los datos sobre los recursos informáticos que ejecutan su aplicación, personalizar el comportamiento de muestreo mediante la definición de reglas de muestreo y definir el nivel de log para ver más o menos información del SDK en los logs de las aplicaciones.

Registre información adicional acerca de las solicitudes y el trabajo que la aplicación realiza en anotaciones y metadatos. Las anotaciones son pares sencillos de clave-valor que se indexan para su uso con expresiones de filtro para poder buscar rastros que contengan datos específicos. Las entradas de metadatos son menos restrictivas y pueden registrar objetos y matrices completos, es decir, todo lo que se pueda serializar en JSON.

> **Anotaciones y metadatos**
>
> Las anotaciones y los metadatos son texto arbitrario que se agrega a los segmentos con el SDK de X-Ray. Las anotaciones se indexan para su uso con expresiones de filtro. Los metadatos no se indexan pero se pueden ver en el segmento sin procesar con la consola o la API de X-Ray. Cualquier persona a la que conceda acceso de lectura a X-Ray puede ver estos datos.

Cuando tenga muchos clientes instrumentados en su código, un único segmento de solicitud puede contener un gran número de subsegmentos, uno para cada llamada realizada con un cliente instrumentado. Puede organizar y agrupar los subsegmentos incluyendo las llamadas del cliente en subsegmentos personalizados. Puede crear un subsegmento personalizado para toda una función o cualquier sección de código. A continuación, puede registrar metadatos y anotaciones en el subsegmento en lugar de escribir todo en el segmento principal.

Para obtener documentación de referencia sobre las clases y los métodos del SDK, consulta el AWS X-Ray SDK para Python ver la referencia sobre las API.

Requisitos

El SDK de X-Ray para Python es compatible con los siguientes lenguajes y versiones de biblioteca.

- Python: 2.7, 3.4 y posteriores
- Django: 1.10 y posteriores
- Flask: 0.10 y posteriores
- aiohttp: 2.3.0 y posteriores

- AWS SDK for Python (Boto): 1.4.0 y posteriores
- botocore: 1.5.0 y posteriores
- enum: 0.4.7 y versiones posteriores, para Python las versiones 3.4.0 y anteriores
- jsonpickle: 1.0.0 y posteriores
- setuptools: 40.6.3 y posteriores
- wrapt: 1.11.0 y posteriores

Administración de dependencias

El SDK de X-Ray para Python está disponible en `pip`.

- Paquete: `aws-xray-sdk`

Añada el SDK como una dependencia en su archivo `requirements.txt`.

Example requirements.txt

```
aws-xray-sdk==2.4.2
boto3==1.4.4
botocore==1.5.55
Django==1.11.3
```

Si utiliza Elastic Beanstalk para implementar su aplicación, Elastic Beanstalk instala todos los paquetes en `requirements.txt` de forma automática.

Configuración del SDK de X-Ray para Python

El SDK de X-Ray para Python tiene una clase denominada `xray_recorder` que proporciona la grabadora global. Puede configurar la grabadora global para que personalice el middleware que crea los segmentos para las llamadas HTTP entrantes.

Secciones

- Complementos del servicio
- Reglas de muestreo
- Registro
- Configuración de la grabadora en código
- Configuración de la grabadora con Django

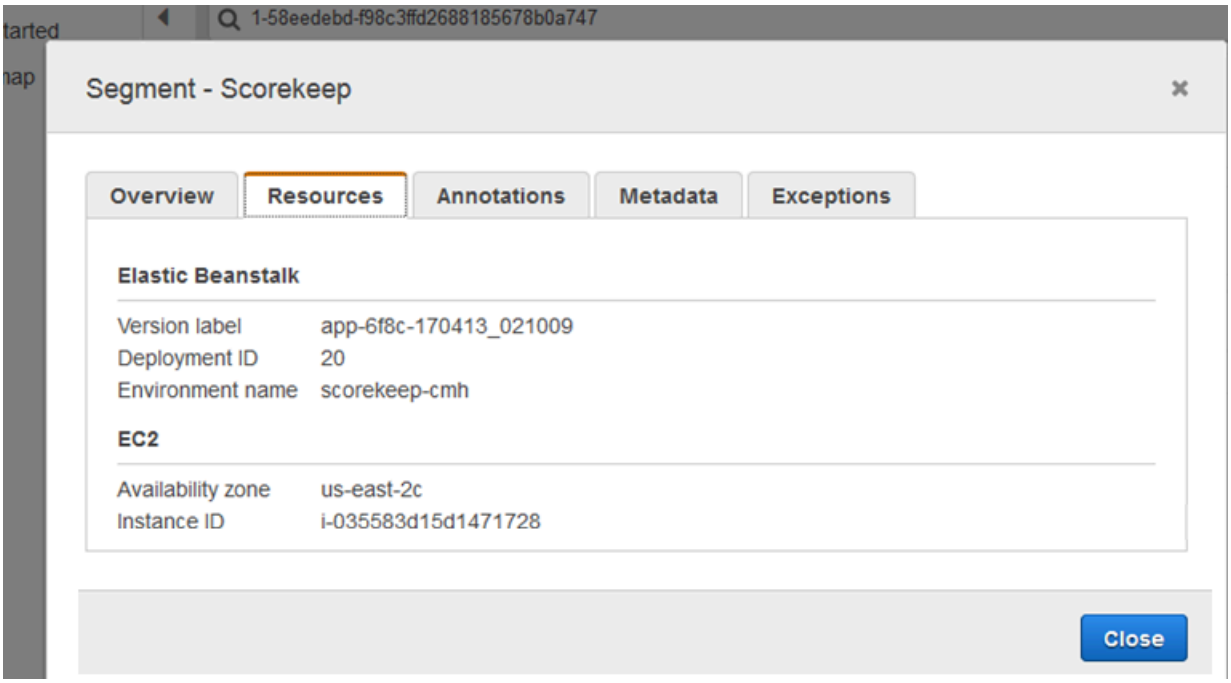
- Variables de entorno

Complementos del servicio

Utilice `plugins` para registrar información sobre el servicio que aloja la aplicación.

Complementos

- Amazon EC2: `EC2Plugin` añade el ID de instancia, la zona de disponibilidad y el grupo de registros de CloudWatch.
- Elastic Beanstalk: `ElasticBeanstalkPlugin` añade el nombre de entorno, la etiqueta de versión y el ID de implementación.
- Amazon ECS: `ECSPlugin` agrega el ID de contenedor.



Para utilizar un complemento, llame a `configure` en el `xray_recorder`.

```
from aws_xray_sdk.core import xray_recorder
from aws_xray_sdk.core import patch_all

xray_recorder.configure(service='My app')
plugins = ('ElasticBeanstalkPlugin', 'EC2Plugin')
xray_recorder.configure(plugins=plugins)
```

```
patch_all()
```

> **Note**
>
> Dado que se transfieren `plugins` como tupla, asegúrese de incluir una `,` después al especificar un único complemento. Por ejemplo, `plugins = ('EC2Plugin',)`

También puede utilizar las variables de entorno, que tienen prioridad frente a los valores establecidos en código, para configurar la grabadora.

Configure los complementos antes de aplicar parches en las bibliotecas para registrar las llamadas posteriores.

El SDK también usa la configuración del complemento para establecer el campo `origin` en el segmento. Eso indica el tipo de recurso de AWS que ejecuta la aplicación. Cuando utiliza varios complementos, el SDK utiliza el siguiente orden de resolución para determinar el origen: ElasticBeanstalk > EKS > ECS > EC2.

Reglas de muestreo

El SDK utiliza las reglas de muestreo que define el usuario en la consola de X-Ray para determinar qué solicitudes registrar. La regla predeterminada rastrea la primera solicitud cada segundo y el 5 % de las solicitudes adicionales de todos los servicios que envían rastros a X-Ray. Cree reglas adicionales en la consola de X-Ray para personalizar la cantidad de datos registrados para cada una de sus aplicaciones.

El SDK aplica las reglas personalizadas en el orden en que se definen. Si una solicitud coincide con varias reglas personalizadas, el SDK solo aplica la primera regla.

> **Note**
>
> Si el SDK no puede comunicarse con X-Ray para obtener las reglas de muestreo, vuelve a una regla local predeterminada de la primera solicitud cada segundo y del 5 % de las solicitudes adicionales por host. Eso puede ocurrir si el host no tiene permiso para llamar a las API de muestreo o no puede conectarse al daemon de X-Ray, que actúa como proxy TCP para las llamadas a las API realizadas por el SDK.

También puedes configurar el SDK para que cargue las reglas de muestreo desde un documento JSON. El SDK puede usar las reglas locales como respaldo para los casos en que el muestreo de X-Ray no esté disponible, o puede usar las reglas locales exclusivamente.

Example sampling-rules.json

```
{
  "version": 2,
  "rules": [
    {
      "description": "Player moves.",
      "host": "*",
      "http_method": "*",
      "url_path": "/api/move/*",
      "fixed_target": 0,
      "rate": 0.05
    }
  ],
  "default": {
    "fixed_target": 1,
    "rate": 0.1
  }
}
```

En este ejemplo se define una regla personalizada y una regla predeterminada. La regla personalizada aplica un porcentaje de muestreo del 5 % sin un número mínimo de solicitudes de rastreo para las rutas incluidas bajo `/api/move/`. La regla predeterminada rastrea la primera solicitud cada segundo y el 10 % de las solicitudes adicionales.

La desventaja de definir las reglas localmente es que el objetivo establecido lo aplica cada instancia de la grabadora de forma independiente, en lugar de ser administrado por el servicio de X-Ray. A medida que se implementan más hosts, el porcentaje establecido se multiplica, lo que dificulta el control de la cantidad de datos registrados.

En AWS Lambda no puede modificar el porcentaje de muestreo. Si un servicio instrumentado llama a su función, Lambda registrará las llamadas que generaron solicitudes muestreadas por ese servicio. Si el rastreo activo está activado y no hay ningún encabezado de rastreo, Lambda toma la decisión de muestreo.

Para configurar las reglas de muestreo de copia de seguridad, llame a `xray_recorder.configure`, tal y como se muestra en el siguiente ejemplo, donde *`reglas`* es un diccionario de reglas o la ruta absoluta a un archivo JSON que contiene reglas de muestreo.

```
xray_recorder.configure(sampling_rules=rules)
```

Para utilizar solo reglas locales, configure la grabadora con un `LocalSampler`.

```
from aws_xray_sdk.core.sampling.local.sampler import LocalSampler
xray_recorder.configure(sampler=LocalSampler())
```

También puede configurar la grabadora global para deshabilitar el muestreo e instrumentar todas las solicitudes entrantes.

Example main.py: deshabilite el muestreo

```
xray_recorder.configure(sampling=False)
```

Registro

El SDK usa el módulo integrado `logging` de Python con un nivel de registro predeterminado `WARNING`. Obtenga una referencia al registrador para la clase `aws_xray_sdk` y llame `setLevel` en la misma para configurar el nivel de log diferente para la biblioteca y el resto de la aplicación.

Example app.py registro

```
logging.basicConfig(level='WARNING')
logging.getLogger('aws_xray_sdk').setLevel(logging.ERROR)
```

Utilice registros de depuración para identificar problemas como la presencia de subsegmentos sin cerrar al generar subsegmentos de forma manual.

Configuración de la grabadora en código

Hay disponibles ajustes adicionales a partir del método `configure` en `xray_recorder`.

- `context_missing`: establezca esta opción en `LOG_ERROR` para evitar que se produzcan excepciones cuando el código instrumentado intente registrar datos sin que haya ningún segmento abierto.
- `daemon_address`: establezca el host y el puerto del oyente del daemon de X-Ray.

- `service`: establezca un nombre de servicio que el SDK utiliza para los segmentos.
- `plugins`: registre información acerca de los recursos de AWS de su aplicación.
- `sampling`: establezca esta opción en `False` para deshabilitar el muestreo.
- `sampling_rules`: establezca la ruta del archivo JSON que contiene sus reglas de muestreo.

Example main.py: deshabilite excepciones de falta de contexto

```
from aws_xray_sdk.core import xray_recorder

xray_recorder.configure(context_missing='LOG_ERROR')
```

Configuración de la grabadora con Django

Si utiliza el marco de Django, puede utilizar el archivo `settings.py` de Django para configurar opciones en la grabadora global.

- `AUTO_INSTRUMENT` (solo Django): registra subsegmentos para operaciones de representación de plantilla y base de datos integrada.
- `AWS_XRAY_CONTEXT_MISSING`: establezca esta opción en `LOG_ERROR` para evitar que se produzcan excepciones cuando el código instrumentado intente registrar datos sin que haya ningún segmento abierto.
- `AWS_XRAY_DAEMON_ADDRESS`: establezca el host y el puerto del oyente del daemon de X-Ray.
- `AWS_XRAY_TRACING_NAME`: establezca un nombre de servicio que el SDK utiliza para los segmentos.
- `PLUGINS`: registre información acerca de los recursos de AWS de su aplicación.
- `SAMPLING`: establezca esta opción en `False` para deshabilitar el muestreo.
- `SAMPLING_RULES`: establezca la ruta del archivo JSON que contiene sus reglas de muestreo.

Para habilitar la configuración de la grabadora en `settings.py`, añada el middleware de Django a la lista de aplicaciones instaladas.

Example settings.py: aplicaciones instaladas

```
INSTALLED_APPS = [
    ...
    'django.contrib.sessions',
    'aws_xray_sdk.ext.django',
```

```
]
```

Configure los ajustes disponibles en un diccionario denominado `XRAY_RECORDER`.

Example settings.py: aplicaciones instaladas

```
XRAY_RECORDER = {
    'AUTO_INSTRUMENT': True,
    'AWS_XRAY_CONTEXT_MISSING': 'LOG_ERROR',
    'AWS_XRAY_DAEMON_ADDRESS': '127.0.0.1:5000',
    'AWS_XRAY_TRACING_NAME': 'My application',
    'PLUGINS': ('ElasticBeanstalkPlugin', 'EC2Plugin', 'ECSPlugin'),
    'SAMPLING': False,
}
```

Variables de entorno

Puede usar variables de entorno con el fin de configurar el SDK de X-Ray para Python. El SDK admite las siguientes variables:

- `AWS_XRAY_TRACING_NAME`: establezca un nombre de servicio que el SDK utiliza para los segmentos. Anula el nombre de servicio que se establece mediante programación.
- `AWS_XRAY_SDK_ENABLED`: cuando se establece en `false`, deshabilita el SDK. De forma predeterminada, el SDK está habilitado a menos que la variable de entorno esté establecida en false.
  - Cuando está deshabilitado, el grabador global genera automáticamente segmentos y subsegmentos ficticios que no se envían al demonio y se deshabilita la aplicación automática de parches. El middleware se registra como un contenedor en el grabador local. Todos los segmentos y subsegmentos que se generan a través del middleware también se vuelven ficticios.
  - Establezca el valor de `AWS_XRAY_SDK_ENABLED` a través de la variable de entorno o interactuando directamente con el objeto `global_sdk_config` de la biblioteca `aws_xray_sdk`. La configuración de la variable de entorno invalida estas interacciones.
- `AWS_XRAY_DAEMON_ADDRESS`: establezca el host y el puerto del oyente del daemon de X-Ray. De forma predeterminada, el SDK utiliza `127.0.0.1:2000` tanto para rastrear datos (UDP) como para el muestreo (TCP). Use esta variable si ha configurado el daemon para que escuche en un puerto diferente o si se ejecuta en un host diferente.

Formato

- El mismo puerto: *`address`*`:`*`port`*
- Puertos diferentes: `tcp:`*`address`*`:`*`port`* `udp:`*`address`*`:`*`port`*

- `AWS_XRAY_CONTEXT_MISSING`: establezca esta opción en `RUNTIME_ERROR` para generar excepciones cuando el código instrumentado intente registrar datos sin que haya ningún segmento abierto.

  Valores válidos

  - `RUNTIME_ERROR`: lance una excepción de tiempo de ejecución.
  - `LOG_ERROR`: registre un error y continúe (predeterminado).
  - `IGNORE_ERROR`: ignore el error y continúe.

  Se pueden producir errores relativos a segmentos o subsegmentos inexistentes al intentar usar un cliente instrumentado en el código de inicio que se ejecuta cuando no hay ninguna solicitud abierta o en el código que inicia un nuevo subproceso.

Las variables de entorno anulan los valores establecidos en el código.

Rastreo de las solicitudes entrantes con el SDK de X-Ray para middleware de Python

Cuando añade el middleware a su aplicación y configura un nombre de segmento, el SDK de X-Ray para Python crea un segmento para cada solicitud muestreada. Este segmento incluye el momento, el método y la disposición de la solicitud HTTP. La instrumentación adicional crea subsegmentos en este segmento.

El SDK de X-Ray para Python admite el siguiente middleware para instrumentar solicitudes HTTP entrantes:

- Django
- Flask
- Bottle

> **Note**
>
> En el caso de funciones de AWS Lambda, Lambda crea un segmento para cada solicitud muestreada. Para obtener más información, consulte AWS Lambda y AWS X-Ray.

Consulte Entorno de trabajo para ver un ejemplo de una función de Python instrumentada en Lambda.

Para scripts o aplicaciones Python en otros marcos de trabajo, puede crear los segmentos manualmente.

Cada segmento tiene un nombre que identifica la aplicación en el mapa de servicio. El nombre del segmento se puede asignar de forma estática o se puede configurar el SDK para que le asigne un nombre dinámico en función del encabezado del host de la solicitud entrante. La nomenclatura dinámica permite agrupar los rastros en función del nombre de dominio de la solicitud y aplicar un nombre predeterminado si el nombre no coincide con el patrón esperado (por ejemplo, si el encabezado del host está falsificado).

> **Solicitudes reenviadas**
>
> Si un equilibrador de carga u otro intermediario reenvía una solicitud a la aplicación, X-Ray toma la IP de cliente del encabezado `X-Forwarded-For` de la solicitud en lugar de tomar la IP de origen del paquete IP. La IP de cliente que se graba para una solicitud reenviada puede estar falsificada, por lo que no se debe confiar en ella.

Cuando se reenvía una solicitud, el SDK crea un campo adicional en el segmento para indicar que se realizó esta acción. Si el segmento contiene el campo `x_forwarded_for` configurado en `true`, el IP del cliente se obtiene a partir del encabezado `X-Forwarded-For` en la solicitud HTTP.

El middleware crea un segmento para cada solicitud entrante con un bloque `http` que contiene la siguiente información:

- Método HTTP: GET, POST, PUT, DELETE, etc.
- Dirección del cliente: la dirección IP del cliente que envió la solicitud.
- Código de respuesta: el código de respuesta HTTP para la solicitud finalizada.

- Intervalo: la hora de inicio (cuando se recibió la solicitud) y la hora de finalización (cuando se envió la respuesta).
- Agente del usuario: el `user-agent` de la solicitud.
- Longitud del contenido: la `content-length` de la respuesta.

Secciones

Agregar el middleware a su aplicación (Django)

Añada el middleware a la lista `MIDDLEWARE` en su archivo `settings.py`. El middleware de X-Ray debe ser la primera línea de su archivo `settings.py` para garantizar que se registren las solicitudes que fallan en otros middleware.

Example settings.py: SDK de X-Ray para middleware de Python

```
MIDDLEWARE = [
    'aws_xray_sdk.ext.django.middleware.XRayMiddleware',
    'django.middleware.security.SecurityMiddleware',
    'django.contrib.sessions.middleware.SessionMiddleware',
    'django.middleware.common.CommonMiddleware',
    'django.middleware.csrf.CsrfViewMiddleware',
    'django.contrib.auth.middleware.AuthenticationMiddleware',
    'django.contrib.messages.middleware.MessageMiddleware',
    'django.middleware.clickjacking.XFrameOptionsMiddleware'
]
```

Añada la aplicación Django del SDK de X-Ray a la lista `INSTALLED_APPS` de su archivo `settings.py`. Eso permitirá configurar la grabadora de X-Ray durante el inicio de la aplicación.

Example settings.py: aplicación Django del SDK de X-Ray para Python

```
INSTALLED_APPS = [
```

```
    'aws_xray_sdk.ext.django',
    'django.contrib.admin',
    'django.contrib.auth',
    'django.contrib.contenttypes',
    'django.contrib.sessions',
    'django.contrib.messages',
    'django.contrib.staticfiles',
]
```

Configure un nombre de segmento en su `settings.py` archivo.

Example settings.py: nombre de segmento

```
XRAY_RECORDER = {
    'AWS_XRAY_TRACING_NAME': 'My application',
    'PLUGINS': ('EC2Plugin',),
}
```

Esto indica a la grabadora de X-Ray que rastree solicitudes servidas por la aplicación Django con el porcentaje de muestreo predeterminado. Puede configurar la grabadora con el archivo de configuración de Django para aplicar reglas de muestreo personalizadas o cambiar otros ajustes.

> **Note**
>
> Dado que se transfieren `plugins` como tupla, asegúrese de incluir una `,` después al especificar un único complemento. Por ejemplo, `plugins = ('EC2Plugin',)` .

Agregar el middleware a su aplicación (flask)

Para instrumentar su aplicación Flask, en primer lugar configure un nombre de segmento en el `xray_recorder`. A continuación, utilice la función `XRayMiddleware` para aplicar un parche a su aplicación Flask en código.

Example app.py

```
from aws_xray_sdk.core import xray_recorder
from aws_xray_sdk.ext.flask.middleware import XRayMiddleware

app = Flask(__name__)
```

```
xray_recorder.configure(service='My application')
XRayMiddleware(app, xray_recorder)
```

Esto indica a la grabadora de X-Ray que rastree solicitudes servidas por la aplicación Flask con el porcentaje de muestreo predeterminado. Puede configurar la grabadora en código para aplicar reglas de muestreo personalizadas o cambiar otros ajustes.

Agregar el middleware a su aplicación (Bottle)

Para instrumentar su aplicación Bottle, en primer lugar configure un nombre de segmento en el `xray_recorder`. A continuación, utilice la función `XRayMiddleware` para aplicar un parche a su aplicación Bottle en código.

Example app.py

```
from aws_xray_sdk.core import xray_recorder
from aws_xray_sdk.ext.bottle.middleware import XRayMiddleware

app = Bottle()

xray_recorder.configure(service='fallback_name', dynamic_naming='My application')
app.install(XRayMiddleware(xray_recorder))
```

Esto indica a la grabadora de X-Ray que rastree solicitudes servidas por la aplicación Bottle con el porcentaje de muestreo predeterminado. Puede configurar la grabadora en código para aplicar reglas de muestreo personalizadas o cambiar otros ajustes.

Instrumentación manual del código de Python

Si no utiliza Django o Flask, puede crear segmentos manualmente. Puede crear un segmento para cada solicitud entrante o crear segmentos en torno a los clientes HTTP o del SDK de AWS para proporcionar contexto para que la grabadora añada subsegmentos.

Example main.py: instrumentación manual

```
from aws_xray_sdk.core import xray_recorder

# Start a segment
segment = xray_recorder.begin_segment('segment_name')
# Start a subsegment
subsegment = xray_recorder.begin_subsegment('subsegment_name')
```

```
# Add metadata and annotations
segment.put_metadata('key', dict, 'namespace')
subsegment.put_annotation('key', 'value')

# Close the subsegment and segment
xray_recorder.end_subsegment()
xray_recorder.end_segment()
```

Configuración de una estrategia de nomenclatura de segmentos

AWS X-Ray utiliza un nombre de servicio para identificar la aplicación y distinguirla del resto de aplicaciones, bases de datos, API externas y recursos de AWS utilizados por la aplicación. Cuando el SDK de X-Ray genera segmentos para las solicitudes entrantes, registra el nombre del servicio de la aplicación en el campo de nombre del segmento.

El SDK de X-Ray puede nombrar los segmentos utilizando el nombre de host en el encabezado de la solicitud HTTP. Sin embargo, este encabezado se puede falsificar, lo que podría provocar nodos inesperados en el mapa de servicio. Para evitar que el SDK nombre los segmentos de forma incorrecta debido a que las solicitudes tienen encabezados de host falsificados, debe especificar un nombre predeterminado para las solicitudes entrantes.

Si la aplicación atiende solicitudes de varios dominios, puede configurar el SDK para que utilice una estrategia de nomenclatura dinámica que refleje esto en los nombres de los segmentos. Una estrategia de nomenclatura dinámica permite al SDK usar el nombre de host para las solicitudes que coinciden con un patrón esperado y aplicar el nombre predeterminado a las solicitudes que no coincidan.

Por ejemplo, es posible que tenga una sola aplicación que atienda solicitudes a tres subdominios: `www.example.com`, `api.example.com` y `static.example.com`. Puede usar una estrategia de nomenclatura dinámica con el patrón `*.example.com` para identificar los segmentos de cada subdominio con un nombre diferente, lo que da como resultado tres nodos de servicio en el mapa de servicio. Si su aplicación recibe solicitudes con un nombre de host que no coincide con el patrón, verá un cuarto nodo en el mapa de servicio con el nombre alternativo que especifique.

Si desea utilizar el mismo nombre para todos los segmentos de solicitud, especifique el nombre de la aplicación cuando configure la grabadora, como se muestra en las secciones anteriores.

Una estrategia de nomenclatura dinámica define un patrón con el que deben coincidir los nombres de host y un nombre predeterminado que se utiliza si el nombre de host de la solicitud HTTP

no coincide con el patrón. Para nombrar segmentos de forma dinámica en Django, añada la configuración DYNAMIC_NAMING a su archivo settings.py.

Example settings.py: nomenclatura dinámica

```
XRAY_RECORDER = {
    'AUTO_INSTRUMENT': True,
    'AWS_XRAY_TRACING_NAME': 'My application',
    'DYNAMIC_NAMING': '*.example.com',
    'PLUGINS': ('ElasticBeanstalkPlugin', 'EC2Plugin')
}
```

Puede utilizar "*" en el patrón para buscar coincidencia con cualquier cadena o "?" para buscar coincidencias con cualquier carácter único. Para Flask, configure la grabadora en código.

Example main.py: nombre de segmento

```
from aws_xray_sdk.core import xray_recorder
xray_recorder.configure(service='My application')
xray_recorder.configure(dynamic_naming='*.example.com')
```

> **Note**
>
> Puede anular el nombre de servicio predeterminado que ha definido en el código mediante la AWS_XRAY_TRACING_NAMEvariable de entorno???.

Aplicación de parches a bibliotecas para instrumentar llamadas posteriores

Para instrumentar llamadas posteriores, utilice el SDK de X-Ray para Python para aplicar parches a las bibliotecas que utiliza la aplicación. El SDK de X-Ray para Python puede aplicar parches a las siguientes bibliotecas.

Bibliotecas compatibles

- botocore, boto3: instrumente clientes de AWS SDK for Python (Boto).
- pynamodb: instrumente la versión de PynamoDB del cliente de Amazon DynamoDB.
- aiobotocore, aioboto3: instrumente las versiones integradas en asyncio de los clientes del SDK para Python.
- requests, aiohttp: instrumente clientes HTTP de alto nivel.

- `httplib`, `http.client`: instrumente los clientes HTTP de bajo nivel y las bibliotecas de más alto nivel que los utilizan.
- `sqlite3`: instrumente los clientes de SQLite.
- `mysql-connector-python`: instrumente los clientes de MySQL.
- `pg8000`: instrumente la interfaz PostgreSQL Pure-Python.
- `psycopg2`: instrumente el adaptador de base de datos PostgreSQL.
- `pymongo`: instrumente clientes de MongoDB.
- `pymysql`: instrumente clientes basados en PyMySQL para MySQL y MariaDB.

Al utilizar una biblioteca con parches, el SDK de X-Ray para Python crea un subsegmento para la llamada y registra información desde la solicitud y la respuesta. Debe haber un segmento disponible para que el SDK cree el subsegmento, ya sea desde el middleware del SDK o desde AWS Lambda.

> **Note**
>
> Si utiliza el ORM de SQLAlchemy, puede instrumentar sus consultas SQL importando la versión del SDK de la sesión y las clases de consulta de SQLAlchemy. Consulte Use ORM SQLAlchemy para obtener instrucciones.

Para aplicar parches a todas las bibliotecas disponibles, utilice la función `patch_all` en `aws_xray_sdk.core`. Es posible que algunas bibliotecas, como `httplib` y `urllib`, necesiten habilitar la aplicación de parches dobles llamando a `patch_all(double_patch=True)`.

Example main.py: aplique parches a todas las bibliotecas compatibles

```
import boto3
import botocore
import requests
import sqlite3

from aws_xray_sdk.core import xray_recorder
from aws_xray_sdk.core import patch_all

patch_all()
```

Para aplicar parches a una sola biblioteca, llame a `patch` con una tupla del nombre de la biblioteca. Para ello, deberá proporcionar una sola lista de elementos.

Example main.py: aplique parches a bibliotecas específicas

```
import boto3
import botocore
import requests
import mysql-connector-python

from aws_xray_sdk.core import xray_recorder
from aws_xray_sdk.core import patch

libraries = ['botocore']
patch(libraries)
```

> **Note**
>
> En algunos casos, la clave que se utiliza aplicar parches a una biblioteca no coincide con el nombre de la biblioteca. Algunas claves sirven como alias para una o varias bibliotecas.
>
> Alias de las bibliotecas
>
> - `httplib`: `httplib` y `http.client`
> - `mysql` – `mysql-connector-python`

Seguimiento del contexto para el funcionamiento asíncrono

Para las bibliotecas integradas de `asyncio` o para crear subsegmentos para funciones asíncronas, también debe configurar el SDK de X-Ray para Python con un contexto asíncrono. Importe la clase `AsyncContext` y pase una instancia de ella a la grabadora de X-Ray.

> **Note**
>
> Las bibliotecas compatibles con el marco de trabajo web, como AIOHTTP, no se gestionan a través del módulo `aws_xray_sdk.core.patcher`. No aparecerán en el catálogo de bibliotecas admitidas de`patcher`.

Example main.py: aplique parches a aioboto3

```
import asyncio
```

```
import aioboto3
import requests

from aws_xray_sdk.core.async_context import AsyncContext
from aws_xray_sdk.core import xray_recorder
xray_recorder.configure(service='my_service', context=AsyncContext())
from aws_xray_sdk.core import patch

libraries = (['aioboto3'])
patch(libraries)
```

Rastreo de llamadas al AWS SDK con el SDK de X-Ray para Python

Cuando la aplicación realiza llamadas Servicios de AWS para almacenar datos, escribir en una cola o enviar notificaciones, el SDK de X-Ray para Python rastrea las llamadas en sentido descendente en subsegmentos. El rastreo Servicios de AWS y los recursos a los que accede dentro de esos servicios (por ejemplo, un bucket de Amazon S3 o una cola de Amazon SQS) aparecen como nodos descendentes en el mapa de rastreo de la consola X-Ray.

El SDK de X-Ray para Python instrumenta automáticamente todos los clientes AWS del SDK cuando se aplica un parche a la `botocore` biblioteca. No puede instrumentar clientes individuales.

Para todos los servicios, puede ver el nombre de la API a la que se llama en la consola de X-Ray. Para un subconjunto de servicios, el SDK de X-Ray agrega información al segmento para proporcionar una mayor granularidad en el mapa de servicio.

Por ejemplo, cuando realiza una llamada con un cliente instrumentado de DynamoDB, el SDK agrega el nombre de tabla al segmento para las llamadas que se dirigen a una tabla. En la consola, cada tabla aparece como nodo independiente en el mapa de servicio, con un nodo genérico de DynamoDB para las llamadas que no se dirigen a una tabla.

Example Subsegmento para una llamada a DynamoDB con el fin de guardar un elemento

```
{
  "id": "24756640c0d0978a",
  "start_time": 1.480305974194E9,
  "end_time": 1.4803059742E9,
  "name": "DynamoDB",
  "namespace": "aws",
  "http": {
    "response": {
      "content_length": 60,
```

```
      "status": 200
    }
  },
  "aws": {
    "table_name": "scorekeep-user",
    "operation": "UpdateItem",
    "request_id": "UBQNSO5AEM8T4FDA4RQDEB94OVTDRVV4K4HIRGVJF66Q9ASUAAJG",
  }
}
```

Cuando accede a recursos designados, las llamadas a los siguientes servicios crean nodos adicionales en el mapa de servicio. Las llamadas que no están dirigidas a recursos concretos crean un nodo genérico en el servicio.

- Amazon DynamoDB: nombre de tabla
- Amazon Simple Storage Service: nombre de bucket y de clave
- Amazon Simple Queue Service: nombre de cola

Rastreo de llamadas a servicios web HTTP posteriores utilizando el SDK de X-Ray para Python

Cuando una aplicación realiza llamadas a microservicios o a API de HTTP públicas, se puede utilizar el SDK de X-Ray para Python con el fin de instrumentar dichas llamadas y añadir la API al gráfico de servicios como un servicio posterior.

Para instrumentar clientes HTTP, debe aplicar parches a la biblioteca que se utiliza para realizar llamadas salientes. Si utiliza `requests` o el cliente HTTP integrado de Python, eso es lo único que tiene que hacer. Para `aiohttp`, también debe configurar la grabadora con un contexto asíncrono.

Si utiliza la API del cliente de `aiohttp` 3, es posible que también deba configurar la sesión de `ClientSession` con una instancia de la configuración de seguimiento proporcionada en el SDK.

Example API del cliente 3 de **`aiohttp`**

```
from aws_xray_sdk.ext.aiohttp.client import aws_xray_trace_config

async def foo():
    trace_config = aws_xray_trace_config()
    async with ClientSession(loop=loop, trace_configs=[trace_config]) as session:
        async with session.get(url) as resp
```

```
            await resp.read()
```

Cuando se instrumenta una llamada a una API web posterior, el SDK de X-Ray para Python registra un subsegmento que contiene información acerca de la solicitud HTTP y la respuesta. X-Ray utiliza el subsegmento para generar un segmento inferido de la API remota.

Example Subsegmento para una llamada HTTP posterior

```
{
  "id": "004f72be19cddc2a",
  "start_time": 1484786387.131,
  "end_time": 1484786387.501,
  "name": "names.example.com",
  "namespace": "remote",
  "http": {
    "request": {
      "method": "GET",
      "url": "https://names.example.com/"
    },
    "response": {
      "content_length": -1,
      "status": 200
    }
  }
}
```

Example Segmento inferido para una llamada HTTP posterior

```
{
  "id": "168416dc2ea97781",
  "name": "names.example.com",
  "trace_id": "1-62be1272-1b71c4274f39f122afa64eab",
  "start_time": 1484786387.131,
  "end_time": 1484786387.501,
  "parent_id": "004f72be19cddc2a",
  "http": {
    "request": {
      "method": "GET",
      "url": "https://names.example.com/"
    },
    "response": {
      "content_length": -1,
      "status": 200
```

```
    }
  },
  "inferred": true
}
```

Generación de subsegmentos personalizados con el SDK de X-Ray para Python

Los subsegmentos amplían el segmento de un rastro con detalles sobre el trabajo realizado para atender una solicitud. Cada vez que usted realiza una llamada con un cliente instrumentado, el SDK de X-Ray registra la información generada en un subsegmento. Puede crear subsegmentos adicionales para agrupar otros subsegmentos, medir el rendimiento de una sección de código o registrar anotaciones y metadatos.

Para administrar los subsegmentos, utilice los métodos `begin_subsegment` y `end_subsegment`.

Example main.py: subsegmento personalizado

```
from aws_xray_sdk.core import xray_recorder

subsegment = xray_recorder.begin_subsegment('annotations')
subsegment.put_annotation('id', 12345)
xray_recorder.end_subsegment()
```

Para crear un subsegmento para una función síncrona, utilice el decorador `@xray_recorder.capture`. Puede transferir un nombre para el subsegmento a la función de captura o dejarlo para utilizar el nombre de la función.

Example main.py: subsegmento de función

```
from aws_xray_sdk.core import xray_recorder

@xray_recorder.capture('## create_user')
def create_user():
...
```

Si se trata de una función asíncrona, utilice el decorador `@xray_recorder.capture_async` y pase un contexto asíncrono a la grabadora.

Example main.py: subsegmento de función asíncrona

```
from aws_xray_sdk.core.async_context import AsyncContext
```

```
from aws_xray_sdk.core import xray_recorder
xray_recorder.configure(service='my_service', context=AsyncContext())

@xray_recorder.capture_async('## create_user')
async def create_user():
    ...

async def main():
    await myfunc()
```

Cuando crea un subsegmento dentro de un segmento o de otro subsegmento, el SDK de X-Ray para Python genera un ID para dicho subsegmento y registra la hora de inicio y la hora de finalización.

Example Subsegmentos con metadatos

```
"subsegments": [{
  "id": "6f1605cd8a07cb70",
  "start_time": 1.480305974194E9,
  "end_time": 1.4803059742E9,
  "name": "Custom subsegment for UserModel.saveUser function",
  "metadata": {
    "debug": {
      "test": "Metadata string from UserModel.saveUser"
    }
  },
```

Adición de anotaciones y metadatos a los segmentos con el SDK de X-Ray para Python

Puede usar anotaciones y metadatos para registrar información adicional sobre las solicitudes, el entorno o la aplicación. Puede añadir anotaciones y metadatos a los segmentos que crea el SDK de X-Ray o a los subsegmentos personalizados que cree usted mismo.

Las anotaciones son pares de clave-valor con valores de cadena, numéricos o booleanos. Las anotaciones se indexan para su uso con expresiones de filtro. Utilice anotaciones para registrar los datos que desee utilizar para agrupar rastros en la consola o cuando llame a la API de `GetTraceSummaries`.

Los metadatos son pares de clave-valor con valores de cualquier tipo, por ejemplo objetos y listas, pero que no se indexan para utilizarlos con expresiones de filtro. Utilice los metadatos para

registrar datos adicionales que desee almacenar en el rastro, pero que no necesite usar para hacer búsquedas.

Además de anotaciones y metadatos, también puede registrar cadenas de ID de usuario en los segmentos. Los identificadores de usuario se registran en un campo aparte en segmentos y se indexan para su uso con la búsqueda.

Secciones

- Registro de anotaciones con el SDK de X-Ray para Python
- Registro de metadatos con el SDK de X-Ray para Python
- Registro de ID de usuario con el SDK de X-Ray para Python

Registro de anotaciones con el SDK de X-Ray para Python

Utilice anotaciones para registrar información sobre segmentos o subsegmentos que desee indexar para las búsquedas.

Requisitos de anotación

- Teclas: la clave de una anotación de X-Ray puede tener hasta 500 caracteres alfanuméricos. No puede utilizar espacios ni símbolos distintos del símbolo de subrayado (_).
- Valores: el valor de una anotación de X-Ray puede tener hasta 1000 caracteres Unicode.
- Número de anotaciones: puede utilizar hasta 50 anotaciones por traza.

Para registrar anotaciones

1. Obtenga una referencia al segmento o subsegmento actual desde `xray_recorder`.

```
from aws_xray_sdk.core import xray_recorder
...
document = xray_recorder.current_segment()
```

o

```
from aws_xray_sdk.core import xray_recorder
...
document = xray_recorder.current_subsegment()
```

2. Llame a `put_annotation` con una clave de cadena y un valor booleano, numérico o de cadena.

```
document.put_annotation("mykey", "my value");
```

También puede utilizar el método `put_annotation` en el `xray_recorder`. Este método registra las anotaciones en el subsegmento actual o, si no hay ningún subsegmento abierto, en el segmento.

```
xray_recorder.put_annotation("mykey", "my value");
```

El SDK registra las anotaciones como pares de clave-valor en un objeto `annotations` del documento de segmento. Si llama dos veces a `put_annotation` con la misma clave, se sobrescriben los valores previamente registrados en ese segmento o subsegmento.

Para encontrar rastros que tengan anotaciones con valores específicos, utilice la palabra clave `annotations.key` en una expresión de filtro.

Registro de metadatos con el SDK de X-Ray para Python

Utilice los metadatos para registrar información sobre segmentos o subsegmentos que no necesite indexar para las búsquedas. Los valores de metadatos pueden ser cadenas, números, booleanos o cualquier objeto que se pueda serializar en un objeto o matriz JSON.

Para registrar metadatos

1. Obtenga una referencia al segmento o subsegmento actual desde `xray_recorder`.

```
from aws_xray_sdk.core import xray_recorder
...
document = xray_recorder.current_segment()
```

o

```
from aws_xray_sdk.core import xray_recorder
...
document = xray_recorder.current_subsegment()
```

2. Llame a `put_metadata` con una clave de cadena; un valor booleano, numérico, de cadena o de objeto y un espacio de nombres de cadena.

```
document.put_metadata("my key", "my value", "my namespace");
```

o

Llame a `put_metadata` con solo una clave y un valor.

```
document.put_metadata("my key", "my value");
```

También puede utilizar el método `put_metadata` en el `xray_recorder`. Este método registra los metadatos en el subsegmento actual o, si no hay ningún subsegmento abierto, en el segmento.

```
xray_recorder.put_metadata("my key", "my value");
```

Si no especifica un espacio de nombres, el SDK utiliza `default`. Si llama dos veces a `put_metadata` con la misma clave, se sobrescriben los valores previamente registrados en ese segmento o subsegmento.

Registro de ID de usuario con el SDK de X-Ray para Python

Registre identificadores de usuario en segmentos de solicitud para identificar al usuario que envió la solicitud.

Para registrar identificadores de usuario

1. Obtenga una referencia al segmento actual desde `xray_recorder`.

   ```
   from aws_xray_sdk.core import xray_recorder
   ...
   document = xray_recorder.current_segment()
   ```

2. Llame a `setUser` con un ID de cadena del usuario que envió la solicitud.

   ```
   document.set_user("U12345");
   ```

Puede llamar a `set_user` en sus controladores para registrar el ID de usuario en cuanto la aplicación empiece a procesar la solicitud.

Para buscar rastros de un ID de usuario, utilice la palabra clave `user` en una expresión de filtro.

Instrumentación de marcos de trabajo web implementados en entornos sin servidor

El SDK de AWS X-Ray para Python admite la instrumentación de marcos web implementados en aplicaciones sin servidor. La arquitectura nativa de la nube carece de servidores, lo que le permite delegar más responsabilidades de gestión en AWS y mejorar la agilidad y la innovación.

La arquitectura sin servidor es un modelo de aplicaciones de software que permite crear y ejecutar aplicaciones y servicios sin preocuparse por los servidores. En esta arquitectura, ya no son necesarias las tareas de administración de la infraestructura, como el aprovisionamiento de servidores o clústeres, la aplicación de parches, el mantenimiento del sistema operativo y el aprovisionamiento de capacidad. Puede crear soluciones sin servidor para prácticamente cualquier tipo de aplicación o servicio de backend. Además, será usted quien se encargue de administrar todo lo necesario para ejecutar y escalar las aplicaciones con alta disponibilidad.

En este tutorial, se muestra cómo AWS X-Ray instrumentar automáticamente un marco web, como Flask o Django, que se implementa en un entorno sin servidor. La instrumentación de rayos X de la aplicación le permite ver todas las llamadas posteriores que se realizan, empezando por Amazon API Gateway y pasando por su AWS Lambda función, y las llamadas salientes que realiza la aplicación.

El SDK de X-Ray para Python admite los siguientes marcos de trabajo de aplicaciones de Python:

- Flask versión 0.8 o posteriores
- Django versión 1.0 o posteriores

En este tutorial se desarrolla un ejemplo de aplicación sin servidor que está implementada en Lambda y se invoca a través de API Gateway. En este tutorial se utiliza Zappa para implementar automáticamente la aplicación en Lambda y para configurar el punto de conexión de API Gateway.

Requisitos previos

- Zappa
- Python: versión 2.7 o 3.6.
- AWS CLI— Compruebe que AWS CLI está configurada con la cuenta Región de AWS en la que va a implementar la aplicación.
- Pip
- Virtualenv

Paso 1: crear un entorno

En este paso, va a crear un entorno virtual utilizando `virtualenv` para hospedar la aplicación.

1. Con el AWS CLI, cree un directorio para la aplicación. A continuación, cambie al nuevo directorio.

   ```
   mkdir serverless_application
   cd serverless_application
   ```

2. Cree un entorno virtual en este nuevo directorio. Utilice el comando siguiente para activarlo.

   ```
   # Create our virtual environment
   virtualenv serverless_env

   # Activate it
   source serverless_env/bin/activate
   ```

3. Instale X-Ray, Flask, Zappa y la biblioteca de solicitudes en el entorno.

   ```
   # Install X-Ray, Flask, Zappa, and Requests into your environment
   pip install aws-xray-sdk flask zappa requests
   ```

4. Añada el código de la aplicación al directorio `serverless_application`. En este caso, puede utilizar como referencia el ejemplo Hello World de Flasks.

   En el directorio `serverless_application`, cree un archivo llamado `my_app.py`. A continuación, utilice un editor de texto para añadir los siguientes comandos. Esta aplicación instrumenta la biblioteca de solicitudes, aplica parches en el middleware de la aplicación de Flask y abre el punto de enlace `'/'`.

   ```
   # Import the X-Ray modules
   from aws_xray_sdk.ext.flask.middleware import XRayMiddleware
   from aws_xray_sdk.core import patcher, xray_recorder
   from flask import Flask
   import requests

   # Patch the requests module to enable automatic instrumentation
   patcher.patch(('requests',))

   app = Flask(__name__)
   ```

```
# Configure the X-Ray recorder to generate segments with our service name
xray_recorder.configure(service='My First Serverless App')

# Instrument the Flask application
XRayMiddleware(app, xray_recorder)

@app.route('/')
def hello_world():
    resp = requests.get("https://aws.amazon.com")
    return 'Hello, World: %s' % resp.url
```

Paso 2: Crear e implementar un entorno de Zappa

En este paso, utilizará Zappa para configurar automáticamente un punto de conexión de API Gateway e implementarlo en Lambda.

1. Inicialice Zappa desde dentro del directorio `serverless_application`. En este ejemplo, hemos utilizado la configuración predeterminada. Sin embargo, si tiene sus propias preferencias de personalización, Zappa le mostrará las instrucciones de configuración.

```
zappa init
```

```
What do you want to call this environment (default 'dev'): dev
...
What do you want to call your bucket? (default 'zappa-*******'): zappa-*******
...
...
It looks like this is a Flask application.
What's the modular path to your app's function?
This will likely be something like 'your_module.app'.
We discovered: my_app.app
Where is your app's function? (default 'my_app.app'): my_app.app
...
Would you like to deploy this application globally? (default 'n') [y/n/
(p)rimary]: n
```

2. Habilite X-Ray. Abra el archivo `zappa_settings.json` y compruebe que sea similar al del ejemplo.

```
{
    "dev": {
```

```
        "app_function": "my_app.app",
        "aws_region": "us-west-2",
        "profile_name": "default",
        "project_name": "serverless-exam",
        "runtime": "python2.7",
        "s3_bucket": "zappa-*********"
    }
}
```

3. Añada `"xray_tracing": true` como entrada en el archivo de configuración.

```
{
    "dev": {
        "app_function": "my_app.app",
        "aws_region": "us-west-2",
        "profile_name": "default",
        "project_name": "serverless-exam",
        "runtime": "python2.7",
        "s3_bucket": "zappa-*********",
        "xray_tracing": true
    }
}
```

4. Implemente la aplicación . Esto configurará automáticamente el punto de conexión de API Gateway y cargará el código en Lambda.

```
zappa deploy
```

```
...
Deploying API Gateway..
Deployment complete!: https://**********.execute-api.us-west-2.amazonaws.com/dev
```

Paso 3: habilitar el rastreo de X-Ray para API Gateway

En este paso, interactuará con la consola de API Gateway para habilitar el rastreo de X-Ray.

1. Inicie sesión en la consola de API Gateway AWS Management Console y ábrala en https://console.aws.amazon.com/apigateway/.
2. Busque la API que acaba de generar. La URL debería parecerse a esta: `serverless-exam-dev`.

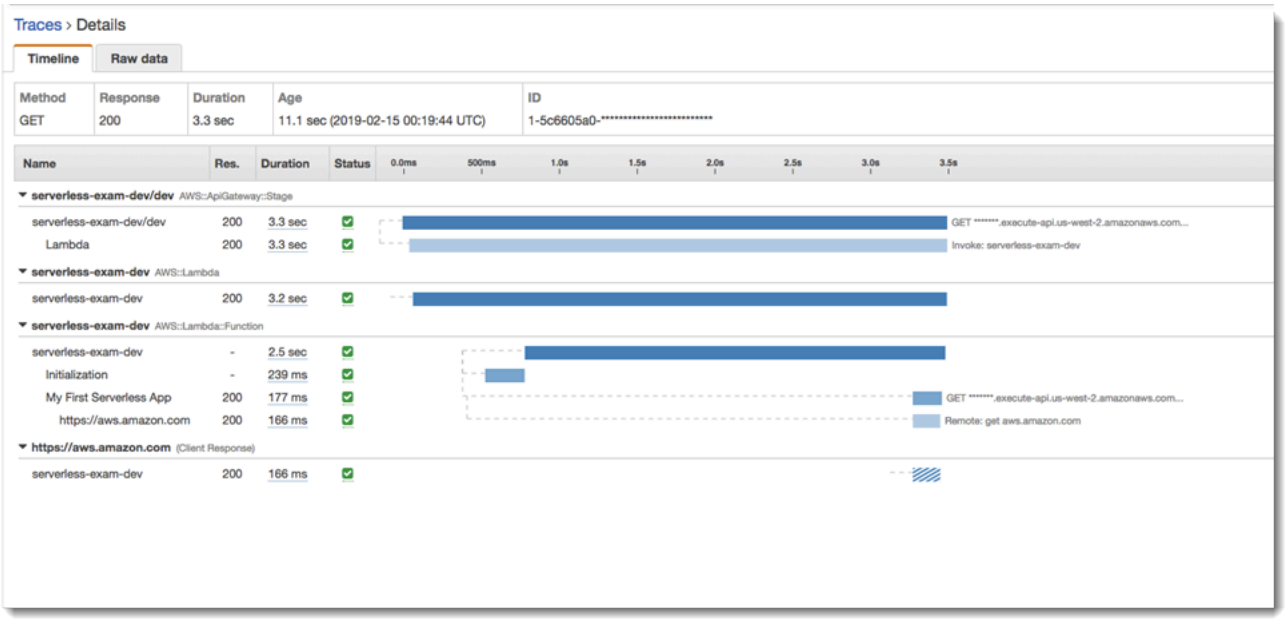
3. Elija Etapas.
4. Seleccione el nombre de la etapa de implementación. El valor predeterminado es `dev`.
5. En la pestaña Logs/Tracing (Registros/rastreo), active la casilla Enable X-Ray Tracing (Habilitar rastreo de X-Ray).
6. Seleccione Guardar cambios.
7. Obtenga acceso al punto de enlace a través del navegador. Si utilizó la aplicación `Hello World` de ejemplo, debería aparecer lo siguiente.

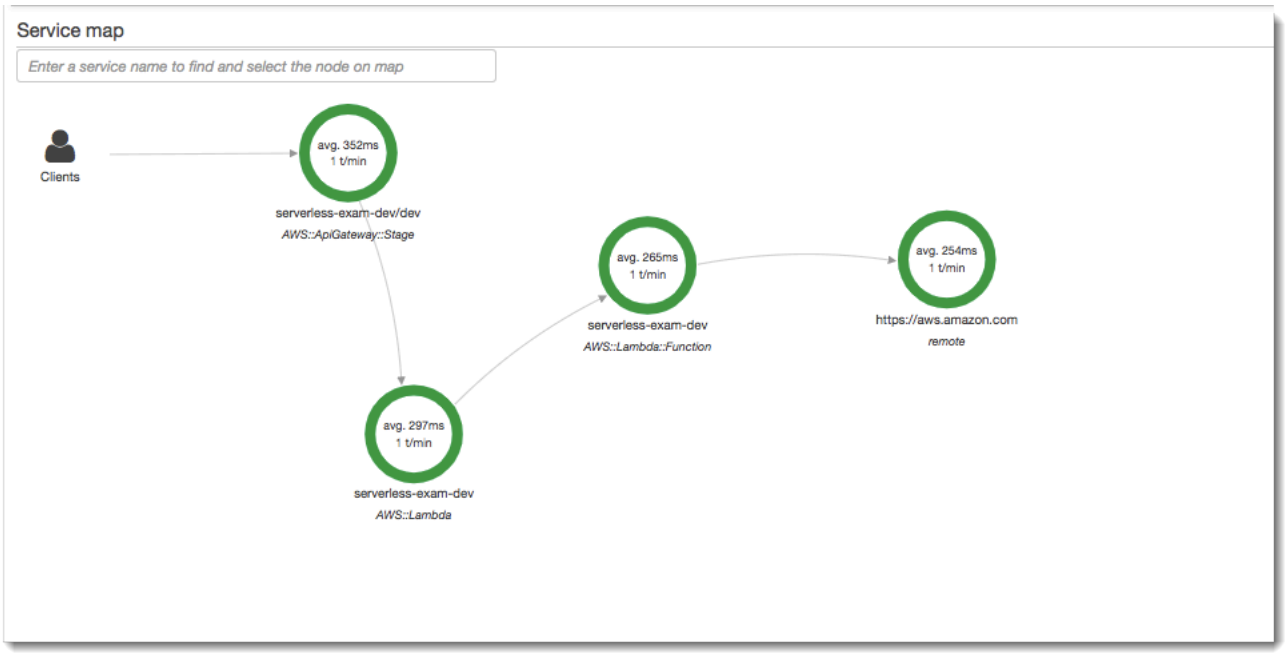
```
"Hello, World: https://aws.amazon.com/"
```

Paso 4: Consultar el registro de seguimiento creado

En este paso, interactuará con la consola de X-Ray para ver el rastro creado por la aplicación de ejemplo. Para ver una explicación detallada del análisis del seguimiento, consulte Uso del mapa de servicio.

1. Inicie sesión en la consola de X-Ray AWS Management Console y ábrala en https://console.aws.amazon.com/xray/home.
2. Consulte los segmentos generados por API Gateway, la función de Lambda y el contenedor de Lambda.
3. En el segmento de la función de Lambda, consulte un subsegmento llamado `My First Serverless App`. Detrás hay un segundo subsegmento llamado `https://aws.amazon.com`.
4. Durante la inicialización, Lambda podría generar también un tercer subsegmento llamado `initialization`.





Paso 5: Eliminar

Termine siempre los recursos que ya no utilice para evitar que se acumulen costos inesperados. Tal y como se explica en este tutorial, existen herramientas como Zappa que optimizan la implementación sin servidor.

Para eliminar la aplicación de Lambda, API Gateway y Amazon S3, ejecute el siguiente comando en el directorio del proyecto a través de la AWS CLI.

```
zappa undeploy dev
```

Siguientes pasos

Añada más funciones a su aplicación añadiendo AWS clientes e instrumentándolos con X-Ray. Consulte más información sobre las opciones de computación sin servidor de Sin servidor en AWS.

Instrumentación de su aplicación con .NET

Hay dos maneras de instrumentar su .NET aplicación para enviar trazas a X-Ray:

- AWS Distro for OpenTelemetry .NET: una AWS distribución que proporciona un conjunto de bibliotecas de código abierto para enviar métricas y rastreos correlacionados a varias soluciones de AWS monitoreo, incluidas Amazon y Amazon OpenSearch Service CloudWatch AWS X-Ray, a través de AWS Distro for Collector. OpenTelemetry
- AWS X-Ray SDK para .NET: conjunto de bibliotecas para generar y enviar trazas a X-Ray mediante el daemon X-Ray.

Para obtener más información, consulte Cómo elegir entre los AWS SDK Distro for OpenTelemetry y X-Ray.

AWS Distro para OpenTelemetry .NET

Con AWS Distro for OpenTelemetry .NET, puede instrumentar sus aplicaciones una vez y enviar métricas y rastreos correlacionados a varias soluciones de AWS monitoreo CloudWatch AWS X-Ray, incluidas Amazon y Amazon OpenSearch Service. El uso de X-Ray con AWS Distro for OpenTelemetry requiere dos componentes: un OpenTelemetry SDK habilitado para su uso con X-Ray y una AWS Distro for OpenTelemetry Collector habilitada para su uso con X-Ray.

Para empezar, consulta la documentación de la AWS Distro. OpenTelemetry .NET

Para obtener más información sobre el uso de la AWS distribución OpenTelemetry con AWS X-Ray y otros Servicios de AWS, consulta la sección AWS Distro for OpenTelemetry o la AWS Distro para ver la documentación. OpenTelemetry

Para obtener más información sobre el soporte y el uso de idiomas, consulta AWS Observabilidad en. GitHub

AWS X-Ray SDK para.NET

El X-Ray SDK para .NET es una biblioteca para instrumentar aplicaciones web de C# .NET, aplicaciones web .NET Core y funciones de .NET Core. AWS Lambda Proporciona clases y métodos para generar y enviar datos de rastreo al daemon de X-Ray. Incluye información sobre las solicitudes entrantes atendidas por la aplicación y las llamadas que la aplicación realiza a bases de datos SQL Servicios de AWS, API web HTTP y aplicaciones descendentes.

> **Note**
>
> El SDK de X-Ray para .NET es un proyecto de código abierto. Puedes seguir el proyecto y enviar las incidencias y solicitudes de cambios en GitHub: github.com/aws/ aws-xray-sdk-dotnet

Para las aplicaciones web, comience por añadir un controlador de mensajes a su configuración web para realizar el seguimiento de las solicitudes entrantes. El controlador de mensajes crea un segmento para cada solicitud rastreada y lo completa cuando se envía la respuesta. Mientras el segmento está abierto, puede utilizar los métodos del cliente del SDK para añadir información al segmento y crear subsegmentos para rastrear llamadas posteriores. El SDK también registra automáticamente las excepciones que produce su aplicación mientras el segmento está abierto.

En el caso de las funciones de Lambda llamadas por una aplicación o un servicio instrumentados, Lambda lee el encabezado de rastreo y rastrea automáticamente las solicitudes muestreadas. Para otras funciones, puede configurar Lambda con el fin de muestrear y rastrear las solicitudes entrantes. En cualquier caso, Lambda crea el segmento y se lo proporciona al SDK de X-Ray.

> **Note**
>
> En Lambda, el SDK de X-Ray es opcional. Si no lo usa en su función, el mapa de servicio seguirá incluyendo un nodo para el servicio de Lambda y uno para cada función de Lambda. Al añadir el SDK, puede instrumentar el código de función para añadir subsegmentos al segmento de función registrado por Lambda. Para obtener más información, consulte AWS Lambda y AWS X-Ray.

A continuación, use el SDK de X-Ray para .NET con el fin de instrumentar a sus clientes del AWS SDK for .NET. Cada vez que realizas una llamada a un canal intermedio Servicio de AWS o a

un recurso con un cliente instrumentado, el SDK registra la información sobre la llamada en un subsegmento. AWS los servicios y los recursos a los que accedes dentro de los servicios aparecen como nodos descendentes en el mapa de rastreo para ayudarte a identificar los errores y los problemas de limitación en las conexiones individuales.

El SDK de X-Ray para .NET también permite la instrumentación de llamadas posteriores a API web HTTP y bases de datos SQL. El método de extensión `GetResponseTraced` para `System.Net.HttpWebRequest` rastrea llamadas HTTP salientes. Puede utilizar la versión de `SqlCommand` del SDK de X-Ray para .NET para instrumentar consultas SQL.

En cuanto empiece a utilizar el SDK, personalice su comportamiento configurando la grabadora y el controlador de mensajes. Puede añadir complementos para registrar los datos sobre los recursos informáticos que ejecutan su aplicación, personalizar el comportamiento de muestreo mediante la definición de reglas de muestreo y definir el nivel de log para ver más o menos información del SDK en los logs de las aplicaciones.

Registre información adicional acerca de las solicitudes y el trabajo que la aplicación realiza en anotaciones y metadatos. Las anotaciones son pares sencillos de clave-valor que se indexan para su uso con expresiones de filtro para poder buscar rastros que contengan datos específicos. Las entradas de metadatos son menos restrictivas y pueden registrar objetos y matrices completos, es decir, todo lo que se pueda serializar en JSON.

> **Anotaciones y metadatos**
>
> Las anotaciones y los metadatos son texto arbitrario que se agrega a los segmentos con el SDK de X-Ray. Las anotaciones se indexan para su uso con expresiones de filtro. Los metadatos no se indexan pero se pueden ver en el segmento sin procesar con la consola o la API de X-Ray. Cualquier persona a la que conceda acceso de lectura a X-Ray puede ver estos datos.

Cuando tenga muchos clientes instrumentados en su código, un único segmento de solicitud puede contener un gran número de subsegmentos, uno para cada llamada realizada con un cliente instrumentado. Puede organizar y agrupar los subsegmentos incluyendo las llamadas del cliente en subsegmentos personalizados. Puede crear un subsegmento personalizado para una función completa o para cualquier sección de código, y registrar los metadatos y las anotaciones en el subsegmento en lugar de escribirlo todo en el segmento principal.

Para acceder a documentos de referencia sobre las clases y los métodos de SDK, consulte lo siguiente:

- AWS X-Ray Referencia de la API de SDK for .NET
- AWS X-Ray Referencia de API de SDK for .NET Core

El mismo paquete admite tanto .NET como .NET Core, pero las clases que se utilizan varían. Los ejemplos de este capítulo contienen un enlace a la referencia del API de .NET, a menos que la clase sea específica de .NET Core.

Requisitos

El X-Ray SDK para .NET requiere la versión 4.5 o posterior de.NET Framework y AWS SDK for .NET.

Para las aplicaciones y funciones de .NET Core, el SDK requiere .NET Core 2.0 o posterior.

Integración del SDK de X-Ray para .NET en su aplicación

NuGet Utilícelo para añadir el X-Ray SDK para .NET a su aplicación.

Para instalar el SDK de X-Ray para .NET con el administrador de NuGet paquetes de Visual Studio

1. Elija Tools, NuGet Package Manager y Manage NuGet Packages for Solution.
2. Busque la opción AWSXRayRecorder.
3. Elija el paquete y, a continuación, haga clic en Install (Instalar).

Administración de dependencias

El SDK de X-Ray para .NET está disponible en Nuget. Instale el SDK con el administrador de paquetes.

```
Install-Package AWSXRayRecorder -Version 2.10.1
```

El paquete NuGet `AWSXRayRecorder v2.10.1` tiene las siguientes dependencias:

NET Framework 4.5

```
AWSXRayRecorder (2.10.1)
|
|-- AWSXRayRecorder.Core (>= 2.10.1)
|   |-- AWSSDK.Core (>= 3.3.25.1)
|
|-- AWSXRayRecorder.Handlers.AspNet (>= 2.7.3)
|   |-- AWSXRayRecorder.Core (>= 2.10.1)
|
|-- AWSXRayRecorder.Handlers.AwsSdk (>= 2.8.3)
|   |-- AWSXRayRecorder.Core (>= 2.10.1)
|
|-- AWSXRayRecorder.Handlers.EntityFramework (>= 1.1.1)
|   |-- AWSXRayRecorder.Core (>= 2.10.1)
|   |-- EntityFramework (>= 6.2.0)
|
|-- AWSXRayRecorder.Handlers.SqlServer (>= 2.7.3)
|   |-- AWSXRayRecorder.Core (>= 2.10.1)
|
|-- AWSXRayRecorder.Handlers.System.Net (>= 2.7.3)
    |-- AWSXRayRecorder.Core (>= 2.10.1)
```

NET Framework 2.0

```
AWSXRayRecorder (2.10.1)
|
|-- AWSXRayRecorder.Core (>= 2.10.1)
|   |-- AWSSDK.Core (>= 3.3.25.1)
|   |-- Microsoft.AspNetCore.Http (>= 2.0.0)
|   |-- Microsoft.Extensions.Configuration (>= 2.0.0)
|   |-- System.Net.Http (>= 4.3.4)
|
|-- AWSXRayRecorder.Handlers.AspNetCore (>= 2.7.3)
|   |-- AWSXRayRecorder.Core (>= 2.10.1)
|   |-- Microsoft.AspNetCore.Http.Extensions (>= 2.0.0)
|   |-- Microsoft.AspNetCore.Mvc.Abstractions (>= 2.0.0)
|
|-- AWSXRayRecorder.Handlers.AwsSdk (>= 2.8.3)
|   |-- AWSXRayRecorder.Core (>= 2.10.1)
|
|-- AWSXRayRecorder.Handlers.EntityFramework (>= 1.1.1)
|   |-- AWSXRayRecorder.Core (>= 2.10.1)
```

```
|   |-- Microsoft.EntityFrameworkCore.Relational (>= 3.1.0)
|
|-- AWSXRayRecorder.Handlers.SqlServer (>= 2.7.3)
|   |-- AWSXRayRecorder.Core (>= 2.10.1)
|   |-- System.Data.SqlClient (>= 4.4.0)
|
|-- AWSXRayRecorder.Handlers.System.Net (>= 2.7.3)
    |-- AWSXRayRecorder.Core (>= 2.10.1)
```

Para obtener más información sobre la administración de dependencias, consulte la documentación de Microsoft sobre la dependencia de NuGet y la resolución de dependencias de paquetes NuGet.

Configuración del SDK de X-Ray para .NET

Puede configurar el SDK de X-Ray para .NET mediante el uso de complementos a fin de incluir información sobre el servicio que sus aplicaciones ejecutan, modificar la conducta predeterminada de muestreo o agregar reglas de muestreo que se aplican a las solicitudes dirigidas a rutas específicas.

Para las aplicaciones web .NET, añada claves a la sección `appSettings` del archivo `Web.config`.

Example Web.config

```
<configuration>
  <appSettings>
    <add key="AWSXRayPlugins" value="EC2Plugin"/>
    <add key="SamplingRuleManifest" value="sampling-rules.json"/>
  </appSettings>
</configuration>
```

Para .NET Core, cree un archivo denominado `appsettings.json` con una clave de nivel superior llamada `XRay`.

Example .NET appsettings.json

```
{
  "XRay": {
    "AWSXRayPlugins": "EC2Plugin",
    "SamplingRuleManifest": "sampling-rules.json"
  }
}
```

A continuación, en el código de la aplicación, cree un objeto de configuración y utilícelo para inicializar la grabadora de X-Ray. Hágalo antes de inicializar la grabadora.

Example .NET Core Program.cs: configuración de grabadora

```
using Amazon.XRay.Recorder.Core;
...
AWSXRayRecorder.InitializeInstance(configuration);
```

Si está instrumentando una aplicación web de .NET Core, también puede pasar el objeto de configuración al método `UseXRay` al configurar el controlador de mensajes. Para las funciones de Lambda utilice el método `InitializeInstance` como se muestra más arriba.

Para obtener más información acerca del API de configuración de .NET Core, consulte Configurar una aplicación ASP.NET Core en docs.microsoft.com.

Secciones

- Complementos
- Reglas de muestreo
- Registro (.NET)
- Registro (.NET Core)
- Variables de entorno

Complementos

Utilice complementos para agregar datos sobre el servicio que aloja su aplicación.

Complementos

- Amazon EC2: `EC2Plugin` añade el ID de instancia, la zona de disponibilidad y el grupo de registros de CloudWatch.
- Elastic Beanstalk: `ElasticBeanstalkPlugin` añade el nombre de entorno, la etiqueta de versión y el ID de implementación.
- Amazon ECS: `ECSPlugin` agrega el ID de contenedor.

Para utilizar un complemento, configure el cliente del SDK de X-Ray para .NET añadiendo el ajuste `AWSXRayPlugins`. Si hay varios complementos para su aplicación, especifíquelos todos en la misma configuración, separados por comas.

Example Web.config - complementos

```
<configuration>
  <appSettings>
    <add key="AWSXRayPlugins" value="EC2Plugin,ElasticBeanstalkPlugin"/>
  </appSettings>
</configuration>
```

Example .NET Core appsettings.json: complementos

```
{
  "XRay": {
    "AWSXRayPlugins": "EC2Plugin,ElasticBeanstalkPlugin"
  }
}
```

Reglas de muestreo

El SDK utiliza las reglas de muestreo que define el usuario en la consola de X-Ray para determinar qué solicitudes registrar. La regla predeterminada rastrea la primera solicitud cada segundo y el 5 % de las solicitudes adicionales de todos los servicios que envían rastros a X-Ray. Cree reglas adicionales en la consola de X-Ray para personalizar la cantidad de datos registrados para cada una de sus aplicaciones.

El SDK aplica las reglas personalizadas en el orden en que se definen. Si una solicitud coincide con varias reglas personalizadas, el SDK solo aplica la primera regla.

> **Note**
>
> Si el SDK no puede comunicarse con X-Ray para obtener las reglas de muestreo, vuelve a una regla local predeterminada de la primera solicitud cada segundo y del 5 % de las solicitudes adicionales por host. Eso puede ocurrir si el host no tiene permiso para llamar a las API de muestreo o no puede conectarse al daemon de X-Ray, que actúa como proxy TCP para las llamadas a las API realizadas por el SDK.

También puedes configurar el SDK para que cargue las reglas de muestreo desde un documento JSON. El SDK puede usar las reglas locales como respaldo para los casos en que el muestreo de X-Ray no esté disponible, o puede usar las reglas locales exclusivamente.

Example sampling-rules.json

```
{
  "version": 2,
  "rules": [
    {
      "description": "Player moves.",
      "host": "*",
      "http_method": "*",
      "url_path": "/api/move/*",
      "fixed_target": 0,
      "rate": 0.05
    }
  ],
  "default": {
    "fixed_target": 1,
    "rate": 0.1
  }
}
```

En este ejemplo se define una regla personalizada y una regla predeterminada. La regla personalizada aplica un porcentaje de muestreo del 5 % sin un número mínimo de solicitudes de rastreo para las rutas incluidas bajo `/api/move/`. La regla predeterminada rastrea la primera solicitud cada segundo y el 10 % de las solicitudes adicionales.

La desventaja de definir las reglas localmente es que el objetivo establecido lo aplica cada instancia de la grabadora de forma independiente, en lugar de ser administrado por el servicio de X-Ray. A medida que se implementan más hosts, el porcentaje establecido se multiplica, lo que dificulta el control de la cantidad de datos registrados.

En AWS Lambda no puede modificar el porcentaje de muestreo. Si un servicio instrumentado llama a su función, Lambda registrará las llamadas que generaron solicitudes muestreadas por ese servicio. Si el rastreo activo está activado y no hay ningún encabezado de rastreo, Lambda toma la decisión de muestreo.

Para configurar reglas de respaldo, indique al SDK de X-Ray para .NET que cargue reglas de muestreo desde un archivo con la configuración `SamplingRuleManifest`.

Example .NET Web.config: reglas de muestreo

```
<configuration>
  <appSettings>
    <add key="SamplingRuleManifest" value="sampling-rules.json"/>
  </appSettings>
</configuration>
```

Example .NET Core appsettings.json: reglas de muestreo

```
{
  "XRay": {
    "SamplingRuleManifest": "sampling-rules.json"
  }
}
```

Para utilizar solo reglas locales, cree la grabadora con una `LocalizedSamplingStrategy`. Si tiene reglas de copia de seguridad configuradas, elimine dicha configuración.

Example .NET global.asax: reglas de muestreo locales

```
var recorder = new AWSXRayRecorderBuilder().WithSamplingStrategy(new
 LocalizedSamplingStrategy("samplingrules.json")).Build();
AWSXRayRecorder.InitializeInstance(recorder: recorder);
```

Example .NET Core Program.cs: reglas de muestreo locales

```
var recorder = new AWSXRayRecorderBuilder().WithSamplingStrategy(new
 LocalizedSamplingStrategy("sampling-rules.json")).Build();
AWSXRayRecorder.InitializeInstance(configuration,recorder);
```

Registro (.NET)

El SDK de X-Ray para .NET usa el mismo mecanismo de registro que AWS SDK for .NET. Si ya ha configurado su aplicación para que registre la salida de AWS SDK for .NET, se aplicará la misma configuración a la salida del SDK de X-Ray para .NET.

Para configurar el registro, añada una sección de configuración denominada `aws` al archivo `App.config` o `Web.config`.

Example Web.config: registro

```
...
<configuration>
  <configSections>
    <section name="aws" type="Amazon.AWSSection, AWSSDK.Core"/>
  </configSections>
  <aws>
    <logging logTo="Log4Net"/>
  </aws>
</configuration>
```

Para obtener más información, consulte Configuración del AWS SDK for .NET para su aplicación en la Guía para desarrolladores del AWS SDK for .NET.

Registro (.NET Core)

El SDK de X-Ray para .NET usa las mismas opciones de registro que AWS SDK for .NET. Para configurar el registro para las aplicaciones .NET Core, transfiera la opción de registro al método `AWSXRayRecorder.RegisterLogger`.

Por ejemplo, para utilizar log4net, cree un archivo de configuración que defina el registrador, el formato de salida y la ubicación del archivo.

Example .NET Core log4net.config

```
<?xml version="1.0" encoding="utf-8" ?>
<log4net>
  <appender name="FileAppender" type="log4net.Appender.FileAppender,log4net">
    <file value="c:\logs\sdk-log.txt" />
    <layout type="log4net.Layout.PatternLayout">
      <conversionPattern value="%date [%thread] %level %logger - %message%newline" />
    </layout>
  </appender>
  <logger name="Amazon">
    <level value="DEBUG" />
    <appender-ref ref="FileAppender" />
  </logger>
</log4net>
```

A continuación, cree el registrador y aplique la configuración en el código del programa.

Example .NET Core Program.cs: registro

```
using log4net;
using Amazon.XRay.Recorder.Core;

class Program
{
  private static ILog log;
  static Program()
  {
    var logRepository = LogManager.GetRepository(Assembly.GetEntryAssembly());
    XmlConfigurator.Configure(logRepository, new FileInfo("log4net.config"));
    log = LogManager.GetLogger(typeof(Program));
    AWSXRayRecorder.RegisterLogger(LoggingOptions.Log4Net);
  }
  static void Main(string[] args)
  {
  ...
  }
}
```

Para obtener más información sobre cómo configurar log4net, consulte Configuration en logging.apache.org.

Variables de entorno

Puede usar variables de entorno para configurar el SDK de X-Ray para .NET. El SDK admite las siguientes variables.

- `AWS_XRAY_TRACING_NAME`: establezca el nombre de servicio que el SDK utiliza para los segmentos. Anula el nombre de servicio que se ha establecido en la estrategia de nomenclatura de segmento del filtro de servlet.
- `AWS_XRAY_DAEMON_ADDRESS`: establezca el host y el puerto del oyente del daemon de X-Ray. De forma predeterminada, el SDK utiliza `127.0.0.1:2000` tanto para rastrear datos (UDP) como para el muestreo (TCP). Use esta variable si ha configurado el daemon para que escuche en un puerto diferente o si se ejecuta en un host diferente.

  Formato

  - El mismo puerto: *`address`*`:`*`port`*
  - Puertos diferentes: `tcp:`*`address`*`:`*`port`* `udp:`*`address`*`:`*`port`*

- `AWS_XRAY_CONTEXT_MISSING`: establezca esta opción en `RUNTIME_ERROR` para generar excepciones cuando el código instrumentado intente registrar datos sin que haya ningún segmento abierto.

  Valores válidos

  - `RUNTIME_ERROR`: lance una excepción de tiempo de ejecución.
  - `LOG_ERROR`: registre un error y continúe (predeterminado).
  - `IGNORE_ERROR`: ignore el error y continúe.

  Se pueden producir errores relativos a segmentos o subsegmentos inexistentes al intentar usar un cliente instrumentado en el código de inicio que se ejecuta cuando no hay ninguna solicitud abierta o en el código que inicia un nuevo subproceso.

Instrumentación de las solicitudes HTTP entrantes con el SDK de X-Ray para .NET

Puede utilizar el SDK de X-Ray para rastrear las solicitudes HTTP entrantes que su aplicación atiende en una instancia de EC2 en Amazon EC2, AWS Elastic Beanstalk o Amazon ECS.

Utilice un controlador de mensajes para instrumentar las solicitudes HTTP entrantes. Cuando agrega el controlador de mensajes de X-Ray a su aplicación, el SDK de X-Ray para .NET crea un segmento para cada solicitud muestreada. Este segmento incluye el momento, el método y la disposición de la solicitud HTTP. La instrumentación adicional crea subsegmentos en este segmento.

> **Note**
>
> En el caso de funciones de AWS Lambda, Lambda crea un segmento para cada solicitud muestreada. Para obtener más información, consulte AWS Lambda y AWS X-Ray.

Cada segmento tiene un nombre que identifica la aplicación en el mapa de servicio. El nombre del segmento se puede asignar de forma estática o se puede configurar el SDK para que le asigne un nombre dinámico en función del encabezado del host de la solicitud entrante. La nomenclatura dinámica permite agrupar los rastros en función del nombre de dominio de la solicitud y aplicar un nombre predeterminado si el nombre no coincide con el patrón esperado (por ejemplo, si el encabezado del host está falsificado).

> **Solicitudes reenviadas**
>
> Si un equilibrador de carga u otro intermediario reenvía una solicitud a la aplicación, X-Ray toma la IP de cliente del encabezado `X-Forwarded-For` de la solicitud en lugar de tomar la IP de origen del paquete IP. La IP de cliente que se graba para una solicitud reenviada puede estar falsificada, por lo que no se debe confiar en ella.

El controlador de mensajes crea un segmento para cada solicitud entrante con un bloque `http` que contiene la siguiente información:

- Método HTTP: GET, POST, PUT, DELETE, etc.
- Dirección del cliente: la dirección IP del cliente que envió la solicitud.
- Código de respuesta: el código de respuesta HTTP para la solicitud finalizada.
- Intervalo: la hora de inicio (cuando se recibió la solicitud) y la hora de finalización (cuando se envió la respuesta).
- Agente del usuario: el `user-agent` de la solicitud.
- Longitud del contenido: la `content-length` de la respuesta.

Secciones

Instrumentación de las solicitudes entrantes (.NET)

Para instrumentar las solicitudes que atiende su aplicación, llame a `RegisterXRay` en el método `Init` del archivo `global.asax`.

Example global.asax: controlador de mensajes

```
using System.Web.Http;
using Amazon.XRay.Recorder.Handlers.AspNet;

namespace SampleEBWebApplication
{
  public class MvcApplication : System.Web.HttpApplication
```

```
  {
    public override void Init()
    {
      base.Init();
      AWSXRayASPNET.RegisterXRay(this, "MyApp");
    }
  }
}
```

Instrumentación de las solicitudes entrantes (.NET Core)

Para instrumentar las solicitudes atendidas por la aplicación, llame al método `UseXRay` antes que a cualquier otro middleware del método `Configure` de su clase Startup, ya que lo ideal es que el middleware X-Ray sea el primer middleware en procesar la solicitud y el último en procesar la respuesta en el proceso.

> **Note**
>
> En el caso de .NET Core 2.0, si tiene un método `UseExceptionHandler` en la aplicación, asegúrese de llamar a `UseXRay` después del método `UseExceptionHandler` para asegurarse de que se registren las excepciones.

Example Startup.cs

<caption>.NET Core 2.1 and above</caption>

```
using Microsoft.AspNetCore.Builder;

public void Configure(IApplicationBuilder app, IHostingEnvironment env)
  {
    app.UseXRay("MyApp");
    // additional middleware
    ...
  }
```

<caption>.NET Core 2.0</caption>

```
using Microsoft.AspNetCore.Builder;

public void Configure(IApplicationBuilder app, IHostingEnvironment env)
  {
```

```
    app.UseExceptionHandler("/Error");
    app.UseXRay("MyApp");
    // additional middleware
    ...
}
```

El método `UseXRay` también puede tomar un objeto de configuración como segundo argumento.

```
app.UseXRay("MyApp", configuration);
```

Configuración de una estrategia de nomenclatura de segmentos

AWS X-Ray utiliza un nombre de servicio para identificar la aplicación y distinguirla del resto de aplicaciones, bases de datos, API externas y recursos de AWS utilizados por la aplicación. Cuando el SDK de X-Ray genera segmentos para las solicitudes entrantes, registra el nombre del servicio de la aplicación en el campo de nombre del segmento.

El SDK de X-Ray puede nombrar los segmentos utilizando el nombre de host en el encabezado de la solicitud HTTP. Sin embargo, este encabezado se puede falsificar, lo que podría provocar nodos inesperados en el mapa de servicio. Para evitar que el SDK nombre los segmentos de forma incorrecta debido a que las solicitudes tienen encabezados de host falsificados, debe especificar un nombre predeterminado para las solicitudes entrantes.

Si la aplicación atiende solicitudes de varios dominios, puede configurar el SDK para que utilice una estrategia de nomenclatura dinámica que refleje esto en los nombres de los segmentos. Una estrategia de nomenclatura dinámica permite al SDK usar el nombre de host para las solicitudes que coinciden con un patrón esperado y aplicar el nombre predeterminado a las solicitudes que no coincidan.

Por ejemplo, es posible que tenga una sola aplicación que atienda solicitudes a tres subdominios: `www.example.com`, `api.example.com` y `static.example.com`. Puede usar una estrategia de nomenclatura dinámica con el patrón `*.example.com` para identificar los segmentos de cada subdominio con un nombre diferente, lo que da como resultado tres nodos de servicio en el mapa de servicio. Si su aplicación recibe solicitudes con un nombre de host que no coincide con el patrón, verá un cuarto nodo en el mapa de servicio con el nombre alternativo que especifique.

Para utilizar el mismo nombre para todos los segmentos de solicitud, especifique el nombre de la aplicación cuando inicialice el controlador de mensajes, tal y como se muestra en la sección anterior. Esto tiene el mismo efecto que crear un `FixedSegmentNamingStrategy` y pasárselo al método `RegisterXRay`.

```
AWSXRayASPNET.RegisterXRay(this, new FixedSegmentNamingStrategy("MyApp"));
```

> **Note**
>
> Puede anular el nombre de servicio predeterminado que ha definido en el código mediante la AWS_XRAY_TRACING_NAMEvariable de entorno???.

Una estrategia de nomenclatura dinámica define un patrón con el que deben coincidir los nombres de host y un nombre predeterminado que se utiliza si el nombre de host de la solicitud HTTP no coincide con el patrón. Para asignar nombres a los segmentos dinámicamente, cree un objeto `DynamicSegmentNamingStrategy` y páseselo al método `RegisterXRay`.

```
AWSXRayASPNET.RegisterXRay(this, new DynamicSegmentNamingStrategy("MyApp",
 "*.example.com"));
```

Rastreo de llamadas AWS del SDK con el X-Ray SDK para .NET

Cuando la aplicación realiza llamadas Servicios de AWS para almacenar datos, escribir en una cola o enviar notificaciones, el X-Ray SDK for .NET rastrea las llamadas en sentido descendente en subsegmentos. El rastreo Servicios de AWS y los recursos a los que accede dentro de esos servicios (por ejemplo, un bucket de Amazon S3 o una cola de Amazon SQS) aparecen como nodos descendentes en el mapa de rastreo de la consola X-Ray.

Puede instrumentar a todos sus AWS SDK for .NET clientes llamando `RegisterXRayForAllServices` antes de crearlos.

Example SampleController.cs: instrumentación de cliente de DynamoDB

```
using Amazon;
using Amazon.Util;
using Amazon.DynamoDBv2;
using Amazon.DynamoDBv2.DocumentModel;
using Amazon.XRay.Recorder.Core;
using Amazon.XRay.Recorder.Handlers.AwsSdk;

namespace SampleEBWebApplication.Controllers
{
  public class SampleController : ApiController
  {
```

```
    AWSSDKHandler.RegisterXRayForAllServices();
    private static readonly Lazy<AmazonDynamoDBClient> LazyDdbClient = new
 Lazy<AmazonDynamoDBClient>(() =>
    {
      var client = new AmazonDynamoDBClient(EC2InstanceMetadata.Region ??
 RegionEndpoint.USEast1);
      return client;
    });
```

Si desea instrumentar clientes para algunos servicios y no para otros, llame a `RegisterXRay` en lugar de `RegisterXRayForAllServices`. Reemplace el texto resaltado por el nombre de la interfaz de cliente del servicio.

```
AWSSDKHandler.RegisterXRay<IAmazonDynamoDB>()
```

Para todos los servicios, puede ver el nombre de la API a la que se llama en la consola de X-Ray. Para un subconjunto de servicios, el SDK de X-Ray agrega información al segmento para proporcionar una mayor granularidad en el mapa de servicio.

Por ejemplo, cuando realiza una llamada con un cliente instrumentado de DynamoDB, el SDK agrega el nombre de tabla al segmento para las llamadas que se dirigen a una tabla. En la consola, cada tabla aparece como nodo independiente en el mapa de servicio, con un nodo genérico de DynamoDB para las llamadas que no se dirigen a una tabla.

Example Subsegmento para una llamada a DynamoDB con el fin de guardar un elemento

```
{
  "id": "24756640c0d0978a",
  "start_time": 1.480305974194E9,
  "end_time": 1.4803059742E9,
  "name": "DynamoDB",
  "namespace": "aws",
  "http": {
    "response": {
      "content_length": 60,
      "status": 200
    }
  },
  "aws": {
    "table_name": "scorekeep-user",
    "operation": "UpdateItem",
```

```
    "request_id": "UBQNSO5AEM8T4FDA4RQDEB94OVTDRVV4K4HIRGVJF66Q9ASUAAJG",
  }
}
```

Cuando accede a recursos designados, las llamadas a los siguientes servicios crean nodos adicionales en el mapa de servicio. Las llamadas que no están dirigidas a recursos concretos crean un nodo genérico en el servicio.

- Amazon DynamoDB: nombre de tabla
- Amazon Simple Storage Service: nombre de bucket y de clave
- Amazon Simple Queue Service: nombre de cola

Rastreo de llamadas a servicios web HTTP posteriores con el SDK de X-Ray para .NET

Cuando su aplicación realiza llamadas a microservicios o a las API de HTTP públicas, puede utilizar el método de extensión `GetResponseTraced` para `System.Net.HttpWebRequest` del SDK de X-Ray para .NET con el fin de instrumentar dichas llamadas y agregar la API al gráfico de servicios como servicio posterior.

Example HttpWebRequest

```
using System.Net;
using Amazon.XRay.Recorder.Core;
using Amazon.XRay.Recorder.Handlers.System.Net;

private void MakeHttpRequest()
{
  HttpWebRequest request = (HttpWebRequest)WebRequest.Create("http://names.example.com/
api");
  request.GetResponseTraced();
}
```

Para las llamadas asíncronas, utilice `GetAsyncResponseTraced`.

```
request.GetAsyncResponseTraced();
```

Si utiliza `system.net.http.httpclient`, utilice el controlador de delegación `HttpClientXRayTracingHandler` para registrar las llamadas.

Example HttpClient

```
using System.Net.Http;
using Amazon.XRay.Recorder.Core;
using Amazon.XRay.Recorder.Handlers.System.Net;

private void MakeHttpRequest()
{
  var httpClient = new HttpClient(new HttpClientXRayTracingHandler(new
 HttpClientHandler()));
  httpClient.GetAsync(URL);
}
```

Cuando se instrumenta una llamada a un API web posterior, el del SDK de X-Ray para .NET registra un subsegmento con información sobre la solicitud HTTP y la respuesta. X-Ray utiliza el subsegmento para generar un segmento inferido para la API.

Example Subsegmento para una llamada HTTP posterior

```
{
  "id": "004f72be19cddc2a",
  "start_time": 1484786387.131,
  "end_time": 1484786387.501,
  "name": "names.example.com",
  "namespace": "remote",
  "http": {
    "request": {
      "method": "GET",
      "url": "https://names.example.com/"
    },
    "response": {
      "content_length": -1,
      "status": 200
    }
  }
}
```

Example Segmento inferido para una llamada HTTP posterior

```
{
  "id": "168416dc2ea97781",
  "name": "names.example.com",
```

```
  "trace_id": "1-62be1272-1b71c4274f39f122afa64eab",
  "start_time": 1484786387.131,
  "end_time": 1484786387.501,
  "parent_id": "004f72be19cddc2a",
  "http": {
    "request": {
      "method": "GET",
      "url": "https://names.example.com/"
    },
    "response": {
      "content_length": -1,
      "status": 200
    }
  },
  "inferred": true
}
```

Rastreo de consultas SQL con el SDK de X-Ray para .NET

El SDK de X-Ray para .NET proporciona una clase de encapsulamiento `System.Data.SqlClient.SqlCommand` denominada `TraceableSqlCommand` que puede utilizar en lugar de `SqlCommand`. Puede inicializar un comando SQL con la clase `TraceableSqlCommand`.

Seguimiento de consultas SQL con métodos síncronos y asíncronos

Los siguientes ejemplos muestran cómo utilizar `TraceableSqlCommand` para rastrear automáticamente las consultas de SQL Server de forma síncrona y asíncrona.

Example **`Controller.cs`**: instrumentación de cliente de SQL (síncrono)

```
using Amazon;
using Amazon.Util;
using Amazon.XRay.Recorder.Core;
using Amazon.XRay.Recorder.Handlers.SqlServer;

private void QuerySql(int id)
{
  var connectionString = ConfigurationManager.AppSettings["RDS_CONNECTION_STRING"];
  using (var sqlConnection = new SqlConnection(connectionString))
  using (var sqlCommand = new TraceableSqlCommand("SELECT " + id, sqlConnection))
  {
    sqlCommand.Connection.Open();
    sqlCommand.ExecuteNonQuery();
```

```
  }
}
```

Puede ejecutar la consulta de forma asíncrona utilizando el método `ExecuteReaderAsync`.

Example **`Controller.cs`**: instrumentación de clientes de SQL (asíncronos)

```
using Amazon;
using Amazon.Util;
using Amazon.XRay.Recorder.Core;
using Amazon.XRay.Recorder.Handlers.SqlServer;
private void QuerySql(int id)
{
  var connectionString = ConfigurationManager.AppSettings["RDS_CONNECTION_STRING"];
  using (var sqlConnection = new SqlConnection(connectionString))
  using (var sqlCommand = new TraceableSqlCommand("SELECT " + id, sqlConnection))
  {
    await sqlCommand.ExecuteReaderAsync();
  }
}
```

Recopilación de consultas SQL realizadas a SQL Server

Puede habilitar la captura de `SqlCommand.CommandText` como parte del subsegmento creado por la consulta SQL. `SqlCommand.CommandText` aparece como el campo `sanitized_query` en el JSON del subsegmento. De forma predeterminada, esta característica está deshabilitada por motivos de seguridad.

> **Note**
>
> No habilite la característica de recopilación si está incluyendo información confidencial como texto sin cifrar en sus consultas SQL.

Puede habilitar la recopilación de consultas SQL de dos formas:

- Establezca la propiedad `CollectSqlQueries` en `true` en la configuración global de su aplicación.
- Establezca el parámetro `collectSqlQueries` de la instancia `TraceableSqlCommand` en `true` para recopilar llamadas dentro de la instancia.

Habilitar la propiedad CollectSqlQueries global

Los siguientes ejemplos muestran cómo habilitar la propiedad `CollectSqlQueries` para .NET y .NET Core.

.NET

Para establecer la propiedad `CollectSqlQueries` en `true` en la configuración global de su aplicación en .NET, modifique el `appsettings` de su archivo `Web.config` o `App.config`, tal y como se muestra.

Example **`App.config`** o bien **`Web.config`**: habilitación global de la recopilación de consultas SQL

```
<configuration>
<appSettings>
    <add key="CollectSqlQueries" value="true">
</appSettings>
</configuration>
```

.NET Core

Para establecer la propiedad `CollectSqlQueries` en `true` en la configuración global de su aplicación en .NET Core, modifique el archivo `appsettings.json` en la clave de X-Ray, tal y como se muestra.

Example **`appsettings.json`**: habilitación global de la recopilación de consultas SQL

```
{
  "XRay": {
    "CollectSqlQueries":"true"
  }
}
```

Habilitación del parámetro collectSqlQueries

Puede establecer el parámetro `collectSqlQueries` en la instancia `TraceableSqlCommand` en `true` para recopilar el texto de consulta SQL para las consultas de SQL Server realizadas con esa instancia. Si se establece el parámetro en `false` se deshabilita la característica `CollectSqlQuery` para la instancia `TraceableSqlCommand`.

> **Note**
>
> El valor de `collectSqlQueries` en la instancia `TraceableSqlCommand` anula el valor establecido en la configuración global de la propiedad `CollectSqlQueries`.

Example Ejemplo **`Controller.cs`**: habilitación de la recopilación de consultas SQL para la instancia

```
using Amazon;
using Amazon.Util;
using Amazon.XRay.Recorder.Core;
using Amazon.XRay.Recorder.Handlers.SqlServer;

private void QuerySql(int id)
{
  var connectionString = ConfigurationManager.AppSettings["RDS_CONNECTION_STRING"];
  using (var sqlConnection = new SqlConnection(connectionString))
  using (var command = new TraceableSqlCommand("SELECT " + id, sqlConnection,
 collectSqlQueries: true))
  {
    command.ExecuteNonQuery();
  }
}
```

Creación de subsegmentos adicionales

Los subsegmentos amplían el segmento de un rastro con detalles sobre el trabajo realizado para atender una solicitud. Cada vez que usted realiza una llamada con un cliente instrumentado, el SDK de X-Ray registra la información generada en un subsegmento. Puede crear subsegmentos adicionales para agrupar otros subsegmentos, medir el rendimiento de una sección de código o registrar anotaciones y metadatos.

Para administrar los subsegmentos, utilice los métodos `BeginSubsegment` y `EndSubsegment`. Realice el trabajo que desee en el subsegmento en un bloque `try` y utilice `AddException` para rastrear excepciones. Llame a `EndSubsegment` en un bloque `finally` para asegurarse de que el subsegmento está cerrado.

Example Controller.cs: subsegmento personalizado

```
AWSXRayRecorder.Instance.BeginSubsegment("custom method");
```

```
try
{
  DoWork();
}
catch (Exception e)
{
  AWSXRayRecorder.Instance.AddException(e);
}
finally
{
  AWSXRayRecorder.Instance.EndSubsegment();
}
```

Cuando crea un subsegmento dentro de un segmento o de otro subsegmento, el SDK de X-Ray para .NET genera un ID para dicho subsegmento y registra la hora de inicio y la hora de finalización.

Example Subsegmentos con metadatos

```
"subsegments": [{
  "id": "6f1605cd8a07cb70",
  "start_time": 1.480305974194E9,
  "end_time": 1.4803059742E9,
  "name": "Custom subsegment for UserModel.saveUser function",
  "metadata": {
    "debug": {
      "test": "Metadata string from UserModel.saveUser"
    }
  },
```

Agregue anotaciones y metadatos a los segmentos con el SDK de X-Ray para .NET

Puede usar anotaciones y metadatos para registrar información adicional sobre las solicitudes, el entorno o la aplicación. Puede añadir anotaciones y metadatos a los segmentos que crea el SDK de X-Ray o a los subsegmentos personalizados que cree usted mismo.

Las anotaciones son pares de clave-valor con valores de cadena, numéricos o booleanos. Las anotaciones se indexan para su uso con expresiones de filtro. Utilice anotaciones para registrar los datos que desee utilizar para agrupar rastros en la consola o cuando llame a la API de `GetTraceSummaries`.

Los metadatos son pares de clave-valor con valores de cualquier tipo, por ejemplo objetos y listas, pero que no se indexan para utilizarlos con expresiones de filtro. Utilice los metadatos para

registrar datos adicionales que desee almacenar en el rastro, pero que no necesite usar para hacer búsquedas.

Secciones

Registro de anotaciones con el SDK de X-Ray para .NET

Utilice anotaciones para registrar información sobre segmentos o subsegmentos que desee indexar para las búsquedas.

Se requiere lo siguiente para todas las anotaciones de X-Ray:

Requisitos de anotación

- Teclas: la clave de una anotación de X-Ray puede tener hasta 500 caracteres alfanuméricos. No puede utilizar espacios ni símbolos distintos del símbolo de subrayado (_).
- Valores: el valor de una anotación de X-Ray puede tener hasta 1000 caracteres Unicode.
- Número de anotaciones: puede utilizar hasta 50 anotaciones por traza.

Para grabar anotaciones fuera de una función AWS Lambda

1. Obtenga una instancia de `AWSXRayRecorder`.

   ```
   using Amazon.XRay.Recorder.Core;
   ...
   AWSXRayRecorder recorder = AWSXRayRecorder.Instance;
   ```

2. Llame a `addAnnotation` con una clave de cadena y un valor booleano, Int32, Int64, doble o de cadena.

   ```
   recorder.AddAnnotation("mykey", "my value");
   ```

Para grabar anotaciones dentro de una función AWS Lambda

Tanto los segmentos como los subsegmentos de una función Lambda se administran mediante el entorno de ejecución de Lambda. Si desea añadir una anotación a un segmento o subsegmento dentro de una función Lambda, debe hacer lo siguiente:

1. Cree el segmento o subsegmento dentro de la función Lambda.
2. Añada la anotación al segmento o subsegmento.
3. Finalice el segmento o subsegmento.

El siguiente ejemplo de código muestra cómo añadir una anotación a un subsegmento dentro de una función Lambda:

```
#Create the subsegment
AWSXRayRecorder.Instance.BeginSubsegment("custom method");
#Add an annotation
AWSXRayRecorder.Instance.AddAnnotation("My", "Annotation");
try
{
  YourProcess(); #Your function
}
catch (Exception e)
{
  AWSXRayRecorder.Instance.AddException(e);
}
finally #End the subsegment
{
  AWSXRayRecorder.Instance.EndSubsegment();
}
```

El SDK de X-Ray registra las anotaciones como pares clave-valor en un `annotations` objeto del documento de segmento. Si se llama a la `addAnnotation` operación dos veces con la misma clave, se sobrescribe un valor previamente registrado en el mismo segmento o subsegmento.

Para encontrar rastros que tengan anotaciones con valores específicos, utilice la palabra clave `annotations.key` en una expresión de filtro.

Registro de metadatos con el SDK de X-Ray para .NET

Usa los metadatos para registrar información sobre segmentos o subsegmentos que no necesites indexar para utilizarla en una búsqueda. Los valores de los metadatos pueden ser cadenas,

números, valores booleanos o cualquier otro objeto que se pueda serializar en un objeto o matriz JSON.

Para registrar metadatos

1. Obtenga una instancia de`AWSXRayRecorder`, como se muestra en el siguiente ejemplo de código:

```
using Amazon.XRay.Recorder.Core;
...
AWSXRayRecorder recorder = AWSXRayRecorder.Instance;
```

2. Llama `AddMetadata` con un espacio de nombres de cadena, una clave de cadena y un valor de objeto, como se muestra en el siguiente ejemplo de código:

```
recorder.AddMetadata("my namespace", "my key", "my value");
```

   También puede llamar a la `AddMetadata` operación utilizando solo un par de clave y valor, como se muestra en el siguiente ejemplo de código:

```
recorder.AddMetadata("my key", "my value");
```

Si no especificas un valor para el espacio de nombres, el SDK de X-Ray lo utilizará. `default` Si se llama a la `AddMetadata` operación dos veces con la misma clave, se sobrescribe un valor previamente registrado en el mismo segmento o subsegmento.

Cómo instrumentar tu aplicación con Ruby

Puede instrumentar su aplicación Ruby de dos maneras para enviar rastros a X-Ray:

- AWS Distro for OpenTelemetry Ruby: una AWS distribución que proporciona un conjunto de bibliotecas de código abierto para enviar métricas y rastreos correlacionados a múltiples soluciones de AWS monitoreo, incluidas Amazon y Amazon OpenSearch Service CloudWatch AWS X-Ray, a través de AWS Distro for Collector. OpenTelemetry
- AWS X-Ray SDK para Ruby: conjunto de bibliotecas para generar y enviar trazas a X-Ray mediante el daemon X-Ray.

Para obtener más información, consulte Cómo elegir entre los AWS SDK Distro for OpenTelemetry y X-Ray.

AWS Distro para OpenTelemetry Ruby

Con AWS Distro para OpenTelemetry (ADOT) Ruby, puede instrumentar sus aplicaciones una vez y enviar métricas y rastros correlacionados a varias soluciones de supervisión de AWS, incluidas Amazon CloudWatch, AWS X-Ray y Amazon OpenSearch Service. El uso de X-Ray con ADOT requiere dos componentes: un SDK de OpenTelemetry habilitado para su uso con X-Ray y AWS Distro para OpenTelemetry Collector habilitado para su uso con X-Ray.

Para empezar, consulte la documentación de AWS Distro para OpenTelemetry Ruby.

Para obtener más información sobre el uso de AWS Distro para OpenTelemetry con AWS X-Ray y otros Servicios de AWS, consulte AWS Distro para OpenTelemetry o la documentación de AWS Distro para OpenTelemetry.

Para obtener información adicional sobre los lenguajes compatibles y el uso, consulte AWS Observability en GitHub.

AWS X-Ray SDK for Ruby

El SDK de X-Ray es una biblioteca para las aplicaciones web de Ruby que proporciona clases y métodos para generar y enviar datos de rastreo al daemon de X-Ray. Los datos de rastreo incluyen información sobre las solicitudes HTTP entrantes atendidas por la aplicación y las llamadas que la aplicación realiza a los servicios descendentes mediante el AWS SDK, los clientes HTTP o un cliente de registro activo. También puede crear segmentos de forma manual y agregar información de depuración en anotaciones y metadatos.

Puede descargar el SDK añadiéndolo a su archivo Gemfile y ejecutando `bundle install`.

Example Archivo Gemfile

```
gem 'aws-sdk'
```

Si utiliza Rails, en primer lugar añada el middleware del SDK de X-Ray para rastrear las solicitudes entrantes. Un filtro de solicitudes crea un segmento. Mientras el segmento está abierto, puede utilizar los métodos del cliente del SDK para añadir información al segmento y crear subsegmentos para rastrear llamadas posteriores. El SDK también registra automáticamente las excepciones que

produce su aplicación mientras el segmento está abierto. Para las aplicaciones que no son de Rails, puede crear segmentos manualmente.

A continuación, utilice el SDK de X-Ray para AWS SDK for Ruby instrumentar sus clientes HTTP y SQL configurando la grabadora para que aplique parches a las bibliotecas asociadas. Cada vez que realizas una llamada a un recurso Servicio de AWS o a un flujo con un cliente instrumentado, el SDK registra la información sobre la llamada en un subsegmento. Servicios de AWS y los recursos a los que accedes desde los servicios aparecen como nodos descendentes en el mapa de rastreo para ayudarte a identificar los errores y los problemas de limitación en las conexiones individuales.

En cuanto empiece a utilizar el SDK, personalice su comportamiento configurando la grabadora. Puede añadir complementos para registrar datos sobre los recursos informáticos que ejecutan la aplicación, personalizar el comportamiento de muestreo mediante la definición de reglas de muestreo y proporcionar un registrador para ver más o menos información del SDK en los logs de la aplicación.

Registre información adicional acerca de las solicitudes y el trabajo que la aplicación realiza en anotaciones y metadatos. Las anotaciones son pares sencillos de clave-valor que se indexan para su uso con expresiones de filtro para poder buscar rastros que contengan datos específicos. Las entradas de metadatos son menos restrictivas y pueden registrar objetos y matrices completos, es decir, todo lo que se pueda serializar en JSON.

> **Anotaciones y metadatos**
>
> Las anotaciones y los metadatos son texto arbitrario que se agrega a los segmentos con el SDK de X-Ray. Las anotaciones se indexan para su uso con expresiones de filtro. Los metadatos no se indexan pero se pueden ver en el segmento sin procesar con la consola o la API de X-Ray. Cualquier persona a la que conceda acceso de lectura a X-Ray puede ver estos datos.

Cuando tenga muchos clientes instrumentados en su código, un único segmento de solicitud puede contener un gran número de subsegmentos, uno para cada llamada realizada con un cliente instrumentado. Puede organizar y agrupar los subsegmentos incluyendo las llamadas del cliente en subsegmentos personalizados. Puede crear un subsegmento personalizado para una función completa o para cualquier sección de código, y registrar los metadatos y las anotaciones en el subsegmento en lugar de escribirlo todo en el segmento principal.

Para acceder a la documentación de referencia de las clases y los métodos del SDK, consulte la Referencia de la API del SDK de AWS X-Ray para Ruby.

Requisitos

El SDK de X-Ray requiere Ruby 2.3 o posterior y es compatible con las siguientes bibliotecas:

- AWS SDK for Ruby versión 3.0 o posterior
- Rails versión 5.1 o posterior

Configuración del SDK de X-Ray para Ruby

El SDK de X-Ray para Ruby tiene una clase denominada `XRay.recorder` que proporciona la grabadora global. Puede configurar la grabadora global para que personalice el middleware que crea los segmentos para las llamadas HTTP entrantes.

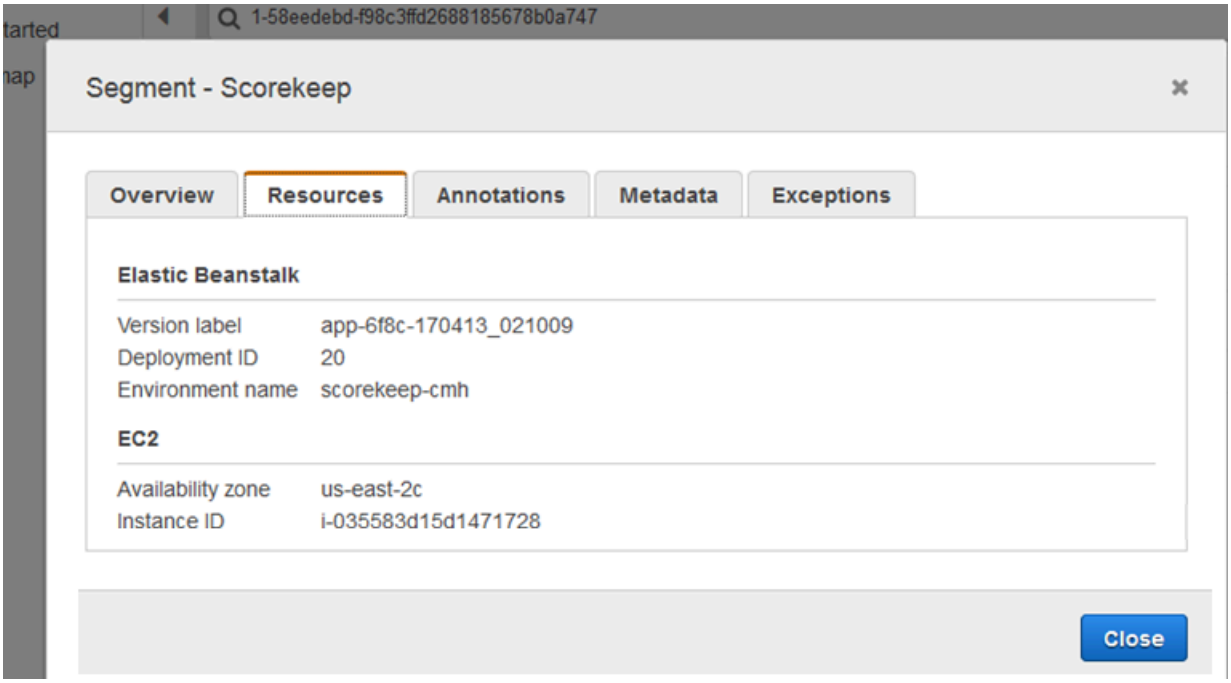
Secciones

Complementos del servicio

Utilice `plugins` para registrar información sobre el servicio que aloja la aplicación.

Complementos

- Amazon EC2: `ec2` añade el ID y la zona de disponibilidad de la instancia.
- Elastic Beanstalk: `elastic_beanstalk` añade el nombre de entorno, la etiqueta de versión y el ID de implementación.
- Amazon ECS: `ecs` agrega el ID de contenedor.



Para utilizar complementos, especifíquelos en el objeto de configuración que se pasa a la grabadora.

Example main.rb: configuración de complementos

```
my_plugins = %I[ec2 elastic_beanstalk]

config = {
  plugins: my_plugins,
  name: 'my app',
}

XRay.recorder.configure(config)
```

También puede utilizar las variables de entorno, que tienen prioridad frente a los valores establecidos en código, para configurar la grabadora.

El SDK también usa la configuración del complemento para establecer el campo `origin` en el segmento. Eso indica el tipo de recurso de AWS que ejecuta la aplicación. Cuando utiliza varios complementos, el SDK utiliza el siguiente orden de resolución para determinar el origen: ElasticBeanstalk > EKS > ECS > EC2.

Reglas de muestreo

El SDK utiliza las reglas de muestreo que define el usuario en la consola de X-Ray para determinar qué solicitudes registrar. La regla predeterminada rastrea la primera solicitud cada segundo y el

5 % de las solicitudes adicionales de todos los servicios que envían rastros a X-Ray. Cree reglas adicionales en la consola de X-Ray para personalizar la cantidad de datos registrados para cada una de sus aplicaciones.

El SDK aplica las reglas personalizadas en el orden en que se definen. Si una solicitud coincide con varias reglas personalizadas, el SDK solo aplica la primera regla.

> **Note**
>
> Si el SDK no puede comunicarse con X-Ray para obtener las reglas de muestreo, vuelve a una regla local predeterminada de la primera solicitud cada segundo y del 5 % de las solicitudes adicionales por host. Eso puede ocurrir si el host no tiene permiso para llamar a las API de muestreo o no puede conectarse al daemon de X-Ray, que actúa como proxy TCP para las llamadas a las API realizadas por el SDK.

También puedes configurar el SDK para que cargue las reglas de muestreo desde un documento JSON. El SDK puede usar las reglas locales como respaldo para los casos en que el muestreo de X-Ray no esté disponible, o puede usar las reglas locales exclusivamente.

Example sampling-rules.json

```
{
  "version": 2,
  "rules": [
    {
      "description": "Player moves.",
      "host": "*",
      "http_method": "*",
      "url_path": "/api/move/*",
      "fixed_target": 0,
      "rate": 0.05
    }
  ],
  "default": {
    "fixed_target": 1,
    "rate": 0.1
  }
}
```

En este ejemplo se define una regla personalizada y una regla predeterminada. La regla personalizada aplica un porcentaje de muestreo del 5 % sin un número mínimo de solicitudes de rastreo para las rutas incluidas bajo `/api/move/`. La regla predeterminada rastrea la primera solicitud cada segundo y el 10 % de las solicitudes adicionales.

La desventaja de definir las reglas localmente es que el objetivo establecido lo aplica cada instancia de la grabadora de forma independiente, en lugar de ser administrado por el servicio de X-Ray. A medida que se implementan más hosts, el porcentaje establecido se multiplica, lo que dificulta el control de la cantidad de datos registrados.

Para configurar reglas de copia de seguridad, defina un hash para el documento en el objeto de configuración que se pasa a la grabadora.

Example main.rb: configuración de la regla de copia de seguridad

```
require 'aws-xray-sdk'
my_sampling_rules =  {
  version: 1,
  default: {
    fixed_target: 1,
    rate: 0.1
  }
}
config = {
  sampling_rules: my_sampling_rules,
  name: 'my app',
}
XRay.recorder.configure(config)
```

Para almacenar las reglas de muestreo por separado, defina el hash en un archivo independiente y haga que el archivo lo incorpore a la aplicación.

Example config/sampling-rules.rb

```
my_sampling_rules =  {
  version: 1,
  default: {
    fixed_target: 1,
    rate: 0.1
  }
}
```

Example main.rb: regla de muestreo desde un archivo

```
require 'aws-xray-sdk'
require 'config/sampling-rules.rb'

config = {
  sampling_rules: my_sampling_rules,
  name: 'my app',
}
XRay.recorder.configure(config)
```

Para utilizar solo reglas locales, requiera las reglas de muestreo y configure el `LocalSampler`.

Example main.rb: muestreo con reglas locales

```
require 'aws-xray-sdk'
require 'aws-xray-sdk/sampling/local/sampler'

config = {
  sampler: LocalSampler.new,
  name: 'my app',
}
XRay.recorder.configure(config)
```

También puede configurar la grabadora global para deshabilitar el muestreo e instrumentar todas las solicitudes entrantes.

Example main.rb: inhabilitar el muestreo

```
require 'aws-xray-sdk'
config = {
  sampling: false,
  name: 'my app',
}
XRay.recorder.configure(config)
```

Registro

De forma predeterminada, la grabadora muestra los eventos de nivel informativo en `$stdout`. Puede personalizar el registro mediante la definición de un registrador en el objeto de configuración que se pasa a la grabadora.

Example main.rb: registro

```
require 'aws-xray-sdk'
config = {
  logger: my_logger,
  name: 'my app',
}
XRay.recorder.configure(config)
```

Utilice registros de depuración para identificar problemas como la presencia de subsegmentos sin cerrar al generar subsegmentos de forma manual.

Configuración de la grabadora en código

Hay disponibles ajustes adicionales a partir del método `configure` en `XRay.recorder`.

- `context_missing`: establezca esta opción en `LOG_ERROR` para evitar que se produzcan excepciones cuando el código instrumentado intente registrar datos sin que haya ningún segmento abierto.
- `daemon_address`: establezca el host y el puerto del oyente del daemon de X-Ray.
- `name`: establezca un nombre de servicio que el SDK utiliza para los segmentos.
- `naming_pattern`: establezca un patrón de asignación de nombres de dominio para utilizar la nomenclatura dinámica.
- `plugins`: registre información acerca de los recursos de AWS de su aplicación con complementos.
- `sampling`: establezca esta opción en `false` para deshabilitar el muestreo.
- `sampling_rules`: establezca el hash que contiene las reglas de muestreo.

Example main.rb: deshabilite excepciones de falta de contexto

```
require 'aws-xray-sdk'
config = {
  context_missing: 'LOG_ERROR'
}

XRay.recorder.configure(config)
```

Configuración de la grabadora con Rails

Si utiliza el marco de trabajo Rails, puede configurar las opciones de la grabadora global en un archivo de Ruby situado en `app_root/initializers`. El SDK de X-Ray admite una clave de configuración adicional para su uso con Rails.

- `active_record`: establezca esta opción en `true` para registrar subsegmentos para las transacciones de la base de datos de grabación activa.

Configure los ajustes disponibles en un objeto de configuración denominado `Rails.application.config.xray`.

Example config/initializers/aws_xray.rb

```
Rails.application.config.xray = {
  name: 'my app',
  patch: %I[net_http aws_sdk],
  active_record: true
}
```

Variables de entorno

Puede usar variables de entorno con el fin de configurar el SDK de X-Ray para Ruby. El SDK admite las siguientes variables:

- `AWS_XRAY_TRACING_NAME`: establezca un nombre de servicio que el SDK utiliza para los segmentos. Anula el nombre de servicio que se ha establecido en la estrategia de nomenclatura de segmento del filtro de servlet.
- `AWS_XRAY_DAEMON_ADDRESS`: establezca el host y el puerto del oyente del daemon de X-Ray. De forma predeterminada, el SDK envía los datos de rastreo a `127.0.0.1:2000`. Use esta variable si ha configurado el daemon para que escuche en un puerto diferente o si se ejecuta en un host diferente.
- `AWS_XRAY_CONTEXT_MISSING`: establezca esta opción en `RUNTIME_ERROR` para generar excepciones cuando el código instrumentado intente registrar datos sin que haya ningún segmento abierto.

  Valores válidos

  - `RUNTIME_ERROR`: lance una excepción de tiempo de ejecución.

- `LOG_ERROR`: registre un error y continúe (predeterminado).
- `IGNORE_ERROR`: ignore el error y continúe.

Se pueden producir errores relativos a segmentos o subsegmentos inexistentes al intentar usar un cliente instrumentado en el código de inicio que se ejecuta cuando no hay ninguna solicitud abierta o en el código que inicia un nuevo subproceso.

Las variables de entorno anulan los valores establecidos en el código.

Rastreo de las solicitudes entrantes con el SDK de X-Ray para middleware de Ruby

Puede usar el SDK de X-Ray para rastrear las solicitudes HTTP entrantes que su aplicación sirve en una instancia EC2 de Amazon EC2 AWS Elastic Beanstalk o Amazon ECS.

Si utiliza Rails, use el middleware de Rails para instrumentar las solicitudes HTTP entrantes. Cuando añade el middleware a su aplicación y configura un nombre de segmento, el SDK de X-Ray para Ruby crea un segmento para cada solicitud muestreada. Cualquier segmento que se haya creado con instrumentación adicional se convierte en subsegmentos del segmento en nivel de la solicitud, el cual provee información sobre la solicitud HTTP y la respuesta. Esta información incluye el momento, el método y la disposición de la solicitud.

Cada segmento tiene un nombre que identifica la aplicación en el mapa de servicio. El nombre del segmento se puede asignar de forma estática o se puede configurar el SDK para que le asigne un nombre dinámico en función del encabezado del host de la solicitud entrante. La nomenclatura dinámica permite agrupar los rastros en función del nombre de dominio de la solicitud y aplicar un nombre predeterminado si el nombre no coincide con el patrón esperado (por ejemplo, si el encabezado del host está falsificado).

> **Solicitudes reenviadas**
>
> Si un equilibrador de carga u otro intermediario reenvía una solicitud a la aplicación, X-Ray toma la IP de cliente del encabezado `X-Forwarded-For` de la solicitud en lugar de tomar la IP de origen del paquete IP. La IP de cliente que se graba para una solicitud reenviada puede estar falsificada, por lo que no se debe confiar en ella.

Cuando se reenvía una solicitud, el SDK crea un campo adicional en el segmento para indicar que se realizó esta acción. Si el segmento contiene el campo `x_forwarded_for` configurado en `true`, el IP del cliente se obtiene a partir del encabezado `X-Forwarded-For` en la solicitud HTTP.

El middleware crea un segmento para cada solicitud entrante con un bloque `http` que contiene la siguiente información:

- Método HTTP: GET, POST, PUT, DELETE, etc.
- Dirección del cliente: la dirección IP del cliente que envió la solicitud.
- Código de respuesta: el código de respuesta HTTP para la solicitud finalizada.
- Intervalo: la hora de inicio (cuando se recibió la solicitud) y la hora de finalización (cuando se envió la respuesta).
- Agente del usuario: el `user-agent` de la solicitud.
- Longitud del contenido: la `content-length` de la respuesta.

Uso del middleware de Rails

Para utilizar el middleware, actualice el archivo Gemfile para que incluya el railtie necesario.

Example Archivo Gemfile: rails

```
gem 'aws-xray-sdk', require: ['aws-xray-sdk/facets/rails/railtie']
```

Para usar el middleware, también debe configurar la grabadora con un nombre que represente la aplicación en el mapa de rastreo.

Example config/initializers/aws_xray.rb

```
Rails.application.config.xray = {
  name: 'my app'
}
```

Instrumentación manual del código

Si no utiliza Rails, cree los segmentos manualmente. Puede crear un segmento para cada solicitud entrante o crear segmentos en torno a los clientes HTTP o AWS SDK parcheados para proporcionar un contexto que permita a la grabadora añadir subsegmentos.

```
# Start a segment
```

```
segment = XRay.recorder.begin_segment 'my_service'
# Start a subsegment
subsegment = XRay.recorder.begin_subsegment 'outbound_call', namespace: 'remote'

# Add metadata or annotation here if necessary
my_annotations = {
  k1: 'v1',
  k2: 1024
}
segment.annotations.update my_annotations

# Add metadata to default namespace
subsegment.metadata[:k1] = 'v1'

# Set user for the segment (subsegment is not supported)
segment.user = 'my_name'

# End segment/subsegment
XRay.recorder.end_subsegment
XRay.recorder.end_segment
```

Configuración de una estrategia de nomenclatura de segmentos

AWS X-Ray utiliza un nombre de servicio para identificar la aplicación y distinguirla del resto de aplicaciones, bases de datos, API externas y AWS recursos que utiliza la aplicación. Cuando el SDK de X-Ray genera segmentos para las solicitudes entrantes, registra el nombre del servicio de la aplicación en el campo de nombre del segmento.

El SDK de X-Ray puede nombrar los segmentos utilizando el nombre de host en el encabezado de la solicitud HTTP. Sin embargo, este encabezado se puede falsificar, lo que podría provocar nodos inesperados en el mapa de servicio. Para evitar que el SDK nombre los segmentos de forma incorrecta debido a que las solicitudes tienen encabezados de host falsificados, debe especificar un nombre predeterminado para las solicitudes entrantes.

Si la aplicación atiende solicitudes de varios dominios, puede configurar el SDK para que utilice una estrategia de nomenclatura dinámica que refleje esto en los nombres de los segmentos. Una estrategia de nomenclatura dinámica permite al SDK usar el nombre de host para las solicitudes que coinciden con un patrón esperado y aplicar el nombre predeterminado a las solicitudes que no coincidan.

Por ejemplo, es posible que tenga una sola aplicación que atienda solicitudes a tres subdominios: `www.example.com`, `api.example.com` y `static.example.com`. Puede usar una estrategia

de nomenclatura dinámica con el patrón `*.example.com` para identificar los segmentos de cada subdominio con un nombre diferente, lo que da como resultado tres nodos de servicio en el mapa de servicio. Si su aplicación recibe solicitudes con un nombre de host que no coincide con el patrón, verá un cuarto nodo en el mapa de servicio con el nombre alternativo que especifique.

Si desea utilizar el mismo nombre para todos los segmentos de solicitud, especifique el nombre de la aplicación cuando configure la grabadora, como se muestra en las secciones anteriores.

Una estrategia de nomenclatura dinámica define un patrón con el que deben coincidir los nombres de host y un nombre predeterminado que se utiliza si el nombre de host de la solicitud HTTP no coincide con el patrón. Para asignar nombre a los segmentos de forma dinámica, especifique un patrón de nomenclatura en el hash config.

Example main.rb: nomenclatura dinámica

```
config = {
  naming_pattern: '*mydomain*',
  name: 'my app',
}

XRay.recorder.configure(config)
```

Puede utilizar "*" en el patrón para buscar coincidencia con cualquier cadena o "?" para buscar coincidencias con cualquier carácter único.

> **Note**
>
> Puede anular el nombre de servicio predeterminado que ha definido en el código mediante la `AWS_XRAY_TRACING_NAME`variable de entorno???.

Aplicación de parches a bibliotecas para instrumentar llamadas posteriores

Para instrumentar llamadas posteriores, utilice el SDK de X-Ray para Ruby con el fin de aplicar parches a las bibliotecas que utiliza la aplicación. El SDK de X-Ray para Ruby puede aplicar parches a las siguientes bibliotecas.

Bibliotecas compatibles

- `net/http`: instrumente clientes HTTP.

- `aws-sdk`: instrumente clientes de AWS SDK for Ruby.

Al utilizar una biblioteca con parches, el SDK de X-Ray para Ruby crea un subsegmento para la llamada y registra información desde la solicitud y la respuesta. Debe haber un segmento disponible para que el SDK cree el subsegmento, ya sea desde el middleware del SDK o mediante una llamada a `XRay.recorder.begin_segment`.

Para aplicar parches a las bibliotecas, especifíquelos en el objeto de configuración que se pasa a la grabadora de X-Ray.

Example main.rb: aplique parches a las bibliotecas

```
require 'aws-xray-sdk'

config = {
  name: 'my app',
  patch: %I[net_http aws_sdk]
}

XRay.recorder.configure(config)
```

Rastreo de llamadas al AWS SDK con el SDK de X-Ray para Ruby

Cuando tu aplicación realiza llamadas Servicios de AWS para almacenar datos, escribir en una cola o enviar notificaciones, el X-Ray SDK for Ruby rastrea las llamadas en sentido descendente en subsegmentos. El rastreo Servicios de AWS y los recursos a los que accede dentro de esos servicios (por ejemplo, un bucket de Amazon S3 o una cola de Amazon SQS) aparecen como nodos descendentes en el mapa de rastreo de la consola X-Ray.

El X-Ray SDK for Ruby instrumenta automáticamente todos los clientes AWS del SDK cuando se aplica un parche a la `aws-sdk` biblioteca. No puede instrumentar clientes individuales.

Para todos los servicios, puede ver el nombre de la API a la que se llama en la consola de X-Ray. Para un subconjunto de servicios, el SDK de X-Ray agrega información al segmento para proporcionar una mayor granularidad en el mapa de servicio.

Por ejemplo, cuando realiza una llamada con un cliente instrumentado de DynamoDB, el SDK agrega el nombre de tabla al segmento para las llamadas que se dirigen a una tabla. En la consola, cada tabla aparece como nodo independiente en el mapa de servicio, con un nodo genérico de DynamoDB para las llamadas que no se dirigen a una tabla.

Example Subsegmento para una llamada a DynamoDB con el fin de guardar un elemento

```
{
  "id": "24756640c0d0978a",
  "start_time": 1.480305974194E9,
  "end_time": 1.4803059742E9,
  "name": "DynamoDB",
  "namespace": "aws",
  "http": {
    "response": {
      "content_length": 60,
      "status": 200
    }
  },
  "aws": {
    "table_name": "scorekeep-user",
    "operation": "UpdateItem",
    "request_id": "UBQNSO5AEM8T4FDA4RQDEB94OVTDRVV4K4HIRGVJF66Q9ASUAAJG",
  }
}
```

Cuando accede a recursos designados, las llamadas a los siguientes servicios crean nodos adicionales en el mapa de servicio. Las llamadas que no están dirigidas a recursos concretos crean un nodo genérico en el servicio.

- Amazon DynamoDB: nombre de tabla
- Amazon Simple Storage Service: nombre de bucket y de clave
- Amazon Simple Queue Service: nombre de cola

Generación de subsegmentos personalizados con el SDK de X-Ray

Los subsegmentos amplían el segmento de un rastro con detalles sobre el trabajo realizado para atender una solicitud. Cada vez que usted realiza una llamada con un cliente instrumentado, el SDK de X-Ray registra la información generada en un subsegmento. Puede crear subsegmentos adicionales para agrupar otros subsegmentos, medir el rendimiento de una sección de código o registrar anotaciones y metadatos.

Para administrar los subsegmentos, utilice los métodos `begin_subsegment` y `end_subsegment`.

```
subsegment = XRay.recorder.begin_subsegment name: 'annotations', namespace: 'remote'
```

```
my_annotations = { id: 12345 }
subsegment.annotations.update my_annotations
XRay.recorder.end_subsegment
```

Para crear un subsegmento para una función, encapsúlelo en una llamada a `XRay.recorder.capture`.

```
XRay.recorder.capture('name_for_subsegment') do |subsegment|
  resp = myfunc() # myfunc is your function
  subsegment.annotations.update k1: 'v1'
  resp
end
```

Cuando crea un subsegmento dentro de un segmento o de otro subsegmento, el SDK de X-Ray genera un ID para dicho subsegmento y registra la hora de inicio y la hora de finalización.

Example Subsegmentos con metadatos

```
"subsegments": [{
  "id": "6f1605cd8a07cb70",
  "start_time": 1.480305974194E9,
  "end_time": 1.4803059742E9,
  "name": "Custom subsegment for UserModel.saveUser function",
  "metadata": {
    "debug": {
      "test": "Metadata string from UserModel.saveUser"
    }
  },
```

Adición de anotaciones y metadatos a los segmentos con el SDK de X-Ray para Ruby

Puede usar anotaciones y metadatos para registrar información adicional sobre las solicitudes, el entorno o la aplicación. Puede añadir anotaciones y metadatos a los segmentos que crea el SDK de X-Ray o a los subsegmentos personalizados que cree usted mismo.

Las anotaciones son pares de clave-valor con valores de cadena, numéricos o booleanos. Las anotaciones se indexan para su uso con expresiones de filtro. Utilice anotaciones para registrar los datos que desee utilizar para agrupar rastros en la consola o cuando llame a la API de `GetTraceSummaries`.

Los metadatos son pares de clave-valor con valores de cualquier tipo, por ejemplo objetos y listas, pero que no se indexan para utilizarlos con expresiones de filtro. Utilice los metadatos para registrar datos adicionales que desee almacenar en el rastro, pero que no necesite usar para hacer búsquedas.

Además de anotaciones y metadatos, también puede registrar cadenas de ID de usuario en los segmentos. Los identificadores de usuario se registran en un campo aparte en segmentos y se indexan para su uso con la búsqueda.

Secciones

- Registro de anotaciones con el SDK de X-Ray para Ruby
- Registro de metadatos con el SDK de X-Ray para Ruby
- Registro de ID de usuario con el SDK de X-Ray para Ruby

Registro de anotaciones con el SDK de X-Ray para Ruby

Utilice anotaciones para registrar información sobre segmentos o subsegmentos que desee indexar para las búsquedas.

Requisitos de anotación

- Teclas: la clave de una anotación de X-Ray puede tener hasta 500 caracteres alfanuméricos. No puede utilizar espacios ni símbolos distintos del símbolo de subrayado (_).
- Valores: el valor de una anotación de X-Ray puede tener hasta 1000 caracteres Unicode.
- Número de anotaciones: puede utilizar hasta 50 anotaciones por traza.

Para registrar anotaciones

1. Obtenga una referencia al segmento o subsegmento actual desde `xray_recorder`.

```
require 'aws-xray-sdk'
...
document = XRay.recorder.current_segment
```

o

```
require 'aws-xray-sdk'
...
```

```
document = XRay.recorder.current_subsegment
```

2. Llame a `update` con un valor hash.

```
my_annotations = { id: 12345 }
document.annotations.update my_annotations
```

El SDK registra las anotaciones como pares de clave-valor en un objeto `annotations` del documento de segmento. Si llama dos veces a `add_annotations` con la misma clave, se sobrescriben los valores previamente registrados en ese segmento o subsegmento.

Para encontrar rastros que tengan anotaciones con valores específicos, utilice la palabra clave `annotations.`*`key`* en una expresión de filtro.

Registro de metadatos con el SDK de X-Ray para Ruby

Utilice los metadatos para registrar información sobre segmentos o subsegmentos que no necesite indexar para las búsquedas. Los valores de metadatos pueden ser cadenas, números, booleanos o cualquier objeto que se pueda serializar en un objeto o matriz JSON.

Para registrar metadatos

1. Obtenga una referencia al segmento o subsegmento actual desde `xray_recorder`.

```
require 'aws-xray-sdk'
...
document = XRay.recorder.current_segment
```

o

```
require 'aws-xray-sdk'
...
document = XRay.recorder.current_subsegment
```

2. Llame a `metadata` con una clave de cadena; un valor booleano, numérico, de cadena o de objeto y un espacio de nombres de cadena.

```
my_metadata = {
  my_namespace: {
    key: 'value'
```

```
  }
}
subsegment.metadata my_metadata
```

Si llama dos veces a `metadata` con la misma clave, se sobrescriben los valores previamente registrados en ese segmento o subsegmento.

Registro de ID de usuario con el SDK de X-Ray para Ruby

Registre identificadores de usuario en segmentos de solicitud para identificar al usuario que envió la solicitud.

Para registrar identificadores de usuario

1. Obtenga una referencia al segmento actual desde `xray_recorder`.

   ```
   require 'aws-xray-sdk'
   ...
   document = XRay.recorder.current_segment
   ```

2. Especifique el ID de cadena del usuario que envió la solicitud en el campo de usuario del segmento.

   ```
   segment.user = 'U12345'
   ```

Puede establecer el usuario en los controladores para registrar el ID de usuario tan pronto como la aplicación comience a procesar la solicitud.

Para buscar rastros de un ID de usuario, utilice la palabra clave `user` en una expresión de filtro.

Integración AWS X-Ray con otros Servicios de AWS

Muchos Servicios de AWS ofrecen distintos niveles de integración de X-Ray, como el muestreo y la adición de encabezados a las solicitudes entrantes, la ejecución del daemon X-Ray y el envío automático de datos de rastreo a X-Ray. La integración en X-Ray puede incluir lo siguiente:

- Instrumentación activa: realiza un muestreo de las solicitudes entrantes y las instrumenta.
- Instrumentación pasiva: instrumenta solicitudes cuyo muestreo lo realizó otro servicio.
- Rastreo de solicitudes: agrega un encabezado de rastreo a todas las solicitudes entrantes y lo propaga.
- Herramientas: ejecuta el daemon de X-Ray para recibir segmentos del SDK de X-Ray.

> **Note**
>
> Los SDK de X-Ray incluyen complementos para una integración adicional con Servicios de AWS. Por ejemplo, puede utilizar el complemento Elastic Beanstalk del SDK de X-Ray para Java con el fin de agregar información acerca del entorno de Elastic Beanstalk que ejecuta su aplicación, incluidos el nombre e ID del entorno.

Estos son algunos ejemplos de los Servicios de AWS que están integrados con X-Ray:

- AWS Distro for OpenTelemetry (ADOT): con ADOT, los ingenieros pueden instrumentar sus aplicaciones una vez y enviar métricas y rastreos correlacionados a varias AWS soluciones de monitoreo, como Amazon CloudWatch, Amazon Service y AWS X-Ray Amazon OpenSearch Managed Service para Prometheus.
- AWS Lambda— Instrumentación activa y pasiva de las solicitudes entrantes en todos los tiempos de ejecución. AWS Lambda añade dos nodos a su mapa de rastreo, uno para el AWS Lambda servicio y otro para la función. Al habilitar la instrumentación, AWS Lambda también ejecuta el daemon X-Ray en los tiempos de ejecución de Java y Node.js para usarlo con el SDK de X-Ray.
- Amazon API Gateway: instrumentación activa y pasiva. API Gateway aplica reglas de muestreo para determinar qué solicitudes registrar y agrega un nodo para la etapa de puerta de enlace al mapa de servicio.
- AWS Elastic Beanstalk: herramientas. Elastic Beanstalk incluye el daemon de X-Ray en las siguientes plataformas:

  - Java SE: 2.3.0 y configuraciones más recientes
  - Tomcat: 2.4.0 y configuraciones más recientes
  - Node.js: 3.2.0 y configuraciones más recientes
  - Windows Server: todas las configuraciones que no sean Windows Server Core liberadas a partir del 9 de diciembre de 2016.

  Puede usar la consola de Elastic Beanstalk para indicar a Elastic Beanstalk que ejecute el daemon en estas plataformas o utilizar la opción `XRayEnabled` en el espacio de nombres `aws:elasticbeanstalk:xray`.
- Elastic Load Balancing: rastreo de solicitudes en equilibradores de carga de aplicaciones El equilibrador de carga de aplicación agrega el ID de rastro al encabezado de la solicitud antes de enviarlo al grupo de destino.
- Amazon EventBridge — Instrumentación pasiva. Si un servicio que publica eventos EventBridge está equipado con el SDK de X-Ray, los destinos de los eventos recibirán el encabezado de rastreo y podrán seguir propagando el ID de rastreo original.
- Amazon Simple Notification Service: instrumentación pasiva. Si un publicador de Amazon SNS hace un rastreo de su cliente con el SDK de X-Ray, el suscriptor puede recuperar el encabezado de rastreo y seguir propagando el rastro original a partir del publicador con el mismo ID de rastro.
- Amazon Simple Queue Service: instrumentación pasiva. Si un servicio rastrea solicitudes utilizando el SDK de X-Ray, Amazon SQS podrá enviar el encabezado de rastreo y continuar propagando el rastro original entre el remitente y el consumidor con un ID de rastro coherente.

Elija uno de los siguientes temas para explorar el conjunto completo de temas integrados. Servicios de AWS

Temas

- AWS Distro para OpenTelemetry y AWS X-Ray
- Soporte de rastreo activo de Amazon API Gateway para AWS X-Ray
- Amazon EC2 y AWS App Mesh
- AWS App Runner y X-Ray
- AWS AppSync y AWS X-Ray
- Registro de llamadas a la API X-Ray con AWS CloudTrail
- CloudWatch integración con X-Ray
- Rastreo de los cambios en la configuración de cifrado de X-Ray con AWS Config

- Amazon Elastic Compute Cloud y AWS X-Ray
- AWS Elastic Beanstalk y AWS X-Ray
- Elastic Load Balancing y AWS X-Ray
- Amazon EventBridge y AWS X-Ray
- AWS Lambda y AWS X-Ray
- Amazon SNS y AWS X-Ray
- AWS Step Functions y AWS X-Ray
- Amazon SQS y AWS X-Ray
- Amazon S3 y AWS X-Ray

AWS Distro para OpenTelemetry y AWS X-Ray

Utilice AWS Distro para OpenTelemetry (ADOT) para recopilar y enviar métricas y rastros a AWS X-Ray y otras soluciones de supervisión, como Amazon CloudWatch, Amazon OpenSearch Service y Amazon Managed Service para Prometheus.

AWS Distro para OpenTelemetry

AWS Distro para OpenTelemetry (ADOT) es una distribución de AWS basada en el proyecto OpenTelemetry de la Cloud Native Computing Foundation (CNCF). OpenTelemetry proporciona un conjunto único de API, bibliotecas y agentes de código abierto para recopilar rastreos y métricas distribuidos. Este kit de herramientas es una distribución de componentes originales de OpenTelemetry que incluye SDK, agentes de instrumentación automática y recopiladores probados, optimizados, protegidos y compatibles con AWS.

Con ADOT, los ingenieros pueden instrumentar sus aplicaciones una vez y enviar métricas y rastros correlacionados a varias soluciones de supervisión de AWS, entre ellas Amazon CloudWatch, AWS X-Ray, Amazon OpenSearch Service y Amazon Managed Service para Prometheus.

ADOT se integra en un número cada vez mayor de Servicios de AWS para simplificar el envío de rastros y métricas a soluciones de supervisión como, por ejemplo, X-Ray. Algunos ejemplos de servicios integrados en ADOT:

- AWS Lambda: las capas Lambda administradas por AWS para ADOT permiten que el usuario empiece directamente, al instrumentar automáticamente una función de Lambda y empaquetar OpenTelemetry junto con una configuración lista para usar para AWS Lambda y X-Ray en una

capa fácil de configurar. Los usuarios pueden habilitar y deshabilitar OpenTelemetry para su función de Lambda sin cambiar el código. Para obtener más información, consulte AWS Distro para OpenTelemetry Lambda.

- Amazon Elastic Container Service (ECS): recopile métricas y rastros de las aplicaciones de Amazon ECS mediante el AWS Distro para OpenTelemetry Collector, para enviarlos a X-Ray y a otras soluciones de supervisión. Para obtener más información, consulte Collecting application trace data en la Guía del desarrollador de Amazon ECS.
- AWSApp Runner: App Runner admite el envío de rastros a X-Ray mediante AWS Distro para OpenTelemetry (ADOT). Utilice los SDK de ADOT para recopilar datos de rastreo para sus aplicaciones en contenedores y utilice X-Ray para analizar y obtener información sobre su aplicación instrumentada. Para obtener más información, consulte AWS App Runner and X-Ray.

Para obtener más información sobre AWS Distro para OpenTelemetry, incluida la integración en otros Servicios de AWS, consulte la documentación de AWS Distro para OpenTelemetry.

Para obtener más información sobre cómo instrumentar la aplicación con AWS Distro para OpenTelemetry y X-Ray, consulte Instrumentación de la aplicación con AWS OpenTelemetry.

Soporte de rastreo activo de Amazon API Gateway para AWS X-Ray

Puede utilizar X-Ray para rastrear y analizar las solicitudes de los usuarios a medida que viajan a través de las API de Amazon API Gateway a los servicios subyacentes. API Gateway admite el rastreo de X-Ray para todos los tipos de punto de conexión de API Gateway: regional, optimizado para bordes y privado. Puede utilizar X-Ray con Amazon API Gateway en todos los Regiones de AWS lugares donde X-Ray esté disponible. Para obtener más información, consulte Rastreo de la ejecución de API de API Gateway con AWS X-Ray en la Guía para desarrolladores de Amazon API Gateway.

> **Note**
>
> X-Ray solo admite el rastreo de las API de REST a través de API Gateway.

Amazon API Gateway proporciona soporte de rastreo activo para AWS X-Ray. Habilite el rastreo activo en sus etapas de la API para realizar el muestreo de solicitudes entrantes y enviar rastros a X-Ray.

Para habilitar el rastreo activo en una etapa de la API

1. Abra la consola de API Gateway en https://console.aws.amazon.com/apigateway/.
2. Elegir una API.
3. Elegir una etapa.
4. En la pestaña Registros/Rastreo, elija Habilitar el rastreo de X-Ray y, a continuación, seleccione Guardar cambios.
5. Seleccione Resources (Recursos) en el panel de navegación del lado izquierdo.
6. Para volver a implementar la API con la nueva configuración, abra el menú desplegable Acciones y, a continuación, elija Implementar API.

API Gateway utiliza reglas de muestreo que define en la consola de X-Ray para determinar qué solicitudes registrar. Puede crear reglas que solo se apliquen a las API o que solo se apliquen a las solicitudes que contengan determinados encabezados. API Gateway registra los encabezados en atributos del segmento, junto con detalles sobre la etapa y la solicitud. Para obtener más información, consulte Configuración de reglas de muestreo de .

> **Note**
>
> Al rastrear las API REST con la integración HTTP de API Gateway, el nombre de servicio de cada segmento se establece en la ruta URL de solicitud desde API Gateway hasta el punto final de integración HTTP, lo que da como resultado un nodo de servicio en el mapa de rastreo de X-Ray para cada ruta URL única. Un gran número de rutas URL puede provocar que el mapa de rastreo supere el límite de 10 000 nodos y provocar un error.
> Para minimizar la cantidad de nodos de servicio creados por API Gateway, considere la posibilidad de pasar los parámetros dentro de la cadena de consulta de URL o en el cuerpo de la solicitud mediante POST. Cualquiera de los dos enfoques garantizará que los parámetros no formen parte de la ruta URL, lo que puede dar lugar a un menor número de rutas URL y nodos de servicio distintos.

Para todas las solicitudes entrantes, API Gateway añade un encabezado de rastreo a las solicitudes HTTP entrantes que no tengan ya uno.

```
X-Amzn-Trace-Id: Root=1-5759e988-bd862e3fe1be46a994272793
```

Formato de identificación de trazas de rayos X

Un `trace_id` de X-Ray consta de tres números separados por guiones. Por ejemplo, `1-58406520-a006649127e371903a2de979`. Esto incluye:

- El número de versión, que es `1`.
- La hora de la solicitud original en Unix (época) con 8 dígitos hexadecimales.

  Por ejemplo, a las 10:00 a.m. del 1 de diciembre de 2016 (hora peninsular española), la hora de la época se expresa en `1480615200` segundos o `58406520` en dígitos hexadecimales.
- Un identificador de 96 bits único a nivel mundial para el rastreo en 24 dígitos hexadecimales.

Si el rastreo activo está deshabilitado, la fase sigue registrando un segmento si la solicitud procede de un servicio que ha muestreado la solicitud e iniciado un rastreo. Por ejemplo, una aplicación web instrumentada puede llamar a una API de API Gateway con un cliente HTTP. Cuando instrumente un cliente HTTP con el SDK de X-Ray, este agrega un encabezado de rastreo a la solicitud saliente que contiene la decisión de muestreo. API Gateway lee el encabezado de rastreo y crea un segmento para las solicitudes muestreadas.

Si utilizas API Gateway para generar un SDK de Java para tu API, puedes instrumentar el cliente del SDK añadiendo un controlador de solicitudes con el generador de clientes, del mismo modo que instrumentarías manualmente un cliente de AWS SDK. Para obtener instrucciones, consulte Rastreo de llamadas al AWS SDK con el X-Ray SDK for Java.

Amazon EC2 y AWS App Mesh

AWS X-Ray se integra AWS App Meshpara administrar los proxies de Envoy para microservicios. App Mesh proporciona una versión de Envoy que puede configurar para enviar datos de rastreo al daemon de X-Ray que se ejecute en un contenedor de la misma tarea o pod. X-Ray admite el rastreo con los siguientes servicios compatibles con App Mesh:

- Amazon Elastic Container Service (Amazon ECS)

- Amazon Elastic Kubernetes Service (Amazon EKS)
- Amazon Elastic Compute Cloud (Amazon EC2)

Utilice las instrucciones siguientes para aprender a habilitar el seguimiento de X-Ray a través de App Mesh.

Para configurar el proxy de Envoy para enviar datos a X-Ray, establezca la variable de entorno `ENABLE_ENVOY_XRAY_TRACING` en su definición de contenedor.

> **Note**
>
> Actualmente la versión App Mesh de Envoy no envía rastros según las reglas de muestreo configuradas. En su lugar, utiliza un porcentaje de muestreo fijo del 5 % para la versión 1.16.3 o posterior de Envoy, o un porcentaje de muestreo del 50 % para las versiones de Envoy anteriores a la 1.16.3.

Example Definición del contenedor de Envoy para Amazon ECS

```
{
      "name": "envoy",
      "image": "public.ecr.aws/appmesh/aws-appmesh-envoy:envoy-version",
      "essential": true,
      "environment": [
        {
          "name": "APPMESH_VIRTUAL_NODE_NAME",
          "value": "mesh/myMesh/virtualNode/myNode"
        },
        {
          "name": "ENABLE_ENVOY_XRAY_TRACING",
          "value": "1"
        }
      ],
      "healthCheck": {
        "command": [
          "CMD-SHELL",
          "curl -s http://localhost:9901/server_info | cut -d' ' -f3 | grep -q live"
        ],
        "startPeriod": 10,
        "interval": 5,
        "timeout": 2,
        "retries": 3
      }
```

> **Note**
>
> Para obtener más información sobre las direcciones de región de Envoy disponibles, consulte Imagen de Envoy en la Guía del usuario de AWS App Mesh .

Para obtener más información sobre la ejecución del daemon de X-Ray en un contenedor, consulte Ejecución del daemon de X-Ray en Amazon ECS. Para una aplicación de muestra que incluya una malla de servicios, un microservicio, un proxy de Envoy y un daemon de X-Ray, implemente la `colorapp` muestra en el repositorio de ejemplos GitHub de App Mesh.

Más información

- Introducción a AWS App Mesh
- Introducción a AWS App Mesh Amazon ECS

AWS App Runner y X-Ray

AWS App Runner es un Servicio de AWS que proporciona una forma rápida, sencilla y rentable de implementar desde el código fuente o una imagen de contenedor directamente hacia una aplicación web escalable y segura en la Nube de AWS. No es necesario aprender nuevas tecnologías, decidir qué servicio informático utilizar o saber cómo aprovisionar y configurar los recursos de AWS. Consulte ¿Qué es AWS App Runner? para obtener más información.

AWS App Runner envía las rastros a X-Ray integrándose en AWS Distro para OpenTelemetry (ADOT). Utilice los SDK de ADOT para recopilar datos de rastreo para sus aplicaciones en contenedores y utilice X-Ray para analizar y obtener información sobre su aplicación instrumentada. Para obtener más información, consulte Tracing for your App Runner application with X-Ray.

AWS AppSync y AWS X-Ray

Puede habilitar y rastrear solicitudes para AWS AppSync. Para obtener más información e instrucciones, consulte Rastreo con AWS X-Ray.

Cuando el seguimiento de X-Ray está habilitado para una API de AWS AppSync, se crea automáticamente un rol vinculado al servicio de AWS Identity and Access Management en su cuenta con los permisos correspondientes. Esto permite a AWS AppSync enviar registros de seguimiento a X-Ray de una manera segura.

Registro de llamadas a la API X-Ray con AWS CloudTrail

AWS X-Ray 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 X-Ray como eventos. Las llamadas capturadas incluyen llamadas desde la consola de

X-Ray y llamadas en código a las operaciones de la API de X-Ray. Con la información recopilada por CloudTrail, puede determinar la solicitud que se realizó a X-Ray, 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 al crear la cuenta y automáticamente tienes acceso 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 Uso del 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 AWS Management Console son multirregionales. Puede crear un registro de seguimiento de una sola región o de varias regiones 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, elige la opción de precios que desea utilizar para él. La opción de precios determina el costo de la incorporación y el almacenamiento de los eventos, así como el periodo de retención predeterminado y máximo del almacén de datos de eventos. Para obtener más información sobre CloudTrail los precios, consulte AWS CloudTrail Precios.

Temas

- Eventos de gestión de rayos X en CloudTrail
- Eventos de datos de rayos X en CloudTrail
- Ejemplos de eventos de X-Ray

Eventos de gestión de rayos X en CloudTrail

AWS X-Ray se integra AWS CloudTrail para registrar las acciones de la API realizadas por un usuario, un rol o un usuario Servicio de AWS en X-Ray. Se puede utilizar CloudTrail para supervisar las solicitudes de la API X-Ray en tiempo real y almacenar registros en Amazon S3, Amazon CloudWatch Logs y Amazon CloudWatch Events. X-Ray admite el registro de las siguientes acciones como eventos en los archivos de CloudTrail registro:

Acciones de la API admitidas

- PutEncryptionConfig

- GetEncryptionConfig
- CreateGroup
- UpdateGroup
- DeleteGroup
- GetGroup
- GetGroups
- GetInsight
- GetInsightEvents
- GetInsightImpactGraph
- GetInsightSummaries
- GetSamplingStatisticSummaries

Eventos de datos de rayos X en CloudTrail

Los eventos de datos proporcionan información sobre las operaciones de recursos realizadas en o dentro de un recurso (por ejemplo PutTraceSegments, que carga documentos segmentados a X-Ray).

Se denominan también operaciones del plano de datos. Los eventos de datos suelen ser actividades de gran volumen. De forma predeterminada, CloudTrail no registra los eventos de datos. El historial de CloudTrail eventos no registra los eventos de datos.

Se aplican cargos adicionales a los eventos de datos. Para obtener más información sobre CloudTrail los precios, consulta AWS CloudTrail Precios.

Puede registrar eventos de datos para los tipos de recursos de X-Ray mediante la CloudTrail consola o las operaciones de la CloudTrail API. AWS CLI Para obtener más información sobre cómo registrar los eventos de datos, consulte Registro de eventos de datos con la AWS Management Console y Registro de eventos de datos con la AWS Command Line Interface en la Guía del usuario de AWS CloudTrail .

En la siguiente tabla se enumeran los tipos de recursos de X-Ray para los que puede registrar eventos de datos. La columna Tipo de evento de datos (consola) muestra el valor que se puede elegir en la lista de tipos de eventos de datos de la CloudTrail consola. La columna de valores resources.type muestra el `resources.type` valor que se debe especificar al configurar los selectores de eventos avanzados mediante las API o. AWS CLI CloudTrail La CloudTrail columna

API de datos en la que se ha registrado muestra las llamadas a la API registradas CloudTrail para el tipo de recurso.

Tipo de evento de datos (consola)	resources.type value	Las API de datos registradas en CloudTrail
Rastro de rayos X	`AWS::XRay::Trace`	• PutTraceSegments • GetTraceSummaries • GetTraceGraph • GetServiceGraph • BatchGetTraces • GetTimeSeriesServiceStatistics • PutTelemetryRecords • GetSamplingTargets

Puede configurar selectores de eventos avanzados para filtrar los `readOnly` campos `eventName` y registrar solo aquellos eventos que sean importantes para usted. Sin embargo, no puede seleccionar eventos añadiendo el selector de `resources.`ARN campos, ya que las trazas de X-Ray no tienen ARN. Para obtener más información acerca de estos campos, consulte AdvancedFieldSelector en la Referencia de la API de AWS CloudTrail . A continuación se muestra un ejemplo de cómo ejecutar el `put-event-selectors` AWS CLI comando para registrar los eventos de datos en una CloudTrail pista. Debe ejecutar el comando en la región en la que se creó la ruta o especificarla; de lo contrario, la operación devolverá una `InvalidHomeRegionException` excepción.

```
aws cloudtrail put-event-selectors --trail-name myTrail --advanced-event-selectors \
'{
   "AdvancedEventSelectors": [
      {
         "FieldSelectors": [
            { "Field": "eventCategory", "Equals": ["Data"] },
            { "Field": "resources.type", "Equals": ["AWS::XRay::Trace"] },
            { "Field": "eventName", "Equals":
 ["PutTraceSegments","GetSamplingTargets"] }
         ],
         "Name": "Log X-Ray PutTraceSegments and GetSamplingTargets data events"
      }
```

```
    ]
}'
```

Ejemplos de eventos de X-Ray

Ejemplo de un evento de gestión, **`GetEncryptionConfig`**

El siguiente es un ejemplo de la entrada del GetEncryptionConfig registro de X-Ray en CloudTrail.

Example

```
{
    "eventVersion"=>"1.05",
    "userIdentity"=>{
        "type"=>"AssumedRole",
        "principalId"=>"AROAJVHBZWD3DN6CI2MHM:MyName",
        "arn"=>"arn:aws:sts::123456789012:assumed-role/MyRole/MyName",
        "accountId"=>"123456789012",
        "accessKeyId"=>"AKIAIOSFODNN7EXAMPLE",
        "sessionContext"=>{
            "attributes"=>{
                "mfaAuthenticated"=>"false",
                "creationDate"=>"2023-7-01T00:24:36Z"
            },
            "sessionIssuer"=>{
                "type"=>"Role",
                "principalId"=>"AROAJVHBZWD3DN6CI2MHM",
                "arn"=>"arn:aws:iam::123456789012:role/MyRole",
                "accountId"=>"123456789012",
                "userName"=>"MyRole"
            }
        }
    },
    "eventTime"=>"2023-7-01T00:24:36Z",
    "eventSource"=>"xray.amazonaws.com",
    "eventName"=>"GetEncryptionConfig",
    "awsRegion"=>"us-east-2",
    "sourceIPAddress"=>"33.255.33.255",
    "userAgent"=>"aws-sdk-ruby2/2.11.19 ruby/2.3.1 x86_64-linux",
    "requestParameters"=>nil,
    "responseElements"=>nil,
    "requestID"=>"3fda699a-32e7-4c20-37af-edc2be5acbdb",
    "eventID"=>"039c3d45-6baa-11e3-2f3e-e5a036343c9f",
```

```
    "eventType"=>"AwsApiCall",
    "recipientAccountId"=>"123456789012"
}
```

Ejemplo de evento de datos, **PutTraceSegments**

El siguiente es un ejemplo de la entrada del registro de eventos de PutTraceSegments datos de X-Ray en CloudTrail.

Example

```
{
  "eventVersion": "1.09",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AROAWYXPW54Y4NEXAMPLE:i-0dzz2ac111c83zz0z",
    "arn": "arn:aws:sts::012345678910:assumed-role/my-service-role/
i-0dzz2ac111c83zz0z",
    "accountId": "012345678910",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AROAWYXPW54Y4NEXAMPLE",
        "arn": "arn:aws:iam::012345678910:role/service-role/my-service-role",
        "accountId": "012345678910",
        "userName": "my-service-role"
      },
      "attributes": {
        "creationDate": "2024-01-22T17:34:11Z",
        "mfaAuthenticated": "false"
      },
      "ec2RoleDelivery": "2.0"
    }
  },
  "eventTime": "2024-01-22T18:22:05Z",
  "eventSource": "xray.amazonaws.com",
  "eventName": "PutTraceSegments",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "198.51.100.0",
  "userAgent": "aws-sdk-ruby3/3.190.0 md/internal ua/2.0 api/xray#1.0.0 os/linux md/
x86_64 lang/ruby#2.7.8 md/2.7.8 cfg/retry-mode#legacy",
  "requestParameters": {
```

```
    "traceSegmentDocuments": [
      "trace_id:1-00zzz24z-EXAMPLE4f4e41754c77d0000",
      "trace_id:1-00zzz24z-EXAMPLE4f4e41754c77d0000",
      "trace_id:1-00zzz24z-EXAMPLE4f4e41754c77d0001",
      "trace_id:1-00zzz24z-EXAMPLE4f4e41754c77d0002"
    ]
  },
  "responseElements": {
    "unprocessedTraceSegments": []
  },
  "requestID": "5zzzzz64-acbd-46ff-z544-451a3ebcb2f8",
  "eventID": "4zz51z7z-77f9-44zz-9bd7-6c8327740f2e",
  "readOnly": false,
  "resources": [
    {
      "type": "AWS::XRay::Trace"
    }
  ],
  "eventType": "AwsApiCall",
  "managementEvent": false,
  "recipientAccountId": "012345678910",
  "eventCategory": "Data",
  "tlsDetails": {
    "tlsVersion": "TLSv1.2",
    "cipherSuite": "ZZZZZ-RSA-AAA128-GCM-SHA256",
    "clientProvidedHostHeader": "example.us-west-2.xray.cloudwatch.aws.dev"
  }
}
```

CloudWatch integración con X-Ray

AWS X-Ray se integra con CloudWatch Application Signals, CloudWatch RUM y CloudWatch Synthetics para facilitar la supervisión del estado de sus aplicaciones. Habilite su aplicación para Application Signals para monitorear y solucionar problemas del estado operativo de sus servicios, páginas de clientes, Synthetics Canaries y dependencias de servicios.

Al correlacionar CloudWatch métricas, registros y trazos de rayos X, el mapa de rastreo de rayos X proporciona una end-to-end vista de sus servicios para ayudarlo a identificar rápidamente los cuellos de botella en el rendimiento e identificar a los usuarios afectados.

Con CloudWatch RUM, puede realizar un monitoreo real de los usuarios para recopilar y ver datos del lado del cliente sobre el rendimiento de su aplicación web a partir de sesiones de usuarios

reales casi en tiempo real. Con CloudWatch RUM, puede analizar AWS X-Ray y depurar la ruta de las solicitudes, empezando por los usuarios finales de su aplicación y pasando por los servicios gestionados descendentes. AWS Eso le ayuda a identificar las tendencias de latencia y los errores que afectan a sus usuarios finales.

Temas

CloudWatch RUM y AWS X-Ray

Con Amazon CloudWatch RUM, puede realizar una supervisión real de los usuarios para recopilar y ver datos del lado del cliente sobre el rendimiento de su aplicación web a partir de sesiones de usuarios reales prácticamente en tiempo real. Con CloudWatch RUM, puede analizar AWS X-Ray y depurar la ruta de las solicitudes, empezando por los usuarios finales de su aplicación y pasando por los servicios gestionados en sentido descendente. AWS Eso le ayuda a identificar las tendencias de latencia y los errores que afectan a sus usuarios finales.

Después de activar el rastreo de rayos X de las sesiones de usuario, CloudWatch RUM agrega un encabezado de rastreo de rayos X a las solicitudes HTTP permitidas y graba un segmento de rayos X para las solicitudes HTTP permitidas. A continuación, podrá ver las trazas y los segmentos de estas sesiones de usuario en la X-Ray y en CloudWatch las consolas, incluido el mapa de trazas de X-Ray.

> **Note**
>
> CloudWatch RUM no se integra con las reglas de muestreo de X-Ray. En su lugar, elija un porcentaje de muestreo cuando configure su aplicación para usar CloudWatch RUM. Las trazas enviadas desde CloudWatch RUM pueden conllevar costes adicionales. Para más información, consulte Precios de AWS X-Ray.

De forma predeterminada, los seguimientos del lado del cliente enviados desde CloudWatch RUM no están conectados a los rastreos del lado del servidor. Para conectar los seguimientos del lado del cliente con los seguimientos del lado del servidor, configure el cliente web CloudWatch RUM para agregar un encabezado de rastreo de X-Ray a estas solicitudes HTTP.

> **Warning**
>
> La configuración del cliente web CloudWatch RUM para agregar un encabezado de rastreo de X-Ray a las solicitudes HTTP puede provocar un error en el intercambio de recursos entre orígenes (CORS). Para evitarlo, añada el encabezado HTTP `X-Amzn-Trace-Id` a la lista de encabezados permitidos en la configuración CORS del servicio posterior. Si utiliza API Gateway como servicio posterior, consulte Habilitar CORS para un recurso de API de REST. Le recomendamos ampliamente que pruebe la aplicación antes de agregar un encabezado de seguimiento de X-Ray del lado del cliente en un entorno de producción. Para obtener más información, consulte la documentación del cliente web CloudWatch RUM.

Para obtener más información sobre la supervisión de usuarios reales en CloudWatch, consulte Uso de CloudWatch RUM. Para configurar su aplicación para usar CloudWatch RUM, incluido el seguimiento de las sesiones de los usuarios con X-Ray, consulte Configurar una aplicación para usar CloudWatch RUM.

Depuración de CloudWatch canarios sintéticos mediante X-Ray

CloudWatch Synthetics es un servicio totalmente gestionado que le permite supervisar sus puntos finales y sus API mediante canarios con scripts que se ejecutan las 24 horas del día, una vez por minuto.

Puede personalizar las scripts de un canary para comprobar si hay cambios en:

- Disponibilidad
- Latencia
- Transacciones
- Vínculos rotos o inactivos
- Step-by-step : finalizaciones de tareas
- Errores de carga de páginas
- Latencias de carga para activos de la interfaz de usuario
- Flujos complejos del asistente
- Flujos de compras en la aplicación

Los canaries siguen las mismas rutas y realizan las mismas acciones y comportamientos que sus clientes y verifican de forma continua la experiencia del cliente.

Para obtener más información acerca de la configuración de las pruebas de Synthetics, consulte Uso de Synthetics para crear y administrar canaries.

Los siguientes ejemplos muestran ejemplos comunes de casos de uso para los problemas de depuración que plantean los canaries de Synthetics. Cada ejemplo muestra una estrategia clave para la depuración mediante el mapa de rastreo o la consola de X-Ray Analytics.

Para obtener más información sobre cómo leer el mapa de rastreo e interactuar con él, consulte Visualización del mapa de servicio.

Para obtener más información sobre cómo leer e interactuar con la consola de X-Ray Analytics, consulte Interactuar con la consola de AWS X-Ray análisis.

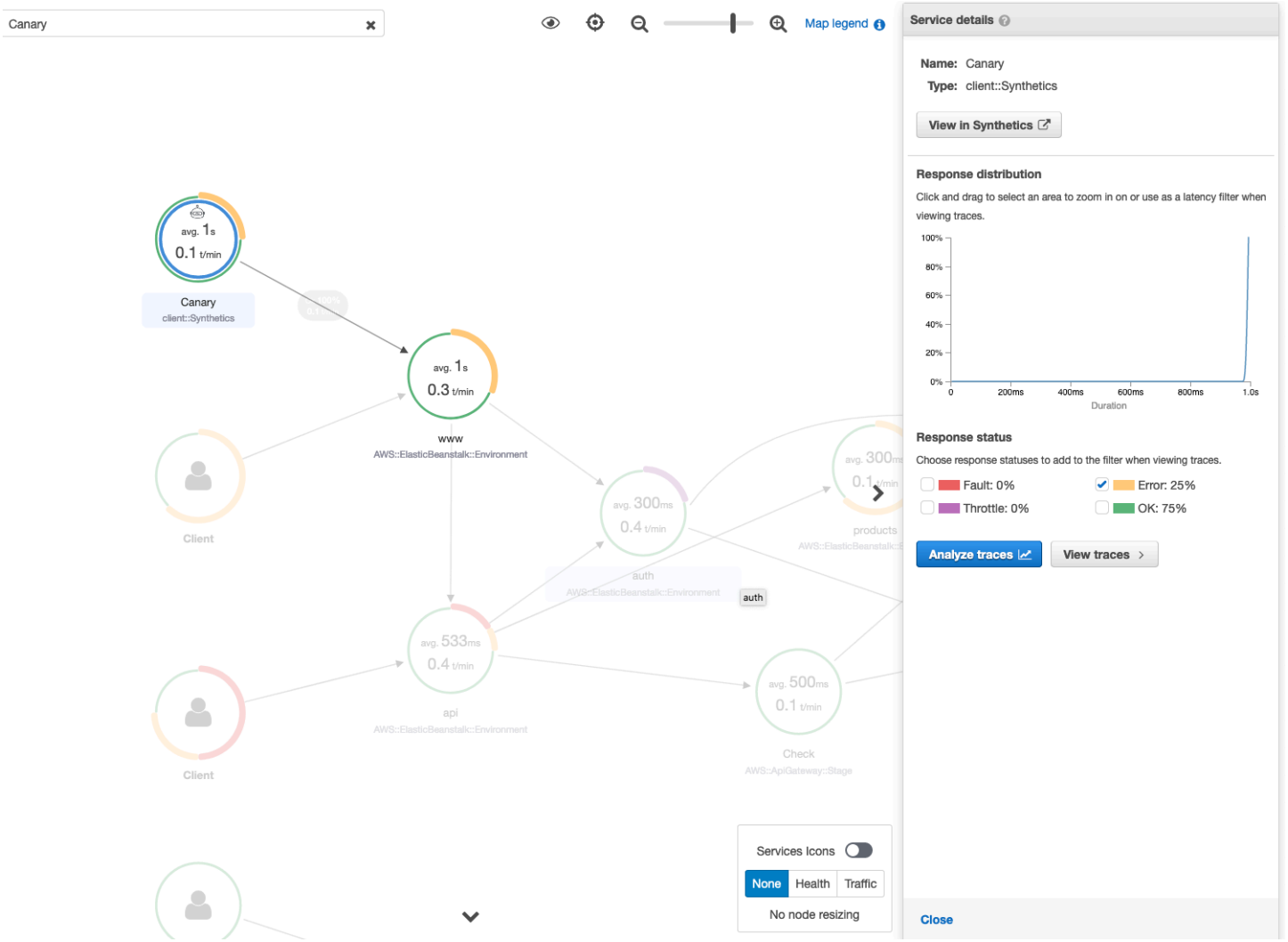
Temas

- Vea los canarios con un aumento de los informes de errores en el mapa de rastreo
- Utilice mapas de detalles de rastreo para los rastreos individuales para ver cada solicitud en detalle
- Determinar la causa raíz de los errores continuos en los servicios ascendentes y descendentes
- Identificar los cuellos de botella y las tendencias de rendimiento
- Comparar las tasas de error y de latencia antes y después de los cambios
- Determinar la cobertura de canary necesaria para todas las API y URL
- Utilizar los grupos para centrarse en las pruebas de synthetics

Vea los canarios con un aumento de los informes de errores en el mapa de rastreo

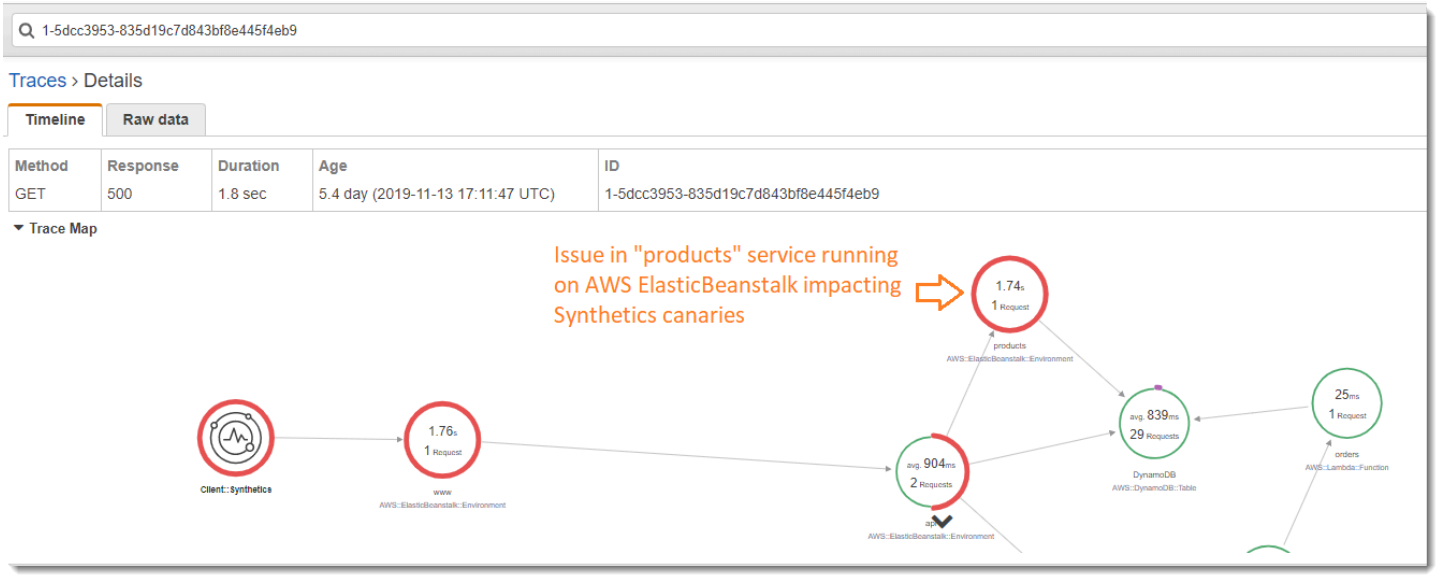
Para ver qué canarios tienen un aumento de errores, fallas, tasas de aceleración o tiempos de respuesta lentos en su mapa de trazas de X-Ray, puede resaltar los nodos cliente de Synthetics Canary mediante el filtro. `Client::Synthetic` Al hacer clic en un nodo se muestra la distribución del tiempo de respuesta de toda la solicitud. Al hacer clic en un borde entre dos nodos, se muestran detalles sobre las solicitudes que viajaron por esa conexión. También puede ver los nodos inferidos «remotos» de los servicios posteriores relacionados en su mapa de rastreo.

Al hacer clic en el nodo de Synthetics, en el panel lateral aparece el botón Ver en Synthetics, que te redirige a la consola de Synthetics, donde puedes comprobar los valores controlados.



Utilice mapas de detalles de rastreo para los rastreos individuales para ver cada solicitud en detalle

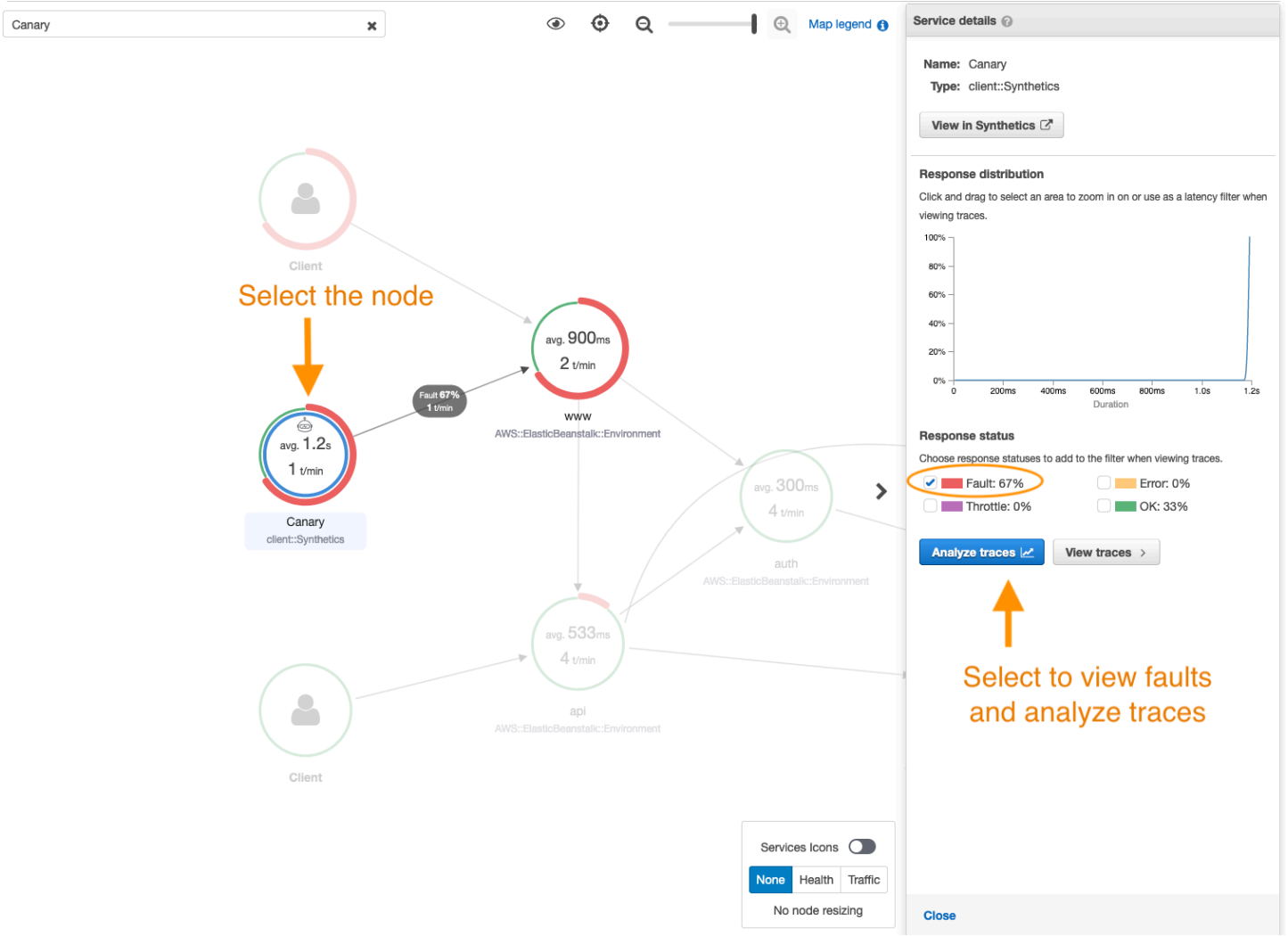
Para determinar qué servicio produce la mayor latencia o está provocando un error, invoque el mapa de detalles del rastreo seleccionando el rastreo en el mapa de rastreo. Los mapas de detalles de rastreo individuales muestran la end-to-end ruta de una sola solicitud. Utilice esto para comprender los servicios invocados y visualizar los servicios ascendentes y descendentes.

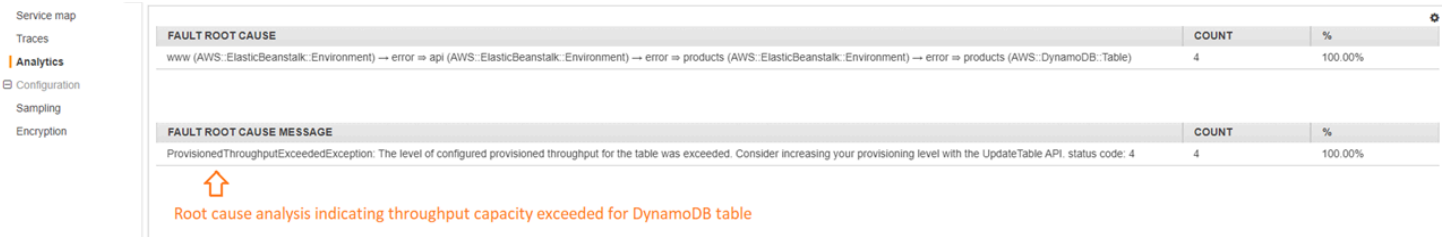


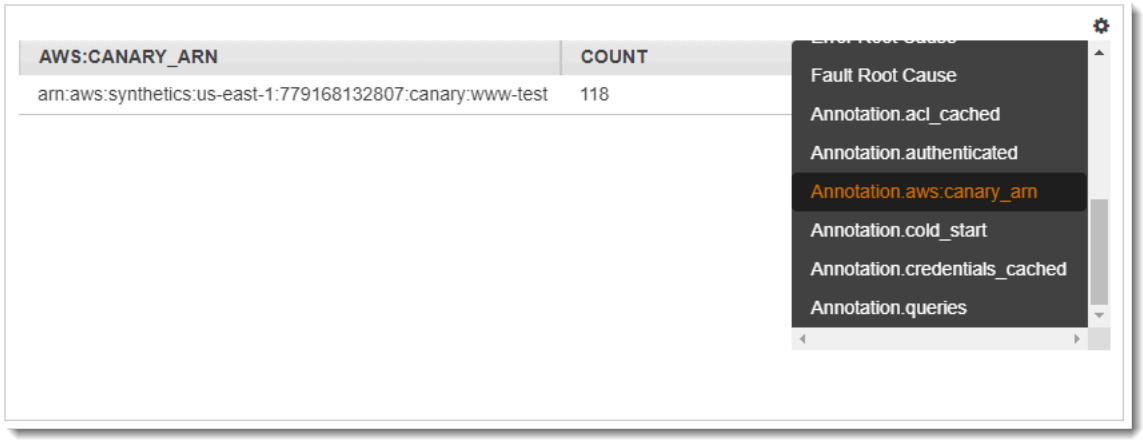
Determinar la causa raíz de los errores continuos en los servicios ascendentes y descendentes

Cuando reciba una CloudWatch alarma por fallos en un Synthetics Canary, utilice el modelado estadístico de los datos de rastreo de X-Ray para determinar la causa raíz probable del problema en la consola de X-Ray Analytics. En la consola de Analytics, la tabla Causa raíz del tiempo de respuesta muestra las rutas de las entidades registradas. X-ray determina qué ruta del rastro del usuario es la causa más probable del tiempo de respuesta. El formato indica una jerarquía de entidades detectadas, que termina en una causa raíz de tiempo de respuesta.

El siguiente ejemplo muestra que la prueba de Synthetics para la API “XXX” que se ejecuta en la puerta de enlace de la API falla debido a una excepción de capacidad de rendimiento de la tabla de Amazon DynamoDB.

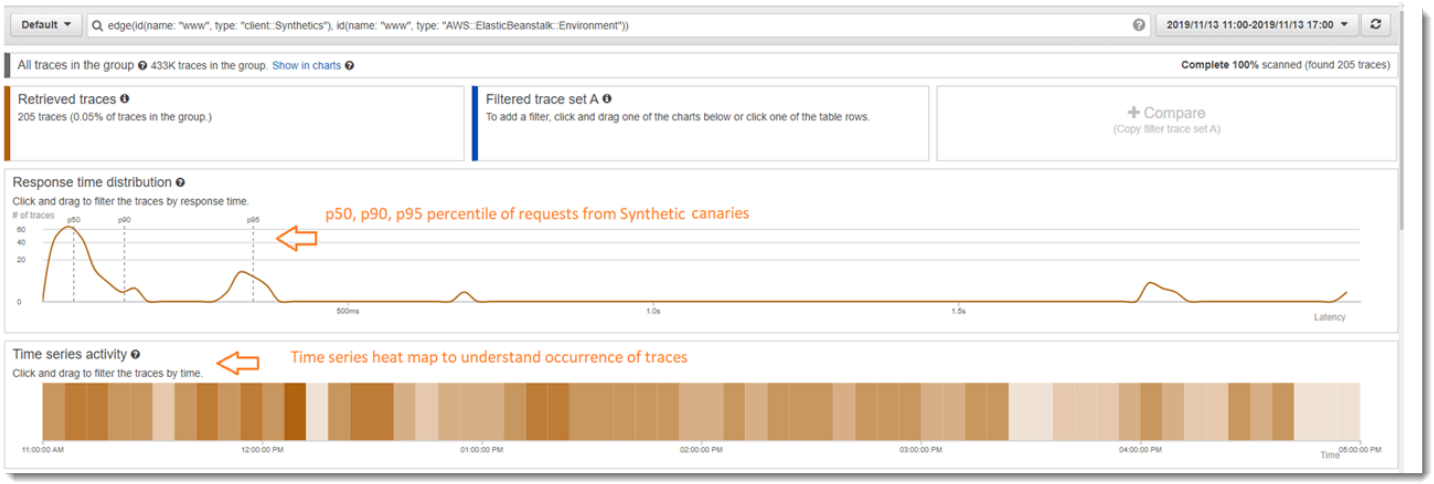

Canary
Map legend
Service details
Name: Canary
Type: client::Synthetics
View in Synthetics
Response distribution
Click and drag to select an area to zoom in on or use as a latency filter when viewing traces.
100%
80%
60%
40%
20%
0%
0
200ms
400ms
600ms
800ms
1.0s
1.2s
Duration
Response status
Choose response statuses to add to the filter when viewing traces.
Fault: 67%
Error: 0%
Throttle: 0%
OK: 33%
Analyze traces
View traces
Select to view faults and analyze traces
Client
Select the node
avg. 900ms
2 t/min
Fault 67%
1 t/min
www
AWS::ElasticBeanstalk::Environment
avg. 1.2s
1 t/min
Canary
client::Synthetics
avg. 300ms
4 t/min
auth
AWS::ElasticBeanstalk::Environment
avg. 533ms
4 t/min
api
AWS::ElasticBeanstalk::Environment
Client
Services Icons
None
Health
Traffic
No node resizing
Close


Service map
Traces
Analytics
Configuration
Sampling
Encryption
FAULT ROOT CAUSE
COUNT
%
www (AWS::ElasticBeanstalk::Environment) ⟶ error ⇒ api (AWS::ElasticBeanstalk::Environment) ⟶ error ⇒ products (AWS::ElasticBeanstalk::Environment) ⟶ error ⇒ products (AWS::DynamoDB::Table)
4
100.00%
FAULT ROOT CAUSE MESSAGE
COUNT
%
ProvisionedThroughputExceededException: The level of configured provisioned throughput for the table was exceeded. Consider increasing your provisioning level with the UpdateTable API. status code: 4
4
100.00%
Root cause analysis indicating throughput capacity exceeded for DynamoDB table



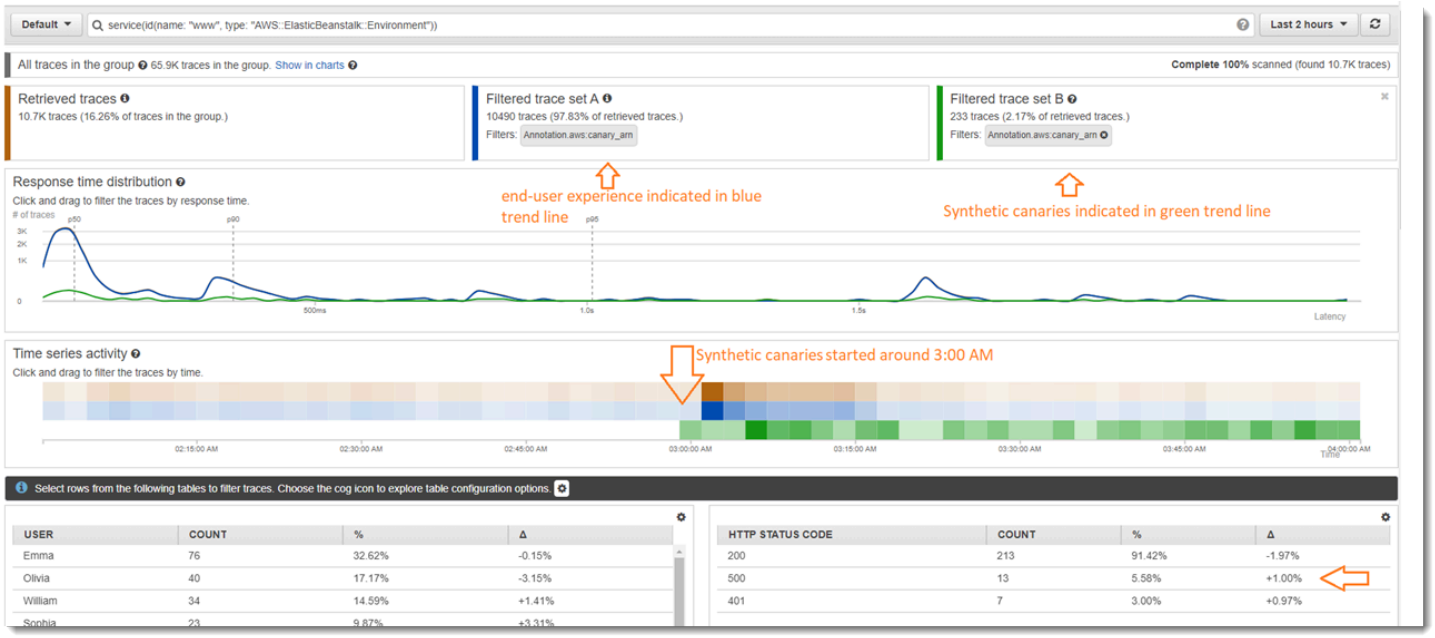
Identificar los cuellos de botella y las tendencias de rendimiento

Puede ver las tendencias en el rendimiento de su terminal a lo largo del tiempo utilizando el tráfico continuo de sus Synthetics Canaries para rellenar un mapa de detalles de rastreo durante un período de tiempo.



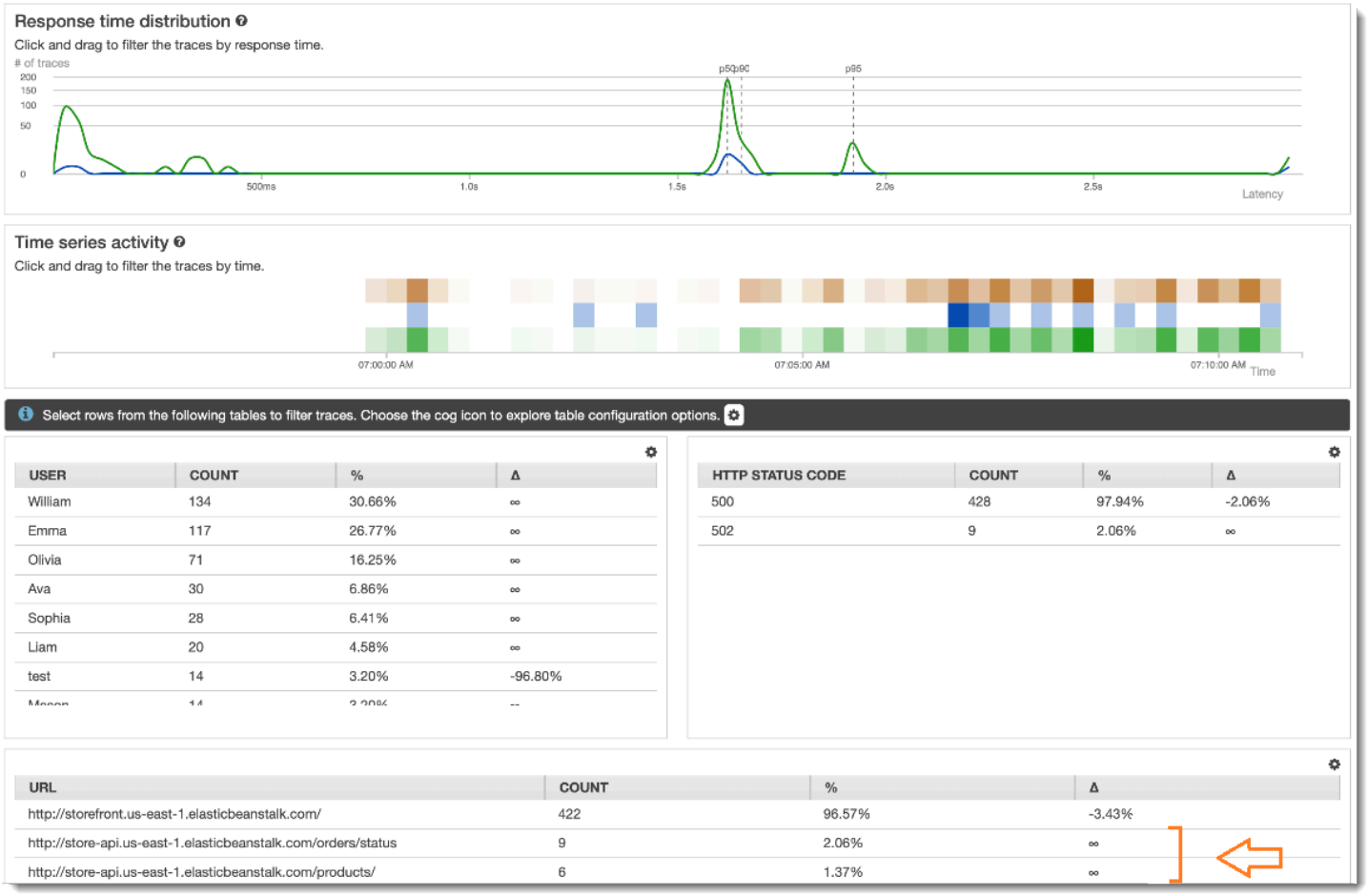
Comparar las tasas de error y de latencia antes y después de los cambios

Pinpoint el momento en que se produjo un cambio para correlacionarlo con un aumento de los problemas detectados por sus canarios. Utilice la consola de X-Ray Analytics para definir los intervalos de tiempo anteriores y posteriores como conjuntos de rastros, creando una diferenciación visual en la distribución del tiempo de respuesta.



Determinar la cobertura de canary necesaria para todas las API y URL

Utilice X-Ray Analytics para comparar la experiencia de los canaries con los usuarios. La interfaz de usuario a continuación muestra una línea de tendencia azul para los canaries y una línea verde para los usuarios. También puede identificar las dos URL de tres que no tienen pruebas de canary.

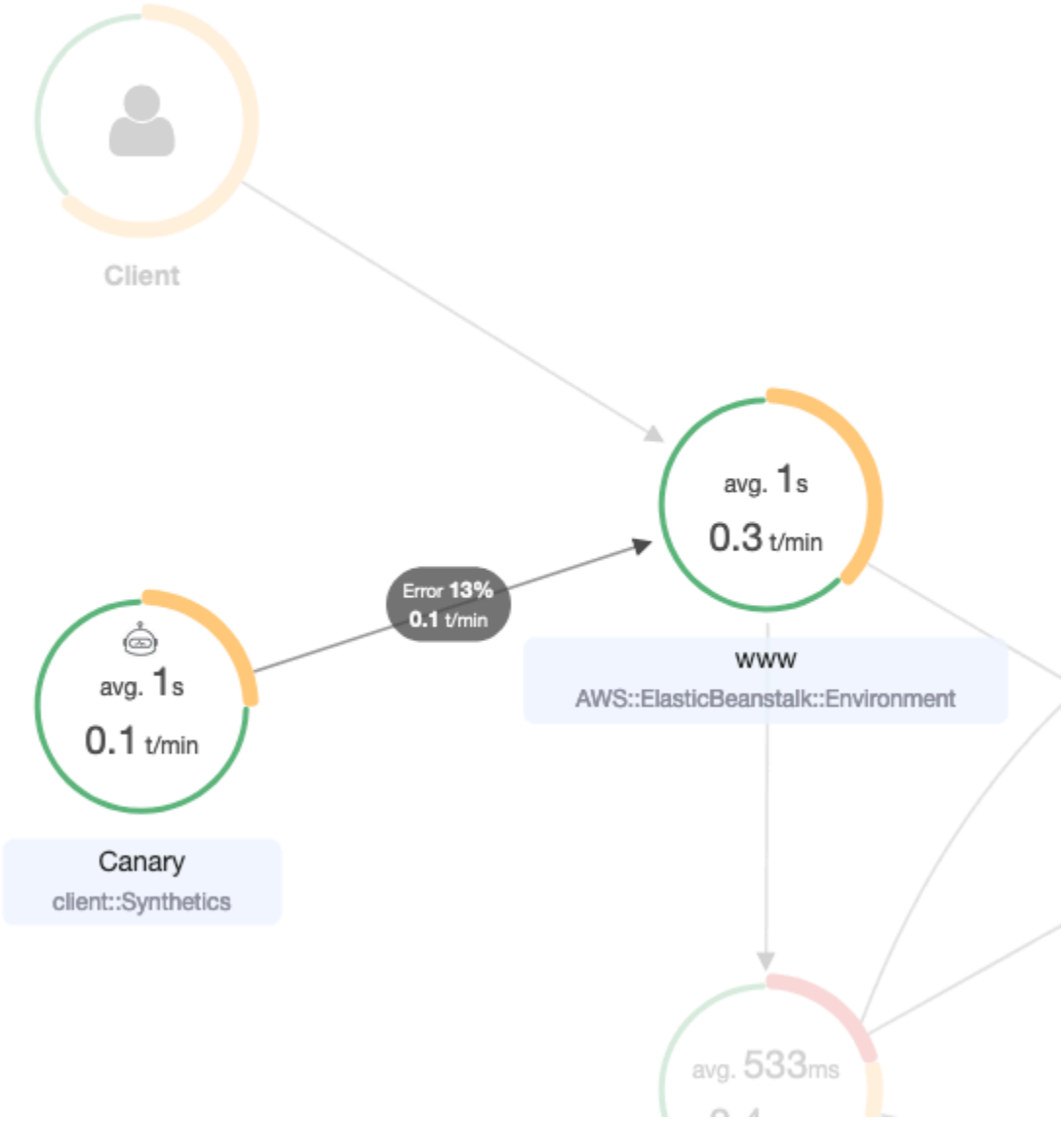


Utilizar los grupos para centrarse en las pruebas de synthetics

Puede crear un grupo de X-Ray utilizando una expresión de filtro para centrarse en un conjunto determinado de flujos de trabajo, como las pruebas de Synthetics para la aplicación “www” que se está ejecutando en AWS Elastic Beanstalk. Utilice las palabras clave complejas `service()` y `edge()` para filtrar por servicios y bordes.

Example Expresión de filtro de grupo

```
"edge(id(name: "www", type: "client::Synthetics"), id(name: "www", type:
 "AWS::ElasticBeanstalk::Environment"))"
```



Rastreo de los cambios en la configuración de cifrado de X-Ray con AWS Config

AWS X-Ray se integra en AWS Config para registrar cambios de configuración realizados en los recursos de cifrado de X-Ray. Puede utilizar AWS Config para realizar un inventario de recursos de cifrado de X-Ray, auditar el historial de configuración de X-Ray y enviar notificaciones basadas en los cambios de recursos.

AWS Config admite el registro de los siguientes cambios de recursos de cifrado de X-Ray como eventos:

- Cambios de configuración: cambiar o añadir una clave de cifrado o volver a la configuración de cifrado de X-Ray predeterminada.

Utilice las siguientes instrucciones para obtener información sobre cómo crear una conexión básica entre X-Ray y AWS Config.

Creación de un disparador de función de Lambda

Debe tener el ARN de una función de AWS Lambda personalizada antes de poder generar una regla de AWS Config personalizada. Siga estas instrucciones para crear una función básica con Node.js que devuelve un valor conforme o no conforme de vuelta a AWS Config en función del estado del recurso `XrayEncryptionConfig`.

Para crear una función de Lambda con un disparador de cambio AWS::XrayEncryptionConfig

1. Abra la consola de Lambda. Elija Crear función.
2. Elija Blueprints (Proyectos) y, a continuación, filtre la biblioteca de proyectos para el proyecto config-rule-change-triggered. Haga clic en el nombre del proyecto o bien elija Configure (Configurar) para continuar.
3. Defina los siguientes campos para configurar el proyecto:
   - En Name (Nombre), escriba un nombre.
   - Para Role (Rol), elija Create new role from template(s) (Crear un rol nuevo a partir de las plantillas).
   - Para Role name (Nombre del rol), escriba un nombre.
   - Para Policy templates (Plantillas de política), elija AWS Config Rules permissions (Permisos de reglas de &CC;).
4. Elija Create function (Crear función) para crear y visualizar su función en la consola de AWS Lambda.
5. Edite el código de la función para reemplazar `AWS::EC2::Instance` por `AWS::XrayEncryptionConfig`. También puede actualizar el campo de descripción para reflejar este cambio.

   Código predeterminado

```
    if (configurationItem.resourceType !== 'AWS::EC2::Instance') {
        return 'NOT_APPLICABLE';
```

```
    } else if (ruleParameters.desiredInstanceType ===
configurationItem.configuration.instanceType) {
        return 'COMPLIANT';
    }
        return 'NON_COMPLIANT';
```

Código actualizado

```
    if (configurationItem.resourceType !== 'AWS::XRay::EncryptionConfig') {
        return 'NOT_APPLICABLE';
    } else if (ruleParameters.desiredInstanceType ===
configurationItem.configuration.instanceType) {
        return 'COMPLIANT';
    }
        return 'NON_COMPLIANT';
```

6. Añada lo siguiente a su rol de ejecución en IAM para acceso a X-Ray. Estos permisos permiten acceso de solo lectura a sus recursos de X-Ray. Si no se proporciona acceso a los recursos apropiados se producirá un mensaje de fuera de ámbito desde AWS Config cuando se evalúa la función de Lambda asociada a la regla.

```
    {
        "Sid": "Stmt1529350291539",
        "Action": [
            "xray:GetEncryptionConfig"
        ],
        "Effect": "Allow",
        "Resource": "*"
     }
```

Creación de una regla de AWS Config personalizada para X-Ray

Cuando se crea la función de Lambda, anote el ARN de la función y vaya a la consola de AWS Config para crear la regla personalizada.

Para crear una regla de AWS Config para X-Ray

1. Abra la página Reglas de la consola de AWS Config.
2. Elija Add rule (Añadir una regla) y, a continuación, elija Add custom rule (Añadir una regla personalizada).

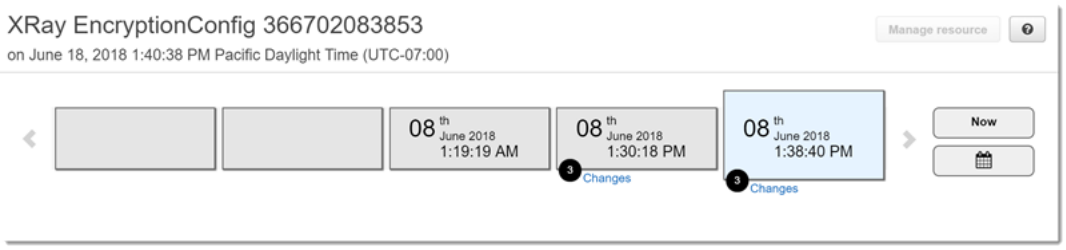
3. En ARN de la función de AWS Lambda, inserte el ARN asociado a la función de Lambda que desea utilizar.
4. Elija el tipo de disparador que desea establecer:
   - Cambios de configuración: AWS Config dispara la evaluación cuando cambia la configuración de un recurso que coincida con el ámbito de regla. La evaluación se realiza después de que AWS Config envía una notificación sobre un cambio de elementos de configuración.
   - Periódica: AWS Config ejecuta las evaluaciones de la regla con la frecuencia que se elija (por ejemplo, cada 24 horas).
5. Para Tipo de recurso, elija EncryptionConfig en la sección X-Ray.
6. Seleccione Save.

La consola de AWS Config comienza a evaluar la conformidad de la regla de forma inmediata. La evaluación puede tardar varios minutos en completarse.

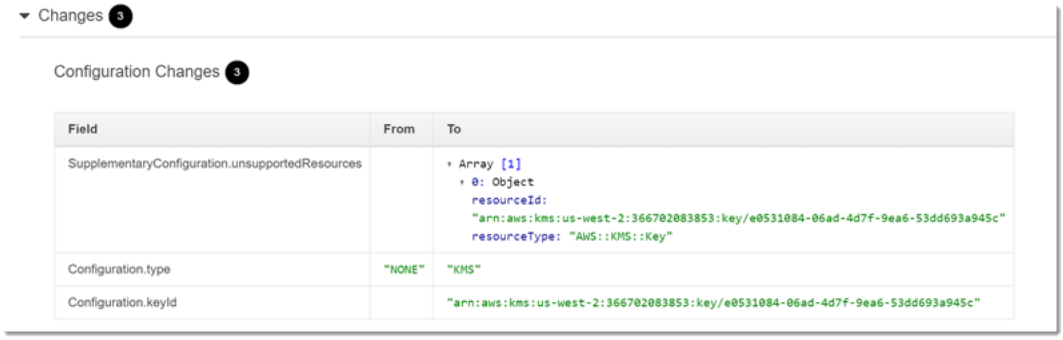
Ahora que esta regla es compatible, AWS Config puede empezar a compilar un historial de auditoría. AWS Config registra los cambios de recursos en forma de escala de tiempo. Para cada cambio en la escala de tiempo de eventos, AWS Config genera una tabla en formato de/a para mostrar lo que ha cambiado en la representación JSON de la clave de cifrado. Los dos cambios de campo asociados a EncryptionConfig son `Configuration.type` y `Configuration.keyID`.

Resultados de ejemplo

A continuación, se muestra un ejemplo de una escala de tiempo de AWS Config que muestra los cambios realizados en fechas y horas concretas.



A continuación, se muestra un ejemplo de una entrada de cambio de AWS Config. El formato de/a ilustra lo que ha cambiado. En este ejemplo se muestra que la configuración de cifrado de X-Ray predeterminada se cambió a una clave de cifrado definida.



Notificaciones de Amazon SNS

Para recibir una notificación de los cambios de configuración, establezca que AWS Config publique las notificaciones de Amazon SNS. Para obtener más información, consulte Monitorización de cambios de recursos de AWS Config por correo electrónico.

Amazon Elastic Compute Cloud y AWS X-Ray

Puede instalar y ejecutar el daemon de X-Ray en una instancia de Amazon EC2 con un script de datos de usuario. Para obtener instrucciones, consulte Ejecución del daemon de X-Ray en Amazon EC2.

Utilice un perfil de instancia para conceder permiso al daemon para cargar datos de rastreo en X-Ray. Para obtener más información, consulte Permiso para el envío de datos a X-Ray desde el daemon.

AWS Elastic Beanstalk y AWS X-Ray

Las plataformas AWS Elastic Beanstalk incluyen el daemon de X-Ray. Puede ejecutar el daemon mediante la configuración de una opción en la consola de Elastic Beanstalk o con un archivo de configuración.

En la plataforma Java SE, puede utilizar un archivo Buildfile para compilar la aplicación con Maven o Gradle en la instancia. El SDK de X-Ray para Java y el AWS SDK for Java están disponibles en Maven, para que pueda implementar únicamente su código de aplicación y compilar la aplicación en la instancia sin tener que agrupar y cargar todas sus de pendencias.

Puede utilizar las propiedades de entorno de Elastic Beanstalk para configurar el SDK de X-Ray. El método que Elastic Beanstalk utiliza para transferir las propiedades del entorno a su aplicación varía

en función de la plataforma. Use las variables de entorno del SDK de X-Ray o las propiedades del sistema según su plataforma.

- Plataforma Node.js: use las variables de entorno.
- Plataforma Java SE: use las variables de entorno.
- Plataforma Tomcat: use las propiedades del sistema.

Para obtener información, consulte la sección Configuración de la depuración en AWS X-Ray en la Guía para desarrolladores de AWS Elastic Beanstalk.

Elastic Load Balancing y AWS X-Ray

Los equilibradores de carga de aplicación de Elastic Load Balancing añaden un ID de rastro a las solicitudes HTTP entrantes en un encabezado denominado `X-Amzn-Trace-Id`.

```
X-Amzn-Trace-Id: Root=1-5759e988-bd862e3fe1be46a994272793
```

Formato de identificación de trazas de rayos X

Un `trace_id` de X-Ray consta de tres números separados por guiones. Por ejemplo, `1-58406520-a006649127e371903a2de979`. Esto incluye:

- El número de versión, que es `1`.
- La hora de la solicitud original en Unix (época) con 8 dígitos hexadecimales.

  Por ejemplo, a las 10:00 a.m. del 1 de diciembre de 2016 (hora peninsular española), la hora de la época se expresa en `1480615200` segundos o `58406520` en dígitos hexadecimales.
- Un identificador de 96 bits único a nivel mundial para el rastreo en 24 dígitos hexadecimales.

Los equilibradores de carga no envían datos a X-Ray ni aparecen como nodo en su mapa de servicio.

Para obtener más información, consulte la sección Rastreo de solicitudes en el equilibrador de carga de aplicaciones en la Guía para desarrolladores de Elastic Load Balancing.

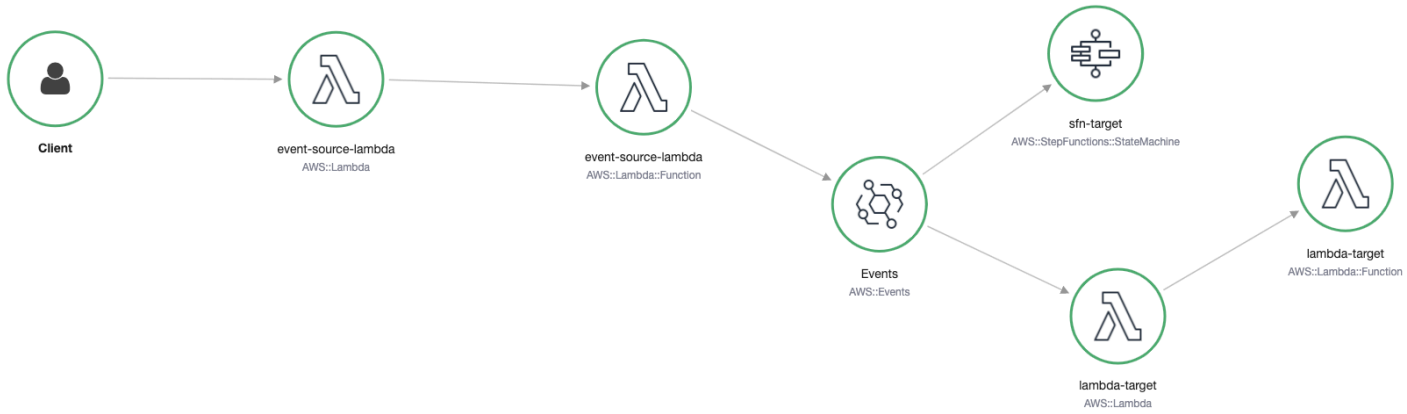
Amazon EventBridge y AWS X-Ray

AWS X-Ray se integra con Amazon EventBridge para rastrear los eventos que se transmiten EventBridge. Si un servicio equipado con el SDK de X-Ray envía eventos a EventBridge, el contexto de rastreo se propaga a los destinos de eventos posteriores dentro del encabezado de rastreo. El SDK de X-Ray recoge automáticamente el encabezado de rastreo y lo aplica a cualquier instrumentación posterior. Esta continuidad permite a los usuarios rastrear, analizar y depurar todos los servicios posteriores y proporciona una visión más completa del sistema.

Para obtener más información, consulte EventBridge X-Ray Integration en la Guía del EventBridge usuario.

Visualización del origen y los destinos en el mapa de servicio de X-Ray

El mapa de rastreo de X-Ray muestra un nodo de EventBridge eventos que conecta los servicios de origen y destino, como en el siguiente ejemplo:



Propague el contexto de rastreo a los destinos de eventos.

El SDK de X-Ray permite que la fuente de EventBridge eventos propague el contexto de rastreo a los objetivos de eventos posteriores. Los siguientes ejemplos específicos del idioma muestran la llamada EventBridge desde una función de Lambda en la que está habilitado el rastreo activo:

Java

Agregue las dependencias necesarias para X-Ray:

- AWS X-Ray SDK para Java
- AWS X-Ray SDK de grabadora para Java

```
package example;

import com.amazonaws.services.lambda.runtime.Context;
import com.amazonaws.services.lambda.runtime.RequestHandler;
import com.amazonaws.services.lambda.runtime.events.SQSEvent;
import com.amazonaws.xray.AWSXRay;
import com.amazonaws.services.eventbridge.AmazonEventBridge;
import com.amazonaws.services.eventbridge.AmazonEventBridgeClientBuilder;
import com.amazonaws.services.eventbridge.model.PutEventsRequest;
import com.amazonaws.services.eventbridge.model.PutEventsRequestEntry;
import com.amazonaws.services.eventbridge.model.PutEventsResult;
import com.amazonaws.services.eventbridge.model.PutEventsResultEntry;
import com.amazonaws.xray.handlers.TracingHandler;

import org.slf4j.Logger;
import org.slf4j.LoggerFactory;

import java.lang.StringBuilder;
import java.util.Map;
import java.util.List;
import java.util.Date;
import java.util.Collections;

/*
   Add the necessary dependencies for XRay:
   https://mvnrepository.com/artifact/com.amazonaws/aws-java-sdk-xray
   https://mvnrepository.com/artifact/com.amazonaws/aws-xray-recorder-sdk-aws-sdk
*/
public class Handler implements RequestHandler<SQSEvent, String>{
  private static final Logger logger = LoggerFactory.getLogger(Handler.class);

  /*
    build EventBridge client
  */
  private static final AmazonEventBridge eventsClient =
 AmazonEventBridgeClientBuilder
          .standard()
          // instrument the EventBridge client with the XRay Tracing Handler.
          // the AWSXRay globalRecorder will retrieve the tracing-context
          // from the lambda function and inject it into the HTTP header.
          // be sure to enable 'active tracing' on the lambda function.
          .withRequestHandlers(new TracingHandler(AWSXRay.getGlobalRecorder()))
          .build();
```

```
  @Override
  public String handleRequest(SQSEvent event, Context context)
  {
    PutEventsRequestEntry putEventsRequestEntry0 = new PutEventsRequestEntry();
    putEventsRequestEntry0.setTime(new Date());
    putEventsRequestEntry0.setSource("my-lambda-function");
    putEventsRequestEntry0.setDetailType("my-lambda-event");
    putEventsRequestEntry0.setDetail("{\"lambda-source\":\"sqs\"}");
    PutEventsRequest putEventsRequest = new PutEventsRequest();
    putEventsRequest.setEntries(Collections.singletonList(putEventsRequestEntry0));
    // send the event(s) to EventBridge
    PutEventsResult putEventsResult = eventsClient.putEvents(putEventsRequest);
    try {
      logger.info("Put Events Result: {}", putEventsResult);
    } catch(Exception e) {
      e.getStackTrace();
    }
    return "success";
  }
}
```

Python

Agregue la siguiente dependencia a su archivo requirements.txt:

```
aws-xray-sdk==2.4.3
```

```
import boto3
from aws_xray_sdk.core import xray_recorder
from aws_xray_sdk.core import patch_all

# apply the XRay handler to all clients.
patch_all()

client = boto3.client('events')

def lambda_handler(event, context):
    response = client.put_events(
        Entries=[
            {
                'Source': 'foo',
                'DetailType': 'foo',
```

```
                'Detail': '{\"foo\": \"foo\"}'
            },
        ]
    )
    return response
```

Go

```
package main

import (
  "context"
  "github.com/aws/aws-lambda-go/lambda"
  "github.com/aws/aws-lambda-go/events"
  "github.com/aws/aws-sdk-go/aws/session"
  "github.com/aws/aws-xray-sdk-go/xray"
  "github.com/aws/aws-sdk-go/service/eventbridge"
  "fmt"
)

var client = eventbridge.New(session.New())


func main() {
 //Wrap the eventbridge client in the AWS XRay tracer
  xray.AWS(client.Client)
  lambda.Start(handleRequest)
}

func handleRequest(ctx context.Context, event events.SQSEvent) (string, error) {
  _, err := callEventBridge(ctx)
  if err != nil {
    return "ERROR", err
  }
  return "success", nil
}


func callEventBridge(ctx context.Context) (string, error) {
    entries := make([]*eventbridge.PutEventsRequestEntry, 1)
    detail := "{ \"foo\": \"foo\"}"
    detailType := "foo"
    source := "foo"
```

```
    entries[0] = &eventbridge.PutEventsRequestEntry{
        Detail: &detail,
        DetailType: &detailType,
        Source: &source,
    }

  input := &eventbridge.PutEventsInput{
     Entries: entries,
  }

  // Example sending a request using the PutEventsRequest method.
  resp, err := client.PutEventsWithContext(ctx, input)

  success := "yes"
  if err == nil { // resp is now filled
      success = "no"
      fmt.Println(resp)
  }
  return success, err
}
```

Node.js

```
const AWSXRay = require('aws-xray-sdk')
//Wrap the aws-sdk client in the AWS XRay tracer
const AWS = AWSXRay.captureAWS(require('aws-sdk'))
const eventBridge = new AWS.EventBridge()

exports.handler = async (event) => {

  let myDetail = { "name": "Alice" }

  const myEvent = {
    Entries: [{
      Detail: JSON.stringify({ myDetail }),
      DetailType: 'myDetailType',
      Source: 'myApplication',
      Time: new Date
    }]
  }

  // Send to EventBridge
  const result = await eventBridge.putEvents(myEvent).promise()
```

```
  // Log the result
  console.log('Result: ', JSON.stringify(result, null, 2))

}
```

C#

Agregue los siguientes paquetes de X-Ray a sus dependencias de C#:

```
<PackageReference Include="AWSXRayRecorder.Core" Version="2.6.2" />
<PackageReference Include="AWSXRayRecorder.Handlers.AwsSdk" Version="2.7.2" />
```

```
using System;
using System.Collections.Generic;
using System.Linq;
using System.Threading.Tasks;
using Amazon;
using Amazon.Util;
using Amazon.Lambda;
using Amazon.Lambda.Model;
using Amazon.Lambda.Core;
using Amazon.EventBridge;
using Amazon.EventBridge.Model;
using Amazon.Lambda.SQSEvents;
using Amazon.XRay.Recorder.Core;
using Amazon.XRay.Recorder.Handlers.AwsSdk;
using Newtonsoft.Json;
using Newtonsoft.Json.Serialization;

[assembly:
 LambdaSerializer(typeof(Amazon.Lambda.Serialization.Json.JsonSerializer))]

namespace blankCsharp
{
  public class Function
  {
    private static AmazonEventBridgeClient eventClient;

    static Function() {
      initialize();
    }
```

```
    static async void initialize() {
      //Wrap the AWS SDK clients in the AWS XRay tracer
      AWSSDKHandler.RegisterXRayForAllServices();
      eventClient = new AmazonEventBridgeClient();
    }

    public async Task<PutEventsResponse> FunctionHandler(SQSEvent invocationEvent,
 ILambdaContext context)
    {
      PutEventsResponse response;
      try
      {
        response = await callEventBridge();
      }
      catch (AmazonLambdaException ex)
      {
        throw ex;
      }

      return response;
    }

    public static async Task<PutEventsResponse> callEventBridge()
    {
      var request = new PutEventsRequest();
      var entry = new PutEventsRequestEntry();
      entry.DetailType = "foo";
      entry.Source = "foo";
      entry.Detail = "{\"instance_id\":\"A\"}";
      List<PutEventsRequestEntry> entries = new List<PutEventsRequestEntry>();
      entries.Add(entry);
      request.Entries = entries;
      var response = await eventClient.PutEventsAsync(request);
      return response;
    }
  }
}
```

AWS Lambda y AWS X-Ray

Puede usarlo AWS X-Ray para rastrear sus AWS Lambda funciones. Lambada ejecuta el daemon de X-Ray y registra un segmento con detalles sobre la invocación y ejecución de la función. Para

realizar una instrumentación adicional, puede agrupar el SDK de X-Ray con su función para registrar las llamadas salientes y añadir anotaciones y metadatos.

Si otro servicio instrumentado llama a la función de Lambda, Lambda rastrea las solicitudes que ya se hayan muestreado sin necesidad de realizar ninguna configuración adicional. El servicio principal puede ser una aplicación web instrumentada u otra función de Lambda. Su servicio puede invocar la función directamente con un cliente de AWS SDK instrumentado o llamando a una API de API Gateway con un cliente HTTP instrumentado.

AWS X-Ray admite el seguimiento de aplicaciones basadas en eventos mediante Amazon AWS Lambda SQS. Utilice la CloudWatch consola para ver una vista conectada de cada solicitud mientras está en cola con Amazon SQS y procesada por una función Lambda descendente. Las trazas de los productores de mensajes ascendentes se vinculan automáticamente a las trazas de los nodos consumidores de Lambda descendentes, lo que crea una end-to-end vista de la aplicación. Para obtener más información, consulte Rastreo de aplicaciones basadas en eventos.

> **Note**
>
> Si tiene habilitadas las trazas para una función Lambda descendente, también debe tener las trazas habilitadas para la función Lambda raíz que llama a la función descendente para que la función descendente genere trazas.

Si un servicio que no está instrumentado invoca la función de Lambda o dicha función se ejecuta en una programación, puede configurar Lambda para que muestree y registre las invocaciones con el rastreo activo.

Para configurar la integración de X-Ray en una AWS Lambda función

1. Abra la consola de AWS Lambda.
2. Seleccione Funciones en el panel de navegación izquierdo.
3. Elija su función.
4. En la pestaña Configuración, desplácese hacia abajo hasta la tarjeta Herramientas de monitoreo adicionales. También puede encontrar esta tarjeta seleccionando Herramientas de supervisión y operaciones en el panel de navegación izquierdo.
5. Seleccione Editar.
6. En AWS X-Ray, habilite Rastreo activo.

En los tiempos de ejecución con un SDK de X-Ray correspondiente, Lambda también ejecuta el daemon de X-Ray.

SDK de X-Ray en Lambda

- SDK de X-Ray para Go: tiempos de ejecución de Go 1.7 y versiones más recientes
- SDK de X-Ray para Java: tiempo de ejecución de Java 8
- SDK de X-Ray para Node.js: tiempos de ejecución de Node.js 4.3 y versiones más recientes
- SDK de X-Ray para Python: tiempos de ejecución de Python 2.7, Python 3.6 y versiones más recientes
- SDK de X-Ray para .NET: tiempos de ejecución de .NET Core 2.0 y versiones más recientes

Para utilizar el SDK de X-Ray en Lambda, agrúpelo con el código de la función cada vez que cree una nueva versión. Puede instrumentar las funciones de Lambda con los mismos métodos que utiliza para instrumentar aplicaciones que se ejecutan en otros servicios. La diferencia principal es que no utiliza el SDK para instrumentar las solicitudes entrantes, tomar decisiones de muestreo y crear segmentos.

La otra diferencia entre la instrumentación de funciones de Lambda y aplicaciones web es que el código de su función no puede modificar el segmento que Lambda crea y envía a X-Ray. Puede crear subsegmentos y registrar anotaciones y metadatos en ellos, pero no puede añadir anotaciones y metadatos al segmento principal.

Para obtener más información, consulte Uso de AWS X-Ray en la Guía para desarrolladores de AWS Lambda .

Amazon SNS y AWS X-Ray

Puede usarlo AWS X-Ray con Amazon Simple Notification Service (Amazon SNS) para rastrear y analizar las solicitudes a medida que recorren sus temas de SNS hasta sus servicios de suscripción compatibles con SNS. Utilice el rastreo de X-Ray con Amazon SNS para analizar las latencias de sus mensajes y sus servicios backend, por ejemplo, cuánto tiempo pasa una solicitud en un tema y cuánto tiempo ha tardado en enviar el mensaje a cada una de las suscripciones del tema. Amazon SNS solo admite rastreo de X-Ray para temas estándar y FIFO.

Si publica en un tema de Amazon SNS desde un servicio que ya está instrumentado con X-Ray, Amazon SNS pasa el contexto de rastreo del publicador a los suscriptores. Además, puede activar

el rastreo activo para enviar datos de segmentos sobre sus suscripciones de Amazon SNS a X-Ray para los mensajes publicados desde un cliente de SNS instrumentado. Active el rastreo activo para un tema de Amazon SNS a través de la consola de Amazon SNS o de la API o la CLI de Amazon SNS. Consulte Instrumentación de su solicitud para obtener más información sobre cómo instrumentar sus clientes de SNS.

Configuración del rastreo activo de Amazon SNS

Puede utilizar la consola de Amazon SNS o la AWS CLI o el SDK para configurar el seguimiento activo de Amazon SNS.

Al utilizar la consola de Amazon SNS, Amazon SNS intenta crear los permisos necesarios para que SNS llame a X-Ray. El intento puede rechazarse si el usuario no tiene los permisos suficientes para modificar las políticas de recursos de X-Ray. Para obtener más información sobre estos permisos consulte Administración de identidades y accesos en Amazon SNS y Ejemplos de casos de control de acceso con Amazon SNS en la Guía para desarrolladores de Amazon Simple Notification Service. Para obtener más información acerca de cómo activar el rastreo activo a través de la consola de Amazon SNS, consulte Habilitar el rastreo activo en un tema de Amazon SNS en la Guía para desarrolladores de Amazon Simple Notification Service.

Al utilizar la AWS CLI o el SDK para activar el seguimiento activo, debe configurar manualmente los permisos mediante políticas basadas en recursos. Use `PutResourcePolicy` para configurar X-Ray con la política basada en recursos necesaria para permitir que Amazon SNS envíe rastros a X-Ray.

Example Ejemplo de política basada en recursos de X-Ray para el rastreo activo de Amazon SNS

En este ejemplo de documento de política se especifican los permisos que Amazon SNS necesita para enviar datos de rastreo a X-Ray:

```
{
    Version: "2012-10-17",
    Statement: [
      {
        Sid: "SNSAccess",
        Effect: Allow,
        Principal: {
          Service: "sns.amazonaws.com",
        },
        Action: [
          "xray:PutTraceSegments",
```

```
          "xray:GetSamplingRules",
          "xray:GetSamplingTargets"
        ],
        Resource: "*",
        Condition: {
          StringEquals: {
            "aws:SourceAccount": "account-id"
          },
          StringLike: {
            "aws:SourceArn": "arn:partition:sns:region:account-id:topic-name"
          }
        }
      }
    ]
  }
```

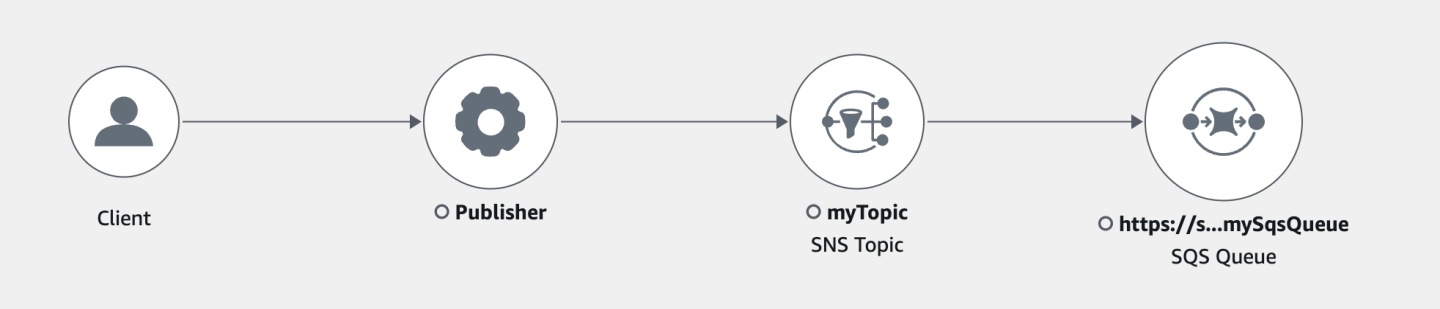
Utilice la CLI para crear una política basada en recursos que dé a Amazon SNS permisos para enviar datos de rastreo a X-Ray:

```
aws xray put-resource-policy --policy-name MyResourcePolicy --policy-document
 '{ "Version": "2012-10-17", "Statement": [ { "Sid": "SNSAccess", "Effect": "Allow",
 "Principal": { "Service": "sns.amazonaws.com" }, "Action": [ "xray:PutTraceSegments",
 "xray:GetSamplingRules", "xray:GetSamplingTargets" ], "Resource": "*",
 "Condition": { "StringEquals": { "aws:SourceAccount": "account-id" }, "StringLike":
 { "aws:SourceArn": "arn:partition:sns:region:account-id:topic-name" } } } ] }'
```

Para usar estos ejemplos, sustituya *partition*, *regionaccount-id*, y *topic-name*por su AWS partición, región, ID de cuenta y nombre de tema de Amazon SNS específicos. Para dar permiso a todos los temas de Amazon SNS para que envíen datos de rastreo a X-Ray, sustituya el nombre del tema por *.

Visualización de rastros de publicadores y suscriptores de Amazon SNS en la consola de X-Ray

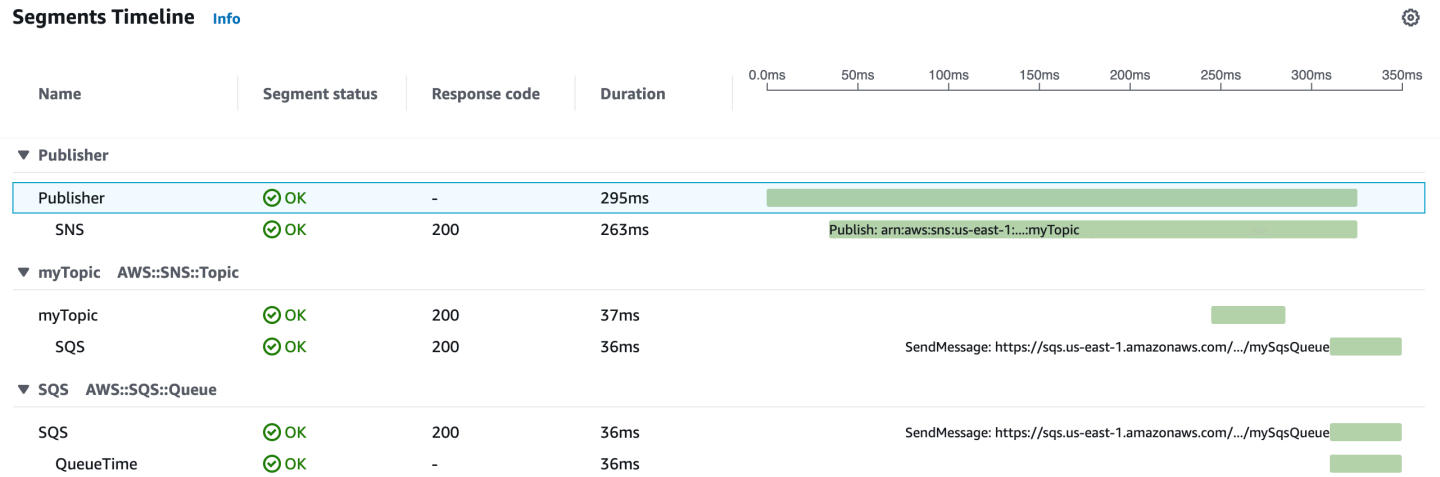
Utilice la consola X-Ray para ver un mapa de rastreo y los detalles del rastreo que muestran una vista conectada de los editores y suscriptores de Amazon SNS. Cuando el rastreo activo de Amazon SNS está activado para un tema, el mapa de rastreo de X-Ray y el mapa de detalles del rastreo muestran los nodos conectados para los editores de Amazon SNS, el tema de Amazon SNS y los suscriptores intermedios:



Tras elegir un rastreo que abarque a un editor y un suscriptor de Amazon SNS, la página de detalles del rastreo de X-Ray muestra un mapa de detalles del rastreo y una cronología del segmento.

Example Ejemplo de escala de tiempo con el publicador y el suscriptor de Amazon SNS

En este ejemplo se muestra una escala de tiempo que incluye a un publicador de Amazon SNS que envía un mensaje a un tema de Amazon SNS que es procesado por un suscriptor de Amazon SQS.

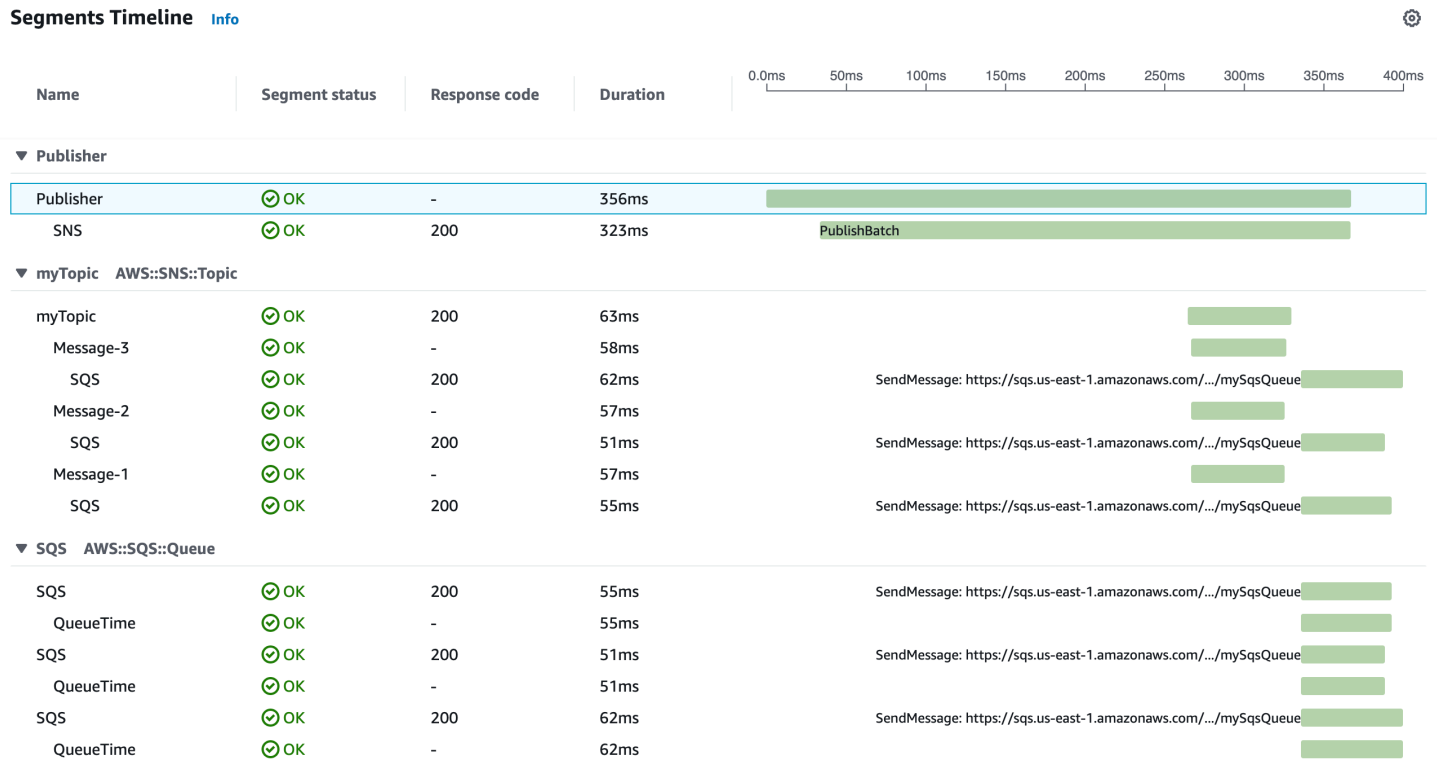


El ejemplo de escala de tiempo anterior proporciona detalles sobre el flujo de mensajes de Amazon SNS:

- El segmento SNS representa la duración de ida y vuelta de la llamada a la API `Publish` desde el cliente.
- El segmento myTopic representa la latencia de la respuesta de Amazon SNS a la solicitud de publicación.
- El subsegmento SQS representa el tiempo de ida y vuelta que tarda Amazon SNS en publicar el mensaje en una cola de Amazon SQS.
- El tiempo entre el segmento MyTopic y el subsegmento SQS representa el tiempo que el mensaje pasa en el sistema Amazon SNS.

Example Ejemplo de escala de tiempo con mensajes de Amazon SNS por lotes

Si se agrupan varios mensajes de Amazon SNS en un solo lote de un rastro, la escala de tiempo de los segmentos muestra los segmentos que representan cada mensaje que se procesa.



AWS Step Functions y AWS X-Ray

AWS X-Ray se integra en AWS Step Functions para rastrear y analizar las solicitudes de Step Functions. Puede visualizar los componentes de su máquina de estado, identificar cuellos de botella en el rendimiento y solucionar problemas de solicitudes que dieron lugar a un error. Para obtener más información, consulte AWS X-Ray y Step Functions en la Guía para desarrolladores de AWS Step Functions.

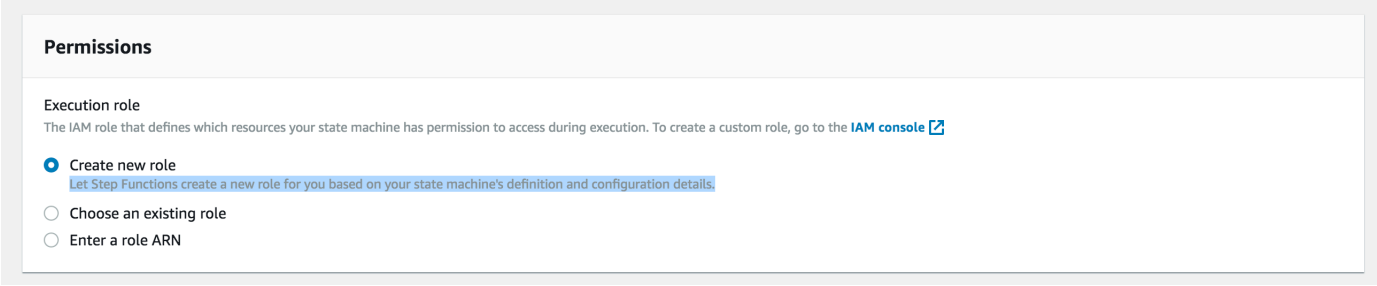
Para habilitar el rastreo de X-Ray al crear una nueva máquina de estado

1. Abra la consola de Step Functions en https://console.aws.amazon.com/states/.
2. Elija Crear máquina de estado.
3. En la página Definir una máquina de estado, elija Crear con fragmentos de código o Empezar con una plantilla. Si decide ejecutar un proyecto de muestra, no podrá habilitar el rastreo de X-Ray durante la creación. En vez de eso, habilite el rastreo de X-Ray después de crear su máquina de estado.

4. Elija Next (Siguiente).
5. En la página Especificar detalles, configure su máquina de estado.
6. Elija Activar rastreo de X-Ray.

Para habilitar el rastreo de X-Ray en una máquina de estado existente

1. En la consola de Step Functions, seleccione la máquina de estado para la que desee activar el rastreo.
2. Elija Edit (Editar).
3. Elija Activar rastreo de X-Ray.
4. (Opcional) Genere automáticamente un nuevo rol para su máquina de estado para incluir los permisos de X-Ray seleccionando Crear nuevo rol en la ventana Permisos.



5. Seleccione Save.

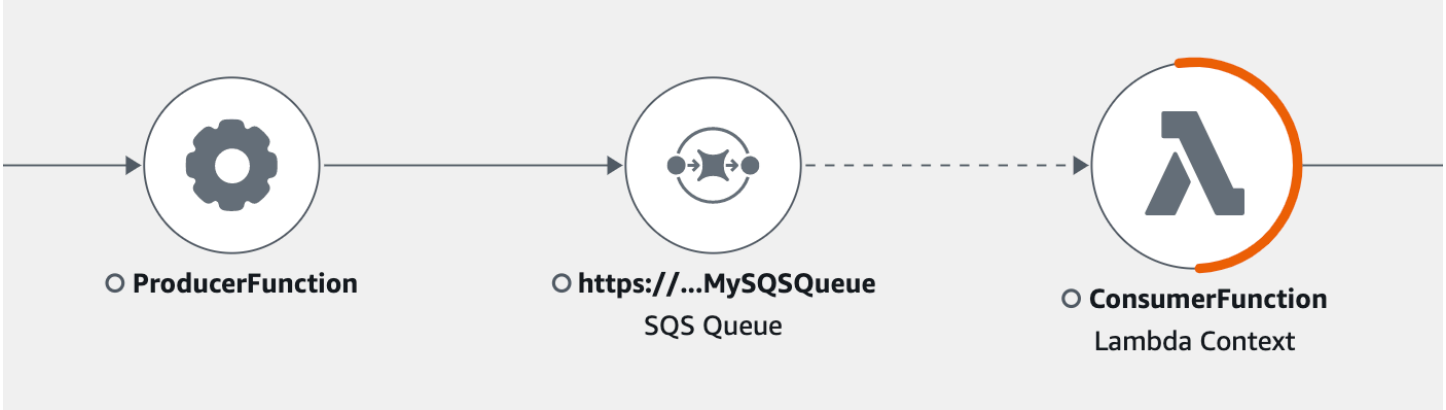
> **Note**
>
> Al crear una nueva máquina de estados, se rastrea automáticamente si la solicitud está muestreada y el rastreo está habilitado en un servicio previo como Amazon API Gateway o AWS Lambda. Para cualquier máquina de estado existente que no esté configurada a través de la consola, por ejemplo, a través de una plantilla de AWS CloudFormation, compruebe que tiene una política de IAM que conceda permisos suficientes para habilitar los rastros de X-Ray.

Amazon SQS y AWS X-Ray

AWS X-Ray se integra con Amazon Simple Queue Service (Amazon SQS) para rastrear los mensajes que pasan por una cola de Amazon SQS. Si un servicio rastrea solicitudes utilizando el

SDK de X-Ray, Amazon SQS podrá enviar el encabezado de rastreo y continuar propagando el rastro original entre el remitente y el consumidor con un ID de rastro coherente. Esta continuidad permite que los usuarios puedan rastrear, analizar y depurar en otros servicios posteriores.

AWS X-Ray admite el seguimiento de aplicaciones basadas en eventos mediante Amazon SQS y. AWS Lambda Utilice la CloudWatch consola para ver una vista conectada de cada solicitud mientras está en cola con Amazon SQS y procesada por una función Lambda descendente. Las trazas de los productores de mensajes ascendentes se vinculan automáticamente a las trazas de los nodos consumidores de Lambda descendentes, lo que crea una end-to-end vista de la aplicación. Para obtener más información, consulte Rastreo de aplicaciones basadas en eventos.



Amazon SQS admite la siguiente instrumentación de encabezado de rastreo:

- Encabezado HTTP predeterminado: el SDK de X-Ray rellena automáticamente el encabezado de rastreo como encabezado HTTP cuando se llama a Amazon SQS a través del AWS SDK. `X-Amzn-Trace-Id` lleva el encabezado de rastreo predeterminado, que se corresponde con todos los mensajes incluidos en una solicitud `SendMessage` o `SendMessageBatch`. Para obtener más información sobre el encabezado HTTP predeterminado, consulte Encabezado de seguimiento.
- Atributo del sistema **`AWSTraceHeader`**: `AWSTraceHeader` es un atributo del sistema de mensajes reservado por Amazon SQS para incluir el encabezado de rastreo de X-Ray con los mensajes de la cola. `AWSTraceHeader` está disponible para su uso incluso cuando la instrumentación automática a través del SDK de X-Ray no lo está, por ejemplo, al crear un SDK de rastreo para un nuevo lenguaje. Cuando se establecen las instrumentaciones de los dos encabezados, el atributo del sistema de mensajes anula el encabezado de rastreo HTTP.

Cuando se ejecuta en Amazon EC2, Amazon SQS solo permite procesar un mensaje cada vez. Esto se aplica cuando se ejecuta en un host local y cuando se utilizan servicios de contenedores AWS Fargate, como Amazon ECS o AWS App Mesh.

El encabezado de rastreo no se incluye en las cuotas del tamaño de mensaje y de atributo del mensaje de Amazon SQS. Al habilitar el rastreo de X-Ray, no se superan las cuotas de Amazon SQS. Para obtener más información sobre AWS las cuotas, consulte Amazon SQS Quotas.

Enviar el encabezado de seguimiento HTTP

Los componentes del remitente de Amazon SQS pueden enviar automáticamente el encabezado de rastreo utilizando una llamada a `SendMessageBatch` o a `SendMessage`. Cuando los clientes AWS del SDK están instrumentados, se les puede realizar un seguimiento automático en todos los idiomas compatibles con el SDK de X-Ray. El rastreo Servicios de AWS y los recursos a los que accede dentro de esos servicios (por ejemplo, un bucket de Amazon S3 o una cola de Amazon SQS) aparecen como nodos descendentes en el mapa de rastreo de la consola X-Ray.

Para obtener información sobre cómo rastrear las llamadas AWS del SDK con su idioma preferido, consulte los siguientes temas de los SDK compatibles:

- Go: Rastreo de llamadas AWS del SDK con el X-Ray SDK for Go
- Java: Rastreo de llamadas al AWS SDK con el X-Ray SDK for Java
- Node.js: Rastreo de llamadas al AWS SDK con el SDK de X-Ray para Node.js
- Python: Rastreo de llamadas al AWS SDK con el SDK de X-Ray para Python
- Ruby: Rastreo de llamadas al AWS SDK con el SDK de X-Ray para Ruby
- .NET: Rastreo de llamadas AWS del SDK con el X-Ray SDK para .NET

Recuperar el encabezado y el contexto de seguimiento

Si utiliza un consumidor posterior de Lambda, la propagación del contexto de rastreo es automática. Para continuar la propagación del contexto con consumidores de Amazon SQS, debe instrumentar manualmente la entrega al componente receptor.

Hay tres pasos principales para recuperar el contexto de rastreo:

- Recibir el mensaje de la cola del atributo `AWSTraceHeader` llamando a la API `ReceiveMessage`.
- Recuperar el encabezado de rastreo del atributo.
- Recuperar el ID de rastreo del encabezado. Si lo desea, también puede añadir otras métricas al segmento.

A continuación se muestra un ejemplo de una implementación escrita con el SDK de X-Ray para Java.

Example : Recuperar el encabezado y el contexto de seguimiento

```
// Receive the message from the queue, specifying the "AWSTraceHeader"
ReceiveMessageRequest receiveMessageRequest = new ReceiveMessageRequest()
        .withQueueUrl(QUEUE_URL)
        .withAttributeNames("AWSTraceHeader");
List<Message> messages = sqs.receiveMessage(receiveMessageRequest).getMessages();

if (!messages.isEmpty()) {
    Message message = messages.get(0);

    // Retrieve the trace header from the AWSTraceHeader message system attribute
    String traceHeaderStr = message.getAttributes().get("AWSTraceHeader");
    if (traceHeaderStr != null) {
        TraceHeader traceHeader = TraceHeader.fromString(traceHeaderStr);

        // Recover the trace context from the trace header
        Segment segment = AWSXRay.getCurrentSegment();
        segment.setTraceId(traceHeader.getRootTraceId());
        segment.setParentId(traceHeader.getParentId());

 segment.setSampled(traceHeader.getSampled().equals(TraceHeader.SampleDecision.SAMPLED));
    }
}
```

Amazon S3 y AWS X-Ray

AWS X-Ray se integra con Amazon S3 para rastrear las solicitudes ascendentes para actualizar los buckets de S3 de la aplicación. Si un servicio rastrea las solicitudes mediante el SDK de X-Ray, Amazon S3 puede enviar los encabezados de rastreo a los suscriptores de eventos posteriores, como AWS Lambda, Amazon SQS y Amazon SNS. X-Ray permite rastrear mensajes para las notificaciones de eventos de Amazon S3.

Puede usar el mapa de rastreo de X-Ray para ver las conexiones entre Amazon S3 y otros servicios que utiliza su aplicación. También puede utilizar la consola para ver métricas como la latencia media y las tasas de errores. Para obtener más información sobre la consola de X-Ray, consulte AWS X-Ray consola.

Amazon S3 admite la instrumentación de encabezados HTTP predeterminados. El SDK de X-Ray rellena automáticamente el encabezado de seguimiento como un encabezado HTTP cuando llama a Amazon S3 a través del AWS SDK. `X-Amzn-Trace-Id` lleva el encabezado de rastreo predeterminado. Para obtener más información sobre los encabezados de rastreo, consulte Encabezado de seguimiento en la página de conceptos. La propagación del contexto de rastreo de Amazon S3 admite los siguientes suscriptores: Lambda, SQS y SNS. Dado que SQS y SNS no emiten datos de segmentos por sí mismos, no aparecerán en el mapa de rastreo o rastreo cuando S3 los active, aunque propagarán el encabezado de rastreo a los servicios descendentes.

Configuración de notificaciones de eventos de Amazon S3

La característica de notificaciones de Amazon S3 le permite recibir notificaciones cuando se producen ciertos eventos en su bucket. A continuación, estas notificaciones se pueden propagar a los siguientes destinos de la aplicación:

- Amazon Simple Notification Service (Amazon SNS)
- Amazon Simple Queue Service (Amazon SQS)
- AWS Lambda

Para obtener una lista de los eventos compatibles, consulte los tipos de eventos compatibles en la Guía para desarrolladores de Amazon S3.

Amazon SNS y Amazon SQS

Debe conceder permisos a Amazon S3 a fin de publicar notificaciones en un tema de SNS o en una cola de SQS. Para conceder estos permisos, debe adjuntar una política AWS Identity and Access Management (IAM) al tema de SNS o a la cola de SQS de destino. Para obtener más información sobre las políticas de IAM necesarias, consulte Conceder permisos para publicar mensajes en un tema de SNS o en una cola de SQS.

Para obtener información sobre la integración de SNS y SQS en X-Ray, consulte Amazon SNS y AWS X-Ray y Amazon SQS y AWS X-Ray.

AWS Lambda

Cuando utiliza la consola de Amazon S3 para configurar notificaciones de eventos en un bucket de S3 para una función de Lambda, la consola configura los permisos necesarios en la función de Lambda para que Amazon S3 tenga permisos para invocar la función en el bucket. Para obtener más

información, consulte ¿Cómo puedo habilitar y configurar notificaciones de eventos para un bucket de S3? en la Guía del usuario de la consola de Amazon Simple Storage Service.

También puede conceder permisos a Amazon S3 AWS Lambda para invocar la función Lambda. Para obtener más información, consulte el tutorial: Uso de AWS Lambda con Amazon S3 en la Guía para desarrolladores de AWS Lambda.

Para obtener más información sobre la integración de Lambda con X-Ray, consulte Instrumentación del código Java en Lambda. AWS

Creación de recursos de X-Ray con AWS CloudFormation

AWS X-Ray está integrado con AWS CloudFormation, un servicio que le ayuda a modelar y configurar sus recursos de AWS para que pueda dedicar menos tiempo a crear y administrar sus recursos e infraestructura. Puede crear una plantilla que describa todos los recursos de AWS que desea y AWS CloudFormation aprovisiona y configura estos recursos por usted.

Cuando utiliza AWS CloudFormation, puede volver a utilizar la plantilla para configurar sus recursos de X-Ray de forma coherente y repetida. Solo tiene que describir los recursos una vez y luego aprovisionar los mismos recursos una y otra vez en varias Cuentas de AWS y regiones.

X-Ray y plantillas de AWS CloudFormation

Para aprovisionar y configurar los recursos de X-Ray y sus servicios conexos, debe entender las plantillas de AWS CloudFormation. Las plantillas son archivos de texto con formato de tipo JSON o YAML. Estas plantillas describen los recursos que desea aprovisionar en sus pilas de AWS CloudFormation. Si no está familiarizado con JSON o YAML, puede utilizar Designer de AWS CloudFormation para comenzar a utilizar las plantillas de AWS CloudFormation. Para obtener más información, consulte ¿Qué es Designer de AWS CloudFormation? en la Guía del usuario de AWS CloudFormation.

X-Ray admite la creación de `AWS::XRay::Group` y `AWS::XRay::SamplingRule` en AWS CloudFormation. Para obtener más información junto con ejemplos de plantillas JSON y YAML, consulte la referencia de tipos de recurso de X-Ray en la Guía del usuario de AWS CloudFormation.

Obtener más información sobre AWS CloudFormation

Para obtener más información acerca de AWS CloudFormation, consulte los siguientes recursos:

- AWS CloudFormation
- Guía del usuario de AWS CloudFormation
- Referencia de la API de AWS CloudFormation
- Guía del usuario de la interfaz de la línea de comandos de AWS CloudFormation

Etiquetado de reglas de muestreo y grupos de X-Ray

Las etiquetas son palabras o frases que puede utilizar para identificar y organizar sus recursos de AWS. Puede agregar varias etiquetas a cada recurso. Cada etiqueta incluye una clave y un valor opcional que define el usuario. Por ejemplo, la clave de etiqueta podría ser **`domain`** y el valor de etiqueta podría ser **`example.com`**. Puede buscar y filtrar sus recursos en función de las etiquetas que añada. Para más información sobre el uso de etiquetas, consulte Etiquetado de recursos de AWS en la Guía de referencia general de AWS.

Puede utilizar etiquetas para aplicar permisos basados en etiquetas a las distribuciones de CloudFront. Para obtener más información, consulte Control de acceso a los recursos de AWS mediante etiquetas.

> **Note**
>
> Actualmente, ni Tag Editor ni AWS Resource Groups admiten recursos de X-Ray. Las etiquetas se agregan y administran mediante la consola o la API de AWS X-Ray.

También puede aplicar etiquetas a recursos a través de la consola, la API y los SDK de X-Ray, la AWS CLI y AWS Tools for Windows PowerShell. Para obtener más información, consulte la documentación siguiente:

- API de X-Ray: consulte las siguientes operaciones en la referencia de la API de AWS X-Ray:
  - ListTagsForResource
  - CreateSamplingRule
  - CreateGroup
  - TagResource
  - UntagResource
- AWS CLI: consulte xray en la Referencia de comandos de la AWS CLI.
- SDK: consulte la documentación del SDK correspondiente en la página Documentación de AWS.

> **Note**
>
> Si no puede agregar o cambiar etiquetas en un recurso de X-Ray, o no puede agregar un recurso que tenga etiquetas específicas, es posible que no tenga permisos para realizar

esta operación. Para solicitar acceso, póngase en contacto con un usuario de AWS de su empresa que tenga permisos de administrador en X-Ray.

Temas

Restricciones de las etiquetas

Se aplican las siguientes restricciones a las etiquetas.

- Número máximo de etiquetas por recurso: 50
- Longitud máxima de la clave: 128 caracteres Unicode.
- Longitud máxima del valor: 256 caracteres Unicode.
- Valores válidos para claves y valores: a-z, A-Z, 0-9, espacio y los siguientes caracteres: _ . : / = + - y @
- Las claves y los valores de las etiquetas distinguen entre mayúsculas y minúsculas.
- No utilice `aws:` como prefijo para claves, ya que está reservado para AWS.

> **Note**
>
> No puede editar ni eliminar las etiquetas del sistema.

Administración de etiquetas en la consola

Puede añadir etiquetas opcionales al crear un grupo de X-Ray o una regla de muestreo. Las etiquetas también se pueden cambiar o eliminar en la consola más adelante.

En los siguientes procedimientos se explica cómo agregar, editar y eliminar etiquetas para sus grupos y reglas de muestreo en la consola X-Ray.

Temas

Agregar etiquetas a un nuevo grupo (consola)

Al crear un nuevo grupo de X-Ray, puede añadir etiquetas opcionales en la página Crear grupo.

1. Inicie sesión en la AWS Management Console y abra la consola de X-Ray en https://console.aws.amazon.com/xray/home.
2. En el panel de navegación, expanda Configuración y elija Grupos.
3. Elija Create group.
4. En la página Crear grupo, especifique un nombre y una expresión de filtro para el grupo. Para obtener más información sobre estas propiedades, consulte Configuración de grupos.
5. En Etiquetas, introduzca una clave de etiqueta y, si lo desea, un valor de etiqueta. Por ejemplo, puede introducir una clave de etiqueta de **`Stage`** y un valor de etiqueta de **`Production`** para indicar que este grupo es para uso en producción. Al añadir una etiqueta, aparece una nueva línea para que añada otra etiqueta, si es necesario. Consulte Restricciones de las etiquetas en este tema para conocer las limitaciones de las etiquetas.
6. Cuando termine de agregar etiquetas, elija Crear grupo.

Agregar etiquetas a una nueva regla de muestreo (consola)

Al crear una nueva regla de muestreo de X-Ray, puede añadir etiquetas en la página Crear regla de muestreo.

1. Inicie sesión en la AWS Management Console y abra la consola de X-Ray en https://console.aws.amazon.com/xray/home.
2. En el panel de navegación, expanda Configuración y elija Muestreo.
3. Seleccione Crear regla de muestreo.

4. En la página Crear regla de muestreo, especifique el nombre, la prioridad, los límites, los criterios coincidentes y los atributos coincidentes. Para obtener más información sobre estas propiedades, consulte Configuración de reglas de muestreo de .
5. En Etiquetas, introduzca una clave de etiqueta y, si lo desea, un valor de etiqueta. Por ejemplo, puede introducir una clave de etiqueta de **`Stage`** y un valor de etiqueta de **`Production`** para indicar que esta regla de muestreo es para uso en producción. Al añadir una etiqueta, aparece una nueva línea para que añada otra etiqueta, si es necesario. Consulte Restricciones de las etiquetas en este tema para conocer las limitaciones de las etiquetas.
6. Cuando termine de agregar etiquetas, elija Crear regla de muestreo.

Edición o eliminación de etiquetas de un grupo (consola)

Puede cambiar o eliminar etiquetas de un grupo de X-Ray en la página Editar grupo.

1. Inicie sesión en la AWS Management Console y abra la consola de X-Ray en https://console.aws.amazon.com/xray/home.
2. En el panel de navegación, expanda Configuración y elija Grupos.
3. En la tabla Grupos, elija el nombre del un grupo.
4. En la página Editar grupo, en Etiquetas, edite las claves y los valores de las etiquetas. No puede tener claves de etiquetas duplicadas. Los valores de las etiquetas son opcionales; puede eliminarlos si lo desea. Para obtener más información sobre otras propiedades de la página Editar grupo, consulte Configuración de grupos. Consulte Restricciones de las etiquetas en este tema para conocer las limitaciones de las etiquetas.
5. Para eliminar una etiqueta, elija X a la derecha de la etiqueta.
6. Cuando haya terminado de editar o eliminar etiquetas, elija Actualizar grupo.

Edición o eliminación de etiquetas de una regla de muestreo (consola)

Puede cambiar o eliminar las etiquetas de una regla de muestreo de X-Ray en la página Editar regla de muestreo.

1. Inicie sesión en la AWS Management Console y abra la consola de X-Ray en https://console.aws.amazon.com/xray/home.
2. En el panel de navegación, expanda Configuración y elija Muestreo.
3. En la tabla Reglas de muestreo, elija el nombre de una regla de muestreo.

4. En Etiquetas, edite las claves y los valores de las etiquetas. No puede tener claves de etiquetas duplicadas. Los valores de las etiquetas son opcionales; puede eliminarlos si lo desea. Para obtener más información sobre otras propiedades de la página Editar regla de muestreo, consulte Configuración de reglas de muestreo de . Consulte Restricciones de las etiquetas en este tema para conocer las limitaciones de las etiquetas.
5. Para eliminar una etiqueta, elija X a la derecha de la etiqueta.
6. Cuando haya terminado de editar o eliminar etiquetas, elija Actualizar regla de muestreo.

Administración de etiquetas en la AWS CLI

Puede añadir etiquetas al crear un grupo o una regla de muestreo de X-Ray. También puede utilizar la AWS CLI para crear y administrar etiquetas. Para actualizar las etiquetas de un grupo o de una regla de muestreo existente, use la consola de AWS X-Ray o las API TagResource o UntagResource.

Temas

- Agregar etiquetas a un nuevo grupo de o regla de muestreo de X-Ray (CLI)
- Añadir etiquetas a un recurso existente (CLI)
- Visualizar las etiquetas de un recurso (CLI)
- Eliminar etiquetas de un recurso (CLI)

Agregar etiquetas a un nuevo grupo de o regla de muestreo de X-Ray (CLI)

Para añadir etiquetas opcionales al crear un nuevo grupo o una nueva regla de muestreo de X-Ray, utilice uno de los siguientes comandos.

- Para añadir etiquetas a un nuevo grupo, ejecute el siguiente comando y sustituya *group_name* por el nombre de su grupo, *mydomain.com* por el punto de conexión de su servicio, *key_name* por una clave de etiqueta y, si lo desea, *value* por un valor de etiqueta. Para obtener más información sobre cómo crear un grupo, consulte Grupos.

```
aws xray create-group \
   --group-name "group_name" \
   --filter-expression "service(\"mydomain.com\") {fault OR error}" \
   --tags [{"Key": "key_name","Value": "value"},{"Key": "key_name","Value": "value"}]
```

A continuación, se muestra un ejemplo.

```
aws xray create-group \
   --group-name "AdminGroup" \
   --filter-expression "service(\"mydomain.com\") {fault OR error}" \
   --tags [{"Key": "Stage","Value": "Prod"},{"Key": "Department","Value": "QA"}]
```

- Para añadir etiquetas a una nueva regla de muestreo, ejecute el siguiente comando y sustituya *key_name* por una clave de etiqueta y, si lo desea, *value* por un valor de etiqueta. Este comando especifica los valores del parámetro `--sampling-rule` como archivo JSON. Para obtener más información sobre cómo crear una regla de muestreo, consulte Reglas de muestreo.

```
aws xray create-sampling-rule \
   --cli-input-json file://file_name.json
```

A continuación puede ver el contenido del archivo JSON *file_name.json* especificado por el parámetro `--cli-input-json`.

```
{
    "SamplingRule": {
        "RuleName": "rule_name",
        "RuleARN": "string",
        "ResourceARN": "string",
        "Priority": integer,
        "FixedRate": double,
        "ReservoirSize": integer,
        "ServiceName": "string",
        "ServiceType": "string",
        "Host": "string",
        "HTTPMethod": "string",
        "URLPath": "string",
        "Version": integer,
        "Attributes": {"attribute_name": "value","attribute_name": "value"...}
    }
    "Tags": [
           {
               "Key":"key_name",
               "Value":"value"
           },
           {
               "Key":"key_name",
```

```
                "Value":"value"
            }
           ]
}
```

El siguiente comando es un ejemplo.

```
aws xray create-sampling-rule \
   --cli-input-json file://9000-base-scorekeep.json
```

A continuación puede ver el contenido del archivo de ejemplo `9000-base-scorekeep.json` especificado por el parámetro `--cli-input-json`.

```
{
    "SamplingRule": {
        "RuleName": "base-scorekeep",
        "ResourceARN": "*",
        "Priority": 9000,
        "FixedRate": 0.1,
        "ReservoirSize": 5,
        "ServiceName": "Scorekeep",
        "ServiceType": "*",
        "Host": "*",
        "HTTPMethod": "*",
        "URLPath": "*",
        "Version": 1
    }
    "Tags": [
            {
                "Key":"Stage",
                "Value":"Prod"
            },
            {
                "Key":"Department",
                "Value":"QA"
            }
           ]
}
```

Añadir etiquetas a un recurso existente (CLI)

Puede ejecutar el comando `tag-resource` para añadir etiquetas a un grupo o una regla de muestreo de X-Ray existente. Este método puede resultar más sencillo que añadir etiquetas ejecutando `update-group` o `update-sampling-rule`.

Para agregar etiquetas a un grupo o a una regla de muestreo, ejecute el siguiente comando, sustituyendo el ARN por el ARN del recurso y especificando las claves y los valores opcionales de las etiquetas que desee agregar.

```
aws xray tag-resource \
   --resource-arn "ARN" \
   --tag-keys [{"Key":"key_name","Value":"value"}, {"Key":"key_name","Value":"value"}]
```

A continuación, se muestra un ejemplo.

```
aws xray tag-resource \
   --resource-arn "arn:aws:xray:us-east-2:01234567890:group/AdminGroup" \
   --tag-keys [{"Key": "Stage","Value": "Prod"},{"Key": "Department","Value": "QA"}]
```

Visualizar las etiquetas de un recurso (CLI)

Puede ejecutar el comando `list-tags-for-resource` para ver una lista de las etiquetas de un grupo o una regla de muestreo de X-Ray.

Para ver una lista de las etiquetas asociadas a un grupo o una regla de muestreo, ejecute el siguiente comando sustituyendo el ARN por el ARN del recurso.

```
aws xray list-tags-for-resource \
   --resource-arn "ARN"
```

A continuación, se muestra un ejemplo.

```
aws xray list-tags-for-resource \
   --resource-arn "arn:aws:xray:us-east-2:01234567890:group/AdminGroup"
```

Eliminar etiquetas de un recurso (CLI)

Puede ejecutar el comando `untag-resource` para eliminar las etiquetas de un grupo o una regla de muestreo de X-Ray.

Para agregar etiquetas de un grupo o de una regla de muestreo, ejecute el siguiente comando, sustituyendo el ARN por el ARN del recurso y especificando las claves de las etiquetas que desee eliminar.

Con el comando `untag-resource` solo puede eliminar etiquetas enteras. Para eliminar los valores de las etiquetas, utilice la consola de X-Ray o elimine las etiquetas y añada otras nuevas con las mismas claves pero con valores diferentes o vacíos.

```
aws xray untag-resource \
   --resource-arn "ARN" \
   --tag-keys ["key_name","key_name"]
```

A continuación, se muestra un ejemplo.

```
aws xray untag-resource \
   --resource-arn "arn:aws:xray:us-east-2:01234567890:group/group_name" \
   --tag-keys ["Stage","Department"]
```

Controlar el acceso a los recursos de X-Ray en función de etiquetas

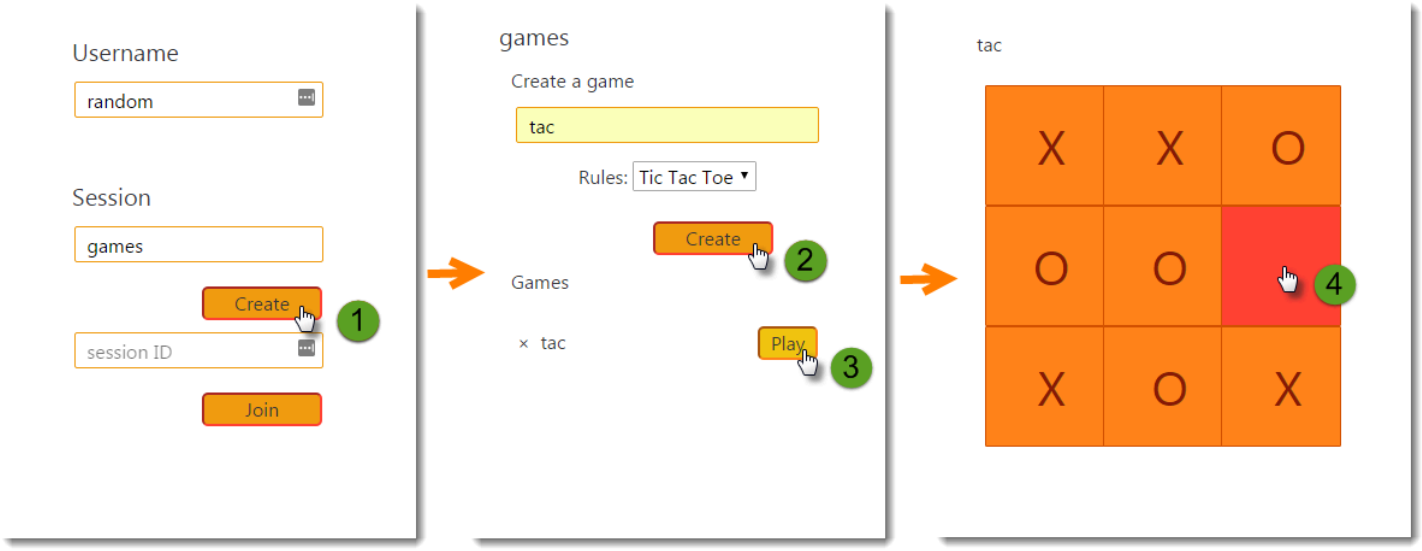
Puede adjuntar etiquetas a los grupos o las reglas de muestreo de X-Ray, o pasar las etiquetas en una solicitud a X-Ray. Para controlar el acceso en función de etiquetas, debe proporcionar información de las etiquetas en el elemento de condición de una política utilizando las claves de condición `xray:ResourceTag/key-name`, `aws:RequestTag/key-name` o `aws:TagKeys`. Para obtener más información sobre estas claves de condición, consulte Control de acceso a los recursos de AWS mediante etiquetas.

Para consultar un ejemplo de política basada en la identidad para limitar el acceso a un recurso en función de las etiquetas de ese recurso, consulte Gestión del acceso a los grupos de rayos X y a las reglas de muestreo en función de las etiquetas.

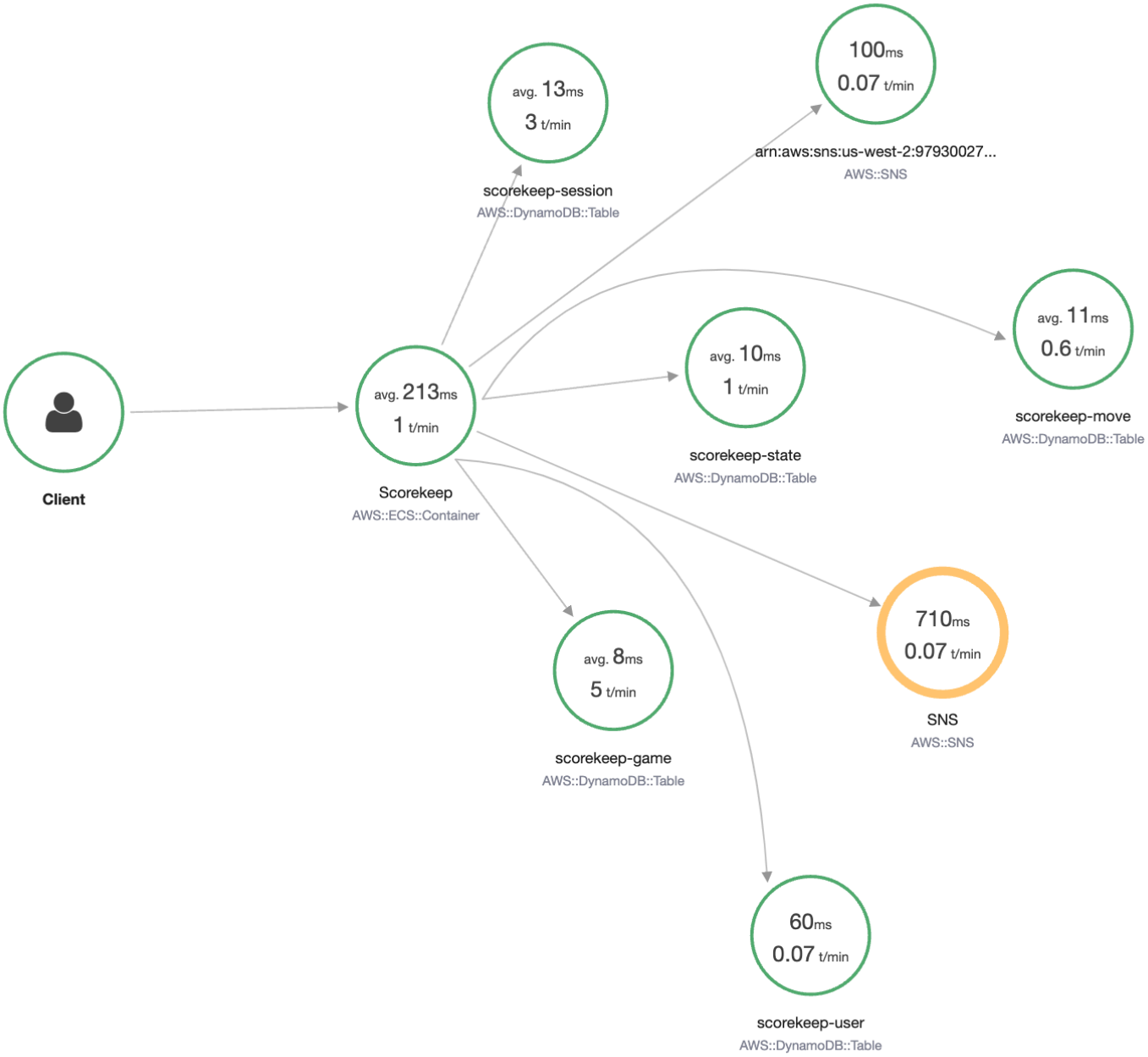
AWS X-Ray ejemplo de aplicación

La aplicación de eb-java-scorekeepejemplo AWS X-Ray, disponible en GitHub, muestra el uso del AWS X-Ray SDK para instrumentar las llamadas HTTP entrantes, los clientes del SDK de DynamoDB y los clientes HTTP. La aplicación de ejemplo se utiliza AWS CloudFormation para crear tablas de DynamoDB, compilar código Java en una instancia y ejecutar el daemon X-Ray sin ninguna configuración adicional.

Consulte el tutorial de Scorekeep para empezar a instalar y utilizar una aplicación de ejemplo instrumentada, utilizando el o el. AWS Management Console AWS CLI



La muestra incluye una aplicación web frontend, la API a la que llama y las tablas de DynamoDB que usa para almacenar los datos. La instrumentación básica con filtros, complementos y clientes de AWS SDK instrumentados se muestra en la rama del proyecto. `xray-gettingstarted` Esta es la ramificación que se implementa en el tutorial Introducción. Dado que esta ramificación solo incluye los aspectos básicos, puede diferenciarla rápidamente de la ramificación `master` para comprender rápidamente los aspectos básicos.



La aplicación de ejemplo muestra una instrumentación básica en estos archivos:

- Filtro de solicitudes HTTP: `WebConfig.java`
- AWS Instrumentación de cliente del SDK: `build.gradle`

La ramificación `xray` de la aplicación incluye el uso de HTTPClient, Anotaciones, consultas SQL, subsegmentos personalizados, una función de AWS Lambda instrumentada, así como scripts y código de inicialización instrumentado.

Para permitir el inicio de sesión de los usuarios y AWS SDK for JavaScript su uso en el navegador, la `xray-cognito` sucursal añade Amazon Cognito para admitir la autenticación y la autorización de los usuarios. Con credenciales recuperadas desde Amazon Cognito, la aplicación web también envía datos de rastreo a X-Ray para registrar la información de la solicitud desde el punto de vista del cliente. El cliente del navegador aparece como su propio nodo en el mapa de rastreo y registra información adicional, incluida la URL de la página que está viendo el usuario y su ID.

Por último, la ramificación `xray-worker` añade una función de Lambda en Python instrumentada que se ejecuta de forma independiente, procesando los elementos de una cola de Amazon SQS. Scorekeep añade un elemento a la cola cada vez que termina un juego. El trabajador de Lambda, activado por CloudWatch eventos, extrae elementos de la cola cada pocos minutos y los procesa para almacenar registros de juegos en Amazon S3 para su análisis.

Temas

Introducción a la aplicación de ejemplo Scorekeep

En este tutorial se utiliza la `xray-gettingstarted` rama de la aplicación de ejemplo Scorekeep, que se utiliza AWS CloudFormation para crear y configurar los recursos que ejecutan la aplicación de

ejemplo y el daemon X-Ray en Amazon ECS. La aplicación utiliza el marco Spring para implementar una API web de JSON y AWS SDK for Java para conservar los datos en Amazon DynamoDB. Un servlet filtra en la aplicación instrumenta todas las solicitudes entrantes atendidas por la aplicación y un controlador de solicitudes en el cliente del AWS SDK instrumenta las llamadas descendentes a DynamoDB.

Puede seguir este tutorial utilizando el o el. AWS Management Console AWS CLI

Secciones

Requisitos previos

Este tutorial se utiliza AWS CloudFormation para crear y configurar los recursos que ejecutan la aplicación de ejemplo y el daemon X-Ray. Se tienen que cumplir los siguientes requisitos previos para instalar y ejecutar el tutorial:

1. Si utiliza un usuario de IAM con permisos limitados, añada las siguientes políticas de usuario en la consola de IAM:

   - `AWSCloudFormationFullAccess`— para acceder y usar CloudFormation
   - `AmazonS3FullAccess`— para cargar un archivo de plantilla CloudFormation utilizando el AWS Management Console
   - `IAMFullAccess`: para crear los roles de instancia de Amazon ECS y Amazon EC2
   - `AmazonEC2FullAccess`: para crear los recursos de Amazon EC2
   - `AmazonDynamoDBFullAccess`: para crear las tablas de DynamoDB
   - `AmazonECS_FullAccess`: para crear recursos de Amazon ECS

- `AmazonSNSFullAccess`: para crear el tema de Amazon SNS
- `AWSXrayReadOnlyAccess`— para obtener permiso para ver el mapa de rastreo y los rastros en la consola de X-Ray

2. Para seguir el tutorial mediante el AWS CLI, instale la CLI versión 2.7.9 o posterior y configure la CLI con el usuario del paso anterior. Asegúrese de que la región esté configurada al configurar AWS CLI con el usuario. Si no se configura una región, hay que anexar `--region` *AWS-REGION* a todos los comandos de la CLI.
3. Asegúrese de que Git esté instalado para clonar el repositorio de aplicaciones de muestra.
4. Utilice el siguiente ejemplo de código para clonar la `xray-gettingstarted` rama del repositorio de Scorekeep:

```
git clone https://github.com/aws-samples/eb-java-scorekeep.git xray-scorekeep -b
 xray-gettingstarted
```

Instale la aplicación Scorekeep mediante CloudFormation

AWS Management Console

Instale la aplicación de ejemplo mediante el AWS Management Console

1. Abra la consola de CloudFormation.
2. Elija Crear pila y, a continuación, elija Con nuevos recursos en el menú desplegable.
3. En la sección Especificar plantilla, elija Cargar un archivo de plantilla.
4. Seleccione Elegir archivo, navegue hasta la carpeta `xray-scorekeep/cloudformation` que se creó al clonar el repositorio de Git y elija el archivo `cf-resources.yaml`.
5. Elija Siguiente para continuar.
6. Escriba `scorekeep` en el cuadro de texto Nombre de la pila y, a continuación, seleccione Siguiente en la parte inferior de la página para continuar. Tenga en cuenta que en el resto de este tutorial se supone que la pila se llama `scorekeep`.
7. Desplázate hasta la parte inferior de la página Configuración de opciones de pila y seleccione Siguiente para continuar.
8. Desplázate hasta la parte inferior de la página de revisión, selecciona la casilla de verificación que indica que se CloudFormation pueden crear recursos de IAM con nombres personalizados y selecciona Crear pila.

9. La CloudFormation pila se está creando ahora. El estado de la pila será `CREATE_IN_PROGRESS` durante unos cinco minutos antes de cambiar a `CREATE_COMPLETE`. El estado se actualizará periódicamente, o el usuario puede actualizar la página.

AWS CLI

Instale la aplicación de ejemplo mediante el AWS CLI

1. Navegue hasta la carpeta `cloudformation` del repositorio `xray-scorekeep` que clonó anteriormente en el tutorial:

```
cd xray-scorekeep/cloudformation/
```

2. Introduzca el siguiente AWS CLI comando para crear la CloudFormation pila:

```
aws cloudformation create-stack --stack-name scorekeep --capabilities
 "CAPABILITY_NAMED_IAM" --template-body file://cf-resources.yaml
```

3. Espere hasta que el estado de la CloudFormation pila sea `CREATE_COMPLETE` correcto, lo que tardará unos cinco minutos. Usa el siguiente AWS CLI comando para comprobar el estado:

```
aws cloudformation describe-stacks --stack-name scorekeep --query
 "Stacks[0].StackStatus"
```

Generación de datos de rastreo

La aplicación de ejemplo incluye una aplicación web front-end. Utilice la aplicación web para generar tráfico a la API y enviar los datos de rastreo a X-Ray. En primer lugar, recupere la URL de la aplicación web mediante la AWS Management Console o la AWS CLI:

AWS Management Console

Busque la URL de la aplicación mediante el AWS Management Console

1. Abra la consola de CloudFormation.
2. Elija la pila `scorekeep` en la lista.

3. Elija la pestaña Salidas en la página de la pila `scorekeep` y elija el enlace URL `LoadBalancerUrl` para abrir la aplicación web.

AWS CLI

Busque la URL de la aplicación mediante el AWS CLI

1. Use el siguiente comando para mostrar la dirección URL de la aplicación web:

```
aws cloudformation describe-stacks --stack-name scorekeep --query
 "Stacks[0].Outputs[0].OutputValue"
```

2. Copie esta URL y ábrala en un navegador para mostrar la aplicación web Scorekeep.

Uso de la aplicación web para generar datos de rastreo

1. Elija Create (Crear) para crear un usuario y una sesión.
2. Escriba un nombre de juego en game name (nombre de juego), establezca Rules (Reglas) en Tic Tac Toe (Tres en raya) y seleccione después Create (Crear) para crear un juego.
3. Seleccione Play (Jugar) para comenzar el juego.
4. Elija una ficha para hacer un movimiento y cambiar el estado del juego.

Cada uno de estos pasos genera solicitudes HTTP a la API y llamadas posteriores a DynamoDB para leer y escribir el usuario, la sesión, el juego, la movida y los datos de estado.

Vea el mapa de rastreo en el AWS Management Console

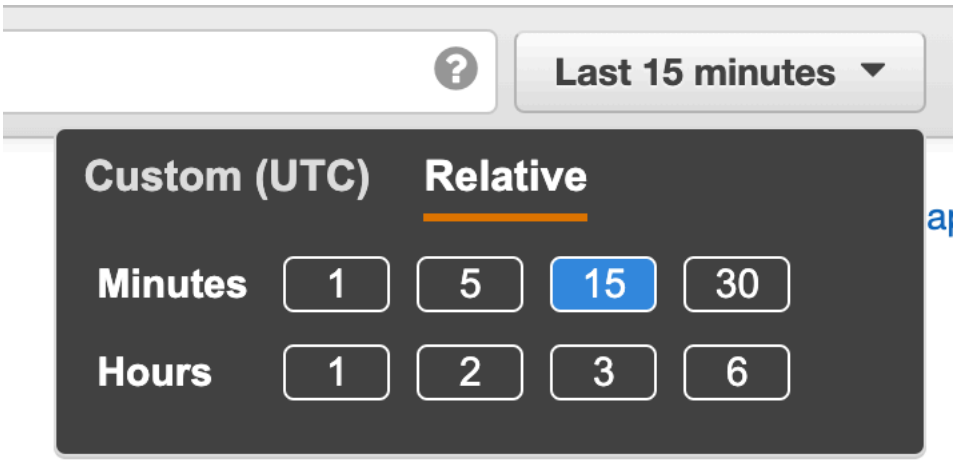
Puede ver el mapa de trazas y las trazas generadas por la aplicación de ejemplo en X-Ray y en CloudWatch las consolas.

X-Ray console

Uso de la consola de X-Ray

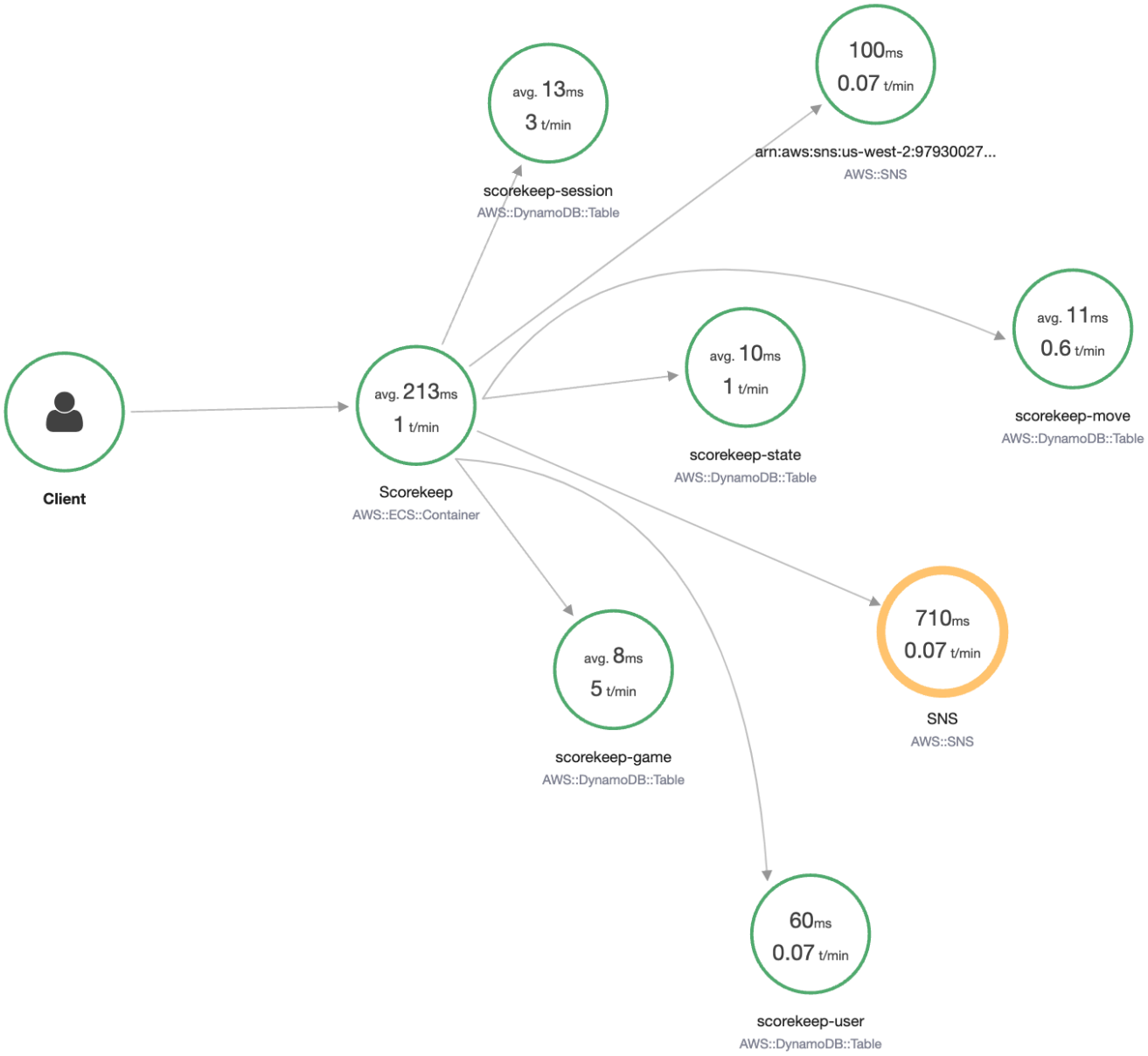
1. Abra la página del mapa de rastreo de la consola de X-Ray.
2. La consola muestra una representación del gráfico de servicios que X-Ray genera a partir de los datos de rastreo que envía la aplicación. Asegúrese de ajustar el período de tiempo del

mapa de rastreo si es necesario, para asegurarse de que mostrará todos los rastros desde que inició la aplicación web.



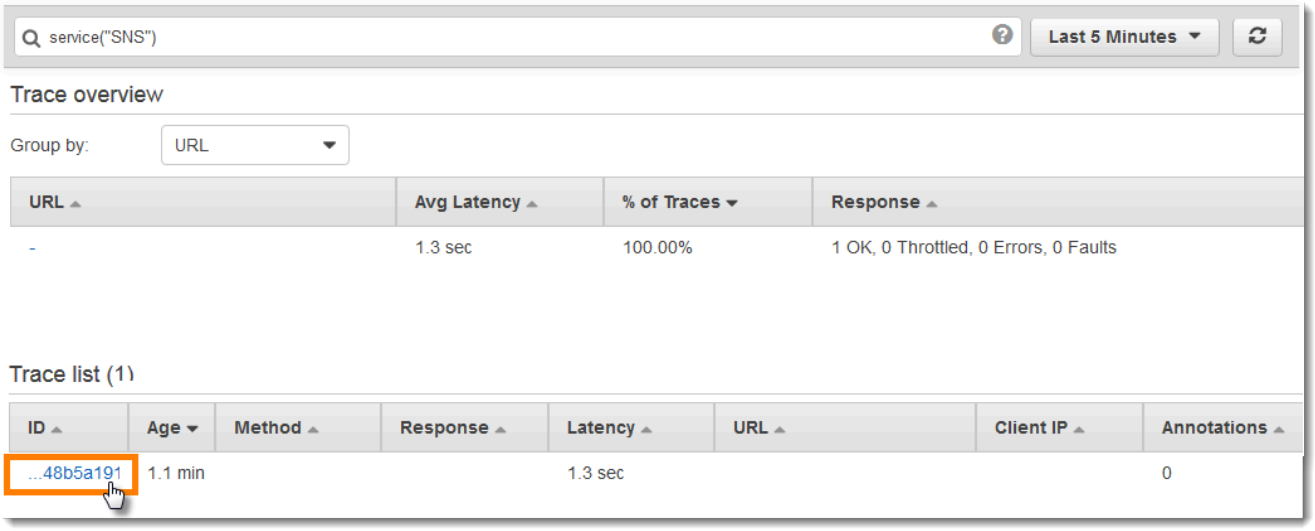
El mapa de seguimiento muestra el cliente de la aplicación web, la API que se ejecuta en Amazon ECS y cada tabla de DynamoDB que utiliza la aplicación. Cada solicitud que se envía a la aplicación, hasta una cantidad máxima configurable de solicitudes por segundo, se rastrea hasta que llega a la API, genera solicitudes para los servicios posteriores y se completa.

Puede elegir cualquier nodo en el gráfico de servicios para ver los rastros de las solicitudes que generaron tráfico hacia ese nodo. Actualmente, el nodo Amazon SNS es amarillo. Profundice para saber por qué.

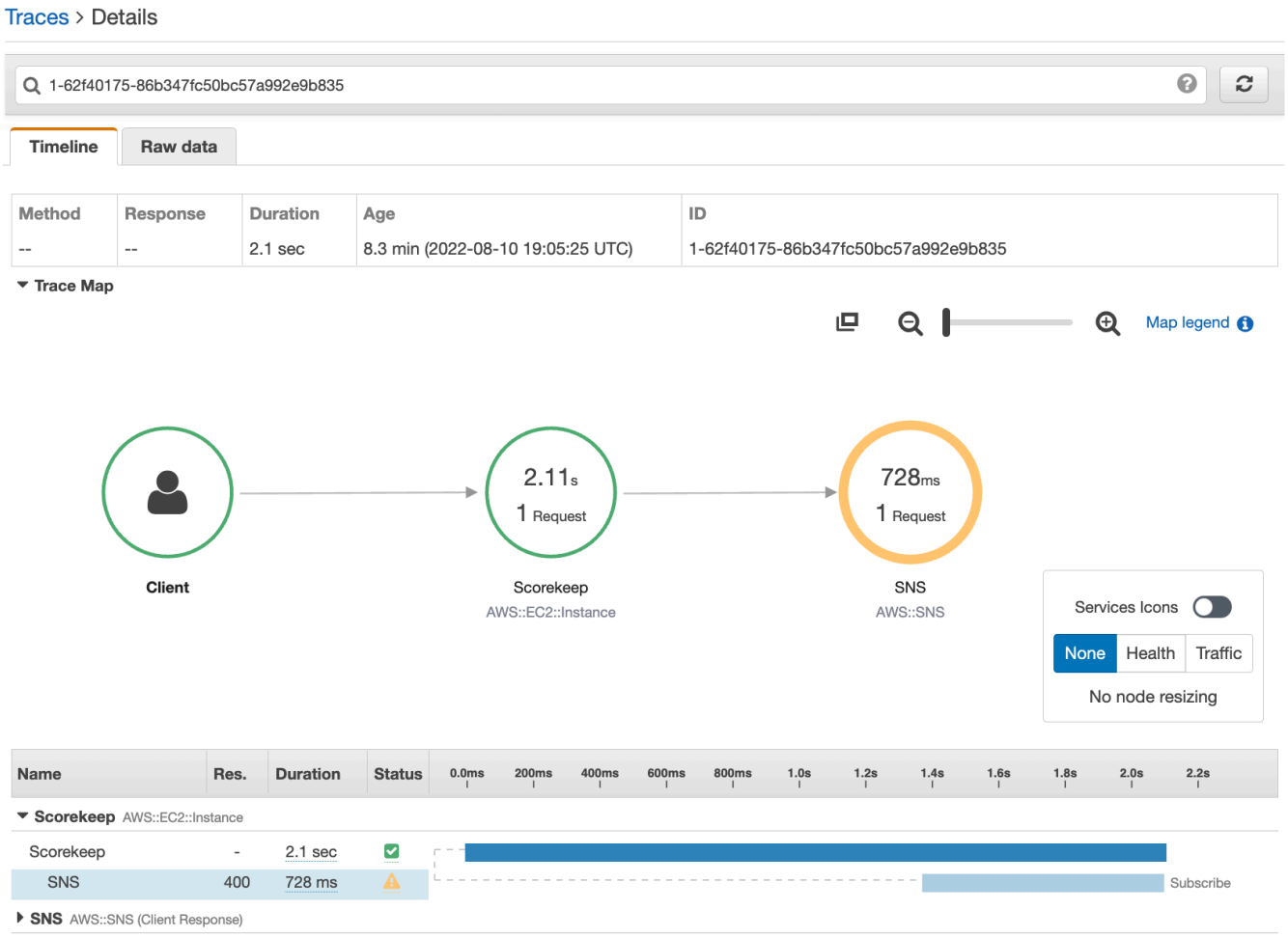


Para encontrar la causa del error

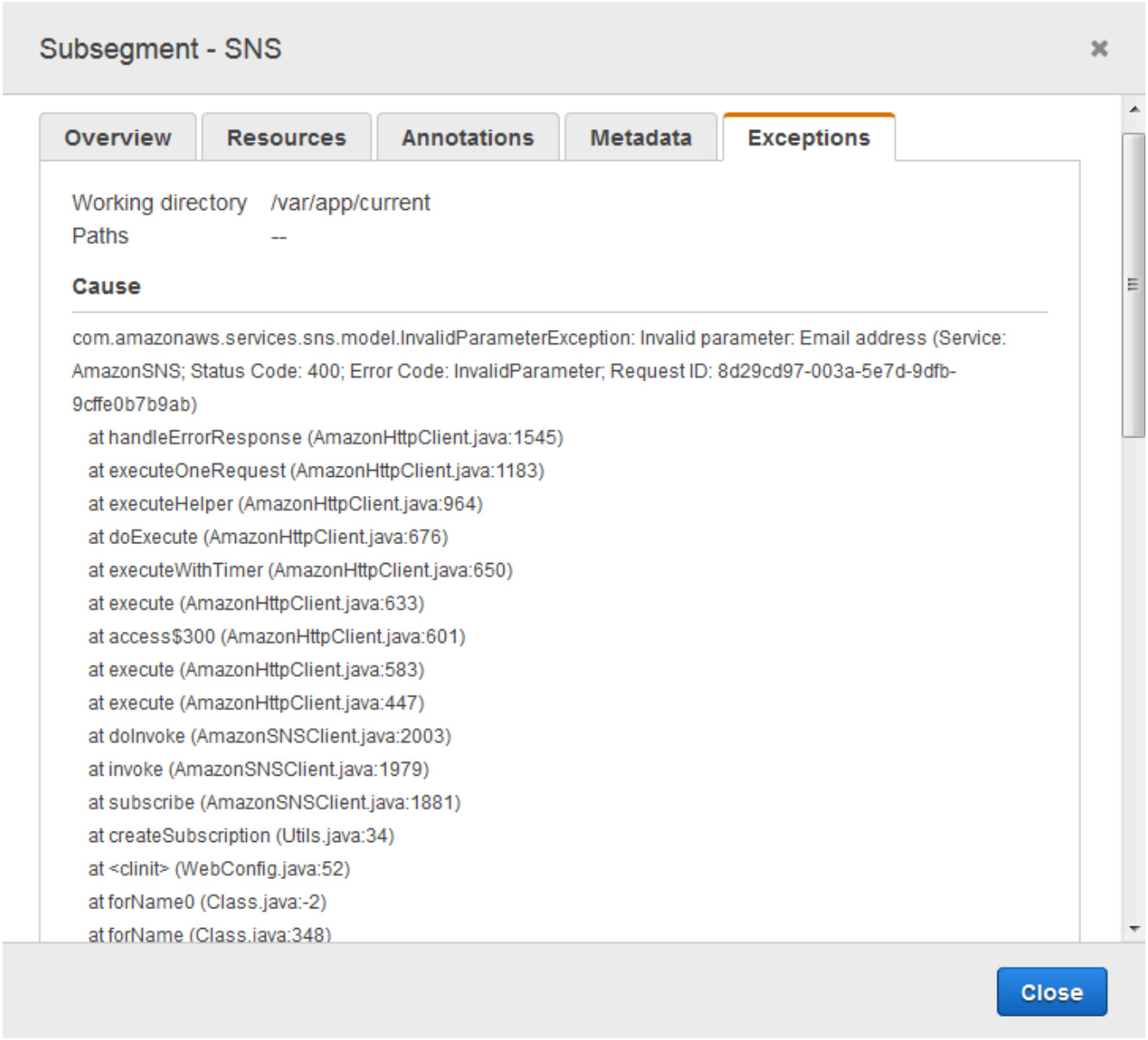
1. Seleccione el nodo denominado SNS. Se muestra el panel de detalles del nodo.
2. Elija View traces (Ver rastreos) para acceder a la pantalla Trace overview (Información general de rastreo).
3. Seleccione el rastro en Trace list (Lista de rastros). Este rastro no tiene método ni URL porque se registró durante el inicio y no en respuesta a una solicitud de entrada.



4. Seleccione el icono de estado de error en el segmento de Amazon SNS en la parte inferior de la página para abrir la página Excepciones del subsegmento de SNS.



5. El SDK de X-Ray captura automáticamente las excepciones producidas por clientes del SDK de AWS instrumentados y registra el seguimiento de la pila.

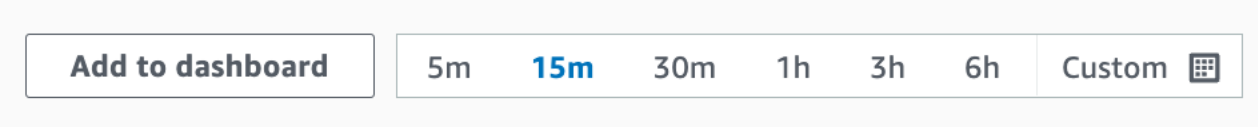


CloudWatch console

Usa la CloudWatch consola

1. Abra la página del mapa de rastreo de X-Ray de la CloudWatch consola.
2. La consola muestra una representación del gráfico de servicios que X-Ray genera a partir de los datos de rastreo que envía la aplicación. Asegúrese de ajustar el período de tiempo del

mapa de rastreo si es necesario, para asegurarse de que mostrará todos los rastros desde que inició la aplicación web.



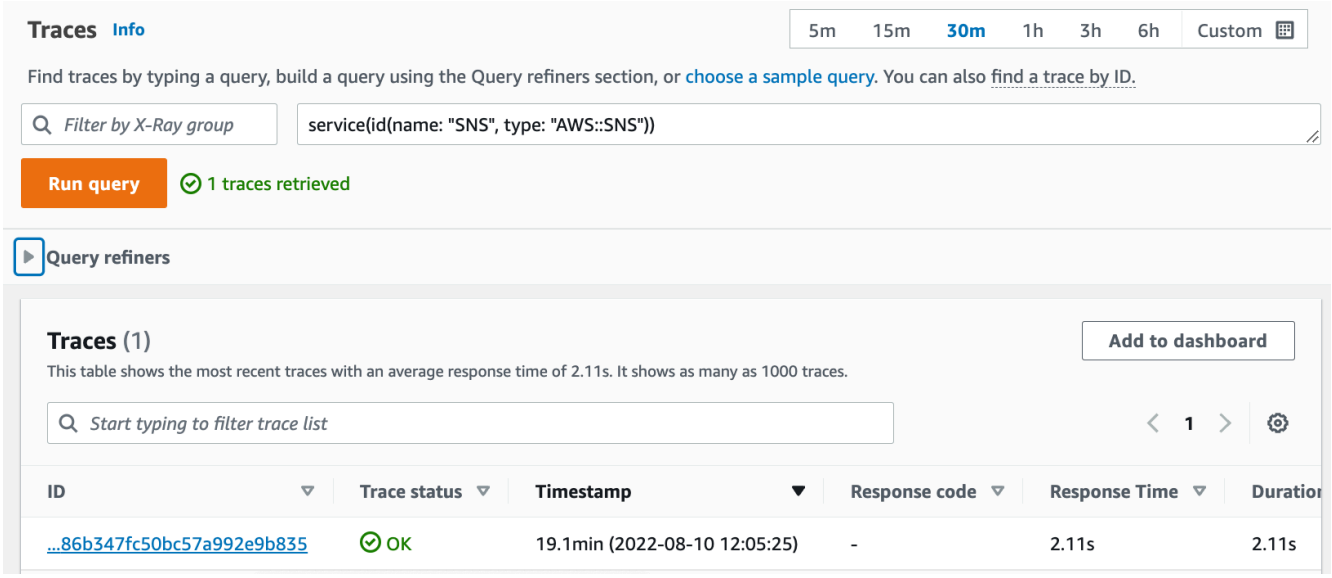
El mapa de seguimiento muestra el cliente de la aplicación web, la API que se ejecuta en Amazon EC2 y cada tabla de DynamoDB que utiliza la aplicación. Cada solicitud que se envía a la aplicación, hasta una cantidad máxima configurable de solicitudes por segundo, se rastrea hasta que llega a la API, genera solicitudes para los servicios posteriores y se completa.

Puede elegir cualquier nodo en el gráfico de servicios para ver los rastros de las solicitudes que generaron tráfico hacia ese nodo. Actualmente, el nodo Amazon SNS es naranja. Profundice para saber por qué.

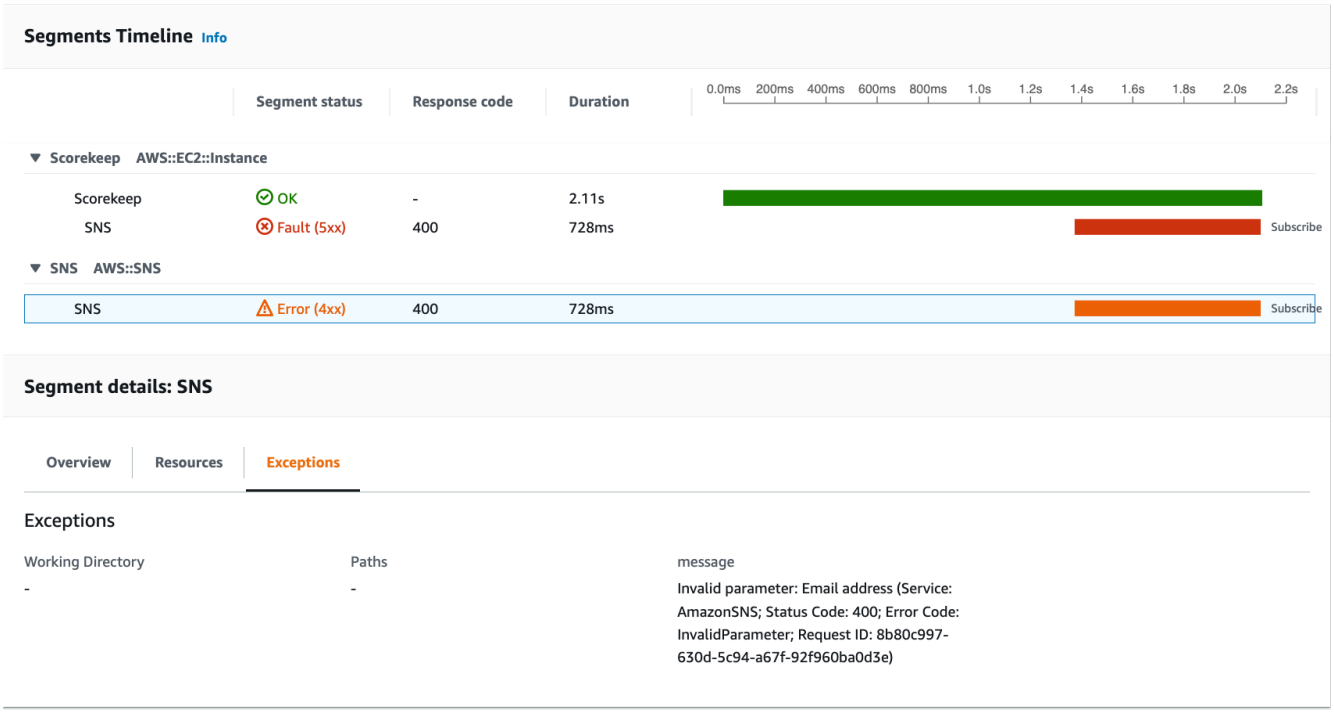

scorekeep-state
DynamoDB Table
scorekeep-game
DynamoDB Table
scorekeep-move
DynamoDB Table
Client
Scorekeep
ECS Container
SNS
SNS
scorekeep-session
DynamoDB Table

Para encontrar la causa del error

1. Seleccione el nodo denominado SNS. El panel de detalles del nodo SNS se muestra debajo del mapa.
2. Seleccione Ver rastros para acceder a la página Rastros.
3. En la parte inferior de la página, elija el rastro de la lista Rastros. Este rastro no tiene método ni URL porque se registró durante el inicio y no en respuesta a una solicitud de entrada.



4. Elija el subsegmento de Amazon SNS en la parte inferior de la escala de tiempo de los segmentos y elija la pestaña Excepciones del subsegmento de SNS para ver los detalles de la excepción.



La causa indica que la dirección de correo electrónico proporcionada en una llamada a `createSubscription` realizada en la clase `WebConfig` no era válida. Lo arreglaremos en la siguiente sección.

Configuración de notificaciones de Amazon SNS

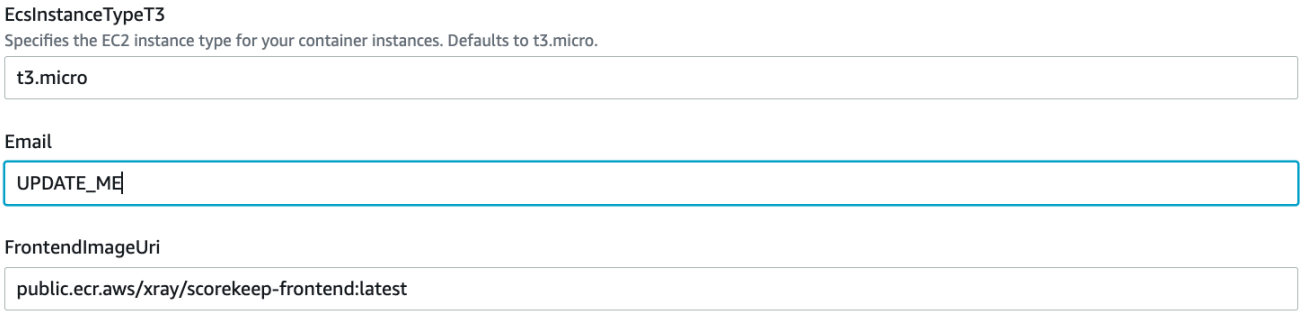
Scorekeep utiliza Amazon SNS para enviar notificaciones cuando los usuarios completan un juego. Cuando la aplicación se inicia, intenta crear una suscripción para una dirección de correo electrónico definida en un parámetro de CloudFormation pila. Esa llamada está fallando actualmente. Configure un correo electrónico de notificación para habilitar las notificaciones y resolver los errores resaltados en el mapa de rastreo.

AWS Management Console

Para configurar las notificaciones de Amazon SNS mediante el AWS Management Console

1. Abra la consola de CloudFormation.
2. Seleccione el botón de opción situado junto al nombre de pila `scorekeep` en la lista y, a continuación, seleccione Actualizar.
3. Asegúrese de seleccionar Usar la plantilla actual y, a continuación, haga clic en Siguiente en la página Actualizar pila.

4. Busque el parámetro Correo electrónico en la lista y sustituya el valor predeterminado por una dirección de correo electrónico válida.



5. Desplácese hasta la parte inferior de la página y elija Siguiente.
6. Desplázate hasta la parte inferior de la página de revisión, selecciona la casilla de verificación que confirma que se CloudFormation pueden crear recursos de IAM con nombres personalizados y selecciona Actualizar pila.
7. La CloudFormation pila se está actualizando ahora. El estado de la pila será `UPDATE_IN_PROGRESS` durante unos cinco minutos antes de cambiar a `UPDATE_COMPLETE`. El estado se actualizará periódicamente, o el usuario puede actualizar la página.

AWS CLI

Para configurar las notificaciones de Amazon SNS mediante el AWS CLI

1. Vaya a la carpeta `xray-scorekeep/cloudformation/` que creó anteriormente y abra el archivo `cf-resources.yaml` en un editor de texto.
2. Busque el valor `Default` en el parámetro Correo electrónico y cámbialo de *`UPDATE_ME`* a una dirección de correo electrónico válida.

```
Parameters:
  Email:
    Type: String
    Default: UPDATE_ME # <- change to a valid abc@def.xyz email address
```

3. Desde la `cloudformation` carpeta, actualice la CloudFormation pila con el siguiente AWS CLI comando:

```
aws cloudformation update-stack --stack-name scorekeep --capabilities
 "CAPABILITY_NAMED_IAM" --template-body file://cf-resources.yaml
```

4. Espera a que se CloudFormation muestre el estado de la pilaUPDATE_COMPLETE, lo que tardará unos minutos. Usa el siguiente AWS CLI comando para comprobar el estado:

```
aws cloudformation describe-stacks --stack-name scorekeep --query
 "Stacks[0].StackStatus"
```

Cuando se completa la actualización, Scorekeep se reinicia y crea una suscripción al tema de SNS. Compruebe su correo electrónico y confirme la suscripción para ver las actualizaciones cuando complete un juego. Abra el mapa de rastreo para comprobar que las llamadas al SNS ya no producen errores.

Explorar la aplicación de ejemplo

La aplicación de ejemplo es una API web HTTP en Java que está configurada para utilizar el SDK de X-Ray para Java. Al implementar la aplicación con la CloudFormation plantilla, esta crea las tablas de DynamoDB, el clúster de Amazon ECS y otros servicios necesarios para ejecutar Scorekeep en ECS. Se crea un archivo de definición de tareas para ECS mediante. CloudFormation Este archivo define las imágenes del contenedor utilizadas por tarea en un clúster de ECS. Estas imágenes se obtienen del ECR público oficial de X-Ray. La imagen del contenedor de la API de Scorekeep tiene la API compilada con Gradle. La imagen de contenedor del contenedor frontend de Scorekeep atiende al frontend mediante el servidor proxy nginx. Este servidor dirige las solicitudes a las rutas que empiezan por /api a la API.

Para instrumentar las solicitudes de HTTP entrantes, la aplicación añade el `TracingFilter` que proporciona el SDK.

Example src/main/java/scorekeep/ .java: filtro WebConfig de servlets

```
import javax.servlet.Filter;
import com.amazonaws.xray.javax.servlet.AWSXRayServletFilter;
...

@Configuration
public class WebConfig {

  @Bean
```

```
  public Filter TracingFilter() {
    return new AWSXRayServletFilter("Scorekeep");
  }
...
```

Este filtro envía datos de rastreo sobre todas las solicitudes entrantes que la aplicación atiende, incluidos el URL, el método, el estado de la respuesta, la hora de inicio y la hora de finalización de la solicitud.

La aplicación también realiza llamadas posteriores a DynamoDB mediante el AWS SDK for Java. Para instrumentar estas llamadas, la aplicación simplemente toma los submódulos AWS relacionados con el SDK como dependencias y el X-Ray SDK for Java instrumenta automáticamente todos los clientes del SDK. AWS

La aplicación utiliza `Docker` para compilar el código de fuente de la instancia con `Gradle Docker Image` y el archivo `Scorekeep API Dockerfile` para ejecutar el archivo ejecutable JAR que Gradle genera en su `ENTRYPOINT`.

Example Uso de Docker para compilar a través de Gradle Docker Image

```
docker run --rm -v /PATH/TO/SCOREKEEP_REPO/home/gradle/project -w /home/gradle/project
 gradle:4.3 gradle build
```

Example ENTRYPOINT de Dockerfile

```
ENTRYPOINT [ "sh", "-c", "java -Dserver.port=5000 -jar scorekeep-api-1.0.0.jar" ]
```

El archivo `build.gradle` descarga todos los submódulos del SDK de Maven durante la compilación declarándolos como dependencias.

Example build.gradle: dependencias

```
...
dependencies {
    compile("org.springframework.boot:spring-boot-starter-web")
    testCompile('org.springframework.boot:spring-boot-starter-test')
    compile('com.amazonaws:aws-java-sdk-dynamodb')
    compile("com.amazonaws:aws-xray-recorder-sdk-core")
    compile("com.amazonaws:aws-xray-recorder-sdk-aws-sdk")
    compile("com.amazonaws:aws-xray-recorder-sdk-aws-sdk-instrumentor")
    ...
```

```
}
dependencyManagement {
    imports {
        mavenBom("com.amazonaws:aws-java-sdk-bom:1.11.67")
        mavenBom("com.amazonaws:aws-xray-recorder-sdk-bom:2.11.0")
    }
}
```

Los submódulos core, AWS SDK y AWS SDK Instrumentor son todo lo que se necesita para instrumentar automáticamente cualquier llamada posterior realizada con el SDK. AWS

Para retransmitir datos de segmentos sin procesar a la API de X-Ray, el daemon de X-Ray debe escuchar el tráfico en el puerto UDP 2000. Para ello, la aplicación ejecuta el daemon de X-Ray en un contenedor que se implementa junto con la aplicación Scorekeep en ECS como contenedor asociado. Consulte el tema Daemon de X-Ray para obtener más información.

Example Definición del contenedor del daemon de X-Ray en una definición de tarea de ECS

```
...
Resources:
  ScorekeepTaskDefinition:
    Type: AWS::ECS::TaskDefinition
    Properties:
      ContainerDefinitions:
      ...

      - Cpu: '256'
        Essential: true
        Image: amazon/aws-xray-daemon
        MemoryReservation: '128'
        Name: xray-daemon
        PortMappings:
          - ContainerPort: '2000'
            HostPort: '2000'
            Protocol: udp
      ...
```

El SDK de X-Ray proporciona una clase denominada `AWSXRay` que proporciona una grabadora global, un `TracingHandler` que se puede utilizar para instrumentar el código. Puede configurar la grabadora global para que personalice el `AWSXRayServletFilter` que crea los segmentos para las llamadas HTTP entrantes. La muestra incluye un bloque estático en la clase `WebConfig` que configura la grabadora global con complementos y reglas de muestreo.

Example src/main/java/scorekeep/ .javaWebConfig: grabadora

```
import com.amazonaws.xray.AWSXRay;
import com.amazonaws.xray.AWSXRayRecorderBuilder;
import com.amazonaws.xray.javax.servlet.AWSXRayServletFilter;
import com.amazonaws.xray.plugins.ECSPlugin;
import com.amazonaws.xray.plugins.EC2Plugin;
import com.amazonaws.xray.strategy.sampling.LocalizedSamplingStrategy;
...

@Configuration
public class WebConfig {
  ...

  static {
    AWSXRayRecorderBuilder builder = AWSXRayRecorderBuilder.standard().withPlugin(new
 ECSPlugin()).withPlugin(new EC2Plugin());

    URL ruleFile = WebConfig.class.getResource("/sampling-rules.json");
    builder.withSamplingStrategy(new LocalizedSamplingStrategy(ruleFile));

    AWSXRay.setGlobalRecorder(builder.build());
    ...

  }
}
```

En este ejemplo se utiliza el compilador para cargar las reglas de muestreo desde un archivo denominado `sampling-rules.json`. Las reglas de muestreo determinan la velocidad a la que el SDK registra los segmentos de las solicitudes entrantes.

Example src/main/java/resources/sampling-rules.json

```
{
  "version": 1,
  "rules": [
    {
      "description": "Resource creation.",
      "service_name": "*",
      "http_method": "POST",
      "url_path": "/api/*",
      "fixed_target": 1,
      "rate": 1.0
```

```
    },
    {
      "description": "Session polling.",
      "service_name": "*",
      "http_method": "GET",
      "url_path": "/api/session/*",
      "fixed_target": 0,
      "rate": 0.05
    },
    {
      "description": "Game polling.",
      "service_name": "*",
      "http_method": "GET",
      "url_path": "/api/game/*/*",
      "fixed_target": 0,
      "rate": 0.05
    },
    {
      "description": "State polling.",
      "service_name": "*",
      "http_method": "GET",
      "url_path": "/api/state/*/*/*",
      "fixed_target": 0,
      "rate": 0.05
    }
  ],
  "default": {
    "fixed_target": 1,
    "rate": 0.1
  }
}
```

El archivo de reglas de muestreo define cuatro reglas de muestreo personalizadas y la regla predeterminada. Para cada solicitud de entrada, el SDK evalúa las reglas personalizadas en el orden en que están definidas. El SDK aplica la primera regla que coincide con el método, la ruta y el nombre de servicio de la solicitud. Para Scorekeep, la primera regla captura todas las solicitudes POST (llamadas de creación de recursos) aplicando un objetivo fijo de una solicitud por segundo y una tasa del 1,0, es decir, el 100 % de las solicitudes después de cumplir el objetivo fijo.

Las otras tres reglas personalizadas aplican una tasa del 5 % sin objetivo fijo a las lecturas de sesiones, juegos y estado (solicitudes GET). De este modo se reduce al mínimo el número de rastros de las llamadas periódicas que el front-end realiza automáticamente cada pocos segundos para

asegurarse de que el contenido está actualizado. Para el resto de solicitudes, el archivo define una velocidad predeterminada de una solicitud por segundo y una tasa del 10 %.

La aplicación de ejemplo también muestra cómo usar funciones avanzadas, como la instrumentación manual de clientes SDK, la creación de subsegmentos adicionales y llamadas HTTP salientes. Para obtener más información, consulte AWS X-Ray ejemplo de aplicación.

Opcional: política de privilegios mínimos

Los contenedores ECS de Scorekeep acceden a los recursos mediante políticas de acceso total, como `AmazonSNSFullAccess` y `AmazonDynamoDBFullAccess`. El uso de políticas de acceso total no es la mejor práctica para las aplicaciones de producción. En el siguiente ejemplo se actualiza la política de IAM de DynamoDB para mejorar la seguridad de la aplicación. Para obtener más información sobre las mejores prácticas de seguridad en las políticas de IAM, consulte Administración de identidad y acceso para AWS X-Ray.

Example Definición de ECS de la plantilla cf-resources.yaml TaskRole

```
ECSTaskRole:
    Type: AWS::IAM::Role
    Properties:
      AssumeRolePolicyDocument:
        Version: "2012-10-17"
        Statement:
          -
            Effect: "Allow"
            Principal:
              Service:
                - "ecs-tasks.amazonaws.com"
            Action:
              - "sts:AssumeRole"
      ManagedPolicyArns:
        - "arn:aws:iam::aws:policy/AmazonDynamoDBFullAccess"
        - "arn:aws:iam::aws:policy/AmazonSNSFullAccess"
        - "arn:aws:iam::aws:policy/AWSXrayFullAccess"
      RoleName: "scorekeepRole"
```

Para actualizar las políticas, primero identifique los ARN de sus recursos de DynamoDB. A continuación, utilice los ARN en una política de IAM personalizada. Por último, aplique esa política al perfil de instancia.

Para identificar el ARN de su recurso de DynamoDB:

1. Abra la consola de DynamoDB.
2. En la barra de navegación izquierda, elija Tablas.
3. Elija cualquiera de las opciones `scorekeep-*` para mostrar la página de detalles de la tabla.
4. En la pestaña Descripción general, seleccione Información adicional para expandir la sección y ver el nombre de recurso de Amazon (ARN). Copie este valor.
5. Inserte el ARN en la siguiente política de IAM y sustituya los valores `AWS_REGION` y `AWS_ACCOUNT_ID` por su región e ID de cuenta específicos. Esta nueva política solo permite las acciones especificadas, en lugar de la política `AmazonDynamoDBFullAccess`, que permite cualquier acción.

   Example

   ```
   {
       "Version": "2012-10-17",
       "Statement": [
           {
               "Sid": "ScorekeepDynamoDB",
               "Effect": "Allow",
               "Action": [
                   "dynamodb:PutItem",
                   "dynamodb:UpdateItem",
                   "dynamodb:DeleteItem",
                   "dynamodb:GetItem",
                   "dynamodb:Scan",
                   "dynamodb:Query"
               ],
               "Resource": "arn:aws:dynamodb:<AWS_REGION>:<AWS_ACCOUNT_ID>:table/
   scorekeep-*"
           }
       ]
   }
   ```

   Las tablas que crea la aplicación siguen una convención de nomenclatura coherente. Puede usar el formato `scorekeep-*` para indicar todas las tablas de Scorekeep.

Cambio de la política de IAM

1. Abra el rol de tarea de Scorekeep (ScorekeepRole) desde la consola de IAM.
2. Elija la casilla de verificación situada junto a la política `AmazonDynamoDBFullAccess` y, a continuación, elija Eliminar para eliminar esta política.
3. Seleccione Añadir permisos, a continuación, Adjuntar políticas y, por último, Crear política.
4. Elija la pestaña JSON y pegue la política que acaba de crear.
5. Elija Siguiente: Etiquetas en la parte inferior de la página.
6. Elija Siguiente: Revisar en la parte inferior de la página.
7. En Nombre, escriba un nombre para la política.
8. Elija Crear política en la parte inferior de la página.
9. Adjunte la política que acaba de crear al rol `scorekeepRole`. Puede que la política adjunta tarde unos minutos en aplicarse.

Si ha adjuntado la nueva política al `scorekeepRole` rol, debe separarla antes de eliminar la CloudFormation pila, ya que esta política adjunta impedirá que se elimine la pila. La política se puede separar automáticamente eliminándola.

Eliminación de su política de IAM personalizada

1. Abra la consola de IAM.
2. Elija Políticas en la barra de navegación izquierda.
3. Busque el nombre de la política personalizada que creó anteriormente en esta sección y elija el botón de opción situado junto al nombre de la política para resaltarlo.
4. Abra la lista desplegable Acciones y, a continuación, elija Eliminar.
5. Escriba el nombre de la política personalizada y, a continuación, elija Eliminar para confirmar la eliminación. Esto separará automáticamente la política del rol `scorekeepRole`.

Limpieza

Siga estos pasos para eliminar los recursos de la aplicación Scorekeep:

> **Note**
>
> Si creó y adjuntó políticas personalizadas mediante la sección anterior de este tutorial, debe eliminar la política de la pila `scorekeepRole` antes de eliminar la CloudFormation pila.

AWS Management Console

Elimine la aplicación de muestra mediante el AWS Management Console

1. Abra la consola de CloudFormation.
2. Seleccione el botón de opción situado junto al nombre de pila `scorekeep` en la lista y, a continuación, seleccione Eliminar.
3. La CloudFormation pila se está borrando ahora. El estado de la pila será `DELETE_IN_PROGRESS` de unos minutos hasta que se eliminen todos los recursos. El estado se actualizará periódicamente, o el usuario puede actualizar la página.

AWS CLI

Elimine la aplicación de muestra mediante el AWS CLI

1. Introduzca el siguiente AWS CLI comando para eliminar la CloudFormation pila:

```
aws cloudformation delete-stack --stack-name scorekeep
```

2. Espere hasta que la CloudFormation pila deje de existir, lo que tardará unos cinco minutos. Usa el siguiente AWS CLI comando para comprobar el estado:

```
aws cloudformation describe-stacks --stack-name scorekeep --query
 "Stacks[0].StackStatus"
```

Siguientes pasos

Obtenga más información sobre X-Ray en el próximo capítulo: AWS X-Ray conceptos.

Para instrumentar su propia aplicación, obtenga más información sobre el SDK de X-Ray para Java o sobre otros SDK de X-Ray:

- SDK de X-Ray para Java: AWS X-Ray SDK para Java
- SDK de X-Ray para Node.js: AWS SDK de X-Ray para Node.js
- SDK de X-Ray para .NET: AWS X-Ray SDK para.NET

Para ejecutar el daemon X-Ray de forma local o activada AWS, consulteAWS X-Ray demonio.

Para contribuir al ejemplo de la aplicación GitHub, consulte eb-java-scorekeep.

Instrumentación AWS manual de los clientes del SDK

El X-Ray SDK para Java instrumenta automáticamente todos los clientes del AWS SDK al incluir el submódulo AWS SDK Instrumentor en las dependencias de compilación.

Puede deshabilitar la instrumentación de clientes automática eliminando el submódulo Instrumentor. Esto le permite instrumentar algunos clientes manualmente a la vez que se pasan otros por alto, o utilizar diferentes controladores de rastreo en clientes distintos.

Para ilustrar la compatibilidad con la instrumentación de clientes de AWS SDK específicos, la aplicación pasa un controlador de rastreo `AmazonDynamoDBClientBuilder` como controlador de solicitudes en el modelo de usuario, juego y sesión. Esta modificación del código indica al SDK que instrumente todas las llamadas a DynamoDB con esos clientes.

Example **`src/main/java/scorekeep/SessionModel.java`**:instrumentación manual de clientes del SDK de AWS

```
import com.amazonaws.xray.AWSXRay;
import com.amazonaws.xray.handlers.TracingHandler;

public class SessionModel {
  private AmazonDynamoDB client = AmazonDynamoDBClientBuilder.standard()
        .withRegion(Constants.REGION)
        .withRequestHandlers(new TracingHandler(AWSXRay.getGlobalRecorder()))
        .build();
  private DynamoDBMapper mapper = new DynamoDBMapper(client);
```

Si eliminas el submódulo AWS SDK Instrumentor de las dependencias del proyecto, solo los clientes del SDK AWS instrumentados manualmente aparecen en el mapa de seguimiento.

Creación de subsegmentos adicionales

En la clase de modelo del usuario, la aplicación crea de forma manual subsegmentos para agrupar todas las llamadas posteriores que se realizaron dentro de la función `saveUser` y agrega metadatos.

Example **src/main/java/scorekeep/UserModel.java**: subsegmentos personalizados

```
import com.amazonaws.xray.AWSXRay;
import com.amazonaws.xray.entities.Subsegment;
...
    public void saveUser(User user) {
    // Wrap in subsegment
    Subsegment subsegment = AWSXRay.beginSubsegment("## UserModel.saveUser");
    try {
      mapper.save(user);
    } catch (Exception e) {
      subsegment.addException(e);
      throw e;
    } finally {
      AWSXRay.endSubsegment();
    }
  }
```

Registro de anotaciones, metadatos e identificadores de usuario

En la clase de modelo de juego, la aplicación registra objetos Game en un bloque de metadatos cada vez que se guarda un juego en DynamoDB. De forma independiente, la aplicación registra los identificadores de juego en anotaciones para su uso con expresiones de filtro.

Example **src/main/java/scorekeep/GameModel.java**: anotaciones y metadatos

```
import com.amazonaws.xray.AWSXRay;
import com.amazonaws.xray.entities.Segment;
import com.amazonaws.xray.entities.Subsegment;
...
  public void saveGame(Game game) throws SessionNotFoundException {
    // wrap in subsegment
    Subsegment subsegment = AWSXRay.beginSubsegment("## GameModel.saveGame");
    try {
      // check session
      String sessionId = game.getSession();
```

```
      if (sessionModel.loadSession(sessionId) == null ) {
        throw new SessionNotFoundException(sessionId);
      }
      Segment segment = AWSXRay.getCurrentSegment();
      subsegment.putMetadata("resources", "game", game);
      segment.putAnnotation("gameid", game.getId());
      mapper.save(game);
    } catch (Exception e) {
      subsegment.addException(e);
      throw e;
    } finally {
      AWSXRay.endSubsegment();
    }
  }
```

En el controlador de movimiento, la aplicación registra los identificadores de usuario con `setUser`. Los identificadores de usuario se registran en un campo aparte en segmentos y se indexan para su uso con la búsqueda.

Example src/main/java/scorekeep/ .java MoveController: ID de usuario

```
import com.amazonaws.xray.AWSXRay;
...
  @RequestMapping(value="/{userId}", method=RequestMethod.POST)
  public Move newMove(@PathVariable String sessionId, @PathVariable String
 gameId, @PathVariable String userId, @RequestBody String move) throws
 SessionNotFoundException, GameNotFoundException, StateNotFoundException,
 RulesException {
    AWSXRay.getCurrentSegment().setUser(userId);
    return moveFactory.newMove(sessionId, gameId, userId, move);
  }
```

Instrumentación de llamadas a HTTP salientes

La clase del generador del usuario muestra cómo la aplicación usa el SDK de X-Ray para la versión de Java de `HTTPClientBuilder` con el fin de instrumentar las llamadas HTTP salientes.

Example **src/main/java/scorekeep/UserFactory.java**: instrumentación de HTTPClient

```
import com.amazonaws.xray.proxies.apache.http.HttpClientBuilder;
```

```
  public String randomName() throws IOException {
    CloseableHttpClient httpclient = HttpClientBuilder.create().build();
    HttpGet httpGet = new HttpGet("http://uinames.com/api/");
    CloseableHttpResponse response = httpclient.execute(httpGet);
    try {
      HttpEntity entity = response.getEntity();
      InputStream inputStream = entity.getContent();
      ObjectMapper mapper = new ObjectMapper();
      Map<String, String> jsonMap = mapper.readValue(inputStream, Map.class);
      String name = jsonMap.get("name");
      EntityUtils.consume(entity);
      return name;
    } finally {
      response.close();
    }
  }
```

Si actualmente utiliza `org.apache.http.impl.client.HttpClientBuilder`, puede simplemente intercambiar la instrucción de importación para esa clase por una para `com.amazonaws.xray.proxies.apache.http.HttpClientBuilder`.

Instrumentación de llamadas a una base de datos PostgreSQL

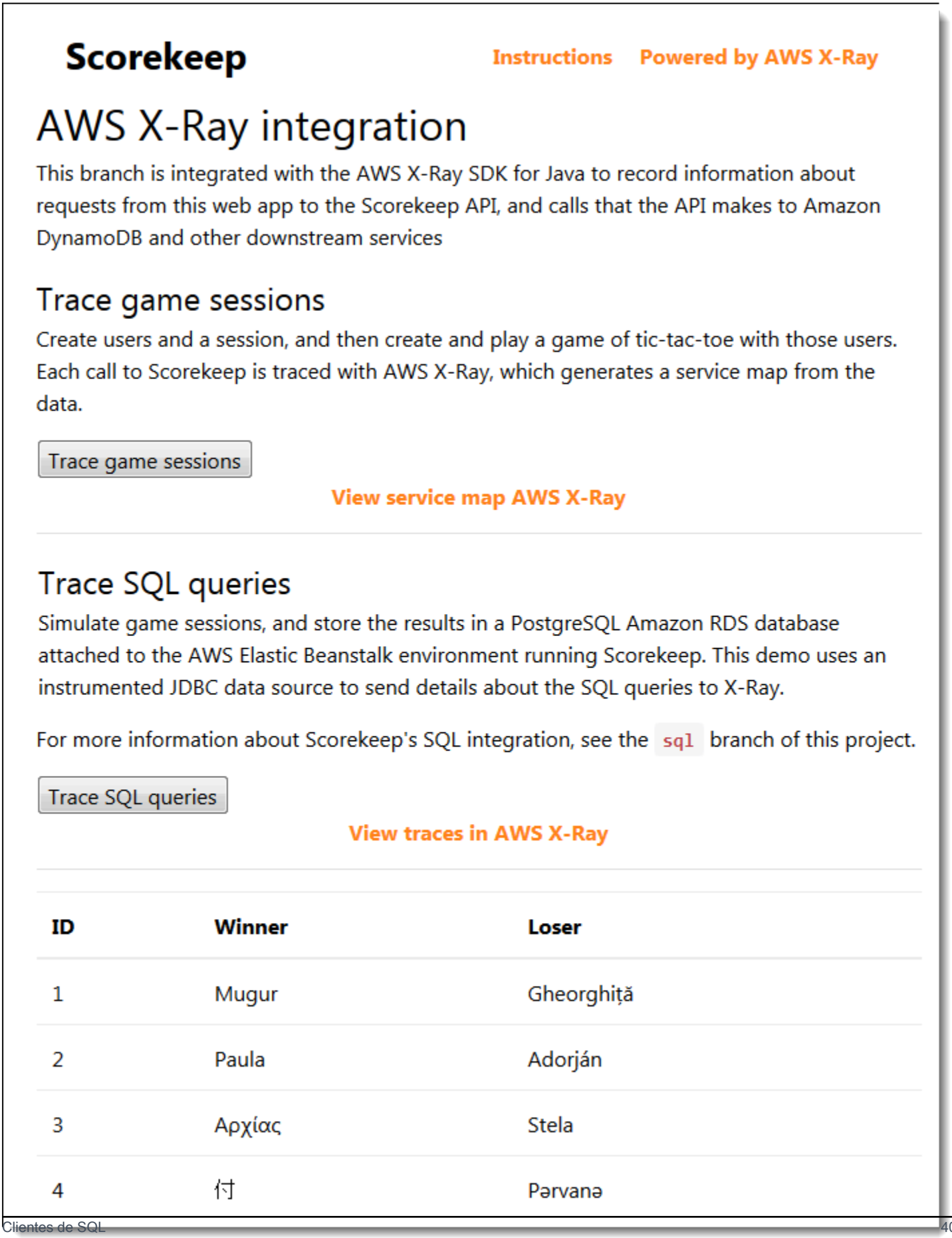
El archivo `application-pgsql.properties` añade el interceptor de rastreo PostgreSQL de X-Ray al origen de datos creado en `RdsWebConfig.java`.

Example **`application-pgsql.properties`**: instrumentación de una base de datos PostgreSQL

```
spring.datasource.continue-on-error=true
spring.jpa.show-sql=false
spring.jpa.hibernate.ddl-auto=create-drop
spring.datasource.jdbc-interceptors=com.amazonaws.xray.sql.postgres.TracingInterceptor
spring.jpa.database-platform=org.hibernate.dialect.PostgreSQL94Dialect
```

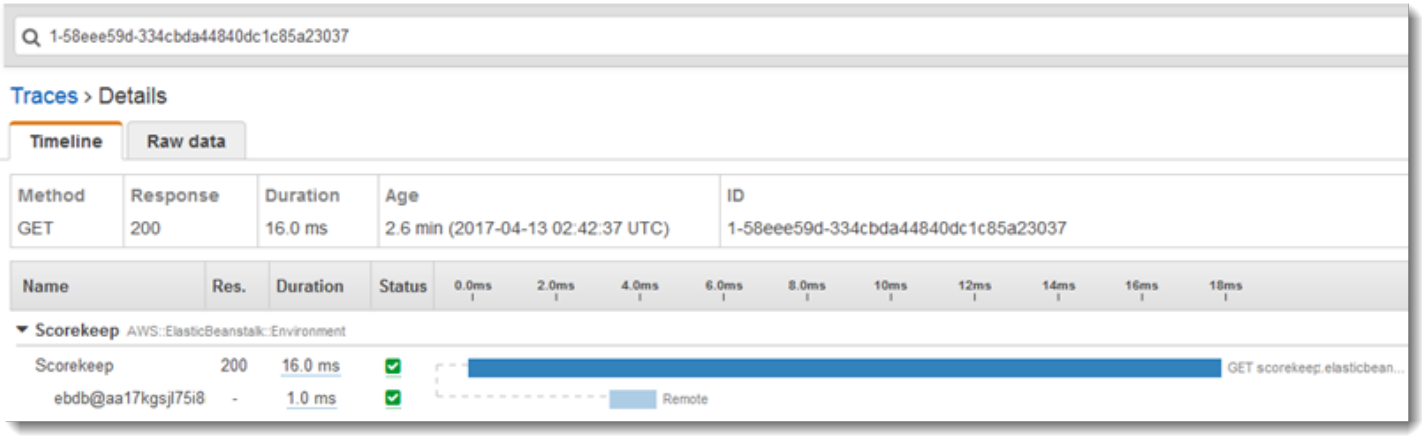
> **Note**
>
> Consulte Configuración de bases de datos con Elastic Beanstalk en la Guía para desarrolladores de AWS Elastic Beanstalk para obtener más información acerca de cómo añadir una base de datos de PostgreSQL al entorno de aplicaciones.

La página de demostración de X-Ray en la ramificación `xray` incluye una demostración que utiliza el origen de datos instrumentado para generar rastros que muestran información sobre las consultas SQL que se generan. Vaya a la ruta `/#/xray` de la aplicación en ejecución o elija Powered by AWS X-Ray en la barra de navegación para ver la página de demostración.


Scorekeep
Instructions
Powered by AWS X-Ray
AWS X-Ray integration
This branch is integrated with the AWS X-Ray SDK for Java to record information about requests from this web app to the Scorekeep API, and calls that the API makes to Amazon DynamoDB and other downstream services
Trace game sessions
Create users and a session, and then create and play a game of tic-tac-toe with those users. Each call to Scorekeep is traced with AWS X-Ray, which generates a service map from the data.
Trace game sessions
View service map AWS X-Ray
Trace SQL queries
Simulate game sessions, and store the results in a PostgreSQL Amazon RDS database attached to the AWS Elastic Beanstalk environment running Scorekeep. This demo uses an instrumented JDBC data source to send details about the SQL queries to X-Ray.
For more information about Scorekeep's SQL integration, see the sql branch of this project.
Trace SQL queries
View traces in AWS X-Ray
ID
Winner
Loser
1
Mugur
Gheorghiță
2
Paula
Adorján
3
Αρχίας
Stela
4
付
Pərvanə

Elija Trace SQL queries (Rastrear consultas SQL) para simular las sesiones de juego y almacenar los resultados en la base de datos asociada. A continuación, elija Ver rastreos en AWS X-Ray) para ver una lista filtrada de los rastreos que se incluyen en la ruta `/api/history` de la API.

Elija uno de los rastros de la lista para ver la escala de tiempo, incluida la consulta SQL.



Funciones de instrumentación AWS Lambda

Scorekeep utiliza dos AWS Lambda funciones. La primera es una función de Node.js de la ramificación `lambda` que genera nombres aleatorios para nuevos usuarios. Cuando un usuario crea una sesión sin introducir ningún nombre, la aplicación llama a una función denominada `random-name` con el AWS SDK for Java. El SDK de X-Ray para Java registra la información sobre la llamada a Lambda en un subsegmento, como cualquier otra llamada realizada con un cliente de SDK AWS instrumentado.

> **Note**
>
> La ejecución de la función de Lambda `random-name` requiere la creación de recursos adicionales fuera del entorno de Elastic Beanstalk. Consulte el archivo readme para obtener más información e instrucciones: AWS Lambda Integration.

La segunda función, `scorekeep-worker`, es una función de Python que se ejecuta de forma independiente de la API de Scorekeep. Cuando un juego termina, la API escribe el ID de sesión y el ID de juego en una cola de SQS. La función de proceso de trabajo lee los elementos de la cola y llama a la API de Scorekeep con el fin de construir registros completos de cada sesión de juego para su almacenamiento en Amazon S3.

Scorekeep incluye AWS CloudFormation plantillas y scripts para crear ambas funciones. Dado que necesita agrupar el SDK de X-Ray con el código de la función, las plantillas crean las funciones sin ningún tipo de código. Al implementar Scorekeep, un archivo de configuración incluido en la carpeta `.ebextensions` crea un paquete de origen que incluye el SDK y actualiza el código de la función y la configuración con el AWS Command Line Interface.

Funciones

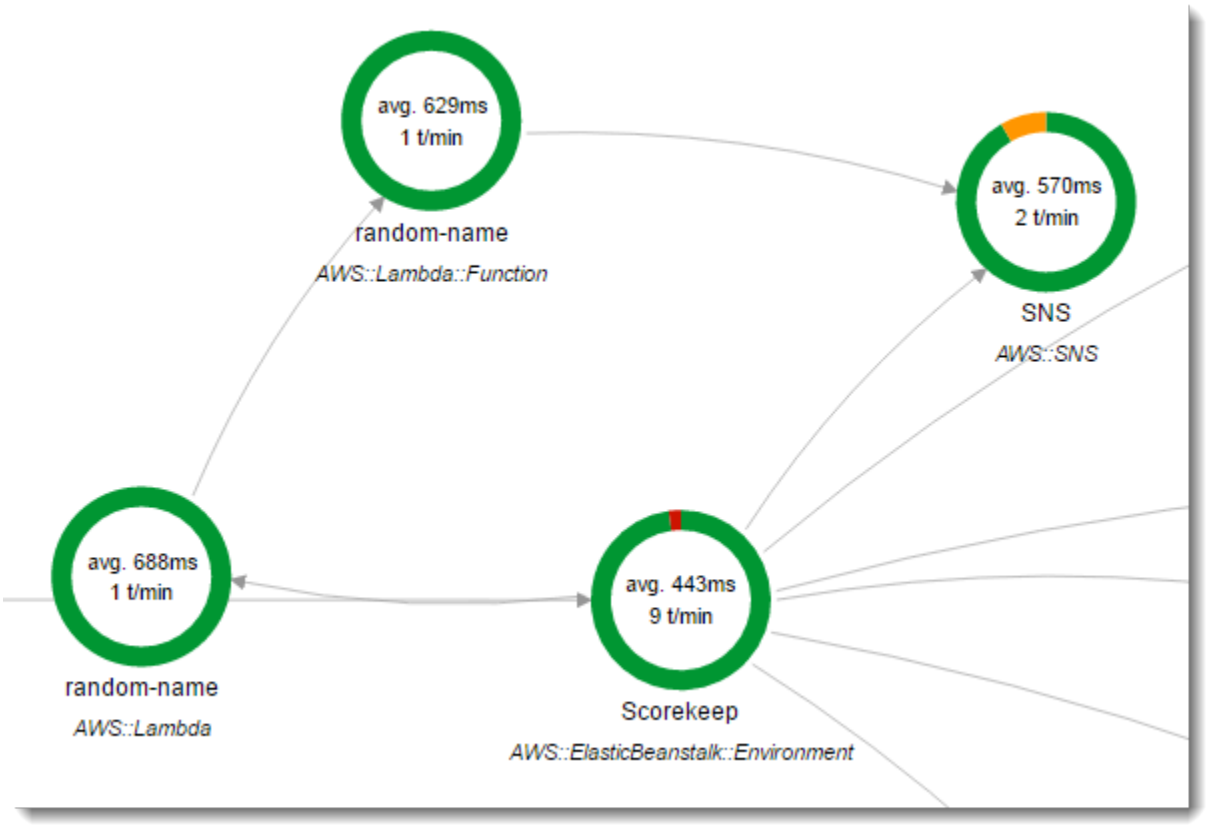
- Nombre aleatorio
- Entorno de trabajo

Nombre aleatorio

Scorekeep llama a la función de nombre aleatorio cuando un usuario comienza una sesión de juego sin iniciar sesión o especificar un nombre de usuario. Cuando Lambda procesa la llamada a `random-name`, lee el encabezado de rastreo, que contiene el ID de rastro y la decisión de muestreo escrita por el SDK de X-Ray para Java.

Para cada solicitud muestreada, Lambda ejecuta el daemon de X-Ray y escribe dos segmentos. El primer segmento registra información sobre la llamada a Lambda que invoca la función. Este segmento contiene la misma información que el subsegmento registrado por Scorekeep, pero desde el punto de vista de Lambda. El segundo segmento representa el trabajo que hace la función.

Lambda pasa el segmento de la función al SDK de X-Ray a través del contexto de la función. Cuando instrumente una función de Lambda, no utilice el SDK con el fin de crear un segmento para las solicitudes entrantes. Lambda proporciona el segmento y usted debe utilizar el SDK para instrumentar clientes y escribir subsegmentos.



La función `random-name` se implementa en Node.js. Utiliza el SDK de Node.js para JavaScript enviar notificaciones con Amazon SNS y el SDK de X-Ray para Node.js para instrumentar el cliente del AWS SDK. Para escribir anotaciones, la función crea un subsegmento personalizado con `AWSXRay.captureFunc` y escribe anotaciones en la función instrumentada. En Lambda, no puede escribir anotaciones directamente en el segmento de la función, únicamente en un subsegmento que cree.

Example **`function/index.js`**: función Lambda random-name

```
var AWSXRay = require('aws-xray-sdk-core');
var AWS = AWSXRay.captureAWS(require('aws-sdk'));

AWS.config.update({region: process.env.AWS_REGION});
var Chance = require('chance');

var myFunction = function(event, context, callback) {
  var sns = new AWS.SNS();
  var chance = new Chance();
  var userid = event.userid;
  var name = chance.first();
```

```
  AWSXRay.captureFunc('annotations', function(subsegment){
    subsegment.addAnnotation('Name', name);
    subsegment.addAnnotation('UserID', event.userid);
  });

  // Notify
  var params = {
    Message: 'Created randon name "' + name + '"" for user "' + userid + '".',
    Subject: 'New user: ' + name,
    TopicArn: process.env.TOPIC_ARN
  };
  sns.publish(params, function(err, data) {
    if (err) {
      console.log(err, err.stack);
      callback(err);
    }
    else {
      console.log(data);
      callback(null, {"name": name});
    }
  });
};

exports.handler = myFunction;
```

Esta función se crea automáticamente al implementar la aplicación de ejemplo en Elastic Beanstalk. La ramificación `xray` incluye un script para crear una función de Lambda en blanco. Los archivos de configuración de la `.ebextensions` carpeta crean el paquete de funciones `npm install` durante la implementación y, a continuación, actualizan la función Lambda con la CLI AWS .

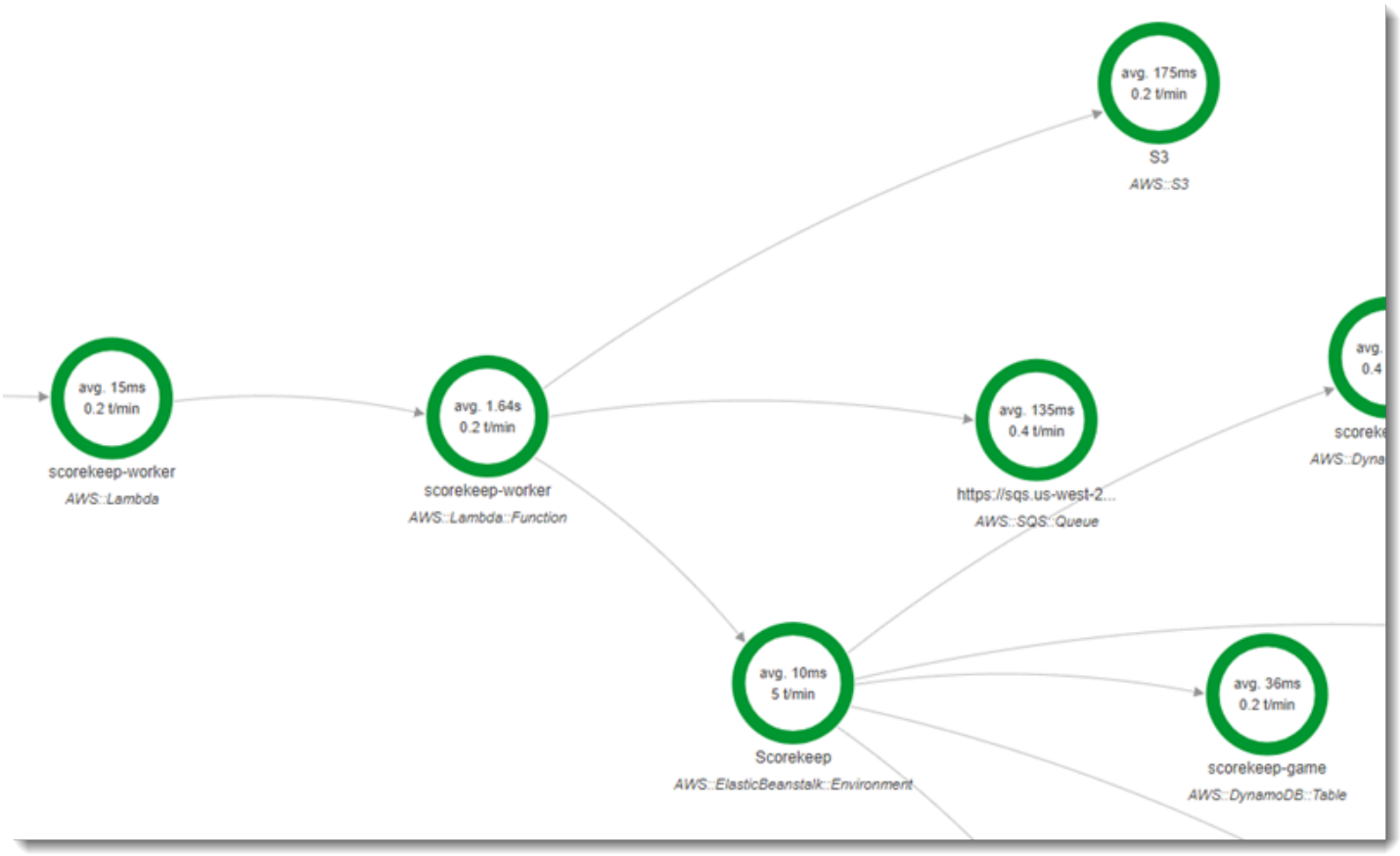
Entorno de trabajo

La función de trabajo instrumentada se proporciona en su propia ramificación, `xray-worker`, ya que no se puede ejecutar a menos que antes cree la función de trabajo y los recursos relacionados. Consulte el archivo readme de la ramificación para obtener instrucciones.

La función se activa mediante un paquete de CloudWatch eventos de Amazon Events cada 5 minutos. Cuando se ejecuta, la función extrae un elemento de una cola de Amazon SQS que administra Scorekeep. Cada mensaje contiene información sobre un juego terminado.

El trabajo extrae los documentos y el registro del juego de otras tablas a las que hace referencia el registro de juego. Por ejemplo, el registro del juego en DynamoDB incluye una lista de los movimientos que se han realizado durante el juego. La lista no contiene los movimientos en sí, sino los ID de los movimientos que están almacenados en una tabla distinta.

Las sesiones y los estados también se almacenan como referencias. Esto impide que las entradas de la tabla de juego sean demasiado grandes, pero requiere llamadas adicionales para obtener toda la información sobre el juego. El proceso de trabajo anula las referencias a todas estas entradas y construye un registro completo del juego como un único documento en Amazon S3. Cuando desee realizar el análisis de los datos, podrá ejecutar consultas en él directamente en Amazon S3 con Amazon Athena sin ejecutar migraciones de datos que realizan muchas lecturas para obtener los datos de DynamoDB.



La función de trabajo tiene habilitado el rastreo activo en su configuración en AWS Lambda. A diferencia de la función de nombres aleatorios, el trabajador no recibe una solicitud de una aplicación instrumentada, por lo que AWS Lambda no recibe un encabezado de seguimiento. Con el rastreo activo, Lambda crea el ID de rastro y toma decisiones de muestreo.

El SDK de X-Ray para Python está solo unas líneas en la parte superior de la función que importa el SDK y ejecuta su `patch_all` función para parchear los HTTClients AWS SDK for Python (Boto) y los HttpClients que utiliza para llamar a Amazon SQS y Amazon S3. Cuando el trabajo llama a la API de Scorekeep, el SDK añade el encabezado de rastreo a la solicitud para rastrear llamadas a través de la API.

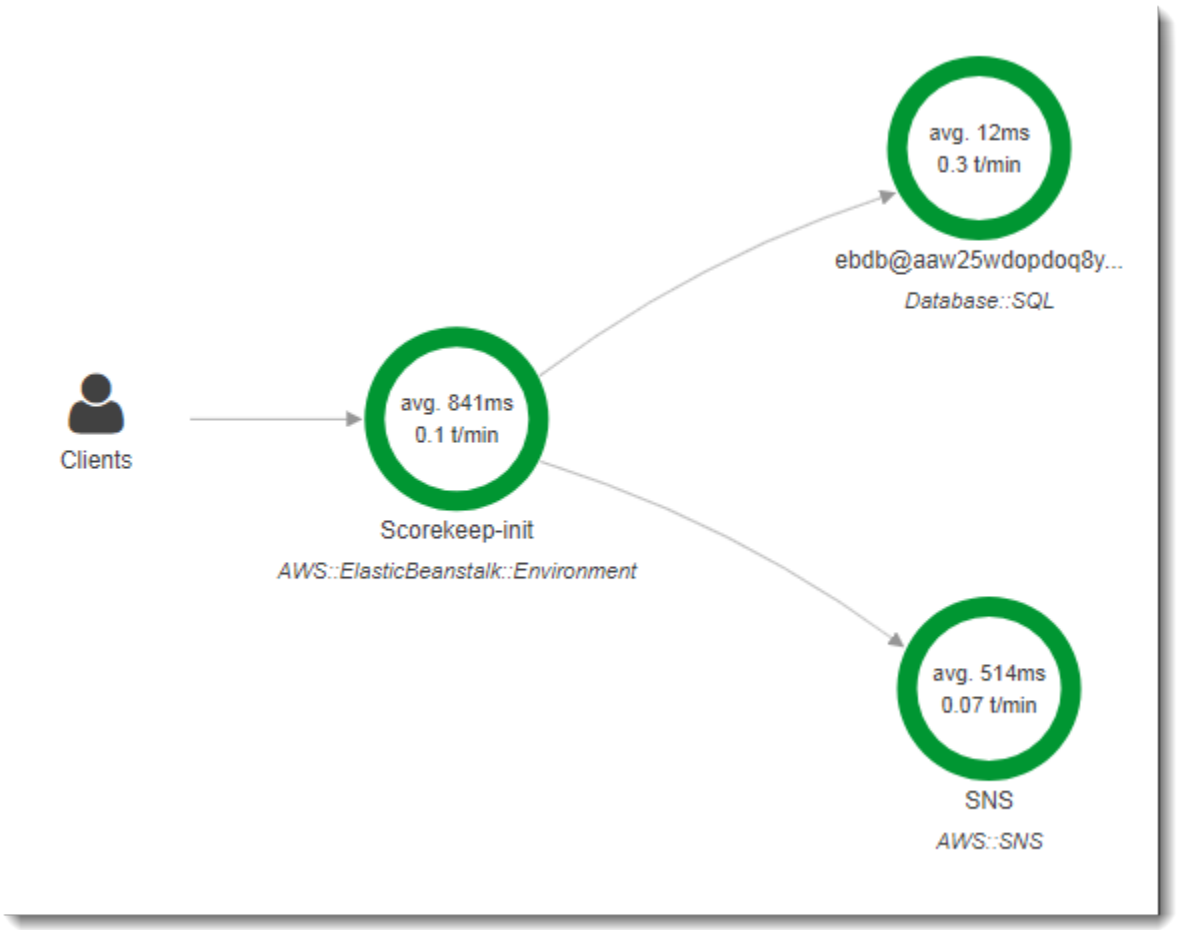
Example **`_lambda/scorekeep-worker/scorekeep-worker.py`**: función Lambda del proceso de trabajo

```
import os
import boto3
import json
import requests
import time
from aws_xray_sdk.core import xray_recorder
from aws_xray_sdk.core import patch_all

patch_all()
queue_url = os.environ['WORKER_QUEUE']

def lambda_handler(event, context):
    # Create SQS client
    sqs = boto3.client('sqs')
    s3client = boto3.client('s3')

    # Receive message from SQS queue
    response = sqs.receive_message(
        QueueUrl=queue_url,
        AttributeNames=[
            'SentTimestamp'
        ],
        MaxNumberOfMessages=1,
        MessageAttributeNames=[
            'All'
        ],
        VisibilityTimeout=0,
        WaitTimeSeconds=0
    )
   ...
```

Instrumentación de código de inicio

El SDK de X-Ray para Java crea automáticamente segmentos para solicitudes entrantes. Siempre que haya una solicitud en el ámbito, puede utilizar clientes instrumentados y registrar subsegmentos sin problema. Sin embargo, si intenta utilizar un cliente instrumentado en código de inicio, obtendrá una SegmentNotFoundException.

El código de inicio se ejecuta fuera del flujo de solicitud/respuesta estándar de una aplicación web, por lo que necesita crear segmentos manualmente para instrumentarlo. Scorekeep muestra la instrumentación de código de inicio en sus archivos `WebConfig`. Scorekeep llama a una base de datos SQL y Amazon SNS durante el startup.



La clase `WebConfig` predeterminada crea una suscripción de Amazon SNS para notificaciones. Para proporcionar un segmento para que el SDK de X-Ray escriba cuando se utiliza el cliente de Amazon SNS, Scorekeep llama a `beginSegment` y `endSegment` en la grabadora global.

Example **src/main/java/scorekeep/WebConfig.java**: cliente del SDK de AWS instrumentado en el código de inicio

```
AWSXRay.beginSegment("Scorekeep-init");
if ( System.getenv("NOTIFICATION_EMAIL") != null ){
  try { Sns.createSubscription(); }
  catch (Exception e ) {
    logger.warn("Failed to create subscription for email "+
 System.getenv("NOTIFICATION_EMAIL"));
  }
}
AWSXRay.endSegment();
```

En `RdsWebConfig`, que Scorekeep utiliza cuando hay una base de datos de Amazon RDS conectada, la configuración también crea un segmento para el cliente SQL que utiliza Hibernate cuando aplica el esquema de base de datos durante el startup.

Example **src/main/java/scorekeep/RdsWebConfig.java**: cliente de base de datos SQL instrumentado en código de inicio

```
@PostConstruct
public void schemaExport() {
  EntityManagerFactoryImpl entityManagerFactoryImpl = (EntityManagerFactoryImpl)
 localContainerEntityManagerFactoryBean.getNativeEntityManagerFactory();
  SessionFactoryImplementor sessionFactoryImplementor =
 entityManagerFactoryImpl.getSessionFactory();
  StandardServiceRegistry standardServiceRegistry =
 sessionFactoryImplementor.getSessionFactoryOptions().getServiceRegistry();
  MetadataSources metadataSources = new MetadataSources(new
 BootstrapServiceRegistryBuilder().build());
  metadataSources.addAnnotatedClass(GameHistory.class);
  MetadataImplementor metadataImplementor = (MetadataImplementor)
 metadataSources.buildMetadata(standardServiceRegistry);
  SchemaExport schemaExport = new SchemaExport(standardServiceRegistry,
 metadataImplementor);

  AWSXRay.beginSegment("Scorekeep-init");
  schemaExport.create(true, true);
  AWSXRay.endSegment();
}
```

`SchemaExport` se ejecuta de forma automática y utiliza un cliente SQL. Dado que el cliente está instrumentado, Scorekeep debe anular la implementación predeterminada y proporcionar un segmento para que lo utilice el SDK cuando se llama al cliente.

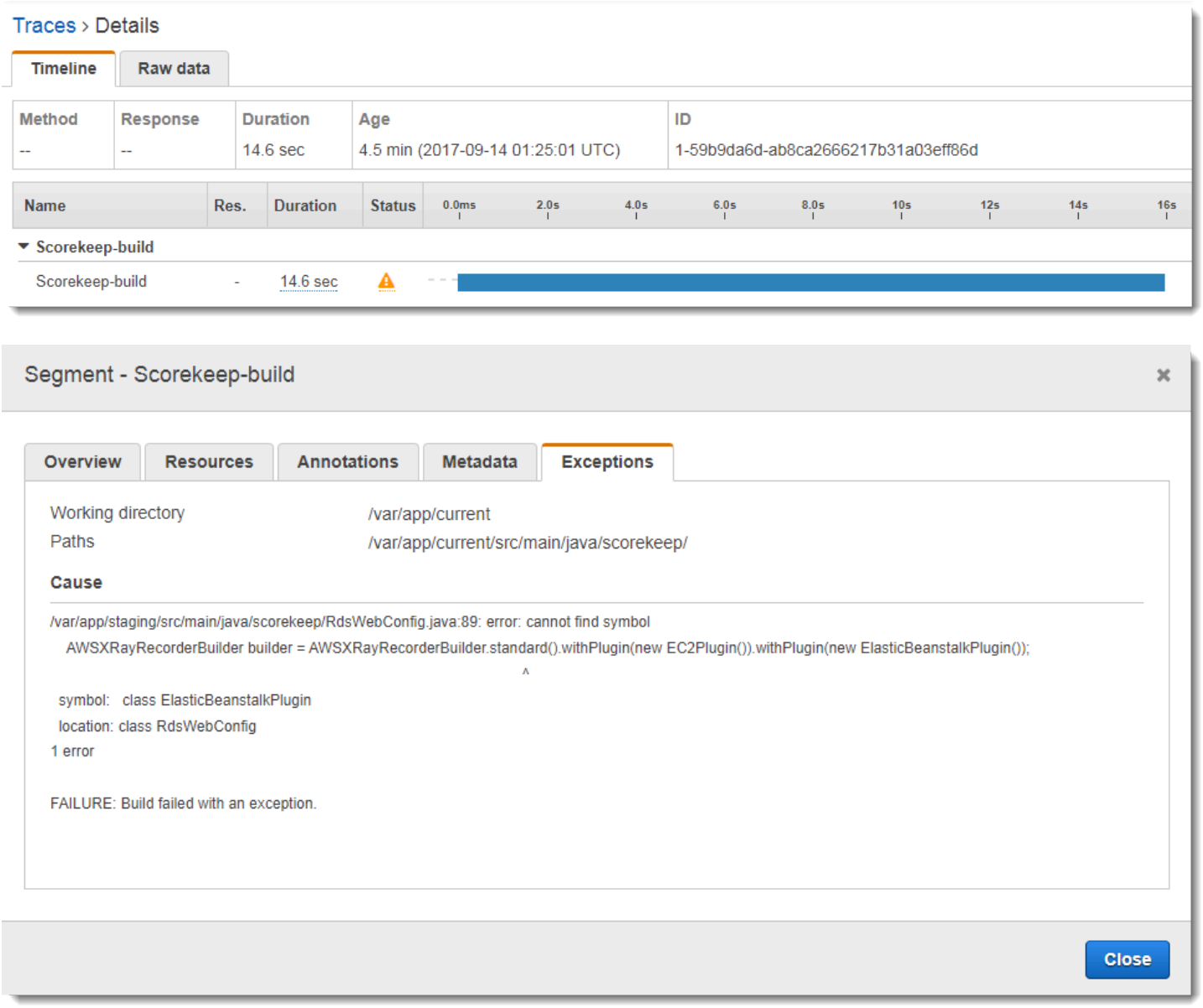
Instrumentación de scripts

También puede instrumentar código que no forme parte de su aplicación. Cuando el daemon de X-Ray se está ejecutando, transmitirá los segmentos que reciba a X-Ray, incluso si no los ha generado el SDK de X-Ray. Scorekeep utiliza sus propios scripts para instrumentar la compilación que compila la aplicación durante la implementación.

Example **`bin/build.sh`**: script de compilación instrumentado

```
SEGMENT=$(python bin/xray_start.py)
gradle build --quiet --stacktrace &> /var/log/gradle.log; GRADLE_RETURN=$?
if (( GRADLE_RETURN != 0 )); then
  echo "Gradle failed with exit status $GRADLE_RETURN" >&2
  python bin/xray_error.py "$SEGMENT" "$(cat /var/log/gradle.log)"
  exit 1
fi
python bin/xray_success.py "$SEGMENT"
```

`xray_start.py`, `xray_error.py` y `xray_success.py` son scripts de Python sencillos que construyen objetos de segmento, los convierten a documentos JSON y los envían al demonio sobre UDP. Si la compilación de Gradle falla, puedes encontrar el mensaje de error haciendo clic en el nodo scorekeep-build del mapa de rastreo de la consola X-Ray.



Instrumentación de un cliente de aplicación web

En la ramificación [`xray-cognito`], Scorekeep utiliza Amazon Cognito para permitir que los usuarios creen una cuenta e inicien sesión con ella para recuperar su información de usuario desde un grupo de usuarios de Amazon Cognito. Cuando un usuario inicia sesión, Scorekeep utiliza un grupo de identidades de Amazon Cognito para obtener credenciales AWS temporales para usarlas con. AWS SDK for JavaScript

El grupo de identidades está configurado para permitir a los usuarios que han iniciado sesión escribir datos de rastreos en AWS X-Ray. La aplicación web utiliza estas credenciales para registrar el ID

del usuario que ha iniciado sesión, la ruta del navegador y la vista del cliente de llamadas a la API Scorekeep.

La mayor parte del trabajo se realiza en una clase de servicio denominada `xray`. Este clase de servicio ofrece métodos para generar los identificadores requeridos, crear segmentos en curso, finalizar segmentos y enviar documentos de segmento a la API de X-Ray.

Example **public/xray.js**: registrar y cargar segmentos

```
...
  service.beginSegment = function() {
    var segment = {};
    var traceId = '1-' + service.getHexTime() + '-' + service.getHexId(24);

    var id = service.getHexId(16);
    var startTime = service.getEpochTime();

    segment.trace_id = traceId;
    segment.id = id;
    segment.start_time = startTime;
    segment.name = 'Scorekeep-client';
    segment.in_progress = true;
    segment.user =  sessionStorage['userid'];
    segment.http = {
      request: {
        url: window.location.href
      }
    };

    var documents = [];
    documents[0] = JSON.stringify(segment);
    service.putDocuments(documents);
    return segment;
  }

  service.endSegment = function(segment) {
    var endTime = service.getEpochTime();
    segment.end_time = endTime;
    segment.in_progress = false;
    var documents = [];
    documents[0] = JSON.stringify(segment);
    service.putDocuments(documents);
  }
```

```
  service.putDocuments = function(documents) {
    var xray = new AWS.XRay();
    var params = {
      TraceSegmentDocuments: documents
    };
    xray.putTraceSegments(params, function(err, data) {
      if (err) {
        console.log(err, err.stack);
      } else {
        console.log(data);
      }
    })
  }
```

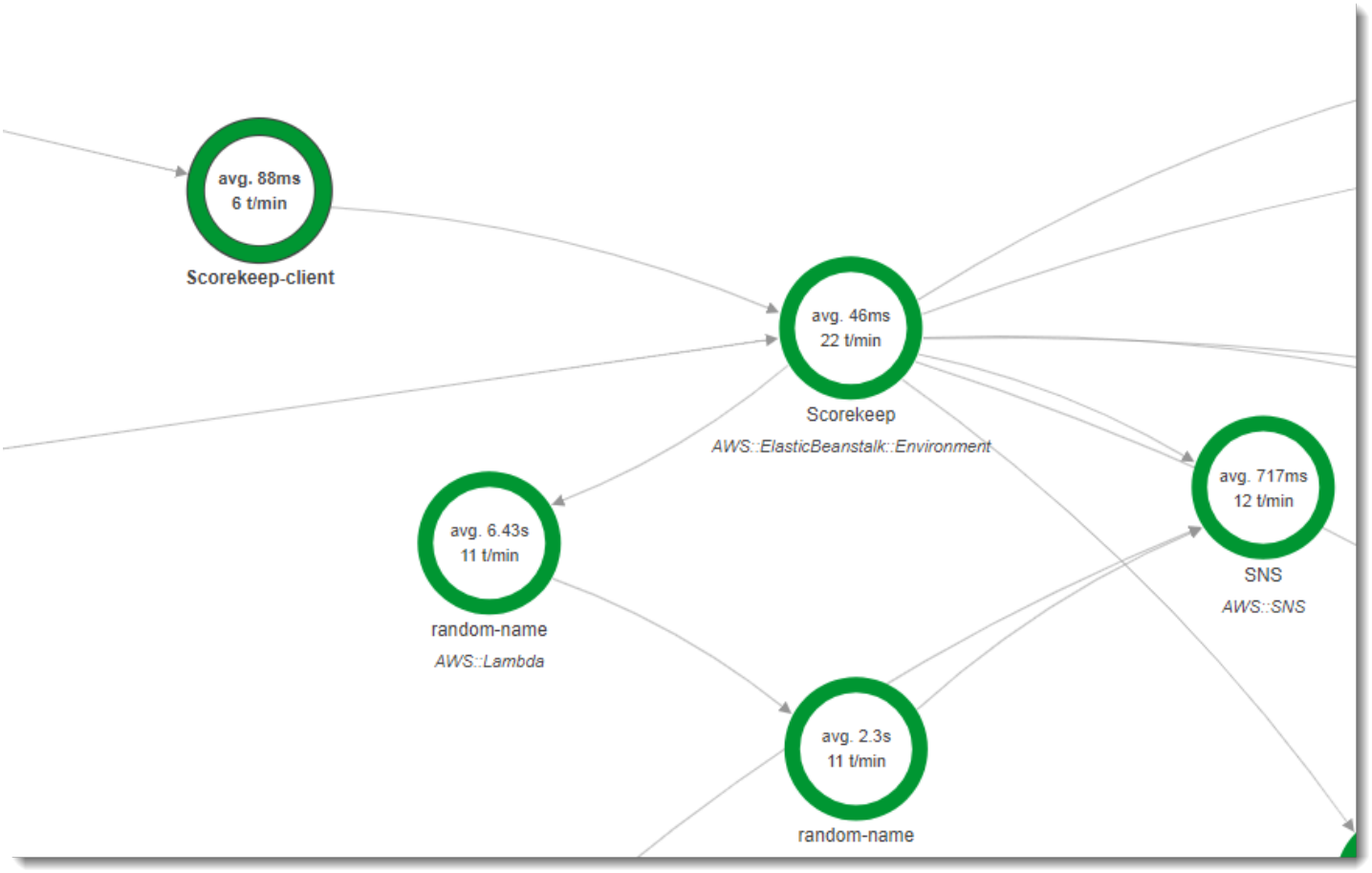
Estos métodos se llaman en el encabezado y funciones `transformResponse` en los servicios de recursos que la aplicación web utiliza para llamar a la API de Scorekeep. Para incluir el segmento de cliente en el mismo rastreo que el segmento que genera la API, la aplicación web debe incluir el ID de rastro y el ID de segmento en un encabezado de seguimiento (`X-Amzn-Trace-Id`) que el SDK de X-Ray puede leer. Cuando la aplicación Java instrumentada recibe una solicitud con este encabezado, el SDK de X-Ray para Java utiliza el mismo ID de rastro y hace que el segmento del cliente de la aplicación web sea el principal de su segmento.

Example **`public/app/services.js`**: registro de segmentos para llamadas de recursos de Angular y escritura de encabezados de rastreo

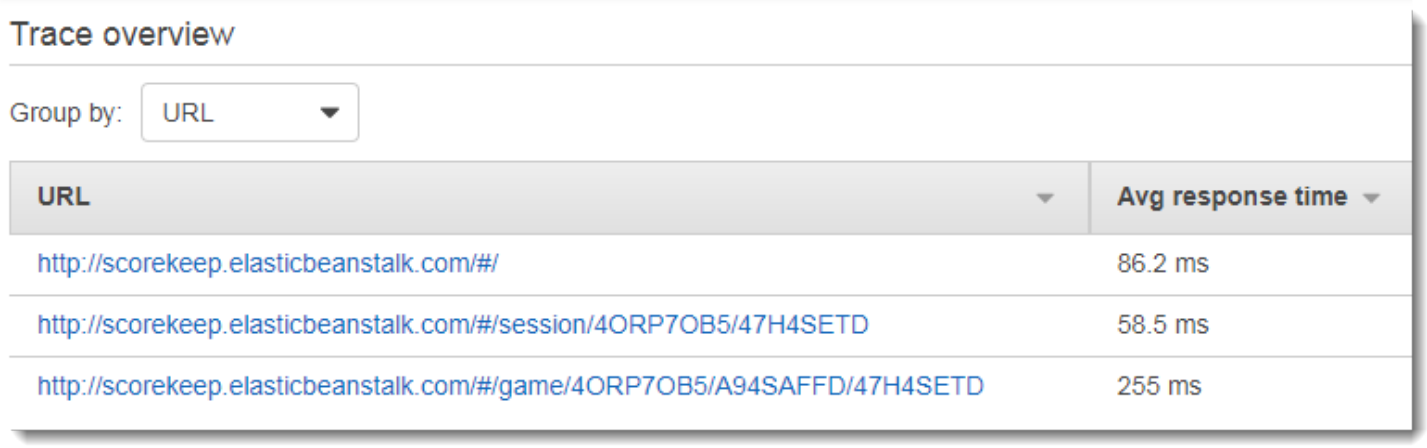
```
var module = angular.module('scorekeep');
module.factory('SessionService', function($resource, api, XRay) {
  return $resource(api + 'session/:id', { id: '@_id' }, {
    segment: {},
    get: {
      method: 'GET',
      headers: {
        'X-Amzn-Trace-Id': function(config) {
          segment = XRay.beginSegment();
          return XRay.getTraceHeader(segment);
        }
      },
      transformResponse: function(data) {
        XRay.endSegment(segment);
        return angular.fromJson(data);
      },
```

```
    },
...
```

El mapa de rastreo resultante incluye un nodo para el cliente de la aplicación web.



Los rastreos que incluyen segmentos desde la aplicación web muestran la dirección URL que el usuario ve en el navegador (rutas que empiezan por `/#/`). Sin la instrumentación de cliente, solo obtiene la dirección URL del recurso de la API que la aplicación web llama (rutas que empiezan por `/api/`).



Uso de clientes instrumentados en subprocesos de trabajo

Scorekeep utiliza un subproceso de trabajo para publicar una notificación en Amazon SNS cuando un usuario gana un juego. La publicación de la notificación tarda más tiempo que el resto de las operaciones de solicitud combinadas y no afecta al cliente o al usuario. Por lo tanto, la realización de la tarea de forma asíncrona es una buena manera de mejorar el tiempo de respuesta.

Sin embargo, el SDK de X-Ray para Java no sabe qué segmento estaba activo cuando se creó el subproceso. Por tanto, cuando se intenta utilizar el cliente AWS SDK for Java instrumentado dentro del subproceso, lanza una `SegmentNotFoundException`, bloqueando el subproceso.

Example Web-1.error.log

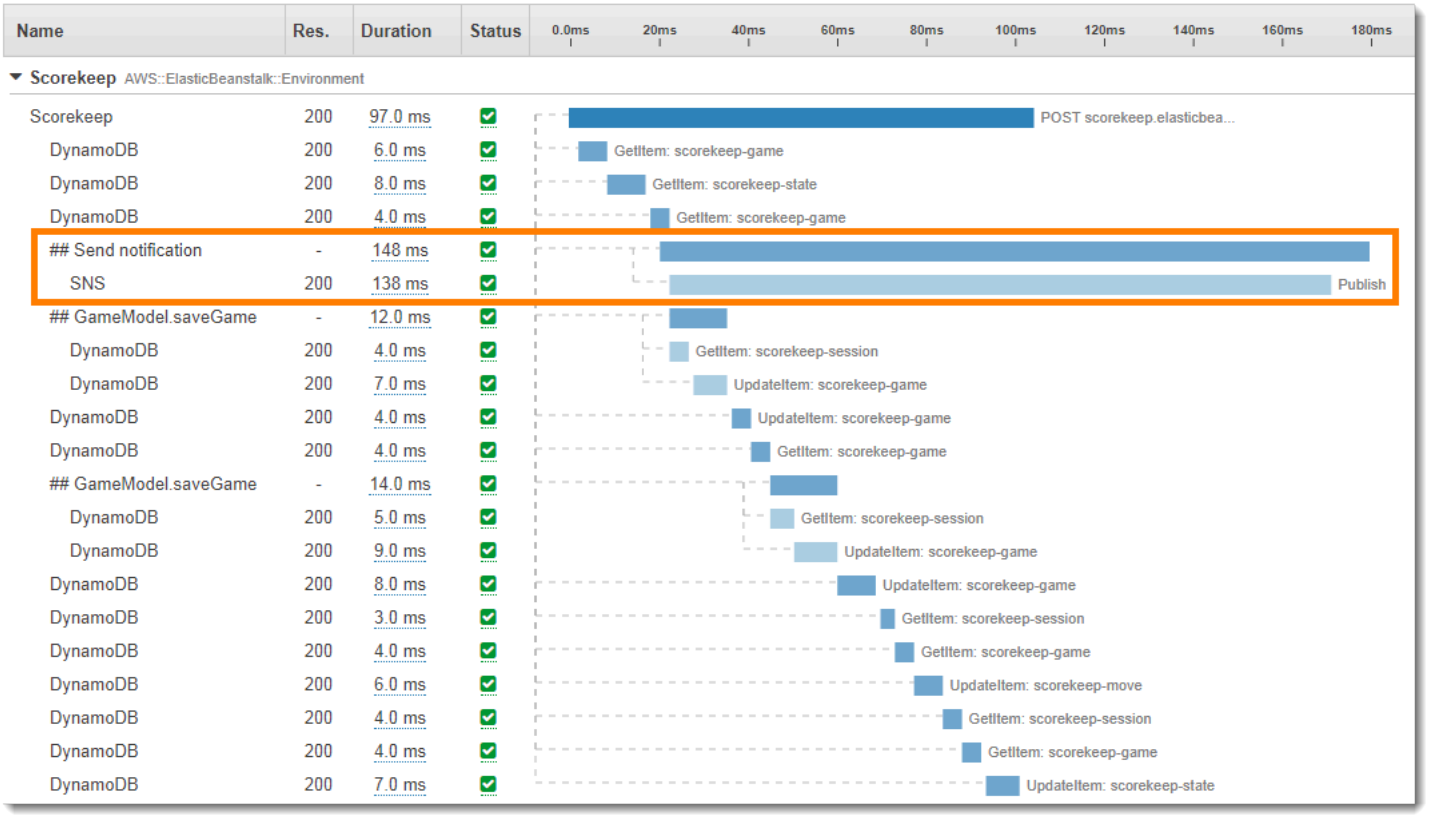
```
Exception in thread "Thread-2" com.amazonaws.xray.exceptions.SegmentNotFoundException:
 Failed to begin subsegment named 'AmazonSNS': segment cannot be found.
        at sun.reflect.NativeConstructorAccessorImpl.newInstance0(Native Method)
        at
 sun.reflect.NativeConstructorAccessorImpl.newInstance(NativeConstructorAccessorImpl.java:62)
        at
 sun.reflect.DelegatingConstructorAccessorImpl.newInstance(DelegatingConstructorAccessorImpl.ja
...
```

Para solucionar este problema, la aplicación utiliza `GetTraceEntity` para obtener una referencia al segmento en el subproceso principal y `Entity.run()` para ejecutar código del subproceso de trabajo con acceso al contexto del segmento.

Example **src/main/java/scorekeep/MoveFactory.java**: transferencia de contexto del rastro a un subproceso de trabajo

```
import com.amazonaws.xray.AWSXRay;
import com.amazonaws.xray.AWSXRayRecorder;
import com.amazonaws.xray.entities.Entity;
import com.amazonaws.xray.entities.Segment;
import com.amazonaws.xray.entities.Subsegment;
...
      Entity segment = recorder.getTraceEntity();
      Thread comm = new Thread() {
        public void run() {
         segment.run(() -> {
            Subsegment subsegment = AWSXRay.beginSubsegment("## Send notification");
            Sns.sendNotification("Scorekeep game completed", "Winner: " + userId);
            AWSXRay.endSubsegment();
          }
        }
```

Dado que la solicitud ya se ha resuelto antes de la llamada a Amazon SNS, la aplicación crea un subsegmento independiente para el subproceso. Esto impide que el SDK de X-Ray cierre el segmento antes de que registre la respuesta desde Amazon SNS. Si no hay ningún subsegmento abierto cuando Scorekeep resuelve la solicitud, se podría perder la respuesta de Amazon SNS.



Consulte Transmisión de contexto de segmento entre subprocesos en una aplicación multiproceso para obtener más información acerca de los subprocesos múltiples.

Solución de problemas AWS X-Ray

En este tema se enumeran errores y problemas comunes que podrían surgir cuando se utiliza la consola, la API o los SDK de X-Ray. Si se encuentra con un problema que no aparezca en esta lista, puede utilizar el botón Comentarios de esta página para notificarlo.

Secciones

Mapa de rastreo de rayos X y páginas de detalles de rastreo

Las siguientes secciones pueden ayudarle si tiene problemas para utilizar el mapa de rastreo de X-Ray y la página de detalles del rastreo:

No veo todos mis CloudWatch registros

La forma de configurar los registros para que aparezcan en el mapa de rastreo de X-Ray y en las páginas de detalles del rastreo depende del servicio.

- Los registros de API Gateway aparecen si se activa el registro en API Gateway.

No todos los nodos del mapa de servicio admiten la visualización de los registros asociados. Vea los registros de los siguientes tipos de nodos:

- Contexto Lambda
- Función de Lambda
- Etapa API Gateway
- Clúster de Amazon ECS
- Instancia de Amazon ECS
- Servicio de Amazon ECS
- Tarea de Amazon ECS

- Clúster de Amazon EKS
- Espacio de nombres Amazon EKS
- Nodo Amazon EKS
- Cápsula Amazon EKS
- Servicio Amazon EKS

No veo todas mis alarmas en el mapa de trazas de los X-Ray

El mapa de rastreo de X-Ray muestra solo el icono de alerta de un nodo si alguna alarma asociada a ese nodo está en estado ALARMA.

El mapa de rastreo asocia las alarmas a los nodos mediante la siguiente lógica:

- Si el nodo representa un AWS servicio, todas las alarmas con el espacio de nombres asociado a ese servicio están asociadas al nodo. Por ejemplo, un nodo de este tipo `AWS::Kinesis` está vinculado a todas las alarmas que se basan en las métricas del CloudWatch espacio de nombres. `AWS/Kinesis`
- Si el nodo representa un AWS recurso, las alarmas de ese recurso específico están vinculadas. Por ejemplo, un nodo de tipo `AWS::DynamoDB::Table` con el nombre «MyTable» está vinculado a todas las alarmas que se basan en una métrica con el espacio de nombres `AWS/DynamoDB` y cuya `TableName` dimensión está establecida en. `MyTable`
- Si el nodo es de tipo desconocido, que se identifica mediante un borde discontinuo alrededor del nombre, no se asociará ninguna alarma a ese nodo.

No veo algunos AWS recursos en el mapa de rastreo

No todos los AWS recursos están representados por un nodo dedicado. Algunos AWS servicios están representados por un único nodo para todas las solicitudes al servicio. Los siguientes tipos de recurso se muestran con un nodo por recurso:

- `AWS::DynamoDB::Table`
- `AWS::Lambda::Function`

  Las funciones Lambda se representan mediante dos nodos: uno para el contenedor Lambda y otro para la función. Esto ayuda a identificar problemas de arranque en frío con las funciones

de Lambda. Los nodos de contenedor de Lambda se asocian a alarmas y paneles de la misma manera que los nodos de función de Lambda.

- `AWS::ApiGateway::Stage`
- `AWS::SQS::Queue`
- `AWS::SNS::Topic`

Hay demasiados nodos en el mapa de rastreo

Utilice grupos de X-Ray para dividir el mapa en varios mapas. Para obtener más información, consulte Uso de expresiones de filtro con grupos.

SDK de X-Ray para Java

Error: excepción en el hilo «Thread-1" com.amazonaws.xray.exceptions.SegmentNotFoundException: No se pudo iniciar el subsegmento denominado 'AmazonSNS': no se encuentra el segmento.

Este error indica que el SDK de X-Ray intentó grabar una llamada saliente a AWS, pero no pudo encontrar un segmento abierto. Esto podría darse en las siguientes situaciones:

- No se ha configurado un filtro de servlet: el SDK de X-Ray crea segmentos para las solicitudes entrantes con un filtro denominado `AWSXRayServletFilter`. Configure un filtro de servlet para instrumentar las solicitudes entrantes.
- Está utilizando clientes instrumentados fuera del código servlet: si utiliza un cliente instrumentado para realizar llamadas en código de inicio u otro tipo de código que no se ejecute en respuesta a una solicitud entrante, debe crear un segmento manualmente. Para ver ejemplos, consulte Instrumentación de código de inicio.
- Está usando clientes instrumentados en subprocesos de procesos de trabajo: al crear un nuevo subproceso, la grabadora de X-Ray pierde su referencia al segmento abierto. Puede utilizar los métodos `getTraceEntity` y `setTraceEntity` para obtener una referencia al segmento o subsegmento actual (`Entity`) y devolverlo a la grabadora dentro del hilo. Consulte Uso de clientes instrumentados en subprocesos de trabajo para ver un ejemplo.

SDK de X-Ray para Node.js

Problema: CLS no funciona con Sequelize

Pase el espacio de nombres del SDK de X-Ray para Node.js a Sequelize con el método `cls`.

```
var AWSXRay = require('aws-xray-sdk');
const Sequelize = require('sequelize');
Sequelize.cls = AWSXRay.getNamespace();
const sequelize = new Sequelize(...);
```

Problema: CLS no funciona con Bluebird

Utilice `cls-bluebird` para que Bluebird funcione con CLS.

```
var AWSXRay = require('aws-xray-sdk');
var Promise = require('bluebird');
var clsBluebird = require('cls-bluebird');
clsBluebird(AWSXRay.getNamespace());
```

El daemon de X-Ray

Problema: El demonio está utilizando credenciales incorrectas

El daemon usa el AWS SDK para cargar las credenciales. Si se emplean varios métodos para proporcionar las credenciales, se utilizará el método que tenga la máxima prioridad. Para obtener más información, consulte Ejecutar el demonio.

Seguridad en AWS X-Ray

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

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

- Seguridad de la nube: AWS es responsable de proteger la infraestructura que se ejecuta Servicios de AWS en la Nube de AWS. AWS también le proporciona servicios que puede utilizar de forma segura. Auditores externos prueban y verifican periódicamente la eficacia de nuestra seguridad en el marco de los programas de conformidad de AWS. Para obtener información sobre los programas de conformidad que se aplican a X-Ray, consulte Servicios de AWS en el ámbito del programa de conformidad.
- Seguridad en la nube: su responsabilidad viene determinada por lo Servicio de AWS que utilice. Usted también es responsable de otros factores, incluida la confidencialidad de los datos, los requisitos de la empresa y la legislación y los reglamentos aplicables.

Esta documentación lo ayudará a comprender cómo aplicar el modelo de responsabilidad compartida cuando se utiliza X-Ray. En los siguientes temas, se le mostrará cómo configurar X-Ray para cumplir sus objetivos de seguridad y conformidad. También aprenderá a usar otros Servicios de AWS que pueden ayudarlo a monitorear y proteger sus recursos de X-Ray.

Temas

Protección de los datos en AWS X-Ray

AWS X-Ray siempre cifra los registros de seguimiento y los datos en reposo relacionados. Cuando necesite auditar y deshabilitar las claves de cifrado por motivos internos o de conformidad, puede

configurar X-Ray para que utilice una AWS Key Management Service (AWS KMS) a la hora de cifrar los datos.

X-Ray proporciona una Clave administrada de AWS denominada `aws/xray`. Utilice esta clave únicamente cuando desee auditar el uso de claves en AWS CloudTrail y no la propia clave. Cuando necesite administrar el acceso a la clave o configurar la rotación de claves, puede crear una clave administrada por el cliente.

Si cambia la configuración de cifrado, X-Ray tardará algún tiempo en generar y propagar las claves de datos. Aunque la nueva clave se esté procesando, X-Ray puede cifrar los datos utilizando la configuración anterior y la nueva de forma combinada. Si se modifica la configuración de cifrado, los datos existentes no volverán a cifrarse.

> **Note**
>
> AWS KMS genera costos cuando X-Ray utiliza una clave de KMS para cifrar o descifrar los datos de rastreo.
>
> - Cifrado predeterminado: gratuito.
> - Clave administrada de AWS: se paga por el uso de las claves.
> - Clave administrada por el cliente: se paga por el uso y el almacenamiento de las claves.
>
> Para obtener más información, consulte AWS Key Management Service Pricing.

> **Note**
>
> Las notificaciones de información de X-Ray envían eventos a Amazon EventBridge, que actualmente no admite claves administradas por el cliente. Para obtener más información, consulte Protección de datos en Amazon EventBridge.

Debe tener acceso de nivel de usuario a una clave administrada por el cliente para configurar X-Ray, utilizarlo y, a continuación, consultar los rastros cifrados. Para obtener más información, consulte Permisos de usuario para cifrado.

CloudWatch console

Para configurar X-Ray de manera que utilice una clave de KMS para el cifrado mediante la consola de CloudWatch

1. Inicie sesión en la AWS Management Console y abra la consola de CloudWatch en https://console.aws.amazon.com/cloudwatch/.
2. Elija Configuración en el panel de navegación izquierdo.
3. Elija Ver ajustes en Cifrado dentro de la sección de Rastros de X-Ray.
4. Elija Editar en la sección Configuración del cifrado.
5. Elija Usar una clave de KMS.
6. Elija una clave en el menú desplegable:
   - aws/xray: utilice la Clave administrada de AWS.
   - Alias de clave: utilice una clave administrada por el cliente en su cuenta.
   - Especifique manualmente un ARN de clave: utilice una clave administrada por el cliente en una cuenta diferente. En el campo que aparece, escriba el nombre de recurso de Amazon (ARN) completo.
7. Elija Actualizar el cifrado.

X-Ray console

Para configurar X-Ray de manera que utilice una clave de KMS para el cifrado mediante la consola de X-Ray

1. Abra la consola de X-Ray.
2. Seleccione Encryption (Cifrado).
3. Elija Usar una clave de KMS.
4. Elija una clave en el menú desplegable:
   - aws/xray: utilice la Clave administrada de AWS.
   - Alias de clave: utilice una clave administrada por el cliente en su cuenta.
   - Especifique manualmente un ARN de clave: utilice una clave administrada por el cliente en una cuenta diferente. En el campo que aparece, escriba el nombre de recurso de Amazon (ARN) completo.

5. Seleccione Apply (Aplicar).

> **Note**
>
> X-Ray no es compatible con claves de KMS asimétricas.

Si X-Ray no puede obtener acceso a la clave de cifrado, deja de almacenar los datos. Esto puede ocurrir si el usuario pierde acceso a la clave de KMS o si se deshabilita una clave que actualmente está en uso. Cuando esto sucede, X-Ray muestra una notificación en la barra de navegación.

Para configurar las opciones de cifrado con la API de X-Ray, consulte Configuración de las opciones de muestreo, grupos y cifrado con la API de AWS X-Ray.

Administración de identidad y acceso para AWS X-Ray

AWS Identity and Access Management (IAM) es una herramienta Servicio de AWS que ayuda al administrador a controlar de forma segura el acceso a AWS los recursos. Los administradores de IAM controlan quién puede estar autenticado (ha iniciado sesión) y autorizado (tiene permisos) para utilizar recursos de X-Ray. La IAM es una Servicio de AWS herramienta que puede utilizar sin coste adicional.

Temas

- Público
- Autenticación con identidades
- Administración de acceso mediante políticas
- Cómo AWS X-Ray funciona con IAM
- AWS X-Ray ejemplos de políticas basadas en la identidad
- Solución de problemas de identidades y accesos en AWS X-Ray

Público

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

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

Administrador de servicio: si está a cargo de los recursos de X-Ray en su empresa, probablemente tenga acceso completo a X-Ray. Su trabajo consiste en determinar a qué características y recursos de X-Ray deben acceder los usuarios del servicio. Luego, debe enviar solicitudes a su administrador de IAM para cambiar los permisos de los usuarios de su servicio. Revise la información de esta página para conocer los conceptos básicos de IAM. Para obtener más información sobre cómo su empresa puede utilizar IAM con X-Ray, consulte Cómo AWS X-Ray funciona con IAM.

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

Autenticación con identidades

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

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

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

Si accede AWS mediante programación, AWS proporciona un kit de desarrollo de software (SDK) y una interfaz de línea de comandos (CLI) para firmar criptográficamente sus solicitudes con sus credenciales. Si no utilizas AWS herramientas, debes firmar las solicitudes tú mismo. Para obtener

más información sobre cómo usar el método recomendado para firmar las solicitudes usted mismo, consulte Firmar las solicitudes de la AWS API en la Guía del usuario de IAM.

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

Cuenta de AWS usuario root

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

Usuarios y grupos de IAM

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

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

Los usuarios son diferentes de los roles. Un usuario se asocia exclusivamente a una persona o aplicación, pero la intención es que cualquier usuario pueda asumir un rol que necesite. Los usuarios tienen credenciales permanentes a largo plazo y los roles proporcionan credenciales temporales.

Para más información, consulte Cuándo crear un usuario de IAM (en lugar de un rol) en la Guía del usuario de IAM.

Roles de IAM

Un rol de IAM es una identidad dentro de usted Cuenta de AWS que tiene permisos específicos. Es similar a un usuario de IAM, pero no está asociado a una determinada persona. Puede asumir temporalmente una función de IAM en el AWS Management Console cambiando de función. Puede asumir un rol llamando a una operación de AWS API AWS CLI o utilizando una URL personalizada. Para más información sobre los métodos para el uso de roles, consulte Uso de roles de IAM en la Guía del usuario de IAM.

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

- Acceso de usuario federado: para asignar permisos a una identidad federada, puede crear un rol y definir sus permisos. Cuando se autentica una identidad federada, se asocia la identidad al rol y se le conceden los permisos define el rol. Para obtener información acerca de roles para federación, consulte Creación de un rol para un proveedor de identidades de terceros en la Guía del usuario de IAM. Si utiliza el IAM Identity Center, debe configurar un conjunto de permisos. El Centro de identidades de IAM correlaciona el conjunto de permisos con un rol en IAM para controlar a qué pueden acceder sus identidades después de autenticarse. Para obtener información acerca de los conjuntos de permisos, consulte Conjuntos de permisos en la Guía del usuario de AWS IAM Identity Center .
- Permisos de usuario de IAM temporales: un usuario de IAM puede asumir un rol de IAM para recibir temporalmente permisos distintos que le permitan realizar una tarea concreta.
- Acceso entre cuentas: puede utilizar un rol de IAM para permitir que alguien (una entidad principal de confianza) de otra cuenta acceda a los recursos de la cuenta. Los roles son la forma principal de conceder acceso entre cuentas. Sin embargo, con algunas Servicios de AWS, puedes adjuntar una política directamente a un recurso (en lugar de usar un rol como proxy). Para obtener información acerca de la diferencia entre los roles y las políticas basadas en recursos para el acceso entre cuentas, consulte Cómo los roles de IAM difieren de las políticas basadas en recursos en la Guía del usuario de IAM.
- Acceso entre servicios: algunos Servicios de AWS utilizan funciones en otros Servicios de AWS. Por ejemplo, cuando realiza una llamada en un servicio, es común que ese servicio ejecute aplicaciones en Amazon EC2 o almacene objetos en Amazon S3. Es posible que un servicio haga esto usando los permisos de la entidad principal, usando un rol de servicio o usando un rol vinculado al servicio.

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

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

Administración de acceso mediante políticas

El acceso se controla AWS creando políticas y adjuntándolas a AWS identidades o recursos. Una política es un objeto AWS que, cuando se asocia a una identidad o un recurso, define sus permisos. AWS evalúa estas políticas cuando un director (usuario, usuario raíz o sesión de rol) realiza una

solicitud. Los permisos en las políticas determinan si la solicitud se permite o se deniega. La mayoría de las políticas se almacenan AWS como documentos JSON. Para obtener más información sobre la estructura y el contenido de los documentos de política JSON, consulte Información general de políticas JSON en la Guía del usuario de IAM.

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

De forma predeterminada, los usuarios y los roles no tienen permisos. Para conceder permiso a los usuarios para realizar acciones en los recursos que necesiten, un administrador de IAM puede crear políticas de IAM. A continuación, el administrador puede agregar las políticas de IAM a los roles y los usuarios pueden asumir esos roles.

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

Políticas basadas en identidades

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

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

Políticas basadas en recursos

Las políticas basadas en recursos son documentos de política JSON que se asocian a un recurso. Ejemplos de políticas basadas en recursos son las políticas de confianza de roles de IAM y las políticas de bucket de Amazon S3. En los servicios que admiten políticas basadas en recursos, los

administradores de servicios pueden utilizarlos para controlar el acceso a un recurso específico. Para el recurso al que se asocia la política, la política define qué acciones puede realizar una entidad principal especificada en ese recurso y en qué condiciones. Debe especificar una entidad principal en una política en función de recursos. Los principales pueden incluir cuentas, usuarios, roles, usuarios federados o. Servicios de AWS

Las políticas basadas en recursos son políticas insertadas que se encuentran en ese servicio. No puedes usar políticas AWS gestionadas de IAM en una política basada en recursos.

Listas de control de acceso (ACL)

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

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

Otros tipos de políticas

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

- Límites de permisos: un límite de permisos es una característica avanzada que le permite establecer los permisos máximos que una política basada en identidad puede conceder a una entidad de IAM (usuario o rol de IAM). Puede establecer un límite de permisos para una entidad. Los permisos resultantes son la intersección de las políticas basadas en la identidad de la entidad y los límites de permisos. Las políticas basadas en recursos que especifique el usuario o rol en el campo `Principal` no estarán restringidas por el límite de permisos. Una denegación explícita en cualquiera de estas políticas anulará el permiso. Para obtener más información sobre los límites de los permisos, consulte Límites de permisos para las entidades de IAM en la Guía del usuario de IAM.
- Políticas de control de servicios (SCP): las SCP son políticas de JSON que especifican los permisos máximos para una organización o unidad organizativa (OU). AWS Organizations AWS Organizations es un servicio para agrupar y gestionar de forma centralizada varios de los Cuentas de AWS que son propiedad de su empresa. Si habilita todas las características en una organización, entonces podrá aplicar políticas de control de servicio (SCP) a una o a todas sus

cuentas. El SCP limita los permisos de las entidades en las cuentas de los miembros, incluidas las de cada una. Usuario raíz de la cuenta de AWS Para más información sobre Organizations y las SCP, consulte Funcionamiento de las SCP en la Guía del usuario de AWS Organizations .

- Políticas de sesión: las políticas de sesión son políticas avanzadas que se pasan como parámetro cuando se crea una sesión temporal mediante programación para un rol o un usuario federado. Los permisos de la sesión resultantes son la intersección de las políticas basadas en identidades del rol y las políticas de la sesión. Los permisos también pueden proceder de una política en función de recursos. Una denegación explícita en cualquiera de estas políticas anulará el permiso. Para más información, consulte Políticas de sesión en la Guía del usuario de IAM.

Varios tipos de políticas

Cuando se aplican varios tipos de políticas a una solicitud, los permisos resultantes son más complicados de entender. Para saber cómo AWS determinar si se debe permitir una solicitud cuando se trata de varios tipos de políticas, consulte la lógica de evaluación de políticas en la Guía del usuario de IAM.

Cómo AWS X-Ray funciona con IAM

Antes de utilizar IAM para administrar el acceso a X-Ray, debe comprender qué características de IAM están disponibles para su uso con X-Ray. Para obtener una visión general de cómo X-Ray y otros Servicios de AWS funcionan con IAM, consulte Servicios de AWS That Work with IAM en la Guía del usuario de IAM.

Puedes usar AWS Identity and Access Management (IAM) para conceder permisos de X-Ray a los usuarios y los recursos informáticos de tu cuenta. IAM controla el acceso al servicio X-Ray a nivel de la API para aplicar los permisos de manera uniforme, independientemente del cliente (consola, AWS SDK AWS CLI) que empleen sus usuarios.

Para usar la consola X-Ray para ver mapas y segmentos de rastreo, solo necesita permisos de lectura. Para habilitar el acceso a la consola, añada la `AWSXrayReadOnlyAccess` política administrada al usuario de IAM.

Para desarrollo local y pruebas, cree un rol de IAM con permisos de lectura y escritura. Asuma el rol y almacene las credenciales temporales para el rol. Puede usar estas credenciales con el daemon X-Ray AWS CLI, el y el AWS SDK. Para obtener más información, consulte Uso de credenciales de seguridad temporales con AWS CLI.

Para implementar su aplicación instrumentada AWS, cree una función de IAM con permisos de escritura y asígnela a los recursos que ejecutan la aplicación. `AWSXRayDaemonWriteAccess`incluye permisos para cargar trazas y algunos permisos de lectura para permitir el uso de reglas de muestreo.

Las políticas de lectura y escritura no incluyen permiso para configurar la configuración de clave de cifrado y reglas de muestreo. Utilice `AWSXrayFullAccess` para obtener acceso a estas configuraciones o añadir API de configuración en una política personalizada. Para el cifrado y el descifrado con una clave administrada por el cliente que cree, también necesita permiso para utilizar la clave.

Temas

- Políticas de X-Ray basadas en identidades
- Políticas de X-Ray basadas en recursos
- Autorización basada en etiquetas de X-Ray
- Ejecutar la aplicación de forma local
- Ejecutar la aplicación en AWS
- Permisos de usuario para cifrado

Políticas de X-Ray basadas en identidades

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. X-Ray admite acciones, claves de condición y recursos específicos. Para obtener información sobre todos los elementos que utiliza en una política JSON, consulte Referencia de los elementos de las políticas JSON de IAM en la Guía del usuario de IAM.

Acciones

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

El elemento `Action` de una política JSON describe las acciones que puede utilizar para conceder o denegar el acceso en una política. Las acciones políticas suelen tener el mismo nombre que la operación de AWS API asociada. Hay algunas excepciones, como acciones de solo permiso que no tienen una operación de API coincidente. También hay algunas operaciones que requieren varias acciones en una política. Estas acciones adicionales se denominan acciones dependientes.

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

Las acciones de políticas de X-Ray utilizan el siguiente prefijo antes de la acción: `xray:`. Por ejemplo, para conceder a alguien permiso para recuperar detalles de los recursos de grupo con la operación de la API `GetGroup` de X-Ray, incluya la acción `xray:GetGroup` en su política. Las instrucciones de la política deben incluir un elemento `Action` o un elemento `NotAction`. X-Ray define su propio conjunto de acciones que describen las tareas que se pueden realizar con este servicio.

Para especificar varias acciones en una única instrucción, sepárelas con comas del siguiente modo:

```
"Action": [
      "xray:action1",
      "xray:action2"
```

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": "xray:Get*"
```

Para ver una lista de las acciones de X-Ray, consulte Acciones definidas por AWS X-Ray en la Guía del usuario de IAM.

Recursos

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

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

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

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

Puede controlar el acceso a los recursos a través de una política de IAM. Para las acciones que admiten permisos de nivel de recursos, se usa un nombre de recurso de Amazon (ARN) para identificar el recurso al que se aplica la política.

Es posible utilizar todas las acciones de X-Ray en una política de IAM para conceder o denegar permiso a los usuarios para utilizar esa acción. Sin embargo, no todas las acciones de X-Ray admiten permisos de nivel de recursos, que le permiten especificar los recursos en los que se puede realizar una acción.

Para las acciones que no admiten permisos de nivel de recursos, debe utilizar "*" como recurso.

Las siguientes acciones de X-Ray admiten permisos de nivel de recursos:

- `CreateGroup`
- `GetGroup`
- `UpdateGroup`
- `DeleteGroup`
- `CreateSamplingRule`
- `UpdateSamplingRule`
- `DeleteSamplingRule`

A continuación, se muestra un ejemplo de una política de permisos basada en identidad para una acción `CreateGroup`: El ejemplo muestra el uso de un ARN relacionado con el nombre de grupo `local-users` con el ID único como elemento comodín. El ID único se genera cuando se crea el grupo y, por lo tanto, no puede predecirse en la política con antelación. Cuando se utiliza `GetGroup`, `UpdateGroup` o `DeleteGroup`, puede definir esto como un elemento comodín o el ARN exacto, incluido el ID.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "xray:CreateGroup"
            ],
            "Resource": [
```

```
                "arn:aws:xray:eu-west-1:123456789012:group/local-users/*"
            ]
        }
    ]
}
```

A continuación, se muestra un ejemplo de una política de permisos basada en identidad para una acción `CreateSamplingRule`:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "xray:CreateSamplingRule"
            ],
            "Resource": [
                "arn:aws:xray:eu-west-1:123456789012:sampling-rule/base-scorekeep"
            ]
        }
    ]
}
```

> **Note**
>
> El ARN de una regla de muestreo se define por su nombre. A diferencia de los ARN de grupo, las reglas de muestreo no tienen un ID generado de manera inequívoca.

Para ver una lista de tipos de recursos de X-Ray y sus ARN, consulte Recursos definidos por AWS X-Ray en la Guía del usuario de IAM. Para obtener información sobre las acciones con las que puede especificar el ARN de cada recurso, consulte Acciones definidas por AWS X-Ray.

Claves de condición

X-Ray no proporciona ninguna clave de condición específica del servicio, pero sí admite el uso de algunas claves de condición globales. Para ver todas las claves de condición AWS globales, consulte las claves de contexto de condición AWS globales en la Guía del usuario de IAM.

Ejemplos

Para ver ejemplos de políticas basadas en identidad de X-Ray, consulte AWS X-Ray ejemplos de políticas basadas en la identidad.

Políticas de X-Ray basadas en recursos

X-Ray admite políticas basadas en recursos para la Servicio de AWS integración actual y futura, como el rastreo activo de Amazon SNS. Las políticas basadas en recursos de X-Ray se pueden actualizar por otros AWS Management Console, o mediante el AWS SDK o la CLI. Por ejemplo, la consola de Amazon SNS intenta configurar automáticamente una política basada en recursos para enviar rastros a X-Ray. En el siguiente documento de política se proporciona un ejemplo de configuración manual de una política basada en recursos de X-Ray.

Example Ejemplo de política basada en recursos de X-Ray para el rastreo activo de Amazon SNS

En este ejemplo de documento de política se especifican los permisos que Amazon SNS necesita para enviar datos de rastreo a X-Ray:

```
{
    Version: "2012-10-17",
    Statement: [
      {
        Sid: "SNSAccess",
        Effect: Allow,
        Principal: {
          Service: "sns.amazonaws.com",
        },
        Action: [
          "xray:PutTraceSegments",
          "xray:GetSamplingRules",
          "xray:GetSamplingTargets"
        ],
        Resource: "*",
        Condition: {
          StringEquals: {
            "aws:SourceAccount": "account-id"
          },
          StringLike: {
            "aws:SourceArn": "arn:partition:sns:region:account-id:topic-name"
          }
        }
```

```
      }
    ]
  }
```

Utilice la CLI para crear una política basada en recursos que dé a Amazon SNS permisos para enviar datos de rastreo a X-Ray:

```
aws xray put-resource-policy --policy-name MyResourcePolicy --policy-document
 '{ "Version": "2012-10-17", "Statement": [ { "Sid": "SNSAccess", "Effect": "Allow",
 "Principal": { "Service": "sns.amazonaws.com" }, "Action": [ "xray:PutTraceSegments",
 "xray:GetSamplingRules", "xray:GetSamplingTargets" ], "Resource": "*",
 "Condition": { "StringEquals": { "aws:SourceAccount": "account-id" }, "StringLike":
 { "aws:SourceArn": "arn:partition:sns:region:account-id:topic-name" } } } ] }'
```

Para usar estos ejemplos, sustituya *partition*, *regionaccount-id*, y *topic-name*por su AWS partición, región, ID de cuenta y nombre de tema de Amazon SNS específicos. Para dar permiso a todos los temas de Amazon SNS para que envíen datos de rastreo a X-Ray, sustituya el nombre del tema por *.

Autorización basada en etiquetas de X-Ray

Puede adjuntar etiquetas a los grupos o las reglas de muestreo de X-Ray, o pasar las etiquetas en una solicitud a X-Ray. 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 `xray:ResourceTag/`*`key-name`*, `aws:RequestTag/`*`key-name`* o `aws:TagKeys`. Para obtener más información acerca del etiquetado de recursos de X-Ray, consulte Etiquetado de reglas de muestreo y grupos de X-Ray.

Para consultar un ejemplo de política basada en la identidad para limitar el acceso a un recurso en función de las etiquetas de ese recurso, consulte Gestión del acceso a los grupos de rayos X y a las reglas de muestreo en función de las etiquetas.

Ejecutar la aplicación de forma local

Su aplicación instrumentada envía datos de rastreo al daemon de X-Ray. El daemon almacena en búfer documentos de segmento y los carga en lotes en el servicio X-Ray. El daemon necesita permisos de escritura para cargar los datos de rastreo y telemetría en el servicio X-Ray.

Al ejecutar el daemon de forma local, se crea un rol de IAM, se asume el rol y se almacenan las credenciales temporales en variables de entorno o en un archivo denominado `credentials` dentro

de una carpeta denominada `.aws` en la carpeta de usuario. Para obtener más información, consulte Uso de credenciales de seguridad temporales con AWS CLI.

Example ~/.aws/credentials

```
[default]
aws_access_key_id={access key ID}
aws_secret_access_key={access key}
aws_session_token={AWS session token}
```

Si ya configuró las credenciales para usarlas con el AWS SDK o AWS CLI, el daemon puede usarlas. En caso de que haya varios perfiles disponibles, el daemon utilizará el perfil predeterminado.

Ejecutar la aplicación en AWS

Cuando ejecute la aplicación AWS, utilice un rol para conceder permiso a la instancia de Amazon EC2 o a la función Lambda que ejecuta el daemon.

- Amazon Elastic Compute Cloud (Amazon EC2): cree un rol de IAM y adjúntelo a la instancia de EC2 como perfil de instancia.
- Amazon Elastic Container Service (Amazon ECS): cree un rol de IAM y adjúntelo a las instancias de contenedor como rol de IAM de instancia de contenedor.
- AWS Elastic Beanstalk (Elastic Beanstalk): Elastic Beanstalk incluye los permisos de X-Ray en su perfil de instancia predeterminado. Puede usar el perfil de instancia predeterminado o añadir permisos de escritura a un perfil de instancia personalizado.
- AWS Lambda (Lambda): agrega permisos de escritura a la función de ejecución de la función.

Para crear un rol y usarlo con X-Ray

1. Abra la consola de IAM.
2. Elija Roles.
3. Elija Crear nuevo rol.
4. En Role Name (Nombre del rol), escriba **`xray-application`**. Elija Paso siguiente.
5. En Role Type (Tipo de rol), elija Amazon EC2.
6. Adjunte la siguiente política administrada para que la aplicación tenga acceso a los Servicios de AWS:

- AWSXRayDaemonWriteAccess— Da permiso al daemon de X-Ray para cargar datos de rastreo.

  Si su aplicación usa el AWS SDK para acceder a otros servicios, añada políticas que permitan el acceso a esos servicios.

7. Elija Paso siguiente.
8. Seleccione Crear rol.

Permisos de usuario para cifrado

X-Ray cifra todos los datos de rastro y de forma predeterminada y puede configurarlo para que use una clave que usted administre. Si elige una clave administrada por el AWS Key Management Service cliente, debe asegurarse de que la política de acceso de la clave le permita conceder permiso a X-Ray para usarla para cifrar. Otros usuarios de su cuenta también tienen que obtener acceso a la clave para ver los datos de rastreo cifrados en la consola de X-Ray.

Para una clave administrada por el cliente, configure su clave con una política de acceso que permita las siguientes acciones:

- El usuario que configura la clave en X-Ray tiene permisos para llamar a `kms:CreateGrant` y `kms:DescribeKey`.
- Los usuarios que pueden tener acceso a los datos de rastreo cifrados tienen permiso para llamar a `kms:Decrypt`.

Cuando se añade un usuario al grupo Usuarios clave en la sección de configuración de clave de la consola de , tienen permisos para ambas operaciones. Los permisos solo deben estar establecidos en la política de claves, por lo que no necesitas ningún AWS KMS permiso para tus usuarios, grupos o funciones. Para obtener más información, consulte Uso de políticas clave en la Guía para AWS KMS desarrolladores.

Para el cifrado predeterminado, o si elige la CMK (`aws/xray`) AWS administrada, el permiso depende de quién tenga acceso a las API de X-Ray. Cualquier persona con acceso a `PutEncryptionConfig`, incluido en `AWSXrayFullAccess`, puede cambiar la configuración de cifrado. Para evitar que un usuario cambie la clave de cifrado, no le conceda permiso para utilizar `PutEncryptionConfig`.

AWS X-Ray ejemplos de políticas basadas en la identidad

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

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

Temas

Prácticas recomendadas relativas a políticas

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

- 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 en muchos casos de uso comunes. Están disponibles en su. Cuenta de AWS Le recomendamos que reduzca aún más los permisos definiendo políticas administradas por el AWS cliente que sean específicas para sus casos de uso. Con el fin de obtener más información, consulte las políticas administradas por AWS o las políticas administradas por AWS para funciones de trabajo en la Guía del usuario de IAM.
- Aplique permisos de privilegio mínimo: cuando establezca permisos con políticas de IAM, conceda solo los permisos necesarios para realizar una tarea. Para ello, debe definir las acciones que se

pueden llevar a cabo en determinados recursos en condiciones específicas, también conocidos como permisos de privilegios mínimos. Con el fin de obtener más información sobre el uso de IAM para aplicar permisos, consulte Políticas y permisos en IAM en la Guía del usuario de IAM.

- Utilice condiciones en las políticas de IAM para restringir aún más el acceso: puede agregar una condición a sus políticas para limitar el acceso a las acciones y los recursos. Por ejemplo, puede escribir una condición de políticas para especificar que todas las solicitudes deben enviarse utilizando SSL. También puedes usar condiciones para conceder el acceso a las acciones del servicio si se utilizan a través de una acción específica Servicio de AWS, por ejemplo AWS CloudFormation. Para obtener más información, consulte Elementos de la política de JSON de IAM: Condición en la Guía del usuario de IAM.
- Utilice el analizador de acceso de IAM para validar las políticas de IAM con el fin de garantizar la seguridad y funcionalidad de los permisos: el analizador de acceso de IAM valida políticas nuevas y existentes para que respeten el lenguaje (JSON) de las políticas de IAM y las prácticas recomendadas de IAM. El analizador de acceso de IAM proporciona más de 100 verificaciones de políticas y recomendaciones procesables para ayudar a crear políticas seguras y funcionales. Para más información, consulte Política de validación de Analizador de acceso de IAM en la Guía de usuario de IAM.
- Requerir autenticación multifactor (MFA): si tiene un escenario que requiere usuarios de IAM o un usuario raíz en Cuenta de AWS su cuenta, active la MFA para mayor seguridad. Para solicitar la MFA cuando se invocan las operaciones de la API, agregue las condiciones de la MFA a sus políticas. Para más información, consulte Configuración del acceso a una API protegido por MFA en la Guía de usuario de IAM.

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

Uso de la consola de X-Ray

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

Para garantizar que esas entidades puedan seguir utilizando la consola de X-Ray, adjunte la política `AWSXRayReadOnlyAccess` AWS gestionada a las entidades. Esta política se describe con más

detalle en las políticas administradas por IAM para X-Ray. Para obtener más información, consulte Adición de permisos a un usuario en la Guía del usuario de IAM.

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

Permitir a los usuarios consultar sus propios permisos

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

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
```

```
        }
    ]
}
```

Gestión del acceso a los grupos de rayos X y a las reglas de muestreo en función de las etiquetas

Puede utilizar las condiciones de su política basada en la identidad para controlar el acceso a los grupos y reglas de muestreo de X-Ray basados en etiquetas. El siguiente ejemplo de política podría utilizarse para denegar a un rol de usuario los permisos para crear, eliminar o actualizar grupos con las etiquetas `stage:prod` `ostage:preprod`. Para obtener más información sobre el etiquetado de las reglas y grupos de muestreo de rayos X, consulte Etiquetado de reglas de muestreo y grupos de X-Ray.

Para denegar a un usuario el acceso para crear, actualizar o eliminar un grupo con una etiqueta `stage:prod` o `stage:preprod` asignarle un rol con una política similar a la siguiente.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowAllXRay",
            "Effect": "Allow",
            "Action": "xray:*",
            "Resource": "*"
        },
        {
            "Sid": "DenyCreateGroupWithStage",
            "Effect": "Deny",
            "Action": [
                "xray:CreateGroup"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/stage": [
                        "preprod",
                        "prod"
                    ]
                }
            }
        },
```

```
        {
            "Sid": "DenyUpdateGroupWithStage",
            "Effect": "Deny",
            "Action": [
                "xray:UpdateGroup",
                "xray:DeleteGroup"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/stage": [
                        "preprod",
                        "prod"
                    ]
                }
            }
        }
    ]
}
```

Para denegar la creación de una regla de muestreo, utilice esta `aws:RequestTag` opción para indicar las etiquetas que no se pueden transferir como parte de una solicitud de creación. Para denegar la actualización o la eliminación de una regla de muestreo, utilice esta `aws:ResourceTag` opción para denegar las acciones basadas en las etiquetas de esos recursos.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowAllXRay",
            "Effect": "Allow",
            "Action": "xray:*",
            "Resource": "*"
        },
        {
            "Sid": "DenyCreateSamplingRuleWithStage",
            "Effect": "Deny",
            "Action": "xray:CreateSamplingRule",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/stage": [
                        "preprod",
```

```
                        "prod"
                    ]
                }
            }
        },
        {
            "Sid": "DenyUpdateSamplingRuleWithStage",
            "Effect": "Deny",
            "Action": [
                "xray:UpdateSamplingRule",
                "xray:DeleteSamplingRule"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/stage": [
                        "preprod",
                        "prod"
                    ]
                }
            }
        }
    ]
}
```

Puede adjuntar estas políticas (o combinarlas en una sola política y, a continuación, adjuntar la política) a los usuarios de su cuenta. Para que el usuario realice cambios en un grupo o regla de muestreo, el grupo o la regla de muestreo no debe estar etiquetado `stage=prepod` o `stage=prod`. La clave de la etiqueta de condición `Stage` coincide con los nombres de las claves de condición `Stage` y `stage` porque no distinguen entre mayúsculas y minúsculas. Para obtener más información acerca de las claves de condición, consulte Elementos de la política de JSON de IAM: Condición en la Guía del usuario de IAM.

Un usuario con un rol que tenga la siguiente política adjunta no puede agregar la etiqueta `role:admin` a los recursos ni eliminar etiquetas de un recurso que esté `role:admin` asociada a ella.

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

```
            "Effect": "Allow",
            "Action": "xray:*",
            "Resource": "*"
        },
        {
            "Sid": "DenyRequestTagAdmin",
            "Effect": "Deny",
            "Action": "xray:TagResource",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/role": "admin"
                }
            }
        },
        {
            "Sid": "DenyResourceTagAdmin",
            "Effect": "Deny",
            "Action": "xray:UntagResource",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/role": "admin"
                }
            }
        }
    ]
}
```

Políticas administradas por IAM para X-Ray

A fin de facilitar la concesión de permisos, IAM admite políticas administradas en cada servicio. Un servicio puede actualizar estas políticas administradas con nuevos permisos cuando publique nuevas API. AWS X-Ray proporciona políticas administradas para casos de uso de solo lectura, solo de escritura y de administrador.

- `AWSXrayReadOnlyAccess`— Lea los permisos para usar la consola de X-Ray o el AWS SDK para obtener datos de rastreo, mapas de rastreo, información y configuración de X-Ray desde la API de X-Ray. AWS CLI Incluye el administrador de acceso a la observabilidad (OAM) `oam:ListSinks` y `oam:ListAttachedSinks` permisos que permiten a la consola ver los rastreos compartidos desde las cuentas de origen como parte de la observabilidad CloudWatch entre cuentas. Las acciones `BatchGetTraceSummaryById` y las de la

`GetDistinctTraceGraphs` API no están pensadas para que el código las invoque y, por lo tanto, no están incluidas en los SDK ni en los SDK. AWS CLI AWS

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "xray:GetSamplingRules",
                "xray:GetSamplingTargets",
                "xray:GetSamplingStatisticSummaries",
                "xray:BatchGetTraces",
                "xray:BatchGetTraceSummaryById",
                "xray:GetDistinctTraceGraphs",
                "xray:GetServiceGraph",
                "xray:GetTraceGraph",
                "xray:GetTraceSummaries",
                "xray:GetGroups",
                "xray:GetGroup",
                "xray:ListTagsForResource",
                "xray:ListResourcePolicies",
                "xray:GetTimeSeriesServiceStatistics",
                "xray:GetInsightSummaries",
                "xray:GetInsight",
                "xray:GetInsightEvents",
                "xray:GetInsightImpactGraph",
                "oam:ListSinks"
            ],
            "Resource": [
                "*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "oam:ListAttachedLinks"
            ],
            "Resource": "arn:aws:oam:*:*:sink/*"
        }

}
```

- `AWSXRayDaemonWriteAccess`— Permisos de escritura para usar el daemon de X-Ray o el AWS SDK para cargar documentos de segmentos y telemetría a la API de X-Ray. AWS CLI Incluye permisos de lectura para obtener reglas de muestreo y notificar los resultados de muestreo.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "xray:PutTraceSegments",
                "xray:PutTelemetryRecords",
                "xray:GetSamplingRules",
                "xray:GetSamplingTargets",
                "xray:GetSamplingStatisticSummaries"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

- `AWSXrayCrossAccountSharingConfiguration`: otorga permisos para crear, administrar y ver los enlaces de Observability Access Manager para compartir los recursos de X-Ray entre cuentas. Se usa para permitir la observabilidad CloudWatch entre cuentas entre cuentas de origen y de monitoreo.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "xray:Link",
                "oam:ListLinks"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
```

```
                "oam:DeleteLink",
                "oam:GetLink",
                "oam:TagResource"
            ],
            "Resource": "arn:aws:oam:*:*:link/*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "oam:CreateLink",
                "oam:UpdateLink"
            ],
            "Resource": [
                "arn:aws:oam:*:*:link/*",
                "arn:aws:oam:*:*:sink/*"
            ]
        }
    ]

}
```

- `AWSXrayFullAccess`: permiso para usar todas las API de X-Ray, incluidos los permisos de lectura, los permisos de escritura y el permiso para configurar las claves de cifrado y las reglas de muestreo. Incluye el administrador de acceso a la observabilidad (OAM) `oam:ListSinks` y `oam:ListAttachedSinks` permisos que permiten a la consola ver los rastros compartidos desde las cuentas de origen como parte de la observabilidad entre cuentas. CloudWatch

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

```
                "oam:ListAttachedLinks"
            ],
            "Resource": "arn:aws:oam:*:*:sink/*"
        }
    ]
}
```

Para añadir una política administrada a un usuario, un grupo o un rol de IAM

1. Abra la consola de IAM.
2. Abra el rol asociado a su perfil de instancia, al usuario de IAM o al grupo de usuarios de IAM.
3. En Permissions (Permisos), asocia la política administrada.

Actualizaciones de X-Ray a las políticas AWS gestionadas

Consulta los detalles sobre las actualizaciones de las políticas AWS gestionadas de X-Ray desde que este servicio comenzó a rastrear estos cambios. Para obtener alertas automáticas sobre cambios en esta página, suscríbase a la fuente RSS en la página del historial de documentos de X-Ray.

Cambio	Descripción	Fecha
Políticas administradas por IAM para X-Ray: se agregaron nuevas políticas `AWSXrayCrossAccountSharingConfiguration` y se actualizaron las políticas `AWSXrayReadOnlyAccess` y `AWSXrayFullAccess`.	X-Ray agregó permisos de Observability Access Manager (OAM) `oam:ListSinks` y `oam:ListAttachedSinks` a estas políticas para permitir que la consola vea los rastros compartidos desde las cuentas de origen como parte de la observabilidad CloudWatch entre cuentas.	27 de noviembre de 2022
Políticas administradas por IAM para X-Ray: actualización de la política `AWSXrayReadOnlyAccess`.	X-Ray agregó una acción de API, `ListResourcePolicies`.	15 de noviembre de 2022

Cambio	Descripción	Fecha
Uso de la consola X-Ray: actualización de la política `AWSXrayReadOnlyAccess`	X-Ray agregó dos nuevas acciones de API `BatchGetTraceSummaryById` y `GetDistinctTraceGraphs`. Estas acciones API no se han diseñado para que se llamen desde el código. Por lo tanto, estas acciones de la API no están incluidas en los SDK ni en los SDK. AWS CLI AWS	11 de noviembre de 2022

Especificación de un recurso en una política de IAM

Puede controlar el acceso a los recursos a través de una política de IAM. Para las acciones que admiten permisos de nivel de recursos, se usa un nombre de recurso de Amazon (ARN) para identificar el recurso al que se aplica la política.

Es posible utilizar todas las acciones de X-Ray en una política de IAM para conceder o denegar permiso a los usuarios para utilizar esa acción. Sin embargo, no todas las acciones de X-Ray admiten permisos de nivel de recursos, que le permiten especificar los recursos en los que se puede realizar una acción.

Para las acciones que no admiten permisos de nivel de recursos, debe utilizar "*" como recurso.

Las siguientes acciones de X-Ray admiten permisos de nivel de recursos:

- `CreateGroup`
- `GetGroup`
- `UpdateGroup`
- `DeleteGroup`
- `CreateSamplingRule`
- `UpdateSamplingRule`

- `DeleteSamplingRule`

A continuación, se muestra un ejemplo de una política de permisos basada en identidad para una acción `CreateGroup`: El ejemplo muestra el uso de un ARN relacionado con el nombre de grupo `local-users` con el ID único como elemento comodín. El ID único se genera cuando se crea el grupo y, por lo tanto, no puede predecirse en la política con antelación. Cuando se utiliza `GetGroup`, `UpdateGroup` o `DeleteGroup`, puede definir esto como un elemento comodín o el ARN exacto, incluido el ID.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "xray:CreateGroup"
            ],
            "Resource": [
                "arn:aws:xray:eu-west-1:123456789012:group/local-users/*"
            ]
        }
    ]
}
```

A continuación, se muestra un ejemplo de una política de permisos basada en identidad para una acción `CreateSamplingRule`:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "xray:CreateSamplingRule"
            ],
            "Resource": [
                "arn:aws:xray:eu-west-1:123456789012:sampling-rule/base-scorekeep"
            ]
        }
    ]
```

```
}
```

> **Note**
>
> El ARN de una regla de muestreo se define por su nombre. A diferencia de los ARN de grupo, las reglas de muestreo no tienen un ID generado de manera inequívoca.

Solución de problemas de identidades y accesos en AWS X-Ray

Utilice la siguiente información para diagnosticar y solucionar los problemas comunes que puedan surgir cuando trabaje con X-Ray e IAM.

Temas

- No tengo autorización para realizar una acción en X-Ray.
- No tengo autorización para realizar la acción iam:PassRole
- Soy administrador y deseo permitir que otros obtengan acceso a X-Ray.
- Quiero permitir a personas externas a mi Cuenta de AWS el acceso a mis recursos de X-Ray.

No tengo autorización para realizar una acción en X-Ray.

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

En el siguiente ejemplo, el error se produce cuando el usuario de `mateojackson` intenta utilizar la consola para ver detalles sobre una regla de muestreo, pero no tiene permisos `xray:GetSamplingRules`.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to
 perform: xray:GetSamplingRules on resource: arn:${Partition}:xray:${Region}:
${Account}:sampling-rule/${SamplingRuleName}
```

En este caso, Mateo pide a su administrador que actualice sus políticas de forma que pueda obtener acceso al recurso de regla de muestreo mediante la acción `xray:GetSamplingRules`.

No tengo autorización para realizar la acción iam:PassRole

Si recibe un error que indica que no tiene autorización para realizar la acción `iam:PassRole`, las políticas deben actualizarse a fin de permitirle pasar un rol a X-Ray.

Algunos servicios de Servicios de AWS le permiten transferir un rol existente a dicho servicio en lugar de crear un nuevo rol de servicio o uno vinculado al servicio. Para ello, debe tener permisos para transferir el rol al servicio.

En el siguiente ejemplo, el error se produce cuando un usuario de IAM denominado `marymajor` intenta utilizar la consola para realizar una acción en X-Ray. Sin embargo, la acción requiere que el servicio cuente con permisos que otorga un rol de servicio. Mary no tiene permisos para transferir el rol al servicio.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

En este caso, las políticas de Mary se deben actualizar para permitirle realizar la acción `iam:PassRole`.

Si necesita ayuda, póngase en contacto con su administrador de AWS. El administrador es la persona que le proporcionó las credenciales de inicio de sesión.

Soy administrador y deseo permitir que otros obtengan acceso a X-Ray.

Para permitir que otros obtengan acceso a X-Ray, debe crear una entidad de IAM (usuario o rol) para la persona o la aplicación que necesita acceso. Esta persona utilizará las credenciales de la entidad para acceder a AWS. A continuación, debe adjuntar una política a la entidad que le conceda los permisos correctos en X-Ray.

Para comenzar de inmediato, consulte Creación del primer grupo y usuario delegado de IAM en la Guía del usuario de IAM.

Quiero permitir a personas externas a mi Cuenta de AWS el acceso a mis recursos de X-Ray.

Puede crear un rol que los usuarios de otras cuentas o las personas externas a la organización puedan utilizar para acceder a sus recursos. Puede especificar una persona de confianza para que asuma el rol. En el caso de los servicios que admitan las políticas basadas en recursos o las listas de

control de acceso (ACL), puede utilizar dichas políticas para conceder a las personas acceso a sus recursos.

Para obtener más información, consulte lo siguiente:

- Para obtener información acerca de si X-Ray admite estas características, consulte Cómo AWS X-Ray funciona con IAM.
- Para obtener información acerca de cómo proporcionar acceso a los recursos de las Cuentas de AWS de su propiedad, consulte Proporcionar acceso a un usuario de IAM a otra Cuenta de AWS de la que es propietario en la Guía del usuario de IAM.
- Para obtener información acerca de cómo proporcionar acceso a los recursos a Cuentas de AWS de terceros, consulte Proporcionar acceso a Cuentas de AWS que son propiedad de terceros en la Guía del usuario de IAM.
- Para obtener información sobre cómo proporcionar acceso mediante una identidad federada, consulte Proporcionar acceso a usuarios autenticados externamente (identidad federada) en la Guía del usuario de IAM.
- Para obtener información sobre la diferencia entre los roles y las políticas basadas en recursos para el acceso entre cuentas, consulte Cómo los roles de IAM difieren de las políticas basadas en recursos en la Guía del usuario de IAM.

Registro y monitoreo en AWS X-Ray

La monitorización es una parte importante del mantenimiento de la fiabilidad, la disponibilidad y el rendimiento de sus soluciones de AWS. Debe recopilar datos de supervisión de todas las partes de su solución de AWS para que pueda depurar un error multipunto de una forma más fácil si se produce. AWS proporciona varias herramientas para supervisar sus recursos de X-Ray y responder a posibles incidentes:

AWS CloudTrailRegistros de

> AWS X-Ray se integra con AWS CloudTrail para registrar las acciones de la API realizadas por un usuario, un rol o un servicio de AWS en X-Ray. Puede utilizar CloudTrail para supervisar las solicitudes de la API de X-Ray en tiempo real y almacenar registros en Amazon S3, Registros de Amazon CloudWatch y Eventos de Amazon CloudWatch. Para obtener más información, consulte Registro de llamadas a la API X-Ray con AWS CloudTrail.

Seguimiento de AWS Config

AWS X-Ray se integra en AWS Config para registrar cambios de configuración realizados en los recursos de cifrado de X-Ray. Puede utilizar AWS Config para realizar un inventario de recursos de cifrado de X-Ray, auditar el historial de configuración de X-Ray y enviar notificaciones basadas en los cambios de recursos. Para obtener más información, consulte Rastreo de los cambios en la configuración de cifrado de X-Ray con AWS Config.

Supervisión de Amazon CloudWatch

Puede usar el SDK de X-Ray para Java con el fin de publicar métricas de Amazon CloudWatch sin muestrear de los segmentos de X-Ray recopilados. Estas métricas se derivan de la hora de inicio y finalización del segmento, y los marcadores de estado limitado, fallo y error. Utilice estas métricas de seguimiento para exponer los reintentos y los problemas de dependencia con los subsegmentos. Para obtener más información, consulte AWS X-Ray métricas del X-Ray SDK para Java.

Validación de conformidad para AWS X-Ray

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

Puede descargar informes de auditoría de terceros utilizando AWS Artifact. Para obtener más información, consulte Descarga de informes en AWS Artifact .

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

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

> **Note**
>
> No Servicios de AWS todas cumplen con los requisitos de la HIPAA. Para más información, consulte la Referencia de servicios compatibles con HIPAA.

- AWS Recursos de de cumplimiento: esta colección de libros de trabajo y guías puede aplicarse a su industria y ubicación.
- AWS Guías de cumplimiento para clientes: comprenda el modelo de responsabilidad compartida desde el punto de vista del cumplimiento. Las guías resumen las mejores prácticas para garantizar la seguridad Servicios de AWS y orientan los controles de seguridad en varios marcos (incluidos el Instituto Nacional de Estándares y Tecnología (NIST), el Consejo de Normas de Seguridad del Sector de Tarjetas de Pago (PCI) y la Organización Internacional de Normalización (ISO)).
- Evaluación de los recursos con reglas en la guía para AWS Config desarrolladores: el AWS Config servicio evalúa en qué medida las configuraciones de los recursos cumplen con las prácticas internas, las directrices del sector y las normas.
- AWS Security Hub— Esto Servicio de AWS proporciona una visión completa del estado de su seguridad interior AWS. Security Hub utiliza controles de seguridad para evaluar sus recursos de AWS y comprobar su cumplimiento con los estándares y las prácticas recomendadas del sector de la seguridad. Para obtener una lista de los servicios y controles compatibles, consulte la Referencia de controles de Security Hub.
- AWS Audit Manager— Esto le Servicio de AWS ayuda a auditar continuamente su AWS consumo para simplificar la gestión del riesgo y el cumplimiento de las normativas y los estándares del sector.

Resiliencia en AWS X-Ray

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

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

Seguridad de la infraestructura en AWS X-Ray

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

Puede utilizar llamadas a API publicadas por AWS para acceder a X-Ray a través de la red. Los clientes deben admitir lo siguiente:

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

Además, las solicitudes deben estar firmadas mediante un ID de clave de acceso y una clave de acceso secreta que esté asociada a una entidad de seguridad de IAM. También puede utilizar AWS Security Token Service (AWS STS) para generar credenciales de seguridad temporales para firmar solicitudes.

Uso de AWS X-Ray con puntos de enlace de la VPC

Si utiliza Amazon Virtual Private Cloud (Amazon VPC) para alojar sus recursos de AWS, puede establecer una conexión privada entre su VPC y X-Ray. Eso habilitará recursos en su Amazon VPC para comunicarse con el servicio de X-Ray sin pasar por la Internet pública.

Amazon VPC es un Servicio de AWS que puede utilizar para lanzar recursos de AWS en una red virtual que usted defina. Con una VPC, puede controlar la configuración de la red, como el rango de direcciones IP, las subredes, las tablas de ruteo y las gateways de red. Para conectar una VPC a X-Ray, debe definir un punto de conexión de VPC de tipo interfaz. El punto de conexión ofrece conectividad escalable de confianza con X-Ray sin necesidad de utilizar una puerta de enlace de Internet, una instancia de traducción de direcciones de red (NAT) o una conexión de VPN. Para obtener más información, consulte What Is Amazon VPC (¿Qué es Amazon VPC?) en la Guía del usuario de Amazon VPC.

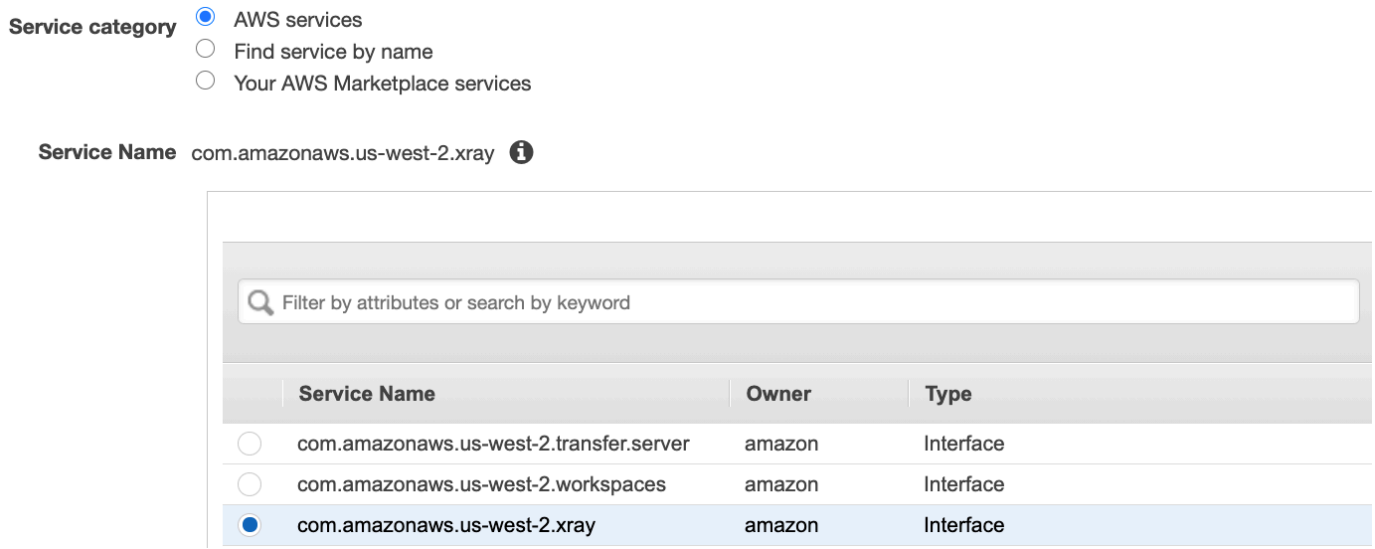
Los puntos de conexión de la VPC de tipo interfaz utilizan la tecnología de AWS PrivateLink, una tecnología de AWS que permite la comunicación privada entre los Servicios de AWS mediante una interfaz de red elástica con direcciones IP privadas. Para obtener más información, consulte la publicación del blog New – AWS PrivateLink for Servicios de AWS y Getting Started en la a Guía del usuario de Amazon VPC.

Para asegurarse de que puede crear un punto de conexión de VPC para X-Ray en la Región de AWS que usted desea, consulte Regiones admitidas.

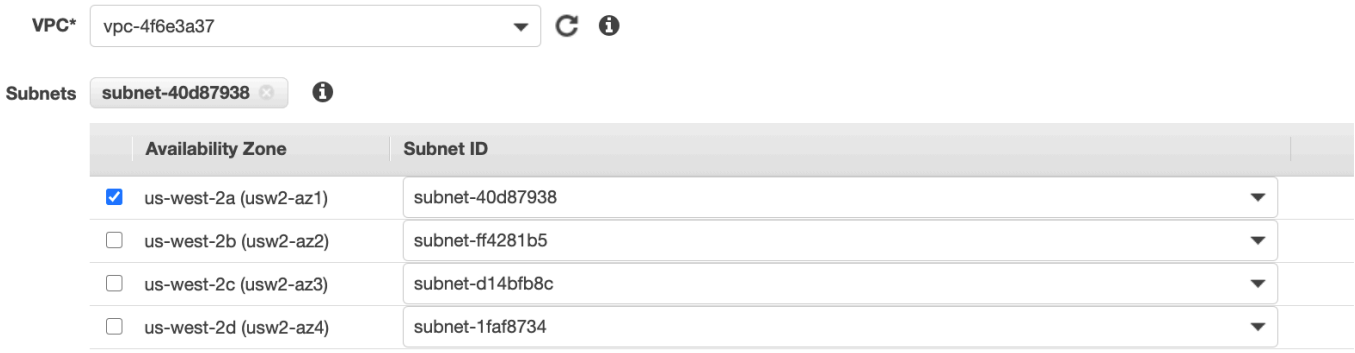
Creación de un punto de conexión de VPC para X-Ray

Para comenzar a utilizar X-Ray con su VPC, cree un punto de conexión de VPC de tipo interfaz para X-Ray.

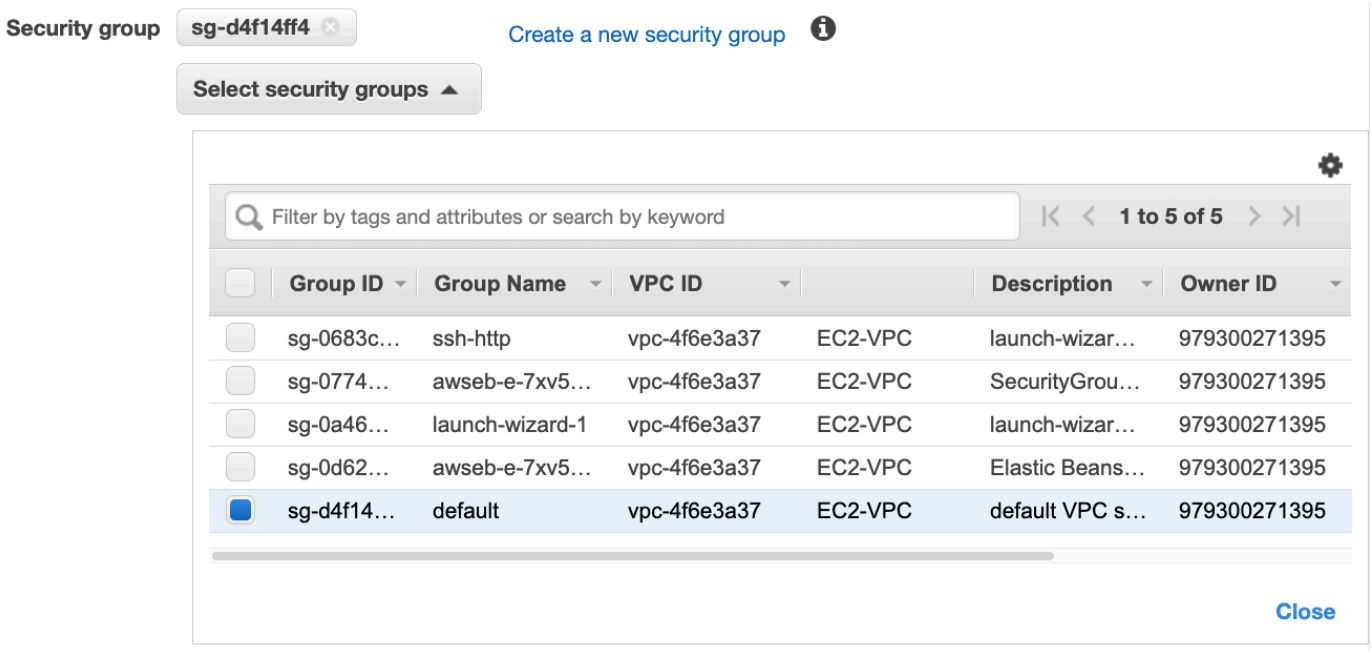
1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. Navegue hasta los puntos de conexión en el panel de navegación y seleccione Crear punto de conexión.
3. Busque y seleccione el nombre del servicio de AWS X-Ray: `com.amazonaws.region.xray`.



4. Seleccione la VPC que desee y, a continuación, seleccione una subred de la VPC para utilizar el punto de conexión de tipo interfaz. Se creará una interfaz de red de punto de conexión en la subred seleccionada. Puede especificar más de una subred en zonas de disponibilidad distintas (si el servicio lo admite) para asegurarse de que el punto de conexión de interfaz sea resistente a errores de zonas de disponibilidad. Si lo hace, se crea una interfaz de red en cada subred que especifique.



5. (Opcional) El DNS privado está habilitado de forma predeterminada para el punto de conexión, de modo que pueda realizar solicitudes a X-Ray mediante el nombre de host de DNS predeterminado. Si lo desea, puede deshabilitarlo.
6. Especificar los grupos de seguridad que se asociarán a la interfaz de red de punto de conexión.



7. (Opcional) Especifique una política personalizada para controlar los permisos de acceso al servicio de X-Ray. De forma predeterminada, se permite totalmente el acceso.

Control del acceso al punto de conexión de VPC de X-Ray

Una política de punto de conexión de VPC es una política de recursos de IAM que puede asociar a un punto de conexión cuando crea o modifica el punto de conexión. Si no adjunta una política al crear un punto de enlace, Amazon VPC adjunta una política predeterminada que le conceda acceso completo al servicio. Una política de punto de enlace no anula ni sustituye a las políticas de usuario

de IAM ni las políticas específicas del servicio. Se trata de una política independiente para controlar el acceso desde el punto de conexión al servicio especificado. Las políticas de punto de conexión deben escribirse en formato JSON. Para obtener más información, consulte Controlar el acceso a servicios con puntos de conexión de VPC en la Guía del usuario de Amazon VPC.

La política de puntos de conexión de VPC le permite controlar los permisos de varias acciones de X-Ray. Por ejemplo, puede crear una política para permitir solo PutTraceSegment y denegar el resto de las acciones. Eso restringe las cargas de trabajo y los servicios en la VPC para que solo se envíen datos de rastreo a X-Ray y se deniegue cualquier otra acción, como recuperar datos, cambiar la configuración de cifrado o crear o actualizar grupos.

A continuación, se muestra un ejemplo de una política de puntos de conexión de X-Ray. Esta política permite a los usuarios que se conectan a X-Ray través de la VPC enviar datos de segmentos a X-Ray y les impide realizar otras acciones de X-Ray.

```
{"Statement": [
    {"Sid": "Allow PutTraceSegments",
      "Principal": "*",
      "Action": [
        "xray:PutTraceSegments"
      ],
      "Effect": "Allow",
      "Resource": "*"
    }
  ]
}
```

Para editar la política de punto de conexión de VPC para X-Ray

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Puntos de conexión.
3. Si aún no ha creado el punto de conexión para X-Ray, siga los pasos descritos en Creación de un punto de conexión de VPC para X-Ray.
4. Seleccione el punto de conexión com.amazonaws.***region***.monitoring y, a continuación, elija la pestaña Política.
5. Elija Editar política y, a continuación, realice los cambios.

Regiones admitidas

Actualmente X-Ray admite puntos de conexión de la VPC en las siguientes regiones de Regiones de AWS:

- Este de EE. UU. (Ohio)
- EE.UU. Este (Norte de Virginia)
- EE.UU. Oeste (Norte de California)
- EE.UU. Oeste (Oregón)
- Africa (Cape Town)
- Asia Pacific (Hong Kong)
- Asia Pacific (Mumbai)
- Asia Pacific (Osaka)
- Asia Pacific (Seoul)
- Asia Pacífico (Singapur)
- Asia Pacífico (Sídney)
- Asia Pacífico (Tokio)
- Canada (Central)
- Europe (Frankfurt)
- Europa (Irlanda)
- Europa (Londres)
- Europa (Milán)
- Europe (Paris)
- Europe (Stockholm)
- Middle East (Bahrain)
- América del Sur (São Paulo)
- AWS GovCloud (Este de EE. UU.)
- AWS GovCloud (Oeste de EE. UU.)

AWS X-Ray API

La API de X-Ray proporciona acceso a todas las funciones de X-Ray a través del AWS SDK o directamente a través de HTTPS. AWS Command Line Interface La Referencia de la API de X-Ray documenta los parámetros de entrada de cada acción de la API, además de los campos y tipos de datos que devuelven.

Puede usar el AWS SDK para desarrollar programas que usen la API X-Ray. Tanto la consola X-Ray como el daemon X-Ray utilizan el AWS SDK para comunicarse con X-Ray. El AWS SDK de cada idioma tiene un documento de referencia para las clases y los métodos que se asignan a las acciones y los tipos de la API X-Ray.

AWS Referencias del SDK

- Java: AWS SDK for Java
- JavaScript – AWS SDK for JavaScript
- .NET: AWS SDK for .NET
- Ruby: AWS SDK for Ruby
- Go: AWS SDK para Go
- PHP: AWS SDK for PHP
- Python: AWS SDK for Python (Boto)

AWS Command Line Interface Es una herramienta de línea de comandos que utiliza el SDK para Python para llamar a AWS las API. Cuando estás aprendiendo una AWS API por primera vez, te AWS CLI proporciona una forma sencilla de explorar los parámetros disponibles y ver el resultado del servicio en formato JSON o de texto.

Consulta la referencia de AWS CLI comandos para obtener más información sobre los `aws xray` subcomandos.

Temas

- Uso de la API de AWS X-Ray con la CLI de AWS
- Envío de datos de seguimiento a AWS X-Ray
- Obtención de datos de AWS X-Ray

- Configuración de las opciones de muestreo, grupos y cifrado con la API de AWS X-Ray
- Using sampling rules with the X-Ray API (Uso de reglas de muestreo con la API de X-Ray)
- AWS X-Ray segmentar documentos

Uso de la API de AWS X-Ray con la CLI de AWS

La interfaz de línea de comandos (CLI) de AWS le permite acceder al servicio de X-Ray directamente y utilizar las mismas API que la consola de X-Ray utiliza para recuperar los gráficos de servicios y los datos de rastreo sin procesar. La aplicación de ejemplo incluye scripts que muestran cómo utilizar estas API con la CLI de AWS.

Requisitos previos

Este tutorial utiliza la aplicación de ejemplo Scorekeep e incluye scripts para generar datos de rastreo y un mapa de servicio. Siga las instrucciones en el tutorial de introducción para iniciar la aplicación.

Este tutorial utiliza la AWS CLI para mostrar el uso básico de la API de X-Ray. La CLI de AWS, disponible para Windows, Linux y OS-X, proporciona acceso de línea de comandos a las API públicas de todos los Servicios de AWS.

> **Note**
>
> Debe verificar que la AWS CLI esté configurada en la misma región en la que se creó la aplicación de ejemplo Scorekeep.

Los scripts incluidos para probar la aplicación de ejemplo utiliza `cURL` para enviar tráfico a la API y `jq` para analizar la salida. Puede descargar el ejecutable de `jq` desde stedolan.github.io y el ejecutable de `curl` desde https://curl.haxx.se/download.html. La mayoría de las instalaciones en Linux y OS X instalaciones incluyen cURL.

Generar datos de seguimiento

La aplicación web sigue funcionando para generar tráfico a la API cada pocos segundos mientras que la instalación está en curso, pero solo genera un tipo de solicitud. Utilice el script `test-api.sh` para ejecutar escenarios de un extremo a otro y generar datos de rastreo más diversos mientras prueba la API.

Para usar el script **`test-api.sh`**

1. Abra la consola de Elastic Beanstalk.
2. Desplácese hasta la consola de administración del entorno.
3. Copie la URL del entorno del encabezado de la página.
4. Abra el script `bin/test-api.sh` y reemplace el valor de la API con el URL del entorno.

```
#!/bin/bash
API=scorekeep.9hbtbm23t2.us-west-2.elasticbeanstalk.com/api
```

5. Ejecute el script para generar tráfico a la API.

```
~/debugger-tutorial$ ./bin/test-api.sh
Creating users,
session,
game,
configuring game,
playing game,
ending game,
game complete.
{"id":"MTBP8BAS","session":"HUF6IT64","name":"tic-tac-toe-test","users":
["QFF3HBGM","KL6JR98D"],"rules":"102","startTime":1476314241,"endTime":1476314245,"states":
["JQVLEOM2","D67QLPIC","VF9BM9NC","OEAA6GK9","2A705O73","1U2LFTLJ","HUKIDD70","BAN1C8FI","G
["BS8F8LQ","4MTTSPKP","463OETES","SVEBCL3N","N7CQ1GHP","O84ONEPD","EG4BPROQ","V4BLIDJ3","9R
```

Uso de la API de X-Ray

La CLI de AWS proporciona comandos para todas las acciones de API que X-Ray ofrece, incluidos los comandos `GetServiceGraph` y `GetTraceSummaries`. Consulte la Referencia de la API de AWS X-Ray para obtener más información acerca de todas las acciones admitidas y los tipos de datos que utilizan.

Example bin/service-graph.sh

```
EPOCH=$(date +%s)
aws xray get-service-graph --start-time $(($EPOCH-600)) --end-time $EPOCH
```

El script recupera un gráfico de servicios de los últimos 10 minutos.

```
~/eb-java-scorekeep$ ./bin/service-graph.sh | less
{
    "StartTime": 1479068648.0,
    "Services": [
        {
            "StartTime": 1479068648.0,
            "ReferenceId": 0,
            "State": "unknown",
            "EndTime": 1479068651.0,
            "Type": "client",
            "Edges": [
                {
                    "StartTime": 1479068648.0,
                    "ReferenceId": 1,
                    "SummaryStatistics": {
                        "ErrorStatistics": {
                            "ThrottleCount": 0,
                            "TotalCount": 0,
                            "OtherCount": 0
                        },
                        "FaultStatistics": {
                            "TotalCount": 0,
                            "OtherCount": 0
                        },
                        "TotalCount": 2,
                        "OkCount": 2,
                        "TotalResponseTime": 0.054000139236450195
                    },
                    "EndTime": 1479068651.0,
                    "Aliases": []
                }
            ]
        },
        {
            "StartTime": 1479068648.0,
            "Names": [
                "scorekeep.elasticbeanstalk.com"
            ],
            "ReferenceId": 1,
            "State": "active",
            "EndTime": 1479068651.0,
            "Root": true,
            "Name": "scorekeep.elasticbeanstalk.com",
```

```
...
```

Example bin/trace-urls.sh

```
EPOCH=$(date +%s)
aws xray get-trace-summaries --start-time $(($EPOCH-120)) --end-time $(($EPOCH-60)) --
query 'TraceSummaries[*].Http.HttpURL'
```

El script recupera las URL de rastros generados hace uno o dos minutos.

```
~/eb-java-scorekeep$ ./bin/trace-urls.sh
[
    "http://scorekeep.elasticbeanstalk.com/api/game/6Q0UE1DG/5FGLM9U3/
endtime/1479069438",
    "http://scorekeep.elasticbeanstalk.com/api/session/KH4341QH",
    "http://scorekeep.elasticbeanstalk.com/api/game/GLQBJ3K5/153AHDIA",
    "http://scorekeep.elasticbeanstalk.com/api/game/VPDL672J/G2V41HM6/
endtime/1479069466"
]
```

Example bin/full-traces.sh

```
EPOCH=$(date +%s)
TRACEIDS=$(aws xray get-trace-summaries --start-time $(($EPOCH-120)) --end-time
 $(($EPOCH-60)) --query 'TraceSummaries[*].Id' --output text)
aws xray batch-get-traces --trace-ids $TRACEIDS --query 'Traces[*]'
```

El script recupera los rastros completos generados hace uno o dos minutos.

```
~/eb-java-scorekeep$ ./bin/full-traces.sh | less
[
    {
        "Segments": [
            {
                "Id": "3f212bc237bafd5d",
                "Document": "{\"id\":\"3f212bc237bafd5d\",\"name\":\"DynamoDB\",
\"trace_id\":\"1-5828d9f2-a90669393f4343211bc1cf75\",\"start_time\":1.479072242459E9,
\"end_time\":1.479072242477E9,\"parent_id\":\"72a08dcf87991ca9\",\"http\":
{\"response\":{\"content_length\":60,\"status\":200}},\"inferred\":true,\"aws\":
{\"consistent_read\":false,\"table_name\":\"scorekeep-session-xray\",\"operation\":
\"GetItem\",\"request_id\":\"QAKE0S8DD0LJM245KAOPMA746BVV4KQNSO5AEMVJF66Q9ASUAAJG\",
\"resource_names\":[\"scorekeep-session-xray\"]},\"origin\":\"AWS::DynamoDB::Table\"}"
```

```
            },
            {
                "Id": "309e355f1148347f",
                "Document": "{\"id\":\"309e355f1148347f\",\"name\":\"DynamoDB\",
\"trace_id\":\"1-5828d9f2-a90669393f4343211bc1cf75\",\"start_time\":1.479072242477E9,
\"end_time\":1.479072242494E9,\"parent_id\":\"37f14ef837f00022\",\"http\":
{\"response\":{\"content_length\":606,\"status\":200}},\"inferred\":true,\"aws\":
{\"table_name\":\"scorekeep-game-xray\",\"operation\":\"UpdateItem\",\"request_id
\":\"388GEROC4PCA6D59ED3CTI5EEJVV4KQNSO5AEMVJF66Q9ASUAAJG\",\"resource_names\":
[\"scorekeep-game-xray\"]},\"origin\":\"AWS::DynamoDB::Table\"}"
            }
        ],
        "Id": "1-5828d9f2-a90669393f4343211bc1cf75",
        "Duration": 0.05099987983703613
    }
...
```


Limpieza

Finalice el entorno de Elastic Beanstalk para desactivar las instancias de Amazon EC2, las tablas de DynamoDB y otros recursos.

Para terminar su entorno de Elastic Beanstalk

1. Abra la consola de Elastic Beanstalk.
2. Desplácese hasta la consola de administración del entorno.
3. Elija Actions (Acciones).
4. Elija Terminate Environment (Terminar entorno).
5. Elija Terminate (Terminar).

Los datos de rastreo se eliminan automáticamente de X-Ray después de 30 días.

Envío de datos de seguimiento a AWS X-Ray

Puede enviar datos de rastreo a X-Ray en forma de documentos de segmento. Un documento de segmento es una cadena con formato JSON que contiene información sobre el trabajo que su aplicación realiza en respuesta a una solicitud. La aplicación puede registrar en segmentos los datos sobre el trabajo que realiza o bien registrar en subsegmentos los datos sobre el trabajo que utiliza servicios y recursos posteriores.

Los segmentos contienen información sobre el trabajo que realiza su aplicación. Un segmento, como mínimo, registra el tiempo empleado en una tarea, un nombre y dos ID. El ID de rastro permite controlar la solicitud mientras va de un servicio a otro. El ID de segmento permite controlar el trabajo que realiza un único servicio para la solicitud.

Example Segmento completo mínimo

```
{
  "name" : "Scorekeep",
  "id" : "70de5b6f19ff9a0a",
  "start_time" : 1.478293361271E9,
  "trace_id" : "1-581cf771-a006649127e371903a2de979",
  "end_time" : 1.478293361449E9
}
```

Cuando se recibe una solicitud, puede enviar un segmento en curso como marcador hasta que se complete la solicitud.

Example Segmento en curso

```
{
  "name" : "Scorekeep",
  "id" : "70de5b6f19ff9a0b",
  "start_time" : 1.478293361271E9,
  "trace_id" : "1-581cf771-a006649127e371903a2de979",
  “in_progress”: true
}
```

Puede enviar los segmentos a X-Ray directamente con `PutTraceSegments` o a través del daemon de X-Ray.

La mayoría de las aplicaciones llaman a otros servicios o acceden a los recursos con el AWS SDK. Registre información acerca de las llamadas posteriores en subsegmentos. X-Ray utiliza subsegmentos para identificar los servicios posteriores que no envían segmentos y crean entradas para segmentos en el gráfico de servicios.

Un subsegmento puede incrustarse en un documento de segmentos completos o enviarse por separado. Envíe subsegmentos por separado para realizar un rastreo asíncrono de las llamadas posteriores para realizar solicitudes de larga ejecución o para evitar superar el tamaño máximo del documento de segmentos (64 kB).

Example Subsegmento

Un subsegmento tiene un `type` de `subsegment` y una `parent_id` que identifica el segmento de origen.

```
{
  "name" : "www2.example.com",
  "id" : "70de5b6f19ff9a0c",
  "start_time" : 1.478293361271E9,
  "trace_id" : "1-581cf771-a006649127e371903a2de979"
  “end_time” : 1.478293361449E9,
  “type” : “subsegment”,
  “parent_id” : “70de5b6f19ff9a0b”
}
```

Para obtener más información acerca de los campos y valores que puede incluir en los segmentos y subsegmentos, consulte AWS X-Ray segmentar documentos.

Secciones

- Generación de identificadores de seguimiento
- ¿Usando PutTraceSegments
- Envío de documentos de segmento al daemon de X-Ray

Generación de identificadores de seguimiento

Para enviar datos a X-Ray, debe generar un identificador de rastreo único para cada solicitud.

Formato de identificación de trazas de rayos X

Un `trace_id` de X-Ray consta de tres números separados por guiones. Por ejemplo, `1-58406520-a006649127e371903a2de979`. Esto incluye:

- El número de versión, que es`1`.
- La hora de la solicitud original en Unix (época) con 8 dígitos hexadecimales.

  Por ejemplo, a las 10:00 a.m. del 1 de diciembre de 2016 (hora peninsular española), la hora de la época se expresa en `1480615200` segundos o `58406520` en dígitos hexadecimales.
- Un identificador de 96 bits único a nivel mundial para el rastreo en 24 dígitos hexadecimales.

> **Note**
>
> X-Ray ahora admite los ID de rastreo que se crean utilizando OpenTelemetry y cualquier otro marco que cumpla con la especificación Trace Context del W3C. Un identificador de rastreo del W3C debe estar formateado en formato de identificador de rastreo de rayos X cuando se envía a X-Ray. Por ejemplo, el identificador de rastreo del W3C `4efaaf4d1e8720b39541901950019ee5` debe tener el mismo formato que `1-4efaaf4d-1e8720b39541901950019ee5` cuando se envía a X-Ray. Los ID de rastreo de rayos X incluyen la marca de tiempo original de la solicitud en Unix epoch Time, pero esto no es obligatorio cuando se envían los ID de rastreo del W3C en formato X-Ray.

Puede escribir un script con el fin de generar ID de rastro para pruebas. A continuación se incluyen dos ejemplos.

Python

```
import time
import os
import binascii

START_TIME = time.time()
HEX=hex(int(START_TIME))[2:]
TRACE_ID="1-{}-{}".format(HEX, binascii.hexlify(os.urandom(12)).decode('utf-8'))
```

Bash

```
START_TIME=$(date +%s)
HEX_TIME=$(printf '%x\n' $START_TIME)
GUID=$(dd if=/dev/random bs=12 count=1 2>/dev/null | od -An -tx1 | tr -d ' \t\n')
TRACE_ID="1-$HEX_TIME-$GUID"
```

Consulte la aplicación de muestra de Scorekeep para scripts que crean ID de rastro y envían segmentos al daemon de X-Ray.

- Python: `xray_start.py`
- Bash: `xray_start.sh`

¿Usando PutTraceSegments

Puede cargar documentos de segmento con la API de `PutTraceSegments`. La API tiene un único parámetro, `TraceSegmentDocuments`, que obtiene una lista de documentos de segmento JSON.

Con la CLI de AWS, utilice el comando `aws xray put-trace-segments` para enviar documentos de segmento directamente a X-Ray.

```
$ DOC='{"trace_id": "1-5960082b-ab52431b496add878434aa25", "id": "6226467e3f845502",
 "start_time": 1498082657.37518, "end_time": 1498082695.4042, "name":
 "test.elasticbeanstalk.com"}'
$ aws xray put-trace-segments --trace-segment-documents "$DOC"
{
    "UnprocessedTraceSegments": []
}
```

> **Note**
>
> El procesador de comandos de Windows y Windows PowerShell tienen requisitos diferentes para citar y escapar de las comillas en las cadenas JSON. Consulte Entrecomillado de cadenas en la Guía del usuario de la AWS CLI para obtener más información.

En la salida se indican los segmentos que no se han procesado correctamente; por ejemplo, si la fecha del ID de rastro es demasiado antigua, verá un error como el siguiente.

```
{
    "UnprocessedTraceSegments": [
        {
            "ErrorCode": "InvalidTraceId",
            "Message": "Invalid segment. ErrorCode: InvalidTraceId",
            "Id": "6226467e3f845502"
        }
    ]
}
```

Puede transferir varios documentos de segmento al mismo tiempo, separados por espacios.

```
$ aws xray put-trace-segments --trace-segment-documents "$DOC1" "$DOC2"
```

Envío de documentos de segmento al daemon de X-Ray

En lugar de enviar documentos de segmento a la API de X-Ray, puede enviar segmentos y subsegmentos al daemon de X-Ray, que se encargará de almacenarlos en búfer y cargarlos en la API de X-Ray en lotes. El SDK de X-Ray envía documentos de segmento al daemon para evitar llamar directamente a AWS .

> **Note**
>
> Consulte Ejecución del daemon de X-Ray localmente para obtener instrucciones sobre cómo ejecutar el demonio.

Envíe el segmento en formato JSON a través del puerto UDP 2000, anteponiéndole el encabezado del demonio, `{"format": "json", "version": 1}\n`

```
{"format": "json", "version": 1}\n{"trace_id": "1-5759e988-bd862e3fe1be46a994272793",
 "id": "defdfd9912dc5a56", "start_time": 1461096053.37518, "end_time": 1461096053.4042,
 "name": "test.elasticbeanstalk.com"}
```

En Linux, puede enviar documentos de segmento al demonio desde un terminal Bash. Guarde el encabezado y el documento de segmento en un archivo de texto y envíelo a `/dev/udp` con `cat`.

```
$ cat segment.txt > /dev/udp/127.0.0.1/2000
```

Example segment.txt

```
{"format": "json", "version": 1}
{"trace_id": "1-594aed87-ad72e26896b3f9d3a27054bb", "id": "6226467e3f845502",
 "start_time": 1498082657.37518, "end_time": 1498082695.4042, "name":
 "test.elasticbeanstalk.com"}
```

Consulte el registro del daemon para comprobar que ha enviado el segmento a X-Ray.

```
2017-07-07T01:57:24Z [Debug] processor: sending partial batch
2017-07-07T01:57:24Z [Debug] processor: segment batch size: 1. capacity: 50
2017-07-07T01:57:24Z [Info] Successfully sent batch of 1 segments (0.020 seconds)
```

Obtención de datos de AWS X-Ray

AWS X-Ray procesa los datos de rastreo que le envías para generar rastreos completos, resúmenes de rastreo y gráficos de servicio en JSON. Puede recuperar los datos generados directamente de la API con la AWS CLI.

Secciones

Recuperación del gráfico de servicios

Puede utilizar la API de `GetServiceGraph` para recuperar el gráfico de servicios de JSON. La API requiere una hora de inicio y de finalización, que se puede calcular a partir de un terminal de Linux con el comando `date`.

```
$ date +%s
1499394617
```

`date +%s` imprime una fecha en cuestión de segundos. Utilice este número como hora de finalización y réstele el tiempo para obtener una hora de inicio.

Example Script para recuperar un gráfico de servicios de los últimos 10 minutos

```
EPOCH=$(date +%s)
aws xray get-service-graph --start-time $(($EPOCH-600)) --end-time $EPOCH
```

En el siguiente ejemplo, se muestra un gráfico de servicio con cuatro nodos que incluye un nodo cliente, una instancia de EC2, una tabla de DynamoDB y un tema de Amazon SNS.

Example GetServiceGraph salida

```
{
    "Services": [
        {
            "ReferenceId": 0,
```

```
            "Name": "xray-sample.elasticbeanstalk.com",
            "Names": [
                "xray-sample.elasticbeanstalk.com"
            ],
            "Type": "client",
            "State": "unknown",
            "StartTime": 1528317567.0,
            "EndTime": 1528317589.0,
            "Edges": [
                {
                    "ReferenceId": 2,
                    "StartTime": 1528317567.0,
                    "EndTime": 1528317589.0,
                    "SummaryStatistics": {
                        "OkCount": 3,
                        "ErrorStatistics": {
                            "ThrottleCount": 0,
                            "OtherCount": 1,
                            "TotalCount": 1
                        },
                        "FaultStatistics": {
                            "OtherCount": 0,
                            "TotalCount": 0
                        },
                        "TotalCount": 4,
                        "TotalResponseTime": 0.273
                    },
                    "ResponseTimeHistogram": [
                        {
                            "Value": 0.005,
                            "Count": 1
                        },
                        {
                            "Value": 0.015,
                            "Count": 1
                        },
                        {
                            "Value": 0.157,
                            "Count": 1
                        },
                        {
                            "Value": 0.096,
                            "Count": 1
                        }
```

```
                ],
                "Aliases": []
            }
        ]
    },
    {
        "ReferenceId": 1,
        "Name": "awseb-e-dixzws4s9p-stack-StartupSignupsTable-4IMSMHAYX2BA",
        "Names": [
            "awseb-e-dixzws4s9p-stack-StartupSignupsTable-4IMSMHAYX2BA"
        ],
        "Type": "AWS::DynamoDB::Table",
        "State": "unknown",
        "StartTime": 1528317583.0,
        "EndTime": 1528317589.0,
        "Edges": [],
        "SummaryStatistics": {
            "OkCount": 2,
            "ErrorStatistics": {
                "ThrottleCount": 0,
                "OtherCount": 0,
                "TotalCount": 0
            },
            "FaultStatistics": {
                "OtherCount": 0,
                "TotalCount": 0
            },
            "TotalCount": 2,
            "TotalResponseTime": 0.12
        },
        "DurationHistogram": [
            {
                "Value": 0.076,
                "Count": 1
            },
            {
                "Value": 0.044,
                "Count": 1
            }
        ],
        "ResponseTimeHistogram": [
            {
                "Value": 0.076,
                "Count": 1
```

```
                },
                {
                    "Value": 0.044,
                    "Count": 1
                }
            ]
        },
        {
            "ReferenceId": 2,
            "Name": "xray-sample.elasticbeanstalk.com",
            "Names": [
                "xray-sample.elasticbeanstalk.com"
            ],
            "Root": true,
            "Type": "AWS::EC2::Instance",
            "State": "active",
            "StartTime": 1528317567.0,
            "EndTime": 1528317589.0,
            "Edges": [
                {
                    "ReferenceId": 1,
                    "StartTime": 1528317567.0,
                    "EndTime": 1528317589.0,
                    "SummaryStatistics": {
                        "OkCount": 2,
                        "ErrorStatistics": {
                            "ThrottleCount": 0,
                            "OtherCount": 0,
                            "TotalCount": 0
                        },
                        "FaultStatistics": {
                            "OtherCount": 0,
                            "TotalCount": 0
                        },
                        "TotalCount": 2,
                        "TotalResponseTime": 0.12
                    },
                    "ResponseTimeHistogram": [
                        {
                            "Value": 0.076,
                            "Count": 1
                        },
                        {
                            "Value": 0.044,
```

```
                        "Count": 1
                    }
                ],
                "Aliases": []
            },
            {
                "ReferenceId": 3,
                "StartTime": 1528317567.0,
                "EndTime": 1528317589.0,
                "SummaryStatistics": {
                    "OkCount": 2,
                    "ErrorStatistics": {
                        "ThrottleCount": 0,
                        "OtherCount": 0,
                        "TotalCount": 0
                    },
                    "FaultStatistics": {
                        "OtherCount": 0,
                        "TotalCount": 0
                    },
                    "TotalCount": 2,
                    "TotalResponseTime": 0.125
                },
                "ResponseTimeHistogram": [
                    {
                        "Value": 0.049,
                        "Count": 1
                    },
                    {
                        "Value": 0.076,
                        "Count": 1
                    }
                ],
                "Aliases": []
            }
        ],
        "SummaryStatistics": {
            "OkCount": 3,
            "ErrorStatistics": {
                "ThrottleCount": 0,
                "OtherCount": 1,
                "TotalCount": 1
            },
            "FaultStatistics": {
```

```
                    "OtherCount": 0,
                    "TotalCount": 0
                },
                "TotalCount": 4,
                "TotalResponseTime": 0.273
            },
            "DurationHistogram": [
                {
                    "Value": 0.005,
                    "Count": 1
                },
                {
                    "Value": 0.015,
                    "Count": 1
                },
                {
                    "Value": 0.157,
                    "Count": 1
                },
                {
                    "Value": 0.096,
                    "Count": 1
                }
            ],
            "ResponseTimeHistogram": [
                {
                    "Value": 0.005,
                    "Count": 1
                },
                {
                    "Value": 0.015,
                    "Count": 1
                },
                {
                    "Value": 0.157,
                    "Count": 1
                },
                {
                    "Value": 0.096,
                    "Count": 1
                }
            ]
        },
        {
```

```
            "ReferenceId": 3,
            "Name": "SNS",
            "Names": [
                "SNS"
            ],
            "Type": "AWS::SNS",
            "State": "unknown",
            "StartTime": 1528317583.0,
            "EndTime": 1528317589.0,
            "Edges": [],
            "SummaryStatistics": {
                "OkCount": 2,
                "ErrorStatistics": {
                    "ThrottleCount": 0,
                    "OtherCount": 0,
                    "TotalCount": 0
                },
                "FaultStatistics": {
                    "OtherCount": 0,
                    "TotalCount": 0
                },
                "TotalCount": 2,
                "TotalResponseTime": 0.125
            },
            "DurationHistogram": [
                {
                    "Value": 0.049,
                    "Count": 1
                },
                {
                    "Value": 0.076,
                    "Count": 1
                }
            ],
            "ResponseTimeHistogram": [
                {
                    "Value": 0.049,
                    "Count": 1
                },
                {
                    "Value": 0.076,
                    "Count": 1
                }
            ]
```

```
        }
    ]
}
```

Recuperación del gráfico de servicios por grupo

Para obtener un gráfico de servicios en función del contenido de un grupo, incluya un `groupName` o `groupARN`. En el ejemplo siguiente, se muestra una llamada a un gráfico de servicios para un grupo denominado Example1.

Example Script para recuperar un gráfico de servicios por nombre para el grupo Example1

```
aws xray get-service-graph --group-name "Example1"
```

Recuperación de registros de seguimiento

Puede utilizar la API de `GetTraceSummaries` para obtener una lista de resúmenes de registros de seguimiento. Estos resúmenes incluyen información que puede utilizar para identificar los registros de seguimiento que desee descargar en su totalidad, y que incluyen anotaciones, información de solicitud y respuesta e identificadores.

Existen dos indicadores `TimeRangeType` disponibles al llamar `aws xray get-trace-summaries`:

- TraceId— La `GetTraceSummaries` búsqueda por defecto utiliza el tiempo de TraceID y devuelve los rastreos iniciados dentro del rango calculado`[start_time, end_time)`. Este rango de marcas de tiempo se calcula en función de la codificación de la marca de tiempo dentro del TraceId, o se puede definir manualmente.
- Hora del evento: para buscar eventos a medida que ocurren a lo largo del tiempo, AWS X-Ray permite buscar registros de seguimiento mediante marcas de tiempo de eventos. El tiempo de evento devuelve registros de seguimiento activos durante el intervalo `[start_time, end_time)`, independientemente del cuándo se inició el seguimiento.

Utilice el comando `aws xray get-trace-summaries` para obtener una lista de resúmenes de registros de seguimiento. Los siguientes comandos obtienen una lista de resúmenes de trazas de entre 1 y 2 minutos anteriores utilizando la hora predeterminada. TraceId

Example Script para obtener resúmenes de rastreo

```
EPOCH=$(date +%s)
aws xray get-trace-summaries --start-time $(($EPOCH-120)) --end-time $(($EPOCH-60))
```

Example GetTraceSummaries salida

```
{
    "TraceSummaries": [
        {
            "HasError": false,
            "Http": {
                "HttpStatus": 200,
                "ClientIp": "205.255.255.183",
                "HttpURL": "http://scorekeep.elasticbeanstalk.com/api/session",
                "UserAgent": "Mozilla/5.0 (Windows NT 6.1; Win64; x64)
 AppleWebKit/537.36 (KHTML, like Gecko) Chrome/59.0.3071.115 Safari/537.36",
                "HttpMethod": "POST"
            },
            "Users": [],
            "HasFault": false,
            "Annotations": {},
            "ResponseTime": 0.084,
            "Duration": 0.084,
            "Id": "1-59602606-a43a1ac52fc7ee0eea12a82c",
            "HasThrottle": false
        },
        {
            "HasError": false,
            "Http": {
                "HttpStatus": 200,
                "ClientIp": "205.255.255.183",
                "HttpURL": "http://scorekeep.elasticbeanstalk.com/api/user",
                "UserAgent": "Mozilla/5.0 (Windows NT 6.1; Win64; x64)
 AppleWebKit/537.36 (KHTML, like Gecko) Chrome/59.0.3071.115 Safari/537.36",
                "HttpMethod": "POST"
            },
            "Users": [
                {
                    "UserName": "5M388M1E"
                }
            ],
            "HasFault": false,
```

```
            "Annotations": {
                "UserID": [
                    {
                        "AnnotationValue": {
                            "StringValue": "5M388M1E"
                        }
                    }
                ],
                "Name": [
                    {
                        "AnnotationValue": {
                            "StringValue": "Ola"
                        }
                    }
                ]
            },
            "ResponseTime": 3.232,
            "Duration": 3.232,
            "Id": "1-59602603-23fc5b688855d396af79b496",
            "HasThrottle": false
        }
    ],
    "ApproximateTime": 1499473304.0,
    "TracesProcessedCount": 2
}
```

Utilice el ID de registro de seguimiento del resultado para recuperar un registro de seguimiento completo con la API de `BatchGetTraces`.

Example BatchGetTraces comando

```
$ aws xray batch-get-traces --trace-ids 1-596025b4-7170afe49f7aa708b1dd4a6b
```

Example BatchGetTraces salida

```
{
    "Traces": [
        {
            "Duration": 3.232,
            "Segments": [
                {
                    "Document": "{\"id\":\"1fb07842d944e714\",\"name\":
\"random-name\",\"start_time\":1.499473411677E9,\"end_time\":1.499473414572E9,
```

\"parent_id\":\"0c544c1b1bbff948\",\"http\":{\"response\":{\"status\":200}},
\"aws\":{\"request_id\":\"ac086670-6373-11e7-a174-f31b3397f190\"},\"trace_id\":
\"1-59602603-23fc5b688855d396af79b496\",\"origin\":\"AWS::Lambda\",\"resource_arn\":
\"arn:aws:lambda:us-west-2:123456789012:function:random-name\"}",
                    "Id": "1fb07842d944e714"
                },
                {
                    "Document": "{\"id\":\"194fcc8747581230\",\"name\":\"Scorekeep
\",\"start_time\":1.499473411562E9,\"end_time\":1.499473414794E9,\"http\":{\"request
\":{\"url\":\"http://scorekeep.elasticbeanstalk.com/api/user\",\"method\":\"POST\",
\"user_agent\":\"Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML,
 like Gecko) Chrome/59.0.3071.115 Safari/537.36\",\"client_ip\":\"205.251.233.183\"},
\"response\":{\"status\":200}},\"aws\":{\"elastic_beanstalk\":{\"version_label\":\"app-
abb9-170708_002045\",\"deployment_id\":406,\"environment_name\":\"scorekeep-dev\"},
\"ec2\":{\"availability_zone\":\"us-west-2c\",\"instance_id\":\"i-0cd9e448944061b4a
\"},\"xray\":{\"sdk_version\":\"1.1.2\",\"sdk\":\"X-Ray for Java\"}},\"service
\":{},\"trace_id\":\"1-59602603-23fc5b688855d396af79b496\",\"user\":\"5M388M1E
\",\"origin\":\"AWS::ElasticBeanstalk::Environment\",\"subsegments\":[{\"id\":
\"0c544c1b1bbff948\",\"name\":\"Lambda\",\"start_time\":1.499473411629E9,\"end_time
\":1.499473414572E9,\"http\":{\"response\":{\"status\":200,\"content_length\":14}},
\"aws\":{\"log_type\":\"None\",\"status_code\":200,\"function_name\":\"random-name
\",\"invocation_type\":\"RequestResponse\",\"operation\":\"Invoke\",\"request_id
\":\"ac086670-6373-11e7-a174-f31b3397f190\",\"resource_names\":[\"random-name\"]},
\"namespace\":\"aws\"},{\"id\":\"071684f2e555e571\",\"name\":\"## UserModel.saveUser
\",\"start_time\":1.499473414581E9,\"end_time\":1.499473414769E9,\"metadata\":{\"debug
\":{\"test\":\"Metadata string from UserModel.saveUser\"}},\"subsegments\":[{\"id\":
\"4cd3f10b76c624b4\",\"name\":\"DynamoDB\",\"start_time\":1.49947341469E9,\"end_time
\":1.499473414769E9,\"http\":{\"response\":{\"status\":200,\"content_length\":57}},
\"aws\":{\"table_name\":\"scorekeep-user\",\"operation\":\"UpdateItem\",\"request_id
\":\"MFQ8CGJ3JTDDVVVASUAAJGQ6NJ82F738BOB4KQNSO5AEMVJF66Q9\",\"resource_names\":
[\"scorekeep-user\"]},\"namespace\":\"aws\"}]}]}",
                    "Id": "194fcc8747581230"
                },
                {
                    "Document": "{\"id\":\"00f91aa01f4984fd\",\"name\":
\"random-name\",\"start_time\":1.49947341283E9,\"end_time\":1.49947341457E9,
\"parent_id\":\"1fb07842d944e714\",\"aws\":{\"function_arn\":\"arn:aws:lambda:us-
west-2:123456789012:function:random-name\",\"resource_names\":[\"random-name\"],
\"account_id\":\"123456789012\"},\"trace_id\":\"1-59602603-23fc5b688855d396af79b496\",
\"origin\":\"AWS::Lambda::Function\",\"subsegments\":[{\"id\":\"e6d2fe619f827804\",
\"name\":\"annotations\",\"start_time\":1.499473413012E9,\"end_time\":1.499473413069E9,
\"annotations\":{\"UserID\":\"5M388M1E\",\"Name\":\"Ola\"}},{\"id\":\"b29b548af4d54a0f
\",\"name\":\"SNS\",\"start_time\":1.499473413112E9,\"end_time\":1.499473414071E9,
\"http\":{\"response\":{\"status\":200}},\"aws\":{\"operation\":\"Publish\",

```
\"region\":\"us-west-2\",\"request_id\":\"a2137970-f6fc-5029-83e8-28aadeb99198\",
\"retries\":0,\"topic_arn\":\"arn:aws:sns:us-west-2:123456789012:awseb-e-
ruag3jyweb-stack-NotificationTopic-6B829NT9V5O9\"},\"namespace\":\"aws\"},{\"id\":
\"2279c0030c955e52\",\"name\":\"Initialization\",\"start_time\":1.499473412064E9,
\"end_time\":1.499473412819E9,\"aws\":{\"function_arn\":\"arn:aws:lambda:us-
west-2:123456789012:function:random-name\"}}]}",
                    "Id": "00f91aa01f4984fd"
                },
                {
                    "Document": "{\"id\":\"17ba309b32c7fbaf\",\"name\":
\"DynamoDB\",\"start_time\":1.49947341469E9,\"end_time\":1.499473414769E9,
\"parent_id\":\"4cd3f10b76c624b4\",\"inferred\":true,\"http\":{\"response
\":{\"status\":200,\"content_length\":57}},\"aws\":{\"table_name
\":\"scorekeep-user\",\"operation\":\"UpdateItem\",\"request_id\":
\"MFQ8CGJ3JTDDVVVASUAAJGQ6NJ82F738BOB4KQNSO5AEMVJF66Q9\",\"resource_names\":
[\"scorekeep-user\"]},\"trace_id\":\"1-59602603-23fc5b688855d396af79b496\",\"origin\":
\"AWS::DynamoDB::Table\"}",
                    "Id": "17ba309b32c7fbaf"
                },
                {
                    "Document": "{\"id\":\"1ee3c4a523f89ca5\",\"name\":\"SNS
\",\"start_time\":1.499473413112E9,\"end_time\":1.499473414071E9,\"parent_id\":
\"b29b548af4d54a0f\",\"inferred\":true,\"http\":{\"response\":{\"status\":200}},\"aws
\":{\"operation\":\"Publish\",\"region\":\"us-west-2\",\"request_id\":\"a2137970-
f6fc-5029-83e8-28aadeb99198\",\"retries\":0,\"topic_arn\":\"arn:aws:sns:us-
west-2:123456789012:awseb-e-ruag3jyweb-stack-NotificationTopic-6B829NT9V5O9\"},
\"trace_id\":\"1-59602603-23fc5b688855d396af79b496\",\"origin\":\"AWS::SNS\"}",
                    "Id": "1ee3c4a523f89ca5"
                }
            ],
            "Id": "1-59602603-23fc5b688855d396af79b496"
        }
    ],
    "UnprocessedTraceIds": []
}
```


El registro de seguimiento completo incluye un documento para cada segmento, compilado a partir de todos los documentos de segmento recibidos que tienen el mismo ID de registro de seguimiento. Estos documentos no representan los datos tal y como la aplicación se los envió a X-Ray, sino que representan los documentos procesados generados por el servicio de X-Ray. X-Ray crea el documento de rastreo completo compilando los documentos de segmento que envía la aplicación, y eliminando los datos que no se ajustan al esquema de documentos de segmento.

X-Ray también crea segmentos inferidos para las llamadas posteriores a los servicios que no envían los segmentos propiamente dichos. Por ejemplo, si llama a DynamoDB con un cliente instrumentado, el SDK de X-Ray registra un subsegmento con detalles sobre la llamada desde su punto de vista, pero no envía el segmento correspondiente. X-Ray usa la información del subsegmento para crear un segmento inferido que represente el recurso de DynamoDB en el mapa de rastreo y lo agrega al documento de rastreo.

Para obtener varios registros de seguimiento desde la API, se necesita una lista de ID de registros de seguimiento, que se puede extraer de la salida de `get-trace-summaries` con una consulta de la AWS CLI. Redirija la lista a la entrada de `batch-get-traces` para obtener registros de seguimiento completos de un período específico.

Example Script para obtener registros de seguimiento completos de un período de un minuto

```
EPOCH=$(date +%s)
TRACEIDS=$(aws xray get-trace-summaries --start-time $(($EPOCH-120)) --end-time
 $(($EPOCH-60)) --query 'TraceSummaries[*].Id' --output text)
aws xray batch-get-traces --trace-ids $TRACEIDS --query 'Traces[*]'
```

Recuperación y ajuste de las causas raíz de Analytics

Al generar un resumen de rastreo con la GetTraceSummaries API, los resúmenes de rastreo parciales se pueden reutilizar en su formato JSON para crear una expresión de filtro refinada basada en las causas fundamentales. Consulte los ejemplos que aparecen a continuación para ver el procedimiento de ajuste.

Example Ejemplo GetTraceSummaries de salida: sección de causa raíz del tiempo de respuesta

```
{
  "Services": [
    {
      "Name": "GetWeatherData",
      "Names": ["GetWeatherData"],
      "AccountId": 123456789012,
      "Type": null,
      "Inferred": false,
      "EntityPath": [
        {
          "Name": "GetWeatherData",
          "Coverage": 1.0,
```

```
          'Remote": false
        },
        {
          "Name": "get_temperature",
          "Coverage": 0.8,
          "Remote": false
        }
      ]
    },
    {
      "Name": "GetTemperature",
      "Names": ["GetTemperature"],
      "AccountId": 123456789012,
      "Type": null,
      "Inferred": false,
      "EntityPath": [
        {
          "Name": "GetTemperature",
          "Coverage": 0.7,
          "Remote": false
        }
      ]
    }
  ]
}
```

Al editar y crear omisiones en la salida anterior, este JSON puede actuar de filtor para las entidades de causa raíz coincidentes. Para cada campo presente en el JSON, todas las coincidencias candidatas deben ser exactas o no se devolverá el registro de seguimiento. Los campos eliminados se convierten en valores comodín, un formato que es compatible con la estructura de consultas de expresión de filtro.

Example Causa raíz de tiempo de respuesta reformateado

```
{
  "Services": [
    {
      "Name": "GetWeatherData",
      "EntityPath": [
        {
          "Name": "GetWeatherData"
        },
        {
```

```
          "Name": "get_temperature"
        }
      ]
    },
    {
      "Name": "GetTemperature",
      "EntityPath": [
        {
          "Name": "GetTemperature"
        }
      ]
    }
  ]
}
```

Este JSON se utiliza como parte de una expresión de filtro a través de una llamada a `rootcause.json = #[{}]`. Consulte el capítulo Expresiones de filtro para obtener más información sobre cómo ejecutar consultas con expresiones de filtro.

Example Ejemplo de filtro JSON

```
rootcause.json = #[{ "Services": [ { "Name": "GetWeatherData", "EntityPath": [{ "Name":
 "GetWeatherData" }, { "Name": "get_temperature" } ] }, { "Name": "GetTemperature",
 "EntityPath": [ { "Name": "GetTemperature" } ] } ] }]
```

Configuración de las opciones de muestreo, grupos y cifrado con la API de AWS X-Ray

AWS X-Ray dispone de varias API para configurar las reglas de muestreo, las reglas de grupos y la configuración de cifrado.

Secciones

- Configuración de cifrado
- Reglas de muestreo
- Grupos

Configuración de cifrado

Se usa PutEncryptionConfig para especificar una clave de AWS Key Management Service (AWS KMS) que se usará para el cifrado.

> **Note**
>
> X-Ray no es compatible con claves de KMS asimétricas.

```
$ aws xray put-encryption-config --type KMS --key-id alias/aws/xray
{
    "EncryptionConfig": {
        "KeyId": "arn:aws:kms:us-east-2:123456789012:key/c234g4e8-39e9-4gb0-84e2-
b0ea215cbba5",
        "Status": "UPDATING",
        "Type": "KMS"
    }
}
```

Para el ID de clave, puede utilizar un alias (tal y como se muestra en el ejemplo), un ID de clave o un nombre de recurso de Amazon (ARN).

Utilice GetEncryptionConfig para obtener la configuración actual. Cuando X-Ray termina de aplicar la configuración, el estado cambia de UPDATING a ACTIVE.

```
$ aws xray get-encryption-config
{
    "EncryptionConfig": {
        "KeyId": "arn:aws:kms:us-east-2:123456789012:key/c234g4e8-39e9-4gb0-84e2-
b0ea215cbba5",
        "Status": "ACTIVE",
        "Type": "KMS"
    }
}
```

Para dejar de usar una clave de KMS y utilizar el cifrado predeterminado, establezca el tipo de cifrado en NONE.

```
$ aws xray put-encryption-config --type NONE
{
```

```
    "EncryptionConfig": {
        "Status": "UPDATING",
        "Type": "NONE"
    }
}
```

Reglas de muestreo

Puede administrar las reglas de muestreo en su cuenta con la API de X-Ray. Para obtener más información acerca de cómo añadir y administrar etiquetas, consulte Etiquetado de reglas de muestreo y grupos de X-Ray.

Obtener todas las reglas de muestreo con `GetSamplingRules`.

```
$ aws xray get-sampling-rules
{
    "SamplingRuleRecords": [
        {
            "SamplingRule": {
                "RuleName": "Default",
                "RuleARN": "arn:aws:xray:us-east-2:123456789012:sampling-rule/Default",
                "ResourceARN": "*",
                "Priority": 10000,
                "FixedRate": 0.05,
                "ReservoirSize": 1,
                "ServiceName": "*",
                "ServiceType": "*",
                "Host": "*",
                "HTTPMethod": "*",
                "URLPath": "*",
                "Version": 1,
                "Attributes": {}
            },
            "CreatedAt": 0.0,
            "ModifiedAt": 1529959993.0
        }
    ]
}
```

La regla predeterminada se aplica a todas las solicitudes que no coinciden con otra regla. Es la regla con prioridad más baja y no se puede eliminar. Sin embargo, puede cambiar el porcentaje y el tamaño de depósito con `UpdateSamplingRule`.

Example Entrada de la API para **UpdateSamplingRule** – 10000-default.json

```
{
    "SamplingRuleUpdate": {
        "RuleName": "Default",
        "FixedRate": 0.01,
        "ReservoirSize": 0
    }
}
```

En el siguiente ejemplo se utiliza el archivo anterior como entrada para cambiar la regla predeterminada a uno por ciento sin depósito. Las etiquetas son opcionales. Si decide añadir etiquetas, tenga en cuenta que le hará falta una clave de etiqueta y que los valores de etiqueta son opcionales. Para eliminar etiquetas existentes de una regla de muestreo, utilice UntagResource.

```
$ aws xray update-sampling-rule --cli-input-json file://1000-default.json --tags
 [{"Key": "key_name","Value": "value"},{"Key": "key_name","Value": "value"}]
{
    "SamplingRuleRecords": [
        {
            "SamplingRule": {
                "RuleName": "Default",
                "RuleARN": "arn:aws:xray:us-east-2:123456789012:sampling-rule/Default",
                "ResourceARN": "*",
                "Priority": 10000,
                "FixedRate": 0.01,
                "ReservoirSize": 0,
                "ServiceName": "*",
                "ServiceType": "*",
                "Host": "*",
                "HTTPMethod": "*",
                "URLPath": "*",
                "Version": 1,
                "Attributes": {}
            },
            "CreatedAt": 0.0,
            "ModifiedAt": 1529959993.0
        },
```

Crear reglas de muestreo adicionales con `CreateSamplingRule`. Al crear una regla, la mayoría de los campos de la regla son obligatorios. En el siguiente ejemplo se crean dos reglas. Esta primera

regla establece un porcentaje de base para la aplicación de ejemplo Scorekeep. Empareja todas las solicitudes servidas por la API que no coinciden con una regla de prioridad superior.

Example Entrada de la API para **UpdateSamplingRule** – 9000-base-scorekeep.json

```
{
    "SamplingRule": {
        "RuleName": "base-scorekeep",
        "ResourceARN": "*",
        "Priority": 9000,
        "FixedRate": 0.1,
        "ReservoirSize": 5,
        "ServiceName": "Scorekeep",
        "ServiceType": "*",
        "Host": "*",
        "HTTPMethod": "*",
        "URLPath": "*",
        "Version": 1
    }
}
```

La segunda regla también se aplica a Scorekeep, pero tiene una prioridad mayor y es más específica. Esta regla establece un porcentaje de muestreo muy bajo para las solicitudes de sondeo. Estas son las solicitudes GET realizadas por el cliente cada pocos segundos para comprobar si hay cambios en el estado del juego.

Example Entrada de la API para **UpdateSamplingRule** – 5000-polling-scorekeep.json

```
{
    "SamplingRule": {
        "RuleName": "polling-scorekeep",
        "ResourceARN": "*",
        "Priority": 5000,
        "FixedRate": 0.003,
        "ReservoirSize": 0,
        "ServiceName": "Scorekeep",
        "ServiceType": "*",
        "Host": "*",
        "HTTPMethod": "GET",
        "URLPath": "/api/state/*",
        "Version": 1
    }
```

```
}
```

Las etiquetas son opcionales. Si decide añadir etiquetas, tenga en cuenta que le hará falta una clave de etiqueta y que los valores de etiqueta son opcionales.

```
$ aws xray create-sampling-rule --cli-input-json file://5000-polling-scorekeep.json --
tags [{"Key": "key_name","Value": "value"},{"Key": "key_name","Value": "value"}]
{
    "SamplingRuleRecord": {
        "SamplingRule": {
            "RuleName": "polling-scorekeep",
            "RuleARN": "arn:aws:xray:us-east-1:123456789012:sampling-rule/polling-
scorekeep",
            "ResourceARN": "*",
            "Priority": 5000,
            "FixedRate": 0.003,
            "ReservoirSize": 0,
            "ServiceName": "Scorekeep",
            "ServiceType": "*",
            "Host": "*",
            "HTTPMethod": "GET",
            "URLPath": "/api/state/*",
            "Version": 1,
            "Attributes": {}
        },
        "CreatedAt": 1530574399.0,
        "ModifiedAt": 1530574399.0
    }
}
$ aws xray create-sampling-rule --cli-input-json file://9000-base-scorekeep.json
{
    "SamplingRuleRecord": {
        "SamplingRule": {
            "RuleName": "base-scorekeep",
            "RuleARN": "arn:aws:xray:us-east-1:123456789012:sampling-rule/base-
scorekeep",
            "ResourceARN": "*",
            "Priority": 9000,
            "FixedRate": 0.1,
            "ReservoirSize": 5,
            "ServiceName": "Scorekeep",
            "ServiceType": "*",
            "Host": "*",
```

```
            "HTTPMethod": "*",
            "URLPath": "*",
            "Version": 1,
            "Attributes": {}
        },
        "CreatedAt": 1530574410.0,
        "ModifiedAt": 1530574410.0
    }
}
```

Para eliminar una regla de muestreo, utilice `DeleteSamplingRule`.

```
$ aws xray delete-sampling-rule --rule-name polling-scorekeep
{
    "SamplingRuleRecord": {
        "SamplingRule": {
            "RuleName": "polling-scorekeep",
            "RuleARN": "arn:aws:xray:us-east-1:123456789012:sampling-rule/polling-
scorekeep",
            "ResourceARN": "*",
            "Priority": 5000,
            "FixedRate": 0.003,
            "ReservoirSize": 0,
            "ServiceName": "Scorekeep",
            "ServiceType": "*",
            "Host": "*",
            "HTTPMethod": "GET",
            "URLPath": "/api/state/*",
            "Version": 1,
            "Attributes": {}
        },
        "CreatedAt": 1530574399.0,
        "ModifiedAt": 1530574399.0
    }
}
```

Grupos

Puede utilizar la API de X-Ray para administrar los grupos de su cuenta. Los grupos son una colección de registros de seguimiento que se definen mediante una expresión de filtro. Puede utilizar grupos para generar gráficos de servicios adicionales y suministrar métricas de Amazon CloudWatch. Consulte Obtención de datos de AWS X-Ray para obtener más detalles sobre cómo utilizar las

métricas y los gráficos de servicios mediante la API de X-Ray. Para obtener más información acerca de los grupos, consulte Configuración de grupos. Para obtener más información acerca de cómo añadir y administrar etiquetas, consulte Etiquetado de reglas de muestreo y grupos de X-Ray.

Utilice `CreateGroup` para crear un grupo. Las etiquetas son opcionales. Si decide añadir etiquetas, tenga en cuenta que le hará falta una clave de etiqueta y que los valores de etiqueta son opcionales.

```
$ aws xray create-group --group-name "TestGroup" --filter-expression
 "service(\"example.com\") {fault}" --tags [{"Key": "key_name","Value": "value"},
{"Key": "key_name","Value": "value"}]
{
    "GroupName": "TestGroup",
    "GroupARN": "arn:aws:xray:us-east-2:123456789012:group/TestGroup/UniqueID",
    "FilterExpression": "service(\"example.com\") {fault OR error}"
}
```

Utilice `GetGroups` para obtener todos los grupos existentes.

```
$ aws xray get-groups
{
    "Groups": [
        {
            "GroupName": "TestGroup",
            "GroupARN": "arn:aws:xray:us-east-2:123456789012:group/TestGroup/UniqueID",
            "FilterExpression": "service(\"example.com\") {fault OR error}"
        },
  {
            "GroupName": "TestGroup2",
            "GroupARN": "arn:aws:xray:us-east-2:123456789012:group/TestGroup2/
UniqueID",
            "FilterExpression": "responsetime > 2"
        }
    ],
 "NextToken": "tokenstring"
}
```

Utilice `UpdateGroup` para actualizar un grupo. Las etiquetas son opcionales. Si decide añadir etiquetas, tenga en cuenta que le hará falta una clave de etiqueta y que los valores de etiqueta son opcionales. Para eliminar etiquetas existentes de un grupo, utilice UntagResource.

```
$ aws xray update-group --group-name "TestGroup" --group-arn "arn:aws:xray:us-
east-2:123456789012:group/TestGroup/UniqueID" --filter-expression
```

```
 "service(\"example.com\") {fault OR error}" --tags [{"Key": "Stage","Value": "Prod"},
{"Key": "Department","Value": "QA"}]
{
    "GroupName": "TestGroup",
    "GroupARN": "arn:aws:xray:us-east-2:123456789012:group/TestGroup/UniqueID",
    "FilterExpression": "service(\"example.com\") {fault OR error}"
}
```

Utilice `DeleteGroup` para eliminar un grupo.

```
$ aws xray delete-group --group-name "TestGroup" --group-arn "arn:aws:xray:us-
east-2:123456789012:group/TestGroup/UniqueID"
    {
    }
```

Using sampling rules with the X-Ray API (Uso de reglas de muestreo con la API de X-Ray)

El SDK de AWS X-Ray utiliza la API de X-Ray para obtener reglas de muestreo, notificar resultados de muestreo y obtener las cuotas. Puede utilizar estas API para entender mejor cómo funcionan las reglas de muestreo o para implementar muestras en un lenguaje que el SDK de X-Ray no admita.

Comience por obtener todas las reglas de muestreo con `GetSamplingRules`.

```
$ aws xray get-sampling-rules
{
    "SamplingRuleRecords": [
        {
            "SamplingRule": {
                "RuleName": "Default",
                "RuleARN": "arn:aws:xray:us-east-1::sampling-rule/Default",
                "ResourceARN": "*",
                "Priority": 10000,
                "FixedRate": 0.01,
                "ReservoirSize": 0,
                "ServiceName": "*",
                "ServiceType": "*",
                "Host": "*",
                "HTTPMethod": "*",
                "URLPath": "*",
```

```
                "Version": 1,
                "Attributes": {}
            },
            "CreatedAt": 0.0,
            "ModifiedAt": 1530558121.0
        },
        {
            "SamplingRule": {
                "RuleName": "base-scorekeep",
                "RuleARN": "arn:aws:xray:us-east-1::sampling-rule/base-scorekeep",
                "ResourceARN": "*",
                "Priority": 9000,
                "FixedRate": 0.1,
                "ReservoirSize": 2,
                "ServiceName": "Scorekeep",
                "ServiceType": "*",
                "Host": "*",
                "HTTPMethod": "*",
                "URLPath": "*",
                "Version": 1,
                "Attributes": {}
            },
            "CreatedAt": 1530573954.0,
            "ModifiedAt": 1530920505.0
        },
        {
            "SamplingRule": {
                "RuleName": "polling-scorekeep",
                "RuleARN": "arn:aws:xray:us-east-1::sampling-rule/polling-scorekeep",
                "ResourceARN": "*",
                "Priority": 5000,
                "FixedRate": 0.003,
                "ReservoirSize": 0,
                "ServiceName": "Scorekeep",
                "ServiceType": "*",
                "Host": "*",
                "HTTPMethod": "GET",
                "URLPath": "/api/state/*",
                "Version": 1,
                "Attributes": {}
            },
            "CreatedAt": 1530918163.0,
            "ModifiedAt": 1530918163.0
        }
```

```
    ]
}
```

El resultado incluye la regla predeterminada y las reglas personalizadas. Consulte Reglas de muestreo si aún no ha creado reglas de muestreo.

Evalúe las reglas frente a las solicitudes entrantes en orden de prioridad ascendente. Cuando una regla coincida, utilice el porcentaje fijo y el tamaño de depósito para tomar una decisión de muestreo. Registre solicitudes muestreadas y pase por alto (para fines de rastreo) las solicitudes sin muestrear. Deje de evaluar las reglas cuando tome una decisión de muestreo.

El tamaño de un depósito de reglas es el número objetivo de rastreos que registrar por segundo antes de aplicar el porcentaje fijo. El depósito se aplica en todos los servicios acumulativamente, por lo que no se puede utilizar directamente. Sin embargo, si es distinto de cero, podrá tomar prestado un rastreo por segundo desde el depósito hasta que X-Ray asigne una cuota. Antes de recibir una cuota, registre la primera solicitud cada segundo y aplique el porcentaje fijo a las solicitudes adicionales. El porcentaje fijo es un número decimal entre 0 y 1,00 (100 %).

El siguiente ejemplo muestra una llamada a `GetSamplingTargets` con información detallada sobre las decisiones de muestreo tomadas durante los últimos 10 segundos.

```
$ aws xray get-sampling-targets --sampling-statistics-documents '[
    {
        "RuleName": "base-scorekeep",
        "ClientID": "ABCDEF1234567890ABCDEF10",
        "Timestamp": "2018-07-07T00:20:06",
        "RequestCount": 110,
        "SampledCount": 20,
        "BorrowCount": 10
    },
    {
        "RuleName": "polling-scorekeep",
        "ClientID": "ABCDEF1234567890ABCDEF10",
        "Timestamp": "2018-07-07T00:20:06",
        "RequestCount": 10500,
        "SampledCount": 31,
        "BorrowCount": 0
    }
]'
{
```

```
    "SamplingTargetDocuments": [
        {
            "RuleName": "base-scorekeep",
            "FixedRate": 0.1,
            "ReservoirQuota": 2,
            "ReservoirQuotaTTL": 1530923107.0,
            "Interval": 10
        },
        {
            "RuleName": "polling-scorekeep",
            "FixedRate": 0.003,
            "ReservoirQuota": 0,
            "ReservoirQuotaTTL": 1530923107.0,
            "Interval": 10
        }
    ],
    "LastRuleModification": 1530920505.0,
    "UnprocessedStatistics": []
}
```

La respuesta de X-Ray incluye una cuota que utilizar en lugar de tomarla prestada del depósito. En este ejemplo, el servicio ha tomado prestados 10 rastros desde el depósito en 10 segundos y ha aplicado el porcentaje fijo del 10 por ciento a las otras 100 solicitudes, lo que se traduce en un total de 20 solicitudes muestreadas. La cuota es buena durante cinco minutos (que se indica mediante el tiempo de vida) o hasta que se asigna una nueva cuota. X-Ray también podría asignar un intervalo de informes más largo que el predeterminado, aunque no aquí.

> **Note**
>
> La respuesta de X-Ray podría no incluir una cuota la primera vez que llama. Continue tomando prestado del depósito hasta que se les asigne una cuota.

Los otros dos campos de la respuesta podrían indicar problemas con la entrada. Compruebe `LastRuleModification` respecto a la última vez que llamó a `GetSamplingRules`. Si es más reciente, obtenga una nueva copia de las reglas. `UnprocessedStatistics` puede incluir errores que indican que una regla se ha eliminado, que el documento de estadísticas en la entrada era demasiado antiguo o errores de permisos.

AWS X-Ray segmentar documentos

Un segmento de rastreo es una representación JSON de una solicitud que atiende su aplicación. Un segmento de rastreo registra información sobre la solicitud original, información sobre el trabajo que la aplicación realiza localmente y subsegmentos con información sobre las llamadas posteriores que la aplicación realiza a AWS los recursos, las API HTTP y las bases de datos SQL.

Un documento de segmento transmite información sobre un segmento a X-Ray. Un documento de segmento puede tener un tamaño de hasta 64 kB y contener un segmento completo con subsegmentos, un fragmento de un segmento que indique que una solicitud está en curso o un único subsegmento que se envía por separado. Puede enviar documentos de segmento directamente a X-Ray mediante la API de `PutTraceSegments`.

X-Ray compila y procesa los documentos de segmento para generar resúmenes de rastros y rastros completos que admiten consultas a los que puede obtener acceso mediante las API de `GetTraceSummaries` y `BatchGetTraces`, respectivamente. Además de los segmentos y subsegmentos que envía a X-Ray, el servicio utiliza la información de los subsegmentos para generar segmentos inferidos, que se añaden al rastro completo. Los segmentos inferidos representan los servicios y recursos posteriores en el mapa de rastreo.

X-Ray proporciona un esquema JSON para los documentos de segmento. Puede descargar el esquema aquí: xray-segmentdocument-schema-v 1.0.0. Los campos y objetos incluidos en el esquema se describen con más detalle en las secciones siguientes.

X-Ray indexa un subconjunto de los campos de segmento para su uso con expresiones de filtro. Por ejemplo, si establece el campo `user` de un segmento en un identificador único, puede buscar los segmentos asociados a usuarios específicos en la consola de X-Ray o mediante la API de `GetTraceSummaries`. Para obtener más información, consulte Uso de expresiones de filtro.

Cuando instrumente su aplicación con el SDK de X-Ray, el SDK generará automáticamente los documentos de segmento. En lugar de enviar documentos directamente a X-Ray, el SDK los transmite a través de un puerto UDP local al daemon de X-Ray. Para obtener más información, consulte Envío de documentos de segmento al daemon de X-Ray.

Secciones

- Annotations
- Metadatos
- AWS datos de recursos
- Errores y excepciones
- Consultas SQL

Campos de segmentos

Un segmento registra información de rastreo sobre una solicitud que atiende su aplicación. Como mínimo, un segmento registra el nombre, ID, hora de inicio, ID de rastro y el tiempo total de la solicitud.

Example Segmento completo mínimo

```
{
  "name" : "example.com",
  "id" : "70de5b6f19ff9a0a",
  "start_time" : 1.478293361271E9,
  "trace_id" : "1-581cf771-a006649127e371903a2de979",
  "end_time" : 1.478293361449E9
}
```

Los siguientes campos son obligatorios o necesarios en determinadas circunstancias para los segmentos.

> **Note**
>
> Los valores deben ser cadenas (de hasta 250 caracteres), a menos que se indique lo contrario.

Campos de segmentos obligatorios

- `name`: nombre lógico del servicio que gestiona la solicitud (hasta 200 caracteres). Por ejemplo, el nombre de su aplicación o el nombre de dominio. Los nombres pueden contener letras Unicode, números y espacios en blanco, así como los siguientes símbolos: `_`, `.`, `:`, `/`, `%`, `&`, `#`, `=`, `+`, `\`, `-`, `@`
- `id`: un identificador de 64 bits para el segmento, único entre otros segmentos del mismo rastro, en 16 dígitos hexadecimales.

- `trace_id`: un identificador único que conecta todos los segmentos y subsegmentos procedentes de una única solicitud de cliente.

  Formato de identificación de trazas de rayos X

  Un `trace_id` de X-Ray consta de tres números separados por guiones. Por ejemplo, `1-58406520-a006649127e371903a2de979`. Esto incluye:

  - El número de versión, que es`1`.
  - La hora de la solicitud original en Unix (época) con 8 dígitos hexadecimales.

    Por ejemplo, a las 10:00 a. m. del 1 de diciembre de 2016 (hora peninsular española) se indica en `1480615200` segundos o `58406520` en dígitos hexadecimales.
  - Un identificador de 96 bits único a nivel mundial para el rastreo en 24 dígitos hexadecimales.

  > **Note**
  >
  > X-Ray ahora admite los ID de rastreo que se crean utilizando OpenTelemetry y cualquier otro marco que cumpla con la especificación Trace Context del W3C. Un identificador de rastreo del W3C debe estar formateado en formato de identificador de rastreo de rayos X cuando se envía a X-Ray. Por ejemplo, el identificador de rastreo del W3C `4efaaf4d1e8720b39541901950019ee5` debe tener el mismo formato que `1-4efaaf4d-1e8720b39541901950019ee5` cuando se envía a X-Ray. Los ID de rastreo de rayos X incluyen la marca de tiempo original de la solicitud en Unix epoch Time, pero esto no es obligatorio cuando se envían los ID de rastreo del W3C en formato X-Ray.

  > **Seguridad de ID de rastro**
  >
  > Los ID de rastro se pueden ver en los encabezados de respuesta. Genere ID de rastro con algoritmo aleatorio seguro para garantizar que los atacantes no puedan calcular futuros ID de rastro y enviar solicitudes con esos ID a su aplicación.

- `start_time`: número que representa el momento en que se creó el segmento, en segundos de punto flotante en formato de tiempo Unix. Por ejemplo, `1480615200.010` o `1.480615200010E9`. Use tantos decimales como necesite. Se recomienda una precisión de microsegundos cuando sea posible.

- `end_time`: número que representa el momento en que se cerró el segmento. Por ejemplo, `1480615200.090` o `1.480615200090E9`. Especifique un `end_time` o `in_progress`.
- `in_progress`: booleano que se establece en `true` en lugar de especificar un `end_time` para registrar que se inició un subsegmento pero que no se completó. Envíe un segmento en curso cuando su aplicación reciba una solicitud que llevará tiempo atender, para rastrear la recepción de la solicitud. Cuando la respuesta se envía, envíe el segmento completo para sobrescribir el segmento en curso. Envíe solo un segmento completo o uno o cero segmentos en curso por solicitud.

> **Nombres de servicio**
>
> El `name` de un segmento debe coincidir con el nombre de dominio o el nombre lógico del servicio que genere el segmento. Sin embargo, este requisito no se exige. Cualquier aplicación que tenga permiso para `PutTraceSegments` puede enviar segmentos con cualquier nombre.

Los siguientes campos son opcionales para los segmentos.

Campos de segmentos opcionales

- `service`: un objeto con información sobre su aplicación.
  - `version`: una cadena que identifica la versión de la aplicación que atiende la solicitud.
- `user`: una cadena que identifica el usuario que envía la solicitud.
- `origin`— El tipo de AWS recurso que ejecuta la aplicación.

  Valores admitidos

  - `AWS::EC2::Instance`: una instancia de Amazon EC2.
  - `AWS::ECS::Container`: un contenedor de Amazon ECS.
  - `AWS::ElasticBeanstalk::Environment`: un entorno de Elastic Beanstalk

  Si hay varios valores que sean aplicables a su aplicación, utilice el que sea más específico. Por ejemplo, supongamos que un Docker multicontenedor en Elastic Beanstalk ejecuta su aplicación en un contenedor de Amazon ECS que, a su vez, se ejecuta en una instancia de Amazon EC2. En este caso, el origen se establecería en `AWS::ElasticBeanstalk::Environment`, puesto que es el elemento principal de los otros dos recursos.

- `parent_id`: un ID de subsegmento que especifica si la solicitud se originó desde una aplicación instrumentada. El SDK de X-Ray añade el ID del subsegmento principal al encabezado de rastreo para las llamadas HTTP posteriores. En el caso de subsegmentos anidados, un subsegmento puede tener un segmento o un subsegmento como padre.
- `http`: objetos `http` con información sobre la solicitud HTTP original.
- `aws`— `aws`objeto con información sobre el AWS recurso en el que la aplicación atendió la solicitud.
- `error`, `throttle`, `fault` y `cause`: campos de error que indican que se ha producido un error y que incluyen información sobre la excepción que ha causado el error.
- `annotations`: objeto `annotations` con pares de clave-valor que X-Ray debe indexar para las búsquedas.
- `metadata`: objeto `metadata` con los datos adicionales que desea almacenar en el segmento.
- `subsegments`: matriz de objetos `subsegment`.

Subsegmentos

Puedes crear subsegmentos para registrar las llamadas Servicios de AWS y los recursos que realices con el AWS SDK, las llamadas a las API web HTTP internas o externas o las consultas a bases de datos SQL. También puede crear subsegmentos para depurar o anotar bloques de código en su aplicación. Los subsegmentos pueden contener otros subsegmentos, por lo que un subsegmento personalizado que registre los metadatos de una llamada a una función interna puede contener otros subsegmentos personalizados y subsegmentos para llamadas posteriores.

Un subsegmento registra una llamada posterior desde el punto de vista del servicio que llama. X-Ray utiliza subsegmentos para identificar los servicios posteriores que no envían segmentos y crean entradas para segmentos en el gráfico de servicios.

Un subsegmento puede incrustarse en un documento de segmentos completos o enviarse por separado. Envíe subsegmentos por separado para realizar un rastreo asíncrono de las llamadas posteriores para realizar solicitudes de larga ejecución o para evitar superar el tamaño máximo del documento de segmentos.

Example Segmento con un subsegmento incrustado

Un subsegmento independiente tiene un `type` de `subsegment` y un `parent_id` que identifica el segmento principal.

```
{
```

```
  "trace_id"   : "1-5759e988-bd862e3fe1be46a994272793",
  "id"         : "defdfd9912dc5a56",
  "start_time" : 1461096053.37518,
  "end_time"   : 1461096053.4042,
  "name"       : "www.example.com",
  "http"       : {
    "request"  : {
      "url"        : "https://www.example.com/health",
      "method"     : "GET",
      "user_agent" : "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6)
 AppleWebKit/601.7.7",
      "client_ip"  : "11.0.3.111"
    },
    "response" : {
      "status"         : 200,
      "content_length" : 86
    }
  },
  "subsegments" : [
    {
      "id"         : "53995c3f42cd8ad8",
      "name"       : "api.example.com",
      "start_time" : 1461096053.37769,
      "end_time"   : 1461096053.40379,
      "namespace"  : "remote",
      "http"       : {
        "request"  : {
          "url"    : "https://api.example.com/health",
          "method" : "POST",
          "traced" : true
        },
        "response" : {
          "status"         : 200,
          "content_length" : 861
        }
      }
    }
  ]
}
```

En el caso de las solicitudes de larga ejecución, puede enviar un segmento en curso para notificar a X-Ray que la solicitud se ha recibido y, a continuación, enviar por separado los subsegmentos para que se rastreen antes de que se complete la solicitud original.

Example Segmento en curso

```
{
  "name" : "example.com",
  "id" : "70de5b6f19ff9a0b",
  "start_time" : 1.478293361271E9,
  "trace_id" : "1-581cf771-a006649127e371903a2de979",
  "in_progress": true
}
```

Example Subsegmentos independientes

Un subsegmento independiente tiene un `type` de `subsegment`, un `trace_id` y un `parent_id` que identifica el segmento principal.

```
{
  "name" : "api.example.com",
  "id" : "53995c3f42cd8ad8",
  "start_time" : 1.478293361271E9,
  "end_time" : 1.478293361449E9,
  "type" : "subsegment",
  "trace_id" : "1-581cf771-a006649127e371903a2de979"
  "parent_id" : "defdfd9912dc5a56",
  "namespace"  : "remote",
  "http"       : {
      "request"  : {
          "url"    : "https://api.example.com/health",
          "method" : "POST",
          "traced" : true
      },
      "response" : {
          "status"         : 200,
          "content_length" : 861
      }
  }
}
```

Cuando se complete la solicitud, cierre el segmento reenviándolo con un `end_time`. El segmento completo sobrescribe el segmento en curso.

También puede enviar subsegmentos por separado para solicitudes realizadas que activen flujos de trabajo asíncronos. Por ejemplo, una API web puede devolver una respuesta `OK 200`

inmediatamente antes de iniciar el trabajo que el usuario ha solicitado. Puede enviar un segmento completo a X-Ray en cuanto se envíe la respuesta, seguido de subsegmentos para el trabajo realizado más adelante. Al igual que con los segmentos, también puede enviar un fragmento de un subsegmento para registrar que el subsegmento se ha iniciado y, a continuación, sobrescribirlo con un subsegmento completo una vez que se haya completado la llamada posterior.

Los siguientes campos son obligatorios o necesarios en determinadas circunstancias para los subsegmentos.

> **Note**
>
> Los valores son cadenas (de hasta 250 caracteres), a menos que se indique lo contrario.

Campos de subsegmentos obligatorios

- `id`: un identificador de 64 bits para el subsegmento, único entre otros segmentos del mismo rastro, en 16 dígitos hexadecimales.
- `name`: nombre lógico del subsegmento. En el caso de las llamadas posteriores, asigne un nombre al subsegmento detrás del recurso o servicio llamado. Para los subsegmentos personalizados, asigne el nombre al subsegmento detrás del código que lo instrumenta (por ejemplo, un nombre de función).
- `start_time`: número que representa el momento en que se creó el subsegmento, en segundos de punto flotante en tiempo Unix, con una precisión de milisegundos. Por ejemplo, `1480615200.010` o `1.480615200010E9`.
- `end_time`: número que representa el momento en que se cerró el subsegmento. Por ejemplo, `1480615200.090` o `1.480615200090E9`. Especifique un valor para `end_time` o `in_progress`.
- `in_progress`: booleano que se establece en `true` en lugar de especificar un `end_time` para registrar que se inició un subsegmento pero que no se completó. Envíe solo un subsegmento completo y uno o cero subsegmentos en curso por solicitud posterior.
- `trace_id`: ID de rastro del segmento principal del subsegmento. Solo es necesario si el envío del subsegmento se realiza por separado.

Formato de identificación de trazas de rayos X

Un `trace_id` de X-Ray consta de tres números separados por guiones. Por ejemplo, `1-58406520-a006649127e371903a2de979`. Esto incluye:

- El número de versión, que es `1`.
- La hora de la solicitud original en Unix (época) con 8 dígitos hexadecimales.

  Por ejemplo, a las 10:00 a. m. del 1 de diciembre de 2016 (hora peninsular española) se indica en `1480615200` segundos o `58406520` en dígitos hexadecimales.
- Un identificador de 96 bits único a nivel mundial para el rastreo en 24 dígitos hexadecimales.

> **Note**
>
> X-Ray ahora admite los ID de rastreo que se crean utilizando OpenTelemetry y cualquier otro marco que cumpla con la especificación Trace Context del W3C. Un identificador de rastreo del W3C debe estar formateado en formato de identificador de rastreo de rayos X cuando se envía a X-Ray. Por ejemplo, el identificador de rastreo del W3C `4efaaf4d1e8720b39541901950019ee5` debe tener el mismo formato que `1-4efaaf4d-1e8720b39541901950019ee5` cuando se envía a X-Ray. Los ID de rastreo de rayos X incluyen la marca de tiempo original de la solicitud en Unix epoch Time, pero esto no es obligatorio cuando se envían los ID de rastreo del W3C en formato X-Ray.

- `parent_id`: ID del segmento principal del subsegmento. Solo es necesario si el envío del subsegmento se realiza por separado. En el caso de subsegmentos anidados, un subsegmento puede tener un segmento o un subsegmento como padre.
- `type` – `subsegment`. Solo es necesario si el envío del subsegmento se realiza por separado.

Los siguientes campos son opcionales para los subsegmentos.

Campos de subsegmentos opcionales

- `namespace`: `aws` para las llamadas al SDK de AWS; `remote` para las demás llamadas posteriores.
- `http`: objeto `http` con información sobre una llamada HTTP saliente.
- `aws`— `aws`objeto con información sobre el AWS recurso descendente al que ha llamado la aplicación.

- `error`, `throttle`, `fault` y `cause`: campos de error que indican que se ha producido un error y que incluyen información sobre la excepción que ha causado el error.
- `annotations`: objeto `annotations` con pares de clave-valor que X-Ray debe indexar para las búsquedas.
- `metadata`: objeto `metadata` con los datos adicionales que desea almacenar en el segmento.
- `subsegments`: matriz de objetos `subsegment`.
- `precursor_ids`: matriz de identificadores de subsegmento que identifica los subsegmentos con el mismo segmento principal que se completó antes de este subsegmento.

Datos de solicitudes HTTP

Utilice un bloque HTTP para registrar los detalles de una solicitud HTTP que ha atendido su aplicación (en un segmento) o que ha realizado la aplicación en una API HTTP posterior (en un subsegmento). La mayoría de los campos de este objeto se asignan a la información proporcionada en una solicitud y respuesta HTTP.

`http`

Todos los campos son opcionales.

- `request`: información sobre una solicitud.
  - `method`: el método de solicitud. Por ejemplo, `GET`.
  - `url`: la dirección URL completa, obtenida del protocolo, nombre de host y ruta de la solicitud.
  - `user_agent`: la cadena de agente de usuario del cliente del solicitante.
  - `client_ip`: la dirección IP del solicitante. Se puede recuperar del `Source Address` del paquete de direcciones IP o, en el caso de las solicitudes reenviadas, de un encabezado `X-Forwarded-For`.
  - `x_forwarded_for`: (solo segmentos) booleano que indica que se ha leído el `client_ip` desde un encabezado `X-Forwarded-For` y no es fiable, ya que podría haberse falsificado.
  - `traced`: (solo subsegmentos) booleano que indica que la llamada posterior es a otro servicio rastreado. Si este campo está establecido en `true`, X-Ray considera que el rastro se debe dividir hasta que el servicio posterior cargue el segmento con un `parent_id` que coincida con el `id` del subsegmento que contiene este bloque.
- `response`: información sobre una respuesta.
  - `status`: entero que indica el estado HTTP de la respuesta.

- `content_length`: entero que indica la longitud del cuerpo de la respuesta en bytes.

Cuando instrumente una llamada a una API web posterior, este campo registra un subsegmento con información sobre la solicitud HTTP y la respuesta. X-Ray utiliza el subsegmento para generar un segmento inferido de la API remota.

Example Segmento para las llamadas HTTP atendidas por una aplicación en ejecución en Amazon EC2

```
{
  "id": "6b55dcc497934f1a",
  "start_time": 1484789387.126,
  "end_time": 1484789387.535,
  "trace_id": "1-5880168b-fd5158284b67678a3bb5a78c",
  "name": "www.example.com",
  "origin": "AWS::EC2::Instance",
  "aws": {
    "ec2": {
      "availability_zone": "us-west-2c",
      "instance_id": "i-0b5a4678fc325bg98"
    },
    "xray": {
        "sdk_version": "2.11.0 for Java"
    },
  },
  "http": {
    "request": {
      "method": "POST",
      "client_ip": "78.255.233.48",
      "url": "http://www.example.com/api/user",
      "user_agent": "Mozilla/5.0 (Windows NT 6.1; WOW64; rv:45.0) Gecko/20100101
 Firefox/45.0",
      "x_forwarded_for": true
    },
    "response": {
      "status": 200
    }
  }
```

Example Subsegmento para una llamada HTTP posterior

```
{
```

```
  "id": "004f72be19cddc2a",
  "start_time": 1484786387.131,
  "end_time": 1484786387.501,
  "name": "names.example.com",
  "namespace": "remote",
  "http": {
    "request": {
      "method": "GET",
      "url": "https://names.example.com/"
    },
    "response": {
      "content_length": -1,
      "status": 200
    }
  }
}
```

Example Segmento inferido para una llamada HTTP posterior

```
{
  "id": "168416dc2ea97781",
  "name": "names.example.com",
  "trace_id": "1-62be1272-1b71c4274f39f122afa64eab",
  "start_time": 1484786387.131,
  "end_time": 1484786387.501,
  "parent_id": "004f72be19cddc2a",
  "http": {
    "request": {
      "method": "GET",
      "url": "https://names.example.com/"
    },
    "response": {
      "content_length": -1,
      "status": 200
    }
  },
  "inferred": true
}
```

Annotations

Los segmentos y subsegmentos pueden incluir un objeto `annotations` con uno o varios campos que X-Ray indexa para su uso con expresiones de filtro. Los campos pueden tener valores de

cadena, numéricos o booleanos (pero no objetos ni matrices). X-Ray indexa hasta 50 anotaciones por rastro.

Example Segmento para llamadas HTTP con anotaciones

```
{
  "id": "6b55dcc497932f1a",
  "start_time": 1484789187.126,
  "end_time": 1484789187.535,
  "trace_id": "1-5880168b-fd515828bs07678a3bb5a78c",
  "name": "www.example.com",
  "origin": "AWS::EC2::Instance",
  "aws": {
    "ec2": {
      "availability_zone": "us-west-2c",
      "instance_id": "i-0b5a4678fc325bg98"
    },
    "xray": {
        "sdk_version": "2.11.0 for Java"
    },
  },
  "annotations": {
    "customer_category" : 124,
    "zip_code" : 98101,
    "country" : "United States",
    "internal" : false
  },
  "http": {
    "request": {
      "method": "POST",
      "client_ip": "78.255.233.48",
      "url": "http://www.example.com/api/user",
      "user_agent": "Mozilla/5.0 (Windows NT 6.1; WOW64; rv:45.0) Gecko/20100101
 Firefox/45.0",
      "x_forwarded_for": true
    },
    "response": {
      "status": 200
    }
  }
```

Para que las claves funcionen con filtros, deben estar en orden alfanumérico. Se admite el guion bajo, pero no otros símbolos ni espacios en blanco.

Metadatos

Los segmentos y subsegmentos pueden incluir un objeto `metadata` que contenga uno o varios campos con valores de cualquier tipo, incluidos objetos y matrices. X-Ray no indexa los metadatos, y los valores pueden ser de cualquier tamaño siempre que el documento del segmento no supere el tamaño máximo (64 kB). Puede ver los metadatos en el documento del segmento completo devuelto por la API de `BatchGetTraces`. Las claves de campo (`debug` en el siguiente ejemplo) que comienzan por: `AWS.` están reservadas para que las utilicen los SDK y los clientes AWS proporcionados.

Example Subsegmento personalizado con metadatos

```
{
  "id": "0e58d2918e9038e8",
  "start_time": 1484789387.502,
  "end_time": 1484789387.534,
  "name": "## UserModel.saveUser",
  "metadata": {
    "debug": {
      "test": "Metadata string from UserModel.saveUser"
    }
  },
  "subsegments": [
    {
      "id": "0f910026178b71eb",
      "start_time": 1484789387.502,
      "end_time": 1484789387.534,
      "name": "DynamoDB",
      "namespace": "aws",
      "http": {
        "response": {
          "content_length": 58,
          "status": 200
        }
      },
      "aws": {
        "table_name": "scorekeep-user",
        "operation": "UpdateItem",
        "request_id": "3AIENM5J4ELQ3SPODHKBIRVIC3VV4KQNSO5AEMVJF66Q9ASUAAJG",
        "resource_names": [
          "scorekeep-user"
        ]
```

```
      }
    }
  ]
}
```

AWS datos de recursos

Para los segmentos, el objeto `aws` contiene información sobre el recurso en el que se ejecuta la aplicación. Se pueden aplicar varios campos a un solo recurso. Por ejemplo, una aplicación que se ejecute en un entorno Docker multicontenedor en Elastic Beanstalk podría tener información sobre la instancia de Amazon EC2, el contenedor de Amazon ECS que se ejecuta en la instancia y el propio entorno de Elastic Beanstalk.

`aws` (Segmentos)

Todos los campos son opcionales.

- `account_id`— Si su aplicación envía segmentos a otra Cuenta de AWS, registre el ID de la cuenta que ejecuta la aplicación.
- `cloudwatch_logs`— Matriz de objetos que describen un único grupo de CloudWatch registros.
  - `log_group`— El nombre del grupo de CloudWatch registros.
  - `arn`— El ARN del grupo de CloudWatch registros.
- `ec2`: información sobre una instancia de Amazon EC2.
  - `instance_id`: el ID de la instancia de EC2.
  - `instance_size`: el tipo de la instancia de EC2.
  - `ami_id`: el ID de imagen de máquina de Amazon.
  - `availability_zone`: la zona de disponibilidad en la que se ejecuta la instancia.
- `ecs`: información sobre un contenedor de Amazon ECS.
  - `container`: el nombre de host de su contenedor.
  - `container_id`: el ID completo de su contenedor.
  - `container_arn`: el ARN de su instancia de contenedor.
- `eks`: la información acerca de un clúster de Amazon EKS.
  - `pod`: el nombre de host de su pod de EKS.
  - `cluster_name`: el nombre del clúster de EKS.
  - `container_id`: el ID completo de su contenedor.

- `elastic_beanstalk`: información sobre un entorno de Elastic Beanstalk. Puede encontrar esta información en un archivo denominado `/var/elasticbeanstalk/xray/environment.conf` en las plataformas más recientes de Elastic Beanstalk.
  - `environment_name`: el nombre del entorno.
  - `version_label`: el nombre de la versión de la aplicación que está implementada actualmente en la instancia que ha atendido la solicitud.
  - `deployment_id`: número que indica el ID de la última implementación satisfactoria en la instancia que ha atendido la solicitud.
- `xray`: metadatos sobre el tipo y la versión de la instrumentación utilizada.
  - `auto_instrumentation`: booleano que indica si se utilizó la instrumentación automática (por ejemplo, el agente Java).
  - `sdk_version`. La versión del SDK o del agente que se está utilizando.
  - `sdk`: el tipo de SDK.

Example AWS bloquear con complementos

```
"aws":{
   "elastic_beanstalk":{
      "version_label":"app-5a56-170119_190650-stage-170119_190650",
      "deployment_id":32,
      "environment_name":"scorekeep"
   },
   "ec2":{
      "availability_zone":"us-west-2c",
      "instance_id":"i-075ad396f12bc325a",
      "ami_id":
   },
   "cloudwatch_logs":[
      {
         "log_group":"my-cw-log-group",
         "arn":"arn:aws:logs:us-west-2:012345678912:log-group:my-cw-log-group"
      }
   ],
   "xray":{
      "auto_instrumentation":false,
      "sdk":"X-Ray for Java",
      "sdk_version":"2.8.0"
   }
```

```
}
```

En el caso de los subsegmentos, registre la información sobre Servicios de AWS los recursos a los que accede su aplicación. X-Ray utiliza esta información para crear segmentos inferidos que representan los servicios posteriores del mapa de servicio.

`aws` (subsegmentos)

Todos los campos son opcionales.

- `operation`— El nombre de la acción de API invocada contra un recurso Servicio de AWS o.
- `account_id`— Si su aplicación accede a los recursos de una cuenta diferente o envía segmentos a una cuenta diferente, registre el ID de la cuenta propietaria del AWS recurso al que accedió la aplicación.
- `region`: si el recurso está en una región diferente a la de la aplicación, este campo registra la región. Por ejemplo, `us-west-2`.
- `request_id`: un identificador único para la solicitud.
- `queue_url`: para las operaciones incluidas en una cola de Amazon SQS, la dirección URL de la cola.
- `table_name`: para las operaciones de una tabla de DynamoDB, el nombre de la tabla.

Example Subsegmento para una llamada a DynamoDB con el fin de guardar un elemento

```
{
  "id": "24756640c0d0978a",
  "start_time": 1.480305974194E9,
  "end_time": 1.4803059742E9,
  "name": "DynamoDB",
  "namespace": "aws",
  "http": {
    "response": {
      "content_length": 60,
      "status": 200
    }
  },
  "aws": {
    "table_name": "scorekeep-user",
    "operation": "UpdateItem",
    "request_id": "UBQNSO5AEM8T4FDA4RQDEB94OVTDRVV4K4HIRGVJF66Q9ASUAAJG",
```

```
  }
}
```

Errores y excepciones

Cuando se produzca un error, puede registrar información sobre el error y las excepciones que se generan. Registre los errores en los segmentos cuando la aplicación devuelva un error al usuario, y en los subsegmentos cuando una llamada posterior devuelva un error.

tipos de error

Establezca uno o varios de los campos siguientes en `true` para indicar que se ha producido un error. Se pueden aplicar varios tipos si se trata de errores compuestos. Por ejemplo, un error `429 Too Many Requests` de una llamada posterior podría hacer que la aplicación devolviera un error `500 Internal Server Error`, en cuyo caso se aplicarían los tres tipos.

- `error`: booleano que indica que se ha producido un error del cliente (el código de estado de la respuesta fue 4XX Client Error).
- `throttle`: booleano que indica que se ha limitado una solicitud (el código de estado de la respuesta fue 429 Too Many Requests).
- `fault`: booleano que indica que se ha producido un error del servidor (el código de estado de la respuesta fue 5XX Server Error).

Indique la causa del error incluyendo un objeto cause en el segmento o subsegmento.

`cause`

Una causa puede ser un ID de excepción de 16 caracteres o un objeto con los siguientes campos:

- `working_directory`: la ruta completa del directorio de trabajo donde se produjo la excepción.
- `paths`: la matriz de rutas a las bibliotecas o módulos que se estaban usando cuando se produjo la excepción.
- `exceptions`: la matriz de objetos exception.

Incluya información detallada sobre el error en uno o varios objetos exception.

`exception`

Todos los campos son opcionales.

- `id`: un identificador de 64 bits para la excepción, único entre otros segmentos del mismo rastro, en 16 dígitos hexadecimales.
- `message`: el mensaje de excepción.
- `type`: el tipo de excepción.
- `remote`: booleano que indica que la excepción se produjo por un error devuelto por un servicio posterior.
- `truncated`: entero que indica el número de marcos de pila que se han omitido de `stack`.
- `skipped`: entero que indica el número de excepciones que se omitieron entre esta excepción y su excepción secundaria, es decir, la excepción que la ha causado.
- `cause`: ID de excepción del elemento principal de la excepción, es decir, la excepción que provocó esta excepción.
- `stack`: matriz de objetos stackFrame.

Si está disponible, registre la información acerca de la pila de llamada en objetos stackFrame.

`stackFrame`

Todos los campos son opcionales.

- `path`: la ruta relativa al archivo.
- `line`: la línea dentro del archivo.
- `label`: el nombre de la función o método.

Consultas SQL

Puede crear subsegmentos para las consultas que la aplicación realiza en una base de datos SQL.

`sql`

Todos los campos son opcionales.

- `connection_string`: para SQL Server u otras conexiones de base de datos que no usen cadenas de conexión URL, este campo registra la cadena de conexión, sin incluir las contraseñas.
- `url`: para una conexión a la base de datos que utilice una cadena de conexión URL, este campo registra la dirección URL, sin incluir las contraseñas.

- `sanitized_query`: la consulta a la base de datos, con todos los valores proporcionados por el usuario eliminados o reemplazados con un marcador de posición.
- `database_type`: el nombre del motor de base de datos.
- `database_version`: el número de versión del motor de base de datos.
- `driver_version`: el nombre y número de versión del controlador del motor de base de datos que usa la aplicación.
- `user`: el nombre de usuario de la base de datos.
- `preparation`: `call` si la consulta utiliza un `PreparedCall`; `statement` si la consulta utiliza un `PreparedStatement`.

Example Subsegmento con una consulta SQL

```
{
  "id": "3fd8634e78ca9560",
  "start_time": 1484872218.696,
  "end_time": 1484872218.697,
  "name": "ebdb@aawijb5u25wdoy.cpamxznpdoq8.us-west-2.rds.amazonaws.com",
  "namespace": "remote",
  "sql" : {
    "url": "jdbc:postgresql://aawijb5u25wdoy.cpamxznpdoq8.us-
west-2.rds.amazonaws.com:5432/ebdb",
    "preparation": "statement",
    "database_type": "PostgreSQL",
    "database_version": "9.5.4",
    "driver_version": "PostgreSQL 9.4.1211.jre7",
    "user" : "dbuser",
    "sanitized_query" : "SELECT  *  FROM  customers  WHERE  customer_id=?;"
  }
}
```

Historial de documentos para AWS X-Ray

En la siguiente tabla se describen los cambios importantes en la documentación de AWS X-Ray. Para recibir notificaciones sobre los cambios en esta documentación, puede suscribirse a una fuente RSS.

Última actualización de la documentación: 8 de febrero de 2023

Cambio	Descripción	Fecha
Funcionalidad agregada	X-Ray ahora registra eventos de datos `PutTraceSegments`, incluidos `GetTraceSummaries`, y `BatchGetTraces` para AWS CloudTrail. X-Ray ahora también registra el evento `GetSamplingStatisticSummaries` de administración en CloudTrail. Para obtener más información, consulte Registrar llamadas a la API X-Ray con AWS CloudTrail.	7 de marzo de 2024
Funcionalidad agregada	X-Ray ahora admite los ID de rastreo creados mediante OpenTelemetry o cualquier otro marco que cumpla con la especificación Trace Context del W3C. Para obtener más información, consulte Envío de datos de rastreo a X-Ray.	25 de octubre de 2023
Funcionalidad agregada	A partir de ahora, puede configurar el rastreo activo de Amazon SNS, lo que le	8 de febrero de 2023

	permite rastrear y analizar las solicitudes a medida que avanzan a través de los temas de Amazon SNS. Para obtener más información, consulte Amazon SNS y. AWS X-Ray	
Tema sobre el SDK de X-Ray para Node.js actualizado	Se agregaron detalles para la instrumentación de los clientes que utilizan la V3. AWS SDK for JavaScript Para obtener más información, consulte Rastreo de llamadas del AWS SDK con el SDK de X-Ray para Node.js.	7 de febrero de 2023
Detalles de la política administrada de IAM actualizados	Se agregó el permiso de IAM para la observabilidad entre cuentas a las políticas administradas `AWSXRayReadOnlyAccess` , `AWSXRayFullAccess` y `AWSXrayCrossAccountSharingConfiguration` . Para obtener más información, consulte Políticas administradas de IAM para X-Ray.	7 de febrero de 2023

Funcionalidad agregada	AWS X-Ray ahora es compatible con la observabilidad entre cuentas, lo que le permite supervisar y solucionar problemas de las aplicaciones que abarcan varias cuentas dentro de una. Región de AWS Para obtener más información, consulte Rastreo entre cuentas.	27 de noviembre de 2022
Funcionalidad agregada	Ahora puede ver los rastros vinculados entre los productores de mensajes, una cola de Amazon SQS y los consumidores, lo que proporciona una vista conectada de los rastros enviados desde aplicaciones basadas en eventos. Para obtener más información, consulte Rastreo de aplicaciones basadas en eventos.	20 de noviembre de 2022
Detalles de la política administrada de IAM actualizados	Se agregó el permiso de IAM para incluir políticas de recursos en la política administrada `AWSXRayReadOnlyAccess` . Para obtener más información, consulte Políticas administradas de IAM para X-Ray.	15 de noviembre de 2022

Permisos de la consola de IAM y detalles de la política administrada actualizados	Se actualizó el conjunto de permisos de IAM que utiliza la consola de X-Ray, junto con la descripción de la política administrada `AWSXRayReadOnlyAccess`. Para obtener más información, consulte Uso de la consola X-Ray.	11 de noviembre de 2022
Se agregó AWS una distribución para Ruby OpenTelemetry	AWS Distro for OpenTelemetry (ADOT) proporciona un conjunto único de API, bibliotecas y agentes de código abierto para recopilar rastreos y métricas distribuidos. ADOT Ruby le permite instrumentar su aplicación Ruby para X-Ray y otros backends de rastreo. Para obtener más información, consulte AWS Distro for Ruby. OpenTelemetry	7 de febrero de 2022
Funcionalidad agregada	Ahora puede ver las trazas y configurar X-Ray desde la CloudWatch consola. Para obtener más información, consulte Consola de X-Ray.	24 de enero de 2022

CloudWatch RUM integrado	Con AWS X-Ray el CloudWatch RUM, puede analizar y depurar la ruta de las solicitudes empezando por los usuarios finales de su aplicación y pasando por los servicios AWS gestionados posteriores. Para obtener más información, consulte CloudWatch RUM y. AWS X-Ray	3 de diciembre de 2021
AWS Distribución integrada para OpenTelemetry	The AWS Distro for OpenTelemetry (ADOT) proporciona un conjunto único de API, bibliotecas y agentes de código abierto para recopilar rastreos y métricas distribuidos. ADOT le permite instrumentar su aplicación para X-Ray y otros backends de rastreo. Para obtener más información, consulte Instrumentación de su aplicación.	23 de septiembre de 2021
Funcionalidad agregada	AWS X-Ray ahora se integra con Amazon Virtual Private Cloud, lo que permite que los recursos de su Amazon VPC se comuniquen con el servicio de X-Ray sin tener que pasar por la Internet pública. Para obtener más información, consulte Uso AWS X-Ray con puntos de enlace de VPC.	20 de mayo de 2021

Funcionalidad agregada	AWS X-Ray ahora se integra con AWS CloudFormation, lo que le permite aprovisionar y configurar los recursos de X-Ray. Para obtener más información, consulte Creación de recursos de X-Ray con CloudFormation.	6 de mayo de 2021
Funcionalidad agregada	AWS X-Ray ahora se integra con Amazon EventBridge para rastrear los eventos que se transmiten EventBridge. Eso proporciona a los usuarios una visión más completa de su sistema. Para obtener más información, consulte Amazon EventBridge y AWS X-Ray.	2 de marzo de 2021
Daemon agregado a ECR	Ahora el daemon se puede descargar de Amazon ECR. Para obtener más información, consulte Descarga del daemon.	1 de marzo de 2021
Funcionalidad agregada	AWS X-Ray ahora admite notificaciones relacionadas con estadísticas para Amazon EventBridge. Esto le permite tomar medidas automáticas sobre la información que utiliza EventBridge. Para obtener más información, consulte Notificaciones de información.	15 de octubre de 2020

Daemons descargables agregados	AWS X-Ray presenta el daemon de soporte para Linux ARM64. Para obtener más información, consulte AWS X-Ray daemonbrazil ws	1 de octubre de 2020
Funcionalidad agregada	AWS X-Ray ahora admite la integración activa con Amazon CloudWatch Synthetics. Eso le permite ver detalles sobre un nodo cliente de valores controlados de Synthetics, como el tiempo de respuesta y el estado. También puede realizar análisis en la consola de Analytics en función de la información de un nodo cliente de valores controlados de Synthetics. Para obtener más información, consulte Depuración de CloudWatch canarios sintéticos mediante X-Ray.	24 de septiembre de 2020
Funcionalidad agregada	AWS X-Ray ahora admite flujos de trabajo de rastreo end-to-end para. AWS Step Functions Puede visualizar los componentes de su máquina de estado, identificar cuellos de botella en el rendimiento y solucionar problemas de solicitudes que dieron lugar a un error. Para obtener más información, consulte AWS Step Functions y. AWS X-Ray	14 de septiembre de 2020

Funcionalidad agregada	AWS X-Ray presenta información para analizar continuamente los datos de rastreo de su cuenta a fin de identificar problemas emergentes en sus aplicaciones. La información consiste en registros de incidentes y un seguimiento del impacto de los incidentes hasta su resolución. Para obtener más información, consulte Uso de la información en la consola AWS X-Ray	3 de septiembre de 2020
Funcionalidad agregada	AWS X-Ray presenta el agente de autoinstrumentación de Java, que permite a los clientes recopilar datos de rastreo sin tener que modificar la aplicación existente basada en Java. Ahora puede rastrear las aplicaciones web creadas en Java y basadas en servlets con un cambio mínimo de la configuración y sin cambios de código. Para obtener más información, consulte Agente de instrumentación automática de AWS X-Ray para Java.	3 de septiembre de 2020

Funcionalidad agregada	AWS X-Ray ha añadido una nueva página de grupos a la consola de X-Ray para facilitar la creación y la gestión de grupos de trazas. Para obtener más información consulte Configuración de grupos en la consola de X-Ray.	24 de agosto de 2020
Funcionalidad agregada	AWS X-Ray ahora permite añadir etiquetas a los grupos y a las reglas de muestreo. También permite controlar el acceso a los grupos y a las reglas de muestreo en función de las etiquetas. Para obtener más información, consulte Etiquetado de reglas de muestreo y grupos de X-Ray y Administración del acceso a grupos y a reglas de muestreo en función de las etiquetas.	24 de agosto de 2020

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.