

Monitoreo en AWS

✓ **Video:**Introducción a la Semana 4
52 segundos

✓ **Video:**Monitoreo en AWS
3 minutos

✓ **Lectura:**Lectura 4.1: Monitoreo en AWS
30 minutos

✓ **Video:**Introducción a Amazon CloudWatch
5 minutos

📖 **Lectura:**Lectura 4.2: Introducción a Amazon CloudWatch
30 minutos

Mejoramiento

Ejercicio y evaluación de la semana 4

Ir sin servidor

Evaluación de fin de curso

Lectura 4.2: Introducción a Amazon CloudWatch

Cómo funciona CloudWatch

Lo mejor de CloudWatch es que todo lo que necesita para comenzar es una cuenta de AWS. Es un servicio administrado, que le permite concentrarse en el monitoreo, sin administrar ninguna infraestructura subyacente.

La aplicación del directorio de empleados está construida con varios servicios de AWS que trabajan juntos como bloques de construcción. Sería difícil monitorear todos estos diferentes servicios de forma independiente, por lo que CloudWatch actúa como un lugar centralizado donde se recopilan y analizan las métricas. Ya aprendió cómo las instancias EC2 publican la utilización de la CPU como una métrica para CloudWatch. Diferentes recursos de AWS publican diferentes métricas que puede monitorear. Puede ver una lista de servicios que envían métricas a CloudWatch en la sección de recursos de esta unidad.

Muchos servicios de AWS envían métricas automáticamente de forma gratuita a CloudWatch a una velocidad de un punto de datos por métrica en intervalos de 5 minutos, sin que tenga que hacer nada para activar esa recopilación de datos. Esto por sí solo le da visibilidad a sus sistemas sin necesidad de gastar dinero extra para hacerlo. Esto se conoce como **monitoreo básico**. Para muchas aplicaciones, el monitoreo básico hace el trabajo.

Para las aplicaciones que se ejecutan en instancias EC2, puede obtener más granularidad al publicar métricas cada minuto en lugar de cada 5 minutos mediante una función como el **monitoreo detallado**. El monitoreo detallado tiene una tarifa adicional asociada. Puede leer acerca de los precios en la página de precios de CloudWatch vinculada en la sección de recursos de esta unidad.

Desglosar métricas

Cada métrica en CloudWatch tiene una marca de tiempo y está organizada en contenedores llamados **espacios de nombres**. Las métricas en diferentes espacios de nombres están aisladas entre sí; puede considerarlas como pertenecientes a diferentes categorías.

Los servicios de AWS que envían datos a CloudWatch adjuntan **dimensiones** a cada métrica. Una dimensión es un par de nombre/valor que forma parte de la identidad de la métrica. Puede utilizar dimensiones para filtrar los resultados que devuelve CloudWatch. Por ejemplo, puede obtener estadísticas para una instancia EC2 específica especificando la dimensión InstanceId cuando realiza la búsqueda.

Configurar métricas personalizadas

Digamos que para su aplicación desea registrar el número de páginas vistas que obtiene su sitio web. ¿Cómo registraría esta métrica en CloudWatch? Es una métrica de nivel de aplicación, lo que significa que no es algo que la instancia EC2 publicaría en CloudWatch de forma predeterminada. Aquí es donde entran en juego **las métricas personalizadas**. Las métricas personalizadas le permiten publicar sus propias métricas en CloudWatch.

Si desea obtener una visibilidad más granular, puede usar **métricas personalizadas de alta resolución**, que le permiten recopilar métricas personalizadas con una resolución de hasta 1 segundo. Esto significa que puede enviar un punto de datos por segundo por métrica personalizada. Otros ejemplos de métricas personalizadas son:

- Tiempos de carga de la página web
- Solicitud de tasas de error
- Número de procesos o subprocesos en su instancia
- Cantidad de trabajo realizado por su aplicación

Nota : puede comenzar con las métricas personalizadas enviando la métrica mediante programación a CloudWatch mediante la API de PutMetricData.

Comprender los paneles de CloudWatch

Una vez que haya aprovisionado sus recursos de AWS y estén enviando métricas a CloudWatch, podrá visualizar y revisar esos datos mediante la consola de CloudWatch con paneles. Los paneles son páginas de inicio personalizables que utiliza para la visualización de datos para una o más métricas mediante el uso de widgets, como un gráfico o texto.

Puede crear muchos paneles personalizados, cada uno de los cuales se centra en una vista distinta de su entorno. Incluso puede extraer datos de diferentes regiones en un solo tablero para crear una vista global de su arquitectura.

CloudWatch agrega estadísticas según el período de tiempo que especifique al crear su gráfico o solicitar sus métricas. También puede elegir si sus widgets de métricas muestran datos en vivo. Los datos en vivo son datos publicados en el último minuto que no se han agregado por completo.

No está obligado a utilizar CloudWatch exclusivamente para todas sus necesidades de visualización. Puede utilizar herramientas externas o personalizadas para ingerir y analizar métricas de CloudWatch mediante la API GetMetricData.

En cuanto a la seguridad, puede controlar quién tiene acceso para ver o administrar sus paneles de CloudWatch a través de políticas de AWS Identity and Access Management (IAM) que se asocian con usuarios de IAM, grupos de IAM o roles de IAM.

Conozca los registros de CloudWatch

Conoce los registros de CloudWatch

CloudWatch también puede ser el lugar centralizado para almacenar y analizar los registros mediante CloudWatch Logs. CloudWatch Logs puede monitorear, almacenar y acceder a sus archivos de registro desde aplicaciones que se ejecutan en instancias de Amazon EC2, funciones de AWS Lambda y otras fuentes.

CloudWatch Logs le permite consultar y filtrar sus datos de registro. Por ejemplo, supongamos que está investigando un error de lógica de aplicación para su aplicación y sabe que cuando ocurra este error, registrará el seguimiento de la pila. Como sabe que registra el error, consulta sus registros en CloudWatch Logs para encontrar el seguimiento de la pila. También configura **filtros de métricas** en los registros, que convierten los datos de registro en métricas numéricas de CloudWatch que grafica y utiliza en sus tableros.

Algunos servicios están configurados para enviar datos de registro a CloudWatch Logs con un esfuerzo mínimo, como AWS Lambda. Con AWS Lambda, todo lo que necesita hacer es otorgar a la función de Lambda los permisos de IAM correctos para publicar registros en CloudWatch Logs. Otros servicios requieren más configuración. Por ejemplo, si desea enviar los registros de su aplicación desde una instancia EC2 a CloudWatch Logs, primero debe instalar y configurar el agente de CloudWatch Logs en la instancia EC2.

El agente de CloudWatch Logs permite que las instancias de Amazon EC2 envíen automáticamente datos de registro a CloudWatch Logs. El agente incluye los siguientes componentes.

- Un complemento para la interfaz de línea de comandos (CLI) de AWS que envía datos de registro a CloudWatch Logs.
- Una secuencia de comandos que inicia el proceso para enviar datos a CloudWatch Logs.
- Un trabajo cron que garantiza que el daemon siempre se esté ejecutando.

Una vez que el agente está instalado y configurado, puede ver los registros de su aplicación en CloudWatch Logs.

Aprenda la terminología de registros de CloudWatch

Los datos de registro enviados a CloudWatch Logs pueden provenir de diferentes fuentes, por lo que es importante que comprenda cómo están organizados y la terminología utilizada para describir sus registros.

Evento de registro: un evento de registro es un registro de la actividad registrada por la aplicación o el recurso que se supervisa, y tiene una marca de tiempo y un mensaje de evento.

Flujo de registro: los eventos de registro se agrupan en flujos de registro, que son secuencias de eventos de registro que pertenecen al mismo recurso que se supervisa. Por ejemplo, los registros de una instancia EC2 se agrupan en un flujo de registros que luego puede filtrar o consultar para obtener información.

Grupos de registros: los flujos de registros se organizan en grupos de registros. Un grupo de registros se compone de secuencias de registros que comparten la misma configuración de retención y permisos. Por ejemplo, si tiene varias instancias EC2 que alojan su aplicación y está enviando datos de registro de la aplicación a CloudWatch Logs, puede agrupar los flujos de registro de cada instancia en un grupo de registros. Esto ayuda a mantener sus registros organizados.

Configurar una alarma de CloudWatch

Puede crear alarmas de CloudWatch para iniciar acciones automáticamente en función de los cambios de estado sostenidos de sus métricas. Usted configura cuándo se disparan las alarmas y la acción que se realiza.

Primero debe decidir para qué métrica desea configurar una alarma, luego define el umbral en el que desea que se active la alarma. A continuación, defina el período de tiempo especificado en el que la métrica debe cruzar el umbral para que se active la alarma.

Por ejemplo, si desea configurar una alarma para que una instancia EC2 se active cuando la utilización de la CPU supera el umbral del 80 %, también debe especificar el período de tiempo durante el cual la utilización de la CPU supera el umbral. No desea activar una alarma basada en breves picos temporales en la CPU. Solo desea activar una alarma si la CPU se eleva durante un período prolongado de tiempo, por ejemplo, si supera el 80 % durante 5 minutos o más, cuando existe un posible problema de recursos.

Teniendo todo eso en cuenta, para configurar una alarma, debe elegir la métrica, el umbral y el período de tiempo. Una alarma tiene tres estados posibles.

- **Correcto:** la métrica está dentro del umbral definido. Todo parece funcionar con normalidad.
- **ALARMA:** La métrica está fuera del umbral definido. Esto podría ser un problema operativo.
- **INSUFFICIENT_DATA:** la alarma acaba de comenzar, la métrica no está disponible o no hay suficientes datos disponibles para que la métrica determine el estado de la alarma.

Se puede activar una alarma cuando pasa de un estado a otro. Una vez que se activa una alarma, puede iniciar una acción. Las acciones pueden ser una acción de Amazon EC2, una acción de Auto Scaling o una notificación enviada a Amazon Simple Notification Service (SNS).

Utilice las alarmas de CloudWatch para prevenir y solucionar problemas

CloudWatch Logs utiliza filtros de métricas para convertir los datos de registro en métricas que puede generar gráficos o configurar una alarma. Para la aplicación de directorio de empleados, supongamos que configura un filtro de métricas para códigos de respuesta de 500 errores.

Luego, define una alarma para esa métrica que pasará al estado ALARMA si las respuestas de 500 errores superan una cierta cantidad durante un período de tiempo prolongado. Digamos que si son más de cinco respuestas de 500 errores por hora, la alarma debería entrar en estado de ALARMA. A continuación, defina una acción que desee que se lleve a cabo cuando se dispare la alarma.

En este caso, tiene sentido enviarle una alerta por correo electrónico o mensaje de texto para que pueda comenzar a solucionar el problema del sitio web y, con suerte, solucionarlo antes de que se convierta en un problema mayor. Una vez que se configura la alarma, se siente cómodo sabiendo que si el error vuelve a ocurrir, se le notificará de inmediato.

Puede configurar diferentes alarmas por diferentes motivos para ayudarlo a prevenir o solucionar problemas

operativos. En el escenario que se acaba de describir, la alarma activó una notificación de SNS que fue a una persona que investigó el problema manualmente. Otra opción es hacer que las alarmas activen acciones que solucionen automáticamente los problemas técnicos.

Por ejemplo, puede configurar una alarma para activar una instancia EC2 para que se reinicie o ampliar o reducir los servicios. Incluso puede configurar una alarma para activar una notificación SNS, que luego activa una función AWS Lambda. Luego, la función de Lambda llama a cualquier API de AWS para administrar sus recursos y solucionar problemas operativos. Al usar los servicios de AWS juntos de esta manera, responde a los eventos más rápidamente.

Recursos :

- [Sitio externo: AWS: Primeros pasos con Amazon CloudWatch](#)
- [Sitio externo: AWS: ¿Qué es Amazon CloudWatch Logs?](#)
- [Sitio externo: servicios de AWS que publican métricas de CloudWatch](#)
- [Sitio externo: AWS: Ver métricas disponibles](#)
- [Sitio externo: AWS: precios de Amazon CloudWatch](#)
- [Sitio externo: AWS: Amazon Simple Notification Service](#)
- [Sitio externo: AWS: acciones de EC2 Auto Scaling](#)

Marcar como completo

 Me gusta  No me gusta  Informar de un problema