CloudOps Guild
*Together, towards mastery in Cloud and DevOps*

AWS COMMUNITY CARTAGENA

# AWS SysOps Administrator Associate

## Challenge


Speaker
**Mario Serrano**

Date
**28 mayo, 2025**

AWS SysOps Administrador Associate

Challenge

CloudOps Guild

*Together, towards mastery in Cloud and DevOps*

# Semana 3
# Dominio Monitoring, Logging, and Remediation


Reforzar habilidades de monitoreo, análisis de logs y automatización de respuestas ante eventos en AWS, con énfasis en conceptos evaluados en el examen SysOps Administrator Associate.

- Métricas, logs y alarmas con CloudWatch
- System Manager, Run Command y monitoreo proactivo

CloudOps Guild
*Together, towards mastery in Cloud and DevOps*

# Acerca de mi

Esposo y padre de 2 hijos, Ángel y Sara
Ingeniero de sistemas, especialista en telecomunicaciones, MBA
Trabajo en el campo de la tecnología hace más de 20 años.
Áreas de especialización

- Arquitectura TI
- DevOps
- Site Reliability Engineering
- Arquitectura multi cloud (AWS, Azure, OCI)
- https://www.linkedin.com/in/mario-rodrigo-serrano-pineda/
- E-mail: marosepi2020@gmail.com
- https://medium.com/@marioserranopineda

AWS community builders


# Agenda

1. Fundamentos de monitoreo en AWS.
2. Deep Dive – Logs en contexto
3. Automatización y Remediación
4. Recomendaciones generales
5. Preguntas ejemplos

# 1. Fundamentos de monitoreo en AWS

AWS SysOps Administrador Associate

Challenge

CloudOps Guild

*Together, towards mastery in Cloud and DevOps*

# CloudWatch Metrics (Métricas)

Son **datos numéricos que representan el rendimiento** de un recurso en AWS a lo largo del tiempo. Pueden ser recolectados automáticamente por AWS o enviados manualmente por el usuario (métricas personalizadas).

AWS publica métricas por defecto para casi todos sus servicios. Algunos ejemplos:

| Servicio | Ejemplos de métricas | Unidad |
|---|---|---|
| EC2 | CPUUtilization, DiskReadOps | Porcentaje, Count |
| RDS | CPUUtilization, DatabaseConnections | Porcentaje, Count |
| Lambda | Invocations, Duration, Errors | Count, ms |
| ELB | RequestCount, HTTPCode_ELB_5XX_Count | Count |

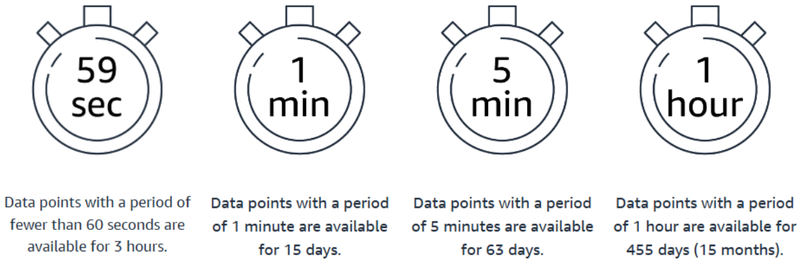
"Estas métricas tienen una **retención y granularidad** que depende del nivel de detalle (1 minuto o 5 minutos)."

# Métricas personalizadas

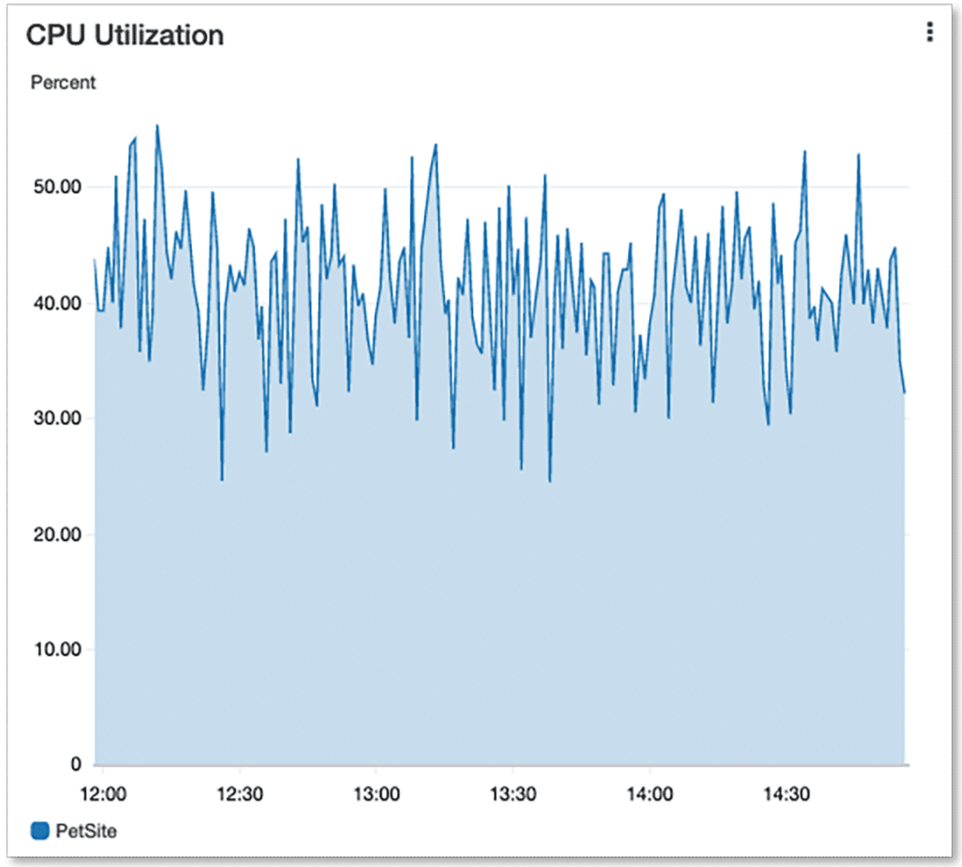
Puedes enviar tus propias métricas a CloudWatch mediante:

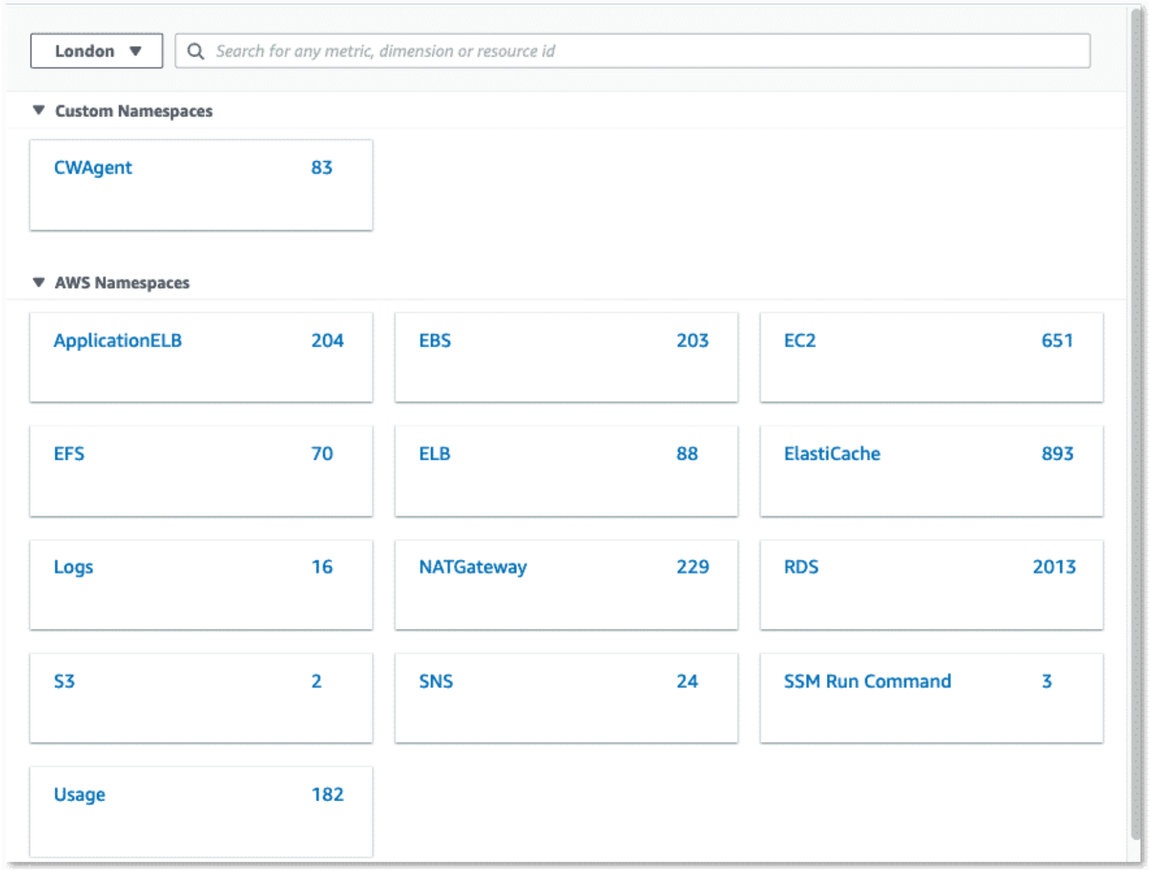
```
aws cloudwatch put-metric-data \
  --namespace "MyApp" \
  --metric-name "ActiveUsers" \
  --value 123 \
  --unit Count
```

Tiempo de retención




Útil para medir datos de negocio, eventos de apps o procesos personalizados.


CPU Utilization
Percent
50.00
40.00
30.00
20.00
10.00
0
12:00
12:30
13:00
13:30
14:00
14:30
PetSite


London
Search for any metric, dimension or resource id
Custom Namespaces
CWAgent 83
AWS Namespaces
ApplicationELB 204
EBS 203
EC2 651
EFS 70
ELB 88
ElastiCache 893
Logs 16
NATGateway 229
RDS 2013
S3 2
SNS 24
SSM Run Command 3
Usage 182

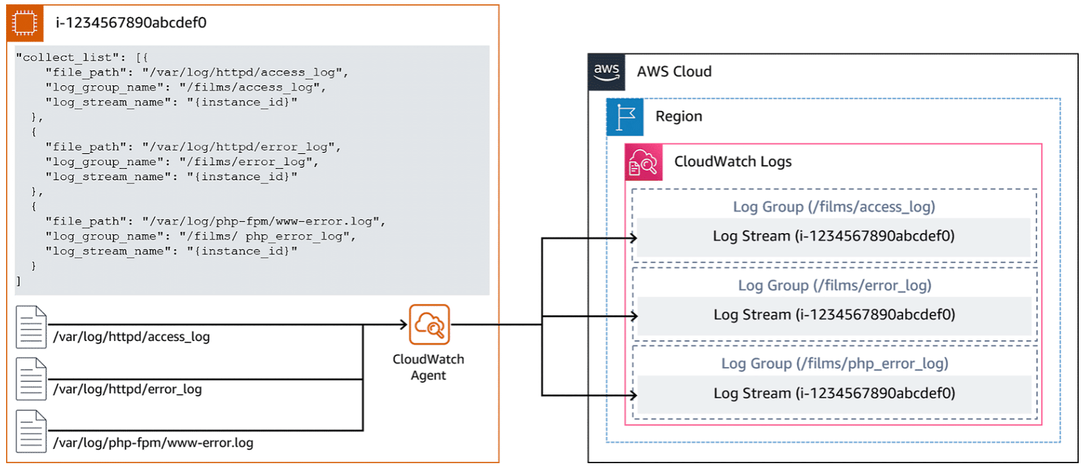
# CloudWatch Logs

Servicio para recolectar y visualizar **logs de aplicaciones, sistemas operativos y servicios AWS**. Centraliza los logs y permite análisis con consultas avanzadas.

¿Qué servicios los generan automáticamente?

| Servicio | ¿Envío automático a Logs? |
|---|---|
| **Lambda** | ✅ Sí, sin configuración adicional |
| **API Gateway** | ✅ Sí, cuando se habilita logging |
| **VPC Flow Logs** | ✅ Con configuración |
| **CloudTrail** | ✅ Puede enviar a Logs o S3 |
| **EC2** | ❌ Se necesita instalar y configurar agente |

Para enviar lo logs desde EC2 es necesario instalar el agente de Cloudwatch

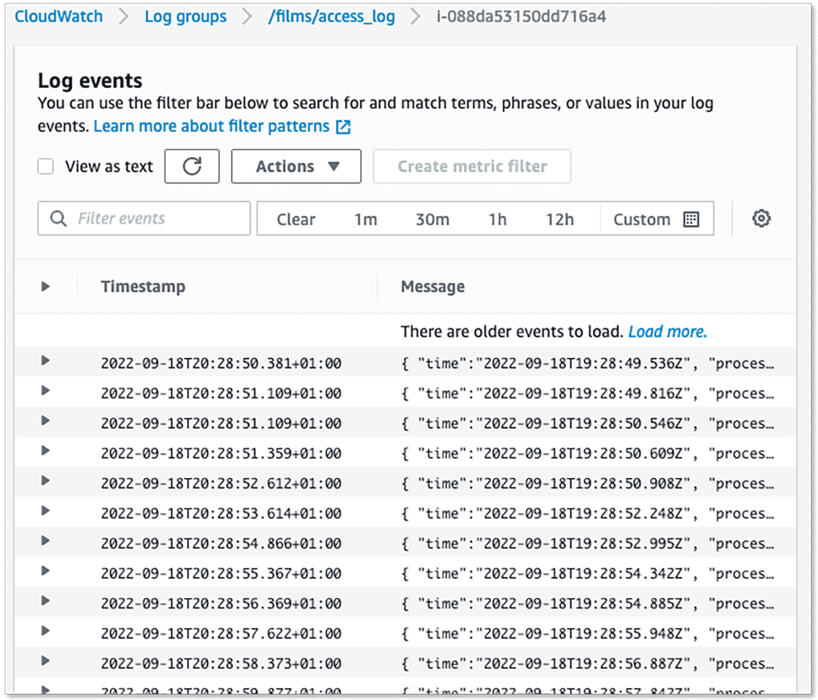


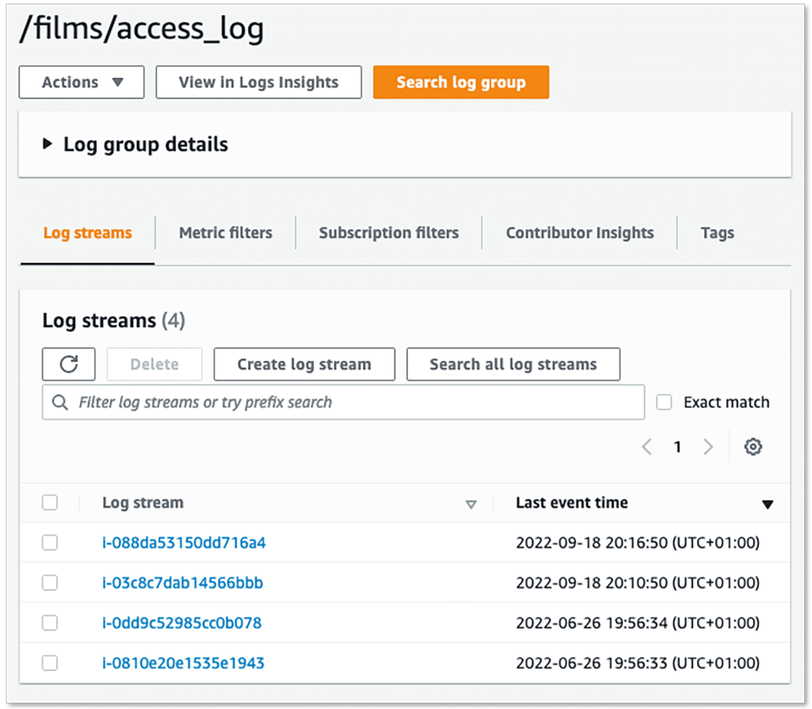
# AWS SysOps Administrador Associate

Challenge

CloudOps Guild

*Together, towards mastery in Cloud and DevOps*





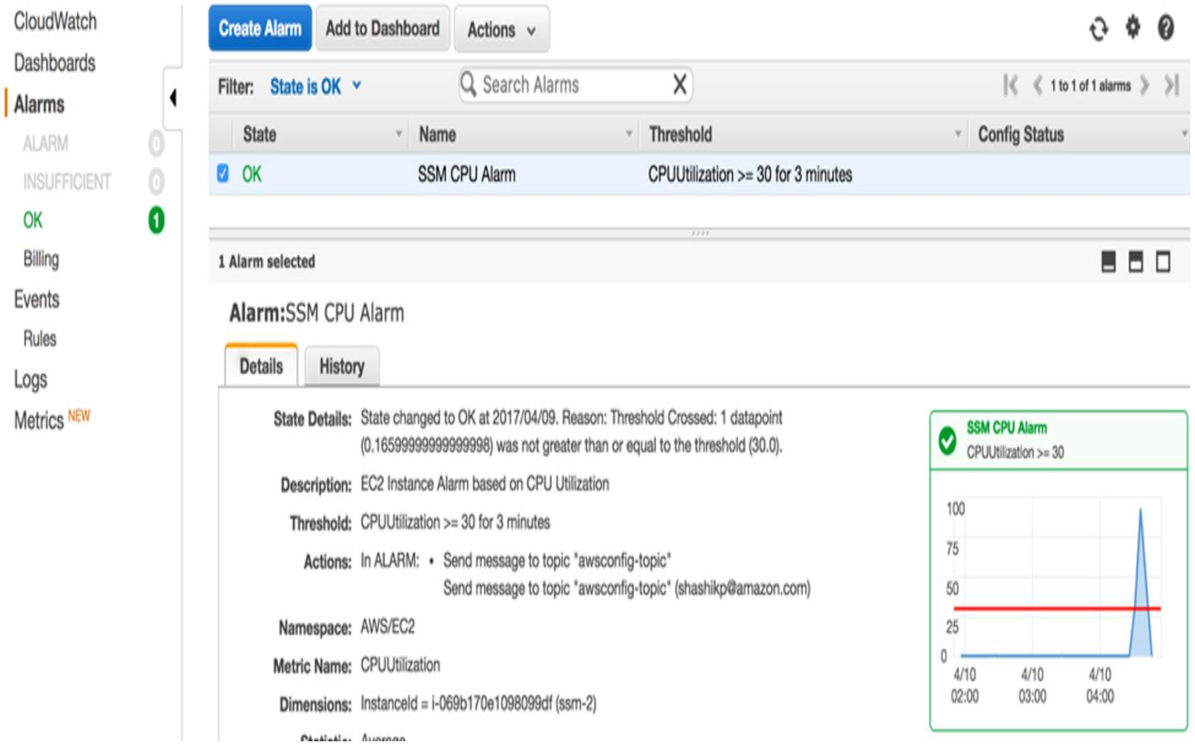
Raw events such as time, remoteIP, host, request, query, method, status, userAgent, and referer are recorded.

# CloudWatch Alarms

Las alarmas permiten supervisar métricas y disparar acciones si una condición se cumple (ej. CPU > 80%).

Tipos de alarma

| Tipo | Descripción |
|---|---|
| **Threshold** | Alarmas tradicionales: comparar métrica con umbral |
| **Composite** | Combina múltiples alarmas (ej. EC2 CPU > 80% *y* Latencia en ELB > 200ms) |




**Acciones comunes de alarmas**
Cuando la condición se cumple, la alarma puede:
•Enviar notificación a **SNS**
•Ejecutar una **función Lambda**
•Ejecutar una **Automation Document (SSM)**
•Disparar **Auto Scaling** (ej. añadir instancia)

📌 Importante: solo puedes asociar acciones cuando el estado de la alarma pasa a ALARM.

# CloudWatch Dashboards

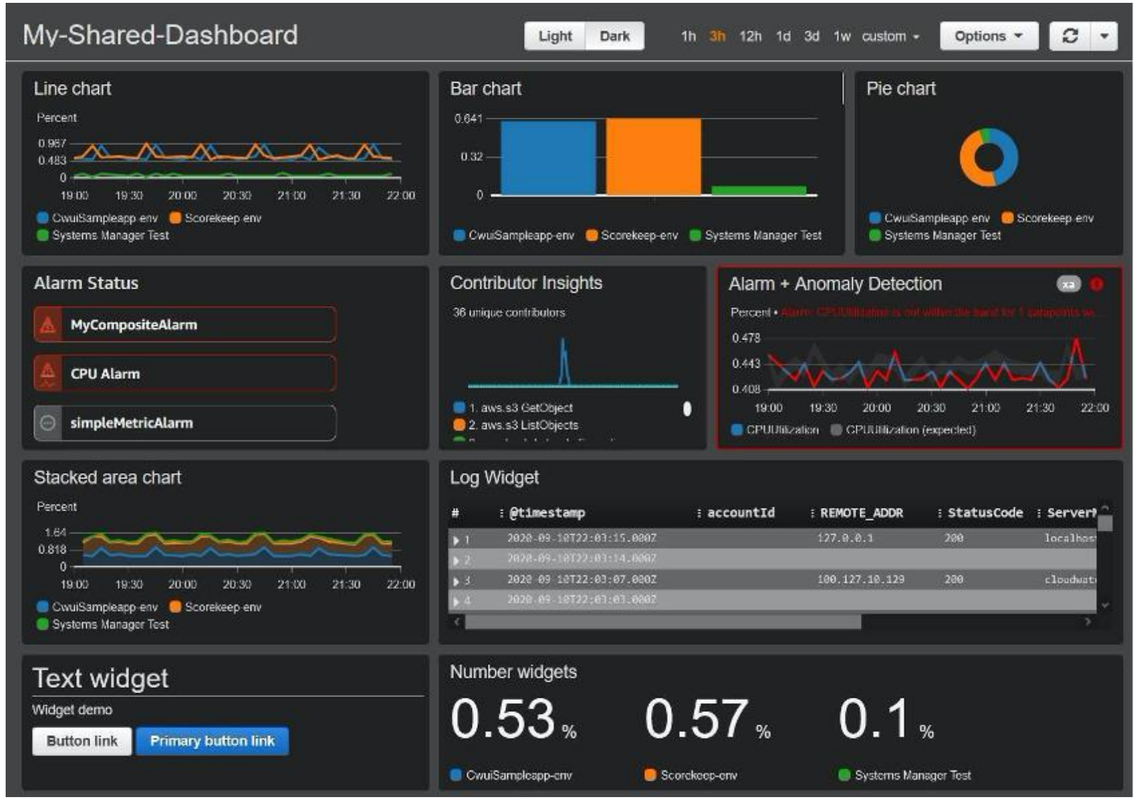
Paneles personalizados para visualizar múltiples métricas en un solo lugar con gráficos, texto, y widgets.

Te permite:

- Visualizar métricas en tiempo real
- Crear reportes ejecutivos
- Agrupar métricas por servicio, región o aplicación

Ejemplo de widgets que puedes incluir:

- Línea de CPU por instancia EC2
- Latencia de ELB
- Gráfico de invocaciones Lambda



# 2. Deep Dive - Logs en contexto

AWS SysOps Administrador Associate

Challenge

CloudOps Guild

*Together, towards mastery in Cloud and DevOps*

AWS SysOps
Administrador
Associate
Challenge

CloudOps Guild
Together, towards mastery in Cloud and DevOps

# Objetivo


En esta parte vamos a ver los tipos de logs que generan los servicios de AWS. Esto es clave en el examen, donde te preguntan cosas como:
*¿Dónde verías errores de red?* o *¿Cómo saber si una función Lambda falló?*"

## EC2

•**Ubicación local de logs**:
/var/log/messages (en Amazon Linux)
•**Para enviarlos a CloudWatch**:
Se necesita el **agente de CloudWatch Logs** instalado.

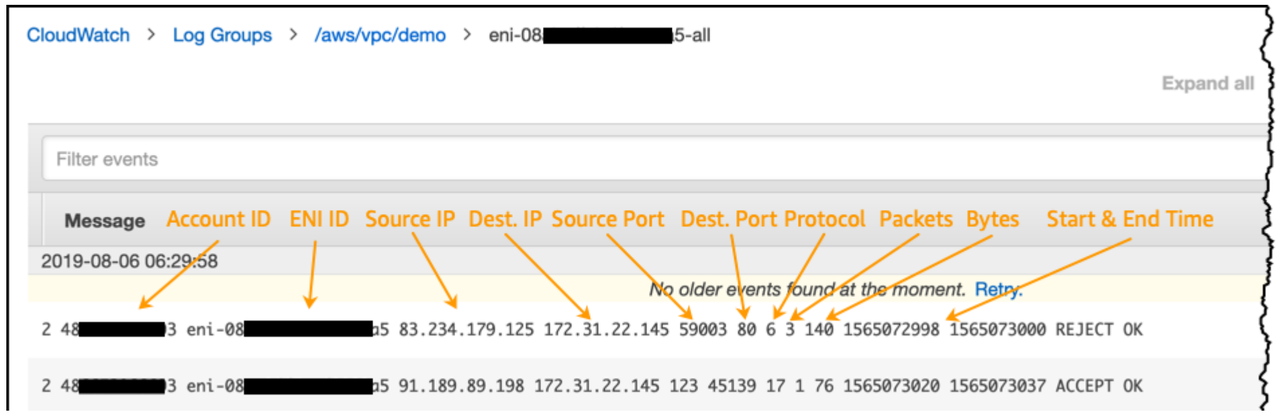
## Lambda

•Logs enviados automáticamente a **CloudWatch Logs**.
•Se organizan en grupos por nombre de función.
•Puedes ver errores y duración de ejecuciones.

## VPC Flow Logs

•Capturan tráfico de red a nivel de interfaz de red (ENI).
•Se usan para:

- Diagnosticar fallos de conectividad.
- Auditar accesos permitidos/denegados.

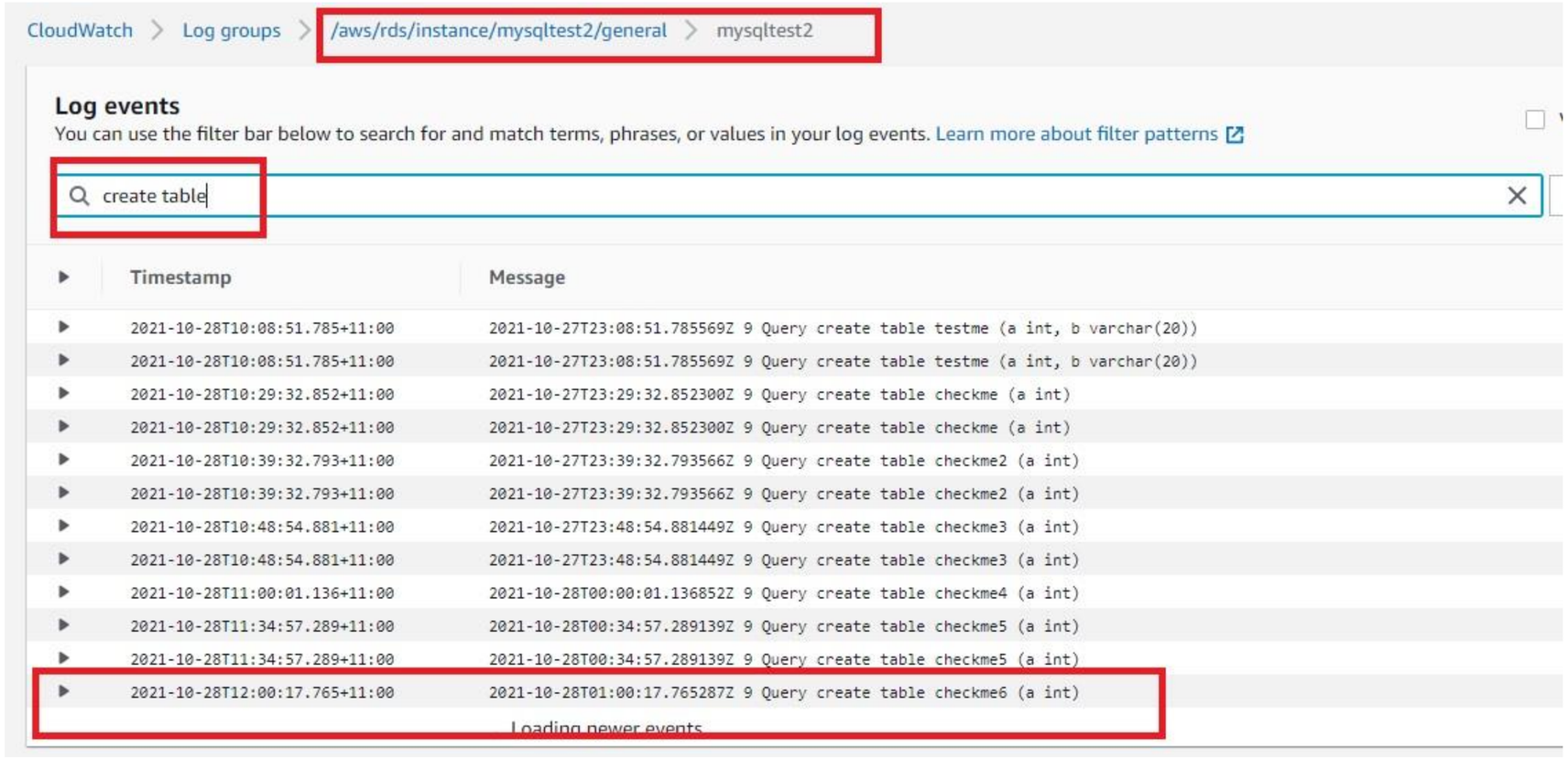


## RDS Logs

•Tipos comunes:

- **Error log**
- **General log**
- **Slow query log**

•Acceso desde la consola de RDS o CloudWatch Logs (si se configura).

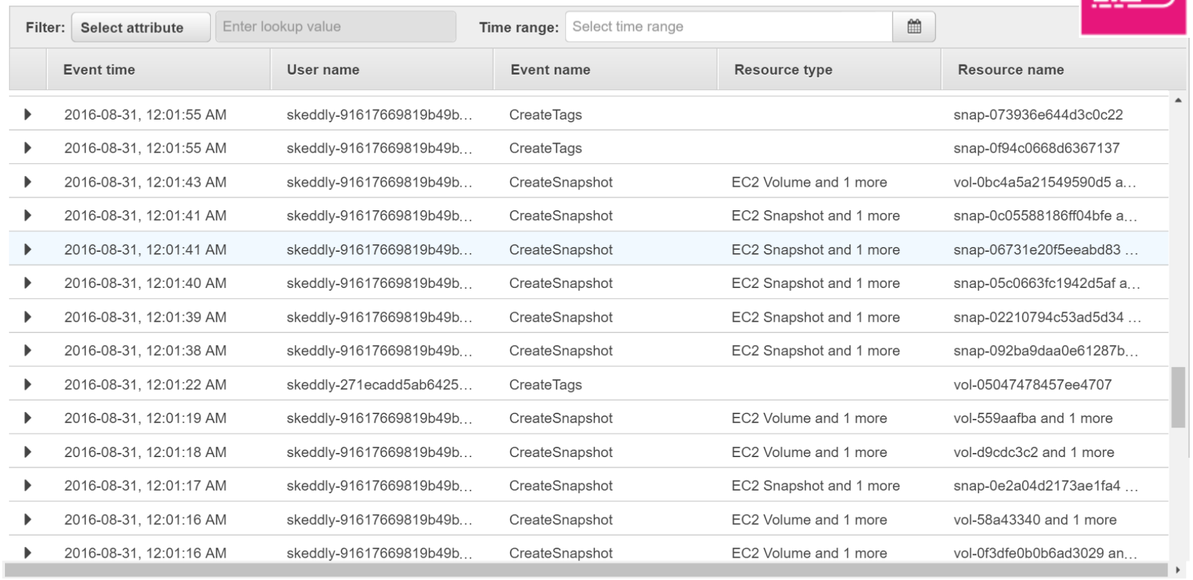




## S3 y CloudTrail

- **S3 Access Logs**: indican qué objeto fue accedido, por quién, desde dónde.
- **CloudTrail**: registra todos los eventos API a nivel de cuenta.

```
79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2be
test-bucket [31/Dec/2019:02:05:35 +0000] 63.115.34.165 - E63F54061B4D37D3
REST.PUT.OBJECT test-file.png
"PUT /test-file.png?X-Amz-Security-Token=token-here&X-Amz-Algorithm=AWS4-
HMAC-SHA256&X-Amz-Date=20191231T020534Z&X-Amz-SignedHeaders=content-
md5%3Bcontent-type%3Bhost%3Bx-amz-acl%3Bx-amz-storage-class&X-Amz-
Expires=300&X-Amz-Credential=ASIASWJRT64ZSKVRP62Z%2F20191231%2Fus-west-
2%2Fs3%2Faws4_request&X-Amz-Signature=XXX
HTTP/1.1" 200 - - - 1 - "https://s3.console.aws.amazon.com/s3/buckets/test-
bucket/?region=us-west-2&tab=overview"
"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_2) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/79.0.3945.88 Safari/537.36" -
Ox6nZZWoBZYJ/a/HLXYw2PVp1nXdSmqdp4fV37m/8SC54q7zTdlAYxuFOWYgOeixYT+yPs6prdc=
- ECDHE-RSA-AES128-GCM-SHA256 -
test-bucket.s3.us-west-2.amazonaws.com TLSv1.2
```

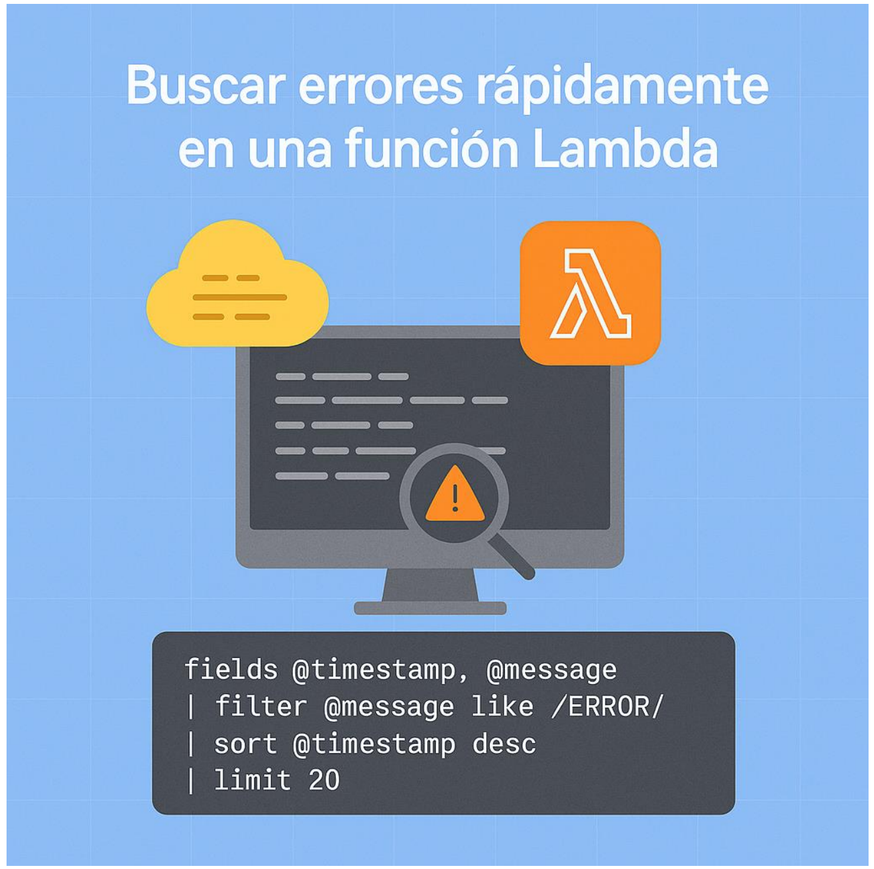


Filter: Select attribute | Enter lookup value | Time range: Select time range

| Event time | User name | Event name | Resource type | Resource name |
|---|---|---|---|---|
| 2016-08-31, 12:01:55 AM | skeddly-91617669819b49b... | CreateTags | | snap-073936e644d3c0c22 |
| 2016-08-31, 12:01:55 AM | skeddly-91617669819b49b... | CreateTags | | snap-0f94c0668d6367137 |
| 2016-08-31, 12:01:43 AM | skeddly-91617669819b49b... | CreateSnapshot | EC2 Volume and 1 more | vol-0bc4a5a21549590d5 a... |
| 2016-08-31, 12:01:41 AM | skeddly-91617669819b49b... | CreateSnapshot | EC2 Snapshot and 1 more | snap-0c05588186ff04bfe a... |
| 2016-08-31, 12:01:41 AM | skeddly-91617669819b49b... | CreateSnapshot | EC2 Snapshot and 1 more | snap-06731e20f5eeabd83 ... |
| 2016-08-31, 12:01:40 AM | skeddly-91617669819b49b... | CreateSnapshot | EC2 Snapshot and 1 more | snap-05c0663fc1942d5af a... |
| 2016-08-31, 12:01:39 AM | skeddly-91617669819b49b... | CreateSnapshot | EC2 Snapshot and 1 more | snap-02210794c53ad5d34 ... |
| 2016-08-31, 12:01:38 AM | skeddly-91617669819b49b... | CreateSnapshot | EC2 Snapshot and 1 more | snap-092ba9daa0e61287b... |
| 2016-08-31, 12:01:22 AM | skeddly-271ecadd5ab6425... | CreateTags | | vol-05047478457ee4707 |
| 2016-08-31, 12:01:19 AM | skeddly-91617669819b49b... | CreateSnapshot | EC2 Volume and 1 more | vol-559aafba and 1 more |
| 2016-08-31, 12:01:18 AM | skeddly-91617669819b49b... | CreateSnapshot | EC2 Volume and 1 more | vol-d9cdc3c2 and 1 more |
| 2016-08-31, 12:01:17 AM | skeddly-91617669819b49b... | CreateSnapshot | EC2 Snapshot and 1 more | snap-0e2a04d2173ae1fa4 ... |
| 2016-08-31, 12:01:16 AM | skeddly-91617669819b49b... | CreateSnapshot | EC2 Volume and 1 more | vol-58a43340 and 1 more |
| 2016-08-31, 12:01:16 AM | skeddly-91617669819b49b... | CreateSnapshot | EC2 Volume and 1 more | vol-0f3dfe0b0b6ad3029 an... |

## Logs Insights – Búsqueda avanzada

"Cuando tenemos muchos logs en CloudWatch, usamos **Logs Insights** para hacer búsquedas rápidas, por ejemplo: ¿Hubo un error hoy en una función Lambda?"




📌 Esta consulta:

- Filtra los mensajes que contienen la palabra "ERROR"
- Muestra las columnas de timestamp y mensaje
- Ordena los resultados del más reciente al más antiguo
- Muestra solo los últimos 20

# 3. Automatización y Remediación

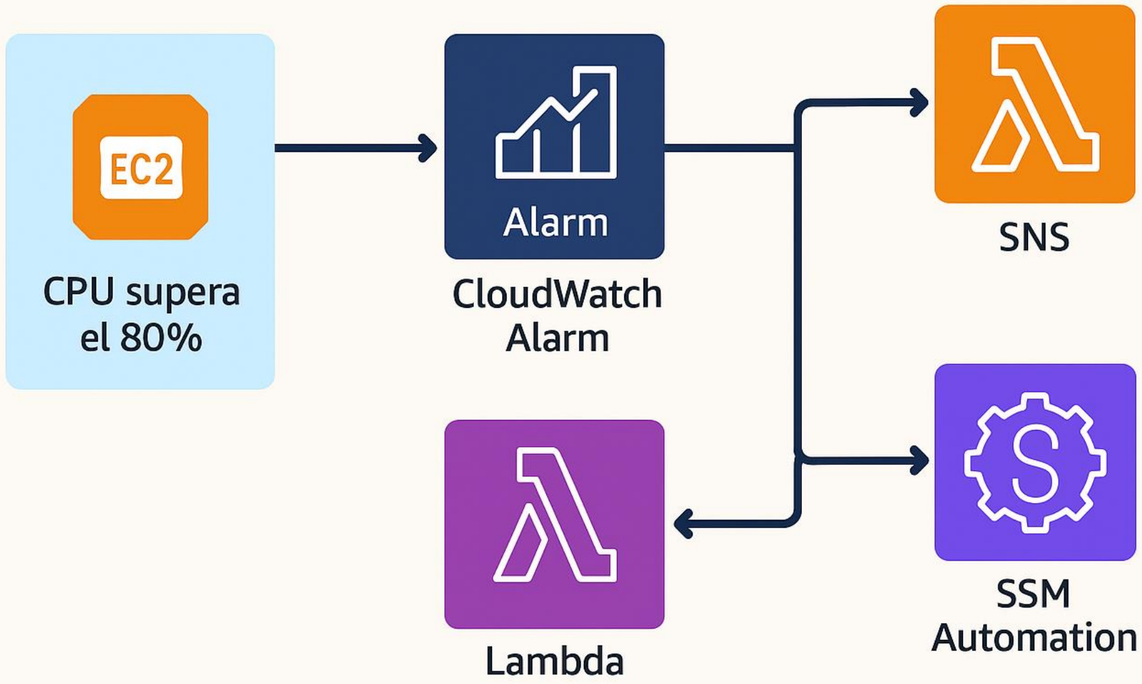
AWS SysOps Administrador Associate

Challenge

CloudOps Guild

*Together, towards mastery in Cloud and DevOps*

# Remediación automática




🔄 **Paso a paso del flujo**

🔶 **1. EC2: CPU supera el 80%**
•Se detecta que la métrica CPUUtilization de una instancia EC2 **supera el 80%**.
•Este es el umbral definido como condición para generar una alarma.

🔶 **2. CloudWatch Alarm**
•Se activa una **alarma de CloudWatch** configurada previamente.
•Esta alarma está vinculada a la métrica CPUUtilization.

🔶 **3. Disparadores vinculados a la alarma**
La alarma puede ejecutar **una o varias acciones automáticas**:

🔷 **Opción A: SNS (Simple Notification Service)**
•Envía una notificación (email, SMS, HTTP) a suscriptores.
•Puede ser utilizada para invocar:
  •Funciones **Lambda**
  •Automatizaciones en **SSM**
  •Alertas a herramientas de monitoreo externas

🔷 **Opción B: Lambda**
•Ejecuta una función que puede:
  •Reiniciar la instancia
  •Escalar vertical/horizontalmente
  •Generar reportes o alertas personalizadas

🔷 **Opción C: SSM Automation**
•Ejecuta un **Runbook (Document)** predefinido.
•Puede realizar acciones como:
  •Parar o iniciar instancias
  •Ejecutar comandos de diagnóstico
  •Aplicar configuraciones correctivas

## Alternativa: Automatización basada en eventos

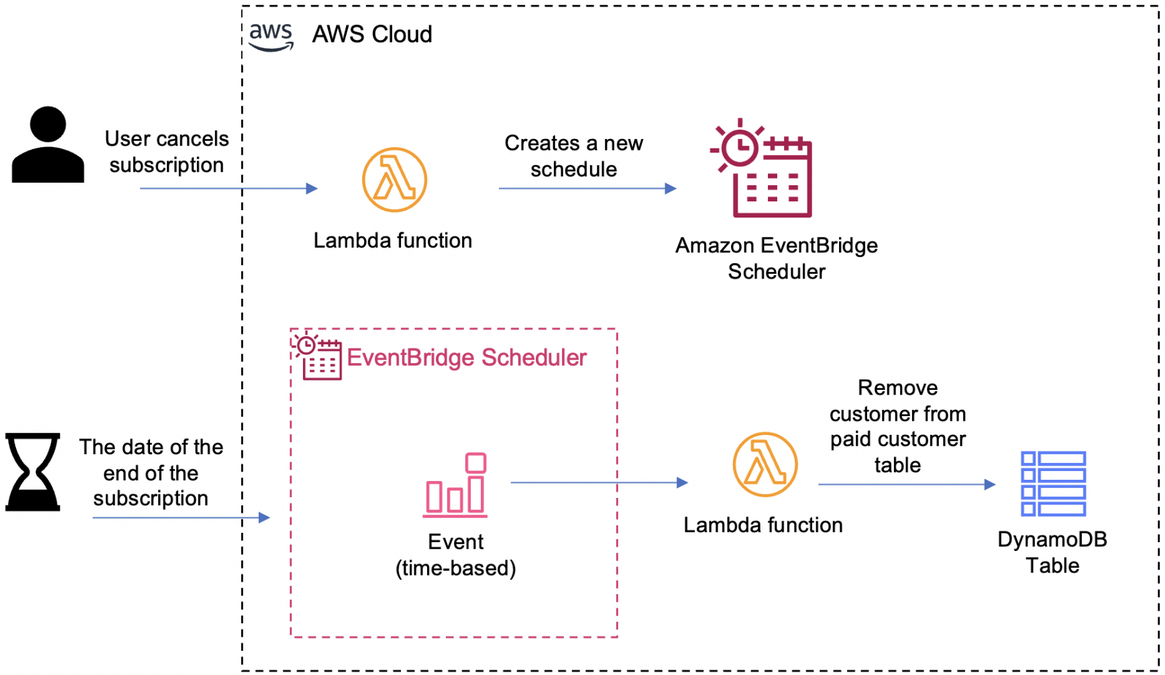
"Si no se basa en una métrica sino en un evento de estado (por ejemplo, la instancia pasó a 'stoppec puedes usar **Amazon EventBridge**."

## Flujo con EventBridge:

1.Evento detectado (EC2 Instance State-change Notification)

2.Regla de EventBridge lo intercepta.

3.Ejecuta:
- •Lambda
- •Step Function
- •SSM Automation
- •Notificación



# 4. Recomendaciones generales

AWS SysOps Administrador Associate

Challenge

CloudOps Guild

*Together, towards mastery in Cloud and DevOps*



# Recomendaciones finales

- Memoriza **cuáles servicios generan logs automáticamente** y cuáles requieren configuración manual.
- Entiende **cómo conectar una alarma a una acción (SNS, Lambda, etc.)**.
- Aprende a diferenciar entre **Logs, Metrics y Events**.
- Recuerda que **CloudWatch Dashboards son solo visuales, no disparan acciones**.
- Practica crear una alarma y vincularla a una acción (Lambda o SSM).
- Explora Logs Insights con diferentes filtros.
- Revisa ejemplos de remediación en la consola y en documentación.
- En preguntas de examen o labs:
  - **NO asumas que todos los servicios envían logs automáticamente a CloudWatch Logs.**
  - Siempre evalúa si hay que **habilitar el log delivery** y si debes **crear el grupo de logs tú mismo** o AWS lo hará.
  - **AWS te evaluará sobre cómo actuar ante eventos operativos sin intervención manual.**

# 5. Preguntas ejemplos

## AWS SysOps Administrador Associate

Challenge

CloudOps Guild

*Together, towards mastery in Cloud and DevOps*



**1. Activar logs en Application Load Balancer**
**Escenario:**
Una empresa quiere habilitar auditoría en su infraestructura web. El equipo de seguridad solicita acceso a los registros de tráfico HTTP del Application Load Balancer (ALB) para análisis.

**Pregunta:**
¿Cuál es el procedimiento correcto para activar los logs de acceso en un ALB?

**A.** Activar VPC Flow Logs en las subnets públicas donde está el ALB
**B.** Habilitar logs de acceso en el ALB y especificar un bucket de Amazon S3
**C.** Configurar CloudTrail para capturar eventos del ALB
**D.** Agregar un agente CloudWatch Logs al ALB
**E.** No hay que hacer nada, los logs de los ALB se envían automáticamente a Cloudwatch.



**2. Detectar detención inesperada de una instancia EC2**
**Escenario:**
Un administrador de sistemas nota que una instancia EC2 se detuvo sin intervención humana. Se requiere automatizar la detección y notificación de este tipo de eventos.

**Pregunta:**
¿Qué servicio de AWS usarías para detectar este tipo de eventos y notificar al equipo?

**A.** AWS Config
**B.** Amazon CloudTrail
**C.** Amazon EventBridge con una regla de EC2 Instance State-change
**D.** CloudWatch Logs



**3. Troubleshooting de fallo en función Lambda**
**Escenario:**
Una función Lambda falla de forma intermitente. El desarrollador quiere entender por qué y revisar los mensajes de error de cada ejecución.

**Pregunta:**
¿Qué herramienta proporciona el acceso más directo a los errores generados durante la ejecución de una función Lambda?

**A.** CloudTrail
**B.** Amazon Inspector
**C.** CloudWatch Logs
**D.** AWS Config



**4. Enviar logs desde una instancia EC2 a CloudWatch**
**Escenario:**
Un servidor EC2 contiene una aplicación personalizada que genera archivos de log en /var/log/app.log. Se desea visualizar esos logs en CloudWatch Logs para monitoreo centralizado.

**Pregunta:**
¿Qué debes hacer para enviar estos logs desde la instancia EC2 a CloudWatch Logs?

**A.** Habilitar la opción "logsToCloudWatch" en la consola EC2
**B.** Instalar y configurar el agente de CloudWatch Logs en la instancia
**C.** Activar CloudTrail y vincularlo con CloudWatch Logs
**D.** Crear un bucket de S3 y habilitar versionado
**E.** Nada, los logs se envían automáticamente a un logs group de Cloudwatch

**5. Analizar tráfico de red en VPC Flow Logs**
**Escenario:**
Un equipo de redes necesita analizar tráfico denegado en una interfaz de red específica dentro de su VPC para detectar un posible fallo en las reglas de seguridad.

**Pregunta:**
¿Qué se requiere para recolectar y analizar el tráfico en los VPC Flow Logs?

**A.** Instalar CloudWatch Agent en la VPC
**B.** Crear Flow Logs y enviarlos a CloudWatch Logs o S3
**C.** Usar Amazon GuardDuty
**D.** Consultar los registros desde AWS Config

# Agradecimientos


CloudOps Guild
*Together, towards mastery in Cloud and DevOps*

AWS COMMUNITY
CARTAGENA




**Próxima sesión:**

**Semana 4: Monitoreo y Logs (Laboratorios)**