[Publish] - 1. Habilita los registros de acceso al utilizar ELBv2

El hallazgo de seguridad **"Habilitar los registros de acceso (Access logs) al usar ELBv2"** resalta la necesidad crítica de tener visibilidad sobre el tráfico que fluye a través de tus aplicaciones. Los balanceadores de carga (Application Load Balancers y Network Load Balancers) son la puerta de entrada a tus servicios.

Estos registros capturan información detallada sobre cada una de las solicitudes recibidas por tu balanceador, incluyendo:

- La dirección IP del cliente.
- La hora de la solicitud.
- La ruta y el método de la solicitud (GET, POST, etc.).
- Los códigos de respuesta del backend.
- La latencia y los bytes transferidos.

Tener esta información es fundamental para la **investigación de incidentes de seguridad**, el **análisis de tráfico**, la **depuración de errores** de la aplicación y el **cumplimiento de auditorías**. Sin estos registros, es casi imposible saber quién ha accedido a tus sistemas, cuándo y cómo.

Análisis de los Balanceadores de Carga Reportados

Los siguientes balanceadores de carga (ELBv2) han sido identificados por no tener los registros de acceso habilitados.

Tipo	Nombre del Recurso	Número de Cuenta
LoadBalancer	loadbalancer/app/Colabora/1d5feb4717929008	398984081329
LoadBalancer	loadbalancer/app/django-lb/30a6513ddc6c110e	002670977573
LoadBalancer	loadbalancer/app/GS-Connection-SAP/fbfa9801af1a972	613703092215
LoadBalancer	loadbalancer/app/gs-services/844a3cc33b5	002670977573

	de0c7	
LoadBalancer	loadbalancer/app/ServDigitales/392f0dbef015d8d1	890342916428
LoadBalancer	loadbalancer/net/datalakeNLBSAPdevint/b824f9f600578d9a	613703092215

Preguntas para tu Equipo (Acción Requerida)

A diferencia de otros hallazgos, la necesidad de registros de acceso es universal. No hay un escenario legítimo en un entorno de producción o desarrollo donde no se deban tener. Sin embargo, para una implementación ordenada, por favor considera lo siguiente:

1. **Bucket de S3 Centralizado:** ¿Se deben enviar todos los registros de acceso a un único bucket de S3 centralizado (la mejor práctica para la seguridad sería utilizar la cuenta de Log Archive), o cada cuenta/aplicación gestionará su propio bucket?
2. **Políticas de Ciclo de Vida:** ¿Qué política de retención de datos necesitamos para estos registros? (ej. 365 días). Debemos configurar políticas de ciclo de vida en el bucket de S3 para mover los registros a un almacenamiento más económico (como S3 Glacier) o eliminarlos después de un cierto período para controlar los costos.

Consideraciones de Costo

Habilitar los registros de acceso introduce costos mínimos, pero es importante entenderlos.

- **ELBv2:** No hay ningún cargo por parte del balanceador de carga por habilitar esta función.
- **Amazon S3:**
  - **Costo de Almacenamiento:** Se te cobrará por el espacio de almacenamiento que ocupen los archivos de registro en S3. Este costo depende del volumen de tráfico que reciban tus balanceadores. Para un tráfico moderado, el costo suele ser de unos pocos dólares al mes.
  - **Costo de Solicitudes (PUT):** El balanceador de carga realizará solicitudes `PUT` a S3 para escribir los archivos de registro, lo que incurre en un costo muy pequeño por cada mil solicitudes.

Conclusión sobre Costos:

El costo de almacenar los registros de acceso es marginal en comparación con el inmenso valor que proporcionan para la seguridad y la operatividad. El riesgo de no tener visibilidad durante un incidente de seguridad supera con creces el costo del almacenamiento en S3.

Cómo Solucionarlo: Habilitar los Registros de Acceso

El proceso para habilitar los registros de acceso es el mismo para cada balanceador de carga.

1. **Crear o Designar un Bucket de S3:**
   - Asegúrate de tener un bucket de S3 para almacenar los registros.
   - Este bucket debe tener una política que permita al servicio de Elastic Load Balancing escribir objetos en él. AWS proporciona una política de ejemplo que puedes adaptar.
2. **Habilitar los Registros en el Balanceador:**
   - Navega a la consola de **EC2**.
   - En el panel de navegación izquierdo, en **Carga y Escalado**, elige **Balanceadores de Carga**.
   - Selecciona uno de los balanceadores de la lista.
   - En la pestaña **Atributos**, haz clic en **Editar**.
   - En la sección **Monitoreo**, marca la casilla **Habilitar** para los **Registros de acceso**.
   - Especifica el nombre del bucket de S3 que preparaste en el paso 1.
   - Haz clic en **Guardar cambios**.
3. **Repetir:** Realiza este proceso para todos los balanceadores de carga identificados.

Recomendación

Se recomienda **habilitar los registros de acceso en todos los balanceadores de carga listados**. Esta es una práctica de higiene de seguridad fundamental.

Refrencias:

Enable access logs for your Application Load Balancer - Elastic Load Balancing