ManageEngine
Log360

5 errores comunes en la configuración de AWS que llevan a ciberataques

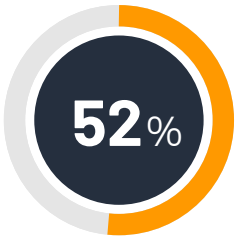
www.manageengine.com/latam/log360

Tabla de contenidos

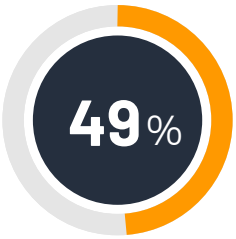
Introducción

La tecnología de nube ha estado en el mercado desde hace casi una década. Ahora, dado el aumento en la adopción del trabajo a distancia, 59 por ciento del uso de la nube por parte de las empresas supera sus planes anteriores. Aunque es conveniente para las operaciones empresariales, este auge en la adopción de la nube y el trabajo a distancia también es un imán para que los ciberdelincuentes lancen ataques, y muchas empresas están mal preparadas para enfrentar las amenazas de seguridad en la nube. Los atacantes lo ven todo; vigilan a las empresas constantemente y buscan vulnerabilidades y oportunidades para hackear.

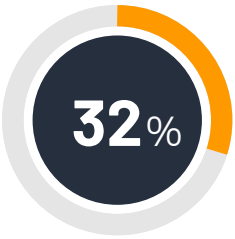
Cuando se trata de la nube, los hackers suelen aprovecharse de los errores y comportamientos humanos más que de los fallos técnicos de seguridad. Según una encuesta reciente, los **errores de configuración de la nube son la principal causa de las violaciones de datos en la nube**. Además, las estadísticas revelan que



de los encuestados dijeron que el **desconocimiento** de la seguridad en la nube y de las políticas causó una violación de datos.



de los encuestados afirmaron que la **falta de controles adecuados** y vigilancia son responsables de la pérdida de datos.



piensan que la negligencia en el **comportamiento de los intrusos** dio lugar a incidentes de seguridad.

Estas cifras revelan una clara necesidad de gestionar los errores de configuración de la nube de forma más eficaz y eficiente para evitar incidentes adversos. Indican la necesidad de implementar una herramienta que pueda proporcionar una mejor visibilidad de la infraestructura de la nube, detectar y remediar automáticamente los errores de configuración y enviar notificaciones oportunas en caso de cambios de configuración inapropiados y peligrosos.

En este e-book, hablaremos de los errores de configuración más comunes en Amazon Web Services (AWS) que debería evitar para frenar los incidentes y las infracciones de seguridad.

Configurar AWS Cloud Trail:
Requisitos previos para la auditoría

Para obtener una visibilidad completa en su entorno de AWS Cloud y para reforzar las configuraciones de seguridad, primero debe **habilitar la recopilación de logs de CloudTrail**. CloudTrail es un servicio de AWS que proporciona el historial de eventos para toda la actividad de la cuenta de AWS. Genera datos de log para todas las llamadas a la API realizadas dentro de AWS, incluida la consola de gestión de AWS, los kits de desarrollo de software (SDK), las herramientas de línea de comandos y otros servicios de AWS. Habilitar el registro de CloudTrail para todas las regiones ayuda a prevenir posibles brechas en el monitoreo, y también le permite cumplir con los mandatos normativos y llevar a cabo investigaciones forenses después de los incidentes.

Los datos de log generados se almacenan en un bucket de Amazon S3. Sin embargo, si los ciberatacantes lograran ingresar en su red en la nube, lo primero que harían sería desactivar su CloudTrail y tratar de comprometer los archivos de log. Por esta razón, es vital tomar las siguientes precauciones para que sus archivos de log de CloudTrail sean a prueba de ataques:

- **Garantizar la integridad de los archivos de log de CloudTrail:** Habilite la validación de la integridad de los archivos de log de CloudTrail para poder rastrear cualquier cambio realizado en los datos de los archivos de log después de que se almacenen en el bucket de S3.
- **Evitar los intentos de acceso no autorizados:** Habilite el registro de acceso para el bucket de CloudTrail S3 para que pueda rastrear todas las solicitudes de acceso y detectar los intentos de acceso no autorizados.
- **Duplicar la seguridad para acceder a los archivos de log:** Active la opción de autenticación multifactor (MFA) para eliminar los buckets de CloudTrail S3, de modo que incluso si una cuenta se ve comprometida, pueda garantizar la seguridad de los archivos de log.

Errores comunes en la configuración de AWS y **cómo corregirlos**

Error 1

Proporcionar acceso sin restricciones a los grupos de seguridad de EC2

Los grupos de seguridad (SG) asociados a las instancias de AWS Elastic Cloud Compute (EC2) son similares a un firewall y controlan el acceso a nivel de protocolo y puerto. Estos SG son un conjunto de reglas que filtran el tráfico entrante (ingreso) y saliente (egreso) de una instancia EC2. Una instancia EC2 puede tener varios SG, y las reglas de un SG se pueden modificar en cualquier momento. Estas reglas de SG permiten que un origen específico, como una IP o un rango de direcciones IP, acceda a la instancia utilizando puertos de destino o un protocolo determinado, como el Protocolo de Control de Transmisión (TCP), el Protocolo de Datagramas de Usuario (UDP), el Protocolo Simple de Transferencia de Correo (SMTP) o HTTP/HTTPS. Al configurar las reglas de SG, asegúrese de:

- Dar permisos sólo a rangos de IP específicos para acceder a las instancias EC2.
- Permitir el tráfico sólo desde los puertos especificados. No se recomienda abrir todos los puertos, ya que abre la instancia al tráfico no deseado.

Si no se tienen en cuenta estos aspectos al configurar los SG, esto no sólo puede obstaculizar las operaciones diarias, sino que también puede atraer una amplia gama de ataques maliciosos, como fuerza bruta, denegación de servicio (DoS) o man-in-the-middle (MITM).

Cómo detectar y solucionar este problema

Cuando habilita el registro mediante CloudTrail y se monitorean los datos de log mediante una herramienta de gestión de logs de terceros o una solución nativa, debería poder detectar el acceso no restringido. Configure su herramienta de monitoreo para detectar si los SG conectados a sus instancias EC2 permiten el acceso sin restricciones para los puertos que no sean 25 (SMTP), 80 y 443 (HTTP y HTTPS).

Error 2

Hacer públicas las imágenes de equipo de Amazon (AMI), o proporcionar acceso sin restricciones a las AMI

Una AMI proporciona la información necesaria para lanzar una instancia EC2. Cuando se crea una instancia EC2, se debe especificar la AMI a la que pertenece. Una AMI incluye:

- Los permisos que controlan las cuentas de AWS para lanzar instancias EC2.
- Un mapeo de los dispositivos en bloque que especifica los volúmenes que se asociarán a la instancia cuando se lance.
- Una plantilla que contiene la configuración de software (sistema operativo, servidor de aplicaciones y aplicaciones) que se utilizará para lanzar la instancia EC2.

Los usuarios de AWS pueden crear sus propias AMI, utilizar las AMI disponibles públicamente o comprar AMI personalizadas. Cuando un usuario crea una AMI, tiene la opción de hacerla pública, compartirla sólo con cuentas específicas o hacerla privada.

El acceso sin restricciones a las AMI o el hecho de hacerlas públicas hará que estas AMI estén disponibles en la Comunidad de Amazon; cualquier persona que tenga una cuenta de AWS puede utilizar estas AMI disponibles públicamente para lanzar instancias EC2.

Cómo solucionar este problema

Dado que las AMI contienen datos propietarios o sensibles, como las capturas de pantalla de aplicaciones específicas de la empresa, debe asegurarse de que siempre estén configuradas como privadas. Cualquier AMI que esté disponible públicamente se debe monitorear cuidadosamente.

Error 3

No cancelar las claves de acceso de usuario no utilizadas

Las claves de acceso de usuario de la gestión de accesos e identidades (IAM) de AWS son credenciales a largo plazo para que los usuarios de IAM o los usuarios de la ruta de la cuenta de AWS accedan a las CLI o API de AWS. Es esencial que proporcione prudentemente las claves de acceso de usuario a sus empleados y que también monitoree las claves de acceso de usuario de forma regular para eliminar las claves de acceso de usuario no utilizadas o inapropiadas.

Cualquier persona que tenga su clave de acceso obtiene el mismo nivel de acceso a sus recursos de AWS. AWS toma las medidas necesarias para proteger sus claves de acceso; teniendo en cuenta el modelo de responsabilidad compartida, usted también debe garantizar la seguridad de sus claves de acceso. No eliminar las claves de acceso no utilizadas puede causar que las cuentas de usuario se vean comprometidas o incluso que sean apropiadas por otros. Además, eliminar estas claves no utilizadas le ayudará a cumplir con muchas normativas como ISO 27001, HIPAA, PCI DSS, etc.

Consejos adicionales:

Además de eliminar las claves de acceso de usuario no utilizadas, asegúrese de tomar las siguientes medidas de seguridad:

- No proporcione claves de acceso a sus proveedores externos, ya que podrían obtener acceso permanente a su cuenta.
- Utilice credenciales de seguridad temporales (roles IAM) siempre que sea posible en lugar de claves de acceso. Esto ayudará a prevenir el acceso no autorizado de usuarios no deseados.
- Si es posible, no tenga claves de acceso para el usuario raíz de su cuenta de AWS. Si tiene claves de acceso para su usuario raíz, un solo compromiso podría exponer todo su recurso en la nube.
- Utilice diferentes claves de acceso para diferentes aplicaciones. Esto ayudará a proteger las otras aplicaciones si las claves de acceso de una aplicación se ven comprometidas.
- Rote sus claves de acceso periódicamente para reducir el riesgo de que se vean comprometidas.
- Configure la MFA para sus operaciones más sensibles, de modo que sus recursos permanezcan seguros incluso si la clave de acceso se ve comprometida.

Consejos adicionales:
¿Cuáles requisitos de cumplimiento le obligan a gestionar las claves de usuario no utilizadas?

- ISO 27001 - A.9.2.4 - Gestión de la información de autentificación secreta de los usuarios.

- HIPAA 164.308(a)(5)(ii)(D) - Procedimientos para crear, cambiar y proteger contraseñas.

Cómo detectar y solucionar este problema Auditar las cuentas de AWS es una de las mejores formas d e detectar las claves de acceso no utilizadas. Siga los pasos a continuación en su consola de gestión de AWS para detectar y eliminar las claves de acceso no utilizadas.

- Inicie sesión en la consola de AWS. Seleccione **Usuarios** en la opción de servicio IAM del panel lateral izquierdo.
- Haga clic en el nombre de usuario que desea auditar.
- En el panel siguiente, haga clic en la pestaña **Credenciales de seguridad**.
- Examine la columna **Último uso** y asegúrese de que no diga N/A. Si dice N/A, significa que la clave de acceso nunca ha sido utilizada por el usuario seleccionado y por lo tanto es una clave no utilizada.

Tendrá que repetir este procedimiento para cada cuenta de usuario sospechosa, y comprobar si la clave de acceso está utilizada o no utilizada. Como alternativa, también puede encontrar las claves de acceso no utilizadas descargando el informe de credenciales y ejecutando comandos específicos en la interfaz de línea de comandos (CLI).
Después de obtener la lista de claves de acceso no utilizadas, puede eliminarlas desde la misma consola.

Error 4

Proporcionar acceso sin restricciones al cluster de Redshift

Un almacén de datos de Redshift es un conjunto de recursos informáticos llamados nodos, que se organizan en un grupo llamado cluster. Cada cluster ejecuta un motor de Amazon Redshift y contiene una o varias bases de datos.

Cuando se aprovisiona por primera vez un cluster de Amazon Redshift, nadie tiene acceso a él de forma predeterminada. Para conceder a otros usuarios acceso a este clúster, debe asociarlo a un grupo de seguridad y definir reglas para permitir el acceso.

Nota:
Si está en la plataforma EC2-VPC, puede asociar un grupo de seguridad de nube privada virtual (VPC) existente o definir uno nuevo. Si está en la plataforma EC2-Classic, debe definir el grupo de seguridad y asociarlo a un cluster. Si no configura correctamente los grupos de seguridad asociados al cluster, estos clusters de Redshift serán de acceso público. Por tanto, cualquiera en Internet puede establecer una conexión a su base de datos, aumentando el riesgo de seguridad de ataques de fuerza bruta, inyecciones SQL o ataques DoS.

Consejo adicional:
Para proteger aún más el tráfico del cluster de Redshift, habilite el cifrado para todo el tráfico en la red. Para ello, debe tener habilitado el parámetro **require_ssl**.

Cómo solucionarlo
No configure el grupo de seguridad de forma que esté abierto a un amplio rango de direcciones IP. Proporcione acceso entrante a rangos de IP específicos, y también exponga sólo los puertos que sean necesarios.

Error 5

Acceso excesivamente permisivo a los recursos en la nube

Nunca permitiríamos ninguna conexión directa a nuestros dispositivos de red a través de Internet sin un firewall. Sin embargo, cuando se trata de la nube, a veces los administradores omiten involuntariamente la configuración de las reglas de acceso entrante; esto permite el acceso directo de recursos sensibles a través de Internet. A continuación, se presentan algunos ejemplos de acceso excesivamente permisivo proporcionado a los componentes y recursos en la nube que podrían causar un desastre de seguridad en la nube.

- **Cluster de Kubernetes expuesto a Internet:** En los últimos dos años, el uso de Kubernetes ha aumentado rápidamente, ya que muchas empresas de nube lo han adoptado como la forma predeterminada de organizar y escalar sus cargas de trabajo basadas en contenedores. Un análisis reciente muestra que los servicios etcd, un almacén de clave-valor distribuido de código abierto que se utiliza para mantener y gestionar la información crítica que los sistemas distribuidos necesitan para seguir funcionando, han aparecido en Internet sin la autenticación adecuada.

Según esta investigación, una simple búsqueda en Shodan reveló casi 2.284 servidores etcd en Internet, lo que evidencia que se trata de un problema al que se debe prestar atención cuando se configuran los clusters. Asegúrese de que el puerto 2379 para el cluster de Kubernetes no está expuesto a internet.

Cómo solucionarlo

Constantly audit and review the VPC security groups and network access control lists (NACLs) that guard the inbound and outbound traffic to resources. Track changes to these groups and get alerted when the above protocols and ports are configured for unrestricted access.

Consejos adicionales:

Además de eliminar las claves de acceso de usuario no utilizadas, asegúrese de tomar las siguientes medidas de seguridad:

- **No es solo el etcd:** Dependiendo de la configuración de su cluster, otros servicios también implican vulnerabilidades que podrían provocar un incidente de seguridad. Por ejemplo, la API Kubelet que es utilizada por Kubernetes para gestionar contenedores en nodos individuales o en algunos clusters; si esta API está disponible sin autenticar, podría generar un exploit de Kubelet. Los hackers podrían aprovechar esta oportunidad para ejecutar código en sus contenedores, e incluso tomar el control de todo su cluster, por lo que siempre debe tener un gateway de autenticación para la API de Kubelet.

- **Un contenedor comprometido es igual a un cluster comprometido:** Como sabe, un cluster de Kubernetes aloja un conjunto de contenedores de aplicaciones, por lo que es importante garantizar la seguridad de todas y cada una de las aplicaciones que se ejecutan en el cluster para evitar que todo el cluster se vea comprometido.
  Si el control de acceso basado en roles (RBAC) no está configurado para estos clusters, los atacantes que obtienen acceso a un solo contenedor en un cluster pueden escalar fácilmente sus privilegios y obtener el control total de éste. Por lo tanto, siempre se debe configurar el RBAC para estos clusters. Si realmente quiere seguir el comportamiento predeterminado en el que se incorpora un token que da acceso a la API de Kubernetes en cada contenedor, asegúrese de restringir los derechos que el usuario tiene sobre los demás recursos del cluster.

- **Acceso sin restricciones a puertos conocidos:** Asegúrese de que los puertos y protocolos conocidos no están habilitados en el host de la nube sin ninguna restricción. De lo contrario, esto permitiría el acceso fácil y sin restricciones a estos hosts por parte de actores maliciosos a través de Internet. Garantice el acceso a las entidades necesarias para:

  - **Sistema de archivos de internet común (CIFS)** para evitar el acceso no autorizado a los datos.
  - **Protocolo de transferencia de archivos (FTP),** a través del puerto 20/21 para evitar el acceso no autorizado a los datos y la violación de datos accidental.
  - **Protocolo de control de mensajes de Internet (ICMP)** para evitar el acceso no autorizado a los datos, el análisis de vulnerabilidades de red malicioso, o los ataques DoS contra la infraestructura de nube.

- **Puerto 27017 (MongoDB), puerto 1433 (MSSQL), puerto 3306 (MySQL), puerto 1521 (Oracle DB), y puerto 5432 (PostgreSQL)** para evitar la violación de datos accidental y el acceso no autorizado y la filtración de datos.

- **Protocolo de desktop remoto (RDP)** a través del **puerto 3389** para evitar el acceso no autorizado a los recursos y las violaciones de seguridad.

- **Llamada a procedimiento remoto (RPC)** a través del **puerto 135** y **SMTP a través del puerto 25** para evitar la filtración de datos.

- **Secure Shell (SSH)** a través del **puerto 22** y **Telnet** a través del **puerto 23** para evitar la filtración de datos.

Acerca de Log360

Actualmente es necesario contar con una solución que monitoree, audite y le ayude a gestionar su infraestructura en la nube de AWS. Presentamos Log360, una solución integral de gestión de eventos e información de seguridad (SIEM) que le proporciona:

- Una consola central que recopila, analiza y monitora los datos de log de CloudTrail y el bucket de S3 para ofrecer una visibilidad completa de las actividades que se realizan en su entorno de AWS.
- Información exhaustiva sobre las actividades de los usuarios en su AWS.
- Notificaciones en tiempo real e informes detallados sobre los cambios que se producen en los grupos de seguridad de la VPC, los cambios de subred, etc.
- Informes detallados sobre los cambios de configuración en recursos críticos como ELB, RDS, EC2, etc. para detectar cambios no autorizados al instante y detener la filtración de datos.
- Detalles sobre los cambios en los archivos almacenados en el bucket de S3 para garantizar la integridad de los archivos almacenados en estos recursos.
- Detalles exhaustivos sobre el tráfico de S3 y ELB para que pueda obtener visibilidad sobre quién accede a qué recursos en su entorno de AWS.

$ Cotización | Descargar | Programar una demo