ManageEngine
Log360 Cloud

Beneficios y arquitectura de Log360 Cloud

La importancia del almacenamiento seguro de logs

Los equipos de seguridad recurren a los logs cuando investigan incidentes y fallos de seguridad. A menudo, los atacantes intentan acceder a los registros de log, modificarlos o borrarlos para cubrir sus huellas. Es importante asegurarse de que los logs recopilados de la red se almacenan de forma segura y no han sido manipulados. Por eso, varias normativas de cumplimiento exigen que las organizaciones apliquen medidas para garantizar la integridad y fiabilidad de los archivos de log como parte de su proceso de gestión de logs. Sin embargo, la gestión de logs plantea retos a los equipos de seguridad, que se traducen en un almacenamiento inseguro, costos elevados e ineficacia. Estos retos pueden superarse almacenando los logs en una plataforma segura en la nube.

Beneficios del almacenamiento en la nube

Seguridad:

Aunque no hay garantía de la ciberseguridad, el almacenamiento de logs en la nube proporciona medidas de seguridad adicionales en comparación con el almacenamiento on-premises. Obtenga más información sobre las funciones de seguridad de la plataforma en la nube de Zoho Corporation aquí.

Optimización de costos y almacenamiento:

Almacenar logs en la nube suele ser bastante más económico, lo que ayuda a los equipos de TI a ahorrar costos de espacio en disco. Los equipos de seguridad solo tienen que pagar por el espacio de almacenamiento que necesitan en la nube.

Accesibilidad:

Los técnicos autorizados pueden acceder a los datos de log de forma fácil y segura desde cualquier lugar.

Escalabilidad:

A medida que las redes crecen, también lo hace el volumen de datos de log que se deben gestionar. Para los equipos de seguridad es mucho más sencillo escalar en la nube, sin preocuparse por la infraestructura.

ManageEngine
Log360 Cloud

ManageEngine Log360 Cloud es una solución basada en la nube que permite a las organizaciones gestionar y almacenar logs de forma segura. La solución utiliza un agente para subir logs a la nube.

- El motor de búsqueda integrado permite a los equipos de seguridad realizar consultas y recuperar la información que necesitan en un escenario determinado.
- Se pueden generar informes de auditoría para revisar los principales eventos de seguridad que se producen en la red.
- Las fuentes de log compatibles son equipos Windows/Linux, firewalls, entre otros

Arquitectura

Log360 Cloud utiliza el servicio Zoho Logs desarrollado por la empresa matriz, Zoho Corporation, para indexar los logs. Se utiliza un servidor UD (servidor de carga y descarga), que también es un servicio de Zoho, para garantizar que los datos del agente se carguen a Zoho Logs sin problema.

Enfoque con agente

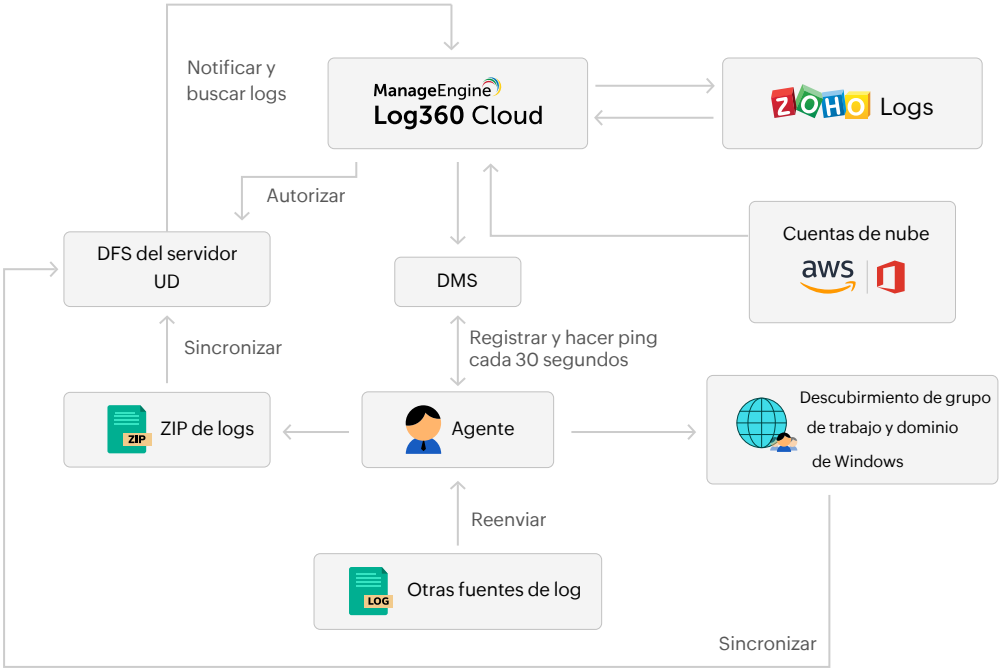
- Se debe instalar el agente de Log360 Cloud en cualquier equipo para poder comunicarse con Log360 Cloud. Al instalar el agente, se debe ingresar la clave de acceso obtenida al registrarse.
- El agente descubre automáticamente los grupos de trabajo y dispositivos de dominio de Windows. Otras fuentes de log pueden reenviar sus datos al equipo en el que está instalado el agente.
- Los detalles del host se envían al servidor UD, que tiene su propio DFS (sistema de archivos distribuido), y los detalles se actualizan en la base de datos de Log360 Cloud.
- Se utiliza un servicio de mensajería, denominado DMS, para comunicar al agente los cambios realizados en la GUI de Log360 Cloud. Cada agente debe registrarse en el DMS. Posteriormente, el agente hace un ping al DMS cada 30 segundos para comprobar si hay nuevas comunicaciones.
- Los datos de log recibidos de las fuentes de log se comprimen cada 5 minutos y se envían al servidor UD, que solicita autorización a Log360 Cloud.
- Una vez comprobada la licencia y el espacio de almacenamiento, se autoriza la solicitud y los datos se escriben en el DFS. Posteriormente se envía una notificación a Zoho Logs.
- A continuación, Zoho Logs obtiene los datos e indexa los logs para generar informes y realizar búsquedas.

Enfoque sin agente

- Integre varias cuentas en la nube (por ejemplo, AWS, M365) en Log360 Cloud.
- Configure fuentes de datos específicas (por ejemplo, Cloud Trail, S3, M365) para la recopilación de logs dentro de cada cuenta en la nube.
- Log360 Cloud recopila automáticamente logs de las fuentes de datos definidas a intervalos regulares de 10 minutos.

- Los logs recopilados se someten a comprobaciones de almacenamiento y licencia.

- Una vez validados, los logs se escriben en un sistema de archivos distribuido (DFS) y se envían a Zoho Logs para su posterior análisis y gestión.



Precio

El precio de la solución se basa en el espacio de almacenamiento que necesite la organización. El plan básico cuesta $300/año, para un máximo de 75 GB de almacenamiento y 90 días de retención.

Puede encontrar más información sobre los precios aquí.