ManageEngine
EventLog Analyzer

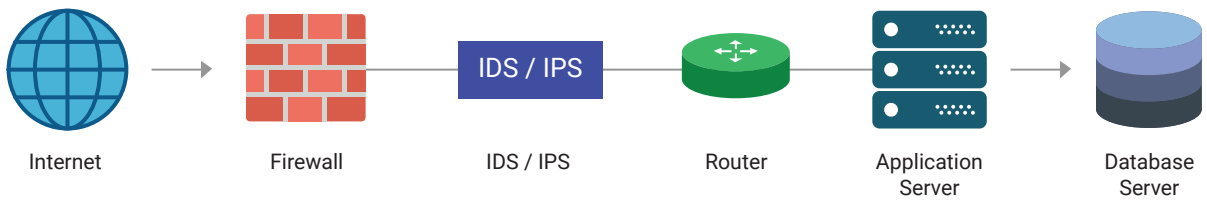
Auditoría de **SQL Server con** EventLog Analyzer

Auditoría de SQL Server con EventLog Analyzer

Las bases de datos forman la columna vertebral de la infraestructura de red de una organización. En la actualidad, las organizaciones recopilan, procesan y almacenan más datos que nunca. Por lo tanto, la seguridad de las bases de datos se vuelve extremadamente importante dado el crecimiento en el tamaño de la base de datos, la complejidad y los métodos de ataque cada vez más sofisticados.

Cómo ocurren los ataques a las bases de datos

Aquí hay una descripción general rápida de cómo ocurre una violación de datos:



Desde fuera de la organización, las bases de datos generalmente se acceden a través de una aplicación front-end, generalmente una aplicación web alojada en el servidor web de la compañía. Los usuarios malintencionados se disfrazan de tráfico de red válido para cruzar todos los dispositivos de seguridad perimetrales, tales como los firewalls y los sistemas de detección y prevención de intrusiones. A continuación, proceden a buscar y manipular una vulnerabilidad en la aplicación para obtener el control de la base de datos, un proceso conocido como inyección SQL (SQL injection). Los atacantes también pueden inundar la base de datos con solicitudes aparentemente válidas, haciendo que sus servicios no estén disponibles para otros usuarios. Este es otro tipo de ataque común conocido como denegación de servicio.

Desde el interior de la organización, los usuarios con los permisos adecuados pueden violar directamente la base de datos o incluso causar daños físicos a los servidores y otros medios de almacenamiento.

Los atacantes son expertos en encontrar puntos débiles en la política de seguridad de su base de datos. Cuando se deja sin controlar, la integridad de su base de datos podría verse seriamente comprometida debido a varios factores, que incluyen:

Cambios no autorizados:

Si no existe un proceso de gestión de cambios riguroso, pueden ocurrir una multitud de cambios no autorizados en su base de datos y pueden afectar la integridad de los datos.

Usuarios no autorizados:

Cuando los permisos no se asignan correctamente, los usuarios no autorizados pueden acceder a una base de datos.

Usuarios invitados:

Los usuarios invitados deben estar inhabilitados para usar bases de datos confidenciales a menos que se les conceda acceso explícitamente.

Política de contraseñas débil:

Las contraseñas de cuentas de usuario que son débiles o no se modifican a menudo son susceptibles de ataques.

Actualizaciones irregulares:

Si no se aplican las actualizaciones y parches liberados por el proveedor de su base de datos, su servidor puede ser susceptible a virus y otros ataques.

Backups irregulares:

Sin una buena política de backups en su lugar, puede perder una gran cantidad de datos si su servidor deja de funcionar por algún motivo.

Auditoría de bases de datos: la necesidad de una herramienta para la generación de informes de bases de datos

Emplear una buena política de seguridad es solo parte de un servidor de base de datos totalmente seguro. El monitoreo continuo de las transacciones de la base de datos, los accesos de los usuarios, los cambios en las cuentas, los cambios en el nivel del servidor, etc. al utilizar logs de la base de datos son aspectos necesarios a tener en cuenta para garantizar que todo funcione sin problemas. También es una medida de seguridad en sí misma, ya que capta todos los intentos de ataques o indicadores de compromiso en su base de datos, lo que le permite tomar medidas correctivas inmediatas y ajustar su política de seguridad si es necesario.

Sin embargo, debido al volumen de logs generados, es virtualmente imposible pasarlos manualmente. Los proveedores de bases de datos no suelen proporcionar mecanismos exhaustivos de notificaciones o alertas. El uso de una aplicación de terceros tales como EventLog Analyzer puede resolver este problema proporcionando el análisis de logs necesario para proteger sus bases de datos.

Audite Microsoft SQL Server con EventLog Analyzer

EventLog Analyzer es una herramienta de auditoría y conformidad de TI que puede importar y analizar logs de bases de datos SQL con facilidad. La herramienta proporciona exhaustivos informes y alertas para Microsoft SQL Server para mejorar su seguridad. Para monitorear los logs del servidor SQL con EventLog Analyzer, debe:

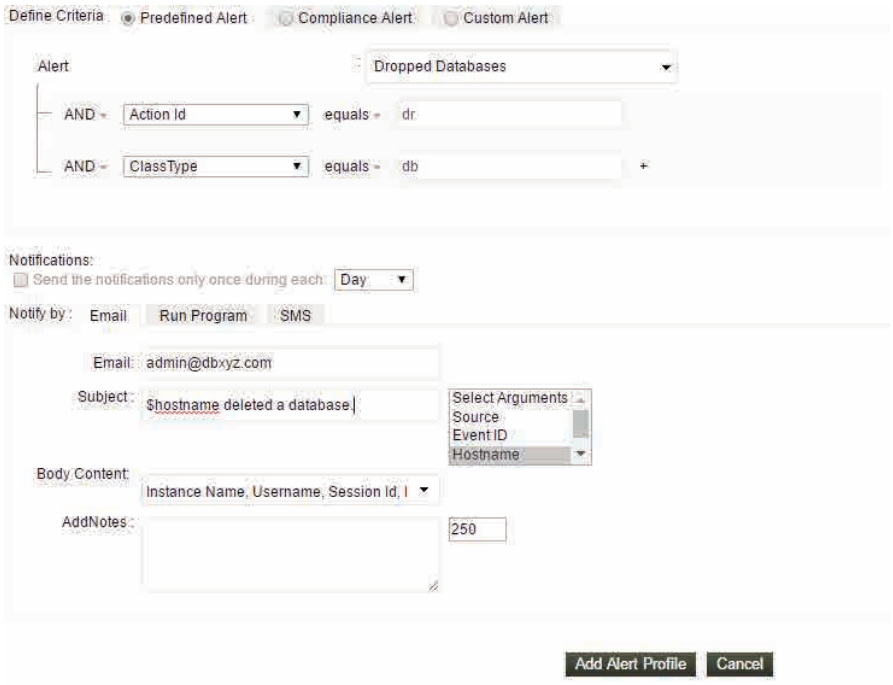
- Habilitar el inicio de sesión en su Microsoft SQL Server.
- Importar los logs al servidor de EventLog Analyzer.

A continuación, puede proceder a ver los informes generados al instante. También puede crear informes personalizados o configurar perfiles de alerta y recibir notificaciones por SMS o correo electrónico en tiempo real sobre eventos específicos de SQL Server. Los informes se proporcionan en un formato gráfico intuitivo, lo que facilita la comprensión de los eventos en su servidor de base de datos. Todos los informes se pueden personalizar, programar, distribuir vía correo electrónico o exportar a formatos PDF y CSV.

Los informes y alertas de SQL Server se clasifican en cinco grupos, lo que le permite analizar los eventos que desee con facilidad.

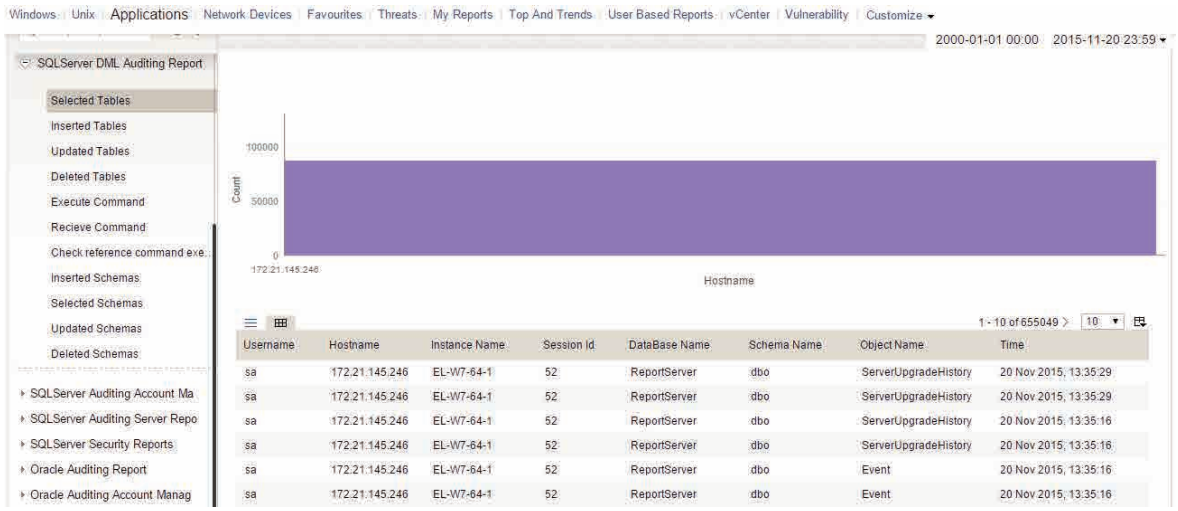
Auditoría DDL de SQL Server: monitoree y realice un seguimiento de los cambios que se producen en el nivel estructural de la base de datos, tales como cambios en las tablas, vistas, procedimientos, triggers, esquemas y más. Descubre fácilmente los detalles de quién hizo qué cambio, cuándo y desde dónde.

Escenario: con una alerta para las bases de datos caídas, el administrador recibe notificaciones instantáneas de una gran cantidad de datos que se eliminan. Si no se espera esto, pueden tomar medidas correctivas inmediatas para restaurar los datos e identificar al usuario responsable.



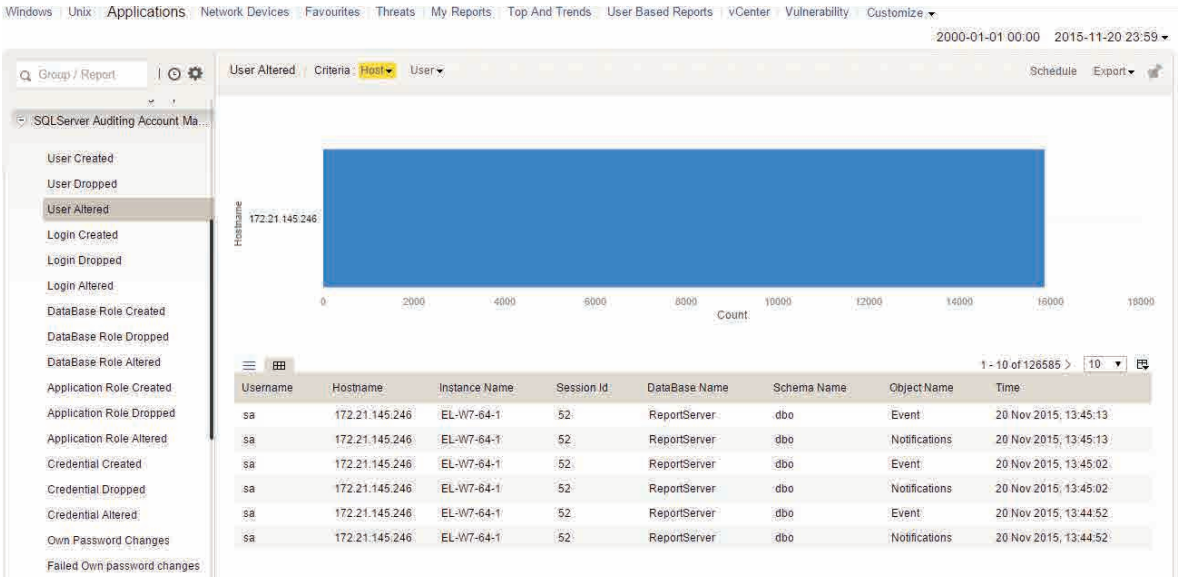
Auditoría DML de SQL Server: audite todas las actividades de nivel funcional que suceden en la base de datos. Averigüe cuándo se ejecutan las consultas funcionales, quién las ejecutó y desde dónde. Realice un seguimiento instantáneo de toda la actividad de cambio en datos confidenciales, tales como los datos que se visualizan, actualizan, eliminan o se realizan nuevas entradas.

Escenario: el informe de tablas seleccionadas ayuda a un administrador a comprender qué datos se están viendo en la base de datos.



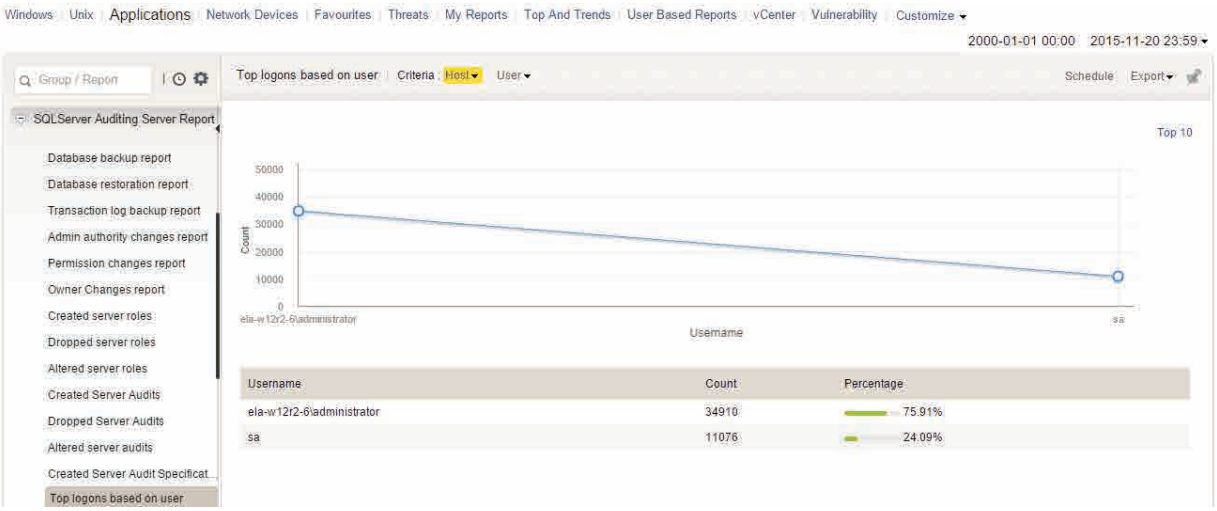
Administración de cuentas de SQL Server: la administración y monitoreo de cuentas de servidores de bases de datos es muy importante al momento de configurar autorizaciones para recursos tanto dentro como fuera de la base de datos. Haga un seguimiento de cada cambio realizado en cuentas como la creación de cuentas privilegiadas, inicios y cierres de sesión, contraseñas y más.

Escenario: el informe modificado por el usuario ayuda al administrador a realizar un seguimiento de los permisos del usuario. Si un usuario obtiene acceso a una base de datos confidencial, el administrador puede tomar medidas correctivas inmediatas.



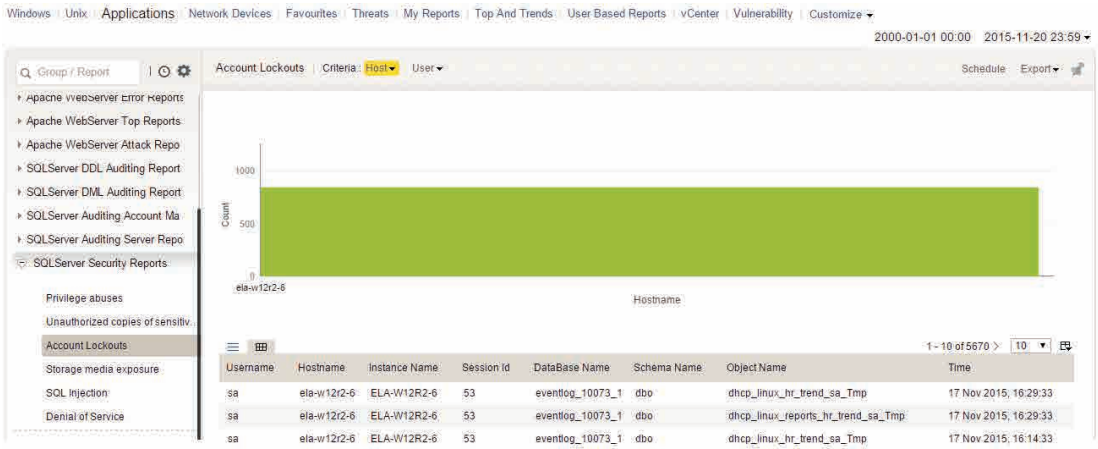
Auditoría de SQL Server: audite actividades de SQL Server tales como inicios, cierres, inicios de sesión y fallas de inicio de sesión. Además, obtenga informes detallados sobre la copia de seguridad de la base de datos, restauración, auditoría, especificaciones de auditoría, autoridades administrativas y más. Conozca las principales actividades de inicio de sesión en la base de datos y visualice los patrones de tendencia de cualquier error de inicio de sesión.

Escenario: los principales inicios de sesión basados en el usuario es un informe de tendencias que ayuda al administrador a comprender quién está más activo en la base de datos. Un valor superior al esperado para cualquier usuario también podría indicar que una cuenta está en peligro.



Seguridad de SQL Server: EventLog Analyzer ayuda a mitigar las violaciones de seguridad internas y externas al proporcionar informes detallados sobre varios ataques de seguridad que pueden ocurrir en una base de datos tales como inyección SQL (SQL injection) y ataques de denegación de servicio. Estos ayudan al administrador a realizar un análisis forense detallado sobre cómo sucedió el ataque. También se pueden rastrear los bloqueos de cuenta, abusos de privilegios, copia no autorizada de datos confidenciales y más, ayudándolos a reaccionar de forma instantánea a las violaciones de seguridad.

Escenario: varios bloqueos de cuenta en un corto período de tiempo, identificados por el informe de bloqueos de cuenta, podrían ser indicativos de piratas informáticos que intentan obtener acceso a la base de datos.



Con sus amplias capacidades de auditoría y alerta, EventLog Analyzer es la herramienta perfecta para monitorear la actividad, obtener información, descubrir y evitar intentos de violación en su SQL Server.

Acerca de EventLog Analyzer

EventLog Analyzer es un software integral para la administración de logs y conformidad de TI para SIEM. Proporciona información detallada sobre los logs de sus equipos en forma de informes para ayudar a mitigar las amenazas y ayudarlo a lograr una seguridad de red completa.

https://blogs.manageengine.com/eventloganalyzer

Acerca de ManageEngine

ManageEngine ofrece las herramientas de administración de TI en tiempo real que permiten a un equipo de TI satisfacer las necesidades de soporte y servicios en tiempo real de una organización. En todo el mundo, más de 60.000 empresas establecidas y emergentes -incluido más del 60 por ciento de Fortune 500- confían en los productos ManageEngine para garantizar el rendimiento óptimo de su infraestructura de TI crítica, que incluye redes, servidores, aplicaciones, desktops y más. ManageEngine es una división de Zoho Corp. con oficinas en todo el mundo, incluidos los Estados Unidos, el Reino Unido, la India, Japón y China.