ManageEngine
EventLog Analyzer

Auditoria do SQL Server com o EventLog Analyzer

www.manageengine.com/br/eventlog/

Introdução

Os bancos de dados são o elemento mais essencial da rede de uma organização, pois armazenam e processam os dados comerciais críticos da empresa. Esses dados são de alto valor para os criminosos virtuais, que estão produzindo novos métodos para atacá-los todos os dias. Além disso, o volume médio de dados processados pelas organizações está crescendo.

Gerenciar grandes quantidades de dados e protegê-los contra ataques é uma tarefa assustadora que pode revelar práticas de segurança ruins. É por isso que a integridade, a auditoria e a segurança do banco de dados são os principais tópicos de preocupação em muitas organizações.

A importância da auditoria do banco de dados

Seus bancos de dados são suscetíveis a ataques externos e internos. Os invasores estão aptos a encontrar pontos fracos que permitem que eles encontrem o caminho para sua rede e seus bancos de dados. As atividades de auditoria que ocorrem em seu banco de dados podem ajudá-lo a garantir que tudo esteja funcionando sem problemas em seus servidores e a detectar ameaças que poderiam levar à perda de dados. A auditoria ajuda perceber eventos como:

- **Mudanças incorretas:** se não houver um processo rigoroso de gerenciamento de mudança, uma grande quantidade incorreta poderá ocorrer em seu banco de dados e interromper a integridade dos dados. Por exemplo, se vários usuários tiverem acesso de gravação a um banco de dados, os que são mportantes poderão ser sobrescritos com os valores errados. Quando essas mudanças inválidas são feitas em uma coluna crítica, como números de contas bancárias, isso pode ter efeitos desastrosos.

- **Atividade não autorizada:** quando as permissões e contas de usuário não são gerenciadas com eficácia, eles podem obter direitos elevados e acesso não autorizado a dados confidenciais que conseguirão modificar. Além disso, invasores externos podem tentar os acessar com credenciais roubadas. As contas de usuário que eles usam podem não ter privilégios suficientes para acessar os dados, resultando em tentativas de acesso não autorizado. Você precisa monitorar todos esses eventos para bloquear ataques no primeiro estágio.

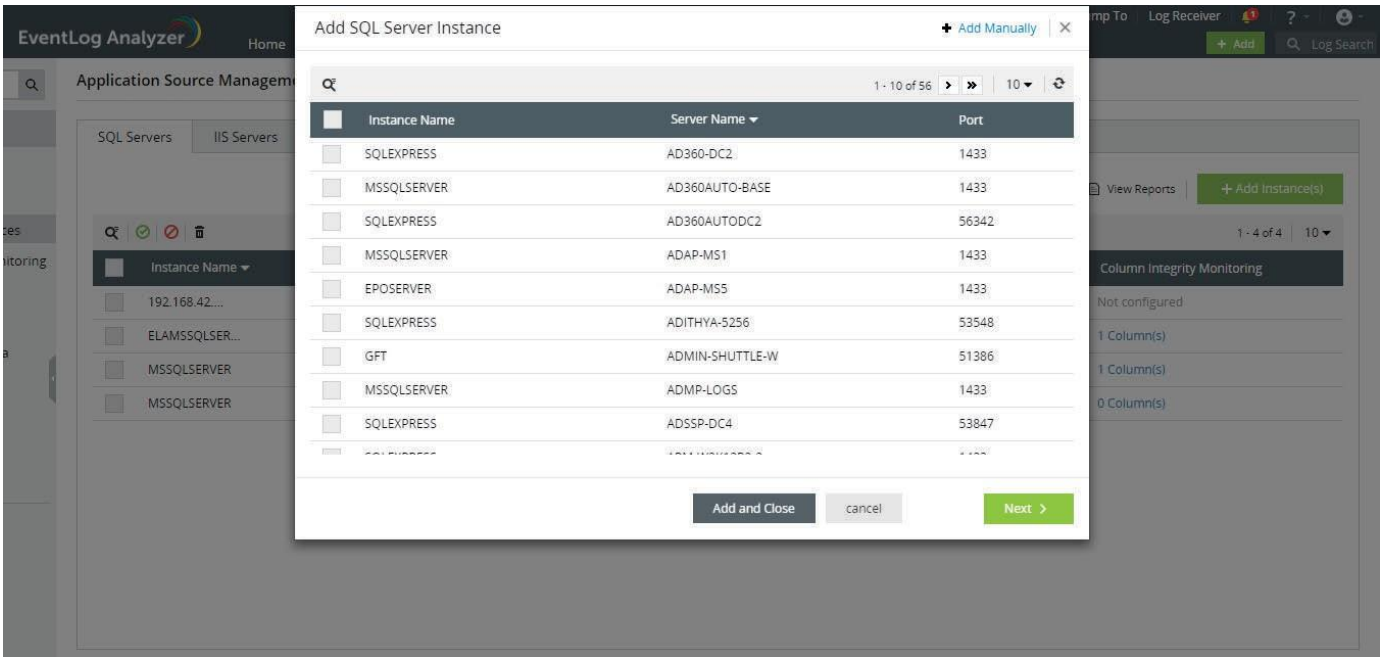
- **Atividade suspeita de login:** contas de usuário com senhas fracas podem ser facilmente comprometidas. Os invasores podem obter o controle dessas contas com facilidade, hackeando usando força bruta ou outros métodos de quebra de senha. Se essas contas forem privilegiadas e tiverem acesso elevado, os hackers terão acesso livre a dados altamente confidenciais.

- **Atualizações inconsistentes:** A não aplicação de atualizações e patches lançados pelo fornecedor do banco de dados pode tornar o servidor vulnerável a vírus e outros ataques.

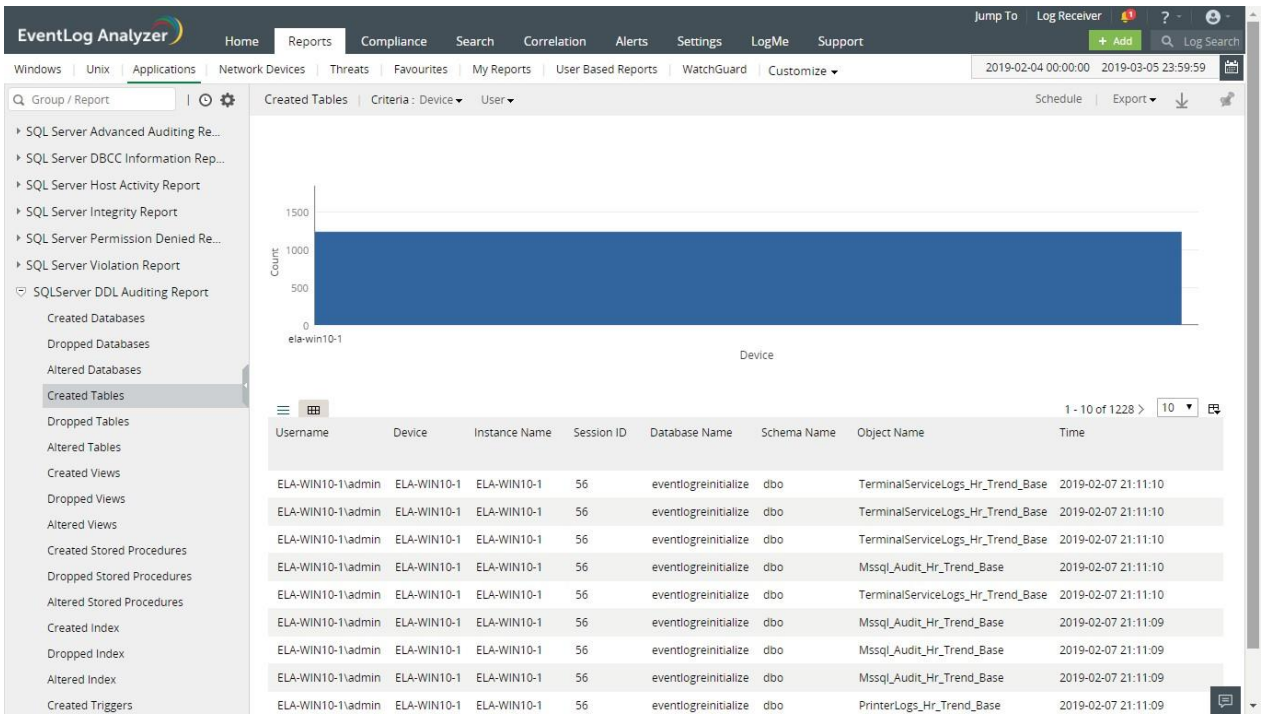
- **Backups inconsistentes:** Sem uma boa política de backup, você pode perder muitos dados se o servidor ficar inativo por qualquer motivo.

Destaques da auditoria do SQL Server com o EventLog Analyzer

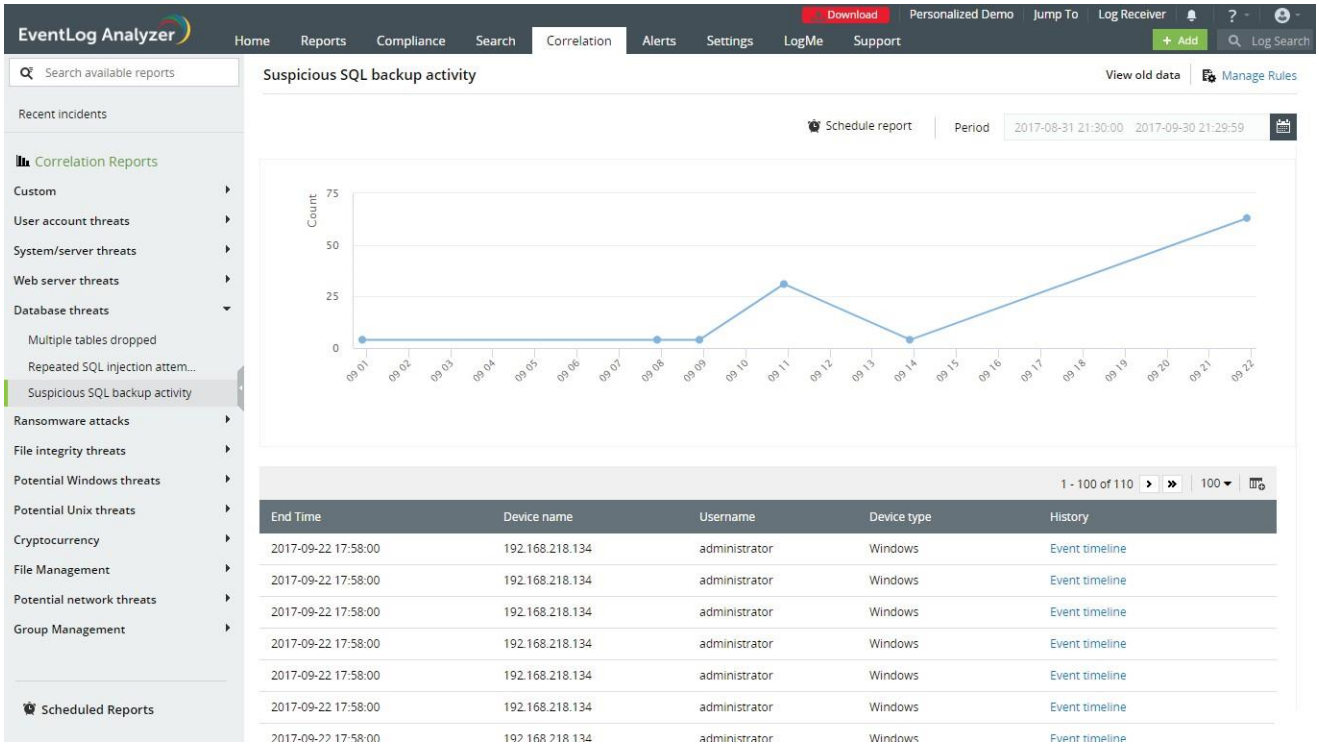
O EventLog Analyzer é uma solução de gerenciamento de logs, auditoria e conformidade de TI que analisa logs de bancos de dados com facilidade. Essa ferramenta fornece relatórios e alertas abrangentes para o Microsoft SQL Server que ajudam a melhorar sua postura de segurança. Ele oferece vários recursos, incluindo:



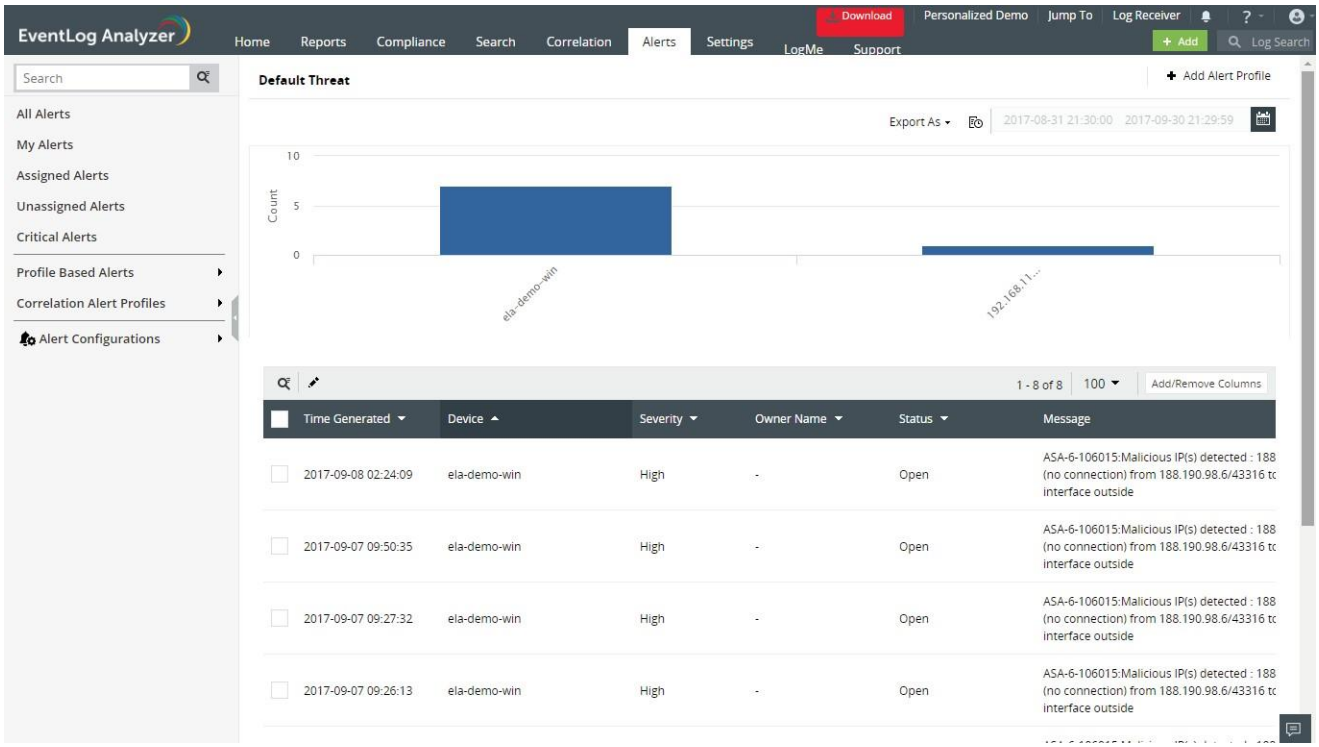
- **Descoberta automática de instâncias do SQL Server:** detecta automaticamente todas as instâncias do SQL Server em sua rede para que você possa começar a auditá-las imediatamente.



- **Relatórios e alertas de auditoria em profundidade:** obtenha informações detalhadas sobre:
  - **Atividade de DDL e DML:** entenda como seus bancos de dados e tabelas estão sendo usados e modificados.
  - **Atividade do SQL Server:** acompanhe as inicializações e desligamentos do SQL Server e as mudanças feitas em contas de usuário e objetos no nível do servidor, como auditoria e objetos de especificação de auditoria.
  - **Atividade de banco de dados de baixo nível:** aprofunde-se na atividade do banco de dados com relatórios de auditoria avançada sobre processos de banco de dados, mudanças de segurança, aplicações conectadas e muito mais.
  - **Integridade da coluna:** proteja colunas críticas em seus bancos de dados contra adulteração ou modificação incorreta. O controle de mudanças é feito em valores de dados e mantém a sua integridade geral.



- **Correlação de eventos:** obtenha mais contexto sobre eventos em SQL Servers com correlação de eventos. Esse recurso correlaciona eventos que ocorrem no SQL Server e em outras aplicações e dispositivos para descobrir padrões suspeitos de atividade. Por exemplo, a regra predefinida de Backup do SQL Server suspeito identifica possíveis hacks de força bruta de suas máquinas Windows seguidas por um evento de backup SQL.



Inteligência contra ameaças: receba notificações com base nos feeds de ameaças mais recentes e identifique os agentes mal-intencionados conhecidos que tentam interagir com seu banco de dados.

Cenários de auditoria do banco de dados

O EventLog Analyzer fornece mais de 120 relatórios e alertas predefinidos para o Microsoft SQL Server. Alguns dos relatórios mais usados e o que eles podem fazer estão listados abaixo:

Nome do relatório/alerta	Categoria	Caso de uso
Bancos de dados ignorados	Auditoria do DDL	**Detecte anomalias ou remoção em massa de dados:** certifique-se de que os dados críticos não sejam perdidos para sempre, lançando esforços imediatos de recuperação.
Tabelas selecionadas	Auditoria do DML	**Rastreie os acessos ao banco de dados:** entenda quais dados estão sendo acessados e por quem.
Conta de usuário alterada	Gerenciamento de contas	**Gerencie os usuários do banco de dados:** impeça que contas não autorizadas obtenham acesso a dados confidenciais.
Principais logons com base no usuário	Auditoria do servidor	**Descubra tendências de logon no servidor:** identifique os usuários mais ativos e detecte contas potencialmente comprometidas em casos de atividade anormalmente alta.

Backup suspeito do SQL Server	Segurança	**Detecte atividade de backup suspeita:** receba notificação sobre backups de bancos de dados não autorizados.
Coluna modificada	Monitoramento da integridade da coluna	**Mantenha a integridade dos dados:** controle as mudança feitas nos valores das colunas confidenciais do banco de dados.
Aplicações conectadas	Auditoria avançada	**Controle aplicações dependentes:** Faça a auditoria de todas as aplicações que fazem interface com seu banco de dados e garanta que as não autorizadas não sejam utilizadas

Com suas capacidades de auditoria abrangentes e alertas, o EventLog Analyzer é a ferramenta perfeita para monitorar atividades, obter insights e descobrir e evitar tentativas de violação em seu SQL Server.