ManageEngine
EventLog Analyzer

Um guia para configurar agentes para coleta de logs no EventLog Analyzer

www.manageengine.com/br/eventlog/

Introdução

O EventLog Analyzer, uma solução abrangente de SIEM, pode coletar logs de eventos do Windows usando

- Método de coleta de log sem agente e
- método de coleta de log baseado em agente

Não existe a "melhor opção" definida para a coleta de logs. Em vez disso, seu tipo é determinado pelas necessidades da organização. Este guia explica a arquitetura e a configuração dos seus agentes de coleta.

Recomendamos que você escolha o modo de coleta de log baseado em sua infraestrutura, políticas e requisitos de TI. Entre em contato com nossa equipe de suporte em eventlog-support@manageengine.com para obter melhores orientações sobre como selecionar o modo de coleta.

Coleta de logs baseada em agente

A coleta de log baseada em agente é particularmente útil para coletar logs facilmente na WAN e por meio de firewalls. Um fator que força a implantação de agentes de coleta de log é a indisponibilidade de uma conexão de rede existente. Eles também são úteis na coleta de logs de dispositivos localizados nas zonas restritas de sua rede, como DMZs. Além disso, a reduz o uso da CPU do servidor, proporcionando melhor controle sobre a taxa de EPS (eventos por segundo).

Quando você pode escolher a coleta de log baseada em agente?

Com o EventLog Analyzer, você pode escolher o método de coleta de log baseado em agente nas seguintes circunstâncias:

1. Quando a política de segurança de TI da sua organização não permitir acesso às portas de comunicação WMI/DCOM em dispositivos Windows (pode ser um servidor, uma estação de trabalho ou um controlador de domínio).

2. Quando não há conexão de rede entre o servidor onde o EventLog Analyzer está instalado e o dispositivo do qual os dados de log serão coletados.

3. Quando você deseja equilibrar a sobrecarga em sua rede.

4. Para facilitar a coleta de logs em WANs e firewalls.

5. Para monitorar alterações críticas em arquivos e pastas usando o recurso de monitoramento de integridade de arquivo.

Arquitetura

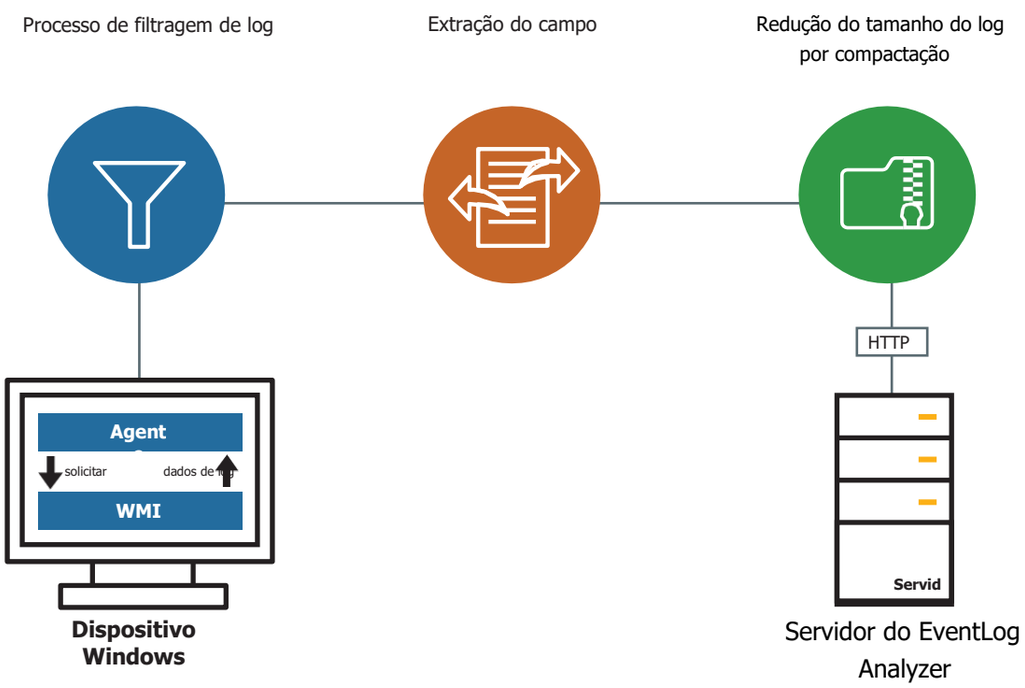
Esta seção ilustra a arquitetura da implantação de coleta de log baseada em agente.

O agente deve ser instalado no dispositivo Windows desejado para coletar dados de log deste remotamente e, em seguida, enviar os que foram coletados para o servidor EventLog Analyzer. Em contrapartida, na coleta de log sem agente, o agente reside no próprio servidor EventLog Analyzer e não no dispositivo Windows.

Para implantar o agente em um dispositivo específico, execute o arquivo **EventLogAgent.msi** localizado no diretório **lib\native** na pasta de instalação

Como funciona o agente?

- O agente acessa a infraestrutura WMI do dispositivo internamente e obtém os dados de log diretamente por meio de consultas WMI.
- Assim que os dados de log são coletados, o agente executa o pré-processamento, que inclui filtragem de log e extração de campo na fonte, antes de compactar o arquivo e enviar os dados com segurança para o servidor EventLog Analyzer pelo protocolo HTTP.
- Como os dados do log já foram processados até esse ponto, o servidor precisa apenas os indexar para gerar os relatórios e alertas em tempo real.



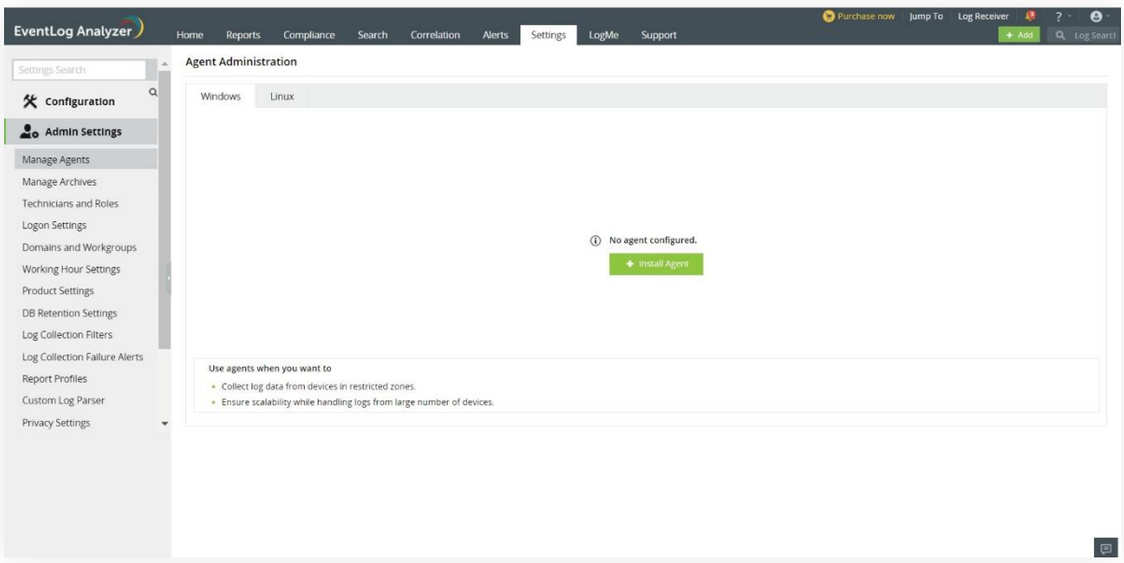
Etapas para configurar a coleta de log baseada em agente

Com o EventLog Analyzer, configurar e gerenciar agentes de coleta de logs é incrivelmente fácil. A ferramenta coleta os dados de log no modo sem agente por padrão. Mesmo no modo de coleta de log baseado em agente, ele alterna automaticamente para o modo sem agente sempre que é desinstalado, garantindo a coleta e o processamento contínuos de log.

Etapas de instalação

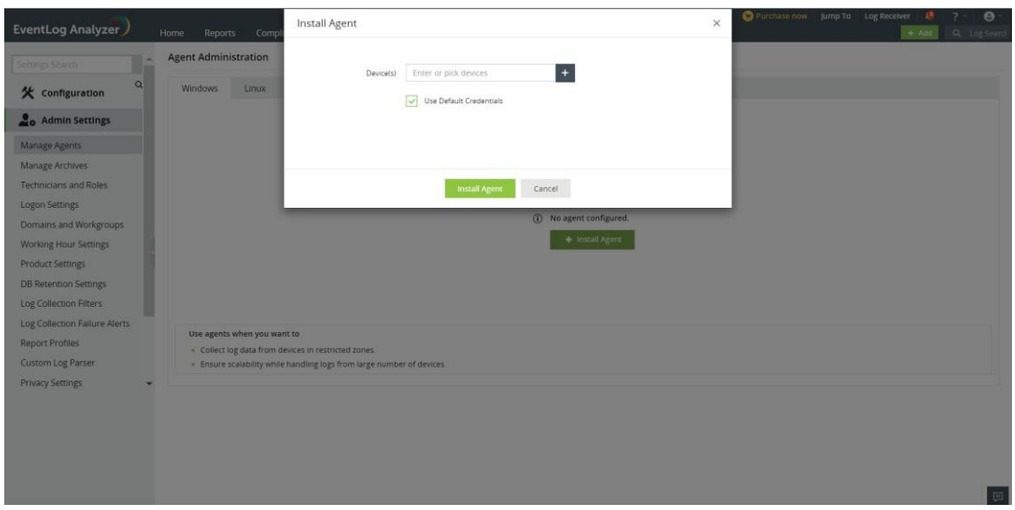
Siga as etapas abaixo para instalar o agente EventLog Analyzer.

- Na guia **Configurações**, navegue até **Configurações de administrador --> Gerenciar agentes.**
- Clique em **+ Instalar agente** e, em seguida, clique no ícone **+** correspondente aos dispositivos.

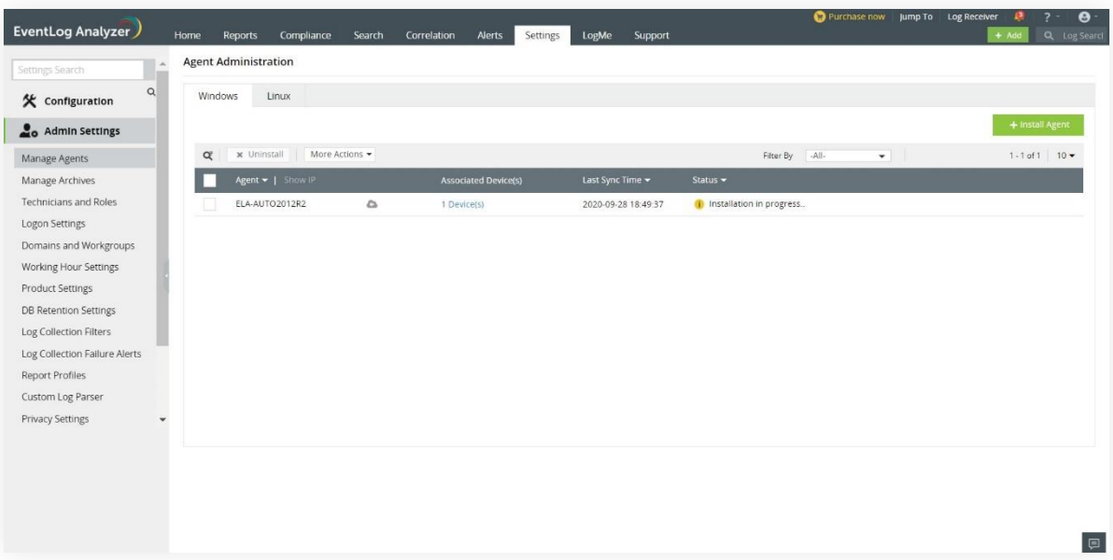


- Selecione os dispositivos nos quais deseja instalar o agente.
- Insira o nome de login e a senha para acessar os dispositivos. Esta conta deve ter privilégios de administrador para que o agente seja instalado com sucesso. Como alternativa, você também pode selecionar a opção **Usar credenciais padrão**.

Nota: Se vários dispositivos forem selecionados, verifique se as credenciais são válidas para todos eles.

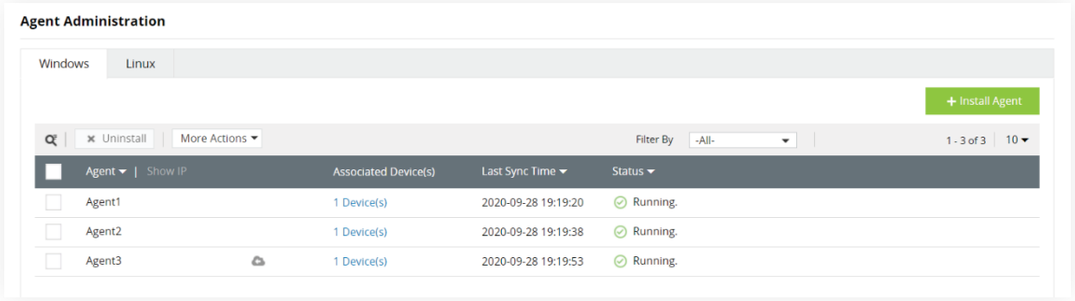


- Use o link **Verificar credencial** para validar as credenciais inseridas.
- Por fim, clique em **Instalar agente** para iniciar a instalação.



Administração do agente

Os agentes instalados podem ser facilmente gerenciados a partir do link **Gerenciamento de Agentes** na seção **Configurações de Administrador**.



Esta página permite visualizar os dispositivos adicionados a um agente e o seu status do serviço com a opção de Iniciar, Parar e Reiniciar.

Você também pode editar ou excluir o agente e adicionar/remover dispositivos a serem monitorados pelo ele.

Nota: A administração do agente pode ser executada remotamente somente se houver uma conectividade de rede entre o agente e o servidor do EventLog Analyzer.

Coleta segura de logs

O EventLog Analyzer garante que a coleta de logs de suas fontes por meio dos agentes seja segura.

Os padrões de criptografia abaixo são seguidos pelos agentes do EventLog Analyzer versão 4.1 e superiores que são agrupados com os servidores do EventLog Analyzer versão 12120 e superiores.

- Dados confidenciais, como IDs exclusivos e chaves que são transferidos entre agentes e servidores durante o processo inicial de registro do agente são criptografados usando o algoritmo AES no modo ECB junto com a soma de verificação de integridade SHA256. As chaves são adicionalmente protegidas com o algoritmo RSA.
- Todas as outras comunicações entre o agente e o servidor são criptografadas usando o algoritmo AES no modo ECB [SHA256 Digest] juntamente com as chaves de sessão.
- Os arquivos zip são protegidos por senha, com uma senha diferente para cada agente e uma soma de verificação de integridade SHA 256.

Nos agentes EventLog Analyzer 4.0 e anteriores, toda a comunicação entre agentes e servidores é criptografada usando o algoritmo DES.

O Transport Layer Security versão 1.2 é compatível com todas as versões do EventLog Analyzer.

Sobre o EventLog Analyzer

O EventLog Analyzer é uma ferramenta abrangente de gerenciamento de logs e conformidade de TI para SIEM. A solução fornece informações detalhadas sobre seus dados de log com relatórios de auditoria e perfis de alerta para mitigar ameaças e proteger sua rede.

https://blogs.manageengine.com/eventloganalyzer

Sobre a ManageEngine

A ManageEngine fornece as ferramentas de gerenciamento de TI em tempo real que capacitam a equipe a atender às necessidades da organização relacionadas a serviços e suporte em tempo real. Em todo o mundo, mais de 60.000 empresas estabelecidas e emergentes – incluindo mais de 60 por cento das empresas da Fortune 500 – confiam nos produtos da ManageEngine para garantir o desempenho ideal de sua infraestrutura de TI crítica, incluindo redes, servidores, aplicações, desktops e mais. A ManageEngine é uma divisão da Zoho Corp., com pontos em países do mundo inteiro, entre eles Estados Unidos, Reino Unido, Índia, Japão e China.