ManageEngine

EventLog Analyzer

Guia de Início Rápido

Guia de início rápido do EventLog Analyzer da ManageEngine

Conteúdo

Instale e inicie o EventLog Analyzer

Faça o download do arquivo EXE na página de download.

Antes de iniciar a instalação, verifique os requisitos do sistema.

Para instalar o EventLog Analyzer em um **Sistema Operacional Windows**, execute:

- **ManageEngine_EventLogAnalyzer.exe** para a versão de 32 bits
- **ManageEngine_EventLogAnalyzer_64bit.exe** para a versão de 64 bits

Para instalar o EventLog Analyzer em um **Sistema operacional Linux**, execute:

- **ManageEngine_EventLogAnalyzer.bin** para a versão de 32 bits
- **ManageEngine_EventLogAnalyzer_64bit.bin** para a versão de 64 bits

Nota:

Antes de instalar o EventLog Analyzer em um sistema operacional Linux,

- execute os seguintes comandos no Unix Terminal ou Shell: **chmod +x ManageEngine_EventLogAnalyzer.bin**
- Em seguida, execute ManageEngine_EventLogAnalyzer.bin clicando duas vezes, ou executando ./ManageEngine_EventLogAnalyzer.bin no Terminal ou Shell.

Quando a instalação começar, você será guiado pelas seguintes etapas:

- Selecione **Aceitar os termos e condições do contrato de licença** depois de lê-los com atenção.
- **Selecione a pasta** na qual deseja instalar o produto.
  O local padrão de instalação é *C:\ManageEngine\EventLog Analyzer*. A localização pode ser alterada usando a opção **Explorar**.
- Insira a **porta do servidor da web**. O número de porta padrão é 8400.
  Verifique se a porta padrão ou a selecionada não está em uso.

- Selecione a opção **Instalar o EventLog Analyzer como serviço** para instalar o produto como um serviço Windows ou Linux. Por padrão, esta opção vem selecionada. Desmarque esta opção para instalar como uma aplicação. Alternativamente, você pode instalá-lo como este modo e, em seguida, convertê-lo em um serviço. Recomendamos a instalação neste modo.
- Insira o nome da pasta onde deseja que o produto seja mostrado. O nome padrão é **ManageEngine EventLog Analyzer**.
- Insira suas informações para obter assistência técnica.

Após a conclusão da instalação, o assistente exibe o arquivo ReadMe e inicia o servidor do EventLog Analyzer.

Antes de executar o produto, verifique se os pré-requisitos foram atendidos.

Conectando-se ao servidor do EventLog Analyzer

Depois que o servidor foi iniciado com êxito, siga as etapas abaixo para acessar o EventLog Analyzer.

- Abra um navegador da web compatível. Digite a URL como ***http://<device name>:8400*** (onde *<devicename>* é o nome da máquina que executa o EventLog Analyzer e *8400* é a porta do servidor web padrão)
- Faça login no EventLog Analyzer usando a combinação de nome de usuário/senha padrão **admin/admin** e selecione uma das três opções em **Fazer login em** (**Autenticação local**, **Autenticação do Radius** ou **Nome de domínio**).
- Clique no botão **Login**.

Adicione dispositivos para monitoramento

Adicione dispositivos Windows

Em todos os dispositivos Windows, certifique-se de que o WMI e o DCOM estejam habilitados e que o log esteja habilitado para os respectivos módulos/objetos. Para encaminhar os logs de eventos do Windows no formato syslog, use um utilitário de terceiros, como o SNARE.

(a) Adicione dispositivos Windows a partir de um domínio

1. Selecione o **domínio** no menu suspenso na guia Configurações. Os dispositivos Windows no domínio selecionado são detectados e listados automaticamente.
2. Selecione os **dispositivos** necessários clicando nas caixas de seleção apropriadas. Você pode encontrar qualquer dispositivo usando a opção de pesquisa integrada ou o filtro UO.
3. Clique no botão **Adicionar**.

(b) Adicione dispositivos Windows a partir de um grupo de trabalho

Você pode adicionar um dispositivo de um grupo de trabalho clicando no link **Adicionar dispositivo de grupo de trabalho**. Isso listará os dispositivos em seus grupos.

1. Selecione o grupo de trabalho no menu suspenso Selecionar **grupo de trabalho** na guia Configurações.
2. Selecione os **dispositivos** desejados clicando nas caixas de seleção apropriadas.
3. Clique no botão **Adicionar**.

Nota: Você pode **atualizar**, **recarregar** e **excluir** um grupo de trabalho, clicando nos ícones apropriados ao lado do menu suspenso **Selecionar domínio**.

(c) Adicione dispositivos Windows manualmente

Você também tem a opção de adicionar o dispositivo manualmente, conforme mostrado abaixo, clicando no link **Configurar manualmente**.

1. Insira o **nome do dispositivo** ou o **endereço IP**.
2. Insira o **Nome de usuário** e a **senha** com credenciais de administrador e clique no link **Verificar login**.
3. Clique no botão **Adicionar**.

Nota: Se o EventLog Analyzer estiver instalado em um computador com UNIX, ele não poderá coletar logs de eventos de dispositivos Windows. Porém, aplicações de terceiros podem ser usadas para converter logs de eventos do Windows em syslogs e enviá-los para o EventLog Analyzer.

Adicione dispositivos Syslog

Na página **Gerenciamento do dispositivo**, navegue até a guia **Dispositivos Syslog** e clique no botão **+Adicionar dispositivos**. Insira o **nome do dispositivo** ou o **endereço IP** no campo Dispositivos e clique no botão **Adicionar**.

Siga as etapas abaixo para descobrir e adicionar automaticamente os dispositivos Syslog à sua rede:

1. Clique no link **Descobrir e Incluir** na janela **Incluir Dispositivos Syslog**. Você pode descobrir os dispositivos Syslog em sua rede por **Intervalo de IP (IP inicial até IP final) ou CIDR**.
2. Insira o **IP inicial** e o **IP final** ou o **intervalo CIDR** para descobrir os dispositivos Syslog.

3. Escolha as **credenciais SNMP** para descobrir automaticamente os dispositivos Syslog em sua rede. Por padrão, as credenciais SNMP públicas podem ser usadas para verificar os dispositivos Syslog em sua rede.
Como alternativa, você pode adicionar credenciais SNMP clicando em **+Adicionar Botão de Credencial.** Depois de selecionar as credenciais SNMP, clique no botão **Verificar** para descobrir automaticamente os dispositivos Syslog no intervalo IP ou CIDR especificado.
4. Selecione os **dispositivos**, clicando nas caixas de seleção apropriadas.
Você pode pesquisar facilmente um dispositivo usando o campo de pesquisa ou filtrar por tipo de dispositivo e fabricante.
5. Clique no botão **Adicionar dispositivos** para adicionar os dispositivos a serem monitorados.

Para adicionar mais dispositivos, como servidores de impressão, servidores de terminal, dispositivos Oracle, dispositivos VMware e muito mais, consulte a página Adicionar dispositivos .

Importe logs

Com o EventLog Analyzer você tem a opção de importar qualquer arquivo de log simples e de gerar relatórios predefinidos para Windows (formato EVTX), dispositivos Syslog, aplicações e dados arquivados. Para obter informações sobre como importar logs, consulte a seção Importar arquivo de log.

Use relatórios predefinidos

O EventLog Analyzer fornece relatórios pré-configurados que ajudam a analisar a segurança da rede e a monitorar as atividades internas do usuário. Os relatórios incluem informações sobre aproximadamente 750 fontes de log, incluindo:

- Dispositivos de rede como firewalls, roteadores, switches, IDS/IPS

- Aplicações que incluem bancos de dados Oracle e Microsoft SQL Server
- Servidores da web
- Máquinas Windows e Linux/Unix
- Sistemas IBM AS400

Os grupos de relatórios são Windows, Aplicações, Dispositivos de rede, Vulnerabilidade, vCenter, Meus relatórios, Favoritos e Relatórios personalizados.

Crie relatórios personalizados

Os seus relatórios personalizados criados são listados na seção Meus relatórios. Novos relatórios podem ser adicionados, relatórios existentes podem ser agendados, editados ou excluídos.
Consulte a seção Criar relatórios personalizados para saber como criar um relatório personalizado.

Pesquise por logs

A função de pesquisa de log do EventLog Analyzer é extremamente simples e permite pesquisar qualquer informação. Por padrão, o termo de pesquisa inserido é pesquisado na mensagem de log. Os resultados da pesquisa podem ser salvos nos formatos PDF e CSV.

Para obter mais informações sobre o recurso de pesquisa, consulte a seção Como pesquisar, que explica como realizar uma pesquisa, e a seção Como extrair campos adicionais, que explica como extrair campos de logs brutos.

Crie perfis de alerta

O EventLog Analyzer pode ser configurado para gerar um alerta quando ocorrer um evento de segurança específico. É possível:

- Escolher entre mais de 500 critérios de alarme predefinidos ou definir alertas personalizados.
- Receber notificações em tempo real via e-mail ou SMS quando ocorrer um evento preocupante.
- Atribuir um programa para ser executado quando o alerta for gerado.
- Configurar quais dispositivos ou grupos de dispositivos devem ser monitorados para os eventos.
- Especificar com que frequência e em quantos minutos um evento deve ocorrer para que o alerta seja acionado.
- Ser alertado sobre todos os eventos específicos da política de conformidade.
- Receber alertas sobre correlações, como a ocorrência de dois ou mais chamadas de eventos que requerem uma investigação mais aprofundada.

Consulte a seção Criar perfis de alerta para saber como configurar um alerta.

Configure alertas de e-mail e SMS

O EventLog Analyzer pode notificá-lo imediatamente quando um incidente crítico de segurança ocorre em sua rede.

- Para receber alertas por e-mail e relatórios agendados, você deve configurar o servidor de e-mail no EventLog Analyzer.
- Para receber alertas no seu celular, você precisa definir as configurações de SMS.

Consulte o Documento de ajuda para ver as etapas de configuração.

Configurações avançadas

- **Migração de banco de dados**: além do banco de dados PostgreSQL, o EventLog Analyzer é compatível com o Microsoft SQL Server como um banco de dados back-end. Se você já o tem em sua empresa, poderá utilizá-lo. Para saber mais, consulte a seção Migrando dados do PostgreSQL para o banco de dados do Microsoft SQL no documento de ajuda.
- **Configurações do arquivo**: o EventLog Analyzer grava arquivos de log periodicamente. O intervalo de arquivamento e o período de retenção podem ser configurados. Os dados de log arquivados também são criptografados e carimbados com data/hora.