ManageEngine
EventLog Analyzer

EventLog Analyzer:

GUIA DAS MELHORES PRÁTICAS

www.eventloganalyzer.com

Índice

Este guia descreve as melhores práticas que, se seguidas, garantem um funcionamento suave e desempenho ideal do EventLog Analyzer.

Requisitos do sistema

Requisitos de hardware

As soluções de gerenciamento de logs exigem muitos recursos, e a seleção do hardware correto desempenha um papel fundamental para garantir o desempenho ideal.

A tabela a seguir indica os requisitos de hardware sugeridos com base no tipo de fluxo.

	Baixo fluxo	Fluxo normal	Alto fluxo
Núcleos do processador	6	12	24
RAM	16 GB	32 GB	64 GB
IOPS	150	750	1.500 *
Espaço em disco	1.2 TB	3 TB *	4 TB *
Capacidade da placa de rede	1 GB/s	1 GB/s	10 GB/s
Arquitetura da CPU	64 bits	64 bits	64 bits

Nota:

- Os **valores mencionados acima são aproximados**. Recomenda-se executar um ambiente de teste semelhante ao de produção com os detalhes de configuração mencionados na tabela acima. Com base no fluxo exato e no tamanho dos dados, os requisitos do sistema podem ser ajustados.
- Para IOPS mais altas, podemos usar RAID ou SSD.

Use a tabela a seguir para determinar o tipo de fluxo para sua instância.

Tipo de log	Tamanho (em bytes)	Categoria	Unidades de log Baixo fluxo (EPS)	 Fluxo normal (EPS)	 Fluxo elevado (EPS)
Windows	900	Windows	300	1.500	3.000
Linux, HP, pfSense, Juniper	150	Syslogs tipo 1	2.000	10.000	20.000
Cisco. Sonicwall, Huaweii, Netscreen, Meraki, H3C	300	Syslogs tipo 2	1.500	6.000	12.000
Barracuda, Fortinet, Checkpoint	450	Syslogs tipo 3	1.200	4.000	7.000
Palo Alto, Sophos, F5, Firepower e outros syslogs	600	Syslogs tipo 4	800	2.500	5.000

Nota:

- Um servidor de instalação única pode gerenciar um máximo de 3.000 logs do Windows ou qualquer um dos valores de fluxo elevado mencionados para cada tipo de log na tabela acima.
- Para tipos de log não listados na tabela acima, selecione a categoria apropriada com base no tamanho do log. Por exemplo, no caso de logs do SQL Server, quando o tamanho do byte é 900 e o EPS é 3.000, deve ser considerado que isso é um fluxo elevado.
- Se o fluxo combinado for maior do que aquilo que um único node pode gerenciar, recomenda-se implementar a **configuração distribuída.**
- Recomenda-se também escolher a próxima faixa superior se a análise avançada de ameaças e muitas regras de correlação foram usadas.

Recomendações gerais

Infraestrutura VM

- Você deve alocar 100% de RAM/CPU à máquina virtual que está executando o EventLog Analyzer. O compartilhamento de memória/CPU com outras máquinas virtuais no mesmo host pode causar falta de RAM/CPU e impactar negativamente o desempenho do EventLog Analyzer.
- Use o provisionamento thick, pois o provisionamento thin aumenta a latência de E/S. No caso do VMware, selecione o provisionamento thick zerado rapidamente, pois o zerado lentamente tem desempenho inferior.
- A habilitação de snapshots de VM não é recomendada, pois o host duplica os dados em vários blocos, aumentando as leituras e gravações, resultando em maior latência de E/S e desempenho reduzido.

CPU e RAM

- A utilização da CPU do servidor sempre deve ser mantida abaixo de 85% para que o desempenho seja o ideal.
- Para um desempenho ideal, 50% da RAM do servidor deve ficar livre para uso fora da memória dinâmica do Elasticsearch.

Disco

- A latência do disco afeta o desempenho do EventLog Analyzer. O armazenamento de conexão direta (DAS) é recomendado tanto quanto a taxa de transferência de dados de um SSD com latência quase zero e alta taxa de transferência. Uma rede de área de armazenamento (SAN) corporativa pode ser mais rápida do que um SSD.

Navegadores da web

O EventLog Analyzer foi avaliado como compatível com os seguintes navegadores e versões, usando uma resolução de tela de 1024x768, pelo menos:

- Internet Explorer 11 e Edge
- Firefox 4 e posterior
- Chrome 8 e posterior

Bancos de dados

O EventLog Analyzer pode usar os seguintes bancos de dados como seu back-end.

Fornecido no pacote do produto

- PostgreSQL

Bancos de dados externos

- Microsoft SQL 2012 e superior

Observe os requisitos de hardware necessários para configurar o banco de dados do Microsoft SQL para o EventLog Analyzer:

RAM	CPU	IOPS	Espaço em disco
8 GB	6	300-500	300-500 GB

Sistemas operacionais

O EventLog Analyzer pode ser instalado em computadores que executam os seguintes sistemas operacionais e versões:

- Windows 7 e superior e Windows Server 2008 e superior
- Linux: Red Hat 8.0 e versões superiores/todas as versões de RHEL, Mandrake/Mandriva, SUSE, Fedora, CentOS, Ubuntu, Debian

Servidor de instalação

- As soluções SIEM consomem muitos recursos. Para um desempenho ideal, é recomendável implantar um servidor dedicado.
- O EventLog Analyzer usa o Elasticsearch. Espera-se que o seu processo use o espaçooff-heap de memória para um melhor desempenho. A memória off-heap é mantida pelo sistema operacional e será liberada quando necessário.

Recomendações adicionais do Elasticsearch Node

Hardware	Mínimo	Recomendado
Velocidade básica	2.4 GHz	3 GHz
Núcleo	12	16
RAM	64	64
Espaço em disco	1.2 TB	1.5 TB
IOPS	1.500*	1.500*

Como otimizar o espaço em disco rígido

Os dois principais fatores que contribuem para o espaço em disco rígido são o banco de dados e os arquivos gravados. Os arquivos do banco de dados (ou do índice) contêm os dados de log mais recentes que podem ser reportados e pesquisados, enquanto os arquivos gravados contêm os históricos mais antigos. Os arquivos gravados precisam ser carregados primeiro no produto antes que possam ser pesquisados ou incluídos em relatórios.

Espaço necessário no disco rígido

O espaço em disco rígido necessário para armazenar logs pode ser calculado usando o procedimento detalhado no guia de otimização de desempenho no site do EventLog Analyzer

Gerenciar o tamanho do banco de dados

Os dados de log ficam no banco de dados e são periodicamente comprimidos e armazenados entre os arquivos gravados. Quanto mais longo for o período de retenção no banco de dados, maior será o espaço em disco rígido necessário e menor será o seu desempenho. O período de retenção predefinido é de 32 dias e é configurável (Definições > Definições de administrador > Definições de retenção de banco de dados). Minimize este valor para obter um desempenho ideal.

Gerenciar o tamanho do arquivo

Os arquivos gravados são mantidos durante um período específico antes de serem eliminados permanentemente. Como podem ser armazenados para sempre, o tamanho da pasta de arquivo pode crescer indefinidamente. O período de retenção do arquivo é para sempre e configurável (Definições > Definições de configuração > Ver arquivos gravados > Definições com definições > Definições de administrador > Ver arquivos gravados > Definições). O tamanho da pasta de arquivo também pode ser gerenciado, atribuindo uma unidade dedicada separada como local de arquivamento ou transferindo manualmente o conteúdo para uma unidade de fita ou de armazenamento de alta capacidade periodicamente.

Segurança do EventLog Analyzer

Configuração da instalação

A conta de usuário do sistema operacional usada para instalar e executar o produto deve ser a mesma e ter permissões em todas as pastas e subpastas instaladas. Embora não seja necessário que a conta raiz seja usada em um sistema Linux ou Windows, somente a conta de administrador padrão deve ser usada.

Configuração do usuário

É melhor alterar as senhas predefinidas para as contas de usuário administrador e visitante no cliente web do EventLog Analyzer (Definições > Definições de administrador > Gerenciar técnico)

Certificação SSL

A comunicação servidor-cliente do EventLog Analyzer pode ser protegida usando o protocolo SSL (Secure Sockets Layer). O guia de certificação SSL oferece etapas detalhadas sobre como a obter.

Melhores práticas do banco de dados

Segurança do banco de dados

Para uma instalação suave e sem problemas, o EventLog Analyzer utiliza o usuário root/postgres padrão do banco de dados MySQL ou PostgreSQL sem senha. Recomenda-se atribuir uma senha a esta conta para proteger ainda mais o banco de dados.

Isso não é necessário no caso do Microsoft SQL, pois uma conta de usuário válida com credenciais precisa ser fornecida durante a instalação.

Otimizar o desempenho do banco de dados PostgreSQL

Para otimizar o desempenho do banco de dados PostgreSQL:

- Feche o EventLog Analyzer
- Navegue até <EventLog Analyzer home>/pgsql/data/directory.
- Abra o arquivo postgres_ext.txt.
- Substitua os valores dos parâmetros existentes pelos valores abaixo.
- Salve e reinicie o EventLog Analyzer.

Parâmetro	Comentário
shared_buffers=128 MB	O requisito mínimo é de 128 KB.
work_mem=12 MB	O requisito mínimo é de 64 KB.
maintenance_work_mem=100 MB	O requisito mínimo é de 1 MB.
checkpoint_segments=15	Segmentos de arquivo de log mínimo de 1 e 16 MB cada.
checkpoint_timeout=11 minutes	Amplitude: 30 segundos a 1 hora.
checkpoint_completion_target=0.9	a duração ideal do ponto de verificação é 0,0-1,0.
seq_page_cost=1.0	Este parâmetro é medido numa escala arbitrária.
random_page_cost=2.0	Este parâmetro é medido na mesma escala acima.
effective_cache_size=512MB	
synchronous_commit=off	

Otimizar o desempenho do banco de dados MySQL

Para otimizar o desempenho do banco de dados MySQL:

- Feche o EventLog Analyzer
- Navegue até <EventLog Analyzer home>/bin.
- Abra o arquivo startDB.bat (startDB.sh no caso de uma máquina Linux).
- Substitua o valor existente do parâmetro "--innodb_buffer_pool_size" por um valor adequado ao tamanho de RAM da máquina, conforme indicado na tabela abaixo. Por exemplo, se o tamanho da RAM for 8 GB, o parâmetro deve ser "--innodb_buffer_pool_size_3000M".
- Salve e reinicie o EventLog Analyzer.

Tamanho de RAM	Valor
1 GB	Valor padrão (não é necessário substituir)
2 GB	1200 M
3 GB	1500 M
4 GB	1500 M
8 GB	3000 M
16 GB	3000 M

Backup do banco de dados

Recomenda-se fazer um backup do banco de dados do EventLog Analyzer a cada quinzena para que os dados não sejam perdidos em caso de desastre. Os arquivos estão localizados em <EventLog Analyzer home>/mysql ou <EventLog Analyzer home>/pgsql, conforme aplicável ao número da versão. Para fazer backup dos dados, feche o serviço do EventLog Analyzer e faça uma cópia de todos os arquivos e pastas no local. Isso pode ser feito manualmente ou usando qualquer software de backup de terceiros. O procedimento para fazer backup dos dados do banco de dados do Microsoft SQL pode ser encontrado neste link. Também é aconselhável manter um backup dos dados arquivados, que se encontra em <EventLog Analyzer>/archive. Ao restaurar dados de um backup, verifique se o número da versão do produto é o mesmo de quando o backup foi feito.

Como otimizar o desempenho da pesquisa de logs

1. Forneça heap suficiente para o Elasticsearch

Para obter o desempenho ideal, mantenha a taxa de memória dinâmica para dados de 1:30. Isso significa que você deve alocar aproximadamente 1 GB de memória (heap) para cada 30 GB de dados no Elasticsearch Node. Para um melhor desempenho, você pode reduzir essa proporção (ou seja, 1:25 é melhor que 1:30).

O Elasticsearch também usa um cache de sistema de arquivos para fornecer pesquisas mais rápidas. Recomenda-se ter espaço livre suficiente em sua RAM equivalente à memória heap alocada para Elasticsearch. Se isso não for viável, certifique-se de que pelo menos 30% da RAM do servidor esteja livre. O sistema operacional usará essa RAM livre para armazenar em cache os índices do Elasticsearch e fornecer o melhor desempenho.

Nota: O heap alocado ao Elasticsearch não deve exceder 32 GB.

Exemplo:

Suponha que tenhamos **100 GB de dados de pesquisa**.

Então, o tamanho do heap para Elasticsearch deve ser de pelo menos → **100/30 4 GB**

Heap insuficiente é o motivo subjacente para vários problemas de desempenho, como:

- Desempenho lento de processamento/indexação de log
- Registro em cache
- Resultados da pesquisa com atraso
- Pesquisas com falha

Descubra o tamanho total dos dados armazenados no Elasticsearch

O Elasticsearch pode ser executado em uma instância comum compartilhada (<ManageEngine>/elasticsearch/ES) ou local (<EventLogAnalyzer>/ES)

Etapas para determinar o local do Elasticsearch (diretório ES):

- Quando o EventLog Analyzer for instalado como uma aplicação autônoma (ou seja, executado sem o Log360), o ES local estará em uso, localizado no diretório **<EventLogAnalyzer>\ES**.

- Se o EventLog Analyzer tiver sido instalado junto com o Log360, a configuração padrão do Elasticsearch (ES comum) estará em uso, localizada no diretório **<ManageEngine>\elasticsearch\ES**.

Etapas para verificar o tamanho dos dados do Elasticsearch:

1. Navegue até **<ES dorectory>\config.**
2. Abra o arquivo **elasticsearch.yml** na pasta config.
3. Procure **path.data** definido neste arquivo.

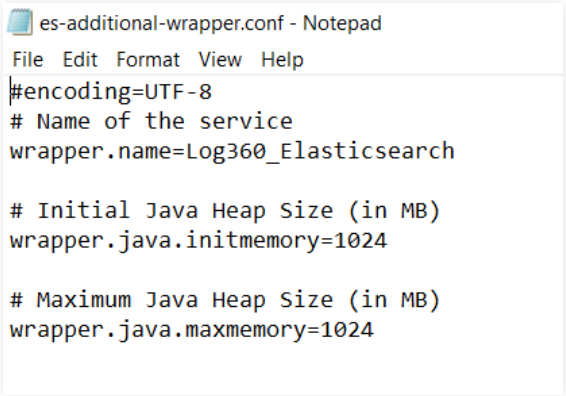
Navegue até a pasta de dados especificada na configuração **path.data** e verifique o tamanho da pasta.

Nota: Para garantir o desempenho ideal, monitore e faça a manutenção regularmente dos seus dados do Elasticsearch e limite o tamanho de um único node ES entre 800 GB e 1.2 TB.

Etapas para ajustaro heap (memória):

1. Navegue até o diretório ES, dependendo se ele é uma versão autônoma ou de pacote (com o Log360).
2. Navegue até **/ES/config.**
3. Abra o arquivo de configuração → **es- additional-wrapper.conf** e visualize o tamanho dao heap.

   Nota: Certifique-se de que o usuário conectado tenha permissão para gravar.



4. O tamanho do heap é gravado em MB.

   a. Tanto o wrapper.java.initmemory quanto o wrapper.java.maxmemory precisam ser definidos com o mesmo valor. Aqui está definido como 1024, ou seja, a memória do Elasticsearch está definida como (1024 MB/1024) = 1 GB.

   b. Se for necessário aumentar para 25 GB, então precisamos definir os dois valores para 25 x 1024 = 25600

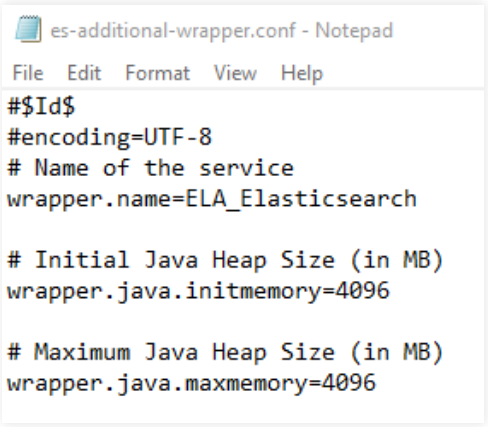
Etapas para aumentar o tamanho da memória dinâmica ES:

1. Abra o arquivo de configuração → **es-additional-wrapper.conf.**

2. Edite os valores de **wrapper.java.initmemory** e **wrapper.java.maxmemory** para aumentar o tamanho da memória dinâmica.

3. Certifique-se de que os valores de wrapper.java.initmemory e wrapper.java.maxmemory sejam os mesmos. Caso contrário, o produto não será inicializado corretamente.

4. Se o produto estiver em execução, interrompa o Elasticsearch indo **para ES/compartimento** e execute **stopES.bat** usando o prompt de comando admin ou apenas reinicie o EventLog Analyzer. Isso reiniciará o Elasticsearch com a nova memória dinâmica.



Nota:

- No caso de erros **OutOfMemory** e **LowMemory**, a memória dinâmica Elasticsearch expandirá automaticamente até um terço da RAM disponível na máquina.

- É importante observar que aumentar o tamanho da memória dinâmica nem sempre é a solução para melhorar o desempenho. Além da memória dinâmica, outros fatores, como disco e CPU, também podem causar problemas de desempenho. Certifique-se de que os Requisitos do sistema sejam atendidos.

- Também é importante monitorar o uso da memória regularmente para garantir que o sistema esteja funcionando de forma eficiente e ajustar as configurações, se necessário.

- Lembre-se de que o aumento do tamanho da memória dinâmica do Elasticsearch deve ser feito levando em consideração cuidadosamente os recursos disponíveis em sua máquina.

Certifique-se de que o disco não seja o afunilamento:

Se o servidor estiver gerando armazenamentos em cache (ou seja, o processamento de logs estiver lento) ou se as pesquisas estiverem lentas, você poderá:

a. Usar o armazenamento mais rápido, conforme mencionado na página Requisitos do sistema.

b. Verificar se o disco onde os dados estão armazenados não está fragmentado.

c. No **Monitor de recursos do Windows**, você pode verificar a guia **Disco**. Se a **Atividade do disco** exibir que o **tempo ativo maior** é ser sempre 100%, isso indica que o disco pode ter problemas ou não é rápido o suficiente.

2. Use nós de pesquisa adicionais para distribuir a carga de pesquisa/indexação para obter melhor desempenho

Você pode usar o **Gerenciamento do mecanismo de pesquisa**, que é um recurso presente no Log360 (Log360 → Admin → Search Engine Management) para adicionar nós Elasticsearch adicionais a fim de distribuir a carga de pesquisa e indexação usando máquinas extras.

a. Se o tamanho dos dados for muito grande para um único nó, é melhor adicionar nós adicionais para distribuir a carga de pesquisa/indexação.

b. Se o desempenho da pesquisa não for bom o suficiente, adicione nós adicionais.

c. Uma quantidade maior de nós ajuda no processamento mais rápido de logs.

Melhor prática para pesquisa:

- No EventLog Analyzer, **o período de retenção é de 32 dias por padrão** (pode ser aumentado **em Configurações → Configurações do banco de dados** na IU). Se ele for atualizado para 90 dias, então 32 dias de dados serão armazenados como dados ativos que podem ser acessados rapidamente. Os dados além disso serão armazenados como dados sem vida que precisam ser desarquivados e carregados em um mecanismo de pesquisa. Portanto, a pesquisa dos dados ao vivo além disso levará mais tempo do que o normal.

- Ao pesquisar os dados, tanto a memória dinâmica (memória atribuída ao Elasticsearch) quanto a que está fora da memória dinâmica (RAM livre no sistema) são usadas. A RAM livre no sistema permite que o Elasticsearch leia os índices mais rapidamente. Portanto, é aconselhável manter pelo menos a mesma quantidade de RAM livre no servidor equivalente à memória dinâmica fornecida ao Elasticsearch para melhor desempenho. Se isso não for viável, certifique-se de que pelo menos 30% da RAM do servidor esteja livre. O sistema operacional usará essa RAM livre para armazenar em cache os índices do Elasticsearch e fornecer o melhor desempenho.

É necessário ter um disco com boa velocidade de leitura sequencial e aleatória porque o processo de pesquisa envolve a iteração através de muitos arquivos, o que é uma operação intensa de E/S. Os SSDs devem ser preferidos, pois reduzem a carga e as esperas de E/S, além de ajudarem a explorar toda a potência da CPU.

Suporte às melhores práticas

Criar um arquivo de informações de suporte (SIF)

Quando o suporte é necessário, criar um arquivo de informações de suporte (SIF) para enviar à equipe de suporte (eventloganalyzer-support@manageengine.com) é útil e pode economizar tempo. Para criar uma SIF a partir do cliente web, vá para a guia Suporte do produto. Clique em "Criar arquivo de informações de suporte", aguarde 30-40 segundos e clique na guia Suporte novamente. Clique em baixar e envie a SIF baixada para a equipe de suporte, ou clique em "Carregar para o servidor FTP", forneça os detalhes necessários e envie. Se o servidor ou o cliente web não estiver funcionando, compacte os arquivos encontrados na pasta <EventLog Analyzer Home>/server/default/log e carregue o arquivo zip neste link FTP.

Sobre o EventLog Analyzer

O EventLog Analyzer é um software abrangente de gerenciamento de logs e conformidade de TI para SIEM. Ele fornece informações detalhadas sobre os logs de sua máquina na forma de relatórios, que ajudam a minimizar ameaças a fim de alcançar a segurança completa da 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 de TI para 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 escritórios em países do mundo inteiro, entre eles Estados Unidos, Reino Unido, Índia, Japão e China.