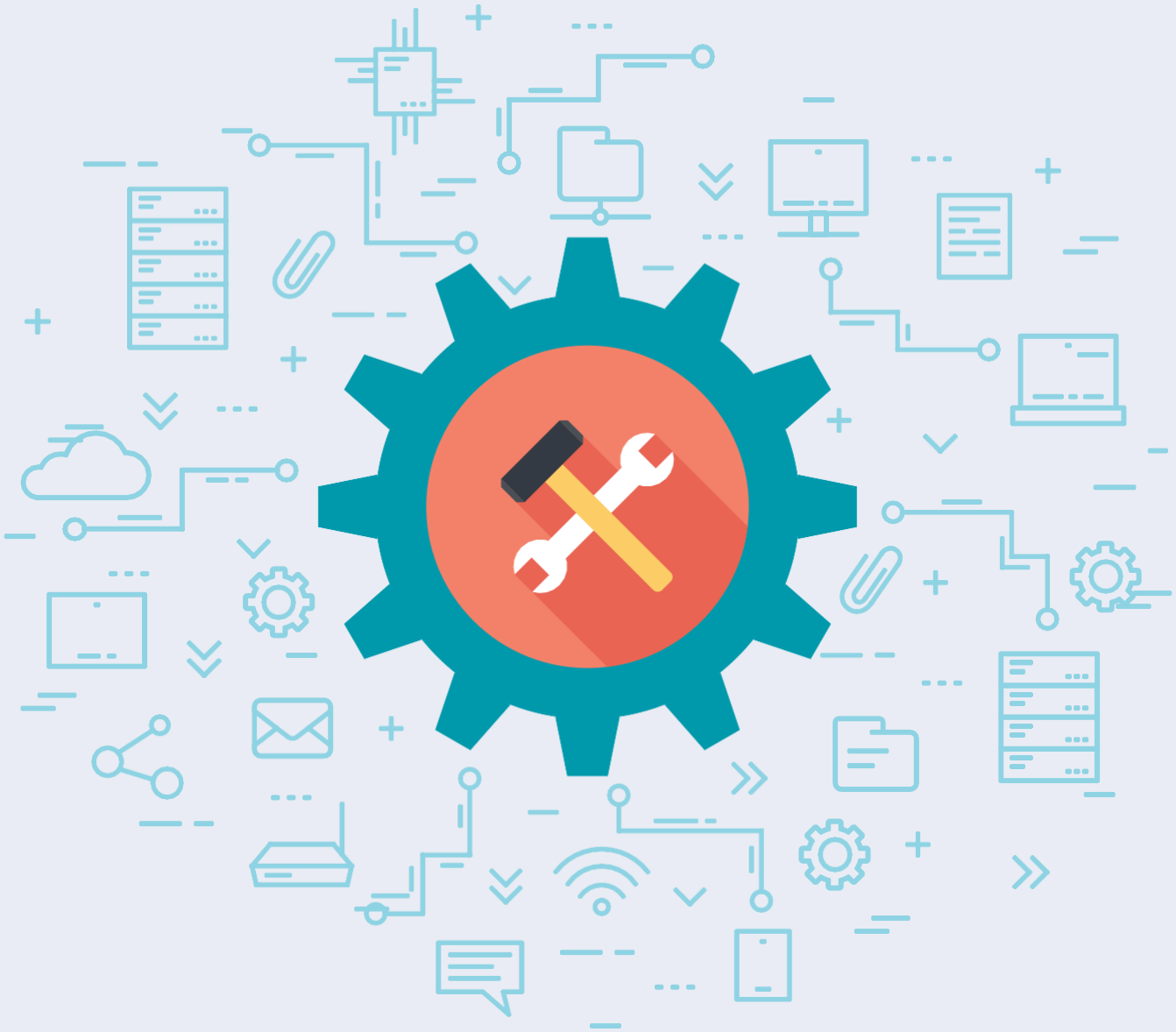
ManageEngine
EventLog Analyzer

Recuperação de Desastres e Guia de Configuração de Alta Disponibilidade



www.manageengine.com/br/eventlog/

Índice

Finalidade do documento

Este documento destaca as provisões para recuperação de desastres na versão distribuída do EventLog Analyzer. Ele também ilustra o funcionamento e os benefícios do recurso de alta disponibilidade no produto.

Versão distribuída do EventLog Analyzer

A versão distribuída do EventLog Analyzer envolve a implantação de um servidor de administração e muitos outros gerenciados. Os servidores gerenciados podem ser instalados em vários locais (um por ambiente de LAN) e conectados ao da administração central.

Servidor gerenciado: o servidor gerenciado é a instalação do EventLog Analyzer que coleta logs de fontes presentes nesse local específico. Essas informações são, então, retransmitidas para o único servidor de administração central.

Servidor administrador: o servidor administrador é a instalação do EventLog Analyzer que agrega informações de todos os outros servidores gerenciados instalados em todo o mundo. Ele atua como um único console central e exibe relatórios, alertas e outras informações de log de todos os servidores gerenciados.

Recuperação de Desastres para a Versão Distribuída do EventLog Analyzer

Os dados de log de todas as fontes são coletados e armazenados no servidor EventLog Analyzer. Eles, então, são analisados para detectar anomalias e ameaças à segurança da rede. Portanto, o servidor EventLog Analyzer é um componente crítico, sob a perspectiva da segurança de rede de uma organização. No caso improvável de uma falha grave em seu ambiente que faz com que o servidor da ferramenta fique inativo, o processamento e a análise de logs parariam. Essa parada pode ser um gateway para violações de segurança. Para evitar esses desastres, a solução tem um mecanismo de backup.

Como medida de recuperação de desastres, o EventLog Analyzer oferece um recurso de alta disponibilidade. Ele permite que cada servidor, tanto de administração quanto gerenciado, seja configurado com um servidor em espera. Esse servidor em espera monitoraria continuamente o principal. Caso o servidor principal falhe, o que está em espera imediatamente entrará e começará a executar todas as tarefas do servidor principal sem qualquer lapso. Leia mais sobre o funcionamento do módulo de alta disponibilidade do EventLog Analyzer nas próximas seções.

Alta disponibilidade no EventLog Analyzer

Para configurar a alta disponibilidade, o procedimento abaixo precisa ser executado em cada instalação do EventLog Analyzer, seja em um servidor de administração ou em um gerenciado.

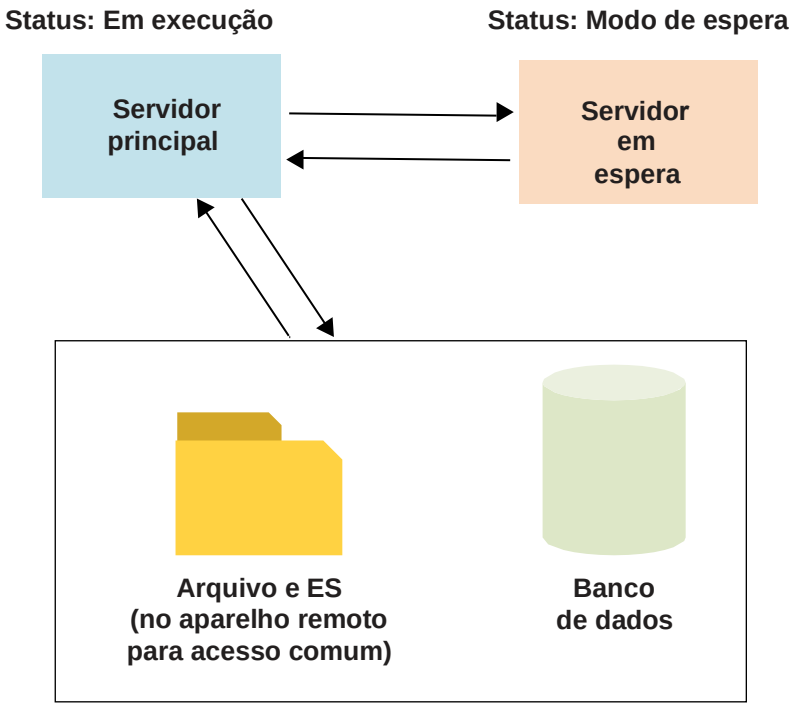
Por que é necessário garantir a alta disponibilidade do EventLog Analyzer?

Por ser uma solução de segurança de rede, o EventLog Analyzer monitora constantemente os dados de log, procura anomalias e padrões de ataque, valida ameaças e ajuda no combate a ataques contra a segurança.

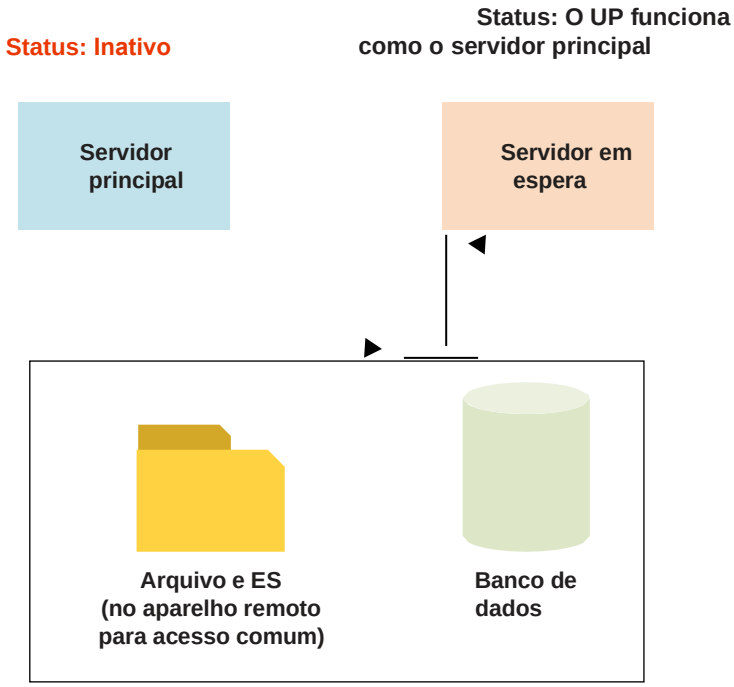
Se o servidor EventLog Analyzer ficar inativo, isso resultará em uma interrupção da coleta e análise de dados de log. Isso pode causar falhas na identificação de incidentes de segurança e, por sua vez, resultar em sérias violações de dados. Tais violações podem causar não apenas enormes perdas e penalidades financeiras de não conformidade, mas também uma perda de credibilidade e reputação. Portanto, é aconselhável garantir a alta disponibilidade do EventLog Analyzer e, assim, mantê-lo em execução o tempo todo.

Funcionamento da alta disponibilidade no EventLog Analyzer

A configuração de alta disponibilidade do EventLog Analyzer inclui duas instalações separadas. Uma delas atua como servidor principal, enquanto a outra atua como servidor em espera. Ambas as instalações apontariam para o mesmo banco de dados. E os dados de log arquivados e de ES estarão disponíveis no compartilhamento de rede comum.



Por padrão, o servidor principal fornecerá todos os serviços necessários. O servidor em espera também será iniciado, mas permanecerá no modo de espera. Mas ele continuará monitorando continuamente o status do servidor principal. Sempre que este falhar, o outro iniciará e aceitará a função do servidor principal. Ele começará a coletar os logs para evitar qualquer perda de dados e continuará a executar todas as funções do principal até que ele seja colocado de volta em serviço.



Pré-requisitos

Antes de começar a configurar o EventLog Analyzer para alta disponibilidade, certifique-se de ter dois endereços IP estáticos e um endereço IP virtual. Os dois servidores, principal e em espera, devem ter a mesma versão. Caso não haja correspondência, entre em contato com o suporte.

Nota: A alta disponibilidade não pode ser configurada em instalações Linux.

Etapas para configurar a alta disponibilidade

A configuração da alta disponibilidade no EventLog Analyzer é simples. As etapas a seguir explicarão como configurar a alta disponibilidade no EventLog Analyzer. Siga a etapa 1 para a nova instalação do EventLog Analyzer. Pule a 1 e vá para a etapa 2 para instalações existentes.

1. Faça download do EventLog Analyzer usando este link e instale-o em dois servidores separados.
   Nota: Os dois servidores, principal e em espera, devem estar na mesma rede, devem executar as mesmas versões do produto e devem usar a mesma porta e protocolo.
   Após a instalação, vá para a etapa 2.b

2. Para verificar se a sua instalação usa ES autônomo ou ES comum: Faça login no console do Log360,
   Navegue até **Admin → Administração → Pesquisar mecanismo de gerenciamento**

   a. Verifique a guia **Componente**. Se o EventLog Analyzer e o Log360 estiverem listados lá, sua instalação usará ES autônomo. Você pode pular esta etapa e ir para a etapa 3.
   Se ele mostrar apenas o Log360, sua instalação está usando o ES comum. Continue com a etapa b) para ES comuns.

   b. Como remover o EventLog Analyzer do Log360:
   No console do Log360, vá **para Admin → Administração → Integração do Log360 → EventLog Analyzer** e clique em **Remover.**

   Nota: O processo pode levar algum tempo para ser concluído. Não saia ou atualize a página.

3. Altere um dos bancos de dados do servidor do EventLog Analyzer para SQL, executando o arquivo changeDBserver.bat localizado em <EventLog_Analyzer Home>\tools. Na caixa de diálogo exibida, insira os detalhes necessários e salve.

4. Agora execute o mesmo arquivo **changeDBserver.bat** no outro servidor e aponte para o mesmo banco de dados.
   Nota:
   (a) Quando você executar o arquivo, uma mensagem de erro dizendo "Banco de dados já existe" será exibida. Essa mensagem de erro pode ser ignorada.

   (b) Certifique-se de que o primeiro servidor esteja inativo durante a execução **changeDBserver.bat** do arquivo no segundo servidor.

5. Observe que os dois servidores, principal e em espera, devem ter endereços IP estáticos. Para configurar o endereço IP estático:
   - Navegue até **Iniciar > Painel de controle > Centro de compartilhamento de rede > Ethernet (conexão de área local).**
   - Selecione o menu **Propriedades**.
   - Agora, desmarque **Versão 6 do protocolo da internet (TCP/IPv6).**
   - Selecione **Versão 4 do protocolo da internet (TCP/IPv4)** e clique em **Propriedades**.
   - Selecione o botão de seleção **Usar o seguinte endereço IP**.
   - Insira um endereço IP estático e a máscara de sub-rede.
   - Por fim, clique em **OK** para salvar a configuração.

   As mesmas etapas mencionadas acima precisam ser seguidas no servidor em espera para configurar o endereço IP estático.

6. Agora, adicione a entrada abaixo no arquivo **wrapper.conf** localizado em *<EventLog Analyzer_Home>\server\conf.*

   No servidor principal, inclua as linhas abaixo:

   wrapper.java.additional.x+1=-DremoteIp=<Secondary Server IP>
   wrapper.java.additional.x+2=-DlocalIp=<Primary Server IP>
   wrapper.java.additional.x+3=-DvirtualIp=<Virtual IP>

   No servidor em espera, adicione as linhas abaixo:

   wrapper.java.additional.x+1=-DremoteIp=<Primary Server IP>
   wrapper.java.additional.x+2=-DlocalIp=<Standby Server IP>
   wrapper.java.additional.x+3=-DvirtualIp=<Virtual IP>
   wrapper.java.additional.x+4=-DSecondary=true

   Nota:
   Os dois servidores, principal e em espera, devem ser configurados com o mesmo endereço IP virtual.

O valor de x varia dependendo da configuração em sua organização. Para encontrar o valor de x que você precisa inserir,

- Navegue até <EventLog Analyzer_Home>\server\conf\wrapper.conf e procure por "wrapper.java.additional.".
- Navegue até a última ocorrência do resultado da pesquisa e anote o valor numérico ao lado de "wrapper.java.additional.". Esse é o seu valor para x.
- Adicione os comandos para os dois servidores, principal e secundário, com base nesse valor de x.

Por exemplo, vamos considerar que a última ocorrência da pesquisa por "wrapper.java.additional." seja "wrapper.java.additional.36". Neste cenário, seu valor para x é 36 e as linhas que você precisaria adicionar ao servidor principal seriam:

wrapper.java.additional.37=-DremoteIp=123.456.789.123
wrapper.java.additional.38=-DlocalIp=123.456.789.124
wrapper.java.additional.39=-DvirtualIp=123.456.789.125

As linhas a serem adicionadas ao servidor em espera são:

wrapper.java.additional.37=-DremoteIp=123.456.789.124
wrapper.java.additional.38=-DlocalIp=123.456.789.123
wrapper.java.additional.39=-DvirtualIp=123.456.789.125
wrapper.java.additional.40=-DSecondary=true

Além disso, certifique-se de que

- o endereço IP virtual está no intervalo de IP da rede local. Ao usar esse endereço IP, o script de alta disponibilidade adicionará ou removerá automaticamente o IP virtual durante a inicialização e o desligamento do produto.
- Os processos do EventLog Analyzer estão vinculados ao IP virtual. No caso de monitoramento do Syslog, os dispositivos Syslog devem ser configurados para encaminhar seus dados de log para esse endereço IP virtual.

7. Agora, nos dois servidores, principal e em espera, edite e atualize o nome da interface (campo InterfaceName) e a máscara de rede IP virtual *(campo VirtualIPNetMask)* nos arquivos **StartHA.vbs** e **StopHA.vbs** localizados no *diretório <EventLog Analyzer_Home>\tools.* O valor do campo *interfaceName* deve ser do nome da conexão encontrado na **Central de compartilhamento de rede**. O campo *VirtualIPNetMask* deve ser preenchido com a máscara de sub-rede do IP virtual.

8. Edite os dados do caminho no arquivo elasticsearch.yml <*EventLogAnalyzer_Home/ES/Config*> para instalar o produto como um serviço. O valor do campo path.data deve ser o valor do local compartilhado comum, para que ele possa armazenar os logs dos dois servidores, principal e em espera, em dados ES. Os campos node.max_local_storage_nodes devem ser modificados para 2, para viabilizar a compatibilidade com a versão mais recente do ES em alta disponibilidade (node.max_local_storage_nodes: 2).

9. Antes de iniciar o EventLog Analyzer, verifique se ele está instalado como um serviço. Se ele não estiver instalado como um serviço, execute o comando **service.bat –I** a partir do *diretório <EventLog Analyzer_Home>\bin* para instalar o produto como um serviço.

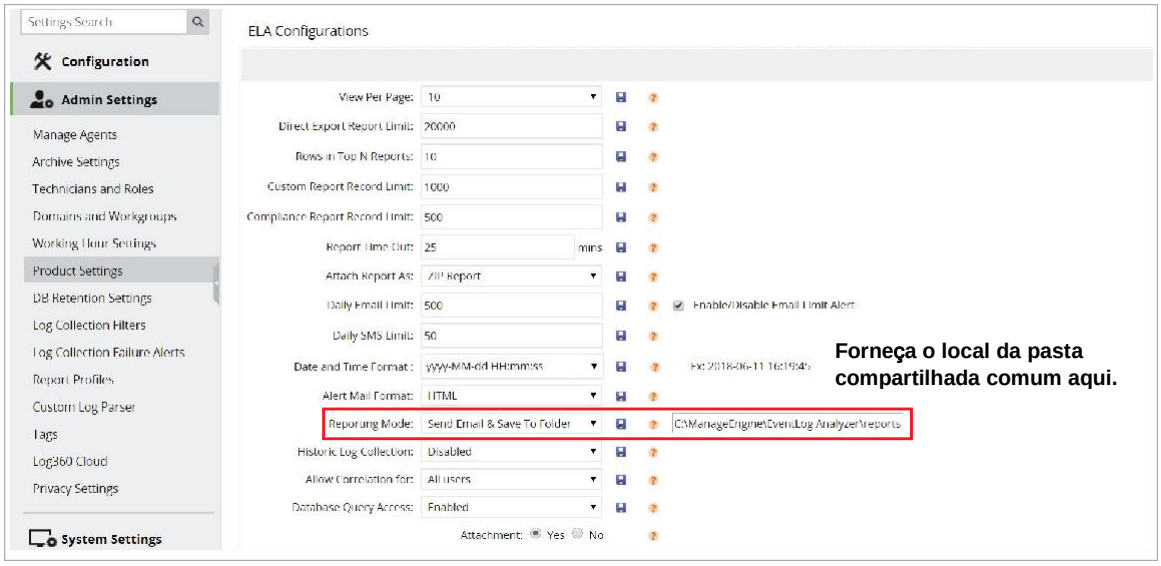
10. Inicie o servidor principal a partir do console dos Serviços do Windows.

Nota: Use apenas uma credencial de administrador para iniciar o serviço EventLog Analyzer nos dois servidores, principal e em espera.

11. Agora, no EventLog Analyzer, navegue até **Configurações> Arquivar> Configurações** e altere o local dos dados de log de arquivamento para a pasta compartilhada comum fornecendo seu caminho UNC exato.

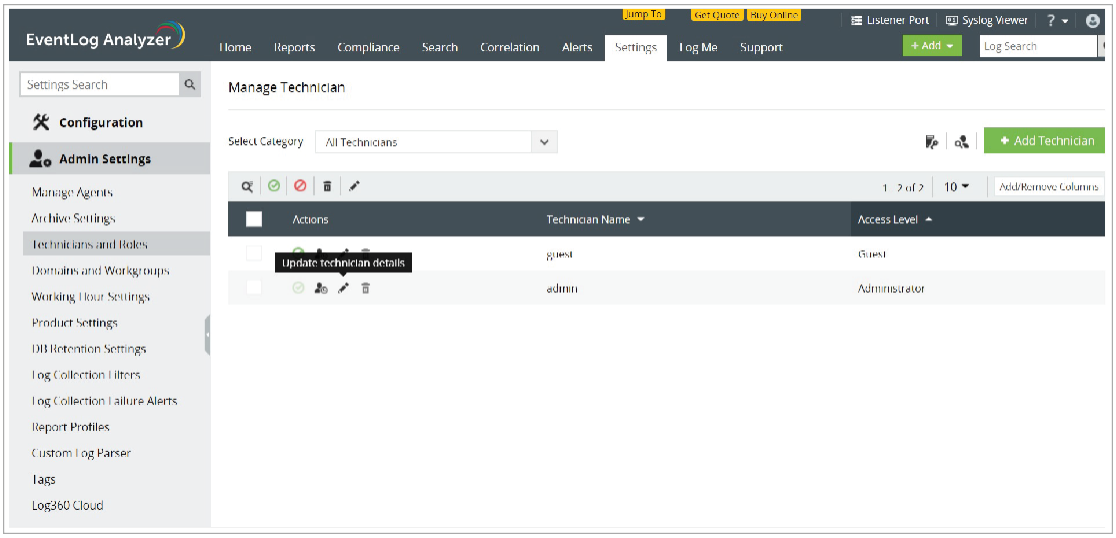
12. Você também precisa alterar o local de armazenamento dos relatórios personalizados. Para fazer isso, navegue até **Configurações> Configurações do administrador> Configurações do produto.** Na página **Configurações ELA**, forneça o local comum da pasta compartilhada no campo *caixa caminho UNC para o Modo de relatório*. Isso alterará o local de relatórios personalizados para a pasta compartilhada comum.

Nota: Verifique se você selecionou as opções **Enviar e-mail e Salvar na pasta** no *Modo de relatório*.



13. As notificações por e-mail serão enviadas aos usuários do produto que têm privilégios de administrador.

    Para configurar ou alterar o endereço de e-mail do usuário admin, navegue até **Configurações>Configurações administrativas> Técnicos e funções.** Isso exibirá os técnicos do produto e suas funções correspondentes. Clique no ícone de edição do usuário admin e será exibida a caixa de diálogo *Atualizar detalhes do técnico*, na qual você pode editar o endereço de e-mail do usuário admin.



14. Depois de configurar a alta disponibilidade, siga estas etapas para integrar o EventLog Analyzer ao Log360: Acesse **Admin→ Integração com o Log360**.

- Serão apresentadas duas guias, cada uma representando um componente do Log360.
- Digite **o endereço IP virtual** e o número da porta do servidor EventLog Analyzer configurado com alta disponibilidade.
- Selecione a conexão **Protocolo** na lista suspensa.
- Clique em **Integrar agora**.

Etapas para ativar o servidor em espera automaticamente

- Tente iniciar o serviço EventLog Analyzer no servidor em espera enquanto o servidor principal estiver operacional.

  O startup do serviço falhará, mas isso acionará um processo chamado **wscript.exe**, que começará a monitorar a disponibilidade do servidor principal.

- Assim que o servidor principal ficar inativo, o servidor em espera será iniciado automaticamente e as notificações por e-mail serão enviadas aos administradores imediatamente.

- Solução de problemas do servidor principal quando ele ficar inativo. Ao concluir a solução de problemas, desligue o servidor em espera manualmente e, em seguida, inicie o servidor principal.

- Quando o servidor principal estiver funcionando, execute a etapa 1 para iniciar o script no servidor em espera.

Etapas para atualizar o EventLog Analyzer para a versão mais recente.

Pré-requisitos:

- Antes de prosseguir com o processo de atualização, certifique-se de que haja espaço em disco suficiente no servidor EventLog Analyzer.

- Faça uma cópia de toda a pasta EventLog ou tire um instantâneo do servidor para ter um backup caso o upgrade falhe.

- Se você usa um banco de dados Microsoft SQL, solicitamos que você tire um instantâneo de seu banco de dados.

- Não interrompa nem cancele o processo de atualização. Se a atualização falhar, entre em contato com o suporte.

- É importante iniciar o produto após cada atualização bem-sucedida. Siga as etapas novamente para executar outra atualização.

Siga estas etapas para atualizar o EventLog Analyzer:

1. Antes de atualizar, certifique-se de parar os dois servidores, principal e em espera.

2. Aplique o pacote de serviços no servidor principal. Quando a atualização estiver concluída, inicie o servidor principal. Certifique-se de que o servidor principal esteja funcionando bem após a atualização.

3. Pare o servidor principal e, em seguida, aplique o pacote de serviços no servidor em espera. Quando a atualização estiver concluída, inicie o servidor em espera. Verifique se ele está funcionando bem e, em seguida, interrompa o servidor em espera.

4. Agora, ambos os servidores serão atualizados para a versão mais recente. Você pode iniciar o servidor principal e, em seguida, o servidor em espera, respectivamente.

Para obter mais esclarecimentos e dúvidas, entre em contato com **eventlog-support@manageengine.com.**