

Problema ao enviar email do Splunk - ação de alerta personalizada

Aplicabilidade

Splunk Enterprise Splunk Cloud

Descrição

Criado um novo aplicativo para substituir o endereço do remetente para alertas provenientes desse aplicativo específico.

Criado um arquivo .conf local para os valores substituídos no seguinte arquivo:

```
/opt/splunk/etc/apps/<app_name>/local/alert_actions.conf
```

O conteúdo é o seguinte:

```
[email]  
from = Service Desk <servicedesk@your_domain.com>  
footer.text =
```

Investigação

Criar laboratório.

Usando os arquivos de configuração:

- [savedsearch.conf](#)
- [alert_actions.conf](#)

1. Crie um alerta.
2. Altere o campo de email 'de' na Web do Splunk.
3. Altere o email do campo 'de' usando os arquivos de configuração.

Resolução

O Splunk precisa alterar o 'from' na notificação de alertas na interface do usuário da Web 'Configurações do servidor' e na CLI `alert_actions.conf`.

A maneira correta de alterar o campo 'de' é usar a interface do usuário da Web no Cabeçalho de Pesquisa: Configurações do servidor > Configurações de e-mail > Formato de e-mail > Enviar e-mails como

A alteração foi feita no Cabeçalho de Pesquisa e funcionou corretamente. Por algum motivo, o campo 'de' não foi aceito diretamente no aplicativo personalizado.

Certifique-se sempre de que o alerta em `savedsearchs.conf` não contenha um servidor de e-mail diferente que possa ter precedência sobre o servidor de e-mail definido em `alert_actions.conf`

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.