

Splunkから電子メールを送信するときに問題が発生しました – カスタムアラートアクション

適用性

SplunkエンタープライズSplunkクラウド

説明

特定のアプリケーションから受信したアラートの送信者アドレスを上書きする新しいアプリケーションを作成しました。

次のファイルで、オーバーライドされた値のローカル.confファイルを作成しました：

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

内容は次のとおりです。

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

調査

ラボを作成します。

設定ファイルを使用する場合：

- [savedsearches.conf \(保存検索.conf \)](#)
- [alert_actions.conf \(アラート アクション.conf \)](#)

1. アラートを作成します。
2. Splunk Webの送信元フィールドの電子メールを変更します。
3. 構成ファイルを使用して、'差出人'フィールドの電子メールを変更します。

解決方法

Splunkは、Web UIの「Server settings」とCLIのalert_actions.confにあるアラート通知の「from」を変更する必要があります。

「from」フィールドを変更する正しい方法は、検索ヘッドのWeb UIを使用することです。サーバ設定>電子メール設定>電子メール形式>電子メールの送信

検索ヘッドに変更が加えられ、正しく動作しました。何らかの理由で、'from'フィールドはカスタムアプリで直接受け付けられませんでした。

savedsearches.conf のアラートには、alert_actions.conf で設定されているサーバの電子メールよりも優先される可能性のある別の電子メールサーバが含まれていないことを常に確認してください

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。