

AWS用Splunkアドオン – 復号に失敗しました

適用性

Splunkアプリケーションアドオン

説明

環境：

Splunk Deployment Server(DS)を使用して、AWS用Splunk-Add-onをSplunk Heavy Forwarder(HF)にプッシュします。HFはAWSログファイルの収集用に設定されます。

問題：

AWSのログはまだ取り込まれています。

調査

HFインスタンスのログファイルで次のエラーメッセージが見つかりました。

splunkd.log:

```
07-03-2019 13:28:35.327 -0600 ERROR Crypto - Decryption operation failed: AES-GCM Decryp
07-03-2019 13:28:35.327 -0600 WARN ConfigEncryptor - Decryption operation failed: AES-GC
```

エラーメッセージに基づくと、これは次のSplunkの回答の記事で説明されている問題と非常によく似ています。

Splunk Enterprise 7.2.1をインストールし、クラスタマスターとして昇格しました。Splunk Webがロードされていません。

<https://answers.splunk.com/answers/723728/installed-splunk-enterprise-721-and-promoted-it-as.html>

解決方法

配置サーバーで、次の操作を行います。

1. splunk.secretのバックアップコピーを\$SPLUNK_HOME/etc/authディレクトリに作成しました。
2. splunk.secretを削除
3. Heavy Forwarder(HF)からDeployment Server(DS)にsplunk.secret keyをコピーしました。
4. /opt/splunk/etc/system/local/server.confファイルのバックアップコピーを作成しました。
5. server.confファイルのpass4SymmKeyでコメントアウト
6. server.confファイルの[sslConfig] stanzaの下にsslPasswordを再入力しました。
7. Splunkの再起動
8. 新しいSplunk_TA_aws/local/passwords.confファイルをHFにプッシュしました。

今後の推奨事項：

1. HWからDSインスタンスにsplunk.secret keyをコピーする現在のアプローチは実行可能なソリューションですが、次のものが必要な場合があります

将来検討する予定です

DSが他のフォワーダ/導入クライアントと連携するためには、同じsplunk.secret keyがすべてのフォワーダ/クライアントに配布される必要があります。これにより、復号化に失敗したエラーを回避できます。

2. もう1つの方法は、DSインスタンスのpasswords.confファイルでクリアテキスト形式のパスワードを設定することです。

次に、展開クライアント(HF)で、ファイルがDSからプッシュされた後にパスワードを暗号化します。HWはパスワードを復号化する

再起動直後。

関連リンク

Splunkの回答

Splunk Enterprise 7.2.1をインストールし、クラスタマスターとして昇格しました。Splunk Webがロードされていません。 <https://answers.splunk.com/answers/723728/installed-splunk-enterprise-721-and-promoted-it-as.html>

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。