

Splunk Add-on for AWS — 解密失敗

適用性

Splunk應用載入項

說明

環境：

使用Splunk Deployment Server(DS)將AWS的Splunk-Add-on推送到Splunk Heavy Forwarder(HF)，後者配置為收集AWS日誌檔案。

問題：

AWS日誌仍然被侵入。

調查

在HF例項的日誌檔案中發現了以下錯誤消息。

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
```

根據錯誤資訊，這與以下Splunk Answers文章中涉及的問題非常相似：

已安裝Splunk Enterprise 7.2.1並將其升級為集群主節點。Splunk Web未載入。

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

解析

在部署伺服器上：

- 1.在\$SPLUNK_HOME/etc/auth目錄中製作了splunk.secret的備份副本。
- 2.刪除的splunk.secret
- 3.將splunk.secret金鑰從重型轉發器(HF)複製到部署伺服器(DS)。
- 4.製作了/opt/splunk/etc/system/local/server.conf檔案的備份副本。
- 5.在server.conf檔案的pass4SymmKey中註釋掉
- 6.在server.conf檔案的[sslConfig] stanza下重新輸入sslPassword。
- 7.重新啟動Splunk
- 8.將新的Splunk_TA_aws/local/passwords.conf檔案推送至高頻。

今後的建議：

- 1.當前將splunk.secret金鑰從硬體複製到DS例項的方法是一個可行的解決方案，但可能需要採取以下措施
供今後考慮。
為了使DS與其他轉發器/部署客戶端合作，必須向所有轉發器/客戶端分發相同的splunk.secret金鑰。這樣可以避免因解密錯誤而失敗。

- 2.另一種方法是在DS例項的passwords.conf檔案中以明文格式設定密碼。
然後，一旦從DS推送檔案，讓部署客戶端(HF)對密碼進行加密。HW將解密密碼在重新啟動後立即重新啟動。

相關連結

Splunk答案

已安裝Splunk Enterprise 7.2.1並將其升級為集群主節點。Splunk Web未載入。
<https://answers.splunk.com/answers/723728/installed-splunk-enterprise-721-and-promoted-it-as.html>

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。