

用于AWS的Splunk加载项 — 解密失败

适用范围

Splunk应用加载项

描述

环境：

使用Splunk Deployment Server(DS)将AWS的Splunk-Add-on推送到Splunk Heavy Forwarder(HF)，后者配置为收集AWS日志文件。

问题：

AWS日志仍然被摄取。

调查

在HF实例的日志文件中发现以下错误消息。

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
```

根据错误消息，这与以下Splunk Answers文章中涉及的问题非常相似：

已安装Splunk Enterprise 7.2.1并将其升级为集群主用设备。Splunk Web未加载。

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

分辨率

在部署服务器上：

- 1.在\$SPLUNK_HOME/etc/auth目录中制作了splunk.secret的备份副本。
- 2.删除的splunk.secret
- 3.将splunk.secret密钥从重型转发器(HF)复制到部署服务器(DS)。
- 4.制作了/opt/splunk/etc/system/local/server.conf文件的备份副本。
- 5.在server.conf文件的pass4SymmKey中注释掉
- 6.在server.conf文件中的[sslConfig] stanza下重新输入sslPassword。
- 7.重新启动Splunk
- 8.将新的Splunk_TA_aws/local/passwords.conf文件推送到高频。

未来的建议：

- 1.当前将splunk.secret密钥从硬件复制到DS实例的方法是一个可行的解决方案，但可能需要以下几点供将来考虑。
为了使DS与其他转发器/部署客户端配合工作，必须向所有转发器/客户端分发相同的splunk.secret密钥。这样可以避免因解密错误而失败。

- 2.另一种方法是在DS实例的passwords.conf文件中以明文格式设置密码。
然后，让部署客户端(HF)在从DS推送文件后加密密码。HW将解密密码在重新启动后立即启动。

相关链接

Splunk答案

已安装Splunk Enterprise 7.2.1并将其升级为集群主用设备。Splunk Web未加载。
<https://answers.splunk.com/answers/723728/installed-splunk-enterprise-721-and-promoted-it-as.html>

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。