

Splunk-Add-on für AWS - Entschlüsselung fehlgeschlagen

Geltungsbereich

Splunk-Apps-Add-ons

Beschreibung

Umgebung:

Verwenden eines Splunk-Bereitstellungsservers (DS) zum Übertragen von Splunk-Add-on für AWS an den Splunk Heavy Forwarder (HF), der für das Sammeln von AWS-Protokolldateien konfiguriert ist.

Problem:

AWS-Protokolle wurden noch aufgenommen.

Untersuchung

Die folgende Fehlermeldung wurde in den Protokolldateien der HF-Instanz gefunden.

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
```

Basierend auf der Fehlermeldung ähnelt dies stark dem Problem, das im folgenden Splunk Answers-Artikel angesprochen wird:

Splunk Enterprise 7.2.1 installiert und als Cluster-Master hochgestuft. Splunk Web wird nicht geladen.

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

Auflösung

Auf dem Bereitstellungsserver:

1. Sicherungskopie von splunk.secret im Verzeichnis \$SPLUNK_HOME/etc/auth erstellt.
2. Entfernen splunk.secret
3. Splunk.Secret-Schlüssel vom Heavy Forwarder (HF) zum Bereitstellungsserver (DS) kopiert.
4. Sicherungskopie der Datei /opt/splunk/etc/system/local/server.conf erstellt.
5. Auskommentiert in pass4SymmKey in server.conf-Datei
6. sslPassword in der Datei server.conf unter [sslConfig] stanza erneut eingegeben.
7. Splunk neu gestartet
8. Neue Datei Splunk_TA_aws/local/passwords.conf in das HF-Laufwerk verschoben.

Künftige Empfehlungen

1. Der aktuelle Ansatz, den splunk.secret-Schlüssel von der HW in die DS-Instanz zu kopieren, ist eine praktikable Lösung. Folgendes kann jedoch erforderlich sein:
in Zukunft berücksichtigt werden.

Damit der DS mit anderen Weiterleitungs-/Bereitstellungsclients zusammenarbeiten kann, muss derselbe splunk.secret-Schlüssel an alle Weiterleitungs-/Clients verteilt werden. Dadurch werden Fehler beim Entschlüsseln vermieden.

2. Ein alternativer Ansatz besteht darin, Kennwörter im Klartextformat in der Datei "passwords.conf" für die DS-Instanz festzulegen.

Lassen Sie dann den Deployment Client (HF) die Passwörter verschlüsseln, sobald die Dateien von DS übertragen werden. HW entschlüsselt die Passwörter unmittelbar nach dem Neustart.

Verwandte Links

Punktantworten

Splunk Enterprise 7.2.1 installiert und als Cluster-Master hochgestuft. Splunk Web wird nicht geladen. <https://answers.splunk.com/answers/723728/installed-splunk-enterprise-721-and-promoted-it-as.html>

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.