

Splunk Add-on voor AWS - Decryptie mislukt

toepasbaarheid

Splunk Apps-add-ons

Beschrijving

Milieu:

Een Splunk Deployment Server (DS) gebruiken om Splunk-Add-on voor AWS naar de Splunk Heavy Forwarder (HF) te duwen, die is geconfigureerd voor het verzamelen van AWS-logbestanden.

Kwestie:

AWS-logboeken werden nog steeds ingenomen.

onderzoek

De volgende foutmelding is gevonden in de logbestanden op de HF-instantie.

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
```

Op basis van de foutmelding lijkt dit sterk op het probleem dat wordt behandeld in het volgende artikel in Splunk Answers:

Splunk Enterprise 7.2.1 geïnstalleerd en gepromoot als clustermaster. Splunk Web wordt niet geladen.

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

resolutie

Op de implementatieserver:

1. Maak een back-up van splunk.secret in \$SPLUNK_HOME/etc/auth directory.
2. Verwijderde splunk.secret
3. Gekopieerde splunk.secret-sleutel van heavy forwarder (HF) naar de implementatieserver (DS).
4. Maak een back-up van het bestand /opt/splunk/etc/system/local/server.conf.
5. Opmerkingen in pass4SymmKey in server.conf-bestand
6. SSLPassword opnieuw ingevoerd onder [sslConfig] stanza in het bestand server.conf.
7. Opnieuw opgestarte Splunk
8. Duwde nieuw Splunk_TA_aws/local/passwords.conf bestand naar de HF.

Toekomstige aanbevelingen:

1. De huidige aanpak van het kopiëren van de sleutel splunk.secret van HW naar de DS-instantie is een werkbare oplossing, maar het volgende kan nodig zijn in de toekomst te worden overwogen.

Om de DS te laten samenwerken met andere forwarders/implementatieclients, moet dezelfde splunk.secret-sleutel worden gedistribueerd naar alle forwarders/clients. Dit voorkomt dat het mislukt is om fouten te decoderen.

2. Een alternatieve benadering is om wachtwoorden in een duidelijke tekstindeling in te stellen in het bestand passwords.conf op de instantie DS.

Laat vervolgens de implementatieclient (HF) de wachtwoorden coderen zodra de bestanden van DS worden gepusht. HW zal de wachtwoorden decoderen onmiddellijk nadat het opnieuw is opgestart.

Gerelateerde links

Splunk Antwoorden

Splunk Enterprise 7.2.1 geïnstalleerd en gepromoot als clustermaster. Splunk Web wordt niet geladen. <https://answers.splunk.com/answers/723728/installed-splunk-enterprise-721-and-promoted-it-as.html>

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.