

Splunk Add-on para AWS - Error de descifrado

Aplicabilidad

Complementos de aplicaciones Splunk

Descripción

Entorno:

Uso de un Splunk Deployment Server (DS) para insertar Splunk-Add-on para AWS en Splunk Heavy Forwarder (HF), que está configurado para recopilar archivos de registro de AWS.

Problema:

Los registros de AWS todavía se estaban ingiriendo.

Investigación

Se ha encontrado el siguiente mensaje de error en los archivos de registro de la instancia de HF.

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
```

Según el mensaje de error, esto es muy similar al problema tratado en el siguiente artículo de Splunk Answers:

Se instaló Splunk Enterprise 7.2.1 y se promocionó como clúster principal. La Web de Splunk no se carga.

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

Resolución

En el servidor de implementación:

1. Realizó una copia de seguridad de splunk.secret en el directorio \$SPLUNK_HOME/etc/auth.
2. Eliminado splunk.secret
3. Clave splunk.secret copiada desde el reenviador pesado (HF) al servidor de implementación (DS).
4. Hizo una copia de seguridad del archivo /opt/splunk/etc/system/local/server.conf.
5. Comentado en pass4SymmKey en el archivo server.conf
6. Se ha vuelto a introducir la contraseña ssl en la estrofa [sslConfig] del archivo server.conf.
7. Splunk reiniciado
8. Se envió el nuevo archivo Splunk_TA_aws/local/passwords.conf al HF.

Recomendaciones futuras:

1. El enfoque actual de copiar la clave splunk.secret del hardware a la instancia de DS es una solución factible, pero puede ser necesario lo siguiente para que se considere en el futuro.

Para que DS funcione con otros reenviadores/clientes de implementación, se debe distribuir la misma clave splunk.secret a todos los reenviadores/clientes. Esto evitará que se produzcan errores al descifrar.

2. Un enfoque alternativo es establecer contraseñas en formato de texto no cifrado en el archivo passwords.conf en la instancia DS.

A continuación, permita que el cliente de implementación (HF) cifre las contraseñas una vez que los archivos se envíen desde DS. El hardware descifrará las contraseñas inmediatamente después de reiniciarlo.

Enlaces relacionados

Respuestas de Splunk

Se instaló Splunk Enterprise 7.2.1 y se promocionó como clúster principal. La Web de Splunk no se carga. <https://answers.splunk.com/answers/723728/installed-splunk-enterprise-721-and-promoted-it-as.html>

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).