

لشف - AWS لة فياضة إلى SPLUNK ة فيظو ري فشتلا كف

قيبطتلا ةيلباق

Splunk تاقيبطت ةفاضة

فصولا

ةئيبلا:

Splunk Heavy Software (HF)، إلى AWS ل Splunk-Add-on ع فدل (DS) Splunk رشن م داخ مادختسا
AWS ل جس تافل م ع م جل هنيوكت مت يذلا.

ةلكشملا:

اهلوانت متي لازت ال AWS ع وذج.

ءالجتسا

HF. ل يثم ي ف ل جسلا تافل م ي ف ةيلاتلا أطخال ةلاسري ل ع روثعلا مت

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
```

Splunk ةلاقم ي ف اهتجالع م مت ي تال ةلاسرم لل ادج الاثامم اذه نوكي ،أطخال ةلاسري ل ع ءانب
ةيلاتلا Answers:

Splunk ل يمح ت متي مل .ةعومجمل لماظن ري دمك هتي قرتو 7.2.1 Splunk Enterprise تي ب ت مت
Web.

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

رارق

رشننل مداخل في:

1. \$SPLUNK_HOME/etc/auth لي ل د في splunk.secret نم ةي طاي تح | ةخسن عارج اب مق .
2. splunk.secret ةلازا تمت .
3. (DS) رشننل مداخل | (HF) لي قثل هجومل نم خوسنم splunk.secret حاتفم .
4. /opt/splunk/etc/system/local/server.conf فلم نم ةي طاي تح | ةخسن لمعب مق .
5. server.conf فلم في pass4SymmKey في قيلعتل مت .
6. stanza [sslConfig] نمض sslPassword لخال | ةداع | تمت .
7. Splunk لي غشت ةداع | .
8. HF | دربم Splunk_TA_aws/local/passwords.conf دي دج عفد .

ةيلبقتسمل تاي صوتل:

1. الباق الح DS لي ثم | ةزهجال نم splunk.secret حاتفم خسنل | لالحال جهنل دعي .
يلالال جهنل عابتا مزل ي دق نكلو ، قيبطتلل
لبقتسمل في رابتعالا ني عب هذخا ني عتي
هسفن splunk.secret حاتفملا عيزوت بجي ، ني رخال رشننل مالعم/ني درومل عم DS لمعي يكل
ءاطخال ري فشت ك في لشفال بنجت | اذه ي دوي س . مالعملال/ني درومل عي مچ | لع

2. passwords.conf فلم في حضاو صن قيسننن رورمل تاملك ني عتي وه لي دب جهن كانه .
DS لي ثم | لع
زاهجال موقي . DS نم تافلمل عفد درج ب رورمل تاملك ري فشتل (HF) رشننل لي مع كرتا م
رورمل تاملك ري فشت ك فب
هل غشت ةداع | دعب ةرشابم .

ةلص تا ذ طباور

زرسنأ كنولبس |

Splunk لي محت متي مل . ةعومجمل ماظن ري دمك هتي قرتو Splunk Enterprise 7.2.1 تي بثلث مت
Web. <https://answers.splunk.com/answers/723728/installed-splunk-enterprise-721-and-promoted-it-as.html>

ةمچرتل هذه ل و ح

ةيلآل ا تاي ن ق ت ل ا ن م ة و م ج م ا د خ ت س ا ب د ن ت س م ل ا ا ذ ه Cisco ت م چ ر ت م ل ا ع ل ا ا ح ن ا ع م ج ي ف ن ي م د خ ت س م ل ل م ع د ي و ت ح م م ي د ق ت ل ة ي ر ش ب ل و ا م ك ة ق ي ق د ن و ك ت ن ل ة ي ل آ ة م چ ر ت ل ض ف ا ن ا ة ط ح ا ل م ي ج ر ي . ة ص ا خ ل ا م ه ت غ ل ب Cisco ي ل خ ت . ف ر ت ح م م چ ر ت م ا ه م د ق ي ي ت ل ا ة ي ف ا ر ت ح ا ل ا ة م چ ر ت ل ا ع م ل ا ح ل ا و ه ي ل ا ا م ا د ع و ج ر ل ا ب ي ص و ت و ت ا م چ ر ت ل ا ه ذ ه ة ق د ن ع ا ه ت ي ل و ئ س م Systems (ر ف و ت م ط ب ا ر ل ا) ي ل ص ا ل ا ي ز ي ل ج ن ا ل ا د ن ت س م ل ا