

# Splunk Add-on per AWS - Decrittografia non riuscita

## Applicabilità

Componenti aggiuntivi applicazioni Splunk

## Descrizione

Ambiente:

Utilizzo di un server di distribuzione Splunk (DS) per eseguire il push del componente aggiuntivo Splunk per AWS in Splunk Heavy Forwarder (HF), configurato per la raccolta dei file di registro AWS.

Problema:

I registri AWS venivano ancora ingeriti.

## Indagine

Il seguente messaggio di errore è stato trovato nei file di log nell'istanza 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
```

In base al messaggio di errore, questo è molto simile al problema affrontato nel seguente articolo di Splunk Answers:

Splunk Enterprise 7.2.1 è stato installato e promosso come master del cluster. Splunk Web non in fase di caricamento.

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

## Risoluzione

Nel server di distribuzione:

1. Eseguita una copia di backup di splunk.secret nella directory \$SPLUNK\_HOME/etc/auth.
2. Splunk.secret rimosso
3. Chiave splunk.secret copiata dal server di inoltro pesante (HF) al server di distribuzione (DS).
4. Effettuato una copia di backup del file /opt/splunk/etc/system/local/server.conf.
5. Commentato in pass4SymmKey nel file server.conf
6. Reinserito sslPassword nella stanza [sslConfig] nel file server.conf.
7. Splunk riavviato
8. È stato eseguito il push del nuovo file Splunk\_TA\_aws/local/passwords.conf nell'HF.

Raccomandazioni future:

1. L'approccio corrente per la copia della chiave splunk.secret dall'hardware all'istanza DS è una soluzione fattibile, ma potrebbe essere necessario quanto segue in futuro.

Affinché DS possa funzionare con altri server d'inoltro/client di distribuzione, la stessa chiave splunk.secret deve essere distribuita a tutti i server d'inoltro/client. In questo modo si eviteranno errori di decrittografia non riusciti.

2. Un approccio alternativo consiste nell'impostare le password in formato testo non crittografato nel file passwords.conf sull'istanza DS.

Consentire quindi al client di distribuzione (HF) di crittografare le password dopo il push dei file da DS. Le password verranno decrittografate immediatamente dopo il riavvio.

## Collegamenti correlati

Risposte Splunk

Splunk Enterprise 7.2.1 è stato installato e promosso come master del cluster. Splunk Web non in fase di caricamento. <https://answers.splunk.com/answers/723728/installed-splunk-enterprise-721-and-promoted-it-as.html>

### Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).