

Complemento Splunk para AWS - Falha na descriptografia

Aplicabilidade

Complementos de Aplicativos Splunk

Descrição

Ambiente:

Usando um Servidor de Implantação de Splunk (DS) para enviar o Splunk-Add-on para o AWS para o Splunk Heavy Forwarder (HF), que é configurado para coletar arquivos de log do AWS.

Problema:

Os logs AWS ainda estavam sendo ingeridos.

Investigação

A seguinte mensagem de erro foi encontrada nos arquivos de log na instância 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
```

Com base na mensagem de erro, isso é muito semelhante ao problema abordado no seguinte artigo de Respostas Splunk:

Instalado o Splunk Enterprise 7.2.1 e promovido-o como cluster mestre. O Splunk Web não está sendo carregado.

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

Resolução

No servidor de implantação:

1. Feito uma cópia de backup de splunk.secret no diretório \$SPLUNK_HOME/etc/auth.
2. splunk.secret removido
3. Chave splunk.secret copiada do encaminhador pesado (HF) para o servidor de implantação (DS).
4. Feito um backup do arquivo /opt/splunk/etc/system/local/server.conf.
5. Comentado em pass4SymmKey no arquivo server.conf
6. sslPassword reinserida na estrofe [sslConfig] no arquivo server.conf.
7. Splunk Reiniciado
8. Novo arquivo Splunk_TA_aws/local/passwords.conf enviado por push para o HF.

Recomendações futuras:

1. Abordagem atual da cópia da chave splunk.secret do HW para a instância do DS é uma solução viável, mas pode ser necessário o seguinte a considerar no futuro.

Para que o DS funcione com outros encaminhadores/clientes de implantação, a mesma chave splunk.secret deve ser distribuída para todos os encaminhadores/clientes. Isso evitará erros de falha na descryptografia.

2. Uma abordagem alternativa é definir senhas em formato de texto claro no arquivo passwords.conf na instância DS.

Em seguida, deixe que o cliente de distribuição (HF) criptografe as senhas depois que os arquivos forem enviados do DS. O HW irá descryptografar as senhas imediatamente após ter sido reiniciado.

Links relacionados

Respostas de Splunk

Instalado o Splunk Enterprise 7.2.1 e promovido-o como cluster mestre. O Splunk Web não está sendo carregado. <https://answers.splunk.com/answers/723728/installed-splunk-enterprise-721-and-promoted-it-as.html>

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.