

Os certificados SSL do coletor de eventos HTTP (HEC) não estão funcionando

Aplicabilidade

Empresa Splunk

Descrição

Depois de configurar certificados SSL para HEC em HFs (Heavy Forwarders), o Splunk ainda assume os certificados padrão, não os criados.

Investigação

Pontos a serem considerados:

- No momento, o SSL está configurado apenas em web.conf. Configure o SSL para HEC separadamente.
- Usar certificados autoassinados, não certificados da Web.
- Os certificados da Web removem as senhas de chave privada, mas os certificados autoassinados usados para HEC mantêm a senha.
Como autoassinar certificados chave privada usa a senha

[Como autoassinar certificados](#)

Os certificados de autoassinatura para a Web de tronco ao criar um novo certificado privado para a Web de tronco removem a senha.

[Autoscertificados paraSplunkWeb](#)

Resolução

O certificado SSL para HEC configurado no arquivo web.conf tem uma chave privada sem uma senha,

Siga as seguintes etapas do documento para gerar uma chave privada com uma senha para resolver o problema.

[Gerar uma chave para o certificado do servidor](#)

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.