

Não é possível pesquisar campos com "="

Aplicabilidade

Splunk Enterprise Splunk Cloud

Descrição

Versão do Splunk: 7.0.13

Ao tentar pesquisar um dos seguintes campos correspondendo a uma string:

- pod
- namespace
- container_name
- container_id

Como container_id=aadd1, não retornará resultados.

Investigação

Depois de algumas pesquisas, percebeu-se que os dados HEC nesta configuração são indexados sem nenhum arquivo de configuração, mas para usá-lo corretamente é necessária alguma configuração. Os campos podem ser de fato pesquisados pela configuração com o comando `:: sinal` (especificador de campos de metadados), mas isso não corrige o fato de que eles não podem ser pesquisados com o sinal `=`.

Para que isso funcione, outras configurações devem ser executadas na pesquisa. Parece que, quando há entradas HEC para as kubernetes GCP, os eventos não estão totalmente preparados para serem pesquisados. Particularmente os campos parecem permanecer não indexados, que é parte dos dados brutos, mas não para ser especificado na pesquisa para obter eventos.

Resolução

Como os eventos não obtêm parâmetros de configuração indexados, eles devem ser adicionados da seguinte forma:

Instância: Cabeçalho de pesquisa

Arquivo: campos.conf

Caminho: \$SPLUNK_HOME/etc/apps/search/local

Configuração: Adicione cada campo como uma estrofe com o parâmetro INDEXED=true da seguinte maneira.

```
[pod]
INDEXED=true[namespace]
INDEXED=true[container_name]
INDEXED=true[container_id]
INDEXED=true
```

Depois disso, o cabeçote de pesquisa precisa ser reiniciado e, com isso, novos eventos que chegarem poderão ser pesquisados com o sinal =.

Links relacionados

Respostas de Splunk

Por que eu preciso pesquisar metadados em um argumento de "campos" de um HEC com '::'?:
<https://answers.splunk.com/answers/635676/why-do-i-need-to-search-metadata-in-a-fields-argum.html>

Links Externos

Configurações de log do Kubernetes:

<https://github.com/splunk/splunk-connect-for-kubernetes/tree/develop/helm-chart/splunk-kubernetes-logging>

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.