

Impossibile cercare i campi con "="

Applicabilità

Splunk Enterprise Splunk Cloud

Descrizione

Versione splunk: 7.0.13

Quando si cerca una stringa in uno dei seguenti campi:

- baccello
- spazio dei nomi
- nome_contenitore
- id_contenitore

Analogamente a `container_id=add1`, non restituirà risultati.

Indagine

Dopo alcune ricerche è stato notato che i dati HEC su questa configurazione sono indicizzati senza alcun file di configurazione, ma per usarli correttamente è necessaria una certa configurazione. I campi possono infatti essere ricercati impostando con il `::` sign (specificatore dei campi di metadati), ma questo non risolve il problema relativo all'impossibilità di eseguire ricerche con il segno `=`.

Per eseguire questa operazione, è necessario eseguire ulteriori configurazioni durante la ricerca. Sembra che con gli input HEC per le reti kubernetes GCP gli eventi non siano del tutto preparati per essere rintracciabili. In particolare i campi sembrano non essere indicizzati, che fa parte dei dati grezzi ma non sono da specificare nella ricerca per ottenere eventi.

Risoluzione

Poiché gli eventi non ottengono i parametri di configurazione indicizzati, è necessario aggiungerli come segue:

Istanza: Testa di ricerca

File: `campi.conf`

Percorso: `$SPLUNK_HOME/etc/apps/search/local`

Impostazione: Aggiungere ogni campo come stanza con il parametro INDEXED=true come indicato di seguito.

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

Dopo questo, la testa di ricerca deve essere riavviata, e con questo, i nuovi eventi in arrivo saranno ricercabili con il segno =.

Collegamenti correlati

Risposte Splunk

Perché è necessario cercare i metadati in un argomento "campi" di un HEC con '::':

<https://answers.splunk.com/answers/635676/why-do-i-need-to-search-metadata-in-a-fields-argum.html>

Collegamenti esterni

Impostazioni registrazione Kubernetes:

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

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).