

La stanza del monitor non funziona come previsto.

Applicabilità

Splunk Enterprise

Descrizione

Quando si utilizza Splunk per monitorare i file senza modificare i nomi, ma il contenuto non funziona come previsto, ad esempio:

```
[monitor:///path/reports]
index = splunk_test
initCrcLength = 4096
ignoreOlderThan = 1d
disabled = 0
sourcetype = DiskUsage
```

Indagine

Splunk indica l'indicizzazione dei dati in base al contesto di timestamp nel file e non al momento in cui il file viene effettivamente generato, in quanto il file acquisisce le informazioni di data e ora in base ai dettagli host di quel particolare fuso orario.

Risoluzione

Impostare "DATETIME_CONFIG = CURRENT" nel file props.conf, poiché i nuovi log indicizzati avranno l'ora corrente nel timestamp, che è probabilmente l'ora in cui il file è stato creato, il server d'oltro controllerà il file e lo inoltrerà quasi immediatamente.

Esempio:

```
$SPLUNK_HOME/etc/system/local/props.conf
[source:../mylogs/*.log]
DATETIME_CONFIG = CURRENT
```

Collegamenti correlati

Documentazione relativa a Splunk

Configurazione estrazione timestamp:

https://docs.splunk.com/Documentation/Splunk/latest/Admin/Propsconf?utm_source=answers&utm_medium=question&utm_term=props.conf&utm_campaign=refdoc#Timestamp_extraction_configuration

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).