

ERROR: sendemail:1668 - El demonio Splunkd no responde

Aplicabilidad

Splunk Enterprise

Descripción

Las alertas se programan para cada hora con acciones de alerta a medida que se activan los correos electrónicos y las alertas, pero no se envían como correos electrónicos.

```
08-30-2024 14:39:11.596 +0800 INFO SavedSplunker - savedsearch_id="", search_type=<"">, search
```

Investigación

Tras la investigación, se observaron los siguientes errores en splunkd.log:

```
ERROR ScriptRunner [271749 AlertNotifierWorker-1] - stderr from '/opt/splunk/bin/python3.7 /opt
```

- Esto indica que hay una limitación en el envío de alertas como correos electrónicos con un mayor número de eventos. En este caso, exportó el resultado como un CSV en lugar de un correo electrónico para evitar este problema.

- Sin embargo, se observó que las alertas con menos número de eventos todavía no se activaban como correo electrónico.

- En /opt/splunk/var/log/splunk/python.log, el siguiente error es llenar :

ERROR sendemail:1668 - Splunkd daemon is not responding: ('Error connecting to /servicesNS/abcs

i	時間	事件
>	24/08/26 8:00:35.020	<pre>2024-08-26 08:00:35,020 +0800 ERROR sendemail:1668 - Splunkd daemon is not responding: ('Error connecting to /servicesNS/ds902320/ipm/saved/searches/%5BIP%5D%20K0%20Date%20Changed%20to%20Earlier%20Than%20Current%20Date: The read operation timed out',) Traceback (most recent call last): ... 23 lines omitted ... File "/opt/splunk/etc/apps/search/bin/sendemail.py", line 1661, in <module> results = sendEmail(results, settings, keywords, argvals) File "/opt/splunk/etc/apps/search/bin/sendemail.py", line 243, in sendEmail 顯示全部 32 行 date_minute = 0 host = [REDACTED] index = _internal linecount = 34 source = /opt/splunk/var/log/splunk/python.log sourcetype = splunk_python splunk_server = [REDACTED]</pre>

Resolución

Este mensaje de error indica un problema de tiempo de espera.

Para resolver el problema, siga estos pasos:

i. Vaya a \$SPLUNK_HOME/etc/system/local/web.conf

ii. Aumentar el valor del tiempo de espera

```
splunkdConnectionTimeout = <integer> (default=30)
```

- * The amount of time, in seconds, to wait before timing out when communicating with splunkd.
- * Must be at least 30.
- * Values smaller than 30 will be ignored, resulting in the use of the default value
- * Default: 30

Después de aumentar el valor del tiempo de espera, los correos electrónicos se activan como se esperaba.

Enlaces relacionados

[web.conf](#)

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).