

ERROR: No se pueden agregar pares de búsqueda: reinicio de conexión por peer

Aplicabilidad

Splunk Enterprise

Descripción

Al intentar agregar nuevos indizadores así como nuevos encabezados de búsqueda en el entorno, los indizadores forman parte del clúster pero los encabezados de búsqueda no se configuran como un clúster.

Otros indizadores ya están establecidos como pares para los encabezados de búsqueda en las preguntas, pero los encabezados de búsqueda tienen otros indizadores como pares de búsqueda.

Investigación

- Compruebe que la configuración de SSL es correcta y que no hay problemas relacionados con la conectividad.
- Los errores en splunkd.log muestran: No se pudo establecer la conexión SSL; el par restableció la conexión para la dirección IP del indizador.
- La configuración manual mediante los archivos de configuración y la instalación de la GUI no funciona del mismo modo.
- Confirme que https se utiliza para el URI de los indizadores, ya que SSL está en uso.
- Confirme que los indizadores en cuestión estén configurados en modo clúster.
- Los encabezados de búsqueda no están agrupados

Resolución

Como los indizadores están agrupados, el encabezado de búsqueda debe tener el modo de encabezado de búsqueda habilitado en server.conf; de lo contrario, el clúster de indizadores no reconocerá la instancia correctamente y rechazará la solicitud de peer.

Tenga en cuenta que el jefe de búsqueda necesita una estrofa de agrupamiento, aunque los jefes

de búsqueda no están agrupados.

1. Configure el archivo server.conf de la siguiente manera

```
[clustering]
master_uri = https://x.x.x.x:xxxx (https://x.x.x.xxxxx)
mode = searchhead
pass4SymmKey= yourPass4SymmKey
```

master_uri = el URI principal del clúster para el clúster ****Indexers****, los encabezados de búsqueda se distribuyen no en clúster para este caso.

mode = es necesario para establecer el servidor en modo de encabezado de búsqueda para la comunicación de clúster

pass4SymmKey = clave para el clúster, los usuarios deben agregar su propia clave para dicho atributo

2. Reinicie el servicio e intente volver a agregar los pares de búsqueda, el proceso debe ser exitoso.

Enlaces relacionados

Documentación de Splunk

Agregar pares de búsqueda al encabezado de búsqueda:

<https://docs.splunk.com/Documentation/Splunk/7.3.0/DistSearch/Configuredistributedsearch>

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).