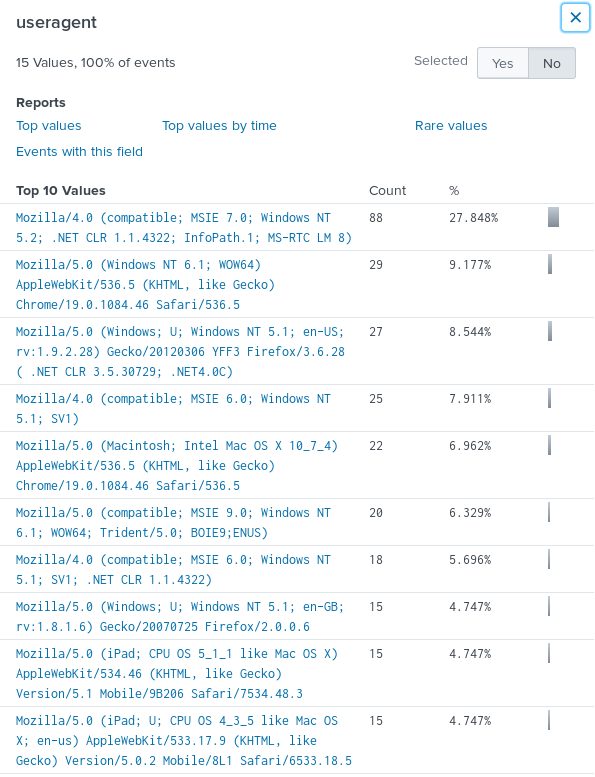
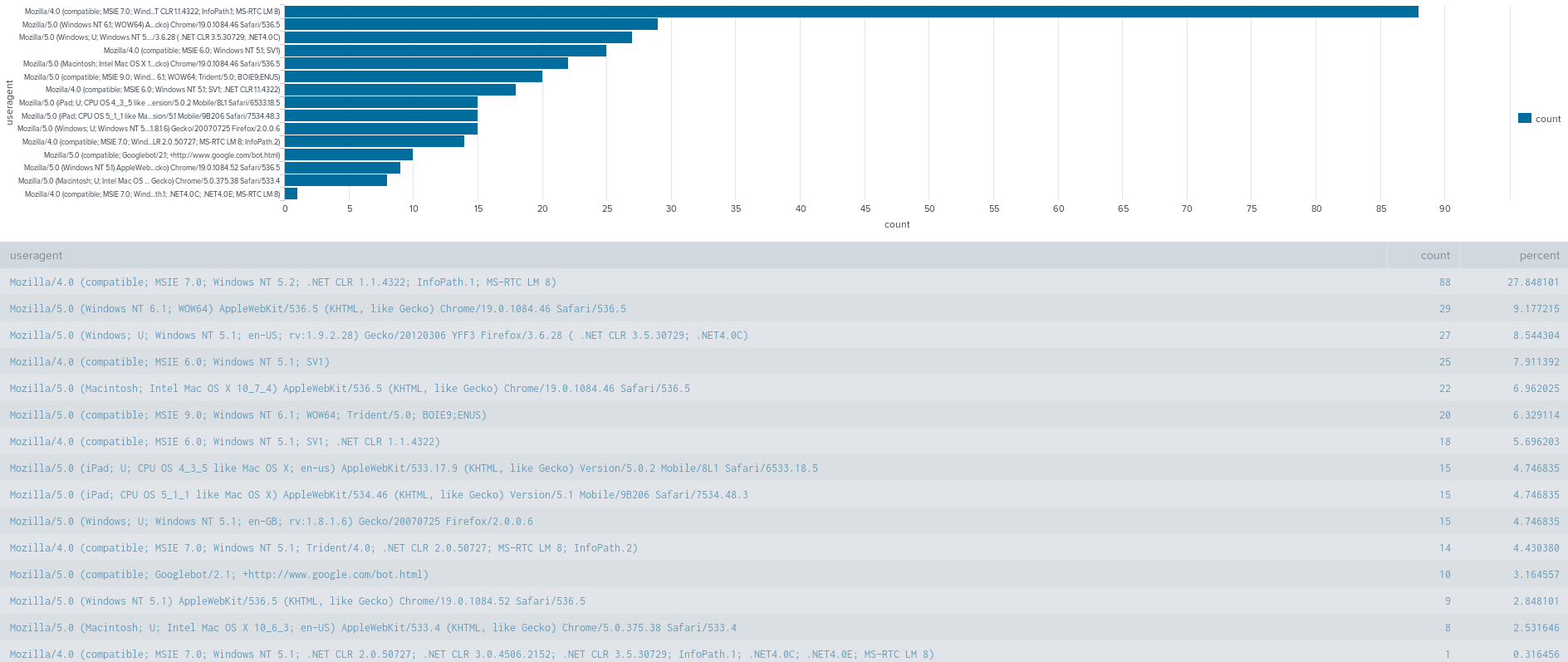
**TALLER 4**

1. Instalar splunk en la máquina virtual
2. Hacer tutorial: buscar los navegadores utilizados por la dirección 74.53.23.135

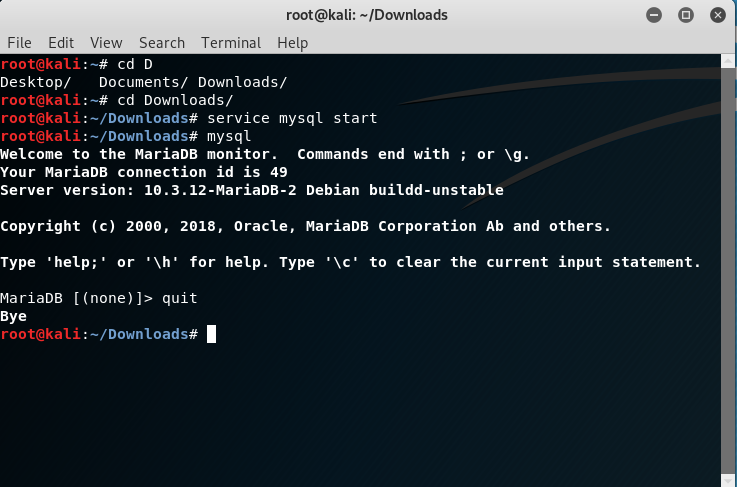


Se filtra por el top 20

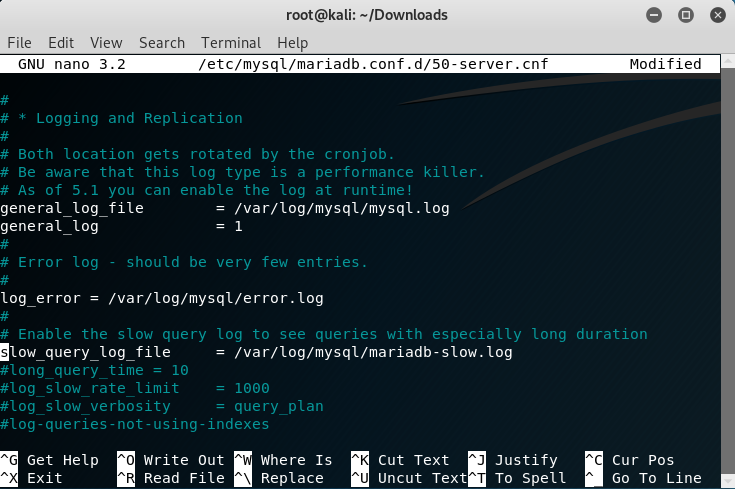


1. Configure la BD MySQL en la máquina virtual.

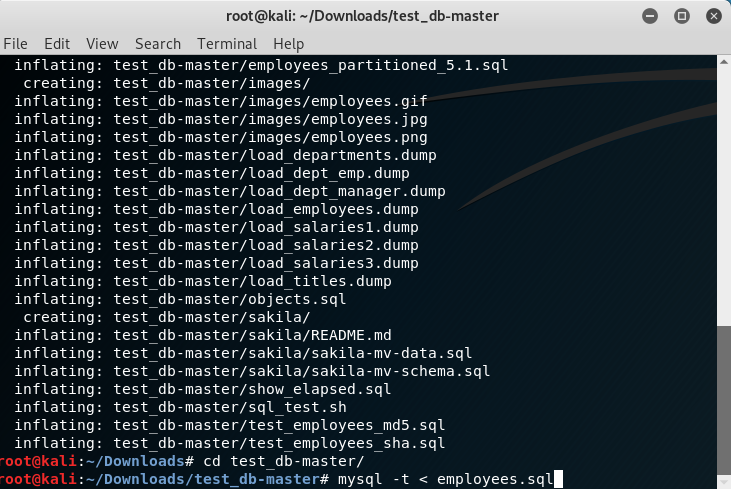
Ya que la base de datos se encuentra instalada dentro de Kali Linux, se procede a iniciar el servicio y probar la correcta conexión.



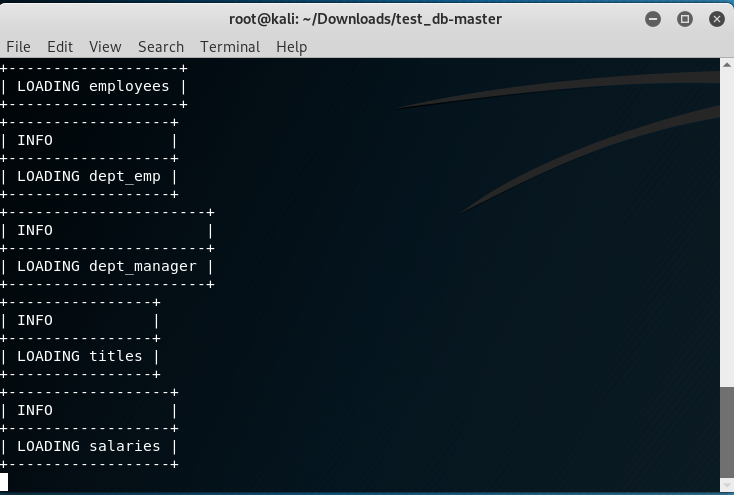
Editamos el archivo /etc/mysql/mariad.conf.d/50-server.cnf para habilitar los logs de errores y el de slow\_query quitando los comentarios para que el SIEM los registre.



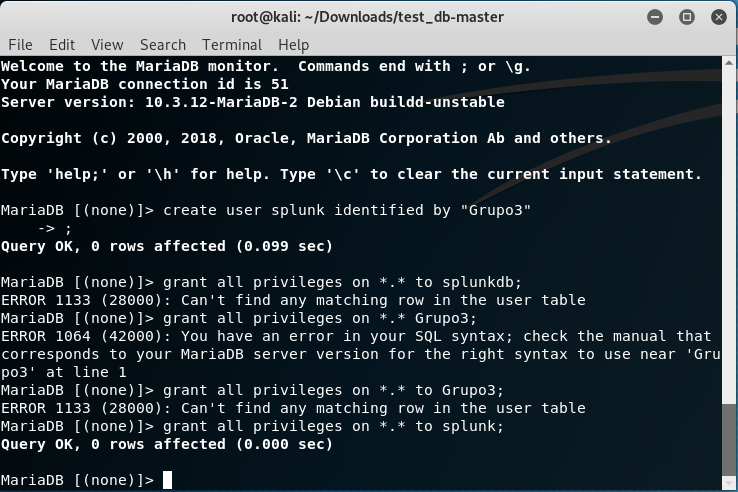
Se carga la base empleados en el motor de Base de datos MySQL.



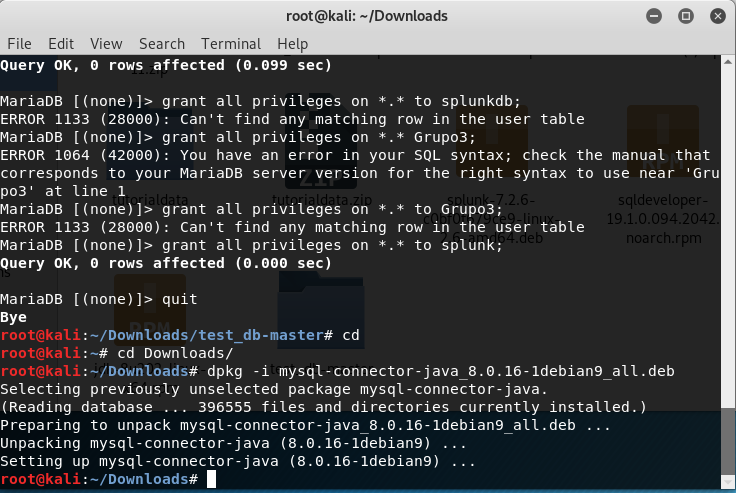
Progreso de la carga de las tablas a la base de datos del motor.



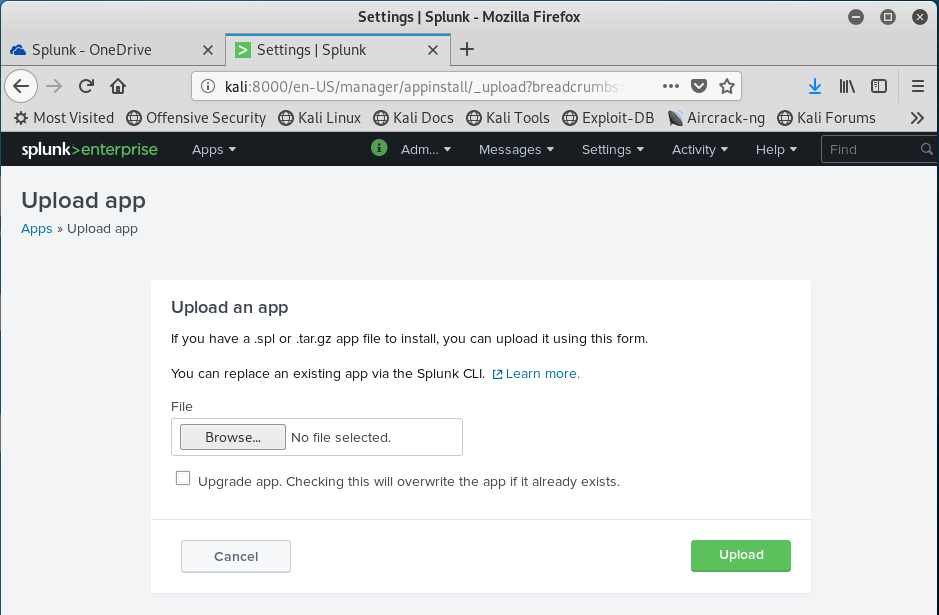
Se proveen todos los privilegios al usuario que se va a conectar desde SPLUNK.



Descomprimimos el conector que va a usar SPLUNK para la conexión con el motor de base de datos de MySQL, previamente descargado de la página del fabriacante.



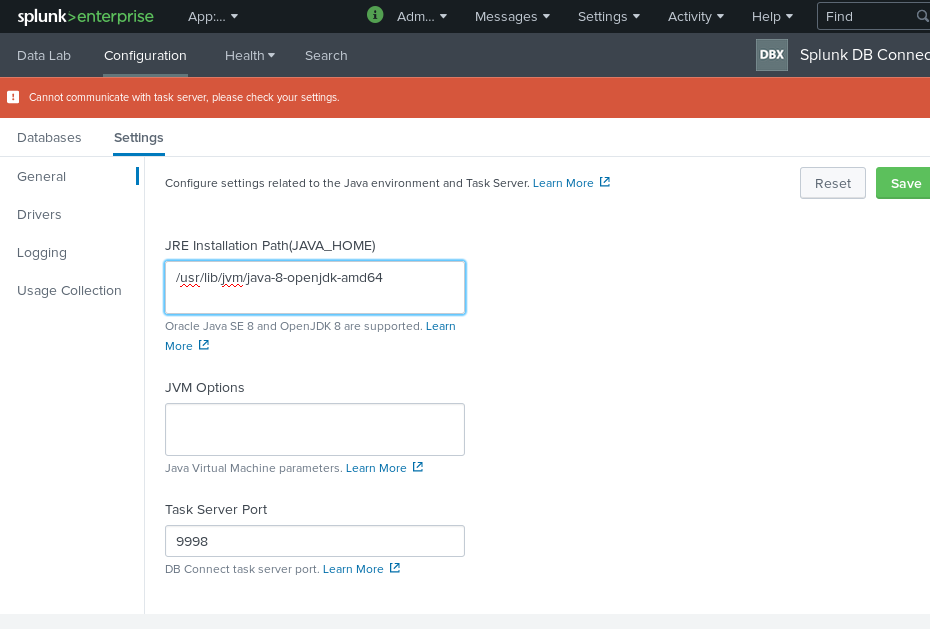
Cargamos la aplicación.



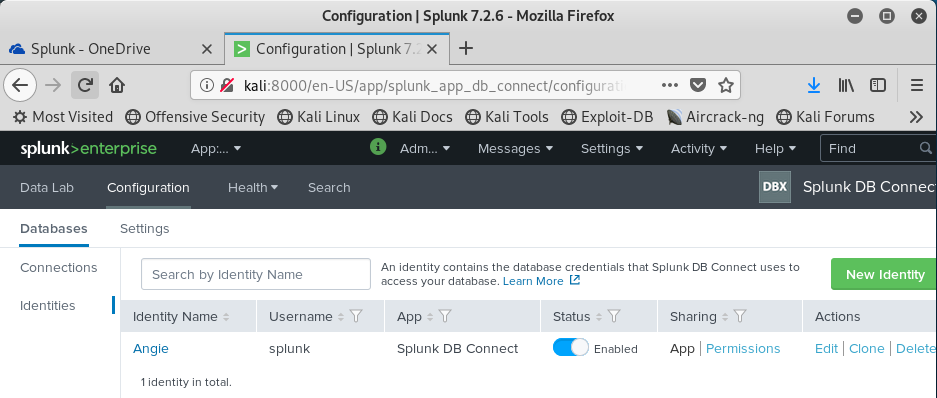
Copiamos el conector previamente descargado y descomprimido a la carpeta de drivers de SPLUNK.



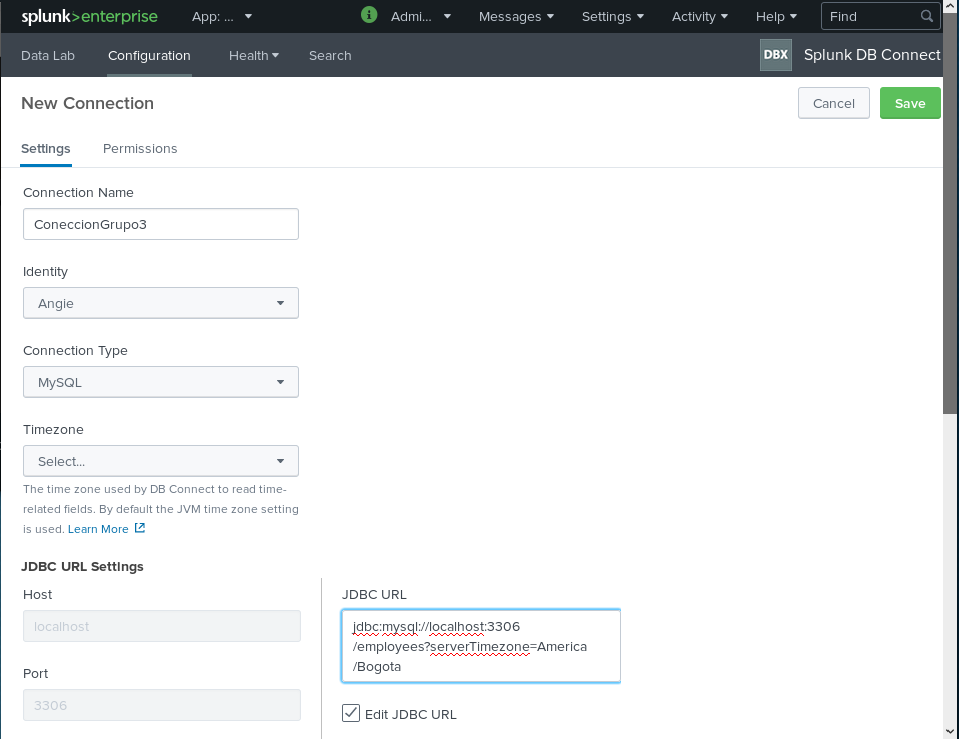
Hacemos la configuración del SDK de Java.



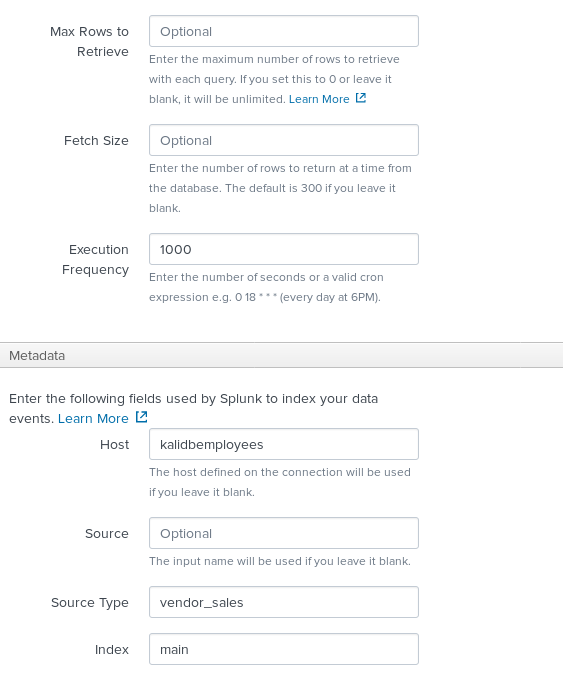
Vemos que el conector a la base de datos se ha configurado correctamente.



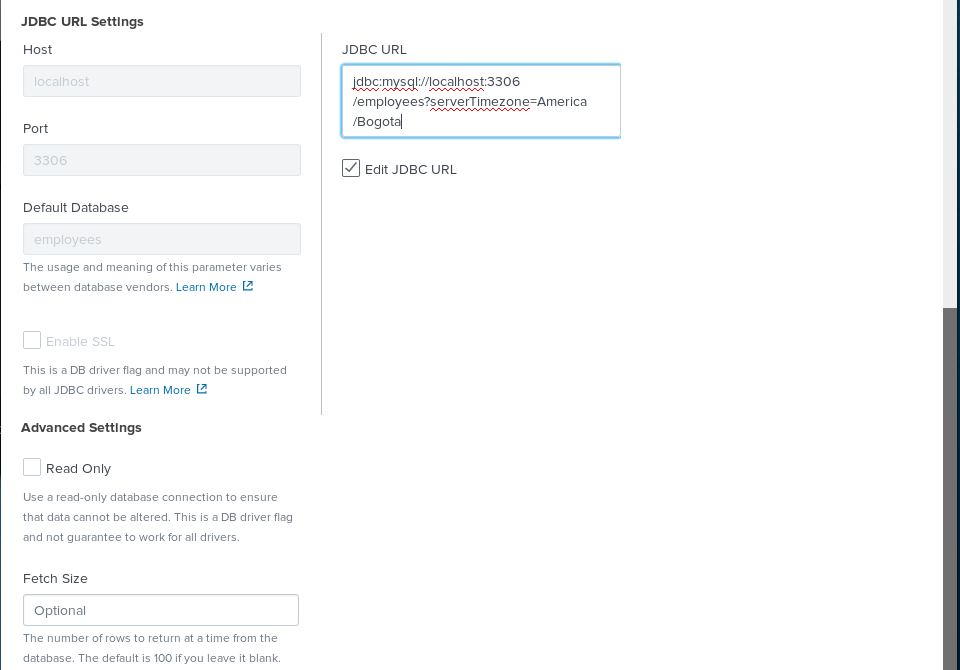
Creamos una nueva conexión en el SPLUNK.



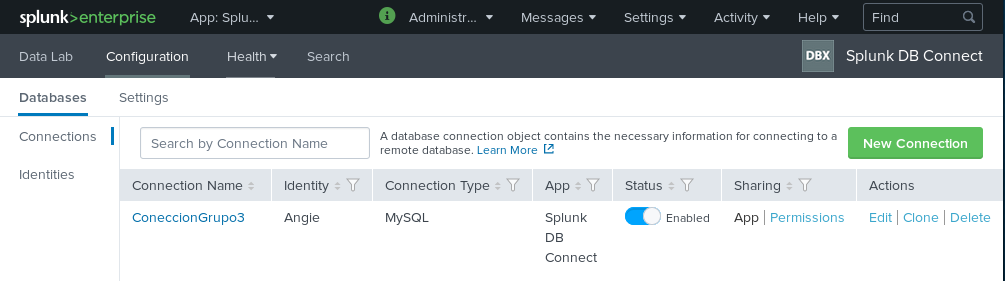
Se agregan los datos de configuración.



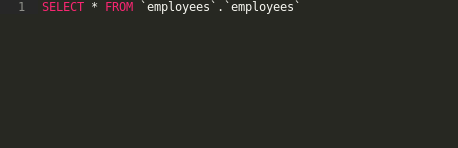
Terminamos con la configuración.



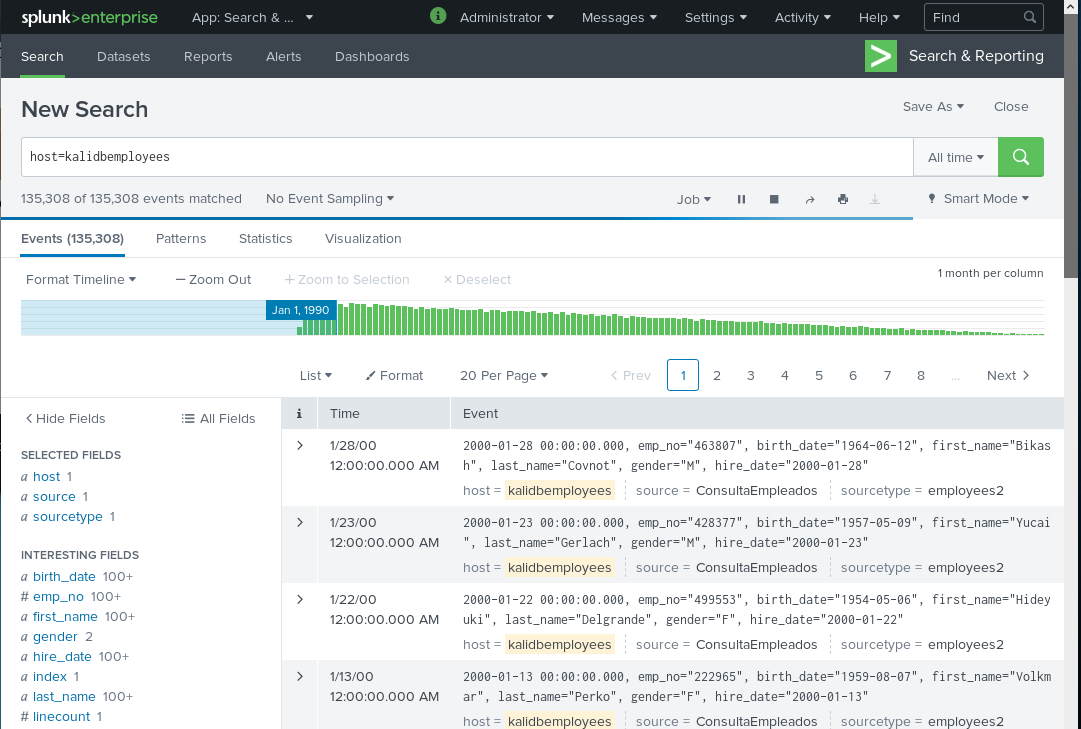
La conexión se ha creado correctamente.



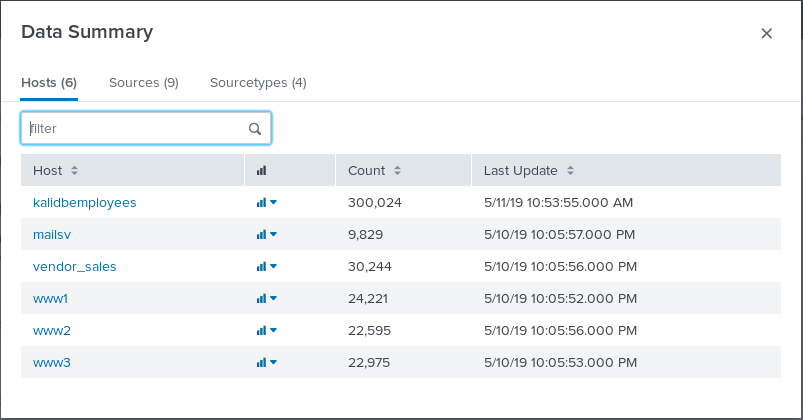
Escribimos la búsqueda que queremos evaluar.



Sobre SPLUNK, ejecutamos una nueva búsqueda para probar el correcto funcionamiento.



Revisamos las pestañas de Data Summary para ver qué datos nos aparecen.



1. Seleccione 2 riesgos que considere críticos detectarlos y que se puedan detectar en un SIEM.
2. Configure splunk para detectar esos 2 riesgos.
3. Pruebe que splunk puede detectar esos 2 riesgos.
4. Cree un repositorio en GitHub para colocar todas las evidencias y resultados del taller.