**CONSTRUYENDO INTELIGENCIA OPERACIONAL**

**BOOTCAMP**

ACTIVIDAD No. 11

Inteligencia artificial en SPLUNK

Objetivo: Que el equipo pruebe aprenda a fijar alarmas una vez que se encuentren condiciones no deseadas en el comportamiento de la variable observada.

Marco Teórico: Para determinar datos fuera de lo esperado (outliers), se fijan umbrales de alarma que pueden determinarse por múltiplos de la desviación estandar. (Por ejemplo 2sigma). Herramientas como splunk permiten al determinar la condición no esperada generar alertas para los responsables de solucionar la situación.

Parte 1: Carga y creación de alerta

Prerrequisitos:

Dataset de prueba.

Apuntar el navegador a:

<https://prd-p-4hqzy.splunkcloud.com/en-GB/>

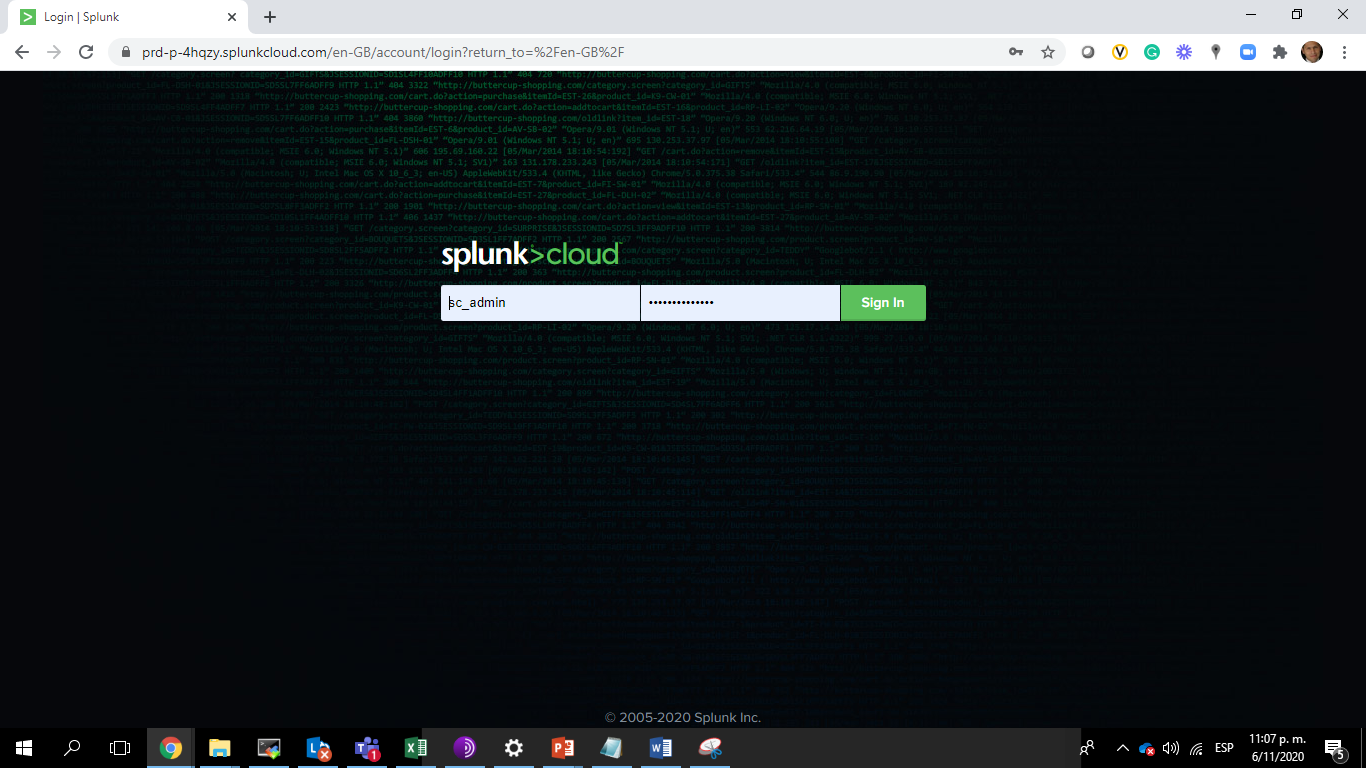


Conectarse con el usuario:

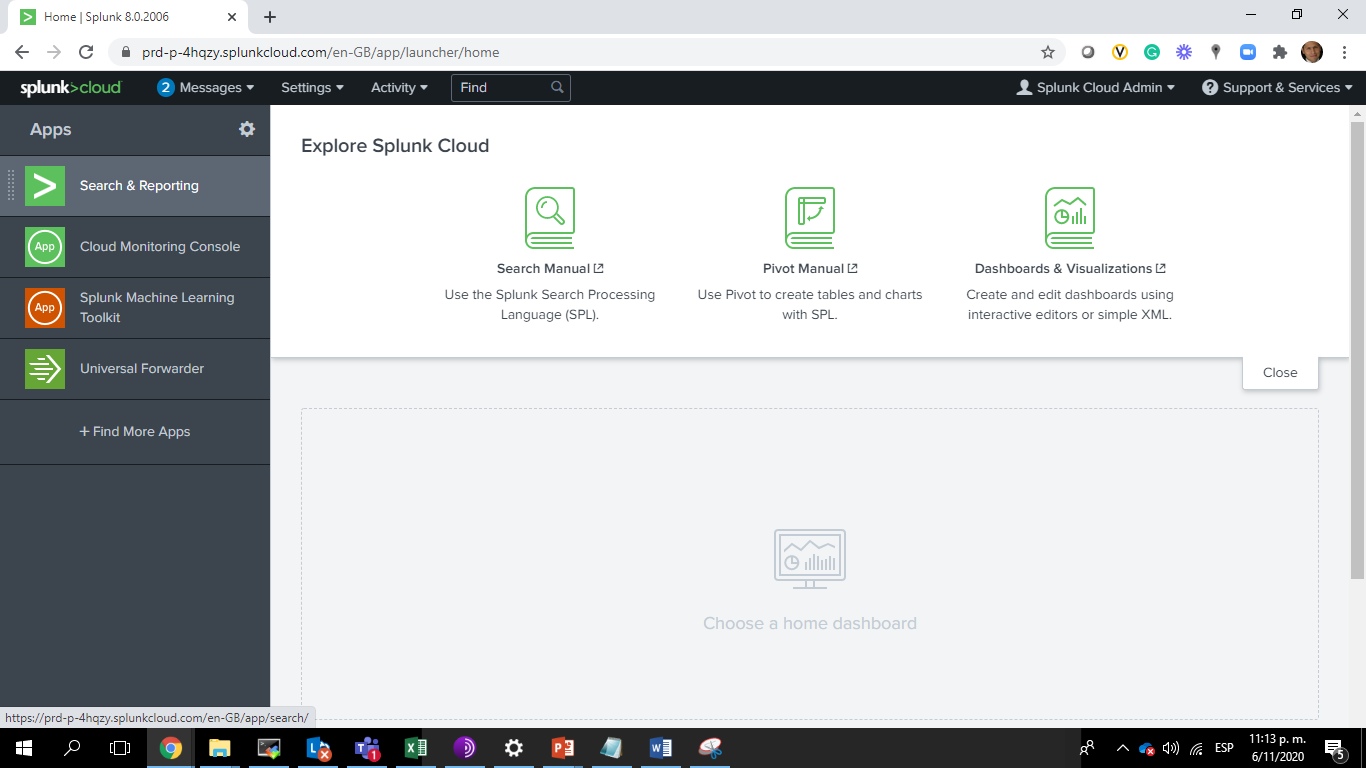
Sc\_admin

y la clave:

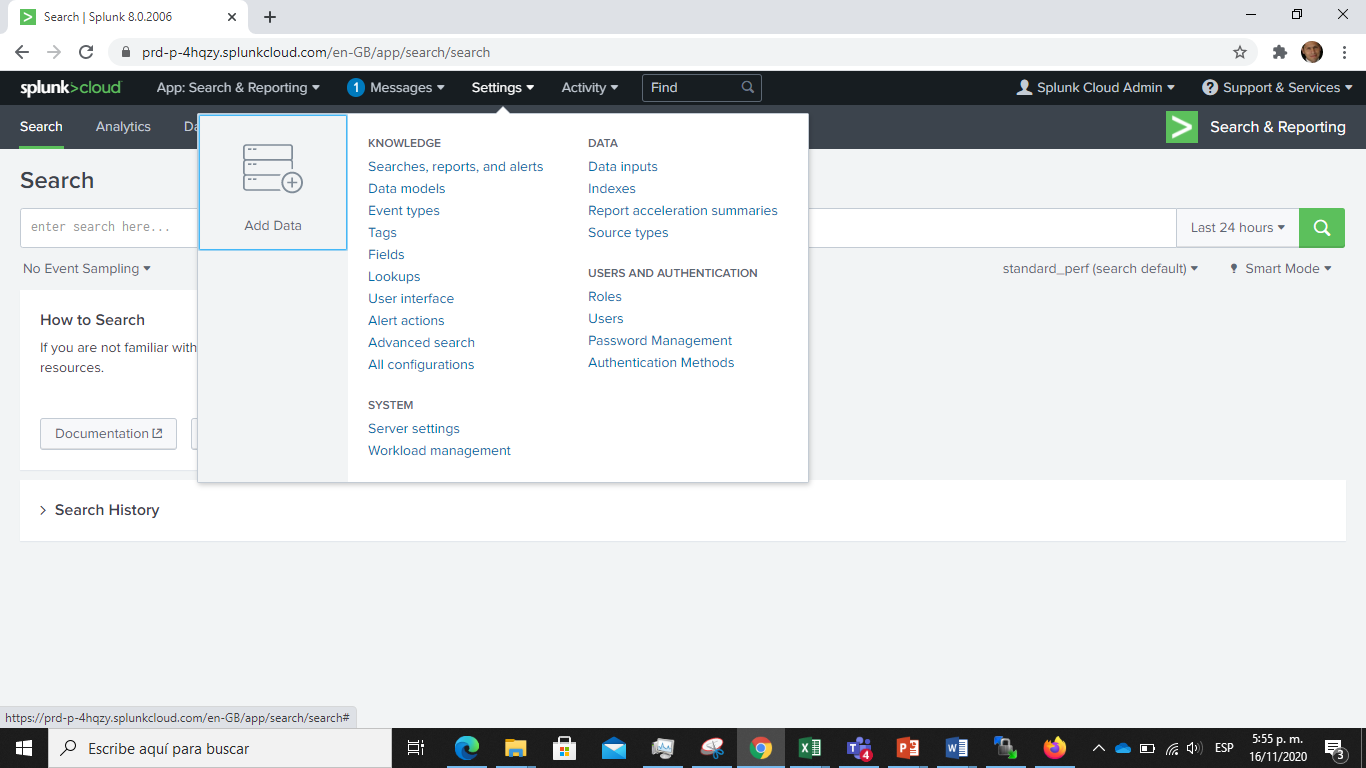
Inteligencia1#



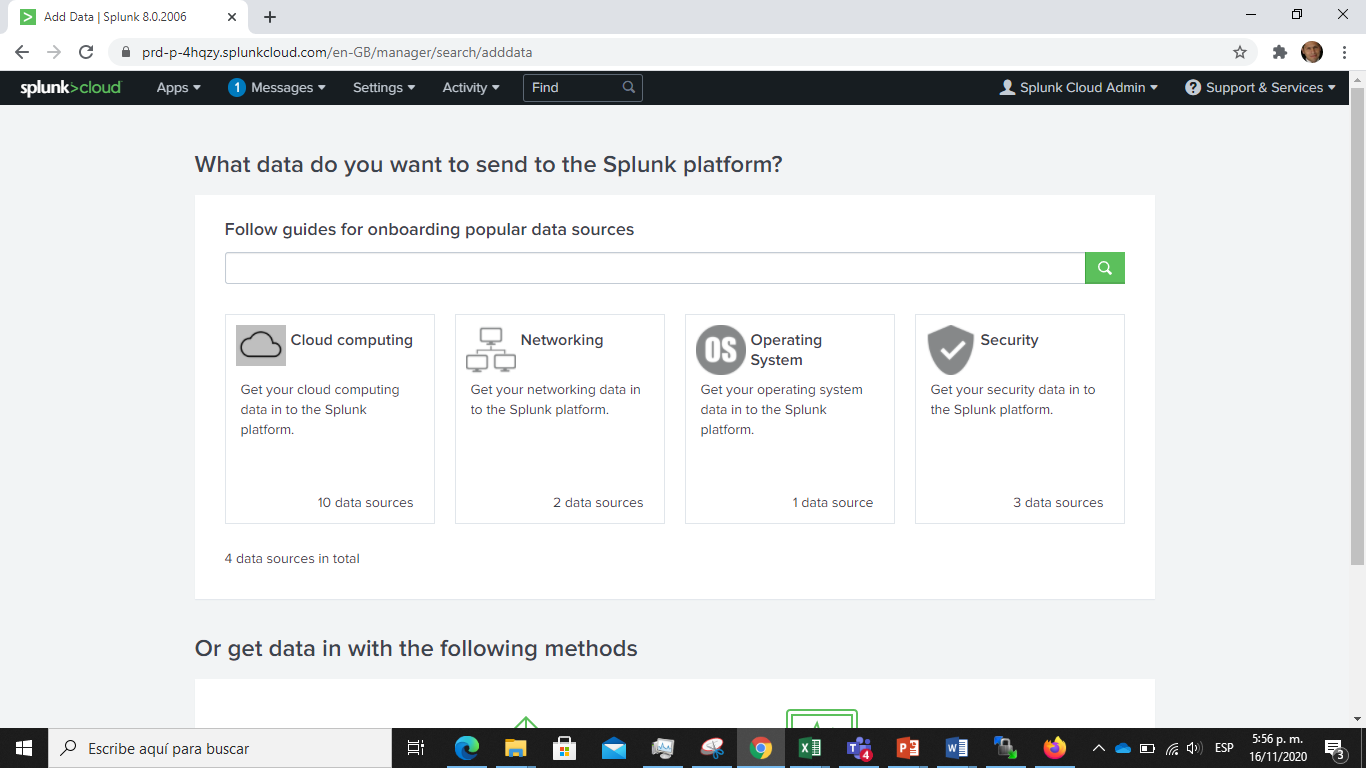
Debe observar la pantalla de bienvenida. Ahora oprimir “Search & Reporting”

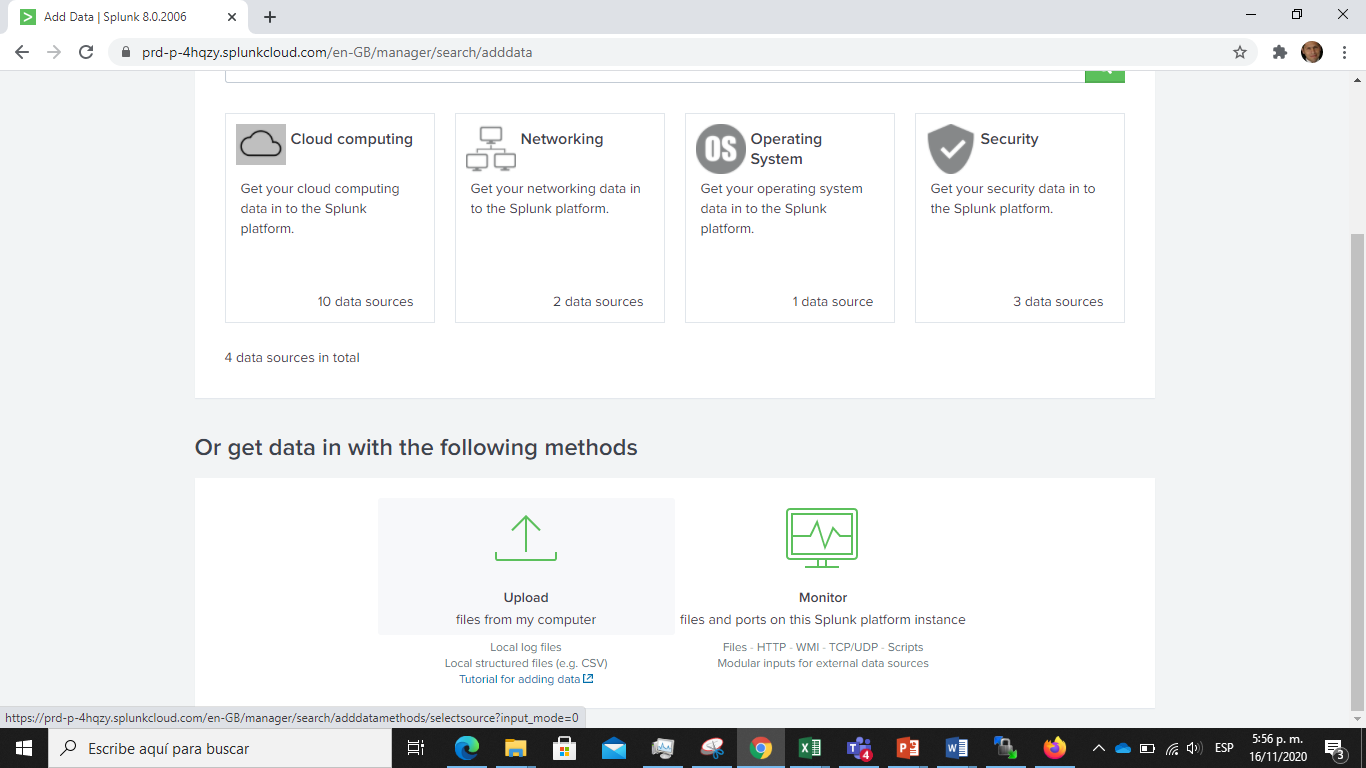


Escoger “Settings” (Configuracion) y luego “Add Data” (adicionar data)

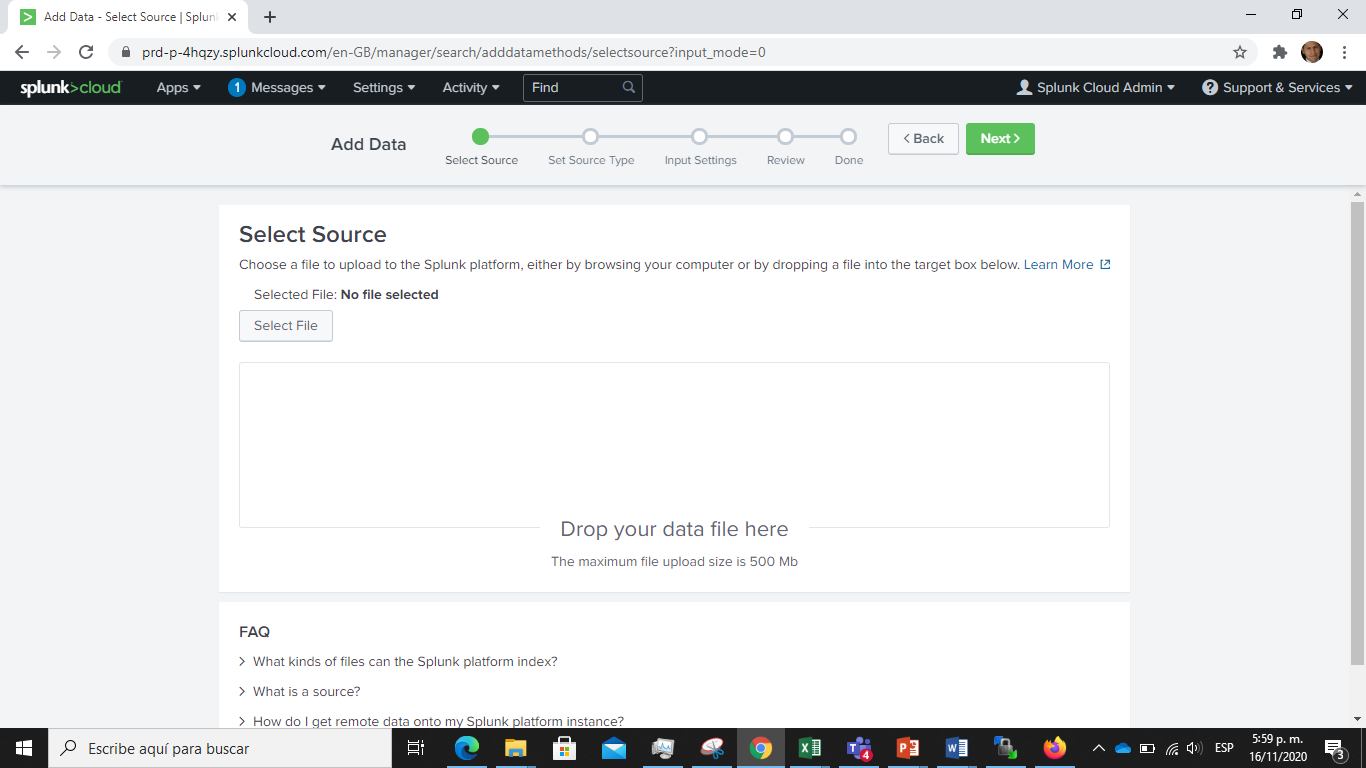


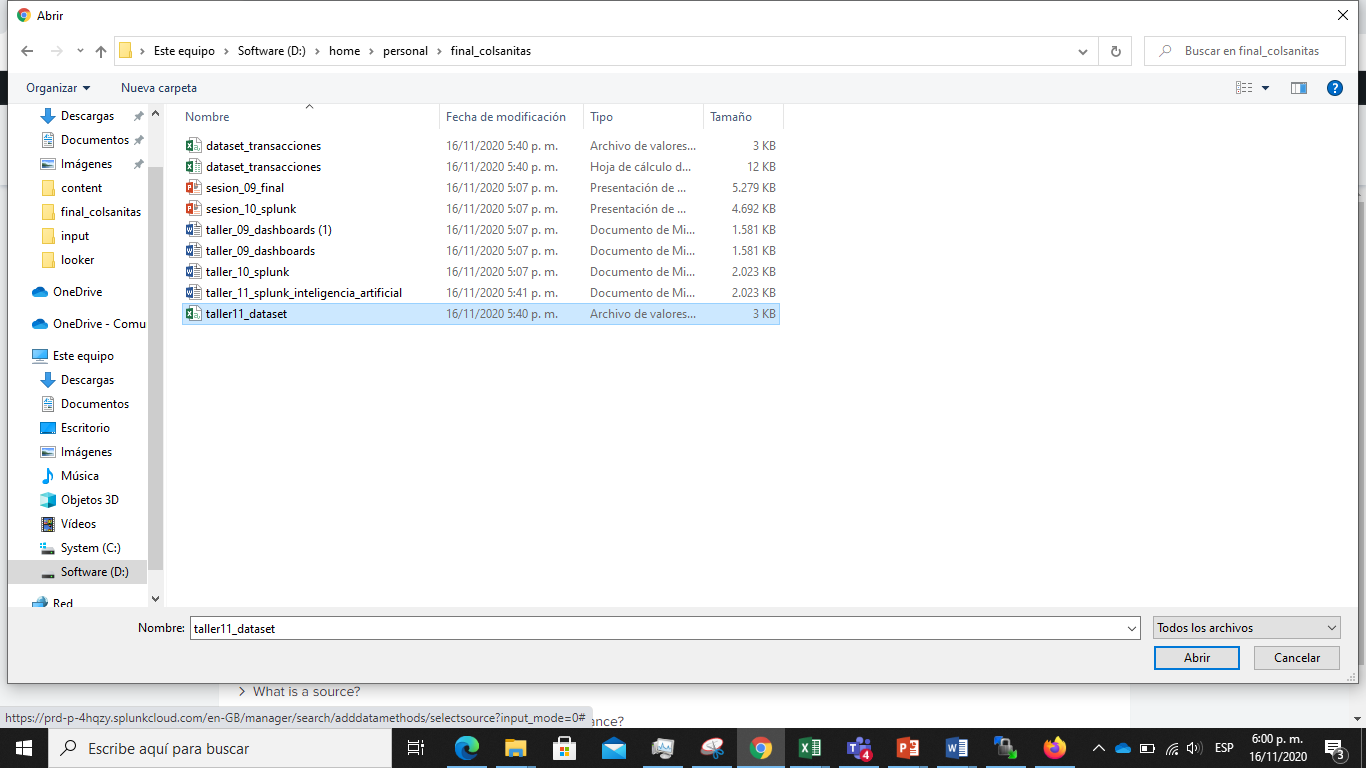
Hacer scroll hacia abajo hasta donde dice “Upload” (Carga)



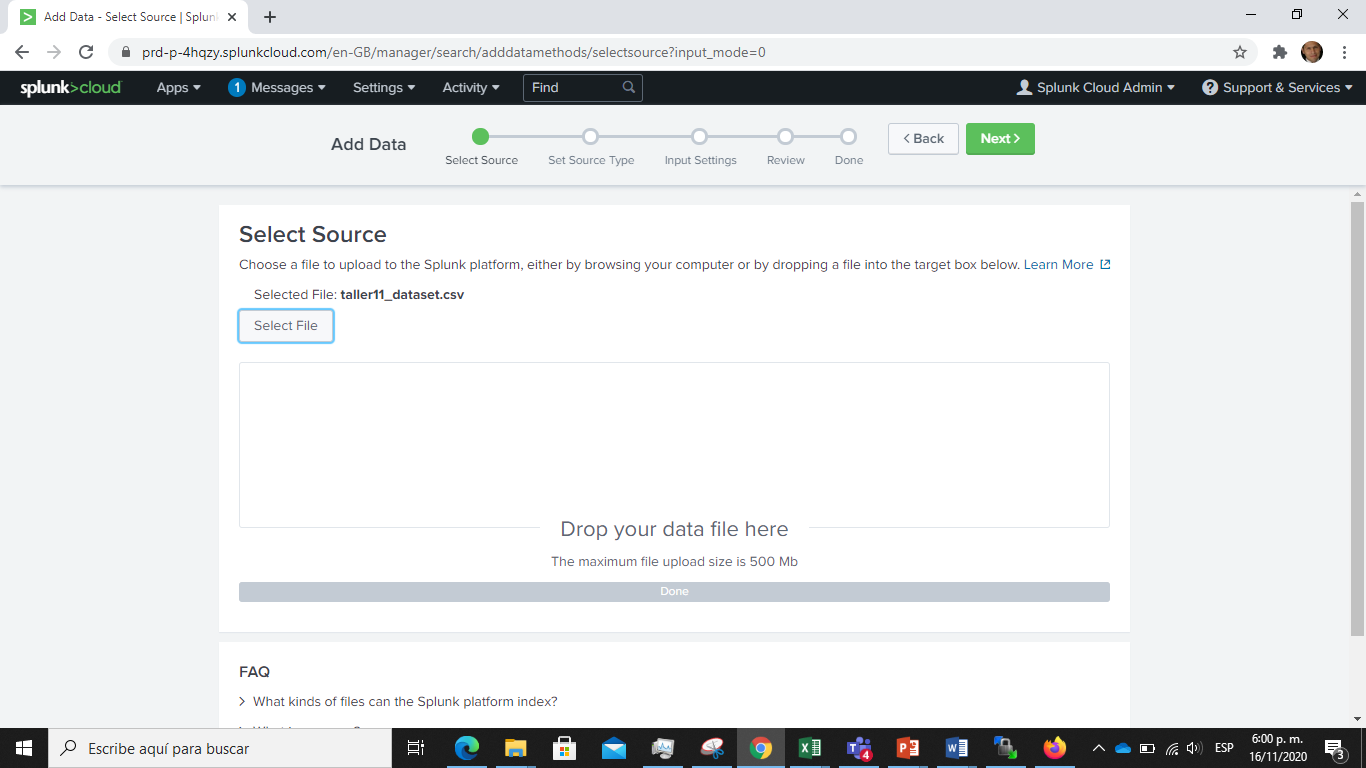


Oprimir “Upload”, luego “Select File” (Seleccionar archivo)





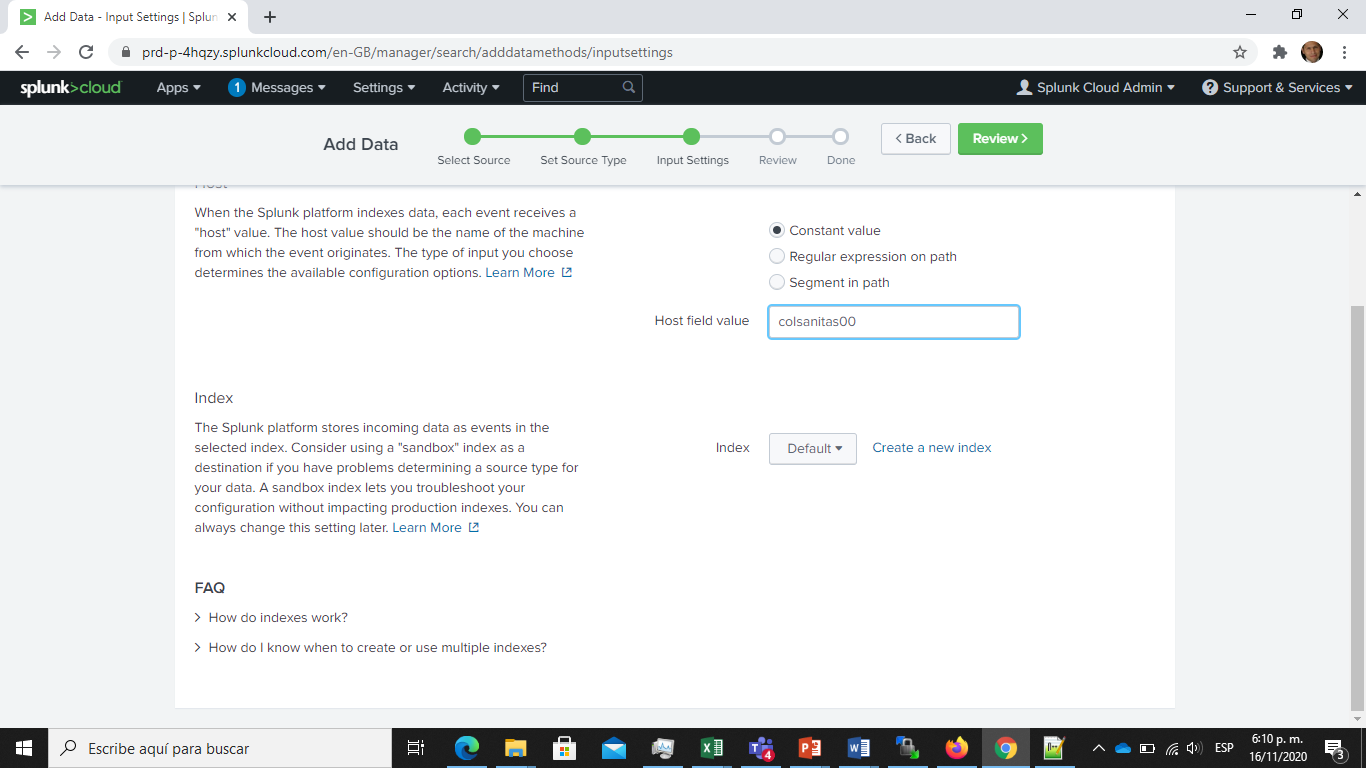
Esperar a que se cargue y aparezca “Done”



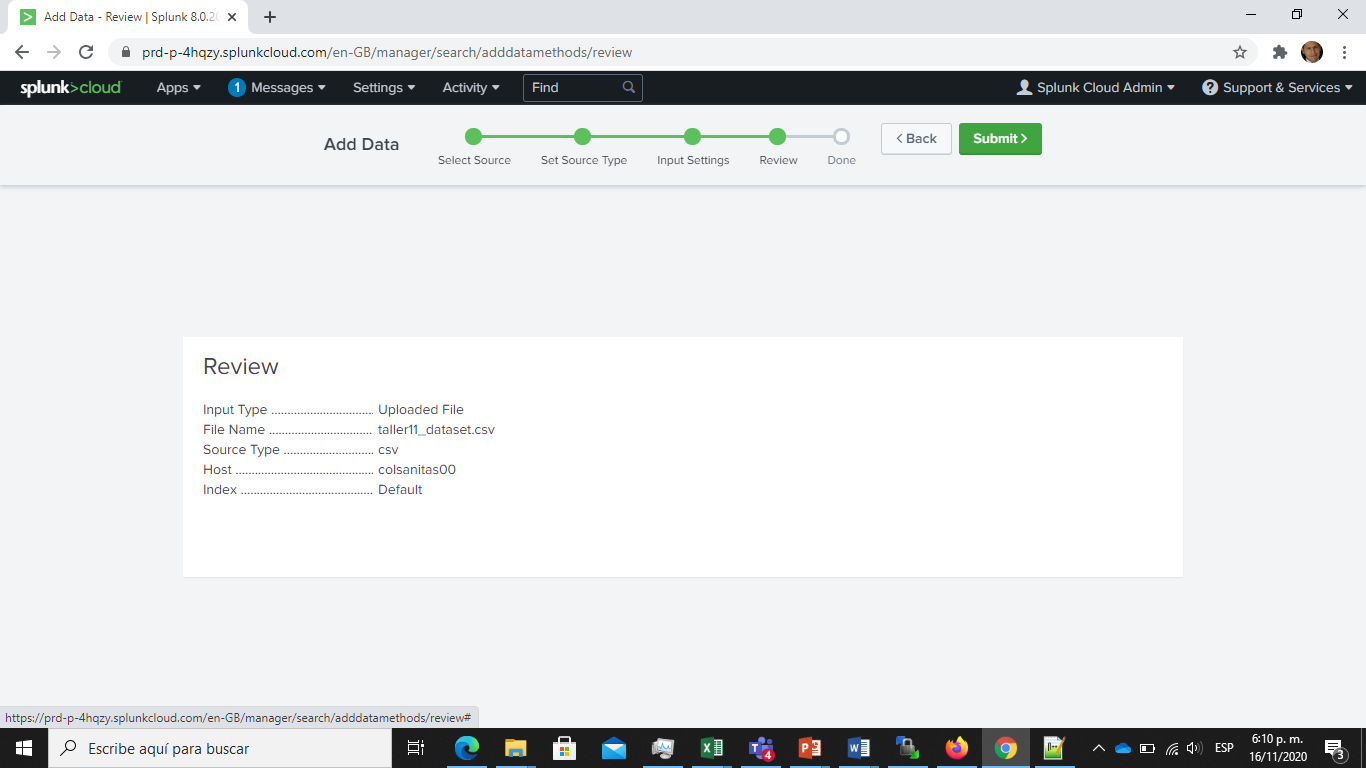
Oprimir “Next” (Siguiente): Notemos que se diferencian las dos columnas, fecha y transacciones



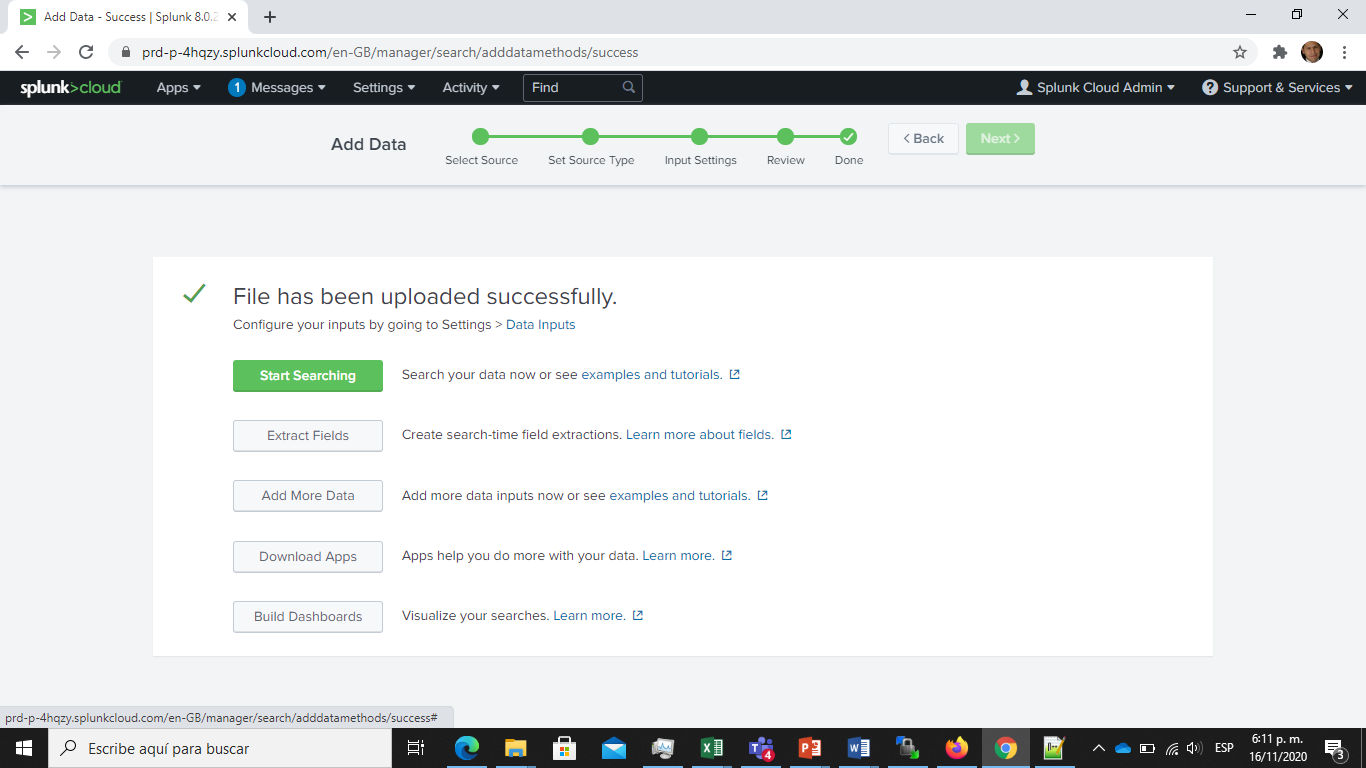
Oprimir “Next” (siguiente), en el campo host (Servidor), colocar “colsanitasXX” donde XX es el número asignado y luego oprimir “Review” (Revisar)



Revisar que se presente la pantalla y luego oprimir “Submit” (Enviar):



Debe presentarse la siguiente pantalla, allí oprimir “Start Searching” (Iniciar la búsqueda):

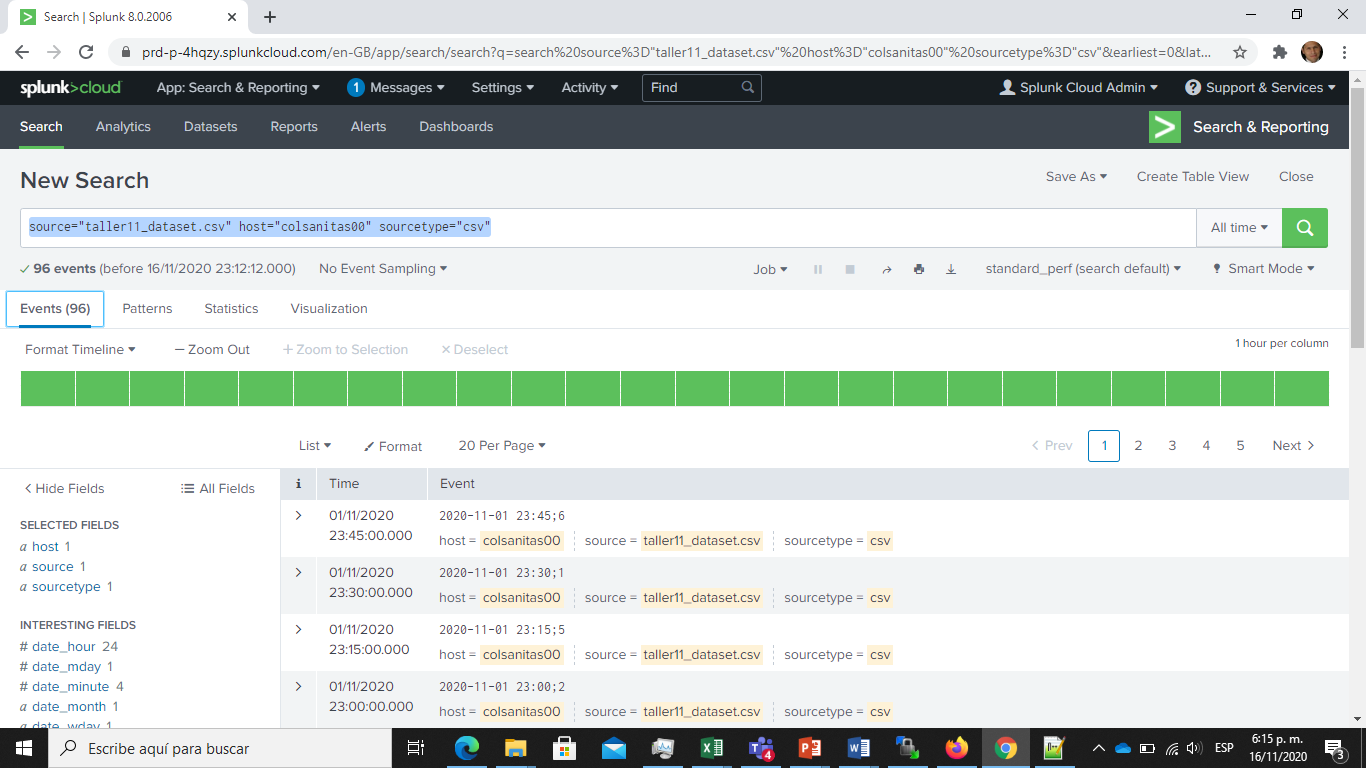


Note que la cadena de busqueda es:

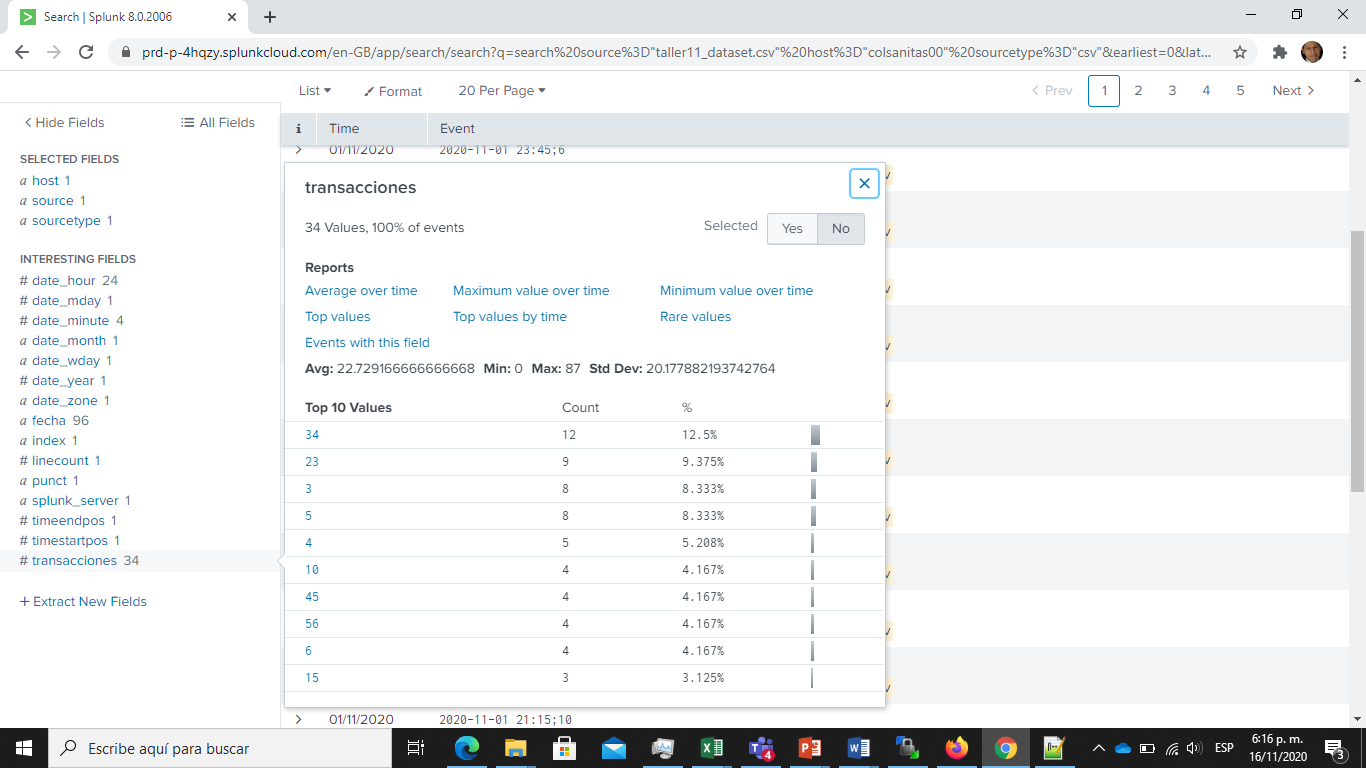
source="taller11\_dataset.csv" host="colsanitas00" sourcetype="csv"

Lo que quiere decir: se están consultando los datos del archivo “taller11\_dataset.csv”, el host “colsanitas00” y el tipo de archivo “csv”

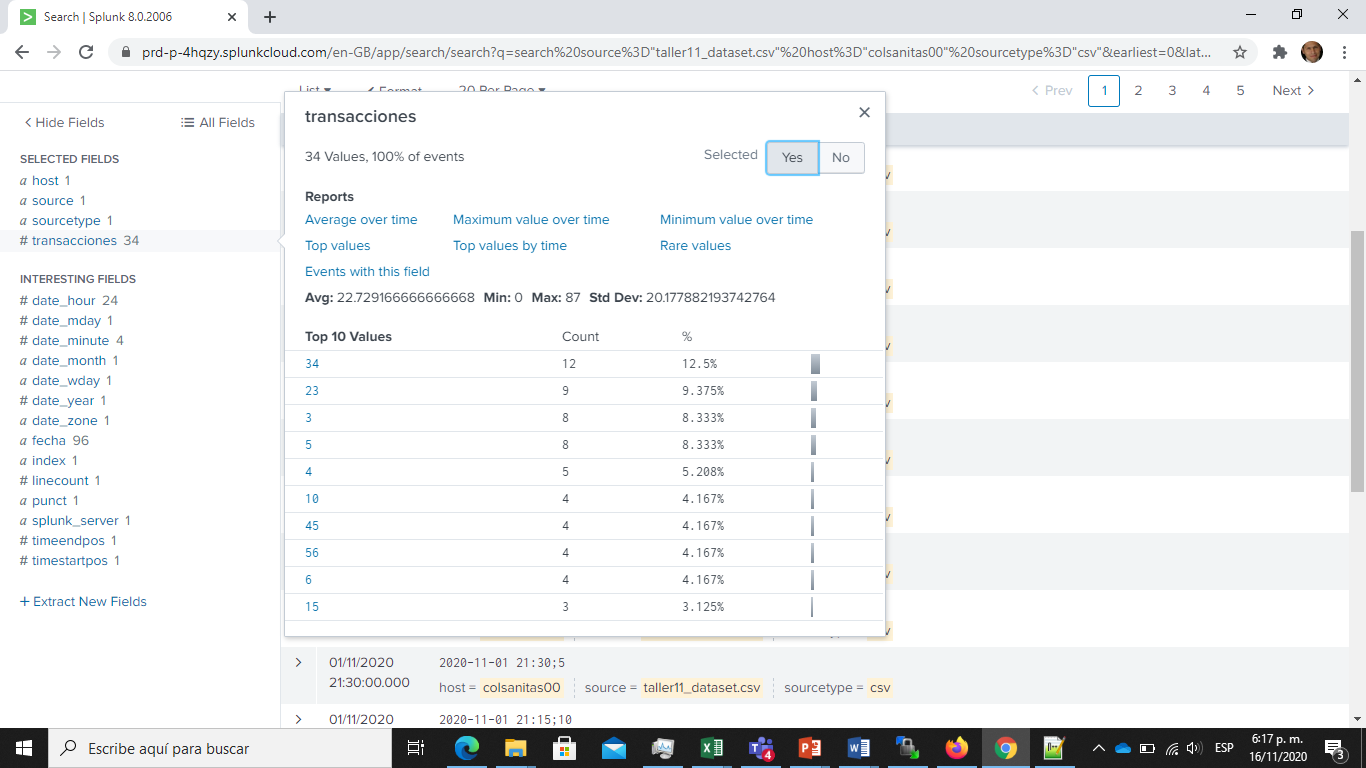
Debe presentarse una pantalla así:



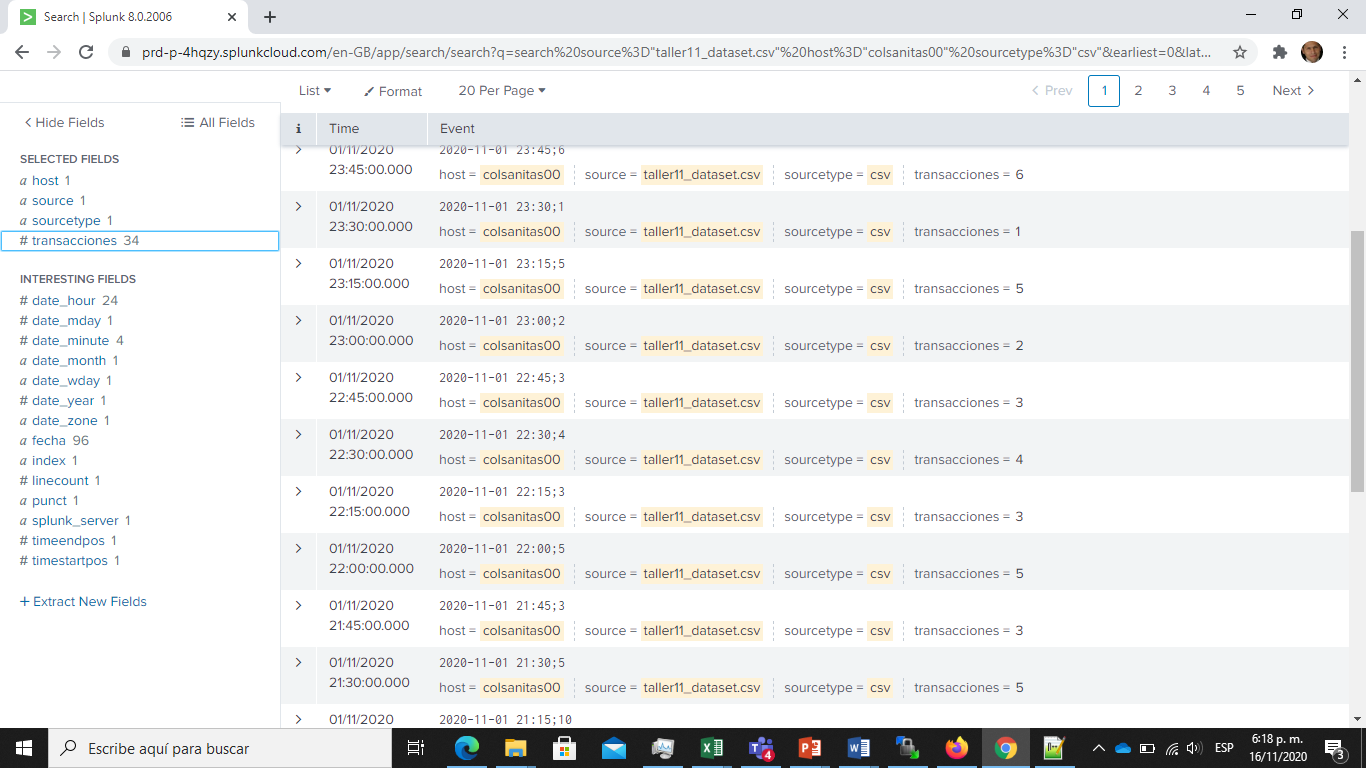
En esta pantalla, a la izquierda, se busca “Transacciones” y se hace click sobre ella, se debe presentar una caja de diálogo. En esta se busca el botón Selected (seleccionado) y se coloca en “Yes”.



Debe quedar así, una vez logrado se cierra este diálogo oprimiendo la “x”:



En el area izquierda se deben mostrar los campos host, source, sourcetype, transacciones como seleccionados



Completar la expresión de búsqueda así:

source="taller11\_dataset.csv" host="colsanitas00" sourcetype="csv" | timechart avg(transacciones) span=15m

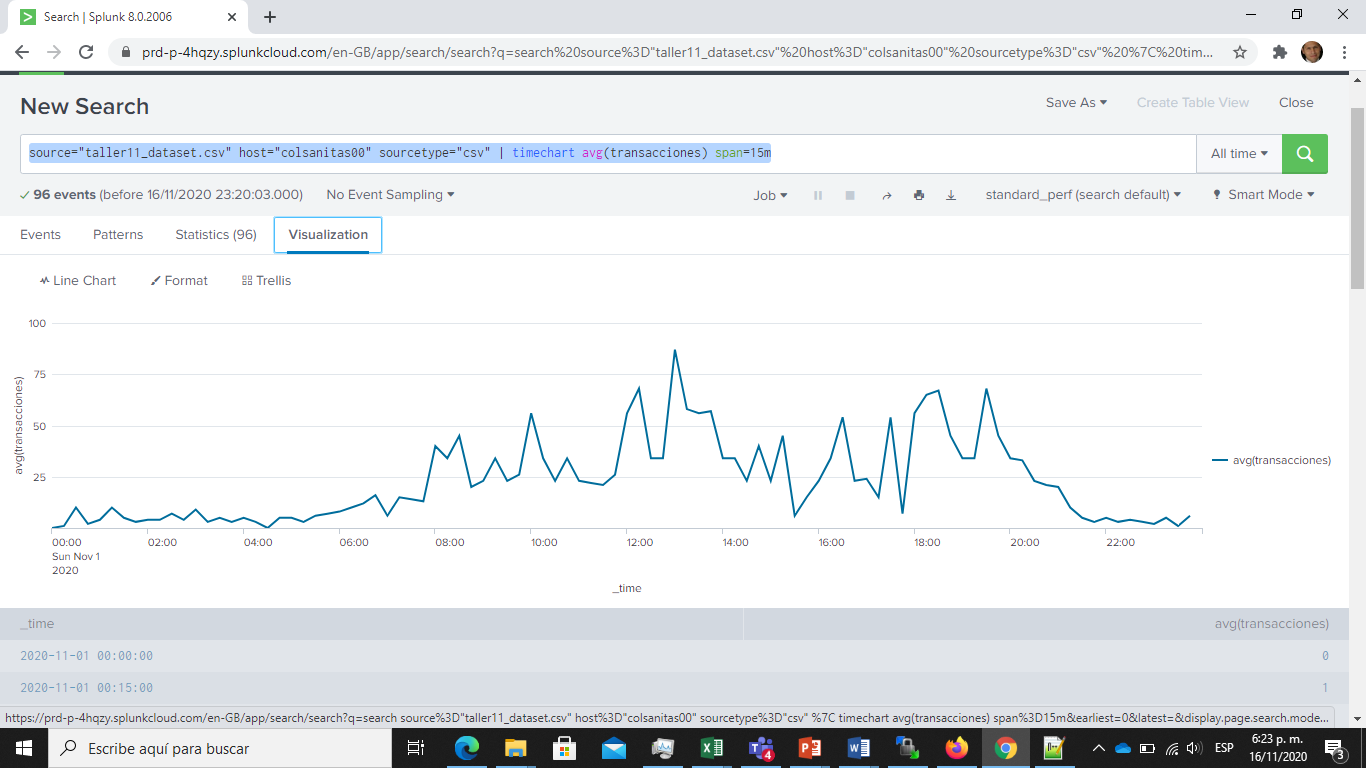
Lo que indica:

Timechart (construir un gráfico que tenga como eje X el tiempo de la observación y en el eje Y el promedio de las transacciones cada 15 minutos.

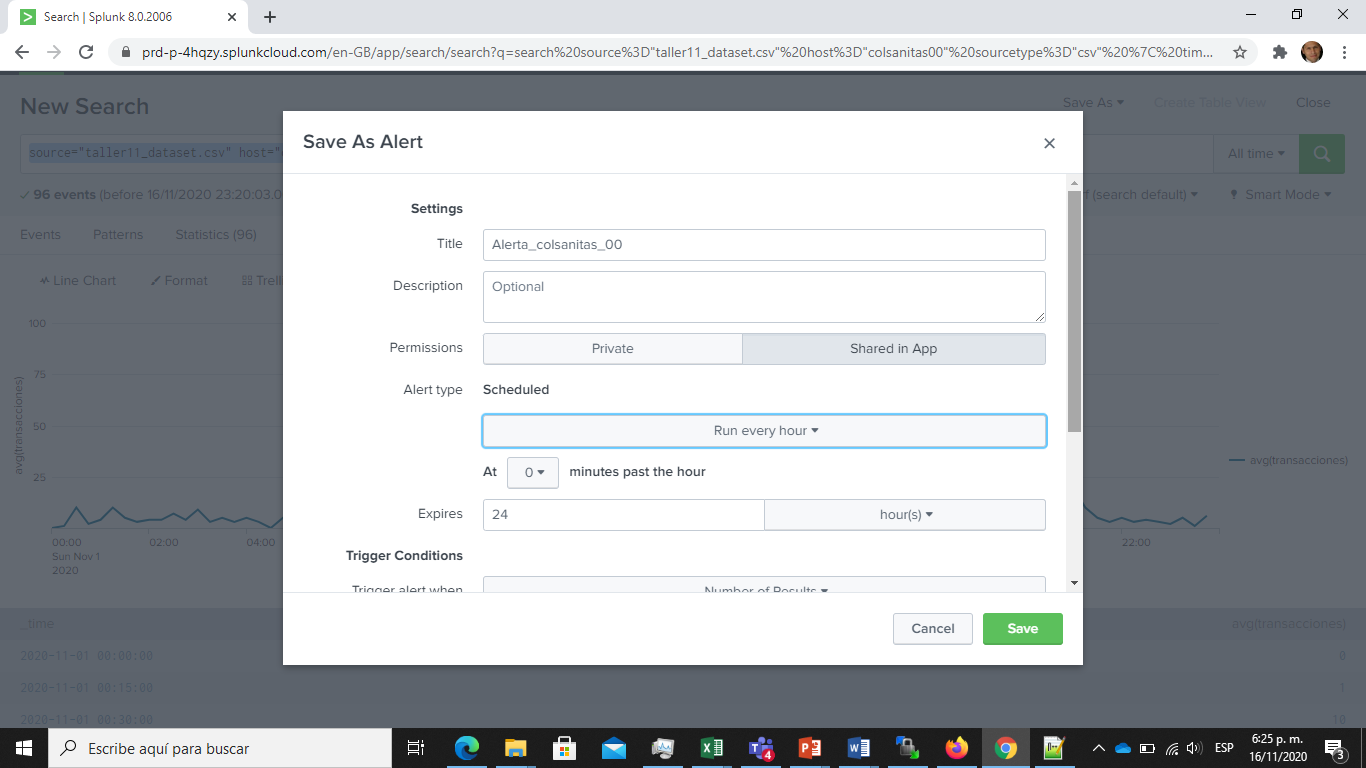
Luego se oprime la “lupa” para ejecutar la búsqueda, esto nos debe dar unas estadísticas así:



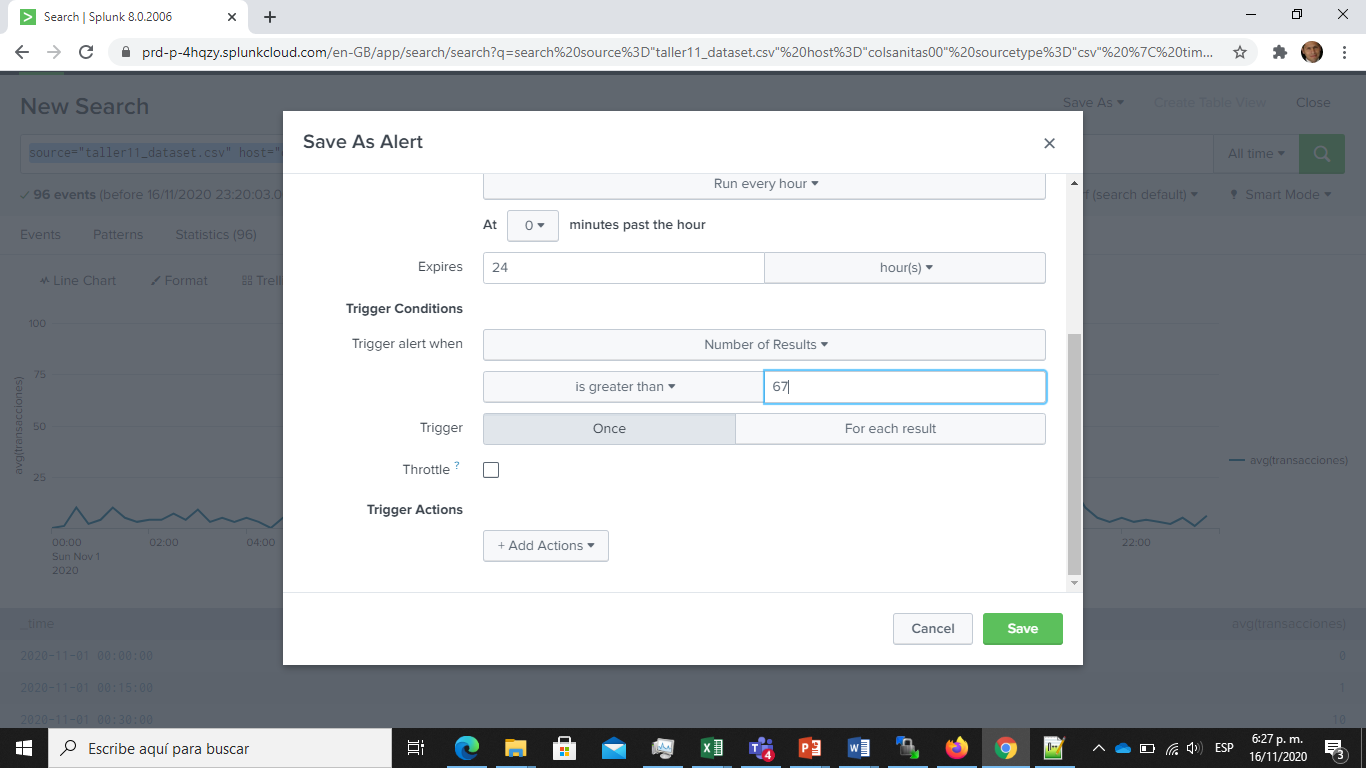
Luego buscarmos “Visualization” y seleccionamos “Line Chart”:



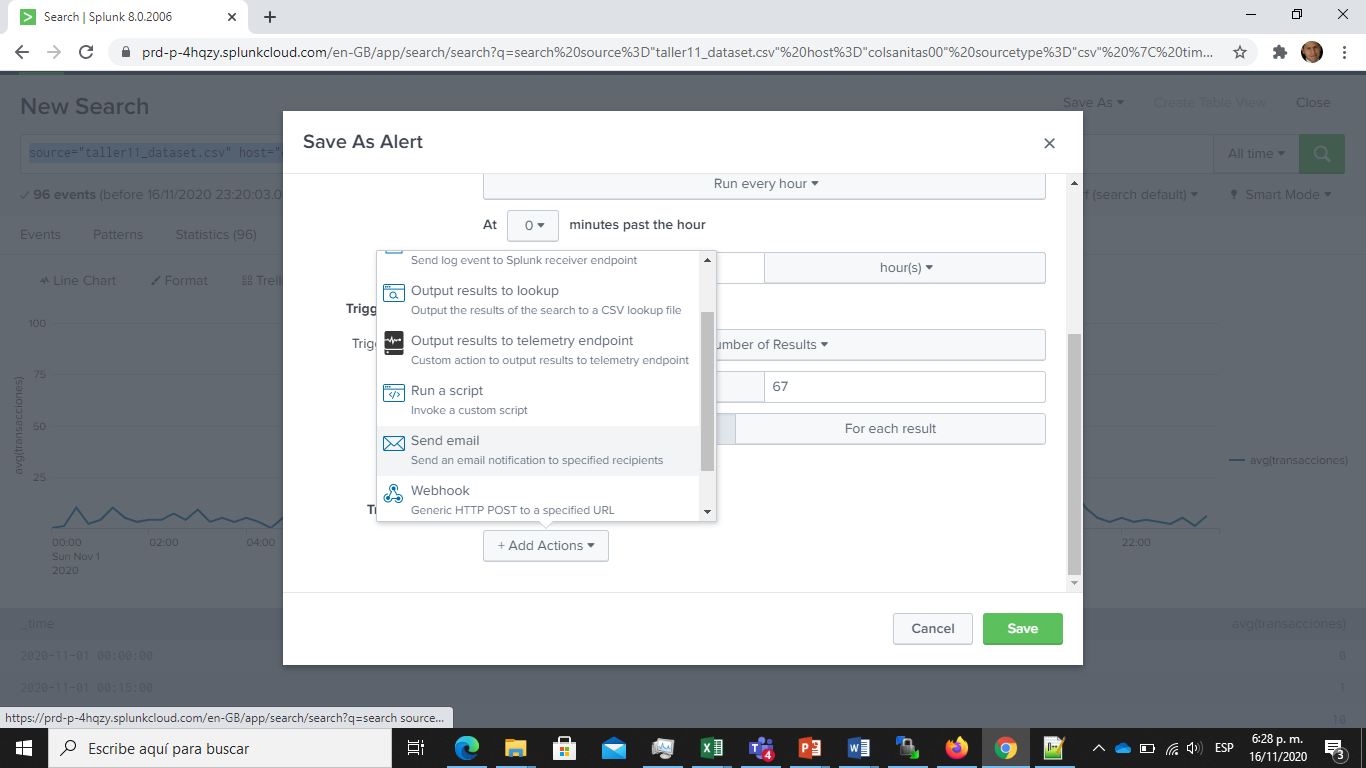
Luego oprimimos “Save As” (guardar como ) y escogemos Alert (Alerta)



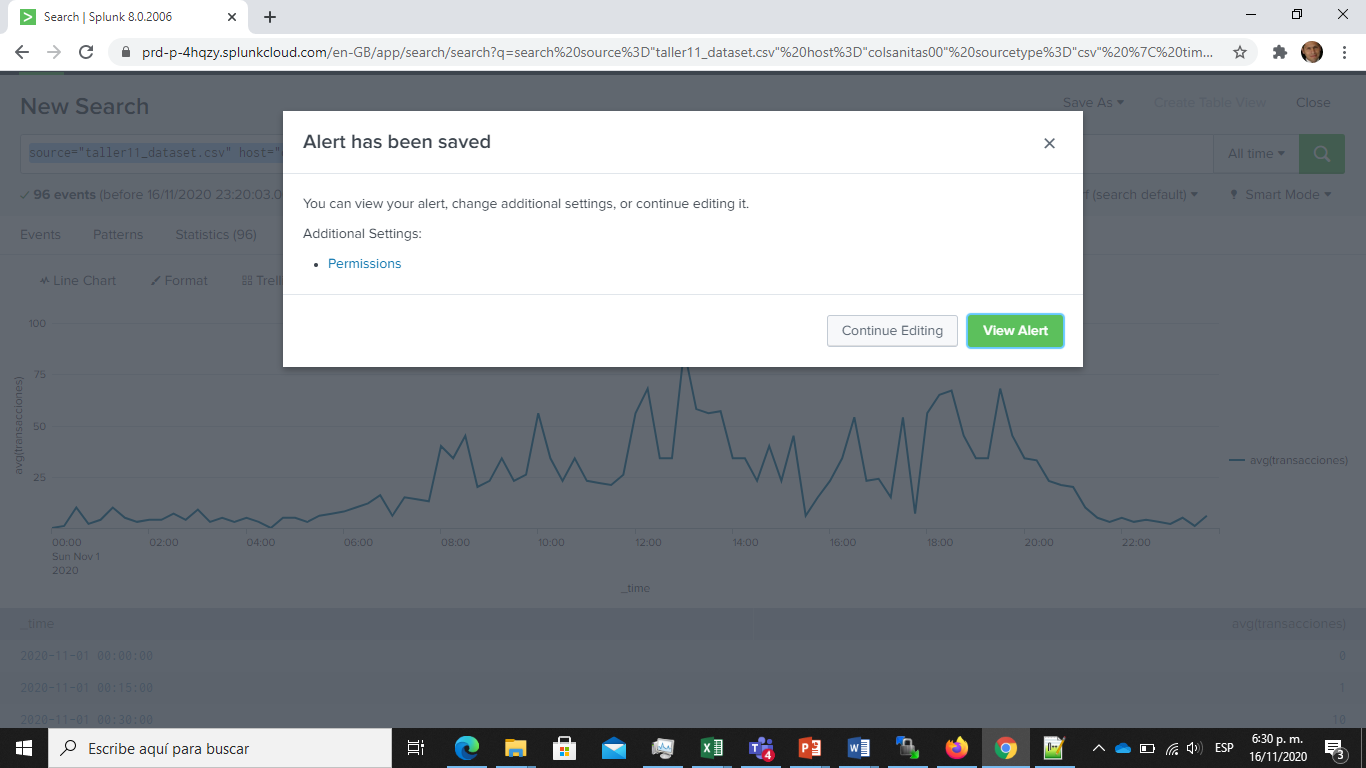
Configuremos la alerta para se dispare cuando se presenten mas de 67 transacciones.



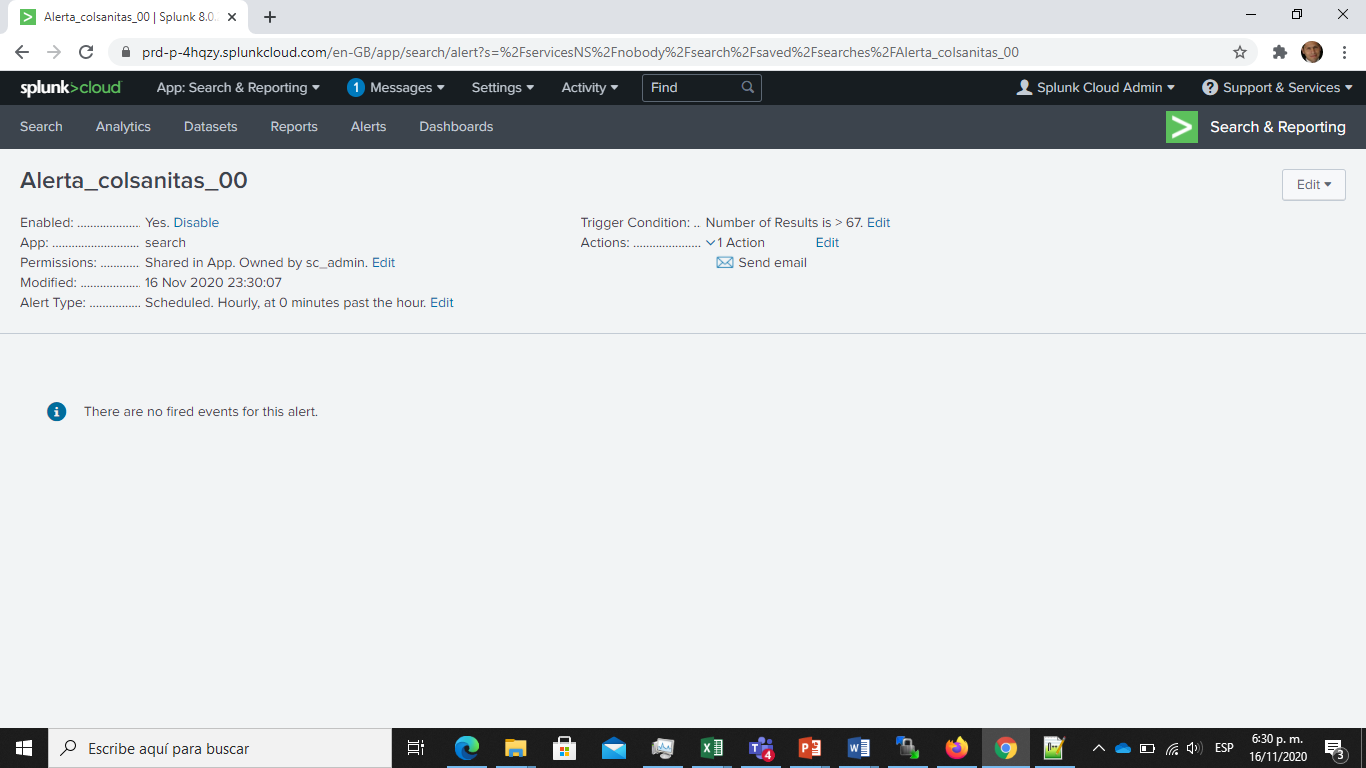
Oprimamos +Add Actions (Adicionar acciones) y busquemos “Send email” (enviar correo)



En el campo de “to” (para), colocamos un correo electrónico válido y luego oprimimos “Save” (Guardar) y luego “view alert” (Ver la alerta)

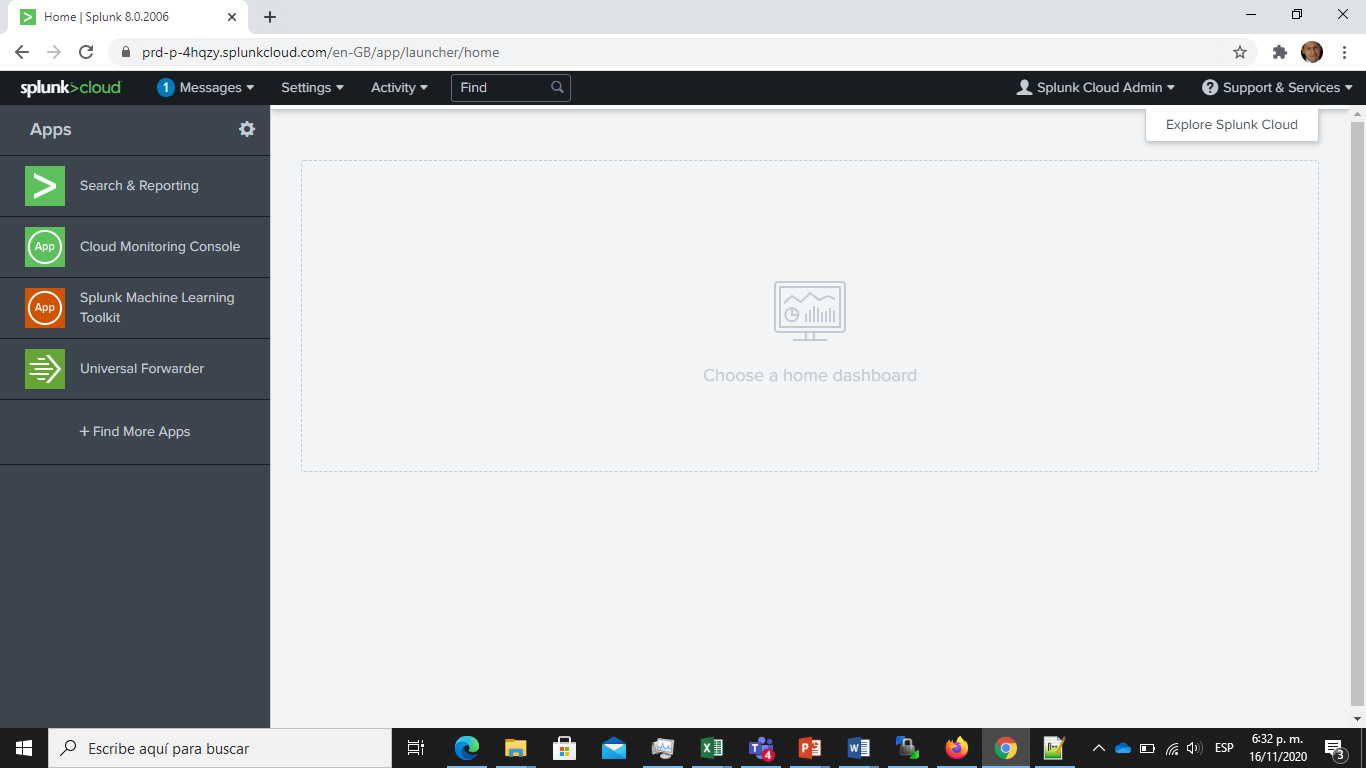


Esto debe mostrar:

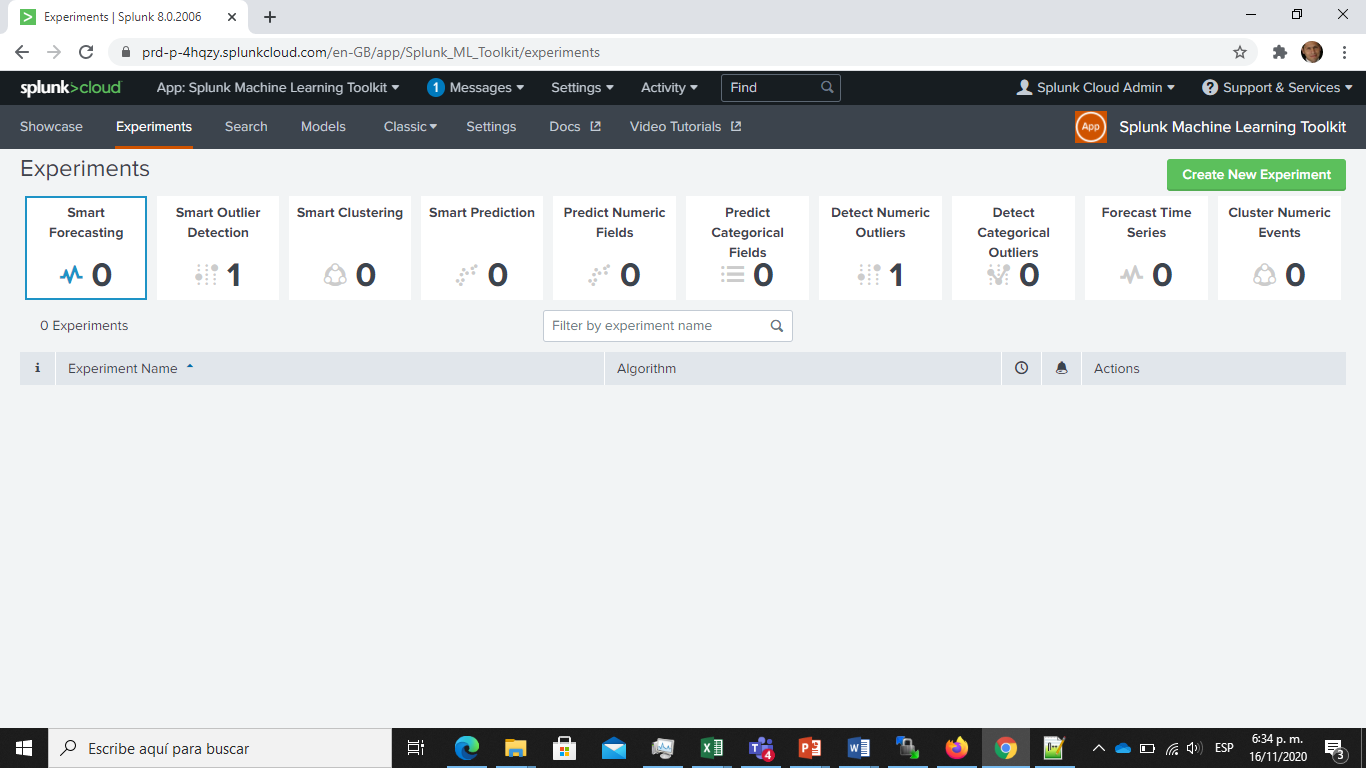


Parte 2: Inteligencia artificial

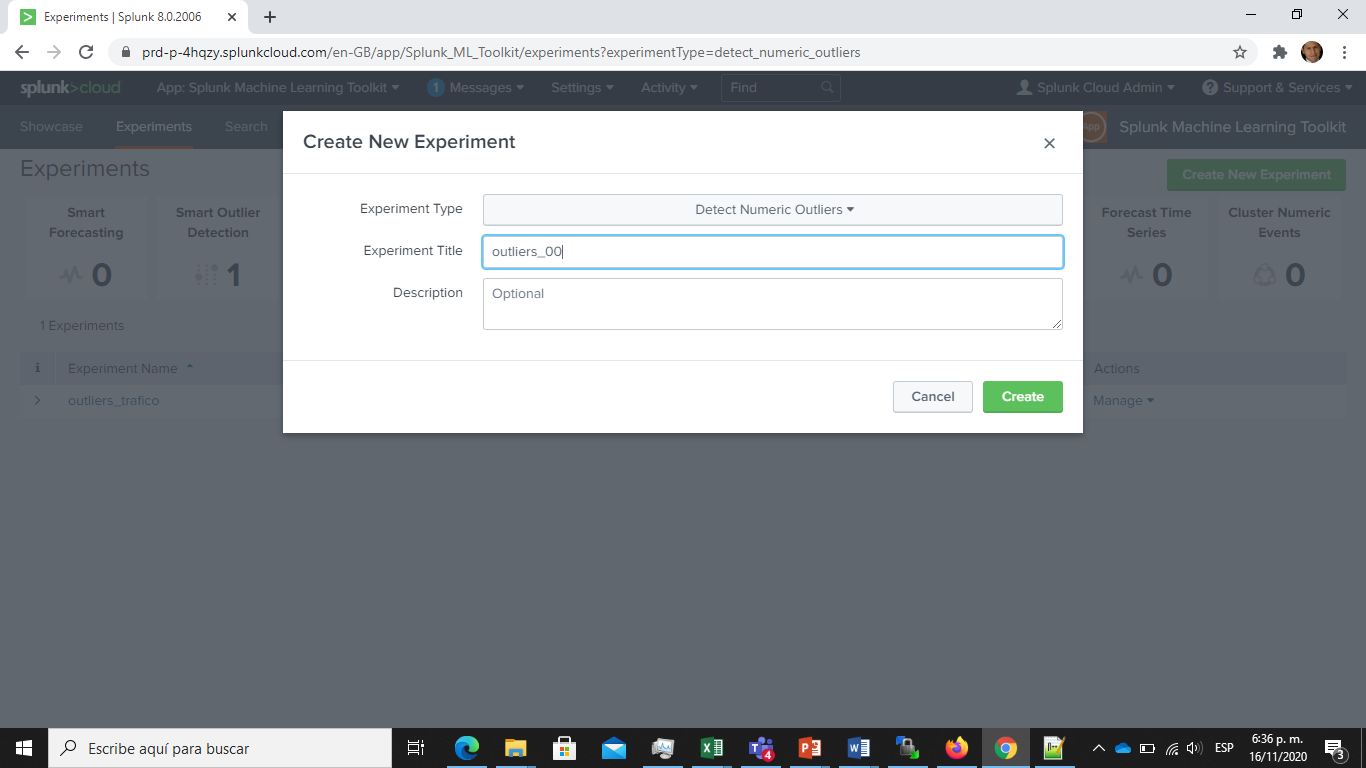
Oprimimos el logo “splunk > cloud” y alli oprimimos “Splunk Machine Learning Toolkit”



Oprimimos “Experiments” (Experimentos), allí oprimimos “Detect Numeric Outliers” (Detectar outliers numéricos) y luego “Create New Experiment” (Crear un nuevo experimento)



En el nombre escribimos “outliersXX” donde XX es el número asignado y luego el boton “Create”



Debe aparecer una pantalla así:



En la expresión de búsqueda escribimos:

host="colsanitasXX" sourcetype="csv" | timechart avg(transacciones) as promedio\_transacciones span=15m

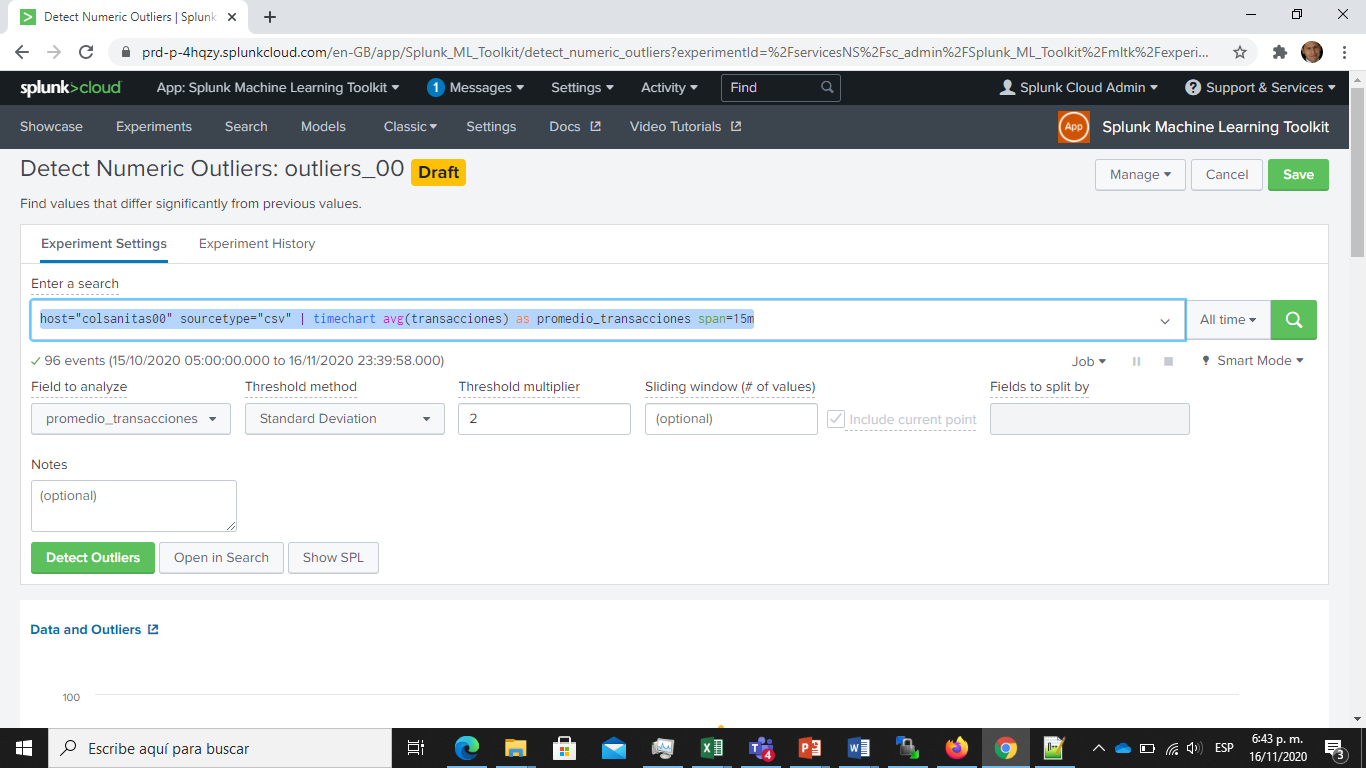
Lo que significa que nuestro servidor origen es “colsanitasXX”, donde XX es el numero asignado.

Adicionalmente que estamos generando una gráfica donde en el eje X tenemos el tiempo y en el eje Y tenemos el promedio de transacciones cada 15 minutos.

En el campo “Field to analyze” (campo a analizar) escogemos “promedio\_transacciones”

Observar que en el campo “Threshold multiplier” (multiplicador de umbral) está el valor 2, lo que quiere decir que estamos mirando aquellos valores mayores a dos veces sigma.

Esto debe mostrarse asi, una vez completado, oprimir “Detect Outliers” (Detectar outliers):



Haciendo scroll hacia abajo, obtenemos un gráfico donde en azul se muestra el área esperada y en blanco el área de outliers. En este ejercicio se presentan cinco puntos fuera de rango.



Cuantos outliers habrá si se selecionan 3 sigmas (desviaciones estándar)?

Y listo! Felicitaciones! Lo hemos logrado! Ya podemos usar inteligencia artificial en splunk con nuestros datasets!