

Taller de Splunk4Rookies

Guía de Laboratorio

Descripción General

Esta guía de laboratorio contiene los ejercicios prácticos para el taller de **Splunk4Rookies**. Antes de continuar con estos ejercicios, asegúrese de unirse a una sesión virtual o de tener una copia de la [presentación con diapositivas de Splunk4Rookies](#), que lo ayudará a poner en contexto las tareas que lleve a cabo.

Requisitos Previos

Para completar estos ejercicios, necesitará su propio entorno de laboratorio de Splunk. Los talleres prácticos de Splunk se imparten a través del [portal de Splunk Show](#), y se necesita una cuenta en splunk.com para poder acceder.

Si aún no tiene una cuenta de Splunk.com, cree una [aquí](#) antes de continuar con el resto del taller.

Índice

Descripción General	1
Requisitos Previos	1
Índice	2
Ejercicio 1: Acceder a tu Entorno de Laboratorio	4
Descripción	4
Pasos	4
Ejercicio 2: Crear una Aplicación y Añadir Datos a Splunk	7
Descripción	7
Pasos	7
Empieza a Explorar tus Datos	14
Descripción	14
Pasos	14
Ejercicios de Desafío	15
Ejercicio 3: Equipo de Operaciones de TI. Investigar las Solicitudes del Servidor Web Correctas frente a las que han Presentado un Error (a lo largo del tiempo)	16
Descripción	16
Pasos	16
Ejercicio 4: Equipo de DevOps. Mostrar los Sistemas Operativos más Habituales de los Clientes y qué Navegadores Web Generan más Errores	20
Descripción	20
Pasos	20
Extraer un campo nuevo	20
Mostrar los sistemas operativos más habituales de los clientes	22
Mostrar qué navegadores web generan más errores	24
Ejercicio 5: Equipos de Ventas/Análisis Empresarial. Mostrar Ingresos Perdidos a causa de Transacciones Fallidas del Sitio Web	27
Descripción	27
Pasos	27
Ejercicio 6: Equipos de Seguridad/Fraude. Mostrar la Actividad del Sitio Web por Ubicación Geográfica	31
Descripción	31
Pasos	31
Ejercicios de Desafío	32
Ejercicio 7: Personalizar tu <i>Dashboard</i>	33
Descripción	33

Pasos	33
Añadir una imagen de fondo a tu <i>dashboard</i>	33
Conectar los paneles al selector de tiempo global	36
Soluciones de los Ejercicios de Desafío	38
Comenzar a Buscar en Splunk	38
Equipos de Seguridad/Fraude. Mostrar cualquier Actividad en el Sitio Web con Origen fuera de los Estados Unidos	38

Ejercicio 1: Acceder a tu Entorno de Laboratorio

Descripción

Necesitarás un entorno de prácticas de Splunk para completar estos ejercicios. ¡Es el momento de obtenerlo!

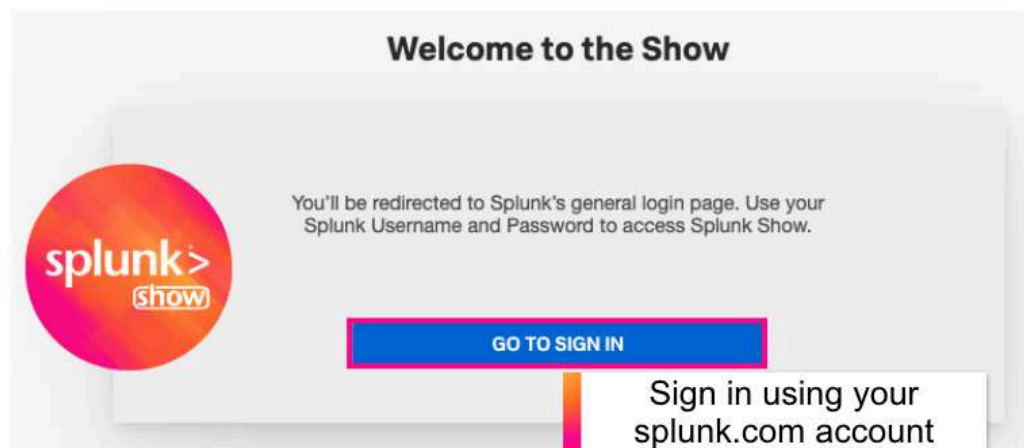
En este ejercicio, crearás tu propio entorno de Splunk Enterprise usando nuestro portal de Splunk Show.

¿Has recibido ya los detalles de tu entorno de Splunk?

Si el anfitrión del taller ya te ha proporcionado el link de tu entorno y los detalles de inicio de sesión, no es necesario que sigas las instrucciones del ejercicio 1 de esta guía de laboratorio. ¡Puedes pasar directamente al [ejercicio 2](#)!

Pasos

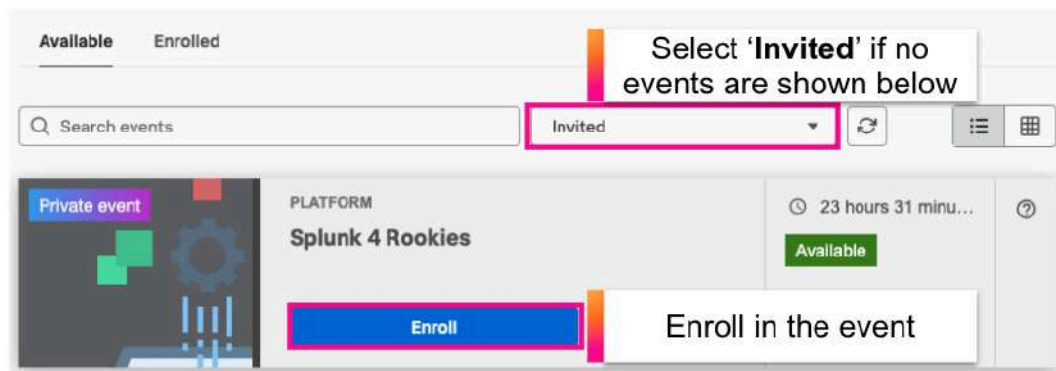
1. Navega a <https://show.splunk.com> e inicia sesión con tu **cuenta de splunk.com**.



¿No tienes una cuenta de Splunk.com?

Para acceder a los eventos de nuestros talleres prácticos, necesitarás una cuenta de Splunk.com. Si aún no tienes una cuenta de Splunk.com, no te preocupes: ¡crear una te llevará tan solo unos minutos! Crea una [aquí](#).

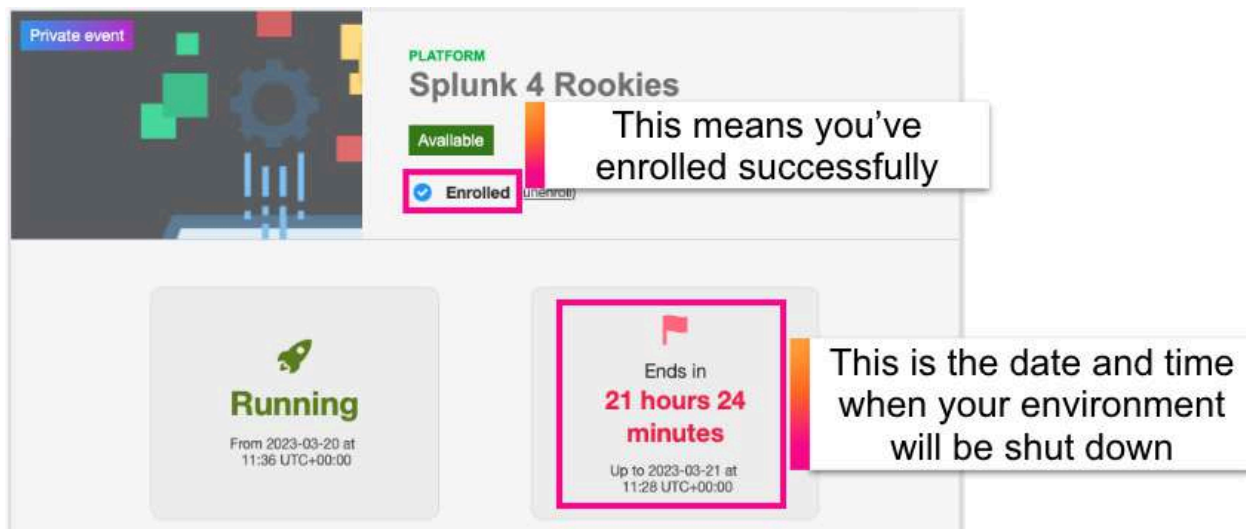
- Una vez que hayas iniciado sesión en Splunk Show, verás la página del evento al que has sido invitado. Si no hay eventos en la lista, intenta seleccionar **Invited** de la lista desplegable.
- Haz click en **Enroll** para unirme al evento.



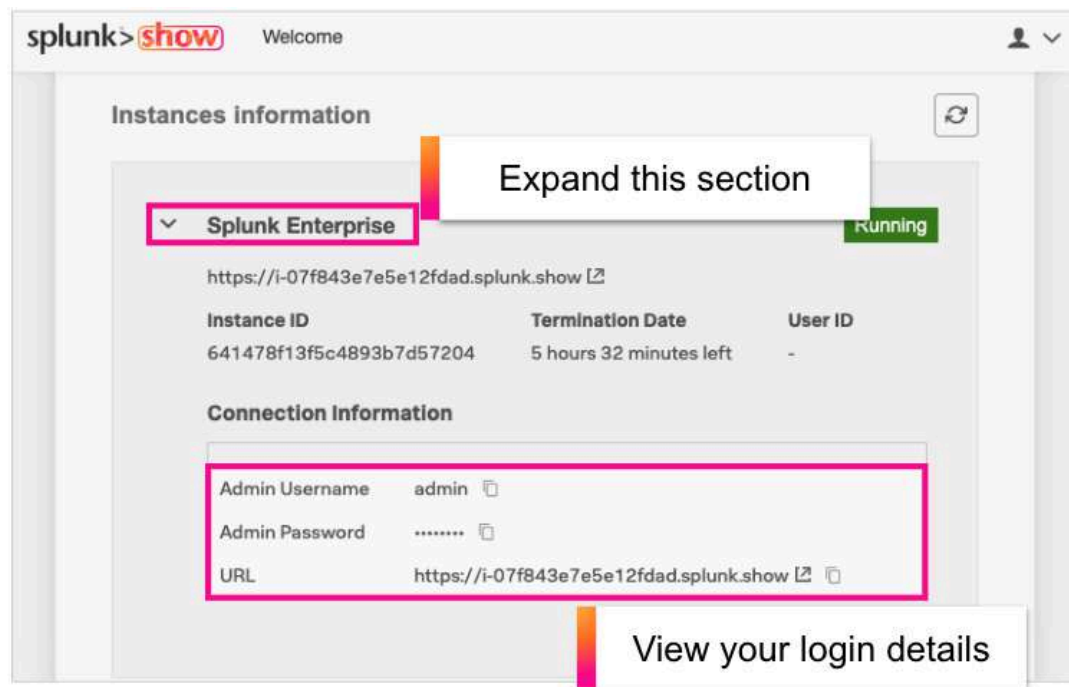
La página se actualizará y el evento mostrará «Enrolled».

Caducidad del entorno de laboratorio

Todos los entornos de Splunk que forman parte de este evento se cerrarán automáticamente en la fecha y la hora especificadas en esta pantalla, así que siéntete libre de seguir explorando tu entorno de laboratorio hasta entonces.

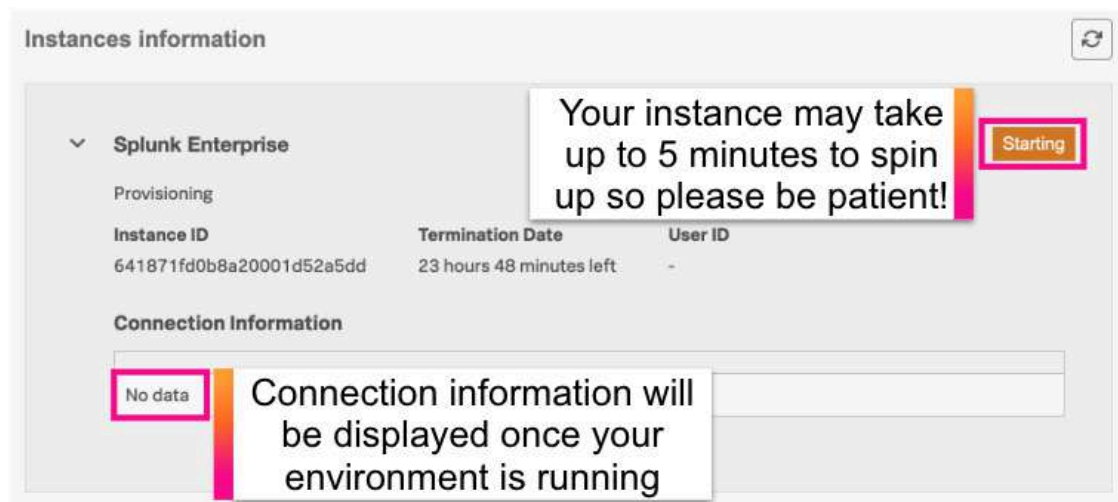


4. Desplázate hacia abajo en la página hasta la sección **Instances Information** y expande la sección «Splunk Enterprise» para encontrar las credenciales de usuario y el enlace a tu entorno de laboratorio.



¿No se muestra la información de conexión?

Si aún no se muestra ninguna información de conexión, significa que tu entorno de laboratorio se está iniciando. Intenta actualizar esta vista en unos minutos.



Ejercicio 2: Crear una Aplicación y Añadir Datos a Splunk

Descripción

Las aplicaciones e integraciones de Splunk brindan contenido y capacidades personalizables para una variedad de tecnologías y casos de uso, lo que acelera el tiempo que lleva obtener valor de tus datos. También son una excelente manera de organizar y compartir tu contenido, como informes y paneles, con otros usuarios de Splunk. Cualquiera puede crear aplicaciones e integraciones, y hoy vamos a crear nuestra propia aplicación que contiene un panel.

Dado que Splunk es una plataforma de datos, también necesitaremos cargar algunos datos.

En este ejercicio, crearás una nueva aplicación y luego añadirás algunos datos a tu entorno de Splunk Enterprise. Configuraremos Splunk para monitorizar los registros del servidor web de ejemplo, que actualmente se generan en el mismo servidor en el que se ejecuta Splunk.

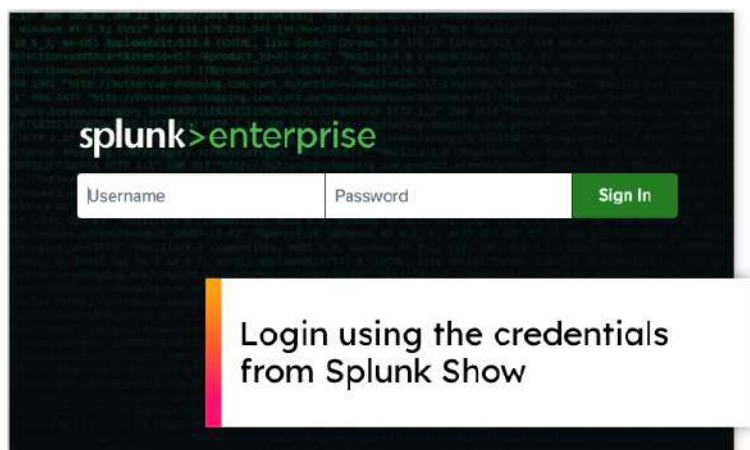
Pasos

1. Navega hasta tu entorno de Splunk usando el enlace de URL exclusivo proporcionado en el evento de Splunk Show (consulta el paso 3 del [ejercicio 1: Acceder a su entorno de laboratorio](#)).

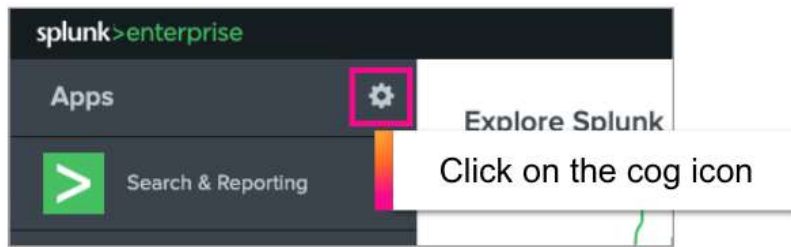


A screenshot of the Splunk login interface. It features three input fields: 'Admin Username' with the value 'admin', 'Admin Password' with masked characters, and 'URL' with the value 'https://i-07f843e7e5e12fdad.splunk.show'. The 'URL' field is highlighted with a red rectangular border. Each field has a small icon to its right.

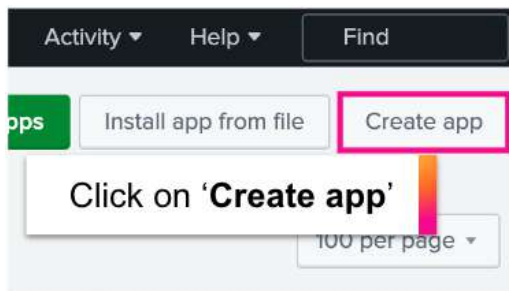
2. Inicie sesión con las credenciales en el evento Splunk Show.



3. En el lateral izquierdo de la página, en la sección **Apps**, haz click en el icono de la rueda dentada.



4. En la esquina superior derecha de la pantalla, haz click en **Create app**.



5. Asigna un nombre a tu aplicación e introduce un nombre de carpeta. Deja todos los demás valores como están y haz click en **Save**.



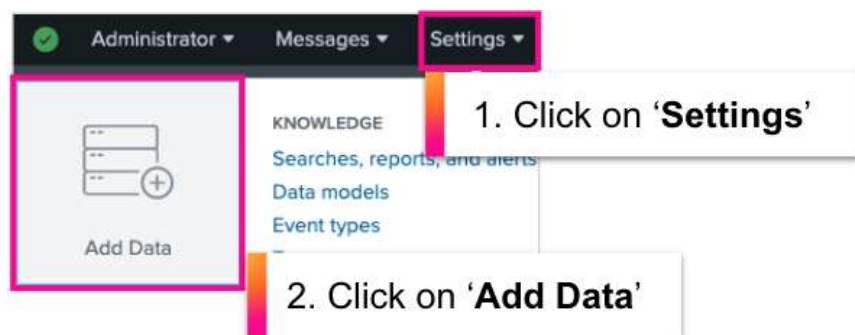
6. Ahora que hemos creado nuestra aplicación en blanco, debemos seleccionarla para que todo lo que hagamos a partir de ahora se cree y se guarde dentro de esta.

Para seleccionar tu aplicación, haz click en la lista desplegable **Apps** en la parte superior izquierda de la página y selecciona tu aplicación.



¡Es hora de añadir algunos datos!

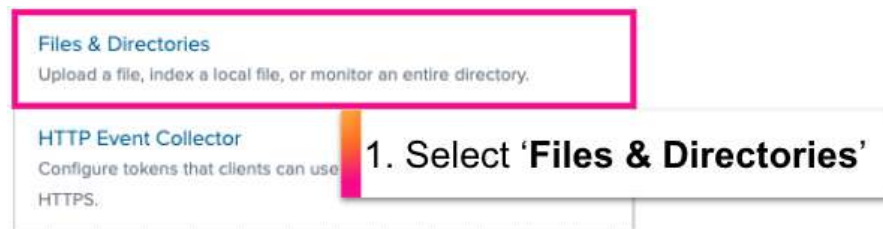
7. Con tu nueva aplicación aún seleccionada en la lista desplegable, accede a **Settings > Add Data**.



8. Para este ejercicio, queremos monitorizar un directorio de forma constante, ya que esto nos permitirá recopilar nuevos datos a medida que los genere el servidor web. Para hacer esto, haz click en **Monitor**.



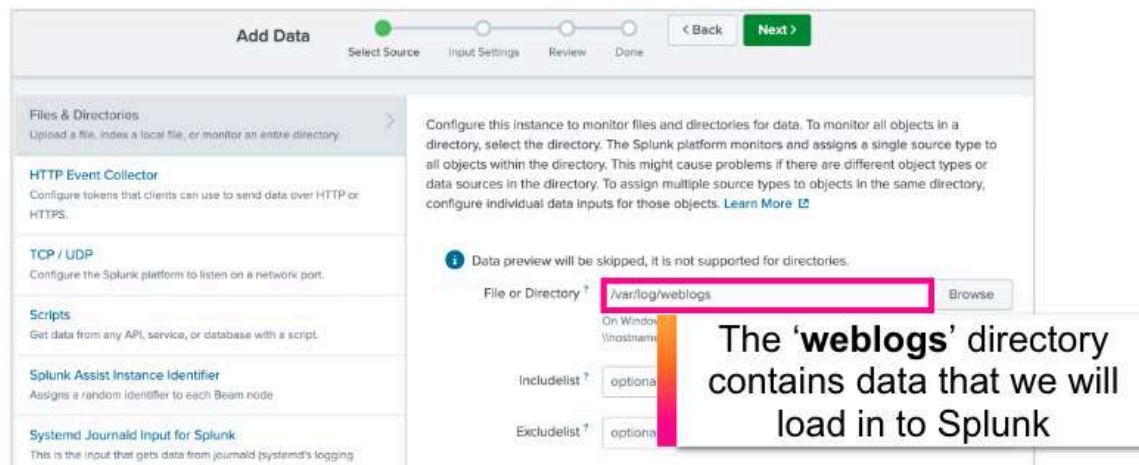
9. Selecciona **Files & Directories** y luego haz click en **Browse**.



10. Navega hasta **/var/log** y selecciona el directorio **weblogs**. Haz click en **Select** para elegir este directorio.



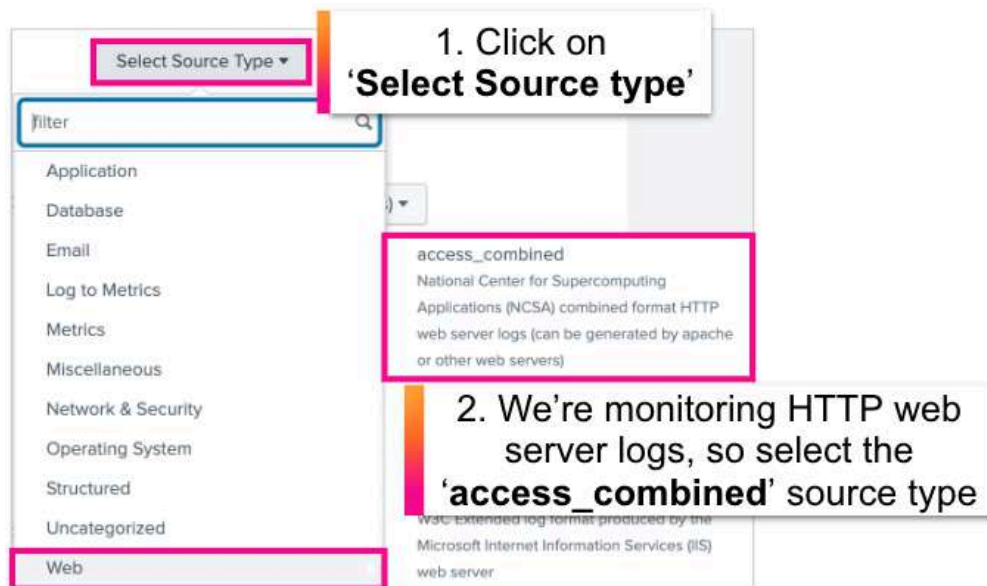
11. Comprueba que la ruta del directorio sea correcta (**/var/log/weblogs**) y haz click en **Next**.



12. Ahora necesitamos seleccionar un tipo de fuente para estos datos. Un tipo de fuente determina cómo Splunk aplica formato a los datos durante el proceso de *indexing*. Splunk viene con un gran conjunto de tipos de fuente predefinidos y, a menudo, puede detectar el tipo de fuente automáticamente. Sin embargo, para este ejercicio deberás especificar el tipo de fuente. En la pantalla **Input Settings**, a la derecha de la sección **Source type**, haz click en **Select**.



13. Haz click en la lista desplegable **Select Source Type** y busca **Web > access_combined**. Como alternativa, puedes comenzar a escribir «access» en el campo **filter** y se mostrará el tipo de fuente «access_combined».



14. Para **App Context**, asegúrate de que tu nueva aplicación esté seleccionada en la lista.




15. Deja todos los demás valores como predeterminados y haz click en **Revisar**.

16. Revisa tu configuración y haz click en **Enviar**.


Review	
Input Type	Directory Monitor
Source Path	/var/log/weblogs
Whitelist	N/A
Blacklist	N/A
Source Type	access_combined
App Context	splunk4rookies
Host	ip-172-31-25-84
Index	default

17. Recibirás un mensaje que indica que tu **archivo de entrada se ha creado correctamente**.


Haz click en **Start Searching** para buscar los datos que acabas de añadir a Splunk.

 **File input has been created successfully.**
Configure your inputs by going to [Settings > Data Inputs](#)


Start Searching

Search your data now or see [examples and tutorials](#). 


Extract Fields

Create search-time field extractions. [Learn more about fields](#). 


Add More Data

Add more data inputs now or see [examples and tutorials](#). 

Download Apps

Apps help you do more with your data. [Learn more](#). 

Build Dashboards

Visualize your searches. [Learn more](#). 

Verás los eventos sin procesar que se muestran en Splunk.

SearchAnalyticsDataSetsReportsAlertsDashboards

splunk4rookies

New Search

Save AsCreate Table ViewClose

source="/var/log/weblogs/*" host="ip-172-31-39-95" sourcetype="access_combined"

All time

✓ 1,467 events (before 17/01/2022 16:29:20.000) No Event Sampling

Job

Events (1,467)PatternsStatisticsVisualization

Format Timeline

Zoom OutZoom to SelectionDeselect

1 minute per column

ListFormat

20 Per Page

< Prev12345678...Next >

< Hide Fields

All Fields

SELECTED FIELDS

a host 1

a source 1

a sourcetype 1

INTERESTING FIELDS

a action 5

bytes 100+

a clientip 67

date_hour 2

date_mday 1

date_minute 25

a date_month 1

date_second 60

i	Time	Event
>	12/01/2022 18:09:15.129	194.215.285.19 -- [12/Jan/2022 18:09:15:129] "GET /cart.do?action=view&itenId=EST-7&product_id=WPSS-2&JSESSIONID=SD9SL10FF5ADFF9 HTTP 1.1" 403 3490 "http://www.buttercupenterprises.com/product.screen?product_id=WPSS-2" "Mozilla/5.0 (Windows; WOW64) AppleWebKit/537.36 Chrome/51.0.2704.106 Safari/537.36" 402 host = ip-172-31-39-95 source = /var/log/weblogs/noise_apache_3.log sourcetype = access_combined
>	12/01/2022 18:09:13.193	141.146.8.66 -- [12/Jan/2022 18:09:13:193] "GET /cart.do?action=changequantity&itenId=EST-26&product_id=MCB-6&JSESSIONID=SD3SL1FF7ADFF5 HTTP 1.1" 200 2278 "http://www.buttercupenterprises.com/cart.do?action=changequantity&itenId=EST-26&product_id=MCB-6" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_2) AppleWebKit/537.36 Chrome/57.0.2957.0 Safari/537.36" 613 host = ip-172-31-39-95 source = /var/log/weblogs/noise_apache_3.log sourcetype = access_combined
>	12/01/2022 18:09:13.191	128.241.220.82 -- [12/Jan/2022 18:09:13:191] "GET /product.screen?product_id=WPSS-2&JSESSIONID=SD4SL2FF5ADFF8 HTTP 1.1" 400 317 "http://www.buttercupenterprises.com/product.screen?product_id=WPSS-2" "Mozilla/5.0 (Linux; Android 6.0.1; Nexus 5 Build/MRA58N) AppleWebKit/537.36 Chrome/52.0.2743.8 Mobile Safari/537.36" 818 host = ip-172-31-39-95 source = /var/log/weblogs/noise_apache_3.log sourcetype = access_combined

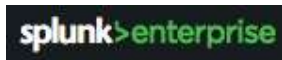
Empieza a Explorar tus Datos

Descripción

En este ejercicio, probarás algunas búsquedas básicas de Splunk usando la sección «Search» de tu nueva aplicación.

Pasos

1. Haz click en el logotipo de Splunk en la esquina superior izquierda de la pantalla para volver a la pantalla de inicio predeterminada.



2. En la sección **Apps**, en el lateral izquierdo de la página, haz click en la nueva aplicación que has creado en el ejercicio 2.

(Nota: El nombre será el que escribiste cuando la creaste).



3. Para buscar, basta con escribir cualquier palabra o frase en la barra de búsqueda. Splunk buscará todos los eventos que contengan esas palabras.

Suficiente. ¡Probemos algunas búsquedas!

En primer lugar, selecciona **Last 60 minutes** en el selector de tiempo (a la derecha de la barra de búsqueda). Tu entorno tiene un generador de eventos que se ejecuta en segundo plano y que crea constantemente datos de ejemplo para que los usemos durante el taller. Estos datos empezaron a generarse en el momento en que te registraste en tu entorno de Splunk. Limitémonos a los últimos 60 minutos de datos...

Prueba con la siguiente búsqueda:

```
purchase 503
```

Se devolverán todos los eventos de Splunk que contengan la palabra **purchase** y el número **503**.

Espacios entre palabras en una búsqueda

En Splunk, un espacio entre dos palabras es un operador lógico implícito **AND**, lo que significa que Splunk buscará automáticamente eventos que contengan ambas palabras (no es necesario que lo especifiquemos).

4. Eso es genial, pero ¿qué pasa si hay eventos, por ejemplo, con las palabras *purchased*, *purchasing* o *purchaser*? Bien, podemos usar un asterisco comodín (*) para buscar cualquier evento que contenga **503** y cualquier palabra que comience con **pur**:

```
pur* 503
```

Un comodín es útil si queremos ser un poco más flexibles en la búsqueda.

5. ¿Recuerdas el operador **AND** que mencionamos en el paso 3? Bien, también puedes usar los otros operadores lógicos: **OR** y **NOT**. Ten en cuenta que estos deben estar en MAYÚSCULAS.

Intentemos usar uno de estos operadores en una búsqueda:

```
503 (purchase OR addtocart)
```

Esta búsqueda devolverá todos los eventos que contengan el número **503** y la palabra **purchase** o la palabra **addtocart**.

6. Hasta ahora, solo hemos buscado texto. Esos números y palabras pueden aparecer en cualquier parte de nuestros datos; entonces, ¿cómo sabemos que estamos buscando los valores correctos? Dependiendo de nuestros datos, **503** podría ser un código de estado de HTTP o podría ser parte de un ID de sesión o un número de teléfono.

Como ya sabemos que estamos viendo registros web, vamos a incluir un conjunto de campo y valor en nuestra búsqueda para ser más específicos:

```
status=503 action=purchase
```

Esto asegurará que nuestros resultados solo devuelvan eventos de **compra** del servidor web en los que el código de estado de HTTP sea **503**. Es importante especificar los nombres de los campos siempre que sea posible para garantizar que tus resultados sean lo más precisos posible.

Ejercicios de Desafío

P1. ¿Cómo podemos encontrar eventos con el estado 200 que no sean eventos de compra?

P2. ¿Cómo podemos encontrar eventos en los que alguien ha recibido un error al intentar añadir o quitar un artículo de su carrito?

(Pista: El código de estado 200 de HTTP significa que la transacción es correcta. El código 400 o un número mayor generalmente significa que se ha producido un error).

✓ Soluciones de los ejercicios de desafío

Las soluciones de los ejercicios de desafío se encuentran al final de este documento.

Ejercicio 3: Equipo de Operaciones de TI. Investigar las Solicitudes del Servidor Web Correctas frente a las que han Presentado un Error (a lo largo del tiempo)

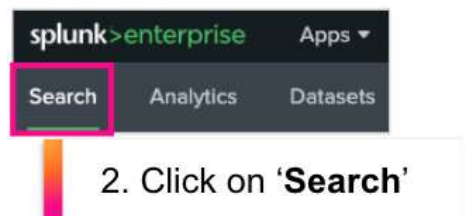
Descripción

Actualmente, el equipo de operaciones de TI no tiene visibilidad del sitio web de Buttercup Enterprises.

En este ejercicio, crearás un panel de visualización para el equipo de operaciones de TI, donde se mostrarán las operaciones correctas del sitio web en contraste con las operaciones que presentaron un error, a lo largo del tiempo.

Pasos

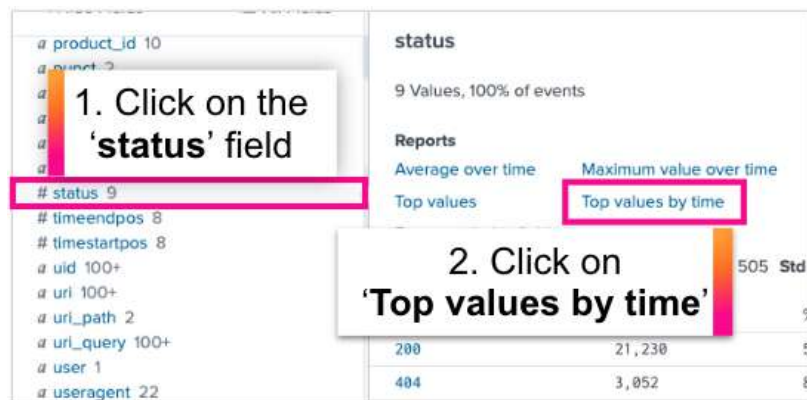
1. Para iniciar una nueva búsqueda, primero asegúrate de que tu aplicación está seleccionada en la lista desplegable «Apps»; luego, haz click en «Search» en la barra de menú de la aplicación.



- Busca todos los eventos del servidor web que se han producido durante los últimos 60 minutos con la opción **Last 60 minutes**:

```
sourcetype=access_combined
```

- Desplázate hacia abajo en la página y busca el campo **status**. Haz click en el nombre del campo para mostrar la ventana del campo y selecciona **Top values by time**.

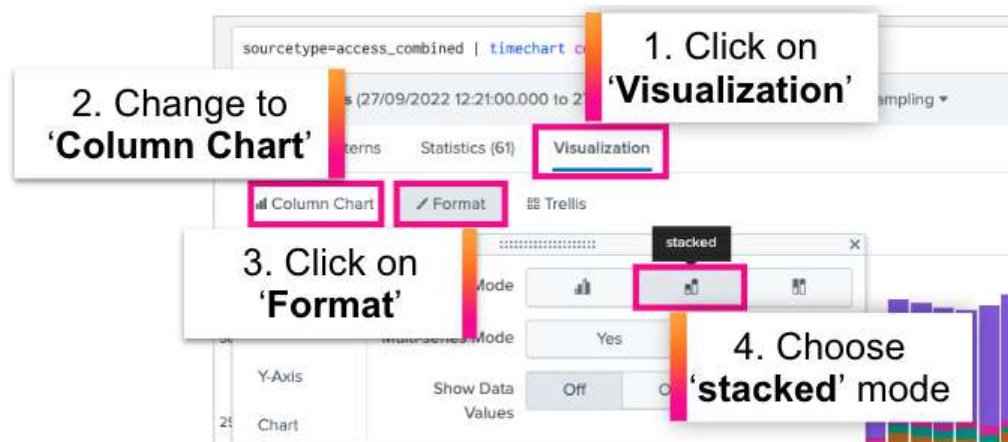


Splunk completará automáticamente tu búsqueda de la siguiente manera:

```
sourcetype=access_combined | timechart count by status limit=10
```

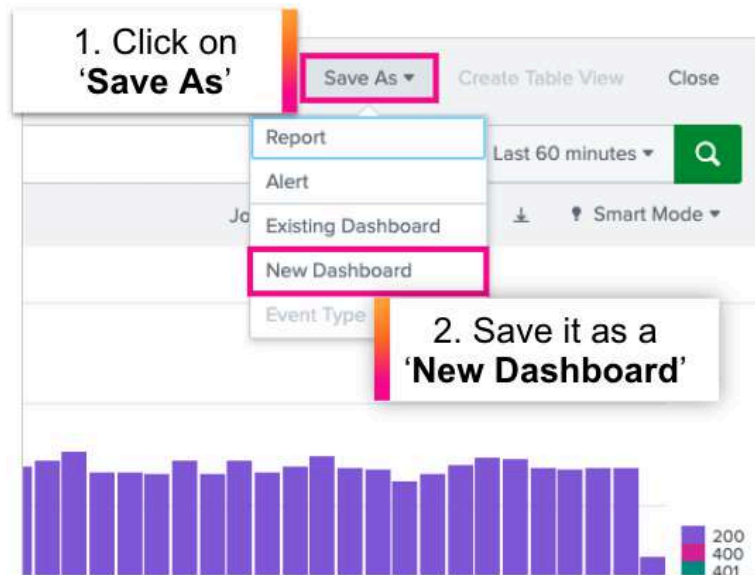
- Se mostrará un gráfico en la pestaña **Visualization**. Cambia la visualización a **Column Chart**.

Haz click en **Format** y luego en la pestaña **General** para cambiar la opción **Stack Mode** a **stacked**. Eres libre de explorar el formato hasta que estés satisfecho con la visualización.



- Ahora que tenemos una buena visualización de los gráficos, vamos a añadirla a un nuevo *dashboard* para que podamos compartir esta información con nuestra empresa (Buttercup Enterprises).

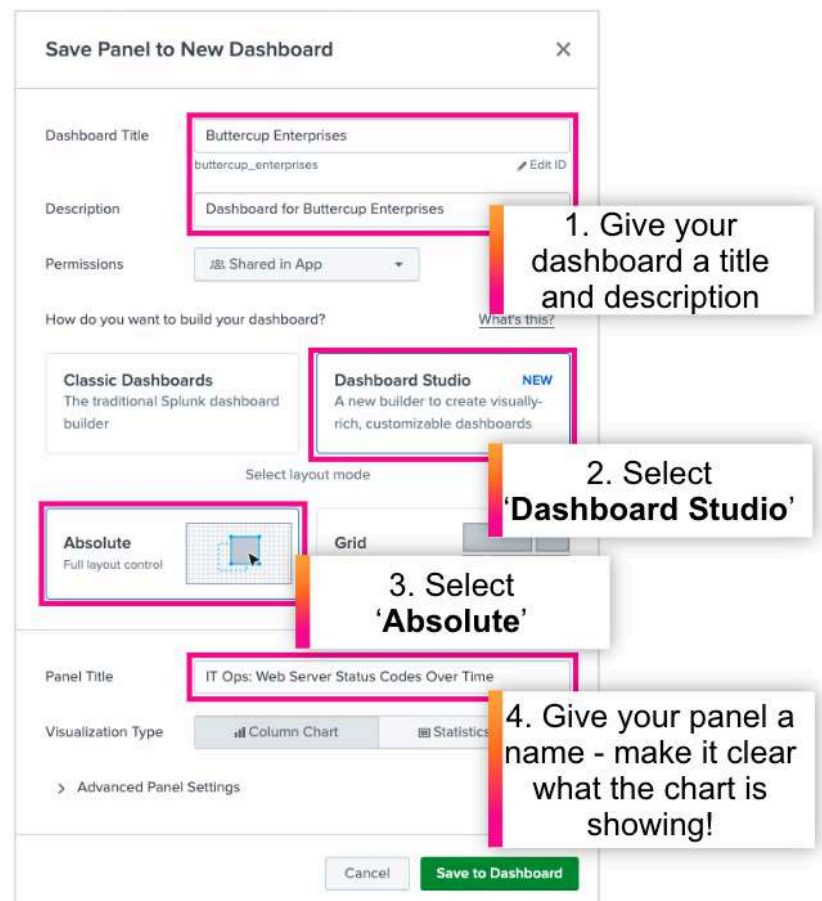
En la esquina superior derecha de la pantalla, selecciona **Save As > New Dashboard**.



- En la pantalla **Save Panel to New Dashboard**, asigna a tu *dashboard* un título adecuado y, opcionalmente, una descripción. Si no se te ocurre un nombre para tu *dashboard*, asígnale el nombre **Buttercup Enterprises**.

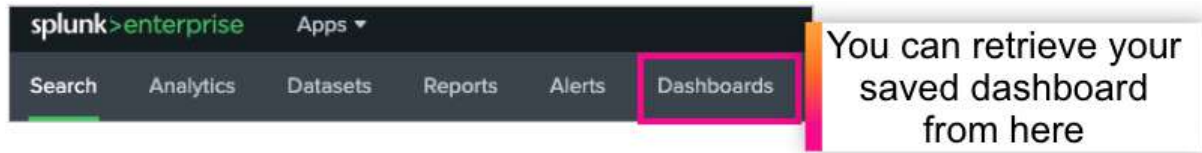
Elige que tipo de *dashboard* quieres usar. Para el taller de hoy, usaremos **Dashboard Studio**. El modo de diseño que vamos a usar será **Absolute**.

Asigna un título a tu panel que describa lo que representa la visualización, por ejemplo, **Operaciones de TI: Códigos de estado del servidor web a lo largo del tiempo**.



7. Haz click en **Save to Dashboard** y luego en **View Dashboard**.

¡Enhorabuena! Acabas de crear un *dashboard* de Splunk con tu primer panel. Cada vez que quieras acceder a un *dashboard*, haz click en **Dashboards** en la barra de menú y selecciona el que quieras ver. Adelante, ¡pruébalo!



Ejercicio 4: Equipo de DevOps. Mostrar los Sistemas Operativos más Habituales de los Clientes y qué Navegadores Web Generan más Errores

Descripción

En este ejercicio, deberás extraer un nuevo campo de tus eventos para crear el informe que necesitamos. Para lograr esto, usaremos el asistente de extracción de campos de Splunk.

Las extracciones de campos personalizados son útiles en una variedad de escenarios, por ejemplo:

- Cuando tienes datos personalizados y Splunk no ha reconocido/extraído un campo en particular que necesitas.
- Cuando necesitas extraer una parte determinada de un evento para poder buscar/informar sobre ese valor.

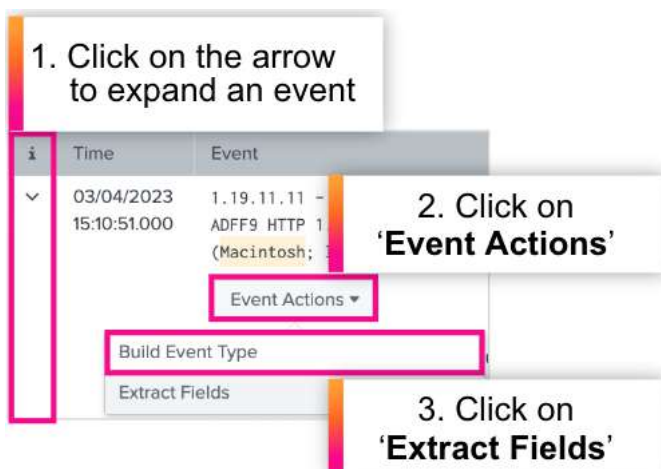
Pasos

Extraer un campo nuevo

1. Haz clic en **Search** si no ves la barra de búsqueda. Busca todos los eventos del servidor web que se han producido durante los últimos 60 minutos con la opción **Last 60 minutes**:

```
sourcetype=access_combined
```

2. Para expandir uno de los eventos, haz click en la flecha (>) a la izquierda del registro temporal (timestamp) del evento. Haz click en la lista desplegable **Event Actions** y selecciona **Extract Fields**:

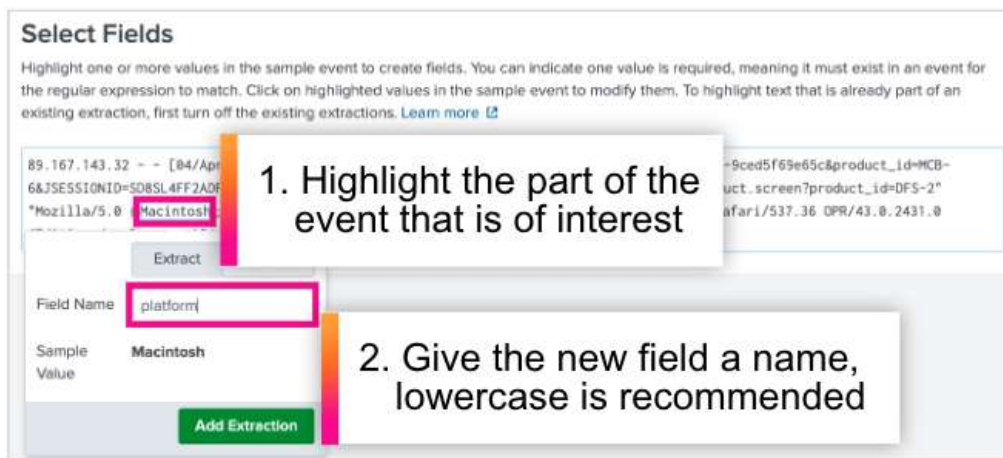


3. Tenemos dos opciones para extraer campos: expresión regex o delimitadores. Para este ejercicio, utilizaremos las expresiones regex. Haz click en **Regular Expression** y luego haz click en **Next**.



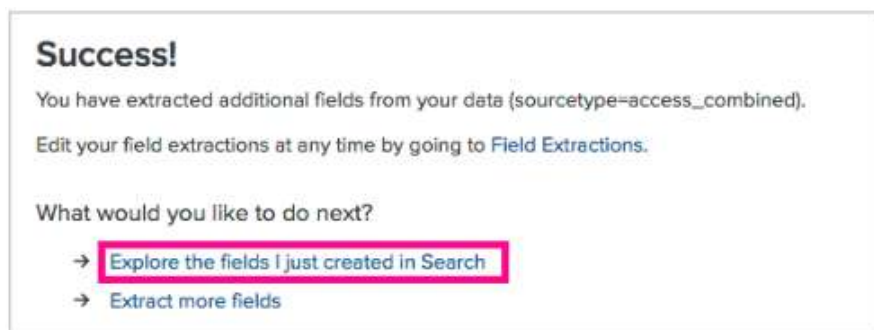
4. Ahora se te presentará un evento de ejemplo para que extraigas tu campo. Para este ejercicio, necesitaremos extraer la información de la plataforma (sistema operativo) de cada evento para poder generar un informe. Busca la información de la plataforma o sistema operativo en tu evento (p. ej., Linux, Macintosh, Windows, etc.) que se encuentra en la secuencia «useragent» hacia el final del evento y resáltala.

Nombra el nuevo campo: **platform** (los nombres de los campos distinguen entre mayúsculas y minúsculas, así que asegúrate de usar todas las letras en minúsculas para simplificar el proceso).



5. Haz click en **Add Extraction** y luego haz click en **Next**.

6. Haz click en **Next** de nuevo para ir a la pantalla **Save**. En la pantalla Save, haz click en **Finish** para guardar tu nueva extracción de campo.



Se mostrará la página «**Success!**». Haz click en **Explore the fields I just created in Search**.

7. Splunk te mostrará los resultados de búsqueda de todos los datos del servidor web durante las últimas 24 horas. Desplázate hacia abajo en la página y busca tu nuevo campo en la lista de la izquierda. ¡Ahora puedes usarlo en tus búsquedas!



Mostrar los sistemas operativos más habituales de los clientes

Ahora que tenemos nuestro nuevo campo, podemos usarlo para generar informes para el equipo de DevOps.

1. Busca todos los eventos del servidor web que se han producido durante los últimos 60 minutos con la opción **Last 60 minutes**:

```
sourcetype=access_combined
```

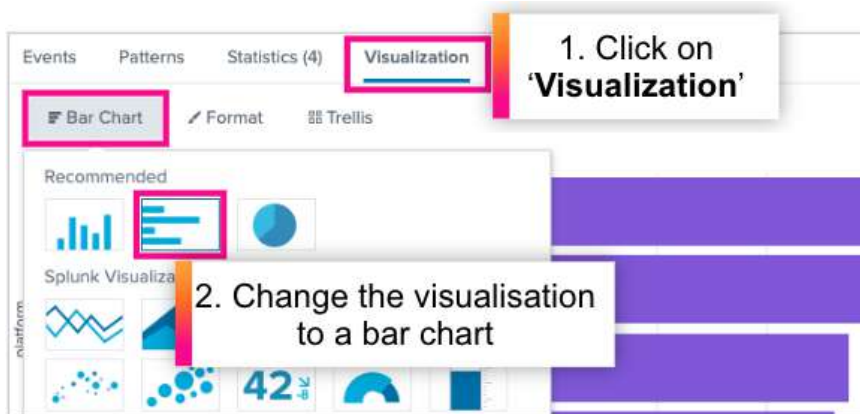
2. Desplázate hacia abajo en la página y busca el campo **platform** que acabas de extraer. Haz click en el nombre del campo para mostrar la ventana del campo y luego selecciona **Top values**.



Splunk completará automáticamente tu búsqueda de la siguiente manera:

```
sourcetype=access_combined | top limit=20 platform
```

3. Selecciona la pestaña **Visualization** si no está ya abierta y cambia la visualización a **Bar Chart**.

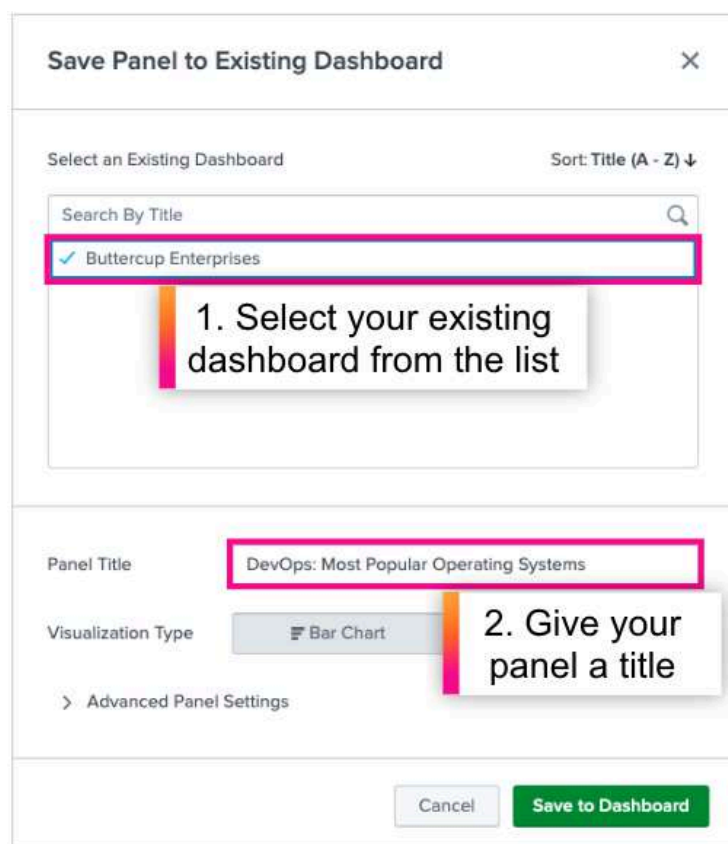
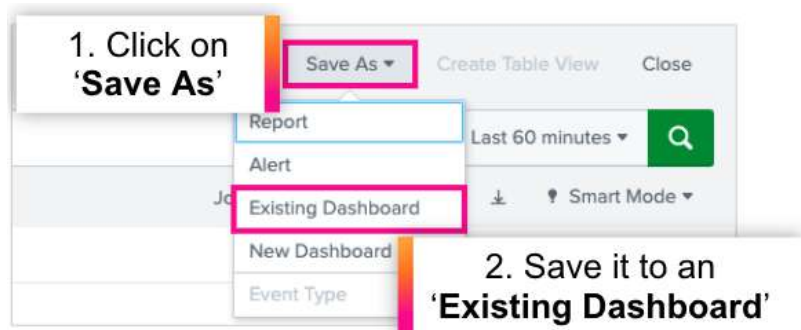


i Sugerencia para limpiar el gráfico

Opcionalmente, puedes añadir la opción `showperc=f` al comando `top` para quitar la columna «percent» de la tabla de estadísticas. Esto ayudará a mantener el gráfico limpio y ordenado y será más fácil visualizarlo en nuestro *dashboard* más adelante.

```
sourcetype=access_combined | top limit=20 platform showperc=f
```

4. Cuando estés satisfecho con el gráfico, guárdalo en el *dashboard* que has creado en el ejercicio anterior mediante **Save As > Existing Dashboard** y selecciona tu *dashboard* de la lista. Por último, ponle un título adecuado al panel de visualización que acabamos de crear, como **DevOps: Sistemas operativos más habituales**, y haz click en **Save to Dashboard**.



Mostrar qué navegadores web generan más errores

Ya tenemos uno de los dos casos de uso de DevOps listo. ¡Solo nos queda uno más para este equipo! Lo siguiente que necesitamos hacer es informar de los errores del navegador web.

1. Busca todos los eventos del servidor web que se han producido durante los últimos 60 minutos con la opción **Last 60 minutes**:

```
sourcetype=access_combined
```

2. Añade un filtro de búsqueda para que solo los eventos con el código de estado de 400 o un número superior sean devueltos (un evento con un valor de estado de 400 o más indica un error de algún tipo).

```
sourcetype=access_combined status>=400
```

3. Desplázate hacia abajo en la página y busca el campo **useragent**.
(Nota: «useragent» es un campo que contiene información sobre los navegadores web que interactúan con nuestro sitio web).
4. Haz click en el nombre del campo para mostrar la ventana del campo y luego selecciona **Top values by time**.



Splunk completará automáticamente tu búsqueda de la siguiente manera:

```
sourcetype=access_combined status>=400  
| timechart count by useragent limit=10
```


5. Selecciona la pestaña **Visualization** si no está ya abierta y cambia la visualización a **Area Chart**.

Para que tu gráfico esté más limpio, limita los resultados de la búsqueda a los 5 «useragents» más comunes. Para ello, cambia el límite a 5 en tu búsqueda.

```
sourcetype=access_combined status>=400  
| timechart count by useragent limit=5
```

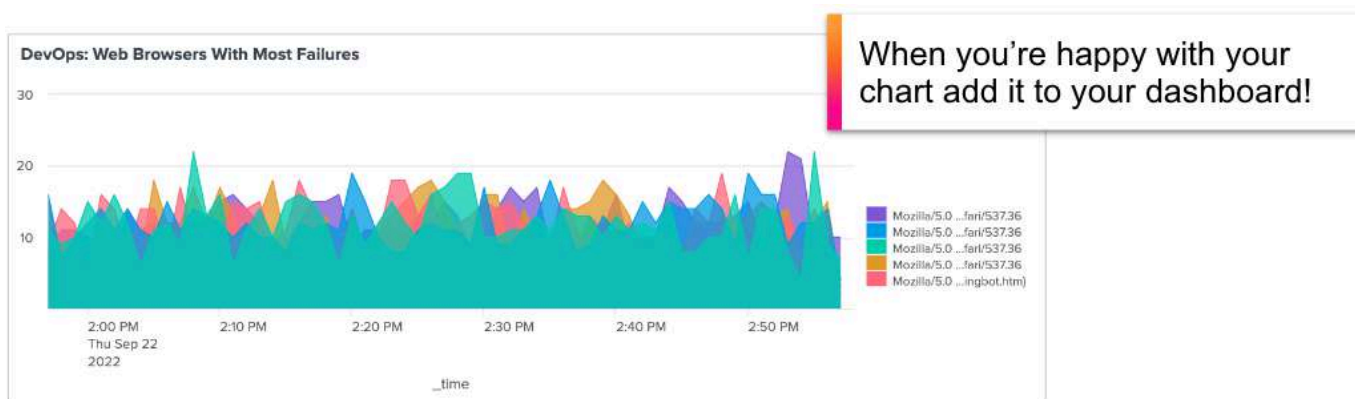
i Sugerencia para limpiar el gráfico

Puedes usar la opción `useother=f` con el comando `timechart` para quitar el valor OTHER de tu gráfico.

```
sourcetype=access_combined status>=400  
| timechart count by useragent limit=5 useother=f
```

Cuando estés satisfecho con el gráfico, añádelo a tu *dashboard* y ponle un título descriptivo al panel de visualización que acabas de crear, como **DevOps: Navegadores web con más errores**.

Nota: Recuerda añadir el panel a tu *dashboard* existente en lugar de crear uno nuevo.



Ejercicio 5: Equipos de Ventas/Análisis Empresarial. Mostrar Ingresos Perdidos a causa de Transacciones Fallidas del Sitio Web

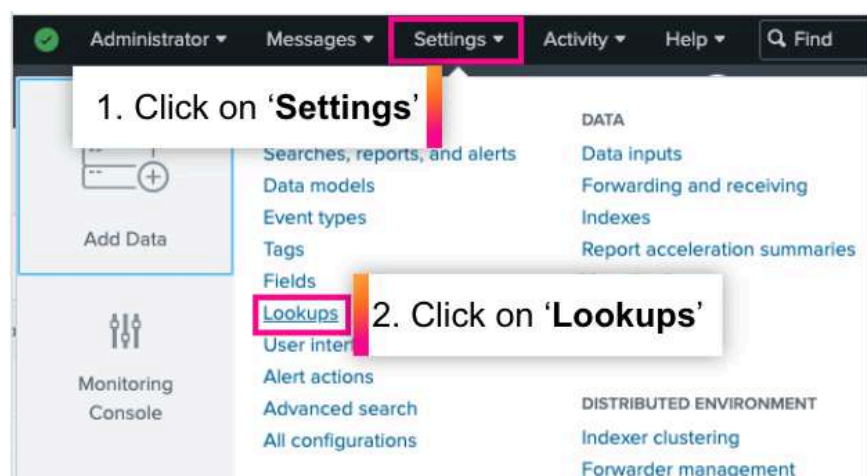
Descripción

Buttercup Enterprises no tiene forma de ver la pérdida de ingresos de su sitio web en tiempo real, y a los jefes ejecutivos les gustaría realizar un seguimiento de las tendencias de pérdida de ingresos en un *dashboard* durante el transcurso del día.

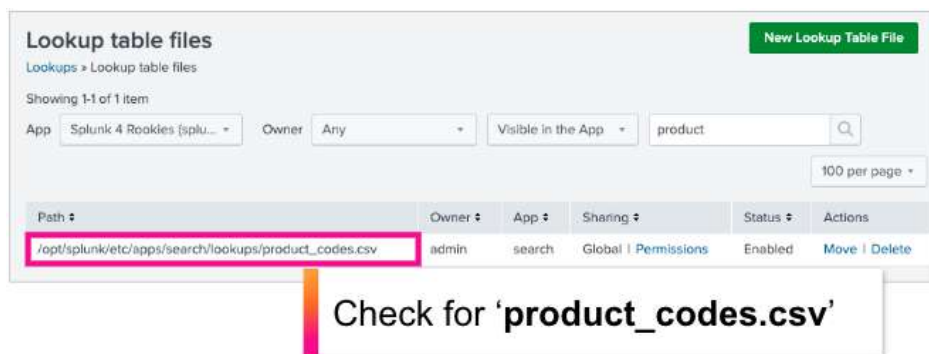
En este ejercicio, crearemos una visualización que muestre la pérdida de ingresos del sitio web de la compañía y la añadiremos a nuestro *dashboard*.

Pasos

1. Navega hasta **Settings > Lookups**.



2. Haz click en **Lookup table files** y comprueba que el archivo **product_codes.csv** existe en tu entorno.



3. Vuelve a tu aplicación y asegúrate de estar en la vista **Search**.



Para ver el contenido del archivo de búsqueda (lookup file) y familiarizarse con los campos y valores que contiene, usa el comando `inputlookup` y el nombre del archivo de búsqueda:

```
| inputlookup product_codes.csv
```

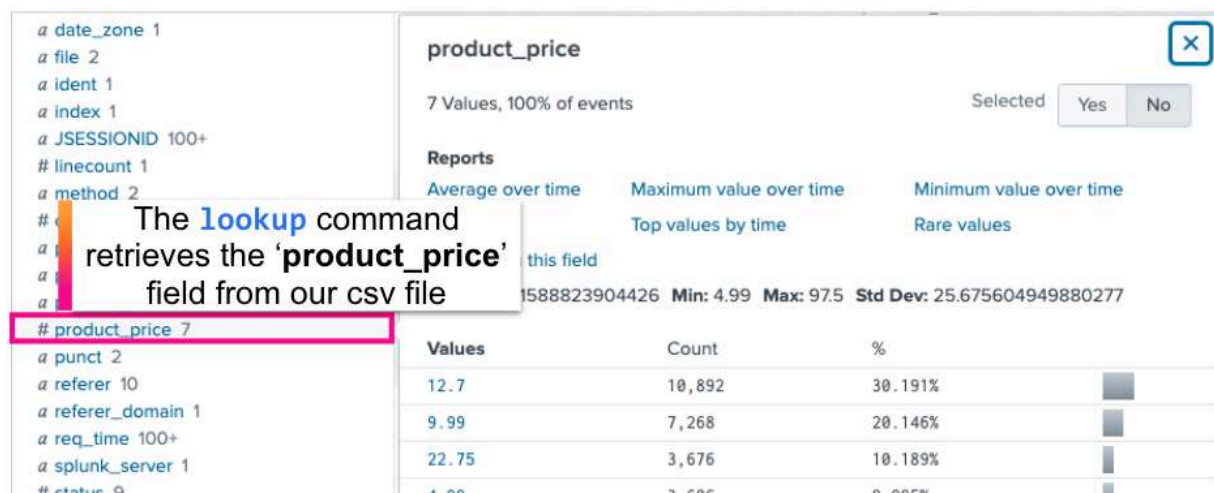
La tabla resultante debería tener este aspecto:

category	product_id	product_name	product_price
Clothing	BS-2	Batguy Slippers	25.7
Books	MCB-5	Mad Comics- Batguy	12.7
Books	MCB-6	Mad Comics- Bronze Man	12.7
Books	MCF-3	Mad Comics- Flyman	12.7
Books	ZSG-2	Zombie Survival Guide	15.21
Clothing	CM-1	Costume- ManHawk	97.5
Gifts	DFS-2	Double Fudge Sundae	22.75
Gifts	PP-5	Pony Potpourri	9.99
Clothing	BW-3	Batguy Watch	9.99
Gifts	WPSS-2	Waterproof Scratch and Sniff	4.99

4. Ahora que has comprobado que el archivo de búsqueda existe y le has echado un vistazo a su contenido, puedes usar el comando `lookup` para extraer el campo **product_price** del archivo y añadirlo a los eventos de compra del servidor web. Para ello, ejecuta la siguiente búsqueda con la opción **Last 60 minutes**:

```
sourcetype=access_combined action=purchase | lookup product_codes.csv product_id
```

Como podrás observar, el campo **product_price** aparece ahora debajo de los campos extraídos en el lateral izquierdo de la página. También se han añadido otros dos campos nuevos: «category» y «product_name».

A screenshot of the Splunk Search interface. On the left, the search bar contains the query: `a date_zone 1`, `a file 2`, `a ident 1`, `a index 1`, `a JSESSIONID 100+`, `# linecount 1`, `a method 2`, `# product_price 7`, `a punct 2`, `a referer 10`, `a referer_domain 1`, `a req_time 100+`, `a splunk_server 1`, `# status 9`. The `# product_price 7` line is highlighted with a red box. On the right, a panel titled 'product_price' shows '7 Values, 100% of events'. Below this, there are sections for 'Reports' (Average over time, Maximum value over time, Minimum value over time, Top values by time, Rare values) and a table of values. A callout box with a red border and a red arrow pointing to the `lookup` command in the search bar contains the text: 'The `lookup` command retrieves the 'product_price' field from our csv file'.

The `lookup` command retrieves the 'product_price' field from our csv file

Values	Count	%
12.7	10,892	30.191%
9.99	7,268	20.146%
22.75	3,676	10.189%
4.99	2,606	9.995%

Splunk ha extraído estos nuevos datos del archivo .csv que hemos especificado usando el campo **product_id**, y que ya existía en nuestros datos. ¡Ahora ya puedes usar estos campos adicionales en tus búsquedas!

5. A continuación, vamos a personalizar nuestra búsqueda para centrarnos en **los eventos de compra que han generado un error**, ya que estos son los eventos que nos interesan para calcular la pérdida de ingresos. Para ello, escribe una búsqueda que encuentre eventos cuyo estado sea **400** o superior (lo cual indica que se ha producido algún tipo de error).

```
sourcetype=access_combined action=purchase status>=400  
| lookup product_codes.csv product_id
```

6. Finalmente, necesitamos calcular la suma total de los valores del campo **product_price** para todos estos eventos de compra fallidos, **a lo largo del tiempo**. Para esto, usaremos el comando **timechart** con la función **sum**.

La función **sum** devuelve la suma de los valores de un campo, por lo que hay que proporcionar el nombre del campo que queremos usar. En este caso, el campo sería **product_price**, ya que la suma de los valores de este campo nos indicará cuántos ingresos hemos perdido en total.

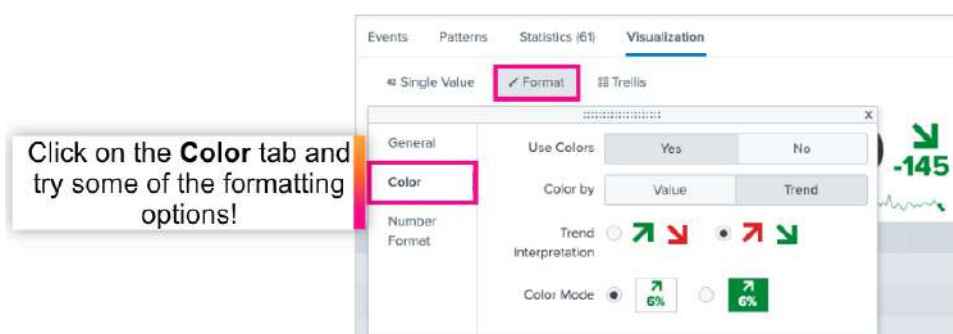
```
sourcetype=access_combined action=purchase status>=400  
| lookup product_codes.csv product_id  
| timechart sum(product_price)
```

¿Quieres obtener más información sobre SPL?

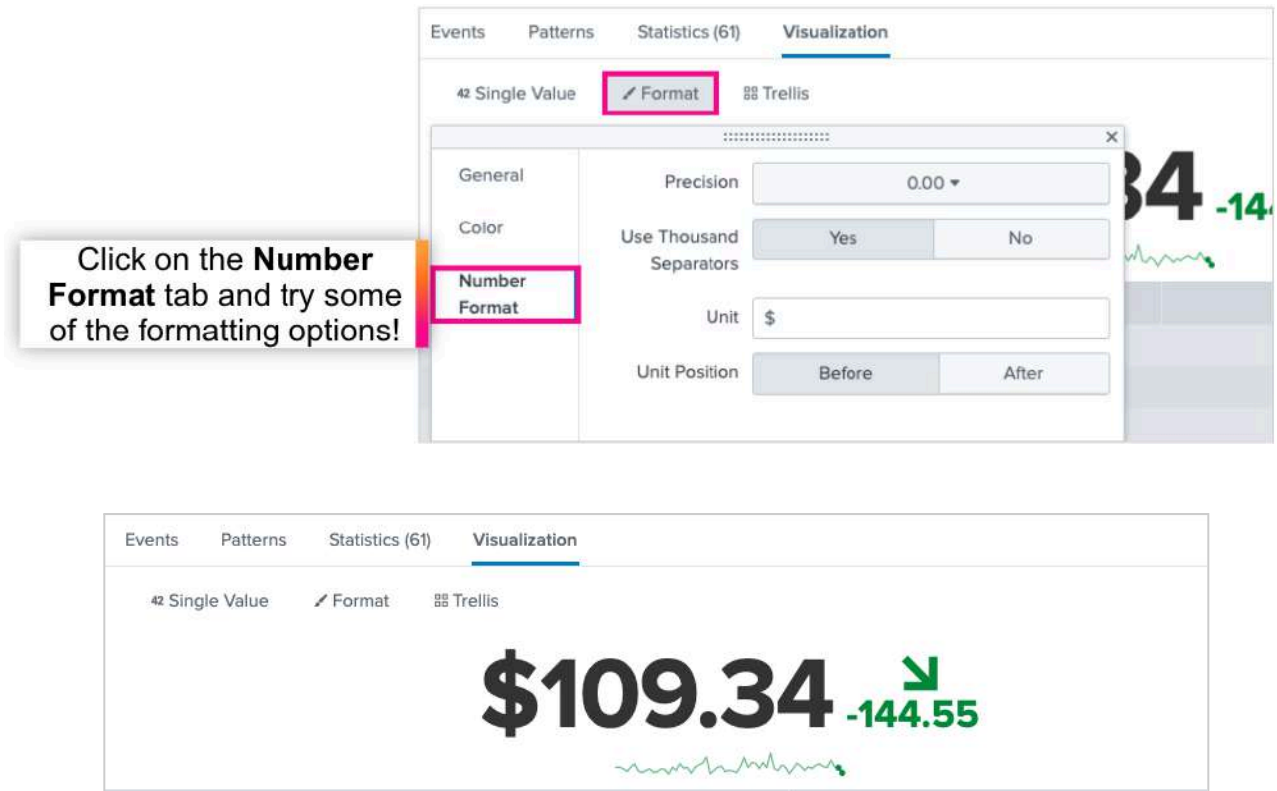
Consulta la página de documentación [Search Reference](#) de Splunk para obtener un catálogo de todos los comandos y funciones de búsqueda, así como información de sintaxis para cada uno, y descripciones y ejemplos de cómo usarlos.

7. Selecciona la pestaña **Visualization** si no está ya abierta y cambia la visualización a **Single Value**.

Haz click en **Format** y usa las pestañas laterales para cambiar las opciones de formato. ¡Intenta añadir un poco de color!



8. Haz click en **Number Format** y escribe un símbolo de unidad monetaria (£, \$ o €) para dejar claro que esta visualización representa un valor monetario. Una vez que estés satisfecho con la visualización, añádela a tu *dashboard* y ponle un título al nuevo panel que has creado, por ejemplo, **Análisis de negocios: Ingresos perdidos**.



Ejercicio 6: Equipos de Seguridad/Fraude. Mostrar la Actividad del Sitio Web por Ubicación Geográfica

Descripción

Buttercup Enterprises tiene su sede en los Estados Unidos, y existe la preocupación de que pueda haber transacciones probablemente fraudulentas provenientes de otros países. Sin embargo, actualmente, el equipo de seguridad no tiene ninguna información sobre el origen (geográfico) del tráfico que pasa por el sitio web.

En este ejercicio, vamos a crear una visualización **Cluster Map**, que muestre la ubicación geográfica de cualquier persona que se haya conectado al sitio web de Buttercup Enterprises.

Pasos

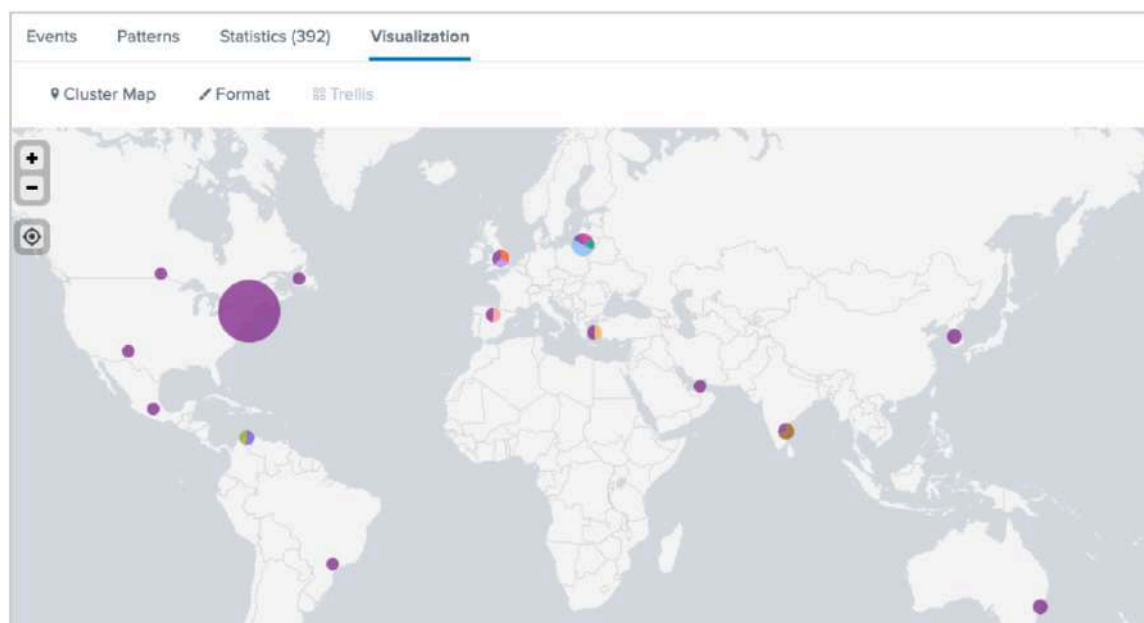
1. Primero, busca todos los eventos del servidor web y usa los comandos `iplocation` y `geostats` para contar los eventos por **City** (ciudad).

(Nota: «City» es uno de los campos en nuestros datos que se crea cuando usamos el comando `iplocation`):

```
sourcetype=access_combined | iplocation clientip | geostats count by City
```

2. Si no está abierta todavía, haz click en la pestaña **Visualization**. Elige el tipo de visualización **Cluster Map**.

Deberías tener un mapa que muestra la ubicación de los clientes que se conectan al sitio web de la compañía semejante a este:



No olvides guardar el mapa en tu *dashboard* y ponerle un nombre descriptivo al panel, por ejemplo, **Seguridad/Fraude: Ubicaciones de clientes**.

Ejercicios de Desafío

El mapa que hemos generado incluye la geolocalización de todos los clientes que visitan la página web de nuestra empresa; pero, dado que Buttercup Enterprises es una compañía con sede en los EE. UU., es posible que el equipo de seguridad sólo esté interesado en ver a los clientes que NO se encuentran en los EE. UU.

P1. ¿Cómo actualizarías tu búsqueda para quitar los eventos con origen en **Estados Unidos** de tu mapa?

Sugerencias:

- La primera parte de cada búsqueda de Splunk incluye un comando implícito [search](#), por lo que no necesitamos usar un comando [search](#) al principio de nuestras búsquedas. Sin embargo, en Splunk, si queremos usar un filtro de búsqueda después de que se haya usado una barra vertical (" | "), por ejemplo, para filtrar ciertos resultados, deberemos especificar el comando [search](#) en alguna parte de nuestra búsqueda (es decir, | [search](#) <search terms>).

Nota: Recuerda que, al buscar, si queremos usar un campo para filtrar nuestros resultados, debemos asegurarnos de que el campo existe en los eventos de nuestra búsqueda. Como hemos visto hoy, algunos comandos añadirán o quitarán campos a medida que Splunk va avanzando por nuestra búsqueda. Mira los comandos que estás usando y recuerda qué campos puedes añadir o quitar de tus eventos.

✓ Soluciones de los ejercicios de desafío

Las soluciones de los ejercicios de desafío se encuentran al [final de este documento](#).

Ejercicio 7: Personalizar tu *Dashboard*

Descripción

Tener un *dashboard* con varios paneles es increíblemente útil, pero el diseño del *dashboard* también es muy importante para garantizar que la información incluida en los paneles sea fácil de ver y entender para todos los usuarios.

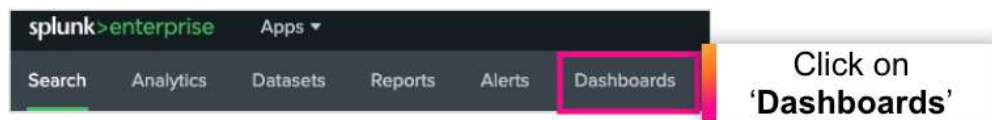
El equipo de marketing de Buttercup Enterprises ha visto lo que hemos creado hasta ahora y nos ha proporcionado una imagen de fondo personalizada que les gustaría que usáramos en nuestro nuevo *dashboard*. En este ejercicio, usaremos la imagen de fondo personalizada y reorganizaremos nuestros paneles para que queden bien con el nuevo fondo. Finalmente, configuraremos cada uno de los paneles para que usen el selector de tiempo global.

¡Una vez hecho esto, podremos compartir nuestro *dashboard* con el resto de la compañía!

Pasos

Añadir una imagen de fondo a tu *dashboard*

1. Primero, abre el *dashboard*. Para ello, haz click en **Dashboards** en el menú superior.



2. Haz click en el nombre de tu *dashboard* para abrirlo.

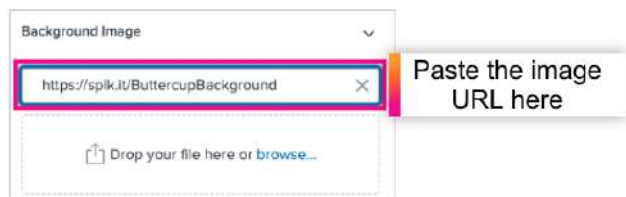


3. Haz click en el botón **Edit** para abrirlo en el editor de *dashboards*



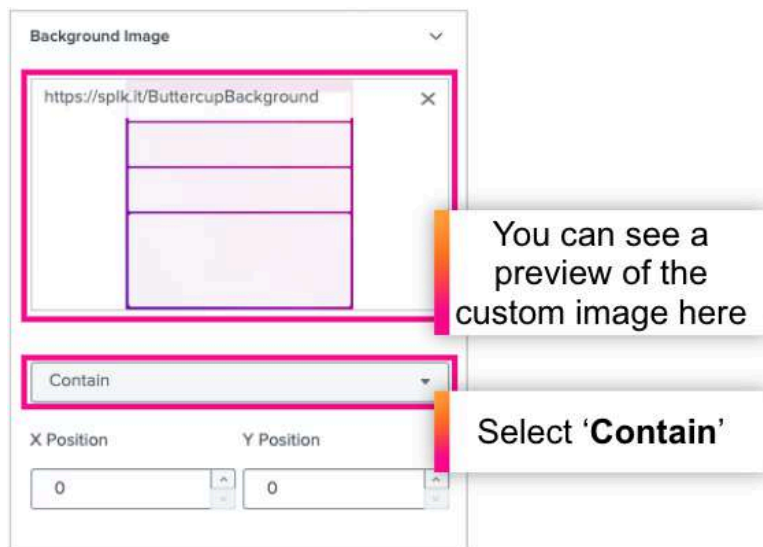
4. Busca la sección **Background Image** en la página de configuración del *dashboard* y copia & pega la siguiente dirección en el cuadro **Enter URL**:

<https://splk.it/ButtercupBackground>



Para usar la imagen, presiona la tecla Intro en tu teclado o haz click en cualquier parte del *dashboard*.

Para asegurarnos de que la imagen personalizada está dentro de las dimensiones de nuestro *dashboard*, haz click en la lista desplegable debajo de la vista previa de la imagen y selecciona **Contain**.



5. Haz click en cada panel y arrastra los cuadrados azules que se muestran alrededor de los bordes para cambiar el tamaño y ajustarlos a las

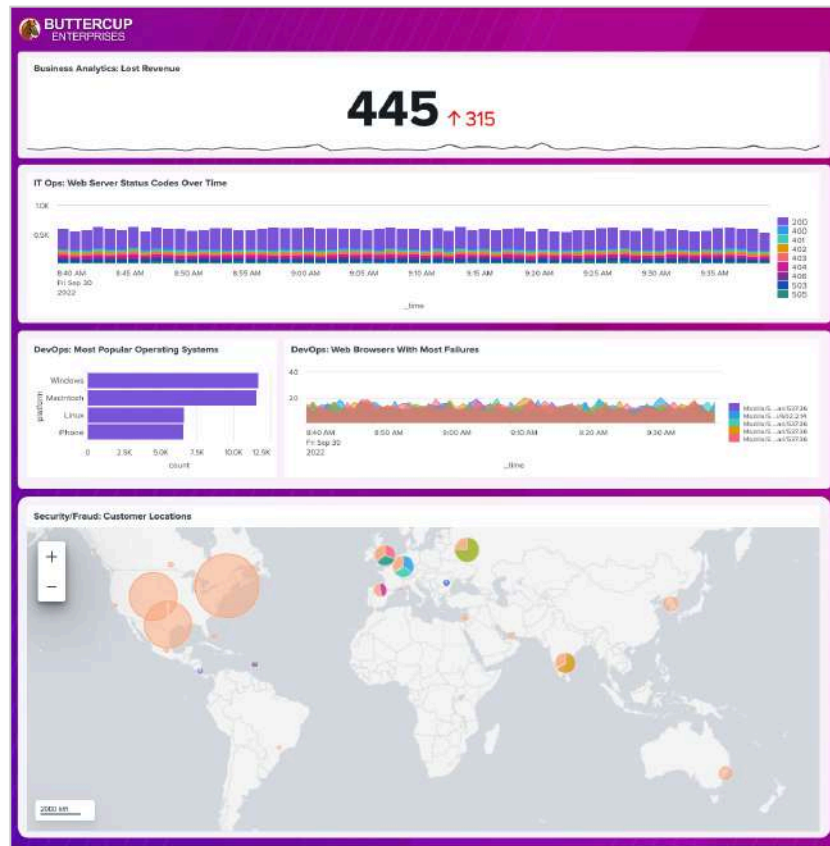


áreas rectangulares de la imagen de fondo.



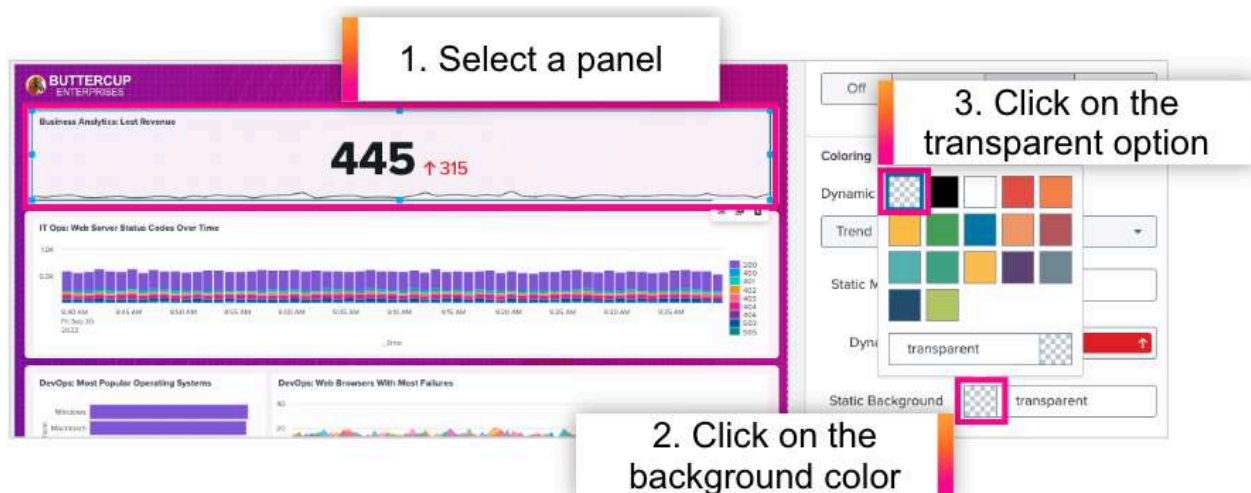
Asegúrate de hacer click en **Save** cuando hayas terminado de reorganizar todos los paneles.

Cuando hayas terminado, el *dashboard* debería tener un aspecto parecido a este:

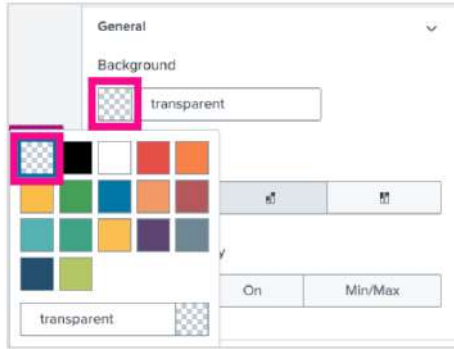


6. Por último, dado que tenemos un fondo de color agradable, vamos a configurar los paneles para que sean transparentes y desataque más el color del fondo. Para hacer esto, haz click en un panel y, en la ventana «Configuration» de la derecha, busca la sección **Coloring**.

Busca la opción **Background** o **Static Background** (el nombre variará de una visualización a otra) y cambia el color de fondo para que sea transparente. Repite este paso para cada panel. Ten en cuenta que la visualización «Cluster Map» no tiene una opción de color de fondo, por lo que puedes omitir este panel.



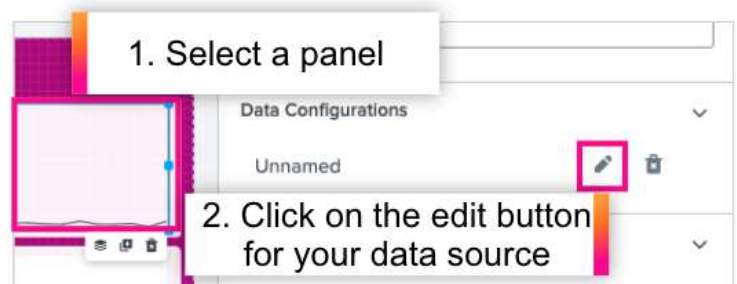
Nota: Algunas visualizaciones pueden tener un nombre ligeramente distinto para la configuración del color de fondo, por ejemplo:



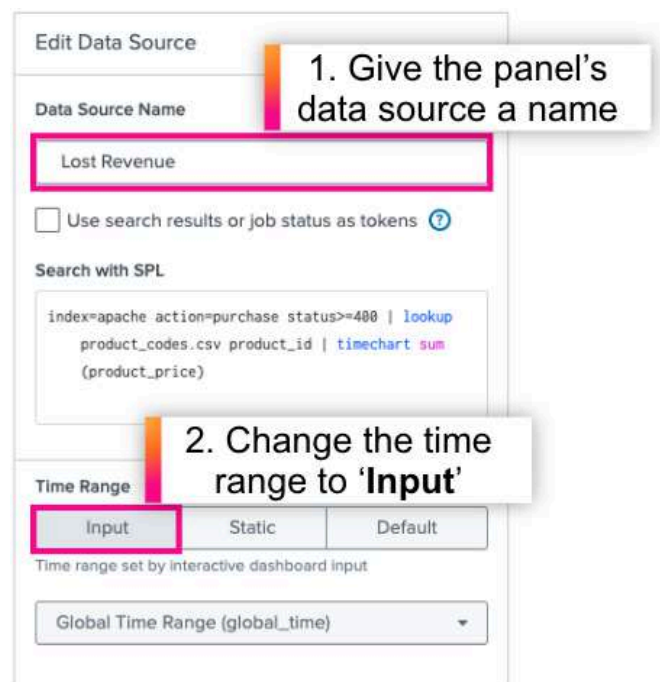
Conectar los paneles al selector de tiempo global

El selector de tiempo global se incluye en todos los *dashboards* nuevos por defecto, y permite al usuario controlar el periodo de tiempo que usan las búsquedas de los paneles. Dado que cada uno de nuestros paneles usaba un periodo de tiempo estático (es decir, **Last 60 minutes**) cuando los añadimos a nuestro *dashboard*, solo tenemos que cambiar cada panel para que use el selector de tiempo global del *dashboard*.

1. Haz click en un panel y, en la ventana «Configuration» de la derecha, busca la sección **Data Configurations**. Haz click en el icono del lápiz para editar la fuente de datos **Unnamed**.

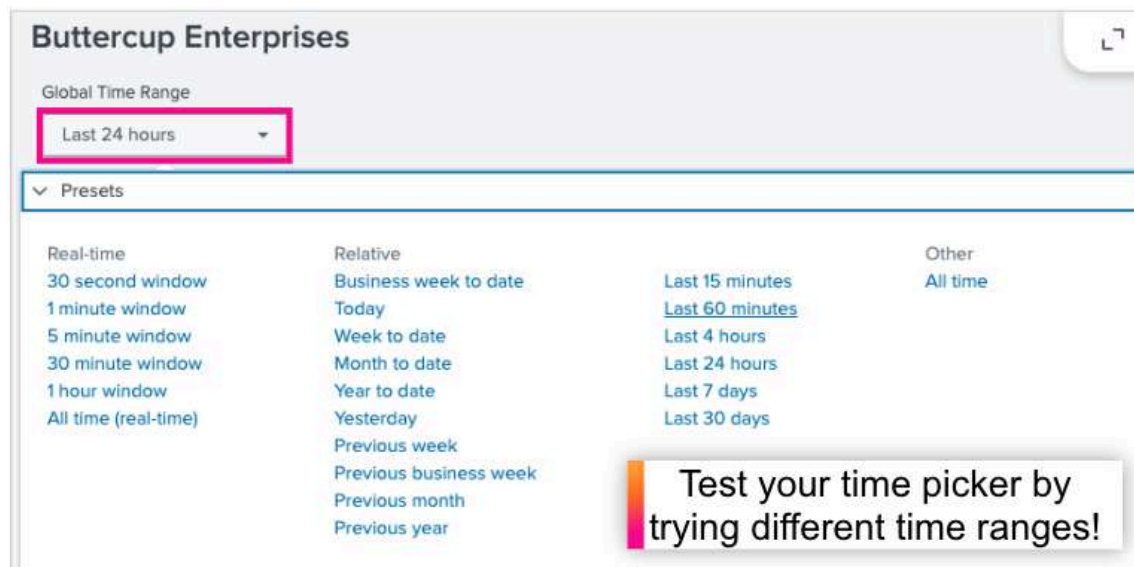


2. Para realizar cambios a las fuentes de datos, primero es necesario darle un nombre a cada una. Usa el nombre de cada panel. Por ejemplo, para la visualización Single Value, usa «Lost Revenue» como nombre de la fuente de datos.



3. Haz click en **Apply & Close** para guardar los cambios. Repite este paso para cada panel y luego, guarda tu *dashboard*.

Ahora que hemos conectado todos los paneles al selector de tiempo global, haz click en **Save** y luego haz click en **View** para ver tu *dashboard* actualizado. Intenta cambiar el periodo de tiempo de búsqueda de tu *dashboard* seleccionando distintas opciones de tiempo de la lista desplegable. Todos los paneles deberían actualizarse y reflejar la nueva configuración de tiempo.



Soluciones de los Ejercicios de Desafío

Las soluciones para los ejercicios de desafío están incluidas a continuación. Si tu solución no es exactamente igual: ¡no te preocupes, ya que suelen haber varias formas de conseguir los resultados correctos!

Comenzar a Buscar en Splunk

- P1. ¿Cómo podemos encontrar eventos con el estado **200** que no sean eventos de compra?

Solución:

```
status=200 action!=purchase
```

 **NOT vs =**

`status=200 NOT action=purchase` también funcionaría, pero no es la manera más eficiente de realizar esta búsqueda debido a la forma en que funciona el operador **NOT**. Si estás interesado en saber por qué, consulta <https://docs.splunk.com/Documentation/Splunk/latest/Search/NOTexpressions> para obtener una explicación completa de las diferencias entre estos dos métodos.

- P2. ¿Cómo podemos encontrar eventos en los que alguien ha recibido un error al intentar añadir o quitar un artículo de su carrito?

Solución:

```
sourcetype=access_combined status>=400 (action=addtocart OR action=remove)
```

Equipos de Seguridad/Fraude. Mostrar cualquier Actividad en el Sitio Web con Origen fuera de los Estados Unidos

- P1. ¿Cómo quitarías los eventos con origen en **Estados Unidos** de tu mapa?

Solución:

```
sourcetype=access_combined | iplocation clientip  
| search Country!="United States" | geostats count by City
```