



Laboratorio 4.1

Splunk para analizar
logs

Ing. Alex Araya Rojas, MT
CISSP, CISM

Febrero 2022

Lab 4.1

Splunk para analizar logs

01

Descargar el instalador

02

Procedimiento

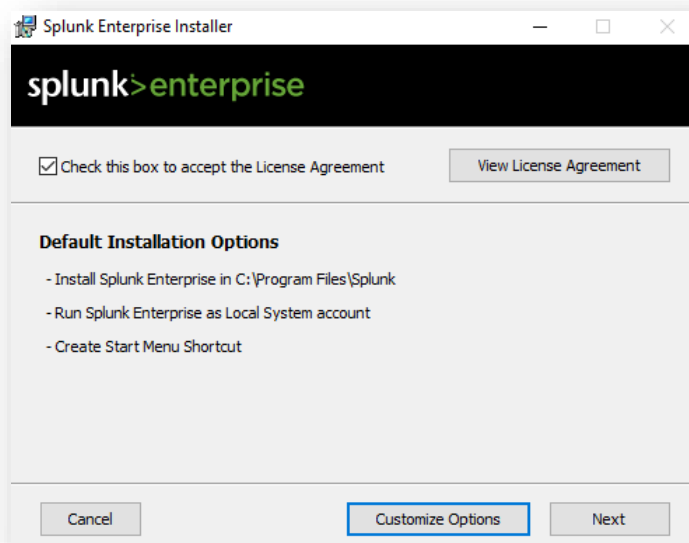
Procedimiento

Descargar el instalador

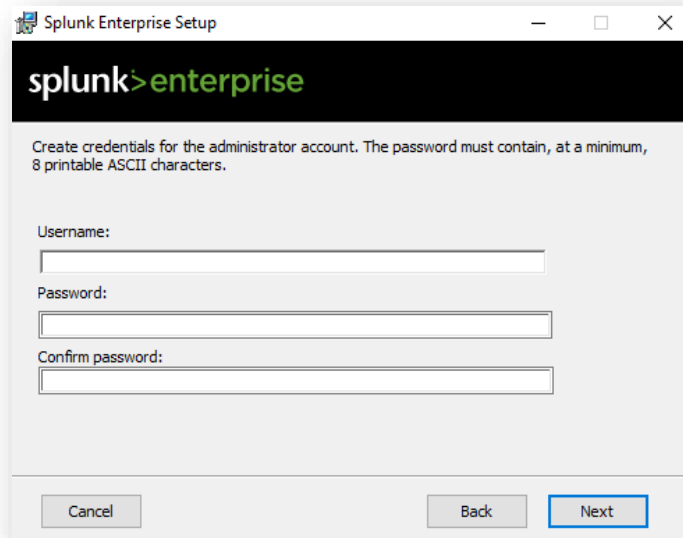
01. Es recomendable que realice estas pruebas en un equipo virtual para no comprometer la seguridad de su equipo de cómputo.
02. En el laboratorio 3.1 se le había solicitado descargar una imagen de Windows 10, verifique que tiene el ISO para realizar una instalación limpia en una máquina virtual.
03. Si no cuenta con el software para instalar máquinas virtuales, puede descargar VMware Player en la carpeta de herramientas del Teams del curso Forense.
04. Una vez que cuente con la máquina virtual de Windows 10, pegue en el escritorio de este equipo el instalador de Splunk, que podrá encontrar en la carpeta de Teams del curso.

Procedimiento

01. Para iniciar el proceso de instalación haga doble click en el instalador y siga los pasos de esta guía, marque el check para indicar que está de acuerdo con los términos de la licencia y presione Next.

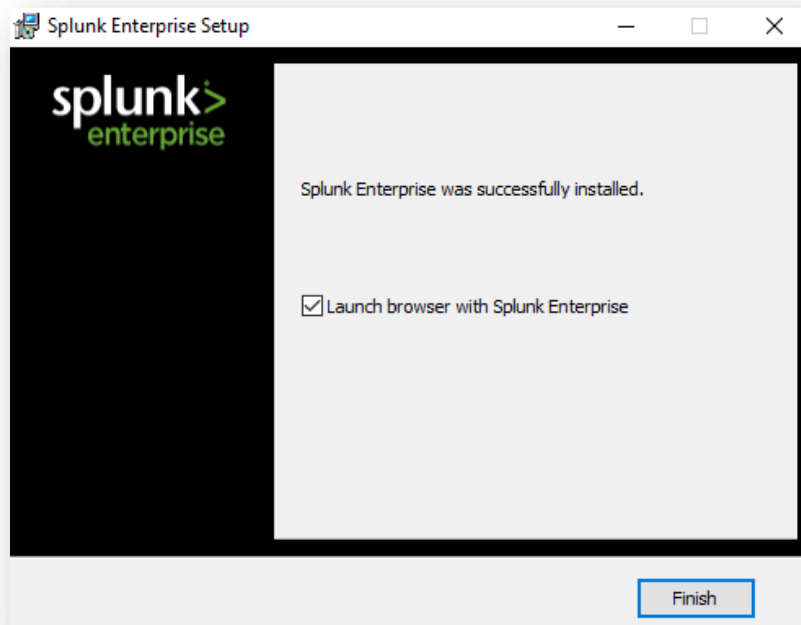


02. Complete los datos solicitados, NO OLVIDE estos valores sino deberá reinstalar la herramienta, presione Next para continuar con la instalación.



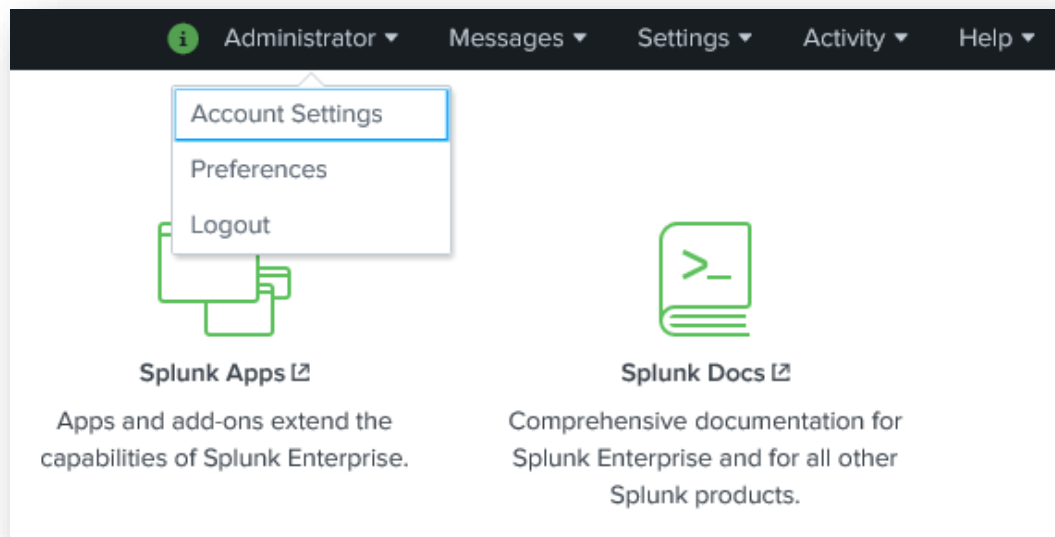
The screenshot shows the 'Splunk Enterprise Setup' window. The title bar includes the application icon and the text 'Splunk Enterprise Setup'. The main content area has a black header with the 'splunk>enterprise' logo. Below the header, a message states: 'Create credentials for the administrator account. The password must contain, at a minimum, 8 printable ASCII characters.' There are three input fields: 'Username:', 'Password:', and 'Confirm password:'. At the bottom, there are three buttons: 'Cancel', 'Back', and 'Next'.

03. Una vez finalizado el proceso de instalación, presione el botón Finish. Marque el check para iniciar la consola inmediatamente finalizado el proceso.



The screenshot shows the 'Splunk Enterprise Setup' window at the completion stage. The title bar is the same. The main content area has a black header with the 'splunk>enterprise' logo. The text 'Splunk Enterprise was successfully installed.' is displayed. Below this, there is a checkbox labeled 'Launch browser with Splunk Enterprise', which is currently checked. At the bottom right, there is a 'Finish' button.

04. La dirección que podrá utilizar de ahora en adelante para ingresar al Splunk en esta máquina virtual es <http://127.0.0.1:8000>
05. Siempre es importante conocer que podemos ingresar a este servidor desde otro equipo siempre y cuando haya conectividad, reemplazando la dirección IP por la asignada al servidor en la red.
06. Esta instancia de Splunk puede ser utilizada por varias personas simultáneamente, razón por la cual es importante configurar algunos elementos generales. En primera instancia temas de reloj, ingrese a Preferencias y Modifique la zona horaria del usuario a GMT -06:00



07. En el punto anterior, es importante marcar la opción de reinicio de los Jobs en background, para que tomen en cuenta la nueva configuración de la hora.
08. Configuremos ahora otros parámetros del servidor, ingrese al menú Settings – Server Settings, luego vaya a General Settings y en esta ventana podrá cambiar desde los puertos del splunk (por default es 8000), la forma de acceso (HTTP o HTTPS), timeout de las sesiones, entre otros elementos. Realice los cambios necesarios para ajustar la herramientas a las necesidades actuales.
09. Inclusive puede cambiar el fondo de la ventana de inicio de sesión.


Login page background

☐ No image

☒ Default image

☐ Custom image

Preview



Click image for full-screen preview.

Supported image files are .jpg, .jpeg or .png, with a recommended resolution of 1024x640.

10. Una de las configuraciones más importantes es la del EMAIL, ya que esta será la forma en la que el splunk nos advertirá primariamente sobre situaciones que ameritan nuestra atención.
11. Configure una nueva cuenta en Gmail para este ejercicio, marque en las opciones de seguridad de esta nueva cuenta que se permitan aplicaciones inseguras para permitir que desde el servidor de splunk se pueda utilizar la cuenta de Gmail para enviar correos electrónicos.

Mail Server Settings

Mail host
Set the host that sends mail for this Splunk instance.

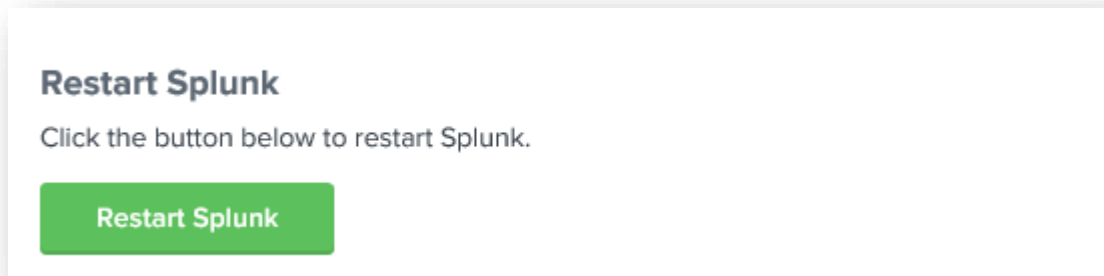
Email security ☐ none ☐ Enable SSL ☒ Enable TLS
Check with SMTP server admin. When SSL is enabled, mail host should include the port. IE: smtp.splunk.com:465

Username
Username to use when authenticating with the SMTP server. Leave empty for no authentication.

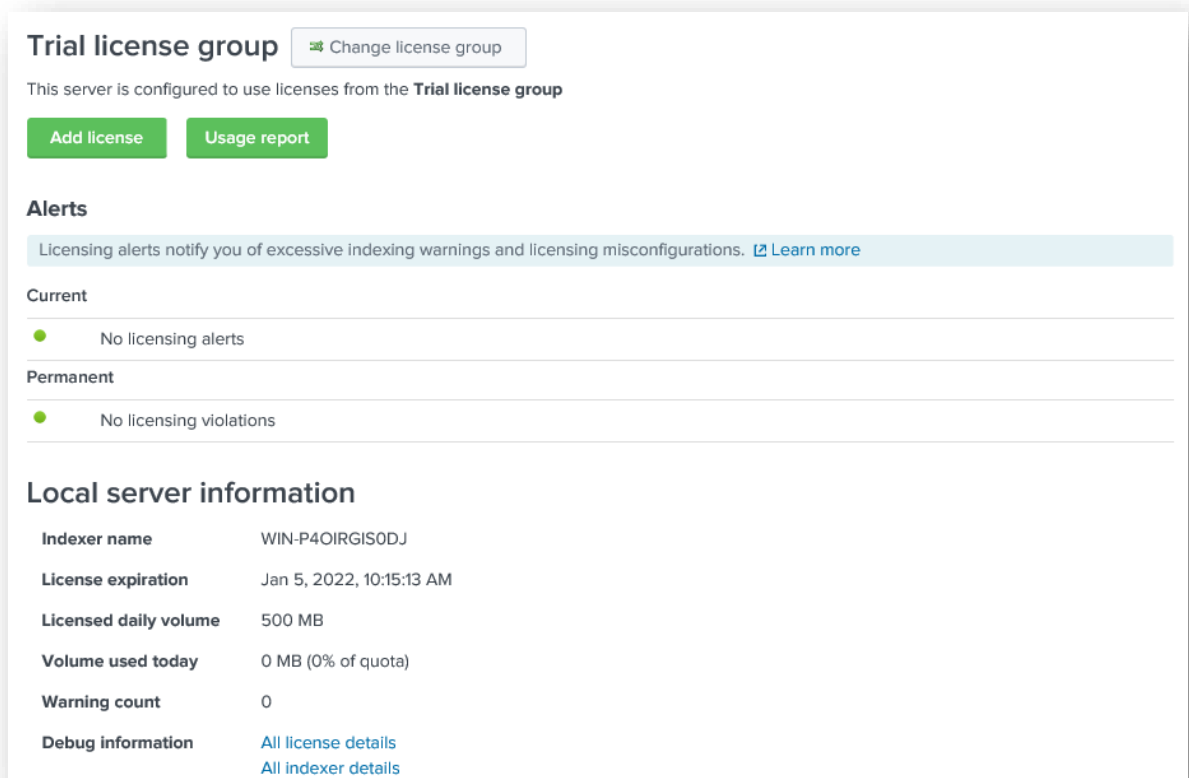
Password
Password to use when authenticating with the SMTP server.

Confirm password

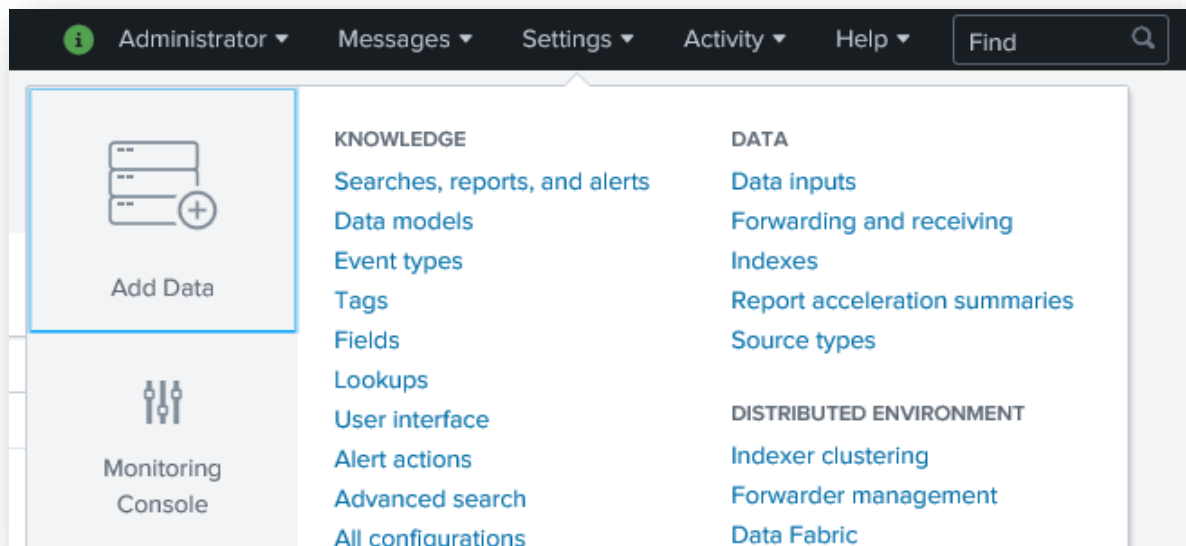
12. Si por alguna razón es necesario reiniciar el servidor de splunk, en Settings – Server Control encontrará una opción para hacerlo.



13. Las versiones gratuitas de splunk le permiten procesar diariamente hasta 500 MB de logs, suficiente para la mayoría de las investigaciones. Para gestionar el tema de la licencia puede ingresar a Settings – Licensing



14. Splunk se alimenta de fuentes de datos, que pueden ser muy diversas, vamos a agregar el registro de eventos del Windows 10 para aprender a buscar registros de interés. Presione Settings y busque la opción ADD DATA



15. Busque el botón verde llamado Monitor, este nos permitirá monitorear nuestro propio servidor de splunk.



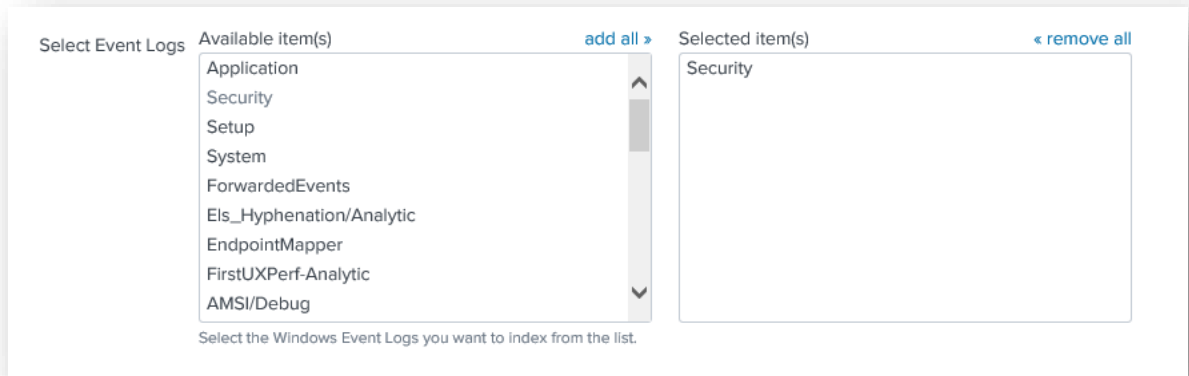
Monitor

files and ports on this Splunk platform instance

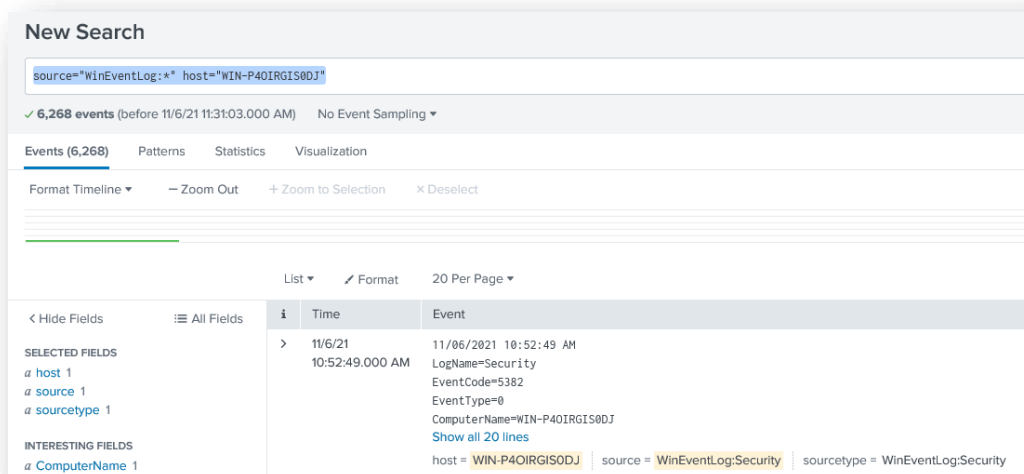
Files - HTTP - WMI - TCP/UDP - Scripts

Modular inputs for external data sources

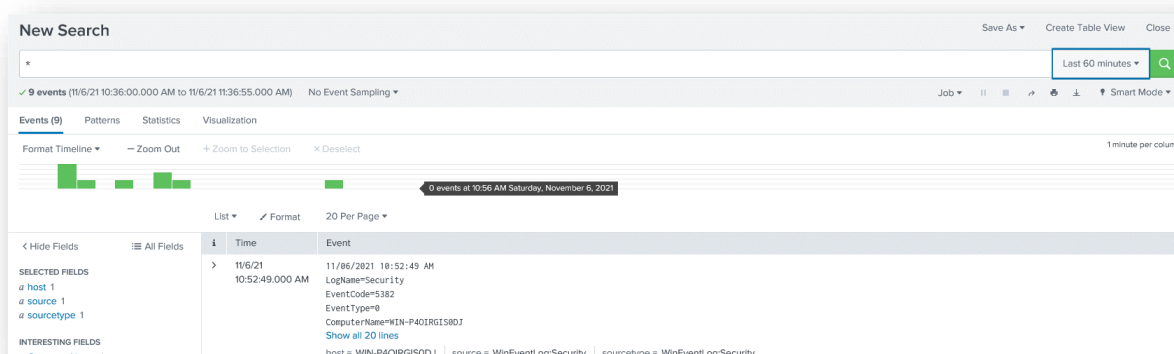
16. Seleccione la opción llamada Local Event Logs, esto nos permitirá agregar los eventos del Windows local.



17. Seleccione los logs de seguridad y presione Next y vaya analizando las pantallas hasta que el sistema le de la opción de empezar a buscar (Start Searching) y lo lleve a la consola de búsqueda.
18. Una vez en la consola de búsqueda, podrá visualizar los elementos contenidos en el log de seguridad de Windows, borre el filtro actual y escriba un “ * “, anote cuántos eventos están siendo mostrados.
19. Cierre la sesión del Windows, intente hacer inicio de sesión con credenciales fallidas unas 3 veces y luego proceda a ingresar con las credenciales válidas.
20. En la barra de búsqueda escriba un “ * ” y presione enter, compare la cantidad de eventos del punto 18 con los actuales, debería tener algunas más!!
21. Edite nuevamente el string de búsqueda y escriba 4625 par visualizar inicios de sesión con credenciales erróneas, sino aparecen, deberá dar unos minutos para que el servidor termine su proceso de indexado inicial.

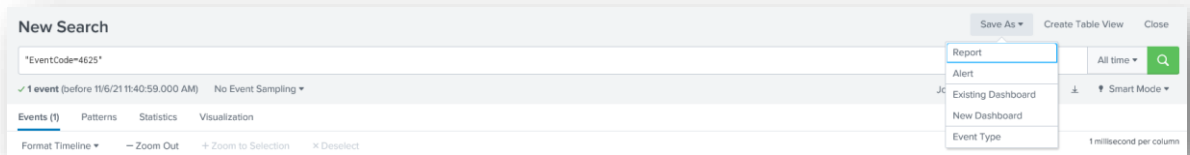


22. Juegue con la barra de tiempo, puede hacer drill down para acercarse y ver los eventos inclusive por segundo. Puede cambiar el indicador de tiempo de All Time a su gusto.



23. A la hora de aplicar filtros de búsqueda, debe ser cuidado ya que por ejemplo, una búsqueda con el texto 4625 le traerá a todos aquellos registros que tengan dicha cadena de texto, ahora, para ser más preciosos, si queremos SOLAMENTE los eventos de falla de autenticación de Windows, deberá escribir por ejemplo: "EventCode=4625" aplique este filtro!!

24. Sería interesante guardar esta búsqueda y que nos empiece a generar notificaciones cuando se presenten más de 2 intentos fallidos de autenticación en menos de 1 minuto, presione Save As – Alert



25. Vaya con cuidado en este proceso, es fácil equivocarse, tenga cuidado con el parámetro Throttle, si tiene dudas de este, pregunte al instructor en los espacios de aclaración de dudas!!

Save As Alert

Settings

Title

Login Fallidos

Description

Optional

Permissions

Private

Shared in App

Alert type

Scheduled

Real-time

Expires

24

hour(s)

Trigger Conditions

Trigger alert when

Number of Results

is greater than

1

in

1

minute(s)

Trigger

Once

For each result

Throttle

☐

26. El Throttle por ejemplo evita que se generen nuevas alertas en un periodo de tiempo posterior a la generación de otra alerta. Esta configuración mostrada por ejemplo, evita que se generen nuevas alertas por 10 segundos una vez generado una alerta!!

Throttle ? ☒

Suppress results containing field value

Suppress triggering for

27. Veamos ahora la sección de acciones de la alerta, presione el botón Add Actions y agregue la notificación por email y a los eventos generados. Presione salvar, cierre el diálogo y haga nuevas pruebas de inicio de sesión fallidos.

+ Add Actions ▼

When triggered ▼

✉ Send email Remove

To

Comma separated list of email addresses.
[Show CC and BCC](#)

Priority

Subject

The email subject, recipients and message can include tokens that insert text based on the results of the search. [Learn More](#)

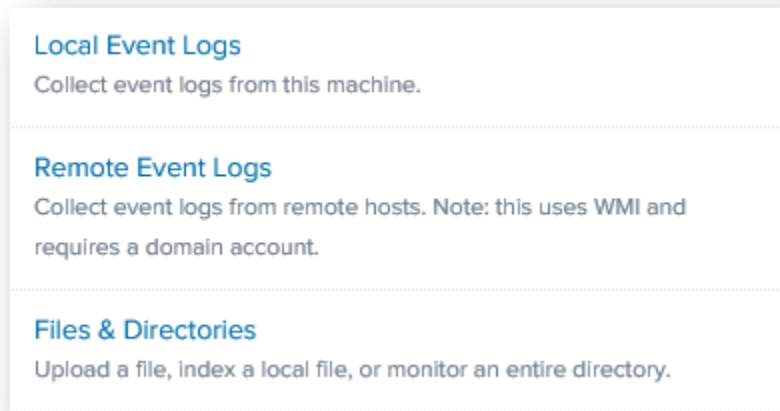
Message

Include ☒ Link to Alert ☒ Link to Results
☐ Search String ☒ Inline [Table ▼](#)
☐ Trigger Condition ☐ Attach CSV

28. Espero que la prueba haya funcionado, si no, revise los pasos o lo validamos en los espacios de aclaración de dudas!!

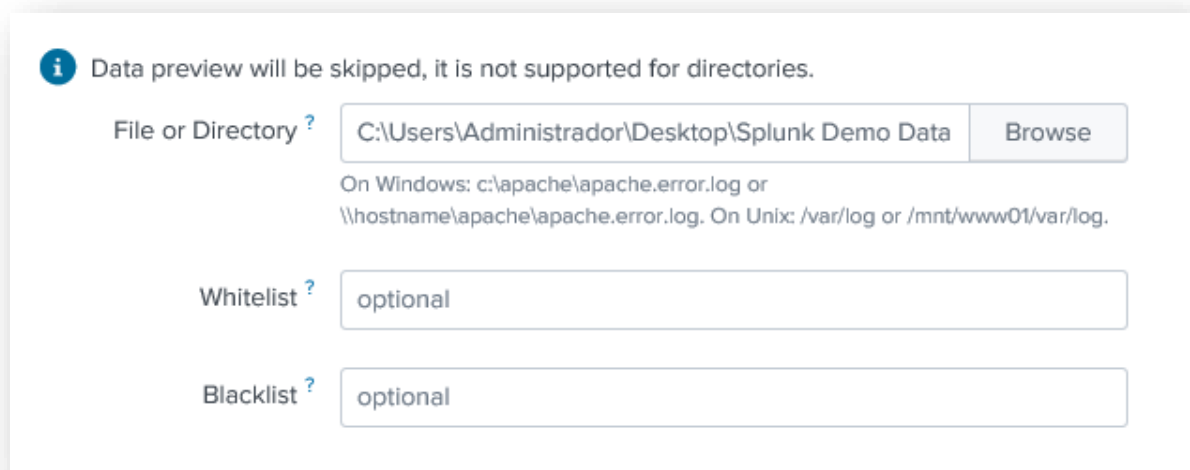
29. En la carpeta donde descargó este lab, existen dos archivos, descárguelos y cópielos a una carpeta en la máquina virtual, por ejemplo en C:\datos

30. Con splunk podemos dejar una carpeta en monitoreo, es muy útil para dejar caer archivos de logs de otras plataformas o ambientes donde existan múltiples investigadores y todos depositen ahí los logs.
31. Vamos a Settings – Add data, usando la opción de Monitor vamos a seleccionar Files & Directories



The screenshot shows a dialog box titled 'Add Data' with three sections separated by horizontal lines. The first section is 'Local Event Logs' with the description 'Collect event logs from this machine.' The second section is 'Remote Event Logs' with the description 'Collect event logs from remote hosts. Note: this uses WMI and requires a domain account.' The third section is 'Files & Directories' with the description 'Upload a file, index a local file, or monitor an entire directory.'

32. Ubicamos el directorio donde habíamos copiado los archivos y presionamos next. Cambie el Host Field Value a Directorio y finalice el proceso para iniciar con las búsquedas.



The screenshot shows the 'Files & Directories' section of the 'Add Data' dialog. At the top, there is an information icon and a message: 'Data preview will be skipped, it is not supported for directories.' Below this, there is a 'File or Directory' label with a question mark, followed by a text input field containing 'C:\Users\Administrador\Desktop\Splunk Demo Data' and a 'Browse' button. Below the text input, there is a note: 'On Windows: c:\apache\apache.error.log or \\hostname\apache\apache.error.log. On Unix: /var/log or /mnt/www01/var/log.' Below this, there are two more input fields: 'Whitelist' and 'Blacklist', both with question marks and the word 'optional' inside the input field.

33. Asd

34. Vaya al string de búsqueda y filtros, escriba un “ * “ y revise si la cantidad de eventos creció. Normalmente este proceso agregará más de 100k eventos, procesados en segundos!!!!

35. Responda las siguientes preguntas:

- a. Cuántos eventos se generaron el 09 de febrero del 2022?
- b. A qué hora se presentó la mayor generación de eventos el 09 de febrero del 2022?