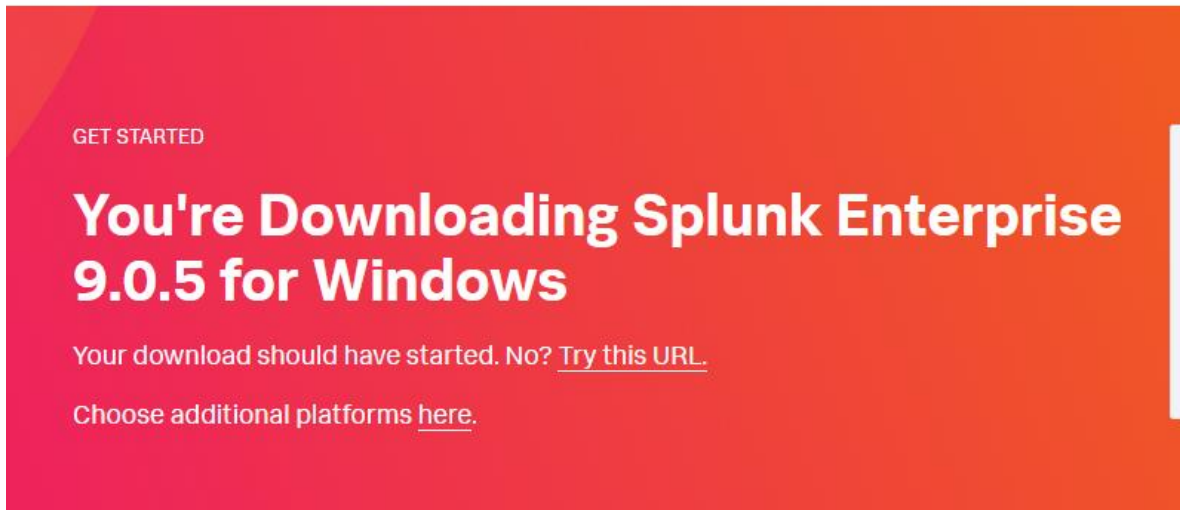


Laboratorio 4.1

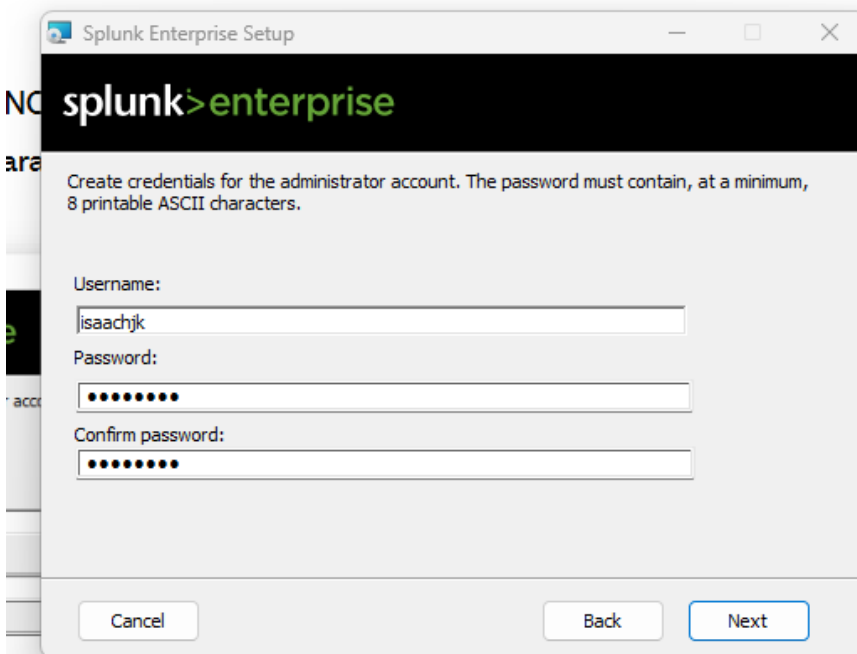
Estudiante: Isaac Vásquez Valenciano

Cedula: 1-1711-0637

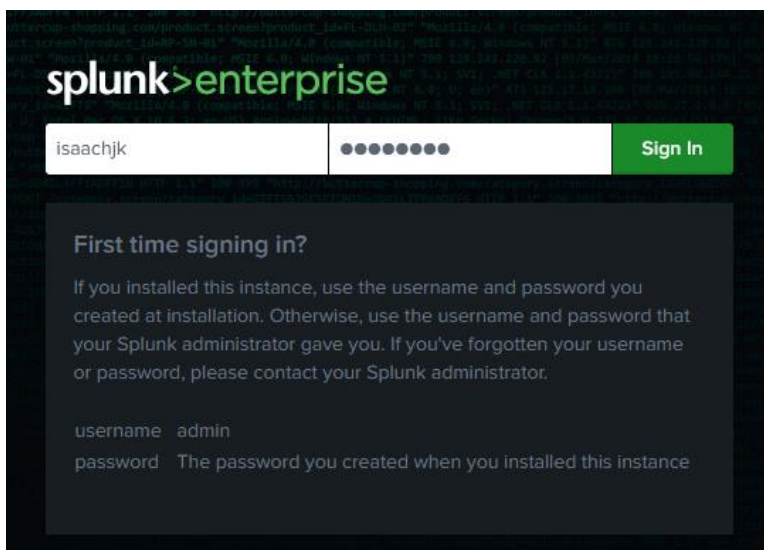
Descargamos Splunk



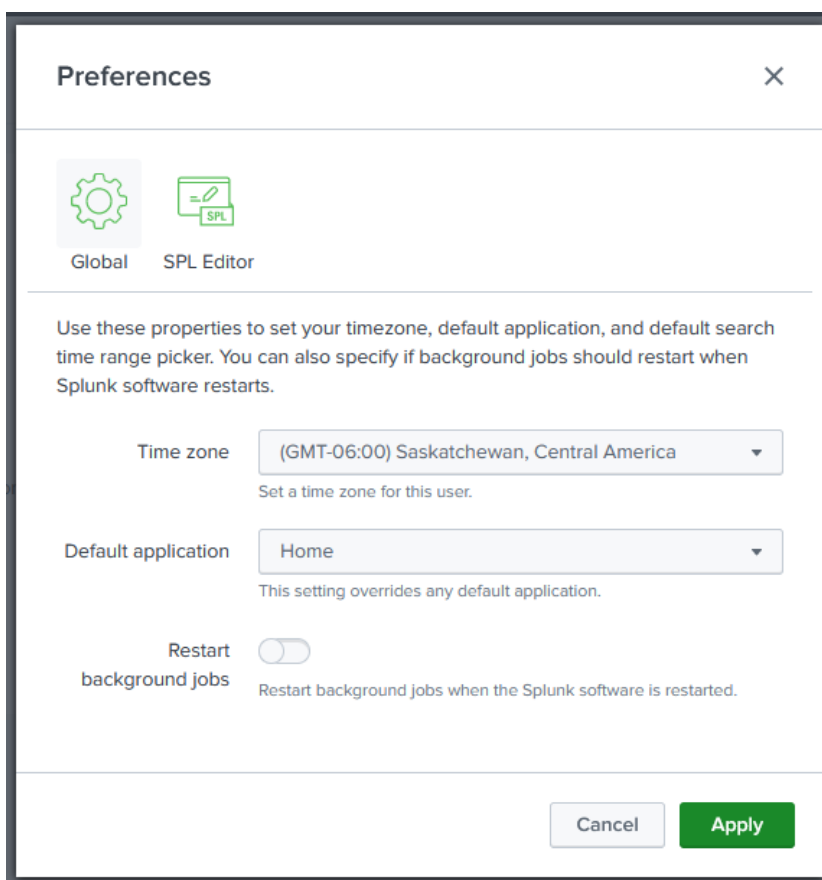
Configuramos el usuario y password



Se accede a la herramienta web en 127.0.0.1:8080



Se modifica la zona horaria



Se configura el email

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

Se procede en agregar events logs de security

Add Data ● ○ ○ ○ < Back Next >

Select Source Input Settings Review Done

Local Event Logs
Collect event logs from this machine.

Remote Event Logs
Collect event logs from remote hosts. Note: this uses WMI and requires a domain account.

Files & Directories
Upload a file, index a local file, or monitor an entire directory.

HTTP Event Collector
Configure tokens that clients can use to send data over HTTP or HTTPS.

TCP / UDP
Configure the Splunk platform to listen on a network port.

Local Performance Monitoring

Configure this instance to monitor local Windows Event Log channels where installed applications, services, and system processes send data. This monitor runs once for every Event Log input that you define. [Learn More](#)

Select Event Logs Available item(s) add all > Selected item(s)

Application	Security
Security	
Setup	
System	
ForwardedEvents	
DirectShowFilterGraph	
DirectShowPluginControl	
Els_Hyphenation/Analytic	
EndpointMapper	

Select the Windows Event Logs you want to index from the list.

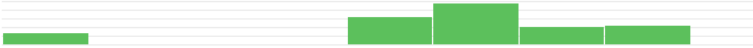
Se realiza la búsqueda global “*”

New Search

✓ 32,524 events (before 6/21/23 2:00:19.000 PM) No Event Sampling ▼

Events (32,524) Patterns Statistics Visualization

Format Timeline ▼ – Zoom Out + Zoom to Selection × Deselect



List ▼ Format 20 Per Page ▼

Aquí buscamos intentos fallidos de inicio de sesión por 4625

4625

✓ 3 events (before 6/21/23 2:04:36.000 PM) No Event Sampling ▼

Events (3) Patterns Statistics Visualization

Format Timeline ▼ — Zoom Out + Zoom to Selection × Deselect

List ▼ Format 20 Per Page ▼

< Hide Fields	≡ All Fields	i	Time	Event
SELECTED FIELDS a host 1 a source 1 a sourcetype 1 INTERESTING FIELDS a ComputerName 1 # date_hour 1 # date_mday 1 # date_minute 1 a date_month 1 # date_second 3 a date_wday 1 # date_year 1 a date_zone 1 a Dirección de red de origen 1 a Dominio_de_cuenta 2 a Estado 1 # EventCode 1 # EventType 1 a Id. de inicio de sesión 1 a Id_de_proceso_del_autor_de_la_llamada 1 a Id_de_seguridad 2 a index 1		>	6/21/23 2:02:17.000 PM	06/21/2023 02:02:17 PM LogName=Security EventCode=4625 EventType=0 ComputerName=Isaac Show all 61 lines host = ISAAC source = WinEventLog:Security sourcetype =
		>	6/21/23 2:02:16.000 PM	06/21/2023 02:02:16 PM LogName=Security EventCode=4625 EventType=0 ComputerName=Isaac Show all 61 lines host = ISAAC source = WinEventLog:Security sourcetype =
		>	6/21/23 2:02:15.000 PM	06/21/2023 02:02:15 PM LogName=Security EventCode=4625 EventType=0 ComputerName=Isaac Show all 61 lines host = ISAAC source = WinEventLog:Security sourcetype =
		>	6/21/23 2:02:14.000 PM	06/21/2023 02:02:14 PM LogName=Security EventCode=4625 EventType=0 ComputerName=Isaac Show all 61 lines host = ISAAC source = WinEventLog:Security sourcetype =

Configuramos una alerta de login fallidos:

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 ?

☐

Trigger Actions

+ Add Actions

Cancel

Save


Configuramos el throttle y el trigger de correo

Throttle ? ☒

Suppress triggering for

Trigger Actions

[+ 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

Ahora analizamos el archivo Log.rtf del laboratorio para responder la pregunta 35

Local Event Logs
Collect event logs from this machine.

Remote Event Logs
Collect event logs from remote hosts. Note: this uses WMI and requires a domain account.

Files & Directories
Upload a file, index a local file, or monitor an entire directory.

HTTP Event Collector
Configure tokens that clients can use to send data over HTTP or HTTPS.

TCP / UDP
Configure the Splunk platform to listen on a network port.

Local Performance Monitoring
Collect performance data from this machine.

Configure this instance to monitor files and directories for data. To monitor all objects in a directory, select the directory. The Splunk platform monitors and assigns a single source type to all objects within the directory. This might cause problems if there are different object types or data sources in the directory. To assign multiple source types to objects in the same directory, configure individual data inputs for those objects. [Learn More](#)

File or Directory ? [Browse](#)

On Windows: c:\apache\apache.error.log or \\hostname\apache.
apache.error.log. On Unix: /var/log or /mnt/www01/var/log.

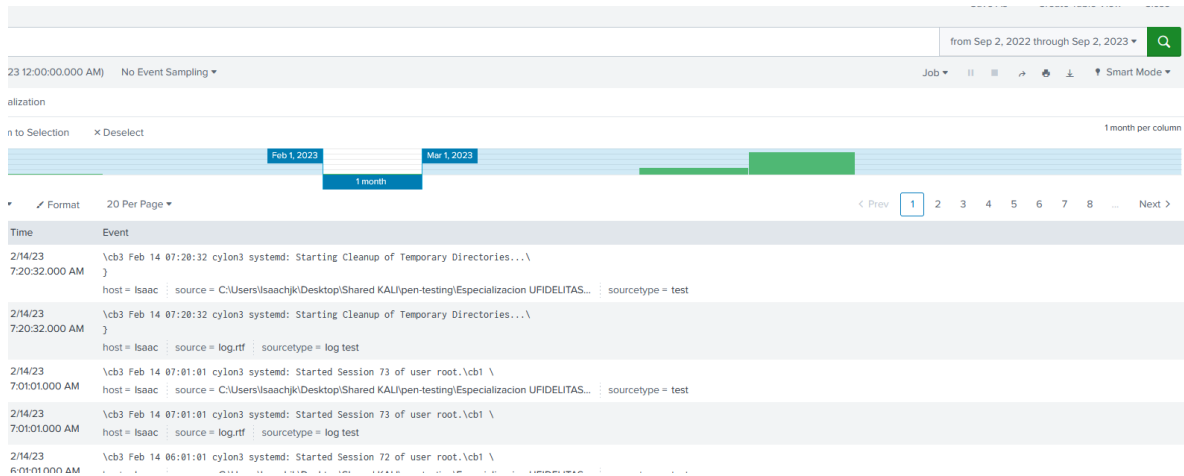
Includelist ?

Excludelist ?

New Search

*

✓ **33,572 events** (1/1/22 12:00:00.000 AM to 1/1/24 12:00:00.000 AM)



Preguntas y respuestas:

- a. ¿Cuántos eventos se generaron el 09 de febrero del 2022?

El archivo no presenta logs de Febrero del 2022, sin embargo, se generaron 380 en febrero del 2023.

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

A las 4:20 am.