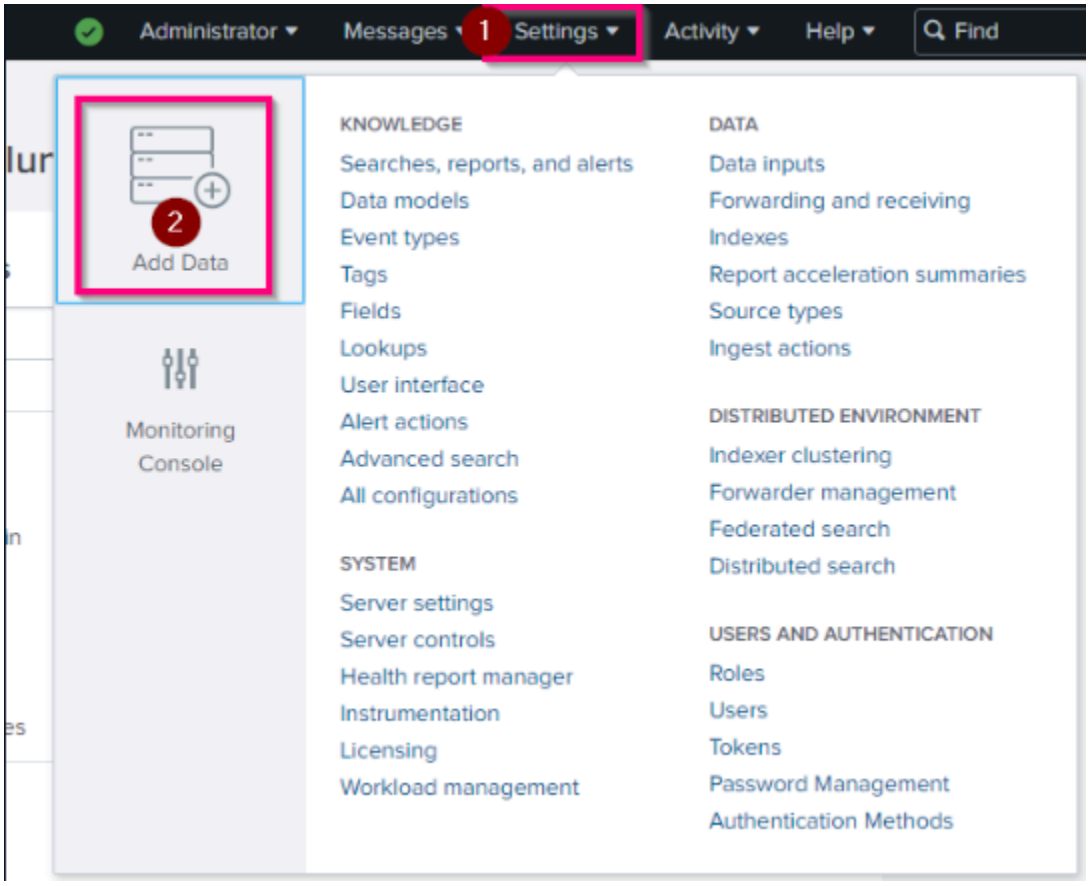
Add Data to Splunk

By: Ryan Stewart

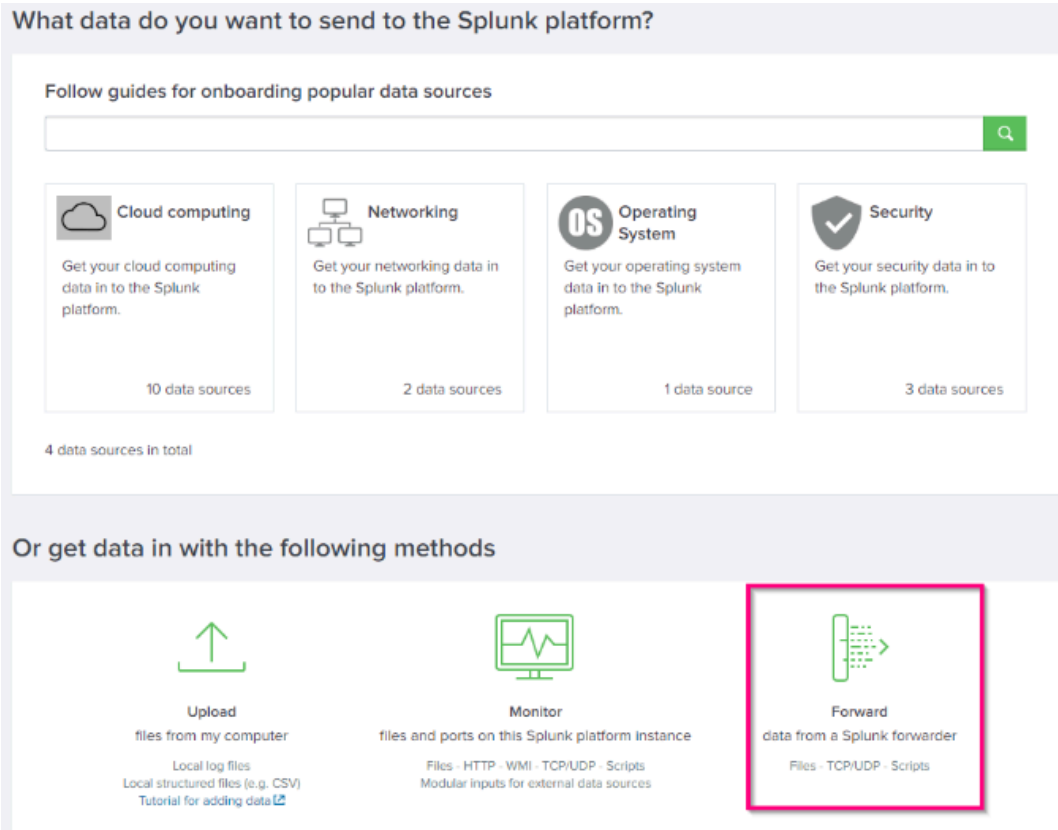
In Splunk, there are various ways to add data. Here, I'll explore adding data using the forwarder installed on a Win10 computer and uploading a log file.

Add Data from Forwarder:

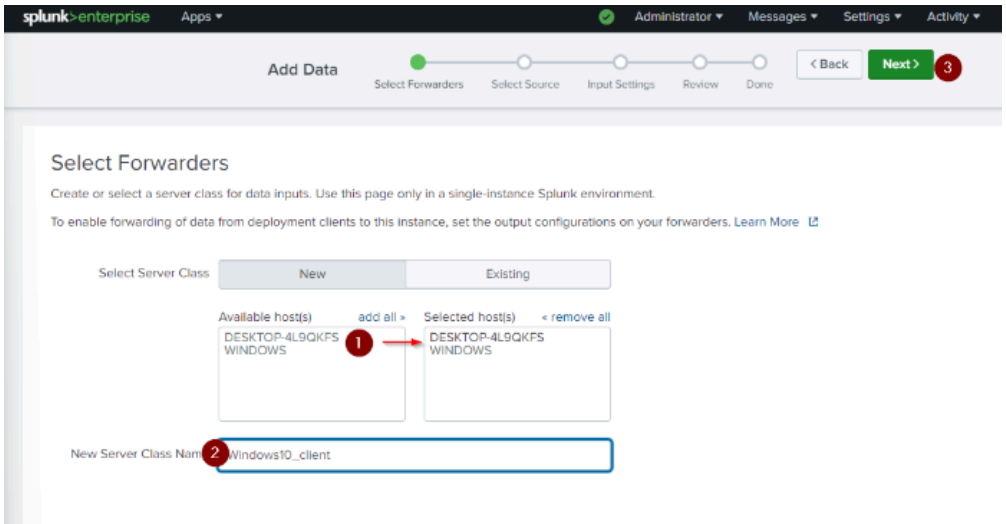
1. Go to **Settings > Add Data.**



2. Select "Forward" at the bottom.

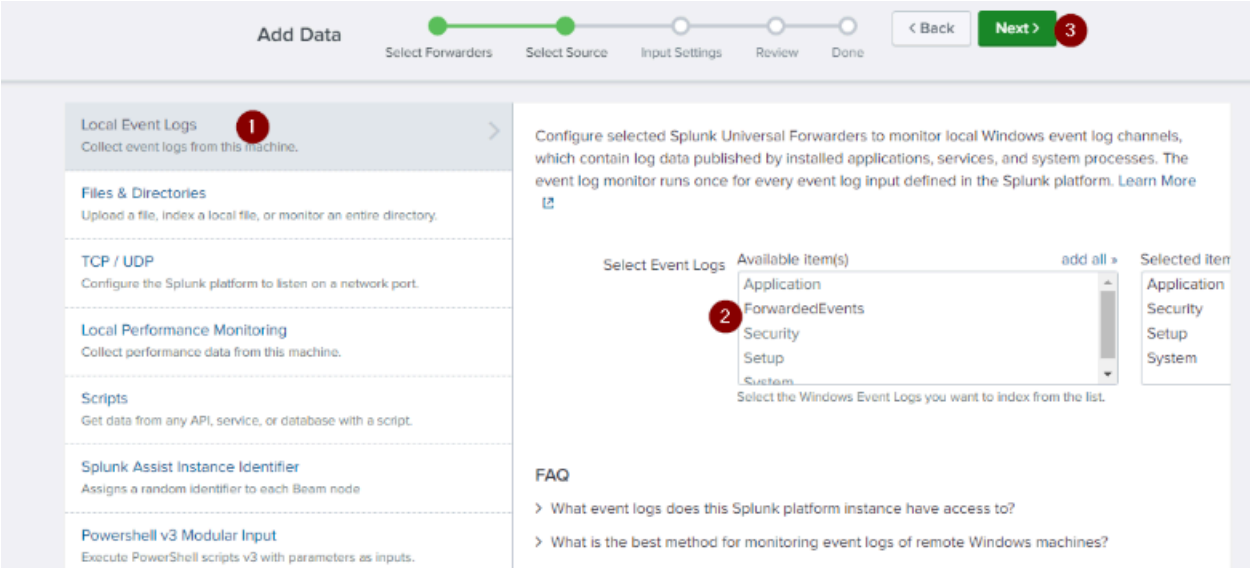


3. Add the computer to the selected host and assign a Server Class Name.
4. Click "Next."



- Select the data you want to monitor, e.g., local event logs from the computer.
- Choose the specific log.

- Click "Next."

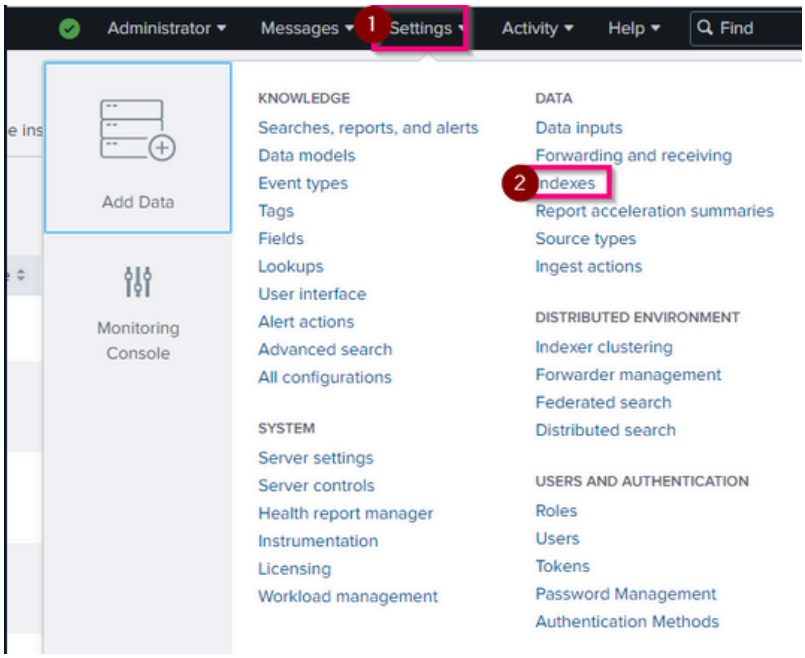


- Select the index for the logs. Create a new index, e.g., "WinLog_clients."
- Click "Review" to verify and then submit.

6. Click "Start Searching" to find the recent connection on the client's computer.

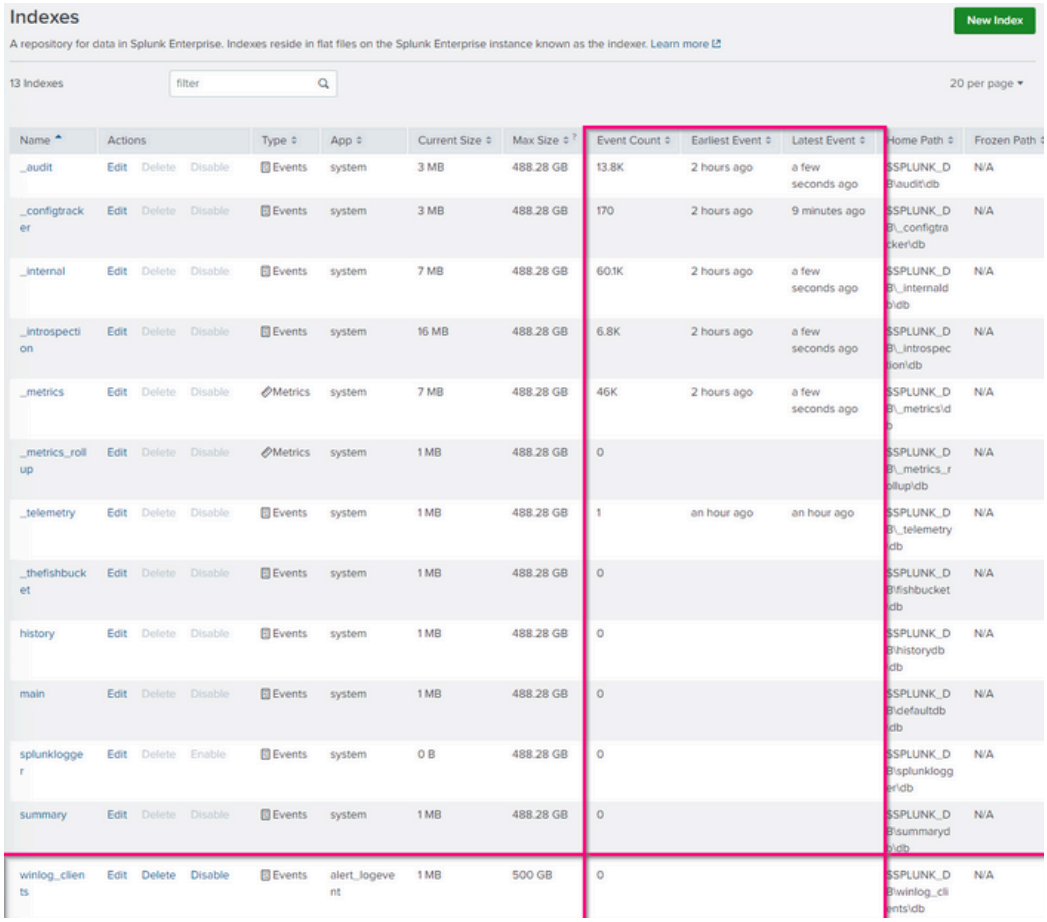
Check Your Indexes:

1. Go to Settings > Indexes.



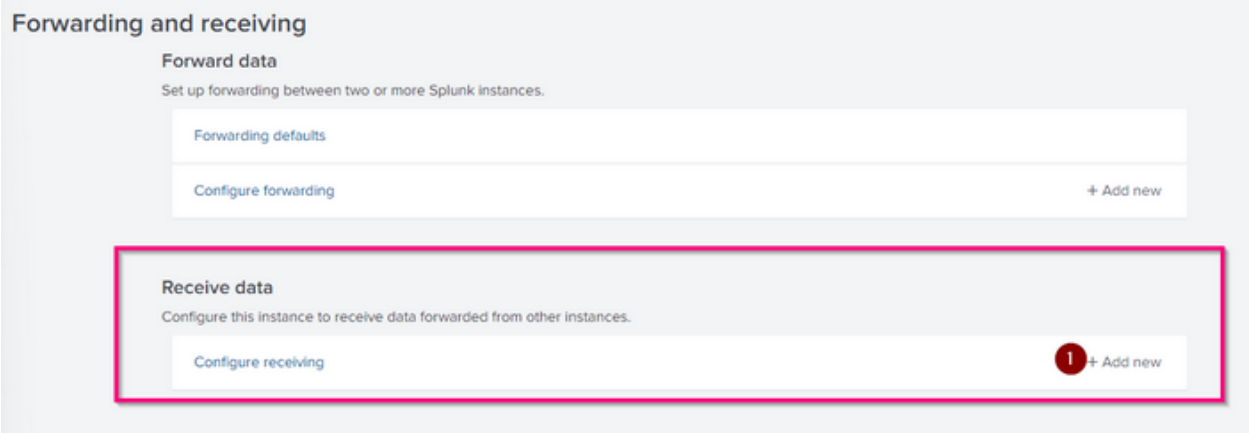
2. Search for the index you created.

- If no events are incoming, proceed to configure.

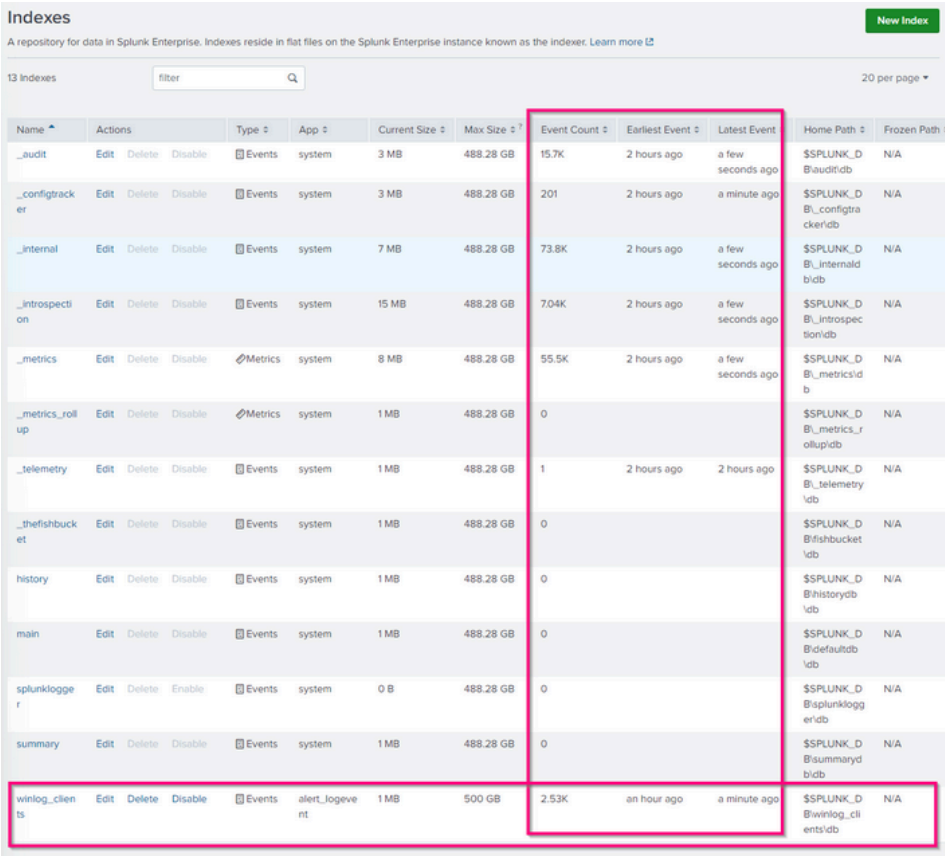


Add Receiver:

1. Go to **Settings > Forwarding and Receiving.**
2. Click to add a new receiving.

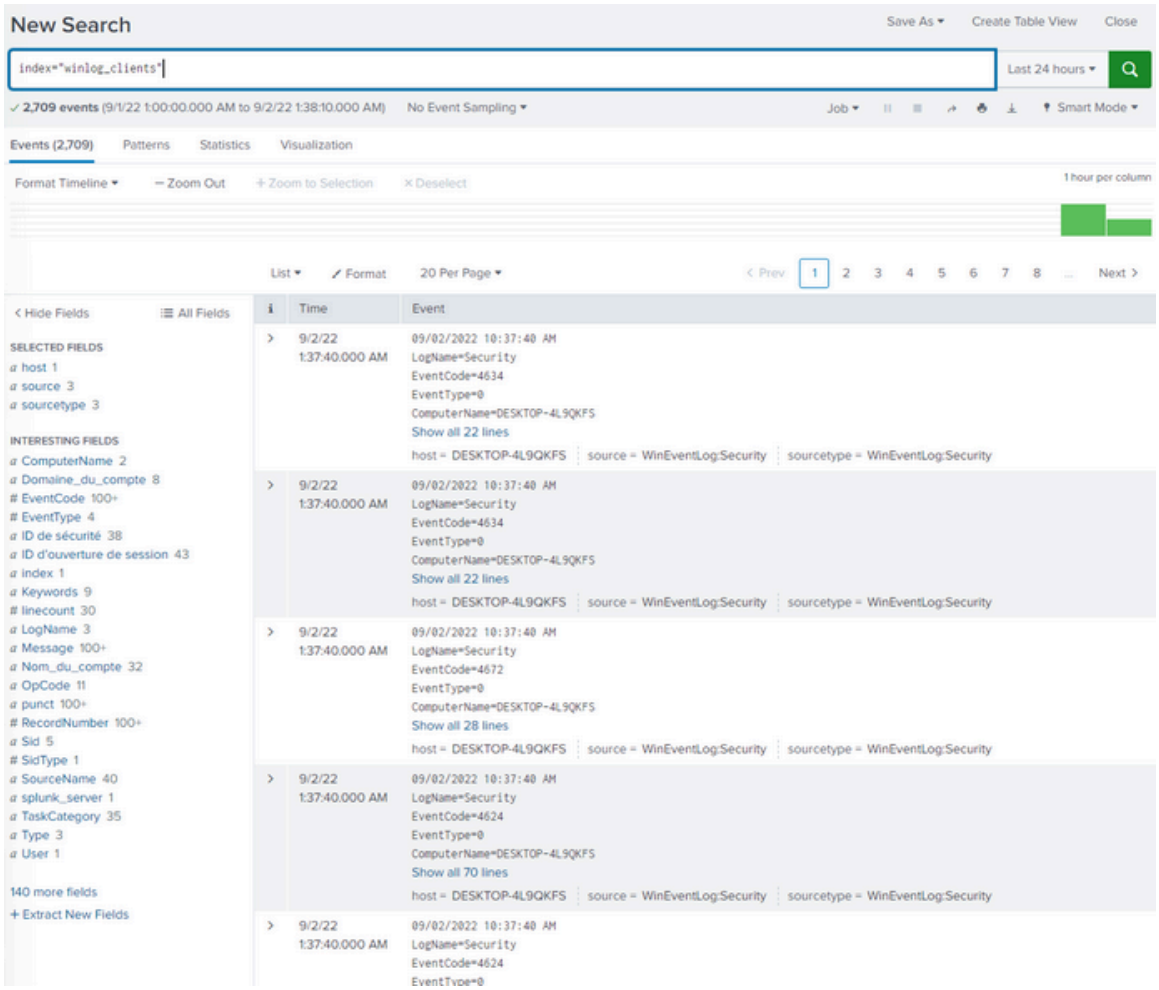


- Add the 9997 port (default).
- Wait a few minutes, then check indexes for new values.



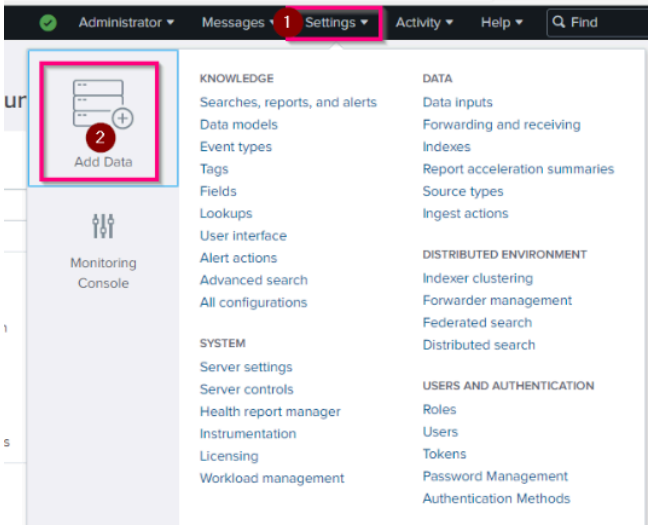
3. Check your indexes again to confirm the data reception.

Try a Quick Search.

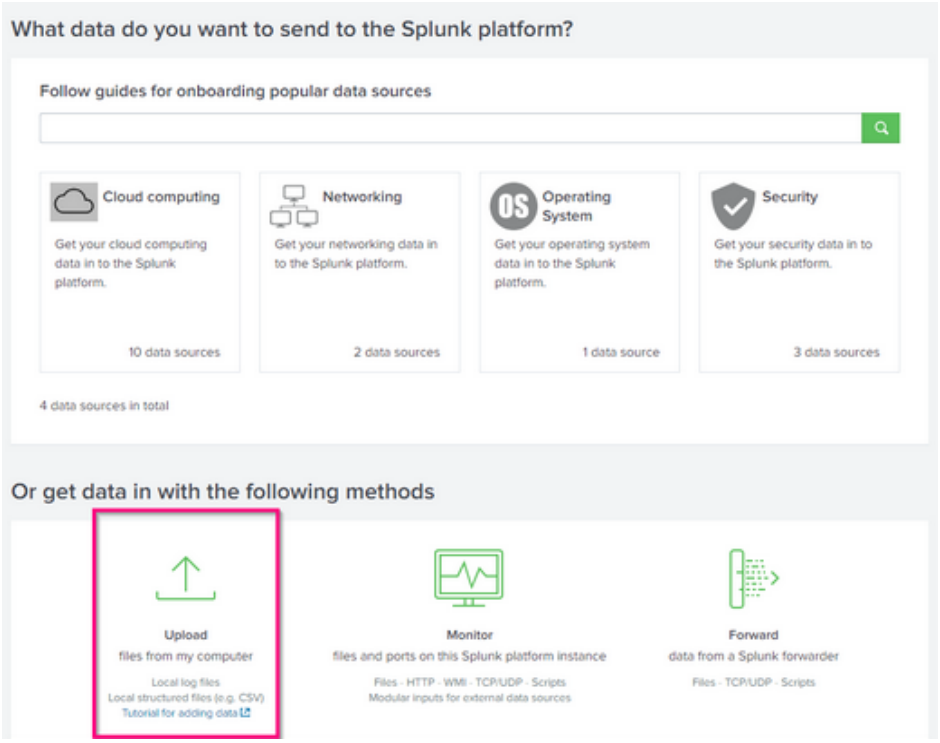


Add Data From Uploaded Logs:

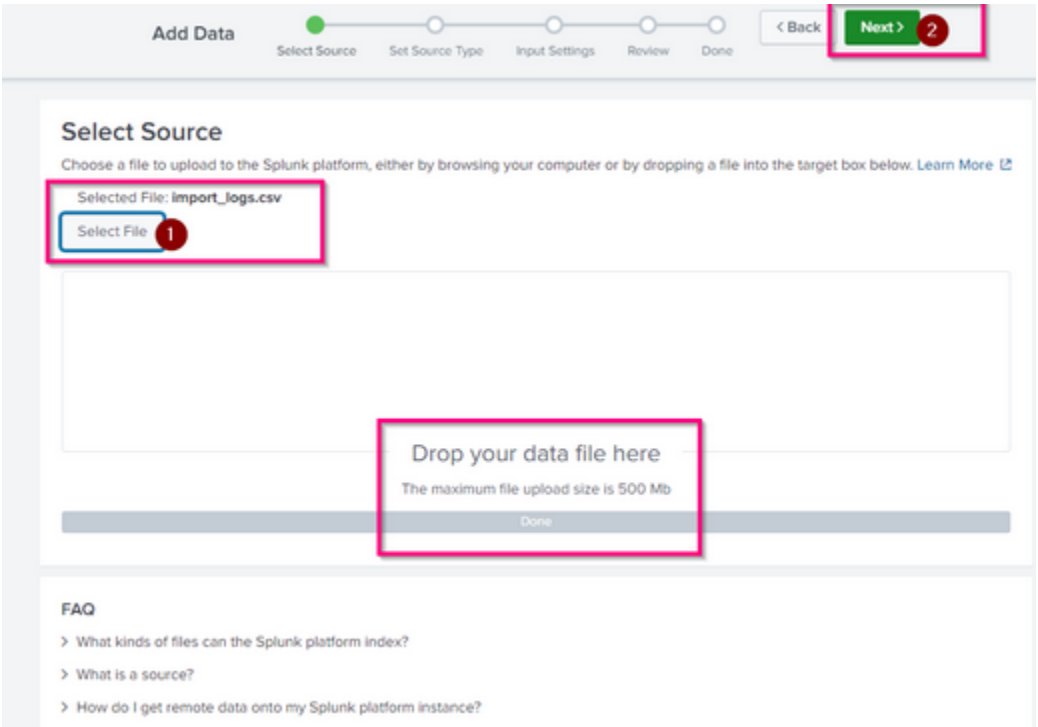
1. Go to Settings > Add Data.



2. Select "Upload" in the bottom left corner.

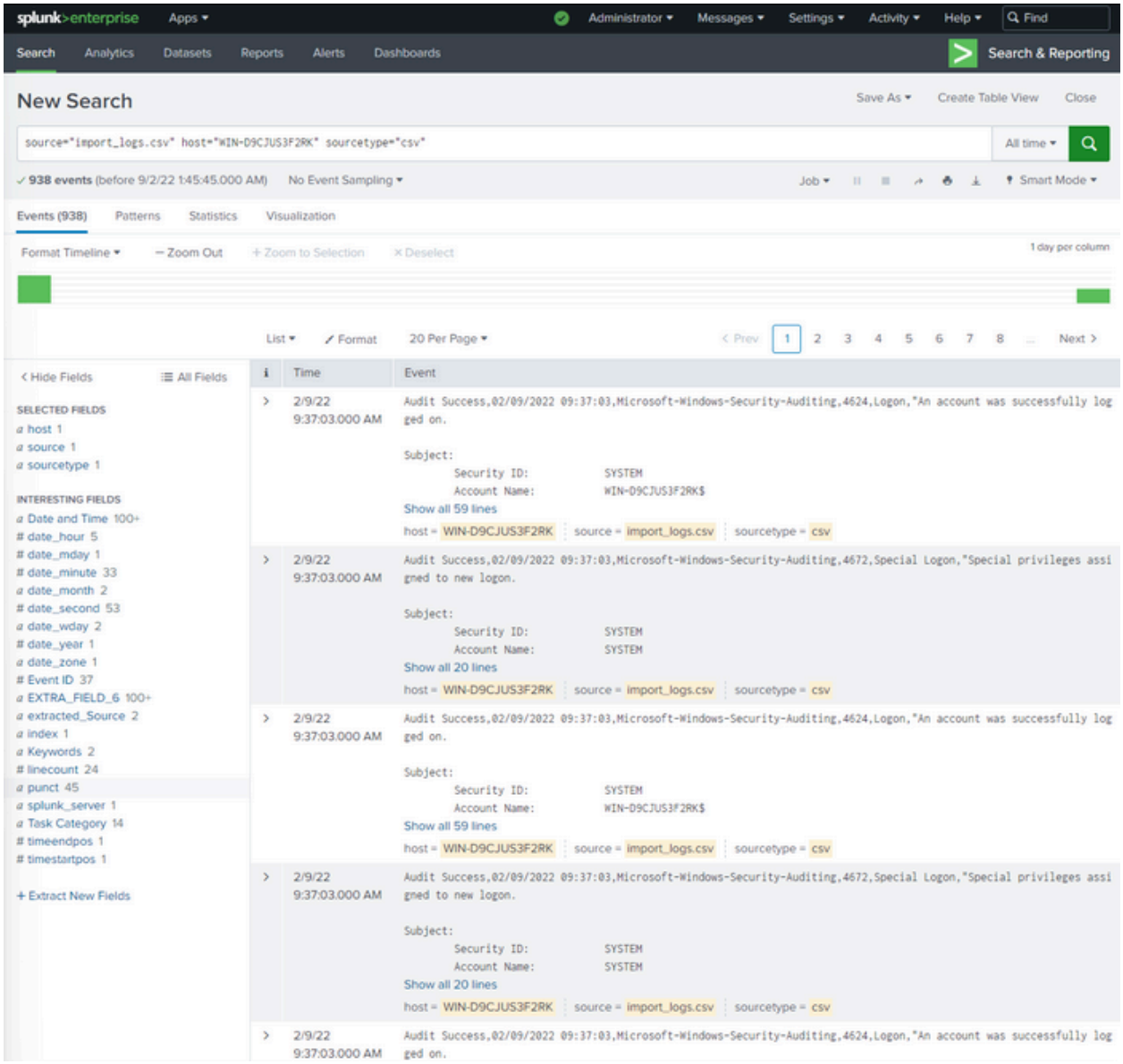


3. Upload the desired file, then click "Next."



- Check how Splunk will read the file, and press "Next" if everything is correct.

4. Select a host field value if needed and choose the index (use default for the exercise).
5. Continue to the end and start searching on the uploaded data.



By following these steps, you can effectively add and monitor data in Splunk, whether through the forwarder on a Windows computer or by uploading log files directly.