# **Performing Log Analysis Using Splunk**

## **Introduction**

Log analysis is the process of examining log data to identify patterns, anomalies, or specific events. This guide outlines the process of uploading log files to Splunk and performing the step-by-step process of log analysis using Splunk. Splunk is a powerful tool for searching, monitoring, and analyzing machine-generated data. By following these steps, you'll be able to upload your log files and start analyzing them using Splunk's features.

## **1. Download and Install Splunk**

1.1. Download Splunk

* Go to the official Splunk website ([www.splunk.com](http://www.splunk.com))
* Click on "Free Splunk" or "Download Splunk"
* Choose the appropriate version for your operating system
* Create an account or log in if prompted
* Start the download

1.2. Install Splunk

* Once downloaded, run the installer
* Follow the installation wizard:
  + Accept the license agreement
  + Choose installation directory
  + Set up admin username and password
* Wait for installation to complete

1.3. Start Splunk

* On Windows: Use the Start menu or desktop shortcut
* On Linux/Mac: Use terminal command ./splunk start

## **2. Initial Splunk Configuration**

2.1. Access Splunk Web Interface

* Open a web browser
* Navigate to<http://localhost:8000>
* Log in with your admin credentials

2.2. Add Data to Splunk

* Click on "Add Data" in the home screen
* Choose data source (e.g., "Upload files", "Monitor", "Forward")
* Follow the wizard to configure your data input
* Select or create an index for your data

## **3. Upload Log Files**

1. From the Splunk home screen, click "Add Data" in the top right corner
2. Select "Upload files from my computer"
3. Click "Select File" or drag and drop your log files into the designated area
4. Choose the log files you want to analyze from your computer
5. Click "Next"

## **4. Configure Input Settings**

1. Review the detected source type for your logs
2. If incorrect, click "Select Source Type" and choose the appropriate type
3. Click "Next"
4. Choose an existing index or create a new one for your logs
5. Click "Review"
6. On the review page, check your settings and click "Submit"

## **5. Start Searching**

1. Once Splunk finishes indexing your files, click "Start Searching"
2. You'll be taken to the Search & Reporting app

## **6. Perform Initial Analysis**

1. In the search bar, type index=<your\_index\_name> (replace with your actual index name)
2. Press Enter or click "Search"
3. Review the events that appear in the results pane
4. Look at the "Fields" sidebar on the left to see what types of data are available

## **7. Analyze Log Volumes**

1. Run the search: index=<your\_index\_name> | timechart count
2. This will show you the volume of logs over time
3. Look for any unusual spikes or drops in log volume

### 

### 

## **8. Identify Common Events**

1. Run the search: index=<your\_index\_name> | top limit=10 sourcetype
2. This will show the most common source types in your logs
3. Repeat with other fields like 'source' or 'host' to understand your data sources

### **9. Search for Error Messages**

1. Modify your search to: index=<your\_index\_name> error OR failed OR exception
2. Review the results to identify common error patterns
3. Click on interesting events to expand and see full details

### **10. Analyze User Activities**

1. If your logs contain user information, search: index=<your\_index\_name> | top limit=10 user
2. This will show the most active users in your logs
3. Look for any suspicious activities or unusual patterns

### **11. Investigate Network Traffic (if applicable)**

1. For network logs, try: index=<your\_index\_name> | iplocation src\_ip | geostats count
2. This will give you a geographical distribution of traffic sources
3. Look for traffic from unexpected locations

### **12. Create Time-based Analysis**

1. Run: index=<your\_index\_name> | bucket \_time span=1h | stats count by \_time
2. This groups your logs into hourly buckets
3. Look for patterns in activity over time, such as busy hours or quiet periods

### **13. Correlate Events**

1. If you have multiple log sources, try to correlate events
2. For example: index=<your\_index\_name> (sourcetype=access\_log OR sourcetype=application\_log) | transaction host maxspan=5m
3. This will group related events from different sources within a 5-minute window

### 

### **14. Look for Security Issues**

1. Search for failed logins: index=<your\_index\_name> failed password
2. Check for unusual account activities: index=<your\_index\_name> account created OR account deleted
3. Look for potential data exfiltration: index=<your\_index\_name> | where bytes\_out > 1000000 | sort - bytes\_out

### **15. Analyze Performance**

1. If you have performance metrics, search: index=<your\_index\_name> response\_time>5000
2. This will show events where response time exceeded 5 seconds
3. Look for patterns in slow performance, such as specific times or users

### **16. Create Visualisations for Key Metrics**

1. Based on your findings, create relevant visualisations
2. For example, a line chart of errors over time or a pie chart of top users
3. Use these to build a dashboard for ongoing monitoring

### **17. Document Findings**

1. For each significant pattern or issue found, document:
   * The search query used
   * A description of the pattern or issue
   * Potential impact or risk
   * Recommended next steps or further investigation needed

The specific analyses you perform will depend on the nature of your log data and what you're trying to achieve. These steps provide a general framework for log analysis, but you should adapt them based on your specific needs and the content of your logs.