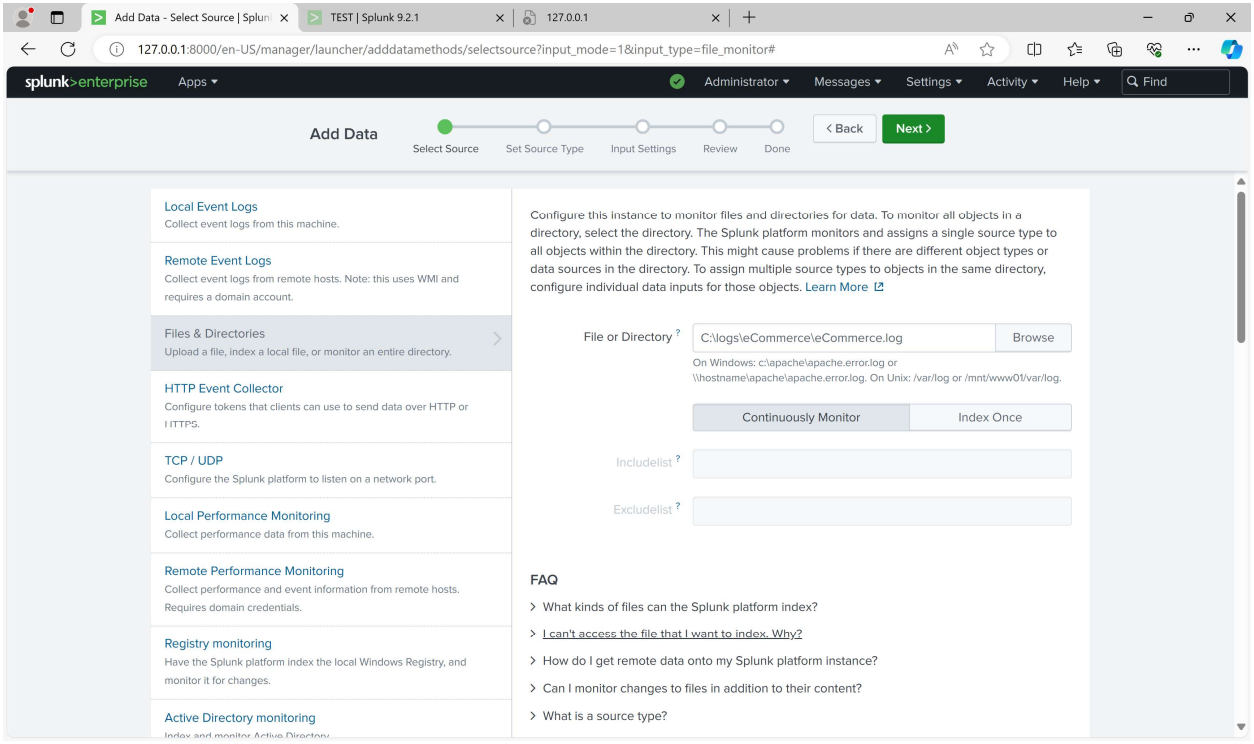
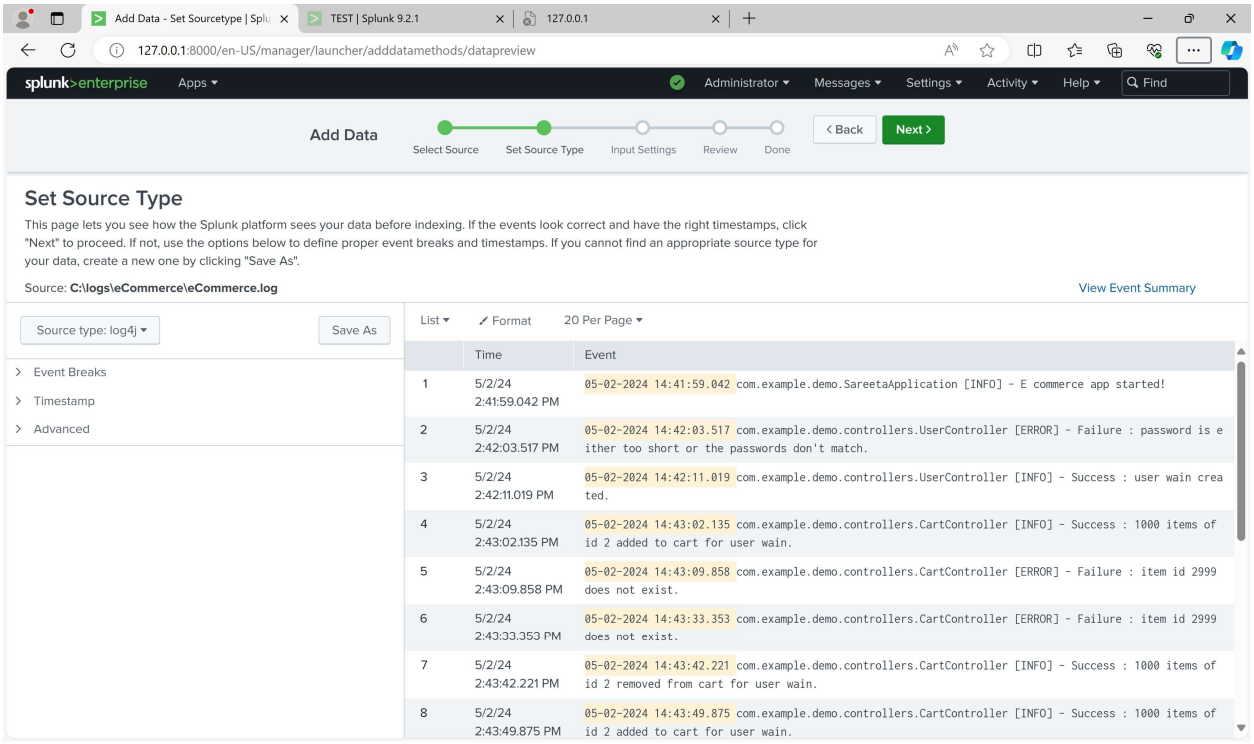
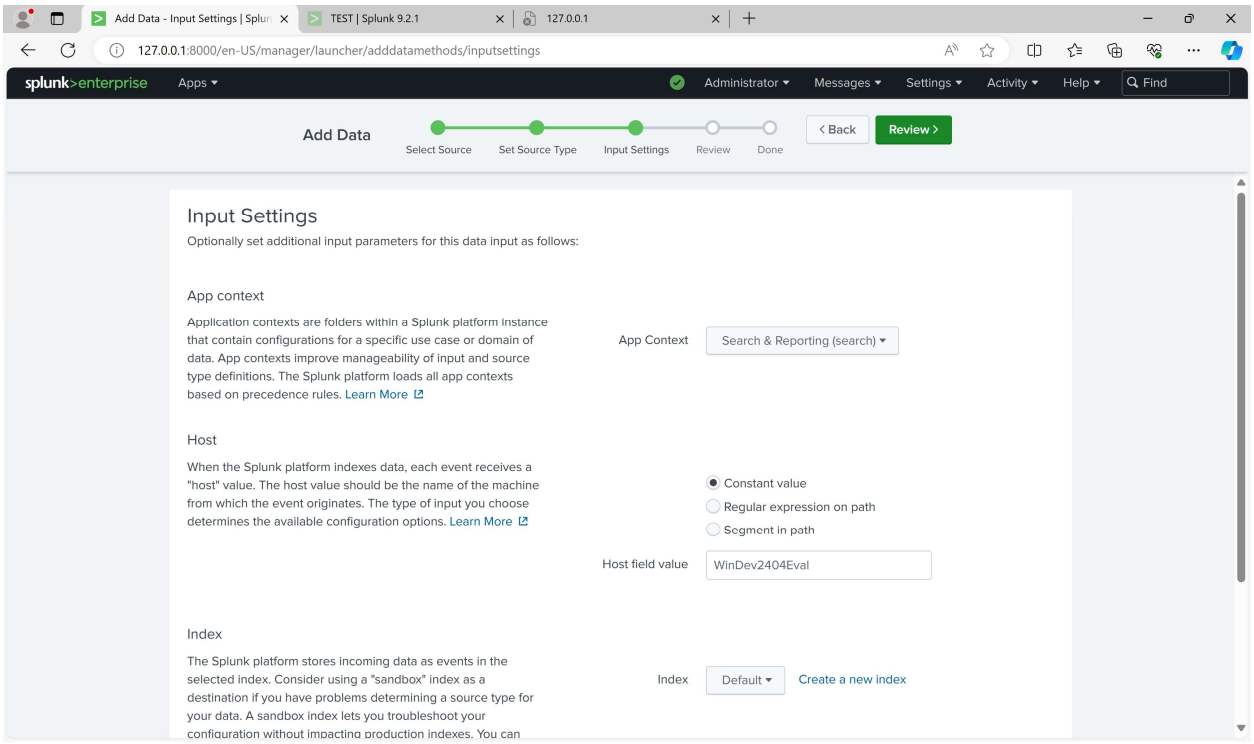
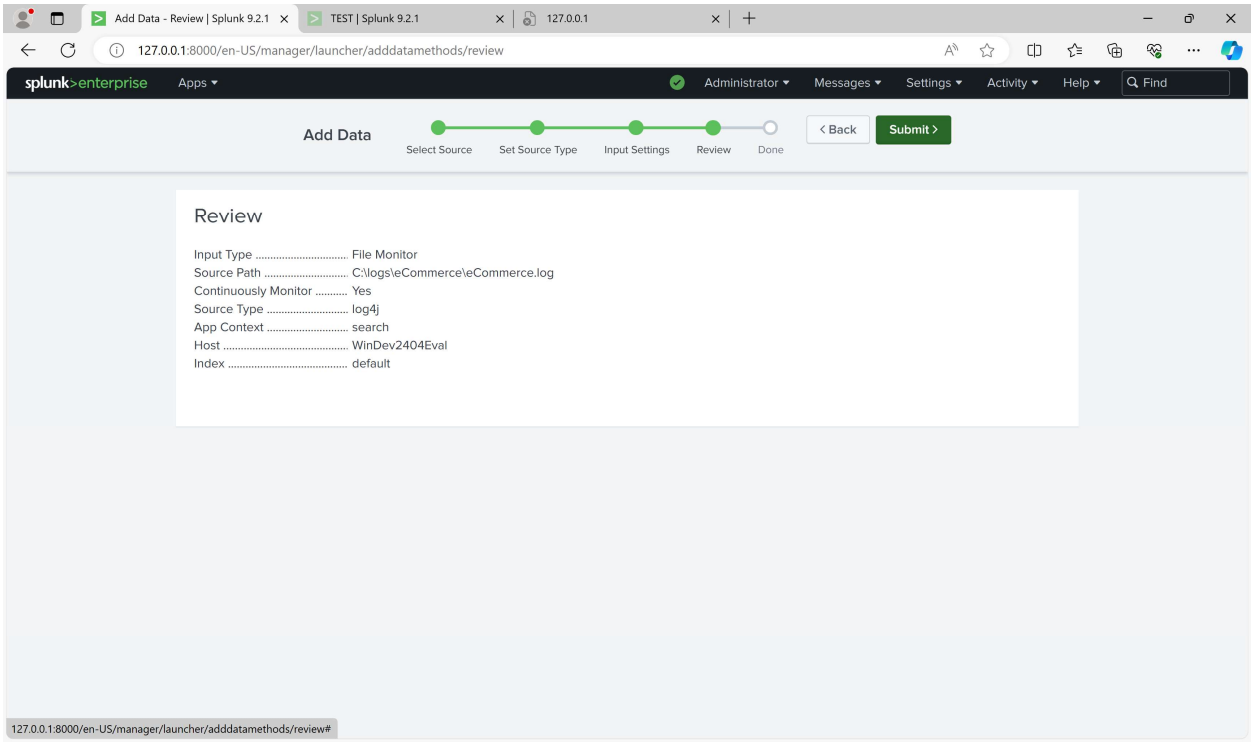
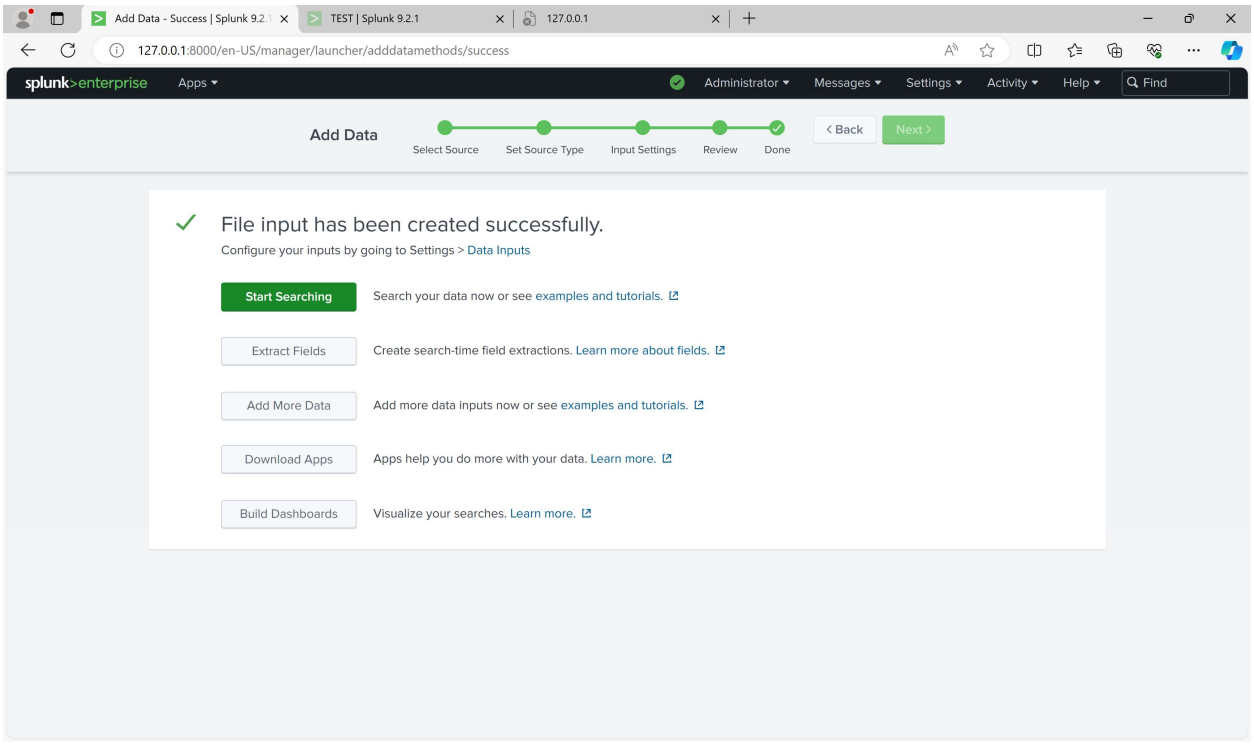
# Add Data


Add Data - Select Source | Splun
TEST | Splunk 9.2.1
127.0.0.1
127.0.0.1:8000/en-US/manager/launcher/adddatamethods/selectsource?input_mode=1&input_type=file_monitor#
splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Add Data
Select Source
Set Source Type
Input Settings
Review
Done
Back
Next
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.
Remote Performance Monitoring
Collect performance and event information from remote hosts. Requires domain credentials.
Registry monitoring
Have the Splunk platform index the local Windows Registry, and monitor it for changes.
Active Directory monitoring
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
C:\logs\eCommerce\eCommerce.log
Browse
On Windows: c:\apache\apache.error.log or \\hostname\apache\apache.error.log. On Unix: /var/log or /mnt/www01/var/log.
Continuously Monitor
Index Once
Includelist
Excludelist
FAQ
What kinds of files can the Splunk platform index?
I can't access the file that I want to index. Why?
How do I get remote data onto my Splunk platform instance?
Can I monitor changes to files in addition to their content?
What is a source type?

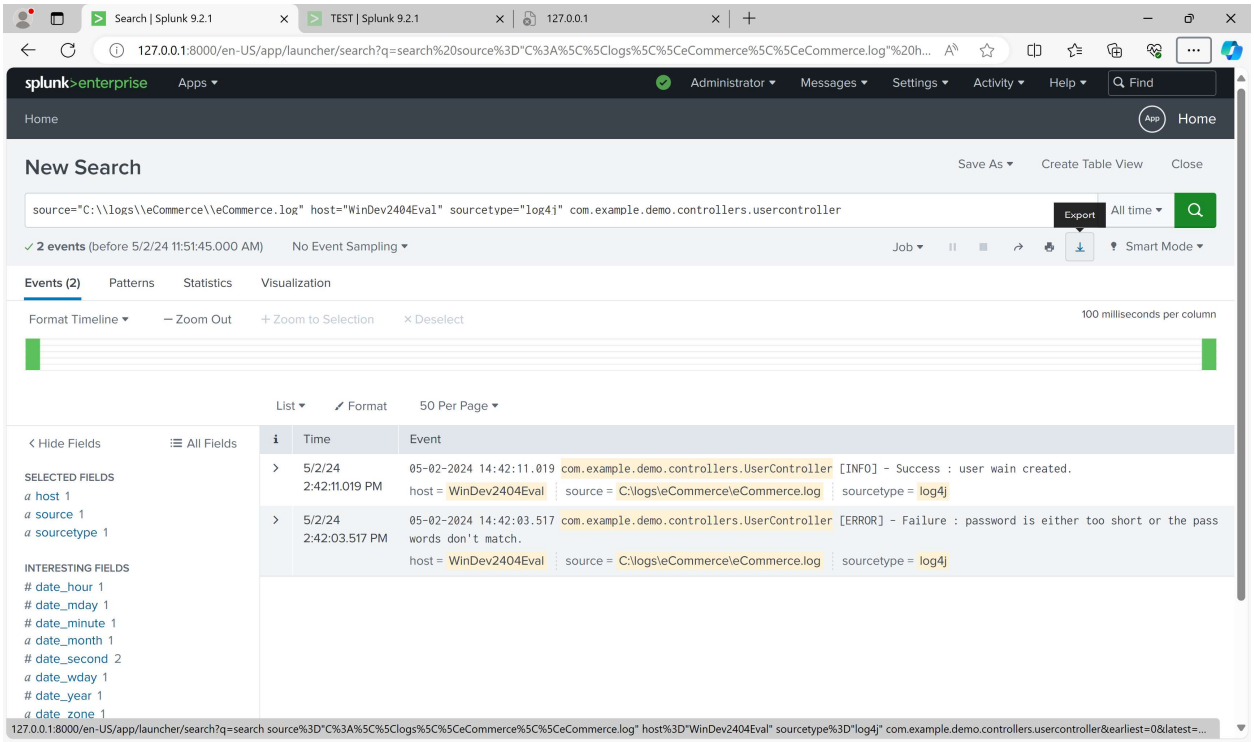

Add Data - Set Sourcetype | Splu
TEST | Splunk 9.2.1
127.0.0.1
127.0.0.1:8000/en-US/manager/launcher/adddatamethods/datapreview
splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Add Data
Select Source
Set Source Type
Input Settings
Review
Done
Back
Next
Set Source Type
This page lets you see how the Splunk platform sees your data before indexing. If the events look correct and have the right timestamps, click "Next" to proceed. If not, use the options below to define proper event breaks and timestamps. If you cannot find an appropriate source type for your data, create a new one by clicking "Save As".
Source: C:\logs\eCommerce\eCommerce.log
View Event Summary
Source type: log4j
Save As
Event Breaks
Timestamp
Advanced
List
Format
20 Per Page
Time
Event
1 5/2/24 2:41:59.042 PM 05-02-2024 14:41:59.042 com.example.demo.SareetaApplication [INFO] - E commerce app started!
2 5/2/24 2:42:03.517 PM 05-02-2024 14:42:03.517 com.example.demo.controllers.UserController [ERROR] - Failure : password is either too short or the passwords don't match.
3 5/2/24 2:42:11.019 PM 05-02-2024 14:42:11.019 com.example.demo.controllers.UserController [INFO] - Success : user wain created.
4 5/2/24 2:43:02.135 PM 05-02-2024 14:43:02.135 com.example.demo.controllers.CartController [INFO] - Success : 1000 items of id 2 added to cart for user wain.
5 5/2/24 2:43:09.858 PM 05-02-2024 14:43:09.858 com.example.demo.controllers.CartController [ERROR] - Failure : item id 2999 does not exist.
6 5/2/24 2:43:33.353 PM 05-02-2024 14:43:33.353 com.example.demo.controllers.CartController [ERROR] - Failure : item id 2999 does not exist.
7 5/2/24 2:43:42.221 PM 05-02-2024 14:43:42.221 com.example.demo.controllers.CartController [INFO] - Success : 1000 items of id 2 removed from cart for user wain.
8 5/2/24 2:43:49.875 PM 05-02-2024 14:43:49.875 com.example.demo.controllers.CartController [INFO] - Success : 1000 items of id 2 added to cart for user wain.

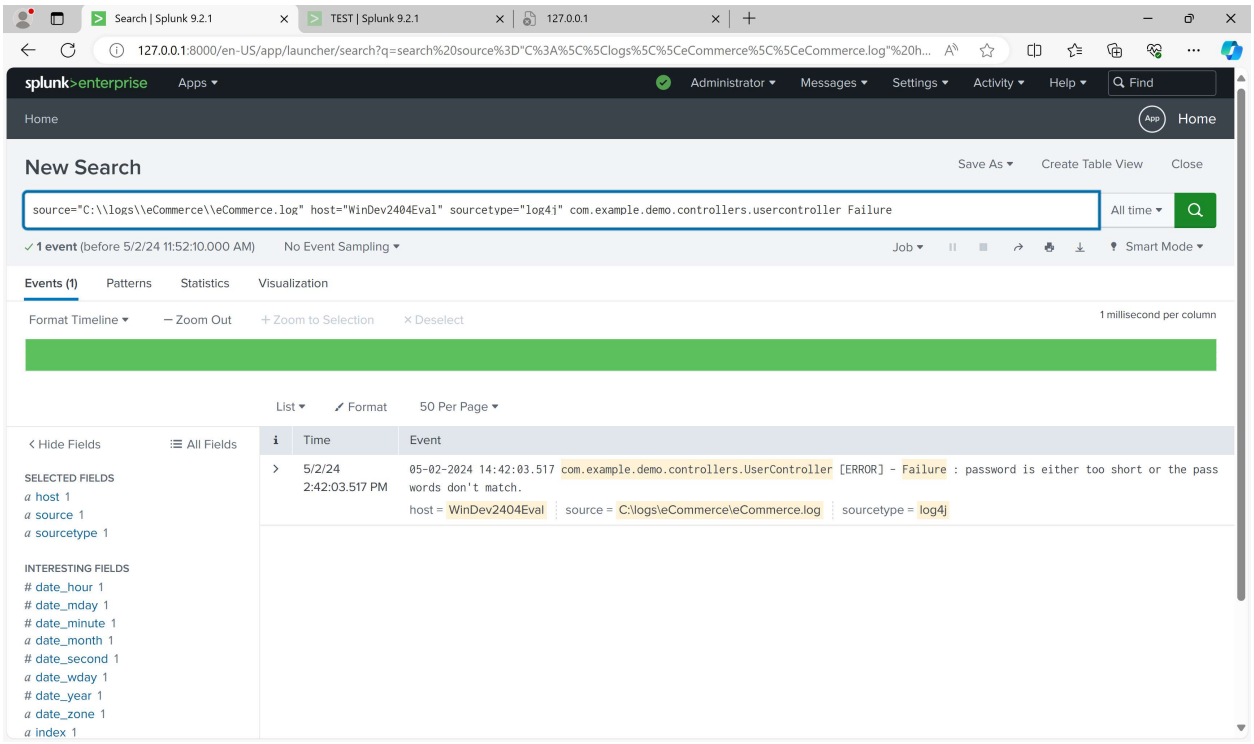

Add Data - Input Settings | Splun
TEST | Splunk 9.2.1
127.0.0.1
127.0.0.1:8000/en-US/manager/launcher/adddatamethods/inputsettings
splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Add Data
Select Source
Set Source Type
Input Settings
Review
Done
Back
Review
Input Settings
Optionally set additional input parameters for this data input as follows:
App context
Application contexts are folders within a Splunk platform instance that contain configurations for a specific use case or domain of data. App contexts improve manageability of input and source type definitions. The Splunk platform loads all app contexts based on precedence rules. Learn More
App Context
Search & Reporting (search)
Host
When the Splunk platform indexes data, each event receives a "host" value. The host value should be the name of the machine from which the event originates. The type of input you choose determines the available configuration options. Learn More
Constant value
Regular expression on path
Segment in path
Host field value
WinDev2404Eval
Index
The Splunk platform stores incoming data as events in the selected index. Consider using a "sandbox" index as a destination if you have problems determining a source type for your data. A sandbox index lets you troubleshoot your
Index
Default
Create a new index

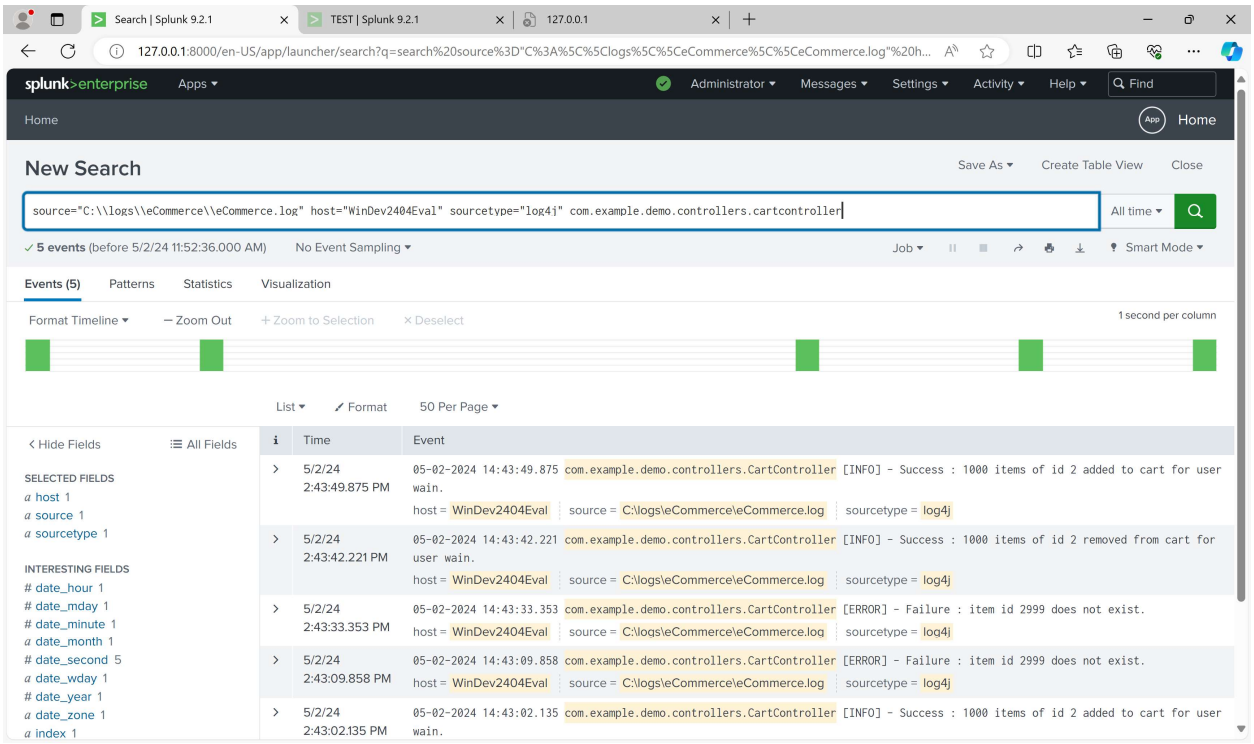

Add Data - Review | Splunk 9.2.1
TEST | Splunk 9.2.1
127.0.0.1
127.0.0.1:8000/en-US/manager/launcher/adddatamethods/review
splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Add Data
Select Source
Set Source Type
Input Settings
Review
Done
Back
Submit
Review
Input Type ..... File Monitor
Source Path ..... C:\logs\eCommerce\eCommerce.log
Continuously Monitor ..... Yes
Source Type ..... log4j
App Context ..... search
Host ..... WinDev2404Eval
Index ..... default
127.0.0.1:8000/en-US/manager/launcher/adddatamethods/review#

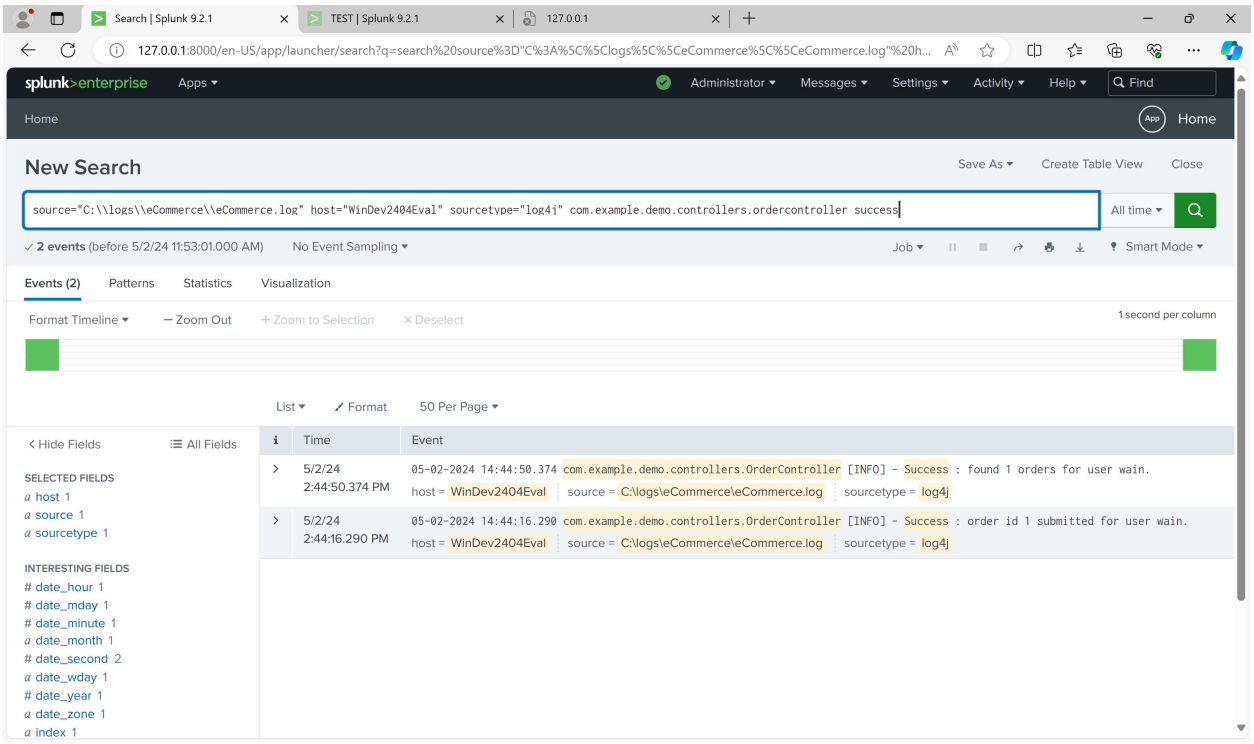

Add Data - Success | Splunk 9.2
TEST | Splunk 9.2.1
127.0.0.1
127.0.0.1:8000/en-US/manager/launcher/adddatamethods/success
splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Add Data
Select Source
Set Source Type
Input Settings
Review
Done
Back
Next
File input has been created 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.

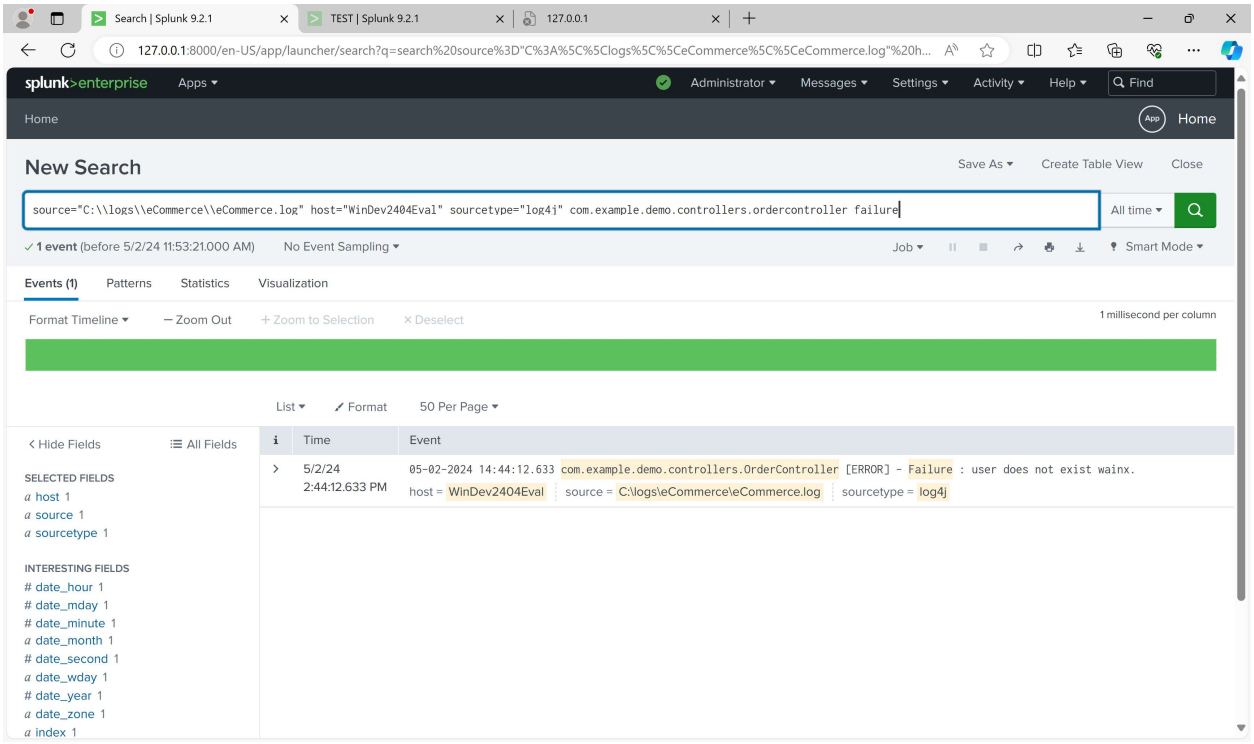
# Search

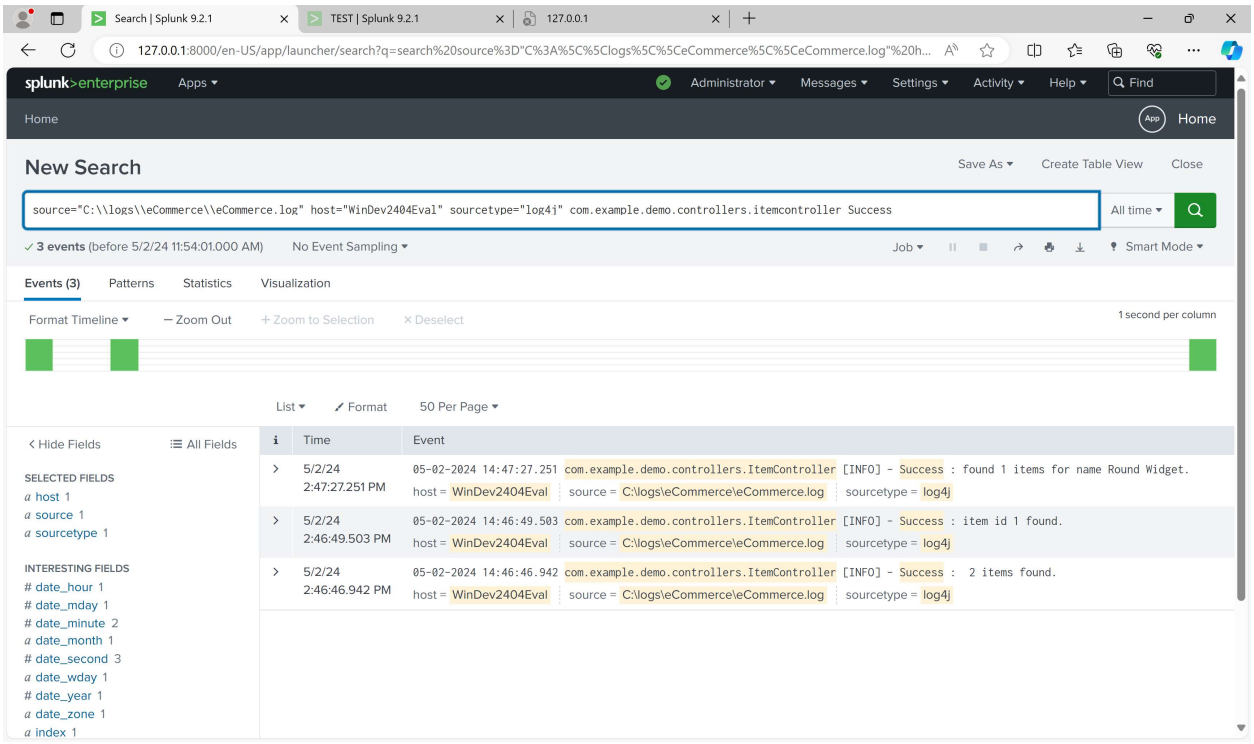

Search | Splunk 9.2.1
TEST | Splunk 9.2.1
127.0.0.1
127.0.0.1:8000/en-US/app/launcher/search?q=search%20source%3D"C%3A%5C%5Clogs%5C%5CeCommerce%5C%5CeCommerce.log"%20h...
splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Home
Home
New Search
Save As
Create Table View
Close
source="C:\\logs\\eCommerce\\eCommerce.log" host="WinDev2404Eval" sourcetype="log4j" com.example.demo.controllers.usercontroller
Export
All time
2 events (before 5/2/24 11:51:45.000 AM)
No Event Sampling
Job
Smart Mode
Events (2)
Patterns
Statistics
Visualization
Format Timeline
Zoom Out
Zoom to Selection
Deselect
100 milliseconds per column
List
Format
50 Per Page
Hide Fields
All Fields
SELECTED FIELDS
host 1
source 1
sourcetype 1
INTERESTING FIELDS
date_hour 1
date_mday 1
date_minute 1
date_month 1
date_second 2
date_wday 1
date_year 1
date_zone 1
Time
Event
5/2/24 2:42:11.019 PM
05-02-2024 14:42:11.019 com.example.demo.controllers.UserController [INFO] - Success : user wain created.
host = WinDev2404Eval source = C:\logs\eCommerce\eCommerce.log sourcetype = log4j
5/2/24 2:42:03.517 PM
05-02-2024 14:42:03.517 com.example.demo.controllers.UserController [ERROR] - Failure : password is either too short or the pass words don't match.
host = WinDev2404Eval source = C:\logs\eCommerce\eCommerce.log sourcetype = log4j
127.0.0.1:8000/en-US/app/launcher/search?q=search source%3D"C%3A%5C%5Clogs%5C%5CeCommerce%5C%5CeCommerce.log" host%3D"WinDev2404Eval" sourcetype%3D"log4j" com.example.demo.controllers.usercontroller&earliest=0&latest=...

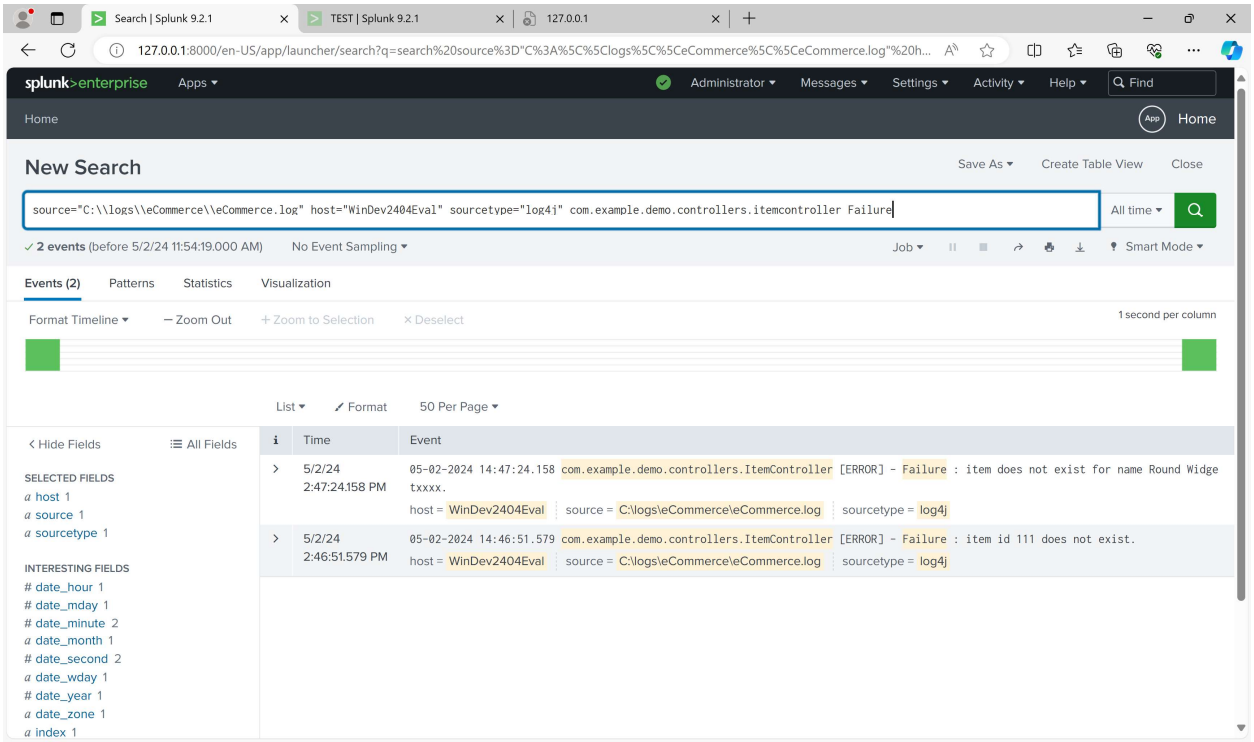

Search | Splunk 9.2.1
TEST | Splunk 9.2.1
127.0.0.1
127.0.0.1:8000/en-US/app/launcher/search?q=search%20source%3D"C%3A%5C%5Clogs%5C%5CeCommerce%5C%5CeCommerce.log"%20h...
splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Home
New Search
Save As
Create Table View
Close
source="C:\\logs\\eCommerce\\eCommerce.log" host="WinDev2404Eval" sourcetype="log4j" com.example.demo.controllers.usercontroller Failure
All time
1 event (before 5/2/24 11:52:10.000 AM)
No Event Sampling
Job
Smart Mode
Events (1)
Patterns
Statistics
Visualization
Format Timeline
Zoom Out
Zoom to Selection
Deselect
1 millisecond per column
List
Format
50 Per Page
Hide Fields
All Fields
Time
Event
5/2/24 2:42:03.517 PM
05-02-2024 14:42:03.517 com.example.demo.controllers.UserController [ERROR] - Failure : password is either too short or the pass words don't match.
host = WinDev2404Eval
source = C:\logs\eCommerce\eCommerce.log
sourcetype = log4j
SELECTED FIELDS
a host 1
a source 1
a sourcetype 1
INTERESTING FIELDS
# date_hour 1
# date_mday 1
# date_minute 1
a date_month 1
# date_second 1
a date_wday 1
# date_year 1
a date_zone 1
a index 1


Search | Splunk 9.2.1
TEST | Splunk 9.2.1
127.0.0.1
127.0.0.1:8000/en-US/app/launcher/search?q=search%20source%3D"C%3A%5C%5Clogs%5C%5CeCommerce%5C%5CeCommerce.log"%20h...
splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Home
New Search
Save As
Create Table View
Close
source="C:\\logs\\eCommerce\\eCommerce.log" host="WinDev2404Eval" sourcetype="log4j" com.example.demo.controllers.cartcontroller
All time
5 events (before 5/2/24 11:52:36.000 AM)
No Event Sampling
Job
Smart Mode
Events (5)
Patterns
Statistics
Visualization
Format Timeline
Zoom Out
Zoom to Selection
Deselect
1 second per column
List
Format
50 Per Page
Hide Fields
All Fields
Time
Event
5/2/24 2:43:49.875 PM
05-02-2024 14:43:49.875 com.example.demo.controllers.CartController [INFO] - Success : 1000 items of id 2 added to cart for user wain.
host = WinDev2404Eval
source = C:\logs\eCommerce\eCommerce.log
sourcetype = log4j
5/2/24 2:43:42.221 PM
05-02-2024 14:43:42.221 com.example.demo.controllers.CartController [INFO] - Success : 1000 items of id 2 removed from cart for user wain.
host = WinDev2404Eval
source = C:\logs\eCommerce\eCommerce.log
sourcetype = log4j
5/2/24 2:43:33.353 PM
05-02-2024 14:43:33.353 com.example.demo.controllers.CartController [ERROR] - Failure : item id 2999 does not exist.
host = WinDev2404Eval
source = C:\logs\eCommerce\eCommerce.log
sourcetype = log4j
5/2/24 2:43:09.858 PM
05-02-2024 14:43:09.858 com.example.demo.controllers.CartController [ERROR] - Failure : item id 2999 does not exist.
host = WinDev2404Eval
source = C:\logs\eCommerce\eCommerce.log
sourcetype = log4j
5/2/24 2:43:02.135 PM
05-02-2024 14:43:02.135 com.example.demo.controllers.CartController [INFO] - Success : 1000 items of id 2 added to cart for user wain.
SELECTED FIELDS
a host 1
a source 1
a sourcetype 1
INTERESTING FIELDS
# date_hour 1
# date_mday 1
# date_minute 1
a date_month 1
# date_second 5
a date_wday 1
# date_year 1
a date_zone 1
a index 1

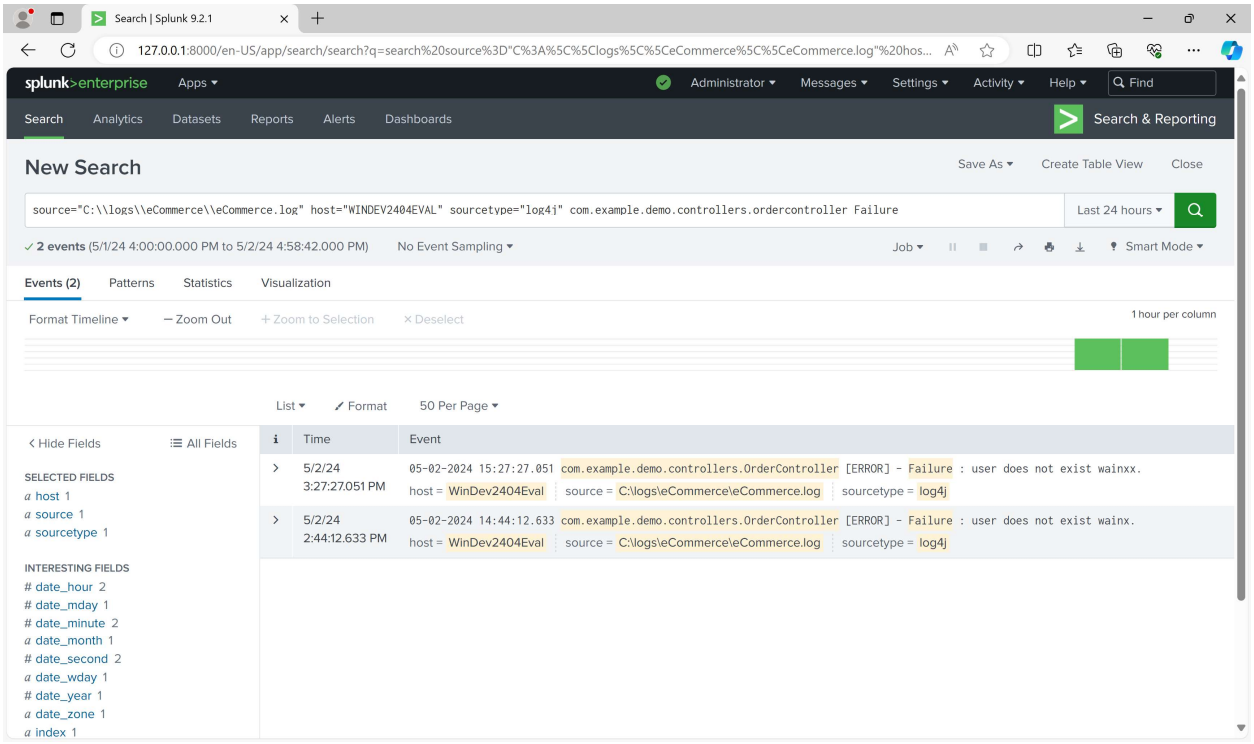

Search | Splunk 9.2.1
TEST | Splunk 9.2.1
127.0.0.1
127.0.0.1:8000/en-US/app/launcher/search?q=search%20source%3D"C%3A%5C%5Clogs%5C%5CeCommerce%5C%5CeCommerce.log"%20h...
splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Home
Home
New Search
Save As
Create Table View
Close
source="C:\\logs\\eCommerce\\eCommerce.log" host="WinDev2404Eval" sourcetype="log4j" com.example.demo.controllers.ordercontroller success
All time
2 events (before 5/2/24 11:53:01.000 AM)
No Event Sampling
Job
Smart Mode
Events (2)
Patterns
Statistics
Visualization
Format Timeline
Zoom Out
Zoom to Selection
Deselect
1 second per column
List
Format
50 Per Page
Hide Fields
All Fields
SELECTED FIELDS
a host 1
a source 1
a sourcetype 1
INTERESTING FIELDS
# date_hour 1
# date_mday 1
# date_minute 1
a date_month 1
# date_second 2
a date_wday 1
# date_year 1
a date_zone 1
a index 1
Time
Event
5/2/24 2:44:50.374 PM
05-02-2024 14:44:50.374 com.example.demo.controllers.OrderController [INFO] - Success : found 1 orders for user wain.
host = WinDev2404Eval source = C:\logs\eCommerce\eCommerce.log sourcetype = log4j
5/2/24 2:44:16.290 PM
05-02-2024 14:44:16.290 com.example.demo.controllers.OrderController [INFO] - Success : order id 1 submitted for user wain.
host = WinDev2404Eval source = C:\logs\eCommerce\eCommerce.log sourcetype = log4j

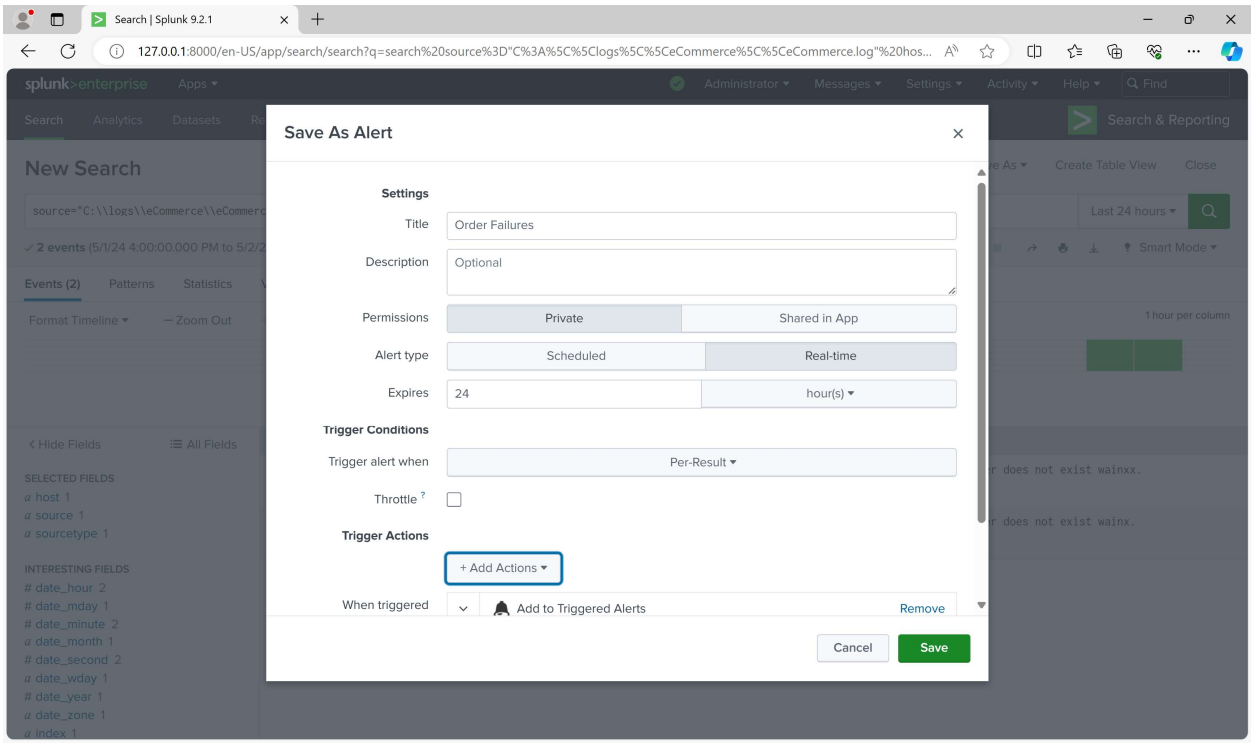

Search | Splunk 9.2.1
TEST | Splunk 9.2.1
127.0.0.1
127.0.0.1:8000/en-US/app/launcher/search?q=search%20source%3D"C%3A%5C%5Clogs%5C%5CeCommerce%5C%5CeCommerce.log"%20h...
splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Home
Home
New Search
Save As
Create Table View
Close
source="C:\\logs\\eCommerce\\eCommerce.log" host="WinDev2404Eval" sourcetype="log4j" com.example.demo.controllers.ordercontroller failure
All time
1 event (before 5/2/24 11:53:21.000 AM)
No Event Sampling
Job
Smart Mode
Events (1)
Patterns
Statistics
Visualization
Format Timeline
Zoom Out
Zoom to Selection
Deselect
1 millisecond per column
List
Format
50 Per Page
Hide Fields
All Fields
SELECTED FIELDS
a host 1
a source 1
a sourcetype 1
INTERESTING FIELDS
# date_hour 1
# date_mday 1
# date_minute 1
a date_month 1
# date_second 1
a date_wday 1
# date_year 1
a date_zone 1
a index 1
Time
Event
5/2/24 2:44:12.633 PM
05-02-2024 14:44:12.633 com.example.demo.controllers.OrderController [ERROR] - Failure : user does not exist wainx.
host = WinDev2404Eval source = C:\logs\eCommerce\eCommerce.log sourcetype = log4j

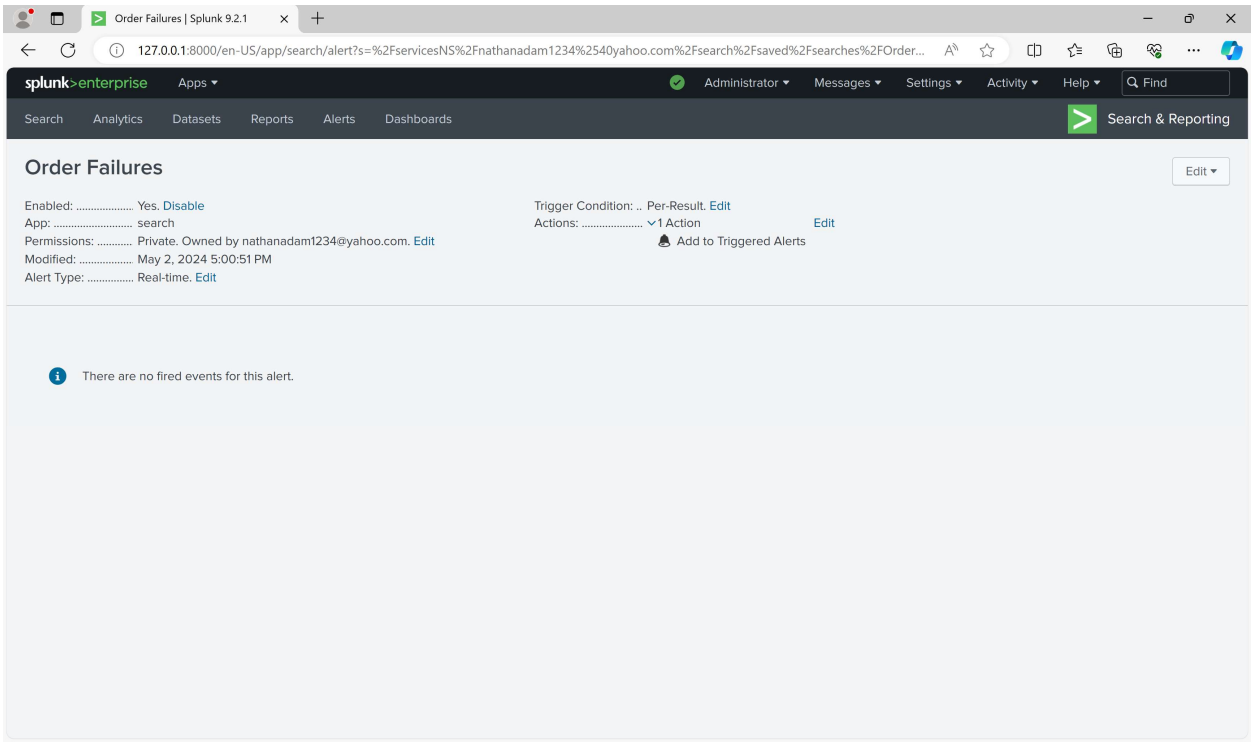

Search | Splunk 9.2.1
TEST | Splunk 9.2.1
127.0.0.1
127.0.0.1:8000/en-US/app/launcher/search?q=search%20source%3D"C%3A%5C%5Clogs%5C%5CeCommerce%5C%5CeCommerce.log"%20h...
splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Home
New Search
Save As
Create Table View
Close
source="C:\\logs\\eCommerce\\eCommerce.log" host="WinDev2404Eval" sourcetype="log4j" com.example.demo.controllers.itemcontroller Success
All time
3 events (before 5/2/24 11:54:01.000 AM)
No Event Sampling
Job
Smart Mode
Events (3)
Patterns
Statistics
Visualization
Format Timeline
Zoom Out
Zoom to Selection
Deselect
1 second per column
List
Format
50 Per Page
Hide Fields
All Fields
SELECTED FIELDS
a host 1
a source 1
a sourcetype 1
INTERESTING FIELDS
# date_hour 1
# date_mday 1
# date_minute 2
a date_month 1
# date_second 3
a date_wday 1
# date_year 1
a date_zone 1
a index 1
Time
Event
5/2/24 2:47:27.251 PM
05-02-2024 14:47:27.251 com.example.demo.controllers.ItemController [INFO] - Success : found 1 items for name Round Widget.
host = WinDev2404Eval source = C:\logs\eCommerce\eCommerce.log sourcetype = log4j
5/2/24 2:46:49.503 PM
05-02-2024 14:46:49.503 com.example.demo.controllers.ItemController [INFO] - Success : item id 1 found.
host = WinDev2404Eval source = C:\logs\eCommerce\eCommerce.log sourcetype = log4j
5/2/24 2:46:46.942 PM
05-02-2024 14:46:46.942 com.example.demo.controllers.ItemController [INFO] - Success : 2 items found.
host = WinDev2404Eval source = C:\logs\eCommerce\eCommerce.log sourcetype = log4j

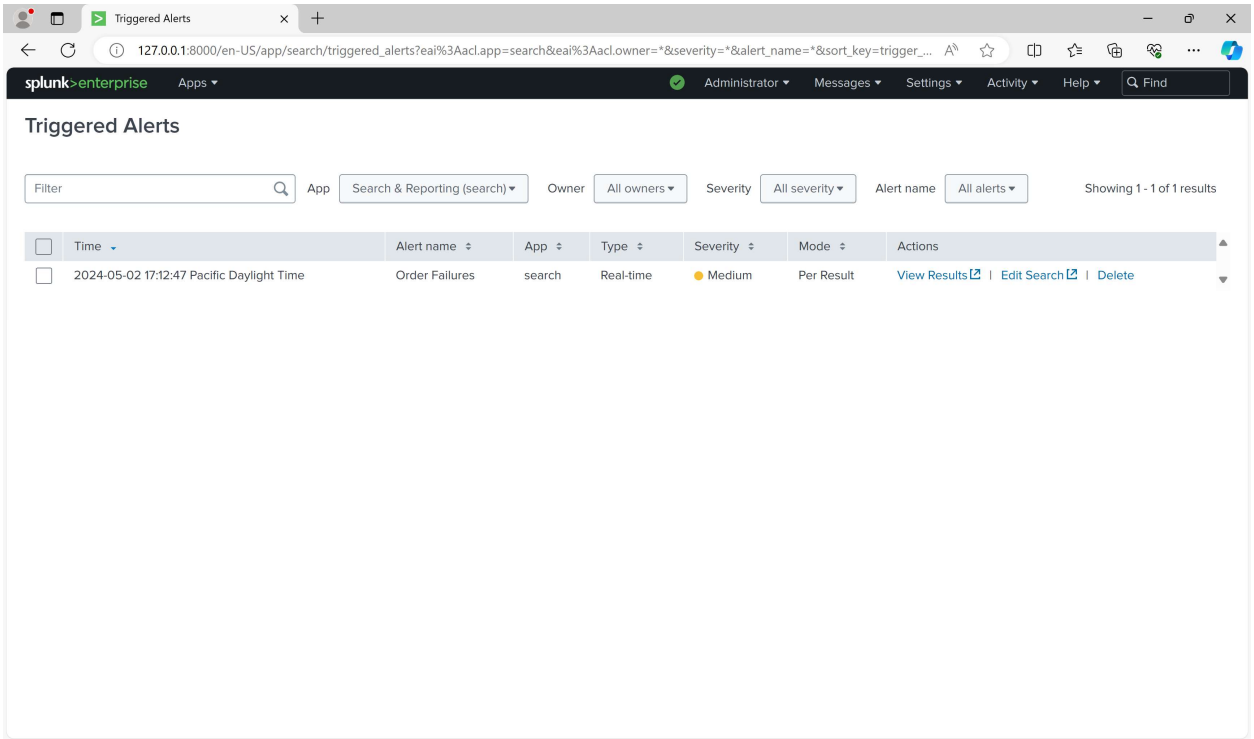

Search | Splunk 9.2.1
TEST | Splunk 9.2.1
127.0.0.1
127.0.0.1:8000/en-US/app/launcher/search?q=search%20source%3D"C%3A%5C%5Clogs%5C%5CeCommerce%5C%5CeCommerce.log"%20h...
splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Home
New Search
Save As
Create Table View
Close
source="C:\\logs\\eCommerce\\eCommerce.log" host="WinDev2404Eval" sourcetype="log4j" com.example.demo.controllers.itemcontroller Failure
All time
2 events (before 5/2/24 11:54:19.000 AM)
No Event Sampling
Job
Smart Mode
Events (2)
Patterns
Statistics
Visualization
Format Timeline
Zoom Out
Zoom to Selection
Deselect
1 second per column
List
Format
50 Per Page
Hide Fields
All Fields
SELECTED FIELDS
a host 1
a source 1
a sourcetype 1
INTERESTING FIELDS
# date_hour 1
# date_mday 1
# date_minute 2
a date_month 1
# date_second 2
a date_wday 1
# date_year 1
a date_zone 1
a index 1
Time
Event
5/2/24 2:47:24.158 PM
05-02-2024 14:47:24.158 com.example.demo.controllers.ItemController [ERROR] - Failure : item does not exist for name Round Widge
txxxx.
host = WinDev2404Eval source = C:\logs\eCommerce\eCommerce.log sourcetype = log4j
5/2/24 2:46:51.579 PM
05-02-2024 14:46:51.579 com.example.demo.controllers.ItemController [ERROR] - Failure : item id 111 does not exist.
host = WinDev2404Eval source = C:\logs\eCommerce\eCommerce.log sourcetype = log4j

# Alerts


Search | Splunk 9.2.1
127.0.0.1:8000/en-US/app/search/search?q=search%20source%3D"C%3A%5C%5Clogs%5C%5CeCommerce%5C%5CeCommerce.log"%20hos...
splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Reporting
New Search
Save As
Create Table View
Close
source="C:\\logs\\eCommerce\\eCommerce.log" host="WINDEV2404EVAL" sourcetype="log4j" com.example.demo.controllers.ordercontroller Failure
Last 24 hours
2 events (5/1/24 4:00:00.000 PM to 5/2/24 4:58:42.000 PM)
No Event Sampling
Job
Smart Mode
Events (2)
Patterns
Statistics
Visualization
Format Timeline
Zoom Out
Zoom to Selection
Deselect
1 hour per column
List
Format
50 Per Page
Hide Fields
All Fields
SELECTED FIELDS
a host 1
a source 1
a sourcetype 1
INTERESTING FIELDS
# date_hour 2
# date_mday 1
# date_minute 2
a date_month 1
# date_second 2
a date_wday 1
# date_year 1
a date_zone 1
a index 1
Time
Event
5/2/24 3:27:27.051 PM
05-02-2024 15:27:27.051 com.example.demo.controllers.OrderController [ERROR] - Failure : user does not exist wainxx.
host = WinDev2404Eval source = C:\logs\eCommerce\eCommerce.log sourcetype = log4j
5/2/24 2:44:12.633 PM
05-02-2024 14:44:12.633 com.example.demo.controllers.OrderController [ERROR] - Failure : user does not exist wainx.
host = WinDev2404Eval source = C:\logs\eCommerce\eCommerce.log sourcetype = log4j


Search | Splunk 9.2.1
127.0.0.1:8000/en-US/app/search/search?q=search%20source%3D"C%3A%5C%5Clogs%5C%5CeCommerce%5C%5CeCommerce.log"%20hos...
Save As Alert
Settings
Title
Order Failures
Description
Optional
Permissions
Private
Shared in App
Alert type
Scheduled
Real-time
Expires
24
hour(s)
Trigger Conditions
Trigger alert when
Per-Result
Throttle
Trigger Actions
+ Add Actions
When triggered
Add to Triggered Alerts
Remove
Cancel
Save


Order Failures | Splunk 9.2.1
127.0.0.1:8000/en-US/app/search/alert?s=%2FservicesNS%2Fnathanadam1234%2540yahoo.com%2Fsearch%2Fsaved%2Fsearches%2FOrder...
splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Reporting
Order Failures
Edit
Enabled: ..... Yes. Disable
App: ..... search
Permissions: ..... Private. Owned by nathanadam1234@yahoo.com. Edit
Modified: ..... May 2, 2024 5:00:51 PM
Alert Type: ..... Real-time. Edit
Trigger Condition: .. Per-Result. Edit
Actions: ..... 1 Action Edit
Add to Triggered Alerts
There are no fired events for this alert.


Triggered Alerts
127.0.0.1:8000/en-US/app/search/triggered_alerts?eai%3Aacl.app=search&eai%3Aacl.owner=*&severity=*&alert_name=*&sort_key=trigger_...
splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Triggered Alerts
Filter
App
Search & Reporting (search)
Owner
All owners
Severity
All severity
Alert name
All alerts
Showing 1 - 1 of 1 results
Time
Alert name
App
Type
Severity
Mode
Actions
2024-05-02 17:12:47 Pacific Daylight Time
Order Failures
search
Real-time
Medium
Per Result
View Results | Edit Search | Delete