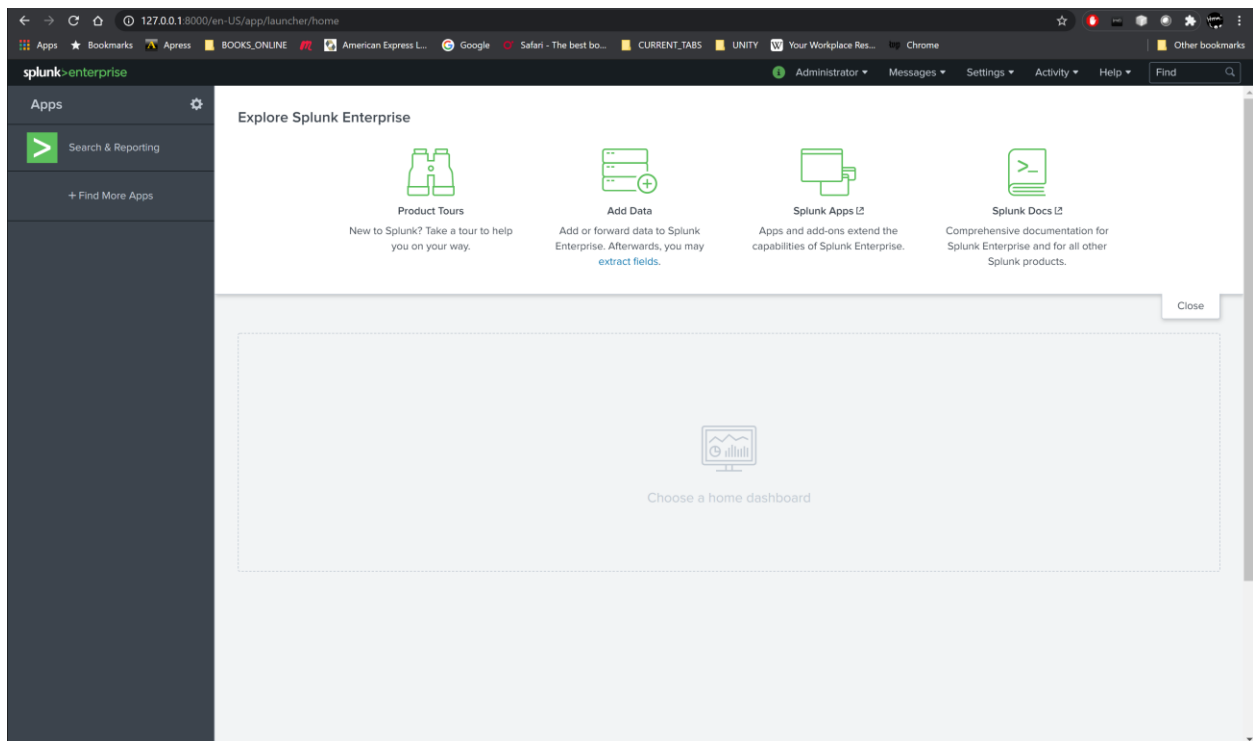


Splunk

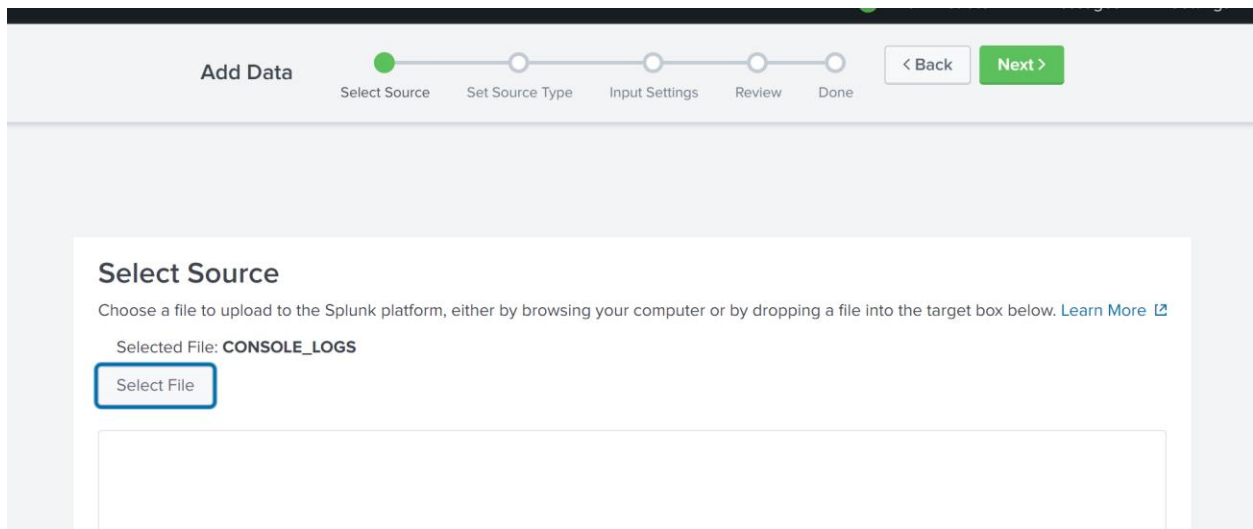
# Splunk

## Using Splunk

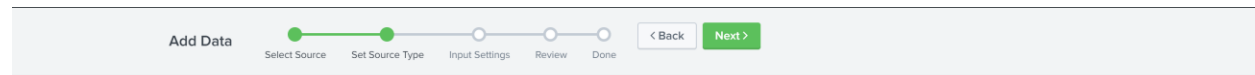
- Installed Splunk
- Working in browser on local machine:



- Uploaded CONSOLE\_LOGS



## Adding my CONSOLE\_LOGS



Before indexing. If the events look correct and have the right timestamps, click Next. If you cannot find an appropriate source type for

View Event Summary

List ▾	Format	20 Per Page ▾	< Prev	1	2	3	4	Next >
	Time	Event						
1	3/25/21 6:02:06.522 PM	2021-03-25 18:02:06.522 INFO 71428 --- [main] com.example.demo.SareetaApplication : Starting SareetaApplication on DESKTOP-G57UGNQ with PID 71428 (D:\2021_A\ONLINE_COURSES\UDACITY\JWOND\PROJECTS\ECOMMERCE_WS\nd035-c4-Security-and-DevOps\starter_code\target\classes started by lafig in D:\2021_A\ONLINE_COURSES\UDACITY\JWOND\PROJECTS\ECOMMERCE_WS\nd035-c4-Security-and-DevOps\starter_code)						
2	3/25/21 6:02:06.523 PM	2021-03-25 18:02:06.523 INFO 71428 --- [main] com.example.demo.SareetaApplication : No active profile set, falling back to default profiles: default						
3	3/25/21 6:02:06.856 PM	2021-03-25 18:02:06.856 INFO 71428 --- [main] .s.d.r.c.RepositoryConfigurationDelegate : Bootstrapping Spring Data JPA repositories in DEFAULT mode.						
4	3/25/21 6:02:06.895 PM	2021-03-25 18:02:06.895 INFO 71428 --- [main] .s.d.r.c.RepositoryConfigurationDelegate : Finished Spring Data repository scanning in 32ms. Found 4 JPA repository interfaces.						
5	3/25/21 6:02:07.355 PM	2021-03-25 18:02:07.355 INFO 71428 --- [main] o.s.b.w.embedded.tomcat.TomcatWebServer : Tomcat initialized with port(s): 8080 (http)						
6	3/25/21 6:02:07.362 PM	2021-03-25 18:02:07.362 INFO 71428 --- [main] o.apache.catalina.core.StandardService : Starting service [Tomcat]						
7	3/25/21 6:02:07.362 PM	2021-03-25 18:02:07.362 INFO 71428 --- [main] org.apache.catalina.core.StandardEngine : Starting Servlet engine: [Apache Tomcat/9.0.37]						
8	3/25/21	2021-03-25 18:02:07.462 INFO 71428 --- [main] o.a.c.c.C.[Tomcat].[localhost].[/] : Initializing Spring embedded WebApplicationContext						

- Review of file:

## Review

Input Type ..... Uploaded File  
 File Name ..... CONSOLE\_LOGS  
 Source Type ..... eCommerce\_Console\_Logs  
 Host ..... DESKTOP-G57UGNQ  
 Index ..... Default

## Indexing and Searching

Searching for all lines with \*Exception\*

**New Search** Save As Create Table View Close

source="CONSOLE\_LOGS" host="DESKTOP-G57UGNQ" sourcetype="eCommerce\_Console\_Logs" | search \*Exception

✓ 3 events (before 3/25/21 9:25:26.000 PM) No Event Sampling

Job Format Timeline Zoom Out Zoom to Selection Deselect 1 minute per column

Format Timeline Zoom Out Zoom to Selection Deselect 1 minute per column

List Format 20 Per Page

< Hide Fields All Fields

SELECTED FIELDS

- host 1
- source 1
- sourcetype 1

INTERESTING FIELDS

- # date\_hour 1
- # date\_mday 1
- # date\_minute 2
- # date\_month 1
- # date\_second 3
- # date\_wday 1
- # date\_year 1
- # date\_zone 1
- # index 1
- # linecount 1
- # punct 3
- # splunk\_server 1

Time	Event
3/25/21 6:33:46.450 PM	2021-03-25 18:33:46.450 WARN 71428 --- [nio-8080-exec-5] .w.s.m.s.DefaultHandlerExceptionResolver : Resolved [org.springframework.web.HttpRequestMethodNotSupportedException: Request method 'GET' not supported] host = DESKTOP-G57UGNQ   source = CONSOLE_LOGS   sourcetype = eCommerce_Console_Logs
3/25/21 6:02:45.230 PM	2021-03-25 18:02:45.230 INFO 71428 --- [nio-8080-exec-3] com.example.demo.service.UserService : UserService.prepareNewUser - DuplicateUsernameException. host = DESKTOP-G57UGNQ   source = CONSOLE_LOGS   sourcetype = eCommerce_Console_Logs
3/25/21 6:02:09.003 PM	2021-03-25 18:02:09.003 INFO 71428 --- [main] o.s.s.web.DefaultSecurityFilterChain : Creating filter chain: any request, [org.springframework.security.web.context.request.async.WebAsyncManagerIntegrationFilter@da11873, org.springframework.security.web.context.SecurityContextPersistenceFilter@3346e986, org.springframework.security.web.header.HeaderWriterFilter@2079fcfc, org.springframework.security.web.filter.CorsFilter@39159b14, org.springframework.security.web.authentication.logout.LogoutFilter@560be8c0, com.example.demo.security.JWTAuthenticationFilter@57ab4b33, com.example.demo.security.JWTAuthenticationVerificationFilter@43b2e7db, org.springframework.security.web.savedrequest.RequestCacheAwareFilter@126d0868, org.springframework.security.web.servletapi.SecurityContextHolderAwareRequestFilter@12a9e864, org.springframework.security.web.authentication.AnonymousAuthenticationFilter@46d51d5e, org.springframework.security.web.session.SessionManagementFilter@7865cc83, org.springframework.security.web.access.ExceptionTranslationFilter@3e1897d, org.springframework.security.web.access.intercept.FilterSecurityInterceptor@84cd310] host = DESKTOP-G57UGNQ   source = CONSOLE_LOGS   sourcetype = eCommerce_Console_Logs

- All logging activities from Controllers:

**New Search** Save As Create Table View Close

source="CONSOLE\_LOGS" host="DESKTOP-G57UGNQ" sourcetype="eCommerce\_Console\_Logs" | search \*Controller

✓ 22 events (before 3/25/21 9:28:34.000 PM) No Event Sampling

Job Format Timeline Zoom Out Zoom to Selection Deselect 1 minute per column

Format Timeline Zoom Out Zoom to Selection Deselect 1 minute per column

List Format 20 Per Page

< Hide Fields All Fields

SELECTED FIELDS

- host 1
- source 1
- sourcetype 1

INTERESTING FIELDS

- # date\_hour 1
- # date\_mday 1
- # date\_minute 15
- # date\_month 1
- # date\_second 14
- # date\_wday 1
- # date\_year 1
- # date\_zone 1
- # index 1
- # linecount 1
- # punct 5
- # splunk\_server 1
- # timeendpos 2
- # timestamppos 1

Time	Event
3/25/21 6:40:21.867 PM	2021-03-25 18:40:21.867 INFO 71428 --- [nio-8080-exec-1] c.e.demo.controllers.OrderController : OrderController:getOrdersForUser - invoked host = DESKTOP-G57UGNQ   source = CONSOLE_LOGS   sourcetype = eCommerce_Console_Logs
3/25/21 6:37:30.954 PM	2021-03-25 18:37:30.954 INFO 71428 --- [nio-8080-exec-9] c.e.demo.controllers.OrderController : OrderController:submit - invoked host = DESKTOP-G57UGNQ   source = CONSOLE_LOGS   sourcetype = eCommerce_Console_Logs
3/25/21 6:34:13.336 PM	2021-03-25 18:34:13.336 INFO 71428 --- [nio-8080-exec-6] c.e.demo.controllers.CartController : CartController:removeFromCart - invoked host = DESKTOP-G57UGNQ   source = CONSOLE_LOGS   sourcetype = eCommerce_Console_Logs
3/25/21 6:30:09.350 PM	2021-03-25 18:30:09.350 INFO 71428 --- [nio-8080-exec-1] c.e.demo.controllers.CartController : CartController:addToCart - sending back cart items. host = DESKTOP-G57UGNQ   source = CONSOLE_LOGS   sourcetype = eCommerce_Console_Logs
3/25/21 6:30:09.346 PM	2021-03-25 18:30:09.346 INFO 71428 --- [nio-8080-exec-1] c.e.demo.controllers.CartController : CartController:addToCart - invoked host = DESKTOP-G57UGNQ   source = CONSOLE_LOGS   sourcetype = eCommerce_Console_Logs
3/25/21 6:28:23.644 PM	2021-03-25 18:28:23.644 INFO 71428 --- [nio-8080-exec-9] c.e.demo.controllers.CartController : CartController:addToCart - sending back cart items. host = DESKTOP-G57UGNQ   source = CONSOLE_LOGS   sourcetype = eCommerce_Console_Logs
3/25/21 6:28:23.624 PM	2021-03-25 18:28:23.624 INFO 71428 --- [nio-8080-exec-9] c.e.demo.controllers.CartController : CartController:addToCart - invoked host = DESKTOP-G57UGNQ   source = CONSOLE_LOGS   sourcetype = eCommerce_Console_Logs
3/25/21 6:23:51.151 PM	2021-03-25 18:23:51.151 INFO 71428 --- [nio-8080-exec-6] c.e.demo.controllers.ItemController : ItemController:getItemsByName - invoked host = DESKTOP-G57UGNQ   source = CONSOLE_LOGS   sourcetype = eCommerce_Console_Logs

## Alerts

- The plan is to set up an alert if we see “bad request returned” in the logs

## Save As Alert

Settings

Title

Bad Request Returned

Description

Reports if we see the "bad requests" in our logs

Permissions

Private

Shared in App

Alert type

Scheduled

Real-time

Run every hour ▾

At 

0 ▾

 minutes past the hour

Expires

24

hour(s) ▾

Trigger Conditions

Trigger alert when

Number of Results ▾

is greater than ▾

5

Trigger

Once

For each result

Throttle ?

☒

Suppress triggering for

60

second(s) ▾

Trigger Actions

Cancel

Save

4

## Save As Alert



Send email

Remove

To nyguerillagirl@gmail.com

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

Priority Highest ▾

Subject Splunk Alert: Too many Bad Reque

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

Message The alert condition for '\$name\$' was triggered.

Include ☒ Link to Alert ☒ Link to Results  
☐ Search String ☐ Inline [Table](#) ▾  
☐ Trigger Condition ☐ Attach CSV  
☐ Trigger Time ☐ Attach PDF  
☒ Allow Empty Attachment

Type HTML &amp; Plain Text Plain Text

Cancel

Save

## Bad Request Returned

Reports if we see the "bad requests" in our logs

Enabled: ..... Yes. [Disable](#)

App: ..... search

Permissions: ..... Private. Owned by figgy. [Edit](#)

Modified: ..... Mar 25, 2021 9:39:34 PM

Alert Type: ..... Scheduled. Hourly, at 0 minutes past the hour. [Edit](#)Trigger Condition: .. Number of Results is > 5. [Edit](#)Actions: ..... ▾ 1 Action [Edit](#)

Send email



There are no fired events for this alert.