

Splunk4Admins - Advanced Data Routing with Forwarders and Ingest Actions

Lab Guide

Overview

This lab guide contains the hands-on exercises for the *Splunk4Admins - Advanced Data Routing with Forwarders and Ingest Actions* workshop. Before proceeding with these exercises, please ensure that you have a copy of the workshop slide deck, which will help to put into context the tasks you are carrying out.

Download the workshop slide deck: <https://splk.it/S4A-ADR-Attendee>

Prerequisites

In order to complete these exercises, you will need your own Splunk instance. Splunk's hands-on workshops are delivered via the [Splunk Show portal](#) and you will need a splunk.com account in order to access this.

If you don't already have a Splunk.com account, please create one [here](#) before proceeding with the rest of the workshop.

Troubleshooting Connectivity

If you experience connectivity issues with accessing either your workshop environment or the event page, please try the following troubleshooting steps. If you still experience issues please reach out to the team running your workshop.

- **Use Google Chrome** (if you're not already)
- If the event page (i.e. <https://show.splunk.com/event/<eventID>>) didn't load when you clicked on the link, try **refreshing the page**
- **Disconnect from VPN** (if you're using one)
- **Clear your browser cache and restart your browser** (if using Google Chrome, go to: Settings > Privacy and security > Clear browsing data)
- **Try using private browsing mode** (e.g. Incognito in Google Chrome) to rule out any cache issues
- **Try using another computer** such as your personal computer - all you need is a web browser! Cloud platforms like AWS can often be blocked on corporate laptops.

Table of Contents

Overview.....	1
Prerequisites.....	1
⚠ Troubleshooting Connectivity.....	1
Exercise 1 – Creating a new indexes and setting source type.....	3
Description.....	3
Steps:.....	3
Part 1 - Creating New Indexes.....	3
Part 2 - Uploading sample data.....	5
Completion Tracker (Optional):.....	9
Exercise 2 – Creating a Ruleset in Ingest Actions.....	10
Description.....	10
Steps:.....	10
Part 1 - Creating Ruleset.....	10
Part 2 - Searching Events.....	11
Completion Tracker (Optional):.....	11
Exercise 3 – Investigating destinations in Ingest Actions.....	12
Description:.....	12
Steps:.....	12
Completion Tracker (Optional):.....	12
Links.....	13

Exercise 1 – Creating a new indexes and setting source type

Description

We will configure a new index and set the appropriate source type settings to parse our sample data

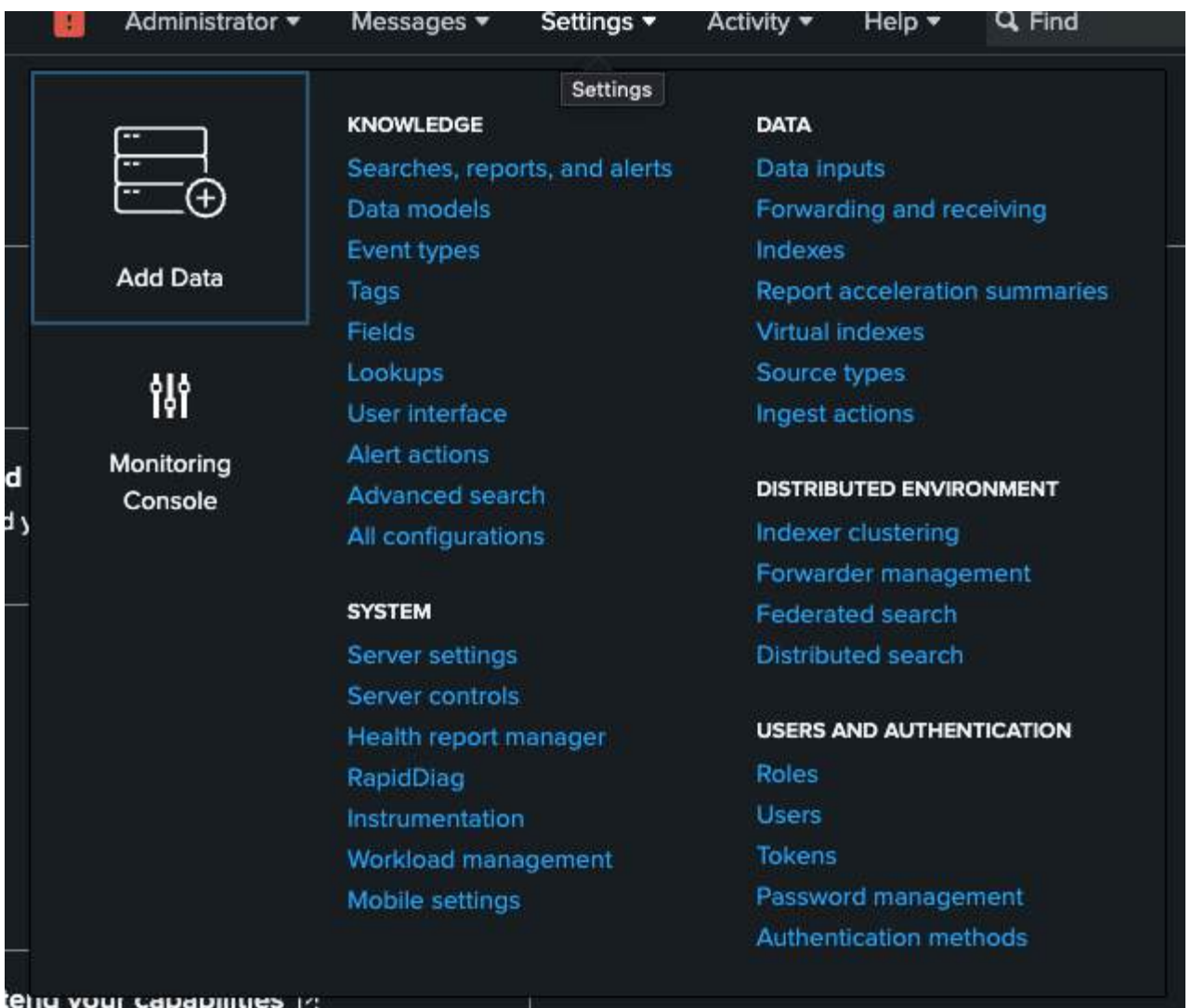
Steps:

Part 1 - Creating New Indexes

1. Click Settings



2. Click Indexes



3. Click "New Index"



4. In the index name enter "adr_error" and leave all other settings at their default

New Index

General Settings

Index Name

adr_error

Set index name (e.g., INDEX_NAME). Search using index=INDEX_NAME.

Index Data Type

Events

Metrics

The type of data to store (event-based or metrics).

Home Path

optional

Hot/warm db path. Leave blank for default (\$SPLUNK_DB/INDEX_NAME/db).

Cold Path

optional

Cold db path. Leave blank for default (\$SPLUNK_DB/INDEX_NAME/colddb).

Thawed Path

optional

Thawed/resurrected db path. Leave blank for default (\$SPLUNK_DB/INDEX_NAME/thaweddb).

Data Integrity Check

Enable

Disable

Enable this if you want Splunk to compute hashes on every slice of your data for the purpose of data integrity.

Max Size of Entire Index

500

GB

Maximum target size of entire index.

Max Size of Hot/Warm/Cold Bucket

auto

GB

Maximum target size of buckets. Enter 'auto_high_volume' for high-volume indexes.

Frozen Path

optional

Frozen bucket archive path. Set this if you want Splunk to automatically archive frozen buckets.

App

Splunk Platform (Hybrid Environment) 1.0.0

Storage Optimization

Tsidx Retention Policy

Enable Reduction

Disable Reduction

Warning: Do not enable reduction without understanding the full implications. It is extremely difficult to rebuild reduced buckets. [Learn More](#)

Reduce tsidx files older than

Days

Age is determined by the latest event in a bucket.

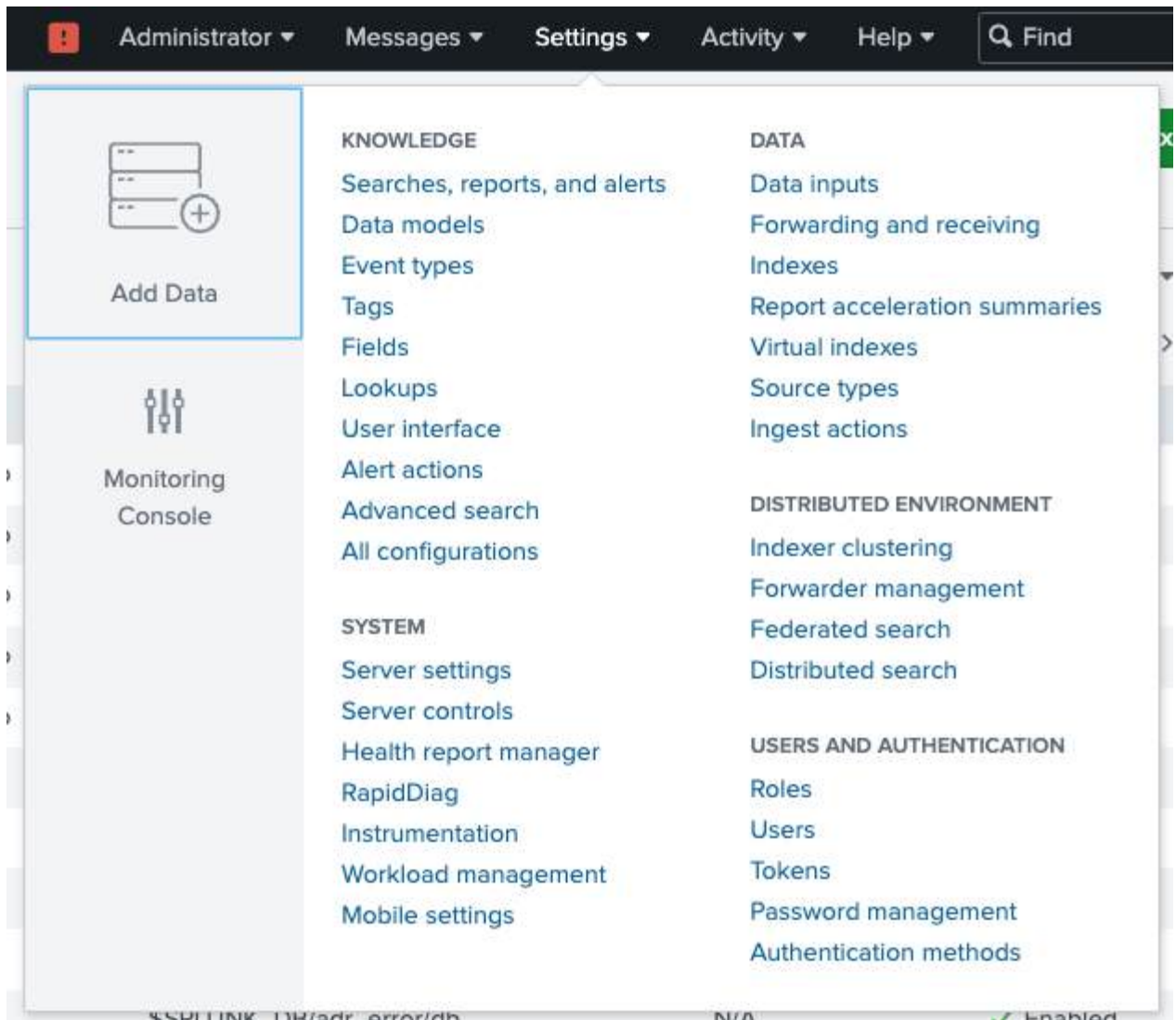
Save

Cancel

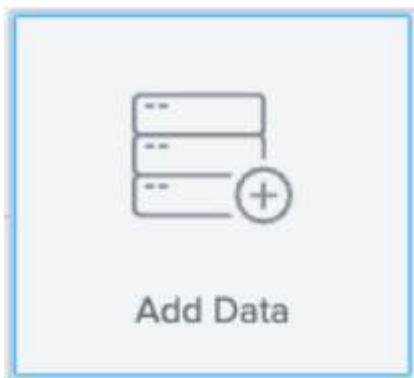
5. Verify the index has been created by clicking on "Settings" and "Indexes"

Part 2 - Uploading sample data

6. Click Settings



7. Click "Add Data" button



8. Click "Upload"

9. On the Select Source screen, click "Select File" and browse to the location you saved the "devops_sample.txt" file

Add Data

Select Source Set Source Type Input Settings Review Done

Select Source

Choose a file to upload to the Splunk platform, either by browsing your computer or by dropping a file into the target box below. [Learn More](#)

Selected File: **devops_sample.txt**

Select File

Drop your data file here

The maximum file upload size is 500 Mb

File Successfully Uploaded

FAQ

- > What kinds of files can the Splunk platform index?
- > What is a source?
- > How do I get remote data onto my Splunk platform instance?

10. Click **"Next"**

11. ON the "Set Source Type" screen expand **"Advanced"** on the far left

Source type: default ▾ **Save As**

> Event Breaks
> Timestamp
✓ Advanced

Name	Value	
SHOULD_LINEMERGE	false	×
LINE_BREAKER	(<u>[\r\n]+\n</u>)	×
TRUNCATE	260	×
TIME_PREFIX	^[\w+ <u>\]</u> \s	×
MAX_TIMESTAMP_LOOKAHEAD	31	×
TIME_FORMAT	<u>/B/Y, %H:%M:%S.%3Q</u>	×

[New setting](#)
[Copy to clipboard](#) **Apply settings**

12. Click **New Setting** to add and modify the following 6 Attributes

SHOULD_LINEMERGE false

LINE_BREAKER ([\r\n]+\n)

TRUNCATE 260

TIME_PREFIX ^[\w+\]\s

MAX_TIMESTAMP_LOOKAHEAD 31

TIME_FORMAT %d/B/Y, %H:%M:%S.%3Q

13. Click **"Apply settings"**

14. Note that the data in the event has been parsed correctly

The screenshot shows the Splunk configuration interface for a source type. On the left, the 'Advanced' settings are visible, including 'SHOULD_LINEMERGE' set to 'false', 'LINE_BREAKER' set to '\n', 'TRUNCATE' set to '200', 'TIME_PREFIX' set to '\d{4}-\d{2}-\d{2}', 'MAX_TIMESTAMP_LOOKAHEAD' set to '31', and 'TIME_FORMAT' set to '%Y/%m/%d %H:%M:%S'. On the right, a list of events is displayed, showing timestamps and event descriptions. The events are numbered 1 through 8, with timestamps ranging from 2/19/25 8:20:18.773 PM to 2/19/25 8:20:36.798 PM. The event descriptions include user login attempts, password changes, disk I/O warnings, and session logouts.

15. Click "Next"

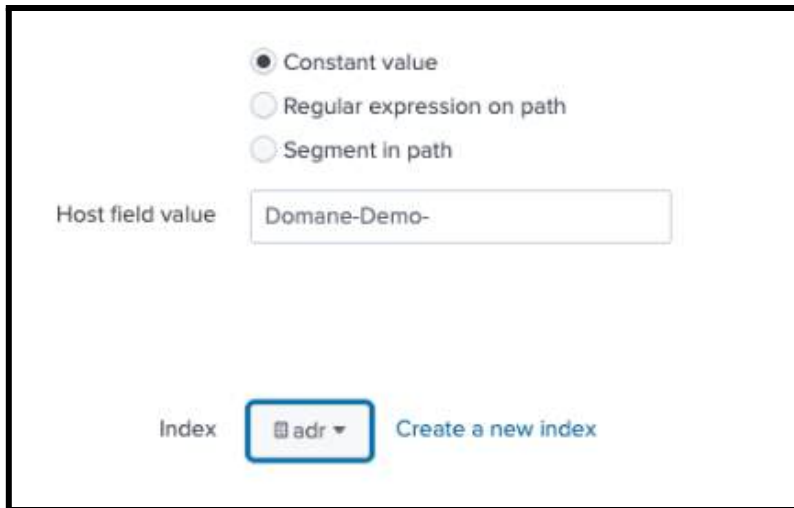
The screenshot shows the Splunk configuration progress bar. It consists of a horizontal line with five circular markers. The first marker is green and labeled 'Add Data'. The second marker is green and labeled 'Select Source'. The third marker is white and labeled 'Set Source Type'. The fourth marker is white and labeled 'Input Settings'. The fifth marker is white and labeled 'Review'. The sixth marker is white and labeled 'Done'. To the right of the progress bar are two buttons: '< Back' and 'Next >'. The 'Next >' button is highlighted in green.

16. On the Save Source Type pop-up enter the name as "bcg:dev"

The screenshot shows the 'Save Source Type' pop-up dialog. It has a title bar with a close button (X). The dialog contains four input fields: 'Name', 'Description', 'Category', and 'App'. The 'Name' field is highlighted with a blue border and contains the text 'bcg:dev'. The 'Description' field is empty. The 'Category' field is a dropdown menu with 'Custom' selected. The 'App' field is a dropdown menu with 'Search & Reporting' selected. At the bottom of the dialog are two buttons: 'Cancel' and 'Save'. The 'Save' button is highlighted in green.

17. Click Save

18. On the "Input settings" screen set the Index value to "**adr_error**"



Constant value
Regular expression on path
Segment in path

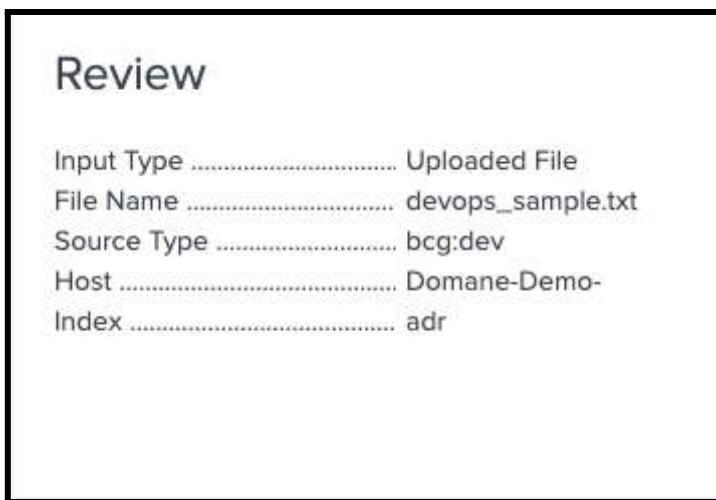
Host field value Domane-Demo-

Index adr Create a new index

19. Click Next

20. Review your settings, they should match the screenshot below

NOTE: the screenshot shows the index as "adr" but the event data should go to the "**adr_error**" index



Review

Input Type Uploaded File
File Name devops_sample.txt
Source Type bcg:dev
Host Domane-Demo-
Index adr

Completion Tracker (Optional):

You can use this drop down to track your progress of each exercise. This is completely optional, but may be a good indicator in more details or complex workshop scenarios.

Incomplete ▾

Exercise 2 – Creating a Ruleset in Ingest Actions

Description

In this exercise we will create a new ruleset to send specific event data to the adr_error index

Steps:

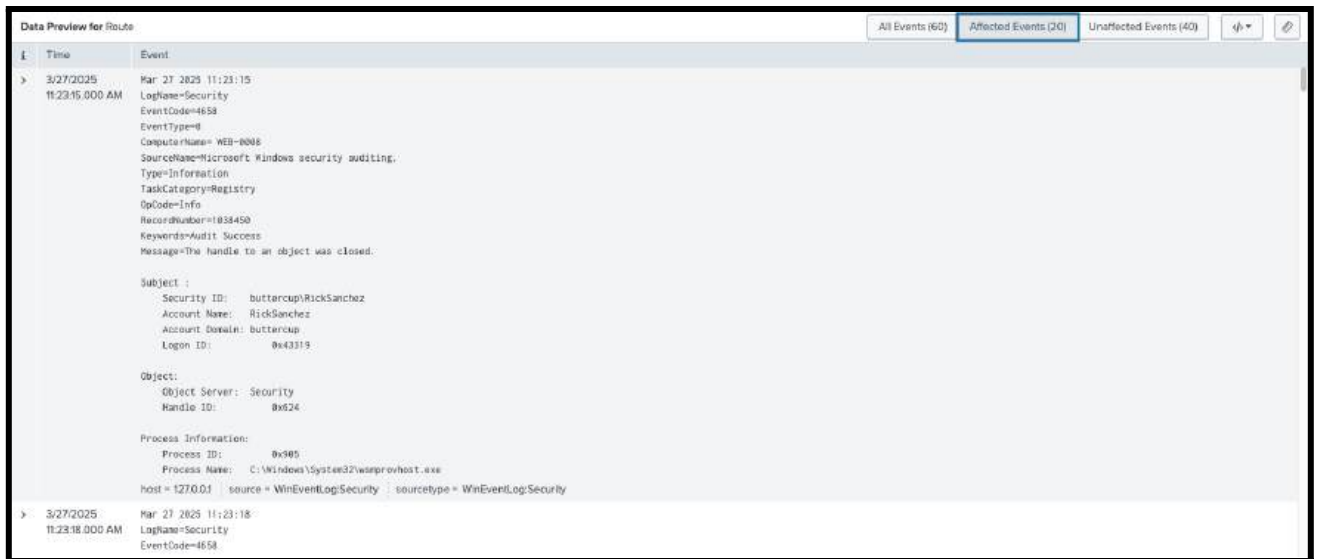
Part 1 - Creating Ruleset

1. Click **Settings**
2. Click **Ingest Actions**
3. Click **New Ruleset** button



4. Under the Event Stream section, set the following:
 - a. **Preview Using: Indexed Data**
 - b. **Sourcetype: WinEventLog**
 - c. **Sample Size: 5000**
 - d. **Time Range: Last 60 minutes**
5. Click Sample (It may take a moment to populate the event data)
6. Next Click **+Add Rule** and select **Set Index**
7. Under the Set Index section set the following
 - a. **Condition: Regex**
 - b. **Regular Expression: Application Error**
 - c. **Set index as: String**
 - i. **Value: adr_error**

8. In the Data Preview click Affected Events and review the index value



9. Click Save

Part 2 - Searching Events

10. Select Search and Reporting
11. In the search bar type: **index=adr_error**

NOTE: You may need to wait a minute or two for the event data to be updated

12. You should now see the Application Error events in the new index

Completion Tracker (Optional):

You can use this drop down to track your progress of each exercise. This is completely optional, but may be a good indicator in more details or complex workshop scenarios.

Incomplete ▾

Exercise 3 – Investigating destinations in Ingest Actions

Description:

In this quick lab, we will look at a predefined destination configured for an S3 bucket in Ingest Actions.

Steps:

1. Click **Settings**
2. Click **Ingest Actions**
3. Locate **WinEventLogSecurity_RouteS3** and click Edit
4. Under Event Stream click **Sample** (It may take a few moments to capture the events)
5. Review **All Events** and **Affected Events**
6. Once the events have returned Expand the "**Route to Destination**"

Note: We are using the regular expression to immediately send only the events that match the user "Rick Sanchez" to the AWS S3 bucket

7. Click Cancel

Completion Tracker (Optional):

You can use this drop down to track your progress of each exercise. This is completely optional, but may be a good indicator in more details or complex workshop scenarios.

Incomplete ▾

Links

Title	Link
Configuring New Source Types	https://lantern.splunk.com/Splunk_Platform/Product_Tips/Data_Management/Configuring_new_source_types
HTTP Event Collector	https://docs.splunk.com/Documentation/Splunk/latest/Data/UsetheHTTPEventCollector
About the Universal Forwarder	https://docs.splunk.com/Documentation/Forwarder/latest/Forwarder/Abouttheuniversalforwarder
Types of Forwarders	https://docs.splunk.com/Documentation/Splunk/latest/Forwarding/Typesofforwarders
Splunk OpenTelemetry	https://docs.splunk.com/observability/en/gdi/opentelemetry/opentelemetry.html
Splunk OTel with UF	https://docs.splunk.com/observability/en/gdi/opentelemetry/collector-with-the-uf.html#collector-with-the-uf
Inputs.conf	https://docs.splunk.com/Documentation/Splunk/latest/admin/Inputsconf
Outputs.conf	https://docs.splunk.com/Documentation/Splunk/latest/Admin/Outputsconf
Forwarding to Third Party systems	https://docs.splunk.com/Documentation/Splunk/latest/Forwarding/Forwarddatatothird-partysystems
Ingest Actions Rulesets	https://docs.splunk.com/Documentation/SVA/current/Architectures/IngestActions#Rulesets
MELT (Metrics, Events, Logs & Traces)	https://www.splunk.com/en_us/blog/learn/melt-metrics-events-logs-traces.html
Why Source types matter	https://docs.splunk.com/Documentation/Splunk/latest/Data/Whysourcetypesmatter