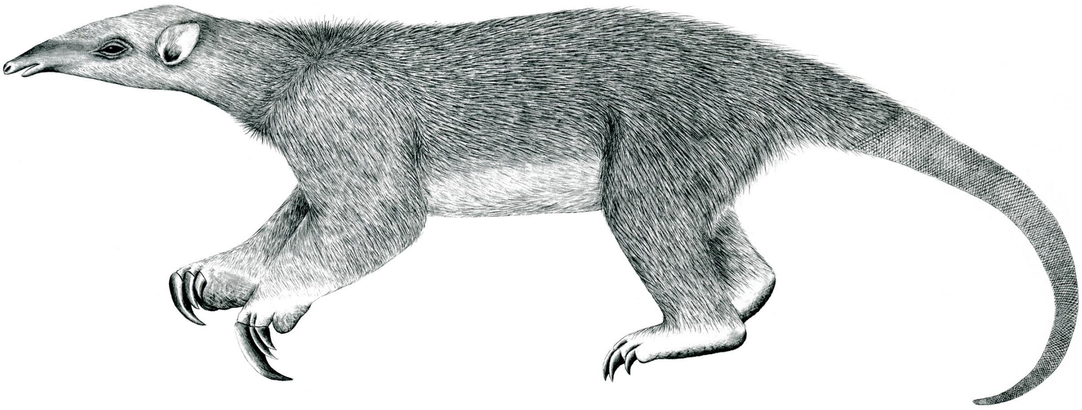
Tranalyzer2

Importing Tranalyzer Flows in Splunk

Type of Import: JSON Stream



Tranalyzer Development Team

Contents

1 Importing Tranalyzer Flows in Splunk

1.1 Prerequisites

- tranalyzer2-0.9.3 is installed with standard/default plugins,
- Splunk 6.5.x is installed, Splunk account exists,
- At least one network interface (Ethernet or WLAN) has network traffic.

1.2 Select Network Interface

Determine the network interface name by entering the following command:

```
ifconfig
```

at the terminal command line. In the output look for the interface name which has the IP address where the network traffic should be collected from:

```
en0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST>
mtu 1500 inet 10.20.6.79 netmask 0xfffffc00 broadcast 10.20.7.255
```

1.3 Configure Tranalyzer jsonSink Plugin

Go to *tranalyzer2-0.9.3/plugins/jsonSink/src/jsonSink.h* and set the configuration parameters as needed:

```
#define SOCKET_ON            1 // Whether to output to a socket (1) or file (0)
#define SOCKET_ADDR "127.0.0.1" // address of the socket
#define SOCKET_PORT        5000 // port of the socket
```

Set `SOCKET_ON` to `1` to configure the output to a socket. Set the IP address of the destination server which should receive the data stream. If the localhost will be the destination, leave the default setting `"127.0.0.1"`. Set the socket server port of the destination.

1.4 Recompile the jsonSink Plugin

Enter the following command:

```
tranalyzer2-0.9.3/plugins/jsonSink/autogen.sh
```

Make sure that the plugin is compiled successfully. In this case the following message will be shown at the command line:

```
Plugin jsonSink copied into USER_DIRECTORY/.tranalyzer/plugins
```

1.5 Start Tranalyzer2

Start generating flow records by launching Tranalyzer2 with the interface name determined on the previous step and setting a file name as the command line arguments by entering the command:

```
tranalyzer -i en0 -w test1 &
```

Note that the file name is optional for JSON stream import, if file name is not indicated the records will be shown in the standard output (besides being streamed over the configured TCP socket).

1.5.1 Check File Output

Check that the flow records are written to the file by entering the command:

```
tail -f test1_flows.txt
```

Flow records should be shown in the terminal.

1.5.2 Collect Traffic

Let Tranalyzer2 run and collect network traffic.

1.6 Start Splunk

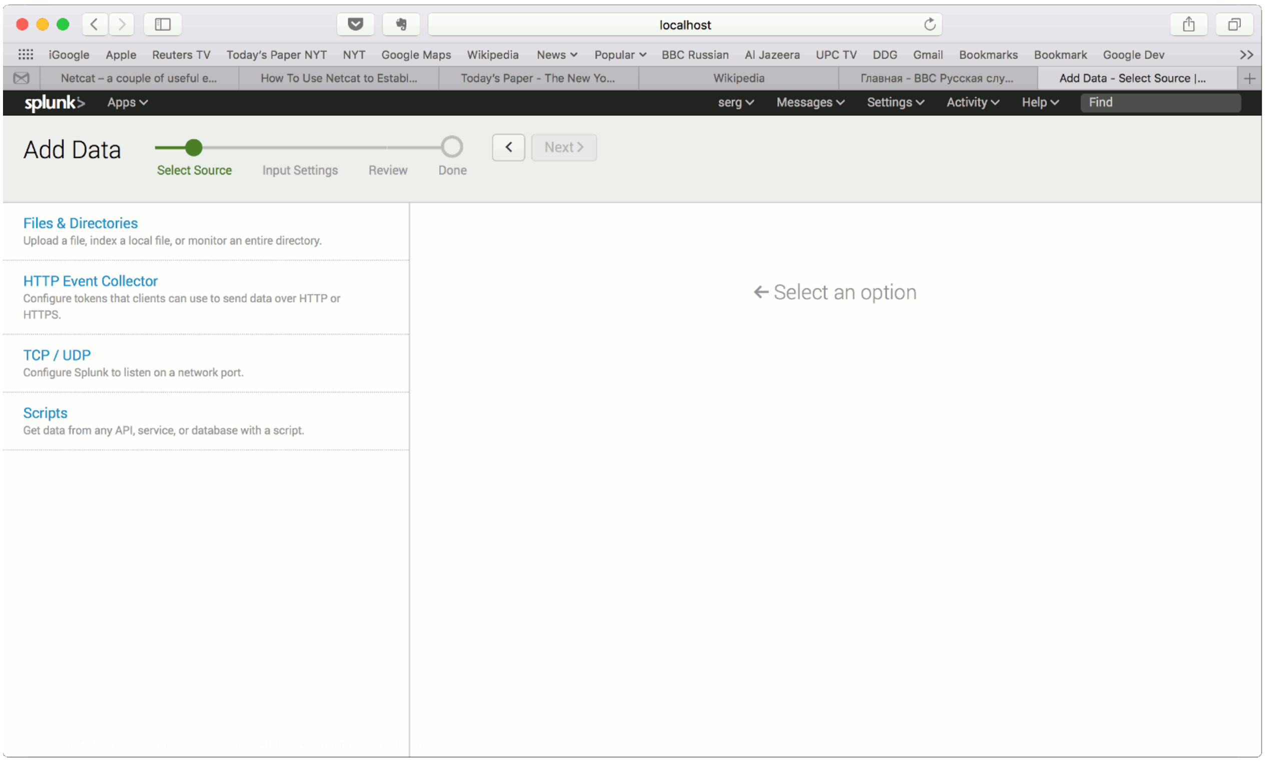
Start Splunk by entering the following command:

```
splunk start
```

in the directory where Splunk is installed. Wait for the confirmation message that Splunk is up and running:

```
The Splunk web interface is at http://splunk_hostname:8000
```

1.7 Login to Splunk, Import and Search Data



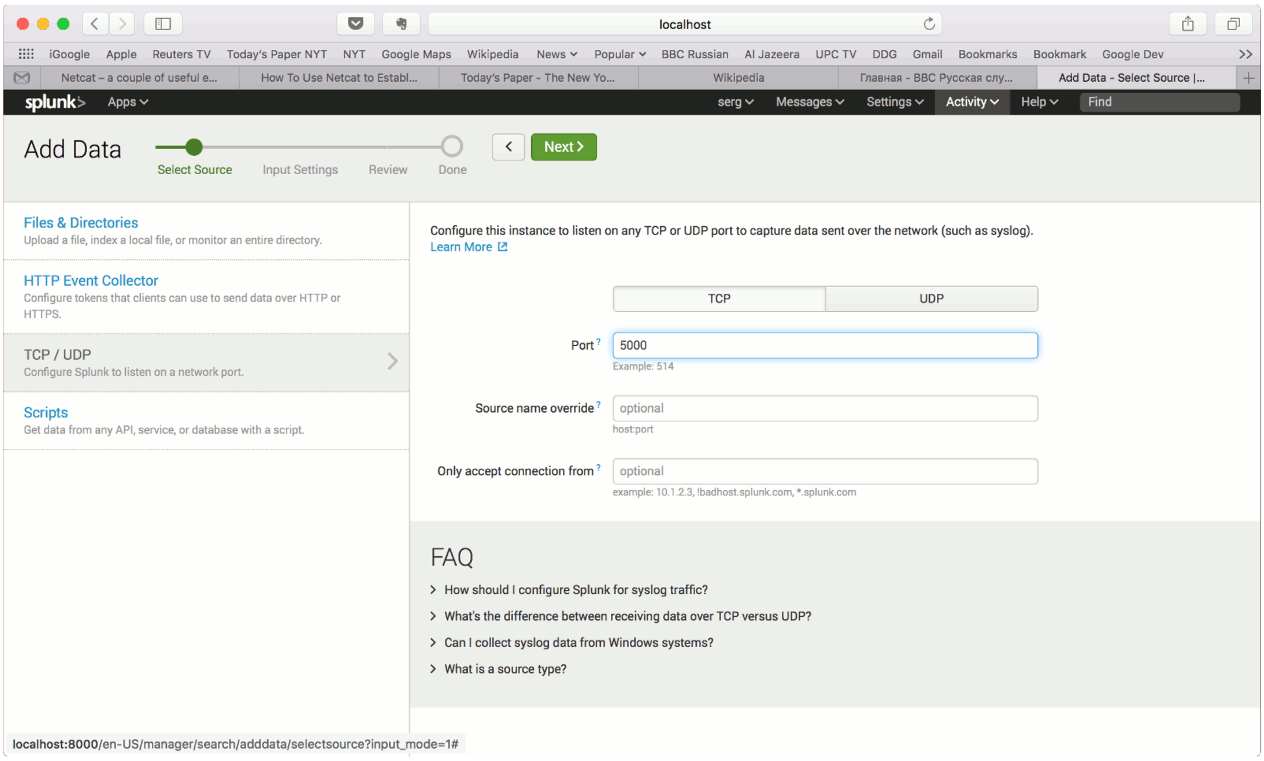
Files & Directories
Upload a file, index a local file, or monitor an entire directory.

HTTP Event Collector
Configure tokens that clients can use to send data over HTTP or HTTPS.

TCP / UDP
Configure Splunk to listen on a network port.

Scripts
Get data from any API, service, or database with a script.

Figure 1: *Select “Add Data”.*



Add Data

Select Source · Input Settings · Review · Done

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 Splunk to listen on a network port.

Scripts
Get data from any API, service, or database with a script.

Configure this instance to listen on any TCP or UDP port to capture data sent over the network (such as syslog).
Learn More

TCP | UDP

Port: 5000
Example: 514

Source name override: optional
host:port

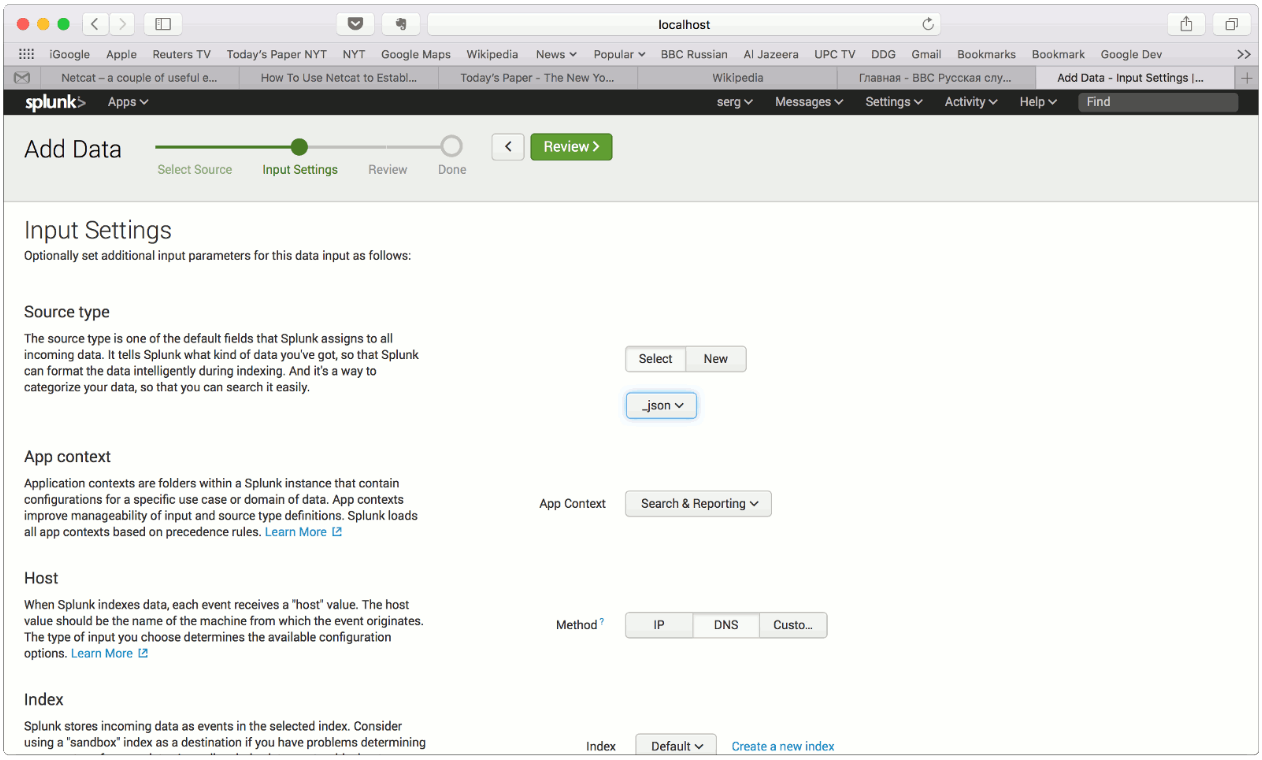
Only accept connection from: optional
example: 10.1.2.3, !badhost.splunk.com, *.splunk.com

FAQ

- How should I configure Splunk for syslog traffic?
- What's the difference between receiving data over TCP versus UDP?
- Can I collect syslog data from Windows systems?
- What is a source type?

localhost:8000/en-US/manager/search/adddata/selectsource?input_mode=1#

Figure 2: *Select "TCP/UDP" and set protocol to "TCP" and set the correct port number (same as in the Tranalyzer2 plugin configuration file, in this example — 5000).*



Add Data

Input Settings

Optionally set additional input parameters for this data input as follows:

Source type

The source type is one of the default fields that Splunk assigns to all incoming data. It tells Splunk what kind of data you've got, so that Splunk can format the data intelligently during indexing. And it's a way to categorize your data, so that you can search it easily.

Select | New

_json

App context

Application contexts are folders within a Splunk instance that contain configurations for a specific use case or domain of data. App contexts improve manageability of input and source type definitions. Splunk loads all app contexts based on precedence rules. Learn More

App Context: Search & Reporting

Host

When Splunk 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

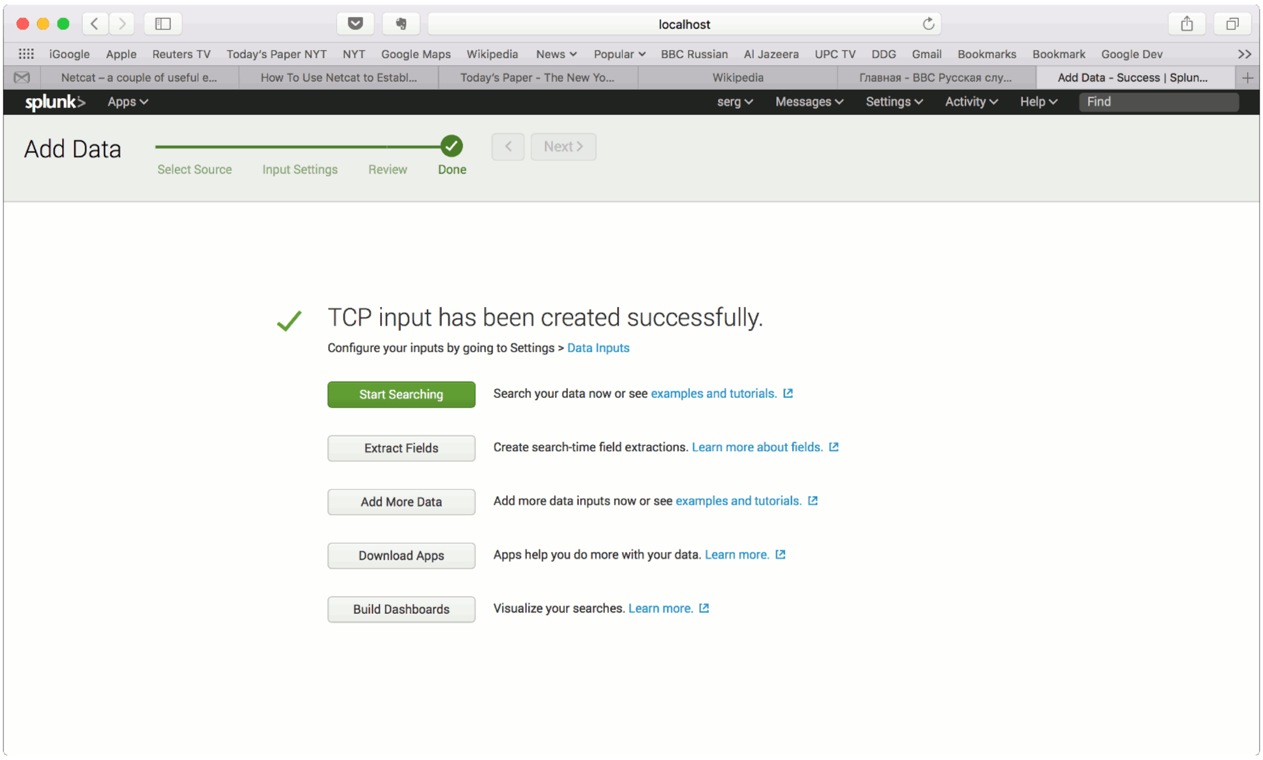
Method: IP | DNS | Custo...

Index

Splunk stores incoming data as events in the selected index. Consider using a "sandbox" index as a destination if you have problems determining

Index: Default | Create a new index

Figure 3: *Select "_json" as Source Type and proceed to "Review".*



TCP input has been created successfully.

Configure your inputs by going to Settings > Data Inputs

Search your data now or see examples and tutorials.

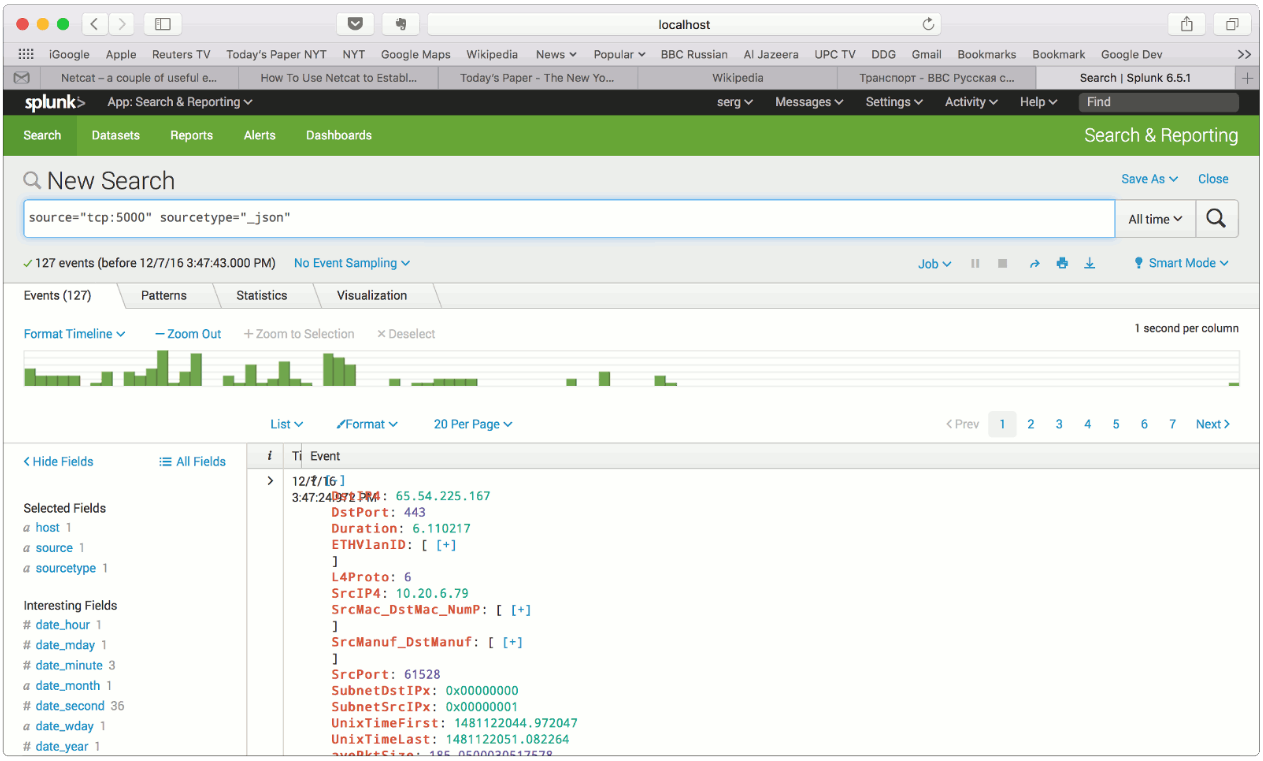
Create search-time field extractions. Learn more about fields.

Add more data inputs now or see examples and tutorials.

Apps help you do more with your data. Learn more.

Visualize your searches. Learn more.

Figure 4: *Select "Start Searching" to make sure that the data is being received by Splunk.*


localhost
iGoogle Apple Reuters TV Today's Paper NYT NYT Google Maps Wikipedia News Popular BBC Russian Al Jazeera UPC TV DDG Gmail Bookmarks Bookmark Google Dev
Netcat – a couple of useful e... How To Use Netcat to Establ... Today's Paper - The New Yo... Wikipedia Транспорт - BBC Русская с... Search | Splunk 6.5.1
splunk> App: Search & Reporting
serg Messages Settings Activity Help Find
Search Datasets Reports Alerts Dashboards
Search & Reporting
New Search
Save As Close
All time
Job
Smart Mode
Events (127) Patterns Statistics Visualization
Format Timeline — Zoom Out + Zoom to Selection × Deselect
1 second per column
List Format 20 Per Page
< Prev 1 2 3 4 5 6 7 Next >
< Hide Fields ☰ All Fields
i Ti Event

```
source="tcp:5000" sourcetype="_json"
```

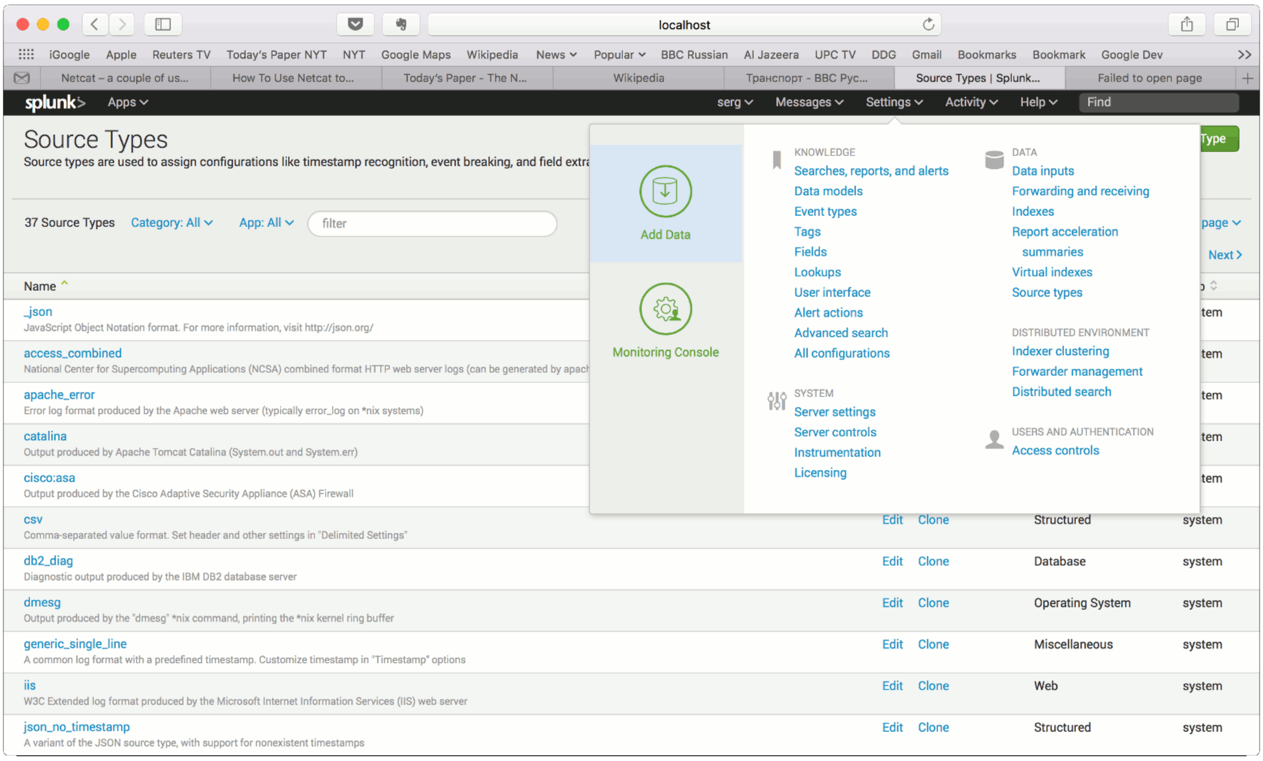
✓127 events (before 12/7/16 3:47:43.000 PM) No Event Sampling

Selected Fields
- a host 1
- a source 1
- a sourcetype 1

Interesting Fields
- # date_hour 1
- # date_mday 1
- # date_minute 3
- a date_month 1
- # date_second 36
- a date_wday 1
- # date_year 1

```
> 12/7/16    [+]
  3:47:24.972 PM  DstIP4: 65.54.225.167
     DstPort: 443
     Duration: 6.110217
     ETHVlanID: [ [+]
     ]
     L4Proto: 6
     SrcIP4: 10.20.6.79
     SrcMac_DstMac_NumP: [ [+]
     ]
     SrcManuf_DstManuf: [ [+]
     ]
     SrcPort: 61528
     SubnetDstIPx: 0x00000000
     SubnetSrcIPx: 0x00000001
     UnixTimeFirst: 1481122044.972047
     UnixTimeLast: 1481122051.082264
     avePktSize: 185.0500030517578
```

Figure 5: *Note that the data is being received, but the Tranalyzer2 specific data record field are not shown yet.*

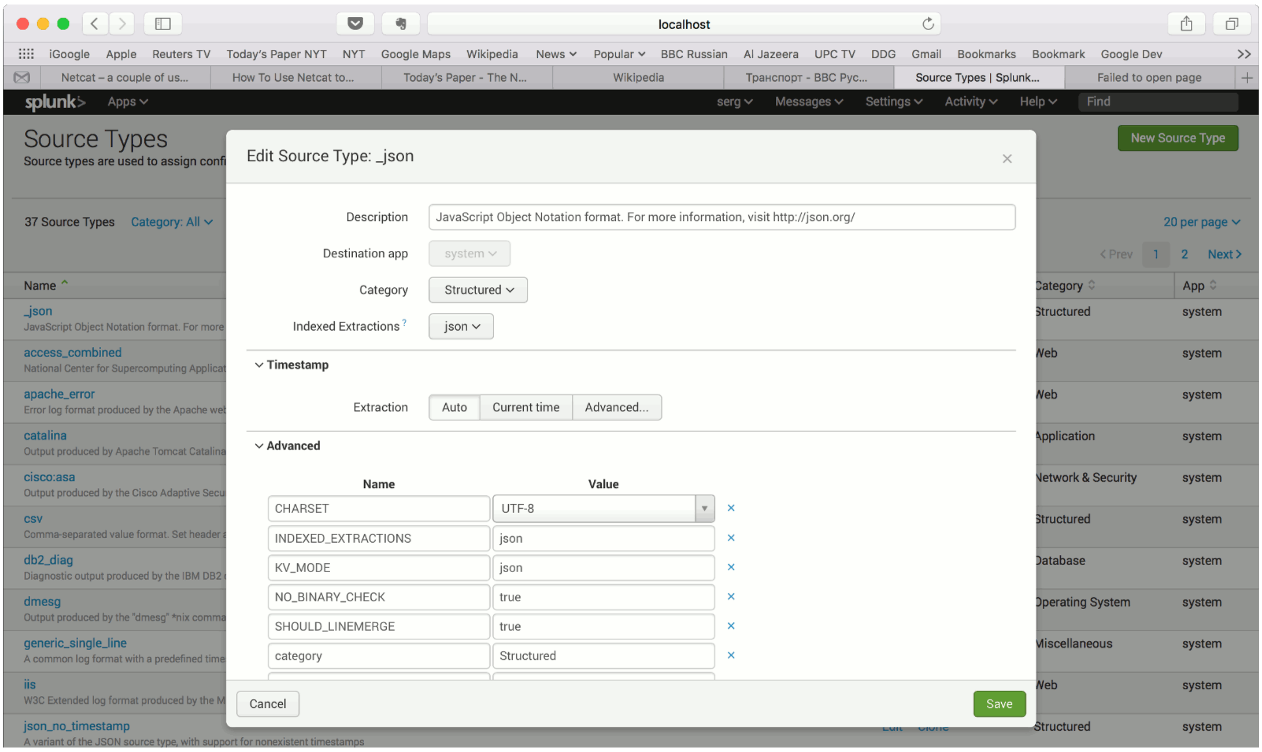


Source Types

Source types are used to assign configurations like timestamp recognition, event breaking, and field extra

Name ^				
_json JavaScript Object Notation format. For more information, visit http://json.org/				tem
access_combined National Center for Supercomputing Applications (NCSA) combined format HTTP web server logs (can be generated by apach				tem
apache_error Error log format produced by the Apache web server (typically error_log on *nix systems)				tem
catalina Output produced by Apache Tomcat Catalina (System.out and System.err)				tem
cisco:asa Output produced by the Cisco Adaptive Security Appliance (ASA) Firewall				tem
csv Comma-separated value format. Set header and other settings in "Delimited Settings"	Edit	Clone	Structured	system
db2_diag Diagnostic output produced by the IBM DB2 database server	Edit	Clone	Database	system
dmesg Output produced by the "dmesg" *nix command, printing the *nix kernel ring buffer	Edit	Clone	Operating System	system
generic_single_line A common log format with a predefined timestamp. Customize timestamp in "Timestamp" options	Edit	Clone	Miscellaneous	system
iis W3C Extended log format produced by the Microsoft Internet Information Services (IIS) web server	Edit	Clone	Web	system
json_no_timestamp A variant of the JSON source type, with support for nonexistent timestamps	Edit	Clone	Structured	system

Figure 6: *Go to "Settings"->"DATA"->"Source Types" and click on "_json" data source type to edit it.*



Edit Source Type: _json

Description: JavaScript Object Notation format. For more information, visit http://json.org/

Destination app: system

Category: Structured

Indexed Extractions: json

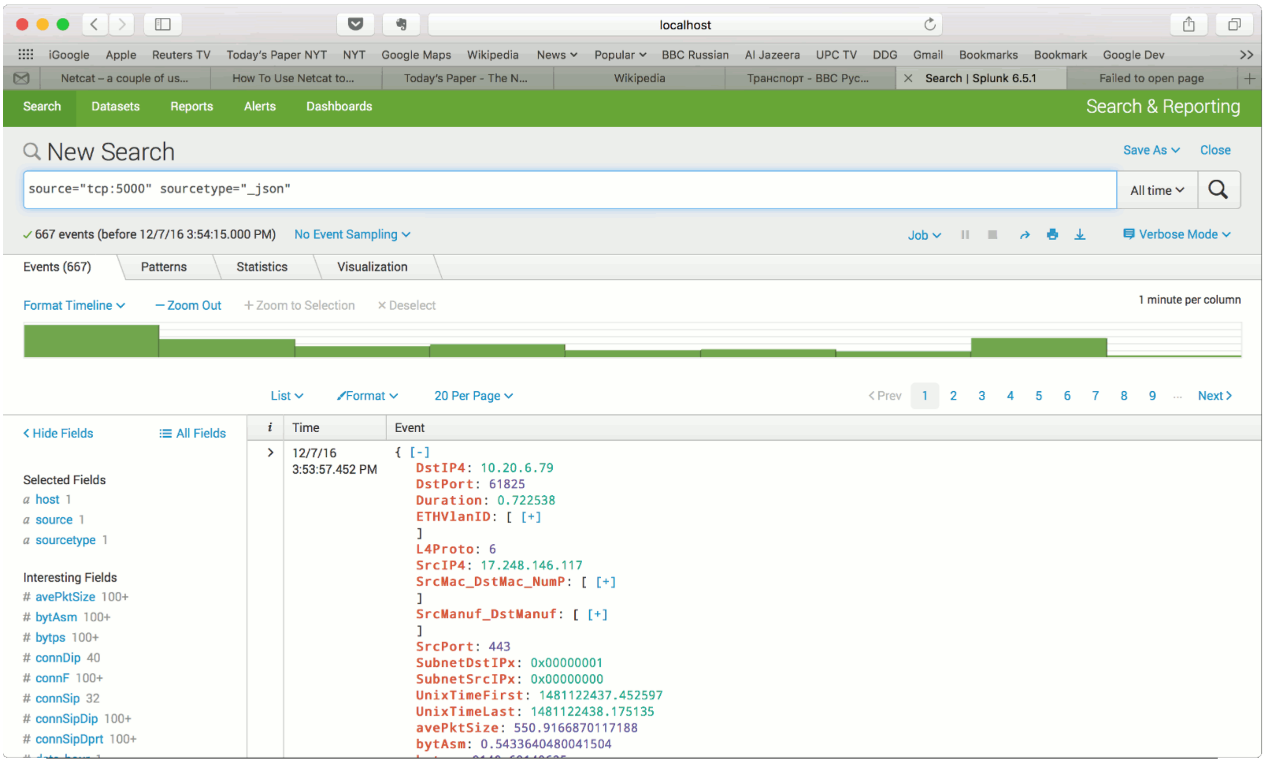
Timestamp

Extraction: Auto | Current time | Advanced...

Advanced

Name	Value
CHARSET	UTF-8
INDEXED_EXTRACTIONS	json
KV_MODE	json
NO_BINARY_CHECK	true
SHOULD_LINEMERGE	true
category	Structured

Figure 7: *Change option "KV_MODE" from "none" to "json" and save the changes.*


localhost
iGoogle Apple Reuters TV Today's Paper NYT NYT Google Maps Wikipedia News Popular BBC Russian Al Jazeera UPC TV DDG Gmail Bookmarks Bookmark Google Dev
Netcat – a couple of us... How To Use Netcat to... Today's Paper - The N... Wikipedia Транспорт - BBC Рус... Search | Splunk 6.5.1 Failed to open page
Search Datasets Reports Alerts Dashboards
Search & Reporting
New Search
Save As Close
All time
Job
Verbose Mode
Events (667) Patterns Statistics Visualization
Format Timeline
Zoom Out
Zoom to Selection
Deselect
1 minute per column
List Format 20 Per Page
Prev 1 2 3 4 5 6 7 8 9 ... Next
Hide Fields All Fields
i Time Event

```
source="tcp:5000" sourcetype="_json"
```

✓ 667 events (before 12/7/16 3:54:15.000 PM) No Event Sampling

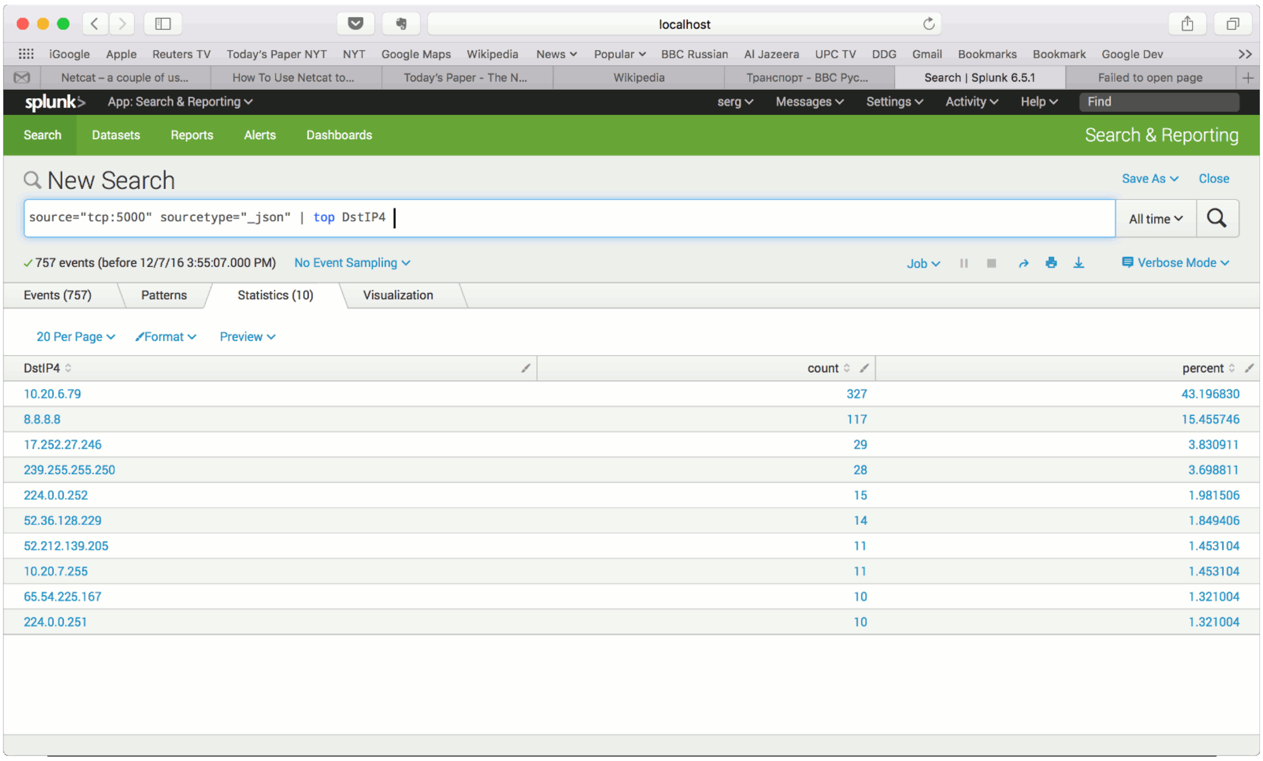
Selected Fields
- a host 1
- a source 1
- a sourcetype 1

Interesting Fields
- # avePktSize 100+
- # bytAsm 100+
- # bytps 100+
- # connDip 40
- # connF 100+
- # connSip 32
- # connSipDip 100+
- # connSipDprt 100+

12/7/16 3:53:57.452 PM

```
{ [-]
  DstIP4: 10.20.6.79
  DstPort: 61825
  Duration: 0.722538
  ETHVlanID: [ [+]
  ]
  L4Proto: 6
  SrcIP4: 17.248.146.117
  SrcMac_DstMac_NumP: [ [+]
  ]
  SrcManuf_DstManuf: [ [+]
  ]
  SrcPort: 443
  SubnetDstIPx: 0x00000001
  SubnetSrcIPx: 0x00000000
  UnixTimeFirst: 1481122437.452597
  UnixTimeLast: 1481122438.175135
  avePktSize: 550.9166870117188
  bytAsm: 0.5433640480041504
```

Figure 8: *Return to the Search window and make sure that the Tranalyzer2 specific fields are recognized by Splunk.*


localhost
iGoogle Apple Reuters TV Today's Paper NYT NYT Google Maps Wikipedia News Popular BBC Russian Al Jazeera UPC TV DDG Gmail Bookmarks Bookmark Google Dev
Netcat – a couple of us... How To Use Netcat to... Today's Paper - The N... Wikipedia Транспорт - BBC Рус... Search | Splunk 6.5.1 Failed to open page
splunk> App: Search & Reporting serg Messages Settings Activity Help Find
Search Datasets Reports Alerts Dashboards Search & Reporting
New Search Save As Close
All time
No Event Sampling Job Verbose Mode
Events (757) Patterns Statistics (10) Visualization
20 Per Page Format Preview

```
source="tcp:5000" sourcetype="_json" | top DstIP4
```

✓ 757 events (before 12/7/16 3:55:07.000 PM)

DstIP4	count	percent
10.20.6.79	327	43.196830
8.8.8.8	117	15.455746
17.252.27.246	29	3.830911
239.255.255.250	28	3.698811
224.0.0.252	15	1.981506
52.36.128.229	14	1.849406
52.212.139.205	11	1.453104
10.20.7.255	11	1.453104
65.54.225.167	10	1.321004
224.0.0.251	10	1.321004

Figure 9: *Query data, e.g. show top destination IP addresses by number of the records.*