



Data Models

Document Usage Guidelines

- Should be used only for enrolled students
- Not meant to be a self-paced document, an instructor is needed
- Lab Exercise slides reference the hands-on lab exercise guide
- Do not distribute

Course Goals

- Define and identify uses of data models and datasets
- Create a data model
- Use a data model in Pivot
- Describe data model acceleration options
- Define `tsidx` files and their role in data model acceleration

Course Outline

- Introduce Data Model Datasets
- Design Data Models
- Create a Pivot
- Accelerate Data Models

Introduce Data Model Datasets

Topic Objectives

- Define data models
- Add event, search, and transaction datasets to data models
- Identify event object hierarchy and constraints
- Add fields based on `eval` expressions to transaction datasets

Data Models

- A data model is a knowledge object that applies an information structure to raw data, making it easier to use
- Each data model is designed by the user to represent a specific category of event data
- The Pivot interface can use data models to generate reports and dashboard panels
- Data models can be accelerated for faster performance

Overview of Data Model Datasets

- Data models are hierarchically structured datasets containing searches and fields
- Each event, search, or transaction is saved as a separate dataset

The screenshot shows the Splunk Enterprise interface for managing data models. The top navigation bar includes 'splunk>enterprise' logo, 'App: Search & Reporting', user 'student1', and links for 'Messages', 'Settings', 'Activity', 'Help', and 'Find'. The main title is 'Buttercup Games Site Activity' under 'Buttercup_Games_Site_Activity'. Below it is a link to '< All Data Models'. On the left, a sidebar titled 'Datasets' has an 'Add Dataset' button. Under 'EVENTS', there is a section for 'Web Requests' which is currently selected. It contains two main categories: 'Successful Requests' (with sub-items: purchases, addtocart, remove) and 'Failed Requests' (with sub-items: failed purchases, failed addtocart, failed remove). To the right of the sidebar, the 'Web Requests' configuration area shows:

- CONSTRAINTS:** index=web sourcetype=access_combined
- Bulk Edit:** A dropdown menu.
- INHERITED:** Fields: _time (Time), host (String), source (String), sourcetype (String).
- EXTRACTED:** Fields: action (String), bytes (Number), categoryid (String), change_type (String), clientip (IPv4), cookie (String), status (Number).

Buttons for 'Constraint', 'Edit', 'Rename', and 'Delete' are located at the top right of the configuration area.

Data Model Dataset Types

Data Models can contain 3 types of datasets:

- Events
- Searches
- Transactions

Buttercup Games Site Activity

Buttercup_Games_Site_Activity

[Edit ▾](#) [Download](#) [Pivot](#) [Documentation](#)

[◀ All Data Models](#)

Datasets [Add Dataset ▾](#)

EVENTS

Web Requests

Web_Requests

CONSTRAINTS

index=web sourcetype=access_combined [Constraint](#) [Edit](#)

Bulk Edit ▾ [Add Field ▾](#)

INHERITED

	Type	
<input type="checkbox"/> host	String	Override
<input type="checkbox"/> source	String	Override
<input type="checkbox"/> sourcetype	String	Override

EXTRACTED

	Type	
<input type="checkbox"/> action	String	Edit
<input type="checkbox"/> bytes	Number	Edit
<input type="checkbox"/> categoryid	String	Edit
<input type="checkbox"/> change_type	String	Edit
<input type="checkbox"/> clientip	IPv4	Edit
<input type="checkbox"/> cookie	String	Edit

Web Requests

Successful Requests

- purchases
- addtocart
- remove

Failed Requests

- failed purchases
- failed addtocart
- failed remove

SEARCHES

User

TRANSACTIONS

visit duration

Data Model Event Datasets

- All event datasets (root and children) contain:
 - Constraints: essentially the search broken down into a hierarchy
 - Fields: associated with the events

The screenshot shows the Splunk Data Model Editor interface. On the left, there's a tree view of event types under a dataset named 'Web Requests'. The tree includes categories like 'Successful Requests' (with 'purchases', 'addtocart', 'remove') and 'Failed Requests' (with 'failed purchases', 'failed addtocart', 'failed remove'). In the center, the 'CONSTRAINTS' tab is selected for the 'Web Requests' dataset. It displays a search bar with the query 'index=web sourcetype=access_combined' and a yellow box labeled 'root search' highlighting it. To the right of the search bar are 'Constraint' and 'Edit' buttons. Below the search bar is a 'Bulk Edit' dropdown and an 'Add Field' button. The main area contains two sections: 'INHERITED' and 'EXTRACTED'. The 'INHERITED' section lists fields: '_time' (Time), 'host' (String), 'source' (String), and 'sourcetype' (String). A yellow box labeled 'fields' highlights this section. The 'EXTRACTED' section lists fields: 'action' (String), 'bytes' (Number), 'categoryid' (String), 'change_type' (String), 'clientip' (IPv4), 'cookie' (String), and 'date_hour' (Number). Each field has an 'Edit' button to its right.

Event Object Hierarchy and Constraints

The screenshot illustrates the Event Object Hierarchy and Constraints in the Splunk Data Model Editor. The hierarchy is as follows:

- Root Node:** Web Requests (Web_Requests)
 - CONSTRAINTS:** index=web sourcetype=access_combined
- Child Node:** Successful Requests
 - CONSTRAINTS:** index=web sourcetype=access_combined status<400
- Grandchild Node:** purchases
 - CONSTRAINTS:** index=web sourcetype=access_combined status<400 action=purchase productId=*

Annotations:

- Annotation 1:** root search string: all access_combined events
- Annotation 2:** all access_combined events with successful requests (status<400)
- Annotation 3:** all access_combined events with successful requests that were purchases (action=purchase) involving a product (productId=*)

Text Box: Each child dataset inherits constraints from the root dataset and parent datasets

Dataset Fields

- Select the fields you want to include in the dataset
- Like constraints, fields are inherited from parent datasets

The screenshot shows the configuration page for the 'Web Requests' dataset. At the top, there are buttons for 'Rename' and 'Delete'. Below that is a 'CONSTRAINTS' section containing the query 'index=web sourcetype=access_combined'. Underneath is a 'Bulk Edit' dropdown and an 'Add Field' button. The main area is divided into two sections: 'INHERITED' and 'EXTRACTED'. The 'INHERITED' section is highlighted with a green border and contains fields: '_time' (Time), 'host' (String), 'source' (String), 'sourcetype' (String). The 'EXTRACTED' section contains fields: 'action' (String), 'bytes' (Number), 'categoryid' (String), 'change_type' (String), and 'clientip' (IPv4). Each field row has an 'Override' or 'Edit' link on the right.

Field	Type	Action
_time	Time	
host	String	Override
source	String	Override
sourcetype	String	Override
action	String	Edit
bytes	Number	Edit
categoryid	String	Edit
change_type	String	Edit
clientip	IPv4	Edit

Data Model Root Search Datasets

- Based on an arbitrary search to define the dataset it represents
- Include a transforming command if you want to include field(s) that aggregate over the entire dataset
- Use the Add Field button to add more fields

index=web _time=* host=* source=* sourcetype=* uri=* status<600 clientip=* referer=* useragent=* (sourcetype=access_* OR source=log)
| eval userid=clientip
| stats first(_time) as earliest, last(_time) as latest, list(uri_path) as uri_list by userid

Buttercup Games Site Activity

Buttercup_Games_Site_Activity

[Edit](#) [Download](#) [Pivot](#) [Documentation](#)

[Rename](#) [Delete](#)

Datasets [Add Dataset ▾](#)

EVENTS

Web Requests

- Successful Requests
 - purchases
 - addtocart
 - remove
- Failed Requests
 - failed purchases
 - failed addtocart
 - failed remove

SEARCHES

User

BASE SEARCH

index=web _time=* host=* source=* sourcetype=* uri=* status<600 clientip=* referer=* useragent=* (sourcetype=access_* OR source=log) | eval userid=clientip | stats first(_time) as earliest, last(_time) as latest, list(uri_path) as uri_list by userid

[Edit](#)

Bulk Edit ▾

Calculated fields are processed in the order above, so ensure any dependent fields are defined first. Drag and drop fields to change their order.

Add Field ▾

- Auto-Extracted
- Eval Expression
- Lookup
- Regular Expression
- Geo IP

Data Model Root Transaction Datasets

- Based on a transaction
- Uses fields that have already been added to the data model using either event or search datasets

Buttercup Games Site Activity

Buttercup_Games_Site_Activity

< All Data Models

Edit ▾ Download Pivot Documentation

Datasets Add Dataset ▾

EVENTS

Web Requests

- Successful Requests
 - purchases
 - addtocart
 - remove
- Failed Requests
 - failed purchases
 - failed addtocart
 - failed remove

SEARCHES

User

TRANSACTIONS

visit duration

visit duration

CONSTRAINTS

Group Datasets Web_Requests Transaction Edit

Group By clientip

Max Pause 10s

Max Span

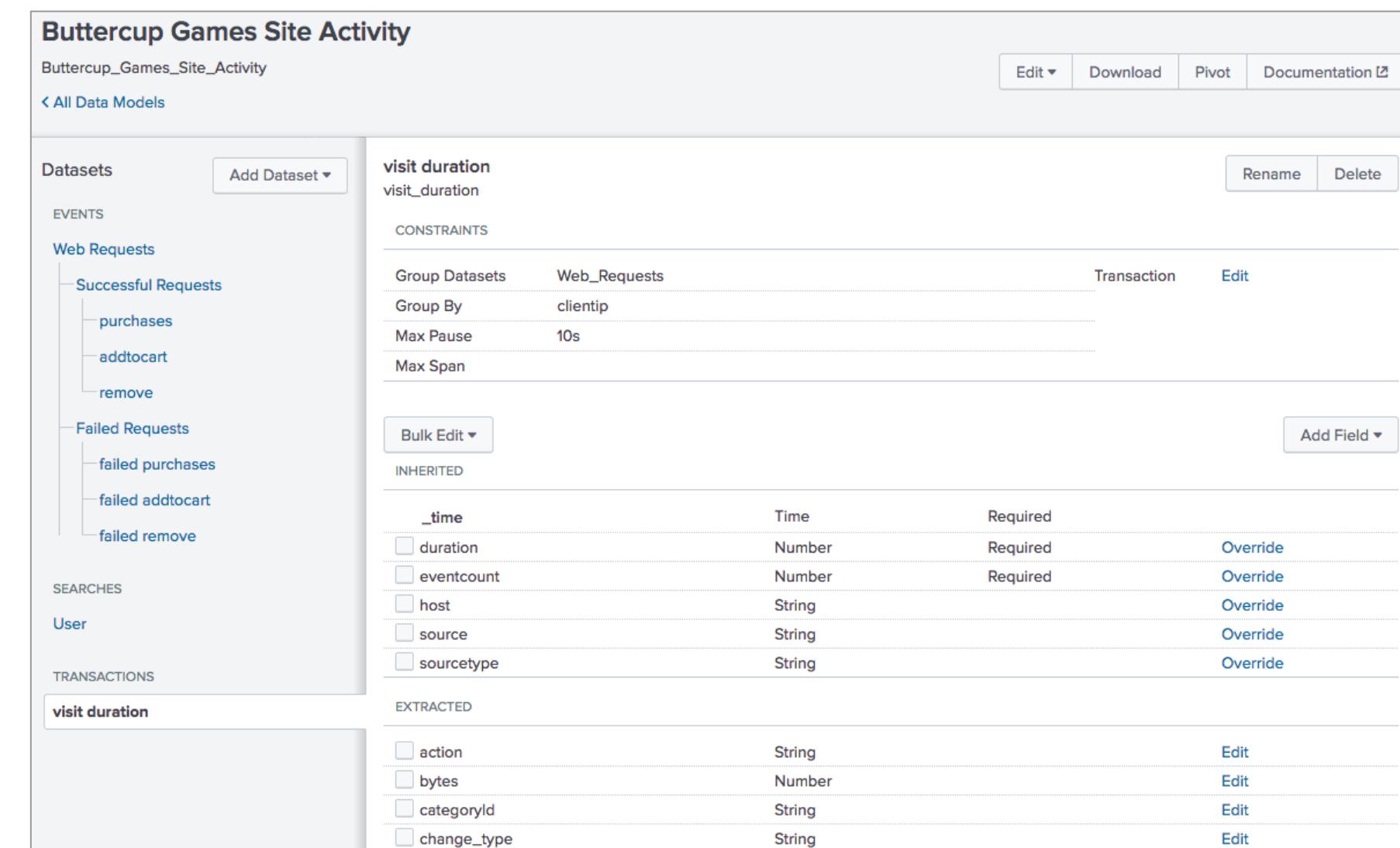
Bulk Edit ▾ Add Field ▾

INHERITED

	Type	Required	
_time	Time	Required	
duration	Number	Required	Override
eventcount	Number	Required	Override
host	String		Override
source	String		Override
sourcetype	String		Override

EXTRACTED

	Type	
action	String	Edit
bytes	Number	Edit
categoryid	String	Edit
change_type	String	Edit



Design Data Models

Topic Objectives

- Create a data model
- Add root event dataset to a data model
- Add fields to data models
- Add child datasets to a data model
- Test a data model
- Define permissions for a data model
- Upload/download data models for backup and sharing

Create a Data Model

Settings > Data models

The screenshot shows the Splunk Enterprise interface with the 'Data Models' page open. At the top right of the main page, there is a green button labeled 'New Data Model'. A green arrow points from this button down to a modal window titled 'New Data Model'. Inside the modal, there are three numbered steps:

- As Title is entered, an ID is automatically generated but can be overwritten (not recommended)
- Choose app context
- Create

The 'Title' field is populated with 'Buttercup Games Site Activity'. The 'ID' field shows the automatically generated ID 'Buttercup_Games_Site_Activity'. The 'App' dropdown is set to 'Search & Reporting'. The 'Description' field contains the word 'optional'. At the bottom right of the modal, there are 'Cancel' and 'Create' buttons.

Add a Root Event

The screenshot illustrates the process of adding a root event dataset in the Splunk Data Model interface.

- Step 1:** In the main interface, under the "Datasets" section, the "Add Dataset" button is highlighted with a green box and a green arrow pointing down to the "Add Event Dataset" dialog.
- Step 2:** In the "Add Event Dataset" dialog, the "Dataset Name" field contains "Web Requests".
- Step 3:** In the "Constraints" field, the value "index=web sourcetype=access_combined" is entered. A callout bubble with orange border and yellow background provides the following explanation: "Constraints are essentially search terms – add child events (discussed later in this topic) to further "narrow" your search".
- Step 4:** The "Preview" button is highlighted with a green box and a green arrow pointing to it from the right side of the dialog. A callout bubble with orange border and yellow background says: "Click Preview to view the events that the constraint returns".

Buttercup Games Site Activity
Buttercup_Games_Site_Activity
Edit ▾ Download Pivot Documentation

Add Event Dataset
Data Model: Buttercup Games Site Activity

Datasets

1 Add Dataset ▾
Root Event
Root Search

To get started, add a dataset using the menu to the left.

Add Event Dataset
Data Model: Buttercup Games Site Activity

Dataset Name: Web Requests
Dataset ID: Web_Requests

Constraints: index=web sourcetype=access_combined

The search must have an explicit index constraint to maximize performance.
Examples:
index=main uri="*.php" OR uri="*.py"
index=main NOT (referer=null OR referer="-")

✓ 1,000 events (before 5/27/22 4:53:23.000 PM)
20 per page ▾ 1 2 3 4 5 6 7 8 ... Next >
Sample: 1,000 events ▾

Event

194.215.205.19 - [27/May/2022:16:53:21] "POST /cart.do?action=addtocart&itemId=EST-27&productId=FS-SG-G03&JSESSIONID=SD6SL2FF1ADFF495
2 HTTP 1.1" 200 478 "http://www.buttercupgames.com" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/1
9.0.1084.46 Safari/536.5" 679

142.233.200.21 - [27/May/2022:16:52:23] "GET /category.screen?categoryId=NULL&JSESSIONID=SD6SL1FF3ADFF4964 HTTP 1.1" 408 2602 "htt
p://www.buttercupgames.com/category.screen?categoryId=NULL" "Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0; BOI
E9;ENUS)" 364

142.233.200.21 - [27/May/2022:16:52:18] "GET /category.screen?categoryId=SIMULATION&JSESSIONID=SD6SL1FF3ADFF4964 HTTP 1.1" 200 3805
"http://www.buttercupgames.com/oldlink?itemId=EST-21" "Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0; BOIE9;ENU
S)" 177

Documentation

Cancel Preview Save

Add a Root Event (cont.)

In this example, the root event of this data model represents all web requests

Buttercup Games Site Activity
Buttercup_Games_Site_Activity
[All Data Models](#)

Datasets [Add Dataset ▾](#)

EVENTS

Web Requests [Web Requests](#)

CONSTRAINTS

root event constraints

`index=web sourcetype=access_combined`

Constraint

Bulk Edit ▾

INHERITED

<input type="checkbox"/>	_time	Time
<input type="checkbox"/>	host	String
<input type="checkbox"/>	source	String
<input type="checkbox"/>	sourcetype	String

Add Field ▾

Auto-Extracted

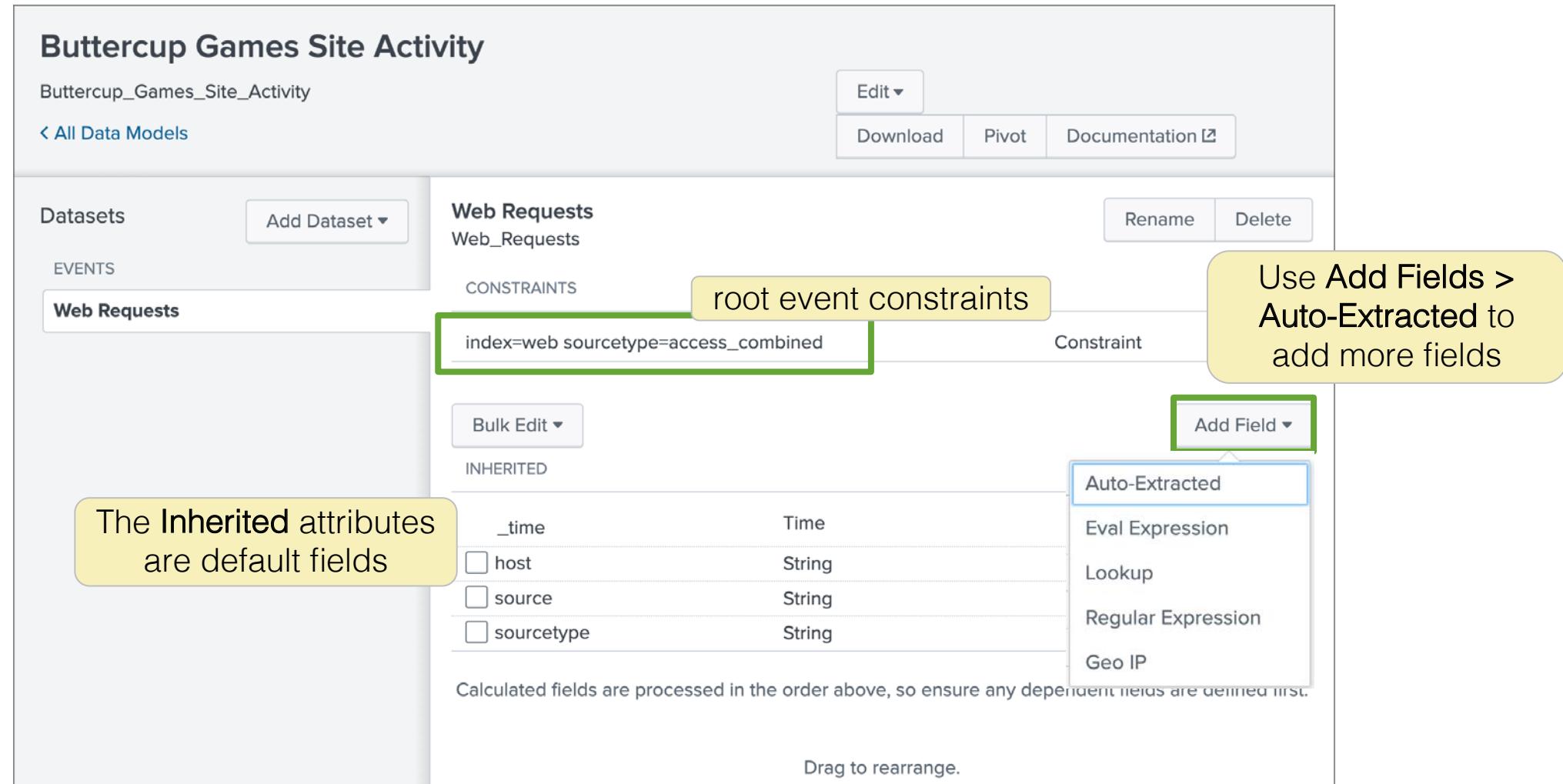
- Eval Expression
- Lookup
- Regular Expression
- Geo IP

Calculated fields are processed in the order above, so ensure any dependent fields are defined first.

Drag to rearrange.

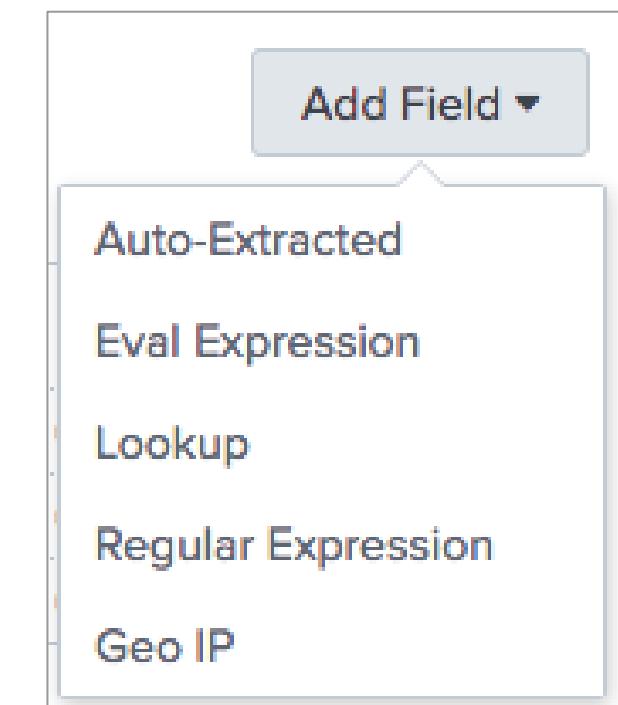
The Inherited attributes are default fields

Use Add Fields > Auto-Extracted to add more fields



Add Fields

- **Auto-Extracted:** default fields or manually extracted fields
- **Eval Expression:** new field based on an expression you define
- **Lookup:** leverage an existing lookup table
- **Regular Expression:** extract a new field based on regex
- **Geo IP:** geographical fields such as latitude/longitude or country



Add Fields: Auto-Extracted

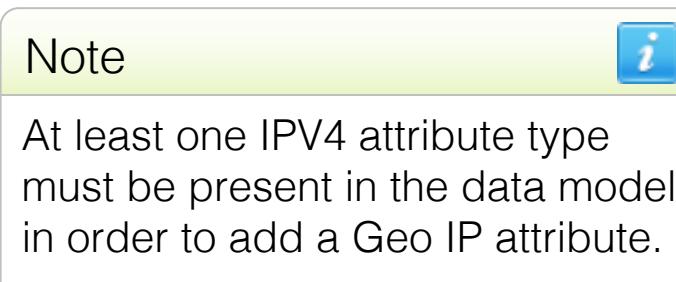
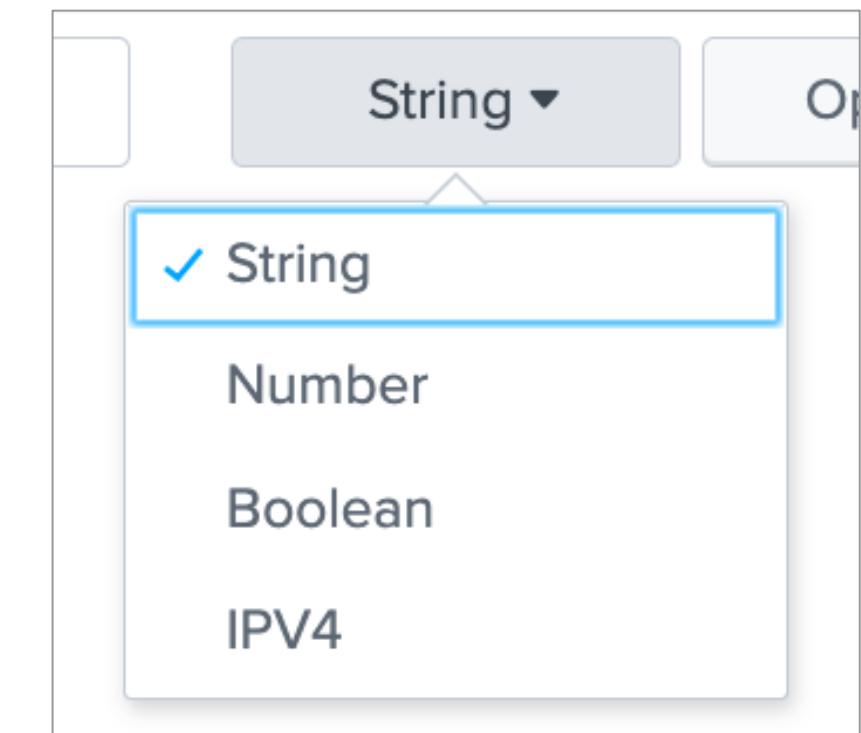
Check auto-extracted fields to add them to the dataset

The screenshot shows the Splunk interface for adding auto-extracted fields. On the left, a vertical menu has 'Auto-Extracted' selected and highlighted with a green border. A green arrow points from this selection to the 'Add Field' dialog on the right. The 'Add Field' dialog title is 'Add Auto-Extracted Field'. It includes a sample size of '1,000 events' (before 5/27/22 5:11:05.000 PM) and a link to 'Missing field? Add by Name'. The main area lists auto-extracted fields with checkboxes for 'Field Name', 'Display Name', and 'Type and Flags'. The 'action' field is selected (checkbox checked), with its example values ('view', 'purchase', 'addtocart', 'remove', 'changequantity') listed below. A yellow callout box highlights this section with the text: 'Example values for the field, action'. Another yellow callout box highlights the 'Display Name' field for the 'action' entry, stating: 'A Display Name can be specified for use in Pivot'. The 'bytes' and 'categoryId' fields are also listed with their respective configurations. At the bottom are 'Cancel' and 'Save' buttons.

Field Name	Display Name	Type and Flags
JSESSIONID		
action	action	String ▾ Optional ▾
bytes	bytes	Number ▾ Optional ▾
categoryId	categoryId	String ▾ Optional ▾
clientip		

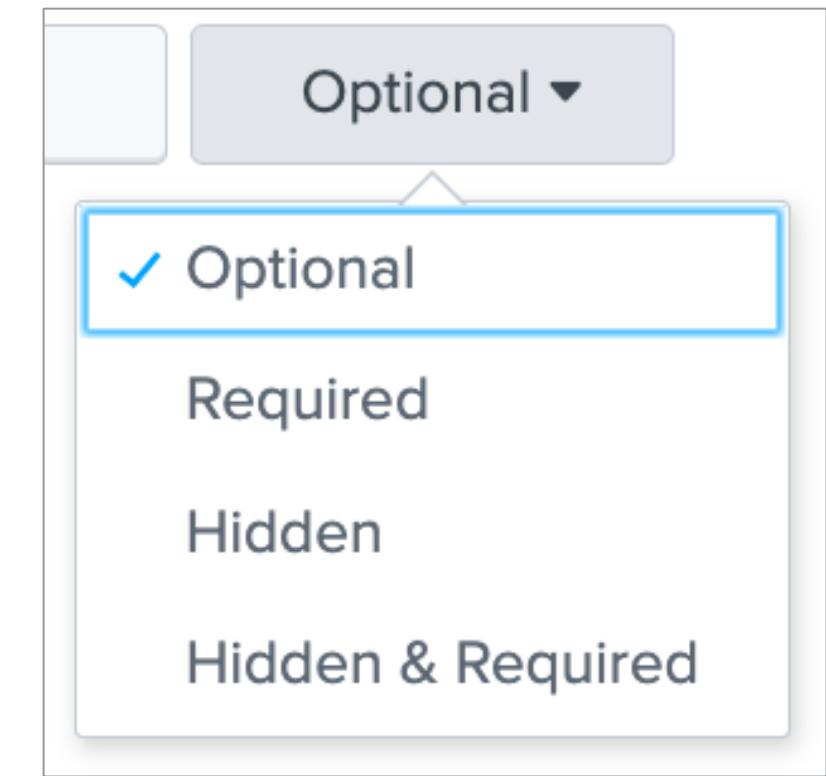
Field Types

- **String:** Recognized as alphanumeric
- **Number:** Recognized as numeric
- **Boolean:** Recognized as true/false or 1/0
- **IPV4:** Recognized as IP addresses



Field Flags

- **Optional:** Field doesn't have to appear in every event
- **Required:** Only events that contain this field are returned in Pivot
- **Hidden:** Field is not displayed to Pivot users when they select the dataset in Pivot
- **Hidden & Required:** Only events that contain this field are returned, and the fields are hidden from use in Pivot



Add Fields: Eval Expressions

Define a new field using an eval expression

The screenshot shows the 'Add Fields with an Eval Expression' interface. A green arrow points from the 'Eval Expression' section to a callout box containing the text: 'In this example, a field named errorReason evaluates the value of the status field'. Another green arrow points from the 'Preview' button to a callout box containing the text: 'Click Preview to verify your eval expression returns events, then Save'. The 'Preview' button is highlighted with a green border.

1 Add Field ▾

2 Eval Expression

3 Preview

4 Save

Add Fields with an Eval Expression

Data Model: Buttercup Games Site Activity Dataset: Web Requests Documentation ▾

Eval Expression

```
if(status>399,"Web error","OK")
```

Examples:

```
case(error =  
if(cidrmatch("192.0.0.0/16", clientip), "local", "other")
```

Learn More ▾

Field

Field Name: errorReason Display Name: Error Reason Type: String ▾ Flags: Optional ▾

Events **Values**

✓ 1,000 events (before 5/27/22 5:18:35.000 PM)

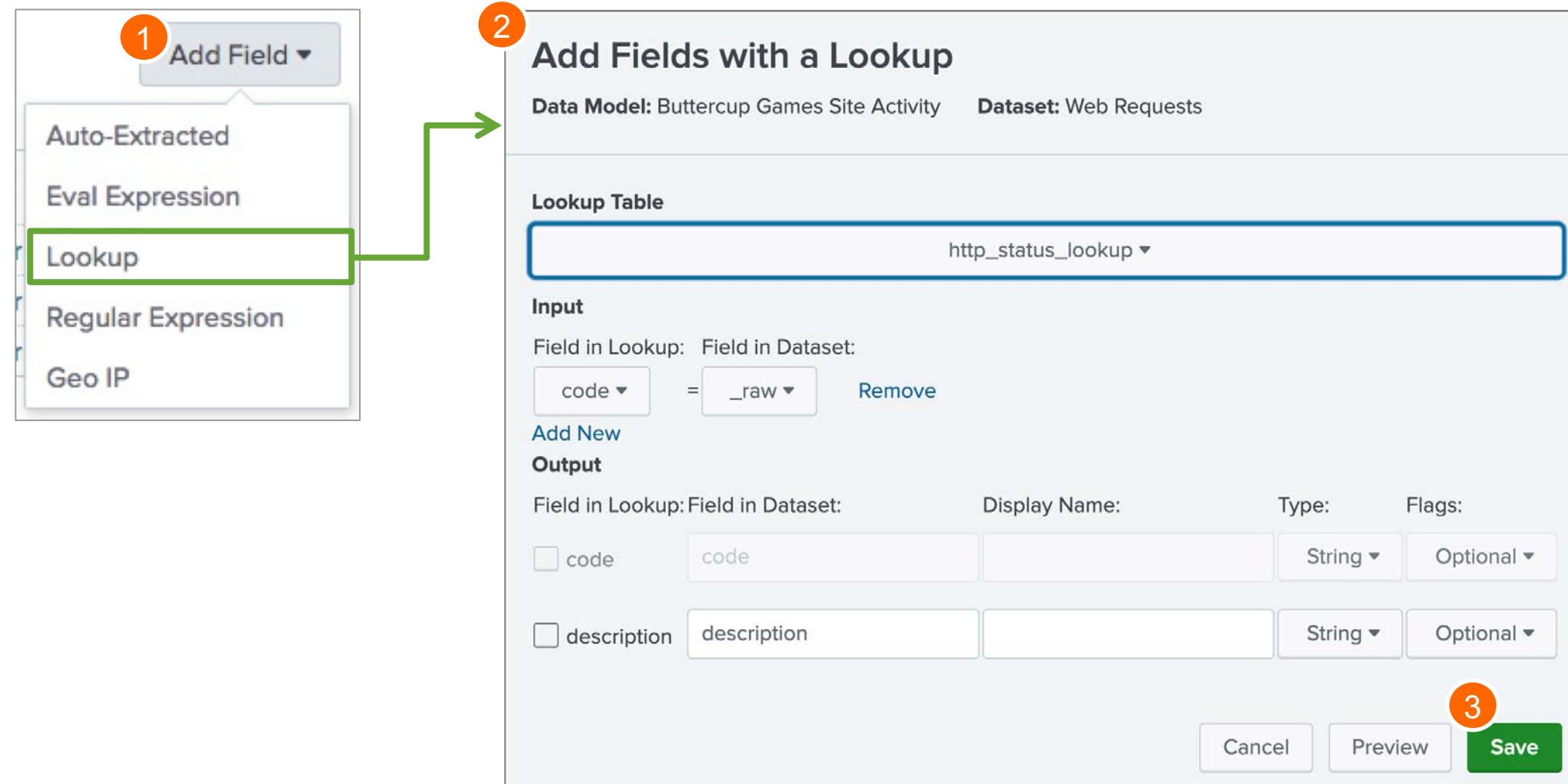
20 per page ▾ < Prev 1 2 3 4 5 6 7 8 ... Next >

Sample: 1,000 events ▾

_time	errorReason	host	source	sourcetype	_raw
2022-05-27 17:18:34	OK	www1	/opt/log/www1/access.log	access_combined	84.34.159.23 - - [27/May/2022:17:18:34] "GET /product.screen?i=123456789"
2022-05-27 17:18:26	OK	www1	/opt/log/www1/access.log	access_combined	84.34.159.23 - - [27/May/2022:17:18:26] "GET /oldlink?itemId=E123456789"

Add Fields: Lookups

- Leverage an existing lookup definition to add fields to the dataset
- Configuration is similar to setting up an automatic lookup



Add Fields: Lookups (cont.)

Click Preview and use the events and values tabs to verify your results

The screenshot shows the 'Add Fields with a Lookup' configuration screen. On the left, under 'Input', a field mapping 'code = status' is defined. Under 'Output', fields 'code', 'status', and 'description' are selected. A 'Display Name' dropdown is set to 'status description'. The 'Events' tab shows 1,000 events. The 'Values' tab is highlighted with a green box and displays a table of HTTP status codes and their counts:

Value	Count	%
OK.	881	88.100
Bad Request.	20	2.000
Internal Server Error.	20	2.000
Service Unavailable.	19	1.900
Request Timeout.	16	1.600
Not Found.	14	1.400
HTTP Version Not Supported.	13	1.300

Add Fields: Regular Expression

You can define a new field using a regular expression

1 Add Field ▾

Auto-Extracted

Eval Expression

Lookup

Regular Expression

Geo IP

2 Extract From `_raw`

Regular Expression

```
userAgent(?<browser>[*()])
```

Example:
From: (?<from>.*) To: (?<to>.*)

Field(s)

Field Name: browser Display Name: browser Type: String Flags: Optional

Events browser

✓ 1,000 events (before 5/27/22 5:54:24.000 PM)

20 per page ▾ 1 2 3 4 5 6 7 8 ... Next >

filter Apply Sample: 1,000 events ▾ All events ▾ All Events Matches Non-Matches

_raw

170.192.178.10 - - [27/May/2022:17:54:16] "GET /oldlink?itemId=EST-26&JSESSIONID=SD7SL3FF4ADFF4956 HTTP/1.1" 200 3726 "http://www.buttercupgames.com/cart.d...

170.192.178.10 - - [27/May/2022:17:53:59] "GET /category.screen?categoryId=SHOOTER&JSESSIONID=SD7SL3FF4ADFF4956 HTTP/1.1" 200 3190 "http://www.buttercupg...

Click Matches or Non-Matches to preview the events that match or don't match the regular expression

Documentation ▾

Cancel Preview Save

Add Fields: GeoIP

- Requires latitude/longitude fields
- Requires at least one IP field configured as an IPv4 field type
- Select the field that contains the mapping to lat/lon
- Identify the lat/lon and geo fields in the data

Add Geo Fields with an IP Lookup

Data Model: Buttercup Games Site Activity Dataset: Web Requests

IP
clientip ▾

Add Field ▾

- Auto-Extracted
- Eval Expression
- Lookup
- Regular Expression
- Geo IP

Field(s)

Include:	Field in GeolP:	Display Name:
<input checked="" type="checkbox"/>	lon	longitude
<input checked="" type="checkbox"/>	lat	latitude
<input checked="" type="checkbox"/>	City	
<input checked="" type="checkbox"/>	Region	
<input checked="" type="checkbox"/>	Country	

Add Child Datasets

New child datasets inherit the parent's constraints and Additional Constraints can be added

Buttercup Games Site Activity

Buttercup_Games_Site_Activity

[Edit](#) [Download](#) [Pivot](#) [Documentation](#)

[All Data Models](#)

Datasets

- EVENTS
- Web Requests**
- Root Event
- Root Transaction
- Root Search
- Child**

[Add Dataset](#) [Bulk Edit](#)

Web Requests

Web_Requests

CONSTRAINTS

index=web sour

Add Child Dataset

Data Model: Buttercup Games Site Activity

Dataset Name
Successful Requests

Additional Constraints
status<400

Examples:
uri="*.php*" OR uri="*.py*"
NOT (referer=null OR referer=)

Dataset ID
Successful_Requests

The dataset ID can only contain letters, numbers, dashes, and underscores. Do not start the dataset ID with a period.

Inherit From
Web Requests

[Cancel](#) [Preview](#) **Save**

This child dataset will contain status less than 400 (successful http request) for all events from the **Web Requests** root event dataset

Add Child Datasets: Fields

- Child datasets inherit all fields from the parent events
- Inherited fields can be overridden and more fields can be added

Successful Requests
Successful_Requests

Rename Delete

CONSTRAINTS

index=web sourcetype=access_combined	Inherited Constraint
status<400	Edit

Bulk Edit ▾

INHERITED

_time	Time
<input type="checkbox"/> clientip	IPv4
<input type="checkbox"/> host	String
<input type="checkbox"/> source	String
<input type="checkbox"/> sourcetype	String
<input type="checkbox"/> status	Number

Add Field ▾

Auto-Extracted

- Eval Expression
- Lookup
- Regular Expression
- Geo IP

Override

<input type="checkbox"/> clientip	IPv4
<input type="checkbox"/> host	String
<input type="checkbox"/> source	String
<input type="checkbox"/> sourcetype	String
<input type="checkbox"/> status	Number

Add a Transaction Dataset

The screenshot shows the 'Add Transaction Dataset' configuration page. At the top, it says 'Data Model: Buttercup Games Site Activity'. A note below states: 'You must specify at least one of the optional fields.' The configuration area includes:

- Dataset Name:** 'visit duration'
- Dataset ID ?** 'visit_duration' (with a note: 'Can only contain letters, numbers and underscores.')
- Group Datasets:** 'Web Requests' (with a remove button 'x') and a '+' button.
- Group by:** 'clientip' (with a remove button 'x') and a '+' button.
- Duration:** 'Max Pause:' set to '10' with a dropdown 'Seconds ▾', and 'Max Span:' (empty field) with a dropdown 'Seconds ▾'.

Callouts with orange circles and numbers:

- 1: Points to the 'Add Dataset ▾' button in the top right corner of the main window.
- 2: Points to the 'Root Transaction' option in a dropdown menu that appears when clicking 'Add Dataset ▾'. Other options in the menu are 'Root Event', 'Root Search', and 'Child'.
- 3: Points to the 'Select a group by field' tooltip near the 'Group by' section.
- 4: Points to the 'Optional select max pause and max span' tooltip near the 'Duration' section.

Transaction Dataset Considerations

- An event or search dataset must exist before adding a transaction dataset
- Auto-extracted fields must be added to the root event or root search dataset to be available in the transaction dataset
- Transaction datasets cannot benefit from persistent data model acceleration

Set Permissions

Edit > Edit Permissions

Note i

Once the data model is displayed for a particular app, the admin can make changes to the data model, regardless of the permissions set by the owner.

Edit Permissions

Data Model: Buttercup Games Site Activity

Owner: student1

App: search

Display For: App

	Read	Write
Everyone	<input checked="" type="checkbox"/>	<input type="checkbox"/>
power	<input type="checkbox"/>	<input type="checkbox"/>
student	<input type="checkbox"/>	<input type="checkbox"/>
user	<input type="checkbox"/>	<input type="checkbox"/>

Cancel Save

1 Edit ▾ Downl
2 Edit Permissions
3 Edit Acceleration
Clone
Delete

3 Specify who or which apps can see the data model

4 Specify who can use (read) and/or edit (write) the data model

5

Test the Data Model

After completing your data model, it is recommended to test your datasets by building a pivot (next topic)

Buttercup Games Site Activity

Buttercup_Games_Site_Activity

< All Data Models

Datasets Add Dataset ▾

EVENTS

Web Requests

Successful Requests

- purchases
- addtocart
- remove

Failed Requests

- failed purchases
- failed addtocart

Note

Datasets are also called objects.

1

2

Select a Dataset

- 11 Objects in Buttercup Games Site Activity
- Web Requests
- Successful Requests
- purchases
- addtocart
- remove
- Failed Requests
- failed purchases
- visi
- User

Choose a dataset from the Buttercup Games Site Activity Data Model to build a report in Pivot

Download and Upload Data Models

- The Splunk Web interface allows for data models to be downloaded or uploaded
- Benefits of downloading/uploading:
 - Back up important data models
 - Collaborate with other Splunk users to create/modify/test data models
 - Move data models from a test environment to production instance

Download a Data Model

The screenshot illustrates the process of downloading a data model from the Splunk Data Models interface. The main window shows the 'Buttercup Games Site Activity' data model with various datasets and constraints. The 'Download' button in the top right corner is highlighted with a green box and an arrow pointing down to a Firefox file download dialog. The dialog displays the file path 'Opening Buttercup_Games_Site_Activity.json', its type as a JSON file (1.3 KB), and its source as 'http://54.201.235.11'. It also asks what Firefox should do with the file, with 'Save File' selected.

Upload a Data Model

The diagram illustrates the workflow for uploading a new data model in Splunk. It consists of three main panels:

- Top Left Panel:** The Splunk Enterprise interface showing the "Data Models" list. A green arrow points from the "Upload Data Model" button in the top right corner of this panel to the "File" input field in the "Upload New Data Model" dialog.
- Top Right Panel:** An "Upload New Data Model" dialog box. It contains fields for "File" (set to "Buttercup_Games_Site_Activity.json"), "ID" (set to "Buttercup_Games_Site_Activity_AC"), and "App" (set to "Search & Reporting"). A green arrow points from the "Upload" button in this dialog to the "Buttercup Games Site Activity" data model page.
- Bottom Panel:** The "Buttercup Games Site Activity" data model page. It shows the "Web Requests" dataset with its constraints and fields. A green arrow points from the "Edit" link in the "Constraints" section back to the "Upload New Data Model" dialog.

Design Data Models Lab Exercise

Time: 10 minutes

Tasks:

- Create a data model and add a root event dataset
- Add auto-extracted fields to the root event dataset and modify their display names
- Add child event datasets to the root event dataset

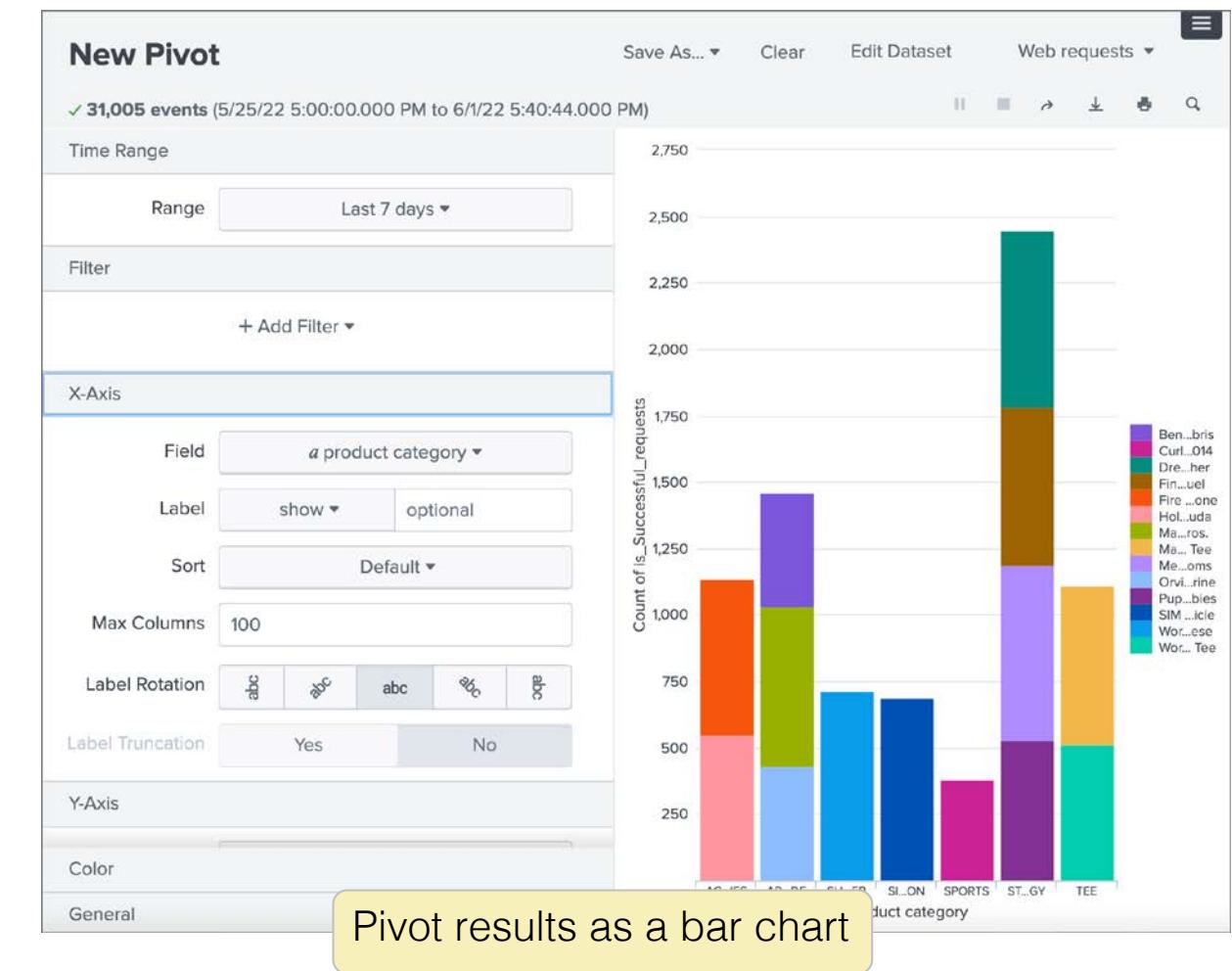
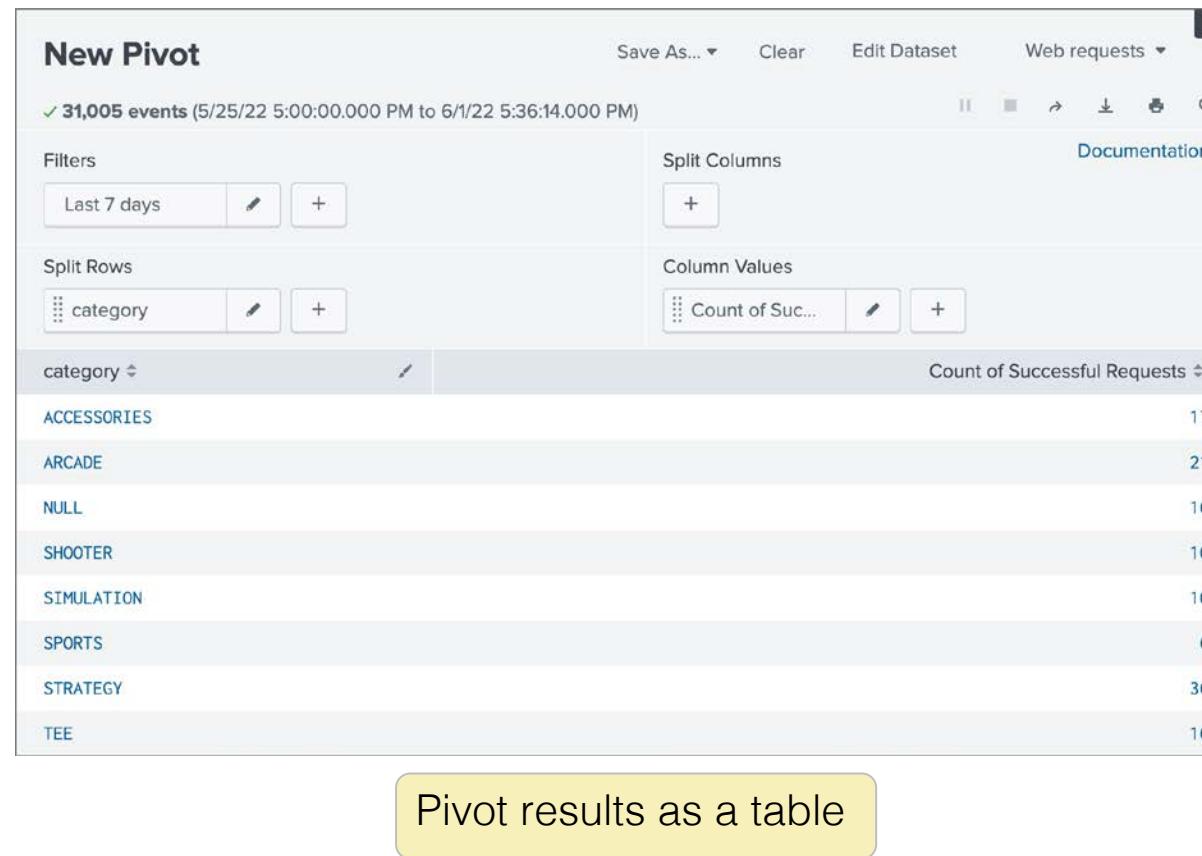
Create a Pivot

Topic Objectives

- Identify benefits of using Pivot
- Create and configure a Pivot
- Visualize a Pivot
- Save a Pivot
- Use Instant Pivot
- Access underlying search for Pivot

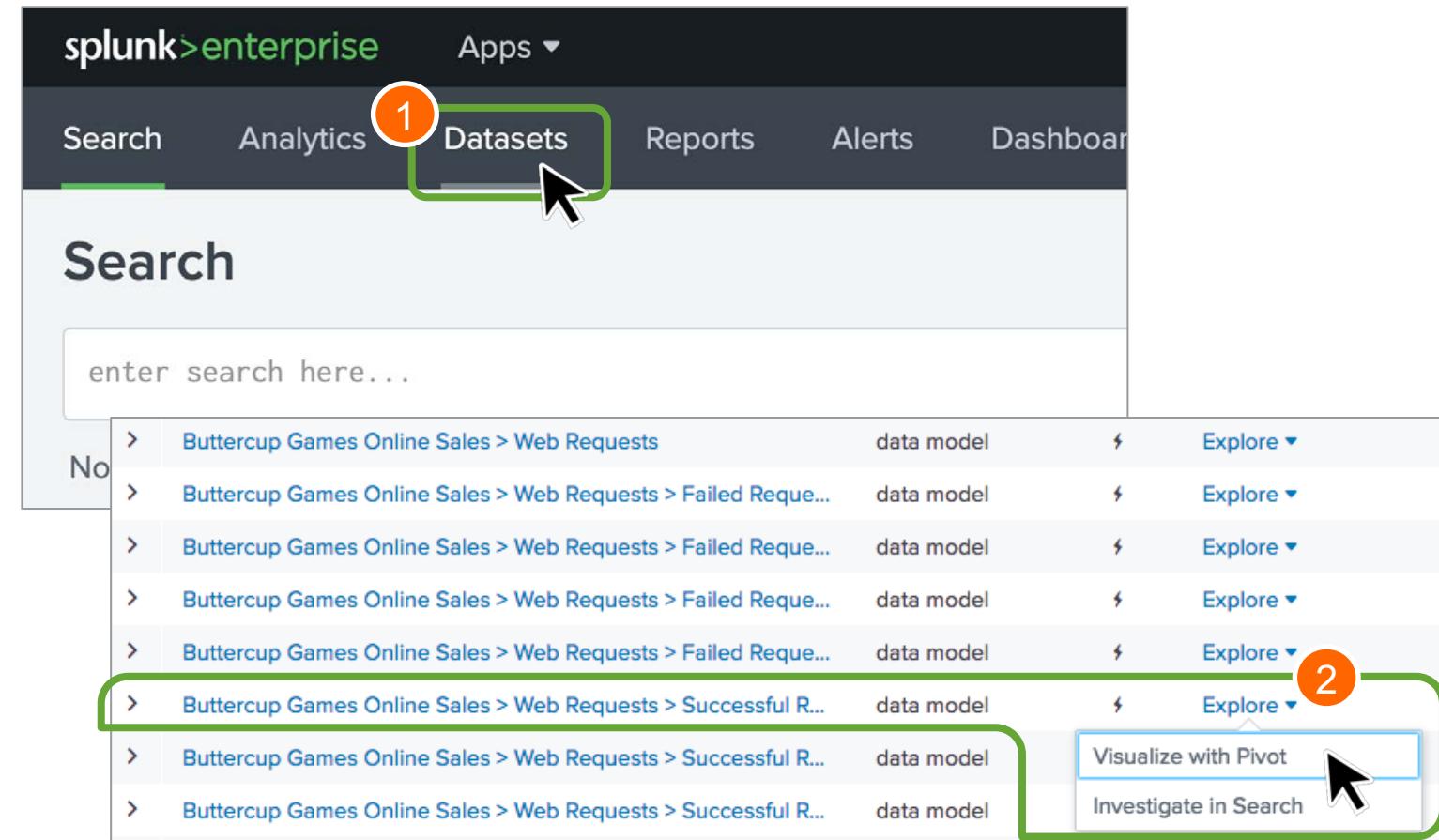
What is Pivot?

- Alternate method to access data without using search language
- Quick way to design visualizations of data using Splunk Web
- Requires use of datasets



Select a Dataset for Pivot

- 1 Select Datasets tab from the app navigation bar
 - Datasets represent specific data from the data model
 - Data models are composed of multiple datasets
- 2 Choose a dataset, then click **Explore > Visualize with Pivot**



Open in Pivot

The Pivot automatically populates with a count of events for the selected dataset

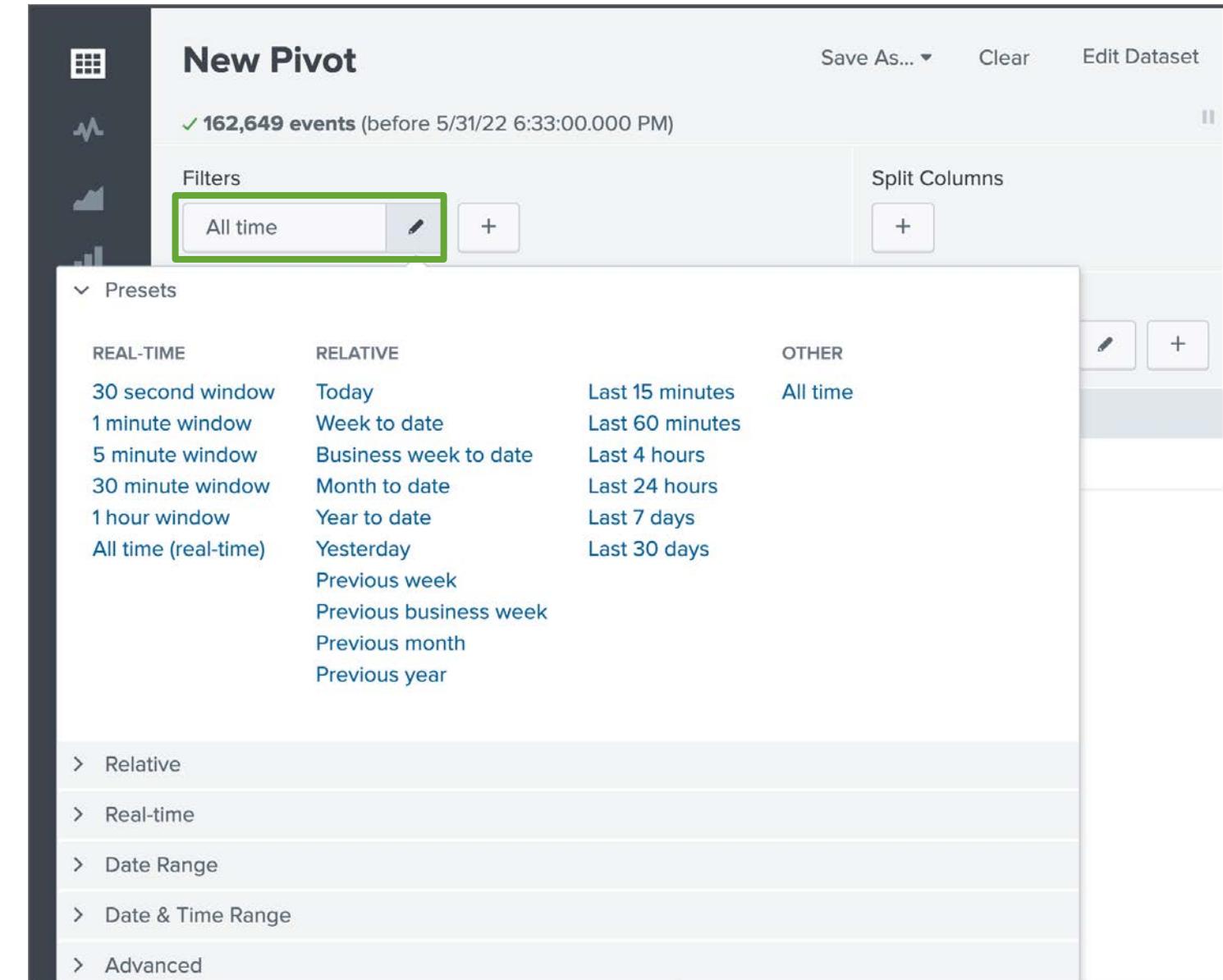
The screenshot shows the Splunk Pivot interface with the following elements:

- Left Sidebar:** A vertical sidebar with icons for different data visualization types: Grid, Line, Area, Bar, Histogram, and Pie.
- Header:** "New Pivot" is displayed prominently. To the right are buttons for "Save As...", "Clear", "Edit Dataset", "Web requests", and a menu icon.
- Top Bar:** Shows a green checkmark and the text "163,593 events (before 6/1/22 5:47:01.000 PM)".
- Filters:** "All time" filter with edit and add buttons.
- Split Rows:** An "Add" button.
- Column Values:** A section containing "Count of Suc..." with a corresponding icon, edit button, and add button. The value "142358" is displayed below it.
- Documentation:** A link labeled "Documentation" with a help icon.
- Bottom:** A horizontal bar with icons for search, refresh, and other navigation functions.

A green box highlights the "Count of Successfull Requests" section, and the value "142358" is highlighted with a green border.

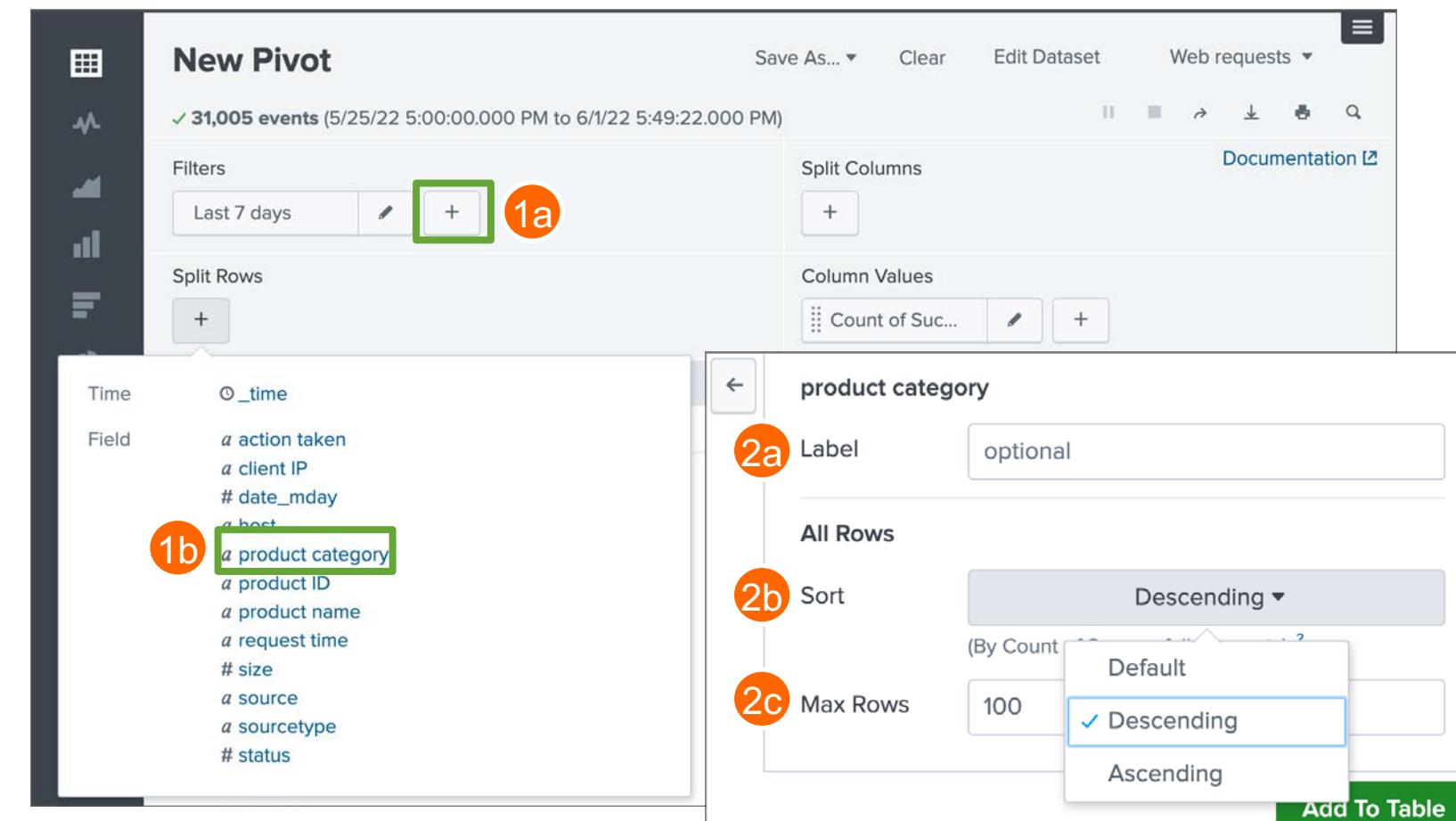
Select a Time Range

- Defaults to returning results over All time
- Click the  to select the desired time range
- The pivot runs immediately upon selecting the new time range



Split Rows

- 1 Click  under Split Rows for a list of available fields to split by
- 2 Choose a field
 - Enter a field **Label** (optional)
 - Choose a **Sort** order
 - Define maximum number of rows to display



New Pivot

31,005 events (5/25/22 5:00:00.000 PM to 6/1/22 5:49:22.000 PM)

Filters: Last 7 days

Split Columns: +

Documentation

Split Rows: +

Time: @_time

Field:

- a action taken
- a client IP
- # date_mday
- a host
- a product category** (highlighted)
- a product ID
- a product name
- a request time
- # size
- a source
- a sourcetype
- # status

product category

2a Label: optional

2b Sort: Descending

2c Max Rows: 100

Add To Table

Split Rows: Results

The screenshot shows the Splunk Pivot interface titled "New Pivot". The interface includes a sidebar with various icons and a main panel with sections for "Filters", "Split Columns", "Split Rows", and "Column Values". The "Split Rows" section contains a table with two columns: "Category" and "Count of Successfull Requests". The table data is as follows:

Category	Count of Successfull Requests
ACCESSORIES	1695
ARCADE	2125
NULL	0
SHOOTER	1029
SIMULATION	983
SPORTS	595
STRATEGY	3589
TEE	1582

Annotations highlight the "categories" column header and the "count by category" column header. A callout box points to the "Format" button at the bottom left of the table area, with the text "Click here to format results".

Format the Results

- Various formatting options are available

The screenshot shows the Splunk Pivot interface titled "New Pivot". At the top, there are filters for "Last 7 days" and "Category". Below the filters, the main table has "Category" as the row key and "Count of Successfull Requests" as the column value. The table lists categories like ACCESSORIES, ARCADE, and NULL, with their respective request counts. A modal dialog for the NULL category is open, showing summary statistics: General (Totals: Yes, No), Summary (Percentages: Yes, No), and a large empty area for further details.

Category	Count of Successfull Requests
ACCESSORIES	1695
ARCADE	2125
NULL	0
	1029
	983
	595
	3589
	1582
	11598

Formatted Results

The screenshot shows a Splunk interface titled "New Pivot". The top navigation bar includes "Save As... ▾", "Clear", "Edit Dataset", "Web requests ▾", and a menu icon. Below the title, it displays "31,005 events (5/25/22 5:00:00.000 PM to 6/1/22 5:57:31.000 PM)". The left sidebar has icons for various data types: grid, line chart, area chart, bar chart, funnel, pie chart, scatter plot, donut chart, and a number "42". The main area is divided into sections: "Filters" (with "Last 7 days" selected), "Split Columns" (with a "+" button), "Documentation" (with a link), "Split Rows" (with "Category" selected), "Column Values" (with "Count of Suc..." selected), and a table view. The table has two columns: "Category" and "Count of Successfull Requests". The data rows are: ACCESSORIES (1695), ARCADE (2125), NULL (0), SHOOTER (1029), SIMULATION (983), SPORTS (595), STRATEGY (3589), and TEE (1582). A green box highlights the total value "11598" at the bottom right of the table.

Category	Count of Successfull Requests
ACCESSORIES	1695
ARCADE	2125
NULL	0
SHOOTER	1029
SIMULATION	983
SPORTS	595
STRATEGY	3589
TEE	1582
	11598

Split Columns

- 1 Click **+** under Split Columns and select a field to split by
- 2 Select the desired formatting options

The screenshot shows the Splunk Pivot interface with the following details:

- New Pivot** screen title.
- Filters**: Last 7 days.
- Split Rows**: Category (selected).
- Time**: @_time.
- Field**:
 - a action taken
 - a client IP
 - # date_mday
 - a host
 - a product category
 - a product ID
 - a product name** (highlighted with a green box)
 - a request time
 - # size
 - a source
 - a source
 - # status
- Successfull Requests** table:
 - 1695
 - 2125
 - 0
 - 1029
 - 183
 - 195
 - 189
 - 182
 - 198
- Formatting Options**:
 - product name
 - All Columns
 - Max Columns: 100 (highlighted with a blue box), Group Others
 - Totals: Yes (highlighted with a blue box), No
- Add To Table** button.

Split Columns: Results

New Pivot
✓ 31,028 events (5/25/22 6:00:00.000 PM to 6/1/22 6:19:55.000 PM)

Save As... Clear Edit Dataset Web requests Documentation ↗

Filters Last 7 days +
Split Rows Category +
Split Columns product name +
Column Values Count of Suc... +

The ALL column shows row totals by Category

Category	Benign Space Debris	Curling 2014	Dream Crusher	Final Sequel	Fire Resistance Suit of Provolone	Holy Blade of Gouda	Manganiello Bros.	Manganiello Bros. Tee	Mediocre Kingdoms	Orvil the Wolverine	Pupp... Zombies	Cubicle	Cheese	Cheese Tee	ALL
STRATEGY	666	599							659		531				2455
ARCADE	429							604		430					1463
ACCESSORIES					583	549									1132
TEE									591						517
SHOOTER														716	716
SIMULATION													689		689
SPORTS	380														380
	429	380	666	599	583	549	604	591	659	430	531	689	716	517	7943

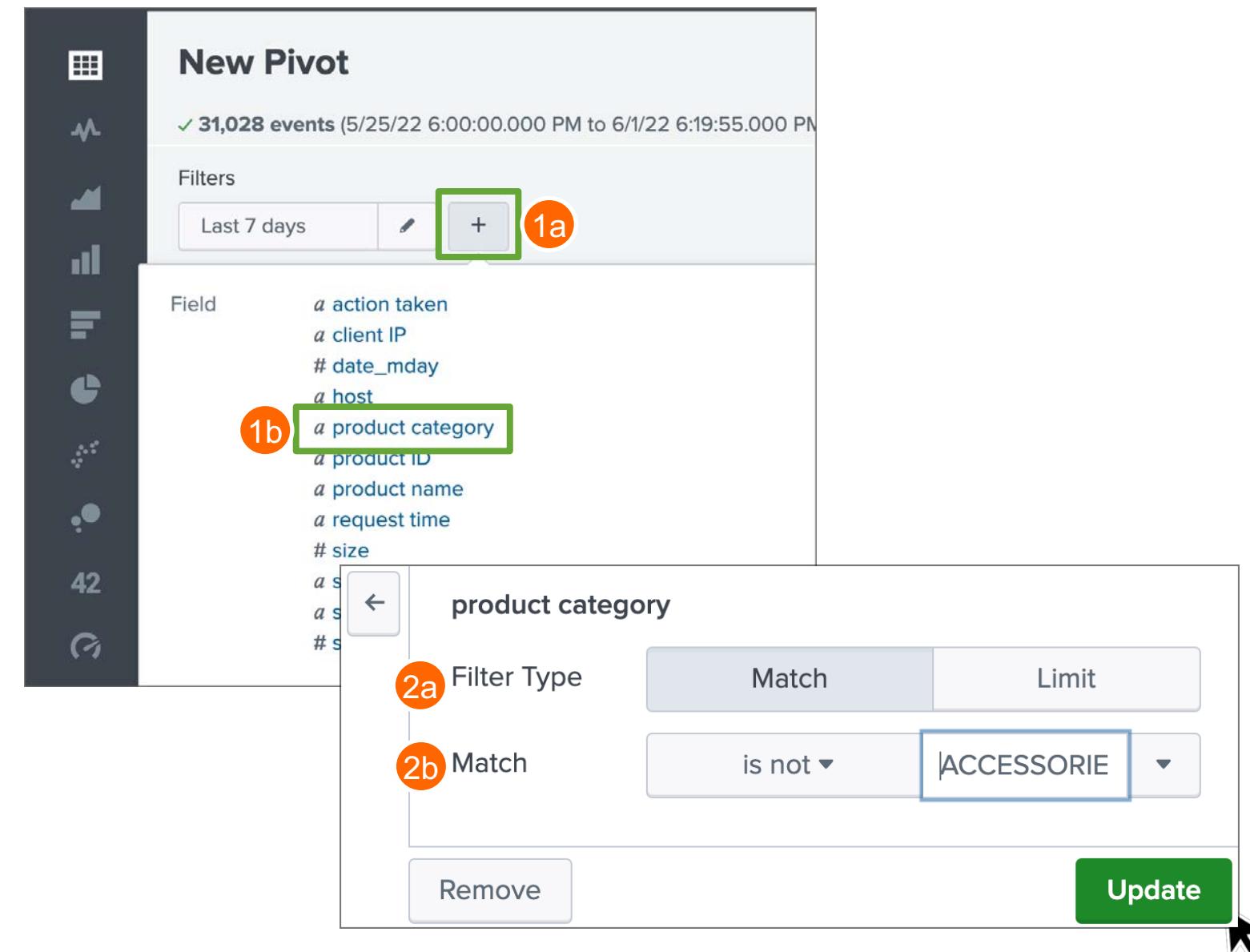
The bottom row shows column totals by Product Name

20 per page ▾ Format

Add Additional Filters

- Refine a pivot by filtering on field-value pairs

- 1 Click **+** under Filters and choose a Field
- 2a Set the Filter Type
- 2b Configure Match filter and value constraints



Filtered Pivot: Results

New Pivot

✓ 29,364 events (5/25/22 6:00:00.000 PM to 6/1/22 6:43:34.000 PM)

Save As... Clear Edit Dataset Web requests ▾

Filters

Last 7 days product cate... +

Pivot is now filtered by time and a field-value

Split Columns

product name +

Documentation ↗

Split Rows

Category +

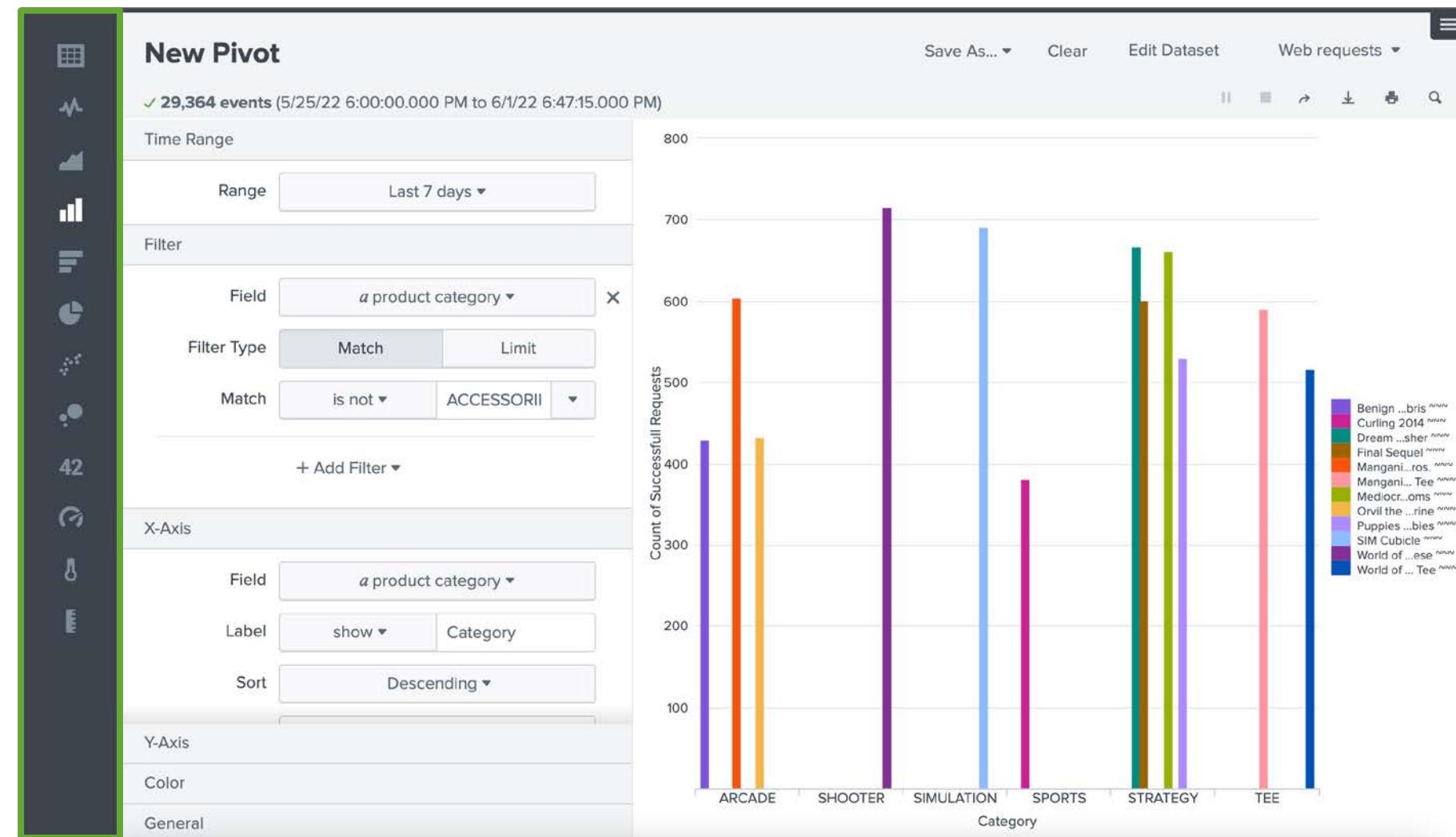
Column Values

Count of Suc... +

Category	Debris	Curling	Dream Crusher	Final Sequel	Manganiello Bros.	Manganiello Bros. Tee	Mediocre Kingdoms	Orvil the Wolverine	Puppies vs. Zombies	SIM Cubicle	World of Cheese	World of Cheese Tee	All
STRATEGY		668	601			662		432	531			2462	
ARCADE	430			604						432		1466	
TEE					591						517	1108	
SHOOTER										716		716	
SIMULATION									692			692	
SPORTS	381											381	
	430	381	668	601	604	591	662	432	531	692	716	517	6825

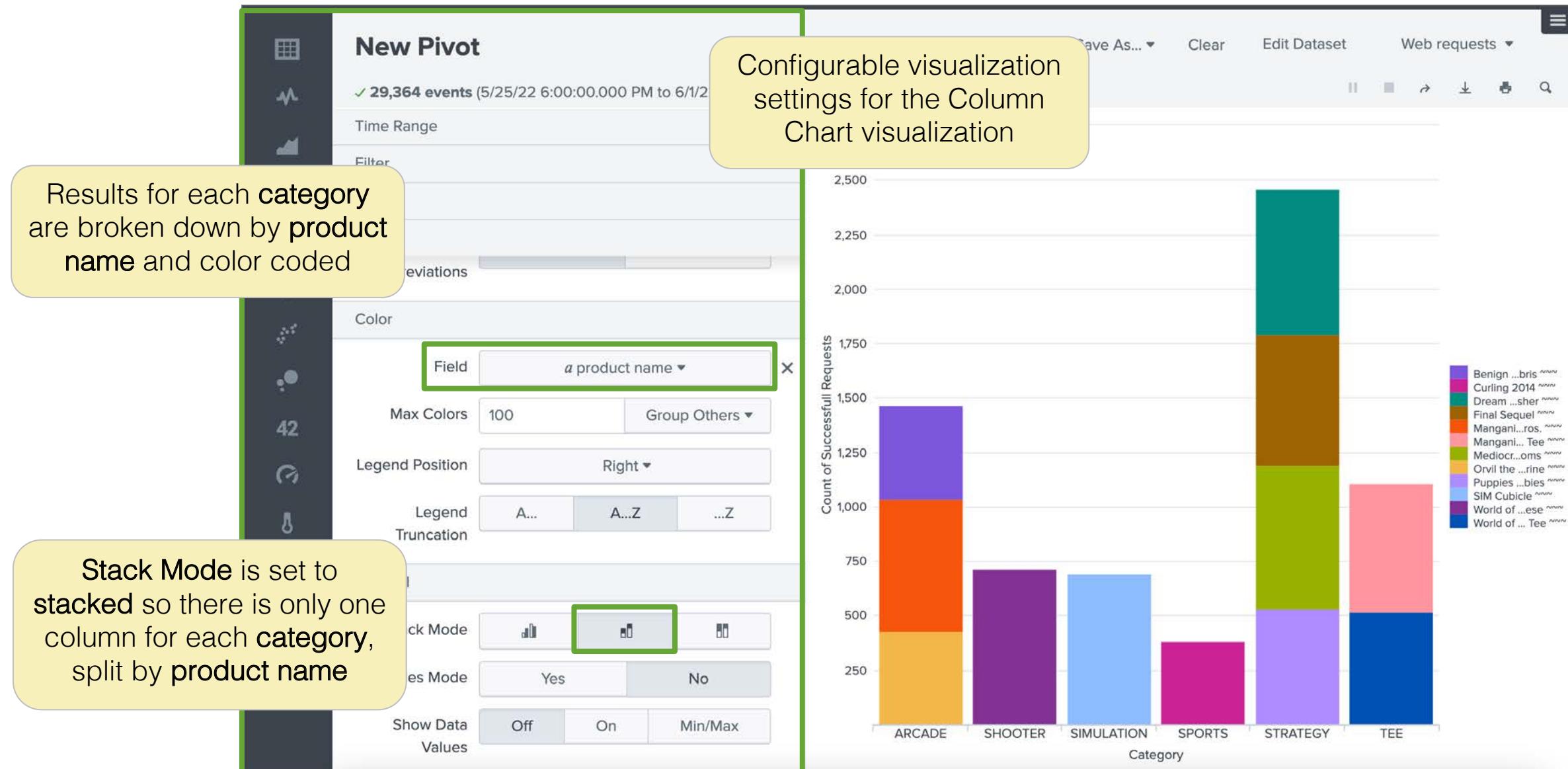
Pivot Visualizations

The Pivot Document Action Bar provides various options for visualizing Pivot results: Line Chart, Area Chart, Column Chart, etc.



Modify Visualization Settings

Each visualization offers different, configurable settings



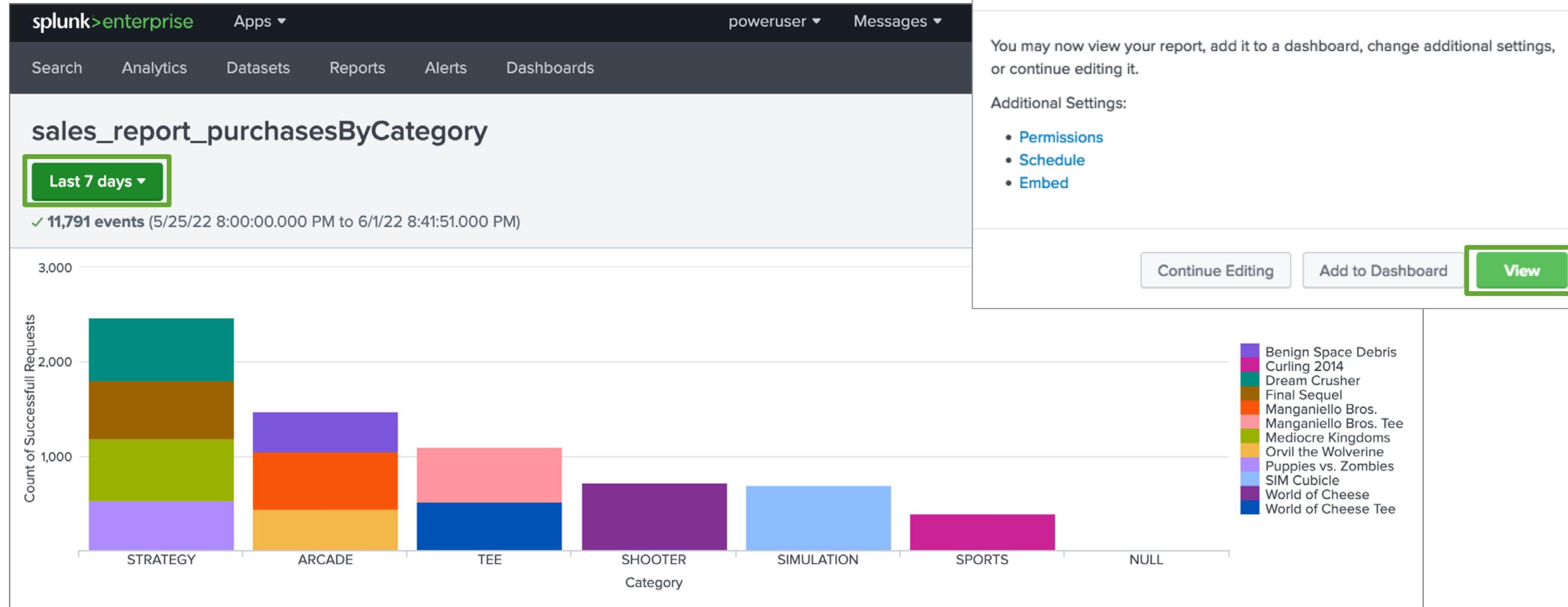
Save a Pivot

Pivots can be saved as reports or as part of a dashboard panel

The screenshot illustrates the process of saving a pivot report. On the left, the 'New Pivot' configuration pane is visible, containing various settings like Time Range, Filter, X-Axis, Y-Axis, Abbreviations, Color, General, Stack Mode, Multi-series Mode, and Show Data Values. In the center, a stacked bar chart displays the 'Count of Successful Requests' for different game categories: ARCADE, SHOOTER, SIMULATION, SPORTS, STRATEGY, and TEE. The Y-axis ranges from 0 to 2,750. The STRATEGY category shows the highest count, exceeding 2,000 requests. On the top right, a 'Save As...' dropdown menu is open, with 'Report' selected (indicated by a red circle with the number 1). A 'Save As Report' dialog box is overlaid on the main interface. It contains fields for 'Title' (set to 'sales_report_purchasesByCategory'), 'Description' (set to 'optional'), and a 'Time Range Picker' section where 'Yes' is selected. At the bottom right of the dialog is a large green 'Save' button, which is also highlighted with a red circle and the number 3, with a mouse cursor pointing at it.

View a Pivot Report

If a Time Range Picker was added to the saved report, it displays when the report is viewed

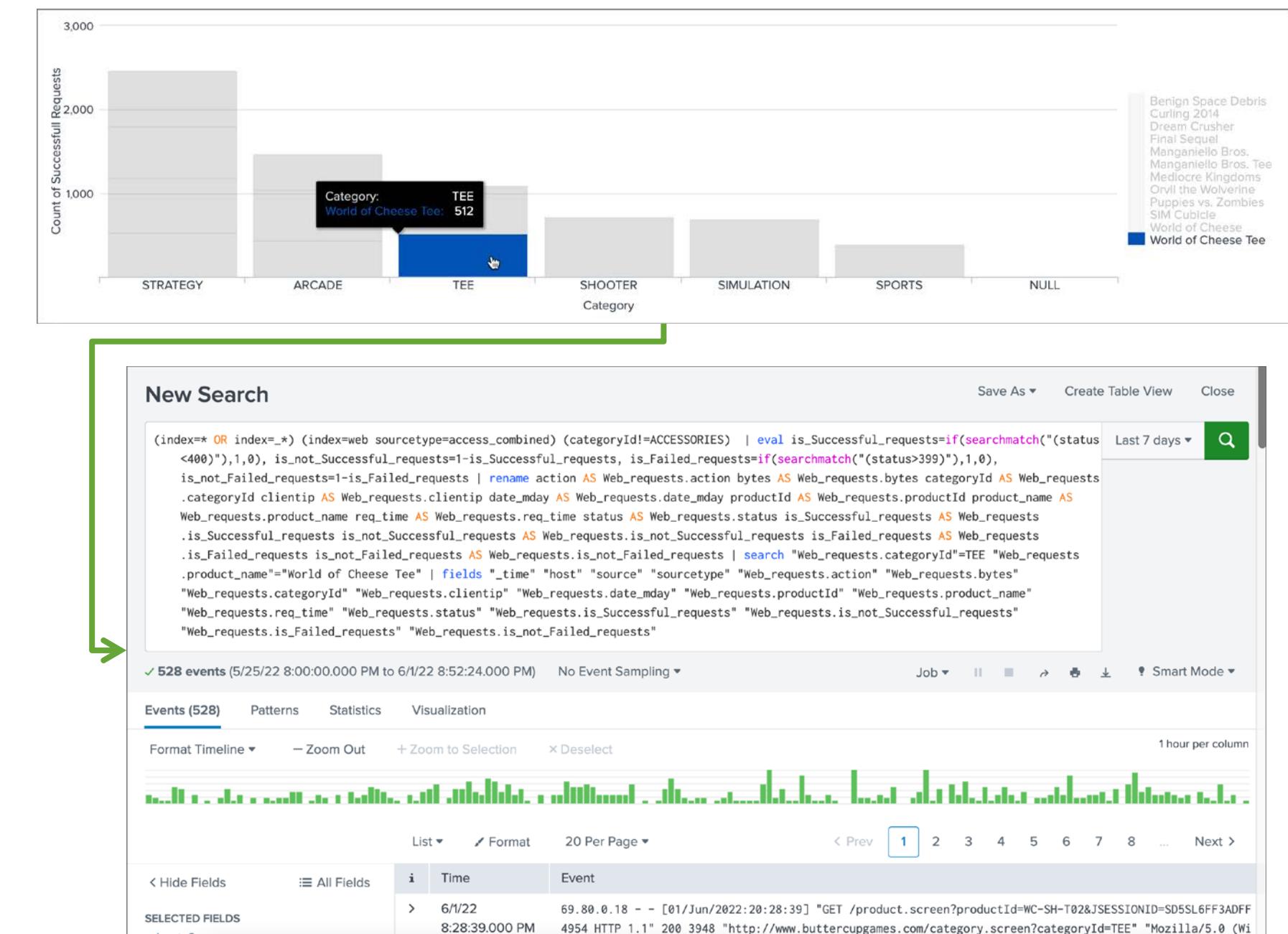


Interact with a Pivot Report

- Mouse over an object to reveal its details
- When you click on part of the report, a drilldown occurs that shows the underlying search details

Note

The search generated by drilldown may be more detailed than your original search. However, it produces the same results.

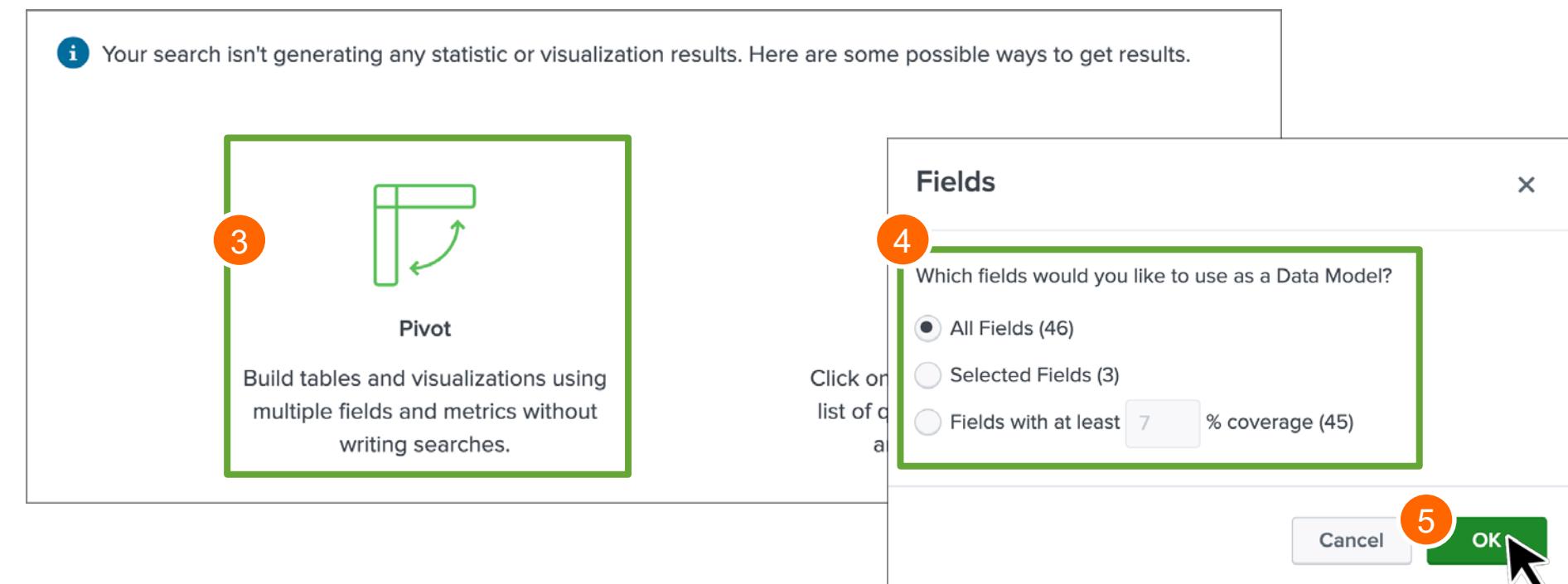
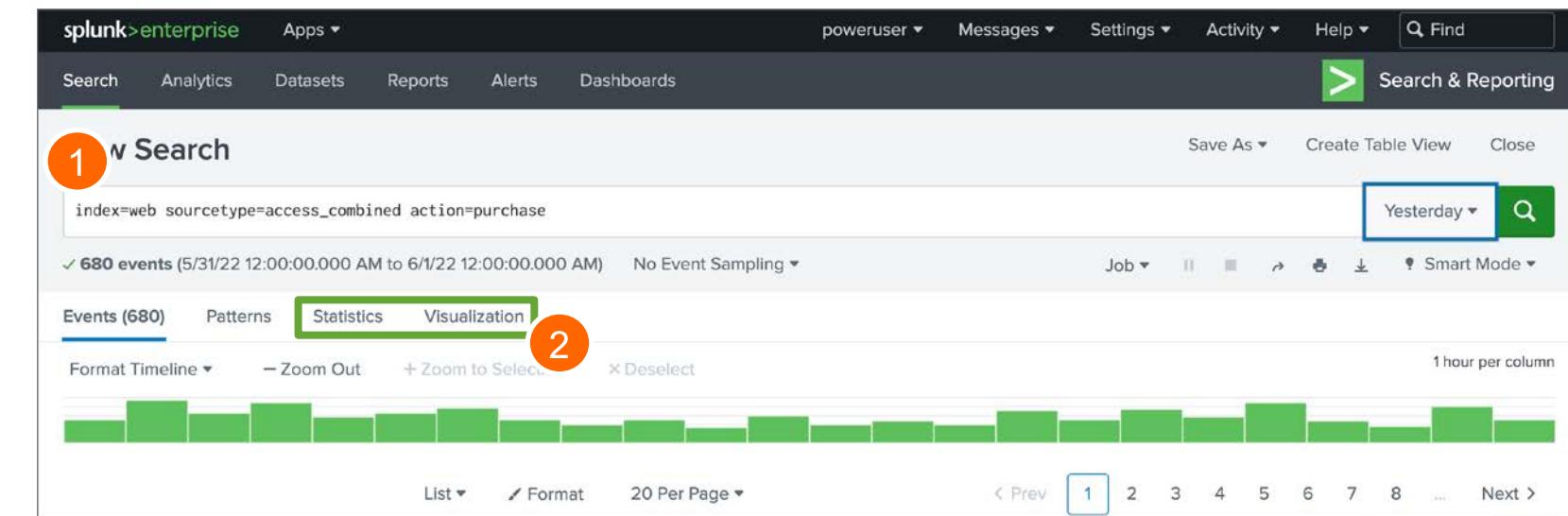


Instant Pivot Overview

- Instant Pivot allows you to utilize the Pivot tool without a preexisting data model
- Instant Pivot creates an underlying data model utilizing the search criteria entered during the initial search

Access Instant Pivot

- 1 Execute a non-transforming search
- 2 Choose Statistics or Visualization tab
- 3 Click Pivot icon
- 4 Select the fields to be included in the data model object
- 5 Click OK to create the Pivot



Save an Instant Pivot as a Report

- A Model Title is required when saving an Instant Pivot as a report
- The Model ID is automatically generated based on the Model Title

The screenshot illustrates the steps to save an Instant Pivot as a report:

- New Pivot**: The main interface shows a search results summary: "680 events (5/31/22 12:00:00.000 AM to 6/1/22 12:00:00.000 AM)". It includes sections for **Filters** (Yesterday), **Split Columns**, and **Column Values**. A **Save As...** button is at the top right, with a dropdown menu open showing "Report" (circled in orange).
- Save As Report**: The **Title** field is populated with "sales_report_purchases". The **Description** field contains "optional". The **Time Range Picker** has "Yes" selected.
- Model Title**: The input field is "purchase data model". Below it, the **Model ID ?** field is populated with "purchase_data_model". A note states: "The data model ID can only contain letters, numbers, dashes, and underscores. Do not start the data model ID with a period."
- Save**: The final step is to click the green **Save** button (circled in orange).

View Underlying Search

View the underlying search for an active Pivot by clicking 

New Pivot

✓ 26,976 events (5/25/22 9:00:00.000 PM to 6/1/22 9:23:19.000 PM)

New Search

```
| pivot Buttercup_Games_Site_Activity Successful_requests count(Successful_requests) AS "Count of Successful requests" SPLITROW categoryId AS Last 7 days Category SPLITCOL product_name SORT 100 categoryId ROWSUMMARY 0 COLSUMMARY 0 NUMCOLUMNS 100 SHOWOTHER 1
```

✓ 26,979 events (5/25/22 9:00:00.000 PM to 6/1/22 9:25:15.000 PM) No Event Sampling

Events Patterns Statistics (7) Visualization

20 Per Page ▾ Format Preview ▾

Category	Benign Space Debris	Curling 2014	Dream Crusher	Final Sequel	Fire Resistance Suit of Provolone	Holy Blade of Gouda	Manganiello Bros.	Manganiello Bros. Tee	Mediocre Kingdoms	NULL	Orvil the Wolverine	Puppies vs. Zombies	SIM Cubicle	World of Cheese
ACCESSORIES	0	0	0	0	588	541	0	0	0	559	0	0	0	0
ARCADE	440	0	0	0	0	0	604	0	0	671	438	0	0	0
SHOOTER	0	0	0	0	0	0	0	0	0	322	0	0	0	720
SIMULATION	0	0	0	0	0	0	0	0	0	294	0	0	697	0
SPORTS	0	384	0	0	0	0	0	0	0	211	0	0	0	0

View Underlying Search (cont.)

```
| pivot Buttercup_Games_Online_Sales successful_request count(successful_request) AS "Count of Successful Requests" SPLITROW categoryId AS category SPLITCOL product_name FILTER categoryId isNot ACCESSORIES TOP 100 count(successful_request) ROWSUMMARY 0 COLSUMMARY 0 NUMCOLUMNS 100 SHOWOTHER 1
```

Data model name

| **pivot Buttercup_Games_Online_Sales**

Object (dataset) name

successful_request
count(successful_request) AS "Count of Successful Requests"

Split row field (or attribute)

SPLITROW categoryId AS category

Split column field (or attribute)
and filter field/value pair

**SPLITCOL product_name FILTER categoryId
isNOT ACCESSORIES**

Create a Pivot Lab Exercise

Time: 15 minutes

Tasks:

- Test your data model by creating a simple Pivot
- Add a field to your data model that uses an eval expression
- Add fields from a lookup to your data model
- Verify that new fields work by creating Pivot reports
- Create a visualization in the Pivot editor
- Add Pivot reports to a dashboard

Accelerate Data Models

Topic Objectives

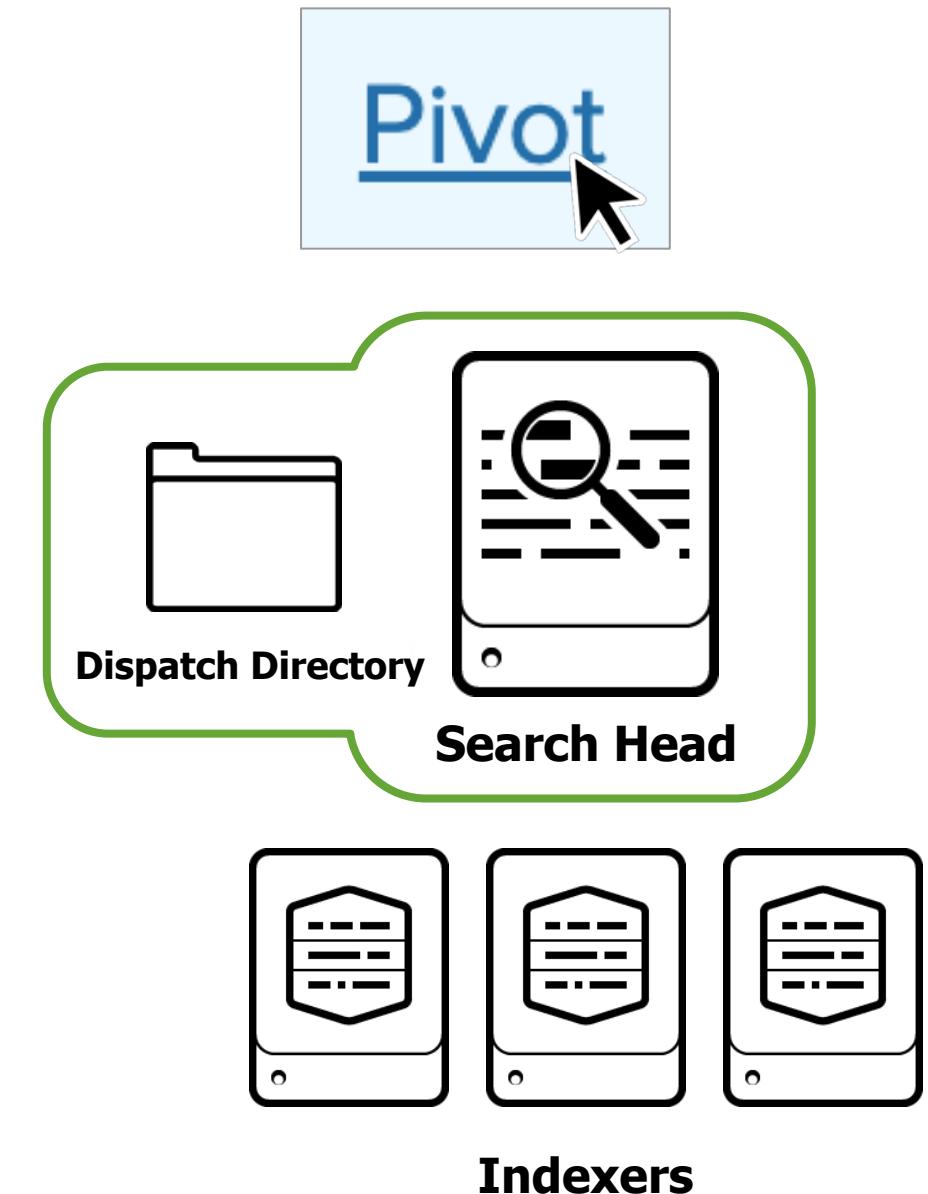
- Define ad-hoc and persistent data model acceleration
- Accelerate a data model
 - Describe the role of `tsidx` files in persistent data model acceleration
 - Review considerations about data model acceleration

Data Model Acceleration

- Generates summaries to speed pivot and report completion times
- Takes the form of inverted time-series index (**tsidx**) files that have been optimized for speed
- Consists of two forms:
 - Ad hoc data model acceleration
 - Persistent data model acceleration

Ad Hoc Data Model Acceleration

- An ad hoc acceleration summary is built anytime a user accesses a data model dataset in Pivot
- Storing summaries in dispatch directories on the search head allows for acceleration of all 3 root dataset types: event, search, and transaction (and their children)



Ad Hoc Data Model Acceleration (cont.)

- Summaries are created for each user currently accessing a data model dataset in Pivot which increases search head load
- The initial acceleration summary is built over all time and as the report is fine-tuned in the Pivot editor, the performance improves
- Ad hoc acceleration is temporary and only exists for the duration of the Pivot session
 - Reports or dashboard panels made in a pivot session do not benefit from ad hoc acceleration when ran outside of the Pivot session

Persistent Data Model Acceleration

- Persistent data model acceleration builds dedicated summaries in indexes and exists as long as the data model exists
- Once accelerated, Splunk maintains the dedicated summaries
- Reports and dashboard panels generated from persistently accelerated data models complete more quickly
- Summaries can be used by `Pivot`, `datamodel`, and `tstats`
- Multiple users can access the summary at the same time

Persistent Data Model Acceleration (cont.)

- Admin permissions or the `accelerate_datamodel` capability is required to accelerate a data model
- Private data models can't be accelerated
- Accelerated data models can't be edited
- When accelerating a data model, only the following datasets are accelerated:
 - Root event datasets
 - Root search datasets that only include streaming commands
 - Child datasets of these qualifying root datasets

Compare Data Model Accelerations

Ad Hoc	Persistent
The acceleration is built every time the Pivot editor is accessed	Explicitly defined before using
Exists only for the duration of user's Pivot editor session	Exists as long as data model exists
Runs over all time (i.e., can't be scoped to specific time range)	Can be scoped to specific time ranges
Has no restrictions while in the Pivot editor	Has some restrictions
Reports run without any acceleration	Reports run faster and perform better overall

The rest of this topic discusses persistent data model acceleration only

Accelerate a Data Model

1. Click Settings > Data Models
2. Select a data model and click Edit > Edit Acceleration
3. Click the Accelerate check box and choose a Summary Range

The screenshot illustrates the process of accelerating a data model in the Splunk interface. It consists of two main panels: the 'Data Models' list and the 'Edit Acceleration' configuration dialog.

1. Data Models: This panel shows a list of five data models. The second item, 'Buttercup Games Site Activity', is selected. A context menu is open over this row, with the 'Edit Acceleration' option highlighted and circled in orange. A green arrow points from this option to the corresponding step in the list below.

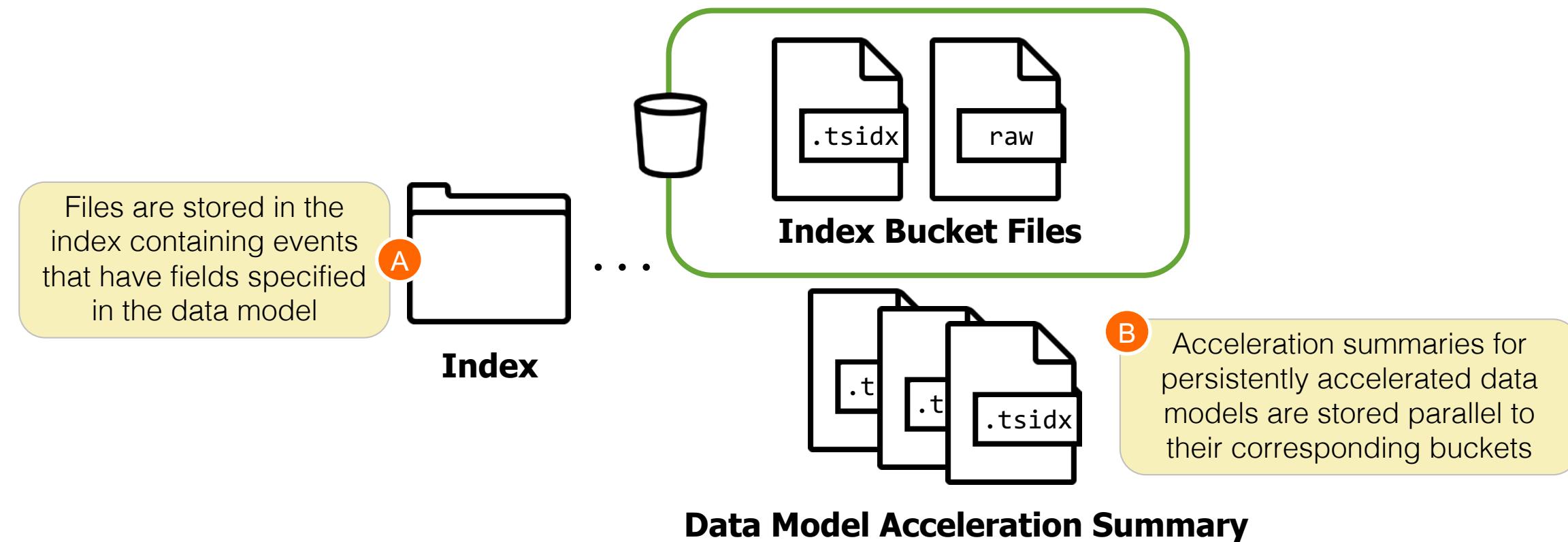
2. Edit Acceleration: This panel is a modal window for the selected data model. It contains the following fields:

- Data Model:** Buttercup Games Site Activity
- Accelerate:** (also highlighted with an orange circle)
- Summary Range:** 1 Day (also highlighted with an orange circle)
- Advanced Settings:** A dropdown menu is open, showing options: 1 Day (highlighted with a blue border), 7 Days, 1 Month, 3 Months, 1 Year, All Time, and Custom.

A green arrow points from the 'Edit Acceleration' button in the Data Models list to the 'Edit Acceleration' button in this dialog. Another green arrow points from the 'Summary Range' dropdown in the dialog back to the 'Edit Acceleration' button in the list.

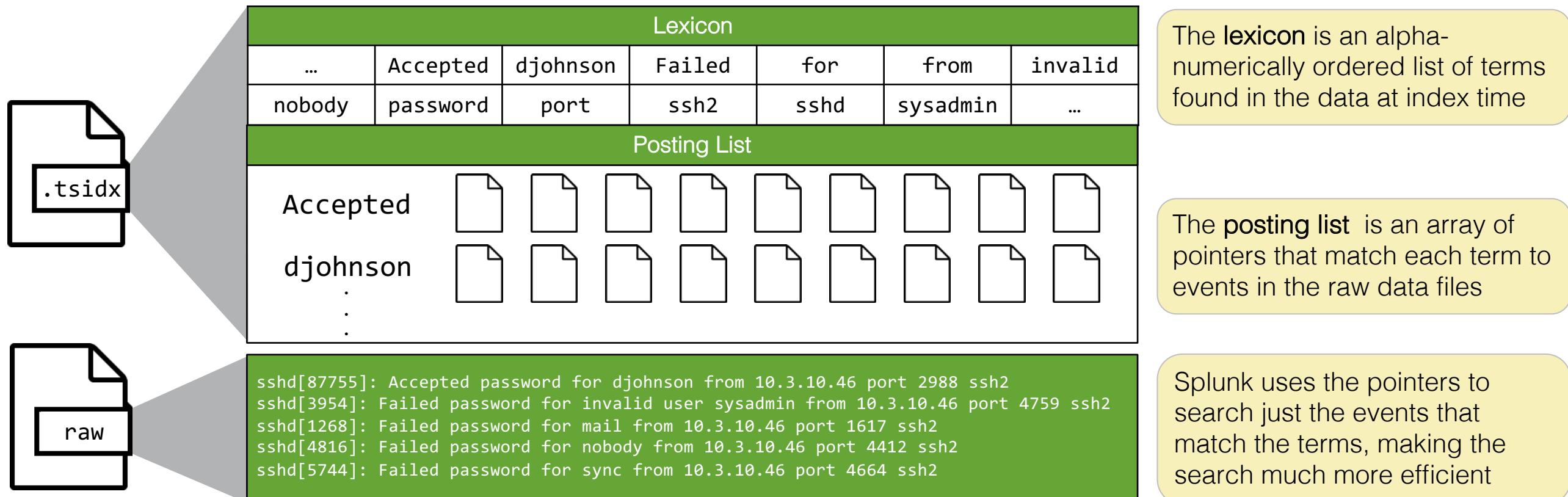
After Accelerating a Data Model

Splunk builds an acceleration summary for the specified summary range in the form of inverted time-series index (`.tsidx`) files



Time Series Index (tsidx) Files

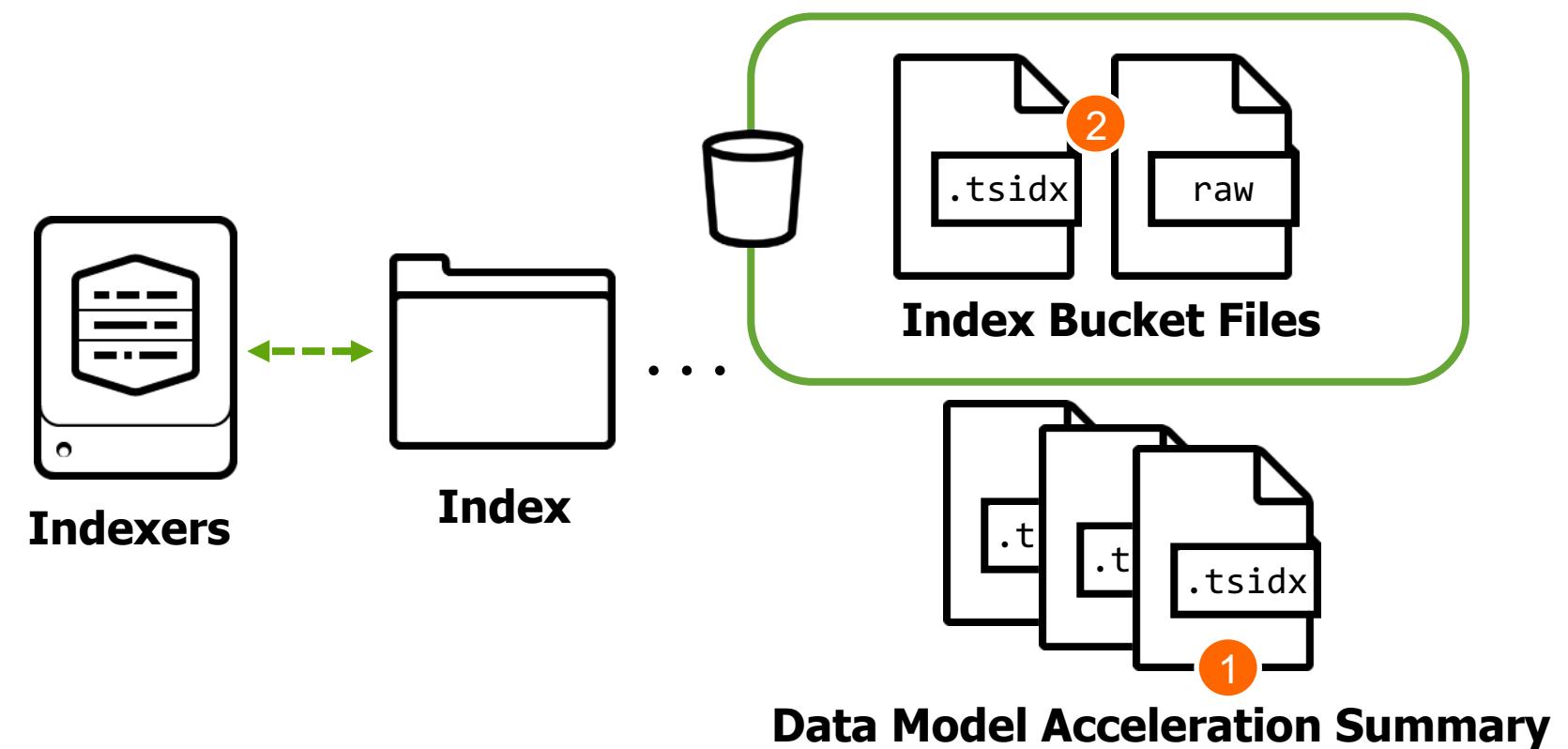
- Exist inside buckets alongside raw data files
- Consist of a lexicon and a posting list and the indexed **field::value** combinations (**host**, **source**, and **sourcetype**)



Search With Data Model Acceleration

① Indexer retrieves information about the data model that has been stored on disk in the `.tsidx` files that make up the acceleration summary

② Indexer pulls additional events from bucket files if search is outside data summary range



Accelerated Data Model Considerations

- The acceleration summary always contains a store of data that at least meets the summary range (may slightly exceed)
- Splunk updates `tsidx` files every 5 minutes and removes outdated summary data every 30 minutes
- Accelerated data model summaries can be accessed through:
 - Pivot editor
 - Searches using `pivot`, `tstats` or `datamodel` (outside the scope of this course)

Accelerate Data Models Lab Exercise

Time: 20 minutes

Tasks:

- Accelerate a data model
- Explore your data model using search commands

Wrap-up Slides

Community

- Splunk Community Portal
community.splunk.com
 - Answers
 - Discussions
 - Splunk Trust
 - User Groups
 - Ideas
- Splunk Blogs
splunk.com/blog/
- Splunk Apps
splunkbase.com
- Splunk Dev Google Group
groups.google.com/forum/#!forum/splunkdev
- Splunk Docs on Twitter
twitter.com/splunkdocs
- Splunk Dev on Twitter
twitter.com/splunkdev
- Splunk Live!
splunklive.splunk.com
- .conf
conf.splunk.com

Support Programs

- Web
 - Documentation: dev.splunk.com and docs.splunk.com
- Splunk Lantern
 - Guidance from Splunk experts
 - lantern.splunk.com
- Global Support
 - Support for critical issues, a dedicated resource to manage your account – 24 x 7 x 365
 - Web: splunk.com/index.php/submit_issue
- Enterprise, Cloud, ITSI, Security Support
 - Web: splunk.com/en_us/about-splunk/contact-us.html#tabs/customersupport
 - Phone: (855) SPLUNK-S or (855) 775-8657

Support ^

Support Portal

Submit a case ticket

Splunk Answers

Ask Splunk experts questions

Contact Us

Contact our customer support

Product Security Updates

Keep your data secure

System Status

Learning Paths (cont.)

Knowledge Manager - Recommended Courses

Free eLearning courses are in blue and courses with an * are present in both learning paths.

- What is Splunk *
- Introduction to Splunk *
- Using Fields *
- Introduction to Knowledge Objects
- Creating Knowledge Objects
- Creating Field Extractions
- Enriching Data with Lookups
- Data Models
- Introduction to Dashboards
- Dynamic Dashboards
- Using Choropleth
- Search Optimization *

Learning Paths

Search Expert - Recommended Courses

Free eLearning courses are in blue and courses with an * are present in both learning paths.

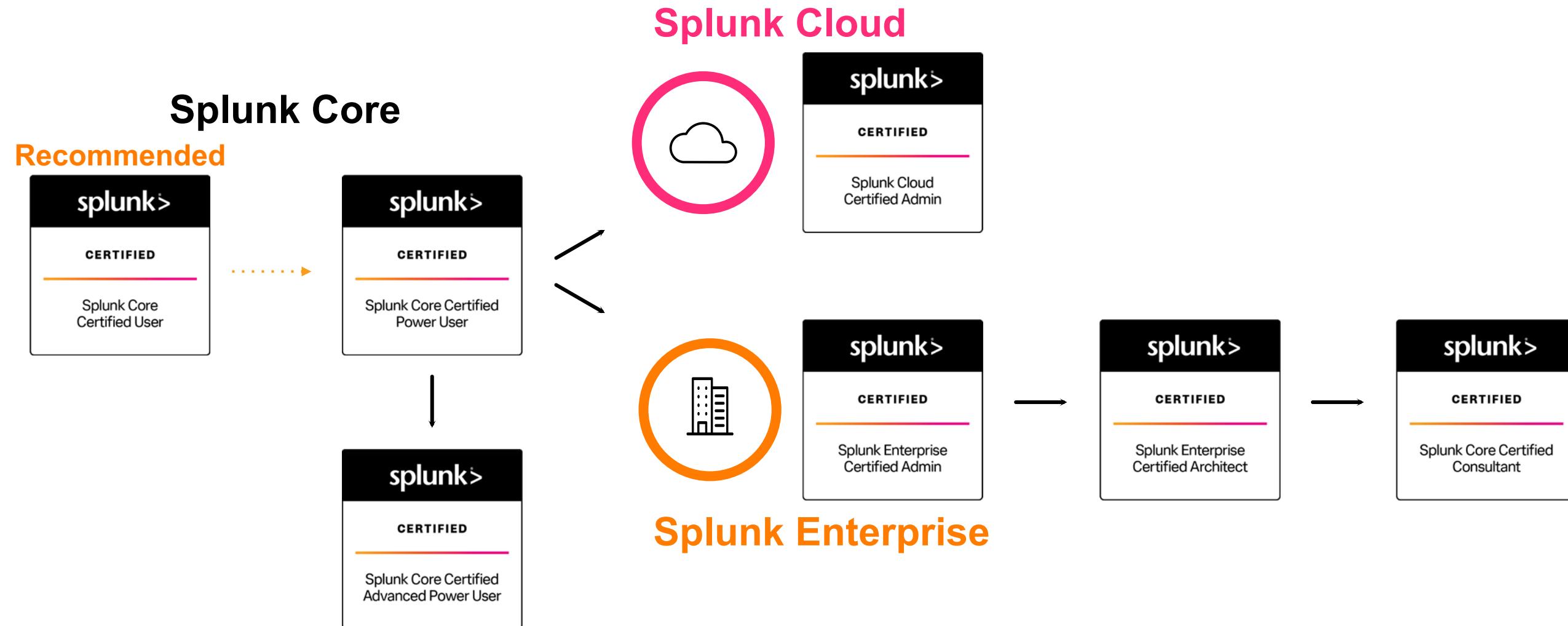
- What is Splunk *
- Introduction to Splunk *
- Using Fields *
- Scheduling Reports and Alerts
- Visualizations
- Statistical Processing
- Working with Time
- Comparing Values
- Result Modification
- Leveraging Lookups and Subsearches
- Correlation Analysis
- Search Under the Hood
- Multivalue Fields
- Search Optimization *

Splunk Certification

Offerings & Requirements

Splunk Core and Beyond

Regardless of which Splunk product you use, it all starts with Splunk Core



Splunk Core Certified User

This entry-level certification demonstrates an individual's basic ability to navigate and use Splunk software



Prerequisite Certification(s):

- None

Prerequisite Course(s):

- None

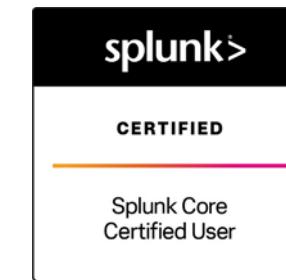
Splunk Core Certified User Exam

Time to [study](#)! We suggest candidates looking to prepare for this exam complete Fundamentals 1 **or** the following courses:

- What is Splunk?
- Intro to Splunk
- Using Fields
- Scheduling Reports and Alerts
- Visualizations
- Statistical Processing
- Working with Time
- Leveraging Lookups and Subsearches
- Search Optimization
- Enriching Data with Lookups
- Data Models

See [here](#) for registration assistance.

Congratulations! You are a...



Recommended Next Step

- Splunk Core Certified Power User

Splunk Core Certified Power User

This entry-level certification demonstrates an individual's foundational competence of Splunk's core software



Prerequisite Certification(s):

- None

Prerequisite Course(s):

- None

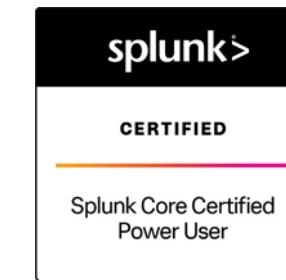
Splunk Core Certified Power User Exam

Time to [study](#)! We suggest candidates looking to prepare for this exam complete Fundamentals 2 **or** the following courses:

- Visualizations
- Statistical Processing
- Working with Time
- Comparing Values
- Result Modification
- Correlation Analysis
- Search Under the Hood
- Introduction to Knowledge Objects
- Creating Knowledge Objects
- Creating Field Extractions
- Data Models
- Using Choropleth

See [here](#) for registration assistance.

Congratulations! You are a...



Recommended Next Steps

- [Splunk Core Certified Advanced Power User](#)
- [Splunk Enterprise Certified Admin](#)
- [Splunk Cloud Certified Admin](#)

Splunk Core Certified Advanced Power User

This certification demonstrates an individual's ability to generate complex searches, reports, and dashboards with Splunk's core software to get the most out of their data



Prerequisite Certification(s):

- [Splunk Core Certified Power User](#)

Prerequisite Course(s):

- None

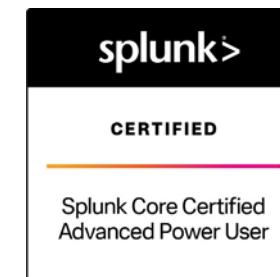
Splunk Core Certified Advanced Power User Exam

Time to [study](#)! We suggest candidates looking to prepare for this exam complete Fundamentals 3, Creating Dashboards, and Advanced Searching & Reporting **or** the following courses:

- Using Fields
- Working with Time
- Comparing Values
- Result Modification
- Leveraging Lookups and Subsearches
- Correlation Analysis
- Search Under the Hood
- Multivalue Fields
- Search Optimization
- Creating Field Extractions
- Enriching Data with Lookups
- Data Models
- Using Choropleth
- Introduction to Dashboards
- Dynamic Dashboards

See [here](#) for registration assistance.

Congratulations! You are a...



Recommended Next Steps

- [Splunk Enterprise Certified Admin](#)
- [Splunk Cloud Certified Admin](#)

Thank You

