Making the Pipeline More Readable

- Put each pipe in the pipeline on a separate line as you type by turning on auto-formatting
- Go to **Preferences > SPL Editor** and turn on Search auto-format

Instead of this:

New Search

```
index=web sourcetype=access_* status=503 | stats sum(price) as lost_revenue | eval lost_revenue = "$" + tostring(lost_revenue, "commas")
```

You'll get this:

New Search

```
index=web sourcetype=access_* status=503
| stats sum(price) as lost_revenue
| eval lost_revenue = "$" + tostring(lost_revenue, "commas")
```

Note

You can also use **Shift + Enter** to go to a new line.

Syntax Coloring

- By default, some parts of the search string are automatically colored as you type
- The color is based on the search syntax
- The rest of the search string remains black

BOOLEAN OPERATORS and **COMMAND MODIFIERS** are in **orange**

```
index=web (sourcetype=acc* OR sourcetype=ven*) action=purchase status<400 | timechart span=1h sum(price) by sourcetype
```

COMMANDS are in **blue**

FUNCTIONS are in **purple**

COMMAND ARGUMENTS are in **green**

Syntax Coloring (cont.)

- You can turn off automatic syntax coloring
  1. Go to **Preferences** > **SPL Editor**
  2. Choose the Themes tab and select Black on White instead of the Light Theme default
  3. Click Apply
- You can also display colored text against a black background by selecting Dark Theme

```
index=web (sourcetype=acc* OR sourcetype=ven*) action=purchase status<400 | timechart span=1h sum(price) by sourcetype
```

Creating a Table

- `table` command returns a table formed by only fields in the argument list
- Columns are displayed in the order given in the command
  - Column headers are field names
  - Each row represents an event
  - Each row contains field values for that event

Scenario

Display the `clientip`, `action`, `productId`, and `status` of customer interactions in the online store for the last 4 hours.

```
index=web sourcetype=access_combined
| table clientip, action, productId,
  status
```

clientip	action	productId	status
220.225.12.171	view	WC-SH-A02	200
220.225.12.171		WC-SH-G04	200
188.173.152.100		CU-PG-G06	200
188.173.152.100	purchase		200
188.173.152.100	purchase	WC-SH-T02	200
188.173.152.100	addtocart	WC-SH-T02	200
188.173.152.100		WC-SH-T02	200
188.173.152.100		WC-SH-A02	200

Renaming Fields in a Table

- To change the name of a field, use the `rename` command
- Useful for giving fields more meaningful names
- When including spaces or special characters in field names, use double straight quotes:

  A `rename productId as ProductID`

  B `rename action as "Customer`

  C `Action" rename status as "HTTP Status"`

Scenario

Display the `clientip`, `action`, `productId`, and `status` of customer interactions in the online store for the last 4 hours.

```
index=web sourcetype=access_combined
| table clientip, action, productId,
status
| rename action as "Customer
Action" rename productId as ProductID,
status as "HTTP
Status"
```

clientip	Customer Action (B)	ProductID (A)	HTTP Status (C)
12.130.60.4			200
27.102.11.11		SC-MG-G10	200
27.102.11.11		DC-SG-G02	200
27.102.11.11			200
27.102.11.11	view	FI-AG-G08	200
99.61.68.230	purchase		200
99.61.68.230	purchase	WC-SH-A01	200
99.61.68.230	addtocart	WC-SH-A01	200

Renaming Fields in a Table (cont.)

Once you rename a field, you can’t access it with the original name

```
index=web sourcetype=access_combined
| table clientip, action, productId,
status
| rename productId as
  ProductID, action as
  "Customer Action",  status
  as "HTTP Status"| table action, status
```

No results found.

```
index=web sourcetype=access_combined
| table clientip, action, productId,
status
| rename productId as
  ProductID, action as
  "Customer Action",  status
  as "HTTP Status"
 | table "Customer Action", "HTTP
 Status"
```

Customer Action	HTTP Status
purchase	200
purchase	200
addtocart	200
	200
	200
view	200
view	200
	200

Using the `fields` Command

- Field extraction is one of the most costly parts of a search
- `fields` command allows you to include or exclude specified fields in your search or report
- To include, use `fields +` (default)
  - Occurs before field extraction
  - Improves performance
- To exclude, use `fields -`
  - Occurs after field extraction
  - No performance benefit
  - Exclude fields used in search to make the table/display easier to read

`fields` Command – Examples

Using command improves performance—only specified fields extracted

Scenario

Display network failures during the previous week.

```
index=security
sourcetype=linux_secu
re (fail* OR invalid)
```

Returned **6,567** results by scanning **6,567** events in **1.425** seconds:

< Hide Fields All Fields

SELECTED FIELDS
a host 4
a source 4
a sourcetype 1

INTERESTING FIELDS
a action 1
a app 1

i	Time	Event
>	1/6/18 11:58:24.000 PM	Sat Jan 06 2018 23:58:24 www3 sshd[4559]: Failed password for nagios from 67.133.102.54 port 4437 ssh2 host = www3 | source = /opt/log/www3/secure.log | sourcetype = linux_secure
>	1/6/18 11:58:24.000 PM	Sat Jan 06 2018 23:58:24 mailsv1 sshd[1258]: Failed password for myuan from 77.123.102.237 port 1611 ssh2 host = mailsv1 | source = /opt/log/mailsv1/secure.log | sourcetype = linux_secure
>	1/6/18	Sat Jan 06 2018 23:58:24 www2 sshd[1896]: Failed password for nagios from 87.194.216

Scenario

Display network failures during the previous week. Retrieve only `user`, `app`, and `src_ip`.

```
index=security
sourcetype=linux_secu
re (fail* OR invalid)
| fields user, app,
src_ip
```

Returned **6,567** results by scanning **6,567** events in **0.753** seconds:

< Hide Fields All Fields

INTERESTING FIELDS
a app 1
a src_ip 100+
a user 100+

+ Extract New Fields

i	Time	Event
>	1/6/18 11:58:24.000 PM	Sat Jan 06 2018 23:58:24 www3 sshd[4559]: Failed password for nagios from 67.133.102.54 port 4437 ssh2
>	1/6/18 11:58:24.000 PM	Sat Jan 06 2018 23:58:24 mailsv1 sshd[1258]: Failed password for myuan from 77.123.102.237 port 1611 ssh2
>	1/6/18 11:58:24.000 PM	Sat Jan 06 2018 23:58:24 www2 sshd[1896]: Failed password for nagios from 87.194.216.51 port 3698 ssh2
>	1/6/18 11:58:24.000 PM	Sat Jan 06 2018 23:58:24 www3 sshd[2746]: Failed password for invalid user db2dba from 203.45.206.135 port 3825 ssh2

Using the dedup Command

Use dedup to remove duplicates from your results

```
index=sales sourcetype=vendor_sales Vendor=Bea* | table Vendor, VendorCity,
VendorStateProvince, VendorCountry
```

Vendor	VendorCity	VendorStateProvince	VendorCountry
Beach Games	Miami	Florida	United States
Beads & Games	Ft. Riley	Kansas	United States
Beach Games	Miami	Florida	United States
Beantown Games	Boston	Massachusetts	United States
Beantown Games	Boston	Massachusetts	United States
Beach Games	Fort Lauderdale	Florida	United States

```
…| dedup Vendor | table
```

Vendor	VendorCity	VendorStateProvince	VendorCountry
Beach Games	Miami	Florida	United States
Beads & Games	Ft. Riley	Kansas	United States
Beantown Games	Boston	Massachusetts	United States
Beauty Games	Butte	Montana	United States

```
…| dedup Vendor, VendorCity | table …
```

Vendor	VendorCity	VendorStateProvince	VendorCountry
Beach Games	Miami	Florida	United States
Beads & Games	Ft. Riley	Kansas	United States
Beach Games	Fort Lauderdale	Florida	United States
Beantown Games	Boston	Massachusetts	United States
Beauty Games	Butte	Montana	United States

Using the `sort` Command

- Use `sort` to order your results in `+ ascending` (default) or `– descending`
- To limit the returned results, use the `limit` option

```
... | sort limit=20 –categoryId, product_name

... | sort 20 count
```

sort Learn More

Sorts search results by the specified fields.

Example:
... | sort ip, -url

Using the `sort` Command (cont.)

`sort -/+<fieldname>` sign followed by fieldname sorts results in the sign's order

`sort -/+ <fieldname>` sign followed by **space** and then fieldname applies sort order to **all** following fields without a different explicit sort order

```
index=sales sourcetype=vendor_sales
Vendor=Bea*
| dedup Vendor, VendorCity
| table Vendor, VendorCity,
VendorStateProvince, VendorCountry
| sort –Vendor, VendorCity
```

Vendor	VendorCity	VendorStateProvince	VendorCountry
Beauty Games	Butte	Montana	United States
Beantown Games	Boston	Massachusetts	United States
Beads & Games	Ft. Riley	Kansas	United States
Beach Games	Fort Lauderdale	Florida	United States
Beach Games	Miami	Florida	United States

```
index=sales sourcetype=vendor_sales
Vendor=Bea*
| dedup Vendor, VendorCity
| table Vendor, VendorCity,
VendorStateProvince, VendorCountry
| sort – Vendor, VendorCity
```

Vendor	VendorCity	VendorStateProvince	VendorCountry
Beauty Games	Butte	Montana	United States
Beantown Games	Boston	Massachusetts	United States
Beads & Games	Ft. Riley	Kansas	United States
Beach Games	Miami	Florida	United States
Beach Games	Fort Lauderdale	Florida	United States

Useful References

- Search Reference: http://docs.splunk.com/Documentation/Splunk/latest/SearchReference
- Search Quick Reference: http://docs.splunk.com/Documentation/Splunk/latest/SearchReference/Sp lunkEnterpriseQuickReferenceGuide

Module 9
Transforming Commands

Getting Top Values

- The `top` command finds the most common values of a given field in the result set
- By default, output displays in table format

src_ip	count	percent
132.55.227.221	105	27.131783
214.156.206.45	9	2.325581
118.6.85.68	9	2.325581
87.194.216.51	8	2.067183
108.65.113.83	6	1.550388
89.11.192.18	5	1.291990
211.166.11.101	5	1.291990
195.69.160.22	5	1.291990
81.18.148.190	4	1.033592
223.205.219.67	4	1.033592

Scenario

Determine which IP addresses generated the most attacks in the last 60 minutes,

```
index=security sourcetype=linux_secure
(fail* OR invalid)
| top src_ip
```

`top` Command

- By default, returns top 10 results
- Automatically returns count and percent columns
- Common constraints: `limit countfield showperc`
- `top` command with `limit=20` is automatically added to your search string when you click Top values in a field window

```
index=web sourcetype=access_combined action=purchase status=200 | top limit=20 categoryId
```

`top` Command – Single Field

- Control # of results displayed using `limit`
- `limit=#` returns this number of results
- `limit=0` returns unlimited results

```
index=security sourcetype=linux_secure
(fail* OR invalid) | top limit=5 src_ip
```

Scenario

During the last hour, display the top 5 IPs that generated the most attacks.

src_ip	count	percent
132.55.227.221	106	27.390181
118.6.85.68	9	2.325581
87.194.216.51	8	2.067183
214.156.206.45	8	2.067183
108.65.113.83	7	1.808786

`top` Command – Multiple Fields

- If the `showperc` is not included – or it is included and set to `t` – a percent column is displayed
- If `showperc=f`, then a percent column is NOT displayed

Scenario

Display the top 3 common values for users and web categories browsed during the last 24 hours.

```
index=network sourcetype=cisco_wsa_squid
| top cs_username  x_webcat_code_full limit=3
```

A B

cs_username A	x_webcat_code_full	count	percent
kjoslin@buttercupgames.com	Sports and Recreation	81	6.617647
kperna@buttercupgames.com	Shopping	61	4.983660
apreusig@buttercupgames.com	Arts and Entertainment B	58	4.738562

top Command – Single Field with by Clause

Scenario 1

Display the top 3 web categories browsed by each user during the last 24 hours.

```
index=network sourcetype=cisco_wsa_squid
| top x_webcat_code_full by cs_username limit=3
```

B A

A B

cs_username	x_webcat_code_full	count	percent
acurry@buttercupgames.com	Uncategorized URLs	5	35.714286
acurry@buttercupgames.com	Shopping	4	28.571429
acurry@buttercupgames.com	Health and Nutrition	3	21.428571
adombrowski@buttercupgames.com	Uncategorized URLs	1	50.000000
adombrowski@buttercupgames.com	Computers and Internet	1	50.000000
apreusig@buttercupgames.com	Arts and Entertainment	58	95.081967

Scenario 2

Display the top 3 users for each web category during the last 24 hours.

```
index=network sourcetype=cisco_wsa_squid
| top cs_username by x_webcat_code_full limit=3
```

C D

D C

x_webcat_code_full	cs_username	count	percent
Advertisements	gnooteboom@buttercupgames.com	5	41.666667
Advertisements	iking@buttercupgames.com	3	25.000000
Advertisements	tzielinski@buttercupgames.com	2	16.666667
Arts and Entertainment	fbryan@buttercupgames.com	61	46.923077
Arts and Entertainment	moh@buttercupgames.com	6	4.615385
Arts and Entertainment	pbunch@buttercupgames.com	4	3.076923

`top` Command – Renaming `countfield` Display

- By default, the display name of the `countfield` is `count`
- `countfield=`*`string`* renames the field for display purposes

Scenario

Display the top 3 user/web categories combinations during the last 24 hours. Rename the count field and show count, but not the percentage.

```
index=network sourcetype=cisco_wsa_squid
| top cs_username x_webcat_code_full limi A
  countfield="Total Viewed" B     showperc=f
```

cs_username	x_webcat_code_full	Total Viewed
kjoslin@buttercupgames.com A	Sports and Recreation	81 B
kperna@buttercupgames.com	Shopping	61
apreusig@buttercupgames.com	Arts and Entertainment	58

Note

A Boolean can be t/f, true/false, as well as 1/0.

`rare` Command

- The `rare` command returns the least common field values of a given field in the results
- Options are identical to the `top` command

Scenario

Identify which product is the least sold by Buttercup Games vendors over the last 60 minutes.

```
index=sales sourcetype=vendor_sales
| rare product_name showperc=f limit=1
```

Events | Patterns | **Statistics (1)** | Visualization

20 Per Page ▾ | Format | Preview ▾

product_name	count
Manganiello Bros. Tee	1

`stats` Command

- `stats` enables you to calculate statistics on data that matches your search criteria
- Common functions include:
  - `count` – returns the number of events that match the search criteria
  - `distinct_count, dc` – returns a count of unique values for a given field
  - `sum` – returns a sum of numeric values
  - `avg` – returns an average of numeric values
  - `list` – lists all values of a given field
  - `values` – lists unique values of a given field

Note

To view all of the functions for `stats`, please see: http://docs.splunk.com/Documentation/Splunk/latest/SearchReference/CommonStatsFunctions

stats Command – count

- `count` returns the number of matching events based on the current search criteria
- Use the `as` clause to rename the countfield

Scenario

Count the invalid or failed login attempts during the last 60 minutes.

```
index=security sourcetype=linux_secure
(invalid OR failed)
| stats count
```

Events | Patterns | **Statistics (1)** | Visualization

20 Per Page ▾ | Format | Preview ▾

count ⇕
380

```
index=security sourcetype=linux_secure
(invalid OR failed)
| stats count as "Potential Issues"
```

Events | Patterns | **Statistics (1)** | Visualization

20 Per Page ▾ | Format | Preview ▾

Potential Issues ⇕
385

stats Command – count(*field*)

Adding a *field* as an argument to the count function returns the number of events where a value is present for the specified field

Scenario

Count the number of events during the last 15 minutes that contain a vendor action field. Also count the total events.

```
index=security sourcetype=linux_secure
| stats count(vendor_action) as ActionEvents, count as TotalEvents
```

A

B

Events (59) Patterns **Statistics (1)** Visualization

20 Per Page ▾ Format Preview ▾

A ActionEvents	B TotalEvents
52	59

stats Command – by *fields*

Scenario

Count the number of events by user, app, and vendor action during the last 15 minutes.

```
index=security sourcetype=linux_secure
| stats count by user, app, vendor_action
```

user	app	vendor_action	count
administrator	sshd	Failed	1
agushto	sshd	Failed	1
backup	sshd	Failed	1
bin	sshd	Failed	2
brian	sshd	Failed	1
db	sshd	Failed	2
db2fenc1	sshd	Failed	2
db4	sshd	Failed	1
dba	sshd	Failed	1
demon	sshd	Failed	1

- `by` clause returns a count for each value of a named field or set of fields
- Can use any number of fields in the `by` *`field`* list

`stats` Command – `distinct_count(`*`field`*`)`

- `distinct_count()` or `dc()` provides a count of how many unique values there are for a given field in the result set
- This example counts how many unique values for `s_hostname`

Scenario

How many unique websites have employees visited in the last 4 hours?

```
index=network sourcetype=cisco_wsa_squid
| stats dc(s_hostname) as "Websites visited:"
```

stats Command – sum(*field*)

Scenario

How much bandwidth did employees consume at each website during the past week?

```
index=network sourcetype=cisco_wsa_squid
| stats sum(sc_bytes) as Bandwidth by s_hostname
| sort -Bandwidth
```

For fields with a numeric value, you can sum the actual values of that field

Events | Patterns | Statistics (520) | Visualization

20 Per Page ▾ | Format | Preview ▾

s_hostname	Bandwidth
www.archerytalk.com	6330733
www.infoblox.com	2818279
www.bjc-aces.com	1849884
www.bradblog.com	1489356
www.ncsl.org	1425778

`stats` Command – `sum(`*`field`*`)` – (cont.)

Scenario

Report the number of retail units sold and sales revenue for each product during the previous week.

```
index=sales sourcetype=vendor_sales
| stats count(price) as "Units Sold"
sum(price) as "Total Sales" by product_name
| sort -"Total Sales"
```

- A A single `stats` command
- B can have multiple functions
- C The `by` clause is applied to both functions
- D `sort` Total Sales in descending order

product_name	Units Sold	Total Sales
Dream Crusher	78	3119.22
World of Cheese	78	1949.22
Manganiello Bros.	45	1799.55
SIM Cubicle	72	1439.28
Final Sequel	55	1374.45
Mediocre Kingdoms	50	1249.50
Orvil the Wolverine	30	1199.70
Benign Space Debris	31	774.69
Curling 2014	28	559.72
World of Cheese Tee	47	469.53

stats Command – avg(*field*)

- The avg function provides the average numeric value for the given numeric field
- An event is not considered in the calculation if it:
  - Does not have the field
  - Has an invalid value for the field

Scenario

What is the average bandwidth used for each website usage type?

```
index=network sourcetype=cisco_wsa_squid
| stats avg(sc_bytes) as "Average Bytes" A
  by usage B
```

B

usage	Average Bytes
Borderline	18870.117341640707
Business	12957.355321020228
Personal	12915.358326596604
Unknown	12747.842960288808
Violation	8831.08888888889

A

`stats` Command – `list(`*`field`*`)`

- `list` function lists all field values for a given field
- This example lists the websites visited by each employee
  - Security logs generate an event for each network request
    - ? The same hostname appears multiple times
  - To return a list of “unique” field values, use the `values` function

Scenario

Which websites has each employee accessed during the last 60 minutes?

```
index=network sourcetype=cisco_wsa_squid
| stats list(s_hostname) as "Websites
  visited:" by cs_username
```

cs_username	Websites visited:
	www.filmschoolrejects.com
apucci@buttercupgames.com	www.zimbio.com
arangel@buttercupgames.com	www.cnet.com
basselin@buttercupgames.com	www.americangangster.net www.americangangster.net www.americangangster.net www.blossomfloristla.com 84654321.cn
bgenin@buttercupgames.com	www.ambrosiasw.com www.ambrosiasw.com www.ambrosiasw.com

`stats` Command – `values(`*`field`*`)`

Scenario

Display by IP address the names of users who have failed access attempts in the last 60 minutes.

```
index=security sourcetype=linux_secure fail*
 | stats values(user) as "User Names",
   count(user) as Attempts by src_ip
```

`values` function lists unique values for the specified field

src_ip	User Names	Attempts
107.3.146.207	administrator pat uni	3
109.169.32.135	harrypotter irc	2
110.138.30.229	daemon	1
111.161.27.20	administrator daemon games	3
112.111.162.4	noone	1

Formatting `stats` Tables

- Tables created with `stats` commands can be formatted
- Color code data in each column, based on rules you define
- Add number formatting (e.g. currency symbols, thousands separators)
- Can also format data on a per-column basis by clicking the icon above that column

product_name	Units Sold	Total Sales
Benign Space Debris	16	399.84
Curling 2014	35	699.65
Dream Crusher	23	919.77
Final Sequel	27	674.73

Formatting `stats` Tables – Examples

product_name	Units Sold	Total Sales
Benign Space Debris	16	399.84
Curling 2014	35	699.65
Dream Crusher	23	919.77
Final Sequel	27	674.73
Fire Resistance Suit of Provolone	17	67.83
Holy Blade of Gouda	44	263.56

Total Sales
£ 399.84
£ 699.65
£ 919.77
£ 674.73
£ 67.83
£ 263.56
£ 999.75
£ 359.64

Module 10:
Creating Reports and Dashboards

What Are Reports?

- Reports are saved searches
- Reports can show events, statistics (tables), or visualizations (charts)
- Running a report returns fresh results each time you run it
- Statistics and visualizations allow you to drill down by default to see the underlying events
- Reports can be shared and added to dashboards

Smart Naming

- Before you begin using Splunk on the job, define a naming convention so you can always find your reports and tell them apart
- For example, you can create something simple like this:
  - <group>_<object>_<description>
    - **group**: the name of the group or department using the knowledge object such as sales, IT, finance, etc.
    - **object**: report, dashboard, macro, etc.
    - **description**: WeeklySales, FailedLogins, etc.
  - Using this example, a quarterly sales report can be identified as:
    - Sales_Report_QuarterlySalesRevenue

Note

If you set up naming conventions early in your implementation, you can avoid some of the more challenging object naming issues. The example is a suggestion. The details are found in the Splunk product documentation: http://docs.splunk.com/Documentation/Splunk/latest/Kn owledge/Developnamingconventionsforknowledgeobjec ttitles

Creating a Report from a Search

1. Run a search
2. Select **Save As**
3. Select **Report**

Creating a Report from a Search (cont.)

- A Give the report a meaningful title (required)
- B Specify a description (optional)
- C Select whether to include or not to include a time range picker
  - The report is saved with the time range that was selected when it was created
  - Adding a time range picker allows you to adjust the time range of the report when you run it

Creating a Report from a Search (cont.)

- You can change Additional Settings, as well as use the dialog buttons:
  - Click **Continue Editing** to make changes to your report
  - Click **Add to Dashboard** to add your report to a dashboard
  - Click **View** to display your report or run it again

Additional Settings

Dialog buttons

Running Reports

- Click **Reports**, then click the report title to run it
  - The report runs using the time range that was specified when it was saved
- Use the time range picker to change the time range of the report (if available)

Editing Reports

- To edit a report's underlying search, select **Edit > Open in Search**
  - You can then edit and re-save, not save, or save-as a new report
- You can also edit the description, permissions, schedule, and acceleration
- Additionally, you can clone or delete the report

Creating Tables and Visualizations

Three main methods to create tables and visualizations in Splunk are:

1. Select a field from the fields sidebar and choose a report to run
2. Use the Pivot interface
   - Start with a dataset

     or
   - Start with Instant Pivot
   - See Module 11 in this presentation for more information about Pivot
1. Use the Splunk search language transforming commands in the Search bar

Viewing Tables and Visualizations

- Statistical reports leverage Splunk's built-in visualizations or table format
- These views give you insights into your organization’s data

Creating Reports From the Field Window

- Numeric fields: choose from six report types with mathematical functions, such as average, maximum value, and minimum value
- This example generates a report that shows the average over time
  - This is known as a **timechart**

Creating a Top Values Report

- For alphanumeric character fields, there are only 3 available reports
- In this example, you want a report that shows the top **categories** purchased
  1. Run basic search: `sourcetype=access_combined status=200 action=purchase`
  2. Click the **categoryId** field
  3. Click **Top values**

Creating a Top Values Report (cont.)

4. The `top` command with `limit=20` is added to the search string
5. A bar chart is returned on the Visualizations tab, displaying the top categories purchased

Changing the Visualization

- Select a visualization from the visualization type dropdown menu
- In this example, the column chart is changed to a pie chart

Changing the Visualization Format

- The **Format** menu allows you to change formatting options
- For example, for bar and column charts:
  - The **General** tab allows you to change Stack and Multi-series modes
  - The **X-Axis** and **Y-Axis** tabs allow you to change the axis labels and orientation
  - **Chart Overlay** allows you to add context to the chart by overlaying other field values

  - The **Legend** tab allows you to position the visualization legend as desired
  - **Stack Mode** allows you to stack colors to improve column chart readability when several colors are involved

Changing the Visualization Format (cont.)

- Show Data Values determines whether to show data values in the visualization
- If Min/Max is selected, data is only shown on the bars containing the minimum and maximum values

Note

When you make a change to the visualization settings – such as Min/Max – the visualization updates immediately.

Note

Learn more about modes and axes in the *Splunk Fundamentals 2* course. These modes require more sophisticated searches.

Viewing Results as a Table

Switch to the **Statistics** tab to view the results as a table

Events | Patterns | **Statistics (7)** | Visualization

20 Per Page ▾ | Format | Preview ▾

categoryId	count	percent
STRATEGY	900	30.622661
ARCADE	554	18.849949
ACCESSORIES	409	13.916298
TEE	385	13.099694
SHOOTER	282	9.595100
SIMULATION	269	9.152773
SPORTS	140	4.763525

Using the Data Overlay Format

- **Heat map** highlights outstanding values

- **High and low values** highlights max and min of non zero values

What Is a Dashboard?

- A dashboard consists of one or more panels displaying data visually in a useful way – such as events, tables, or charts
- A report can be used to create a panel on a dashboard

Adding a Report to a Dashboard

In the report, click Add to Dashboard to begin

Adding a Report to a Dashboard (cont.)

- A Name the dashboard and optionally provide a description
- B Change the permissions (use Private until tested)
  Enter a meaningful title for the panel
- C For **Panel Powered By,** click **Report**
- D
- E For Panel Content, click **Column Chart** to display the visualization in the dashboard

Note

The Dashboard ID is automatically populated with a unique value used by Splunk and should not be changed.

Adding a Report to a Dashboard (cont.)

After it is saved, you can view the dashboard immediately, or select the dashboard from the **Dashboards** view

Why Create Panels from Reports?

- It is efficient to create most dashboard panels based on reports because
  - A single report can be used across different dashboards
  - This links the report definition to the dashboard
- Any change to the underlying report affects every dashboard panel that utilizes that report

Editing Panels

- After saving the panel, a window appears from which you can view the updated dashboard
- Click Edit to customize the dashboard

Editing Panel Layout

Click on the dotted bar on a panel to drag the panel to a new location

More Options icon (discussed on next slide)

Edit Panel Drilldown Options

1. In Edit Dashboard mode, click the More Options icon on any panel and select Edit Drilldown
2. In Drilldown Editor, select Link to search to access search directly from visualization

More Options icon

Drilldown from Visualization to Search

Once drilldown option is set, click an object in a chart or table to see its underlying events in Search view

Clone a Dashboard

1. Click the ellipsis menu (**...**) and select **Clone**
2. Change the **Title** as desired and click **Clone Dashboard**

Export a Dashboard

Dashboards can be exported as PDF or printed

Set the Default Dashboard

- Set a dashboard to appear by default in the bottom panel of your home view
- From the Home app, click **Choose a home dashboard**

View Your Default Dashboard

After you've set a dashboard as default, your home view may look like this:

Module 11
Pivot & Datasets

Selecting a Dataset

1. From the Search & Reporting app, select the **Datasets** tab
   - Displays a list of available lookup table files ("lookups") and data models
   - Each lookup and data model represent a specific category of data
   - Prebuilt lookups and data models make it easier to interact with your data

2. Click **Explore > Visualize with Pivot**

Opening in Pivot

- The Pivot automatically populates with a count of events for the selected object
- In this example, it shows all successful purchase requests for all time

Selecting a Time Range

- The default is **All time**
- Click the pencil icon to select the desired time range
- The pivot runs immediately upon selecting the new time range

Split Rows

- Click + under **Split Rows** for a list of available attributes to populate the rows
- In this example, the rows are split by the **category** attribute, which lists:
  - Each game category on a separate row
  - A count of successful requests for each game category

Split Rows (cont.)

- Once selected, you can:
  - Modify the label
  - Change the sort order
    - **Default** – sorts by the field value in ascending order
    - **Ascending** - sorts by the count in ascending order
    - **Descending** – sorts by the count in descending order
  - Define maximum # of rows to display
- Click **Add to Table** to view the results

Results

New Pivot
Save As...
Clear
Successful Requests
15,903 events (1/4/18 9:00:00.000 PM to 1/11/18 9:53:56.000 PM)
Documentation
Filters
Last 7 days
Split Columns
Split Rows
category
Column Values
Count of Suc...
category
Count of Successful Requests
STRATEGY 4745
ARCADE 2986
ACCESSORIES 2303
TEE 2111
SHOOTER 1495
SIMULATION 1389
SPORTS 874
categories
count by category
20 per page
Format
To format the results, click here

Formatting the Results

For example, to add totals on the Summary tab, click Yes next to Totals

Updated Results (with Total)

Split Columns

- Click + under **Split Columns** and select the desired split
- Specify the maximum number of columns and whether you want Totals

Results

New Pivot

Save As... Clear Successful Requests

✓ 15,825 events (1/4/18 10:00:00.000 PM to 1/11/18 10:09:09.000 PM)

Filters: Last 7 days

Split Columns: product name

Split Rows: category

Column Values: Count of Suc...

category	Benign Space Debris	Curling 2014	Dream Crusher	Final Sequel	Fire Resistance Suit of Provolone	Holey Blade of Gouda	Manganiello Bros.	Manganiello Bros. Tee	Mediocre Kingdoms	Orvil the Wolverine	Puppies vs. Zombies	SIM Cubicle	World of Cheese	World of Cheese Tee	ALL
STRATEGY	0	0	1316	1128	0	0	0	0	1319	0	965	0	0	0	4728
ARCADE	825	0	0	0	0	0	1264	0	0	887	0	0	0	0	2976
ACCESSORIES	0	0	0	0	1248	1038	0	0	0	0	0	0	0	0	2286
TEE	0	0	0	0	0	0	0	1180	0	0	0	0	0	913	2093
SHOOTER	0	0	0	0	0	0	0	0	0	0	0	0	1490	0	1490
SIMULATION	0	0	0	0	0	0	0	0	0	0	0	1380	0	0	1380
SPORTS	0	872	0	0	0	0	0	0	0	0	0	0	0	0	872
	825	872	1316	1128	1248	1038	1264	1180	1319	887	965	1380	1490	913	15825

The ALL column shows row totals by category

The bottom (bolded) row shows column totals by product name

Generated by (C) Splunk Inc, not to be redistributed

Add Additional Filters

- You can refine a pivot by filtering on key/value pairs
  - Think of ‘split by’ as rows and columns as the fields to display
  - Think of filters as a field=value inclusion, exclusion or specific condition to apply to the search (=, <, >, !=, *)
- In the example, the pivot is filtered to exclude events from the ACCESSORIES category

Filtered Pivot

- The ACCESSORIES category is filtered out
- All the other categories remain

category	Benign Space Debris	Curling 2014	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	0	0	1322	1130	0	0	1320	0	968	0	0	0	4740
ARCADE	827	0	0	0	1266	0	0	888	0	0	0	0	2981
TEE	0	0	0	0	0	1186	0	0	0	0	0	917	2103
SHOOTER	0	0	0	0	0	0	0	0	0	0	1494	0	1494
SIMULATION	0	0	0	0	0	0	0	0	0	1385	0	0	1385
SPORTS	0	872	0	0	0	0	0	0	0	0	0	0	872
	827	872	1322	1130	1266	1186	1320	888	968	1385	1494	917	13575

Select a Visualization Format

You can display your pivot as a table or a visualization, such as a column chart

Modify Visualization Settings

- When a visualization control is selected, panels appear that let you configure its settings
- In this example:
  - The results for each category are broken down by **product_name**
  - The stack mode is set to stacked

Some of the settings for the column chart include:
- Field to use to further breakdown the data
- Limit on the number of series to be charted
- Specify labels
- Set sort order
- Set stack mode

Saving a Pivot

- Pivots can be saved as reports
  - You can choose to include a Time Range Picker in the report to allow people who run it to change the time range (default is Yes)

Saving a Pivot (cont.)

When you click **View**, the report is displayed with a Time Range Picker (if that's the option you chose)

Mouse Actions

- Mouse over an object to reveal its details
- If drilldown is enabled, it is possible to click on the object to expose the underlying search

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
- To create an Instant Pivot
  1. Execute a search (search criteria only, no search commands)
  2. Click the **Statistics** or **Visualization** tab
  3. Click the **Pivot** icon
  4. Select the fields to be included in the data model object
  5. Create the pivot (table or chart)

Open Instant Pivot

Saving a Pivot as a Report

- When saving as a report, the **Model Title** is required
  - This is used to create a data model, which is required by the pivot report
- The **Model ID** is automatically generated based on the **Model Title**

Note

Manually changing the Model ID is not recommended.

Add a Pivot to a Dashboard

Similarly, you can save any pivot to a new or existing dashboard

Module 12: Creating and Using Lookups

What Is a Lookup?

- Sometimes static (or relatively unchanging) data is required for searches, but isn't available in the index
- Lookups pull such data from standalone files at search time and add it to search results

What Is a Lookup? (cont.)

- Lookups allow you to add more fields to your events, such as:
  - Descriptions for HTTP status codes (“File Not Found”, “Service Unavailable”)
  - Sale prices for products
  - User names, IP addresses, and workstation IDs associated with RFIDs
- After a lookup is configured, you can use the lookup fields in searches
- The lookup fields also appear in the Fields sidebar
- Lookup field values are case sensitive by default

Note

Admins can change the `case_sensitive_match` option to `false` in `transforms.conf`

A Sample Lookup File

- This example displays a lookup `.csv` file used to associate product information with productId
- First row represents field names (header)

  `productId, product_name, categoryId, price, sale_price, Code`
- The `productId` field exists in the `access_combined` events
  - This is the **input** field
- All of the fields listed above are available to search after the lookup is defined
  - These are the **output** fields

```
GNU nano 2.3.1                File: products.csv

productId,product_name,categoryId,price,sale_price,Code
DB-SG-G01,Mediocre Kingdoms,STRATEGY,24.99,19.99,A
DC-SG-G02,Dream Crusher,STRATEGY,39.99,24.99,B
FS-SG-G03,Final Sequel,STRATEGY,24.99,16.99,C
WC-SH-G04,World of Cheese,SHOOTER,24.99,19.99,D
WC-SH-T02,World of Cheese Tee,TEE,9.99,6.99,E
PZ-SG-G05,Puppies vs. Zombies,STRATEGY,4.99,1.99,F
CU-PG-G06,Curling 2014,SPORTS,19.99,16.99,G
MB-AG-G07,Manganiello Bros.,ARCADE,39.99,24.99,H
MB-AG-T01,Manganiello Bros. Tee,TEE,9.99,6.99,I
FI-AG-G08,Orvil the Wolverine,ARCADE,39.99,24.99,J
BS-AG-G09,Benign Space Debris,ARCADE,24.99,19.99,K
SC-MG-G10,SIM Cubicle,SIMULATION,19.99,16.99,L
WC-SH-A01,Holy Blade of Gouda,ACCESSORIES,5.99,2.99,M
WC-SH-A02,Fire Resistance Suit of Provolone,ACCESSORIES,3.99,1.99,N
```

Creating a Lookup

1. Upload the file required for the lookup
2. Define the lookup type
3. Optionally, configure the lookup to run automatically

Adding a New Lookup Table File

Settings > Lookups > Lookup table files

1. Click **New Lookup Table File**
2. Select a destination app
3. Browse and select the `.csv` file to use for the lookup table
4. Enter a name for the lookup file
5. Save

`inputlookup` Command

- Use the `inputlookup` command to load the results from a specified static lookup
- Useful to:
  - Review the data in the .csv file
  - Validate the lookup

Note

When using the `inputlookup` command, you can specify the filename ending with .csv or the lookup definition name.

New Search

Save As ▾ Close

| inputlookup products.csv

Last 24 hours ▾

✓ 14 results (1/8/18 10:00:00.000 PM to 1/9/18 10:36:03.000 PM) No Event Sampling ▾ Job ▾ Smart Mode ▾

Events Patterns **Statistics (14)** Visualization

20 Per Page ▾ Format Preview ▾

Code	categoryId	price	productId	product_name	sale_price
A	STRATEGY	24.99	DB-SG-G01	Mediocre Kingdoms	19.99
B	STRATEGY	39.99	DC-SG-G02	Dream Crusher	24.99
C	STRATEGY	24.99	FS-SG-G03	Final Sequel	16.99
D	SHOOTER	24.99	WC-SH-G04	World of Cheese	19.99
E	TEE	9.99	WC-SH-T02	World of Cheese Tee	6.99
F	STRATEGY	4.99	PZ-SG-G05	Puppies vs. Zombies	1.99
G	SPORTS	19.99	CU-PG-G06	Curling 2014	16.99
H	ARCADE	39.99	MB-AG-G07	Manganiello Bros.	24.99
I	TEE	9.99	MB-AG-T01	Manganiello Bros. Tee	6.99
J	ARCADE	39.99	FI-AG-G08	Orvil the Wolverine	24.99
K	ARCADE	24.99	BS-AG-G09	Benign Space Debris	19.99
L	SIMULATION	19.99	SC-MG-G10	SIM Cubicle	16.99
M	ACCESSORIES	5.99	WC-SH-A01	Holey Blade of Gouda	2.99
N	ACCESSORIES	3.99	WC-SH-A02	Fire Resistance Suit of Provolone	1.99

Creating a Lookup Definition

Settings > Lookups > Lookup definitions

1. Click **New Lookup Definition**
2. Select a destination app
3. Name the lookup definition
4. Select the lookup type, either File-based or External
5. From the drop-down, select a lookup file
6. Save

Applying Advanced Lookup Options

- Min/max # of matches for each input lookup value
- Default value to output (when fewer than the min # of matches present for a given input)
- Case sensitivity match on/off
- Batch index query: improves performance for large lookup files
- Match type: supplies format for non-exact matching
- Filter lookup: filters results before returning data

`lookup` Command

- If a lookup is not configured to run automatically, use the `lookup` command in your search to use the lookup fields

lookup Help More »
Explicitly invokes field value lookups.

Examples

There is a lookup table specified in a stanza name 'usertogroup' in transform.conf. This lookup table contains (at least) two fields, 'user' and 'group'. For each event, we look up the value of the field 'local_user' in the table and for any entries that matches, the value of the 'group' field in the lookup table will be written to the field 'user_group' in the event.

```
... | lookup usertogroup user as local_user OUTPUT group as user_group
```

- The `OUTPUT` argument is optional
  - If `OUTPUT` not specified, `lookup` returns all the fields from the lookup table except the match fields
  - If `OUTPUT` is specified, the fields overwrite existing fields
- The output lookup fields exist only for the current search
- Use `OUTPUTNEW` when you do not want to overwrite existing fields

Using the `lookup` Command

Scenario

Calculate the sales for each product in the last 24 hours.

Creating an Automatic Lookup

Settings > Lookups > Automatic lookups

1. Click **New Automatic Lookup**
2. Select the Destination app
3. Enter a Name for the lookup

1. Select the Lookup table definition
2. Select host, source, or sourcetype to apply to the lookup and specify the name

Creating an Automatic Lookup (cont.)

5. Define the Lookup input fields

   Field(s) that exist in your events that you are relating to the lookup table

   A. Column name in CSV

   B. Field name in Splunk, if different from column name

6. Define the Lookup output fields

   Field(s) from your lookup table that are added to the events

   C. Field name in lookup table

   D. Name you want displayed in Splunk; otherwise it inherits the column name

7. Save

Using the Automatic Lookup

To use an automatic lookup, specify the output fields in your search

```
index=web sourcetype=access* action=purchase productId=*
| stats sum(price) as sales by productId product_name
```

Last 24 hours

i	Time	Event
>	1/9/18 10:56:54.000 PM	203.45.206.135 - - [09/Jan/2018:22:56:54] "POST /cart.do?action=purchase&itemId=EST-19&JSESSIONID=SD5SL5FF10ADF4951 HTTP 1.1" 200 1427 "http://www.buttercupgames.com/cart.do?action=addtocart&itegoryId=STRATEGY&productId=DC-SG-G02" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_7_4) Ap (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5" 314 host = www1 productId = DC-SG-G02 source = /opt/log/www1/access.log sourcetype = acce
>	1/9/18 10:56:08.00	203.45.206.135 - - [09/Jan/2018:22:56:08] "POST /cart.do?action=purchase&itemId=EST-7&JSE art&it AppleW = access_combined

Events Patterns **Statistics (14)** Visualization

20 Per Page Format Preview

productId	product_name	sales
BS-AG-G09	Benign Space Debris	274.89
CU-PG-G06	Curling 2014	319.84
DB-SG-G01	Mediocre Kingdoms	499.80
DC-SG-G02	Dream Crusher	879.78
FI-AG-G08	Orvil the Wolverine	479.88

price	productId	product_name
24.99	DB-SG-G01	Mediocre Kingdoms
39.99	DC-SG-G02	Dream Crusher
24.99	FS-SG-G03	Final Sequel
24.99	WC-SH-G04	World of Cheese
9.99	WC-SH-T02	World of Cheese Tee

Time-based Lookups

- If a field in the lookup table represents a timestamp, you can create a time-based lookup
- In this example, the search retrieved events for December and January and calculated the sales based on the correct unit price for those dates

product_time	productId	product_name	categoryId	price	sale_price
12/1/17	DB-SG-G01	Mediocre Kingdoms	STRATEGY	24.99	19.99
12/1/17	DC-SG-G02	Dream Crusher	STRATEGY	39.99	24.99
12/1/17	FS-SG-G03	Final Sequel	STRATEGY	24.99	16.99
12/1/17	WC-SH-G04	World of Cheese	SHOOTER	24.99	19.99
12/1/17	WC-SH-T02	World of Cheese Tee	TEE	9.99	6.99
12/1/17	PZ-SG-G05	Puppies vs. Zombies	STRATEGY	4.99	1.99
12/1/17	CU-PG-G06	Curling 2014	SPORTS	19.99	16.99
12/1/17	MB-AG-G07	Manganiello Bros.	ARCADE	39.99	24.99
12/1/17	MB-AG-T01	Manganiello Bros. Tee	TEE	9.99	6.99
12/1/17	FI-AG-G08	Orvil the Wolverine	ARCADE	39.99	24.99
12/1/17	BS-AG-G09	Benign Space Debris	ARCADE	24.99	19.99
12/1/17	SC-MG-G10	SIM Cubicle	SIMULATION	19.99	16.99
12/1/17	WC-SH-A01	Holey Blade of Gouda	ACCESSORIES	5.99	2.99
12/1/17	WC-SH-A02	Fire Resistance Suit of Provolone	ACCESSORIES	3.99	1.99
1/1/18	DB-SG-G01	Mediocre Kingdoms	STRATEGY	24.99	19.99
1/1/18	DC-SG-G02	Dream Crusher	STRATEGY	40.99	24.99
1/1/18	FS-SG-G03	Final Sequel	STRATEGY	25.99	16.99
1/1/18	WC-SH-G04	World of Cheese	SHOOTER	24.99	19.99
1/1/18	WC-SH-T02	World of Cheese Tee	TEE	9.99	6.99
1/1/18	PZ-SG-G05	Puppies vs. Zombies	STRATEGY	4.99	1.99
1/1/18	CU-PG-G06	Curling 2014	SPORTS	20.99	16.99
1/1/18	MB-AG-G07	Manganiello Bros.	ARCADE	39.99	24.99
1/1/18	MB-AG-T01	Manganiello Bros. Tee	TEE	9.99	6.99
1/1/18	FI-AG-G08	Orvil the Wolverine	ARCADE	39.99	24.99
1/1/18	BS-AG-G09	Benign Space Debris	ARCADE	25.99	19.99
1/1/18	SC-MG-G10	SIM Cubicle	SIMULATION	19.99	16.99
1/1/18	WC-SH-A01	Holey Blade of Gouda	ACCESSORIES	6.99	2.99
1/1/18	WC-SH-A02	Fire Resistance Suit of Provolone	ACCESSORIES	4.99	1.99

product_name	Month	price	count	sales	SubTotal Sales
Benign Space Debris	Dec	24.99	828	42,211.44	
Benign Space Debris	Jan	25.99	646	32,933.08	
Benign Space Debris Subtotal					150,289.04
Curling 2014	Dec	19.99	868	35,570.64	
Curling 2014	Jan	20.99	620	25,407.60	
Curling 2014 Subtotal					121,956.48
Dream Crusher	Dec	39.99	1,360	110,132.80	
Dream Crusher	Jan	40.99	1,004	81,303.92	
Dream Crusher Subtotal					382,873.44
Final Sequel	Dec	24.99	1,200	61,176.00	
Final Sequel	Jan	25.99	812	41,395.76	
Final Sequel Subtotal					205,143.52