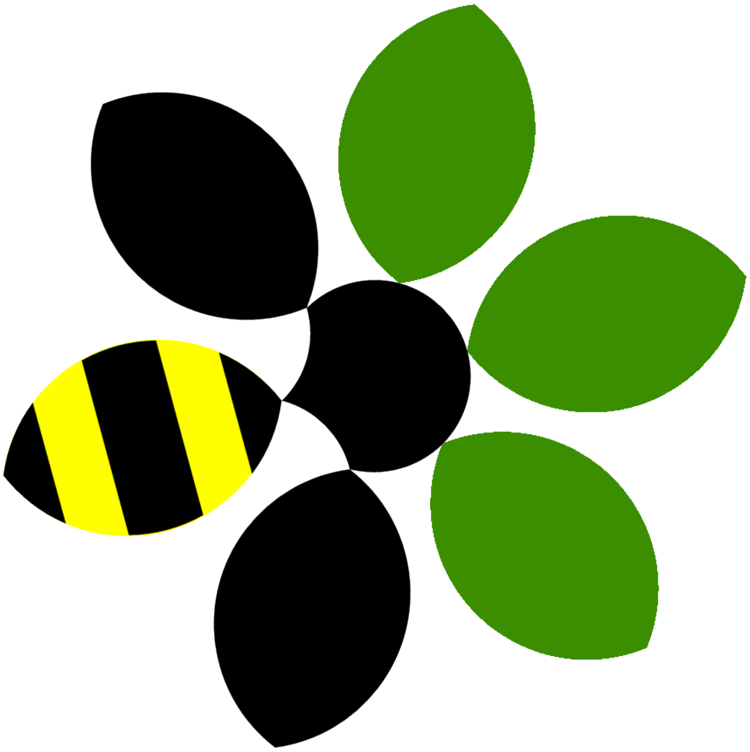
splunk> certification



Certification Demo Preparation Guide: Getting Started with bLeaf

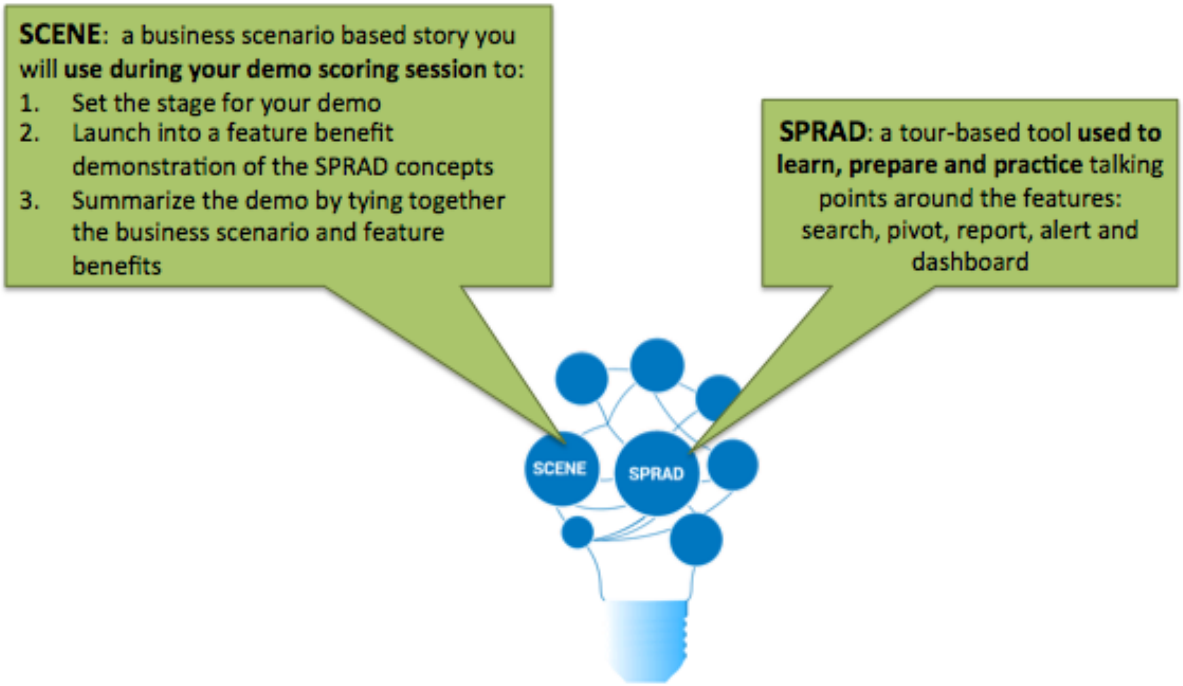
Contents

Getting Started

Introduction

bLeaf is a Splunk App used for the Certification demo. It is used for both **preparation & practice** of your demo AND for **presenting** your demo during your scoring session.

You will use some components of bLeaf to learn, practice and prepare for your demo presentation. You will use other components of bLeaf during your scoring session.



SCENE: a business scenario based story you will **use during your demo scoring session** to:

1. Set the stage for your demo
2. Launch into a feature benefit demonstration of the SPRAD concepts
3. Summarize the demo by tying together the business scenario and feature benefits

SPRAD: a tour-based tool **used to learn, prepare and practice** talking points around the features: search, pivot, report, alert and dashboard

SPRAD Tours: used to learn, practice and prepare key talking points for the Search, Pivot, Report, Alert, and Dashboard features of Splunk. **You will NOT use this portion during your demo presentation**. This is for **learning** and **preparation** only.

SCENE: used during your certification scoring session to introduce the demo scenario and data. Practice using SCENE to: introduce your demo, go into a live demo environment to showcase the SPRAD features, and summarize with the final Scene.

Installation

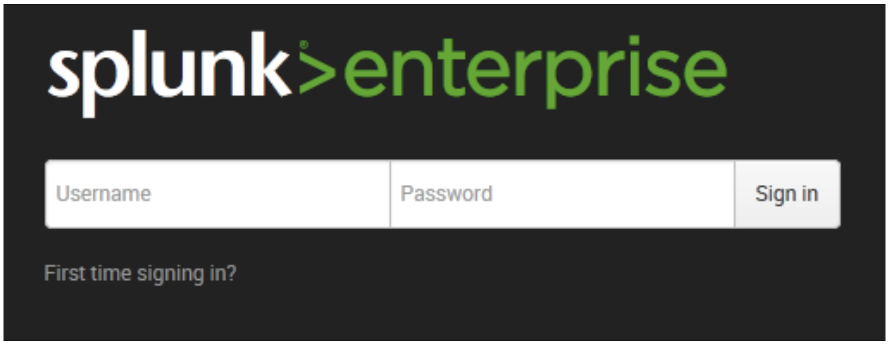
NOTE: You must be running Splunk 6.3 or greater.

Download bLeaf Splunk App.

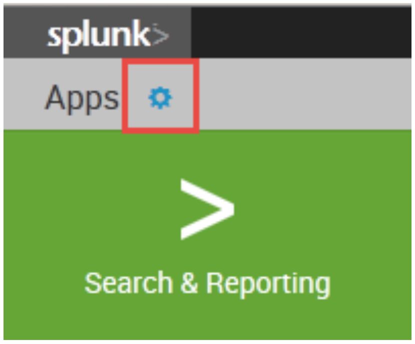
1. Download the bLeaf Splunk App from the enablement portal link.

Install the bLeaf Splunk App using the Splunk User Interface

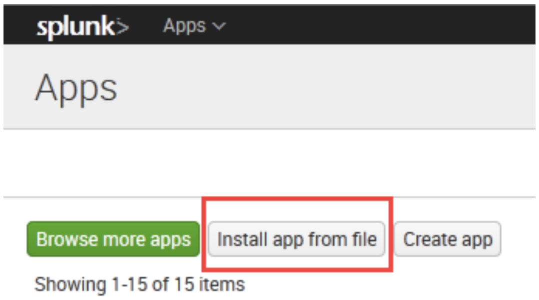
2. Login into the Splunk User Interface



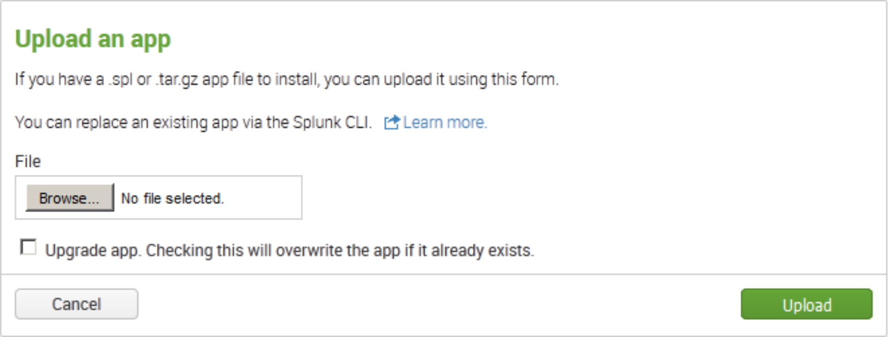
3. Click on the Apps button on the top left corner of the screen.



4. Click on Install app from a file



5. Browse to the location of the bleaf.spl file and open it



Upload an app

If you have a .spl or .tar.gz app file to install, you can upload it using this form.

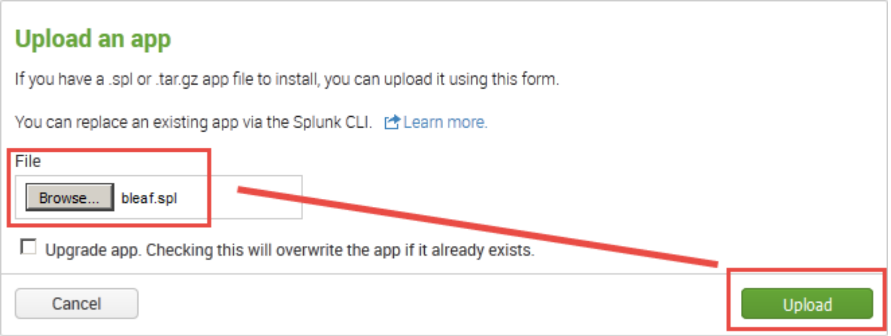
You can replace an existing app via the Splunk CLI. Learn more.

File

Browse... No file selected.

□ Upgrade app. Checking this will overwrite the app if it already exists.

6. To begin the installation process click on the Upload button



Upload an app

If you have a .spl or .tar.gz app file to install, you can upload it using this form.

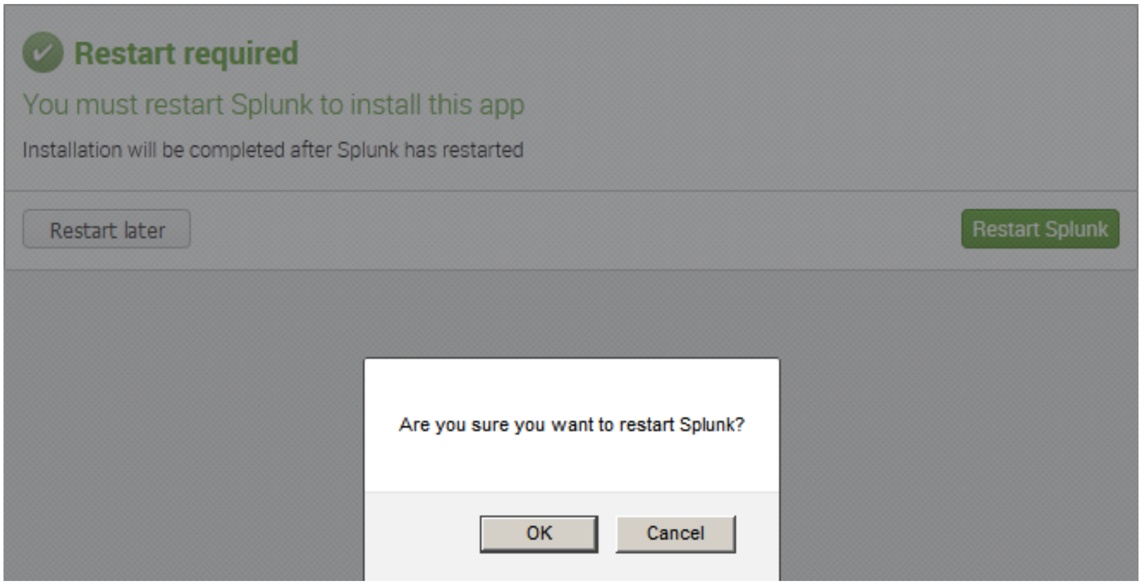
You can replace an existing app via the Splunk CLI. Learn more.

File

Browse... bleaf.spl

□ Upgrade app. Checking this will overwrite the app if it already exists.

7. The bLeaf Splunk App will require to re-start your Splunk instance. Click on the Restart Splunk button and choose OK to continue.



Restart required

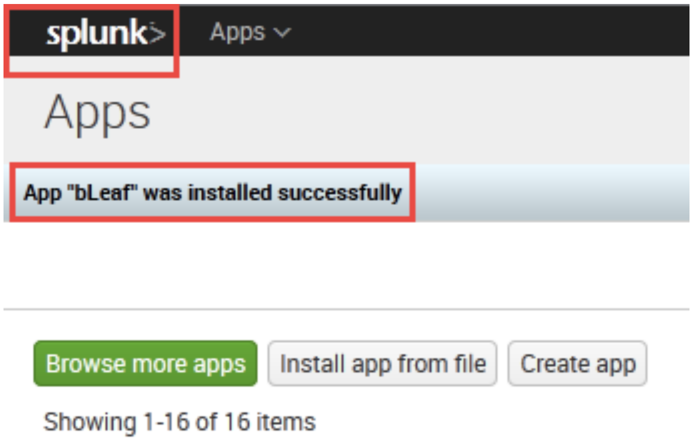
You must restart Splunk to install this app

Installation will be completed after Splunk has restarted

Are you sure you want to restart Splunk?

8. Once your Splunk instance is back up and running you will need to login again.

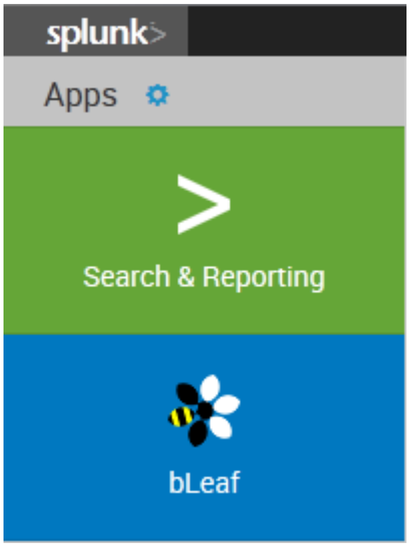
9. If you are in the Apps menu page, you should see a confirmation that application had been successfully installed. Click on the Splunk logo on the top left corner to return to the home page.



App "bLeaf" was installed successfully

Showing 1-16 of 16 items

10. Now you can click on the bLeaf Splunk App icon to start your journey.



Install the bLeaf Splunk App using a command line terminal interface.

1. In this scenario we are installing the application while remotely logged into a Linux server.
2. If configured, you can check for the location of the splunk command.

```
echo $SPLUNK_HOME
/opt/splunk
```

3. In this instance we are using the default location under /opt/splunk/bin.
4. For this installation to work we need Splunk to be up and running.

```
/opt/splunk/bin/splunk status
```

```
splunkd is running (PID: 2803).
splunk helpers are running (PIDs: 2804 2812 2915 2961).
```

5. If your Splunk instance is not running, please use the following command to start it.

```
/opt/splunk/bin/splunk start
```

6. Next we check on the list of installed applications.

```
/opt/splunk/bin/splunk list app
```

7. Please note that you may need to authenticate as a user with enough privileges to accomplish the task.

```
Your session is invalid.  Please login.
Splunk username: admin
Password:
alert_webhook                 CONFIGURED          ENABLED             INVISIBLE
appsbrowser                   CONFIGURED          ENABLED             VISIBLE
framework                     UNCONFIGURED        ENABLED             INVISIBLE
gettingstarted                CONFIGURED          DISABLED            VISIBLE
introspection_generator_addon CONFIGURED          ENABLED             INVISIBLE
launcher                      CONFIGURED          ENABLED             VISIBLE
learned                       UNCONFIGURED        ENABLED             INVISIBLE
legacy                        UNCONFIGURED        DISABLED            INVISIBLE
sample_app                    UNCONFIGURED        DISABLED            INVISIBLE
search                        CONFIGURED          ENABLED             VISIBLE
splunk_archiver               CONFIGURED          ENABLED             INVISIBLE
splunk_httpinput              UNCONFIGURED        ENABLED             INVISIBLE
splunk_management_console     UNCONFIGURED        ENABLED             VISIBLE
SplunkForwarder               UNCONFIGURED        DISABLED            INVISIBLE
SplunkLightForwarder          UNCONFIGURED        DISABLED            INVISIBLE
```

8. If the bleaf app is already installed, use the following command to remove it before moving on to the next step.

```
/opt/splunk/bin/splunk remove app
```

9. Locate the SPL file copied to the local server

```
pwd
/root
cd Downloads/
```

```
ls -l
total 1040
-rw-------. 1 root root 1064701 Oct 19 11:51 bleaf.spl
```

10. Install the bleaf.spl app using the following command.

```
bLeaf: /opt/splunk/bin/splunk install app /root/Downloads/bleaf.spl
App '/root/Downloads/bleaf.spl' installed
You need to restart the Splunk Server (splunkd) for your changes to take effect.
```

11. Restart your Splunk instance

```
/opt/splunk/bin/splunk restart
Stopping splunkd...
Shutting down.  Please wait, as this may take a few minutes.
...                                                        [  OK  ]
Stopping splunk helpers...
[  OK  ]
Done.

Splunk> See your world.  Maybe wish you hadn't.

Checking prerequisites...
Checking http port [8000]: open
Checking mgmt port [8089]: open
Checking appserver port [127.0.0.1:8065]: open
Checking kvstore port [8191]: open
Checking configuration...  Done.
Checking critical directories...        Done
Checking indexes...
Validated: _audit _internal _introspection _thefishbucket history main summary
Done
Checking filesystem compatibility...  Done
Checking conf files for problems...
Done
Checking default conf files for edits...
Validating installed files against hashes from '/opt/splunk/splunk-6.3.0-aa7d4b1ccb80-
linux-2.6-x86_64-manifest'
File 'etc/system/default/web.conf' changed or missing.
Problems were found, please review your files and move customizations to local
All preliminary checks passed.

Starting splunk server daemon (splunkd)...
Done
[  OK  ]

Waiting for web server at http://127.0.0.1:8000 to be available. Done


If you get stuck, we're here to help.
Look for answers here: http://docs.splunk.com
```

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

12. Confirm that your new bleaf application is installed:

```
/opt/splunk/bin/splunk list app
Your session is invalid.  Please login.
Splunk username: admin
Password:
alert_webhook                 CONFIGURED          ENABLED             INVISIBLE
appsbrowser                   CONFIGURED          ENABLED             VISIBLE
bleaf                         UNCONFIGURED        ENABLED             VISIBLE
framework                     UNCONFIGURED        ENABLED             INVISIBLE
gettingstarted                CONFIGURED          DISABLED            VISIBLE
introspection_generator_addon CONFIGURED          ENABLED             INVISIBLE
launcher                      CONFIGURED          ENABLED             VISIBLE
learned                       UNCONFIGURED        ENABLED             INVISIBLE
legacy                        UNCONFIGURED        DISABLED            INVISIBLE
sample_app                    UNCONFIGURED        DISABLED            INVISIBLE
search                        CONFIGURED          ENABLED             VISIBLE
splunk_archiver               CONFIGURED          ENABLED             INVISIBLE
splunk_httpinput              UNCONFIGURED        ENABLED             INVISIBLE
splunk_management_console     UNCONFIGURED        ENABLED             VISIBLE
SplunkForwarder               UNCONFIGURED        DISABLED            INVISIBLE
SplunkLightForwarder          UNCONFIGURED        DISABLED            INVISIBLE
```

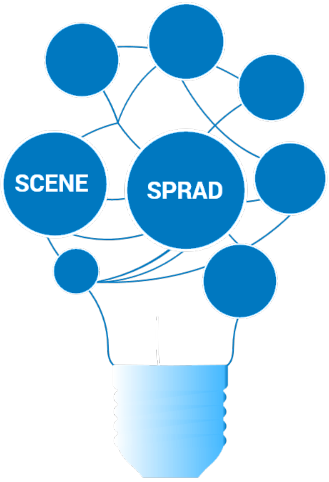
13. Once your Splunk instance is back up and running you will need to login again.
14. If you are in the Apps menu page, you should see a confirmation that application had been successfully installed. Click on the Splunk logo on the top left corner to return to the home page.
15. Now you can click on the bLeaf Splunk App icon to start your journey.

Using SPRAD for Learning & Preparation

The SPRAD button provides a tour of Splunk Enterprise features and benefits. The acronym stands for Search, Pivot, Reports, Alerts and Dashboards. The intent of this feature tour is to help you prepare for your demo scoring session. It will teach you how to highlight the benefits of the key technology features that make Splunk Enterprise easy to use with fast time to value.

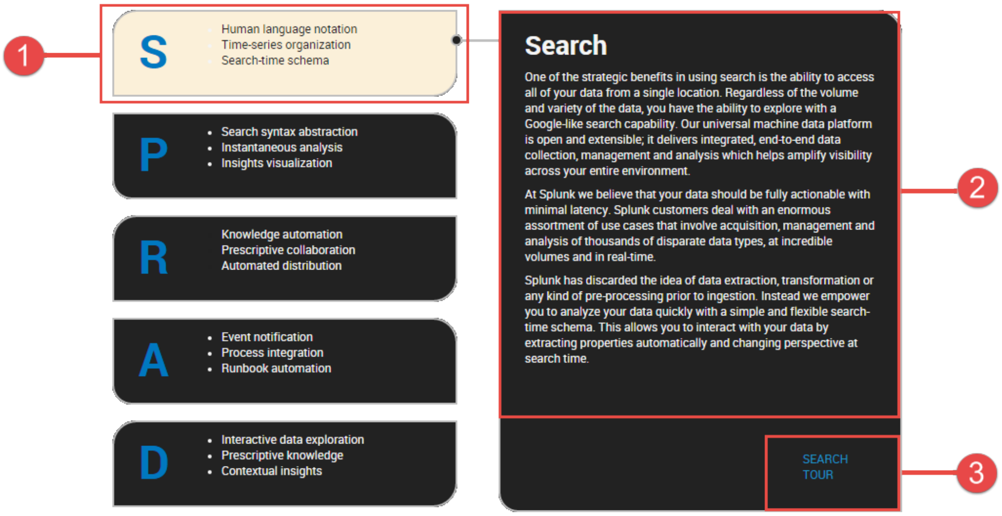
You will be learning the basic terminology and feature benefits of Splunk with this tour.

This section should take you about fifteen to twenty minutes to complete.



Click on the SPRAD button.

When you use the SPRAD tour, you will begin with this screen:



S
Human language notation
Time-series organization
Search-time schema

P
- Search syntax abstraction
- Instantaneous analysis
- Insights visualization

R
Knowledge automation
Prescriptive collaboration
Automated distribution

A
- Event notification
- Process integration
- Runbook automation

D
- Interactive data exploration
- Prescriptive knowledge
- Contextual insights

Search

One of the strategic benefits in using search is the ability to access all of your data from a single location. Regardless of the volume and variety of the data, you have the ability to explore with a Google-like search capability. Our universal machine data platform is open and extensible; it delivers integrated, end-to-end data collection, management and analysis which helps amplify visibility across your entire environment.

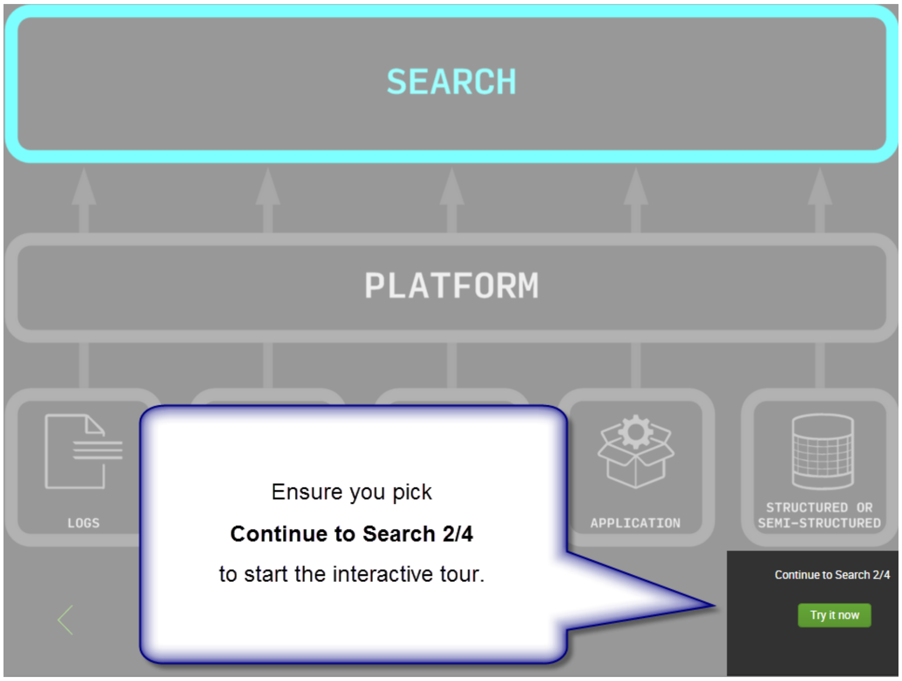
At Splunk we believe that your data should be fully actionable with minimal latency. Splunk customers deal with an enormous assortment of use cases that involve acquisition, management and analysis of thousands of disparate data types, at incredible volumes and in real-time.

Splunk has discarded the idea of data extraction, transformation or any kind of pre-processing prior to ingestion. Instead we empower you to analyze your data quickly with a simple and flexible search-time schema. This allows you to interact with your data by extracting properties automatically and changing perspective at search time.

1. Use the boxes to the left in order to pick the desired tour for your practice round.

2. When you choose a topic, you are given a synopsis of the key highlights for the feature and the benefits associated with it.
3. You may choose to follow the interactive tour.

Please note: The position of the "Try it now" button may confuse you during your initial trial runs. For example, to ensure you progress to the interactive tour, **click the "Continue to Search 2/4"** link above the "Try it now" button.



Ensure you pick

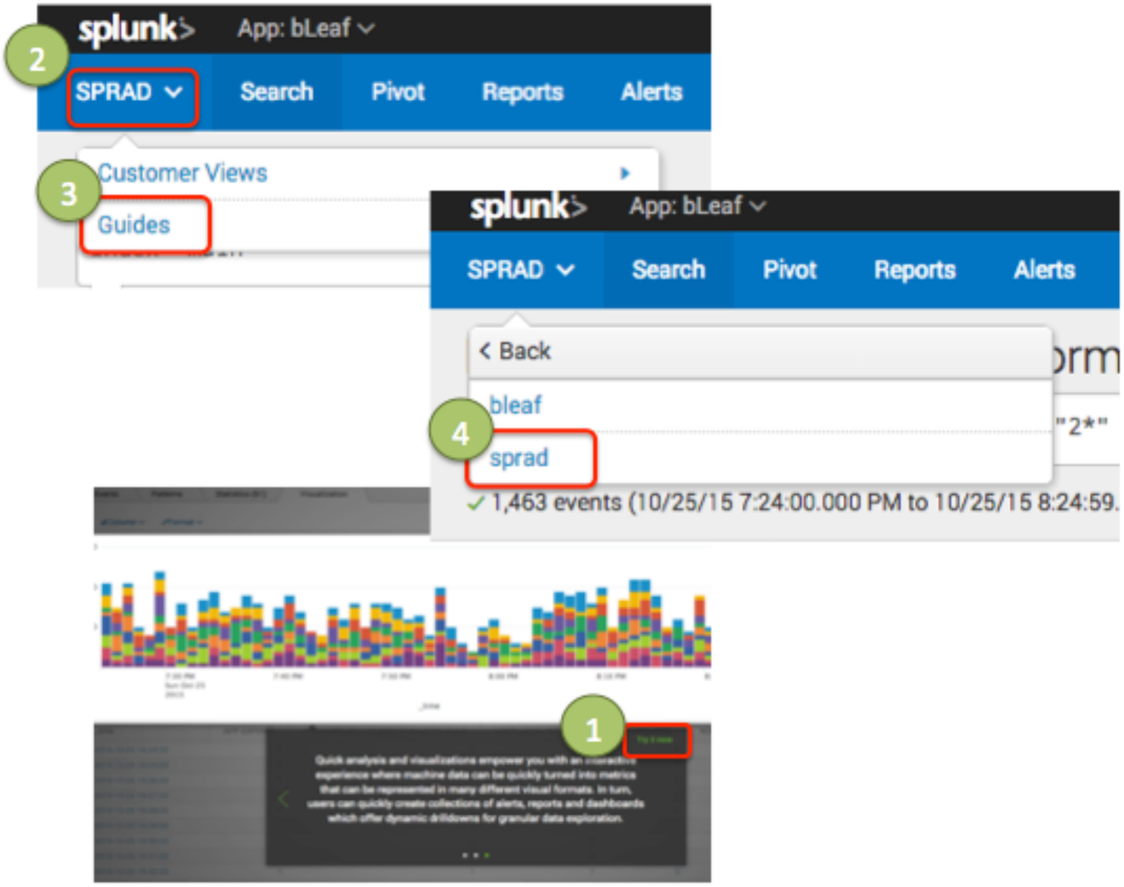
Continue to Search 2/4

to start the interactive tour.

Once you are in the interactive tour, the best way to progress through each stage is to use the right arrow on your keyboard. By doing so, at the end of a given tour you will return to the SPRAD main page.

Of course, you can also click on the green arrow in each dialogue box presented on the screen. In this case, when you reach the last page of a tour, and there isn't a green arrow to click, either press the right arrow on your keyboard, or.:

1. Click **Try it now**. This exits the tour.
2. Click **SPRAD** in the upper left corner.
3. Click **Guides**.
4. Click **sprad**. This returns you to the SPRAD page.
5. Continue to the next tour.



✓ 1,463 events (10/25/15 7:24:00.000 PM to 10/25/15 8:24:59.

Quick analysis and visualizations empower you with an interactive experience where machine data can be quickly turned into metrics that can be represented in many different visual formats. In turn, users can quickly create collections of alerts, reports and dashboards which offer dynamic drilldowns for granular data exploration.

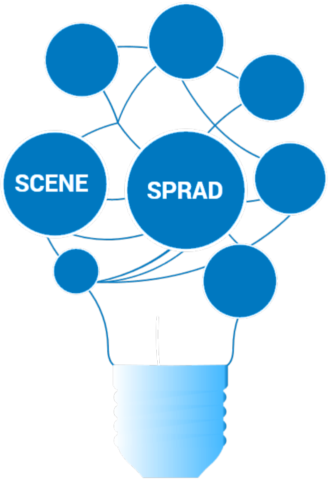
If you want to get back to the start of the SPRAD tour or the SCENE play, please exit the interactive tour and click on the bLeaf logo – located at the top right corner of your bLeaf App.

Using SCENE

After learning and practicing the SPRAD feature benefits, you will use SCENE. This is a scenario-based demonstration that is presented in a simple three-stage play. The idea is to:

1. Introduce a use case in which a user is experiencing difficulty in achieving a business objective.
2. Through the exploration of data, the user finds a potential issue with an application system.
3. Finally, by drilling down right into the data, the user is able to ascertain the reason for the concern.

Be sure to practice how you will balance your allocated time to each of the topics so that you cover them all.

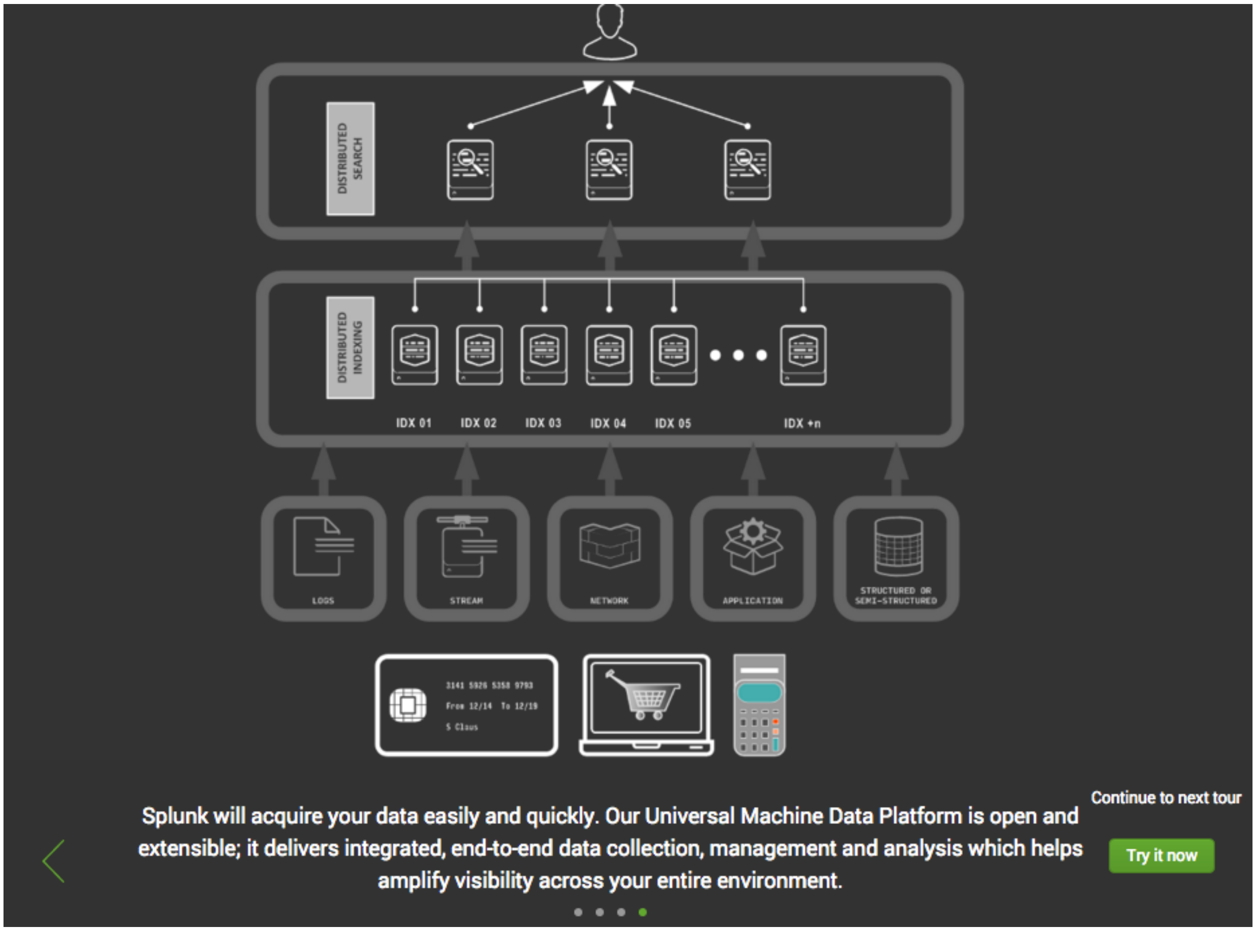


```
Click on the SCENE button.
```

1. Introduce a use case in which a user is experiencing difficulty in achieving a business objective.

The first part of the tour consists of 4 slides to help you introduce the demo scenario to the audience. During this part of the presentation you should relate the scenario to the customer. You should set the stage that you are now going to show them some of the feature benefits of Splunk, and then you will return to the business problem at hand to bring it all together.

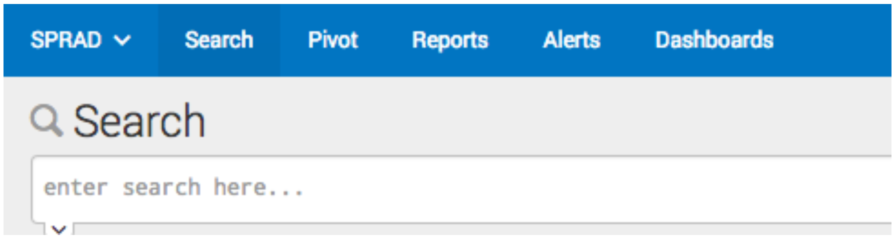
Once you are in the interactive tour, the best way to progress through each stage is to use the right arrow on your keyboard. Of course, you can also click on the green arrow in each dialogue box presented on the screen.



Splunk will acquire your data easily and quickly. Our Universal Machine Data Platform is open and extensible; it delivers integrated, end-to-end data collection, management and analysis which helps amplify visibility across your entire environment.

2. Through the exploration of data, the user finds a potential issue with an application system.

When you reach the last page of the introduction (shown above), click the Try it now button to enter the live demonstration environment. You should highlight the SPRAD components learned earlier while making it relevant to your customer. Be sure to ask questions so you know which parts of which features to highlight. You may use the menus at that top to help you navigate through the features.



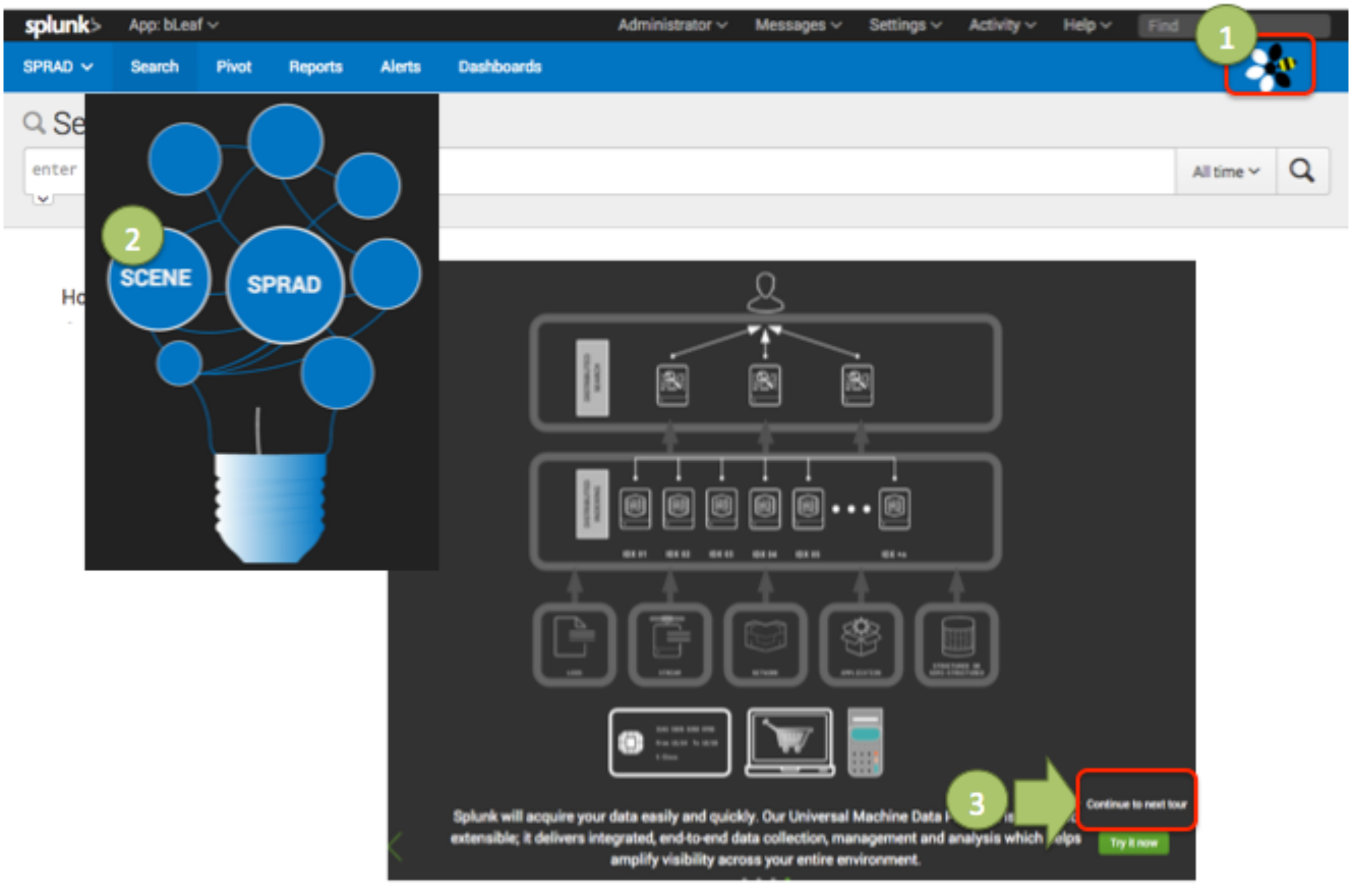
3. Finally, by drilling down right into the data, the user is able to ascertain the reason for the concern.

When you are ready to tie it back to the business problem:

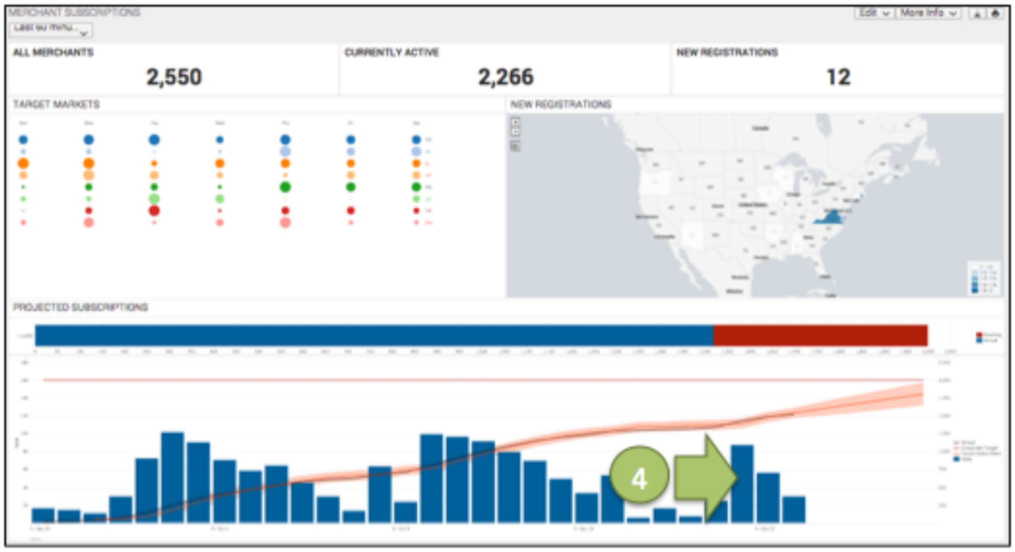
1. Click the **bee** in the upper right corner to return to the main SCENE/SPRAD Page.
2. Select **SCENE**.
3. Scroll through the introduction slides quickly to remind the audience of the business scenario.

This time, on the last slide, click **Continue to next tour**.
The MERCHANT SUBSCRIPTIONS dashboard displays.
Use the interactivity of the MERCHANT SUBSCRIPTIONS dashboard to explore the data. Be sure to watch the sample demo video for an example of how to tell this story. For example, here is a series of clicks to use:

4. From the MERCHANT SUBSCRIPTIONS dashboard, click a bar in the PROJECTED SUBSCRIPTIONS panel. This displays the TRANSACTION CONVERSION dashboard.
5. From the TRANSACTION CONVERSION dashboard, click a red bar in the TOP 10 SYSTEM ERRORS panel. This displays the SYSTEMS ERRORS INVESTIGATION dashboard.
6. From the SYSTEMS ERRORS INVESTIGATION dashboard, click a red bar in the TOP 10 SYSTEM ERRORS to display the SYSTEM ERRORS BY REGION map.
7. From the SYSTEM ERRORS BY REGION map, click a state to display the related raw events and chart.



Splunk will acquire your data easily and quickly. Our Universal Machine Data P is extensible; it delivers integrated, end-to-end data collection, management and analysis which elps amplify visibility across your entire environment.



MERCHANT SUBSCRIPTIONS

ALL MERCHANTS 2,550

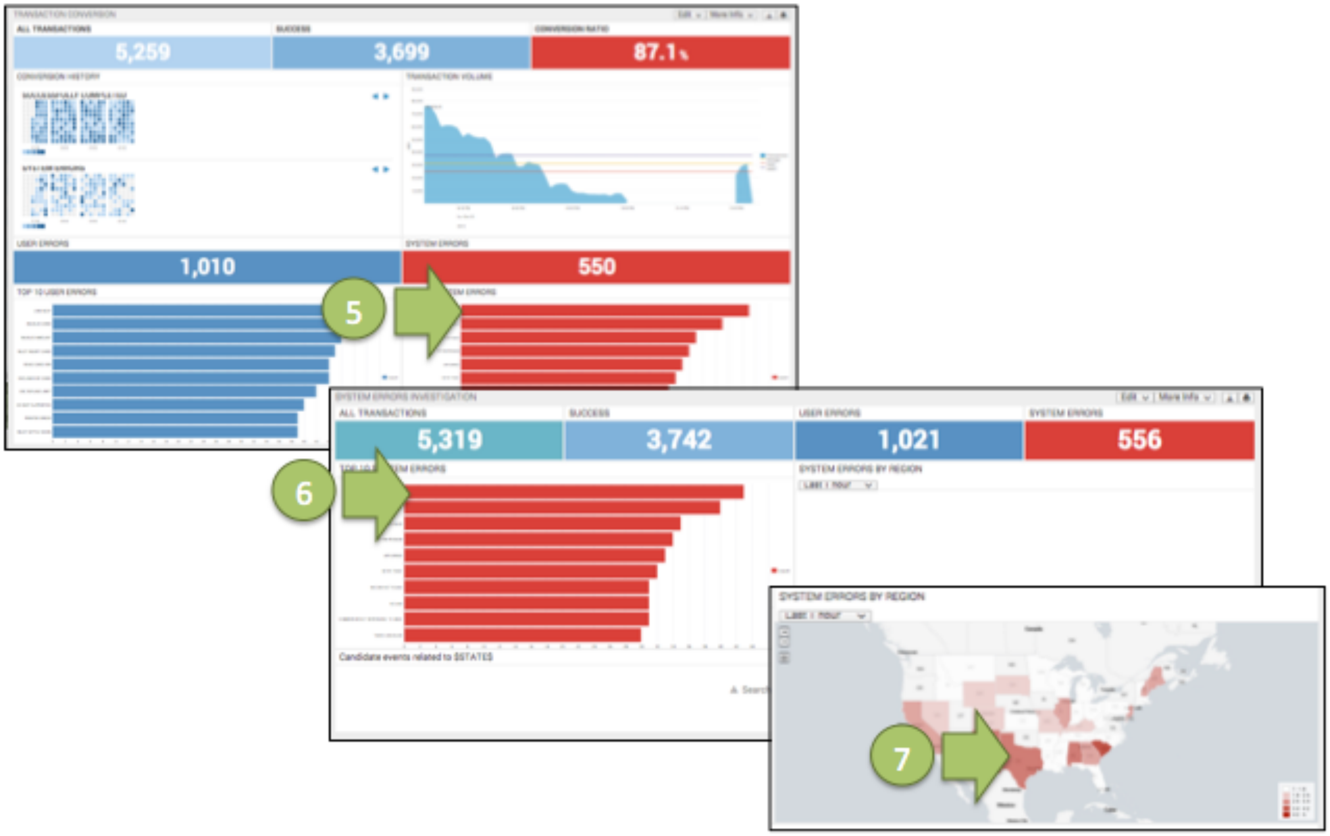
CURRENTLY ACTIVE 2,266

NEW REGISTRATIONS 12

TARGET MARKETS

NEW REGISTRATIONS

PROJECTED SUBSCRIPTIONS



TRANSACTION CONVERSION

ALL TRANSACTIONS 5,259

SUCCESS 3,699

CONVERSION RATIO 87.1%

CONVERSION HISTORY

TRANSACTION VOLUME

USER ERRORS 1,010

SYSTEM ERRORS 550

TOP 10 USER ERRORS

SYSTEM ERRORS INVESTIGATION

ALL TRANSACTIONS 5,319

SUCCESS 3,742

USER ERRORS 1,021

SYSTEM ERRORS 556

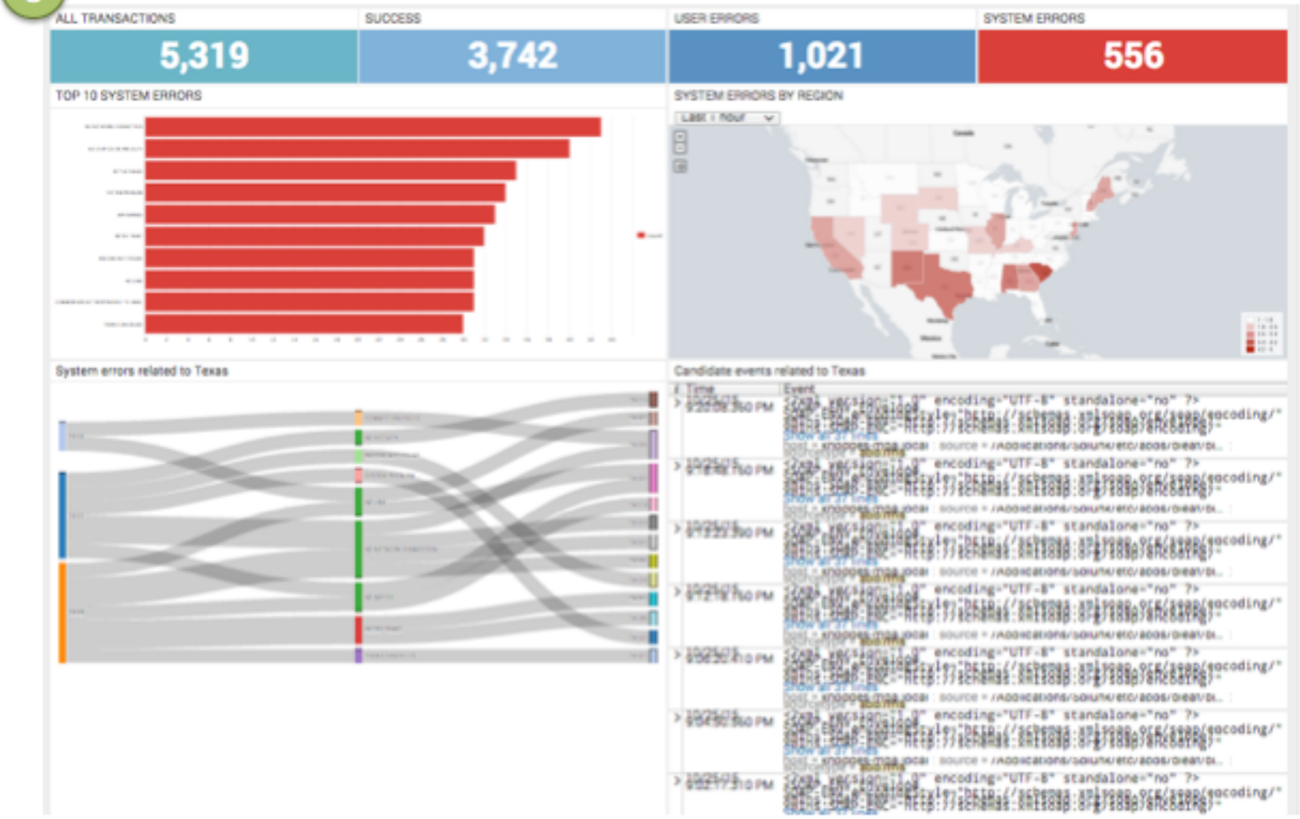
SYSTEM ERRORS BY REGION

Candidate events related to $STATE$

SYSTEM ERRORS BY REGION

Last 1 hour

8


ALL TRANSACTIONS
5,319
SUCCESS
3,742
USER ERRORS
1,021
SYSTEM ERRORS
556
TOP 10 SYSTEM ERRORS
SYSTEM ERRORS BY REGION
Last 1 hour
System errors related to Texas
Candidate events related to Texas
Time
Event