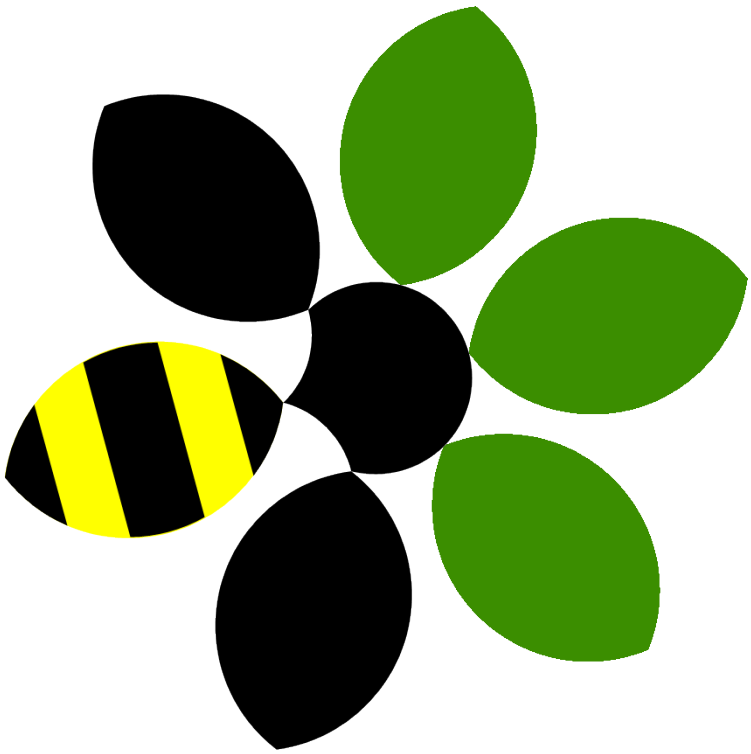
splunk> certification



Certification Demo Microscript Guide: bLeaf Microscripts

Contents

splunk>certification

Introduction

Welcome to bLeaf. This demonstration is organized in two sections:

1. SPRAD — This is a tour-based product demonstration of Splunk Enterprise. The acronym stands for Search, Pivot, Reports, Alerts and Dashboards. The intent of this demonstration is to quickly highlight the benefits of the key technology features that make Splunk Enterprise easy to use and quick to value.

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

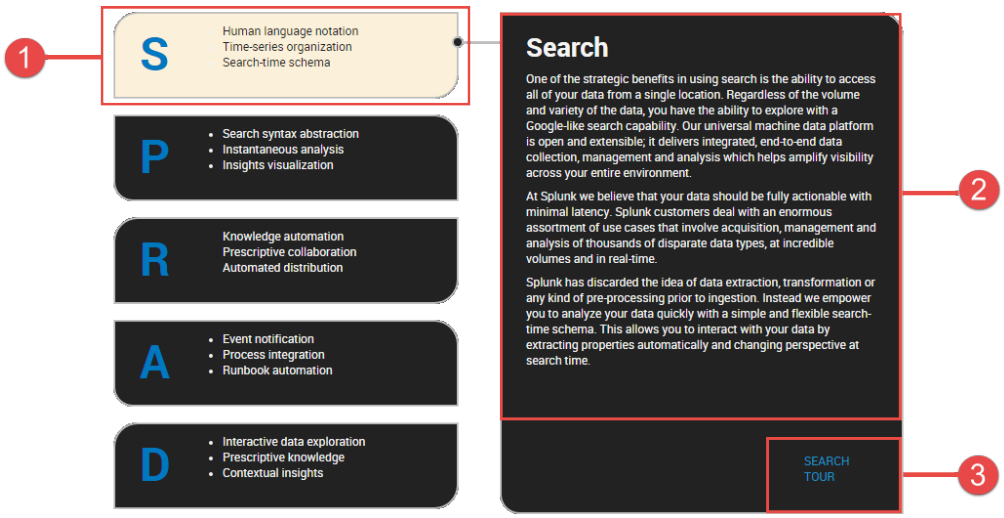
2. SCENE — This is a scenario-based demonstration that is presented in a simple three-stage play. The idea is to introduce a use case in which a user is experiencing difficulty in achieving a business objective. Through the exploration of data, the user finds a potential issue with an application system. Finally, by drilling down right into the data, the user is able to ascertain the reason for the concern.

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

SPRAD

You can deliver the SPRAD demonstration using the tour included in the bLeaf application. Ideally you will be learning the basic terminology and approach using the tour, while delivering the demonstration with a hands-free approach.

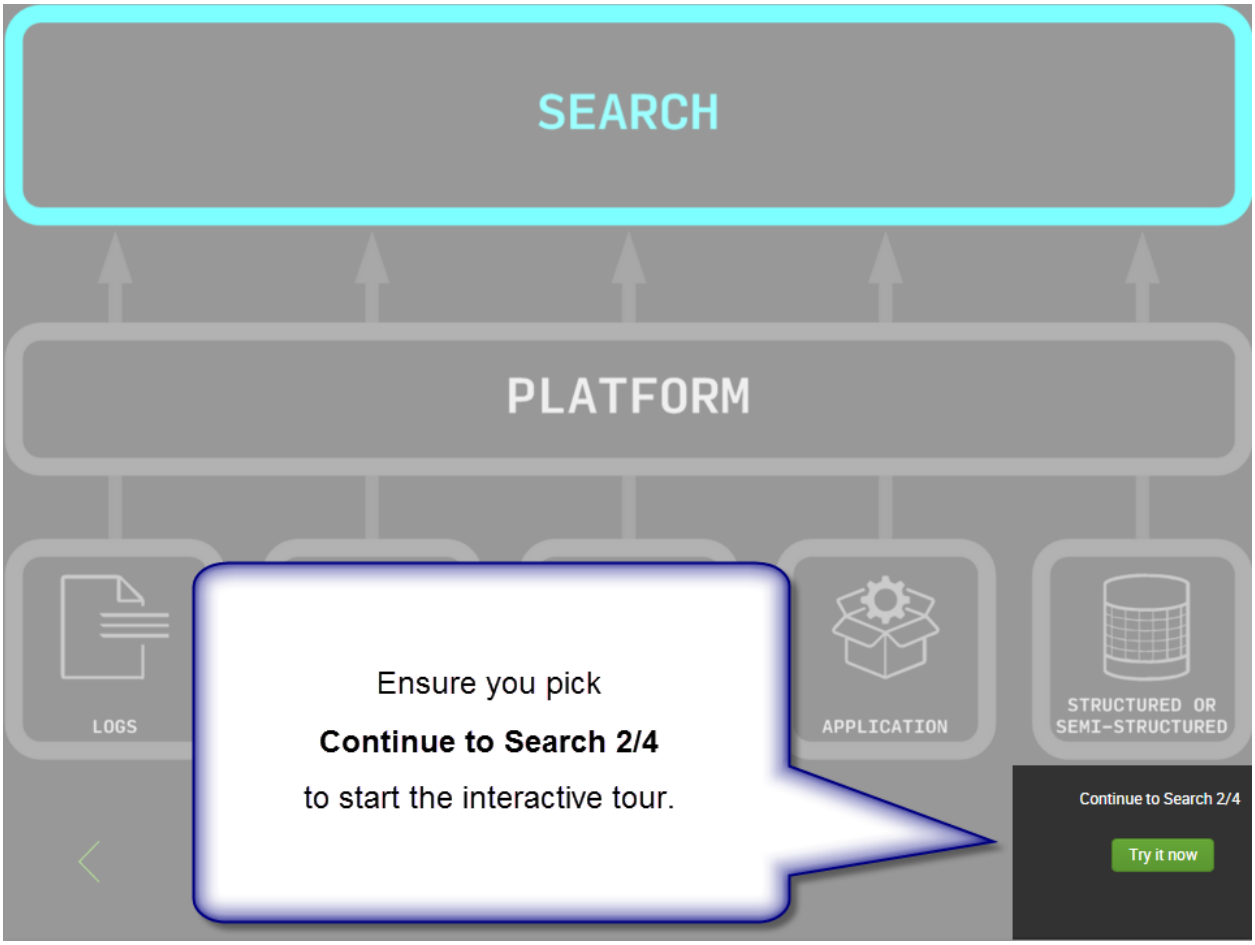
When you use the SPRAD tour, you will begin with this screen:



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.



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. You should always end up back in the SPRAD main page at the end of each interactive tour.

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.

Search

Introduction

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.

Highlights

- Universal machine data platform
- Real-time architecture
- Schema on the fly

Narrative

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.

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.

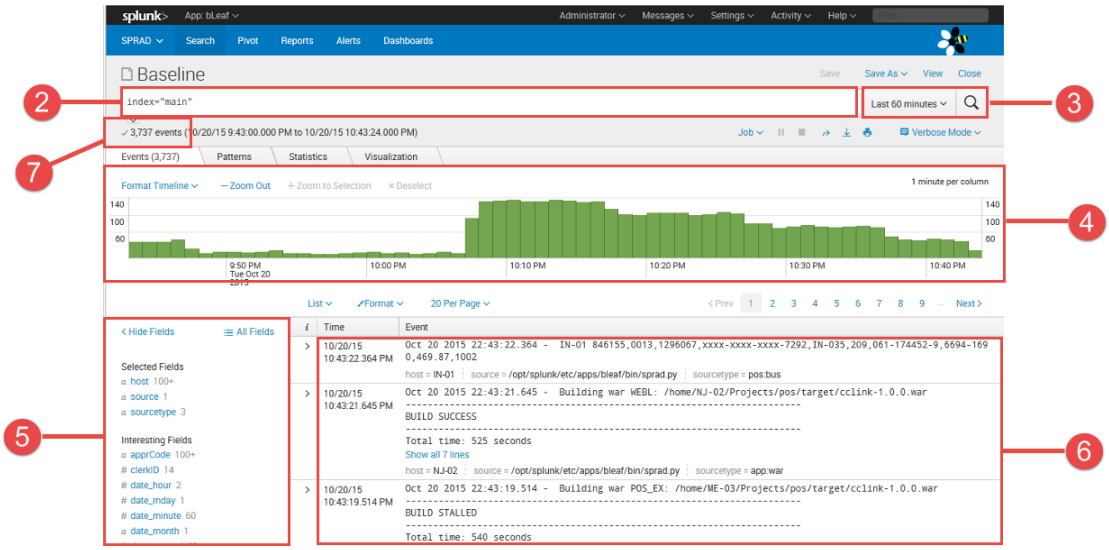
Splunk empowers you to analyze your data quickly with a simple and flexible search-time schema. Splunk has discarded the idea of data extraction, transformation or any kind of pre-processing prior to ingestion. Schema-on-the-fly allows you to interact with your data by extracting properties automatically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

Micro scenarios

```
Click Search menu item.
Enter the search syntax index="main" in the search bar.
Choose the Last 60 minutes in the time picker.
```

1. Search benefit

   The advantage of searching your data with Splunk is in the flexibility to explore, discover and establish knowledge that will help you make business decisions quickly and effectively. You do this by consolidating access to all your data with a Web browser and a Google-style search bar, or by taking advantage of our RESTful API to access the data through your own portal application.



2. Google-like search

   To start with your search experience, imagine that you are part of a team that is investigating a technology problem that has a definitive business impact. From an operational perspective you will be able use search criteria with details that are relevant to that investigation within seconds. In the olden days you would have to visit various teams, databases, applications in order to combine all of the data to create a single point of view.

3. Time-series search

   In your data exploration, it will be very clear that Splunk organizes your data in a time-series format. This is done on purpose so that you can follow a familiar pattern for discovery. For example, you may not know why your CRM application had unscheduled downtime last Tuesday. However, you do know the approximate time of the occurrence. Hence you can begin by searching for all systemic data derived from the servers, network devices and applications that make up your CRM application, at that specific time period.

4. Proportional histogram

   Exploring your data using time as a reference allows you to focus your efforts without need for specific details. Once you have results, you will be able to determine pattern behavior based on the volume of data acquisition. Simply put: you will be able to see and isolate peaks and valleys, which determine uncharacteristic systemic behavior across your environment.

5. Schema on the fly benefits

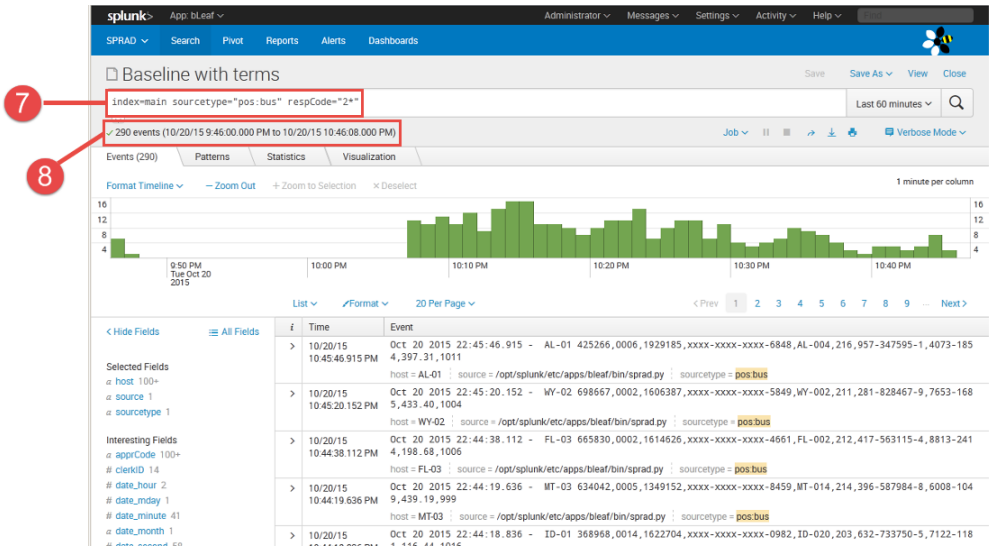
   The search experience empowers you to analyze your data quickly with a simple and flexible search-time schema. This allows you to interact with your data by extracting properties automatically and changing perspective on demand. In the end you are able to focus primarily in

obtaining answers, dealing with relevant problems in your operational landscape and doing it all quickly. The upshot benefit is the cost avoidance related to specialized skills engaged to execute outdated data extraction and transformation techniques.

6. Data results

When your search is active or completed, your data is presented in a reverse-time order. That means the last events are visible first and you are now effectively equipped with a time machine –a way to go back in time to examine the record of behavior left as evidence by your various sources of data. What is even better is the fact that you can search you data manually or through automated ways, using a predetermined window of time or in real-time.

Update the search syntax to index="main" sourcetype="pos:bus" respCode="2*" in the search bar.



7. Number of events

Pay careful attention to the number of events that match your search criteria. Let's explore a more granular way to add more precision to your results by adding more specific terms.

8. Human language notation

The precision and presentation of the search results depends the depth of the criteria used in your exploration. To enhance the precision of your search results, Splunk combines human language keywords and properties obtained from your data. This allows you to interact with your data by reducing massive data sets within minutes and changing perspective on demand, when you search.

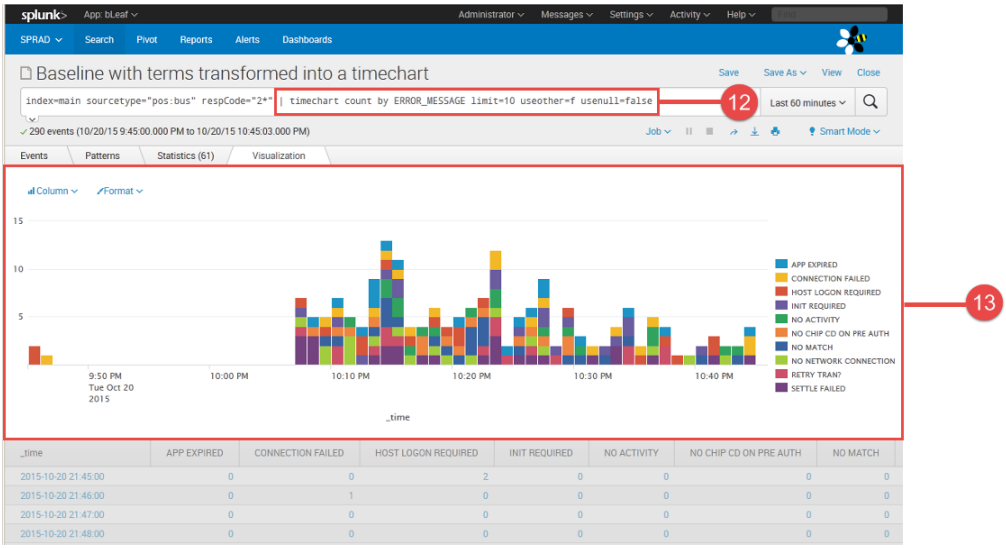
9. Simple criteria

   The type of expertise used to search varies from simple human words to extensive transformative language options for data analysis. For instance, an operations manager may only need to understand human semantics such as “error” or “fail” in order to paint a dashboard panel; a technical data analyst, on the other end of the spectrum, may want to take advantage of the extensive search syntax options in order to transform and align the data to meet a specific type of complex, repetitive analysis.

10. Data reduction

    Pay careful attention to the number of events that match your revised search criteria. Data reduction and granular analysis are key benefits.

Update the search syntax to `index="main" sourcetype="pos:bus" respCode="2*" | timechart count by ERROR_MESSAGE` in the search bar.



11. Presentation benefits

    Your basic search experience is completed with the transformation of your data from a pure, raw text format to an interactive visualization. The Splunk user interface provides a vast collection of graphic options to display your analysis in a collaborative fashion. More importantly, with the Splunk web framework you can extend the presentation of your search and analysis to include third-party graphic libraries.

12. Search syntax richness

The Splunk search language allows you to transform your data for presentation without affecting its original state. In this case the timechart command will count the representing values for a data property and organize the count in proportional time periods that fit your search window. Of course you can change your mind and use a different time period, a specific point in time, or a real-time window.

13. Transformation

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

Pivot

Introduction

Pivot is to search what a spreadsheet is to a calculator. You can achieve very significant results with a calculator as long as you are able to invest the time with calculations and figures on your own. Search is a tool that allows you to reconcile data exploration with a learning opportunity. A spreadsheet will allow you to achieve repeatable results faster because you can automate the calculations once you are able enter the figures once. Pivot is an acceleration tool that allows you to explore and obtain results faster in a mode that is most familiar for most business users.

Highlights

- Search syntax abstraction
- Point-and-click data analysis
- Insights through visualizations

Narrative

Pivot is to search what a spreadsheet is to a calculator. You can achieve very significant results with a calculator as long as you are able to invest the time with calculations and figures on your own. A spreadsheet will allow you to achieve results faster because you can automate the calculations once you are able enter the figures once.

With Pivot we focus on the use of the data. The search syntax is still part of the process; however, the search language is abstracted onto the background so the end users can achieve results with a point-and-click journey. The main requirement to use Pivot is the pre-arrangement of the data properties onto useful data collections for the end users.

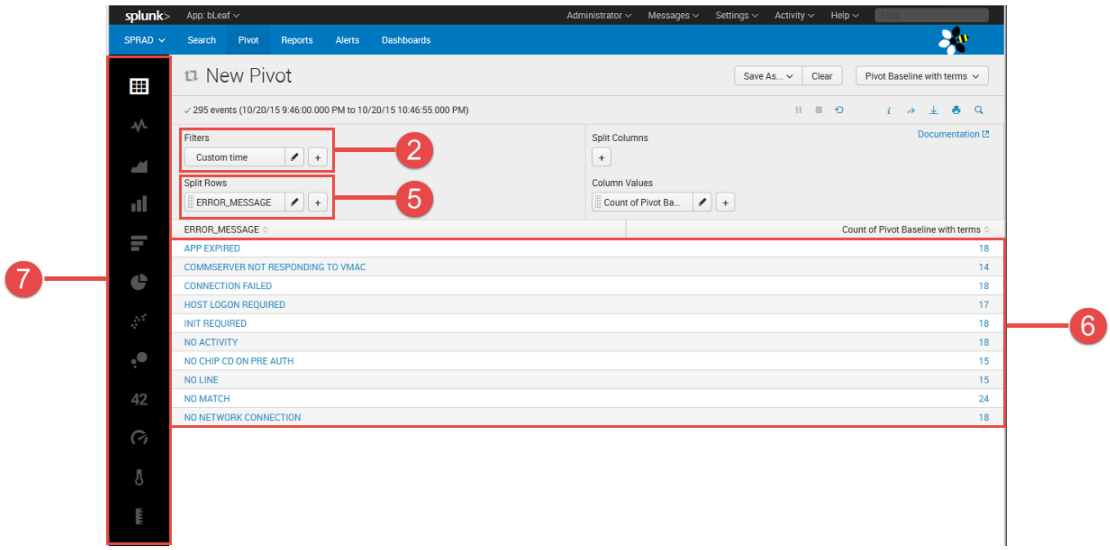
The experience with Pivot is visual and it requires a short learning experience.

Micro scenarios

```
Click Pivot menu item.
Pick the Pivot Baseline with terms knowledge object.
```

1. Pivot benefit

   Pivot allows for the interaction with data without the need of active exploration of the raw data. It relies on data recipes organized in data models. The key advantage is the instantaneous analysis of the data.



2. Time series constant

   The data exploration experience starts with the determination of the time period applicable to the use case. Splunk organizes your data in a time-series format. This is done on purpose so that you can follow a familiar pattern for discovery. For example, you may not know why your CRM application had unscheduled downtime last Tuesday. However, you do know the approximate time of the occurrence. Hence you can begin by searching for all systemic data derived from the servers, network devices and applications that make up your CRM application, at that specific time period.

Choose the Last 60 minutes in the time picker.

3. Point-and-click exploration

   Pivot will allow you to organize the data results into logical groupings based on your specific criteria. Your advantage here is quick realization of results while abstracting the search syntax. With Pivot the learning curve is shortened exponentially.

4. Instantaneous analysis

   To start with your search experience with Pivot, imagine that you are part of a team that is investigating a technology problem that has a definitive business impact. From an operational perspective you will be able use search criteria with details that are relevant to that investigation within seconds. In the olden days you would have to visit various teams, databases, applications in order to combine all of the data to create a single point of view.

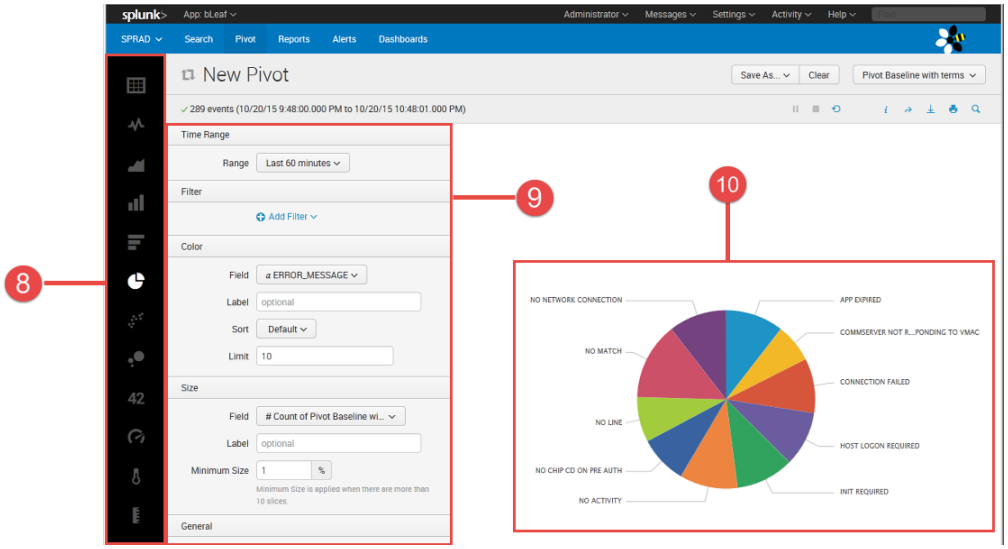
Pick the ERROR_MESSAGE field in the attribute picker.

5. You choose the criteria

   The best way to use Pivot is exploring the relationship of “error OR fail terms in relationship to an arbitrary field in your data model. In this scenario you are provided with all of the available data properties and you can combine them to meet your criteria.

6. Quick results

   You will observe immediate results in the presentation of the enumeration of the data properties. This is a quick an effective way to explore your data and associate calculated values on demand.



7. Instant gratification

   Once you are able to find an acceptable result for your data analysis, you have the option to present the results in tabular format, or in a graphical view. The Pivot interface provides a vast collection of graphic options to display your analysis in an interactive fashion.

Pick the Pie chart from the visualization picker.

8. Visualization quick-pick

   Quick access to visualizations empowers 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.

9. User control

   With the results achieved you the option to refine the visualization presentation for aesthetics or to improve precision in interpretation. This ensures that the relevance of the data presentation is easily accessible with a simple, self-guiding approach that will save you labor.

10. Final product in a short time

    From the moment you started to explore the data to a point when you can visualize the results, only a few minutes have passed. The effective result is your ability to turn data into information and then have the ability to share that with your coworkers.

Reports

Introduction

Splunk reports offer you the advantage of automated knowledge distribution and collaboration. Reports take in the foundation of your search experience and the proprietary knowledge that fuels your operational landscape.

The expectation is that you will obtain reports on demand, on a scheduled basis, or via your e-mail inbox. The upshot benefit is a collaborative approach where operational knowledge becomes a commodity that allows for continuous improvement.

Highlights

- Knowledge automation
- Prescriptive collaboration
- Automated distribution

Narrative

Reports will allow you to recycle knowledge that is important to your group and automate the results in a recurring basis. The knowledge gained becomes an asset to be shared as part of your normal communication procedures.

With the investment on teamwork, you can establish general procedures to allow for cross collaboration between teams that do not communicate in a general basis. For instance, software application maintenance teams can report on resource consumption to a finance team – which allows for a measurement of ROI.

One of the best benefits or reports is that the consumers do not need to be Splunk-trained or technology-driven. That means working with predictive reporting results on adaptable schedules. What you measure and make part of your reports is a progressive list of hard-to-achieve knowledge gathering.

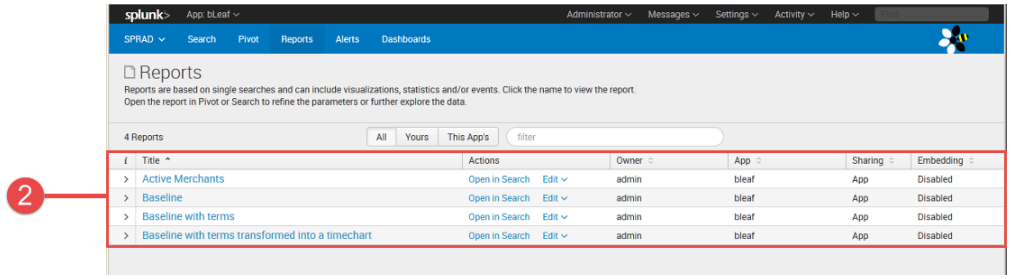
Micro scenarios

```
Click Reports menu item.
```

1. Reporting benefit

   Our approach to solving problems is to expose to you the appropriate techniques and attributes which allow you to analyze and visualize data very quickly. This empowers you and your audience 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

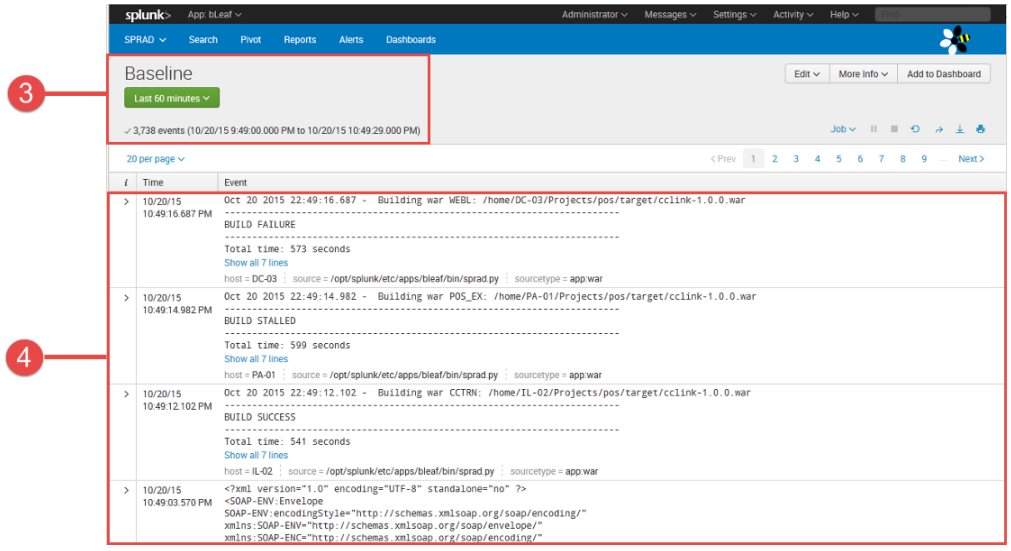
collections of alerts, reports and dashboards which offer dynamic drilldowns for granular data exploration.



Pick the Baseline report.

2. Organization of reports

To start with your search experience, imagine that you are part of a team that is investigating a technology problem that has a definitive business impact. From an operational perspective you will be able use search criteria with details that are relevant to that investigation within seconds. In the olden days you would have to visit various teams, databases, applications in order to combine all of the data to create a single point of view.



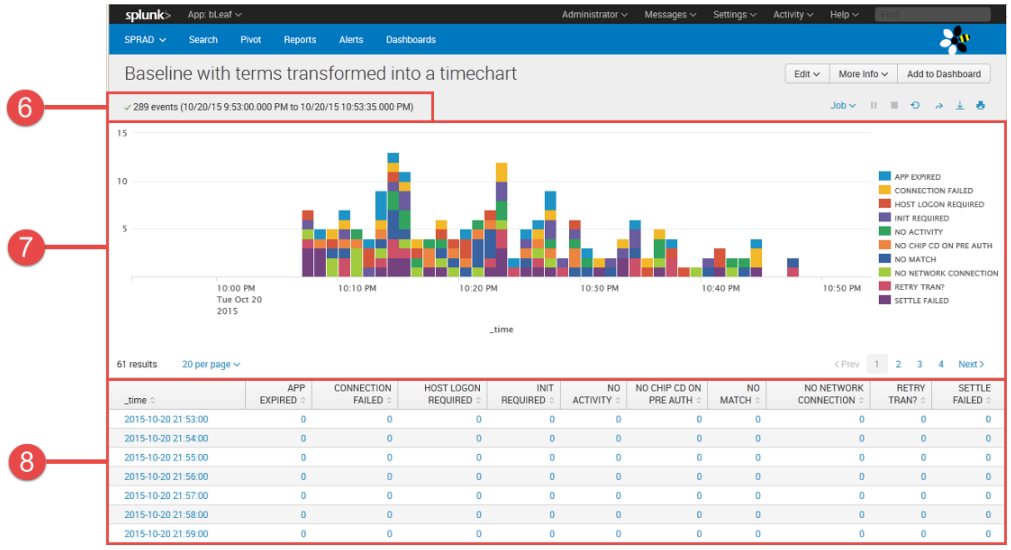
3. Quick, automated results

Each report is catalogued as a knowledge object: an independent entity that holds knowledge applicable to a specific behavioral scenario in your environment. Reports are communal by nature and intent; that means you have the flexibility to share and distribute them as needed.

```
Click Reports menu item.
Pick the Baseline with terms report.
```

4. General events

   With this automated report we are searching for all of the events contained within an arbitrary data set. Pay careful attention to the number of events that match your Baseline criteria. Let's explore a more granular way to add more precision to your results by using a second report with more granular terms.




```
Click Reports menu item.
Pick the Baseline with terms transformed into a timechart report.
```

5. Extrapolating with visualizations

   This automated report contains all events that match “error OR fail” and the results are enumerated by an arbitrary field. It improves the Baseline report because you have a more targeted set of results.

6. Effective data reduction

   With this type of precision the number of resulting events have been reduced significantly and you are now equipped with very specific results for collaboration or report distribution.

7. Interactive data results

Splunk provides you with the option to represent the results in a graphical format that suits your preferred reporting options. In this case, the report will count an arbitrary field and organize the count in proportional time periods for the search window.

8. Full details with access to data

   Because it is important to corroborate the visualization results, the supporting calculations are offered as part of the overall presentation. This provides the flexibility for you to interact with the results, change the criteria or determine a different time window. The upshot benefit is that you can explore the results in a prescriptive fashion and be ready for collaboration with the click of a button.

Alerts

Introduction

The idea of data-driven alerts reflects a strategy where you use your data to support vital operational processes without relying on traditional invasive surgery. The Splunk platform is able to analyze your data in historic mode or real-time and you can propose conditions which reflect risk for operations, security, fraud, etc. This is yet another way to extract even more value from key findings in your data.

Alerts are the result of a behavioral condition that occurs within your operational environment. Splunk considers an alert as a special knowledge item with multiple mechanisms to broadcast notifications, initiate corrective action or to trigger operational processes. The upshot benefit is to expand the qualification of an alert to match conditions across multiple layers of technology and traditional counter-driven blips.

Highlights

- Event notification
- Process integration
- Runbook automation

Narrative

The key advantage of alerts is reflected in a consolidation of the conditional knowledge gained from all of the areas of your business that generate the data. When a condition is found, it may affect various technology areas that support your business. For example, a condition where an application is unreachable may be due to multiple factors, i.e. network connectivity, computer downtime, application breakdown or a total power outage; With Splunk you can identify the condition and then drilldown into the contributing events with speed and ease.

When an alerting condition occurs, it is important to take action based on the context of the nature of the condition. For that reason, Splunk provides the ability to take upon one or multiple actions. These actions allow you to notify interested parties with e-mail messages, kick-start work with external scripts or programs, or you can integrate workflow directly with third-party management systems.

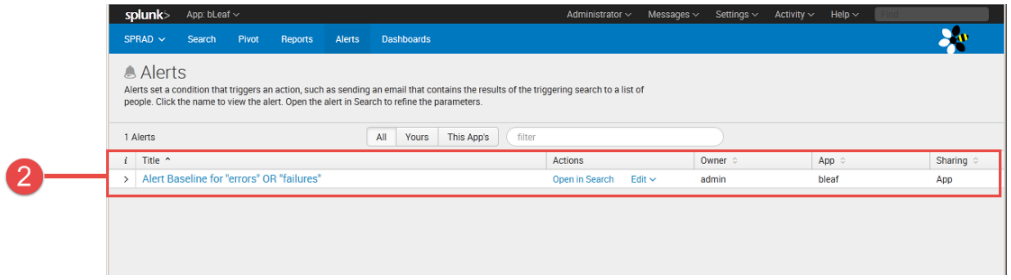
The most common scenario under a condition that triggers critical alerts is the initiation of external, automated work that is part of a runbook. At Splunk we believe that your data should be fully actionable with minimal latency. That means new and innovative ways to manage increasing service requirements by identifying potential problems and beginning to repair those problems in real-time.

Micro scenarios

Click Alerts menu item.

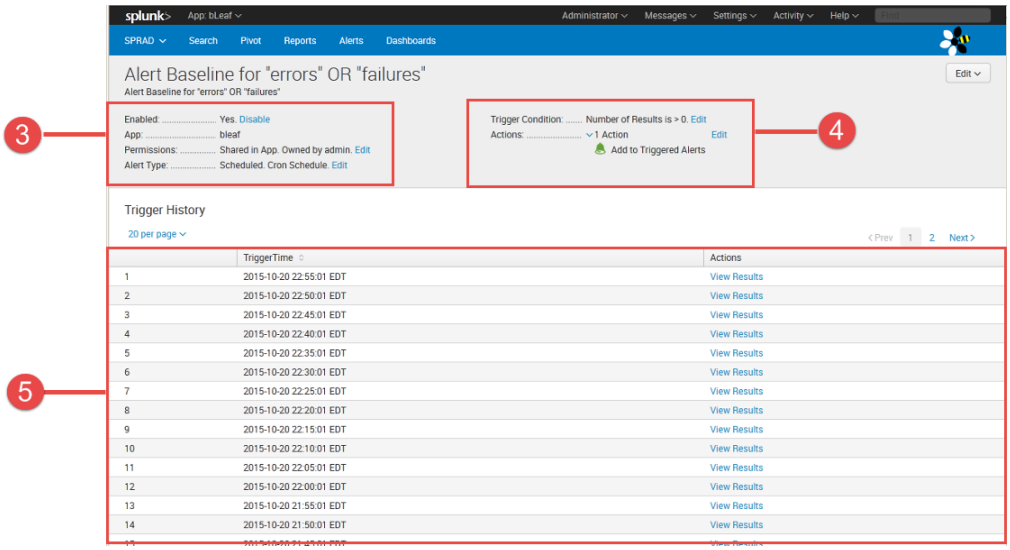
1. Alert benefit

   The advantage of using Splunk for alerting functions is on the conditional relationship that is automated with each individual alert. For example, a CPU may sometimes offer a high percentage use and traditional counter agents see that as a risk. In Splunk, you can extrapolate the relationship between a CPU usage spike and application response. Hence, if the behavior is observed repeatedly across a period of time, then an alert is triggered.



Pick the Alert Baseline for "errors" OR "failures" alert.

2. To start with your search experience, imagine that you are part of a team that is investigating a technology problem that has a definitive business impact. From an operational perspective you will be able use search criteria with details that are relevant to that investigation within seconds. In the olden days you would have to visit various teams, databases, applications in order to combine all of the data to create a single point of view.



3. Results replay

   Another key factor in alerting with Splunk is the instant replay derived from the conditions observed in your data exploration. For instance, finding a significant condition that merits an alert may trigger an investigation across multiple lines of business. When the data is at hand, not only is it possible to drill down into the problem but also across other potential contributors for knowledge gathering.

4. Summary of alert results

   What happens today when you want to investigate an alert trigger by a traditional monitoring system? In most cases you have the result of the alert and its meaning. If you are required to investigate further, you will need direct access to the element affected so you can observe first-hand. With Splunk you have complete control of the historic footprints left behind by the event with a single click.

5. Summary of triggered alerts

   The immediate benefits of having all of your systemic alerts in one place can be summarized with access control, event replay and cross-investigation. When you have full context of a triggering condition, you are able to improve your operational response exponentially and without limits.

Dashboards

Introduction

Splunk dashboards are a culmination of labor in which you consolidate knowledge for collaboration. A dashboard captures key informational findings and analyses which allow you to interact, collaborate and explore findings with a dedicated context. For example, dashboards can be used to reflect an operational viewpoint of your various supporting IT layers. Also, you can enrich results by extrapolating relationships in your data exploration and associating third-party information to augment the end user experience. Thus, you turn an operational viewpoint to a business perspective very quickly.

Today dashboards are a commodity that is shared and sold within our Splunk community. We can be prescriptive about many points of view around technology and, at this point, there are many applications, templates and utilities for your immediate consumption. What we cannot do effectively is predict the nature of your individual needs so we provide a flexible, easy-to-use user interface to build your own. There is no coding needed; it is all point-and-click.

Splunkers share a common bond across the world; Splunk employees, partners and customers are all driven to explore data as a vehicle to solve complex issues. We share our work with others at Splunkbase – where we post Splunk applications, templates and utilities that are useful for many different things.

- Interactive data exploration
- Prescriptive knowledge
- Collaborative insights

Narrative

Dashboards are like radar for air traffic controllers; they provide all of the essential information to continually direct and maintain your business running. IT personnel and business users rely in up-to-date information in order to make decisions and dashboards summarize findings and analyses at a glance. And, because dashboards are interactive portals for exploration, you have complete visibility of your information from a flag in the highest peak of a mountain to the lowest depth in your ocean of data.

What is important to understand is that dashboards provide an opportunity to consolidate knowledge for collaboration. That means you break cultural barriers between separate working groups by making relevant information available, without the need to access all the assets involved. With dashboards, you can narrow down the type information and control the access level to each finding.

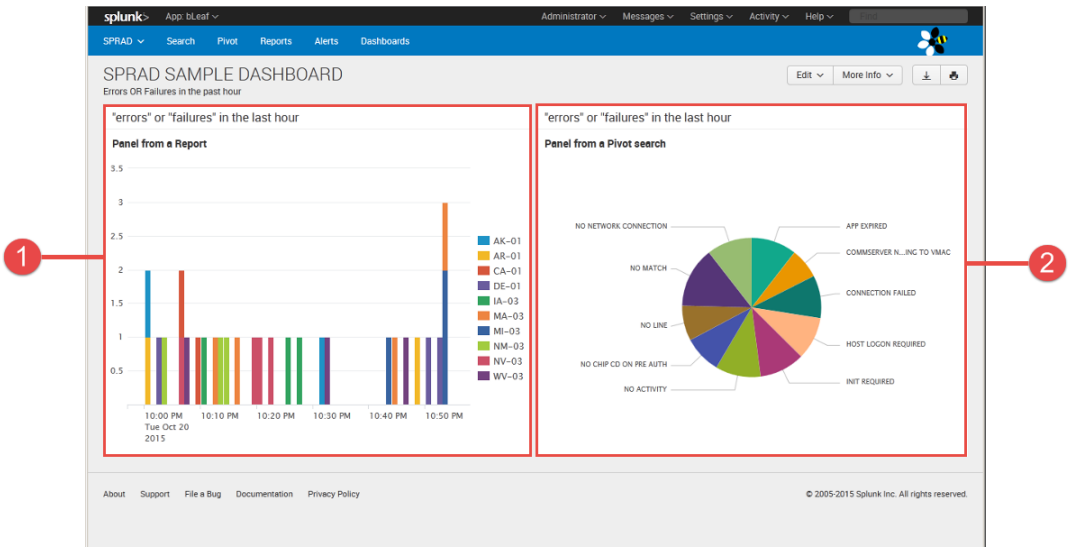
When you are able to consolidate and explore the information and analyses derived from your data, you can easily focus on the specific area of expertise and avoid all the extra noise. The insights you gain through your exploration find a collaborative context and will help improve the overall stance of your business.

Micro scenarios

```
Click Dashboards menu item.
Pick the SPRAD SAMPLE DASHBOARD object.
```

1. Benefits or dashboards

   Splunk dashboards are a culmination of labor in which you consolidate knowledge for collaboration. A dashboard captures key informational findings and analyses which allow you to interact, collaborate and explore findings with a dedicated context. For example, dashboards can be used to reflect an operational viewpoint of your various supporting IT layers. Also, you can enrich results by extrapolating relationships in your data exploration and associating third-party information to augment the end user experience. Thus, you turn an operational viewpoint to a business perspective very quickly.



2. Shared analysis and collaboration

   Any particular knowledge point can now become a report, dashboard panel or alert. In this case you have a dashboard panel that can be shared with your colleagues for continual reference.

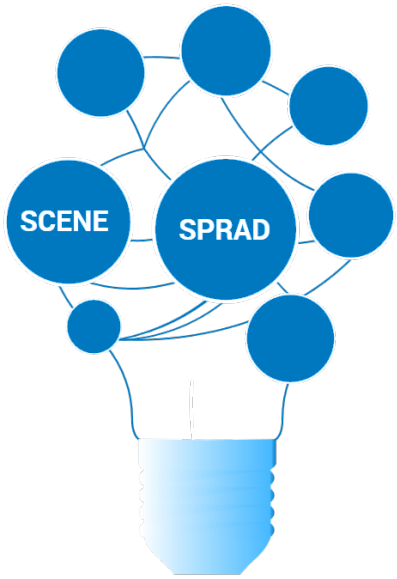
3. Interactive and effortless

   In this scenario you have found error and failure messages. At this point you are dealing with a smaller number of devices and you can focus our attention toward those sources that need it the most. The typical scenario here is that you will find an attention-grabbing event; the best case scenario is that you learn something meaningful that can be automated and shared across your entire organization.

Scene

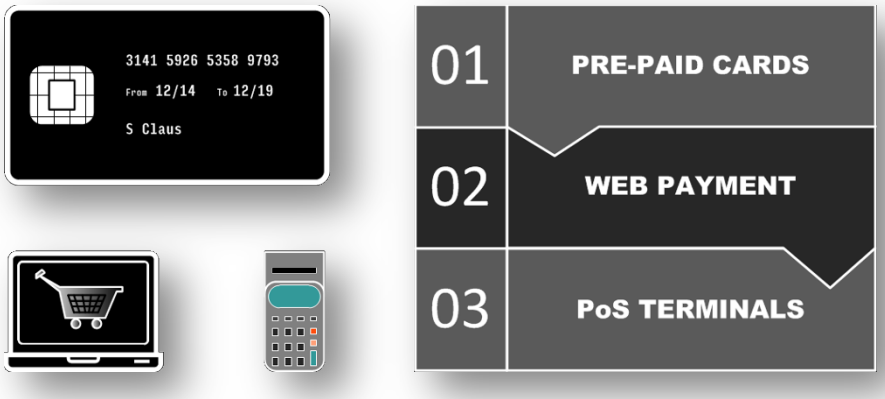
At Splunk everything we do is focused in helping our customers be successful. Our data platform is focused in removing barriers which reflect risk for implementation. Our technology reflects a full integrated solution that is scalable, easy to use and which produces results quickly. Splunk customers typically achieve a positive return on investment in just a few weeks or months, sometimes while still in the testing or evaluation phase.

In this quick demonstration we are walking through some common examples of how customers use Splunk Enterprise during an adoption phase. Today we will explore and create results multiple times. In each scenario we aim to achieve a full result in minutes.



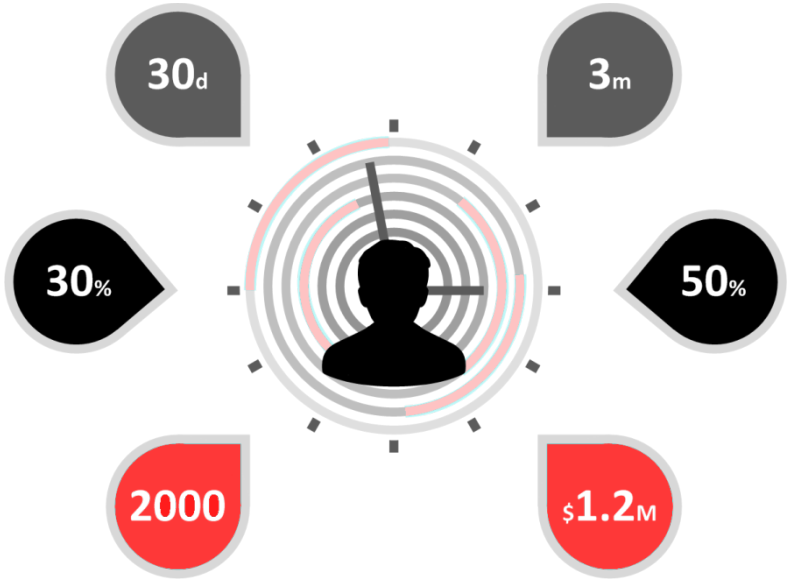

```
Click on the SCENE button.
```

With a foundation of the technology benefits in the Splunk Platform, it is important to relate the use of the technology to the business gains achieved by using it. Splunk Enterprise is a versatile and powerful technology that helps our user achieve value very quickly.



Click on the tour page arrow or use the right arrow key to advance.

For this example, please pretend that you are part of a business which provides payment solutions at a national level. That means you are between merchants and financial insitutions that use your network to broker goods and services. In your line of business you offer a variety of services such as pre-paid cards, online payment solutions and physical point-of-sale terminal devices.

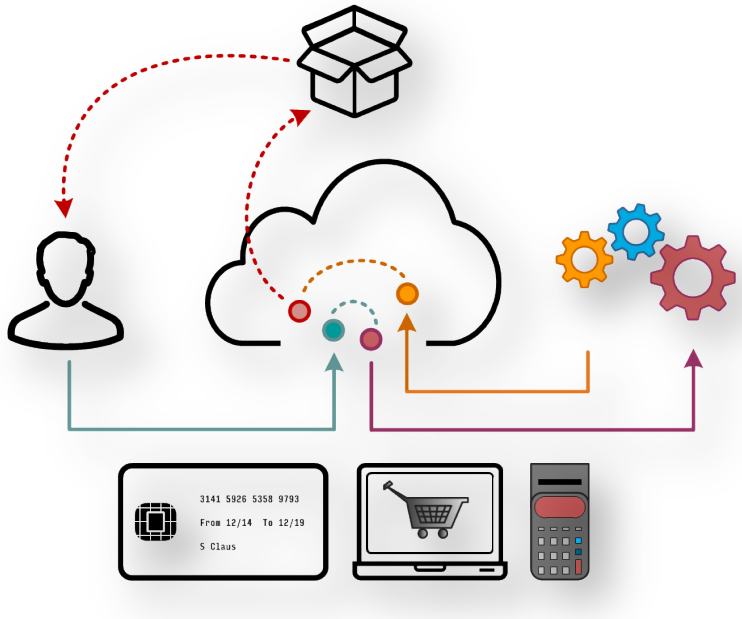


Click on the tour page arrow or use the right arrow key to advance.

As part of your growing list of responsibilities, you have been asked to manage part of a new corporate services campaign. The primare objectives are

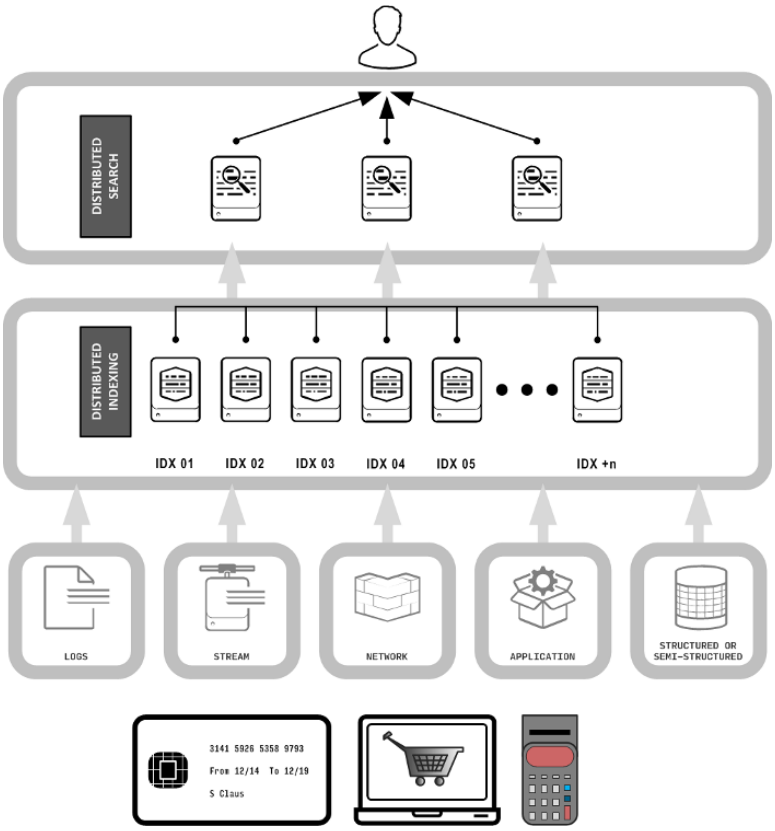
1. In the first thirdy days enlist two thousand customer with a 30% engagement rate.

2. In the first three months, retain 50% of new subscribers and average about $1.2M in transactions per hour.



Click on the tour page arrow or use the right arrow key to advance.

To achieve this monumental task you have directed your IT department to monitor the transaction records in your payment system. This includes all transactions completed by consumers at physical stores through the payment network, and all Web-based requests that use your Webcart Payment. In this manner you can keep track of the new services main objectives and continually adjust to market pressure.



The IT department the idea of using Splunk as a vehicle to collect analyse and present all of that data. Splunk's Universal Machine Data Platform is open and extensible; it delivers integrated, end-to-end data collection, management and analysis which helps amplify visibility across the entire payment services environment.

With this approach you are hoping to make those transactions fully actionable with minimal latency. That means new and innovative ways to manage increasing service requirements by identifying potential problems and beginning to repair those problems in real-time.

Your advantage is the complementary distributed architecture model of the Splunk platform because it allows you scale your deployment in order to meet user demand and analysis of large data sets. The software that runs on a laptop will scale to the datacenter; it breaks traditional nominal scalability and performance boundaries and allows you to go beyond outdated limits preset by legacy data management systems.

Click on the tour page arrow or use the right arrow key to advance. This will take you to the MERCHANT SUBSCRIPTIONS dashboard.

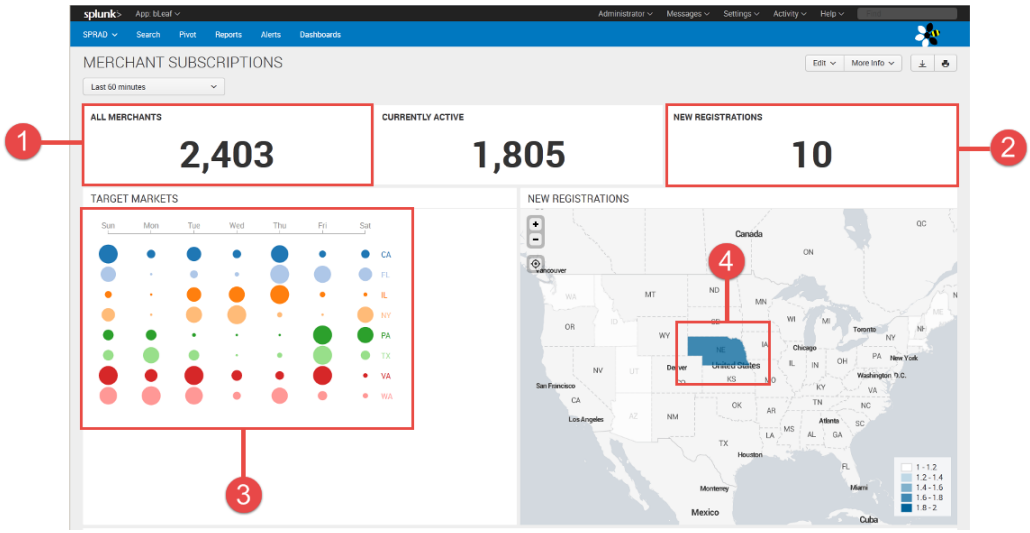
Supporting Dashboards

This scene contains three basic dashboards to draw in the demonstration. We use them to reflect the lessons learned with the SPRAD tour and also to help understand the value of Splunk Enterprise. The supporting dashboards are:

1. MERCHANT SUBSCRIPTIONS
2. TRANSCATION CONVERSION
3. SYSTEM ERROR INVESTIGATION

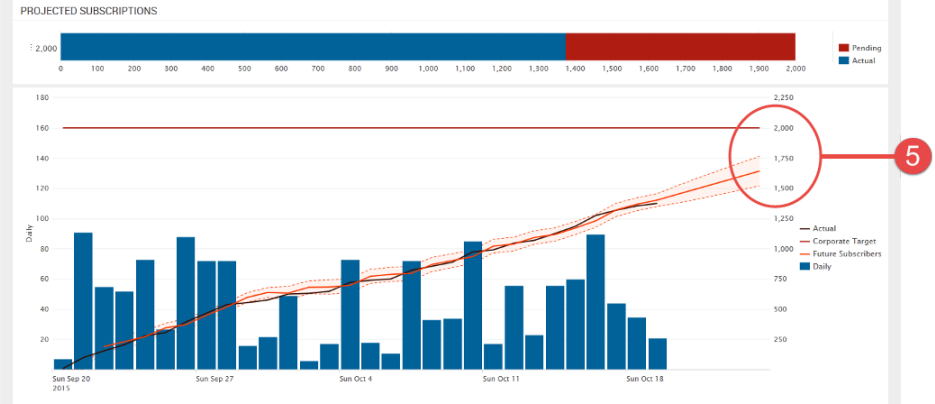
MERCHANT SUBSCRIPTIONS

This dashboard illustrates the relationship between simulated transactions, subscriber engagement and new service registrations. Remember that the primordial short-term goal is to achieve two thousands (2,000) new registrations in the first thirty days.



Please highlight the following:

1- By measuring the rate of currently active merchants, we can extrapolate unique users who have used the payment services during the time period specified in the time picker (60 minutes is the default).
2- The current rate of subscribers in the given time period is adequate but in itself it is just a data point. You need more information to determine whether this is a good or bad number of new registrations.
3- The major markets that are currently part of your target segments offer a good measure of return. The challenge is in understanding if that will help you achieve the target of two thousand new subscribers.
4- Some of our new geographical subscribers areas are in better shape than others. You may now choose a longer time period to elaborate the interaction.



5- Scroll to the bottom of the page. Note the number of active subscriptions since the new campaign begun and compare to what is missing. Relate the actual registration rates against the predicted value.

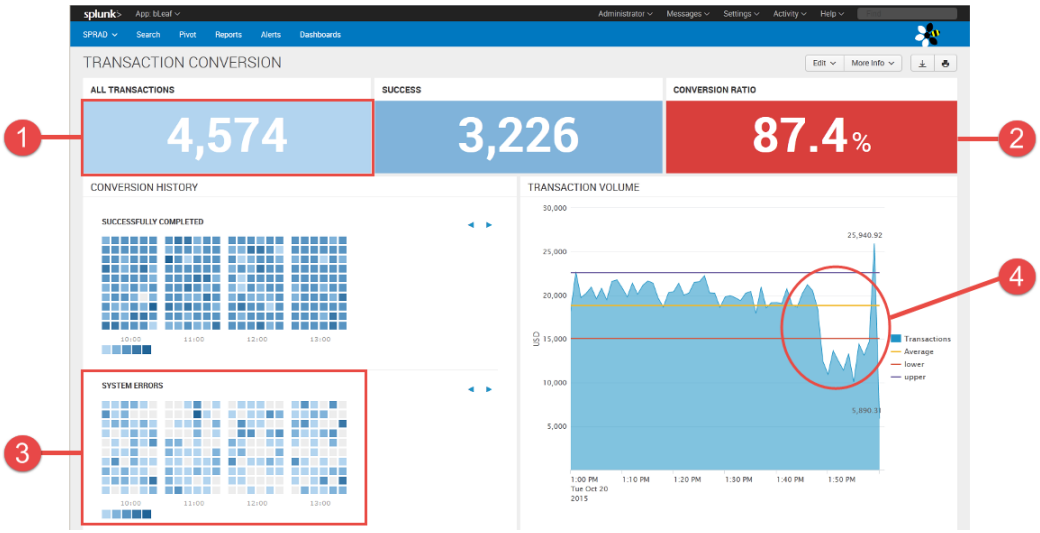
Conclusion

By measuring the numerous transactions generated by the payment system we are able to determine the current engagement associated with the new promotion. It seems the rate of merchant registrations will miss the desired, two thousand subscribers. It will be important to ensure that the rate of subscription is not caused by poor service.

Click on any of the Daily columns in the time chart. This will follow a link to the TRANSACTION CONVERSION dashboard.

TRANSACTION CONVERSION

This dashboard helps a line manager or an analyst determine the performing health of a payment service. In this case we use data to monitor electronic service requests from multiple access points through the banking network; specifically, you are focused on specialized Web services and the physical point-of-sales devices. This dashboard is focused in the past sixty minutes.



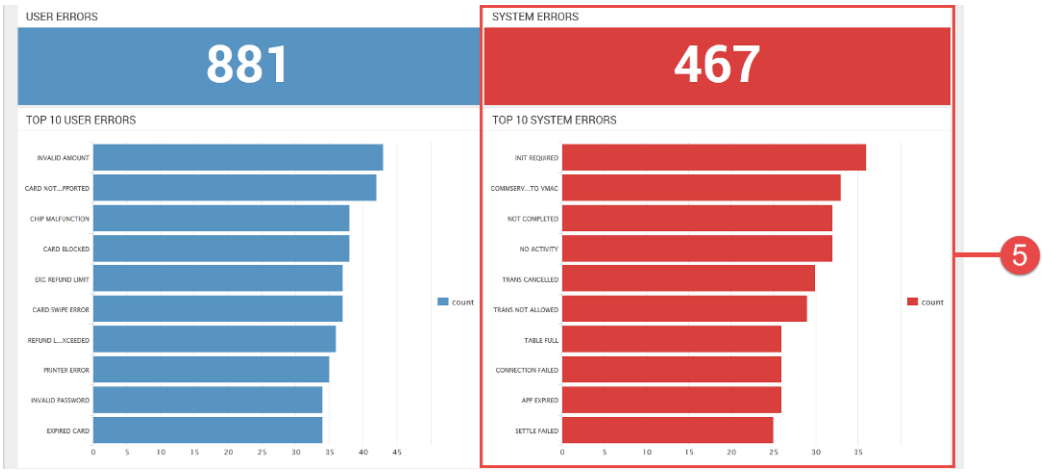
Please highlight the following:

1- Because all of the individual transactions are being monitored, it is possible to determine unique transaction records even if there are multiple systems which support the payment service. In this case we are consolidating identifying requests from the application servers connected to the payment network, the underlying middleware software and from multiple Web services requests.

2- After discarding end-user errors, we concentrate in factoring those requests which are submitted to the payment services applications successfully. We use a ratio between the successfully completed transactions and the ones that were not completed after submission. In this model, anything less than a ninety percent conversion ratio is considered poor service.

3- By examining the calendar diagram, we can quickly glance at the system generated errors through the past four hours. We can quickly establish that there has been a very significant number of system errors caught in through the technology layers in the past four hours.

4- More telling that anything, we can glance at the functional throughput graph and see an indication of depression in the rate of funds traveling through the payment system. This valley of inactivity may be indicative of a systemic issue so we need to explore the data even more.



5- As we approach the actual error messages found in the system, we need to ensure we can examine the right data quickly. For that reason, we will drill-down into the system error to find where the errors are occurring and the behaviour we can observe.

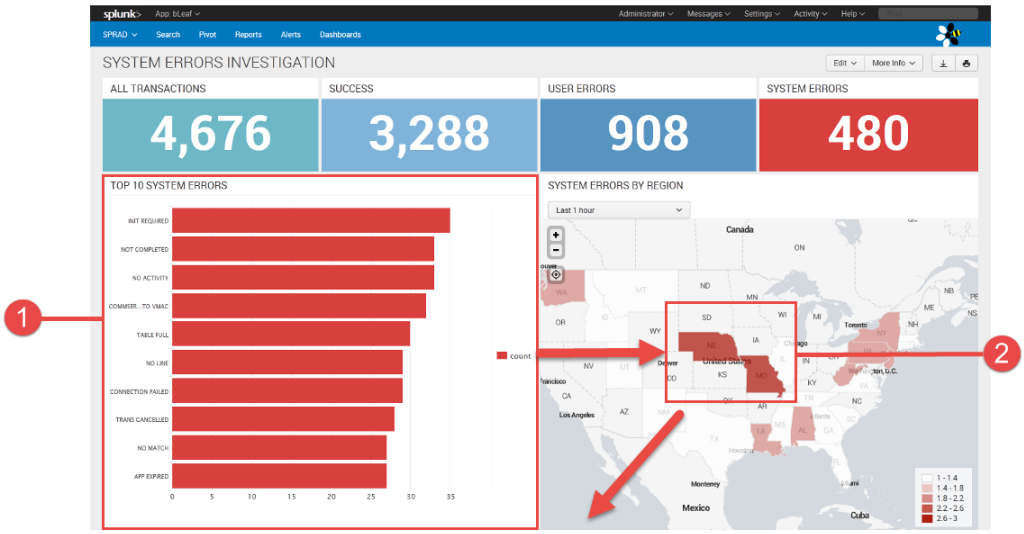
Conclusion

We see an unusually high amount of system errors within the payment service. We are not convinced this is the main reason for the low registration and engagement from the merchant trend. However, we will need to further investigate to either eliminate the system errors as a reason, or confirm a relationship.

Click on any of the TOP SYSTEM ERROR bars in the red chart. This will follow a link to the SYSTEM ERRORS INVESTIGATION dashboard.

SYSTEM ERRORS INVESTIGATION

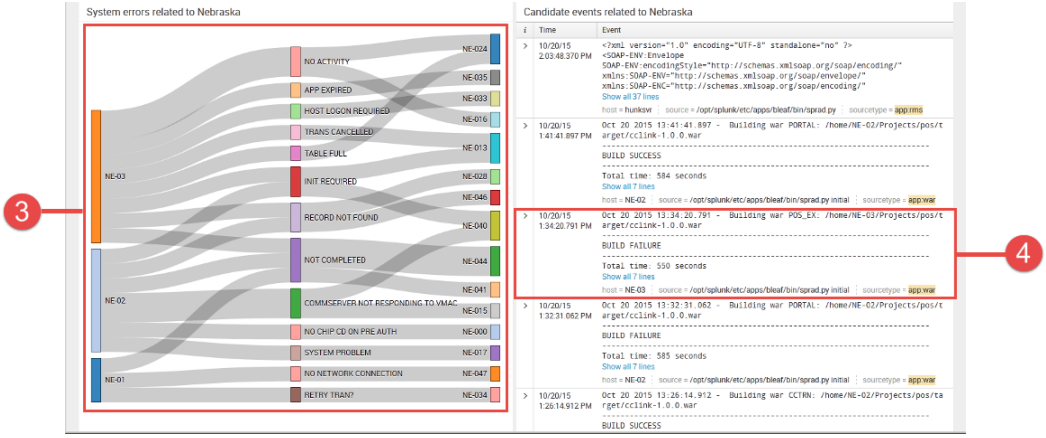
This dashboard is a great source for analysts and system operators. It provides a granular view of potential issues by highlighting system errors. The way this dashboard is organized is by finding an error category, correlating to a geographic region, and then associating areas of concerns with actual applications servers that provide the payment services. For operational personnel, this dashboard also offers a glimpse into the raw data that is potentially associated with the error messages.



Please highlight the following:

1- The organization of the TOP 10 SYSTEM ERRORS provides focus for the operations team in order to establish a priority list to work upon. Network errors and applications errors are distributed across separate team but all team members use the same source of information. For example, the network operations team may prioritize the generic “SYSTEM PROBLEM” in order to remove indicia of network connectivity in the payment system. When you pick that item in the list, you will also receive an associated list of geographic market segments where the problem is present.

2- To further focus on dealing with the problem at hand, an operator will follow the region of highest error congestion. That allows for a direct plan of attack in those concerns that easily identifiable and that have the greater impact across the national payment system grid.



3- The immediate result from this approach is a more granular list of active hosts and merchants who are affected by the faulty conditions. In some cases, the association includes an application module, or just the error at hand.

4- In order to provide closure, the operators are given a discrete list of candidate events that generate error conditions in the geography that is affected. The list is not exhaustive but it provides a specific point of inference in the exploration of the situation. In this case highlight an

occurrence of a “BUILD FAILURE”, or “BUILD STALLED”, or “BUILD SUCCESSFUL” event. These reflect an application package deployment and a systemic delay in service. That means potential subscribers from the affected regions were blocked from service and were unable to subscribe to the new promotion. This explains the system errors and the low registration count.

The event will look somewhat like this:

Conclusion

In this scenario we have determine that there were various systemic operations which caused a service interruption. We have accomplished this by investigating thousands of data points using some custom dashboards created just for this specific use case. The entire investigative effort would have taken hours in a traditional monitoring scenario.

It should be clear, however, that the flexibility and time to value of Splunk are paramount. In cases where the addressable concern is well defined, like with VMware health and performance monitoring, there are ready solutions which can be used in a manner of minutes.

Splunkers share a common bond across the world; Splunk employees, partners and customers are all driven to explore data as a vehicle to solve complex issues. We communicate, collaborate and help each other because we hold a unified belief: Splunk is good. For instance, novice and experienced Splunkers foster collaboration through a question-answer forum in Splunk Answers –where 70% of product questions are answered by the community. Also, we share our work with others at Splunkbase – where we post Splunk applications, templates and utilities that are useful for many different things. We share our thoughts through virtual communities, user groups, blogs and we hold development workshops regularly.