



Using Splunk IT Service Intelligence

Document Usage Guidelines

- Should be used only for enrolled students
- Not meant to be a self-paced document, an instructor is needed
- Do not distribute

Generated for Javier Palacian (javier.palacian@tescobank.com) (C) Splunk Inc, not for distribution

Recommended Course Prerequisites

- Splunk Fundamentals 1
 - or
- Equivalent Splunk Experience

Generated for Javier Palacian (javier.palacian@tescobank.com) (C) Splunk Inc, not for distribution

Course Modules

Module 1: Introducing IT Service Intelligence

Module 2: Visualizing Services with Glass Tables

Module 3: Managing Notable Events

Module 4: Investigating Issues with Deep Dives

Module 1: Introducing IT Service Intelligence

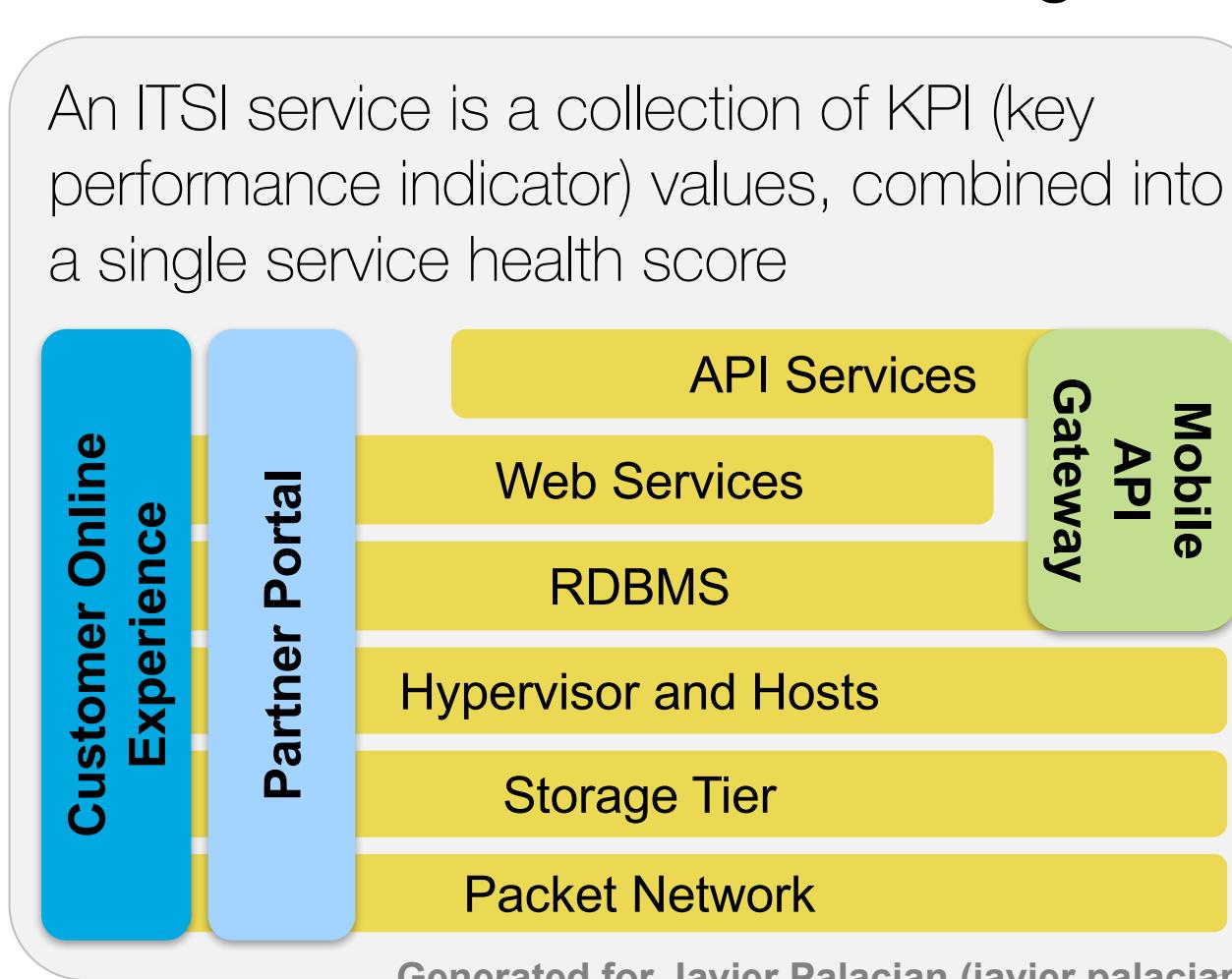
Generated for Javier Palacian (javier.palacian@tescobank.com) (C) Splunk Inc, not for distribution

Objectives

- Define key service intelligence concepts
- Identify IT Service Intelligence features
- Examine the IT Service Intelligence user interface
- List IT Service Intelligence user roles

What is a Service?

- Service: a collection of IT objects that relate to your business goals and need to be monitored together



- Services can be
 - High-level or low-level
 - Tangible
 - Storage tier
 - Abstract, multi-tiered, conceptual
 - Partner portal
 - Groups of people or objects
 - Dynamic or static
 - Wide or narrow in scope
 - Global vs. local
 - Corporate vs. team

Service Monitoring Use Cases

Transaction Troubleshooting

Common Situation: Various execution paths depending on the product purchased. Some tools developed in-house and some industry standard. Purchases that get stuck in the purchase process may increase in price.

Goal: Alert and troubleshoot prioritized by potential income.

Policy Service:

Common Situation: Various local and market-specific APIs perform validation to understand customer behavior and risk. Proprietary gateways don't communicate protocol changes efficiently.

Goal: Quickly detect challenges in low volume markets before sales are significantly impacted.

IT Infrastructure

Common Situation: Alert File and print sharing, WAN connections for various geographical sites, as well as back end services availability are a challenge to coordinate and troubleshoot

Goal: Monitor the entire system and reduce connectivity issues and systems downtime

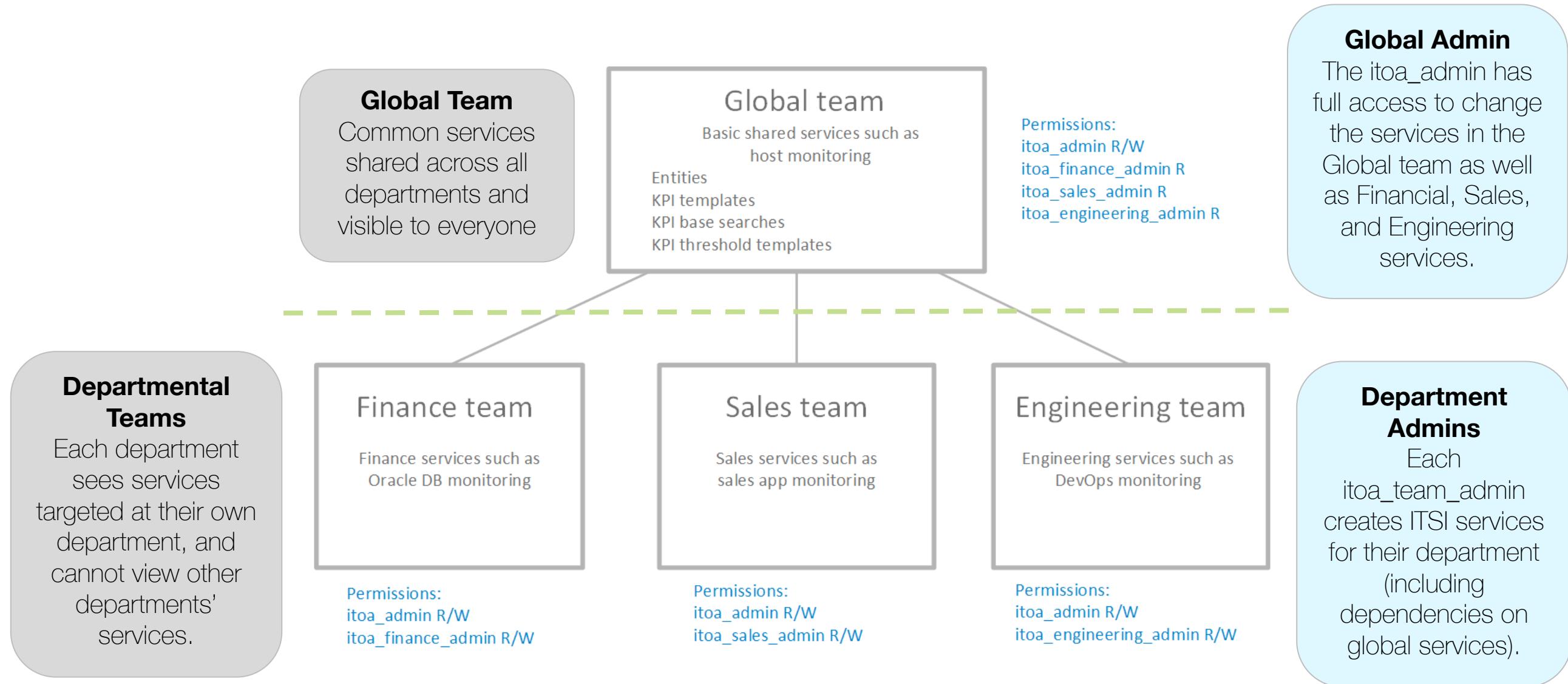
Call Center Monitoring:

Common Situation: Analyzing configuration shortcomings can be challenging when running multiple independent systems operating in silos: telephony, service desk, IVR, and networking

Goal: improve customer experience, reduce wait time / dropped calls

Generated for Javier Palacian (javier.palacian@tescobank.com) (C) Splunk Inc, not for distribution

Teams Have Their Own Views in ITSI



Generated for Javier Palacian (javier.palacian@tescobank.com) (C) Splunk Inc, not for distribution

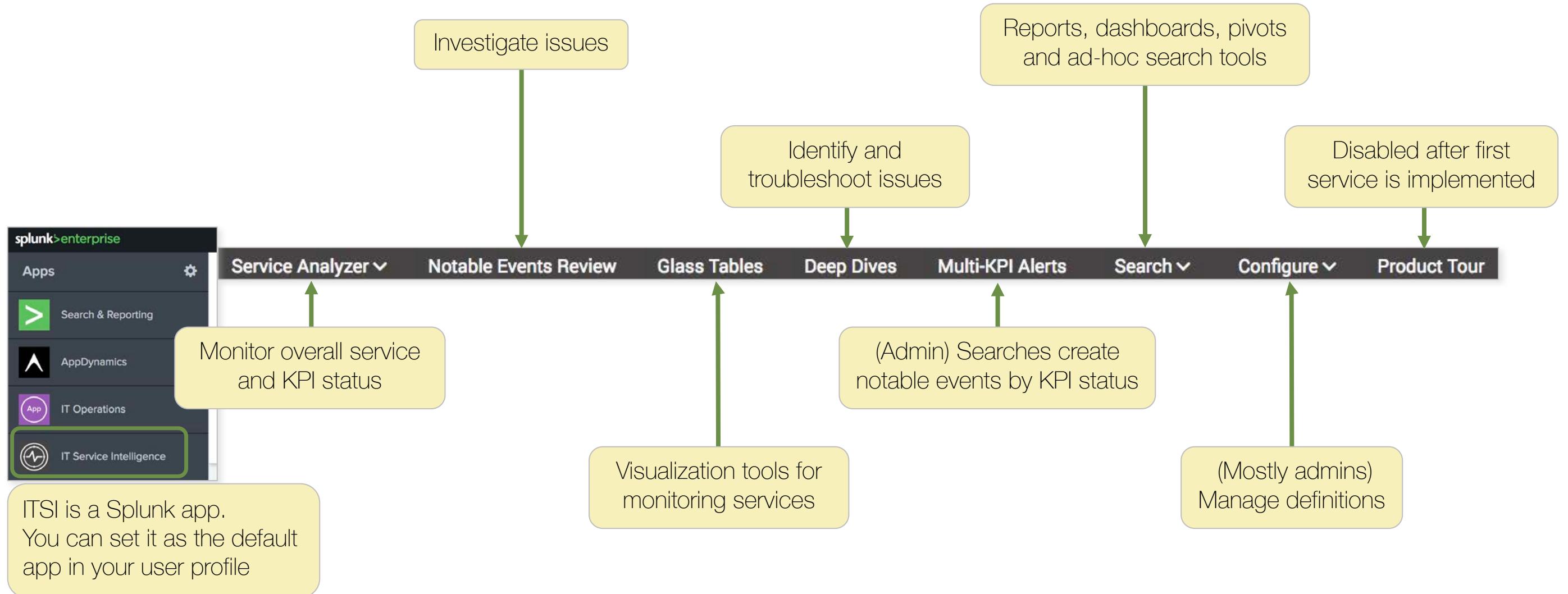
IT Service Intelligence Roles

Role	Description
itoa_user	Views most of ITSI and creates <i>private</i> glass tables or deep dives
itoa_analyst	itoa_user, plus owns notable events
itoa_team_admin	itoa_analyst, and creates <i>shared</i> services, KPIs, and entities for the team
itoa_admin	itoa_team_analyst, plus bulk imports entities/services, read/write/delete backups and restores

- You must have one of these roles (or admin) to use IT Service Intelligence
- Additional roles can be created as needed
- This class is designed for **analysts**

Generated for Javier Palacian (javier.palacian@tescobank.com) (C) Splunk Inc, not for distribution

Accessing IT Service Intelligence / Menus



Generated for Javier Palacian (javier.palacian@tescobank.com) (C) Splunk Inc, not for distribution

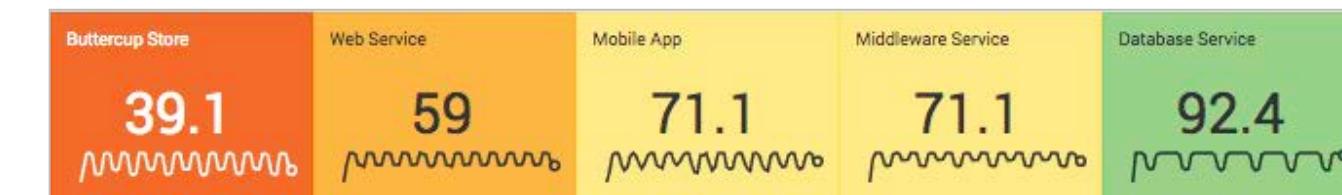
ITSI KPI and Service Health Scores

Scores = alert levels



- A **KPI** (Key Performance Indicator) is a numeric measurement of one factor affecting a service
- A service's overall status is displayed as a **service health score**
 - Values 0 to 100
 - Higher values = better
 - Service health score = aggregation of the status of multiple KPIs' alert thresholds as set by your admin

KPI	Service	Percentage Status Breakdown	Latest Status
4xx Errors Count	Middleware Service		Normal
5xx Errors Count	Middleware Service		Normal



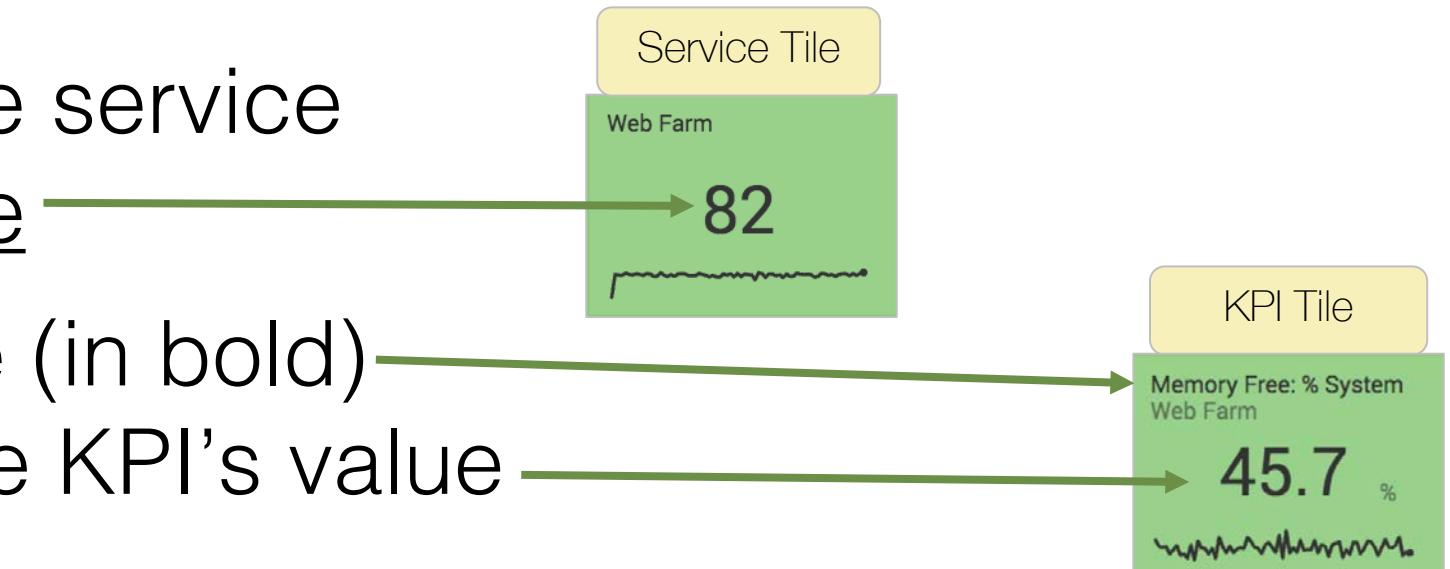
Generated for Javier Palacian (javier.palacian@tescobank.com) (C) Splunk Inc, not for distribution

Service Analyzer: Service and KPI Tiles

- A tile's color shows its alert_level ranging from **normal** (green) to **critical** (red) during the selected time range
 - Click a tile to open a detailed view of the service
 - (Click a KPI tile for service detail, not KPI detail)



- Each service has a tile with the service name and service health score
- Each KPI tile lists its KPI name (in bold) above the service and then the KPI's value



Generated for Javier Palacian (javier.palacian@tescobank.com) (C) Splunk Inc, not for distribution

How Key Performance Indicators Work

- Each KPI in a service has these settings:
 - Schedule: Interval can be measured from every 1 to 15 minutes; Range of measurement can be from 1 minute to 1 day
 - Search expression example: `sourcetype=access_combined_wcookie`
 - Calculation: summarizes fields in the events to generate the KPI numeric alert value, like `count of events` or `sum of price field`
 - Threshold: determine if the value is normal, critical, etc.
- KPI examples: users per hour, sales per minute, errors per day
 - Services on which another service depends are treated as KPIs for calculating a health score
 - Missing KPI events show as alert level “unknown” by default

Generated for Javier Palacian (javier.palacian@tescobank.com) (C) Splunk Inc, not for distribution

KPI Importance Weight

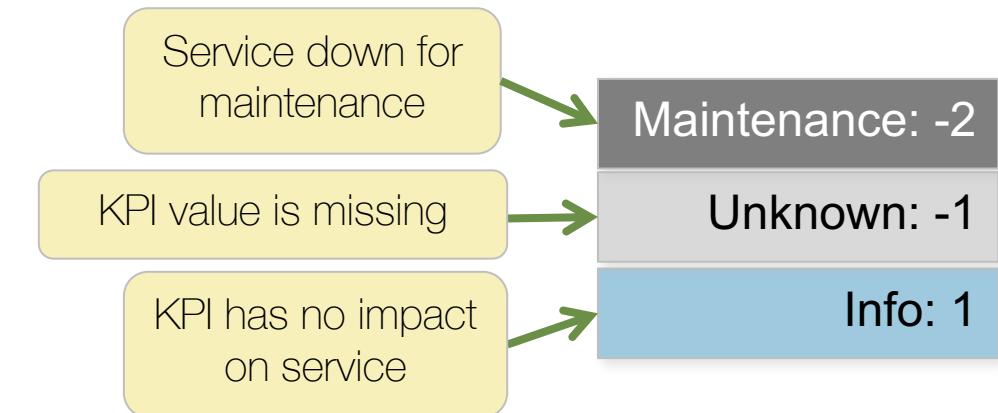
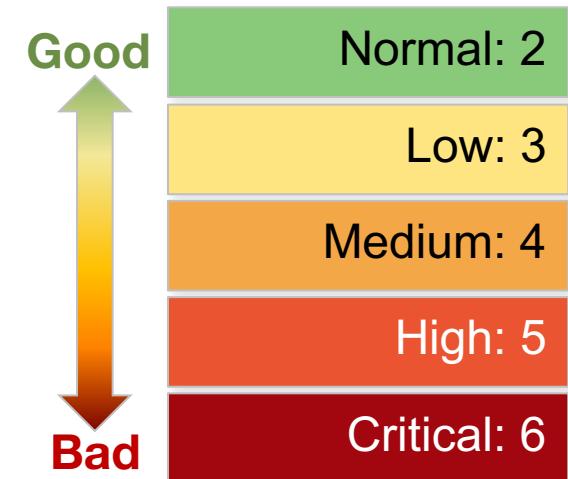
- Service *health* = average of all weighted KPIs expressed as a score from 0-100
- Service *alert* level cannot be higher than the alert level of the lowest minimum health indicator KPI
- Each KPI is assigned an importance weight: 0 to 11
 - A KPI weighted 11 is a minimum health indicator KPI
 - Importance weight of 10 for calculation purposes
 - When a KPI weighted 11 becomes critical, its services become critical (regardless of other KPIs in the services)
 - 5: default
 - 0: KPI is unused for health scoring



Generated for Javier Palacian (javier.palacian@tescobank.com) (C) Splunk Inc, not for distribution

Alert Severities and Levels

- Alert severity is the state of the KPI
 - Normal represents good or optimal
 - Critical represents a serious issue or problem
- A KPI's optimal (normal) value may be at the high, low or middle of its range
 - Low normal: count of error events over past 5 minutes
 - High normal: sales for last day
 - Mid normal: Web volume over past hour
- Special severity levels: Maintenance, Unknown, Info



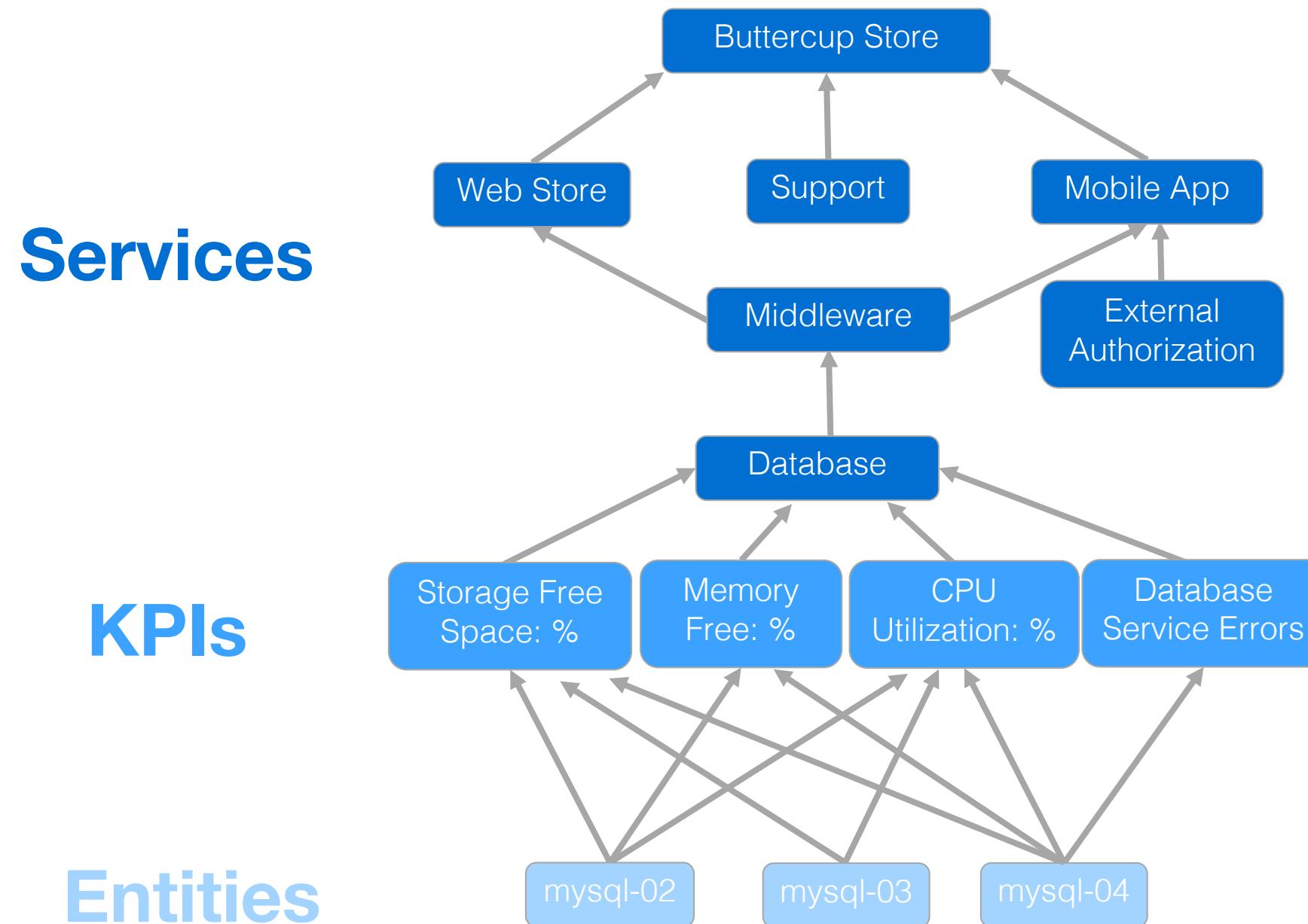
Generated for Javier Palacian (javier.palacian@tescobank.com) (C) Splunk Inc, not for distribution

ITSI Entities

- In creating services, your admins may also (optionally) define entities: IT components on which a service depends
 - Like a configuration item in the ITIL framework
 - An entity is never a service
 - Examples: virtual or physical server, AD/LDAP user, OS process
 - Entities may have multiple identifiers
 - Servers: several IP addresses
 - Two instances of the same web server app: two different entities
- Admins can configure KPIs to be split by entity
 - Entities contribute to the KPI score
 - KPI scores contribute to the Service Health score

Generated for Javier Palacian (javier.palacian@tescobank.com) (C) Splunk Inc. not for distribution

Flexible Dependency Mappings in ITSI



Generated for Javier Palacian (javier.palacian@tescobank.com) (C) Splunk Inc, not for distribution

Notable Events

- Represent an issue or problem with a service, KPI, or an entity
- Created by correlation searches, multi KPI alerts or anomaly detection
- Use the **Notable Events Review** dashboard to view, sort, and work on open notable events

Middleware Service

1468 events Last 60 minutes Service: Middleware Servi... Severity: All Add Filter search Show Timeline

Sorted by? Time

Owner	Severity	Status	Description
unassigned	Critical	New	Web Remove from ...
unassigned	Critical	New	Web View Cart stat...
unassigned	Normal	New	Authorization API ...
unassigned	Normal	New	Search API status ...
unassigned	Normal	New	API View C...

Acknowledge

NewRelic Health Status: Web View Cart

Tue Jul 25 2017 20:35:13 GMT-0100 (CVT)

Overview Comments Activity

Description

Web View Cart status = red

Contributing KPIs Open all in Deep Dive

Possible Affected Services Open all in Deep Dive

- Middleware Service
- Web Store Service

Generated for Javier Palacian (javier.palacian@tescobank.com) (C) Splunk Inc, not for distribution

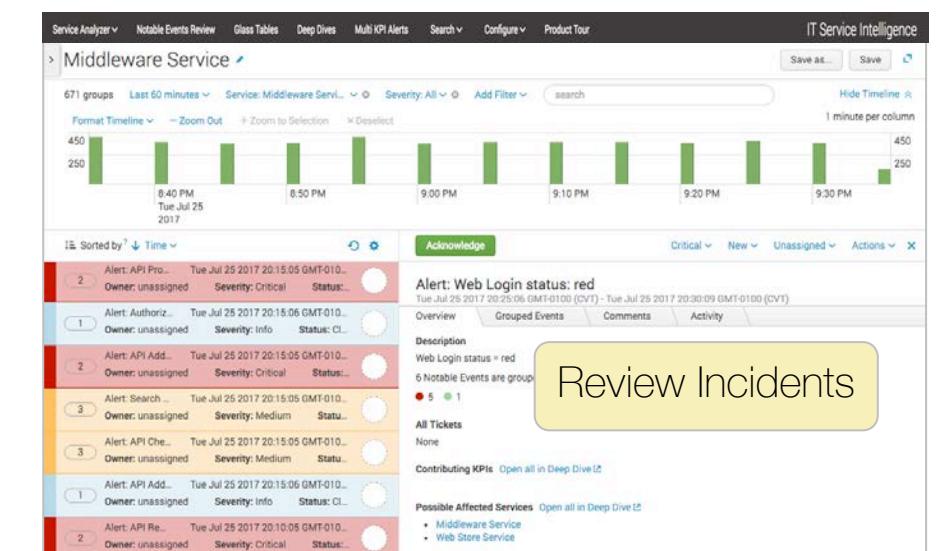
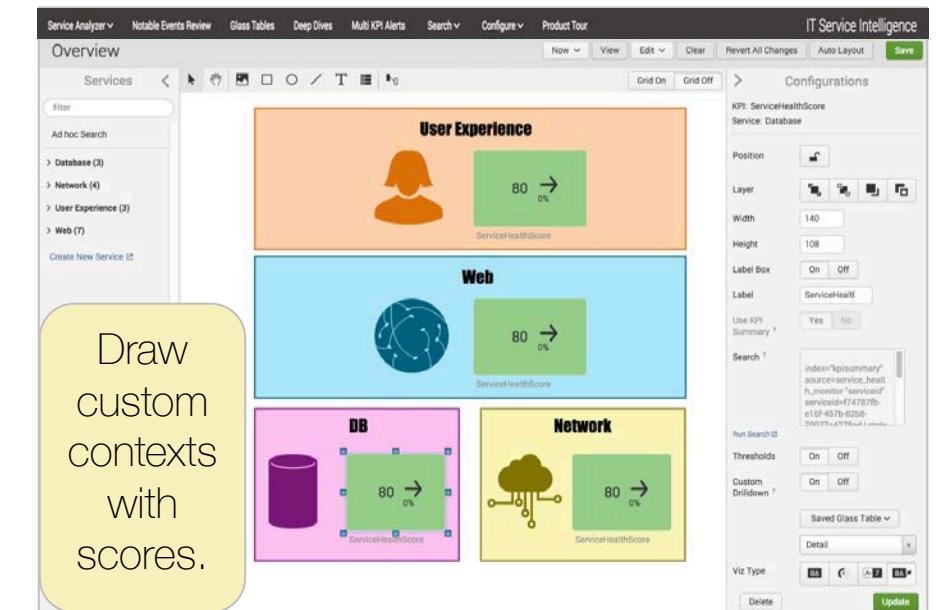
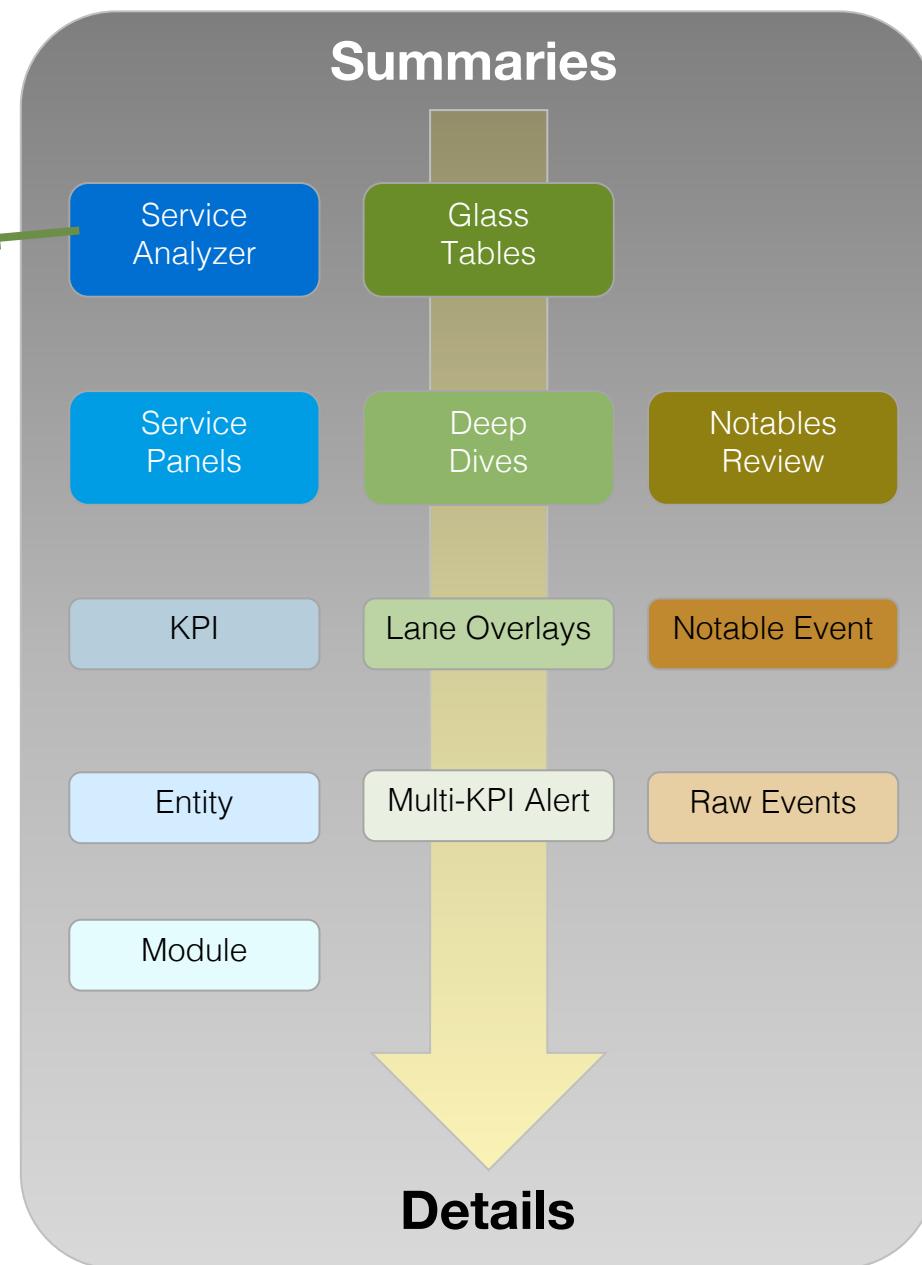
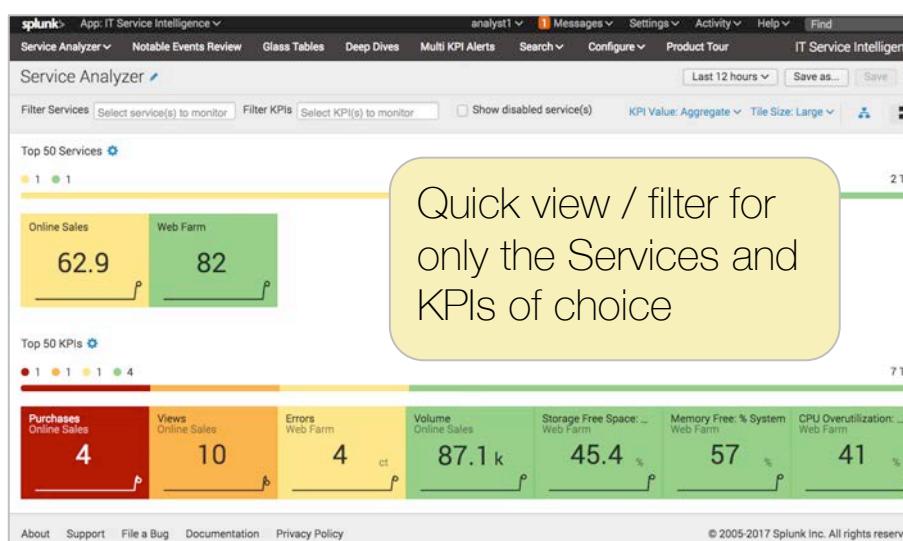
What is Service Monitoring?

- Aggregated health of a layer is less important
- Service health is determined by the health of the components of each layer upon which that service depends

Layer	Components	%	Layer Status
Web Server	(1, 2, 3, 4, 5, 6, 7, 8, 9 .. N)	100	Green
App Server	(1, 2, 3, 4, 5, 6, 7, 8, 9 .. N)	100	Green
Database	(1, 2, 3, 4, 5, 6, 7, 8, 9 .. N)	98	Green
Guest OS	(1, 2, 3, 4, 5, 6, 7, 8, 9 .. N)	100	Green
VM / Hypervisor	(1, 2, 3, 4, 5, 6, 7, 8, 9 .. N)	95	Yellow
Physical Server	(1, 2, 3, 4, 5, 6, 7, 8, 9 .. N)	100	Green
SAN / NAS Storage	(1, 2, 3, 4, 5, 6, 7, 8, 9 .. N)	100	Green
Network	(1, 2, 3, 4, 5, 6, 7, 8, 9 .. N)	100	Green
Mobile	(1, 2, 3, 4, 5, 6, 7, 8, 9 .. N)	100	Green

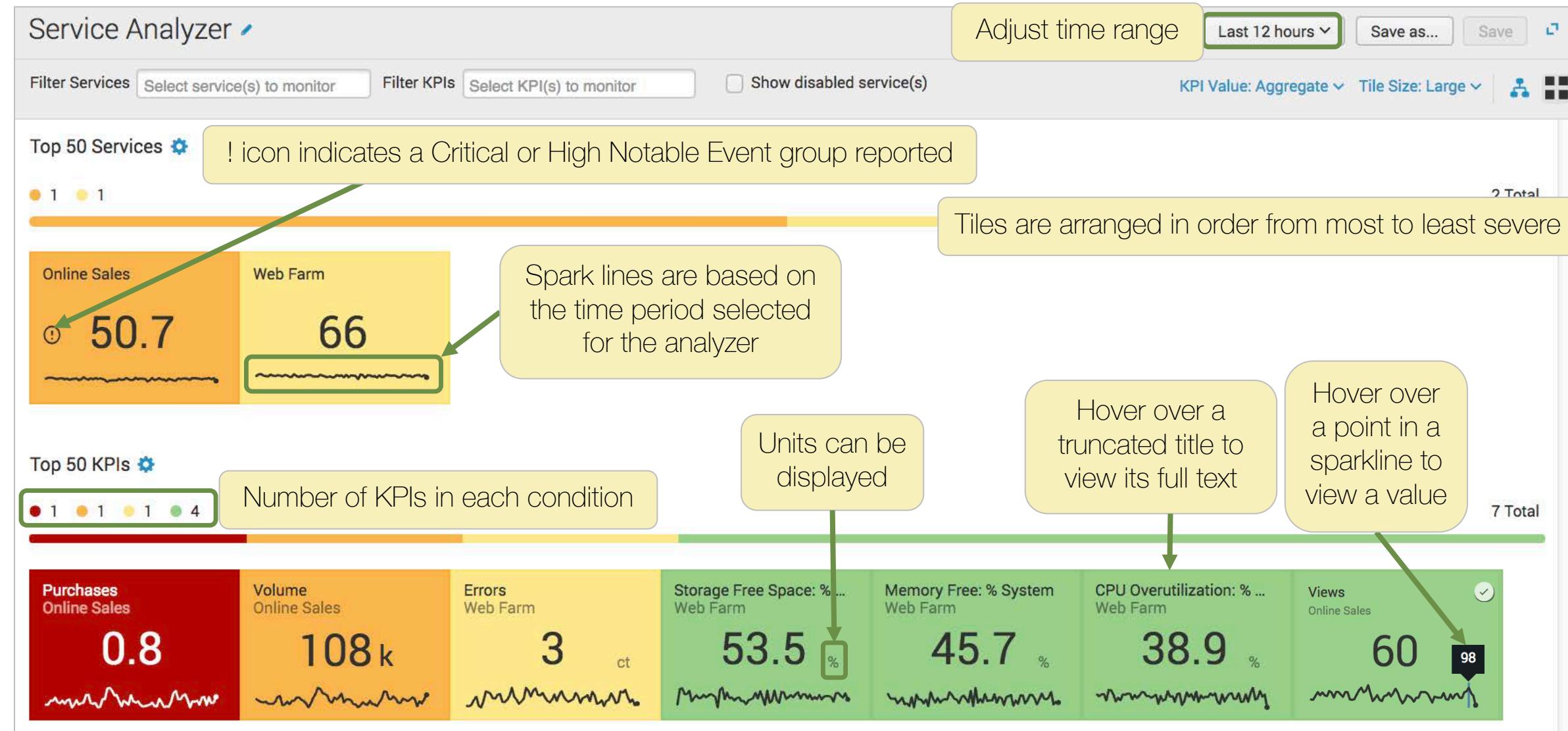
Service
Status
Outage

ITSI User Interface: Summaries to Details



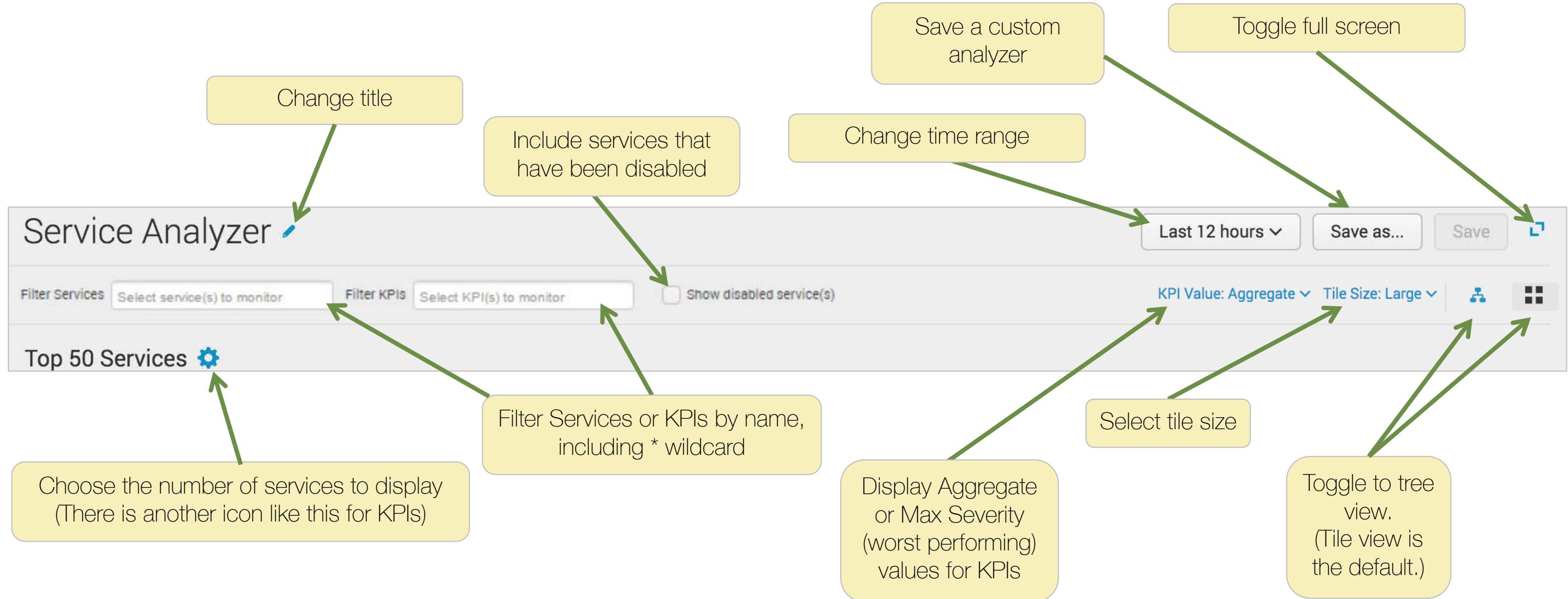
Generated for Javier Palacian (javier.palacian@tescobank.com) (C) Splunk Inc, not for distribution

Service Analyzer Display



Generated for Javier Palacian (javier.palacian@tescobank.com) (C) Splunk Inc, not for distribution

Service Analyzer Controls



Generated for Javier Palacian (javier.palacian@tescobank.com) (C) Splunk Inc, not for distribution

Click a Service Tile to Open Side Panels

Service Analyzer [Edit](#)

Last 12 hours [Save as...](#) [Save](#) [Print](#)

Filter Services [Select service\(s\) to monitor](#) Filter KPIs [Select KPI\(s\) to monitor](#) Show disabled service(s) KPI Value: Aggregate [Tile Size: Large](#)

Top 50 Services [Edit](#) 2 Total

Online Sales 1 Web Farm 1

Online Sales 50.7 Web Farm 66

Top 50 KPIs [Edit](#) 7 Total

Purchases 1 Critical Online Sales 0.9 Errors 10 ct Web Farm

Volume 111 k Online Sales Storage Free Space: % Sys... 45.7 % Web Farm

Online Sales 50.7 [X](#)

3 KPIs [Open all in Deep Dive](#)

Severity	KPI Name	Value
Critical	Purchases	0.9
Medium	Volume	111544
Normal	Views	90

Purchases 0.9 [X](#)

0 Entities

[i](#) No entities found.

1 Critical and High Event Groups [View All](#)

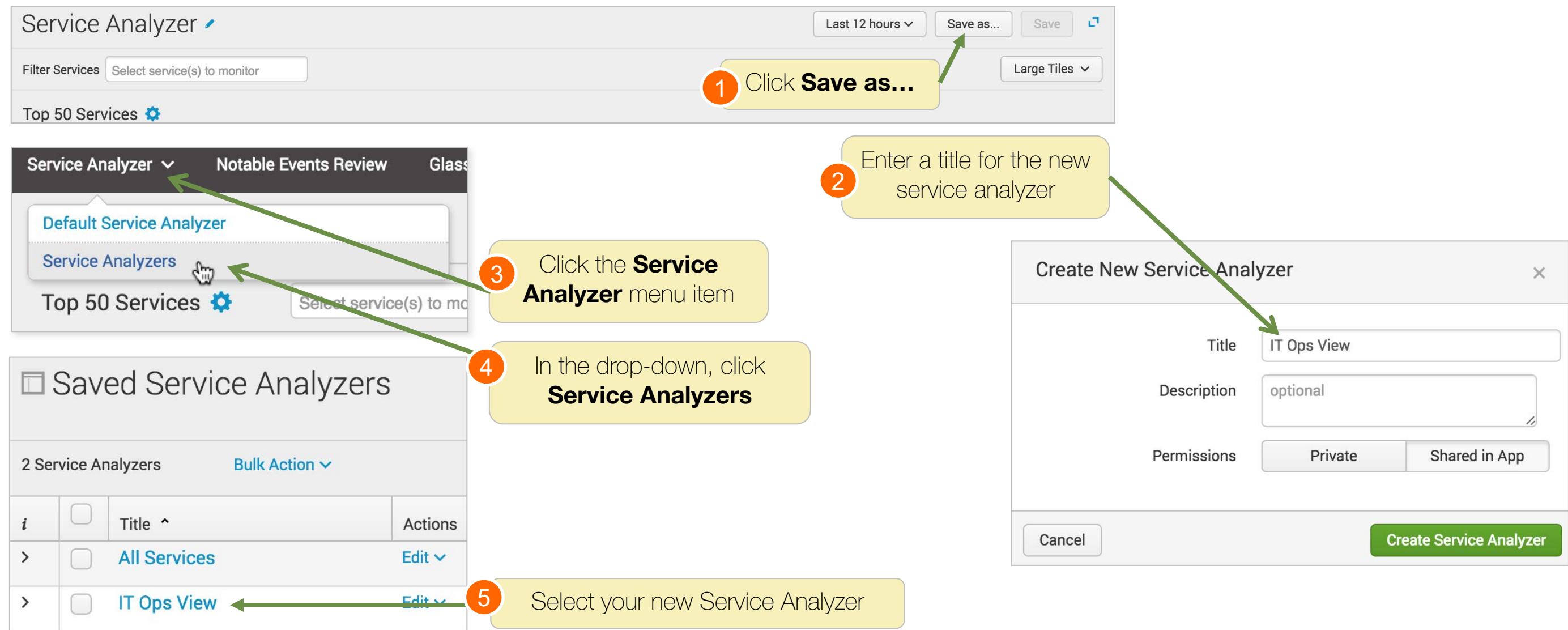
Event Count	Title	Time	Owner
1	There are only 3 servers running in the web farm	May 1 18:40:02 - May 1 18:40:02	Unassigned

The screenshot shows the Splunk Service Analyzer interface. On the left, there are two main sections: 'Top 50 Services' and 'Top 50 KPIs'. In the 'Top 50 KPIs' section, a red tile for 'Purchases' is highlighted with a green oval. A side panel is open for this tile, showing detailed KPI information: 'Purchases' (Value: 0.9, Critical), 'Volume' (Value: 111544, Medium), and 'Views' (Value: 90, Normal). Below the KPIs, there is a section for 'Event Groups' with one critical event listed: 'There are only 3 servers running in the web farm' (Event Count: 1, Time: May 1 18:40:02 - May 1 18:40:02, Owner: Unassigned).

Generated for Javier Palacian (javier.palacian@tescobank.com) (C) Splunk Inc, not for distribution

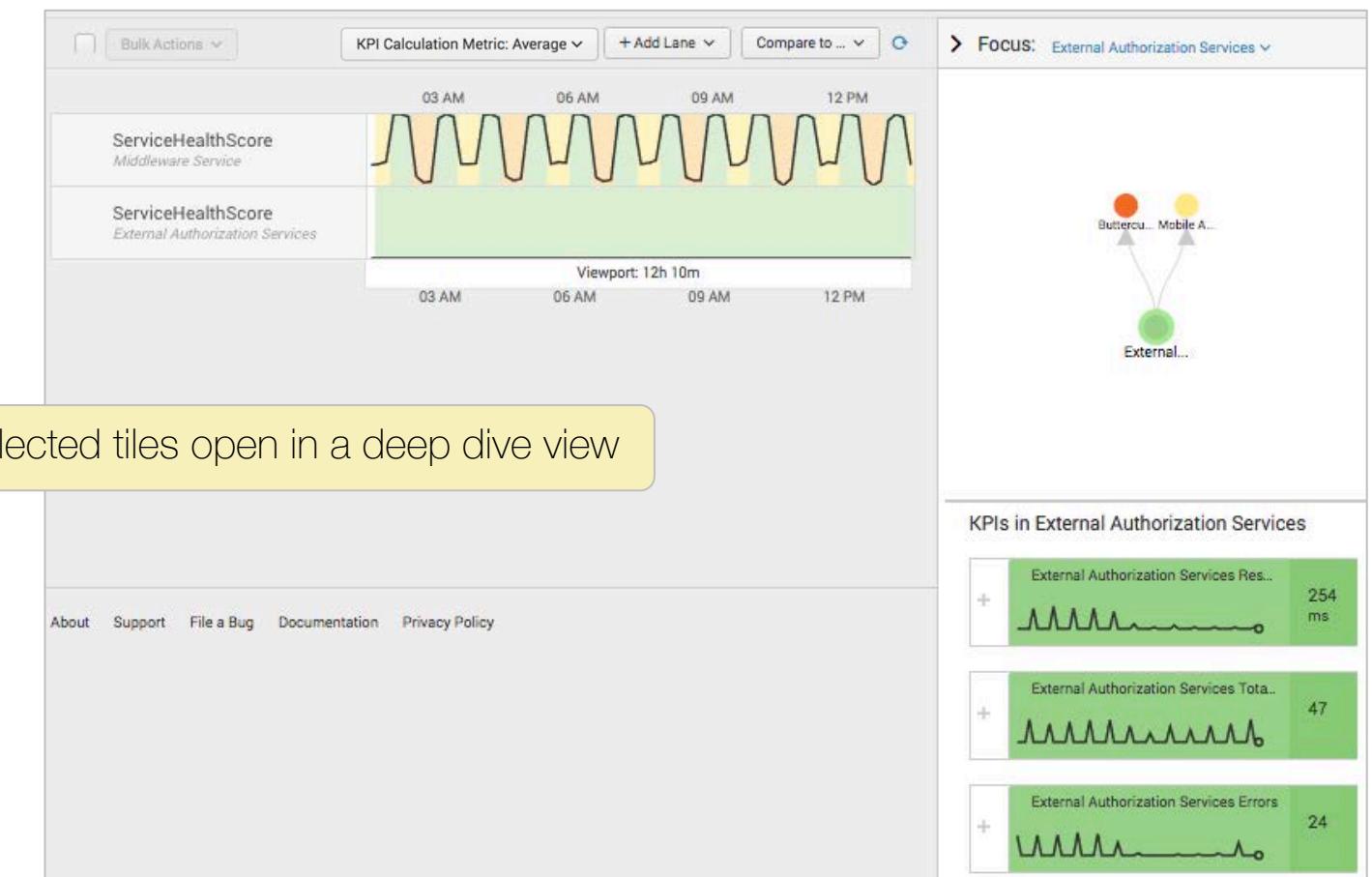
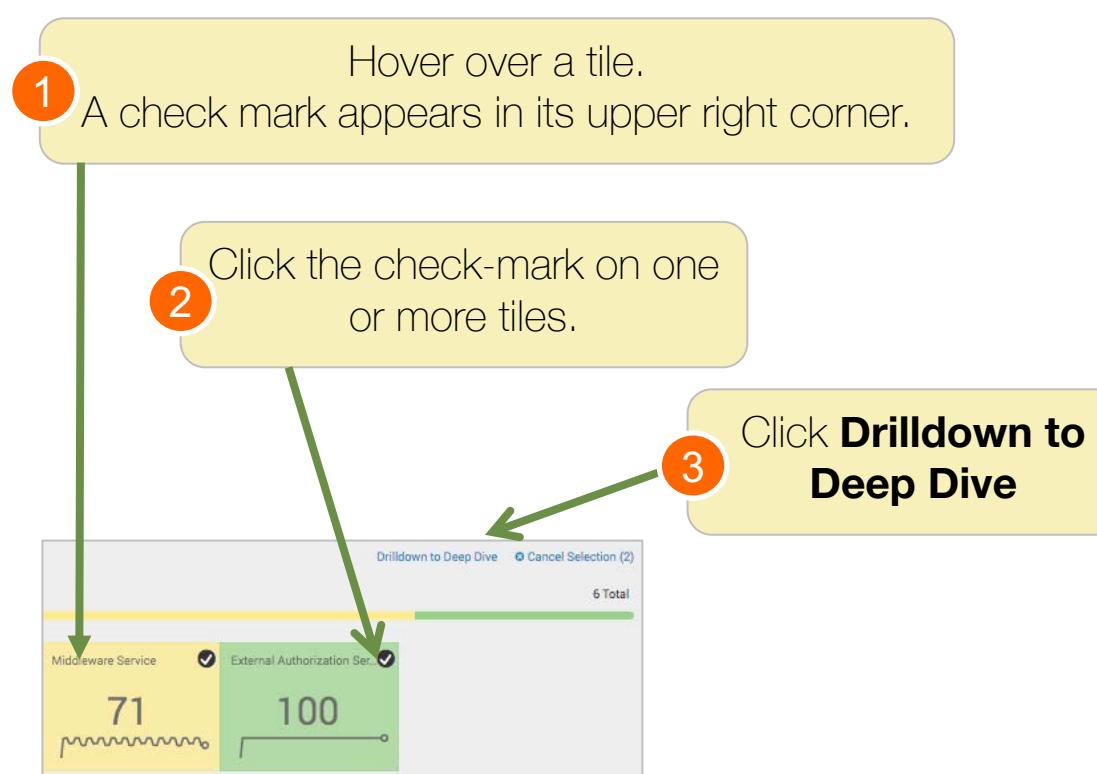
Add a Custom Service Analyzer

To save the current view and filters as a new service analyzer:



Generated for Javier Palacian (javier.palacian@tescobank.com) (C) Splunk Inc, not for distribution

KPI Drilldown to Deep Dive



Generated for Javier Palacian (javier.palacian@tescobank.com) (C) Splunk Inc, not for distribution

Service Analyzer Tree View

An exclamation point indicates a critical service

View service statuses (colors) dependencies (branches)

View KPIs and Critical and High Event Groups

Click to open all KPIs in Deep Dive, sort columns, view KPI details, or view Critical and High Event Groups in Notable Events Review

Toggle to tree view, 1

Online Sales

50

3 KPIs Open all in Deep Dive ↗

Severity	KPI Name	Value
Critical	Purchases	0.4
Normal	Views	30
Normal	Volume	74617

! 1 Critical and High Event Groups View All ↗

Event Count	Title	Time	Owner
5	There are only 3 servers running in the web farm	May 1 18:40:02 - May 1 19:00:01	Unassigned

Online Sales

50

3 KPIs Open all in Deep Dive ↗

Severity	KPI Name	Value
Critical	Purchases	0.4
Normal	Views	30
Normal	Volume	74617

! 1 Critical and High Event Groups View All ↗

Event Count	Title	Time	Owner
5	There are only 3 servers running in the web farm	May 1 18:40:02 - May 1 19:00:01	Unassigned

Web Farm

Event Count Title Time Owner

5 There are only 3 servers running in the web farm May 1 18:40:02 - May 1 19:00:01 Unassigned

27

Generated for Javier Palacian (javier.palacian@tescobank.com) (C) Splunk Inc, not for distribution

Select a Service to Display in the Panel

The screenshot shows the Service Analyzer interface. On the left, there's a tree view of services: 'Online Sales' is expanded, showing 'Web Farm' and 'Web App'. 'Web Farm' is selected and highlighted with a green border. A callout box with a green arrow points from this selection to a larger, detailed view on the right. This detailed view is titled 'Web Farm' and shows '56' as the KPI value. It includes a section for '4 KPIs' with the following data:

Severity	KPI Name	Value
Medium	Errors	7 ct
Medium	Memory Free: % System	36.67 %
Normal	CPU Overutilization: % System	48.08 %
Normal	Storage Free Space: % System	47.98 %

Below this, there's a section for 'Event Groups' stating '0 Critical and High Event Groups' and 'No event groups found.'

Generated for Javier Palacian (javier.palacian@tescobank.com) (C) Splunk Inc, not for distribution

Select a KPI to View its Entities

The screenshot shows the Splunk Service Analyzer interface. On the left, there's a navigation tree with nodes for 'Web Farm' and 'Online Sales'. The 'Web Farm' node is highlighted with a yellow circle and has a warning icon. In the main area, a 'Web Farm' KPI card is displayed, showing a value of 72. Below it, a table lists four KPIs: 'Errors' (Low severity, 3 ct), 'CPU Overutilization: % System' (Normal, 47.21 %), 'Memory Free: % System' (Normal, 42.25 %), and 'Storage Free Space: % System' (Normal, 54.35 %). To the right of this card, a green callout box contains the text: 'Click a KPI and an additional panel appears to the right displaying its entities (if any)'. An arrow points from this text to the 'Errors' row in the KPI table. A second, separate card titled 'Errors' is shown to the right, containing a table with three entities: 'www1' (Info, 2 ct), 'www2' (Info, 1 ct), and 'www3' (Info, 1 ct). The top right of the interface includes buttons for 'Last 12 hours', 'Save as...', 'Save', and a 'KPI Value: Aggregate' dropdown.

Generated for Javier Palacian (javier.palacian@tescobank.com) (C) Splunk Inc, not for distribution

ITSI Analyst Default Permissions

ANALYST PERMISSIONS	Read	Write	Delete	Execute Actions	Change Status	
Homeview	Y	Y	Y	Y	Y	
Glass Tables	Y	Y	Y			
Deep Dives	Y	Y	Y			
Deep Dive Context	Y	Y	Y			
Notable Events	Y	Y	Y			
Event Management State	Y	Y	Y			
Event Actions	Y				Y	
Event Status	Y				Y	
Event Aggregation Policies	Y					
Services	Y					
KPIs	Y					
KPI Threshold Templates	Y					
KPI Base Searches	Y					

These are analyst permissions by default.
Your company's implementation may vary.

Generated for Javier Palacian (javier.palacian@tescobank.com) (C) Splunk Inc, not for distribution

Module 1 Lab Exercise

Time: 15 minutes

Tasks:

- Log on to IT Service Intelligence
- Use the service analyzer

Module 2: Visualizing Services with Glass Tables

Generated for Javier Palacian (javier.palacian@tescobank.com) (C) Splunk Inc, not for distribution

Objectives

- Describe glass tables and their relationship to services
- Use the glass table editor to create and edit glass tables
- Use KPIs and ad-hoc searches on glass tables
- Add glass table drilldown options

Glass Tables

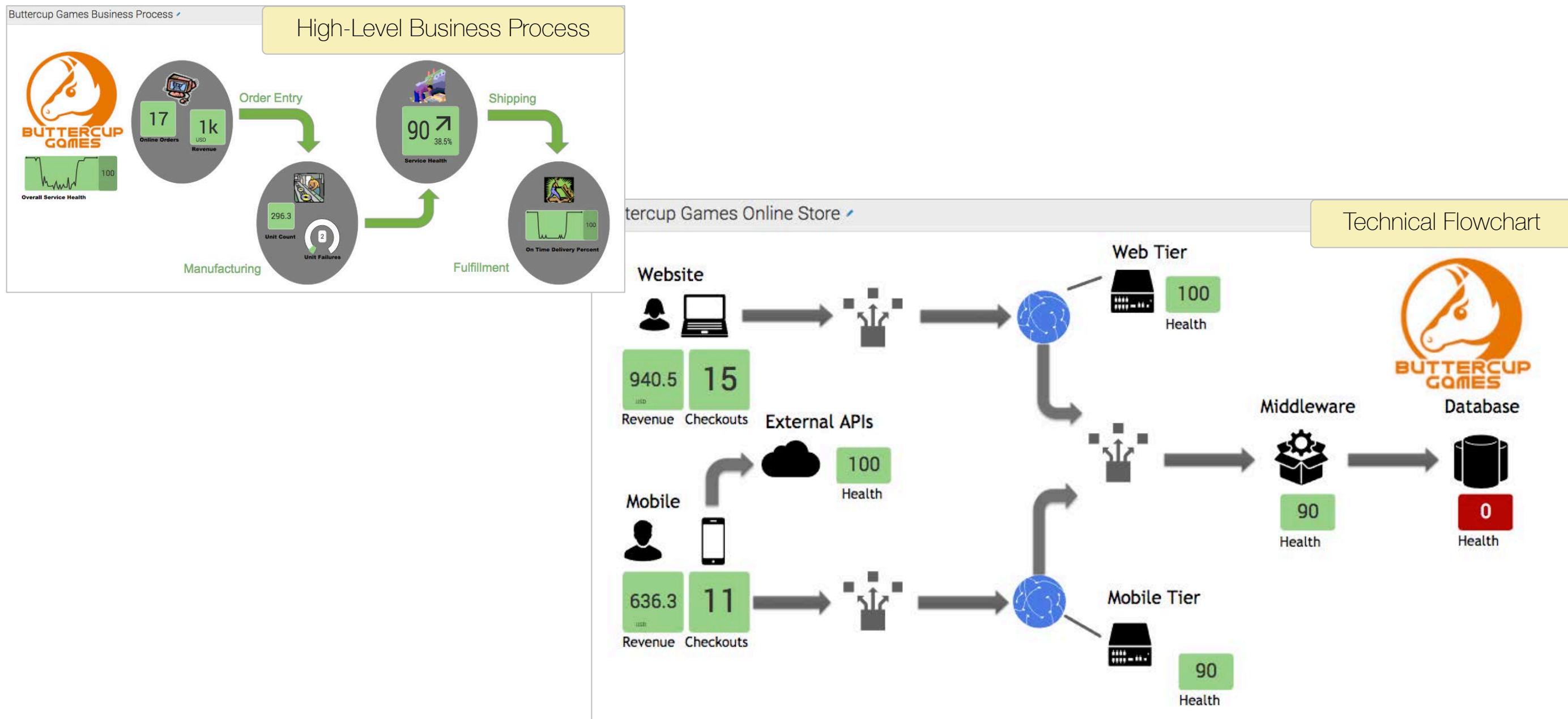
- Glass tables are visualization tools in ITSI that enable users to quickly see the status of their services in real time or at a point in time in the past
- Use the time picker to display KPI and ad-hoc values at a specific time
- Use glass tables to:
 - Create operations center dashboard displays
 - Show the status of services and entities
 - Display KPI scores in a variety of visual styles
 - Use custom icons and graphics to enhance the display

Glass Tables: Uses

- Glass tables will often be the first and most important requirements identified by users
- Many of your service design requirements will be driven by customer statements about what needs to be on the visualizations

“We need a status board that updates every minute, showing the last 5 minutes’ overall efficiency of our online sales, breaking it down by the number times a product has been viewed or bought. We also want to see the total volume of web content that our customers have seen.”

Glass Table Examples



Generated for Javier Palacian (javier.palacian@tescobank.com) (C) Splunk Inc, not for distribution

Scenario

- You are adding a glass table for two teams in your company
- They want to use IT Service Intelligence to monitor their operations:
 - Sales operations team wants to be able to see what's happening in the online sales website
 - IT team needs to be alerted to problems with the web servers and systems related to purchase transactions
- Your initial focus is to create a glass table based on the sales and IT team's requirements (find applicable KPIs that are available and determine any ad hoc searches you may need to supplement the KPIs)

Generated for Javier Palacian (javier.palacian@tescobank.com) (C) Splunk Inc, not for distribution

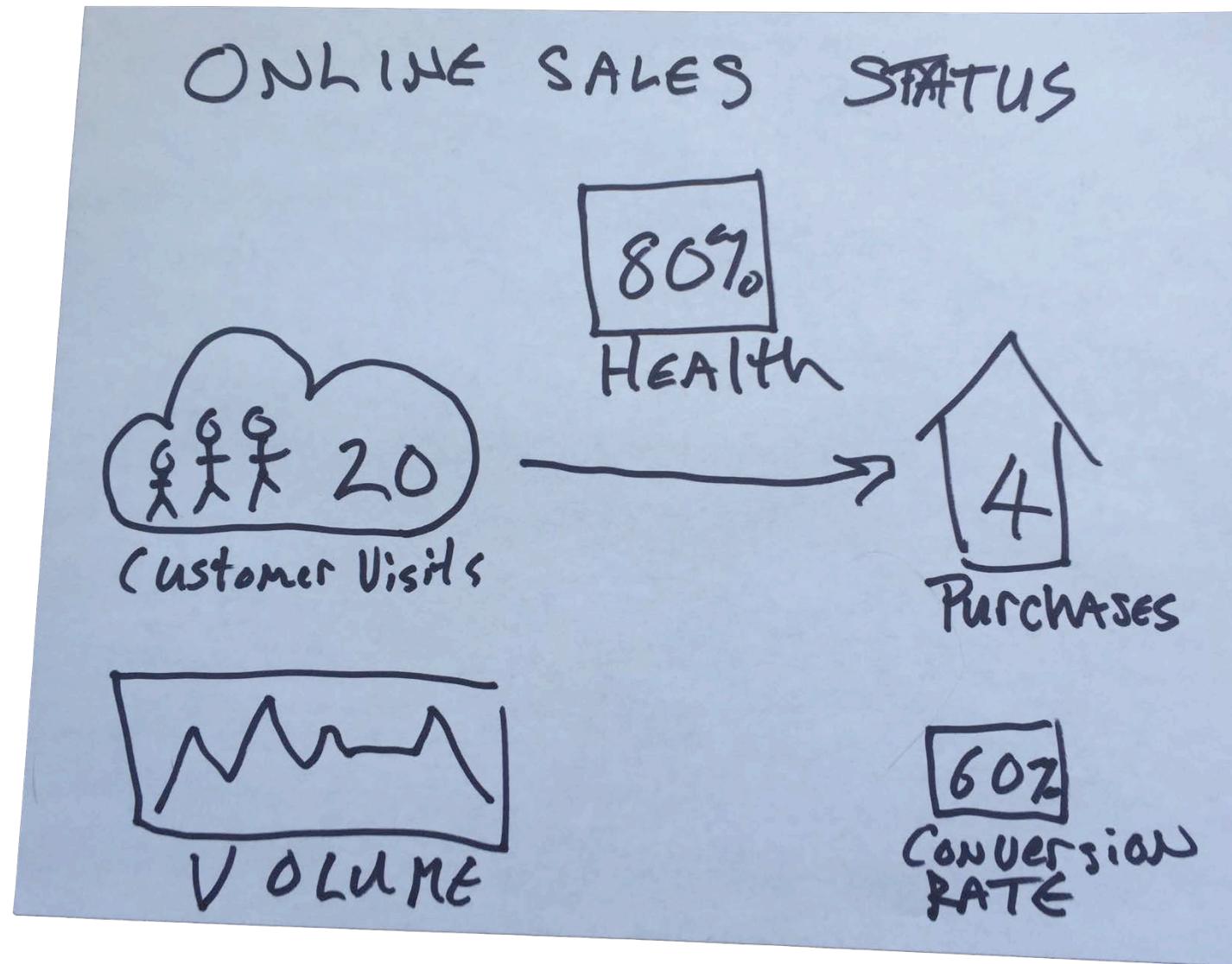
Interview with Sales Operations

“We want a status board that updates every minute shows the last 15 minutes’ overall efficiency of our online sales, broken down by the number of times a product has been viewed or bought, and the total volume of web content our customers viewed.”



Generated for Javier Palacian (javier.palacian@tescobank.com) (C) Splunk Inc, not for distribution

Whiteboard



"This is what we want the status board to look like."

Generated for Javier Palacian (javier.palacian@tescobank.com) (C) Splunk Inc, not for distribution

Interview with the IT Team

“The most important thing for us is our website health. How many errors are being generated? What is the usage of CPUs, memory and disk space per machine? We'd like to see this update every minute and show the last 15 minutes' data. And we want to be alerted if the number of servers in the web farm falls below our service level.”



Generated for Javier Palacian (javier.palacian@tescobank.com) (C) Splunk Inc, not for distribution

Who in IT uses ITSI as an Analyst?

- Tier 1 Operations Analysts – Basic troubleshooting and routing issues to appropriate team
 - Monitors ITSI dashboards created by Tier 3 Analysts/Tools Engineers
- Tier 2 Operations Analysts – Manages and monitors internal tools and applications. Gathers and shares best practices with Tier 1
 - Uses ITSI dashboards, glass tables and deep dives
- Tier 3 Operations Analysts and Tools Engineers – Subject matter experts to whom the tough problems get escalated
 - In ITSI, use all of the above plus service analyzer and notable events
 - Build ITSI tools and automate workflows for coworkers to use

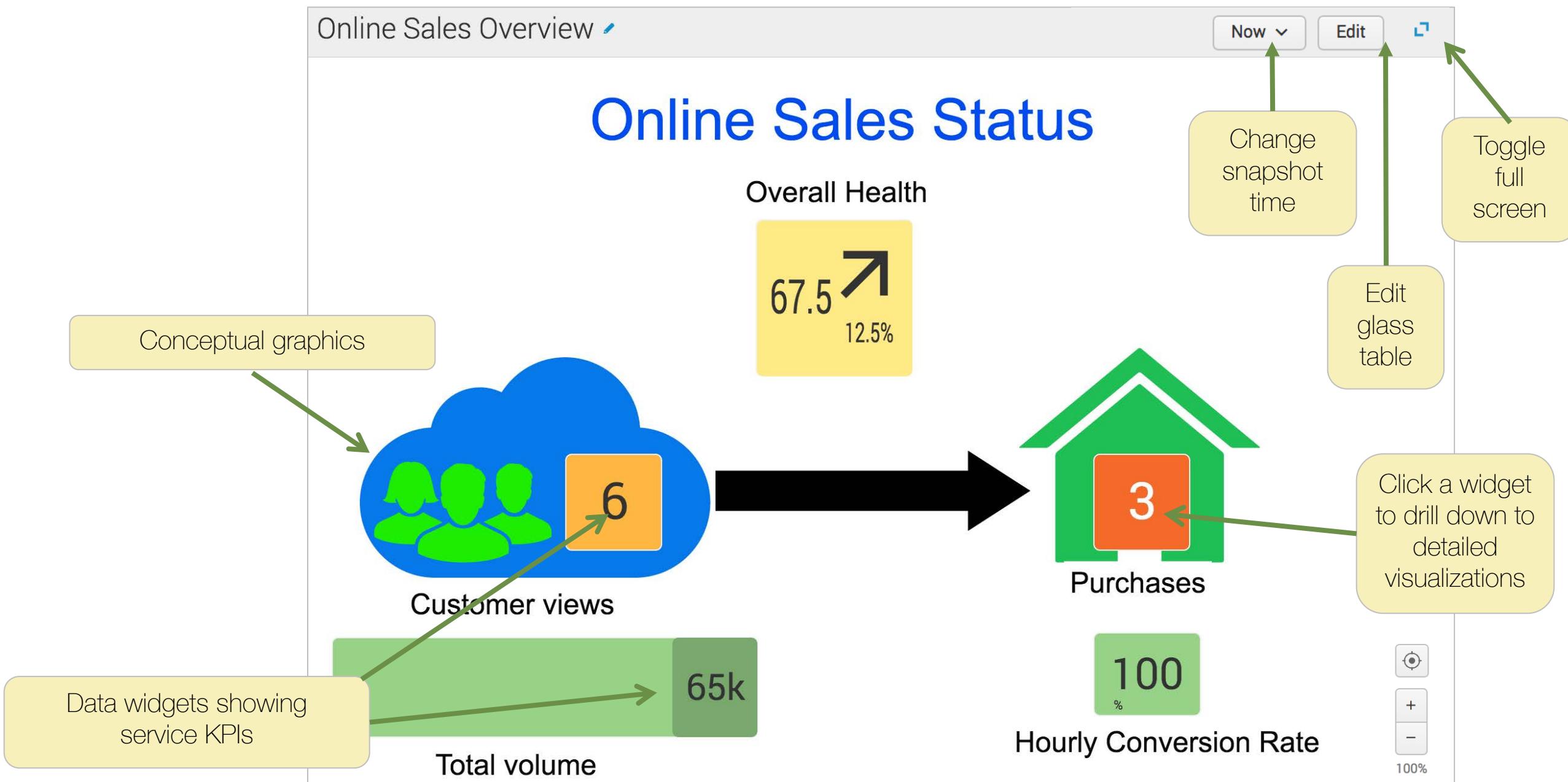
Splunk at Buttercup Games

- Tier 2 Operations Analysts are likely to build glass tables based on KPIs that an admin implemented
- Examine your Service Analyzer to determine the health scores and KPIs your admin has made available
- You may need to build some ad-hoc metrics in addition

Designing Glass Tables

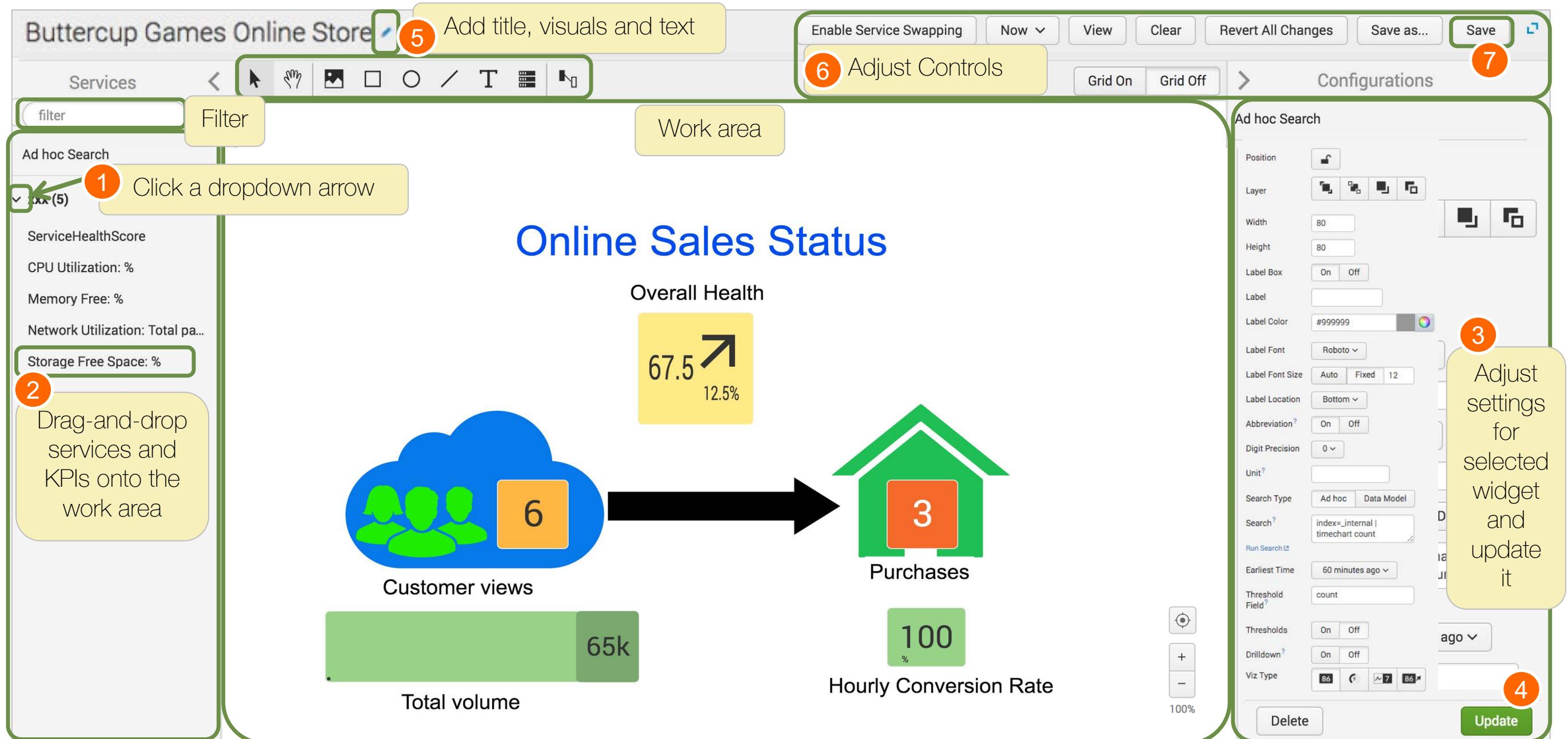
- Determine which views are needed at the site based on workflow, operations center display requirements, etc.
- Plan the visualization ahead of time
 - Use site graphics and icons if possible to enhance conceptual understanding
- Examine existing documentation for design elements
- Flow charts, schematics, overview diagrams, etc.
- Plan the overall structure of the visualization and identify required KPIs or ad-hoc searches

Glass Table: Normal View



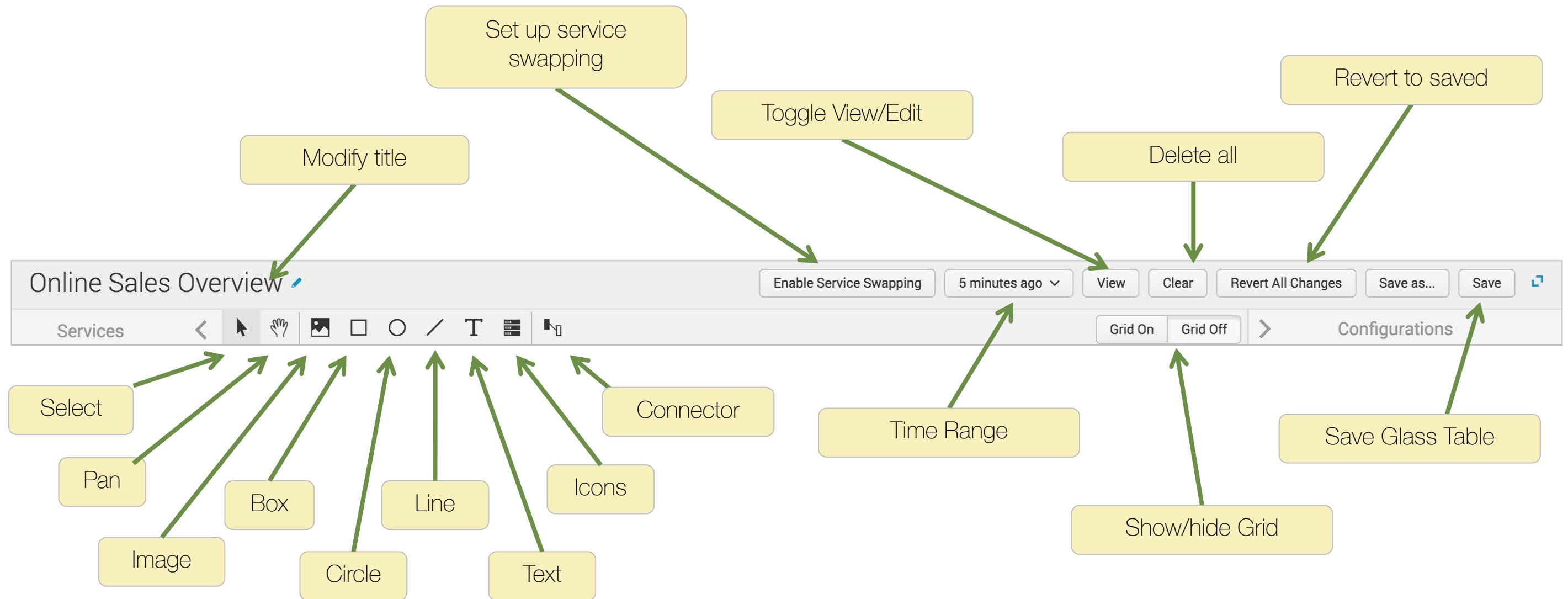
Generated for Javier Palacian (javier.palacian@tescobank.com) (C) Splunk Inc, not for distribution

Building the Glass Table



Generated for Javier Palacian (javier.palacian@tescobank.com) (C) Splunk Inc, not for distribution

Top Bar Controls



Generated for Javier Palacian (javier.palacian@tescobank.com) (C) Splunk Inc, not for distribution

Creating a Glass Table: 1

1 From the menu bar, click **Glass Tables**

2 Click **Create New Glass Table**

#	Title	Actions	Owner	App	Sharing
1	1 - Executive Dashboard	Edit	admin	itsi	App
2	2 - Digital Channels	Edit	admin	itsi	App
3	3 - Operational Status	Edit	admin	itsi	App
4	4 - Digital Transaction	Edit	admin	itsi	App
5	Buttercup Games Business	Edit	admin	itsi	App
6	Buttercup Games Business	Edit	admin	itsi	App
7	Buttercup Games Sales Status	Edit	admin	itsi	App

Generated for Javier Palacian (javier.palacian@tescobank.com) (C) Splunk Inc, not for distribution

Creating a Glass Table: 2

The screenshot shows the Splunk IT Service Intelligence interface for creating a glass table. The main title is "Online Sales Overview".

Step 1: Click dropdown arrows, then drag-and-drop to add KPIs and ad-hoc searches to the glass table.

Step 2: Add conceptual graphics and lay out overall visual structure.

Step 3: Edit widget properties. Set label and threshold values as needed.

Step 4: Click Update.

KPIs and Widgets:

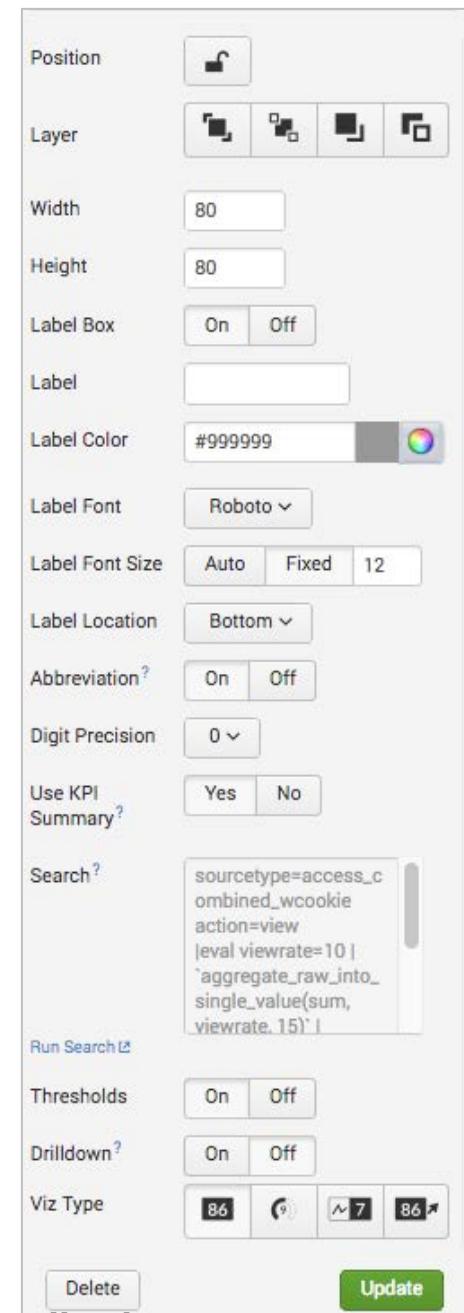
- Overall Health:** Value 51, -19.4% (Orange square)
- Total Volume:** Line chart showing 120k (Orange bar)
- Customer Views:** Cloud icon with 70 (Green square)
- Purchases:** Red house icon with 1
- Hourly Conversion Rate:** Red circle with 100

Bottom Text: As needed, center your glass table on the screen, or zoom in and out

Generated for Javier Palacian (javier.palacian@tescobank.com) (C) Splunk Inc, not for distribution

Configuration Bar: KPIs

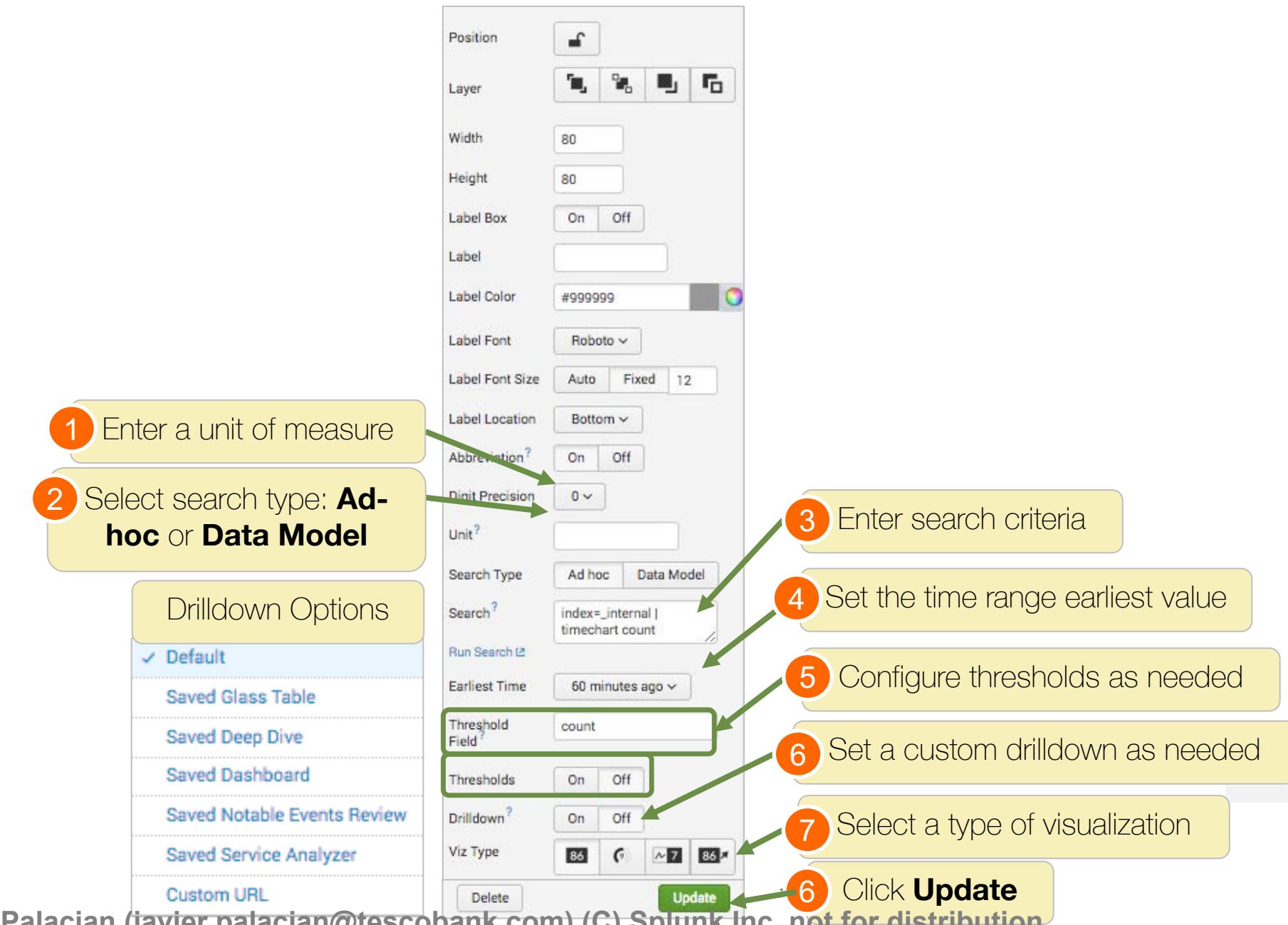
- KPI widgets have additional controls:
 - Width and Height
 - Label controls
 - Search information
 - Threshold on/off
 - Custom drilldown
 - Visualization type
- Use the **Update** button to refresh the glass table with any changes you make to a widget before selecting a different widget



Generated for Javier Palacian (javier.palacian@tescobank.com) (C) Splunk Inc, not for distribution

Configuration Bar: Ad hoc Search Widget

- You can add an ad-hoc search and use a widget to display the result.
- Scroll down under **Configurations** to specify the settings shown here.

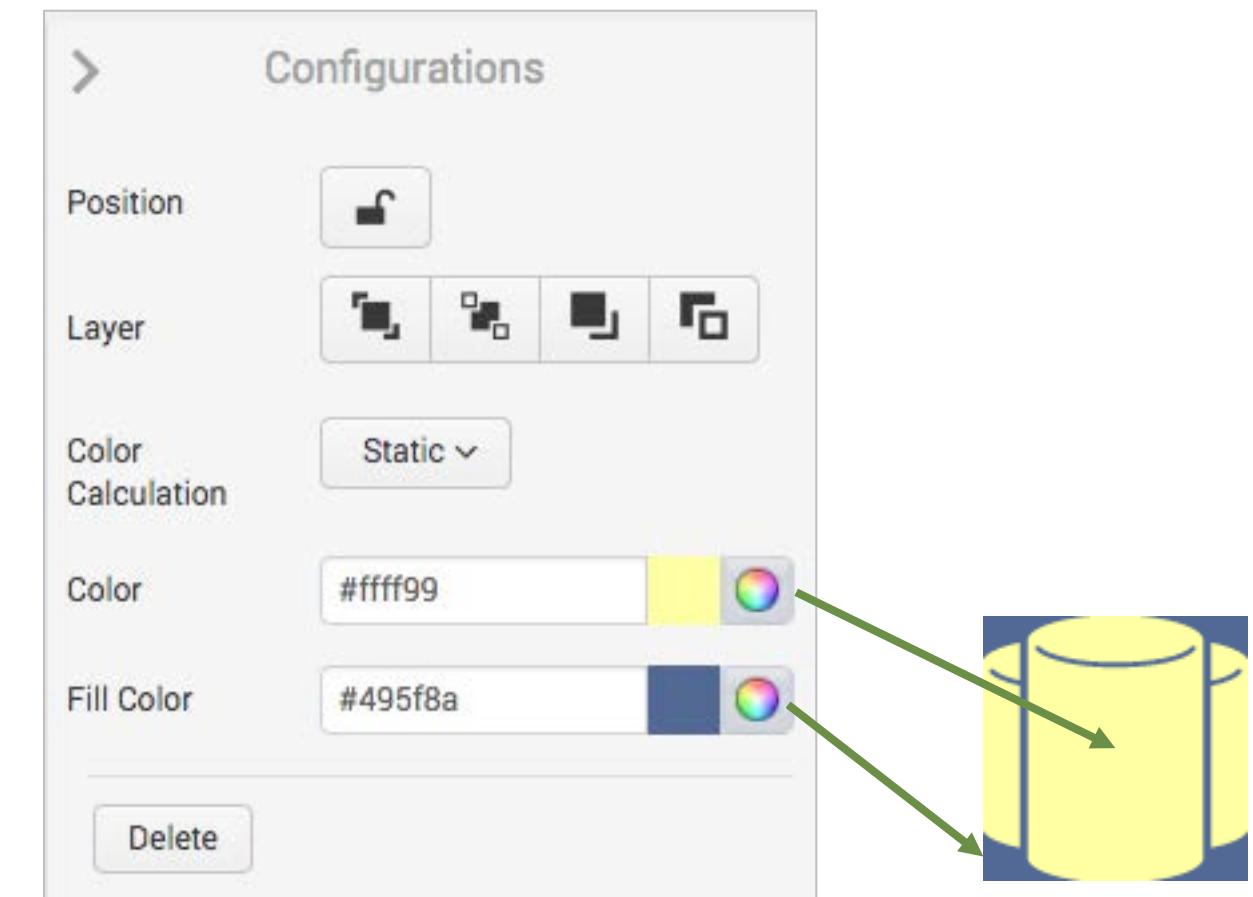


Generated for Javier Palacian (javier.palacian@tescobank.com) (C) Splunk Inc, not for distribution

Configuration Bar: General

Most widgets have controls for:

- Position locking
- Layer control (bring forward/back)
- Color Calculation (set the color to change when data crosses preset or custom thresholds)
- Color (object or fore color)
- Fill color (background color and object outline)
- Deletion (or, use the <delete> key)



Generated for Javier Palacian (javier.palacian@tescobank.com) (C) Splunk Inc, not for distribution

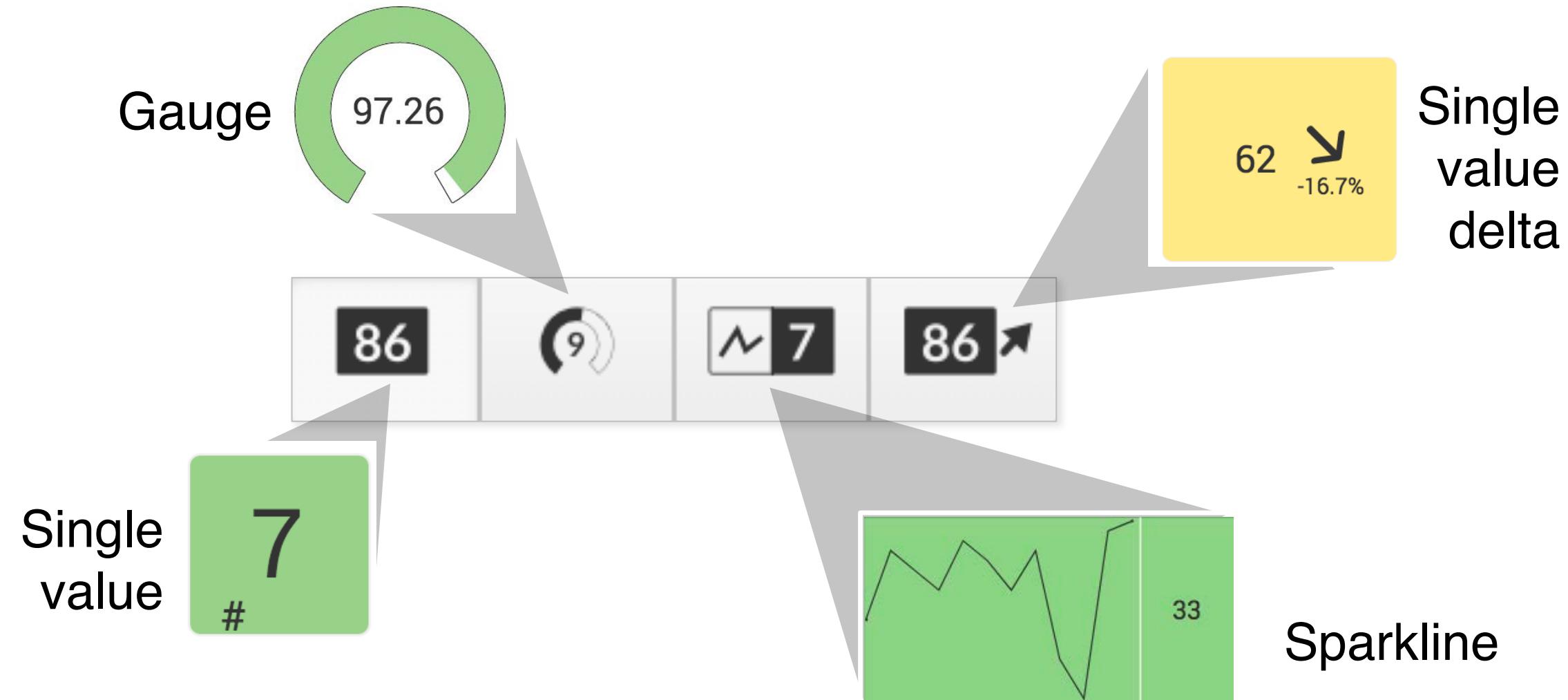
Use Shapes or Icons as Widgets

The diagram illustrates the configuration steps for using shapes or icons as widgets in Splunk. It consists of three main sections:

- Top Left:** Shows the "Configurations" screen with the "Color Calculation" dropdown set to "Static". A callout (1) points to the "Color Calculation" dropdown with the text: "Click the **Color Calculation** dropdown to set shapes or icons to change color based on thresholds for field values". A callout (2) points to the "Ad hoc Search" button with the text: "Select Ad hoc Search or KPI". A callout (3) points to the "KPI" section with the text: "For KPI, select a Service and a KPI. Thresholds already established for the KPI will be used."
- Middle Left:** Shows the "Color Calculation" configuration screen for "Ad hoc Search". It includes fields for "Fill Color" (none), "Width" (283), "Height" (177.8), "Label Box" (On), "Label" (empty), "Label Color" (gray), "Label Font" (empty), "Label Font Size" (empty), "Label Location" (empty), "Search Type" (Ad hoc Search), "Search" (index=_internal | timechart count), "Run Search" (Run Search), "Threshold Field" (count), "Thresholds" (On), "Edit" (button), and "Drilldown" (On). A callout (3) points to the "Search" field with the text: "Ad hoc search: set the search and thresholds yourself".
- Bottom Right:** Shows the "Color Calculation" configuration screen for "KPI". It includes fields for "Service" (Online Sales), "KPI" (ServiceHealthSc...), "Fill Color" (none), and "Drilldown" (On). A callout (4) points to the "Drilldown" button with the text: "Set the drilldown behavior". A callout (5) points to the "Update" button with the text: "Click Update".

Generated for Javier Palacian (javier.palacian@tescobank.com) (C) Splunk Inc, not for distribution

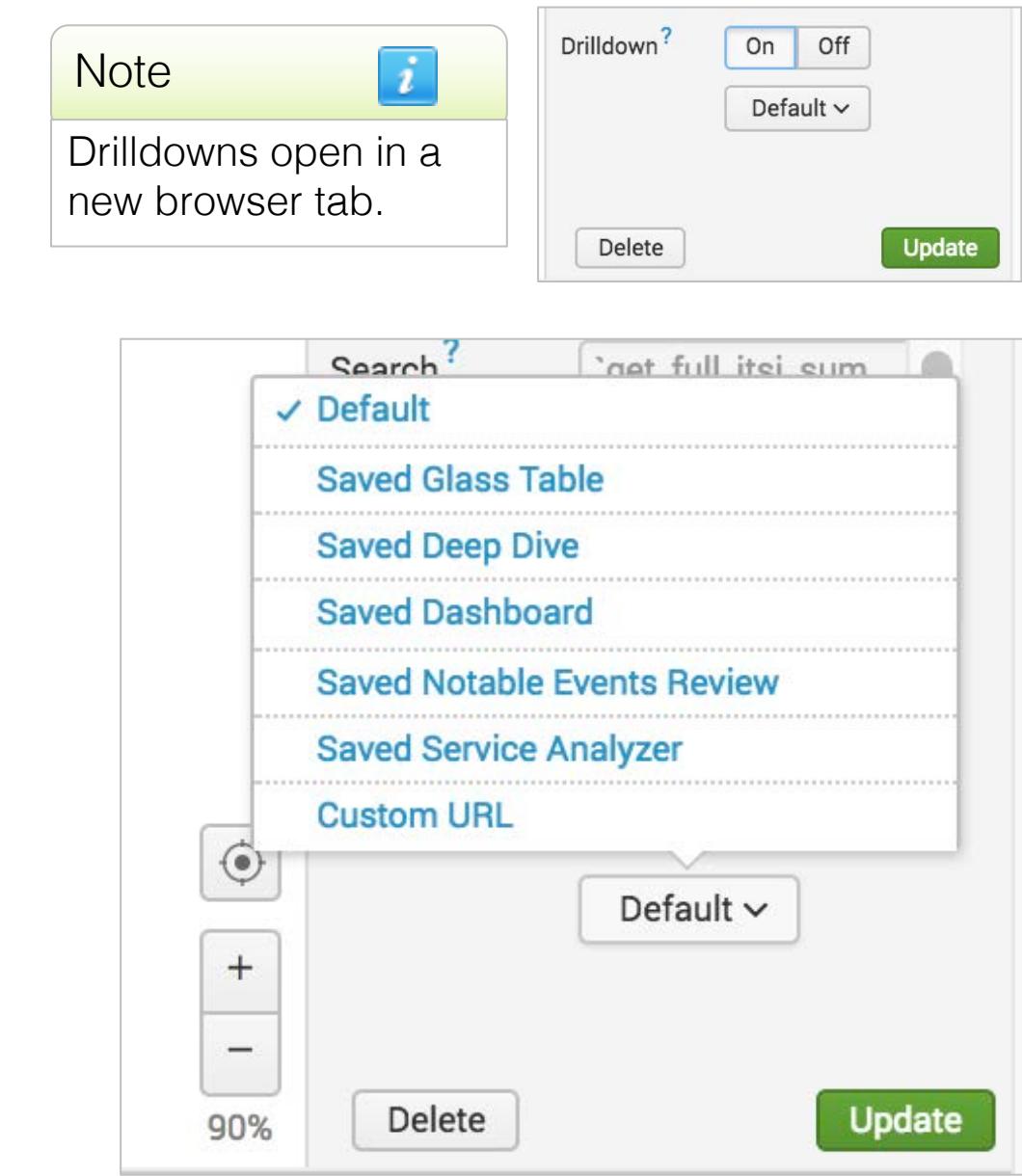
Widget Visualization Types



Generated for Javier Palacian (javier.palacian@tescobank.com) (C) Splunk Inc, not for distribution

Glass Table Drilldown

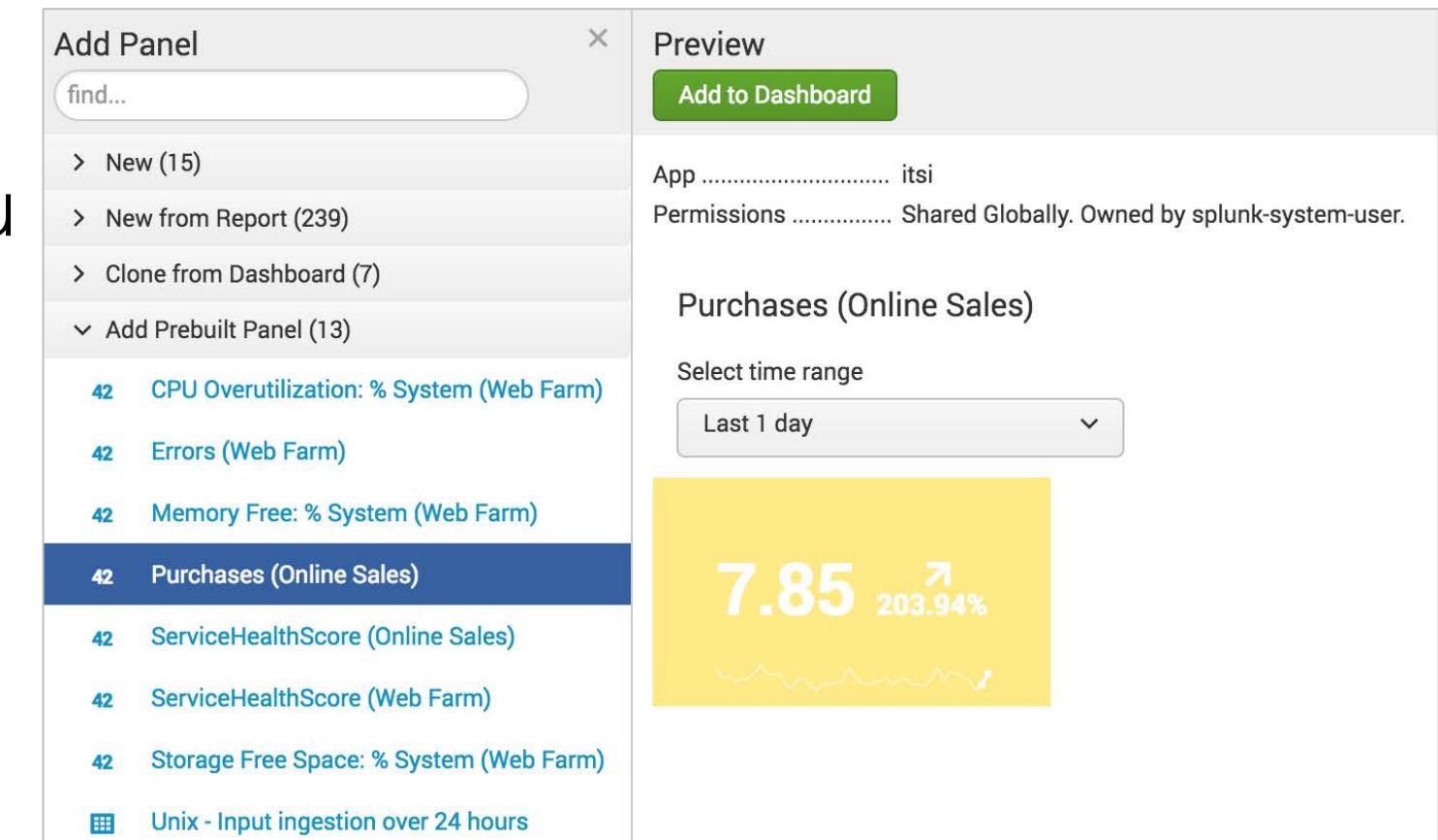
- By default, drilldown is set to off
- You can enable various drilldowns:
 - Default: opens all KPIs for the service in a deep dive
 - A saved Glass Table, Deep Dive, Notable Events Review or Service Analyzer
 - A Splunk dashboard
 - A custom URL
- The default drilldown for an ad-hoc widget is a Deep Dive with a metric lane based on the widget search



Generated for Javier Palacian (javier.palacian@tescobank.com) (C) Splunk Inc, not for distribution

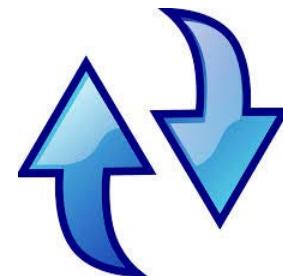
KPIs on Custom Dashboards

- When a KPI is created, a pre-built dashboard panel object is automatically created
 - When editing dashboards, you can add a KPI by selecting **Add Panel** and searching for your KPI in the **Add Prebuilt Panel** list
 - It will be added as a single-value display widget



Service Swapping

- If the KPIs on your glass table are shared by more than one service, you can enable **service swapping**



Edit Service Swapping

3 services (2 selected) 10 per page ▾

	Title ▾	KPIs ▾
<input checked="" type="checkbox"/>	Ecomm	5
<input type="checkbox"/>	Online Sales	4
<input checked="" type="checkbox"/>	Web Farm	5

- A single glass table can toggle its view from displaying the KPI values of one service to displaying the KPI values of another service.

Ecomm ▾ Now ▾ Edit

✓ Ecomm
Web Farm

Generated for Javier Palacian (javier.palacian@tescobank.com) (C) Splunk Inc, not for distribution

Module 2 Lab Exercise

Time: 30 minutes

Task:

Create a new glass table to monitor Online Sales

Generated for Javier Palacian (javier.palacian@tescobank.com) (C) Splunk Inc, not for distribution

Module 3: Managing Notable Events

Generated for Javier Palacian (javier.palacian@tescobank.com) (C) Splunk Inc, not for distribution

Objectives

- Describe key terms (notable events, correlation searches, and multi KPI alerts, anomaly detection, etc.)
- Describe notable event workflow
- Configure notable event options
- Define new correlation searches

Notable Events

- A notable event is generated as an alert action by
 - Correlation searches
 - Multi KPI alerts
 - Anomaly detection
- Notable events indicate an issue or problem that needs attention
- The notable events review dashboard is a service-oriented event console
- Each notable event is similar to a ticket in a tracking system



Generated for Javier Palacian (javier.palacian@tescobank.com) (C) Splunk Inc, not for distribution

Correlation Searches

- Correlation searches run on a schedule and create notable events when they detect an issue
- Events generated by a correlation search are automatically associated with their respective services, which are displayed under “Possible Affected Services” after clicking the notable event
- ITSI admins can set up correlation searches for you as needed, to create notable events that identify unexpected or unwanted conditions
- Both **itoa_admin** and **itoa_analyst** members can own and modify notable events

Notable Event Management Concepts

- Use each notable event as a “ticket” to track the status of the work being done to correct the issue
- Initial notable events are in **new** status and are not owned
- An analyst will take ownership of the notable event, change its status as the status of work changes, and eventually close it
- The owning analyst can also change the severity if needed, and add comments to document the work
- Notable event generation can be integrated with external ticketing systems

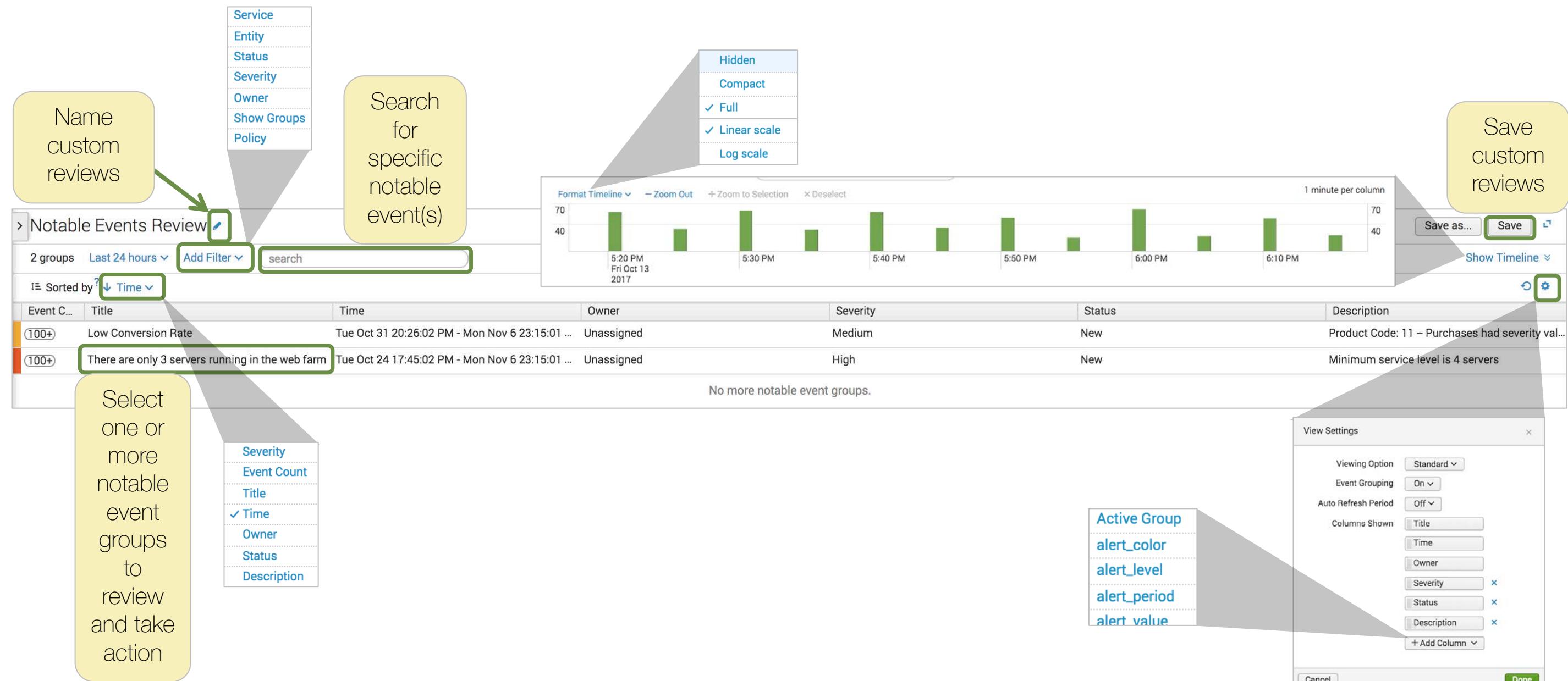


Generated for Javier Palacian (javier.palacian@tescobank.com) (C) Splunk Inc, not for distribution

Notable Event Analyst Workflow

1. Select and filter events
2. Acknowledge a group of events
3. Update status
4. Add comments
5. Use actions – view, search, ping, etc.
6. Ungroup events and work an individual event
7. Define custom views

Notable Events Review: Default View



Generated for Javier Palacian (javier.palacian@tescobank.com) (C) Splunk Inc, not for distribution

Notable Events View Settings

The screenshot shows the Splunk Notable Events view for the 'Middleware Service' search. The interface includes a header with search filters (Last 60 minutes, Service: Middleware Servi..., Severity: All), a toolbar with Save as... and Save buttons, and a main table showing event details like Title, Time, Owner, Severity, Status, and Description.

Annotations:

- Change View settings (1):** A callout points to the gear icon in the top right corner of the main view area.
- View Settings (2):** A callout points to the 'View Settings' button in the 'Event Grouping' section of the modal.
- Click and drag to reorder columns:** A callout points to the column headers in the main table.
- Remove a column:** A callout points to the 'X' button in the 'Columns Shown' dropdown of the View Settings modal.
- Add a column:** A callout points to the '+ Add Column' button in the 'Add a column' section of the View Settings modal.
- Done (3):** A callout points to the 'Done' button in the 'Add a column' section of the View Settings modal.
- Prominent View:** A callout points to the 'Prominent View' section, which highlights recent events.
- Standard View:** A callout points to the 'Standard View' section, which shows a list of events.
- Grouped:** A callout points to the 'Grouped' section, which shows events grouped by title.
- Ungrouped:** A callout points to the 'Ungrouped' section, which shows events listed individually.
- Auto Refresh:** A callout points to the 'Auto Refresh' section of the View Settings modal, which includes options for Off, 1 Min, 5 Min, 30 Min, 60 Min, and 24 Hours.

Generated for Javier Palacian (javier.palacian@tescobank.com) (C) Splunk Inc, not for distribution

Selecting Notable Event(s)

Notable Events Review

Time range, search, filter/view settings, full screen toggle

Save as... Save

357 events Last 24 hours Add Filter search

Sorted by? Time

Notable event list, color-coded severity on left

Severity	Description	Date
Medium	Errors Impacting Revenue	Tue May 2 2017 16:25:03 GMT+0000 (UTC)
High	Response Times Impacting Active U...	Tue May 2 2017 16:00:04 GMT+0000 (UTC)
Medium	Errors Impacting Revenue	Tue May 2 2017 15:55:03 GMT+0000 (UTC)
High	Response Times Impacting Active U...	Tue May 2 2017 15:55:03 GMT+0000 (UTC)
Medium	Errors Impacting Revenue	Tue May 2 2017 15:55:03 GMT+0000 (UTC)
Medium	Errors Impacting Revenue	Tue May 2 2017 15:50:04 GMT+0000 (UTC)
High	Response Times Impacting Active U...	Tue May 2 2017 15:50:03 GMT+0000 (UTC)
High	Response Times Impacting Active U...	Tue May 2 2017 15:45:04 GMT+0000 (UTC)
Medium	Errors Impacting Revenue	Tue May 2 2017 15:45:04 GMT+0000 (UTC)

Acknowledge

High New Unassigned Actions

Response Times Impacting Active Users

Tue May 2 2017 16:00:04 GMT+0000 (UTC)

Overview Comments Activity

Description

Response Times and Active Users status was high (Health Score=33.33) at 2017-05-02 15:50:00.000 PM

Contributing KPIs Open all in Deep Dive

- Active Users
- Response Times
- Average Transaction Response Time

Possible Affected Services Open all in Deep Dive

- Buttercup Store
- Web Service
- Middleware Service

Events generated by a correlation search are automatically associated with their respective services and KPIs, which are displayed under Contributing KPIs and Possible Affected Services

Drilldowns

None

Details

alert_value: 33.33
status: 1
composite_kpi_id: Response Times and Active Users
composite_kpi_name: Response Times and Active Users
mod_time: 1493740804.57

Generated for Javier Palacian (javier.palacian@tescobank.com) (C) Splunk Inc, not for distribution

Notable Events Filter Settings

The screenshot shows the Splunk Notable Events interface. At the top, there are five yellow callout boxes with the following text:

- Change Time filter
- Remove Status filters
- Update or add Severity filters
- Add a filter
- Search by keywords or field = value

Below the callouts, the filter bar includes:

- 2 groups
- Last 24 hours
- Status: New
- Severity: High, Medi...
- Add Filter
- search
- Show Timeline

The event list table has columns: Event C..., Title, Time, Owner, Service, Entity, Owner, Severity, Status, Description. Two events are listed:

Event C...	Title	Time	Owner	Service	Entity	Owner	Severity	Status	Description
(100+)	Low Conversion Rate	Tue Oct 31 20:26:02 PM - Tu...	Unassigned	Show Groups			Medium	New	Product Code: 11 -- Purchase...
(100+)	There are only 3 servers runn...	Tue Oct 24 17:45:02 PM - Tu...	Unassigned	Policy			High	New	Minimum service level is 4 s...

Generated for Javier Palacian (javier.palacian@tescobank.com) (C) Splunk Inc, not for distribution

Acknowledging a Notable Event

Notable Events Review 

357 events Last 24 hours Add Filter search

Sorted by? Time

Errors Impacting Revenue	Tue May 2 2017 16:25:	
Severity: Medium	Status: New	Description: Errors an...

Response Times Impacting Active U...	Tue May 2 2017 16:00:04 GMT+0000 (UTC)	
Severity: High	Status: New	Description: Response Times and Active Users status was high (H...

Errors Impacting Revenue	Tue May 2 2017 16:00:04 GMT+0000 (UTC)	
Severity: Medium	Status: New	Description: Errors and Revenue status was medium (Health S...

Response Times Impacting Active U...	Tue May 2 2017 15:55:03 GMT+0000 (UTC)	
Severity: High	Status: New	Description: Response Times and Active Users status was high (H...

Errors Impacting Revenue	Tue May 2 2017 15:55:03 GMT+0000 (UTC)	
Severity: Medium	Status: New	Description: Errors and Revenue status was medium (Health S...

Errors Impacting Revenue	Tue May 2 2017 15:50:04 GMT+0000 (UTC)	
Severity: Medium	Status: New	Description: Errors and Revenue status was critical (Health Sc...

Response Times Impacting Active U...	Tue May 2 2017 15:50:03 GMT+0000 (UTC)	
Severity: High	Status: New	Description: Response Times and Active Users status was critical...

Response Times Impacting Active U...	Tue May 2 2017 15:45:04 GMT+0000 (UTC)	
Severity: High	Status: New	Description: Response Times and Active Users status was critical...

Errors Impacting Revenue	Tue May 2 2017 15:45:04 GMT+0000 (UTC)	
Severity: Medium	Status: New	Description: Errors and Revenue status was critical (Health Sc...

Save as... Save 

Show Timeline

Acknowledge 

High New Unassigned Actions X

Response Times Impacting Active Users
Tue May 2 2017 16:00:04 GMT+0000 (UTC)

Overview Comments Activity

Description
Response Times and Active Users status was high (Health Score=33.33) at 2017-05-02 15:50:00.000 PM

Contributing KPIs [Open all in Deep Dive](#)

- Active Users
- Response Times
- Average Transaction Response Time

Possible Affected Services [Open all in Deep Dive](#)

- Buttercup Store
- Web Service
- Middleware Service

Drilldowns
None

Details
alert_value: 33.33
status: 1
composite_kpi_id: Response Times and Active Users
composite_kpi_name: Response Times and Active Users
mod_time: 1493740804.57

Generated for Javier Palacian (javier.palacian@tescobank.com) (C) Splunk Inc, not for distribution

Updating a Notable Event

1. Select a notable event
2. Change the status, owner, and optionally the severity
3. Open the **Comments** tab and add comments as needed

The screenshot shows a Splunk Notable Event interface. At the top, there are three yellow buttons labeled "Severity", "Status", and "Owner". Below them, the current values are displayed: "High" for Severity, "In Progress" for Status, and "analyst" for Owner. To the right of these are "Actions" and a close button. The main content area contains the following information:

- Description:** There are only 3 servers running in the web farm
- Date:** Fri Oct 07 2016 08:20:03 GMT-0700 (PDT)
- Overview** (tab is active)
- Comments** (tab is selected, highlighted with a yellow box and an arrow)
- Activity**
- Contributing KPIs:** Open all in Deep Dive ↗
- Possible Affected Services:** Open all in Deep Dive ↗
 - Online Sales
- Drilldowns:** Search: Examine events ↗

Generated for Javier Palacian (javier.palacian@tescobank.com) (C) Splunk Inc, not for distribution

Notable Event Details

- Begin investigating a notable event using the information and links in the event details
- Links provide access to deep dives for affected services or KPIs
- Information at the bottom of the details pane shows the fields in the notable event, including entities, descriptions, timestamps, etc.

The screenshot shows the 'Grouped Details View' interface. At the top, there's a header with 'Acknowledge' and dropdown menus for 'High', 'New', 'Unassigned', 'Actions', and a close button. Below the header, a message states: 'There are only 3 servers running in the web farm' with a timestamp from 'Tue Oct 24 2017 17:45:02 GMT+0000 (UTC)' to 'Tue Nov 7 2017 00:00:04 GMT+0000 (UTC)'. A warning message follows: 'You may not have permissions to view some events in this group.' The main content area has tabs: 'Overview' (selected), 'Grouped Events', 'Comments', and 'Activity'. The 'Description' section says 'Minimum service level is 4 servers'. The 'Group Aggregation Details' section indicates '3800 Notable Events' grouped by 'Default Policy' (with a link). The 'Smart Mode Group Details' section shows 'No Similar Text Values' and 'No Similar Category Values'. The 'All Tickets' section lists 'None'. The 'Contributing KPIs' section has a link 'Open all in Deep Dive'. The 'Possible Affected Services' section lists 'Online Sales' with a link 'Open all in Deep Dive'. A callout box labeled 'Ungrouped Details View also contains:' points to the 'Drilldowns' and 'Details' sections. The 'Drilldowns' section has a 'Search' link. The 'Details' section lists event fields: 'is_use_event_time: 0', 'mod_time: 1510013101.68', 'num_servers: 3', 'service_level: 4', 'severity: 5', 'status: 1', and 'search_name: Web Farm Service Level'. A 'Raw Event' link is at the bottom. Several yellow callout boxes with arrows point to specific features:

- A box points to the 'Default Policy' link in the 'Group Aggregation Details' section.
- A box points to the 'Open all in Deep Dive' link in the 'Contributing KPIs' section.
- A box points to the 'Open all in Deep Dive' link in the 'Possible Affected Services' section.
- A box points to the 'Search' link in the 'Drilldowns' section.
- A box points to the 'Edit in Correlation Search Editor' link in the 'search_name' field of the 'Details' section.

Generated for Javier Palacian (javier.palacian@tescobank.com) (C) Splunk Inc, not for distribution

Notable Event Groups: Common Fields

The screenshot shows the Splunk Notable Event Groups interface. On the left, there's a summary card for 'Low Conversion Rate' with details like 'Owner: unassigned', 'Severity: Medium', and 'Status: New'. A callout bubble with a red border and white text says '1 Click a > to expand' with a red number '1' inside a circle. On the right, the main panel shows a detailed view of the 'Low Conversion Rate' group. It includes sections for 'Description', 'Group Aggregation Details' (showing 154 events), 'All Tickets' (None), 'Contributing KPIs' (Purchases, Views), 'Possible Affected Services' (Online Sales), and 'Common Fields'. The 'Common Fields' section is highlighted with a green rounded rectangle and contains fields like 'alert_color', 'alert_level', 'alert_period', 'alert_value', and 'all_info'. A callout bubble with a red border and white text says '2 Examine the individual field values and their frequencies' with a red number '2' inside a circle. Below this, another callout bubble with a red border and white text says '3 (Optional) Click Show All to view remaining fields and values' with a red number '3' inside a circle. An arrow points from this callout to a 'Show all' button. To the right of the 'Common Fields' section, a yellow callout bubble says 'The Common Fields section lists the fields shared by the groups' Notable Events'. At the bottom, a table shows the frequency of specific field values: 'all_info: 15 values (expand for details)' with five rows of data.

Value	Frequency
Purchases had severity value critical 14 times in Last 15 minutes Views had severity value normal 14 times in Last 15 minutes	125 /154 events
Purchases had severity value critical 14 times in Last 15 minutes Views had severity value normal 11 times in Last 15 minutes	12 /154 events
Purchases had severity value critical 14 times in Last 15 minutes Views had severity value normal 12 times in Last 15 minutes	2 /154 events
Purchases had severity value critical 14 times in Last 15 minutes Views had severity value normal 13 times in Last 15 minutes	2 /154 events
Purchases had severity value critical 1 times in Last 15 minutes Views had severity value normal 1 times in Last 15 minutes	1 /154 events

Generated for Javier Palacian (javier.palacian@tescobank.com) (C) Splunk Inc, not for distribution

Adding a Comment

As you work on a notable event, you will probably want to document your work

1. Click the **Comments** tab
2. Enter a comment
3. Click **Comment**

All comments are displayed in the table below

The screenshot shows a Splunk interface for managing a notable event. At the top, the title of the notable is "Conversion rate was low" and the timestamp is "Thu Mar 31 2016 09:44:02 GMT-0700 (PDT)". Below the title, there are three tabs: "Overview", "Comments", and "Activity". A green arrow points from the text "Click the Comments tab" to the "Comments" tab. A second green arrow points from the text "Enter a comment" to the text input field where the comment "Found error in product description table—revising." is typed. A third green arrow points from the text "Click Comment" to the "Comment" button. Below the tabs, a table displays existing comments. The table has columns for User, Time, and Comment. One visible comment is from "admin" at "2016-03-31 09:46:49" with the text "Investigating cause...".

User	Time	Comment
admin	2016-03-31 09:46:49	Investigating cause...

Viewing and Searching Activity

- View all notable event activity on the **Activity** tab
- All status changes, comments, ownership changes, etc. are displayed here
- Use **Open in search** to open a new search window and search for specific items, such as text in comments, etc.

There are only 3 servers running in the web farm
Fri Oct 07 2016 08:20:03 GMT-0700 (PDT)

Activity Type	Time	User	Activity
Notable Event Update	2016-10-07 08:24:07	admin	status changed from status="New (1)" to status="In Progress (2)".
Notable Event Update	2016-10-07 08:24:00	admin	owner changed from owner="unassigned" to owner="analyst".

[Open in search ↗](#)

Notable Event Actions

1. Select **Actions** —————

2. Choose from:

- Link ticket (to a ticket in an external tracking system)
- Ping host
- Run a script
- Send email

3. Results display on the activity tab

The screenshot shows a Splunk interface for managing events. A context menu is open over an event, with the 'Actions' dropdown selected. The menu includes options like 'BMC Remedy Incident Integration', 'Link ticket', 'Ping host' (which is highlighted with a green box), 'Run a script', 'Send email', and 'Service Now Incident Integration'. A callout bubble provides additional information about the 'Actions' list. Below the menu, the event details show it was running in the background. The 'Activity' tab is selected, displaying a table of recent events and actions. One comment from 'admin' on '2016-10-07 08:59:26' is highlighted with a green box, showing the result of the 'Ping host' action: 'New comment="PING 54.203.66.14 (54.203.66.14) 56(84) bytes of data. -- 54.203.66.14 ping statistics -- 10 packets transmitted, 0 received, 100% packet loss, time 20073ms " is created'. Other entries in the table include a comment from 'admin' at the same time and another action executed by 'admin' at the same time.

Activity Type	Time	User	Comment
Comment created	2016-10-07 08:59:26	admin	New comment="PING 54.203.66.14 (54.203.66.14) 56(84) bytes of data. -- 54.203.66.14 ping statistics -- 10 packets transmitted, 0 received, 100% packet loss, time 20073ms " is created
Comment created	2016-10-07 08:59:26	admin	New comment="No Errors while running ping." is created
Action Executed	2016-10-07 08:59:06	admin	Action="itsi_sample_event_action_ping" executed.

Generated for Javier Palacian (javier.palacian@tescobank.com) (C) Splunk Inc, not for distribution

Notable Event Grouping

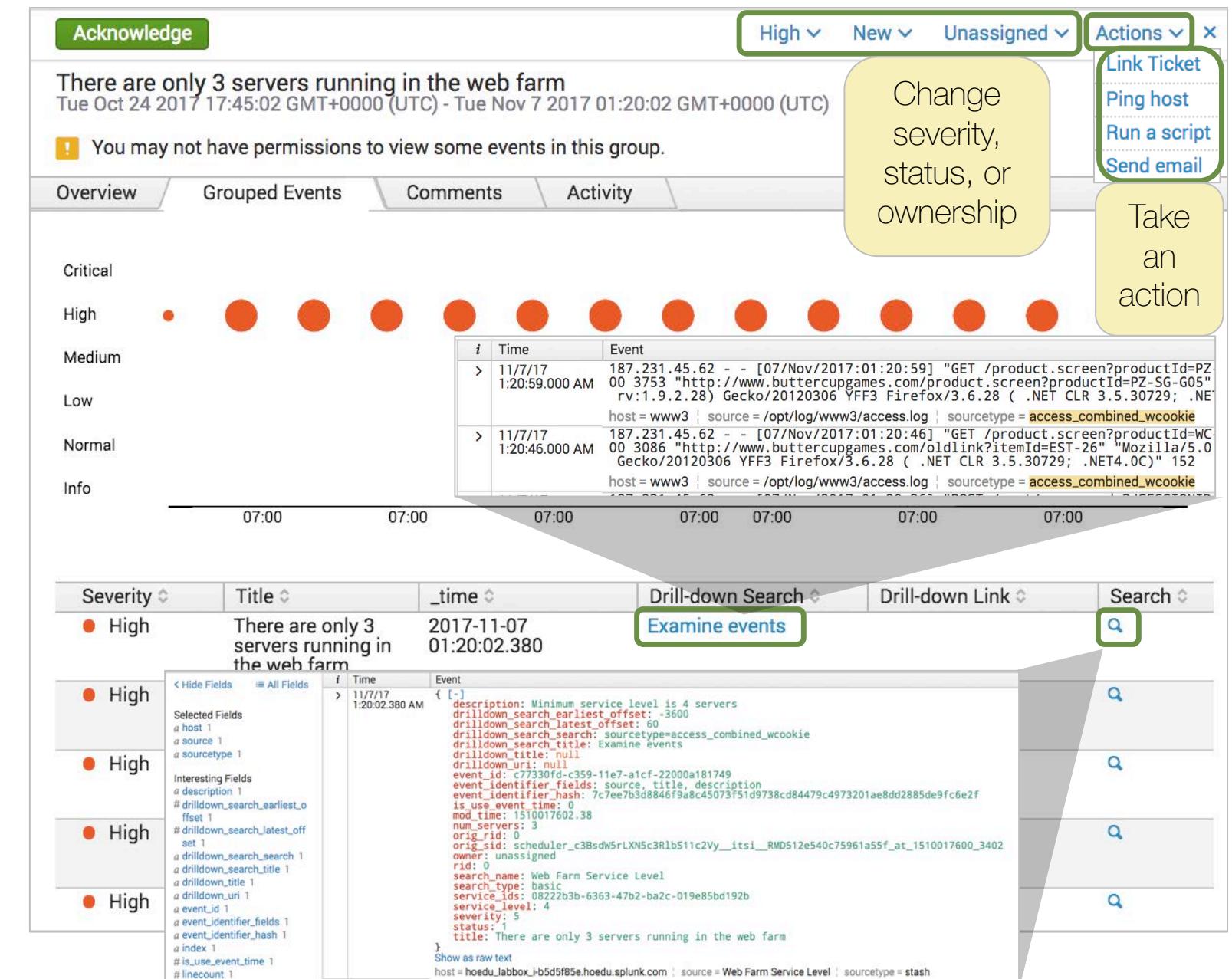
- De-clutters the view, changes all grouped events at once
 - Default: notables are grouped by source (the correlation search that created them) until no new event from that source occurs for 2 hours
 - Admins can manually control grouping with agg. Policies

The screenshot shows the Splunk Notable Events interface. On the left, a list of four individual notable events is shown, each with a severity count (2, 6, 45, 10), status (New), and a brief description. A vertical orange bar highlights the first event. On the right, a summary panel for a group of 6 notable events is displayed. The panel includes a title, date range, and tabs for Overview, Grouped Events (which is selected), Comments, and Activity. The Description section contains a summary of the grouped events. A note at the bottom states: "6 Notable Events are grouped based on the aggregation policy: Default Policy".

- Ctrl-click or shift-click to work on multiple groups together

Grouped Events Tab and Actions

- Shows details about each event in the group
- Setting the severity, status or owner can be applied to the group overall, or individually to each event in the group
 - If applied at group level, changes are lost if the events are ungrouped
- Comments are always at the group level



Generated for Javier Palacian (javier.palacian@tescobank.com) (C) Splunk Inc, not for distribution

Customizing Views

- You can create and save multiple views of the notable event review screen:
 - Set title
 - Filter by owner, status, etc.
 - Group events, choose color options, choose fields
- Examples: All vs. all unassigned, New today, All critical, >10 days old, etc.
- All views are global for all analysts or admins
 - You can control who can edit views by role

Using Custom Views

The screenshot shows the Splunk interface for viewing logs related to the 'Middleware Service'. The top navigation bar includes 'Edit the view name' and 'Save as...' buttons. The search filters are set to 'Last 60 minutes', 'Service: Middleware Serv...', 'Severity: All', and 'Add Filter'. A tooltip indicates that sometimes you may need to scroll up to see these buttons. The main table lists events with columns for Title, Time, Owner, Severity, Status, and Description. The first event is 'NewRelic Health Status: Web Login' from 'Tue Jul 25 17:15:07 PM' with status 'New'. The second event is 'Web View Cart' from 'Tue Jul 25 17:15:07 PM' with status 'Closed'. The third event is 'Web Service' from 'Tue Jul 25 17:15:07 PM' with status 'Closed'. On the left sidebar, there's a 'Views' section with a '+ Add new views' button, a 'Select and edit saved views' button, and a 'Full Lister Page' link. A tooltip for the 'Views' section says 'Use settings for filters and view options to customize'. A gear icon in the top right corner has a tooltip 'Save or update the view (Sometimes you may need to scroll up to see these buttons)'.

Title	Time	Owner	Severity	Status	Description
NewRelic Health Status: Web Login	Tue Jul 25 17:15:07 PM	Unassigned	Normal	New	Web Login status = green
Web View Cart	Tue Jul 25 17:15:07 PM	Unassigned	Info	Closed	Web View Cart status = green
Web Service	Tue Jul 25 17:15:07 PM	Unassigned	Info	Closed	Web Service status = green

Generated for Javier Palacian (javier.palacian@tescobank.com) (C) Splunk Inc, not for distribution

Module 3 Lab Exercise

Time: 30 minutes

Tasks:

- Use notable events during incident response to triage and coordinate actions
- Configure notable event options

Module 4: Investigating Issues with Deep Dives

Generated for Javier Palacian (javier.palacian@tescobank.com) (C) Splunk Inc, not for distribution

Objectives

- Customize new deep dive displays
- Add swim lanes to deep dives
- Configure swim lane options

What are Deep Dives?

- Swim lane-based visualizations for comparing and examining detailed information about one or more KPIs, *aligned by time*
- Lanes show results of time chart searches
- Comparing lanes provides insights into KPIs, services, and issues



Example

The Network service health score turns to high alert. You drill down to see many components plotted in parallel by time. One router and several servers have high alert status. Others are unaffected. You quickly zero in on only the affected devices for further analysis and action.

Deep Dive: Uses

In an anomalous scenario, like an outage, use deep dives to examine and compare alert levels for KPIs in a service over time

- Add, remove and sort lanes as needed
- Access a service's default deep dive from the Service Analyzer
- IT Service Intelligence admins and analysts can modify these default deep dives as needed
 - Modifications are global for all users
- You can also save deep dives with a name
 - These can be accessed from the deep dive menu or as drill-down actions on glass tables

Default Deep Dives

- Each service has a default deep dive that initially shows all of that service's own KPIs
 - This deep dive automatically displays when you select a service or KPI in a service analyzer and click **Drilldown to Deep Dive**
- **Admin** and **analyst** users can modify default deep dives, including adding KPIs from other services, ad-hoc lanes, and customizing display options
 - You can't delete a service KPI: it will be re-added each time a default deep dive is opened
- Changes to default deep dives are persisted globally for all users

Why Default Deep Dives

- You don't need to set up hundreds of deep dives yourself
- Best practice is usually to have primarily default deep dives
 - Configure them as much as you like
 - No need to save them
 - For that service, that deep dive will always look just as you last left it
 - You won't have to keep adding KPIs to it each time
- If you really want different deep dives for different people, you can save some



Generated for Javier Palacian (javier.palacian@tescobank.com) (C) Splunk Inc, not for distribution

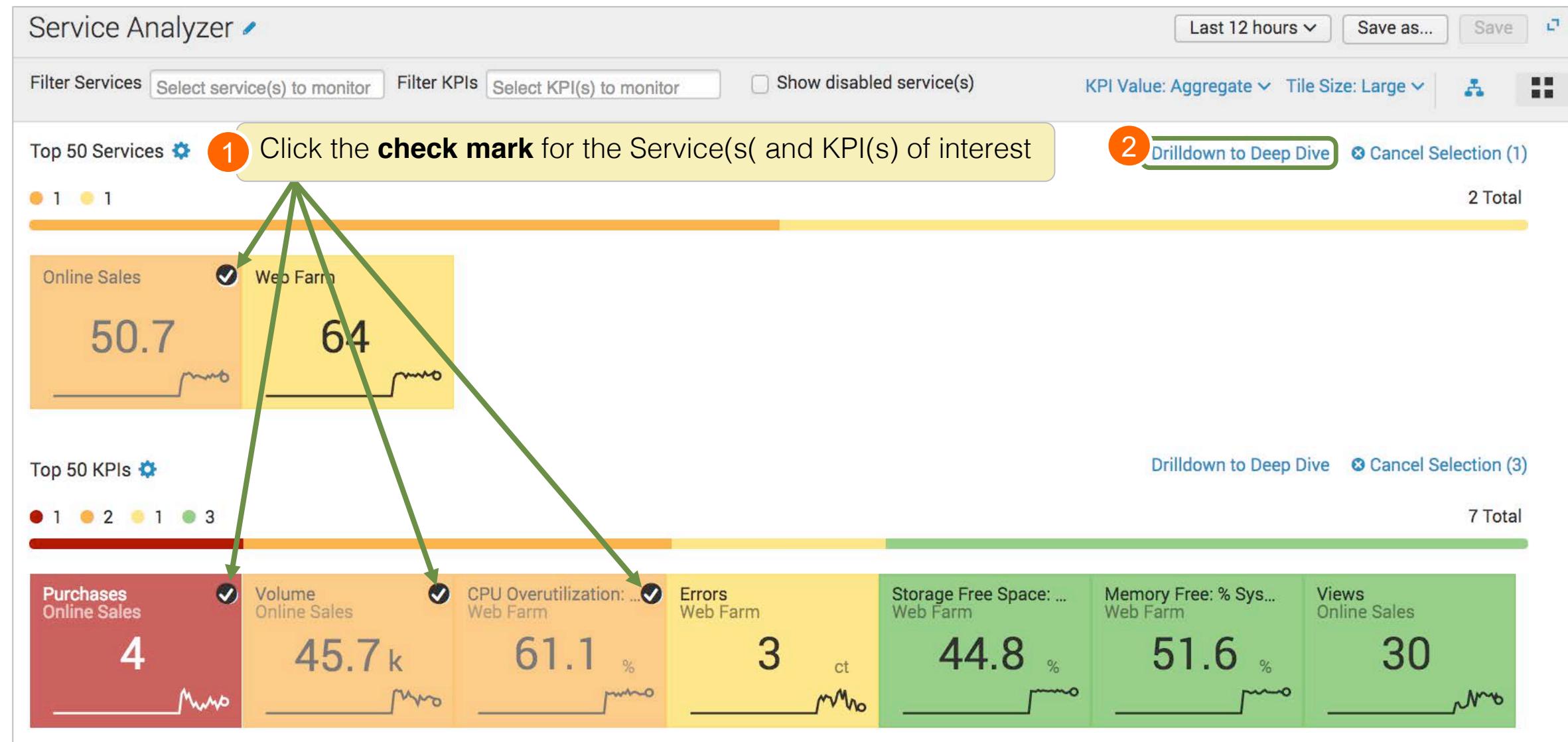
Default Deep Dive Example

- Service-swappable Glass Tables (multiple links from a single widget)
 - If your deep dives are default deep dives, ITSI will automatically go to the deep dive for the current service
 - You won't have to add all your KPIs again
- If your deep dive has been custom named/saved, it may not go to the service you're examining

Custom Deep Dives

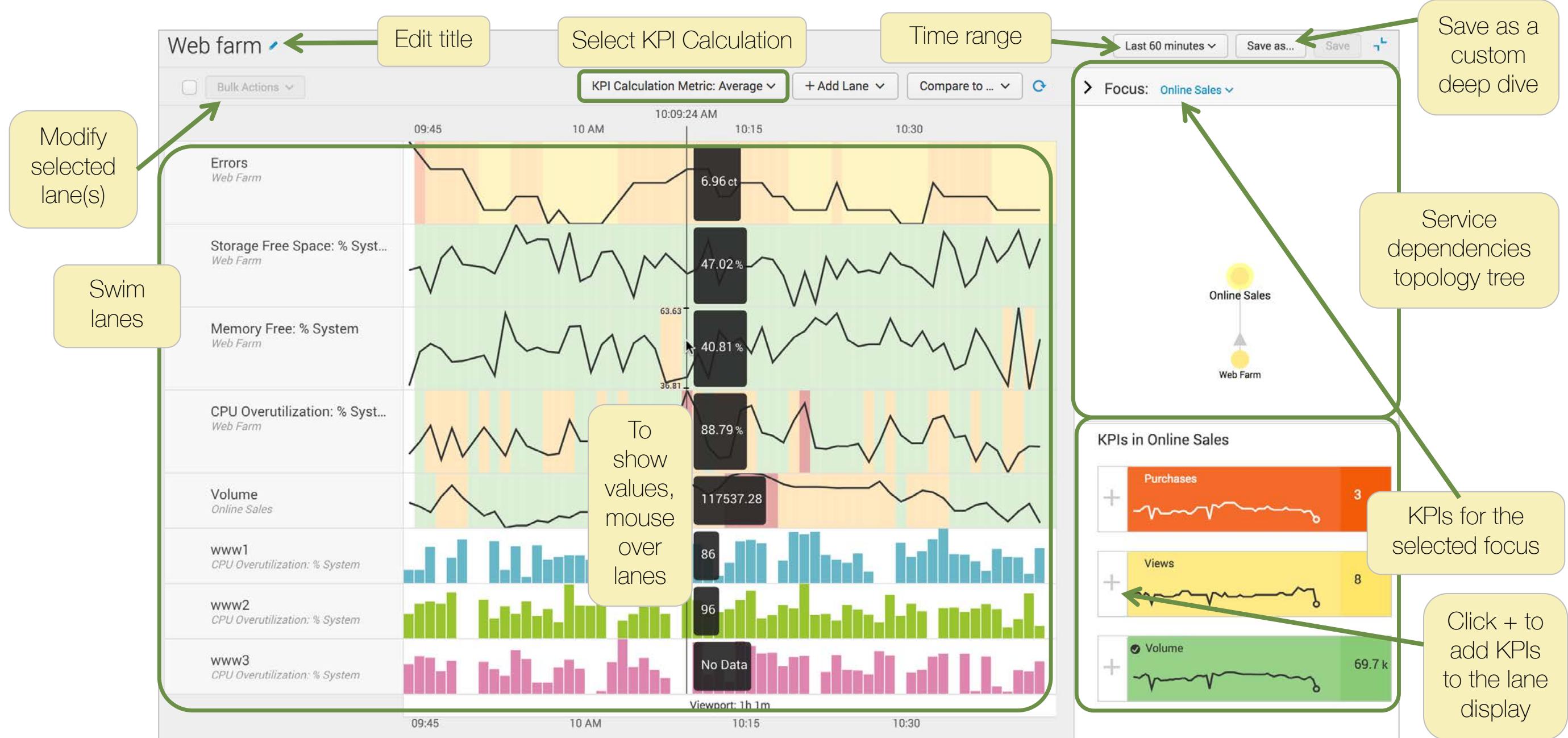
- **Admin** or **analyst** users can create new custom deep dives
- These can start as either a service default deep dive, or as a completely new deep dive
- Custom deep dives can contain any swim lanes for KPIs or other data as needed, and can have their permissions set so that only specific users can see or modify them

From Service Analyzer to Deep Dive



Generated for Javier Palacian (javier.palacian@tescobank.com) (C) Splunk Inc, not for distribution

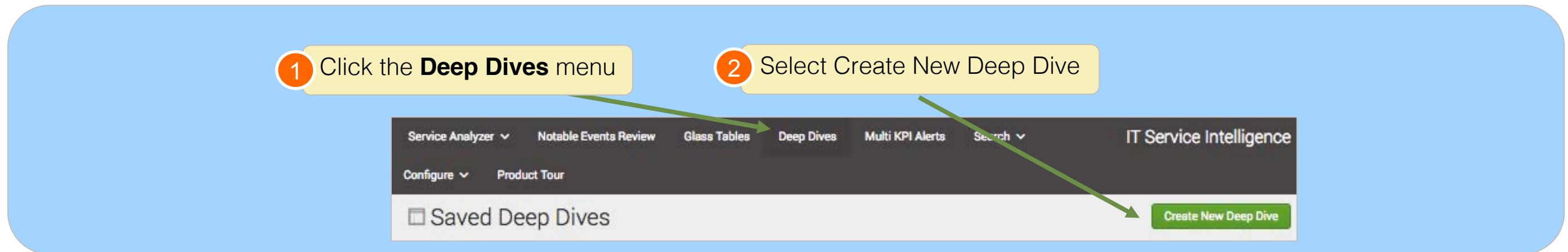
Deep Dive Navigation



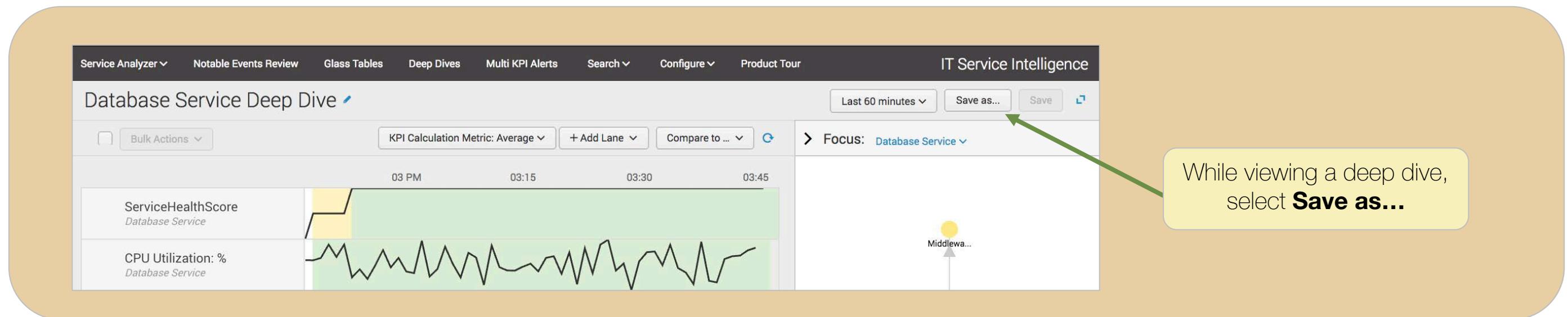
Generated for Javier Palacian (javier.palacian@tescobank.com) (C) Splunk Inc, not for distribution

Creating New Deep Dives

Either:

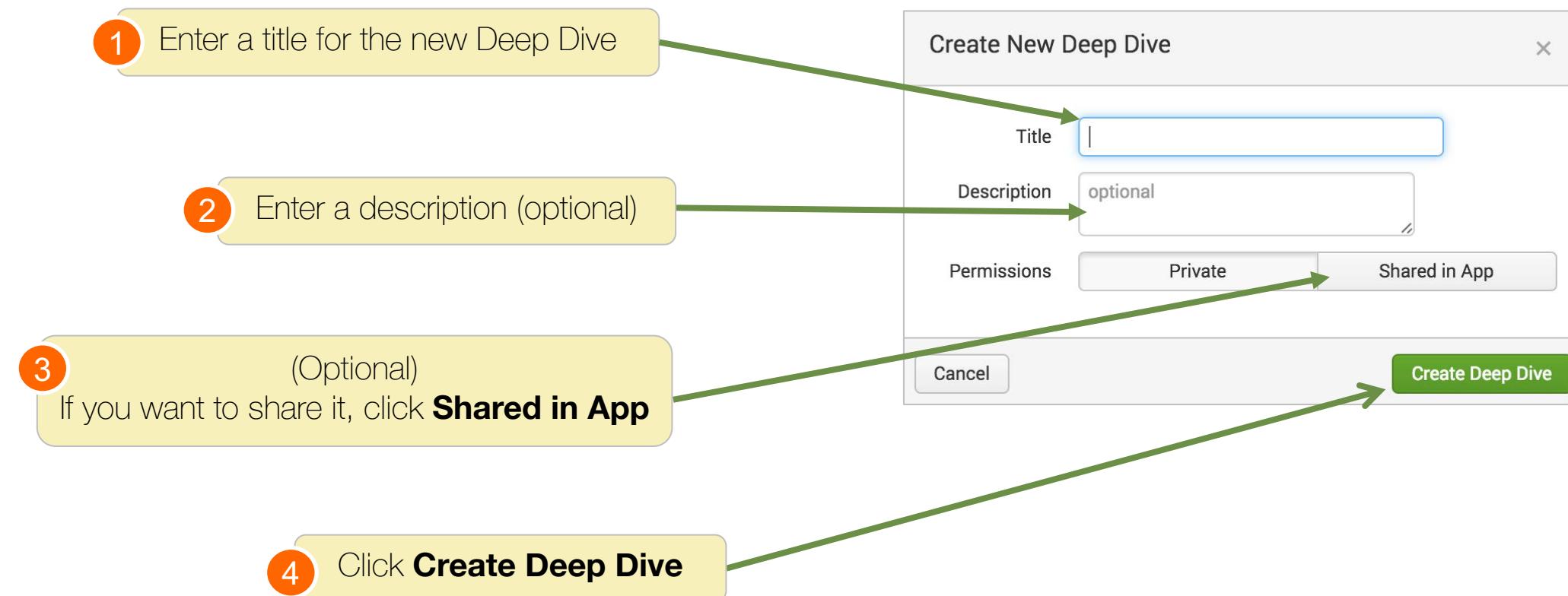


or



Generated for Javier Palacian (javier.palacian@tescobank.com) (C) Splunk Inc, not for distribution

Naming New Deep Dives



If you created it from the **Deep Dive** menu, it is blank to start

Lane Types

- **Metric lane**

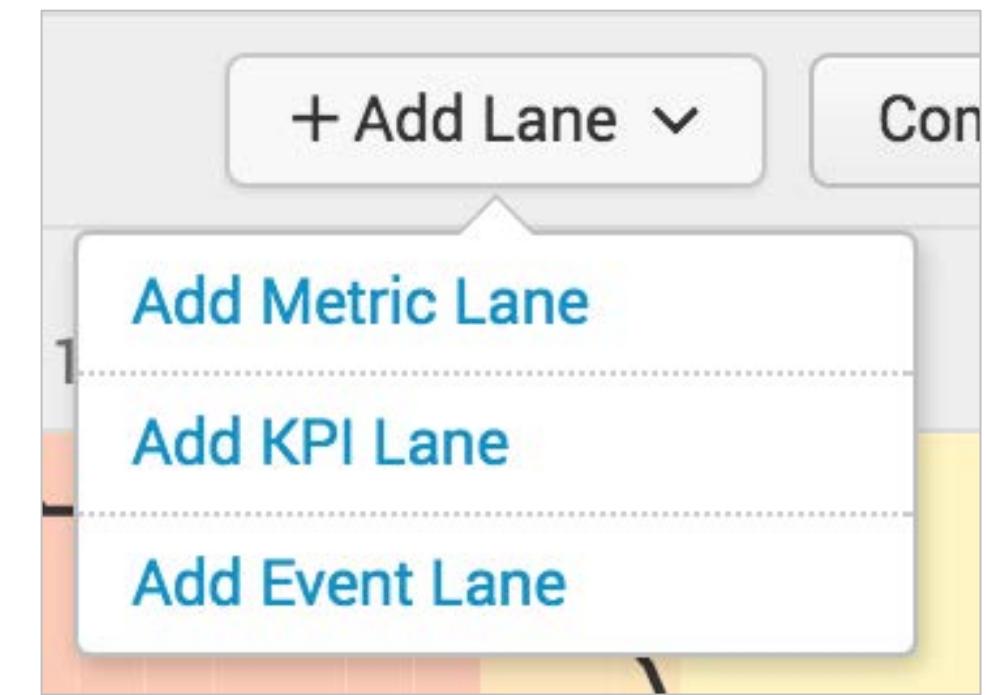
- Based on an ad-hoc search using either a data model or SPL; used to display statistics related to other lanes

- **KPI lane**

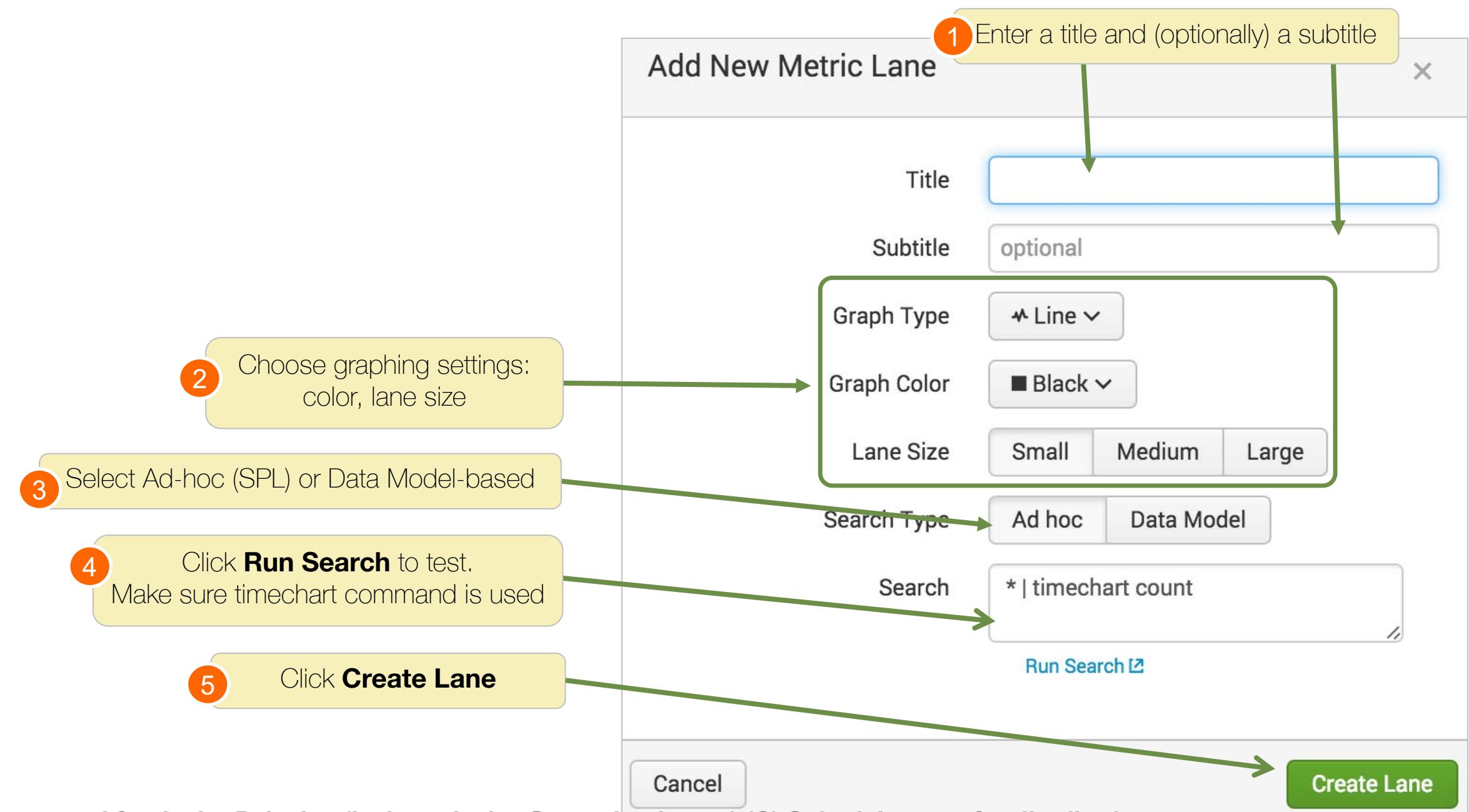
- Add a KPI to the deep dive, from any service
- Or add from the topology tree

- **Event lane**

- Using an ad-hoc search, display event counts in a new swim lane



Adding a Metric Lane



Generated for Javier Palacian (javier.palacian@tescobank.com) (C) Splunk Inc, not for distribution

Adding a KPI Lane

You can also add a KPI lane from the topology tree

The dialog box contains the following fields:

- KPI Title: ServiceHealthScore
- Overwrite KPI Title?: Yes
- Graph Type: Line
- Graph Color: Black
- Lane Size: Medium
- Service: Web Farm
- KPI: ServiceHealthScore
- Accelerate Using KPI Summary?: No
- KPI Search?:
`get_full_itsi_summary_kpi("SHKPI-2a991b17-be25-448f-a8b0-3de02a28fc74") | timechart limit=0 useother=0 avg(alert_value) by kpiid`
- Run Search ↗
- Cancel
- Create Lane

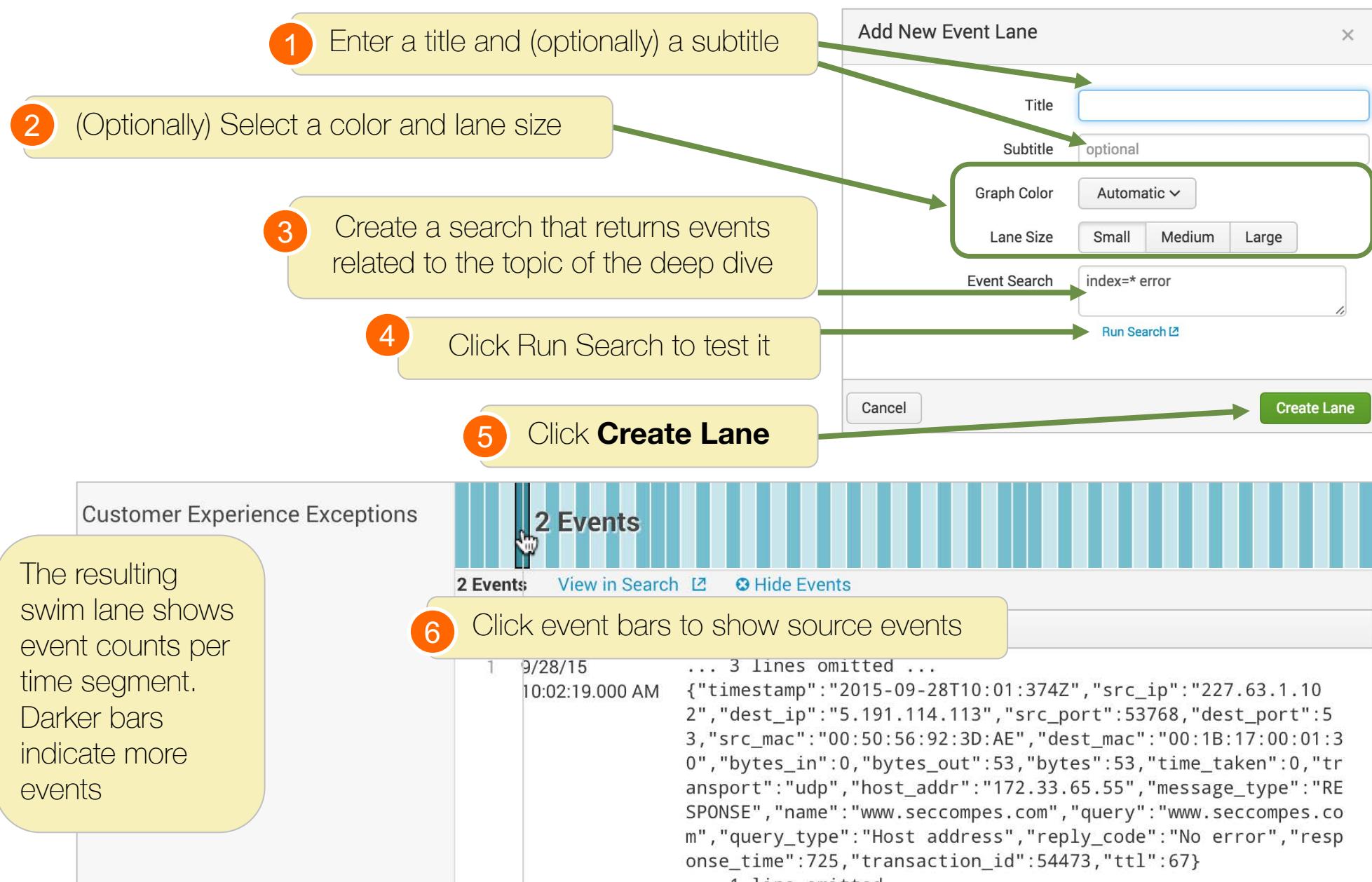
- 1 Use the KPI name or enter a custom title
- 2 Choose graphing and lane options
- 3 Select the service and KPI name
- 4 (Optional) Click **Run Search** to test
- 5 Click **Create Lane**

Generated for Javier Palacian (javier.palacian@tescobank.com) (C) Splunk Inc, not for distribution

Adding an Event Lane

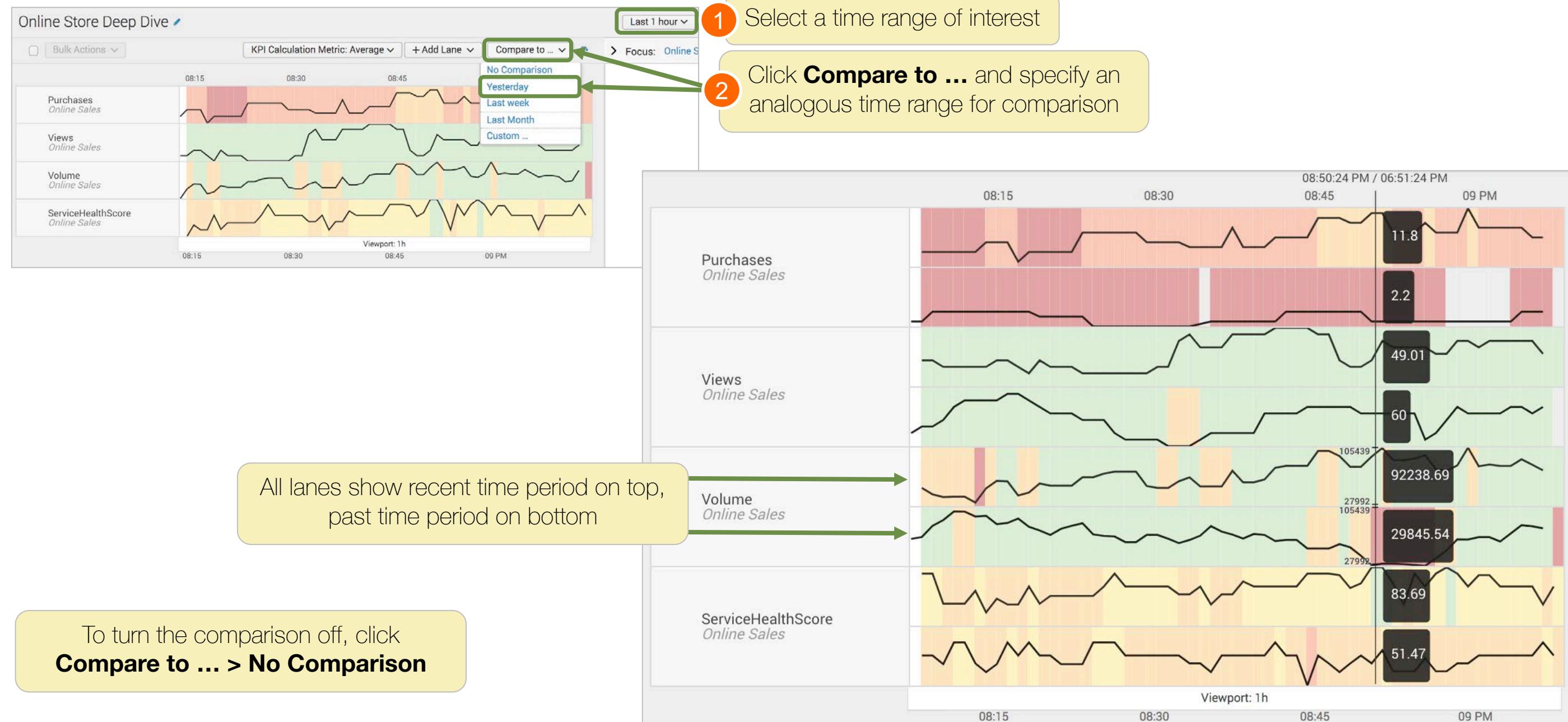
Note 

Event lanes provide fast access to the underlying event detailed information.



Generated for Javier Palacian (javier.palacian@tescobank.com) (C) Splunk Inc, not for distribution

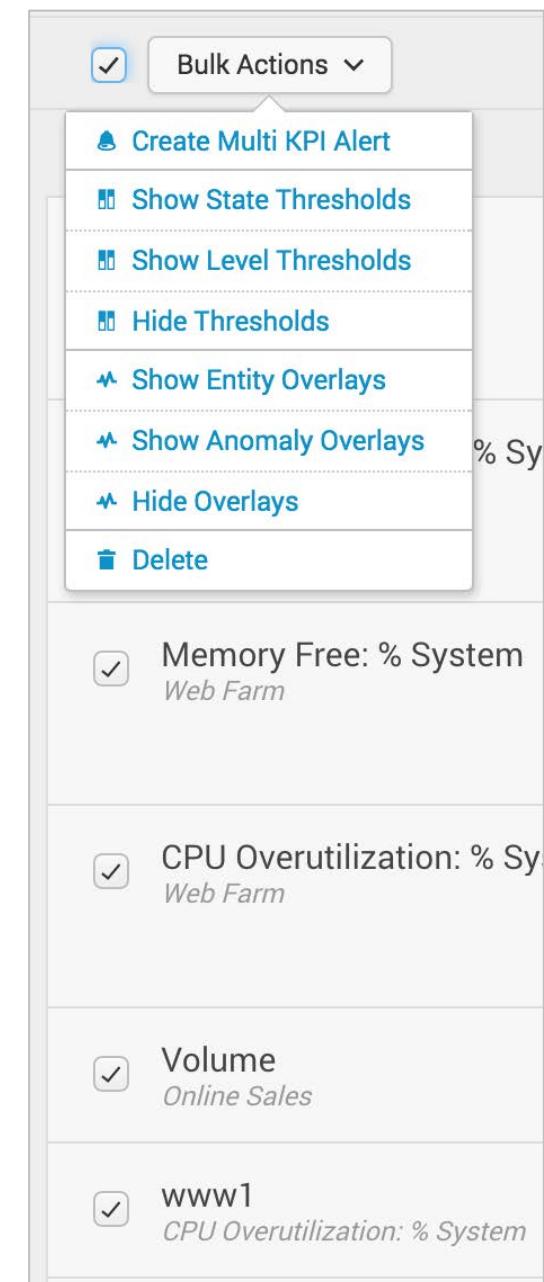
Compare Earlier Time Ranges: Twin-Lane



Generated for Javier Palacian (javier.palacian@tescobank.com) (C) Splunk Inc, not for distribution

Applying Bulk Actions

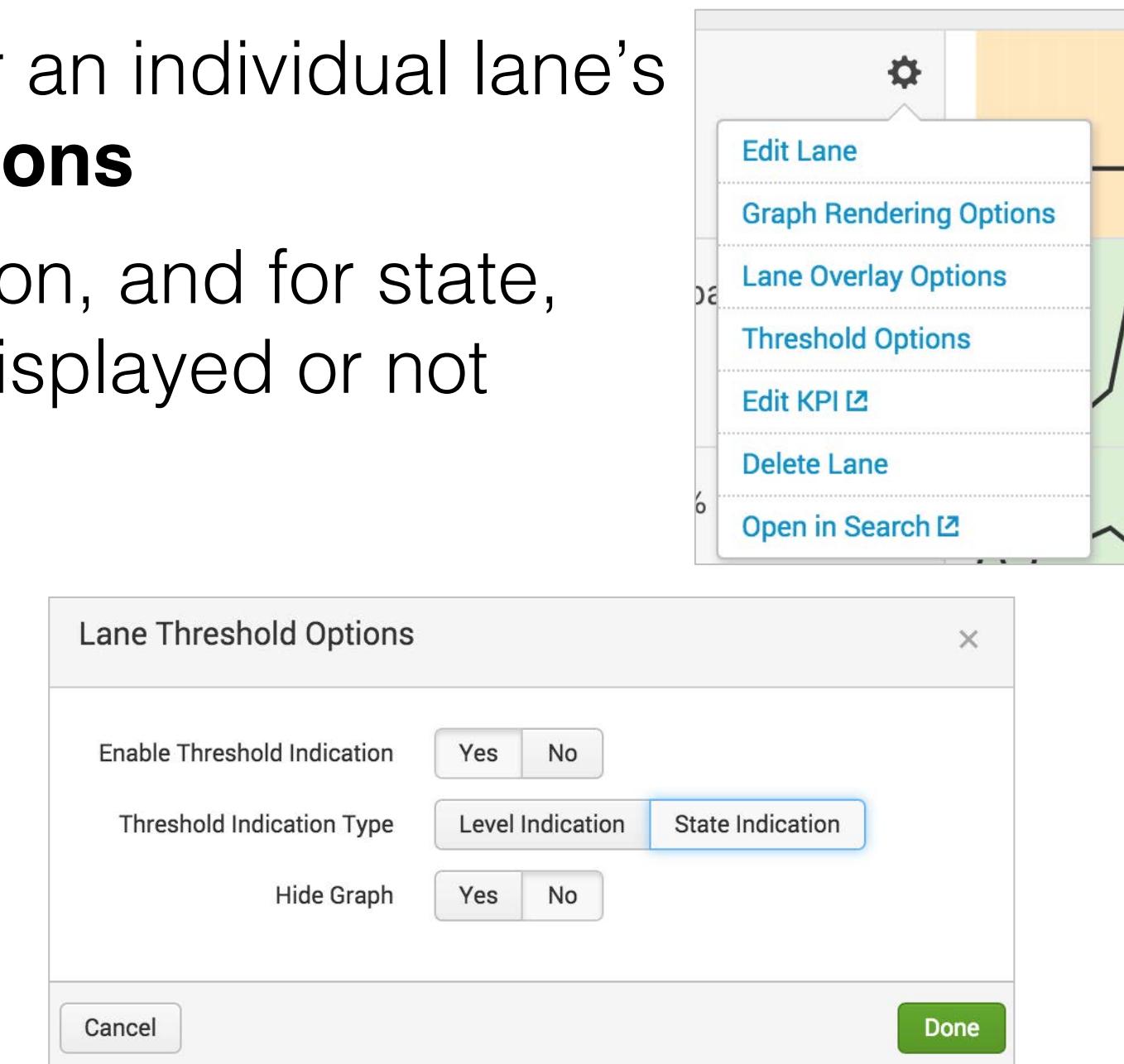
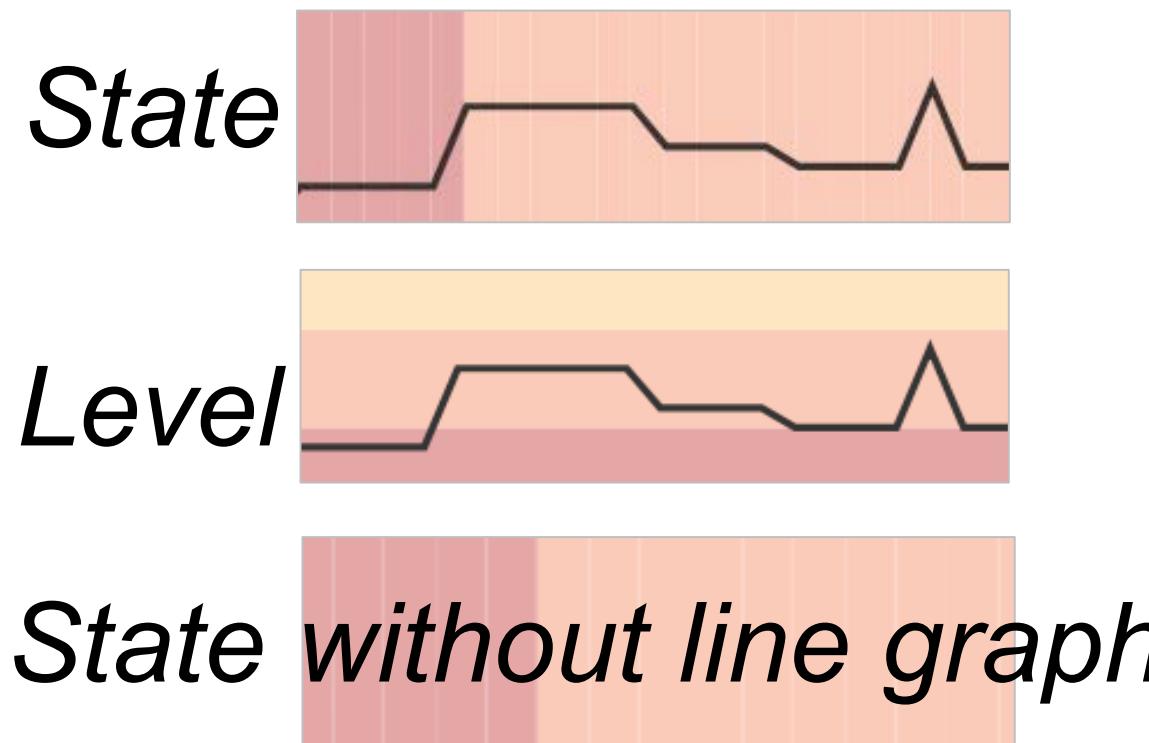
- Select one or more lanes and click **Bulk Actions** to:
 - Create a multi KPI alert based on the selected KPIs (admins typically do this)
 - Show state, level, or no thresholds (state is default)
 - Show or hide entity and / or anomaly overlays
 - Delete lanes
- Use the adjacent checkbox to select all lanes first, or select the specific lanes you want to modify
- Note that multi KPI alert creation and threshold colors only applies to KPI lanes



Generated for Javier Palacian (javier.palacian@tescobank.com) (C) Splunk Inc, not for distribution

Selecting Threshold Display

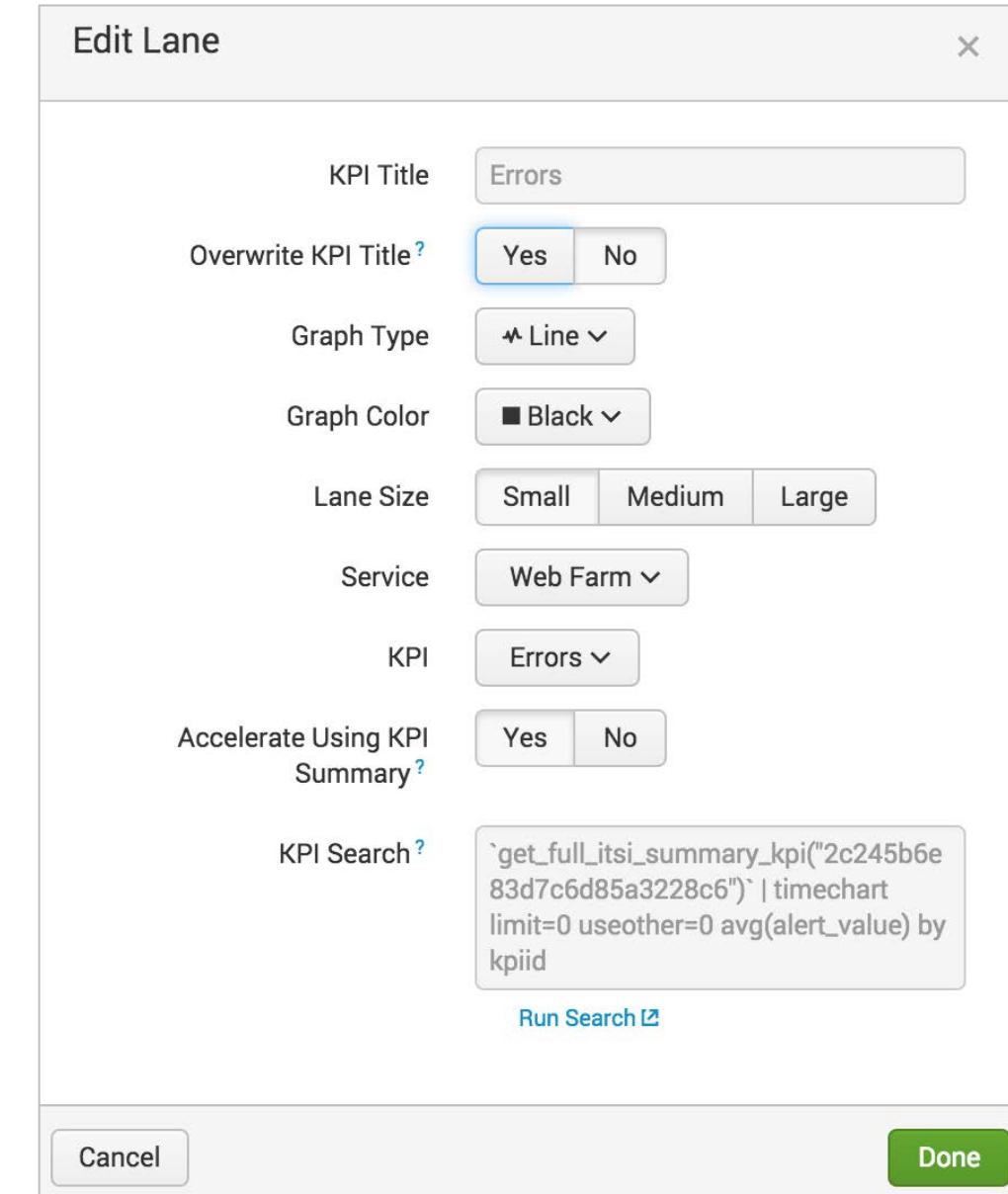
- Use either the bulk actions menu or an individual lane's  icon and choose **Threshold options**
- Choose either level or state indication, and for state, choose if you want the line graph displayed or not



Generated for Javier Palacian (javier.palacian@tescobank.com) (C) Splunk Inc, not for distribution

Editing Lane Appearance

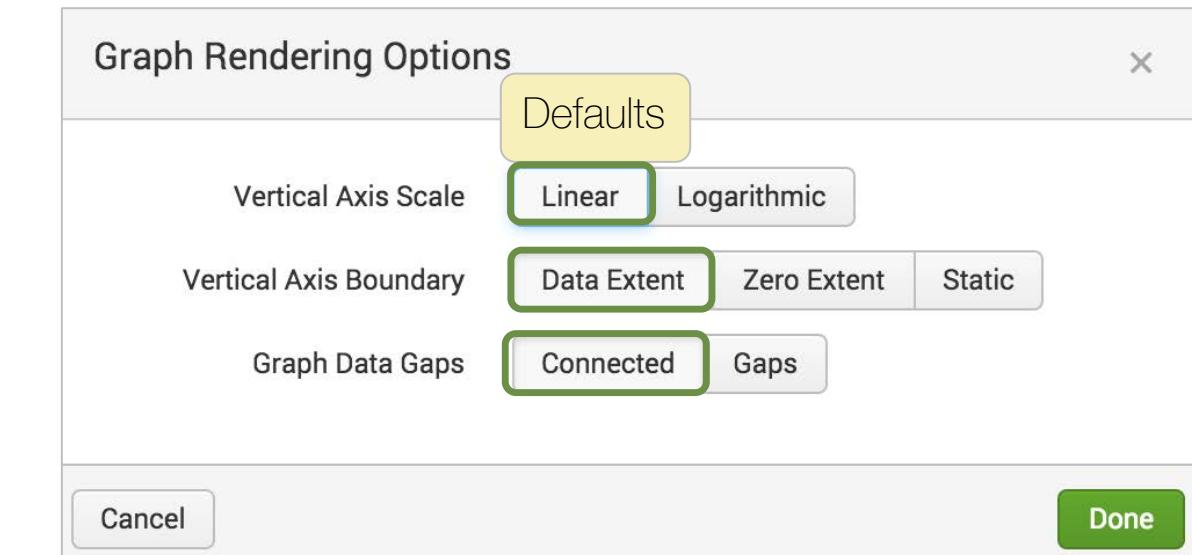
1. Click the lane edit menu  icon and select **Edit Lane**
2. Set the title, graph type, color, lane size, search source, etc.
3. Click **Done**



Generated for Javier Palacian (javier.palacian@tescobank.com) (C) Splunk Inc, not for distribution

Editing Graph Rendering Options

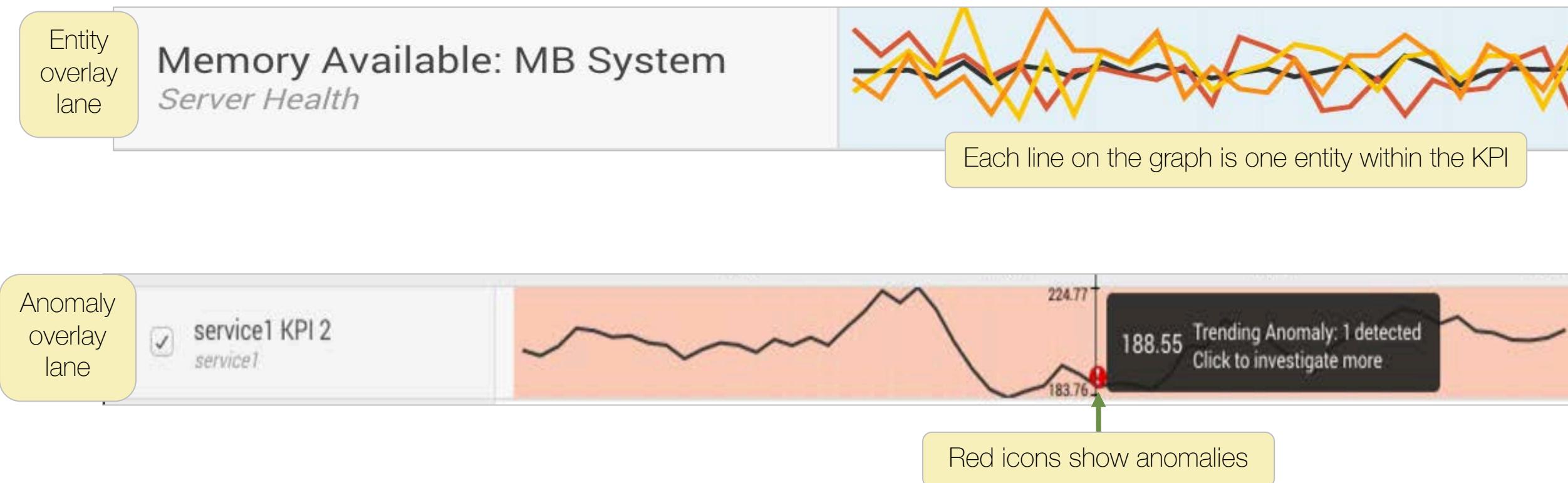
1. Click  and select **Graph Rendering Options**
2. Choose linear or logarithmic scale
3. Specify vertical axis boundary
 - min. and max. automatically determined by data values
 - min. of zero, max. based on data
 - Specify a static min. and max.
4. Click **Gaps** to show data gaps
5. Click **Done**



Generated for Javier Palacian (javier.palacian@tescobank.com) (C) Splunk Inc, not for distribution

Configuring Lane Overlays

- Swim lanes can be configured to include overlays
- Overlays display either multiple entities or anomalies

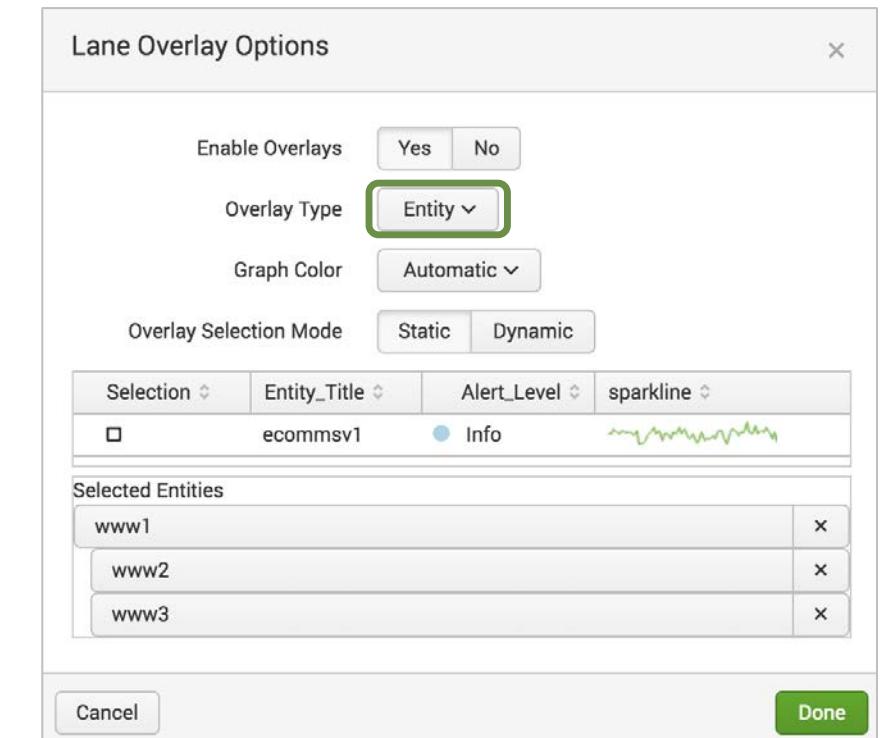


Generated for Javier Palacian (javier.palacian@tescobank.com) (C) Splunk Inc, not for distribution

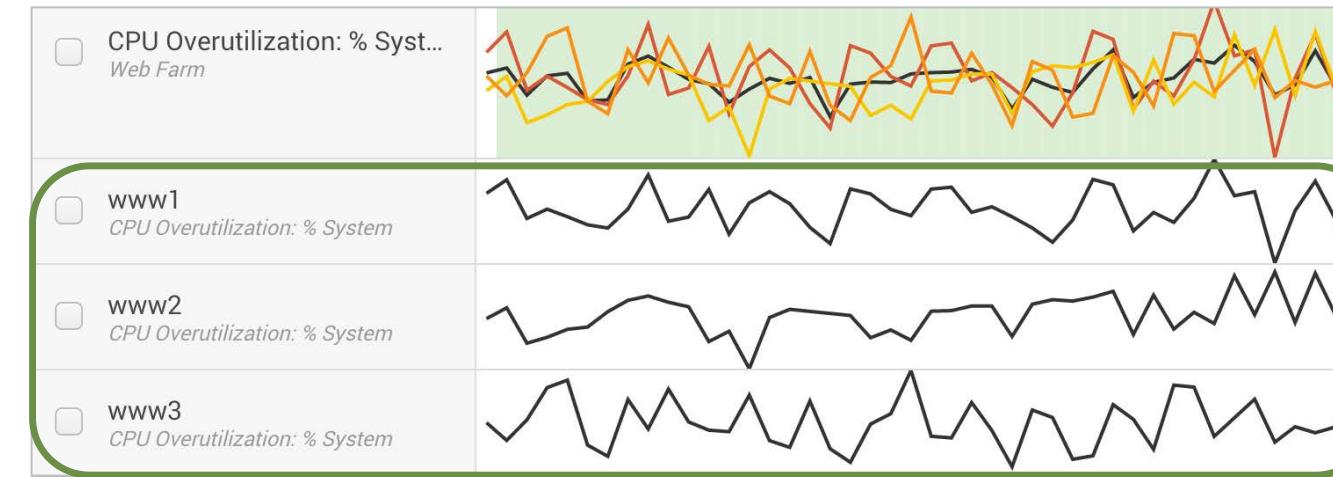
Enabling Entity Lane Overlays

Only available for KPIs split by entity

1. Click the  icon and select **Lane Overlay Options**
2. Select **Yes** to enable overlays, and select **Entity** for the Overlay Type
3. Choose graph color options
4. You can choose either **Dynamic** (worst 3 entities) or **Static** (pick the entities you want to display)
5. Click **Done**



Adding Entity Overlays as Lanes



- Each entity now has its own metric lane displaying only that entity's data
- The new lanes can be configured with their own colors and other graphing options

Generated for Javier Palacian (javier.palacian@tescobank.com) (C) Splunk Inc, not for distribution

Configuring Lane Drilldown

- By default, lanes are not clickable for further drilldown (except event lanes, which are clickable)
 - Use the lane's  icon and select **Open in Search** to explore the lane's data set
- If a lane has been configured for entity lane overlay, you can click the lane and choose **Add Overlay as Lane** to expand each entity into its own lane
- Lanes based on a KPI from a module may also have a custom drill-down setting (created by admins)
 - Example: **OS Host Details**: open the **OS Host Details** dashboard from the Operating System module



Examining KPI Base Searches

Online Sales Monitor online sales

Entities KPI Service Dependencies Settings

KPIs

Service Health

Purchases

Views

KPI description

Search And Calculate

Source

KPI Source: Base Search

Search: sourcetype=access_combined_wcookie action=view | eval viewrate=10

Threshold field: viewrate

Entities

This KPI is not filtered by nor is monitoring any entities

Calculation

Calculating Sum of aggregate over the last 15 minute(s) every 1 minute(s)

Unit

Thresholding

Aggregate Threshold Values

View data from the last 60 minutes ▾

Level	Value
normal	20
low	15
medium	10
high	5

Anomaly Detection

ITS! Anomaly Detection learns the normal patterns of KPIs continuously in real-time, triggering a notable event when a KPI departs from its expected behavior. Certain types of data are not suitable for use with anomaly detection because they produce too many false positives. We recommend that you analyze the KPI data first to check its compatibility with ITS!'s anomaly detection algorithms.

Enable Trending Anomaly Detection: No

Trending Algorithm Sensitivity: 8

Enable Entity Cohesion Anomaly Detection: No

Entity Cohesion Algorithm Sensitivity: 8

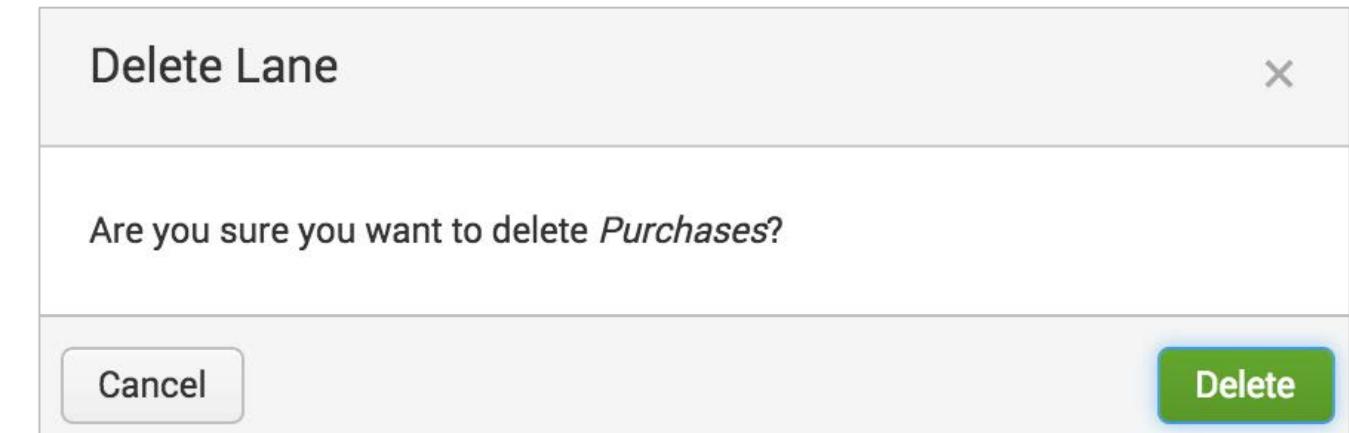
Examine the details of how the KPI was built

Generated for Javier Palacian (javier.palacian@tescobank.com) (C) Splunk Inc, not for distribution

Deleting a Lane

1. Click the lane's  icon and select **Delete Lane**
 - Or use the bulk actions menu
2. Click **Delete** to confirm

In a service's default deep dive, the KPIs belonging to that service will be replaced each time the deep dive is re-opened



Troubleshooting with Module Details View

1 a. Look for a service with an alert that has gone from green to yellow (in this example, the service includes OS Host module).
b. Enable entity overlays or state thresholds.
c. Find and click a KPI that went red just before that time.

2 Click **OS Host Details**

3 View the dashboard to view the health of that entity

The image shows a service health score dashboard with several KPIs. A green arrow points from the 'Memory Free: %' chart to the 'OS Host Details' button in the bottom right corner of the dashboard. Another green arrow points from the 'OS Host Details' button to the detailed OS Host Details dashboard. The detailed dashboard shows various metrics like Memory Used (MB) and Memory Used (%), which are highlighted with a green box. The 'Top 10 Memory Consumers' table is also circled in green.

OS Host Details

Entity mysql-02
Service Database Service

Total Storage Used (%) 0.3 TB / 0.4 TB
Host Events (count) 134 events
CPU Usage (%) Average: 30.2%
Memory Available (%) Average: 55.3%

Memory Used (MB)

Memory Used (%)

Top 10 Memory Consumers

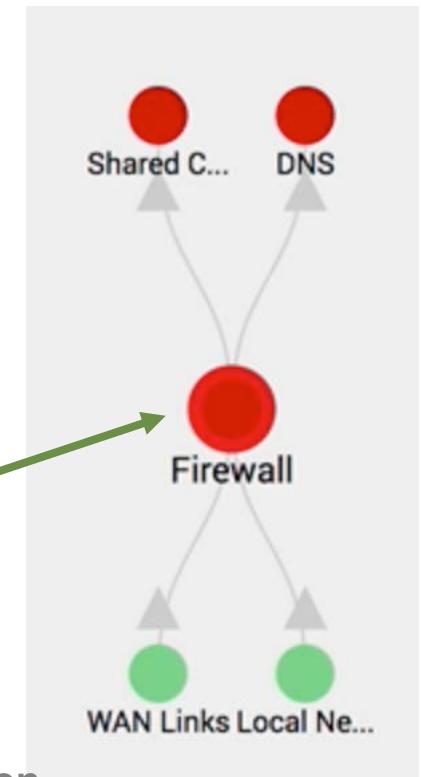
Process	CPU %	Memory (MB)
/usr/sbin/mysqld --basedir=/ --datadir=/var/lib/mysql --user=mysql	11.10	26.26
/sbin/rsyslogd -i/var/run/syslogd.pid -c 5	0.00	4.43
/sbin/init	0.00	0.94
auditd	0.00	0.80
crond	0.00	0.78
/usr/sbin/sshd	0.00	0.72
/sbin/udevd -d	0.00	0.22
[flush-253:0]	0.00	0.00
[flush-8:16]	0.10	0.00
[kauditd]	0.00	0.00

Generated for Javier Palacian (javier.palacian@tescobank.com) (C) Splunk Inc, not for distribution

Other Troubleshooting Workflows

- Service Analyzer > Service > KPI > view Entities
- Service Analyzer > Service > KPI > Deep Dive > Bulk Actions or  > Entity Overlay > view Entity or view Module
- Notable Events Review > Notable Event > Deep Dive ...
- Glass Table > Deep Dive >
 - Enable Overlays (for the KPI with the issue)
 - Identify hosts
 - drilldown to raw data
- See Appendix for screenshots

When troubleshooting,
**drill down until you find
the bottom of the tree:**
the deepest item whose
dependencies are all green



Preventing Problems with Deep Dives

Tier 3 Ops Analysts and Tools Engineers Example:

- After you've used workflows to solve the problem once
 - You know the alert that needs to go to the database team
 - You know which machine will need to be restarted
- If there is a good chance it may recur, you can prevent it before it happens or affects customers
 - Ask your admin to define a Multi KPI Alert (change from composite to status over time)
 - No SPL required, but search criteria can be added (usually by admins)

Deep Dive Role Capabilities

- By default, both **itoa_admin** and **itoa_analyst** members can create, edit and delete deep dives
- Each deep dive can be either:
 - Private, only accessible by the owner
 - Shared with all users who have access to the ITSI app

Module 4 Lab Exercise

Time: 30 minutes

Tasks:

- Modify a default deep dive
- Create a new deep dive

Support programs

• Community

- **Answers:** answers.splunk.com
Post specific questions and get them answered by Splunk community experts.
- **Splunk Docs:** docs.splunk.com
These are constantly updated. Be sure to select the version of Splunk you are using.
- **Wiki:** wiki.splunk.com
A community space where you can share what you know with other Splunk users.
- **IRC Channel:** #splunk on the EFNet IRC server Many well-informed Splunk users “hang out” here.

• Global Support

Support for critical issues, a dedicated resource to manage your account – 24 x 7 x 365.

- **Phone: (855) SPLUNK-S or (855) 775-8657**
- **Web:** http://www.splunk.com/index.php/submit_issue

• Enterprise Support

Access your customer support team by phone and manage your cases online 24 x 7
(depending on support contract).

Generated for Javier Palacian (javier.palacian@tescobank.com) (C) Splunk Inc, not for distribution



splunk®

.conf18:

Monday, October 1 – Thursday, October 4

Splunk University:

Saturday, September 29 – Monday, October 1

ORLANDO FLORIDA

Generated for Javier Palacian (javier.palacian@tescobank.com) © Splunk Inc. not for distribution
Walt Disney World Swan and Dolphin Hotels

Thank You

- Complete the survey to be in this month's drawing for a \$100 Splunk Store voucher
 - Check your inbox for a link to the survey, or access the link on the **My Profile** page



Splunk Education

Re-login **1 My Profile** Password Purchase Credits Checkout

My Profile

To update your profile, click the **Contact Information** tab. Enter the new information in the fields and then click **Submit** to save. Fields with an asterisk(*) are required.

Registrations **2 In-progress and Past** **Contact Information** **Certification**

Registration Number	Course Name	Location	Status	Attended	Completed Date
455-11809-11032-4-135370	Extending Splunk 6 Apps - Virtual Details Evaluation	Virtual Training - The Americas 8-Jan-15 - 8-Jan-15 9:00AM - 1:30PM Pacific Time (US & Canada) Meeting Expired	Confirmed	<input checked="" type="checkbox"/>	

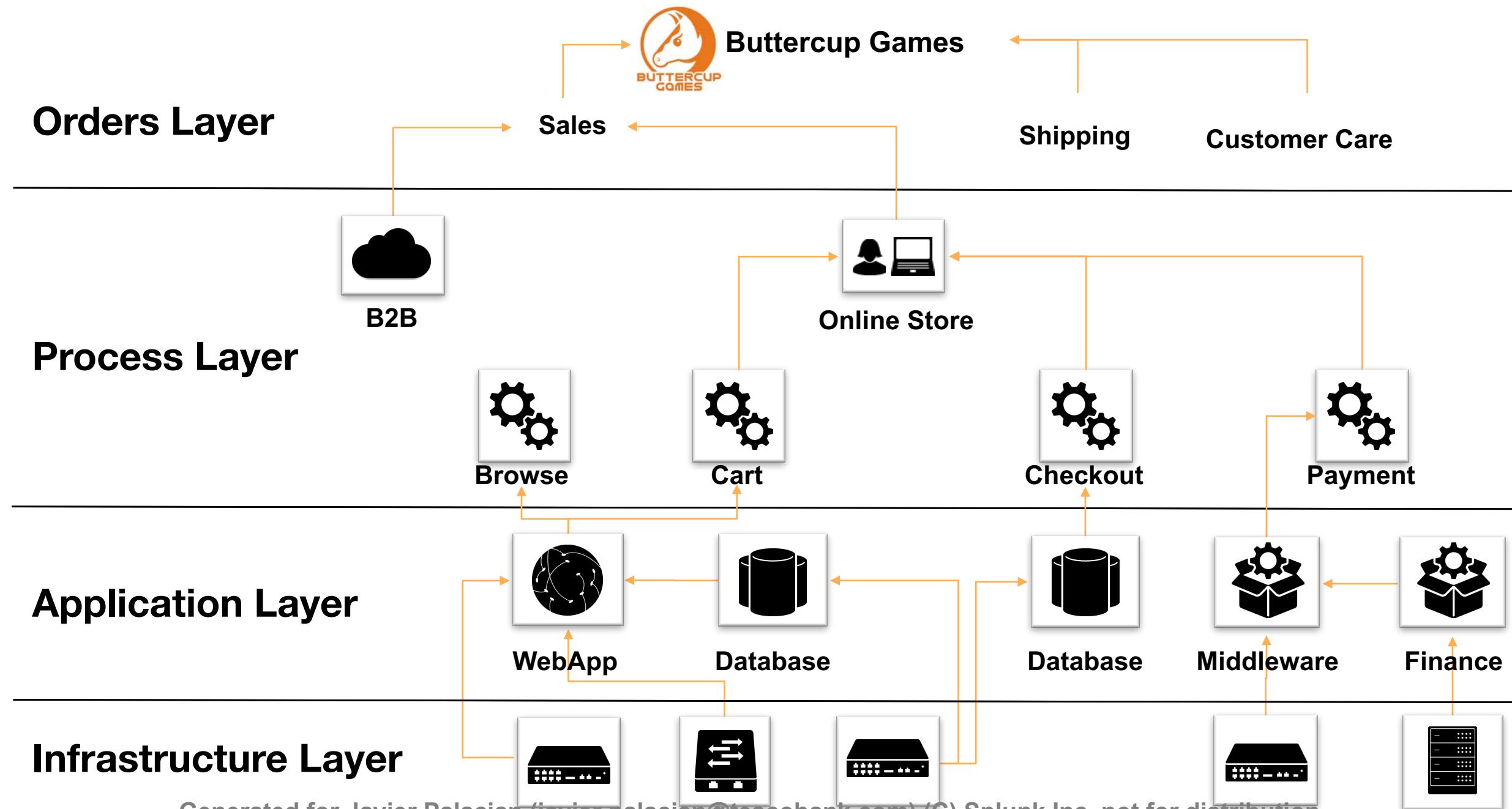
3 ➔ Evaluation

Generated for Javier Palacian (javier.palacian@tescobank.com) (C) Splunk Inc, not for distribution

Appendix

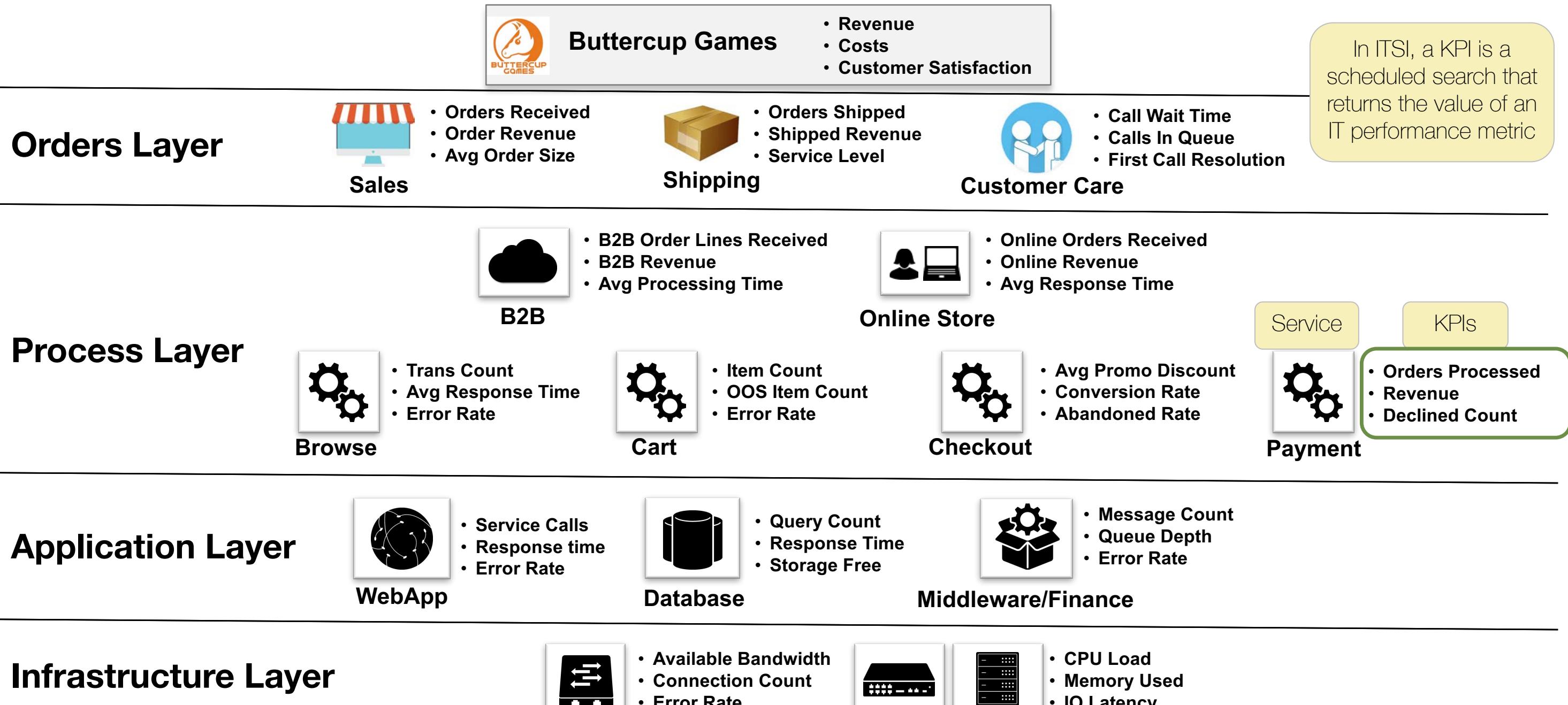
Generated for Javier Palacian (javier.palacian@tescobank.com) (C) Splunk Inc, not for distribution

Buttercup Games Service Layers



Generated for Javier Palacian (javier.palacian@tescobank.com) (C) Splunk Inc, not for distribution

Services & KPIs: Key Performance Indicators



ITSI Modules

- Help users understand and act on data that comes from monitoring services within ITSI
 - Each ITSI Module contains its own predefined metrics, entities, service configurations, and activity views
 - Modules can include entity discovery key performance indicator (KPI) templates, metrics, or entity level drilldowns
- Splunk add-ons
 - Add-ons collect host, network, and other data from computers, and map it to a data model.
 - Add-ons power the data underlying module metrics and entities

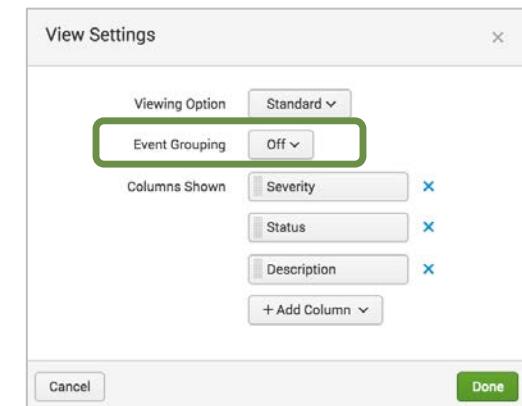
Anomaly Detection (AD)

- Useful if the KPI doesn't spike out of range, but begins to behave atypically within a tolerable range
 - Uses machine learning on past data to model the KPI pattern
 - If new data diverges from the model, a notable event is created
 - After 24 hours anomaly detection data is available for use
 - AD continues to use data to update optimal sensitivity
- Example: Online sales volume
 - Usually follows a sine wave each business day: peak load in the early evening and low load in early morning
 - If it “flatlines” at medium load: no status-based alert, but because the pattern is atypical, AD will notice and create a notable event

Generated for Javier Palacian (javier.palacian@tescobank.com) (C) Splunk Inc, not for distribution

Grouping and Aggregation Policies

- Visual grouping of events across the service stack
 - Manage high numbers of outages and instances
 - Help separate causes from symptoms
- Can be set up to trigger automated actions, like changing notable event status, ownership, running scripts, or sending emails
- If enabled by your admin, default policy groups all notable events by source: name of the correlation search that created the notable event
 - Admins can also manually control grouping with aggregation policies
 - <http://docs.splunk.com/Documentation/ITSI/latest/User/CreateAggregationPolicies>



Generated for Javier Palacian (javier.palacian@tescobank.com) (C) Splunk Inc, not for distribution

Default Grouping Policy

Default Policy Smart Mode

Applies to events which fail to meet the criteria of any other active policy

Grouping Factors

Grouping Factors

Machine learning is used to group notable events based on the similarity of text and categorical factors.

Adjust the importance of each factor:

4 Fields Selected to analyze event similarity

Textual Similarity: 0 Less Important ————— 1 More Important

Categorical Similarity: 0 Less Important ————— 1 More Important

Split events by field

Split events into multiple groups by field name Separate multiple fields by commas

Break group

If the flow of events into the group paused for 7200 in seconds

Group information

Group Title: Same as the first event

Group Description: Same as the first event

Group Severity: Same as the first event

Group Assignee: Same as the first event

Group Status: Same as the first event

Group types for Last 24 hours:

#	Count	Summary	Similar Texts	Similar Fields
1	30	30/91 events are grouped because they share 3 (relatively high) common field values.	event_id, identifier, hash=2dbc9c34ec73cd3857d1805e8a3b4c3cd2383ed11e7e681275c0dc27d8e9b0e	title=Errors Impacting Revenue; service_ids=95c99846-404f-4c92-9923-2a8cb894bff1,bc8f2697-39f0-4d8e-ac77-91a2999b2a9c,09dd51c2-9fc7-4aa4-9f39-da59ac6b6244
2	37	37/91 events are grouped because they share 2 (relatively high) common field values.	None	service_ids=09dd51c2-9fc7-4aa4-9f39-da59ac6b6244; title=Service level alert on KPI: CPU Load %
3	3	3/91 events are grouped because they share 3 (relatively high) common field values.	description=Response Times and Active Users status was critical (Health Score=10.0) at 2017-04-04 12:48:00.000 PM	service_ids=95c99846-404f-4c92-9923-2a8cb894bff1,09dd51c2-9fc7-4aa4-9f39-da59ac6b6244,bc8f2697-39f0-4d8e-ac77-91a2999b2a9c; title=Response Times Impacting Active Users
4	3	3/91 events are grouped because they share 3 (relatively high) common field values.	description=Response Times and Active Users status was high (Health Score=26.67) at 2017-04-04 11:49:00.000 AM	service_ids=95c99846-404f-4c92-9923-2a8cb894bff1,09dd51c2-9fc7-4aa4-9f39-da59ac6b6244

- You can view the standard default grouping policy to understand how notable events are being grouped.
- Admins can create custom aggregation policies

Generated for Javier Palacian (javier.palacian@tescobank.com) (C) Splunk Inc, not for distribution

Multi KPI Alerts

- Multi KPI alerts generate notable events based on one or more KPI values
- KPIs used in an alert can come from more than one service
- A condition you want to be alerted to may depend on the relationship between two or more KPIs
- There are two types of multi KPI alerts
 - Composite
 - Status over time (comparing two or more KPIs for intervals of time)

Multi KPI Alert Examples

- Simple: alert that fires if a given KPI is critical
- More complex: if KPI 1 is normal, but KPI 2 is worse than high, fire an alert (status comparison over intervals of time)
- Example:
 - Web server CPU utilization is poor (`alert_level = high or more`), but visits are `alert_level = normal` (i.e., lots of traffic)
 - ▶ This will lead to poor customer experience due to slow response
 - ▶ Generate a notable event to alert the team

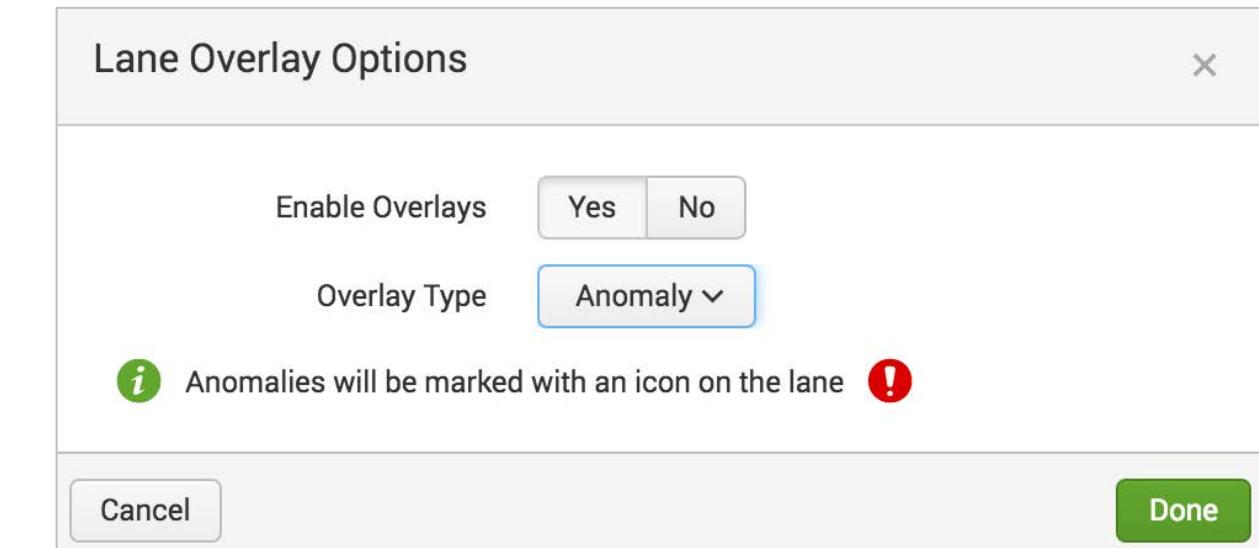
Types of Multi KPI Alerts

- Composite score:
 - Calculates a combined health score of all the KPIs added to the alert
 - Notable event will be created if the combined score is too high or low
 - Example: Combination of web server latency, load time, and CPU load indicates poor customer experience likely
- Status over time:
 - Compare two or more KPIs
 - Create a notable event based on trigger conditions
 - Example: customer visits: KPI is normal, but purchases KPI is low

Adding Anomaly Lane Overlays

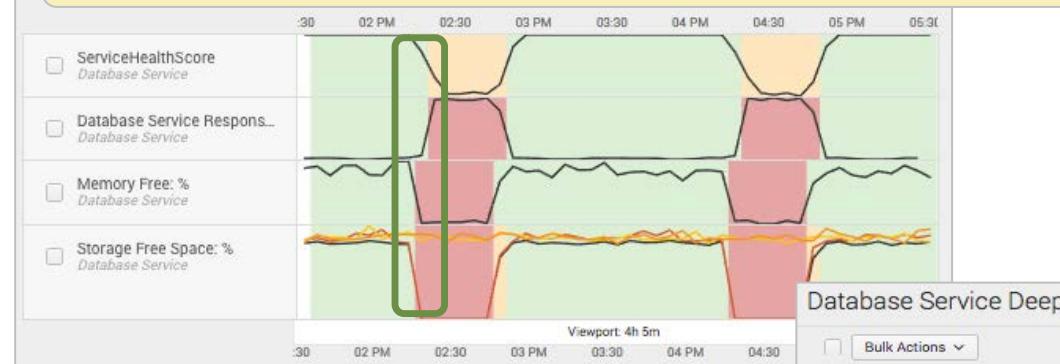
Only available for KPIs with anomaly detection enabled

1. Click the  icon and select **Lane Overlay Options**
2. Select Yes to enable overlays, and select **Anomaly** for the Overlay Type
3. Click **Done**



Deep Dive to Multi KPI Alert

1 Find a Deep Dive condition that would be a useful alert



2 Click-and-drag to zoom to specify the change threshold (orange or yellow) for which you want to trigger the alert



3 Click **Bulk Actions > Create Multi KPI Alert**



Generated for Javier Palacian (javier.palacian@tescobank.com) (C) Splunk Inc, not for distribution

Deep Dive to Multi KPI Alert (cont.)

The screenshot shows the Splunk Multi KPI Alerts interface. On the left, there's a sidebar with service categories like Buttercup Store, Database Service, and others. The main area has three tabs:

- 1. Services:** Shows a list of services with checkboxes to select them.
- 2. KPIs in Selected Services:** A table showing KPIs for the selected services, including ServiceHealthScore, CPU Utilization, Database Service Errors, Requests, Response Time, Memory Free, Network Utilization, and Storage Free Space. Each row includes a '+ Add' button and a status bar.
- 3. Selected KPIs:** A table showing the selected KPIs with checkboxes to remove them. It also displays a note about trigger conditions and a 'Save' button.

A yellow callout bubble points to the 'Save' button in the bottom right of the third section, with the text: "Analysts can view these windows for your reference, but cannot save a Multi KPI alert unless your admin grants you access."

A red circle labeled **4** points to the 'Save' button in the top right of the main window, with the text: "Multi KPI Alerts window opens. Click **Save**".

A red circle labeled **5** points to the 'Save' button in the bottom right of the 'Create Correlation Search' window, with the text: "Admin names the alert search and the notable event and clicks **Save**".

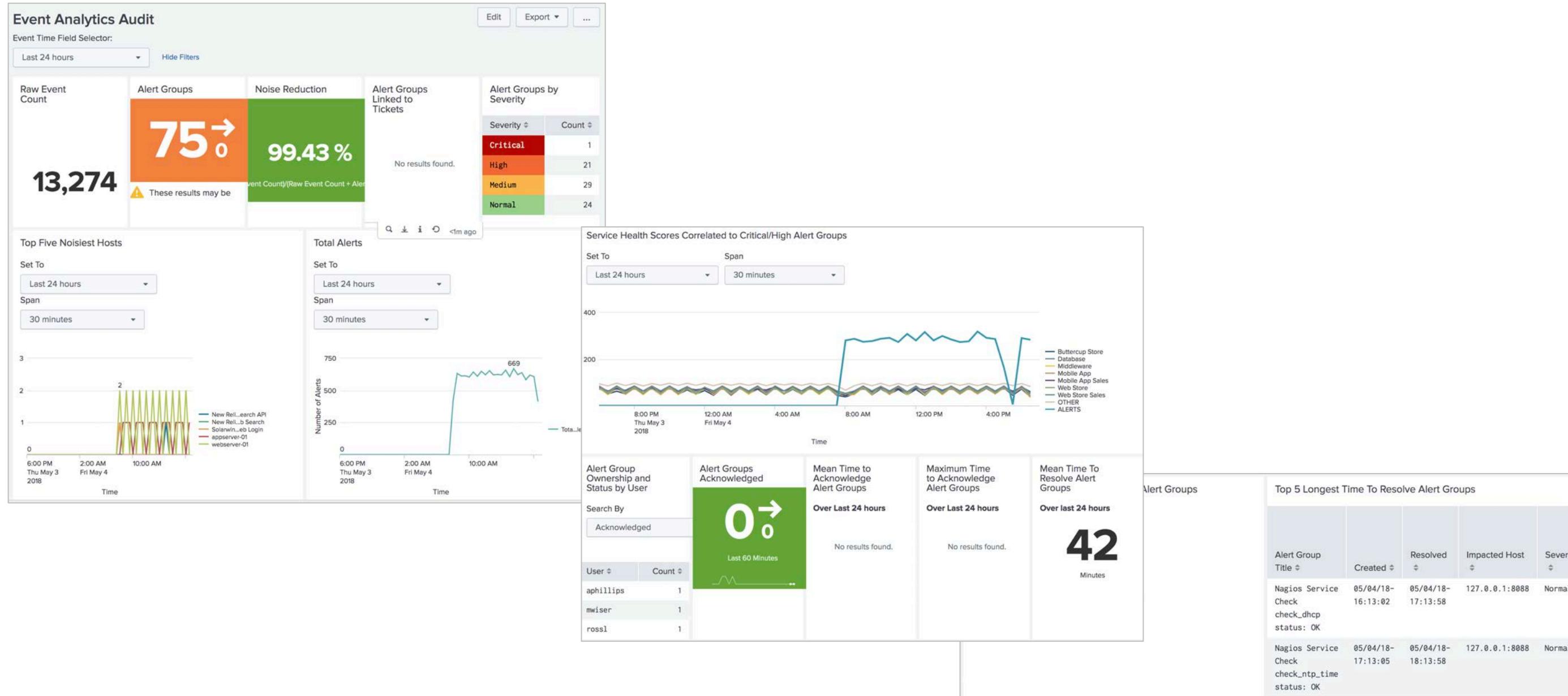
Create Correlation Search

- Search Name:
- Notable Event Title: Supports field substitution in the format of %fieldname%
- Notable Event Description: %event_description% Supports field substitution in the format of %fieldname%
- Schedule Type: Basic Cron
- Run Every: 5 minutes
- Time range: Last 60 minutes
- Severity: Medium

Cancel

Generated for Javier Palacian (javier.palacian@tescobank.com) (C) Splunk Inc, not for distribution

Event Analytics Audit Dashboard



Generated for Javier Palacian (javier.palacian@tescobank.com) (C) Splunk Inc, not for distribution

Event Analytics Audit Dashboard

2 Select a Service

3 For each algorithm, select the algorithm and study the graphs

4

5 Select a time range

6 For each model, click a model and study the graphs

7 Use the best-performing model to predict the service health score

8 Save the prediction as an alert to potential service issues

INSTRUCTIONS

TRAIN

TEST

Machine Learning Algorithms:

- The Linear Regression algorithm fits a straight line to your data.
- The Random Forest Regressor algorithm takes the inputs (KPIs and historical service health scores).
- The Gradient Boosting Regressor algorithm uses a loss function to fit a line to your data, a decision tree.

Note: The decision to use a particular algorithm usually depends on the type of KPI data in your environment.

Service Health Score and KPIs Over Time

Distribution of Service Health Score Values

Fit Model

Time Period: Last 60 minutes

Click on model name to test

type #: GradientBoostingRegressor

model_name #: itsi_predict_web_store_GradientBoostingRegressor

LinearRegression

RandomForestRegressor

R² and RMSE

rSquared: 0.99

RMSE: 1.51

Actual vs. Predicted Service Health Score

Residual Error Histogram

USE

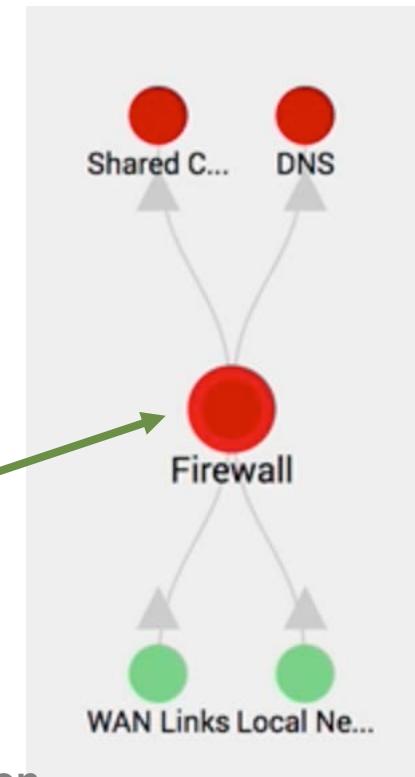
Predicted service health score in 20-30 minutes: 99

27m ago

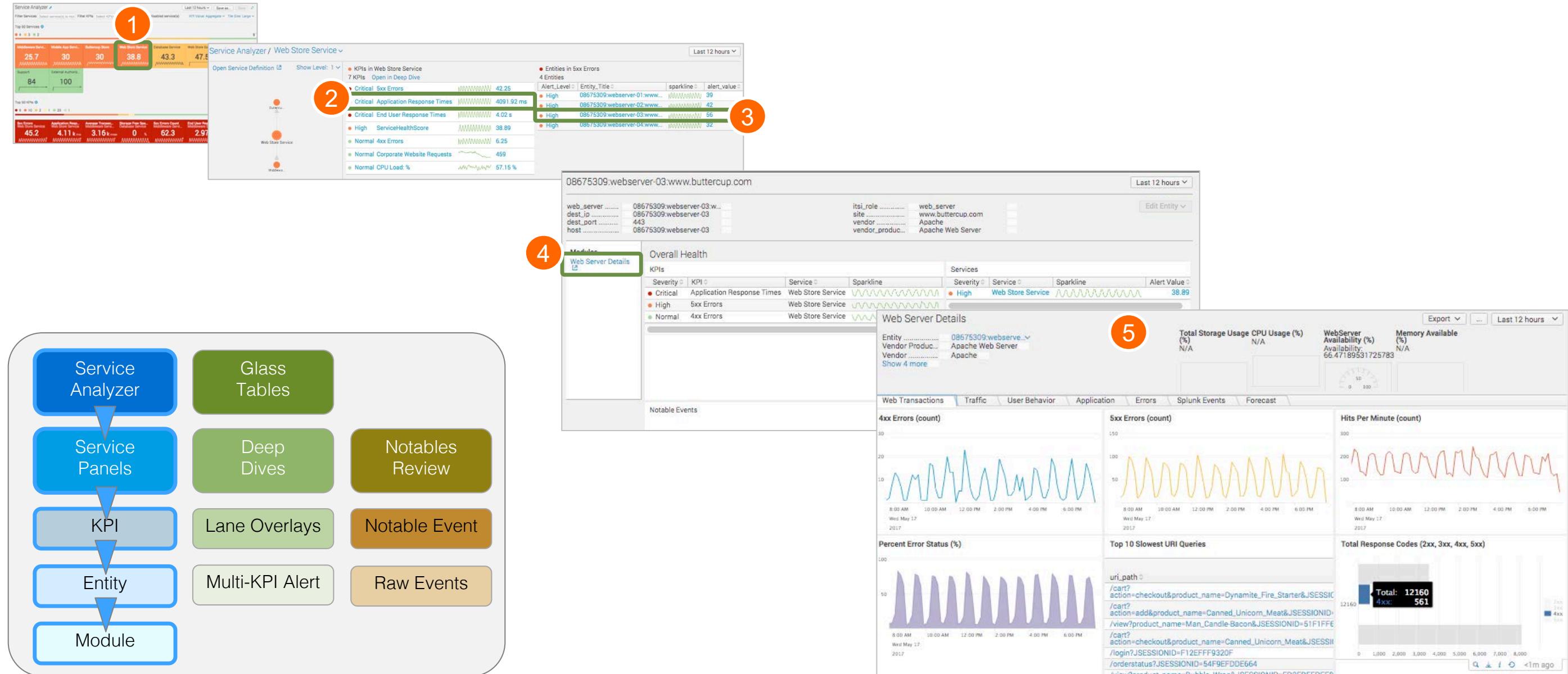
Other Troubleshooting Workflows

- Service Analyzer > Service > KPI > view Entities
- Service Analyzer > Service > KPI > Deep Dive > Bulk Actions or  > Entity Overlay > view Entity or view Module
- Notable Events Review > Notable Event > Deep Dive ...
- Glass Table > Deep Dive >
 - Enable Overlays (for the KPI with the issue)
 - Identify hosts
 - drilldown to raw data

When troubleshooting,
**drill down until you find
the bottom of the tree:**
the deepest item whose
dependencies are all green



SA > Service > KPI > Entities > Module



Generated for Javier Palacian (javier.palacian@tescobank.com) (C) Splunk Inc, not for distribution

SA>Deep Dive>Bulk Actions>Overlay>Module

The screenshot illustrates the Splunk Service Analyzer interface with several key features highlighted:

- 1**: Top navigation bar with service filters and search controls.
- 2**: Service tree view showing the hierarchy from Business down to Web Store Service.
- 3**: Deep Dive view for the Web Store Service, showing KPIs and alert details.
- 4**: Bulk Actions dropdown menu.
- 5**: Lane Overlays configuration panel.
- 6**: Overlay as Lane button and resulting Lane Overlay view.

Conceptual Diagram (Bottom Left):

```

graph TD
    SA[Service Analyzer] --> SP[Service Panels]
    SA --> KPI[KPI]
    SA --> E[Entity]
    SA --> M[Module]
    SP --> DDD[Deep Dives]
    KPI --> LO[Lane Overlays]
    E --> MKA[Multi-KPI Alert]
    DDD --> LO
    DDD --> NE[Notable Event]
    DDD --> RE[Raw Events]
    
```

The Lane Overlay view on the right displays various performance metrics and alerts for the Web Store Service, including:

- Metrics:** ServiceHealthScore, 4xx Errors, 5xx Errors, Application Response Times, End User Response Times, CPU Load %.
- Alerts:** Critical 5xx Errors, Critical Application Response Times.
- Overlays:** Lane overlays for different entities and thresholds.
- Details:** Web Server Details, including IP Address, Site, Vendor Product, Version, and various performance graphs (e.g., 4xx Errors count, 5xx Errors count, Hits Per Minute).

Generated for Javier Palacian (javier.palacian@tescobank.com) (C) Splunk Inc, not for distribution

Notable Events Review > NE > Deep Dive

The screenshot shows the Splunk Notable Events Review interface. On the left, there is a navigation menu with various service monitoring components:

- Service Analyzer
- Glass Tables
- Service Panels
- Deep Dives (highlighted with a red circle containing '3')
- Notables Review (highlighted with a red circle containing '1')
- KPI
- Lane Overlays
- Multi-KPI Alert
- Raw Events
- Entity
- Module

A blue arrow points from the 'Deep Dives' button to the 'Notables Review' button. Another blue arrow points from the 'Notables Review' button to a specific event in the list.

The main area displays a list of notable events. One event is highlighted with a green border:

NewRelic Health Status: API Order Status Wed May 17 20:15:04 PM Unassigned Critical New API Order Status status = red

NewRelic Health Status: API Checkout Wed May 17 20:15:04 PM Unassigned Critical New API Checkout status = red

... (other unhighlighted events)

To the right of the list, a detailed view of the highlighted event is shown:

Acknowledge

NewRelic Health Status: API Checkout Wed May 17 2017 20:15:04 GMT-0700 (PDT)
Owner: unassigned Severity: Critical Status: New D. [button]
NewRelic Health Status: API Checkout Wed May 17 2017 20:15:04 GMT-0700 (PDT)
Owner: unassigned Severity: Critical Status: New D. [button]
NewRelic Health Status: API Checkout Wed May 17 2017 20:15:04 GMT-0700 (PDT)
Owner: unassigned Severity: Critical Status: New D. [button]
NewRelic Health Status: API Checkout Wed May 17 2017 20:15:04 GMT-0700 (PDT)
Owner: unassigned Severity: Critical Status: New D. [button]
NewRelic Health Status: API Checkout Wed May 17 2017 20:15:04 GMT-0700 (PDT)
Owner: unassigned Severity: Critical Status: New D. [button]
NewRelic Health Status: API Checkout Wed May 17 2017 20:15:04 GMT-0700 (PDT)
Owner: unassigned Severity: Critical Status: New D. [button]
NewRelic Health Status: API Checkout Wed May 17 2017 20:15:04 GMT-0700 (PDT)
Owner: unassigned Severity: Critical Status: New D. [button]
NewRelic Health Status: API Checkout Wed May 17 2017 20:15:04 GMT-0700 (PDT)
Owner: unassigned Severity: Critical Status: New D. [button]
NewRelic Health Status: API Checkout Wed May 17 2017 20:15:04 GMT-0700 (PDT)
Owner: unassigned Severity: Critical Status: New D. [button]
NewRelic Health Status: API Checkout Wed May 17 2017 20:15:04 GMT-0700 (PDT)
Owner: unassigned Severity: Critical Status: New D. [button]
NewRelic Health Status: API Checkout Wed May 17 2017 20:15:04 GMT-0700 (PDT)
Owner: unassigned Severity: Critical Status: New D. [button]
NewRelic Health Status: API Checkout Wed May 17 2017 20:15:04 GMT-0700 (PDT)
Owner: unassigned Severity: Critical Status: New D. [button]

Description
API Checkout status = red

Contributing KPIs Open all in Deep Dive

Possible Affected Services Open all in Deep Dive

- Middleware Service
- Web Store Service

Drilldowns
None

Details

```
key_transaction.id: 15498  
key_transaction.end_user_summary.apdex_score: 0.0  
key_transaction.application_summary.host_count: 3  
key_transaction.application_summary.instance_count: 3  
key_transaction.application_summary.error_rate: 100.0  
timestamp: none  
is_use_event_time: 0  
key_transaction.reporting: true  
severity: 5  
mod_time: 1495077304.7  
key_transaction.application  
key_transaction.end_user  
key_transaction.transaction  
key_transaction.health_status: red  
key_transaction.application  
status: 5  
key_transaction.end_user  
orig_severity: 5  
key_transaction.name: API  
key_transaction.application  
search_name: New Relic
```

Title

Bulk Actions

KPI Calculation Metric: Average ▾ + Add Lane ▾ Compare to ... ▾

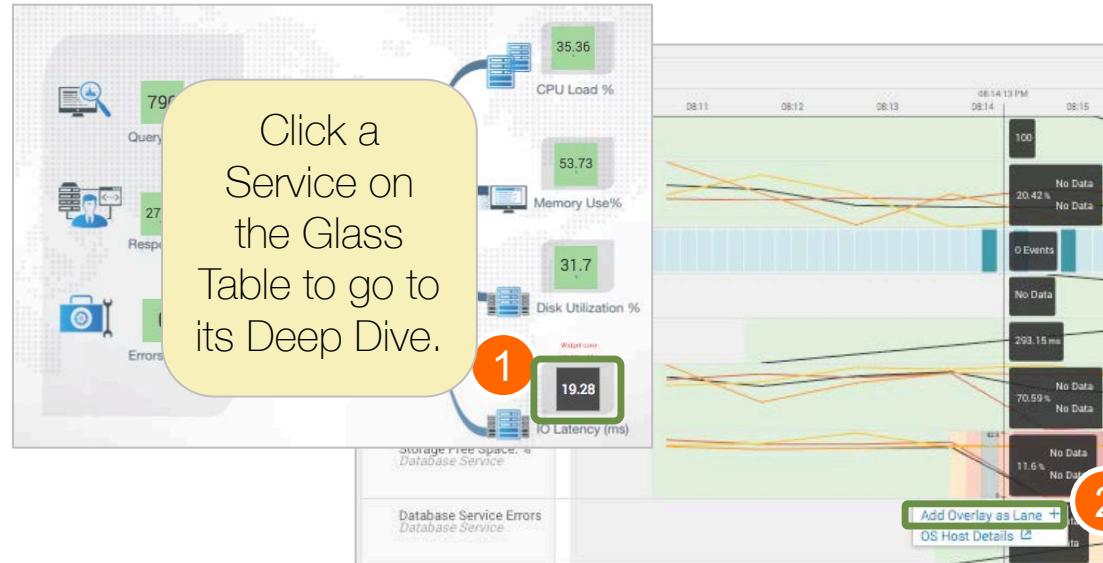
Focus: Web Store Service ▾

Last 24 hours ▾ Save as... ▾ Save ▾

The interface also includes a timeline chart showing ServiceHealthScore for 'Middleware Service' and 'Web Store Service' over a 24-hour period, and a sidebar with KPIs for 'Web Store Service' including '4xx Errors' and '5xx Errors'.

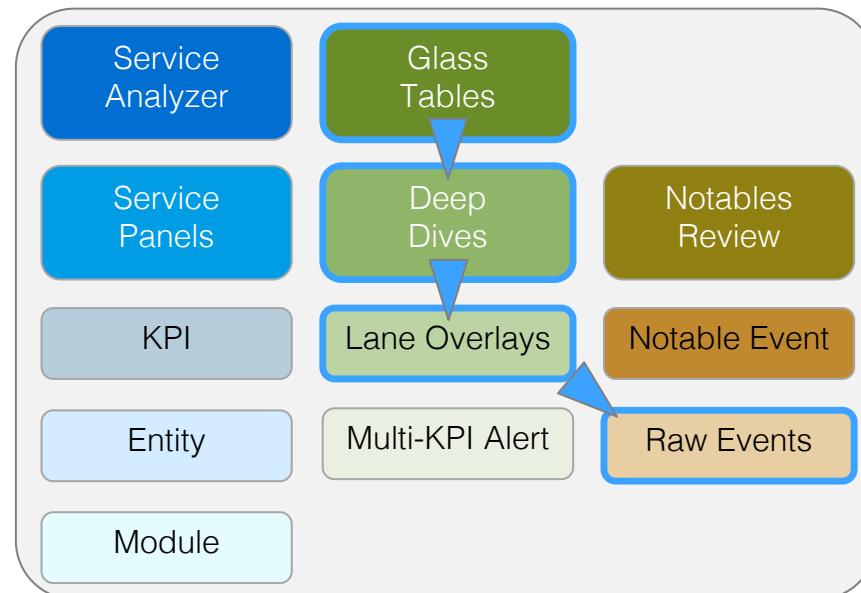
Generated for Javier Palacian (javier.palacian@tescobank.com) (C) Splunk Inc, not for distribution

Glass Table>Deep Dive>Overlay>Drilldown

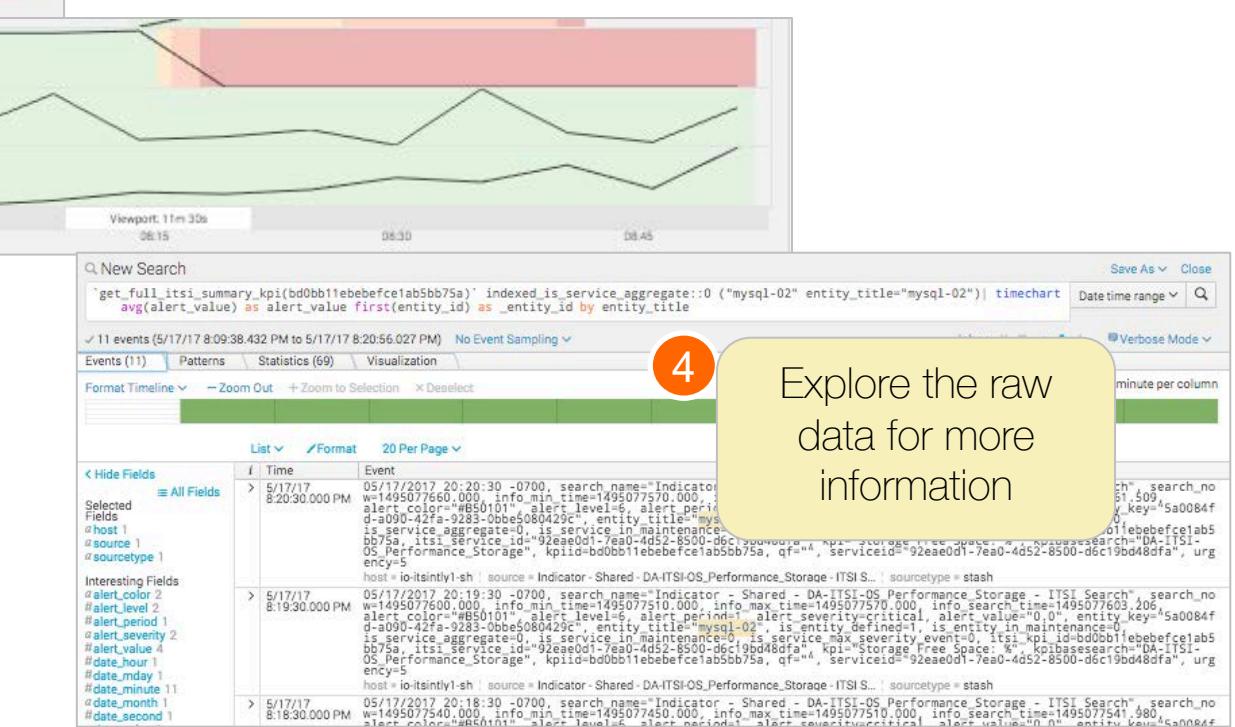


Click and drag along the timeline to zoom in on the time when the problem starts. In the KPI with the first issue, click the settings icon and select **Add Overlay as Lane**

Click the settings icon, and click **Open in Search**



Because they enable you to examine the state of your business services at a specific moment in time, you can start with Glass Tables to analyze the impact of an outage (determine which services are affected and to what degree). You can quickly create a glass table for an issue and use it in the war room.



Generated for Javier Palacian (javier.palacian@tescobank.com) (C) Splunk Inc, not for distribution