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

Recommended Course Prerequisites

- Splunk Fundamentals 1

  or

- Equivalent Splunk Experience

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

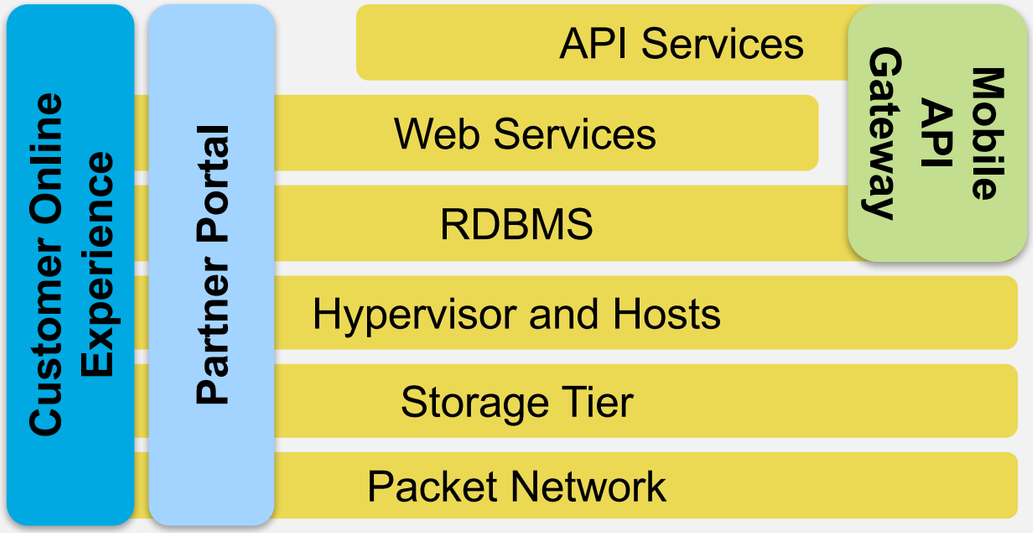
Objectives

- 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

An ITSI service is a collection of KPI (key performance indicator) values, combined into a single service health score



- 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

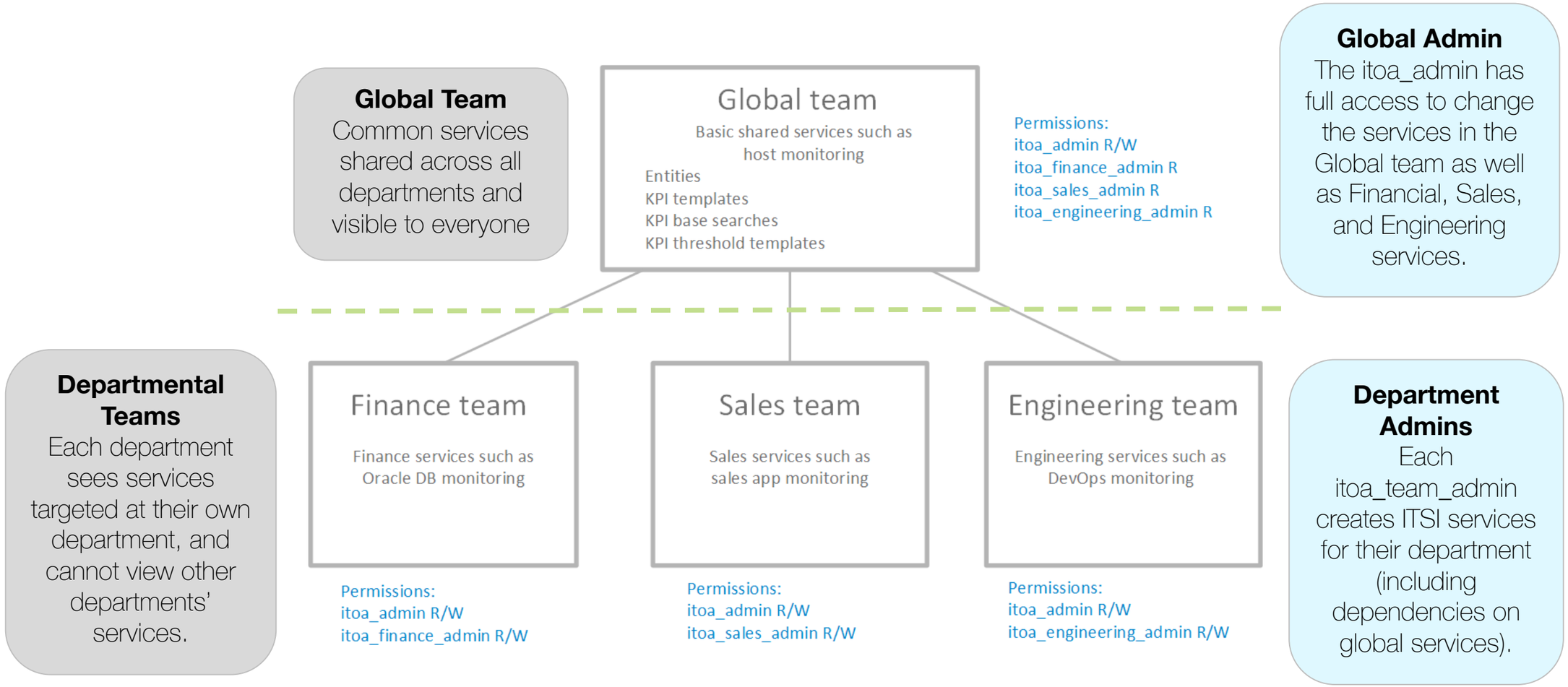
Goal: Monitor the entire system and reduce connectivity issues and systems downtime

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

Teams Have Their Own Views in ITSI

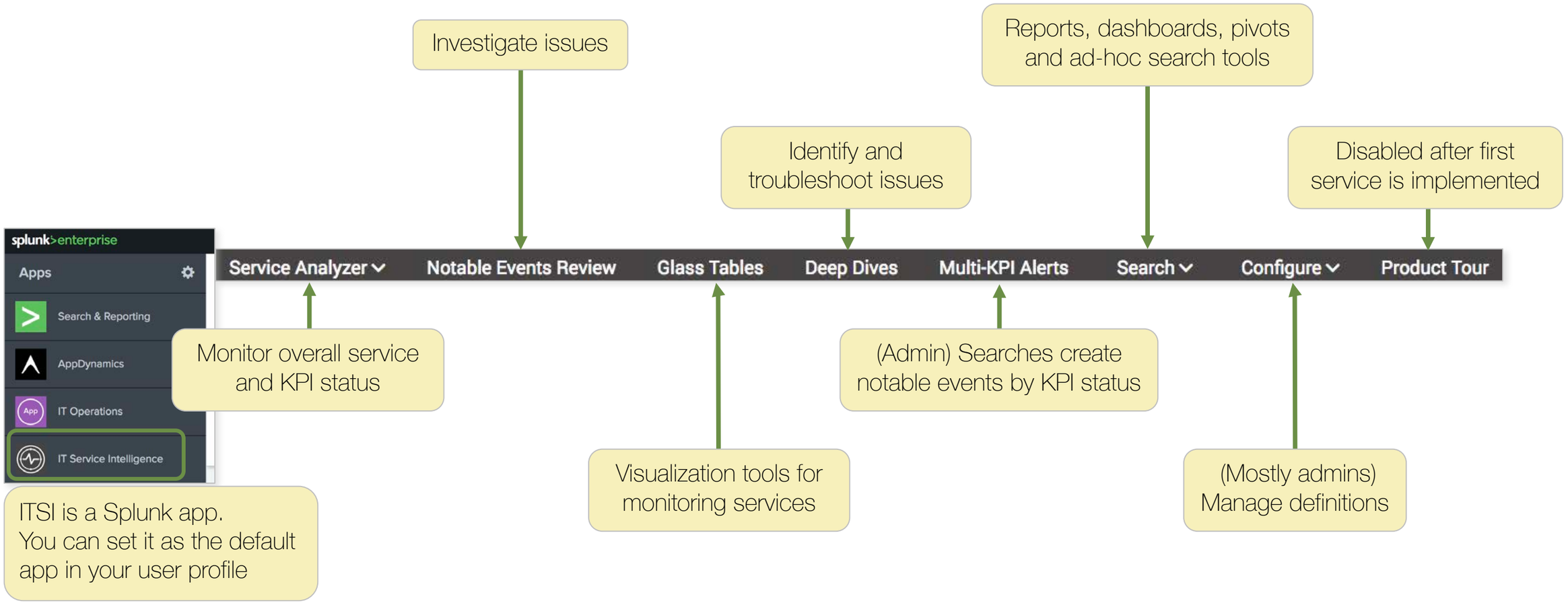


IT Service Intelligence Roles

Role	Description
itoa_user	Views most of ITSI and creates *private* glass tables or deep dives
itoa_analyst	itoa_user, plus owns notable events
itoa_team_admin	itoa_analyst, and creates *shared* 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**

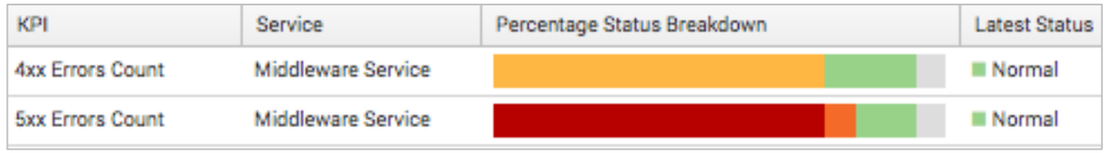
Accessing IT Service Intelligence / Menus



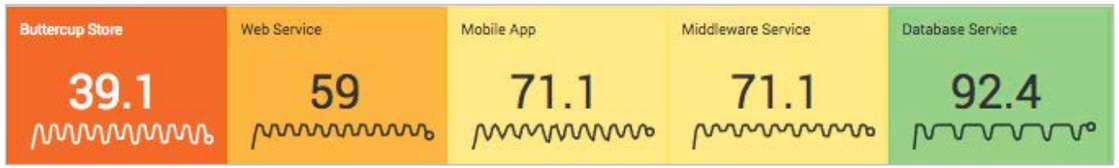
ITSI KPI and Service Health Scores

Scores = alert levels

- A **KPI** (Key Performance Indicator) is a numeric measurement of one factor affecting a service

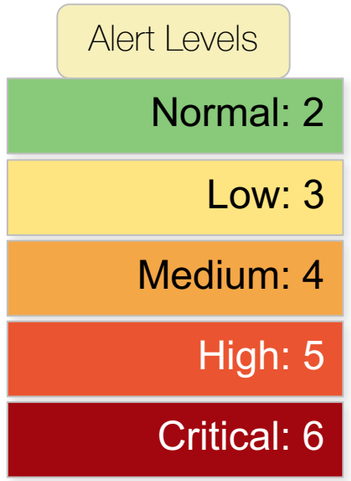


- A service's overall status is displayed as a **service health score**
  - Values 0 to 100
  - Higher values = better
  - Service health score = aggregation of the status of multiple KPIs' alert thresholds as set by your admin

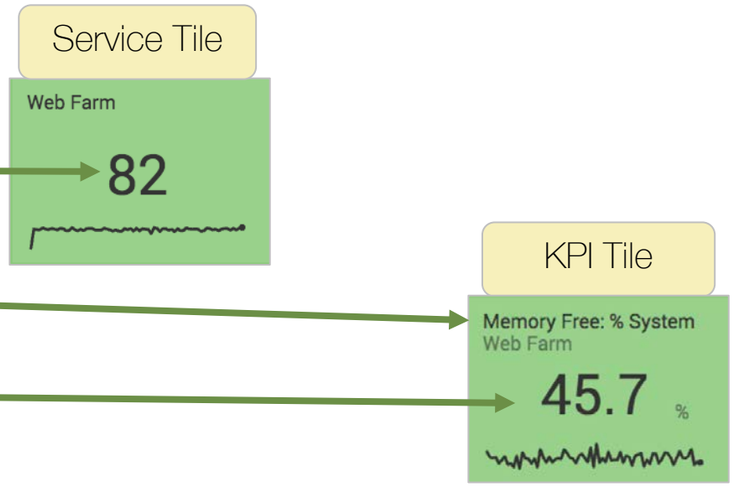


Service Analyzer: Service and KPI Tiles

- A tile's color is 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



How Key Performance Indicators Work

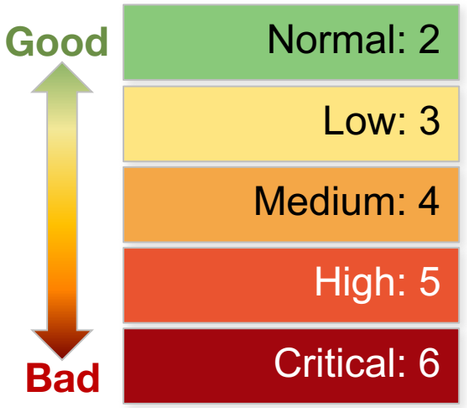
- Each KPI in a service has these settings:
  - Schedule: Interval can be measured from every 1 to 15 minutes; Range of measurement can be from 1 minute to 1 day
  - Search expression example: `sourcetype=access_combined_wcookie`
  - Calculation: summarizes fields in the events to generate the KPI numeric 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

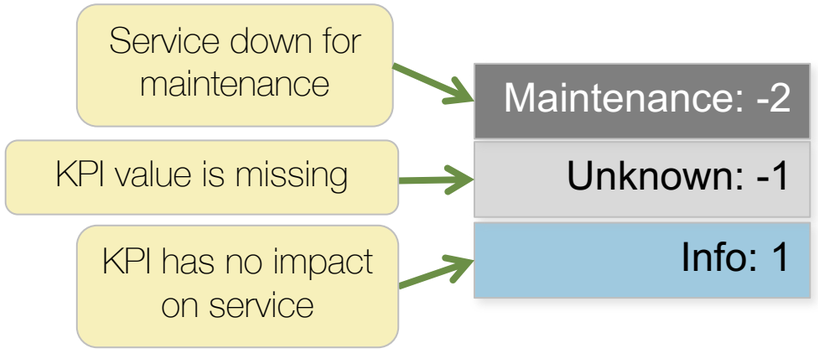
KPI Importance Weight

- 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

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

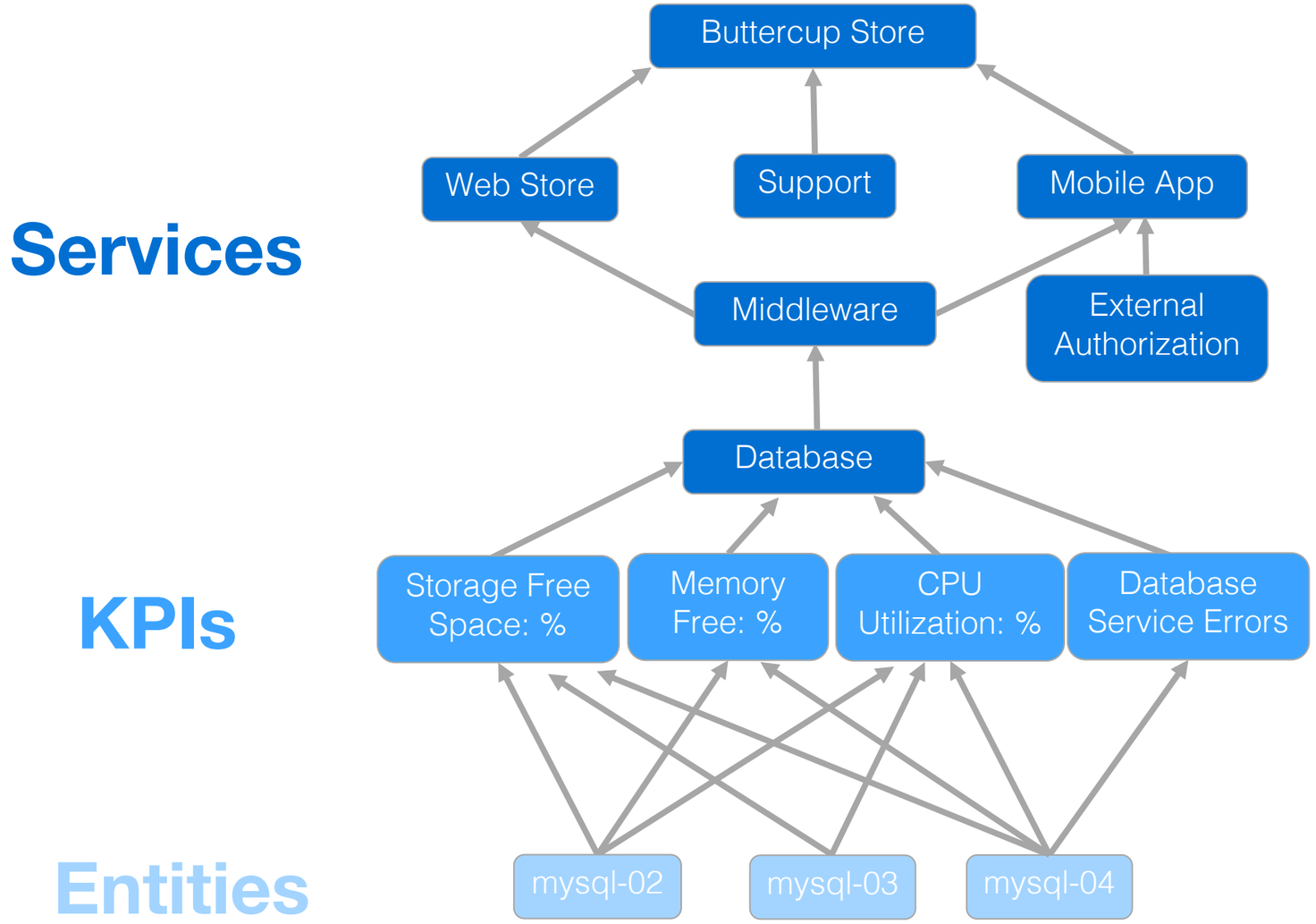




ITSI Entities

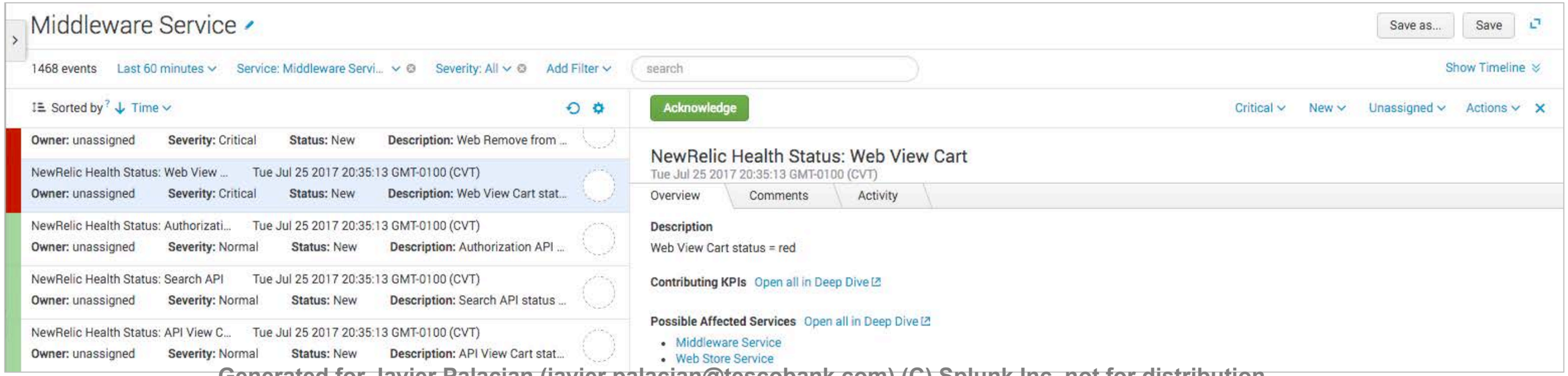
- In creating services, your admins may also (optionally) define entities: IT components on which a service depends
  - Like a configuration item in the ITIL framework
  - An entity is never a service
  - Examples: virtual or physical server, AD/LDAP user, OS process
  - Entities may have multiple identifiers
    - 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

Flexible Dependency Mappings in ITSI



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



What is Service Monitoring?

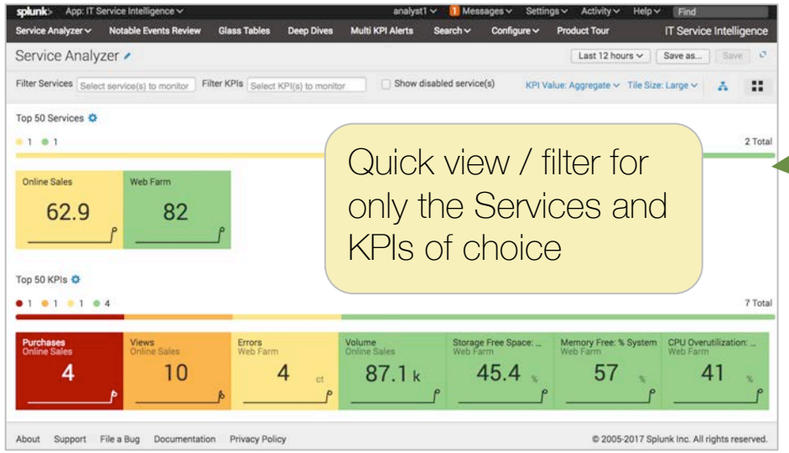
- Aggregated health of a layer is less important
- Service health is determined by the health of the components of each layer upon which that service depends

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

Service Status

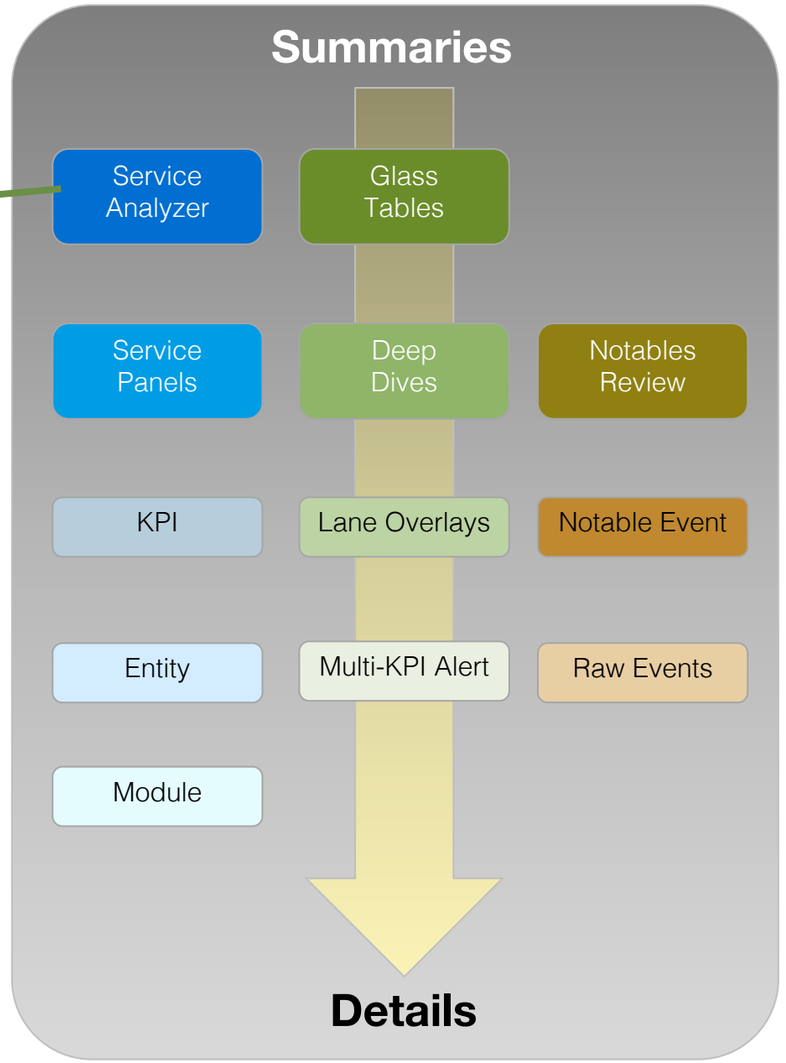
Outage

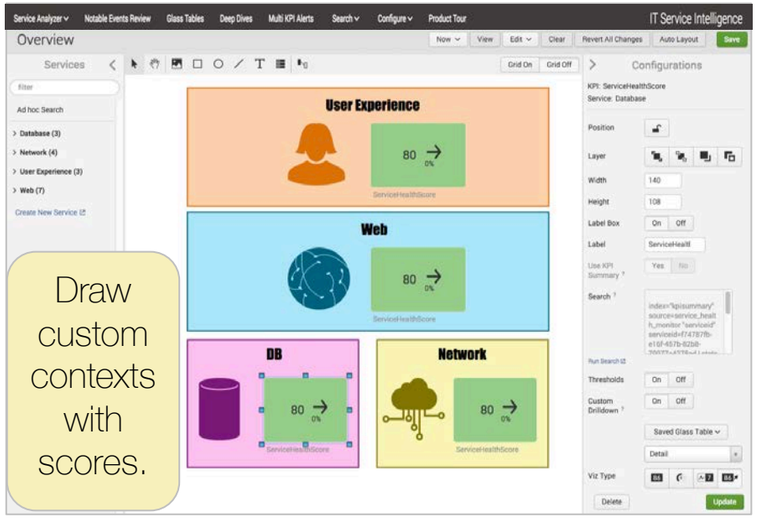
ITSI User Interface: Summaries to Details



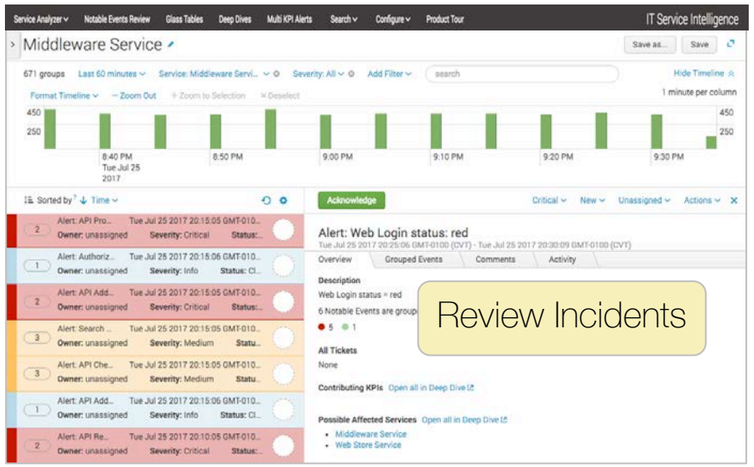
Quick view / filter for only the Services and KPIs of choice

Investigate when things go wrong

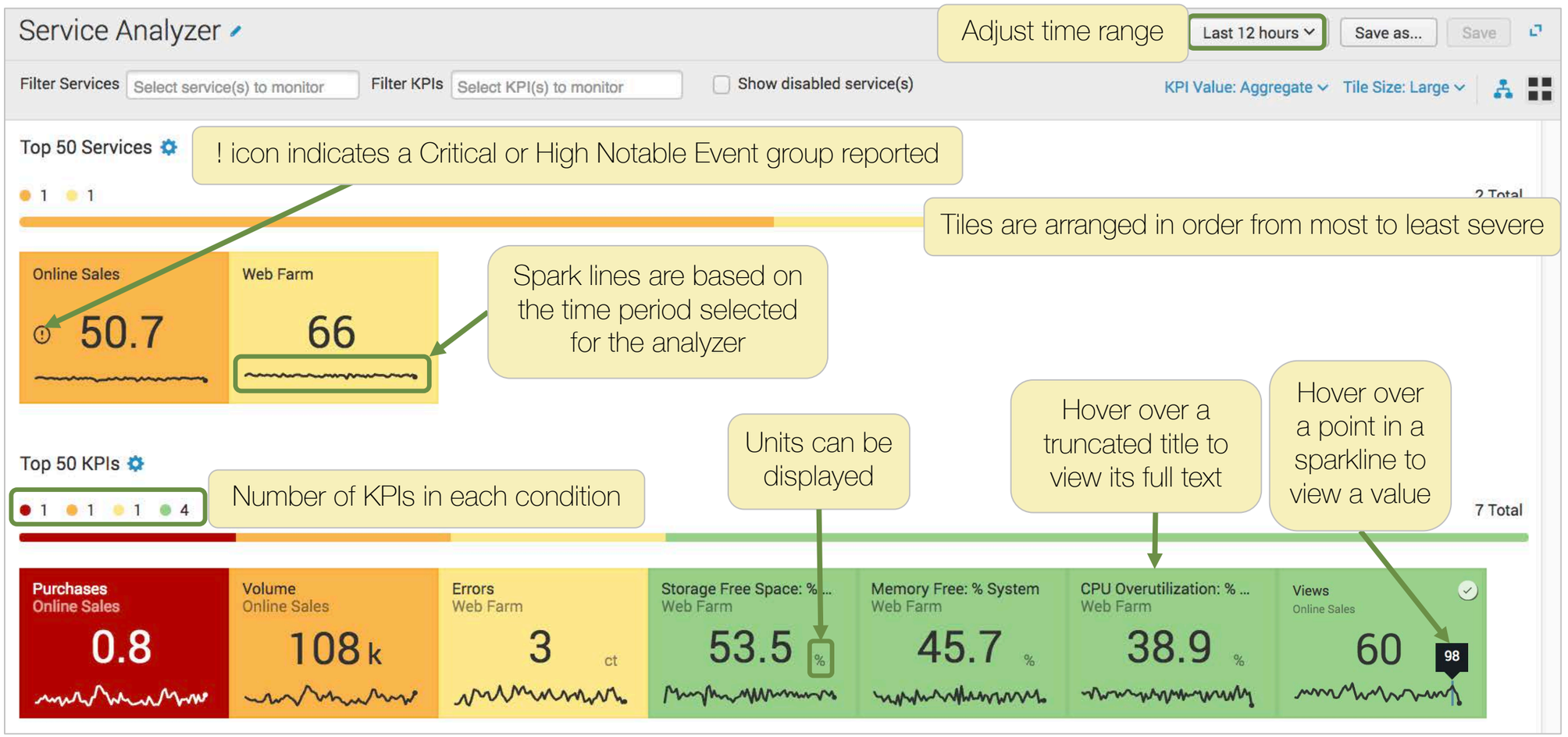




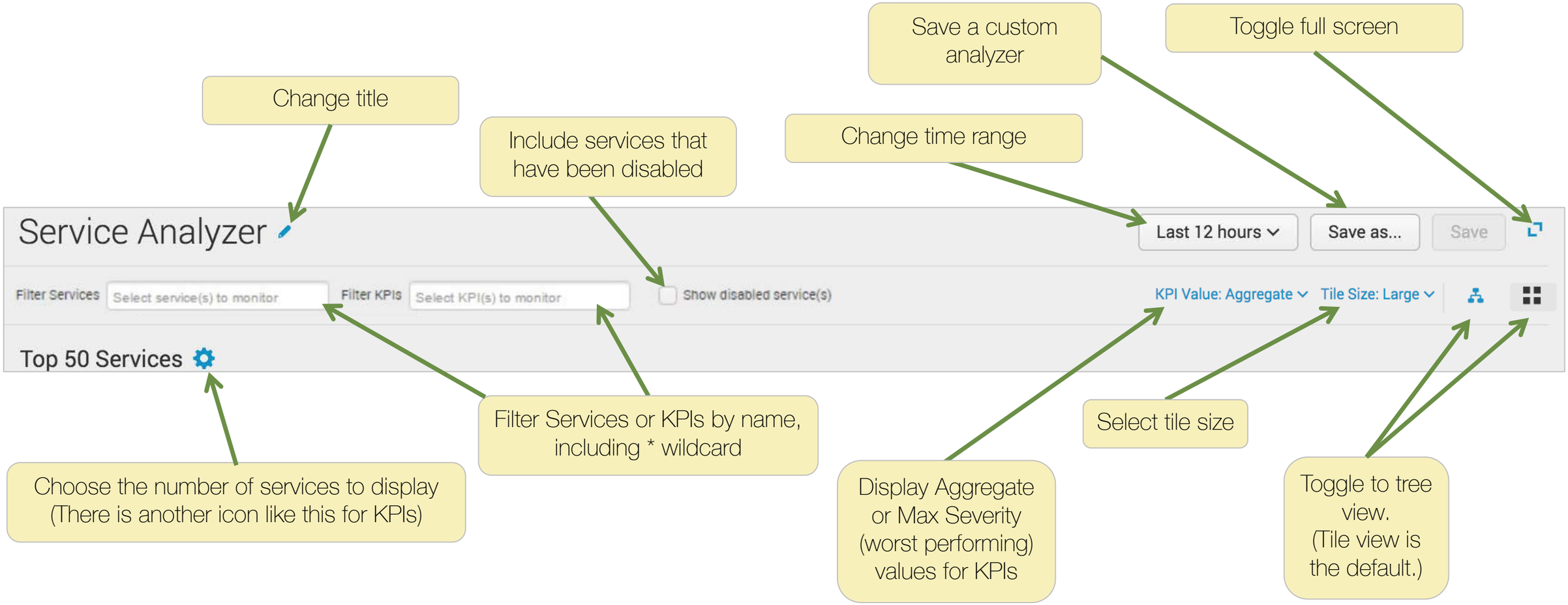
Draw custom contexts with scores.



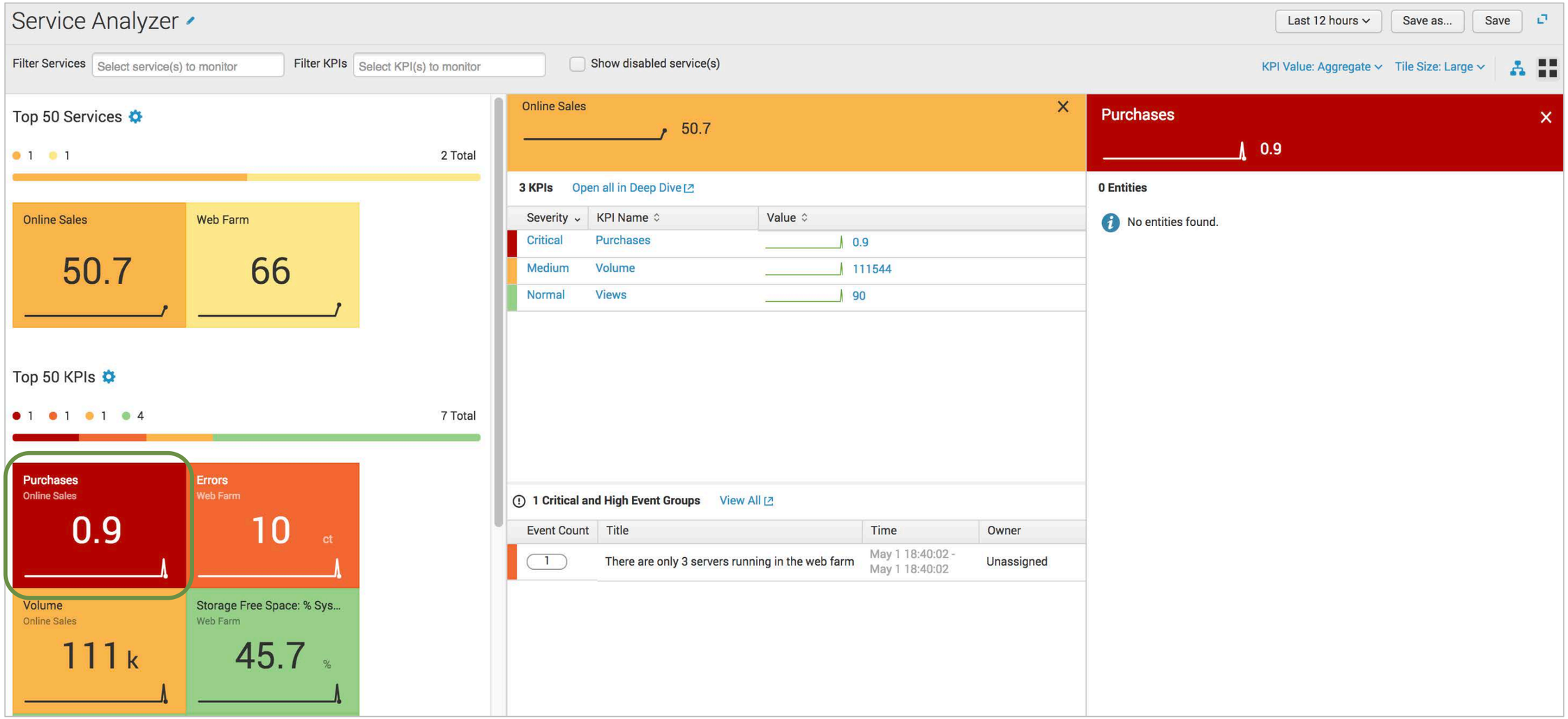
Service Analyzer Display



Service Analyzer Controls

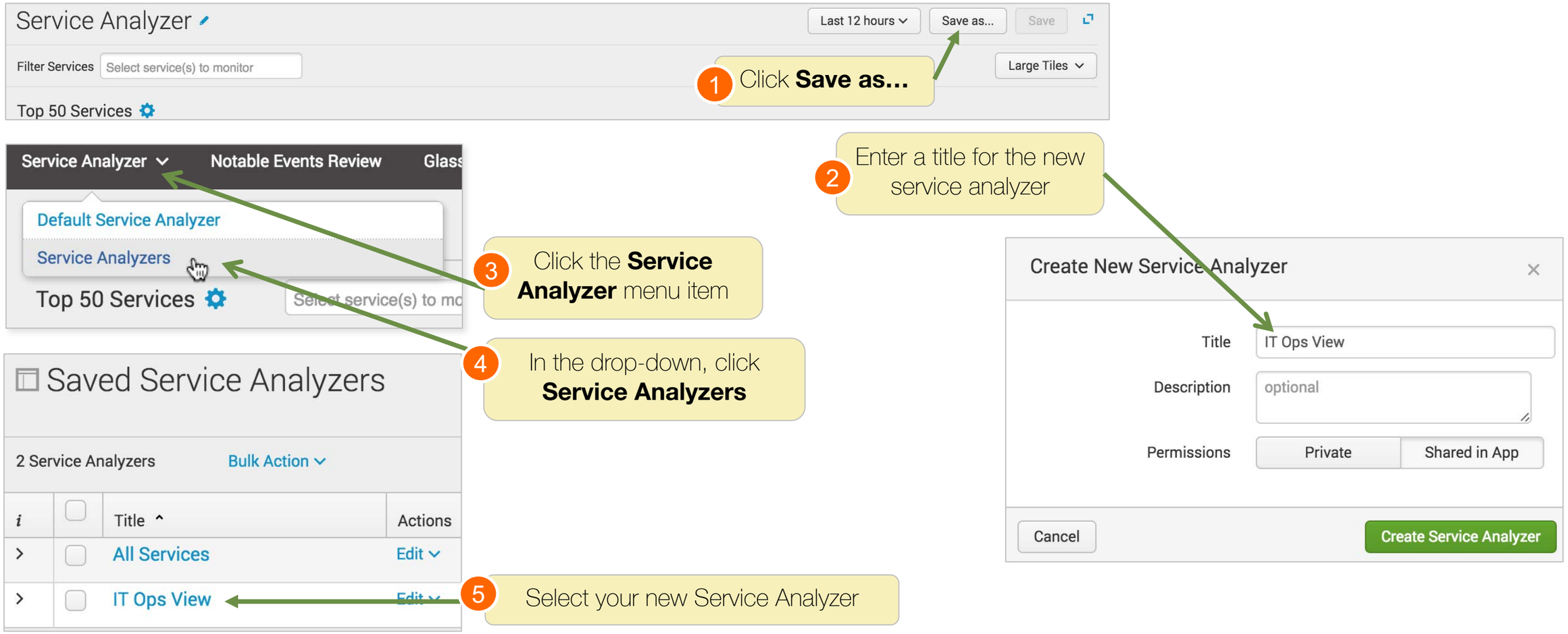


Click a Service Tile to Open Side Panels



Add a Custom Service Analyzer

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



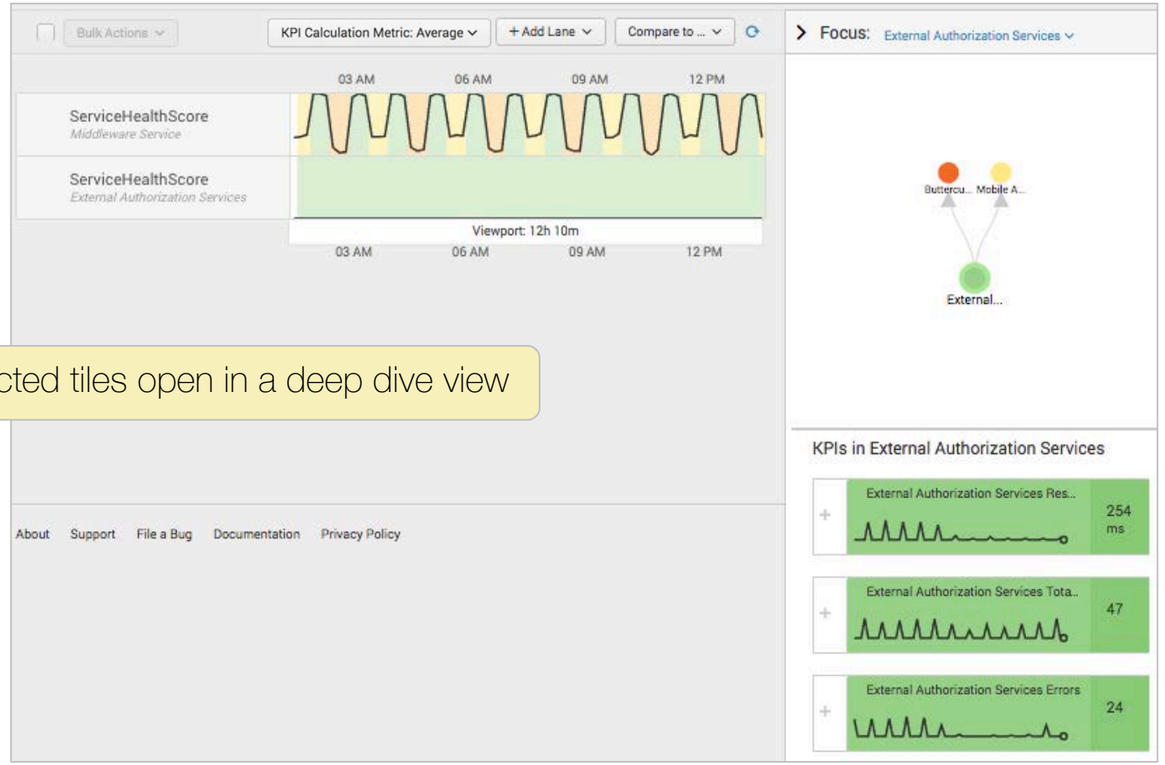
KPI Drilldown to Deep Dive

1. Hover over a tile.
A check mark appears in its upper right corner.

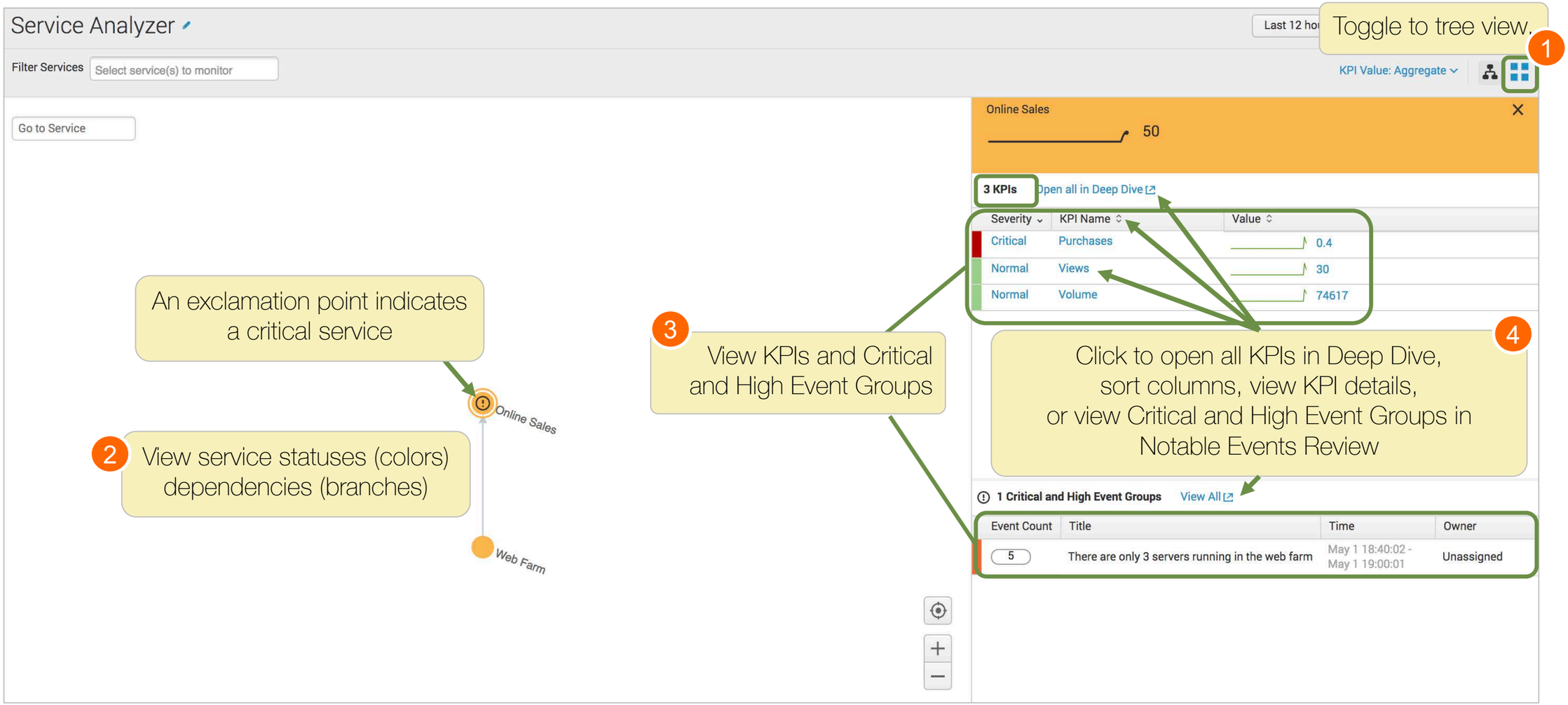
2. Click the check-mark on one or more tiles.

3. Click **Drilldown to Deep Dive**

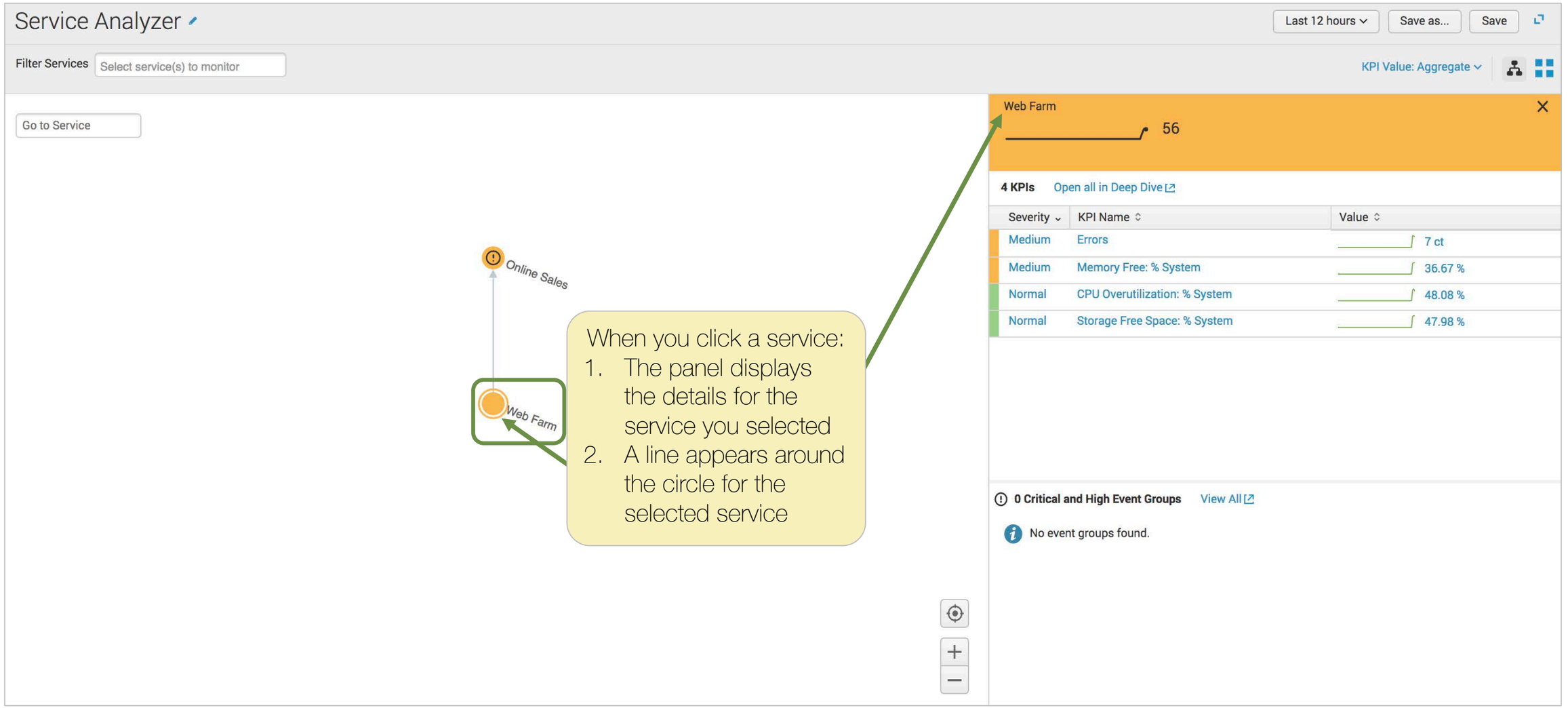
4. Selected tiles open in a deep dive view



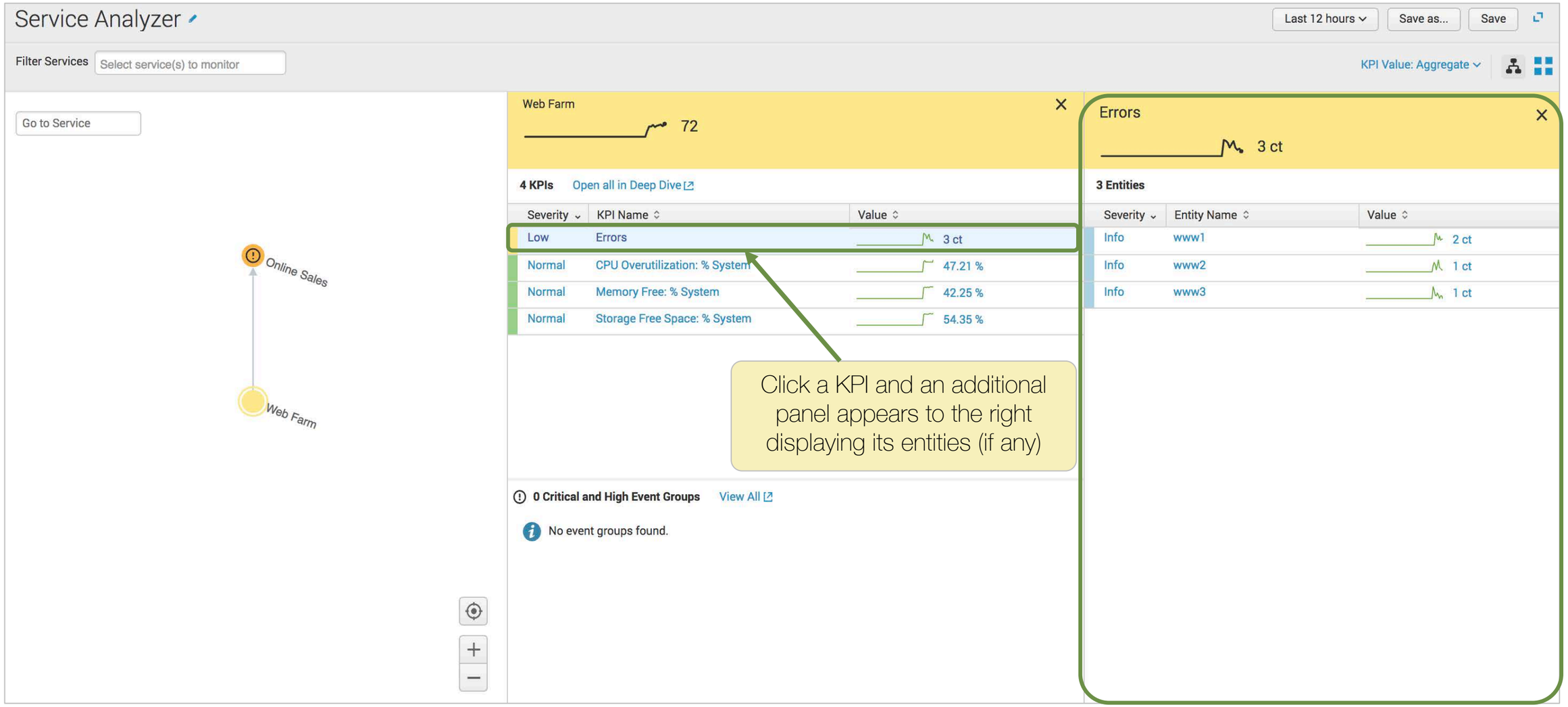
Service Analyzer Tree View



Select a Service to Display in the Panel



Select a KPI to View its Entities



ITSI Analyst Default Permissions

ANALYST PERMISSIONS	Read	Write	Delete	Execute Actions	Change Status
Homeview	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.

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

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

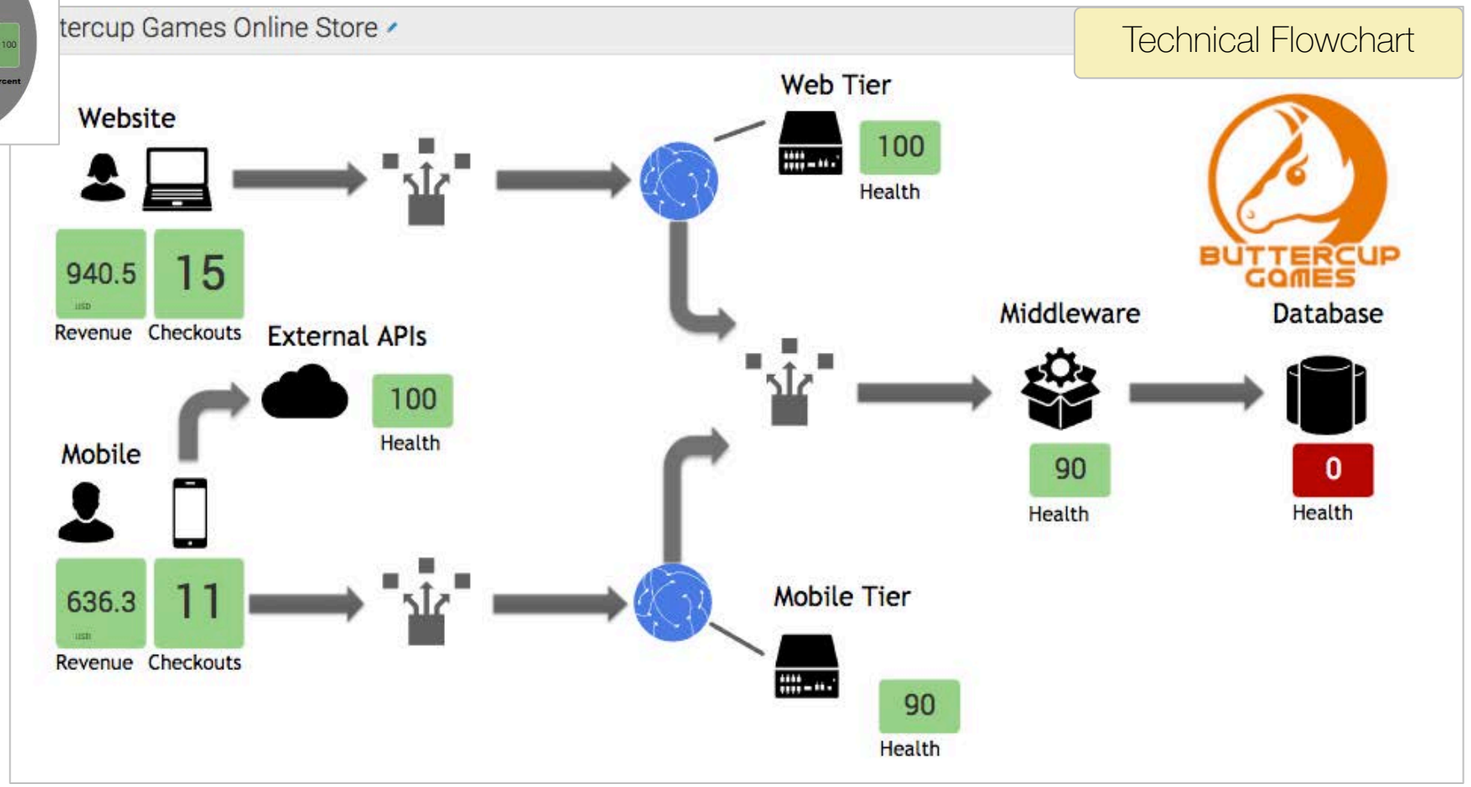
- Glass tables are visualization tools in ITSI that enable users to quickly see the status of their services in real time or at a point in time in the past
- Use the time picker to display KPI and ad-hoc values at a specific time
- Use glass tables to:
  - Create operations center dashboard displays
  - 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



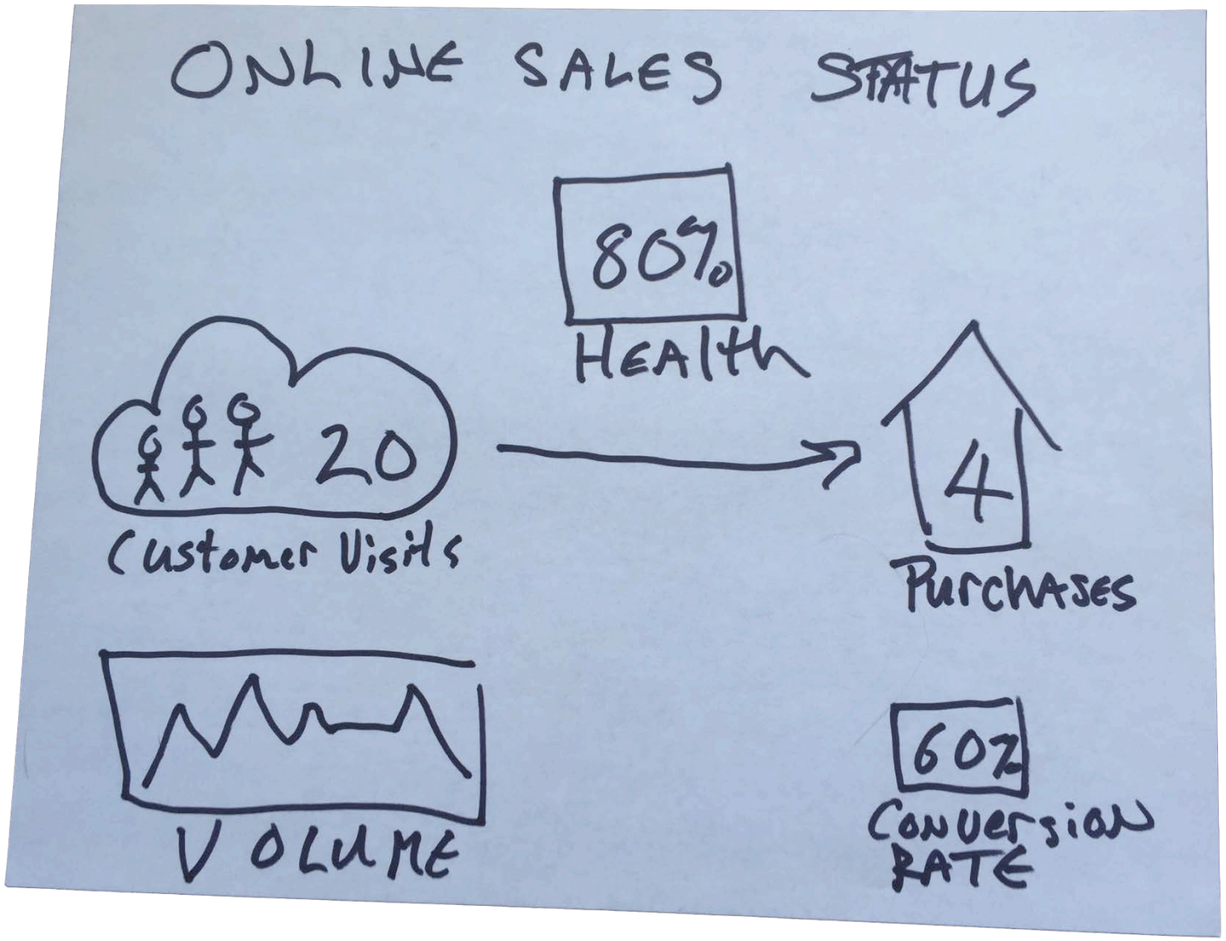
Scenario

- 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)

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."

Whiteboard



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

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."

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

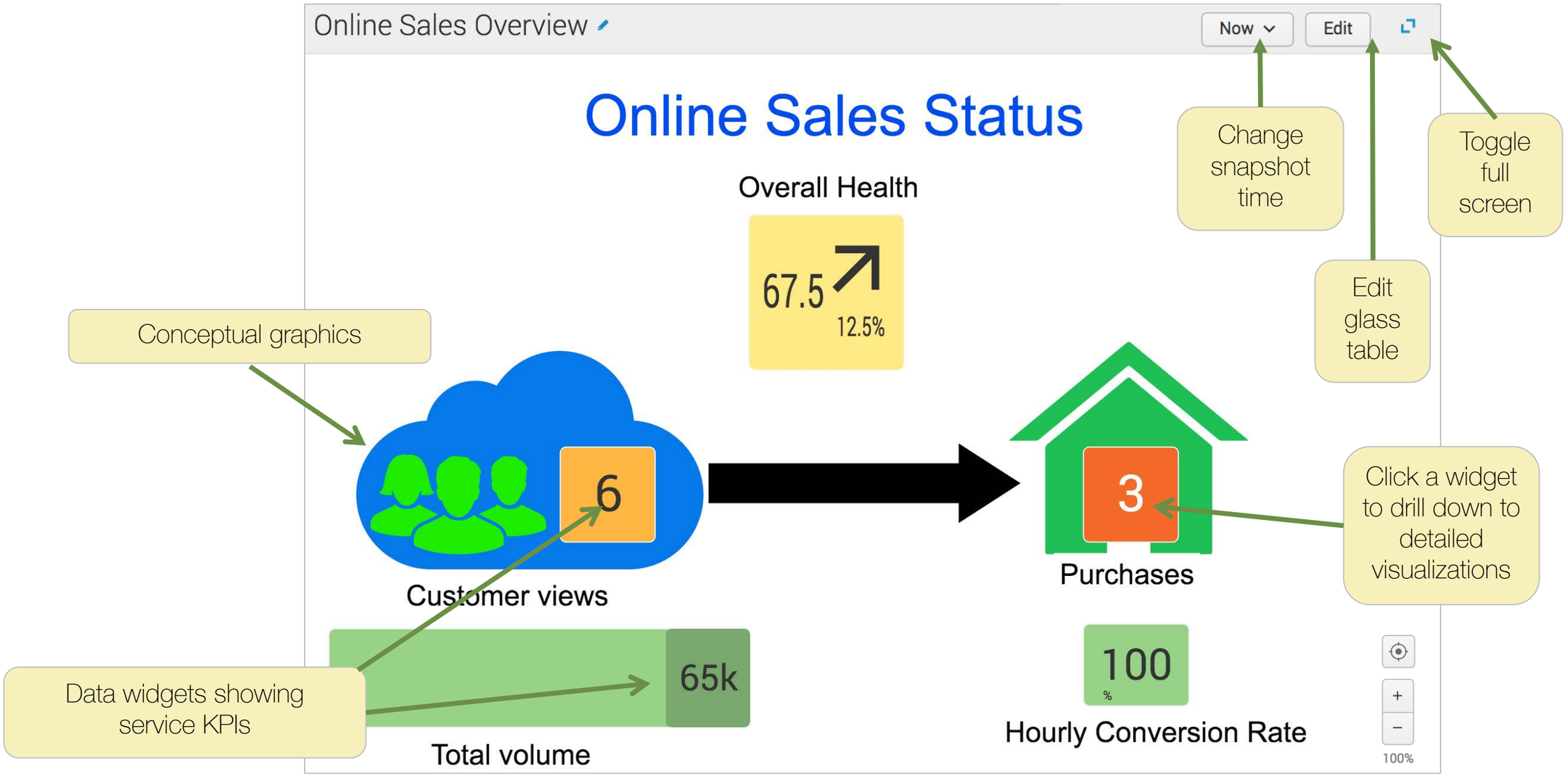
Splunk at Buttercup Games

- 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

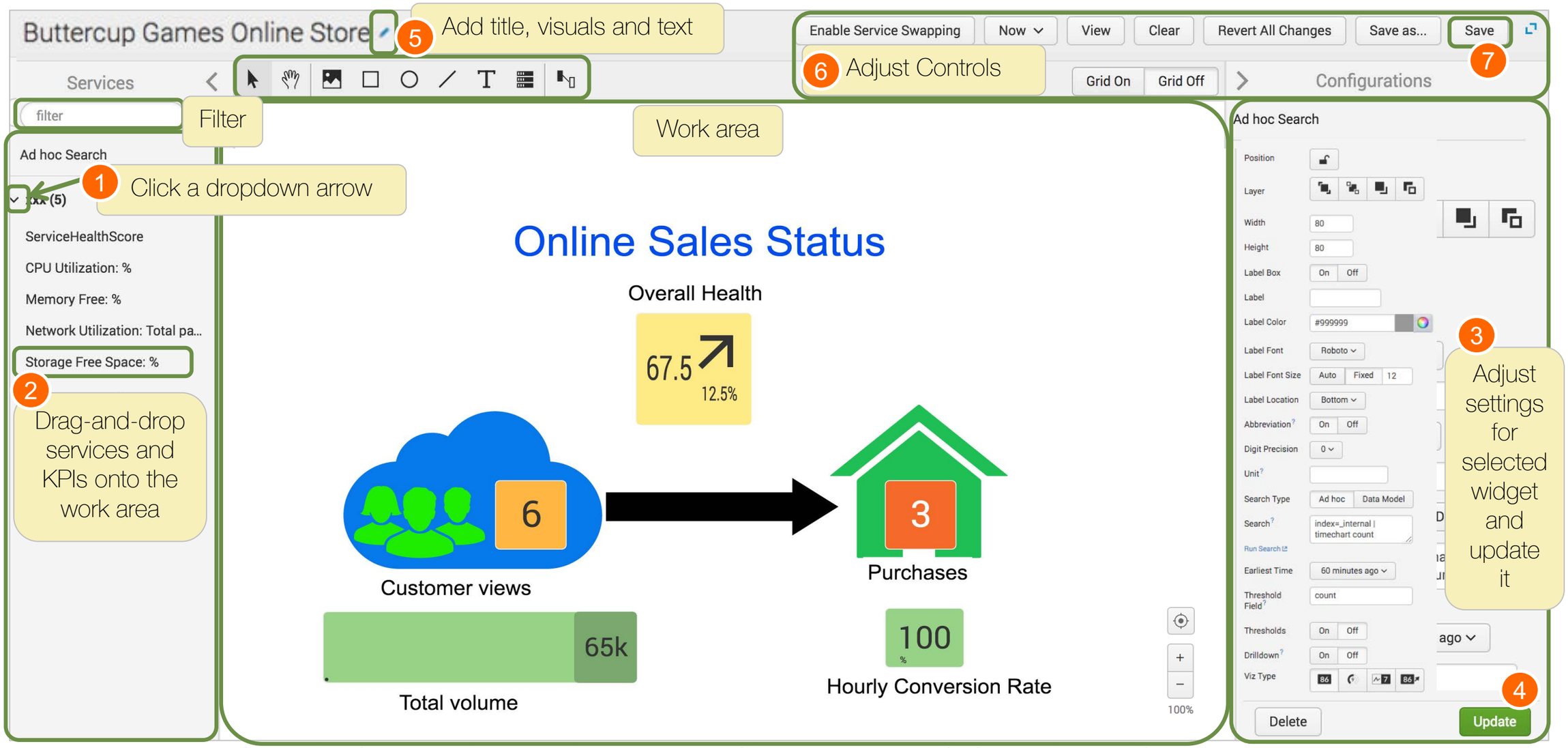
Designing Glass Tables

- 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

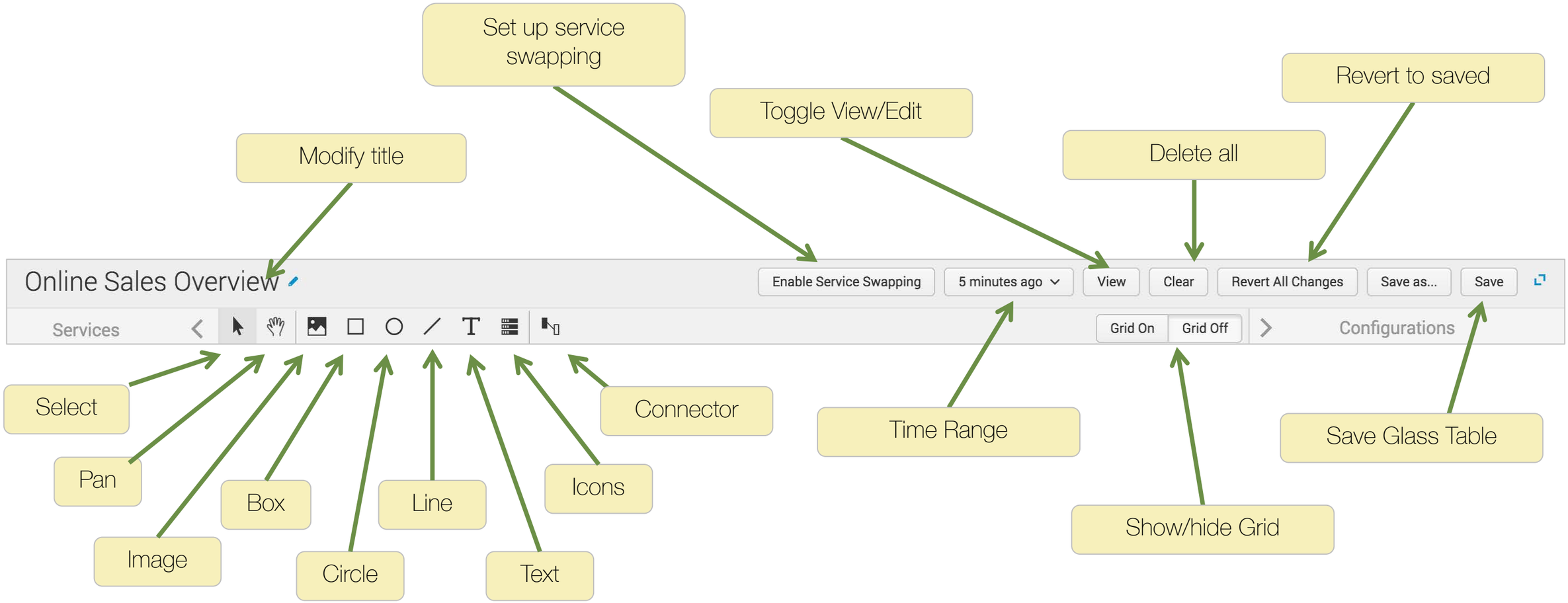
Glass Table: Normal View



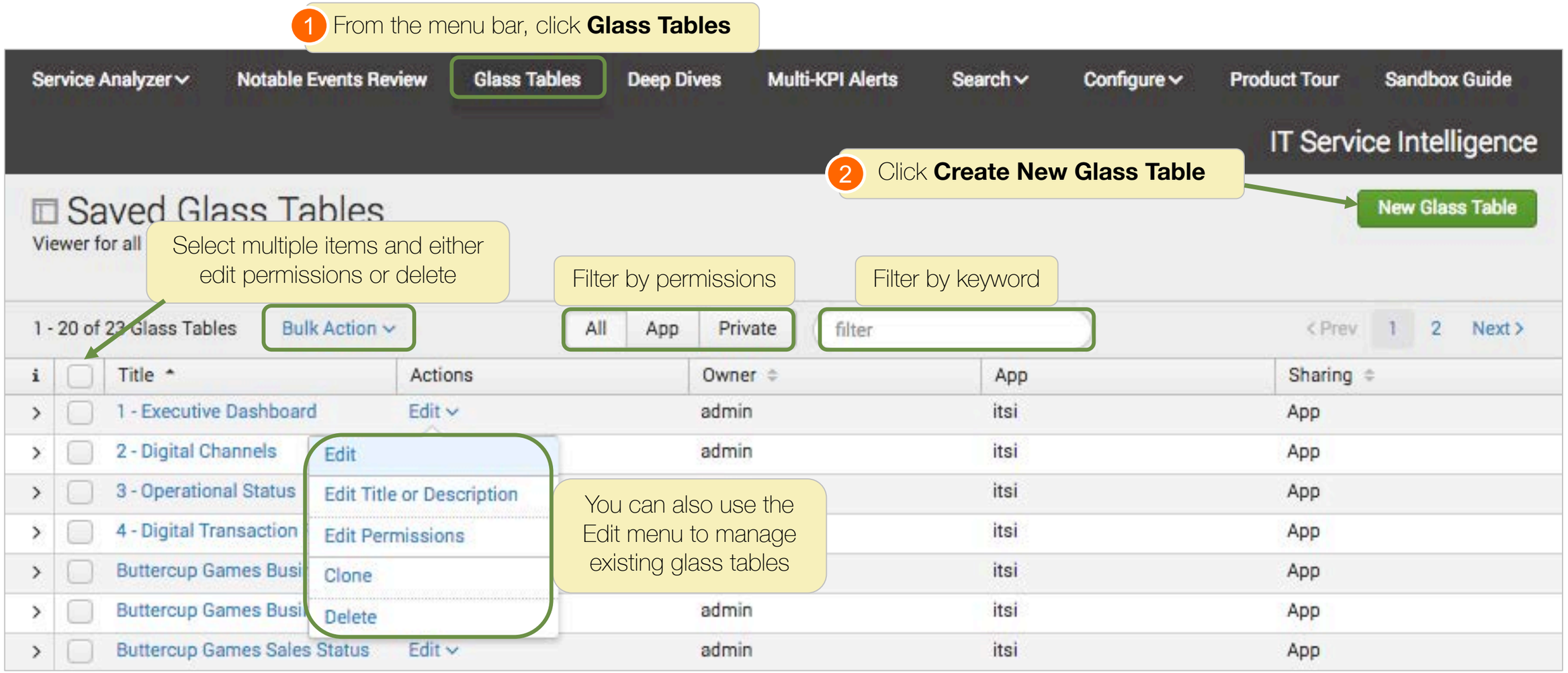
Building the Glass Table



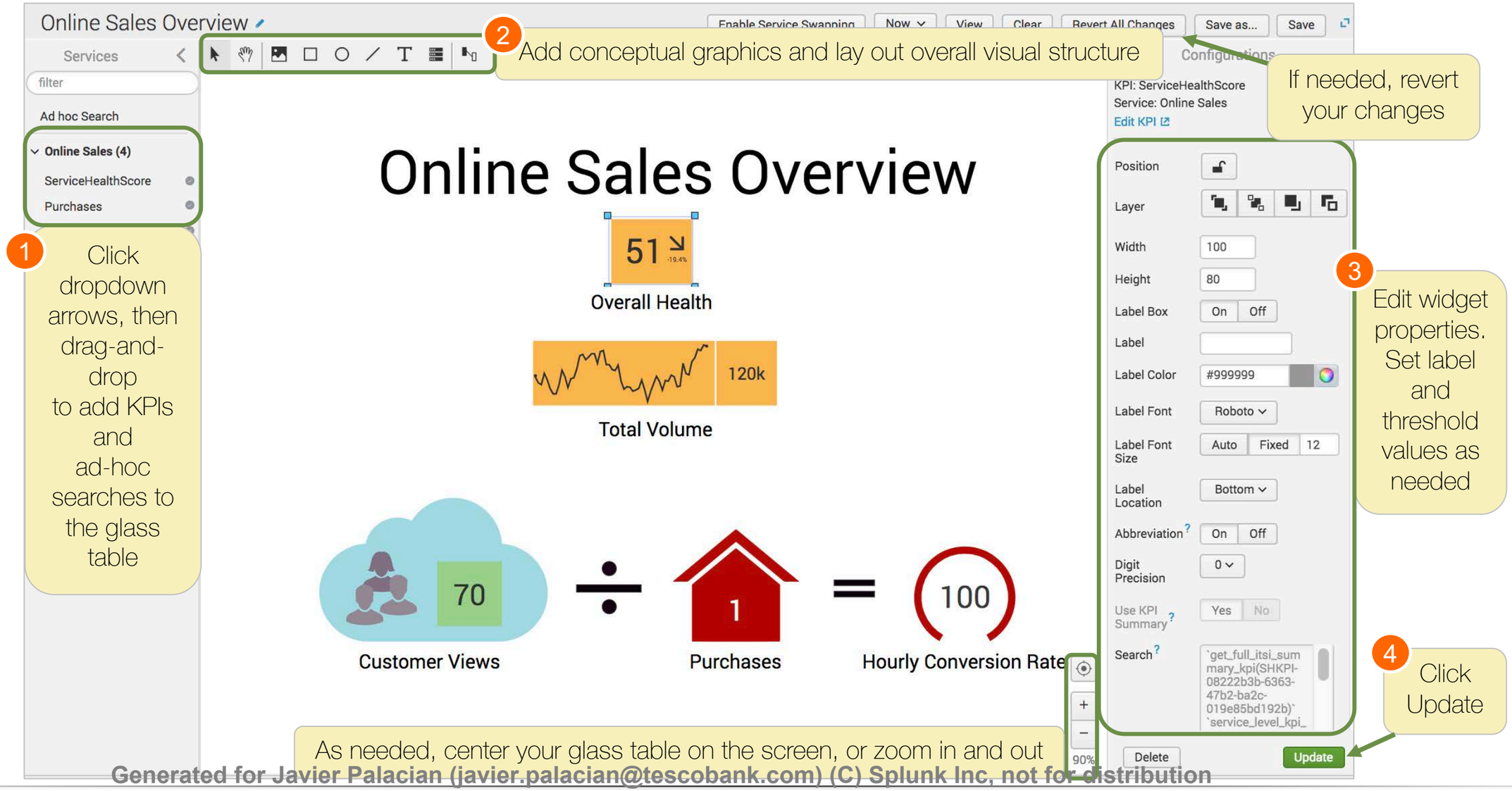
Top Bar Controls



Creating a Glass Table: 1

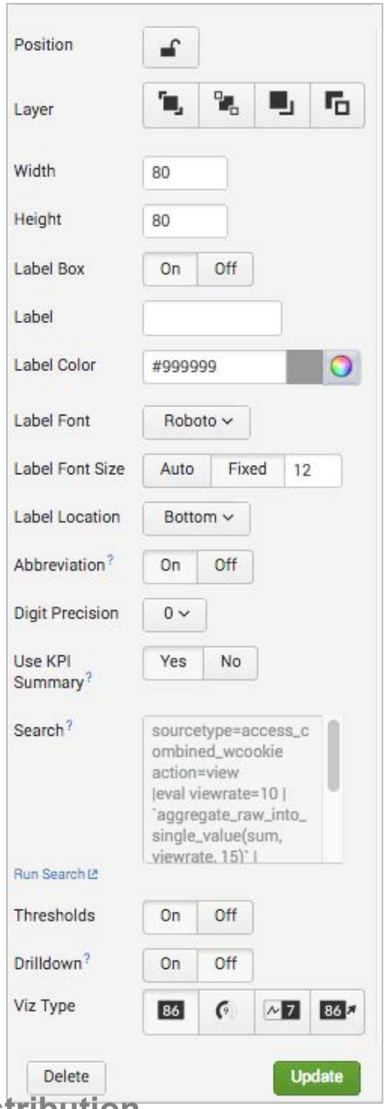


Creating a Glass Table: 2



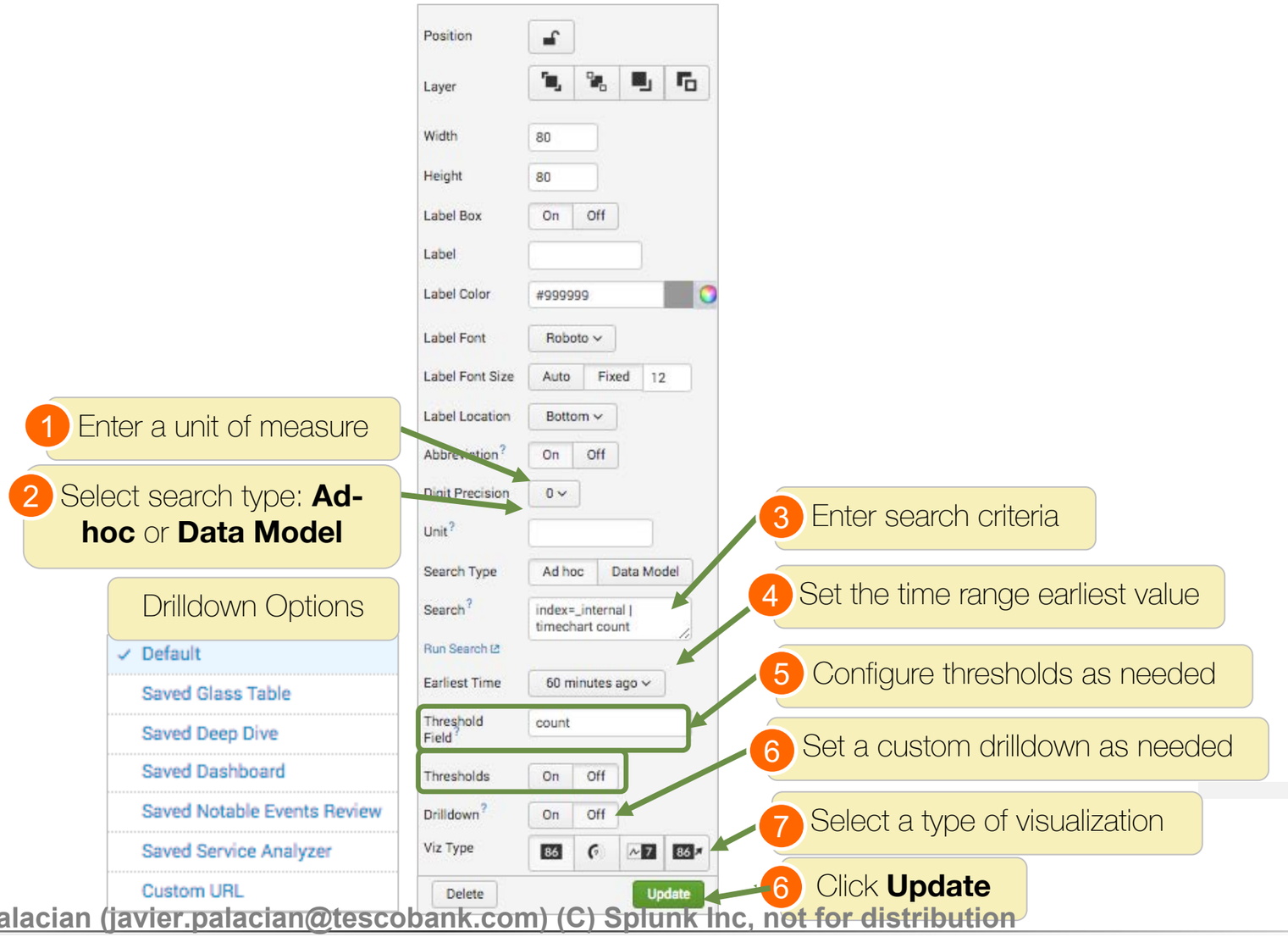
Configuration Bar: KPIs

- 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



Configuration Bar: Ad hoc Search Widget

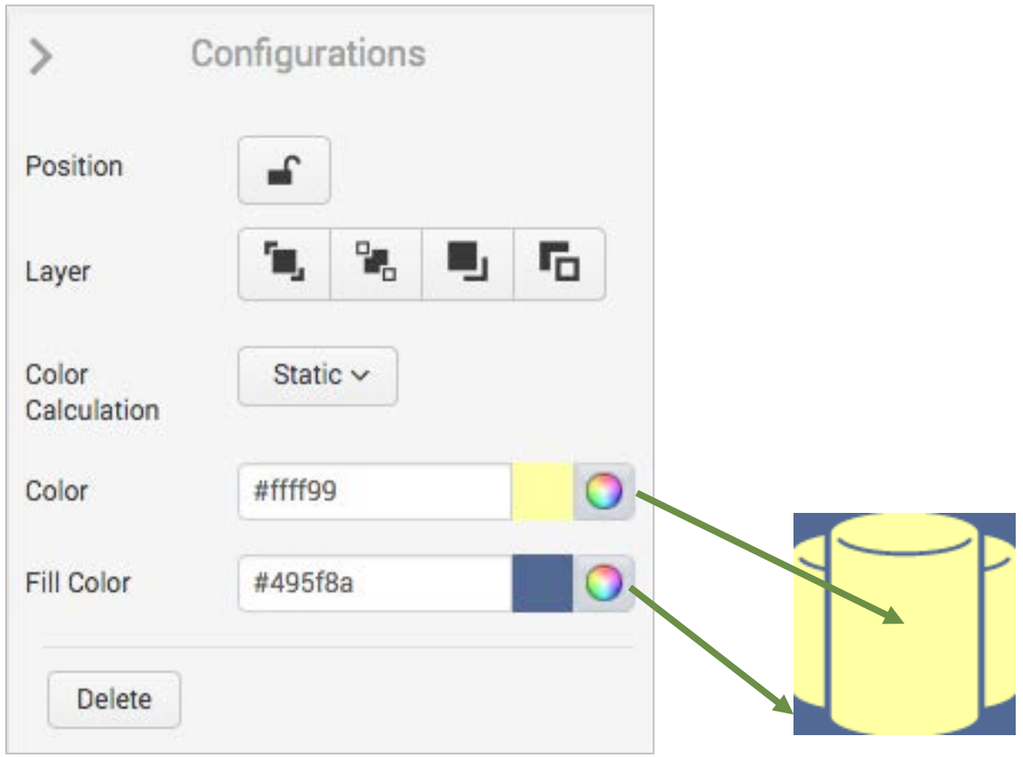
- You can add an ad-hoc search and use a widget to display the result.
- Scroll down under **Configurations** to specify the settings shown here.



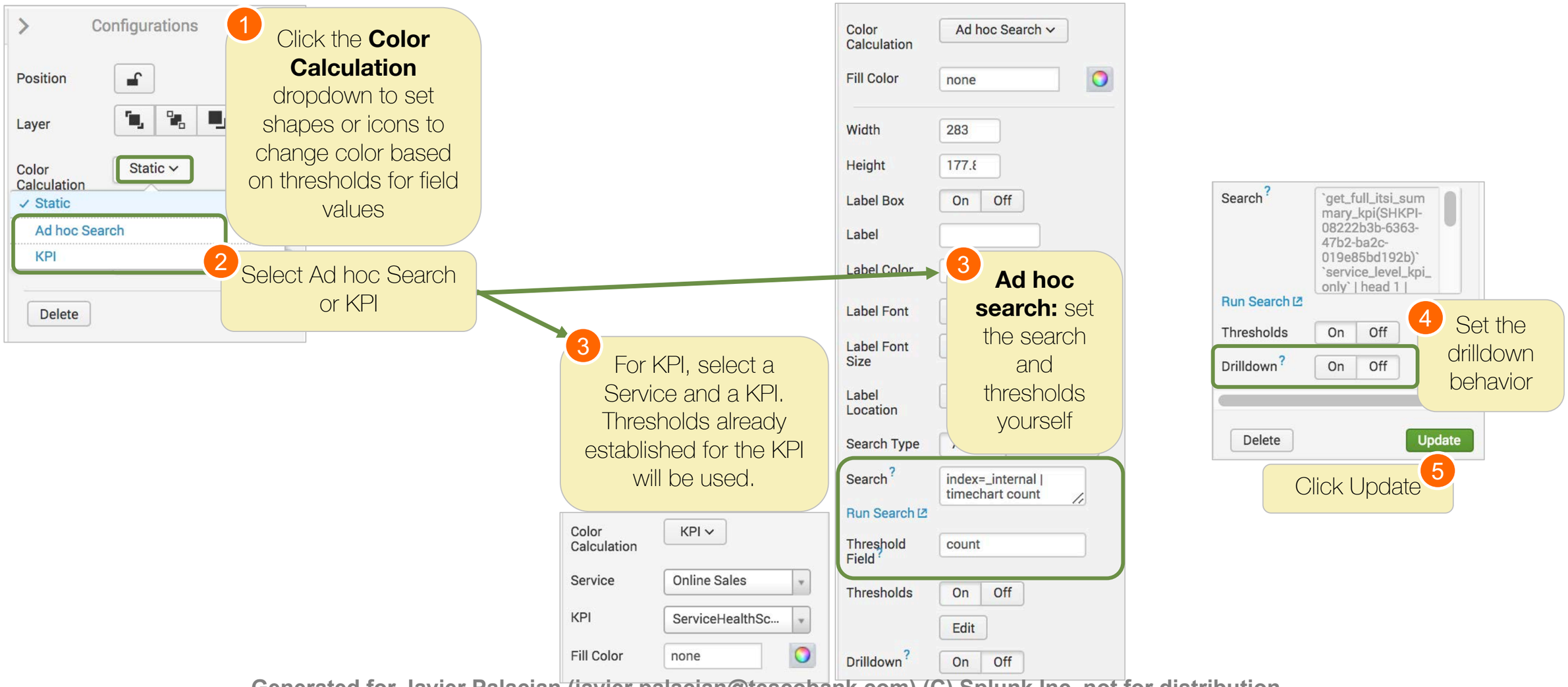
Configuration Bar: General

Most widgets have controls for:

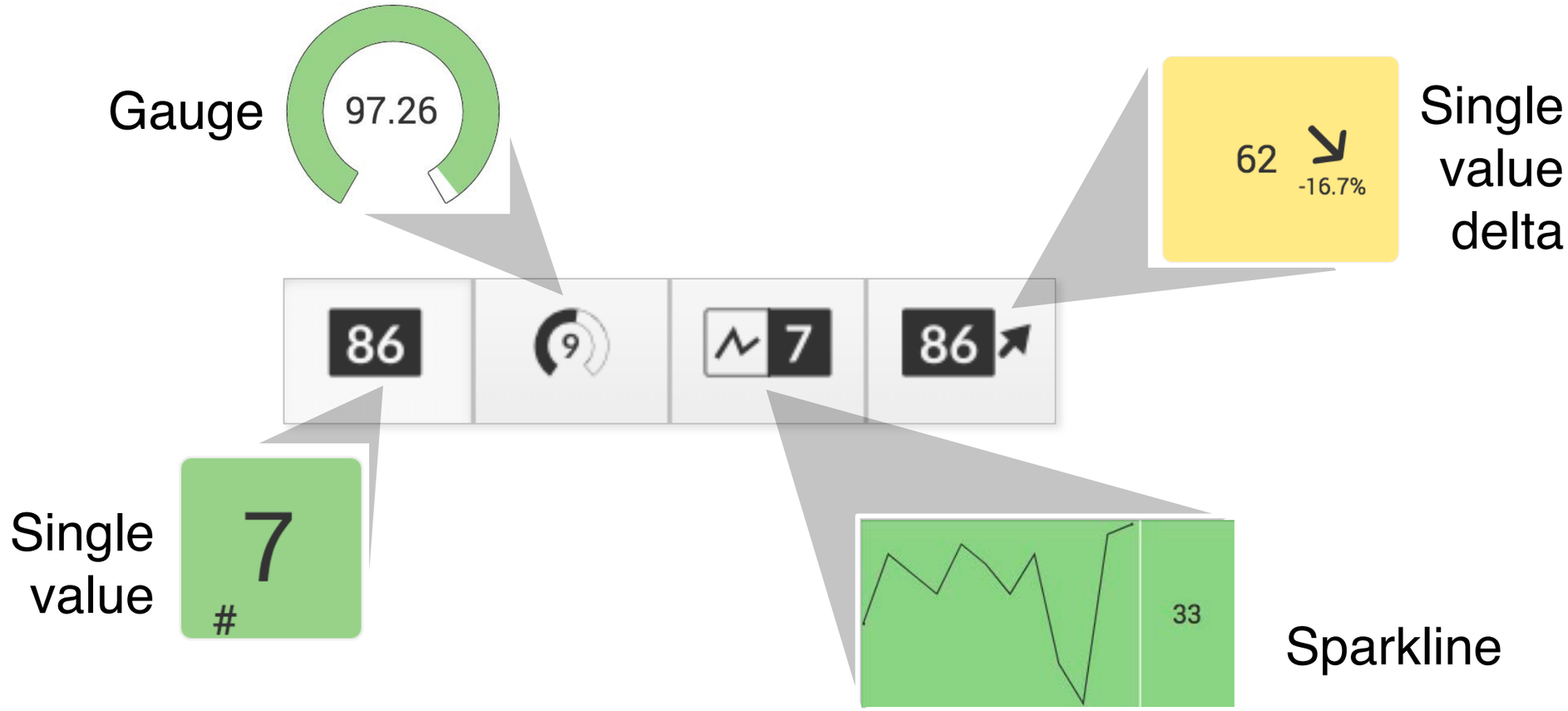
- Position locking
- Layer control (bring forward/back)
- Color Calculation (set the color to change when data crosses preset or custom thresholds)
- Color (object or fore color)
- Fill color (background color and object outline)
- Deletion (or, use the <delete> key)



Use Shapes or Icons as Widgets

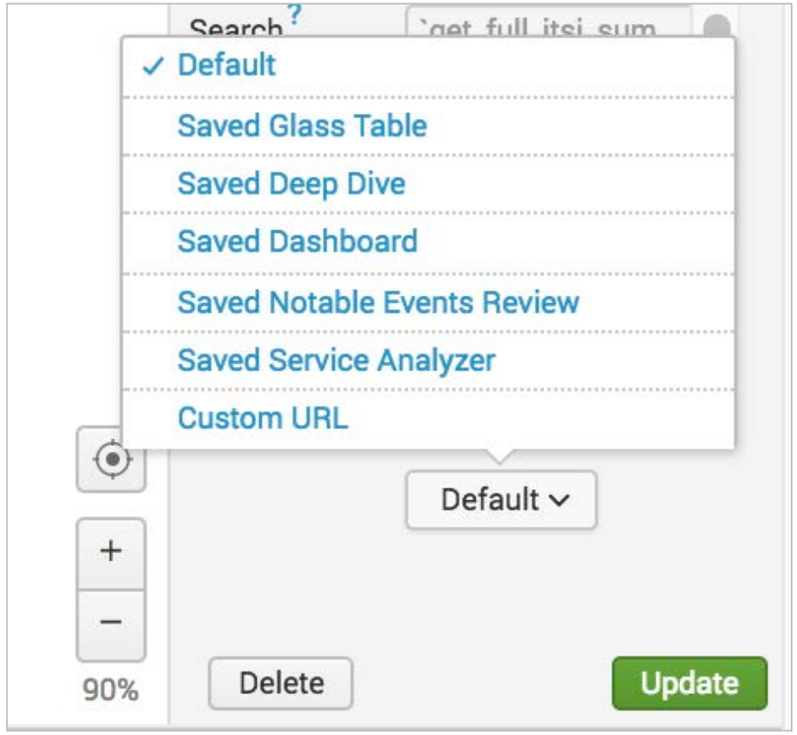


Widget Visualization Types



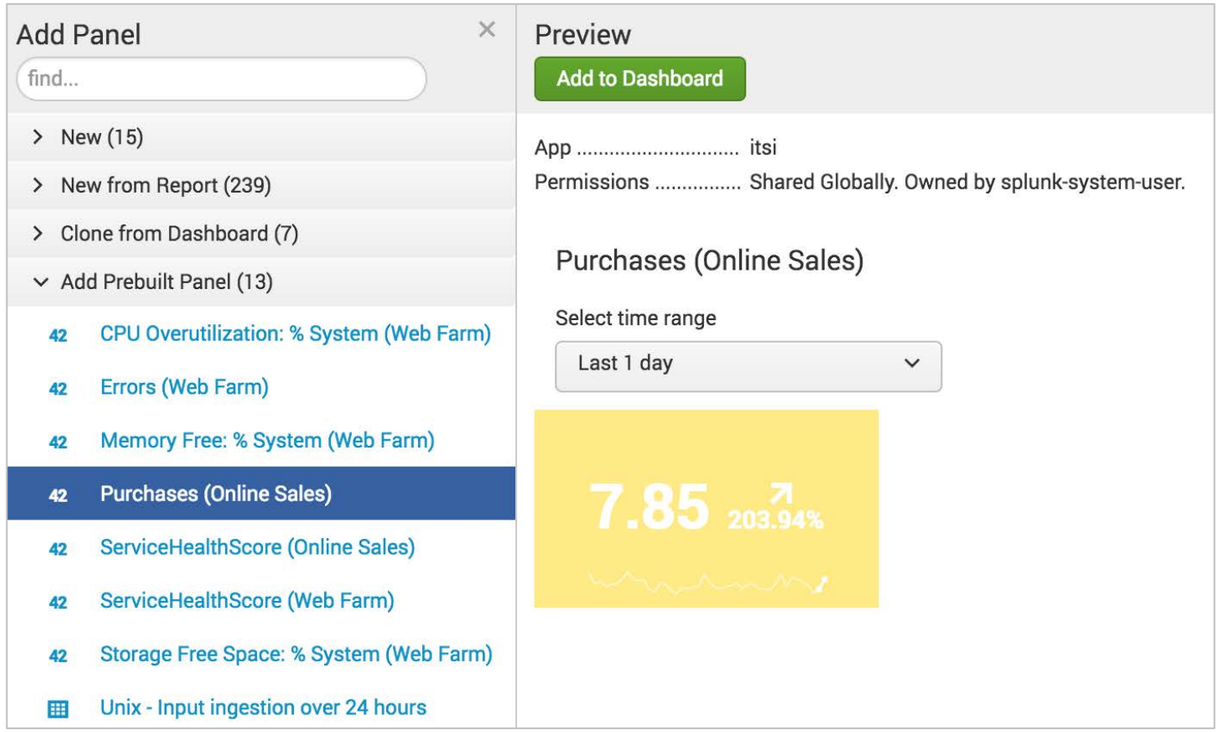
Glass Table Drilldown

- 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



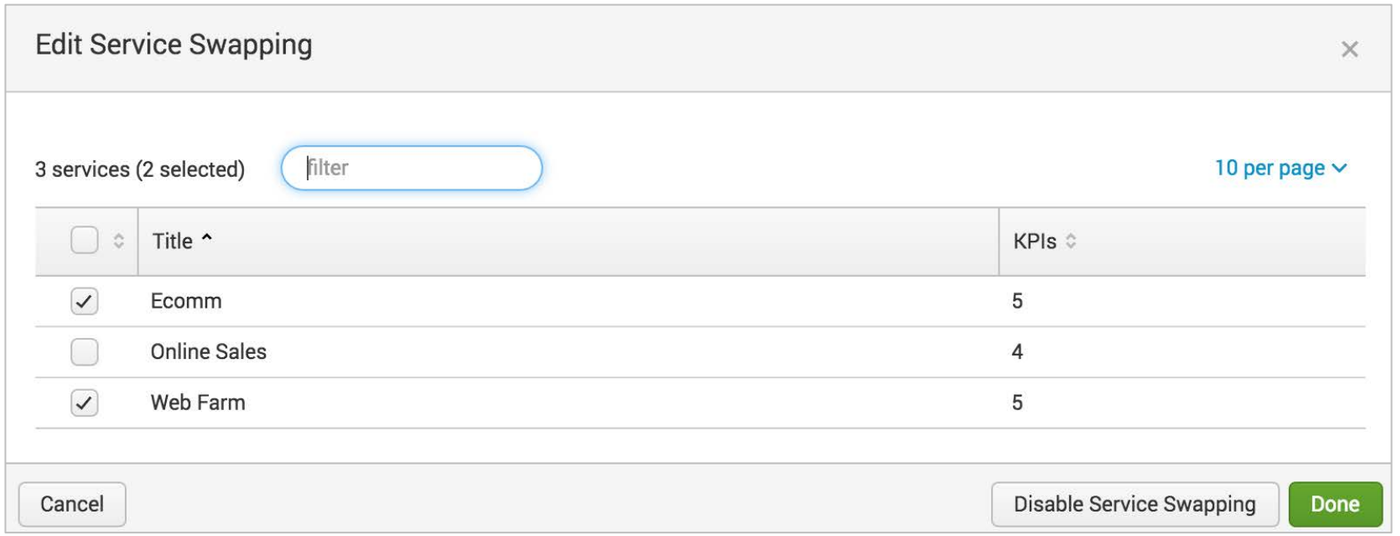
KPIs on Custom Dashboards

- 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**



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

Module 2 Lab Exercise

Time: 30 minutes

Task:

Create a new glass table to monitor Online Sales

Module 3:
Managing Notable Events

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

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

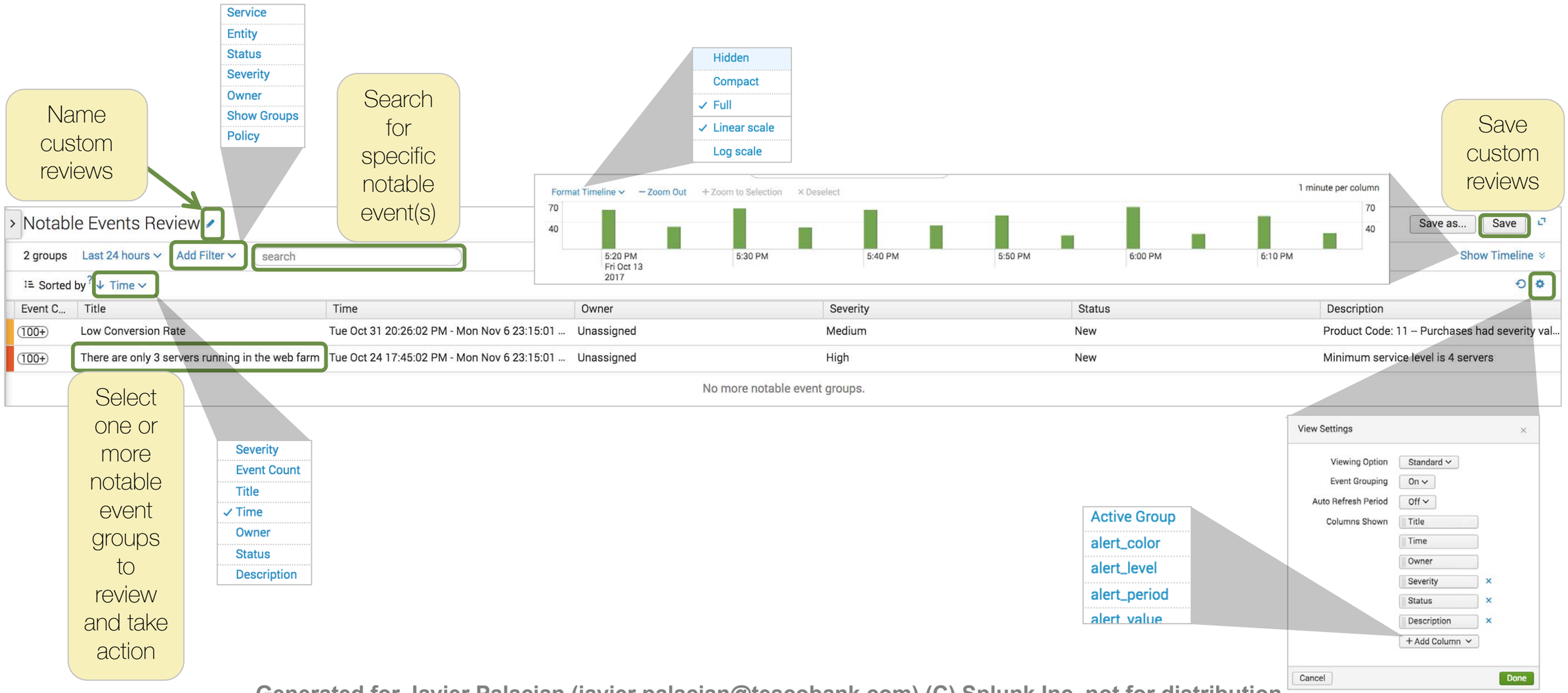
Notable Event Management Concepts

- 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

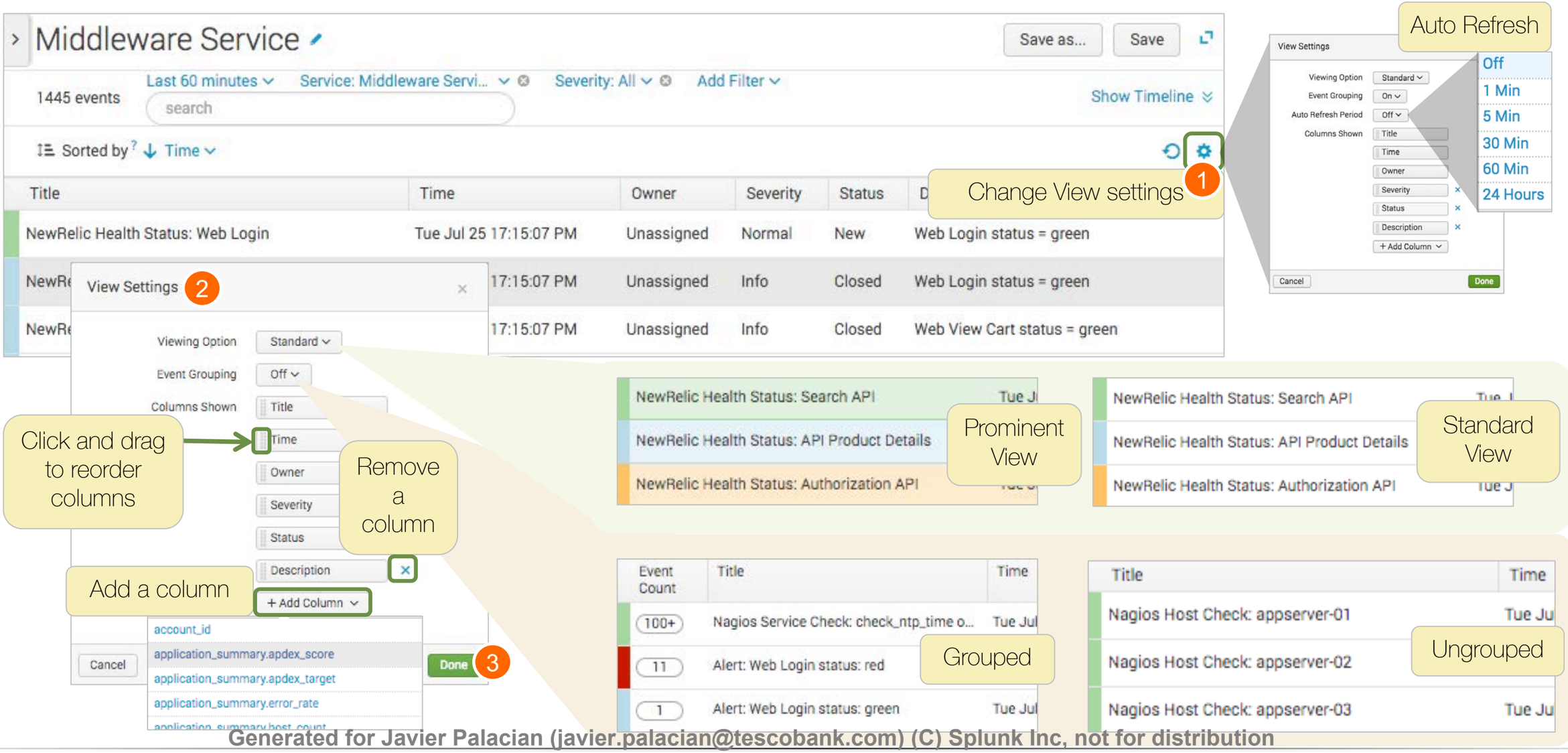
Notable Event Analyst Workflow

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

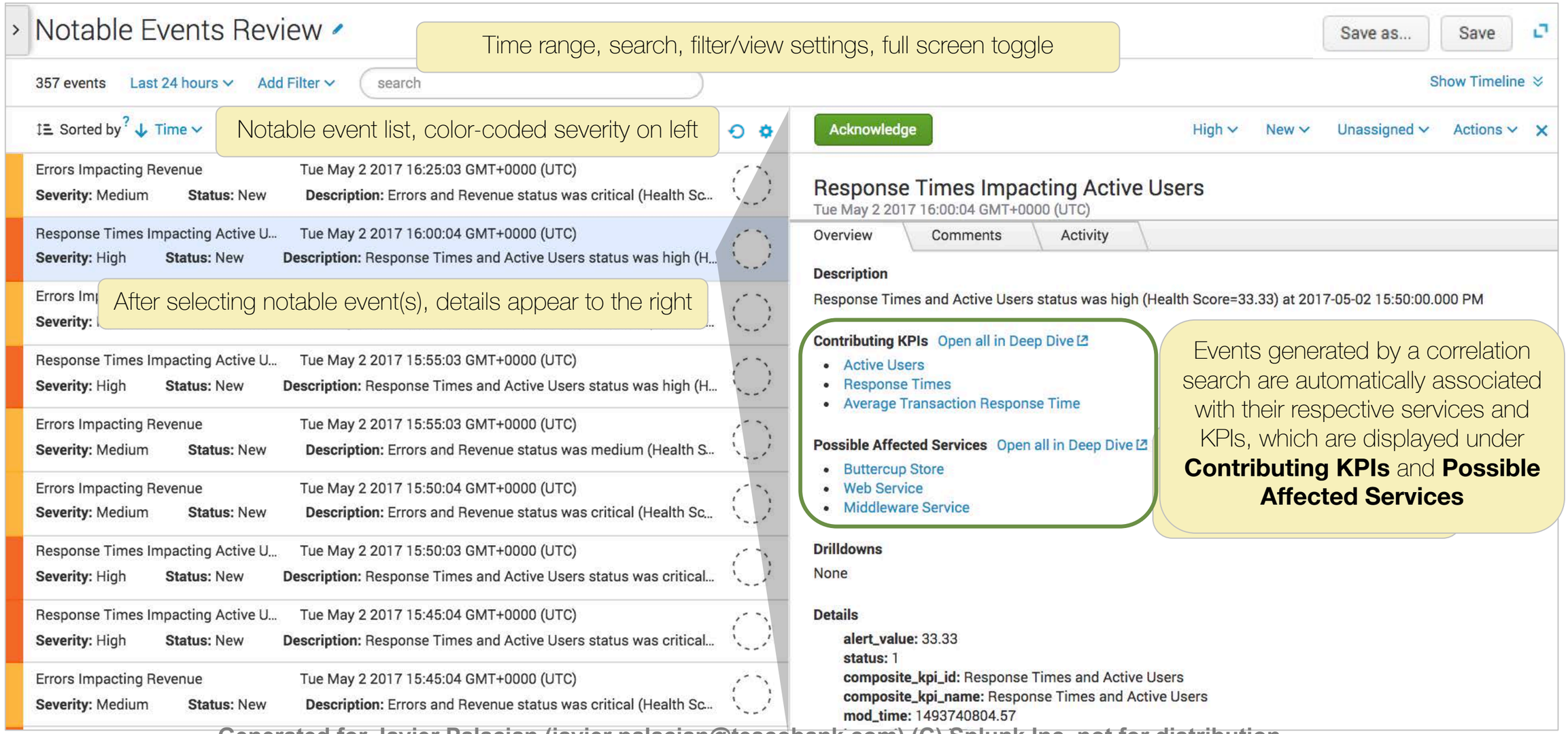
Notable Events Review: Default View



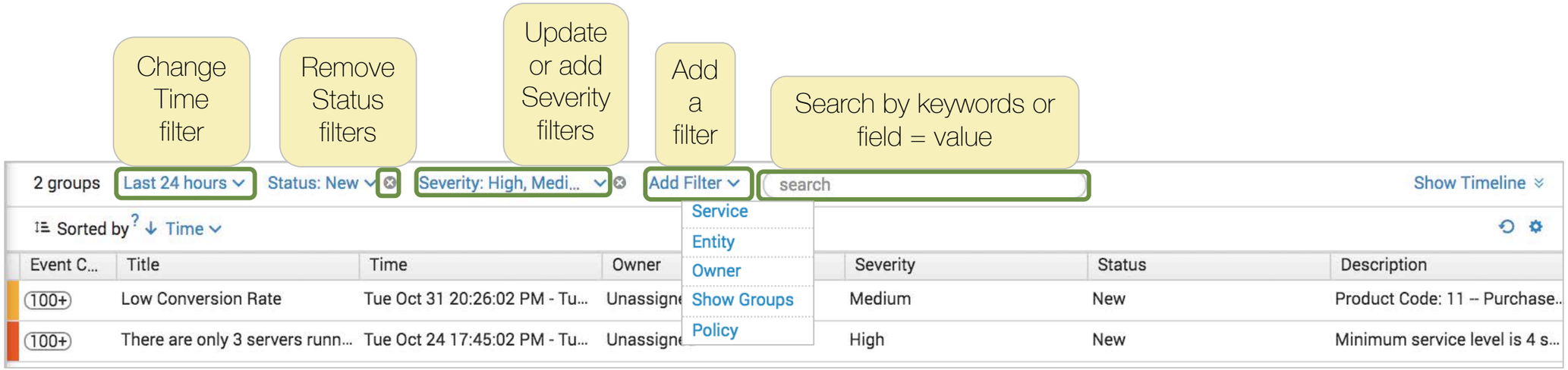
Notable Events View Settings



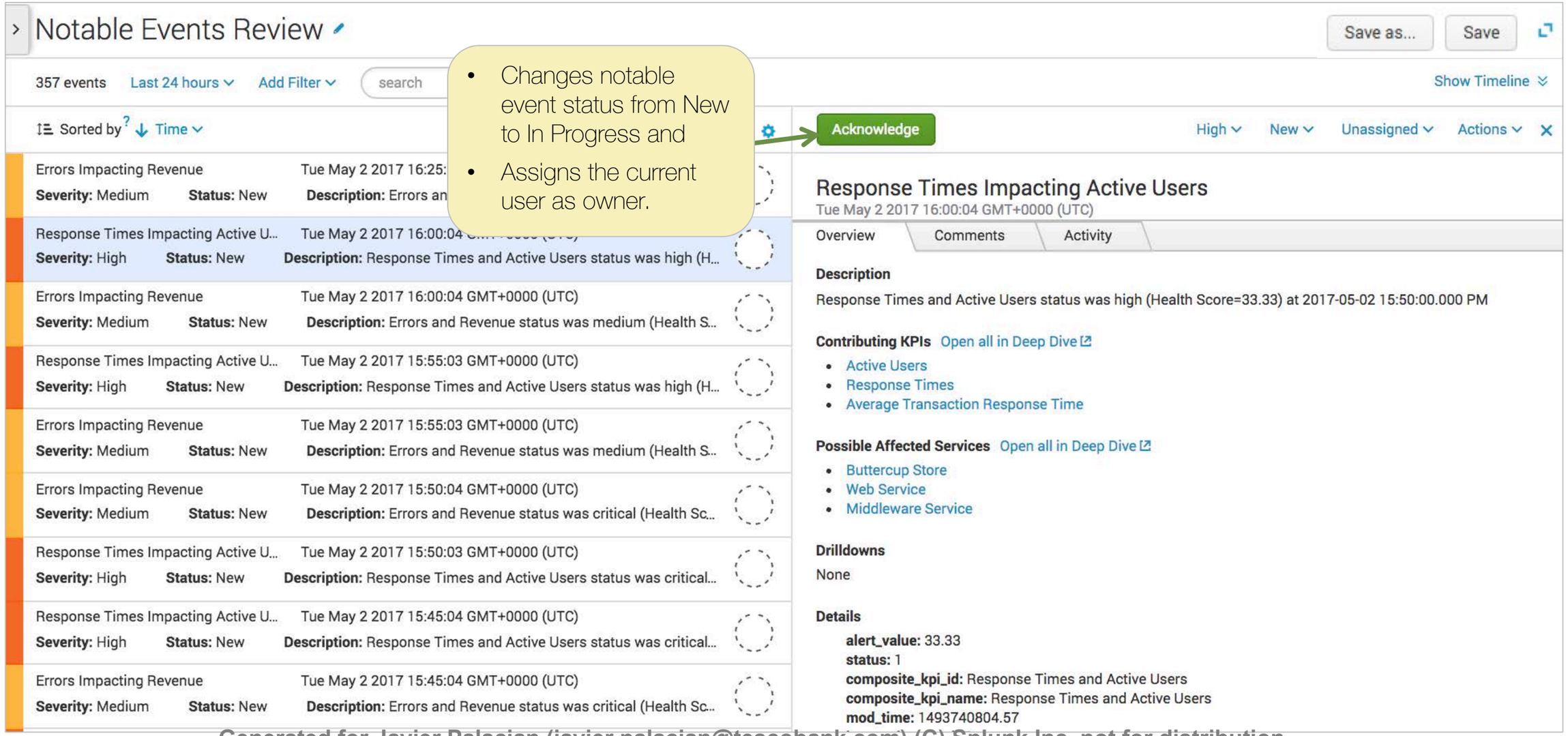
Selecting Notable Event(s)



Notable Events Filter Settings



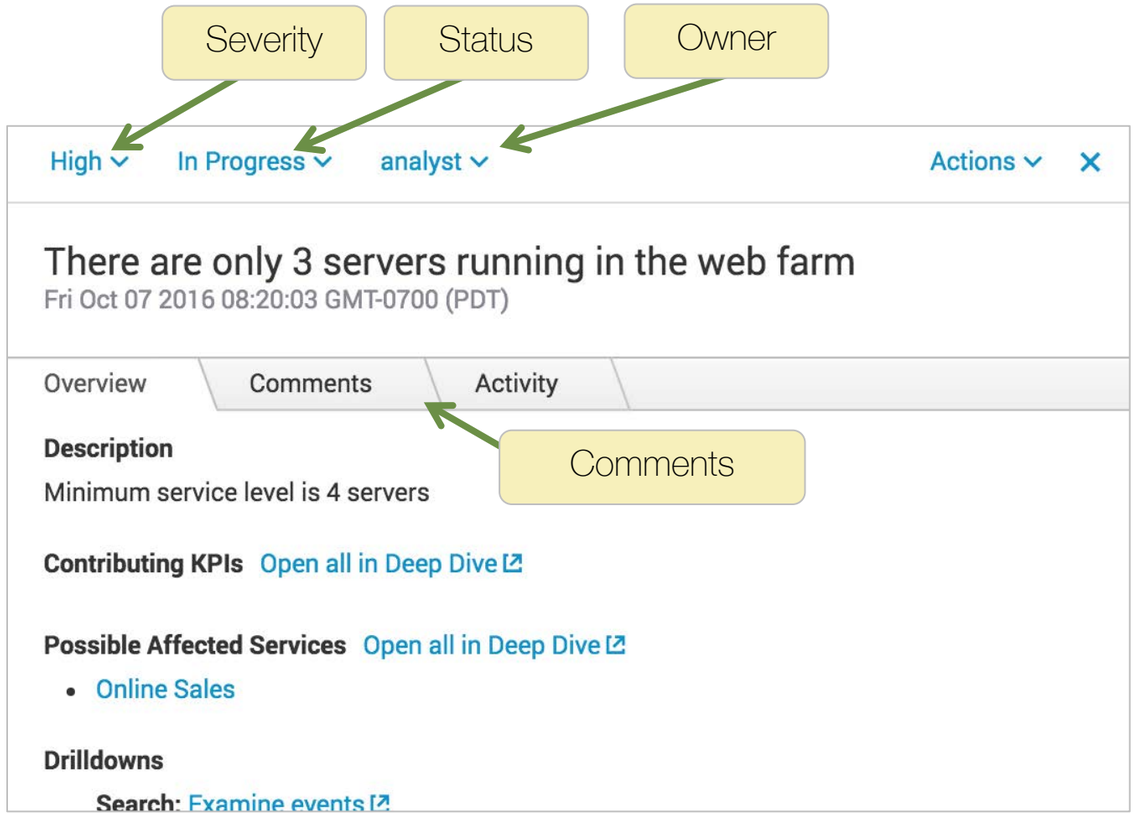
Acknowledging a Notable Event



- Changes notable event status from New to In Progress and
- Assigns the current user as owner.

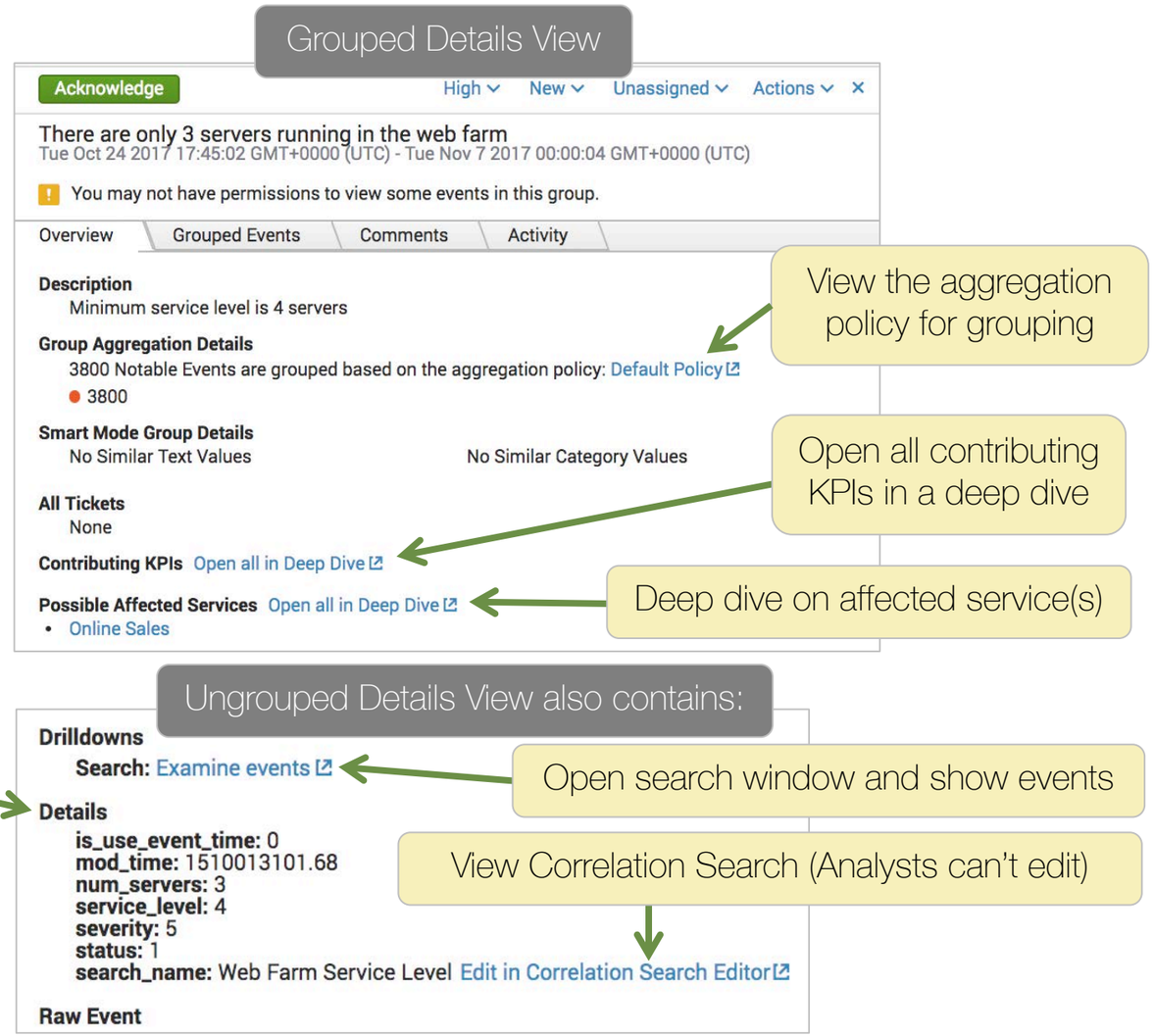
Updating a Notable Event

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

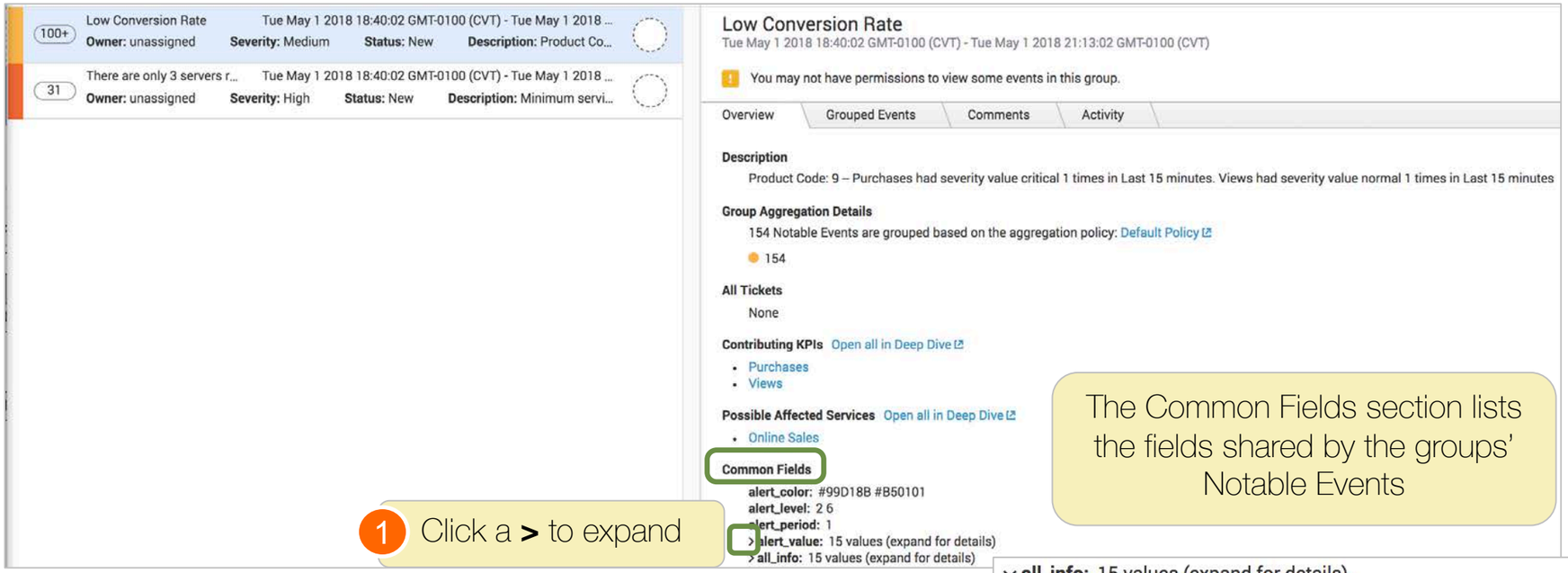


Notable Event Details

- 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.



Notable Event Groups: Common Fields



1 Click a **>** to expand

The Common Fields section lists the fields shared by the groups' Notable Events

all_info: 15 values (expand for details)

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

Show all

2 Examine the individual field values and their frequencies

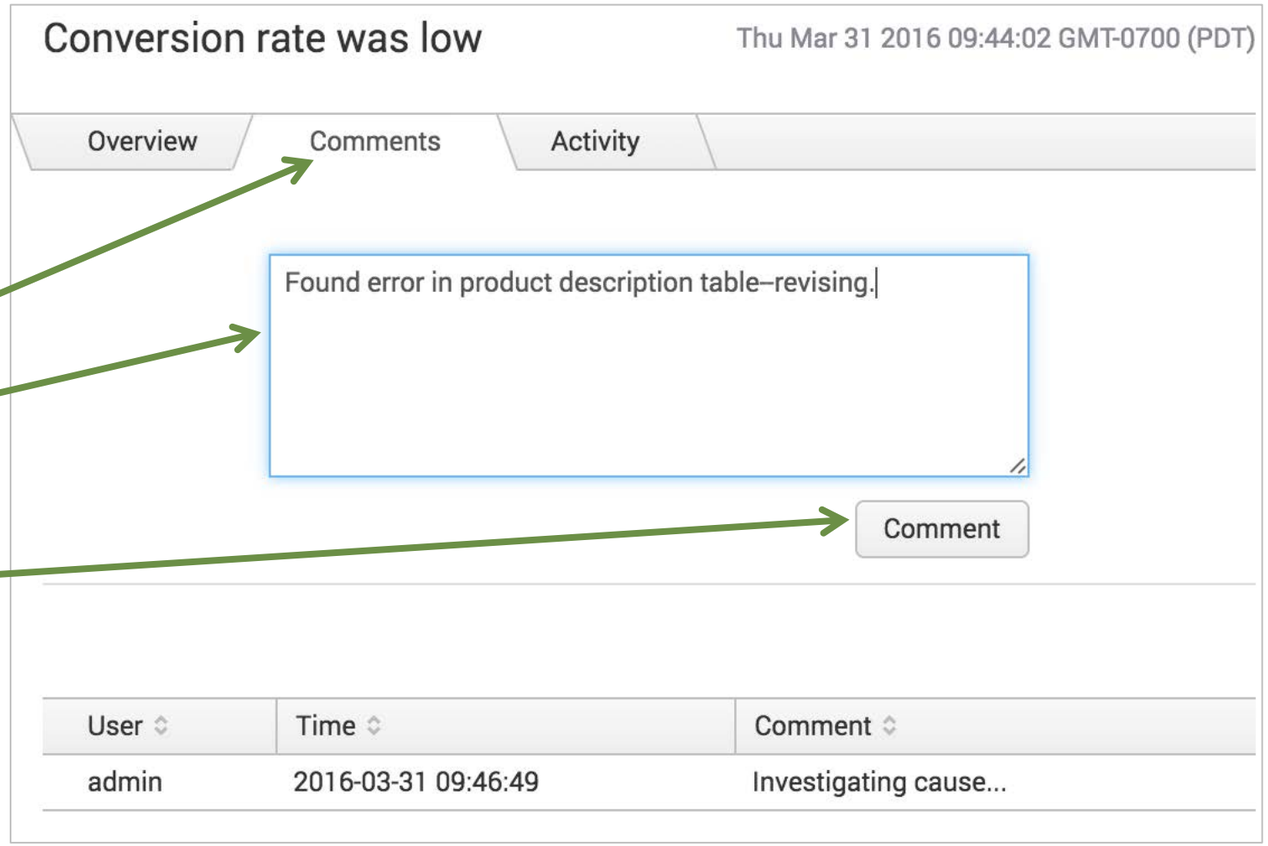
3 (Optional) Click **Show All** to view remaining fields and values

Adding a Comment

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

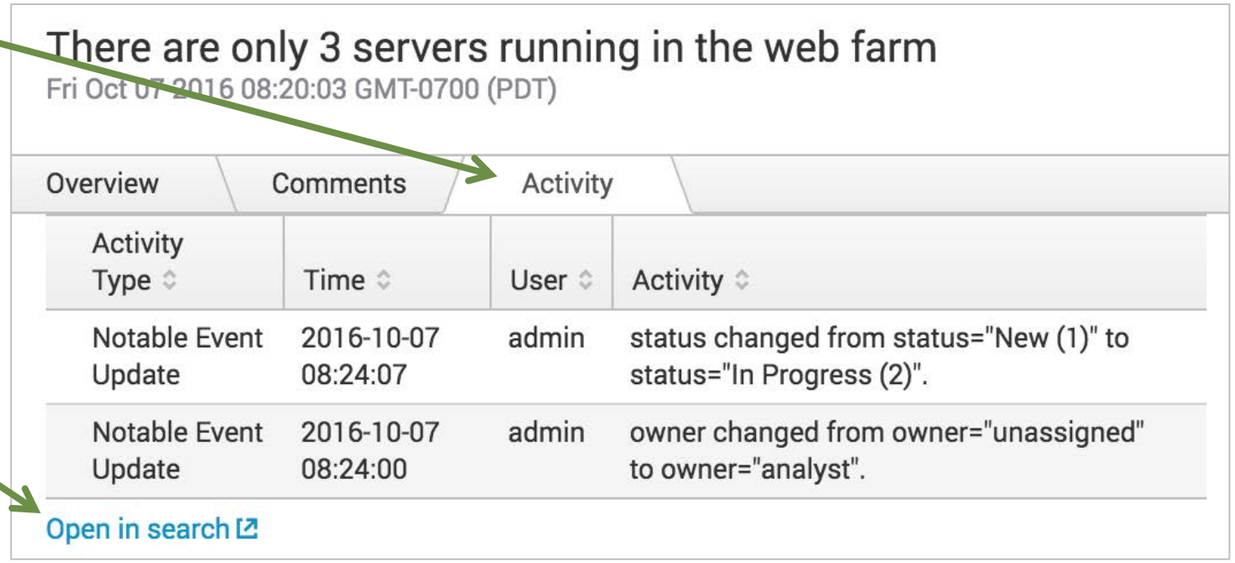
1. Click the **Comments** tab
2. Enter a comment
3. Click **Comment**

All comments are displayed in the table below



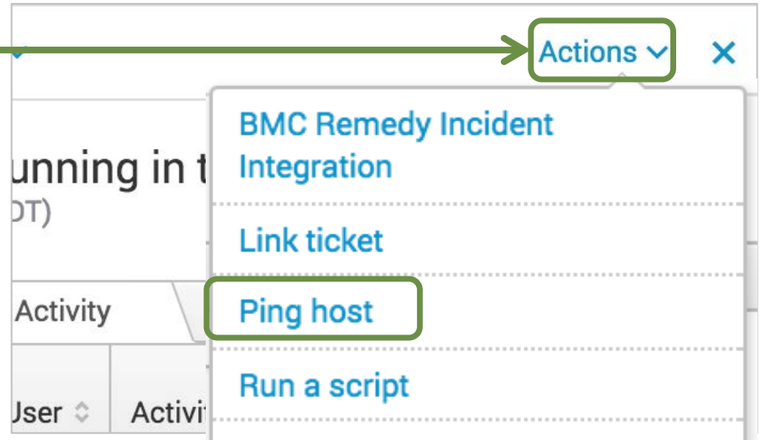
Viewing and Searching Activity

- 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.

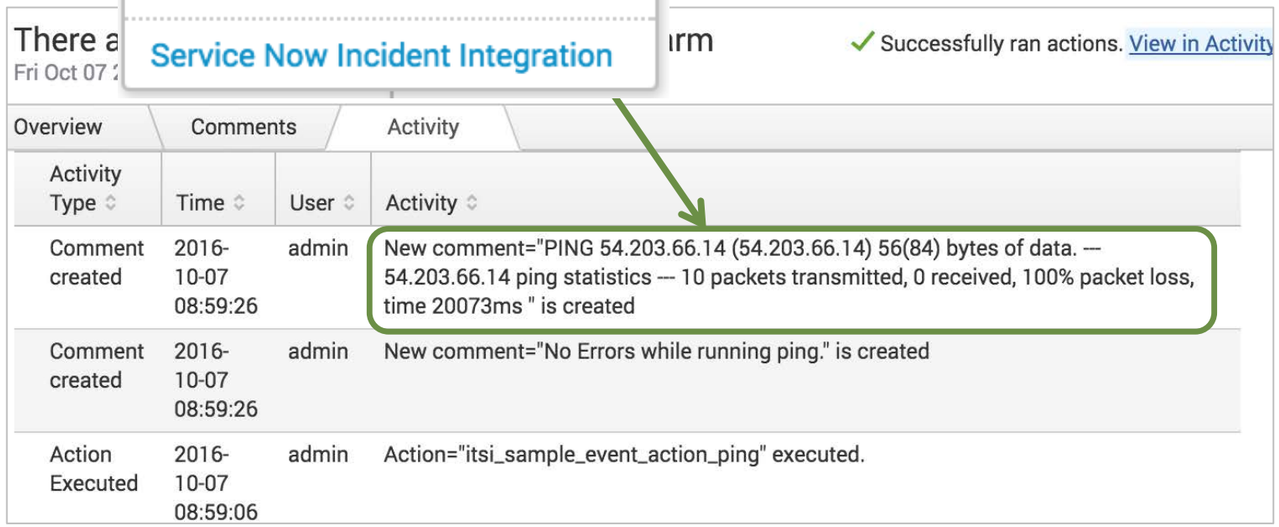


Notable Event Actions

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

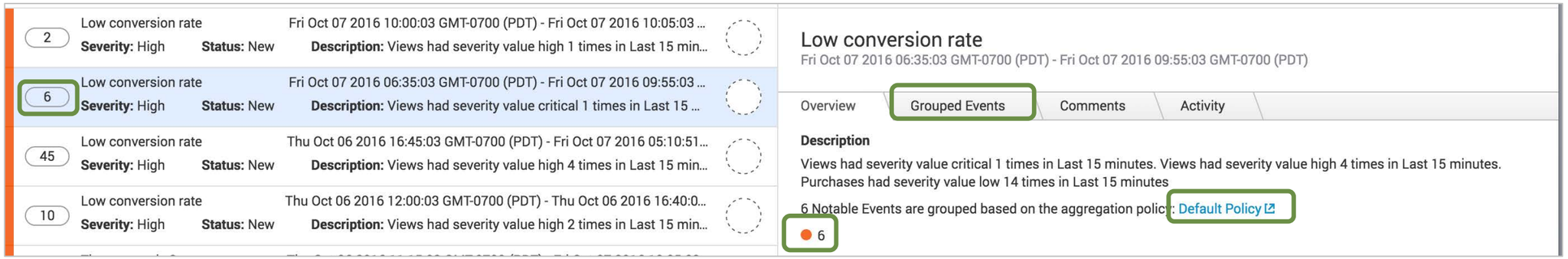


- Actions list can contain custom actions added by your admins
- Integrates with other ticketing systems, such as BMC Remedy or ServiceNow



Notable Event Grouping

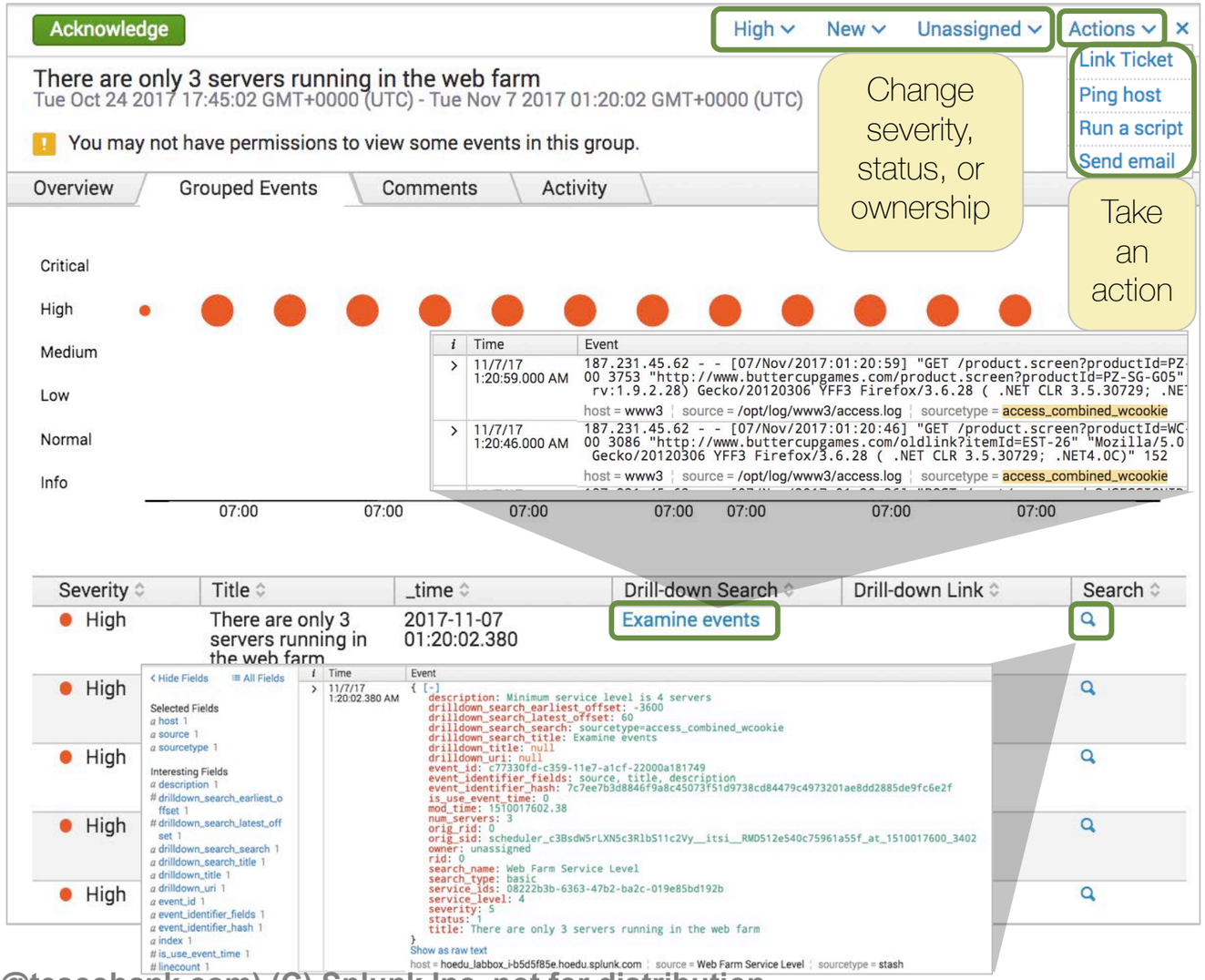
- De-clutters the view, changes all grouped events at once
  - Default: notables are grouped by source (the correlation search that created them) until no new event from that source occurs for 2 hours
  - Admins can manually control grouping with agg. Policies



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

Grouped Events Tab and Actions

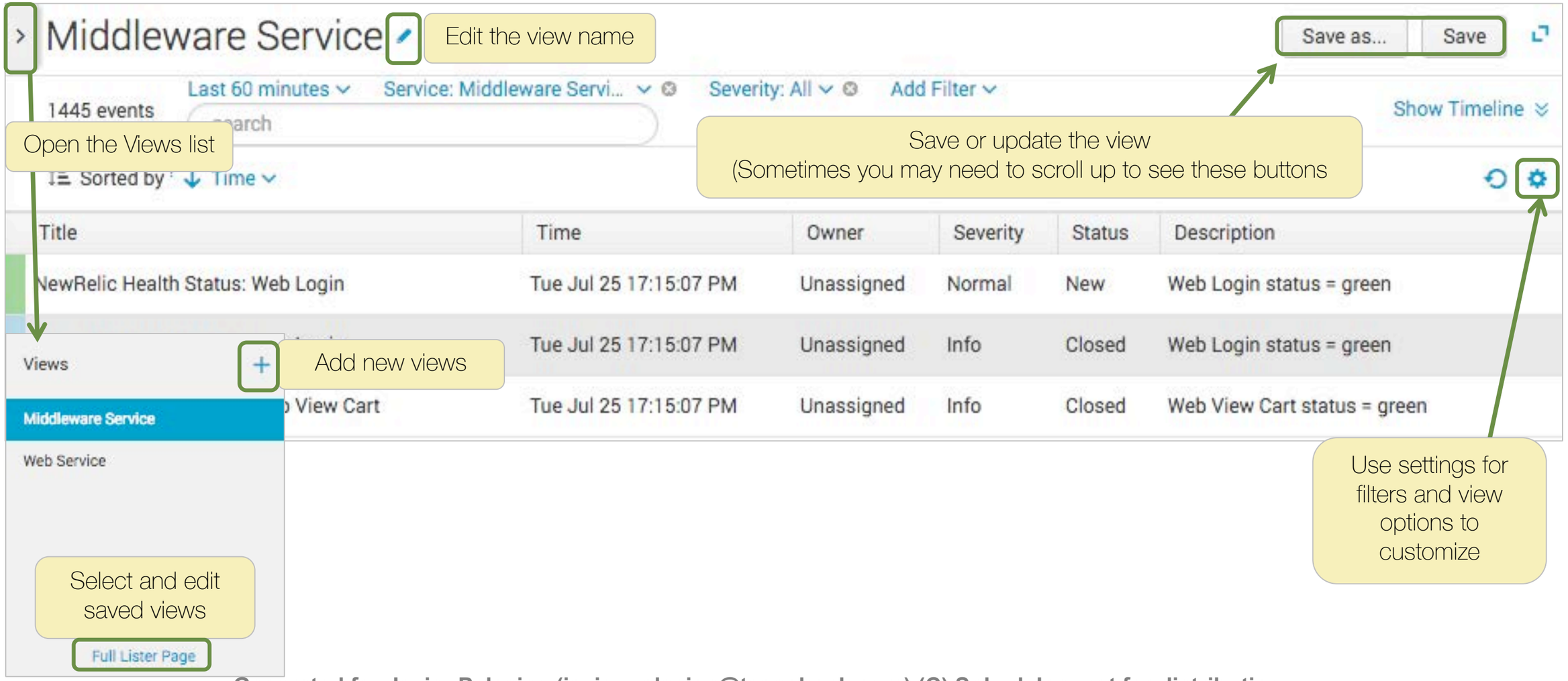
- Shows details about each event in the group
- Setting the severity, status or owner can be applied to the group overall, or individually to each event in the group
  - If applied at group level, changes are lost if the events are ungrouped
- Comments are always at the group level



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



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

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

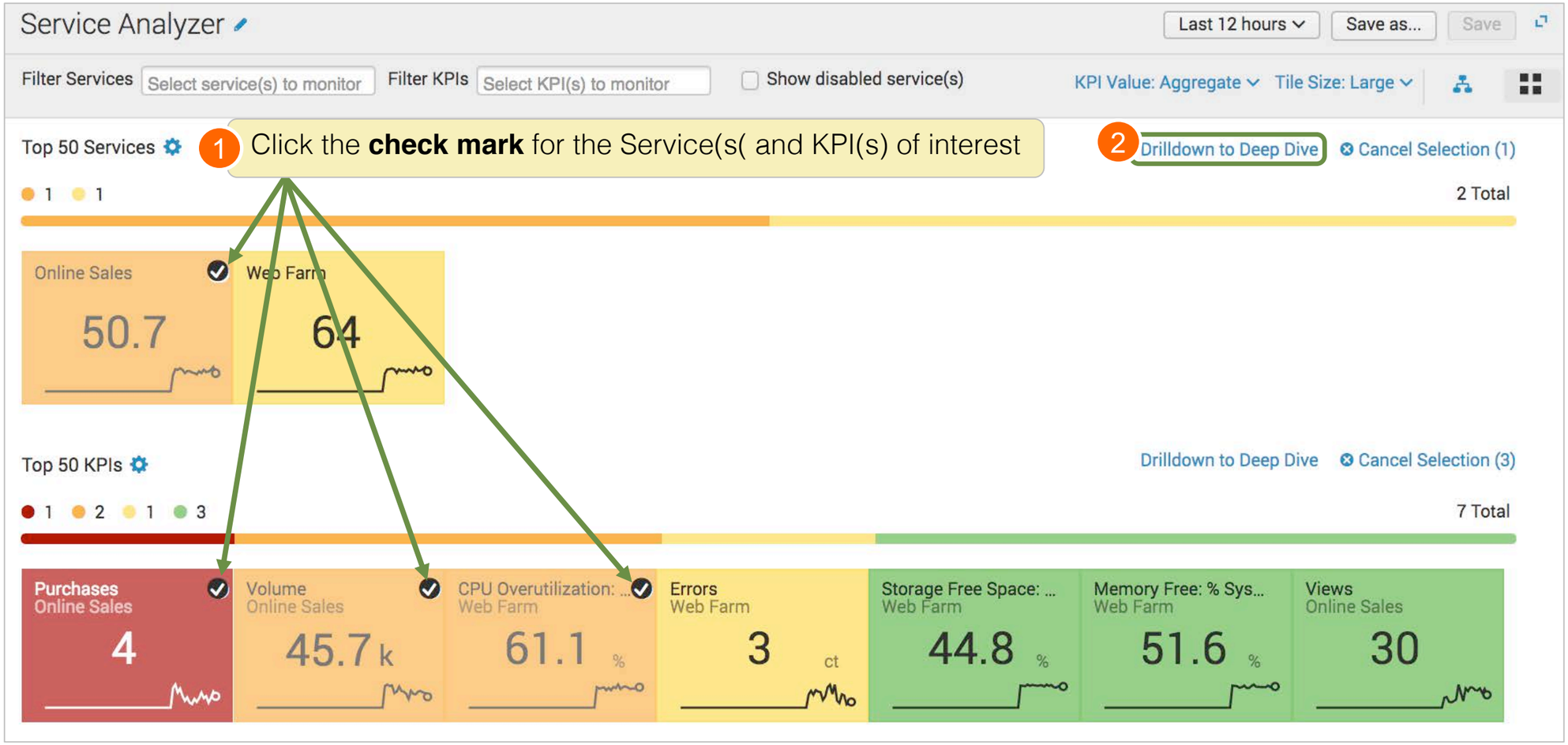
Default Deep Dive Example

- 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



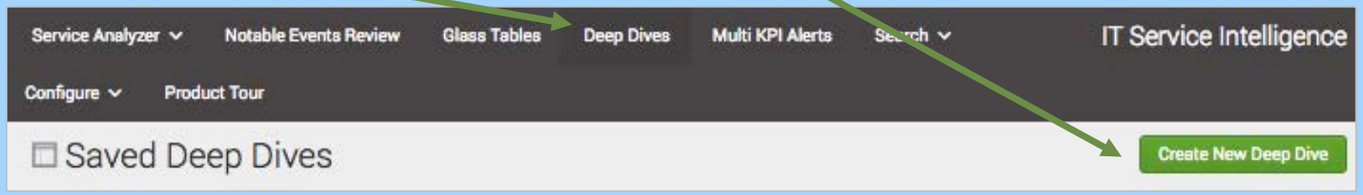
Deep Dive Navigation

Creating New Deep Dives

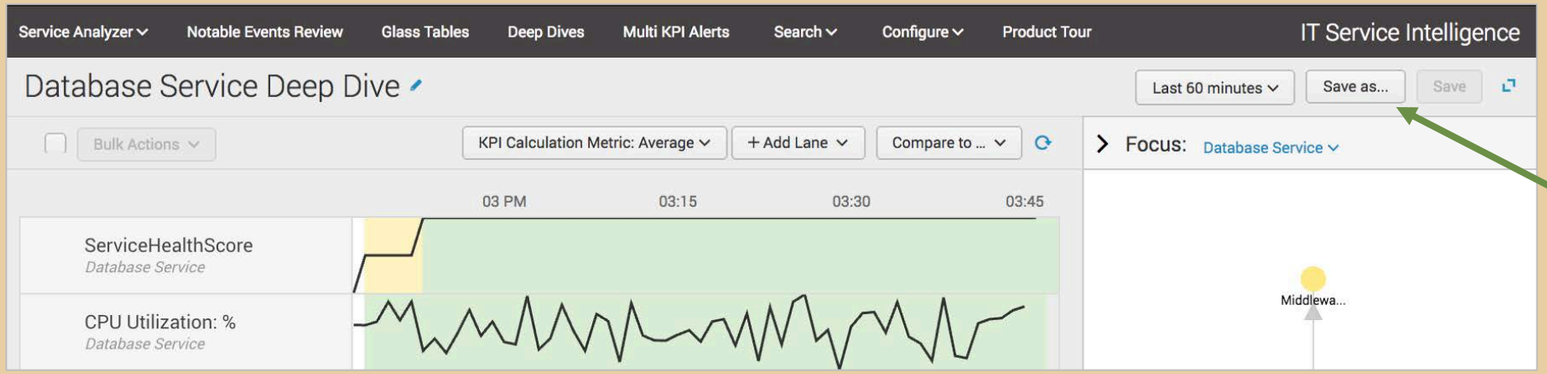
Either:

1 Click the **Deep Dives** menu

2 Select Create New Deep Dive



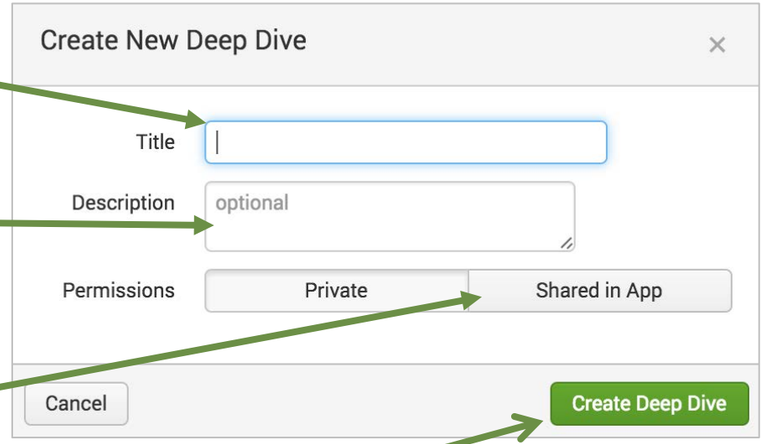
or



While viewing a deep dive, select **Save as…**

Naming New Deep Dives

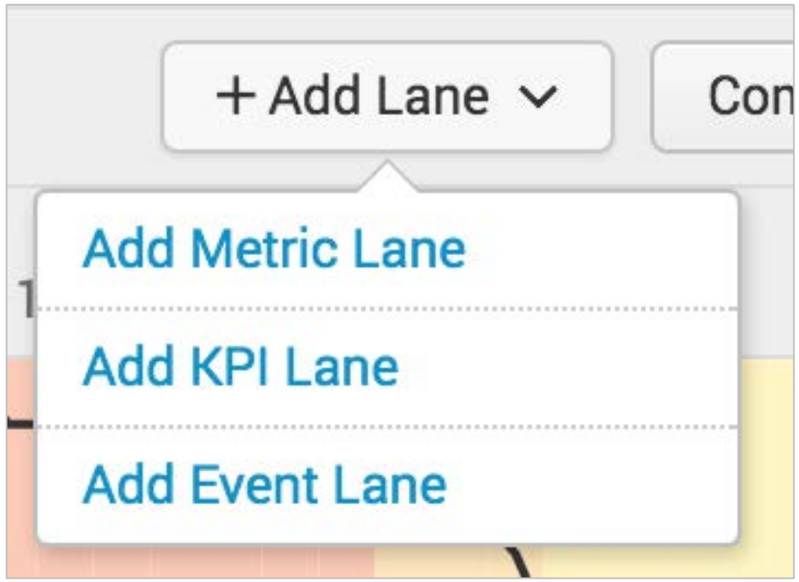
1. Enter a title for the new Deep Dive
2. Enter a description (optional)
3. (Optional)
   If you want to share it, click **Shared in App**
4. Click **Create Deep Dive**



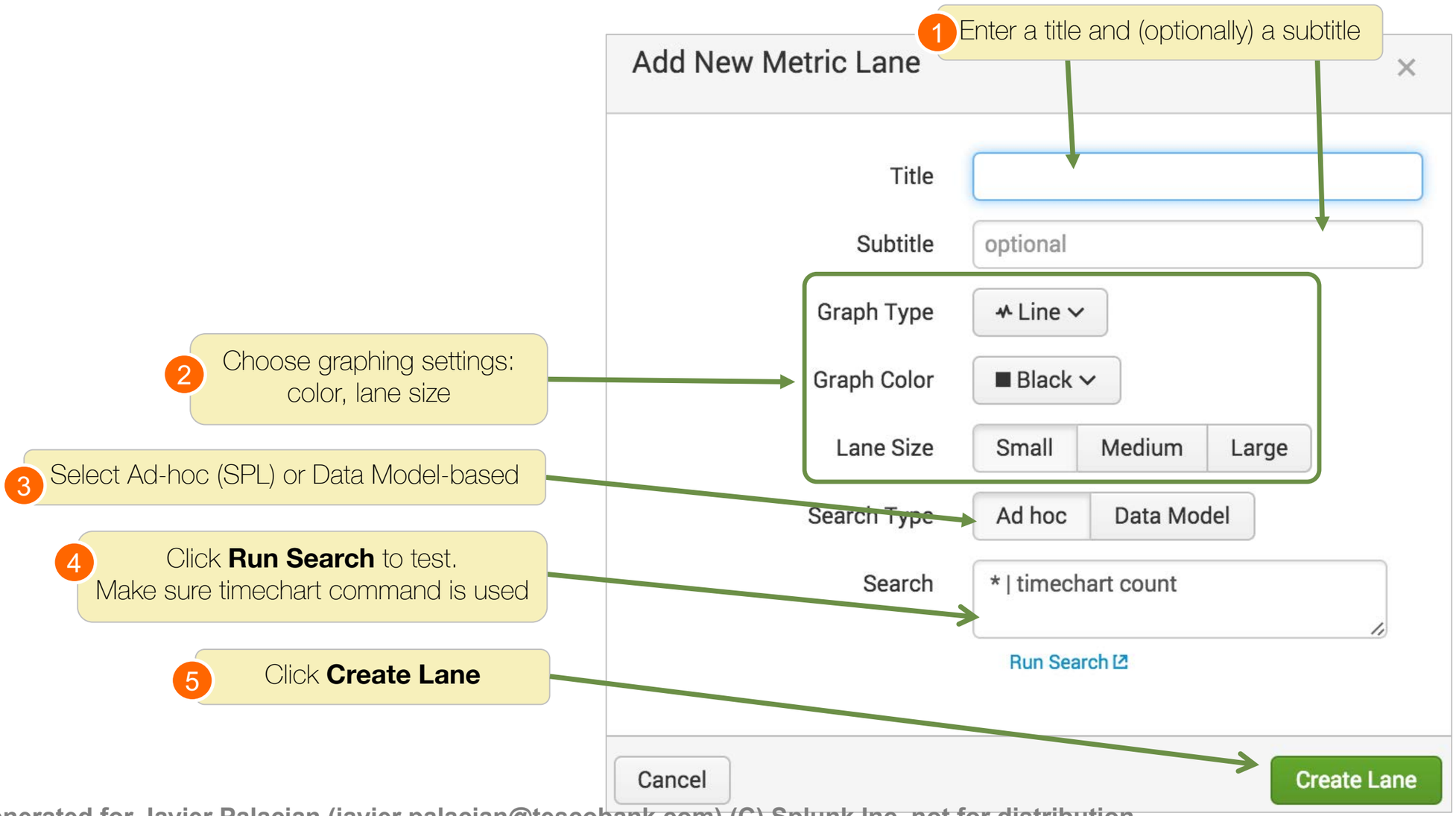
If you created it from the **Deep Dive** menu, it is blank to start

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

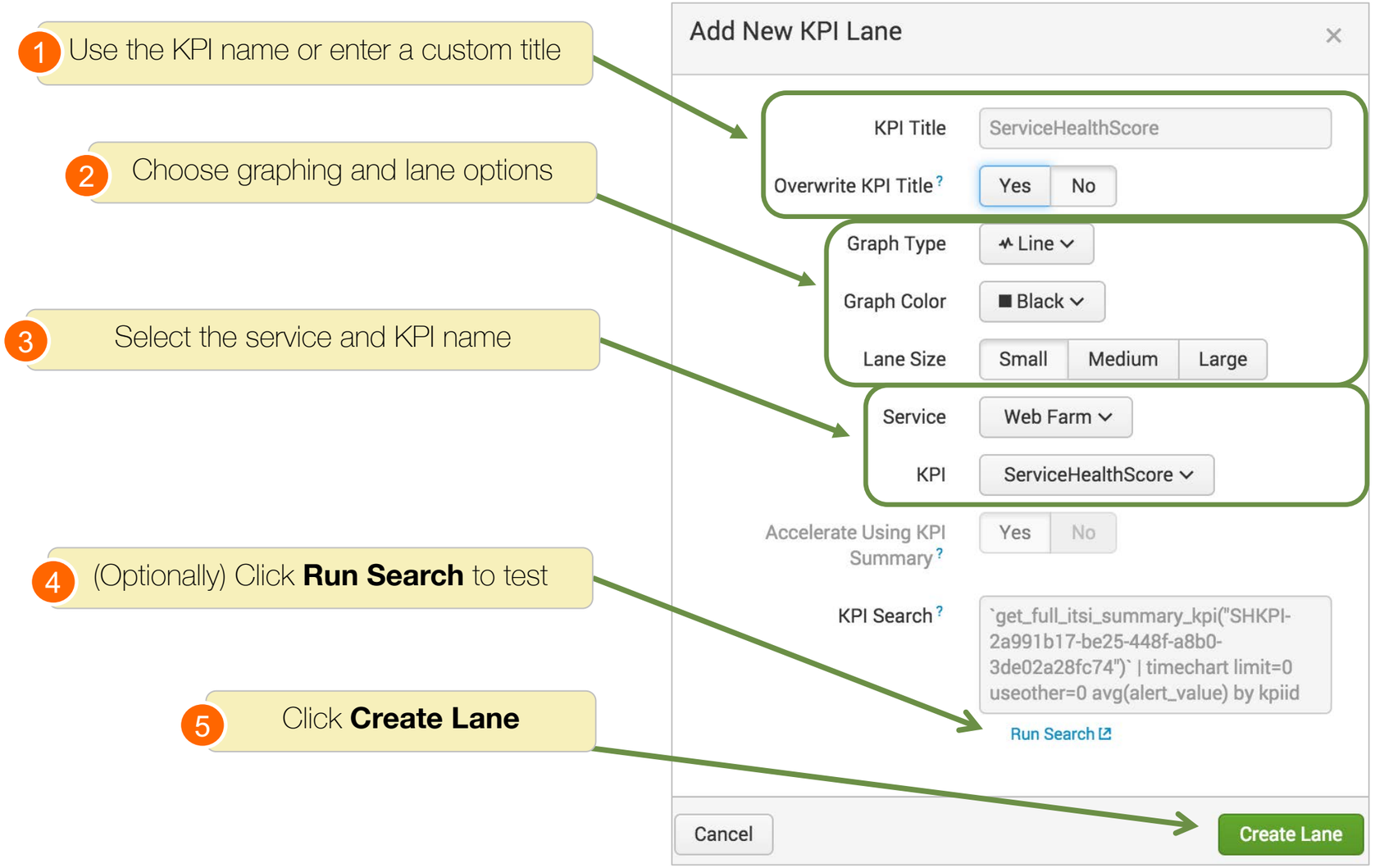


Adding a Metric Lane



Adding a KPI Lane

You can also add a KPI lane from the topology tree

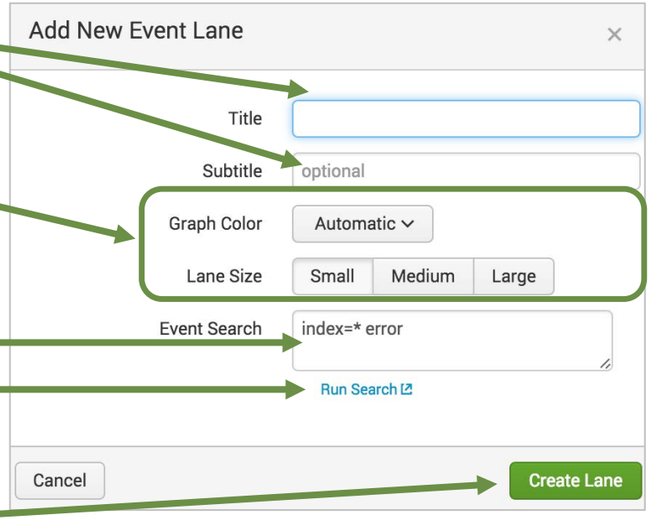


Adding an Event Lane

Note

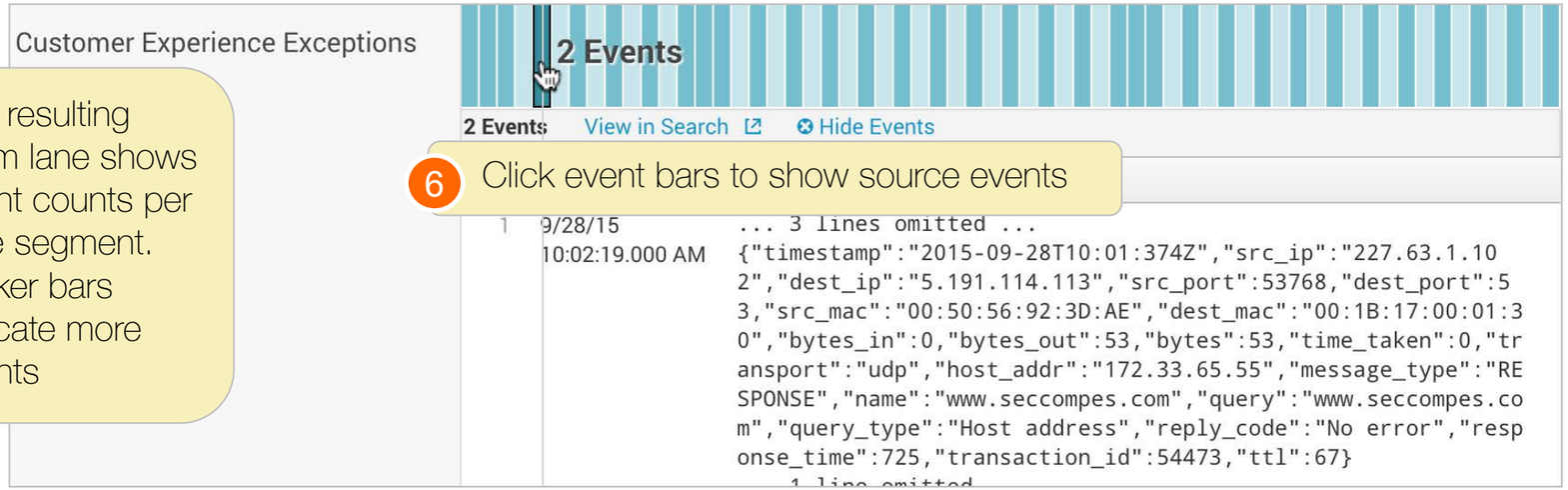
Event lanes provide fast access to the underlying event detailed information.

1. Enter a title and (optionally) a subtitle
2. (Optionally) Select a color and lane size
3. Create a search that returns events related to the topic of the deep dive
4. Click Run Search to test it
5. Click **Create Lane**



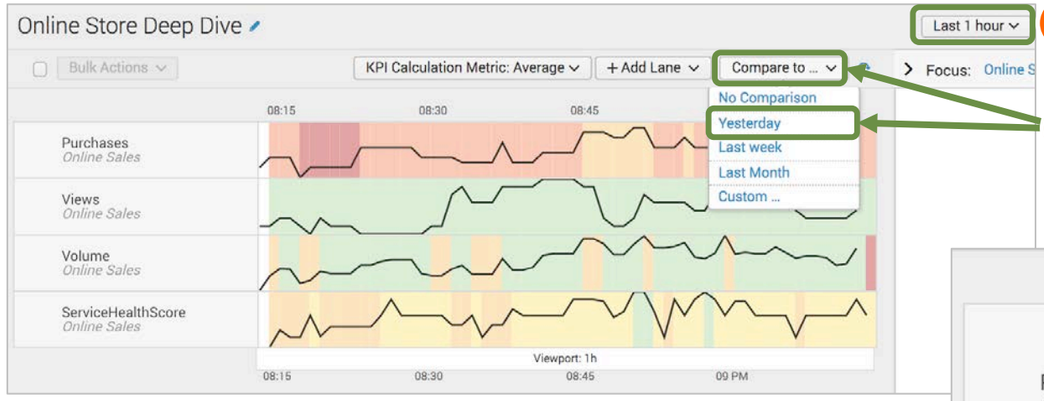
The resulting swim lane shows event counts per time segment. Darker bars indicate more events

6. Click event bars to show source events

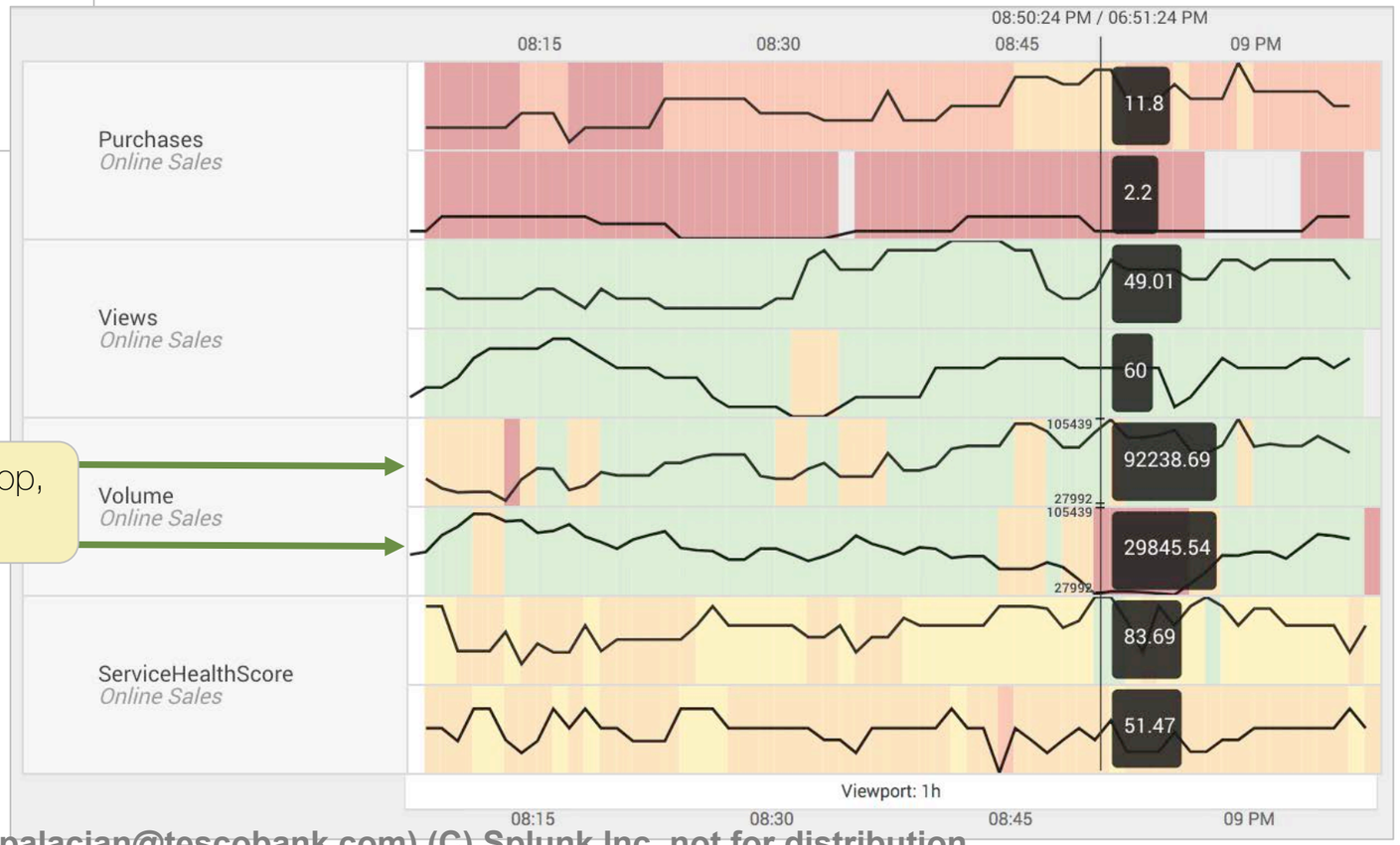


 | 8 June 2018

Compare Earlier Time Ranges: Twin-Lane



1. Select a time range of interest
2. Click **Compare to ...** and specify an analogous time range for comparison

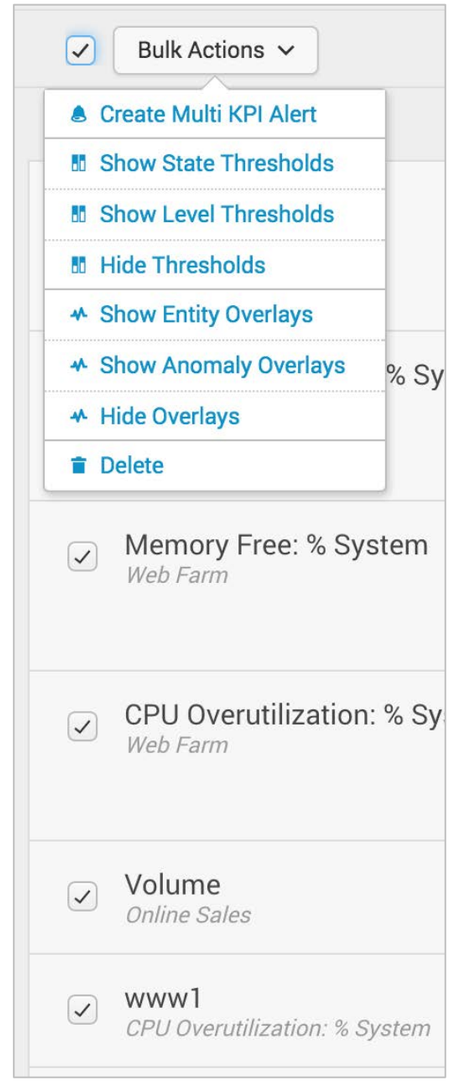


All lanes show recent time period on top, past time period on bottom

To turn the comparison off, click **Compare to ... > No Comparison**

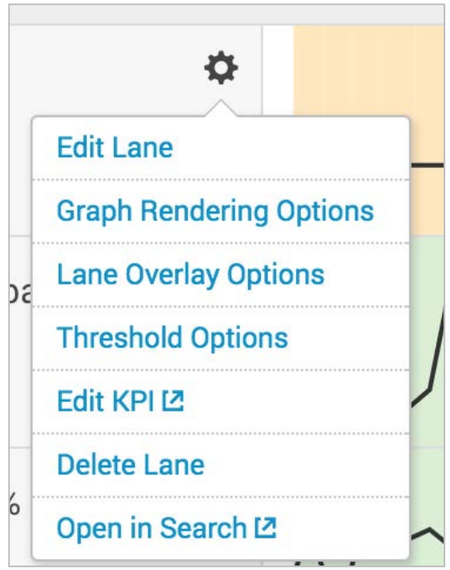
Applying Bulk Actions

- 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



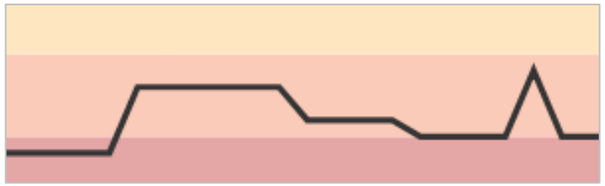
Selecting Threshold Display

- 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

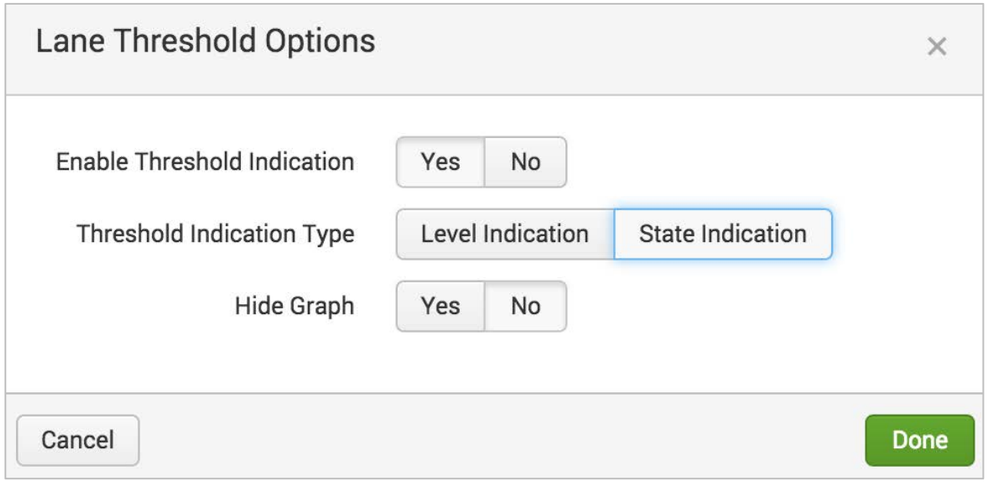


State

Level

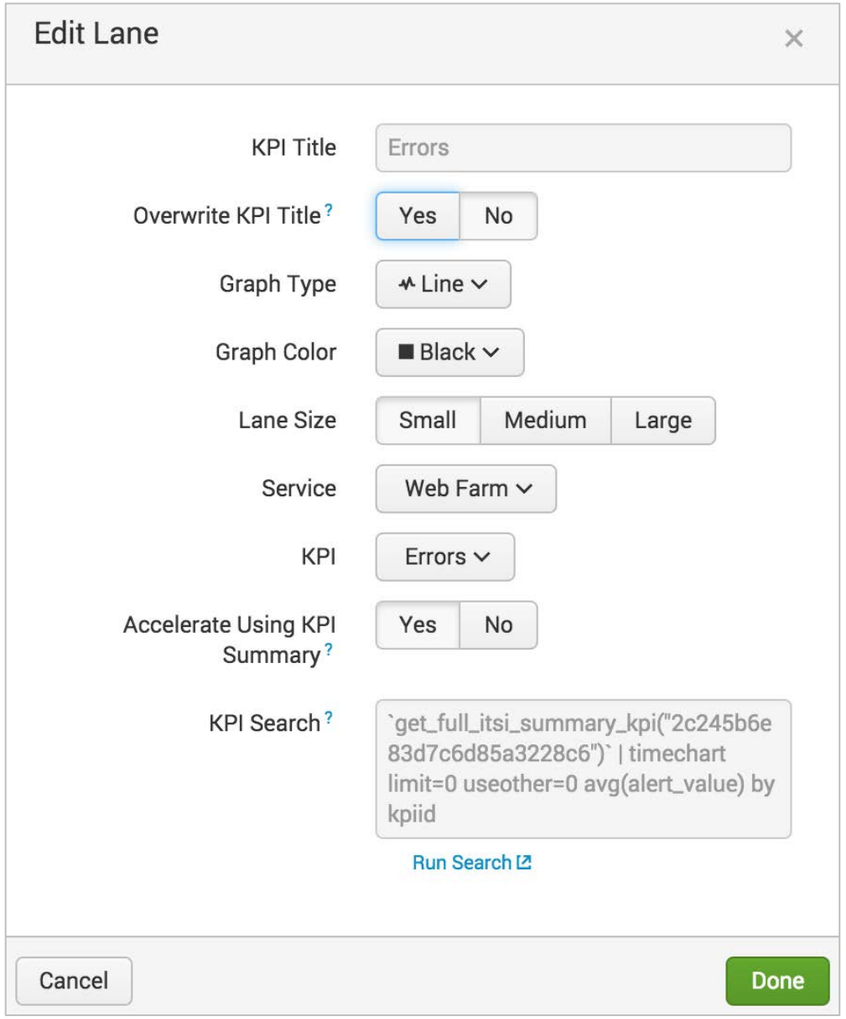


State without line graph



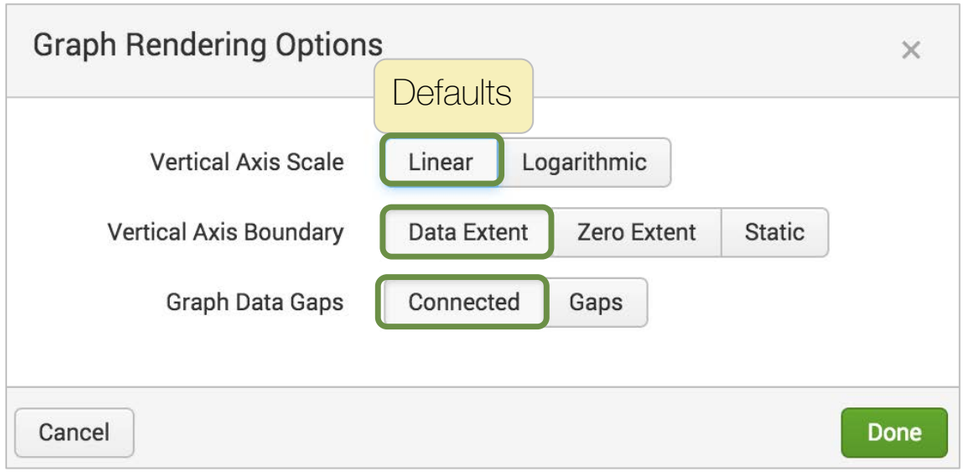
Editing Lane Appearance

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**



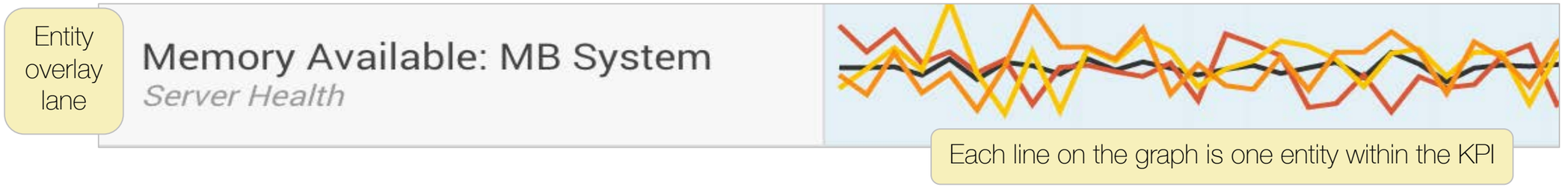
Editing Graph Rendering Options

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**



Configuring Lane Overlays

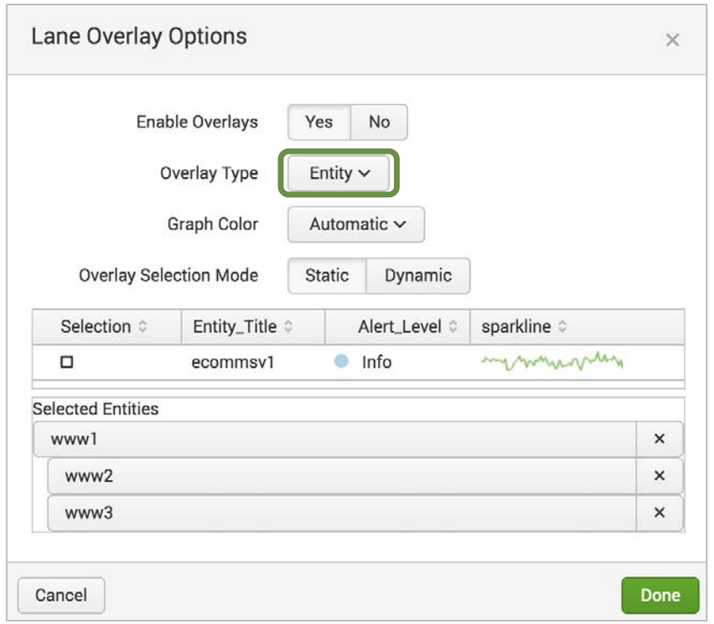
- Swim lanes can be configured to include overlays
- Overlays display either multiple entities or anomalies



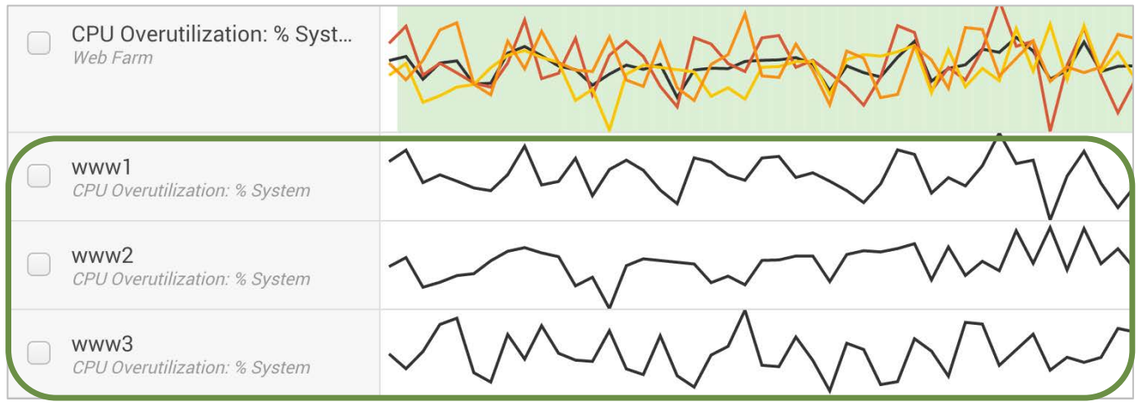
Enabling Entity Lane Overlays

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**



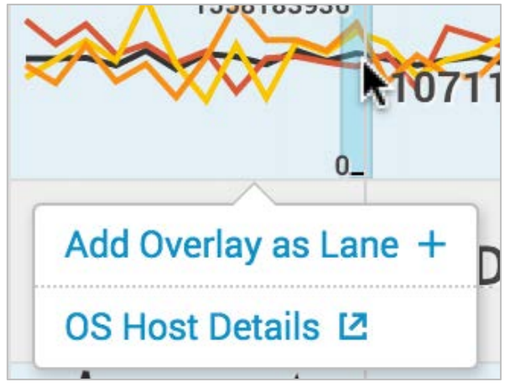
Adding Entity Overlays as Lanes



- 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

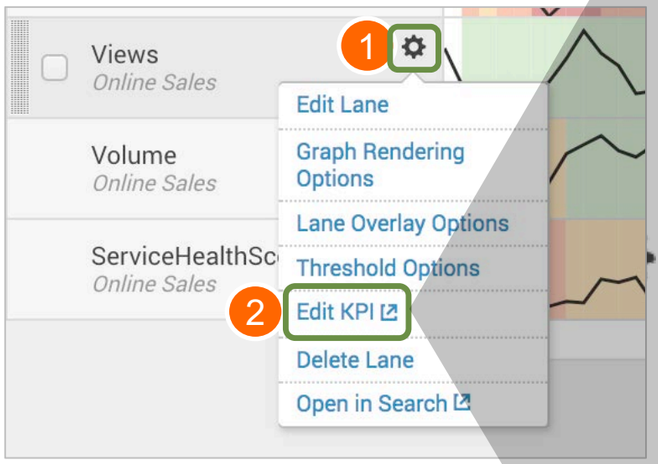
Configuring Lane Drilldown

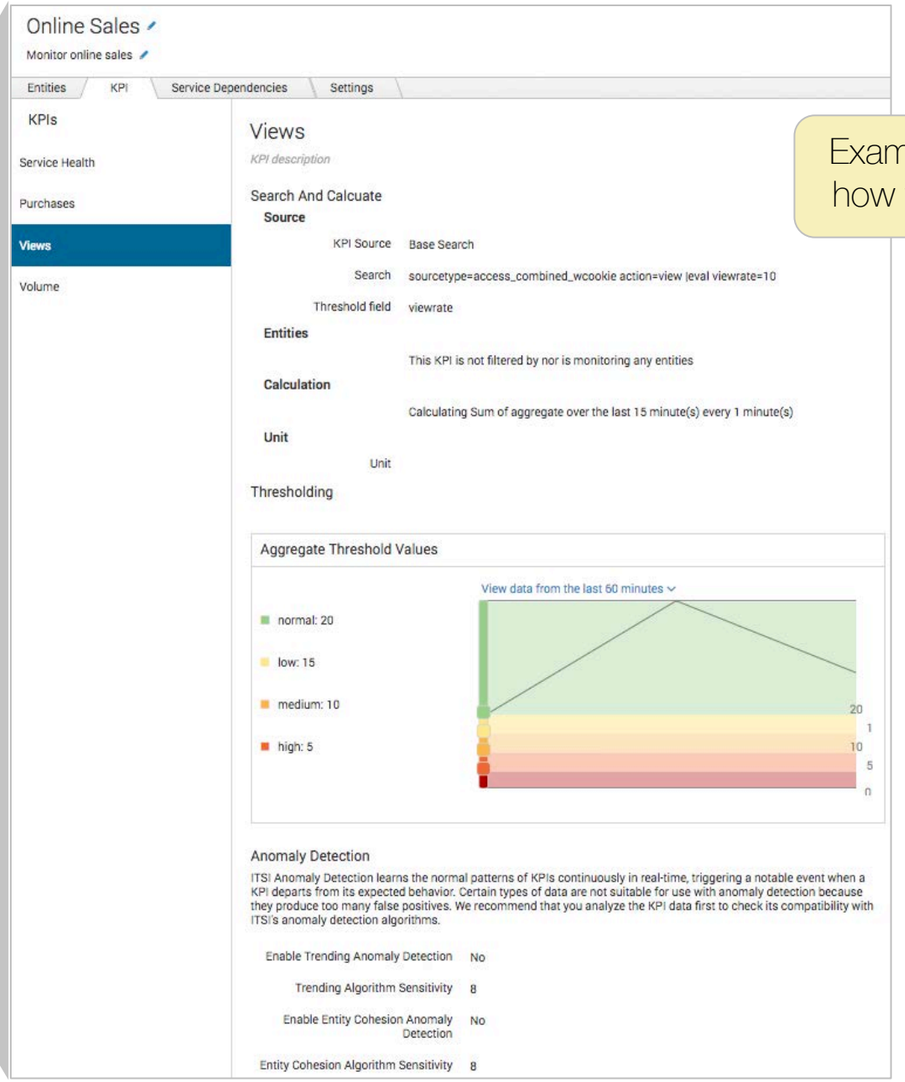
- By default, lanes are not clickable for further drilldown (except event lanes, which are clickable)
  - Use the lane's ⚙ icon and select **Open in Search** to explore the lane's data set



- 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



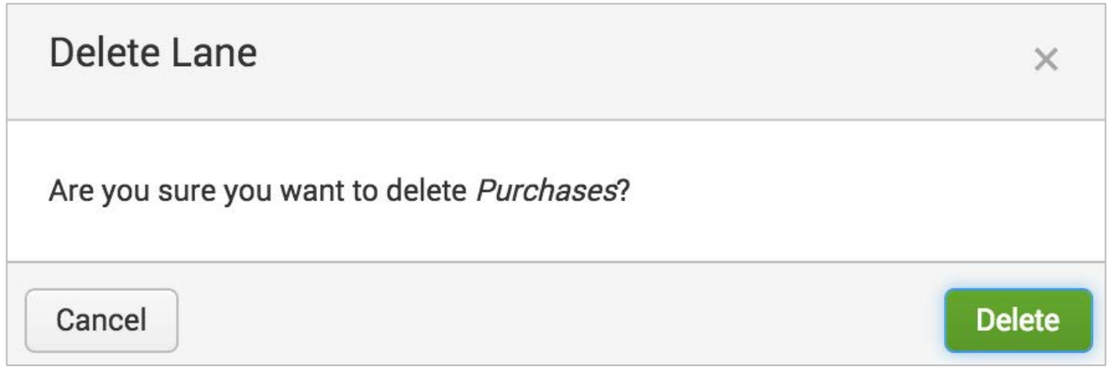


Examine the details of how the KPI was built

Deleting a Lane

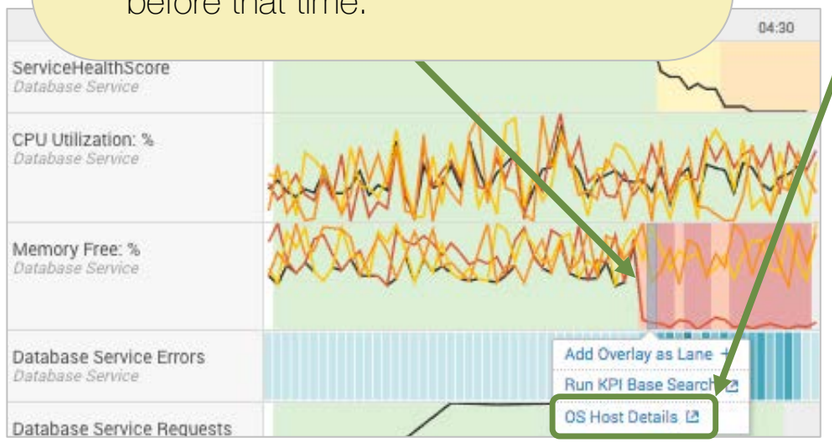
1. Click the lane's ⚙ icon and select **Delete Lane**
   - Or use the bulk actions menu
2. Click **Delete** to confirm

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



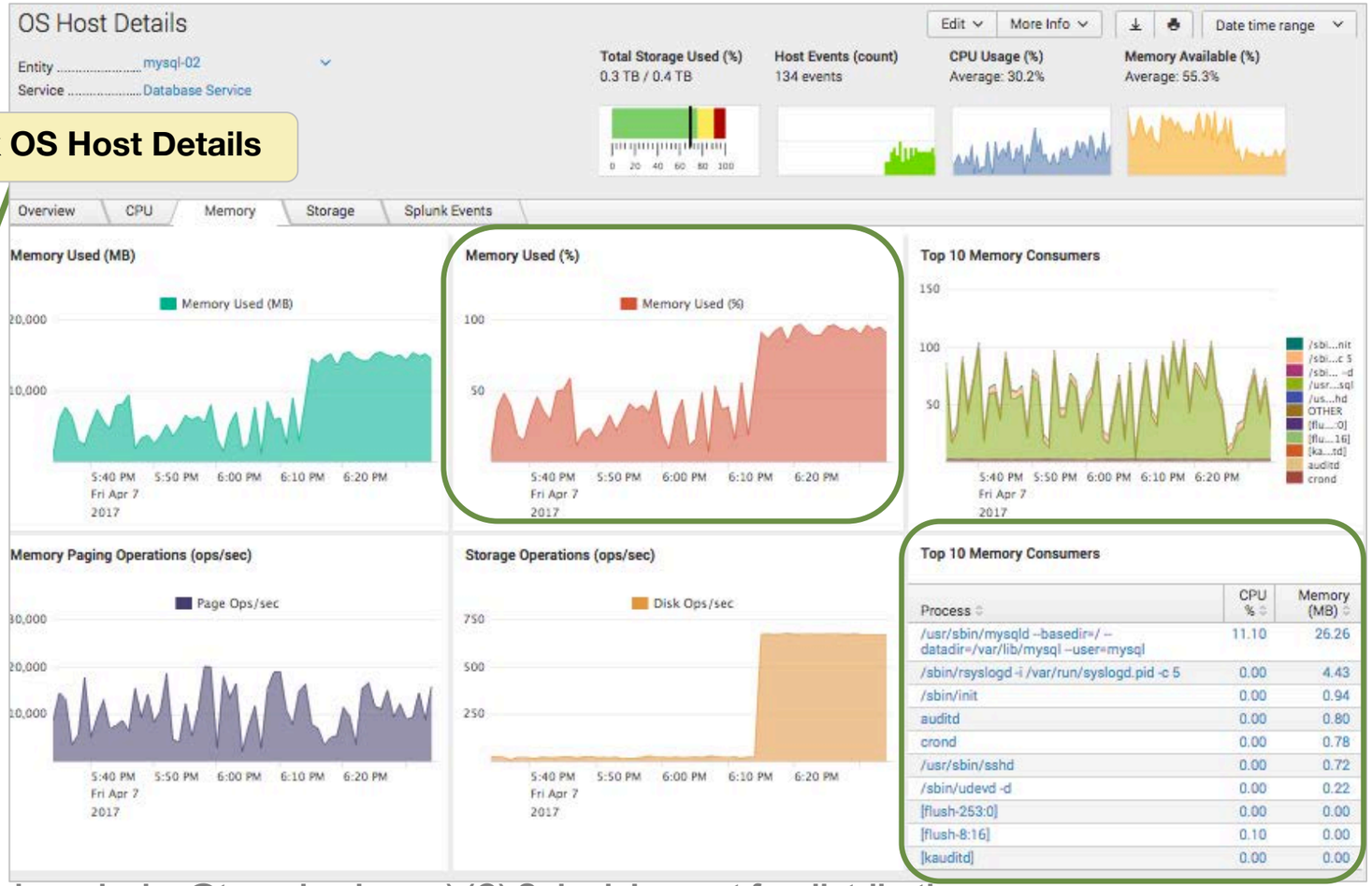
Troubleshooting with Module Details View

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**

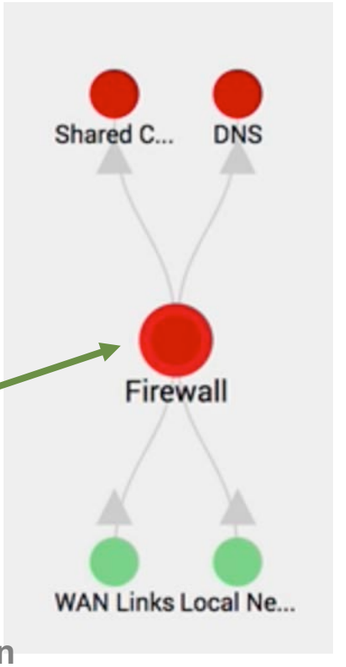
3. View the dashboard to view the health of that entity



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).

.conf18™

splunk>

.conf18:
Monday, October 1 – Thursday, October 4

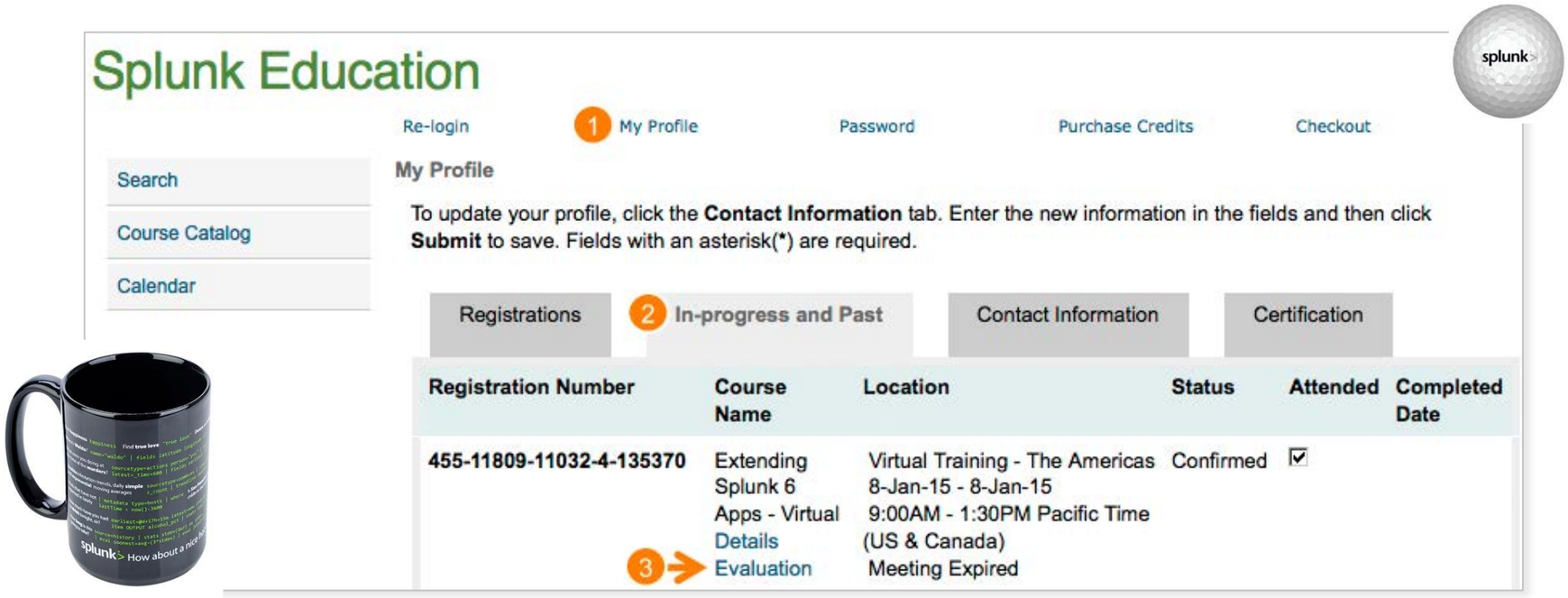
Splunk University:
Saturday, September 29 – Monday, October 1

ORLANDO FLORIDA

Walt Disney World Swan and Dolphin Hotels

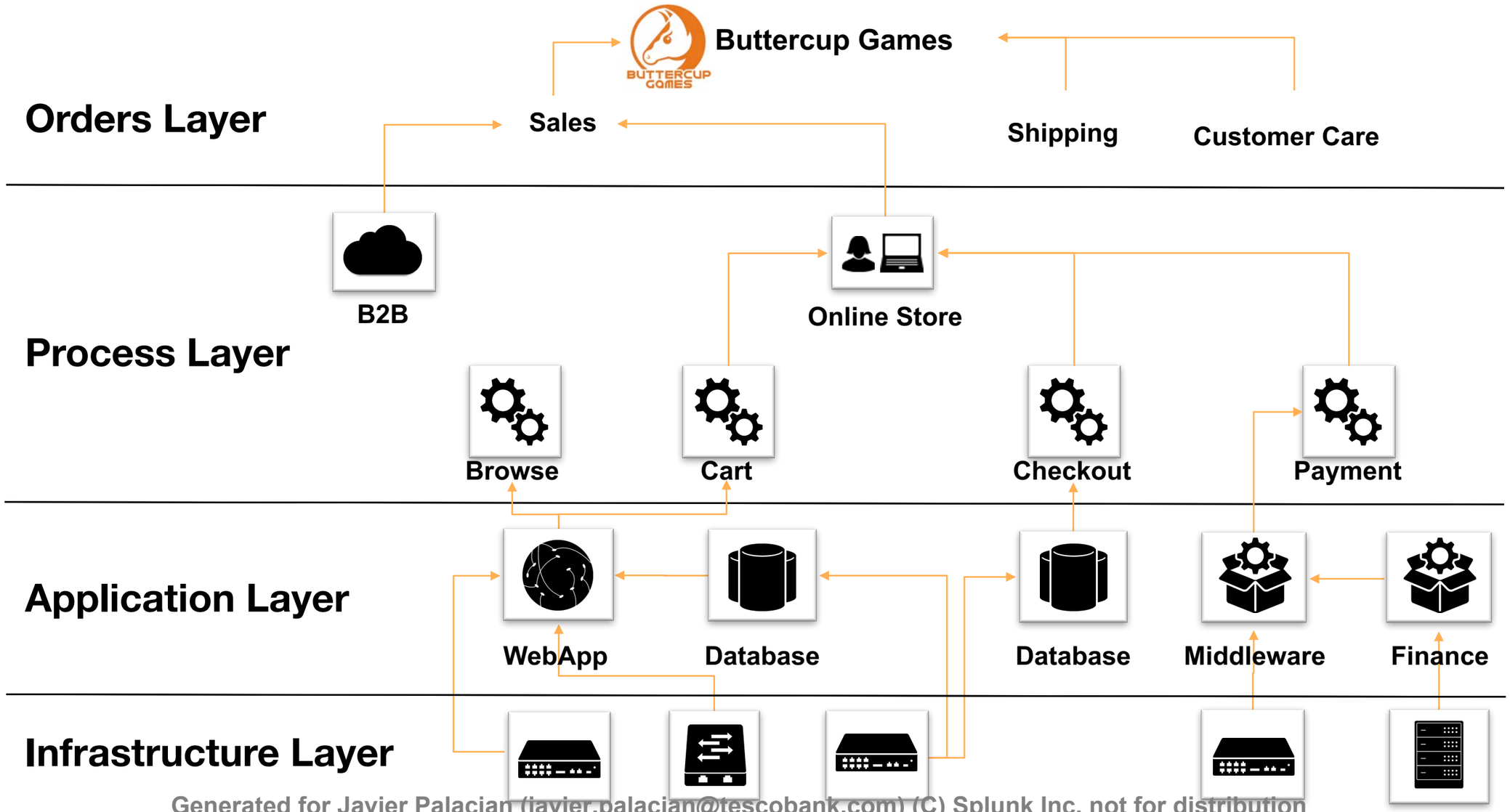
Thank You

- 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



Appendix

Buttercup Games Service Layers



Services & KPIs: Key Performance Indicators

Buttercup Games
- Revenue
- Costs
- Customer Satisfaction

In ITSI, a KPI is a scheduled search that returns the value of an IT performance metric

Orders Layer

Sales
- Orders Received
- Order Revenue
- Avg Order Size

Shipping
- Orders Shipped
- Shipped Revenue
- Service Level

Customer Care
- Call Wait Time
- Calls In Queue
- First Call Resolution

Process Layer

B2B
- B2B Order Lines Received
- B2B Revenue
- Avg Processing Time

Online Store
- Online Orders Received
- Online Revenue
- Avg Response Time

Browse
- Trans Count
- Avg Response Time
- Error Rate

Cart
- Item Count
- OOS Item Count
- Error Rate

Checkout
- Avg Promo Discount
- Conversion Rate
- Abandoned Rate

Payment

Service: Payment

KPIs:
- Orders Processed
- Revenue
- Declined Count

Application Layer

WebApp
- Service Calls
- Response time
- Error Rate

Database
- Query Count
- Response Time
- Storage Free

Middleware/Finance
- Message Count
- Queue Depth
- Error Rate

Infrastructure Layer

- Available Bandwidth
- Connection Count
- Error Rate

- CPU Load
- Memory Used
- IO Latency

ITSI Modules

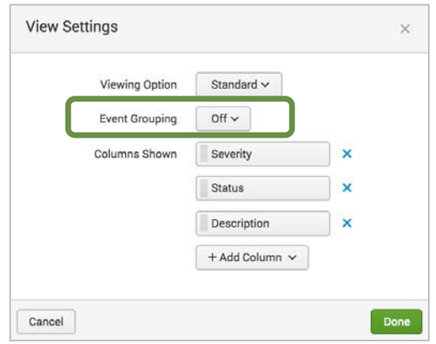
- Help users understand and act on data that comes from monitoring services within ITSI
  - Each ITSI Module contains its own predefined metrics, entities, service configurations, and activity views
  - Modules can include entity discovery key performance indicator (KPI) templates, metrics, or entity 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

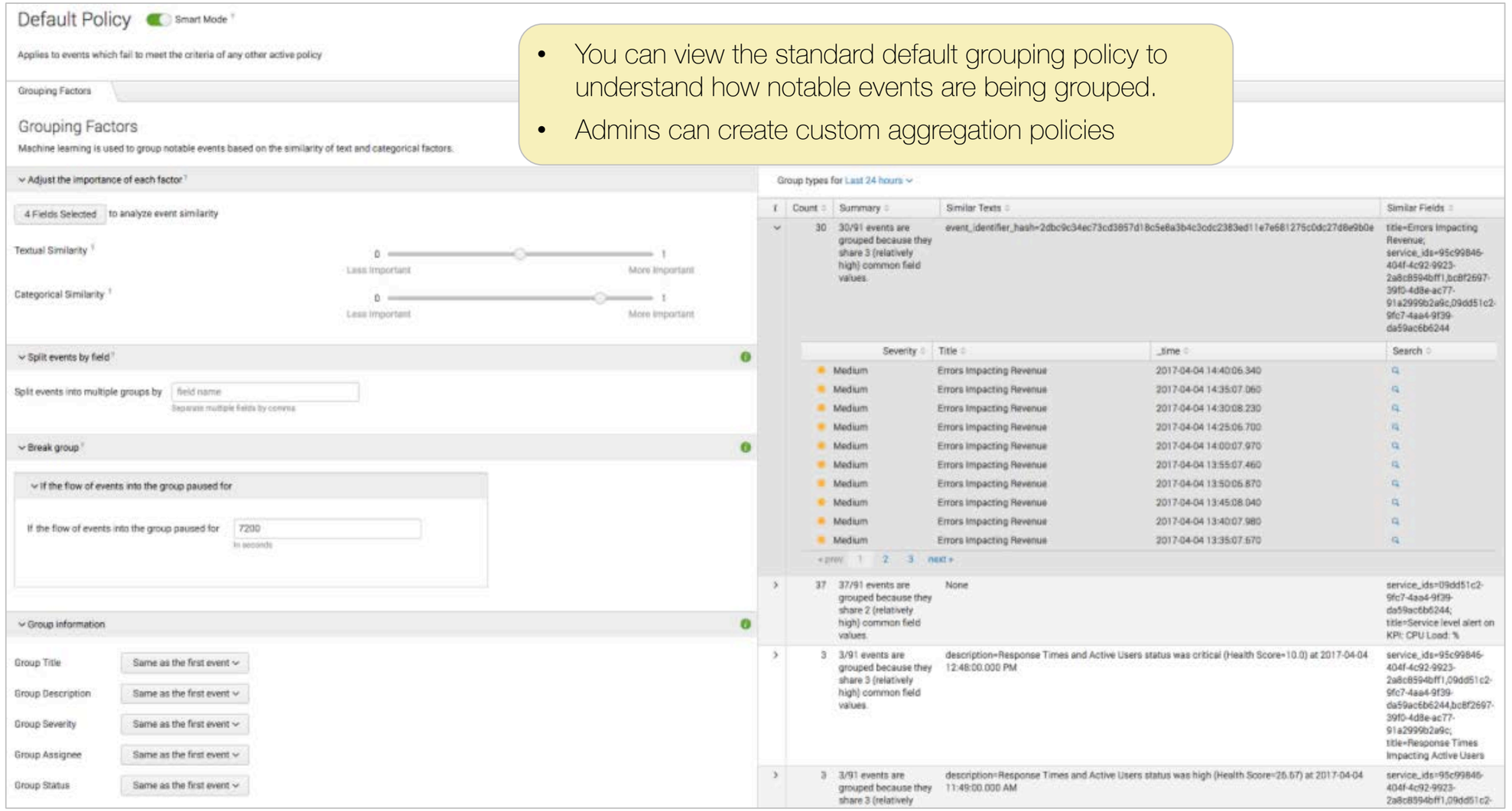
Grouping and Aggregation Policies

- 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

Default Grouping Policy



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

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

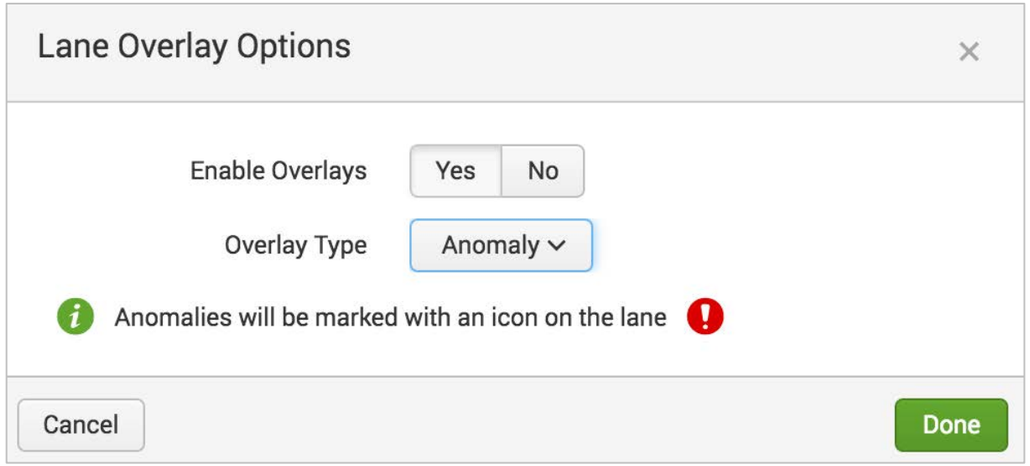
Types of Multi KPI Alerts

- 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

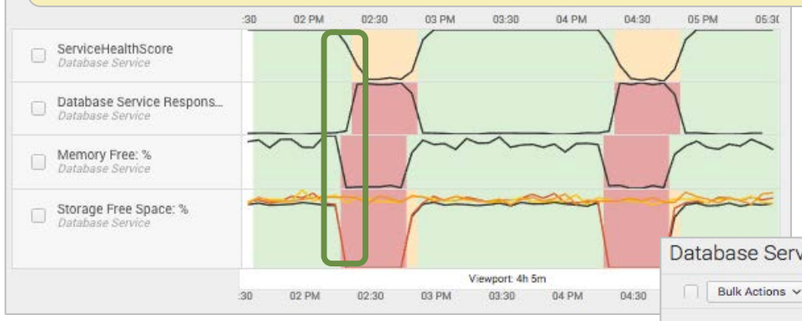
Only available for KPIs with anomaly detection enabled

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**

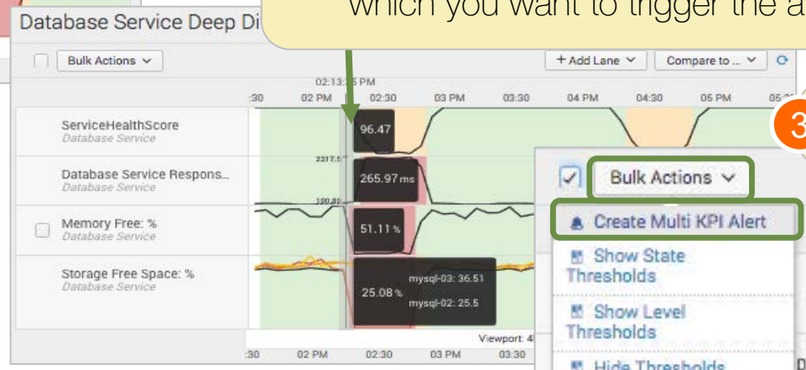


Deep Dive to Multi KPI Alert

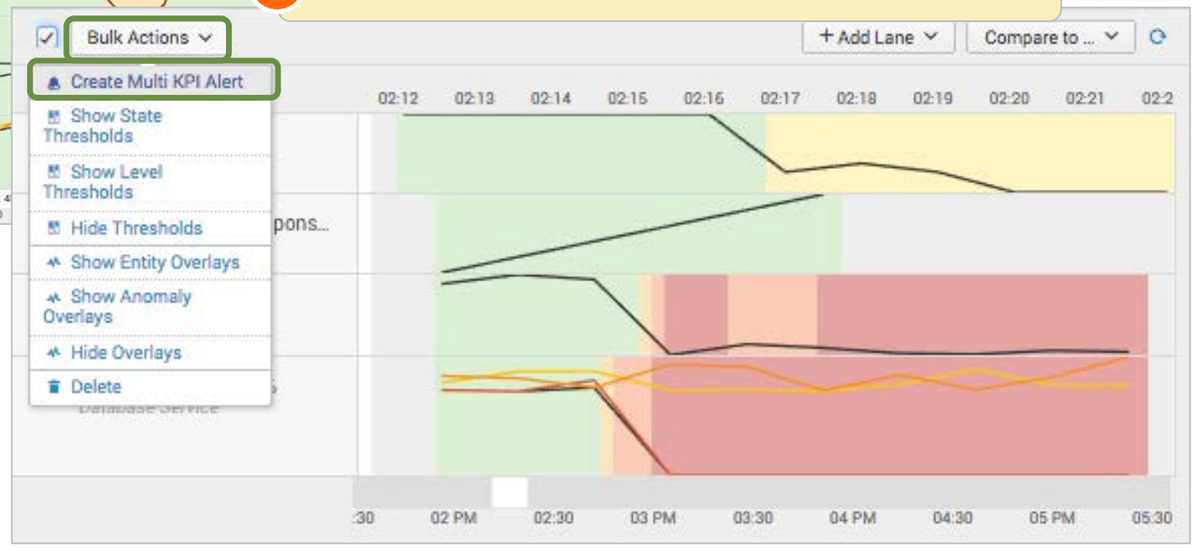
1 Find a Deep Dive condition that would be a useful alert



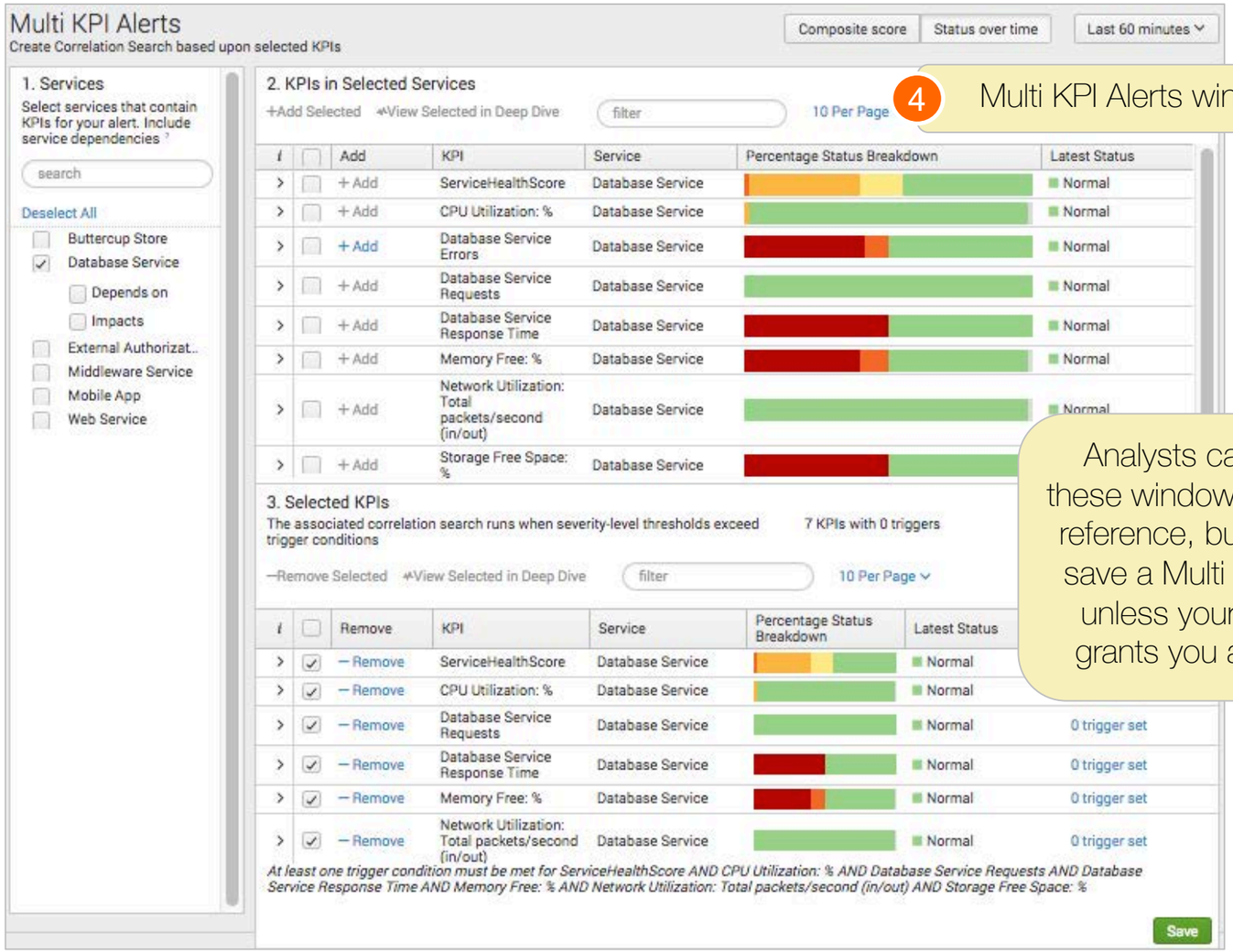
2 Click-and-drag to zoom to specify the change threshold (orange or yellow) for which you want to trigger the alert



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



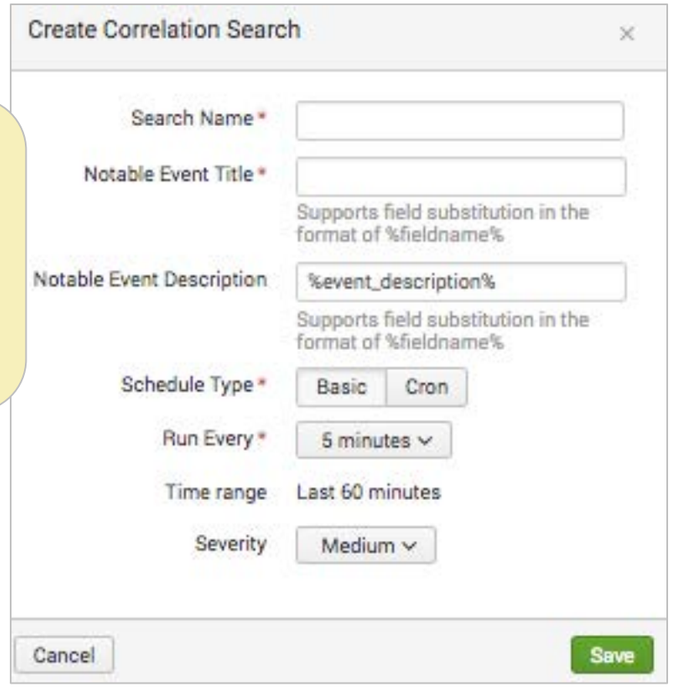
Deep Dive to Multi KPI Alert (cont.)



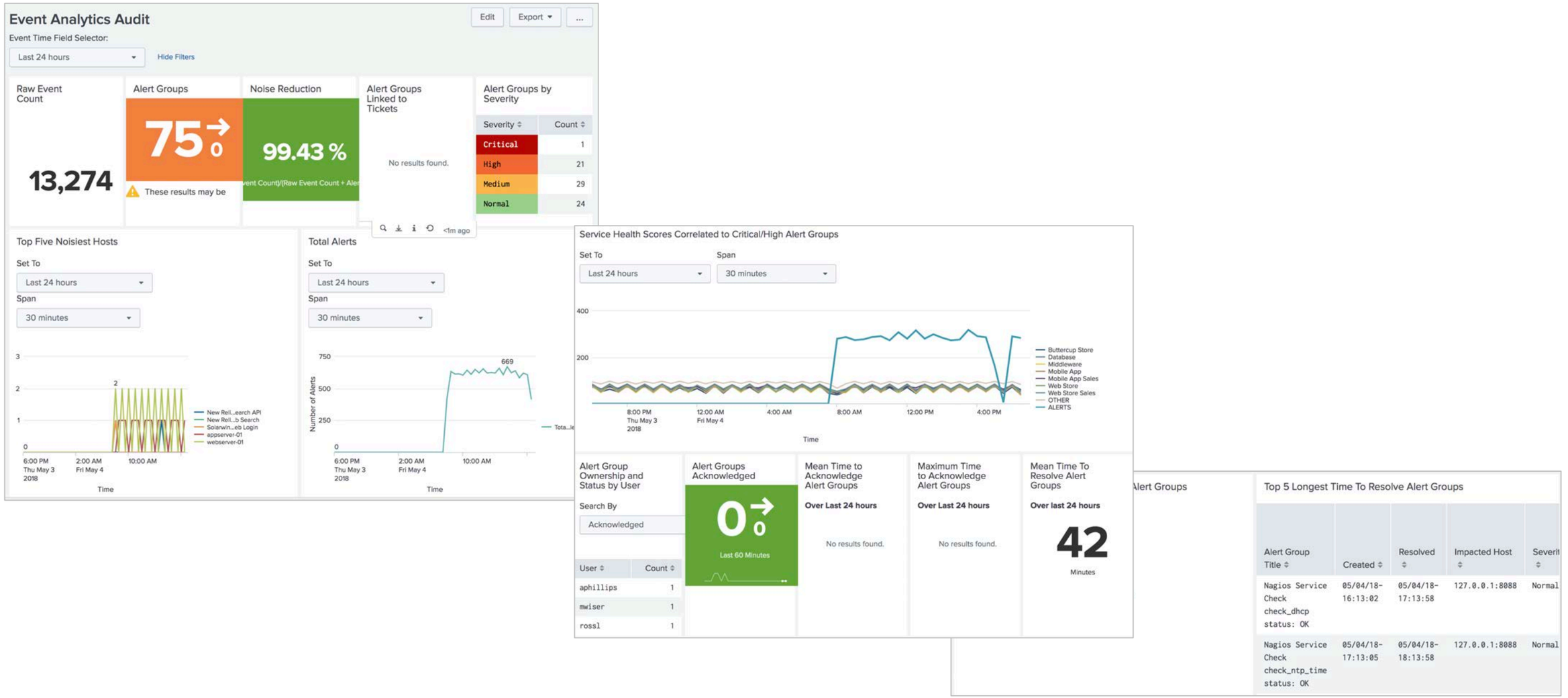
4 Multi KPI Alerts window opens. Click **Save**

Analysts can view these windows for your reference, but cannot save a Multi KPI alert unless your admin grants you access.

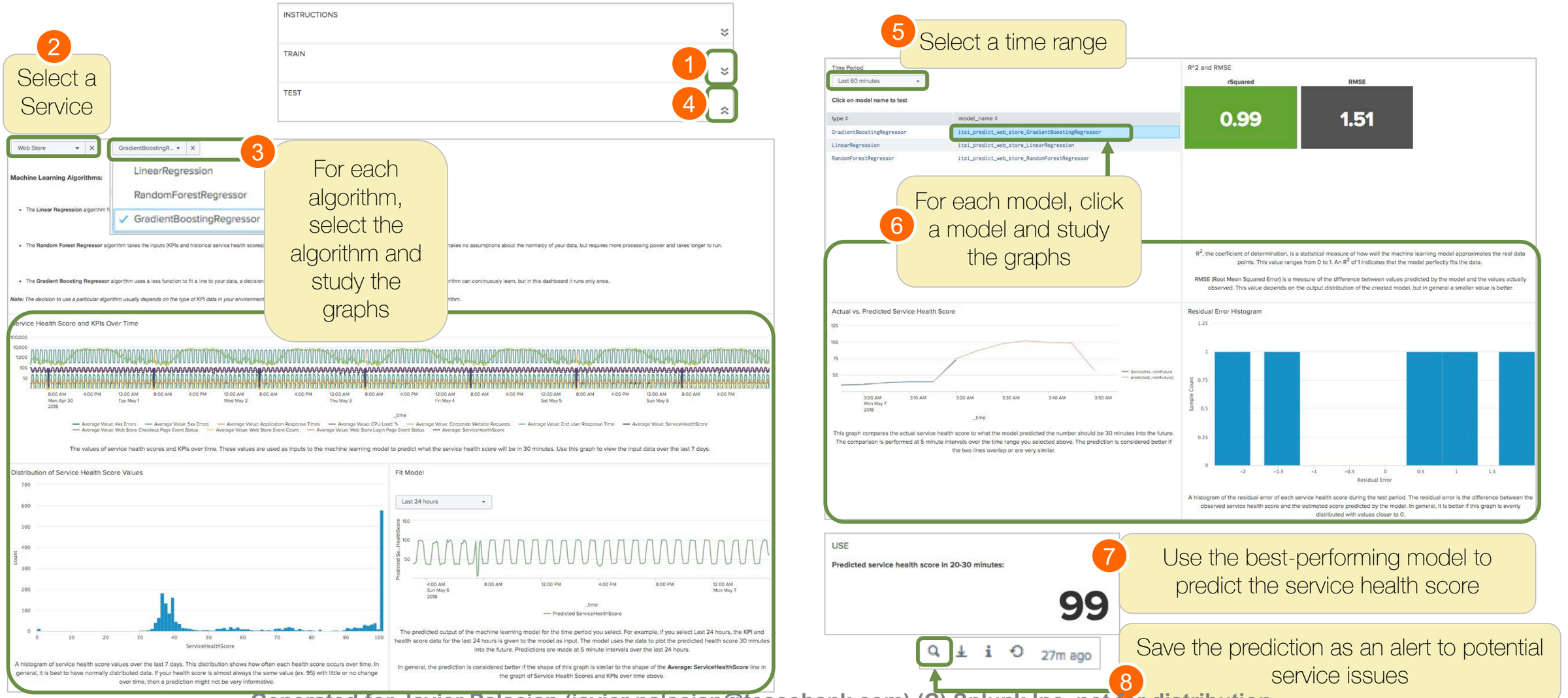
5 Admin names the alert search and the notable event and clicks **Save**



Event Analytics Audit Dashboard



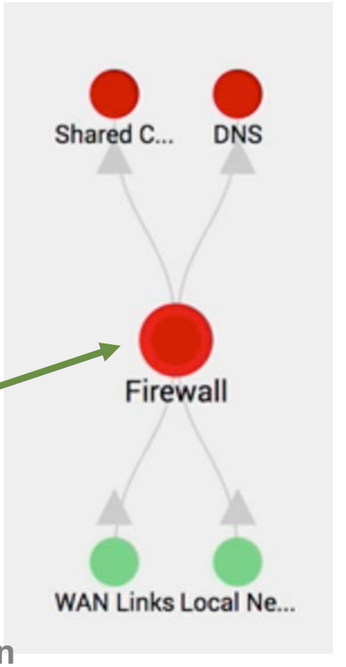
Event Analytics Audit Dashboard



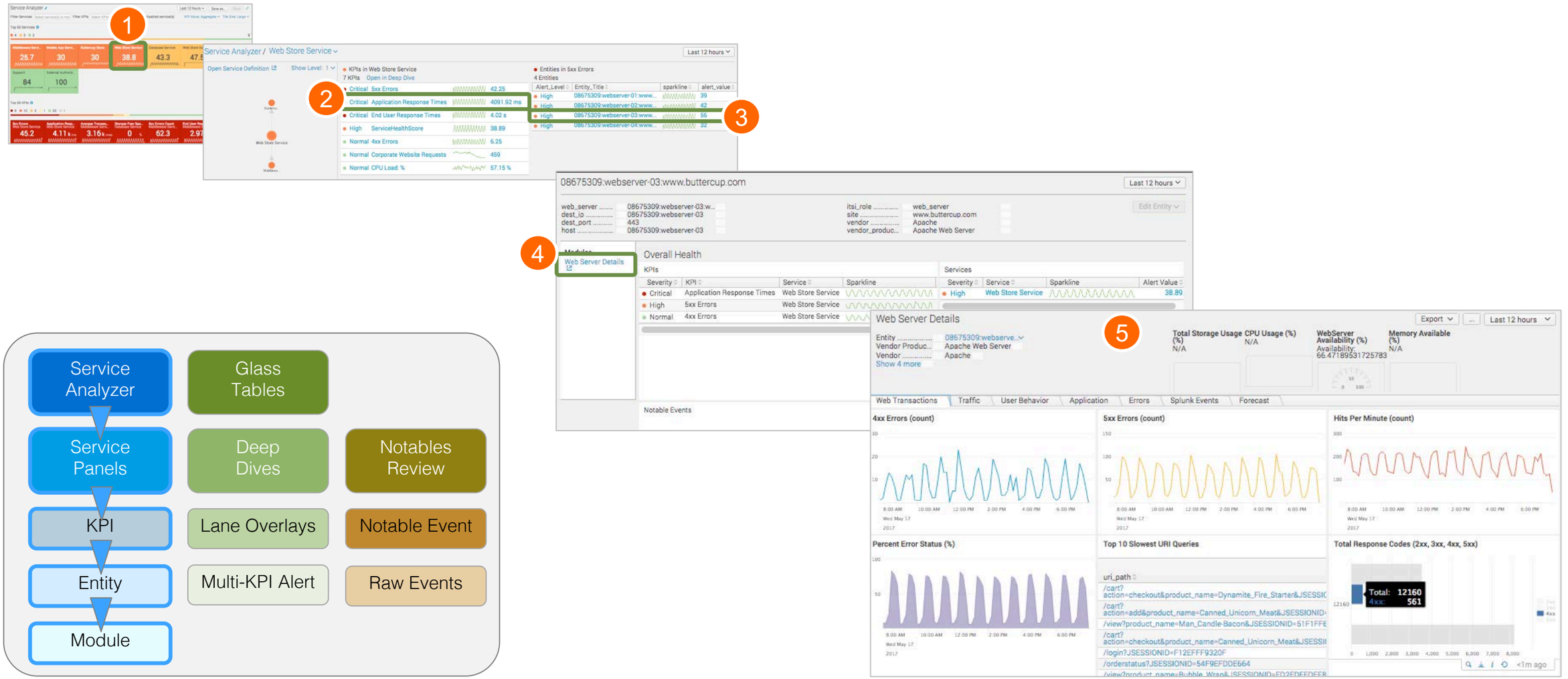
Other Troubleshooting Workflows

- 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

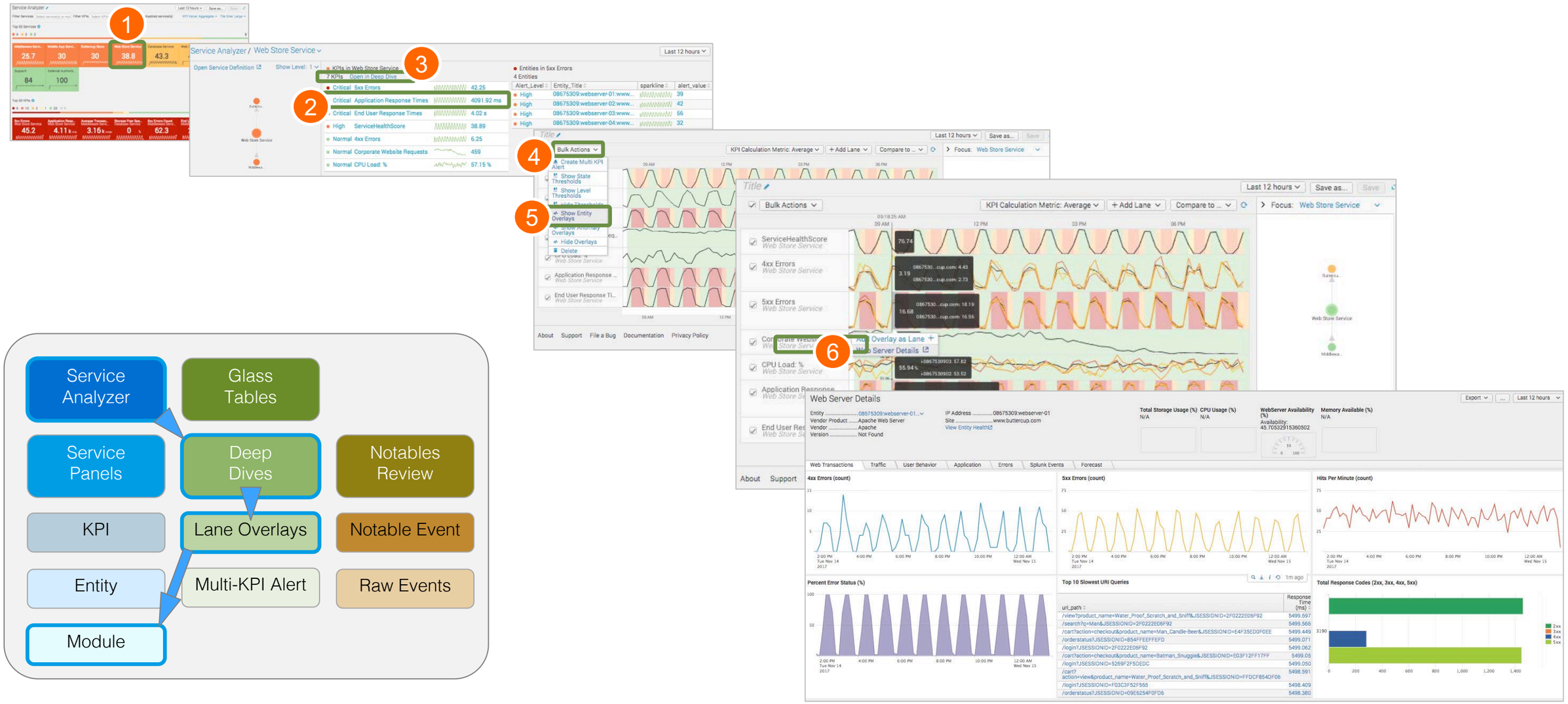
When troubleshooting, **drill down until you find the bottom of the tree:** the deepest item whose dependencies are all green



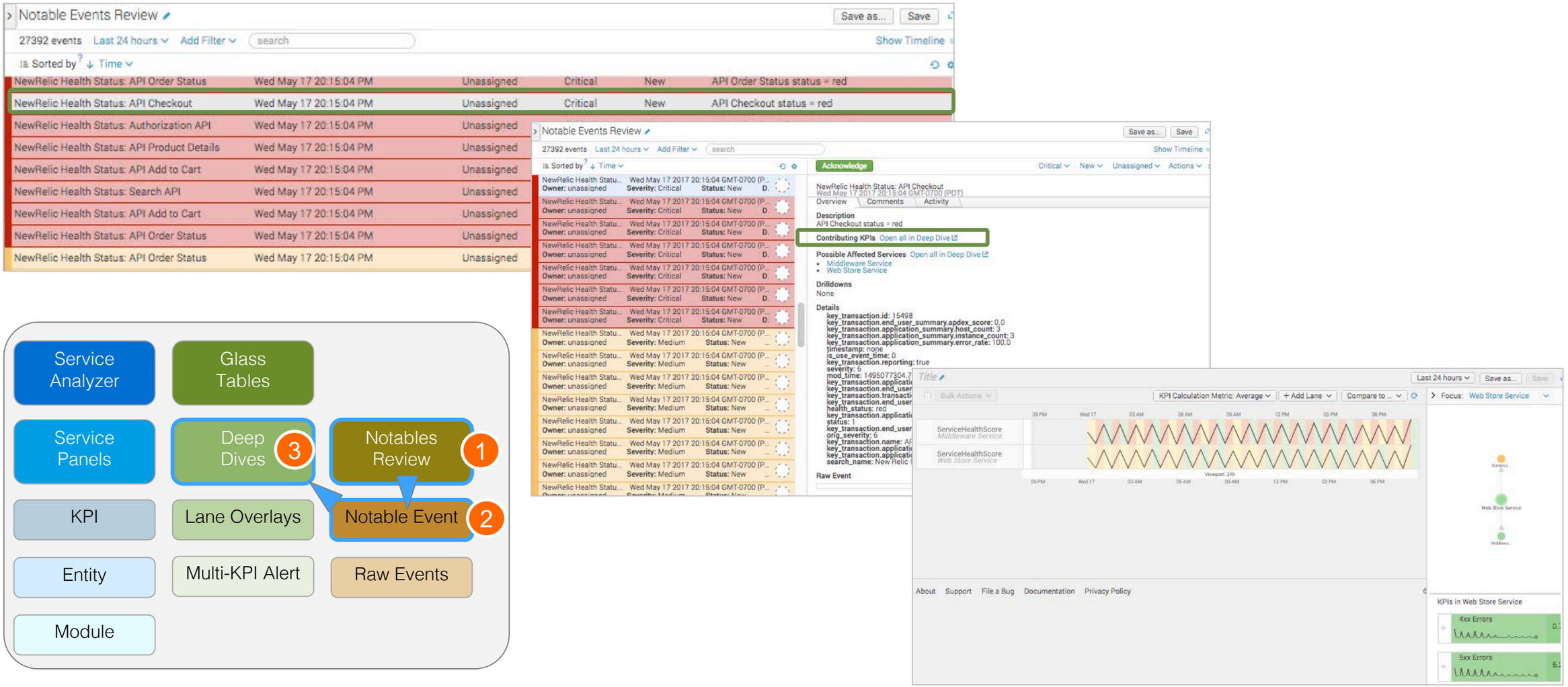
SA > Service > KPI > Entities > Module



SA>Deep Dive>Bulk Actions>Overlay>Module



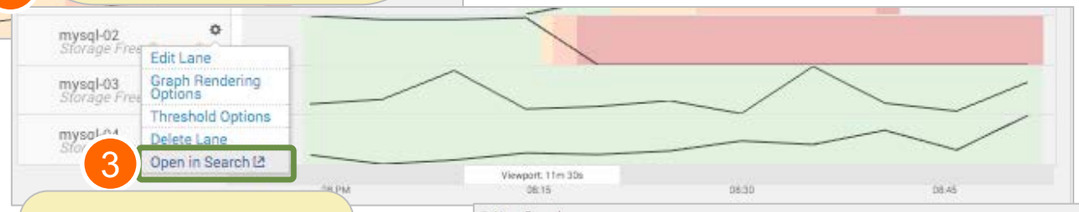
Notable Events Review > NE > Deep Dive



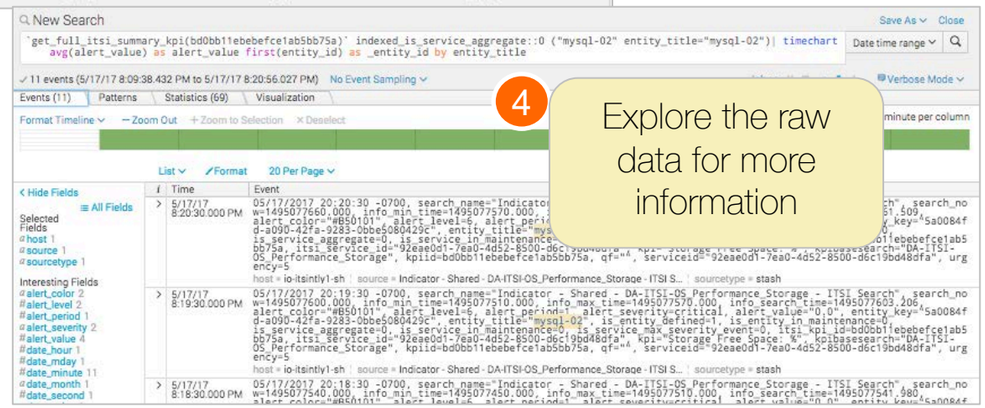
Glass Table>Deep Dive>Overlay>Drilldown

Click a Service on the Glass Table to go to its Deep Dive.

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**



Explore the raw data for more information

Because they enable you to examine the state your business services at a specific moment 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.