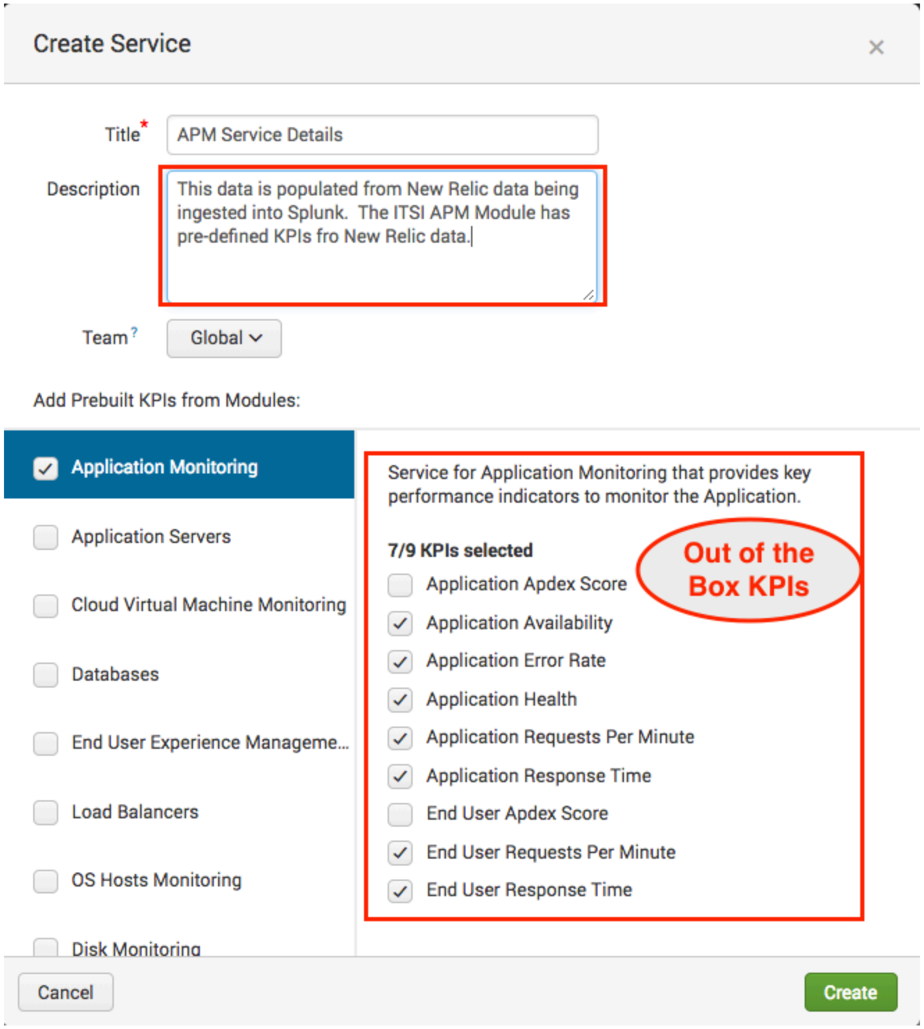
Splunk ITSI with New Relic … Better Together!

Splunk ITSI includes an 'APM Module' with pre-defined Key Performance Indicators (KPIs) for application performance. Adding APM KPIs to an ITSI Service is as simple as adding the New Relic TA, ingesting the data and selecting which KPIs you wish to include in your service. Here's the configuration:



Create Service

Title* APM Service Details

Description: This data is populated from New Relic data being ingested into Splunk. The ITSI APM Module has pre-defined KPIs fro New Relic data.

Team? Global

Add Prebuilt KPIs from Modules:

- ☑ Application Monitoring
- □ Application Servers
- □ Cloud Virtual Machine Monitoring
- □ Databases
- □ End User Experience Manageme...
- □ Load Balancers
- □ OS Hosts Monitoring
- □ Disk Monitoring

Service for Application Monitoring that provides key performance indicators to monitor the Application.

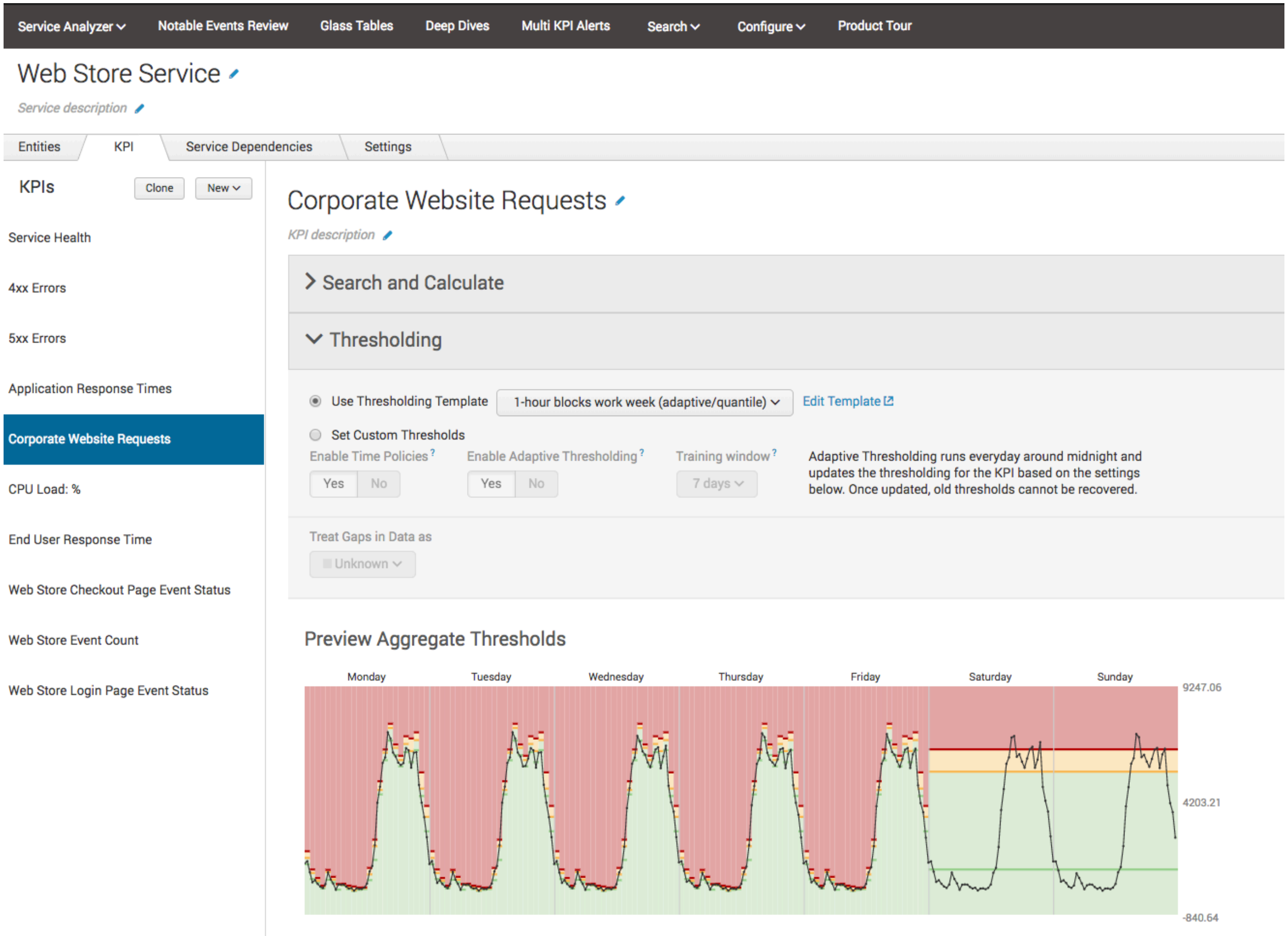
7/9 KPIs selected

- □ Application Apdex Score
- ☑ Application Availability
- ☑ Application Error Rate
- ☑ Application Health
- ☑ Application Requests Per Minute
- ☑ Application Response Time
- □ End User Apdex Score
- ☑ End User Requests Per Minute
- ☑ End User Response Time

Out of the Box KPIs

Splunk ITSI with New Relic … Better Together!

Once the KPIs are added to your service, you can use static thresholds or apply ITSI's machine learning via Adaptive Thresholding to enable alerting. In the screenshot below we created a Service with a KPI for Website Requests. Using ITSI's Adaptive Thresholding we are able to apply machine learning to "learn" what the thresholds should be using standard deviation across weekdays and weekends all with the click of a button.



Web Store Service

Service description

KPIs

Service Health

4xx Errors

5xx Errors

Application Response Times

Corporate Website Requests

CPU Load: %

End User Response Time

Web Store Checkout Page Event Status

Web Store Event Count

Web Store Login Page Event Status

Corporate Website Requests

KPI description

> Search and Calculate

Thresholding

● Use Thresholding Template: 1-hour blocks work week (adaptive/quantile) — Edit Template

○ Set Custom Thresholds

Enable Time Policies: Yes | No

Enable Adaptive Thresholding: Yes | No

Training window: 7 days

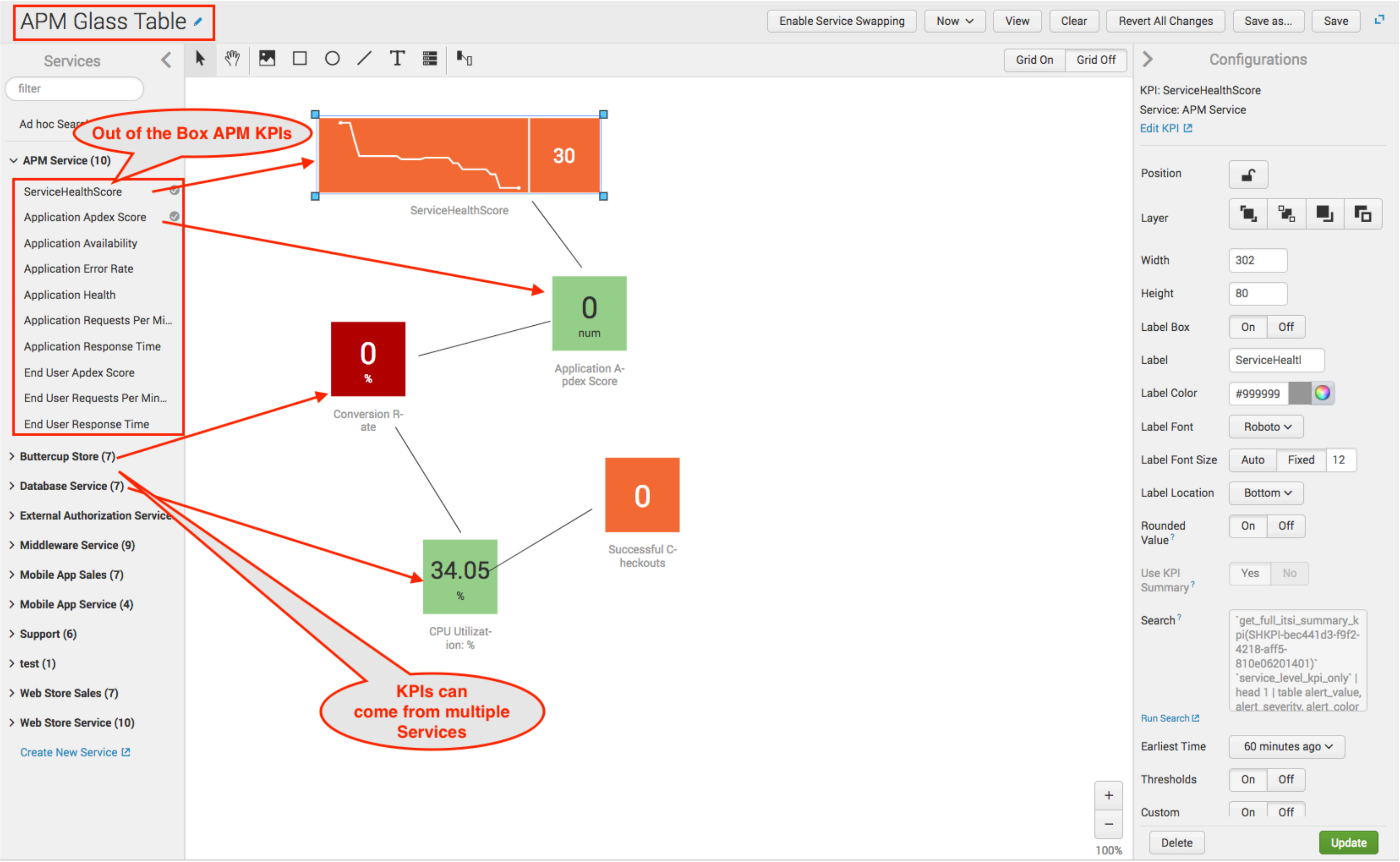
Adaptive Thresholding runs everyday around midnight and updates the thresholding for the KPI based on the settings below. Once updated, old thresholds cannot be recovered.

Treat Gaps in Data as: Unknown

Preview Aggregate Thresholds

Splunk ITSI with New Relic … Better Together!

With your KPIs added and thresholds set, you can create Glass Tables with any KPIs from any of your Services by simply dragging and dropping them onto a blank canvas:



KPI: ServiceHealthScore
Service: APM Service

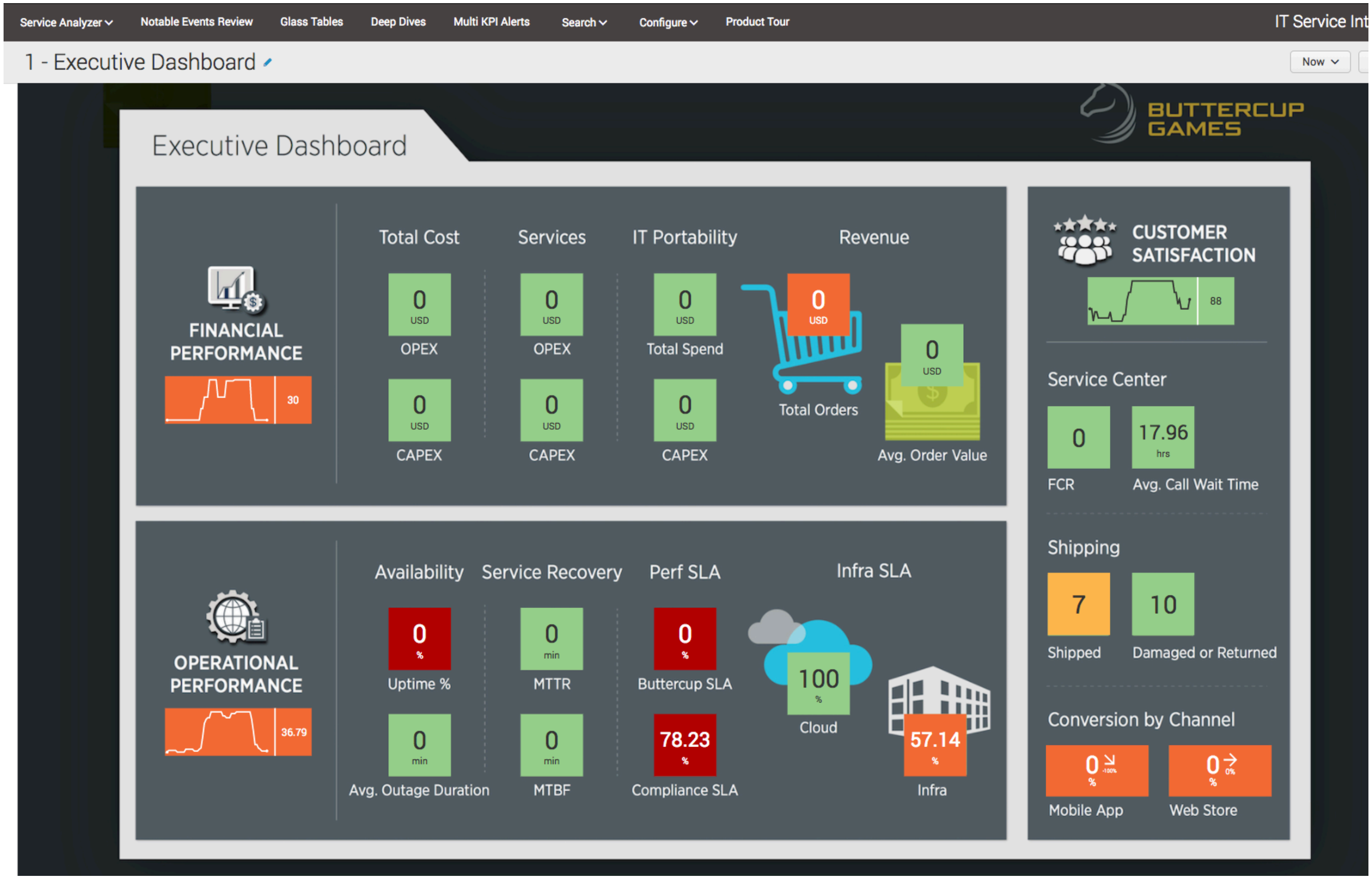
Position
Layer
Width: 302
Height: 80
Label Box: On Off
Label: ServiceHealtl
Label Color: #999999
Label Font: Roboto
Label Font Size: Auto Fixed 12
Label Location: Bottom
Rounded Value?: On Off
Use KPI Summary?: Yes No
Search?:

```
`get_full_itsi_summary_kpi(SHKPI-bec441d3-f9f2-4218-aff5-810e06201401)` `service_level_kpi_only` | head 1 | table alert_value, alert_severity, alert_color
```

Earliest Time: 60 minutes ago
Thresholds: On Off
Custom: On Off

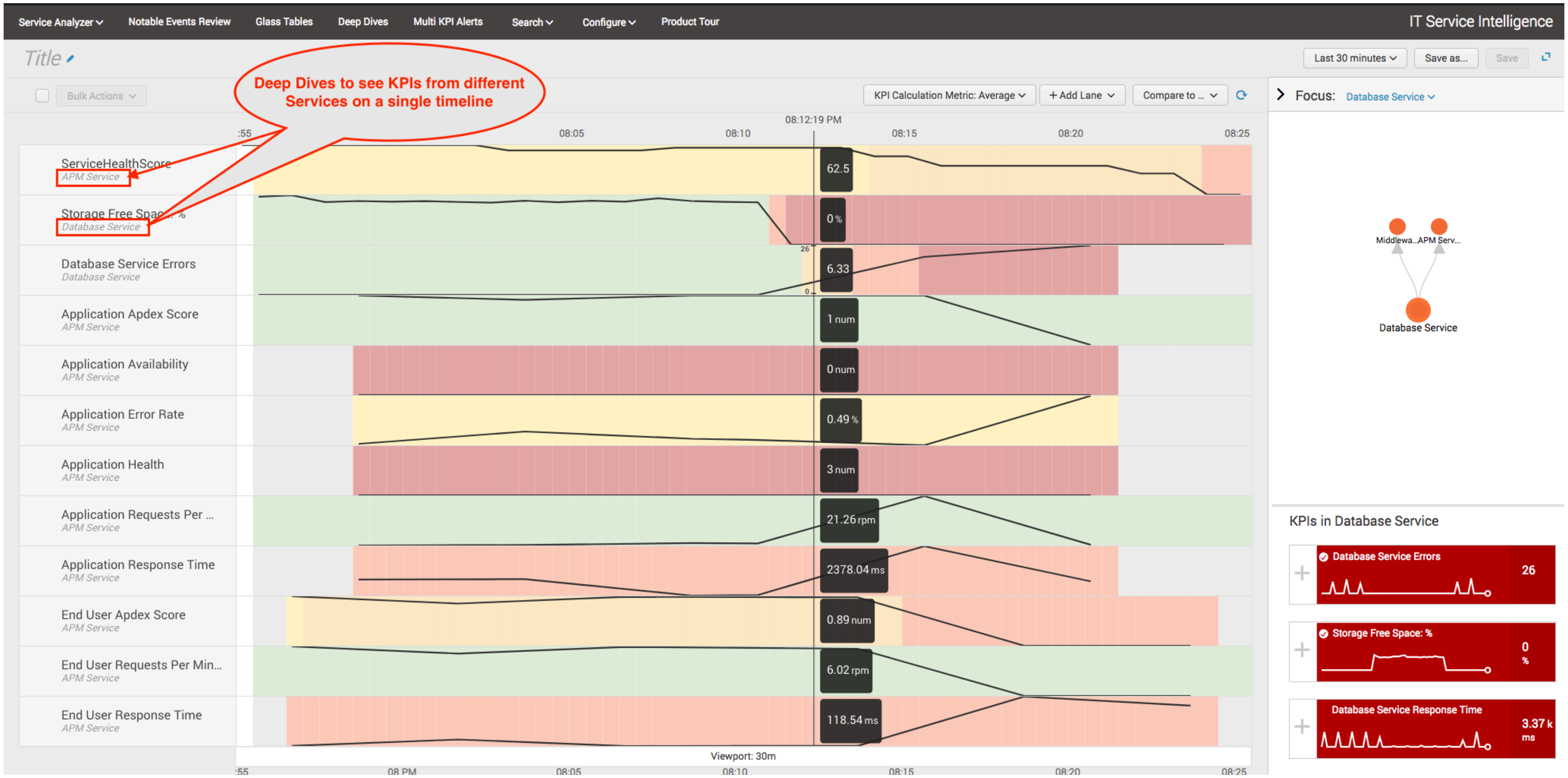
Splunk ITSI with New Relic … Better Together!

Glass Tables are extremely flexible and can contain just about anything you want. From background images to the merging of operational and business metrics on a single dashboard. Here's an example of a bit more polished Glass Table:



Splunk ITSI with New Relic … Better Together!

Glass Tables can include links from the various KPIs to other Glass Tables, other Splunk Dashboards, external websites or ITSI Deep Dives. Here's an example of an ITSI Deep Dive showing KPIs from multiple Services. As you can see it's easy to visually correlate to see the how various KPIs react in relation to each other. It his specific case, the Storage Server ran out of free disk space which ultimately lead to database errors and application performance issues.



Deep Dives to see KPIs from different Services on a single timeline

ServiceHealthScore — APM Service — 62.5

Storage Free Space: % — Database Service — 0 %

Database Service Errors — Database Service — 6.33

Application Apdex Score — APM Service — 1 num

Application Availability — APM Service — 0 num

Application Error Rate — APM Service — 0.49 %

Application Health — APM Service — 3 num

Application Requests Per ... — APM Service — 21.26 rpm

Application Response Time — APM Service — 2378.04 ms

End User Apdex Score — APM Service — 0.89 num

End User Requests Per Min... — APM Service — 6.02 rpm

End User Response Time — APM Service — 118.54 ms

KPIs in Database Service

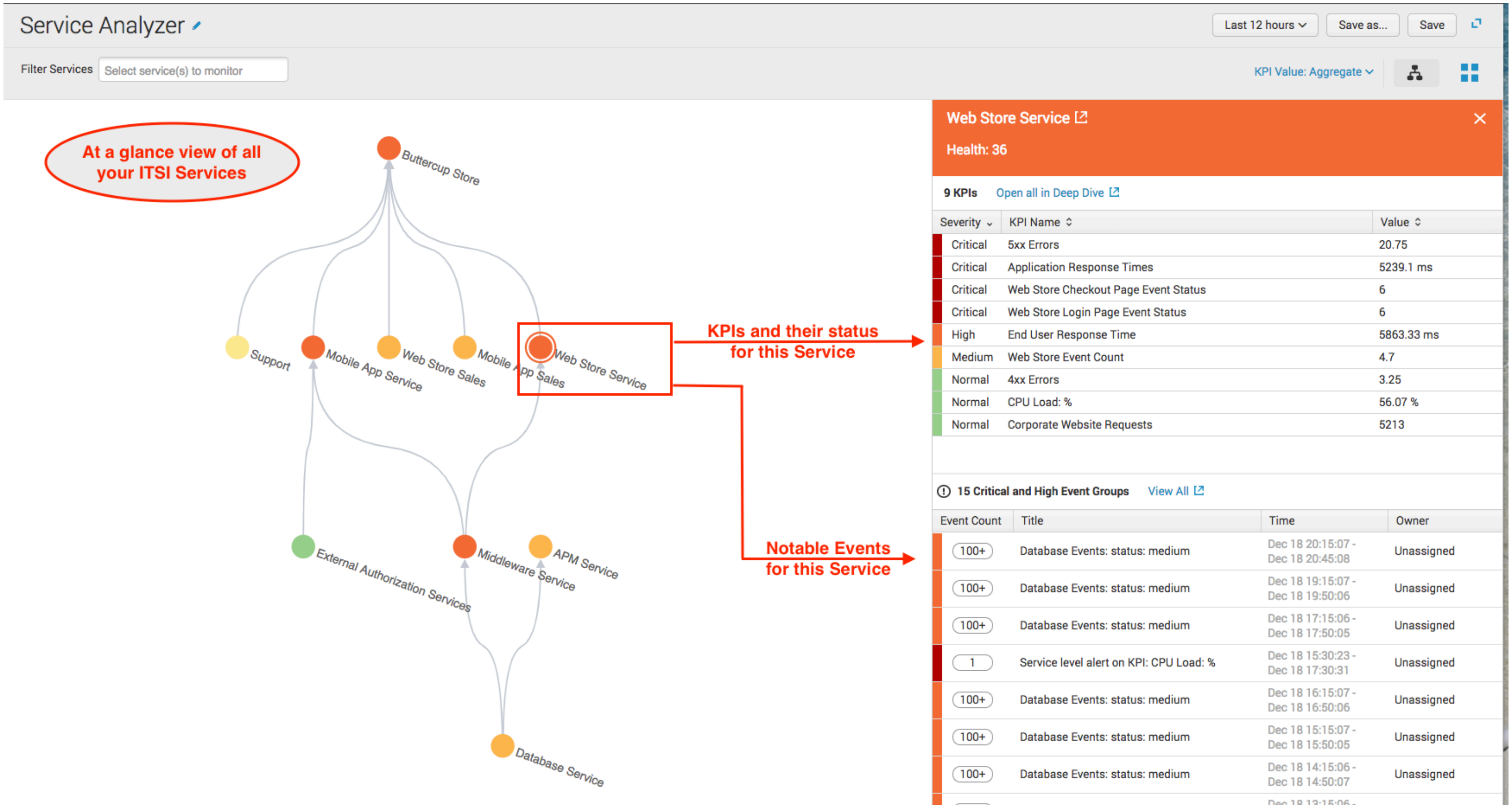
Database Service Errors — 26

Storage Free Space: % — 0 %

Database Service Response Time — 3.37 k ms

Splunk ITSI with New Relic … Better Together!

The Service Analyzer page in ITSI provides an overall picture of all your services and the state of their KPIs. From here you can easily drill down into Deep Dives to quickly troubleshoot.



At a glance view of all your ITSI Services

KPIs and their status for this Service

Notable Events for this Service

Web Store Service

Health: 36

9 KPIs Open all in Deep Dive

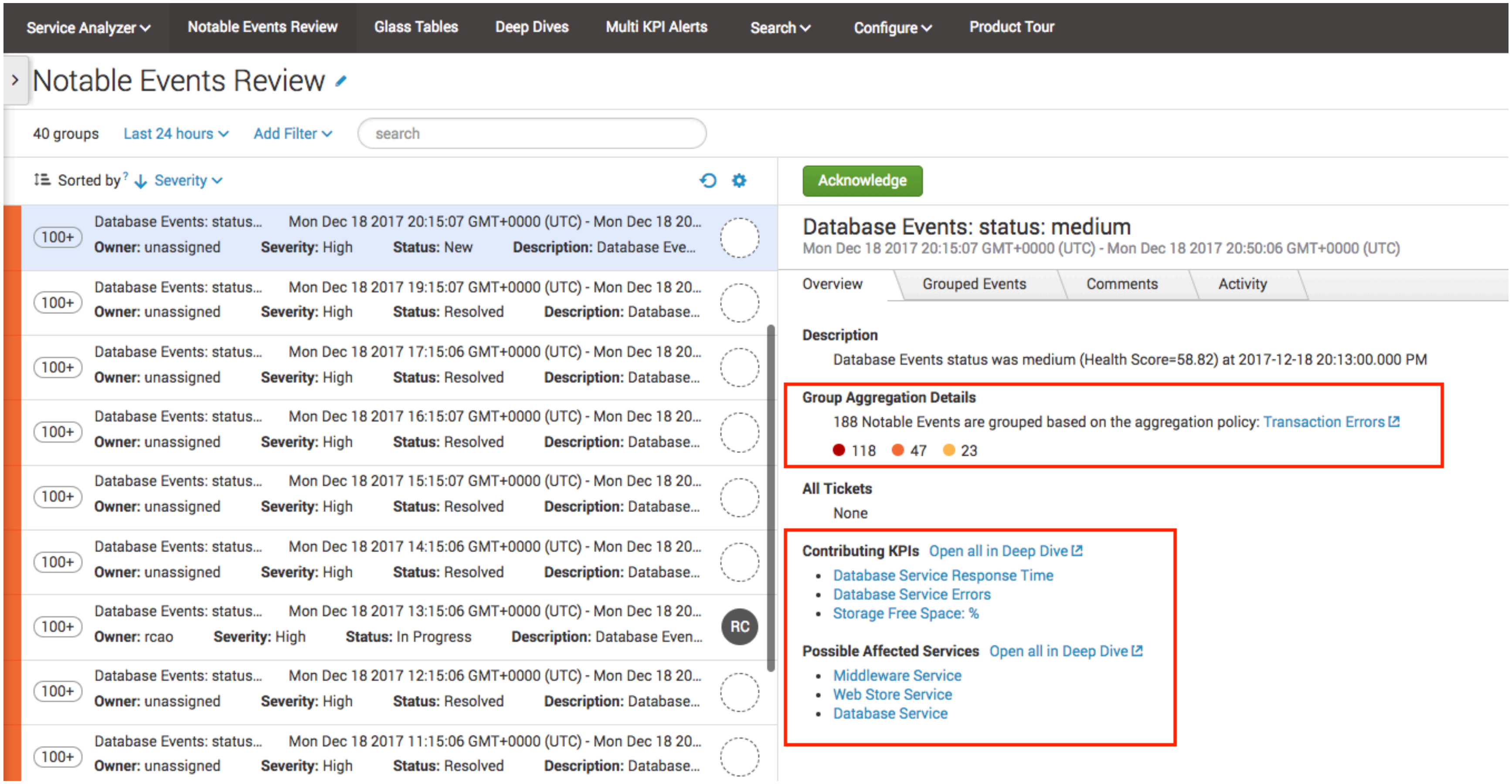
Severity	KPI Name	Value
Critical	5xx Errors	20.75
Critical	Application Response Times	5239.1 ms
Critical	Web Store Checkout Page Event Status	6
Critical	Web Store Login Page Event Status	6
High	End User Response Time	5863.33 ms
Medium	Web Store Event Count	4.7
Normal	4xx Errors	3.25
Normal	CPU Load: %	56.07 %
Normal	Corporate Website Requests	5213

15 Critical and High Event Groups View All

Event Count	Title	Time	Owner
100+	Database Events: status: medium	Dec 18 20:15:07 - Dec 18 20:45:08	Unassigned
100+	Database Events: status: medium	Dec 18 19:15:07 - Dec 18 19:50:06	Unassigned
100+	Database Events: status: medium	Dec 18 17:15:06 - Dec 18 17:50:05	Unassigned
1	Service level alert on KPI: CPU Load: %	Dec 18 15:30:23 - Dec 18 17:30:31	Unassigned
100+	Database Events: status: medium	Dec 18 16:15:07 - Dec 18 16:50:06	Unassigned
100+	Database Events: status: medium	Dec 18 15:15:07 - Dec 18 15:50:05	Unassigned
100+	Database Events: status: medium	Dec 18 14:15:06 - Dec 18 14:50:07	Unassigned
		Dec 18 13:15:06 -	

Splunk ITSI with New Relic … Better Together!

Notable Events provide a way for you to filter the noise and use machine learning to correlate and group similar incidents/alerts. You can use this to quickly identify which KPIs are involved and which Services could be potentially affected downstream or upstream.



Notable Events Review

100+	Database Events: status…	Mon Dec 18 2017 20:15:07 GMT+0000 (UTC) - Mon Dec 18 20…			
	Owner: unassigned	**Severity:** High	**Status:** New	**Description:** Database Eve…	○
100+	Database Events: status…	Mon Dec 18 2017 19:15:07 GMT+0000 (UTC) - Mon Dec 18 20…			
	Owner: unassigned	**Severity:** High	**Status:** Resolved	**Description:** Database…	○
100+	Database Events: status…	Mon Dec 18 2017 17:15:06 GMT+0000 (UTC) - Mon Dec 18 20…			
	Owner: unassigned	**Severity:** High	**Status:** Resolved	**Description:** Database…	○
100+	Database Events: status…	Mon Dec 18 2017 16:15:07 GMT+0000 (UTC) - Mon Dec 18 20…			
	Owner: unassigned	**Severity:** High	**Status:** Resolved	**Description:** Database…	○
100+	Database Events: status…	Mon Dec 18 2017 15:15:07 GMT+0000 (UTC) - Mon Dec 18 20…			
	Owner: unassigned	**Severity:** High	**Status:** Resolved	**Description:** Database…	○
100+	Database Events: status…	Mon Dec 18 2017 14:15:06 GMT+0000 (UTC) - Mon Dec 18 20…			
	Owner: unassigned	**Severity:** High	**Status:** Resolved	**Description:** Database…	○
100+	Database Events: status…	Mon Dec 18 2017 13:15:06 GMT+0000 (UTC) - Mon Dec 18 20…			
	Owner: rcao	**Severity:** High	**Status:** In Progress	**Description:** Database Even…	RC
100+	Database Events: status…	Mon Dec 18 2017 12:15:06 GMT+0000 (UTC) - Mon Dec 18 20…			
	Owner: unassigned	**Severity:** High	**Status:** Resolved	**Description:** Database…	○
100+	Database Events: status…	Mon Dec 18 2017 11:15:06 GMT+0000 (UTC) - Mon Dec 18 20…			
	Owner: unassigned	**Severity:** High	**Status:** Resolved	**Description:** Database…	○

Database Events: status: medium

Mon Dec 18 2017 20:15:07 GMT+0000 (UTC) - Mon Dec 18 2017 20:50:06 GMT+0000 (UTC)

Description

Database Events status was medium (Health Score=58.82) at 2017-12-18 20:13:00.000 PM

Group Aggregation Details

188 Notable Events are grouped based on the aggregation policy: Transaction Errors

● 118 ● 47 ● 23

All Tickets

None

Contributing KPIs Open all in Deep Dive

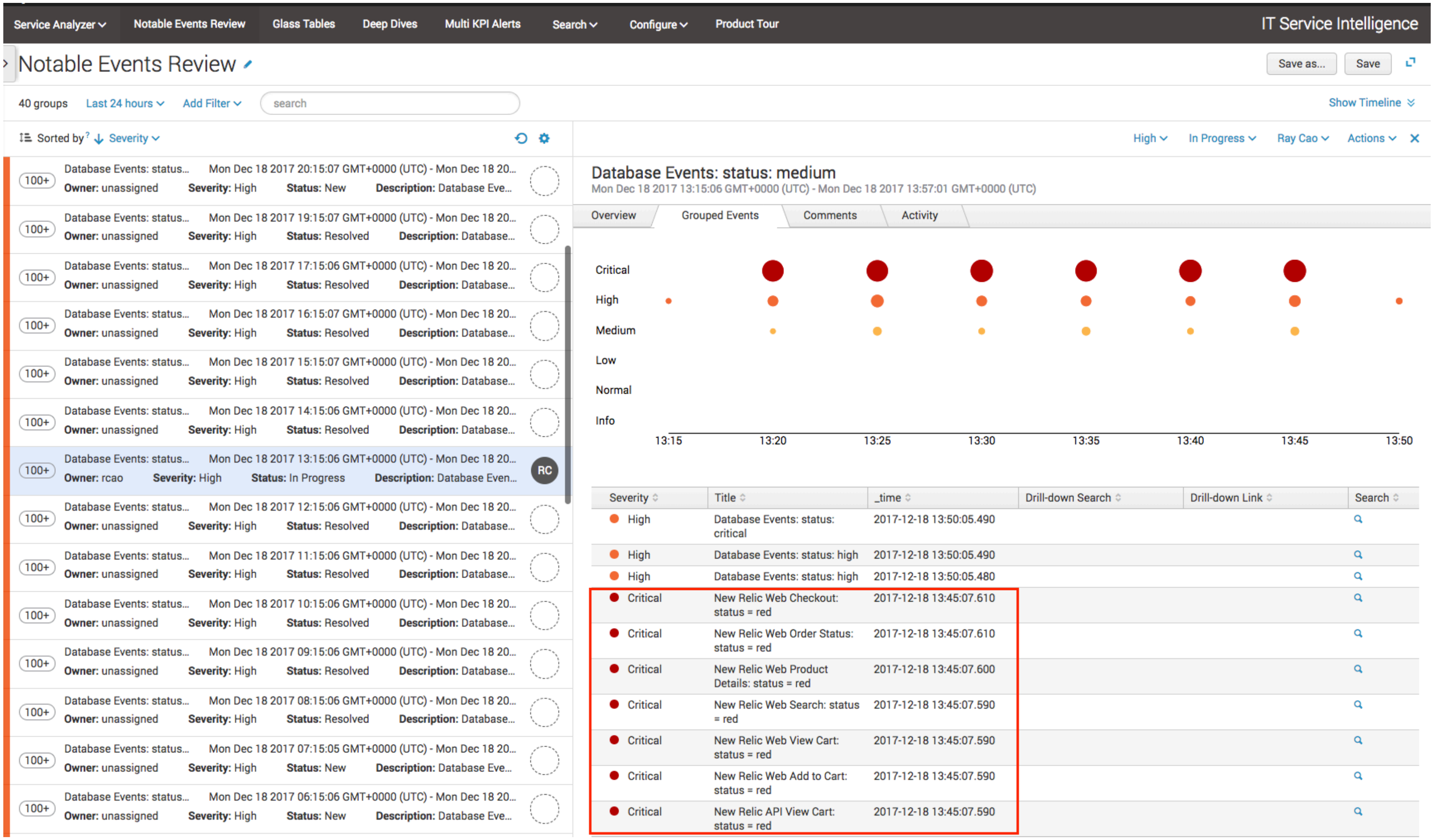
- Database Service Response Time
- Database Service Errors
- Storage Free Space: %

Possible Affected Services Open all in Deep Dive

- Middleware Service
- Web Store Service
- Database Service

Splunk ITSI with New Relic … Better Together!

Looking at the grouping tab, you can easily see patterns within the notable events that may help to quickly isolate trouble spots and lead to reduced MTTR.



Notable Events Review

40 groups

100+ Database Events: status... Mon Dec 18 2017 20:15:07 GMT+0000 (UTC) - Mon Dec 18 20...
Owner: unassigned **Severity:** High **Status:** New **Description:** Database Eve...

100+ Database Events: status... Mon Dec 18 2017 19:15:07 GMT+0000 (UTC) - Mon Dec 18 20...
Owner: unassigned **Severity:** High **Status:** Resolved **Description:** Database...

100+ Database Events: status... Mon Dec 18 2017 17:15:06 GMT+0000 (UTC) - Mon Dec 18 20...
Owner: unassigned **Severity:** High **Status:** Resolved **Description:** Database...

100+ Database Events: status... Mon Dec 18 2017 16:15:07 GMT+0000 (UTC) - Mon Dec 18 20...
Owner: unassigned **Severity:** High **Status:** Resolved **Description:** Database...

100+ Database Events: status... Mon Dec 18 2017 15:15:07 GMT+0000 (UTC) - Mon Dec 18 20...
Owner: unassigned **Severity:** High **Status:** Resolved **Description:** Database...

100+ Database Events: status... Mon Dec 18 2017 14:15:06 GMT+0000 (UTC) - Mon Dec 18 20...
Owner: unassigned **Severity:** High **Status:** Resolved **Description:** Database...

100+ Database Events: status... Mon Dec 18 2017 13:15:06 GMT+0000 (UTC) - Mon Dec 18 20...
Owner: rcao **Severity:** High **Status:** In Progress **Description:** Database Even... RC

100+ Database Events: status... Mon Dec 18 2017 12:15:06 GMT+0000 (UTC) - Mon Dec 18 20...
Owner: unassigned **Severity:** High **Status:** Resolved **Description:** Database...

100+ Database Events: status... Mon Dec 18 2017 11:15:06 GMT+0000 (UTC) - Mon Dec 18 20...
Owner: unassigned **Severity:** High **Status:** Resolved **Description:** Database...

100+ Database Events: status... Mon Dec 18 2017 10:15:06 GMT+0000 (UTC) - Mon Dec 18 20...
Owner: unassigned **Severity:** High **Status:** Resolved **Description:** Database...

100+ Database Events: status... Mon Dec 18 2017 09:15:06 GMT+0000 (UTC) - Mon Dec 18 20...
Owner: unassigned **Severity:** High **Status:** Resolved **Description:** Database...

100+ Database Events: status... Mon Dec 18 2017 08:15:06 GMT+0000 (UTC) - Mon Dec 18 20...
Owner: unassigned **Severity:** High **Status:** Resolved **Description:** Database...

100+ Database Events: status... Mon Dec 18 2017 07:15:05 GMT+0000 (UTC) - Mon Dec 18 20...
Owner: unassigned **Severity:** High **Status:** New **Description:** Database Eve...

100+ Database Events: status... Mon Dec 18 2017 06:15:06 GMT+0000 (UTC) - Mon Dec 18 20...
Owner: unassigned **Severity:** High **Status:** New **Description:** Database Eve...

Database Events: status: medium
Mon Dec 18 2017 13:15:06 GMT+0000 (UTC) - Mon Dec 18 2017 13:57:01 GMT+0000 (UTC)

Severity	Title	_time	Drill-down Search	Drill-down Link	Search
● High	Database Events: status: critical	2017-12-18 13:50:05.490			🔍
● High	Database Events: status: high	2017-12-18 13:50:05.490			🔍
● High	Database Events: status: high	2017-12-18 13:50:05.480			🔍
● Critical	New Relic Web Checkout: status = red	2017-12-18 13:45:07.610			🔍
● Critical	New Relic Web Order Status: status = red	2017-12-18 13:45:07.610			🔍
● Critical	New Relic Web Product Details: status = red	2017-12-18 13:45:07.600			🔍
● Critical	New Relic Web Search: status = red	2017-12-18 13:45:07.590			🔍
● Critical	New Relic Web View Cart: status = red	2017-12-18 13:45:07.590			🔍
● Critical	New Relic Web Add to Cart: status = red	2017-12-18 13:45:07.590			🔍
● Critical	New Relic API View Cart: status = red	2017-12-18 13:45:07.590			🔍