# ITSI for SLED

## Hands-On Workshop

splunk>
a CISCO company

# Forward-looking statements

This presentation may contain forward-looking statements that are subject to the safe harbors created under the Securities Act of 1933, as amended, and the Securities Exchange Act of 1934, as amended. All statements other than statements of historical facts are statements that could be deemed forward-looking statements. These statements are based on current expectations, estimates, forecasts, and projections about the industries in which we operate and the beliefs and assumptions of our management based on the information currently available to us. Words such as “expects,” “anticipates,” “targets,” “goals,” “projects,” “intends,” “plans,” “believes,” “momentum,” “seeks,” “estimates,” “continues,” “endeavors,” “strives,” “may,” variations of such words, and similar expressions are intended to identify such forward-looking statements. In addition, any statements that refer to (1) our goals, commitments, and programs; (2) our business plans, initiatives, and objectives; and (3) our assumptions and expectations, including our expectations regarding our financial performance, products, technology, strategy, customers, markets, acquisitions and investments are forward-looking statements. These forward-looking statements are not guarantees of future performance and involve significant risks, uncertainties and other factors that may cause our actual results, performance or achievements to be materially different from results, performance or achievements expressed or implied by the forward-looking statements contained in this presentation. Readers are cautioned that these forward-looking statements are only predictions and are subject to risks, uncertainties, and assumptions that are difficult to predict, including those identified in the “Risk Factors” section of Cisco’s most recent report on Form 10-Q filed on February 20, 2024 and its most recent report on Form 10-K filed on September 7, 2023, as well as the “Risk Factors” section of Splunk’s most recent report on Form 10-Q filed with the SEC on November 28, 2023. The forward-looking statements made in this presentation are made as of the time and date of this presentation. If reviewed after the initial presentation, even if made available by Cisco or Splunk, on Cisco or Splunk’s website or otherwise, it may not contain current or accurate information. Cisco and Splunk undertake no obligation to revise or update any forward-looking statements for any reason, except as required by law.

In addition, any information about new products, features, functionality or our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only and shall not be incorporated into any contract or other commitment or be relied upon in making a purchasing decision. We undertake no commitment, promise or obligation either to develop the features or functionalities described, in beta or in preview (used interchangeably), or to include any such feature or functionality in a future release. The development, release, and timing of any features or functionality described for our products remains at our sole discretion.



splunk>
a CISCO company

# Please introduce yourself!

- Name
- Company/organisation
- Role
- Are you currently using Splunk?
- What are you interested in using Splunk for?

# Workshop Agenda

- IT Service Intelligence Overview
- Service Creation
- KPIs Creation
- Deep Dives
- Glass Tables
- Next Steps

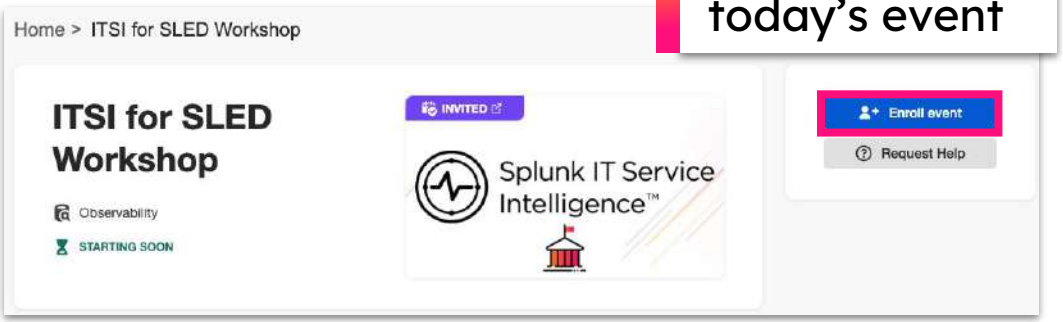
# Enroll in Today's Workshop

## Tasks

1. Get a splunk.com account if you don't have one yet: https://splk.it/SignUp
2. Enroll in the Splunk Show workshop event: https://show.splunk.com/event/<eventID>
3. Download a copy of today's slide deck: https://splk.it/ITSI-SLED-Attendee

## Goal

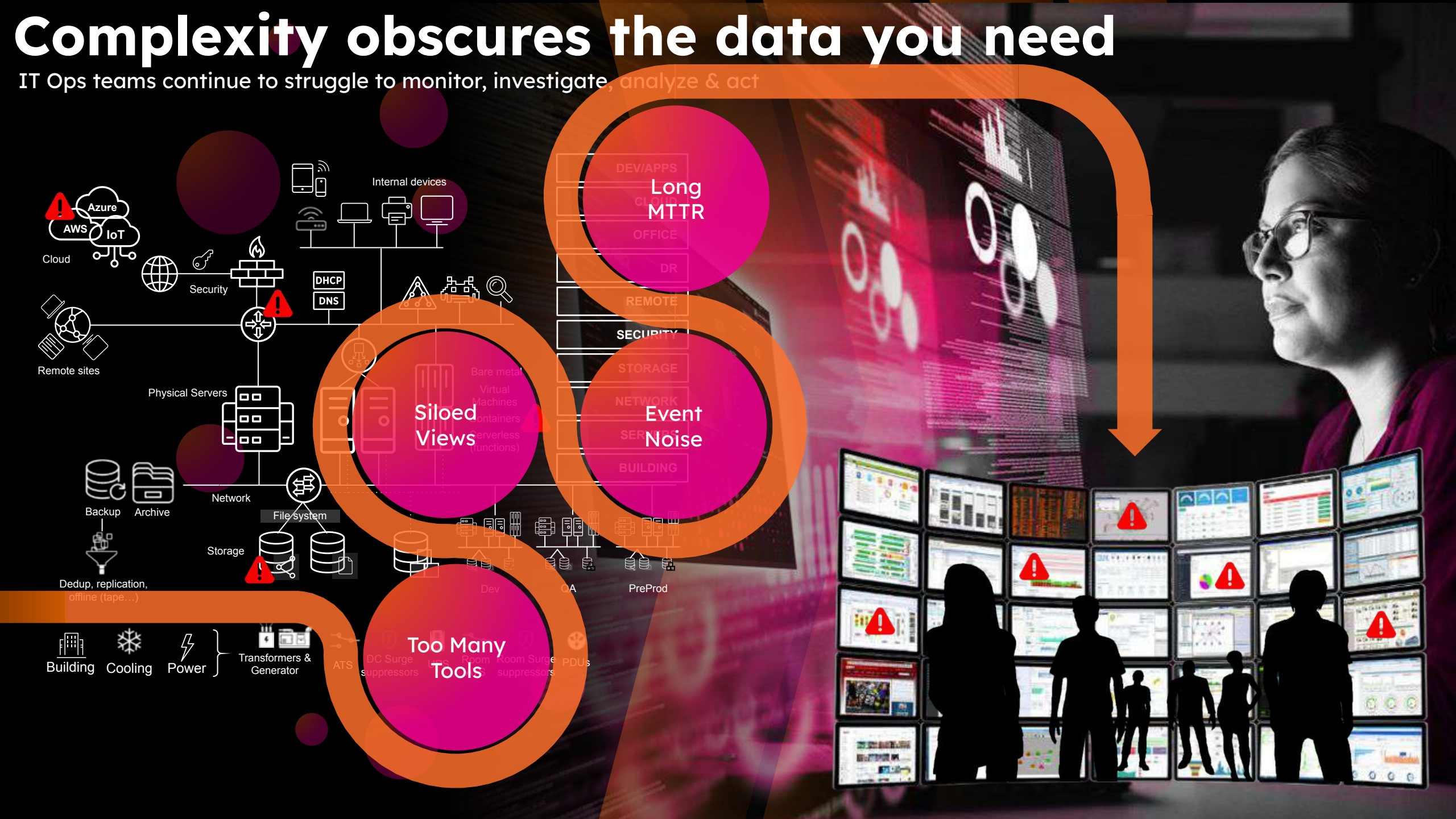
Enroll in today's event



# ITSI Overview

# Complexity obscures the data you need

IT Ops teams continue to struggle to monitor, investigate, analyze & act



# The impact can be significant

## Putting reputation, user experience, employee effectiveness & innovation at risk

### High Impact Costs

Outages and incidents impact the services and apps driving revenues

### Poor User Experiences

Users have trouble accessing critical services.

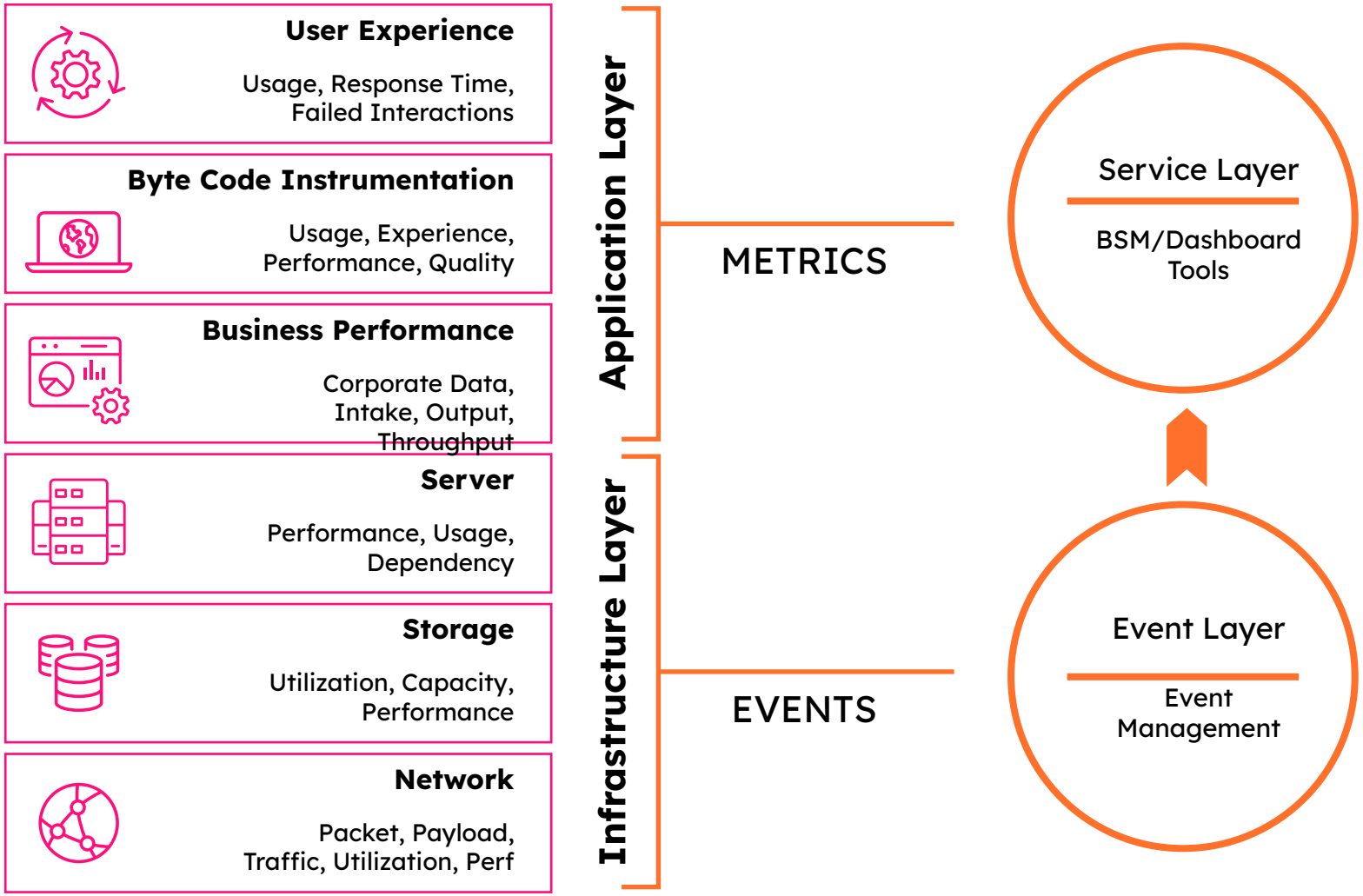
### Decreased Employee Effectiveness

Teams thrash, finger-point, and key employees leave

### Struggle to Innovate

IT spends too much time fixing problems instead of innovating and transforming

# The Old Ways Disappoint




**Challenges**

- Many disparate components
- Brittle integrations
- Data is summarized and lost
- Longer root-cause identification
- End-to-end view challenging
- Labor-intensive to manage
- Not agile for digital business

# Splunk IT Service Intelligence Platform Approach

**User Experience**

Usage, Response Time, Failed Interactions

**Byte Code Instrumentation**

Usage, Experience, Performance, Quality

**Business Performance**

Corporate Data, Intake, Output, Throughput

**Server**

Performance, Usage, Dependency

**Storage**

Utilization, Capacity, Performance

**Network**

Packet, Payload, Traffic, Utilization, Perf

**Application Layer**

**Infrastructure Layer**

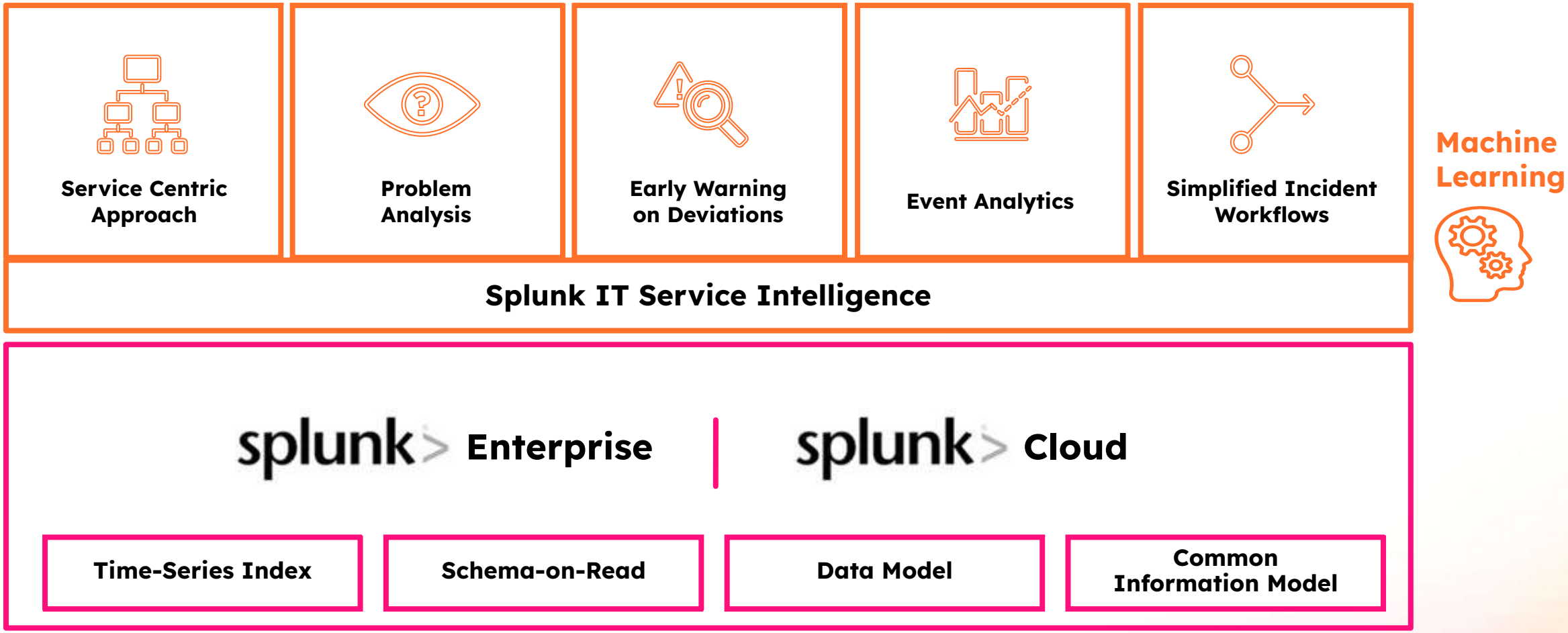
Machine Data


## Splunk Approach:

- Repository for **ALL** data
- Data in original raw format
- Machine learning
- Simplified architecture
- Fewer resources to manage
- Collaborative approach

# Splunk IT Service Intelligence

## Data-driven service monitoring and analytics



# Splunk's Patented Timeseries Index = Our Answer

## ANY DATA SOURCE

### Logs


{time:1554672630000, "sourcetype": "app", "event": "2390549035"}
{time:1554672690580, "sourcetype": "payment", "event": "http auth ftw!"}
{time:1554672690582, "sourcetype": "payment", "event": "declined"}
{time:1554672699180, "sourcetype": "payment", "event": "success"}
...


### Alerts


{
id: "AddBYZrEFEF",
metadata: { ETS_key1: "detector"
},
properties: {
is: "ok",
sf_notificationWasSent: true,
was: "anomalous"
},
sf_eventCategory:
"USER_DEFINED",
sf_eventType: "string",
timestamp: 1554672630000
}


### Events


time:1554672630000, "type": "authfailed", "event": "unauth"
time:1554672630200, "type": "suspend", "account": "129482323"
time:1554672639500, "type": "authfailed", "typeNum": "401"
time:1554672669800, "purpose": "authfailed", "msg": "badPass"


## POWERFUL QUERY AND AGGREGATION

### Ingest

**Code-level Changes**
Custom configuration to send data in the product's format.

**Celebrated ETL**
"We have the most integrations to get data into our product"

### Columnar Data Storage

### Productized Visualizations

**Predefined Schema Requirements**

**Predefined Analytics**

Product Features

### Ingest

Organize any data against the timestamp, or add a timestamp upon ingest

**Raw Format, No Normalization**
Preserve raw data, no translation required at ingest. Unlocks compliance and security use cases

No ETL "Magic" and Overhead. Need to design how the data will be used to ingest the data.

### Raw, Time Series Indexed Storage

### Query

All queries include a time component, data indexed on time

Rapidly return results across all data sources with no configuration

Aggregate events on any metadata **programmatic** declaration

SPL

Flexible Visualization

Alert on Any Data

Predictive Analytics

# Correlation of any Data Source is Key

Logs were just the first to illustrate the problem…

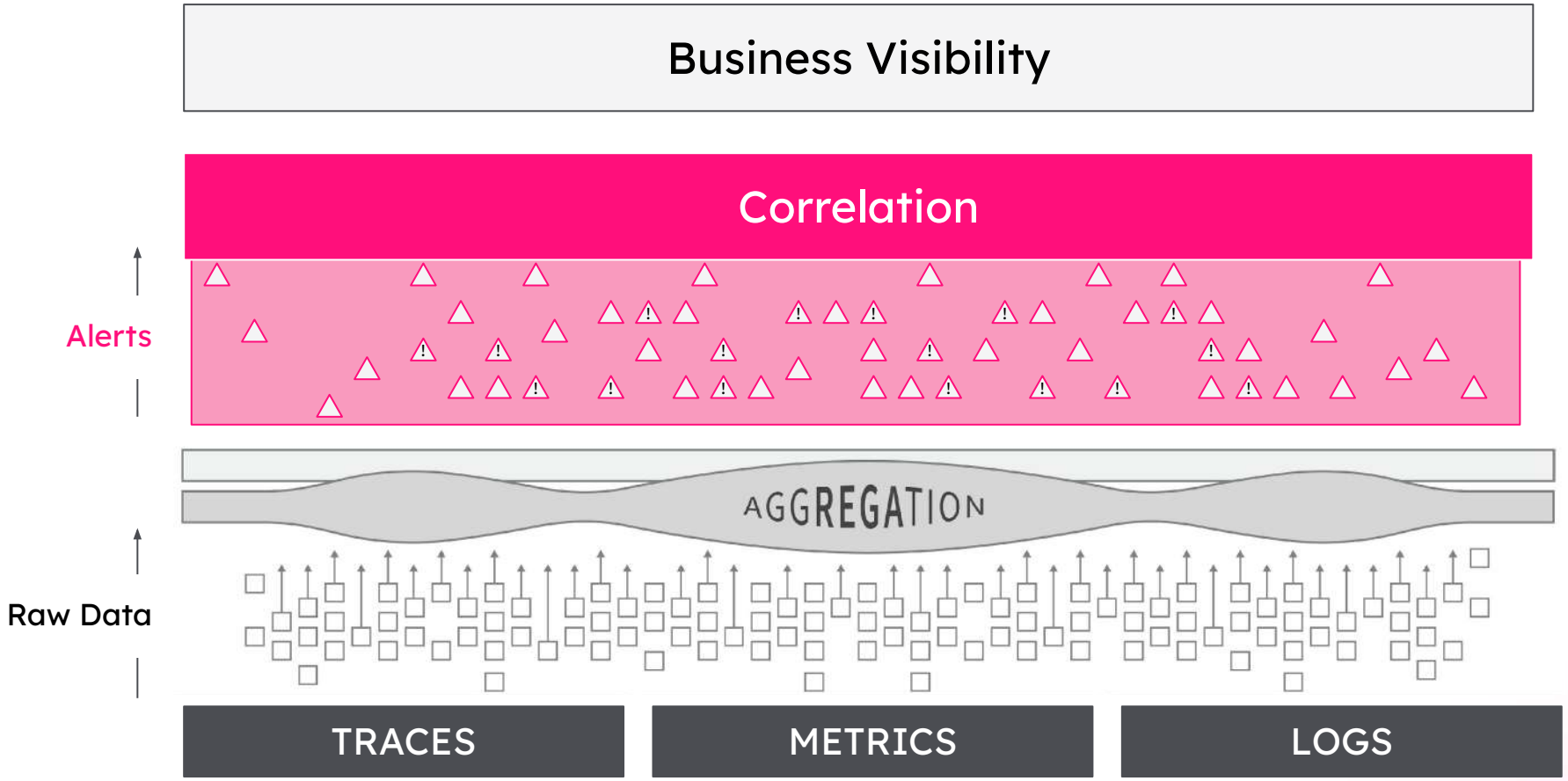
## Database Solutions

- **X** Data Sources + **Y** Questions = **Z** Schema
- **Z** Schema = **Structure / Normalized** data during "ETL"
- Correlation and Query limited to **Y** Questions (w/out code level changes)

## Splunk's Timeseries Index

- No Schema = **Any Data Source** and **Any Question**
- No Schema = **Full Fidelity Metrics, Logs and Events**
- Build Schema upon Query = **Limitless Correlation and Query**

# Data Doesn't Need to Live Together at Aggregation…




Business KPI Dashboards

Data Correlation Platform

Monitoring Tools

# Foundations

## Foundational concepts and Terminology

### Services

- Think of a Service as a box
- A logical grouping of things we monitor and the measurements we place against them

### Services can depend upon other services

- This creates Service Dependencies
- This provides the ability to:
- Set importance levels (weighting)
- Design an impact model
- Reuses these services as building blocks

# Foundations

## Foundational concepts and Terminology

## Entities

- A resources to be monitored:
- Servers
- Databases
- Switches
- Routers
- Physical and / or Virtual

## KPIs (Key Performance Indicators)

Infrastructure KPI Examples:

- CPU
- Memory
- Disk
- Errors

Business KPI Examples:

- Website Usability
- Resident access to services
- Student Engagement

# Workshop Back Story

# Workshop Back Story

The DMV has just deployed a new web service for drivers license renewal, however the engineers forgot to include database monitoring.

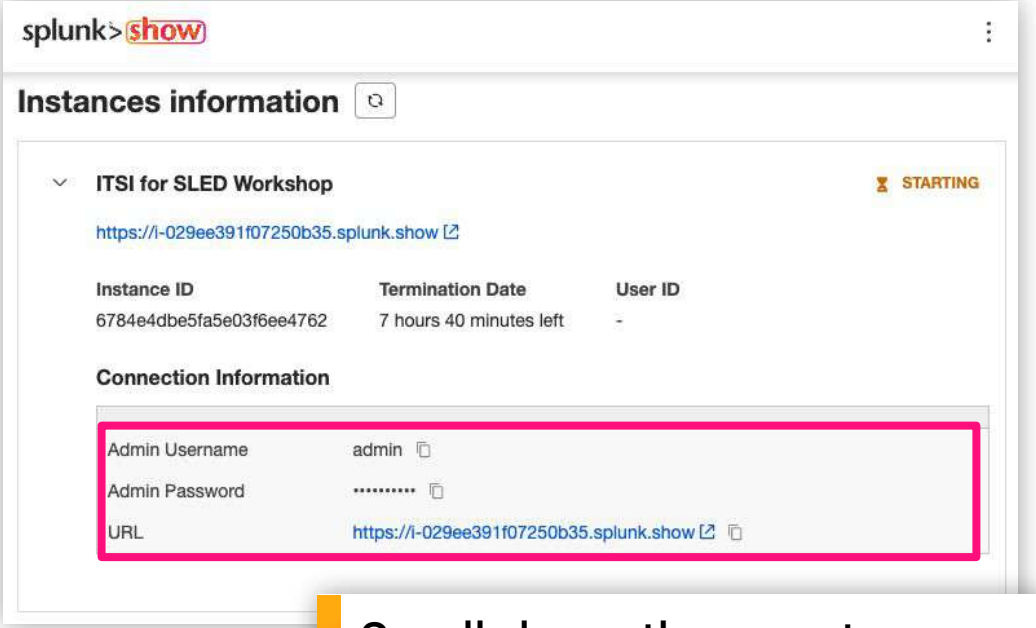
Splunk collectors are already deployed ingesting security and infrastructure data,  the business have requested that we build a **service centric** monitoring solution.

The CxO has just also requested that we include some ‘AI’ as they read on a website Artificial Intelligence can solve everything!

The lab starts on the back of a service decomposition workshop which has identified all the missing **database** components.

# Login to Splunk

Locate your instance URL and credentials in the Splunk Show event
https://show.splunk.com




Scroll down the event page and expand the **ITSI for SLED Workshop** section to view your login details

Log in to your Splunk instance


Login using the credentials from Splunk Show

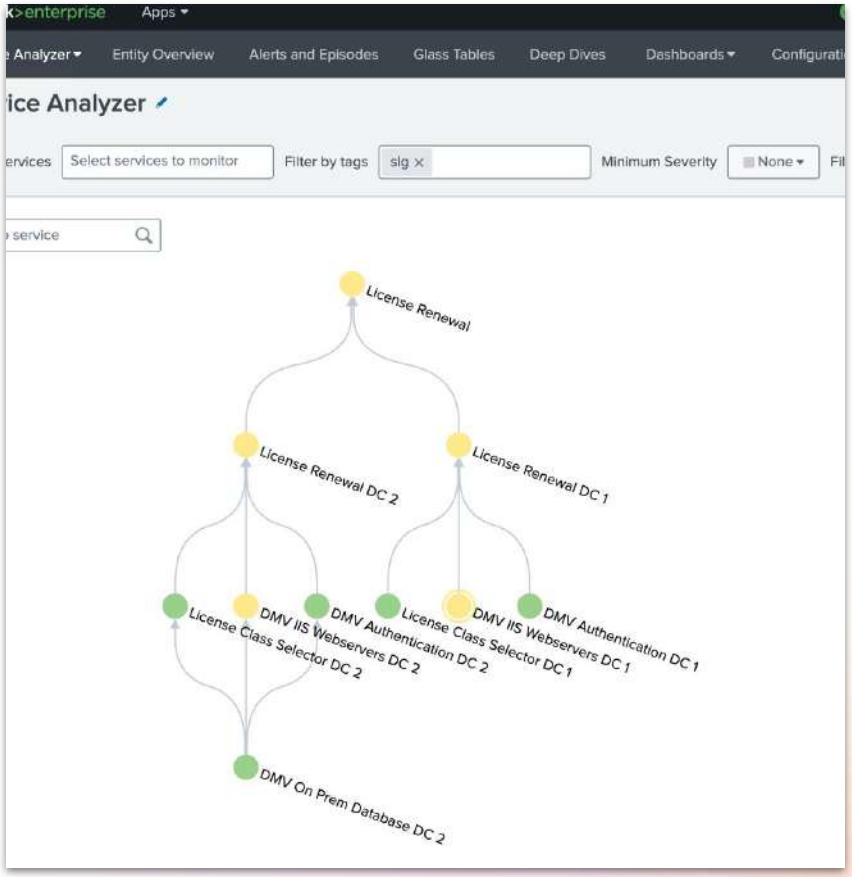
# Services Exercise

# Service Tree

The Service Analyzer tree view provides a visual representation of our services and the dependencies between them.  The health of a service is affected by the health of a child service.

The tree can be built manually, however typically this is imported from a csv, or created via a search.

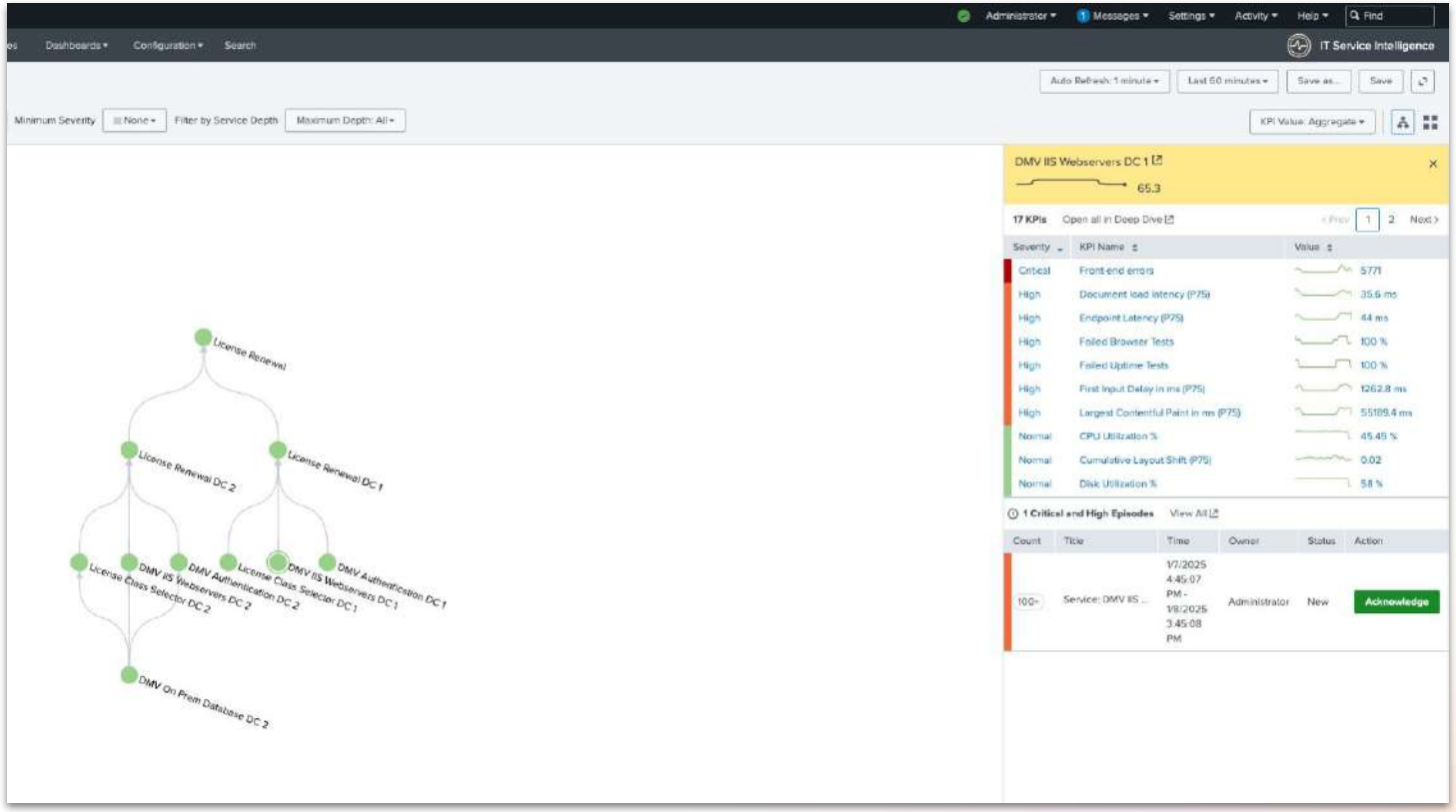
- Click on the different services service and review the KPIs.
- Adjust the time picker to investigate when there was a severity degradation. *(note: there should be issues around an hour before the start of workshop (xx:40 - xx:59)*.



# Service Tree

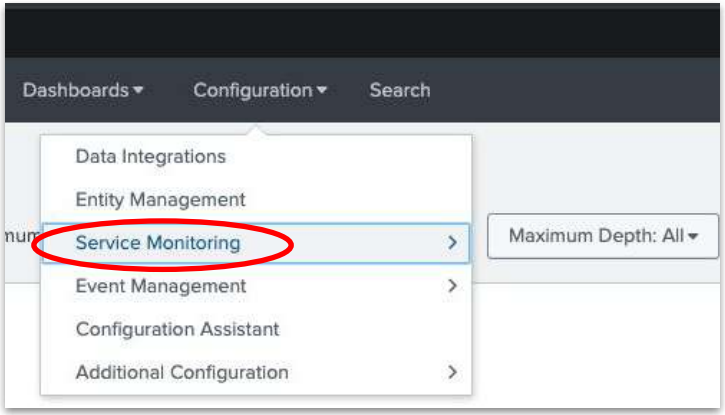
We can see that there is an issue with the Cart Services service.

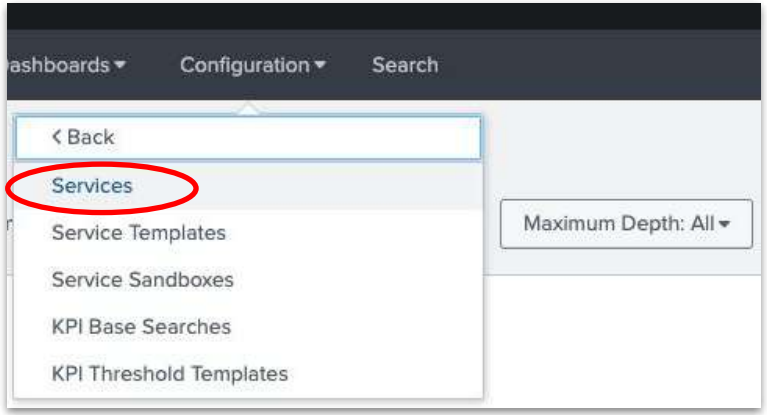
- Click on the impacted service (***DMV IIS Webservers DC 1***) to investigate which KPIs have degraded.
- Review the impacted entities.
- **Hint:** Click “Front-End Errors”



# Services Lab

- Select the Configure menu + Service Monitoring + Services



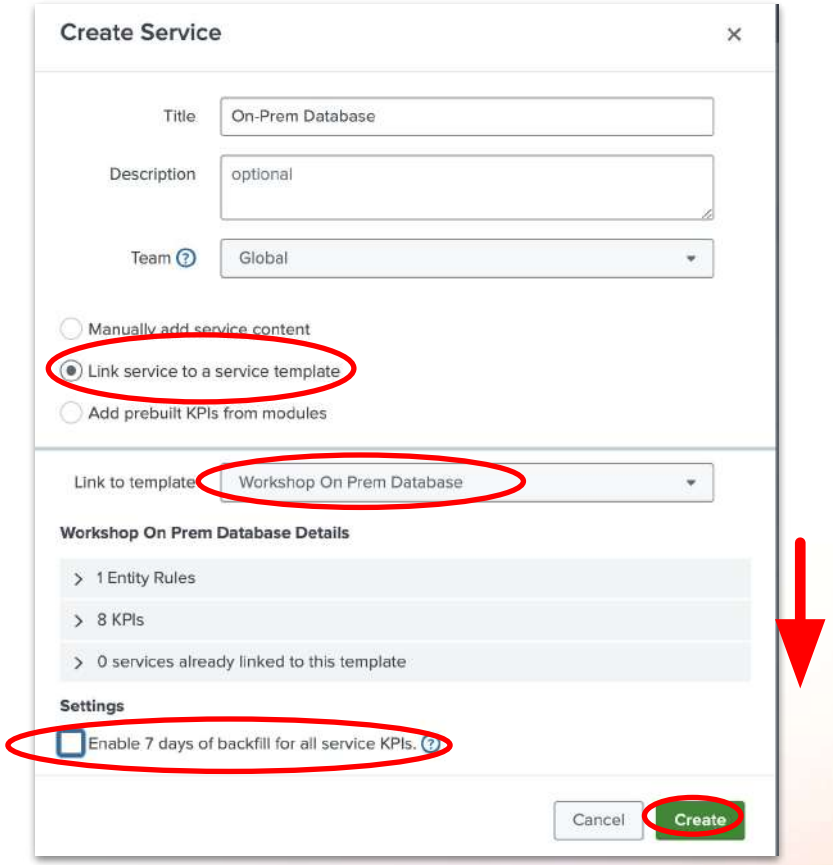




- Click Create Service > Create Service

# Services Lab

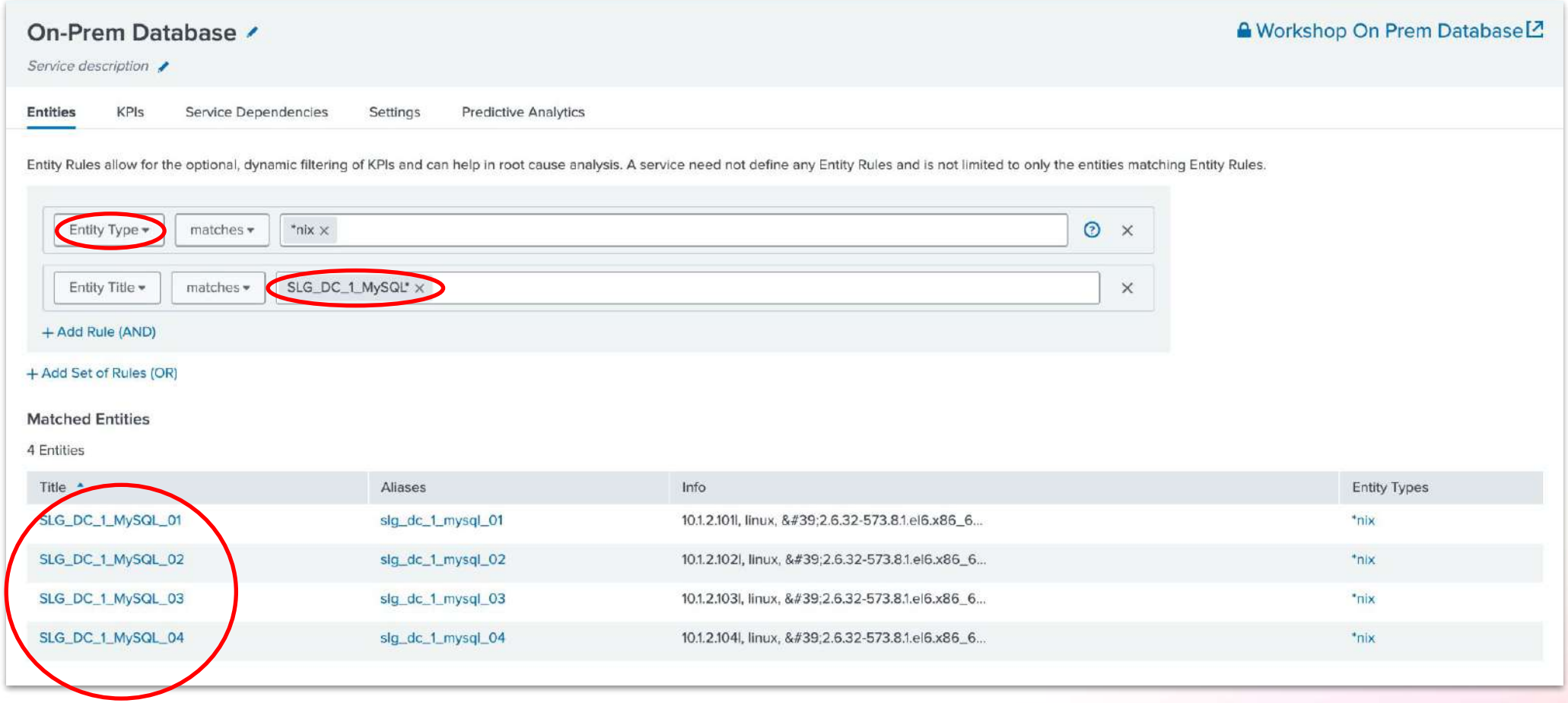
We are going to utilize the ITSI service templates feature, this will build the service with predefined KPIs.

- Name the service ‘On-Prem Database’
- Select ‘*Link service to a service template*’ button
- Choose ‘***Workshop On-Prem Database***’ template
- Click the ‘*Enable 7 days of backfill for all Service KPIs*’ option
  - *Please note sometimes the option is hidden below so you will need to scroll down!*
- Click ‘*Create*’ button



# Services Lab

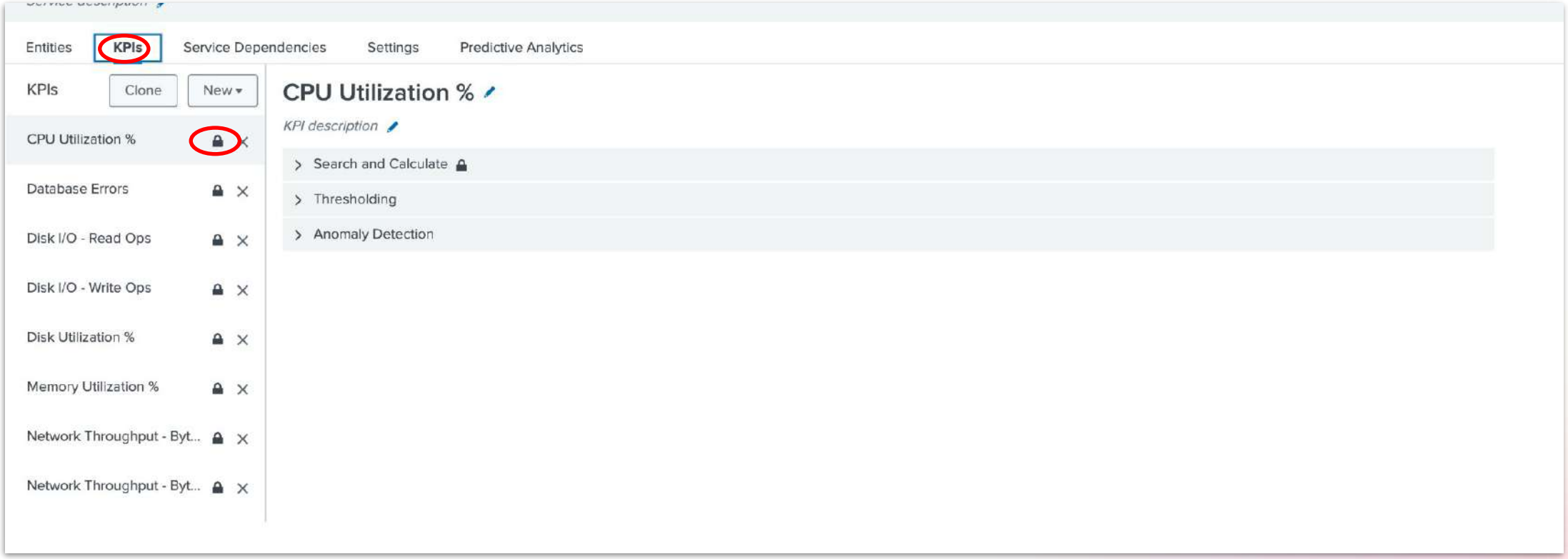
The new ‘On-Prem Database’ service is based on a template, if you review the ‘Entities’ tab we can see that the entities are already filtered.



# Services Lab

Under the KPIs tab we can see some KPIs that have been inherited from the service template, the padlocks indicate that any changes to the template we selected when creating this service will be pushed to this service and in fact all services that use this template.

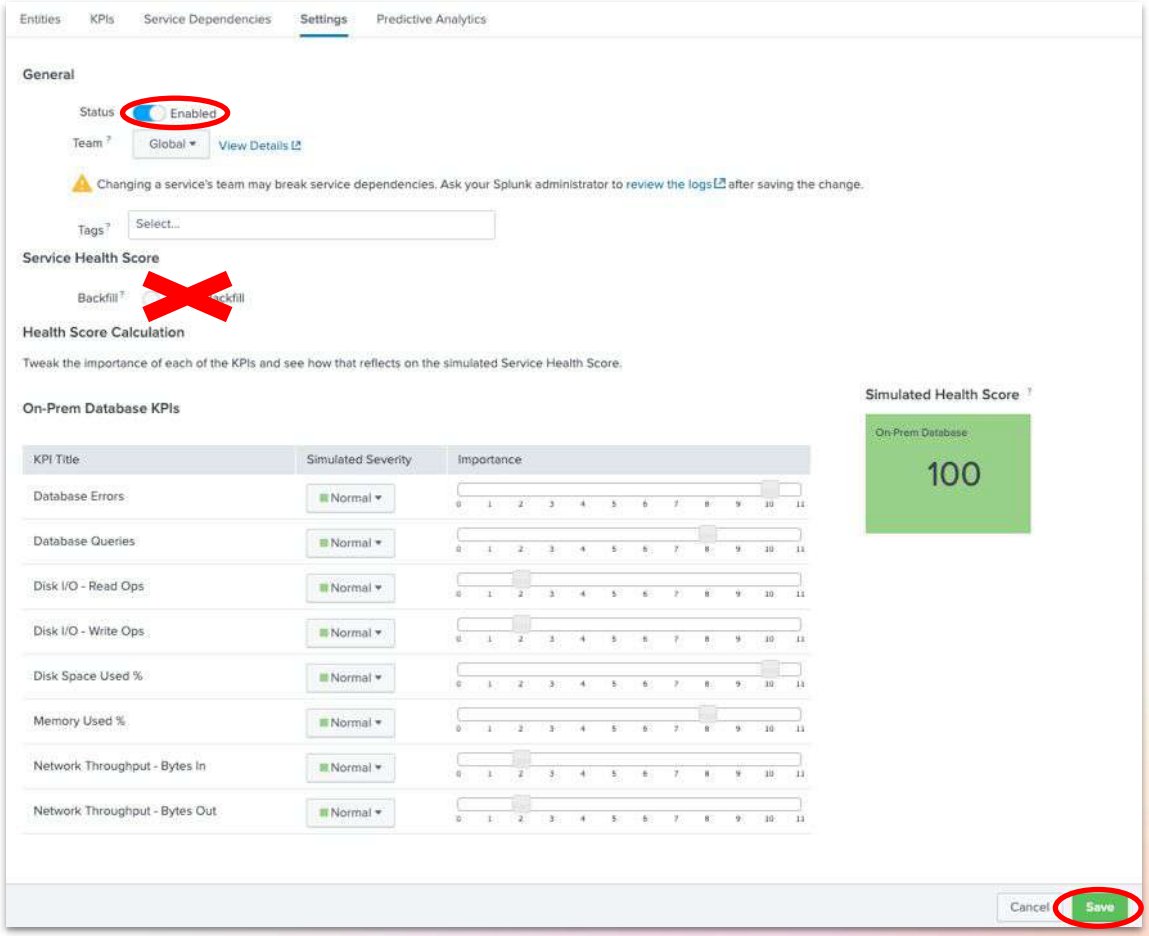
- Click 'Database Queries' KPIs to review.



# Services Lab

The ‘Settings’ tab enables configuration of the service attributes. The new (linked) database service is disabled by default.

- Switch to Setting tab
- Toggle status to ‘*Enable*’
- Investigate the effect changing the Importance and Simulated Severity has, on the Simulated Health Score
- *Please do NOT enable Service Health Score backfill at this point*
- Click the ‘Save’ button



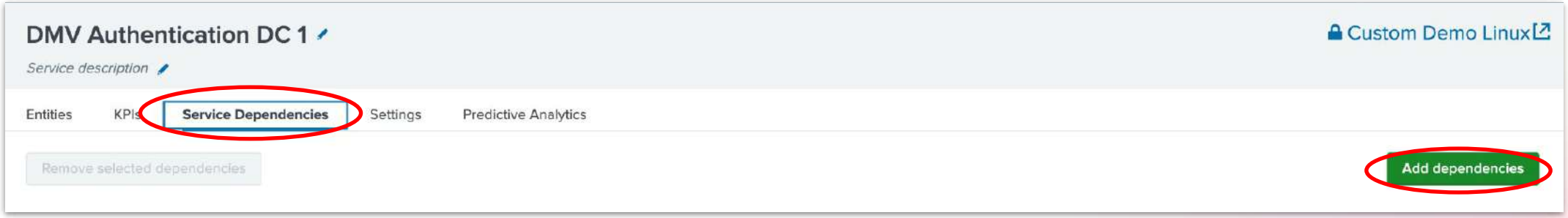
# Services Lab

The new Database service will be a dependency of the **Authorization** service, any service health changes will be propagated to the parent service(s).

- Select *Configure > Services*
- Edit the *'DMV Authentication DC 1' service*

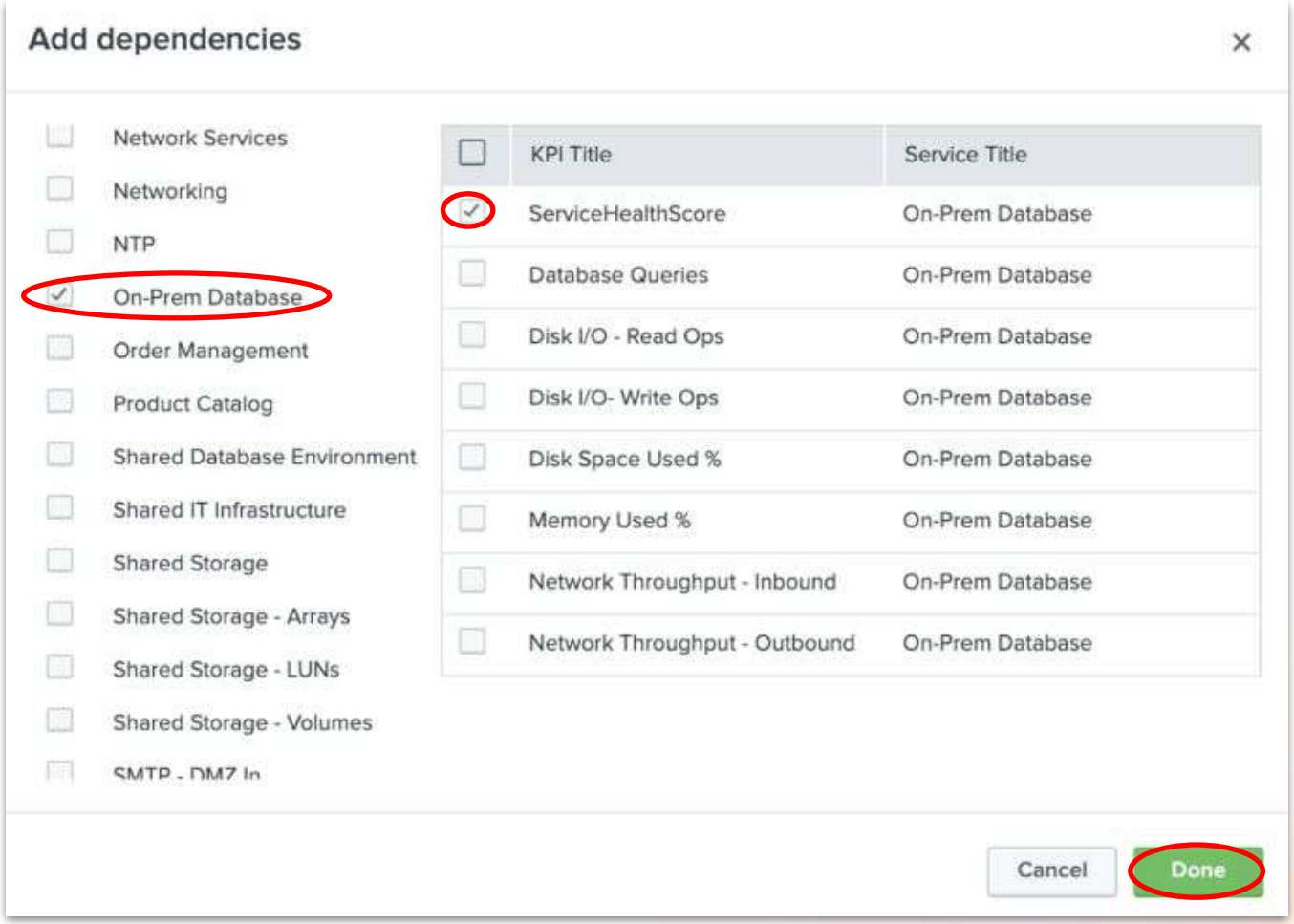
| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Course Picker DC 2 | Edit | Enabled | Synced with Custom Demo Appserver | 3 | 10 | View Health | Global |
| Course Registration | Edit | Enabled | Not linked | 0 | 0 | View Health | Global |
| Course Registration DC 1 | Edit | Enabled | Not linked | 0 | 0 | View Health | Global |
| Course Registration DC 2 | Edit | Enabled | Not linked | 0 | 0 | View Health | Global |
| DMV Authentication DC 1 | Edit | Enabled | Synced with Custom Demo Linux | 1 | 7 | View Health | Global |
| DMV Authentication DC 2 | Edit | Enabled | Synced with Custom Demo Linux | 1 | 7 | View Health | Global |

- *Click 'Service Dependencies' tab and then 'Add dependencies'*



# Services Lab

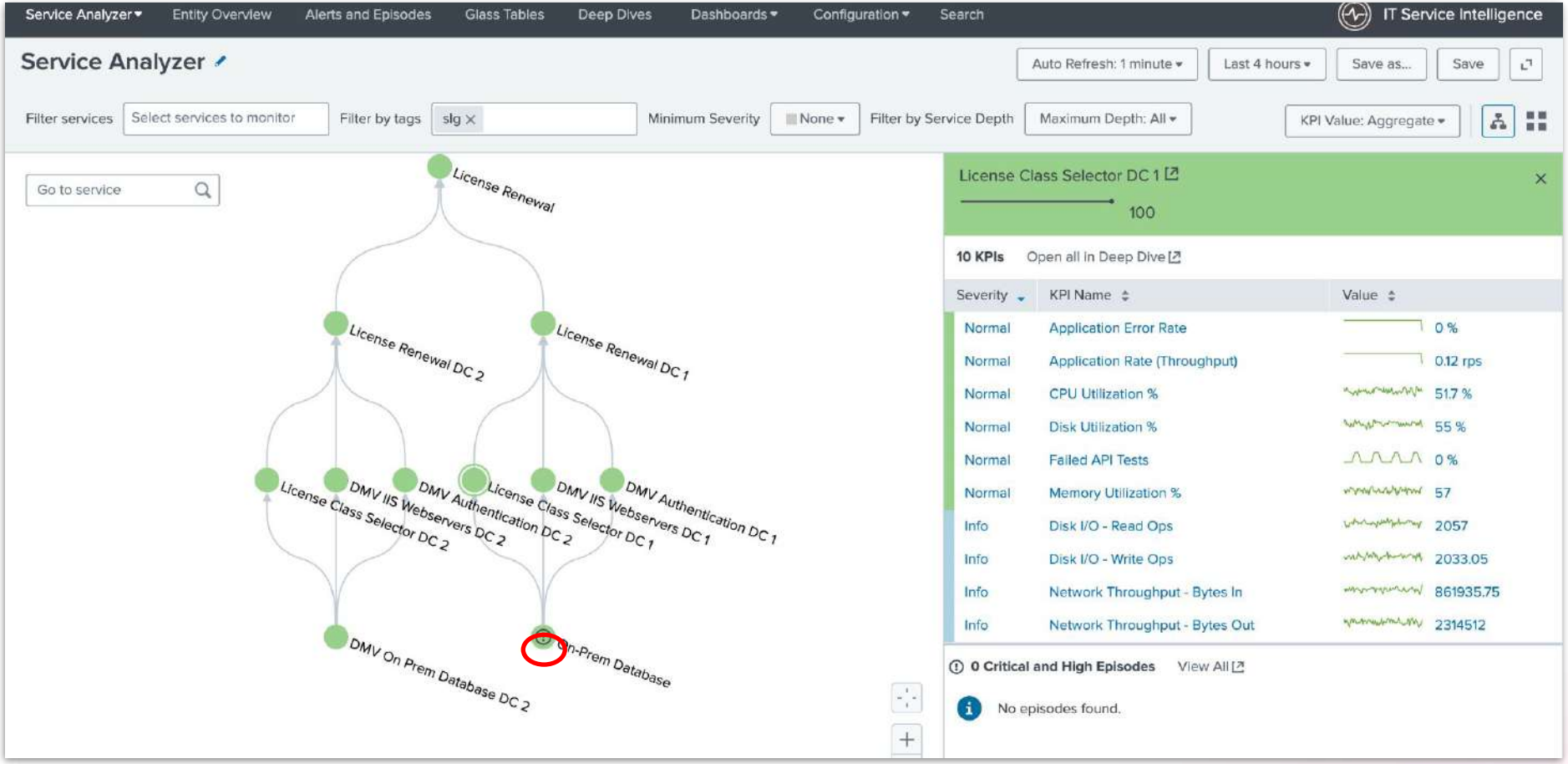
- Tick ‘On-Prem Database’ service
- Tick the ’ServiceHealthScore’
- Press ‘Done’ button
- Click ‘Save’ button



- Now Repeat the previous steps for the ***License Class Selector DC 1*** and ***DMV IIS Webservers DC 1*** services

# Check Service Tree

We can review in the Service Analyzer view that the License Renewal business service now has the new ‘On-Prem Database’ service.




Note: The service health score may be grey until KPIs searches have executed.

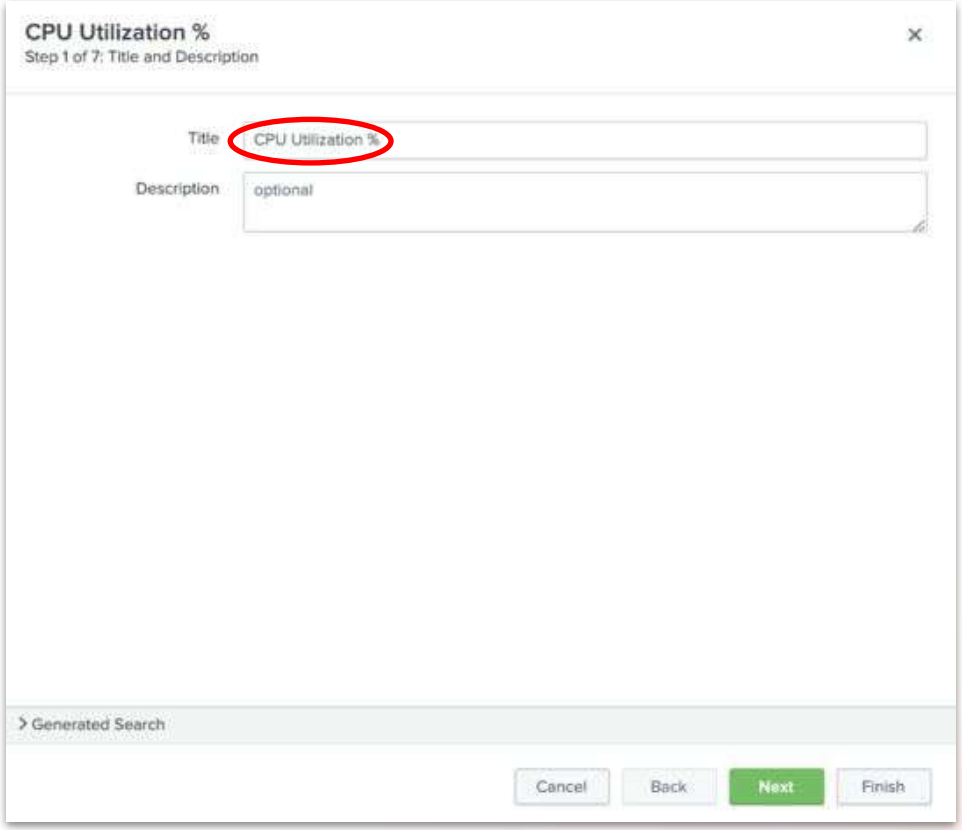
# KPI Exercise

# KPI Lab

The new ‘On-Prem Database’ service is based on a template however we need to add an extra KPI to monitor the CPU utilization.

- Select Configuration > Services
- Select the ‘On-Prem Database’
- Select KPI tab
- Click New > Generic KPI
- Set Title to ‘CPU Utilization %’

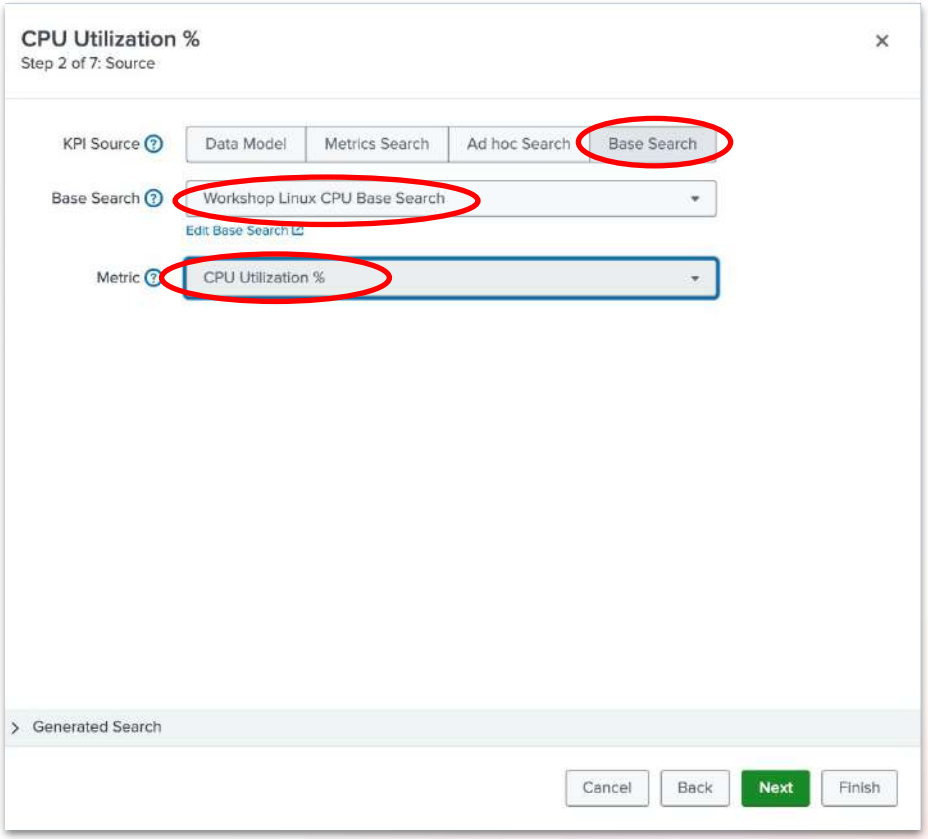
- Click the ‘Next’ button



# KPI Lab

The new KPI source could be driven by a data model, ad-hoc search or a base search.  It is always best to utilize base searches as they can return multiple KPI metrics with a single search.

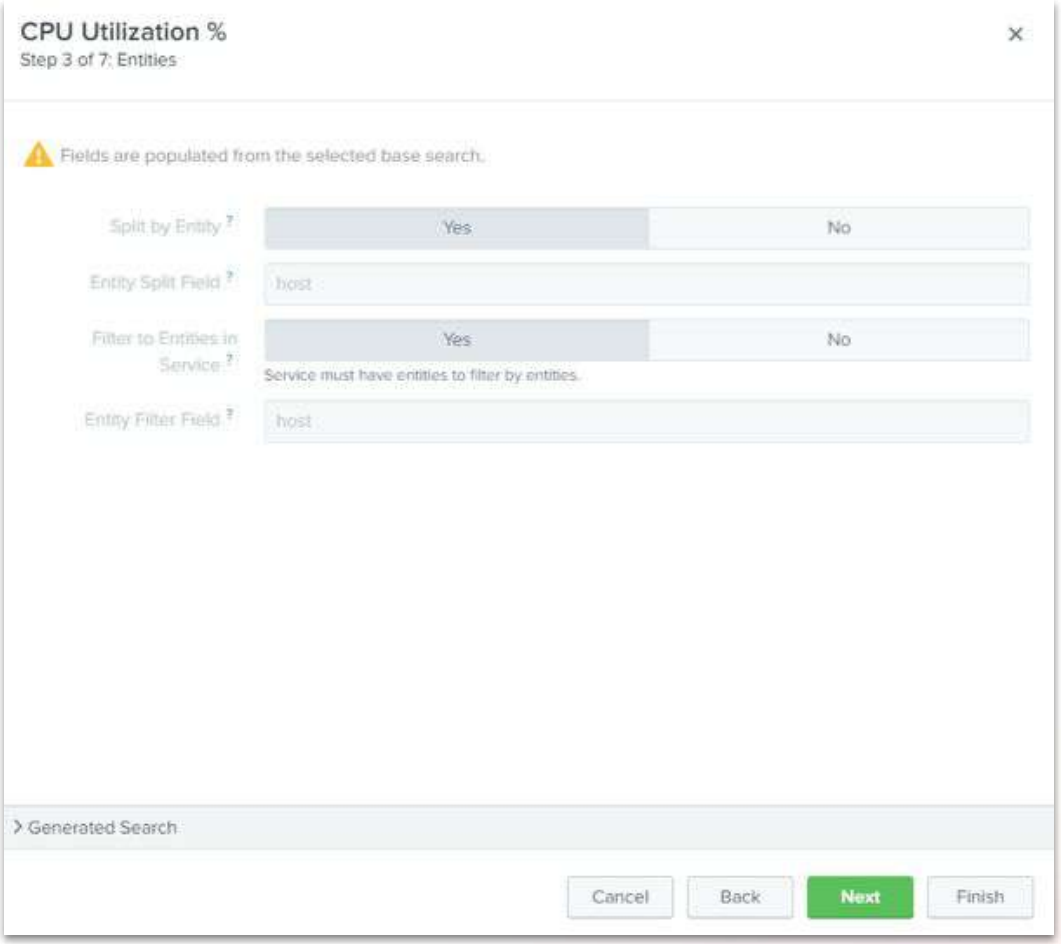
- Click ‘Base Search’
- Select ‘Workshop Linux CPU Base Search
- Select ‘CPU Utilization %’




- Click the ‘Next’ button

# KPI Lab

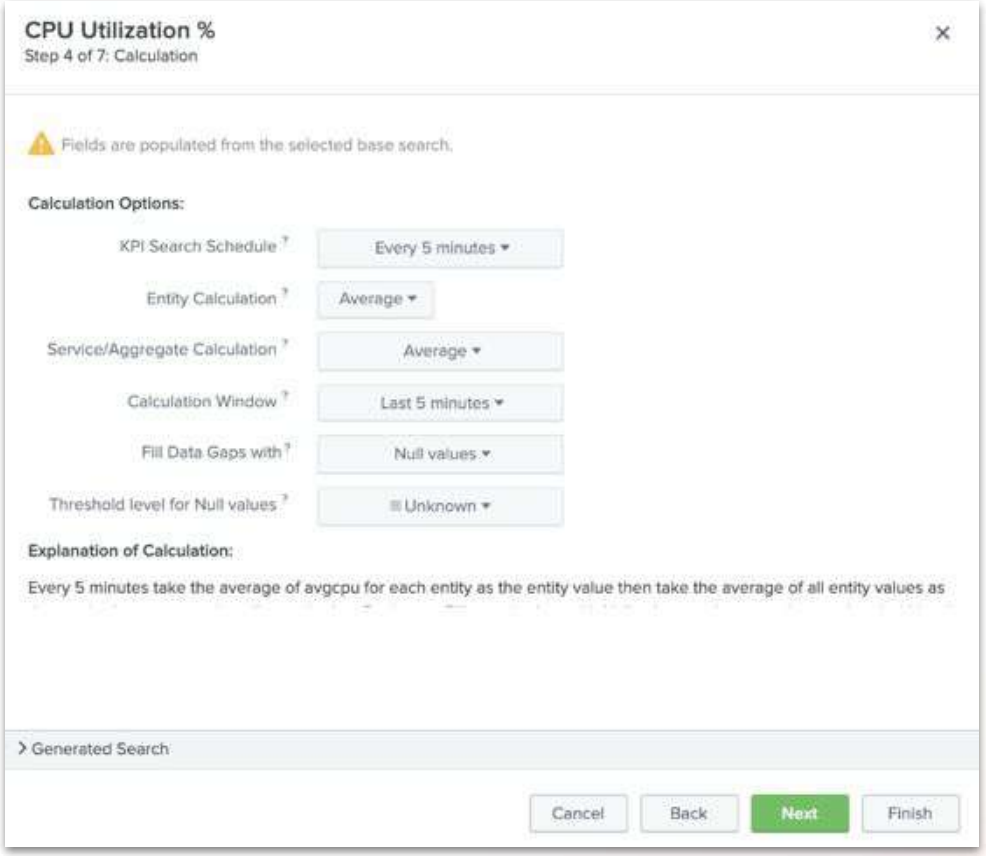
There is no option to split as this KPI is using a base search.




- Click the ‘Next’ button

# KPI Lab

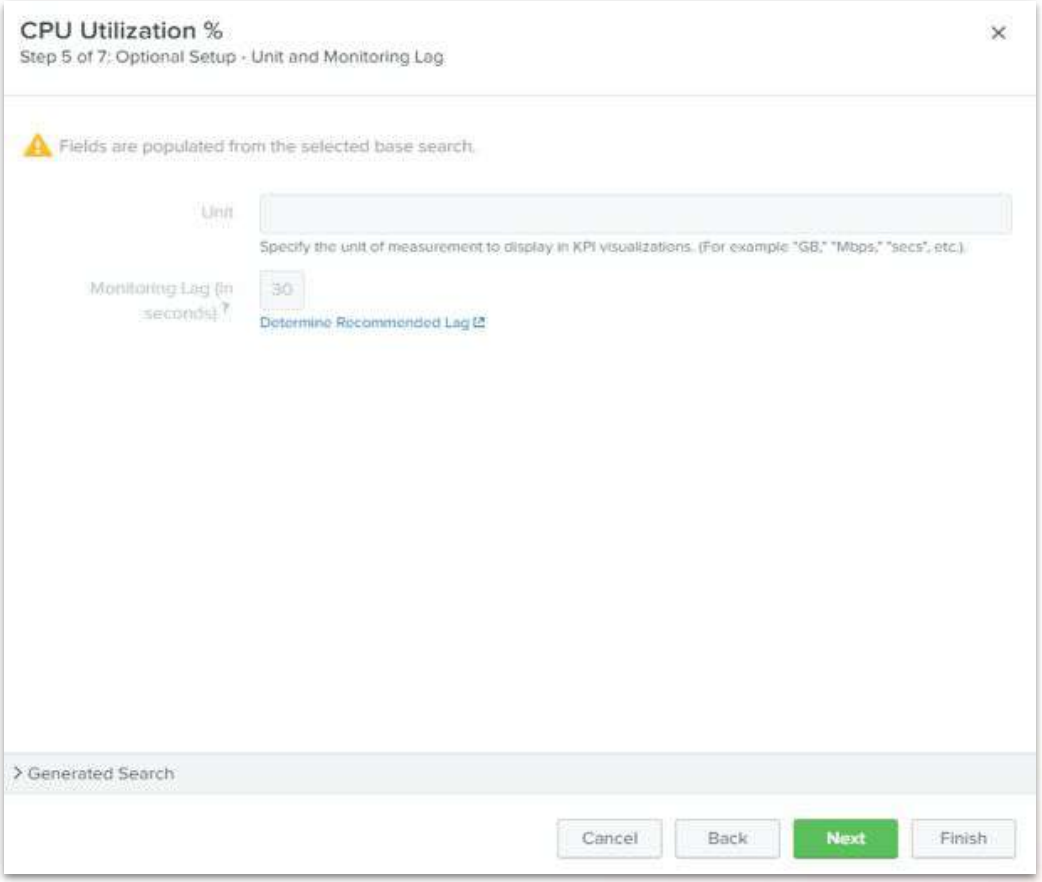
There is no option to configure the calculation as this KPI uses a base search.




- Click the ‘Next’ button

# KPI Lab

The monitoring and unit fields will be populated from the base search.

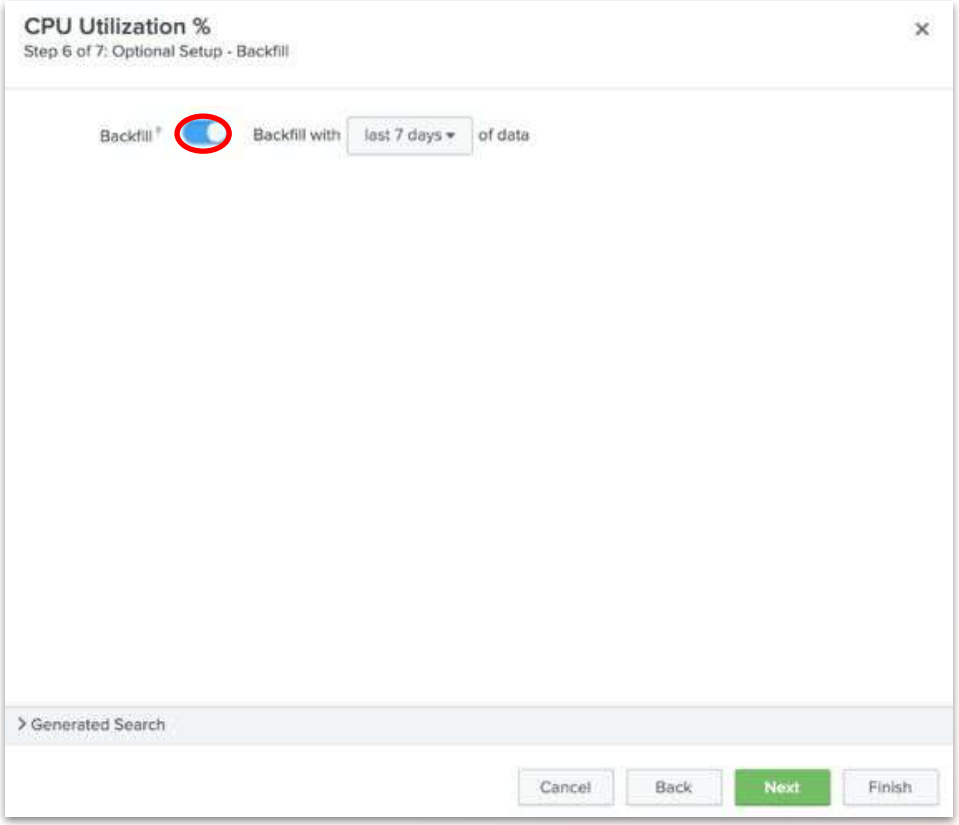



- Click the ‘Next’ button

# KPI Lab

We want this KPI to use data already ingested in Splunk over the last 7 days.

- Click ‘Enable Backfill’ button
- We will leave the backfill period as 7 days



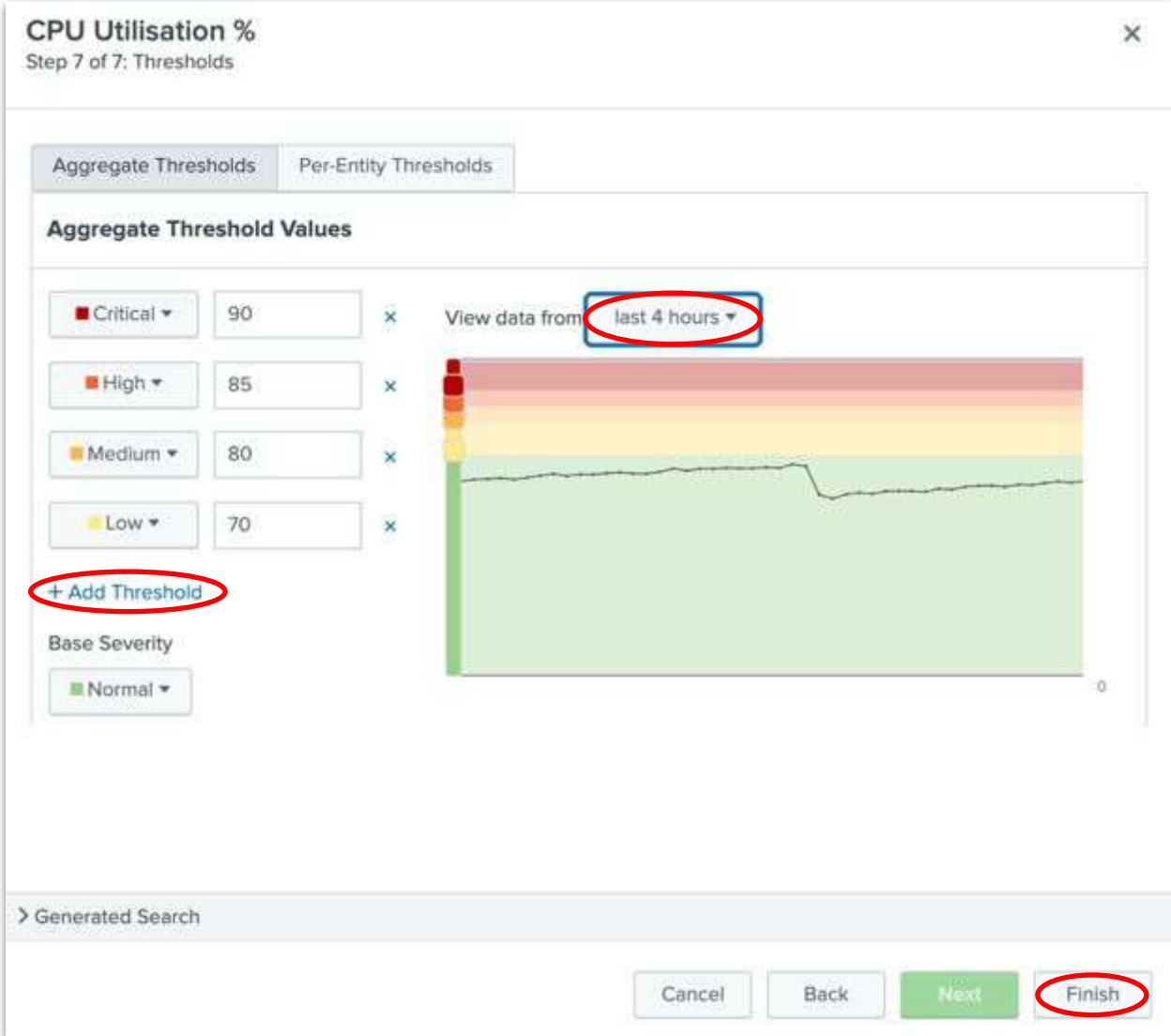

- Click the ‘Next’ button

# KPI Lab

We need to set some static thresholds for this new KPI

- Increase time to 4 hours
- Add & configure threshold:
  - Critical = 95
  - High = 90
  - Medium = 85
  - Low = 70

- Click ‘Finish’ button

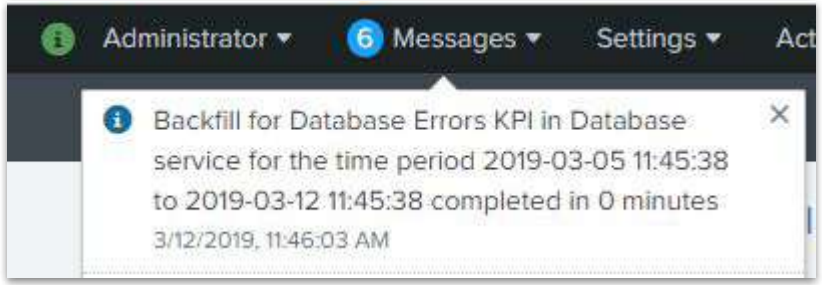


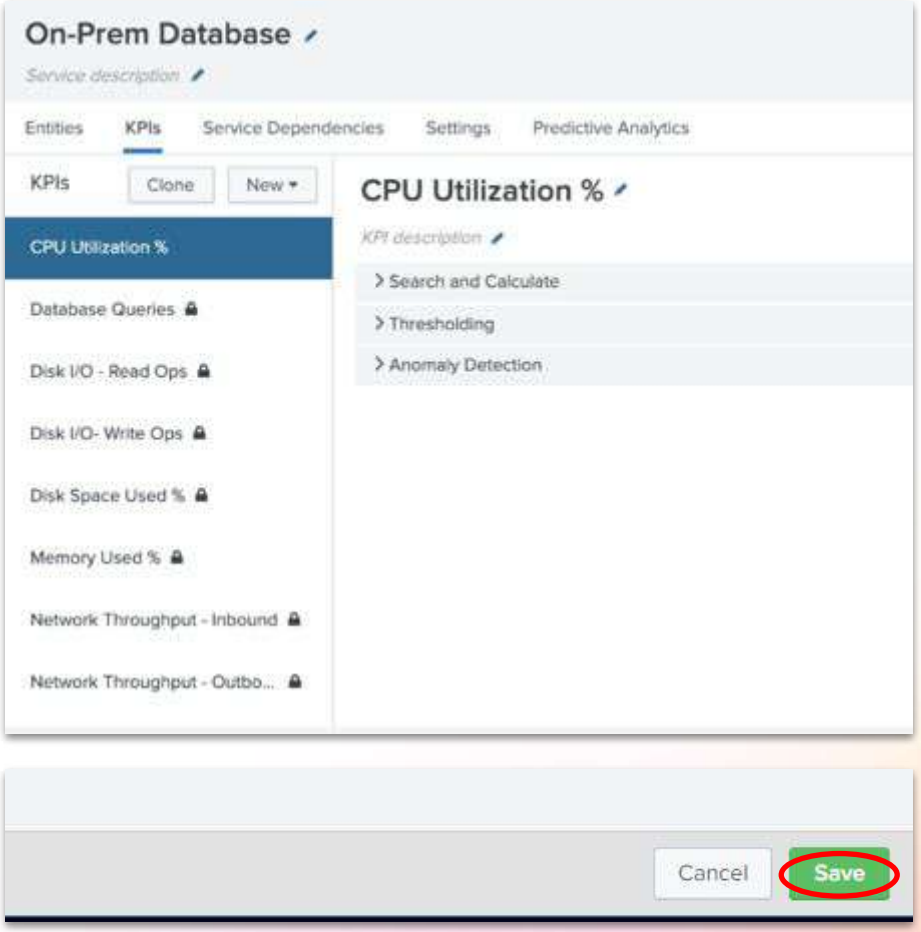
# KPI Lab

Note that the new KPI does not have a padlock icon. Inherited KPIs are locked to the service template so when changes are made these are pushed to the linked services, such as the one we are configuring.

If you edit a locked KPI it will become an orphan and template changes no longer adopted

- Click ‘Save’ button

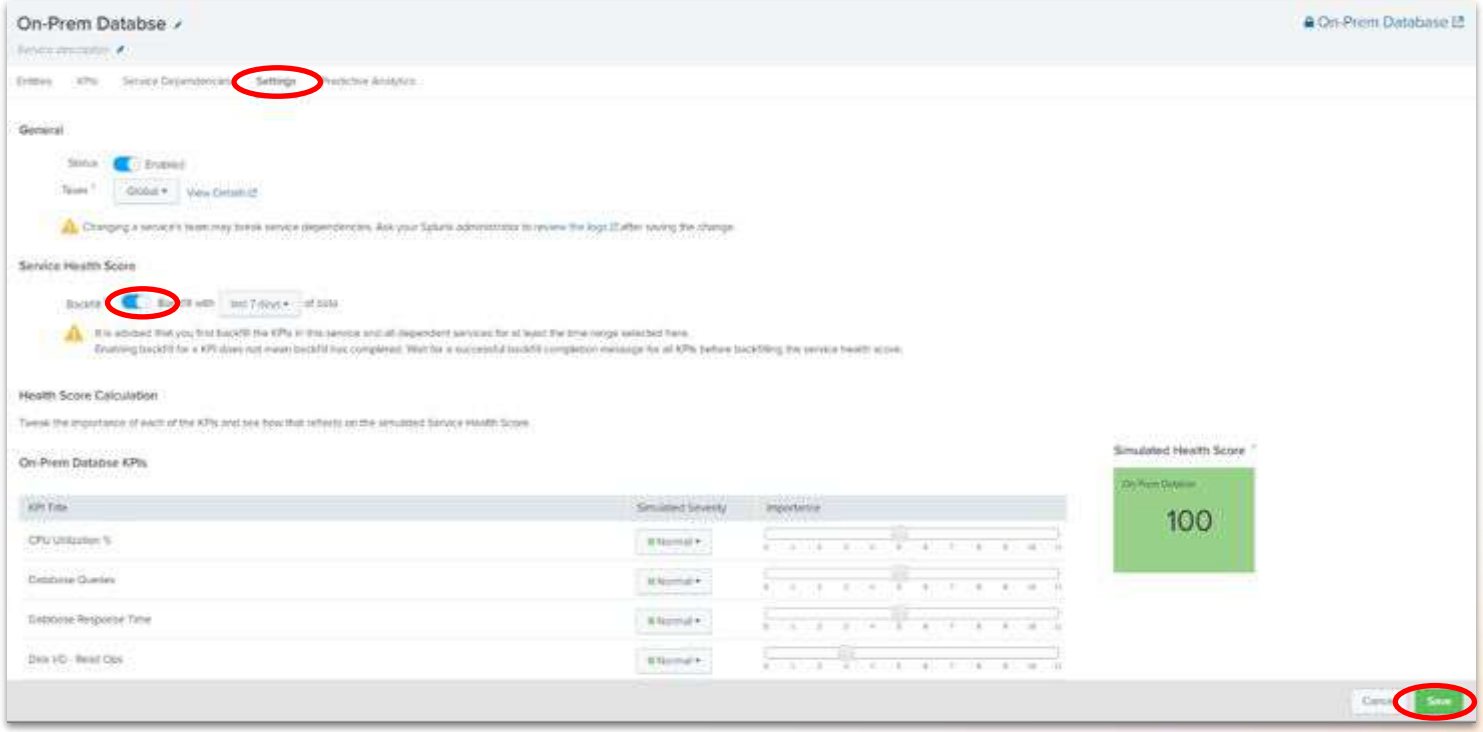


# KPI Lab

We have built a new KPI for our On-Prem Database service. We now want this new service to utilize past data via the Service Health Score backfill capability.

- Switch to the '*Settings*' tab
- Toggle backfill on (last 7 days)
- Click 'Save' button



# Deep Dive

# Deep Dive Use Case

When organisations have outages, they create a war room to identify the root cause as quickly as possible, this involves bringing together many business & technical stakeholders at great expense.

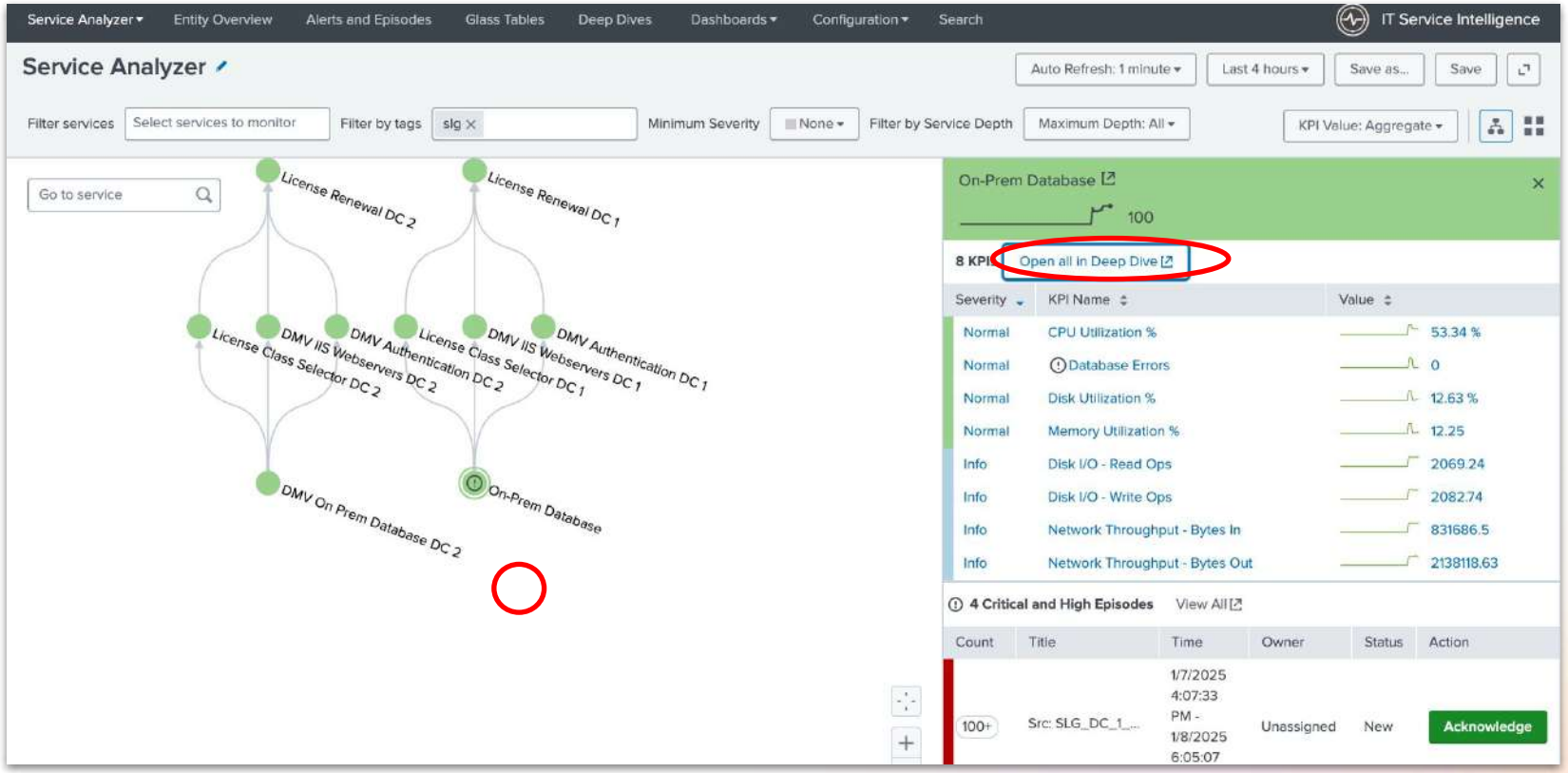
The deep dive capabilities within ITSI brings together multiple data sources into a single visualization.  The correlation of data streams enable quick identification of root cause and effect on the business.

In this lab we will build a deep dive visualization for the new On-Prem Database service, this will bring business and technical KPIs together with raw event data.

*Extra – Once this lab is completed review the comparisons options.*

# Deep Dive Use Case

- Navigate to the '*Default Service Analyzer*' view
- Click '*On-Prem Database*' service
- Click '*Open all in deep dive*'



# Deep Dive Lab

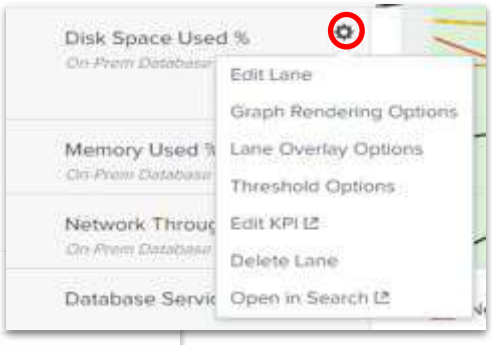
This deep dive view is used to bring all the relevant data to run an efficient war room, we can add/remove swim lanes to make the visualization even more useful.

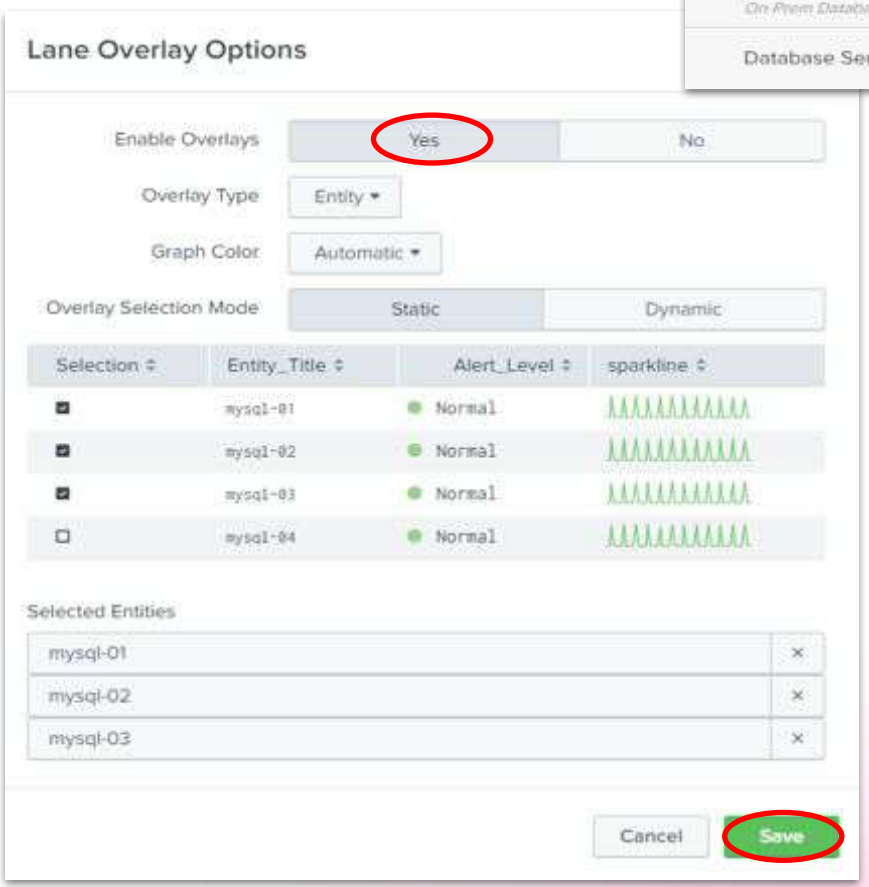
- Select the four swim lanes
- Bulk Actions > Delete

# Deep Dive Lab

To enable investigation into anomalous activity in your KPIs we can drill down on KPIs to gain deeper insights.

- Select ‘Disk Utilization %’
- Select the COG icon next to Disk Space used %
- Select Lane Overlay options
- Select Enable Overlays ‘Yes’
- Click ‘Save’

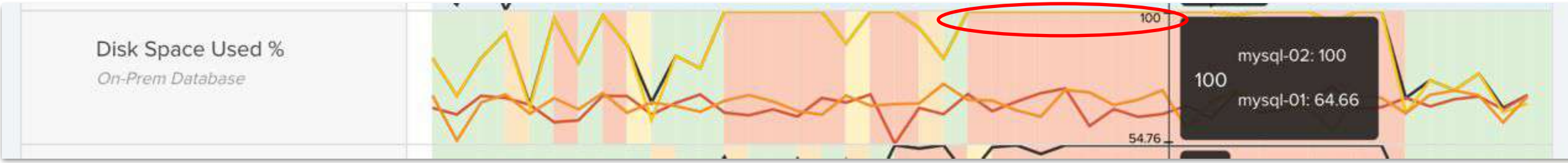


# Deep Dive Lab

We can see that the database disk space entities are behaving differently.

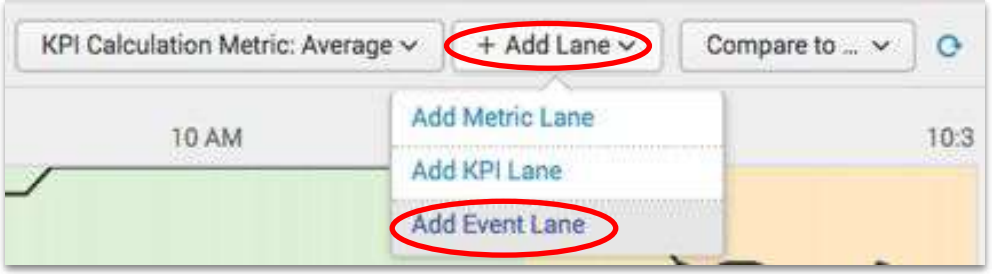
- Hover over the 'Disk Utilization %'
- We can see the individual entities performance right from this view.



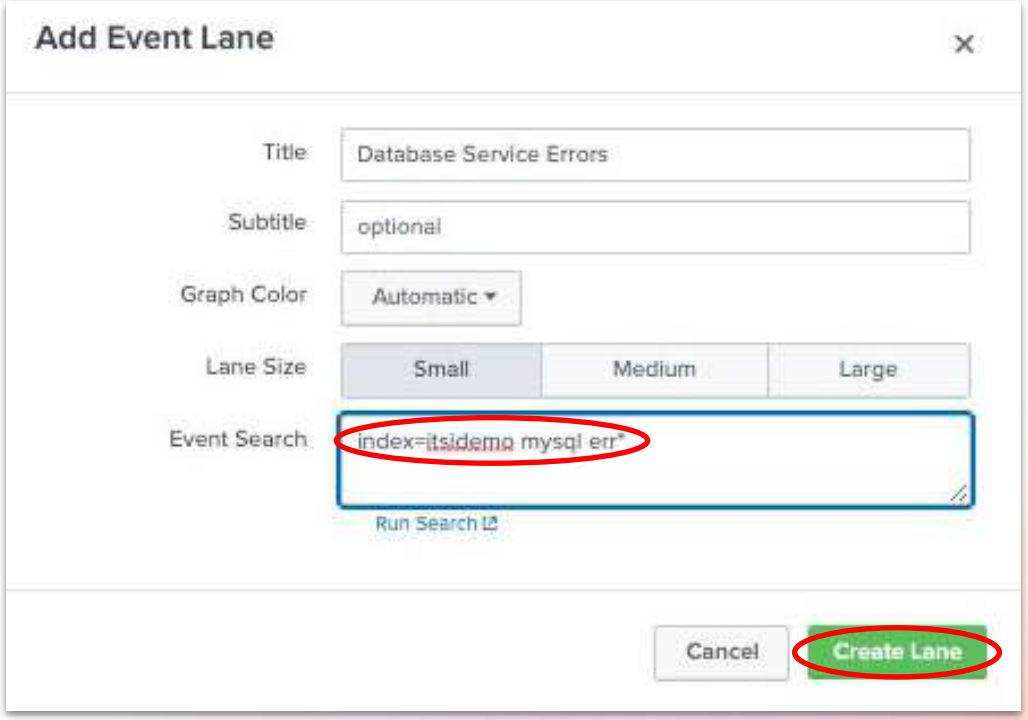
# Deep Dive Lab

We will now add an event lane to the deep dive, this enables us to dive into the root cause.

- Select ‘Add Lane’
- Click ‘Add Event Lane’




- Type ‘Database Service Errors’ Title
- Event Search:
  - *‘index=mysql mysql err*’*

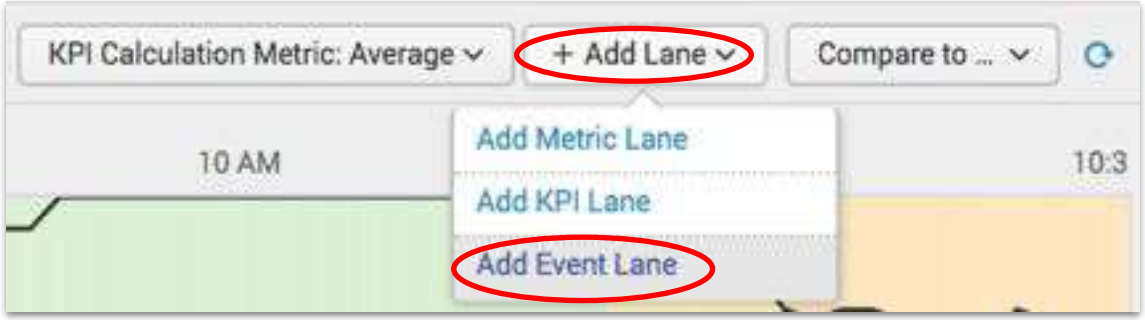



- Click ‘Create Lane’

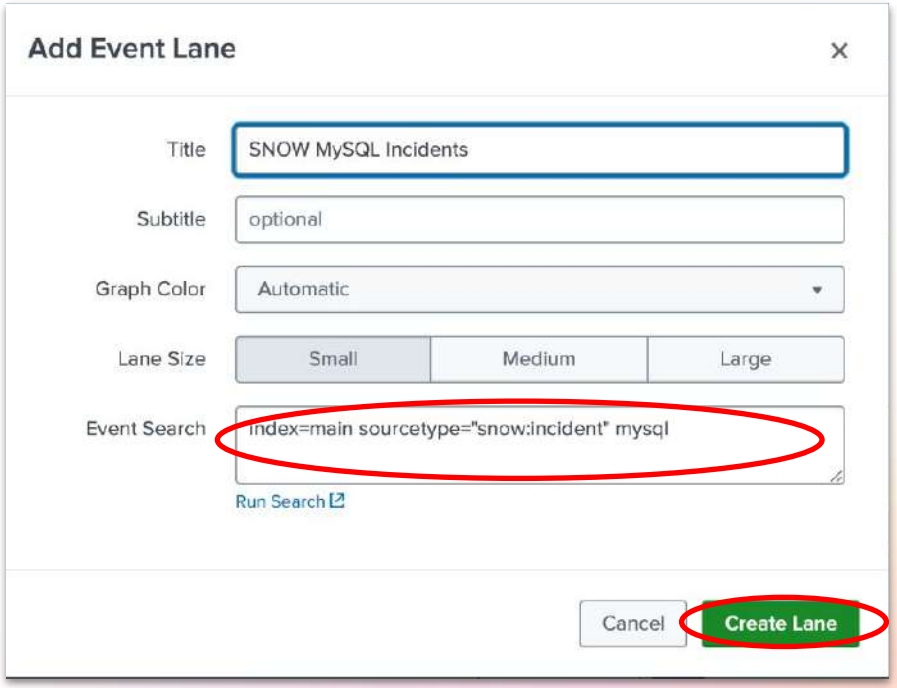
# Deep Dive Lab

We will add another event lane to the deep dive to show us any SNOW Incidents requests for the database service.

- Select ‘Add Lane’
- Click ‘Add Event Lane’




- Type ‘SNOW MySQL Incidents’ as the Title
- Event Search:
  - *‘index=main sourcetype="snow:incident" mysql*

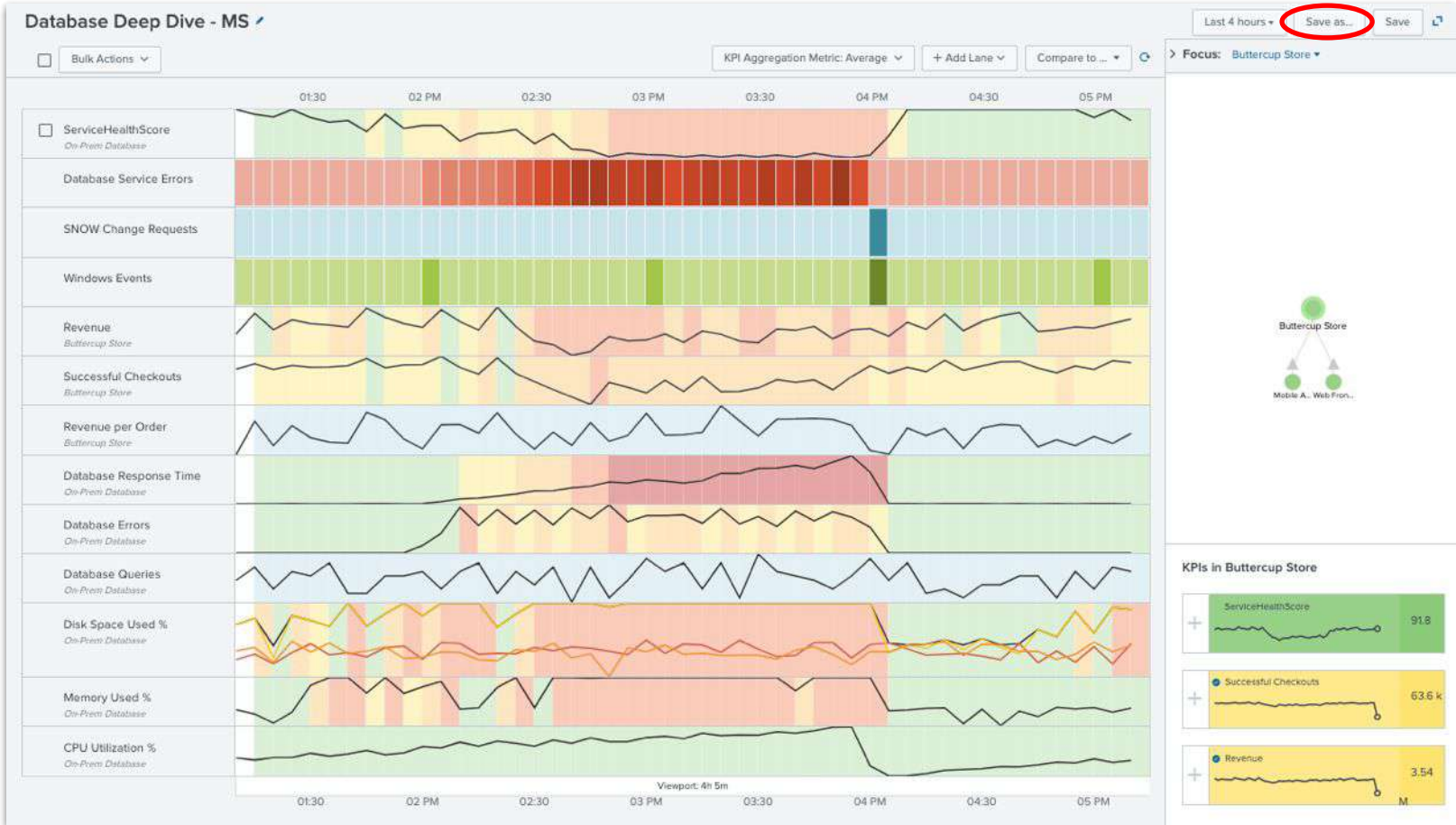



- Click ‘Create Lane’

# Deep Dive Lab

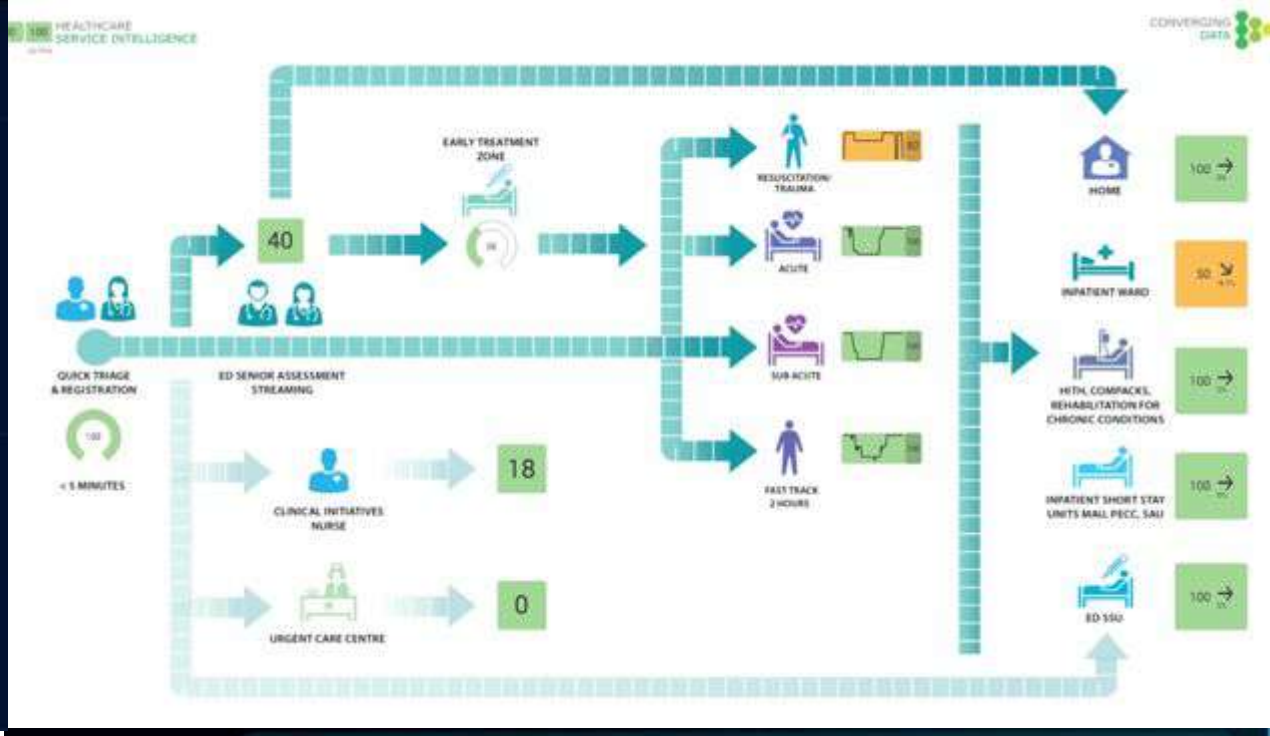
Once you have finished investigating the Deep Dive dashboard

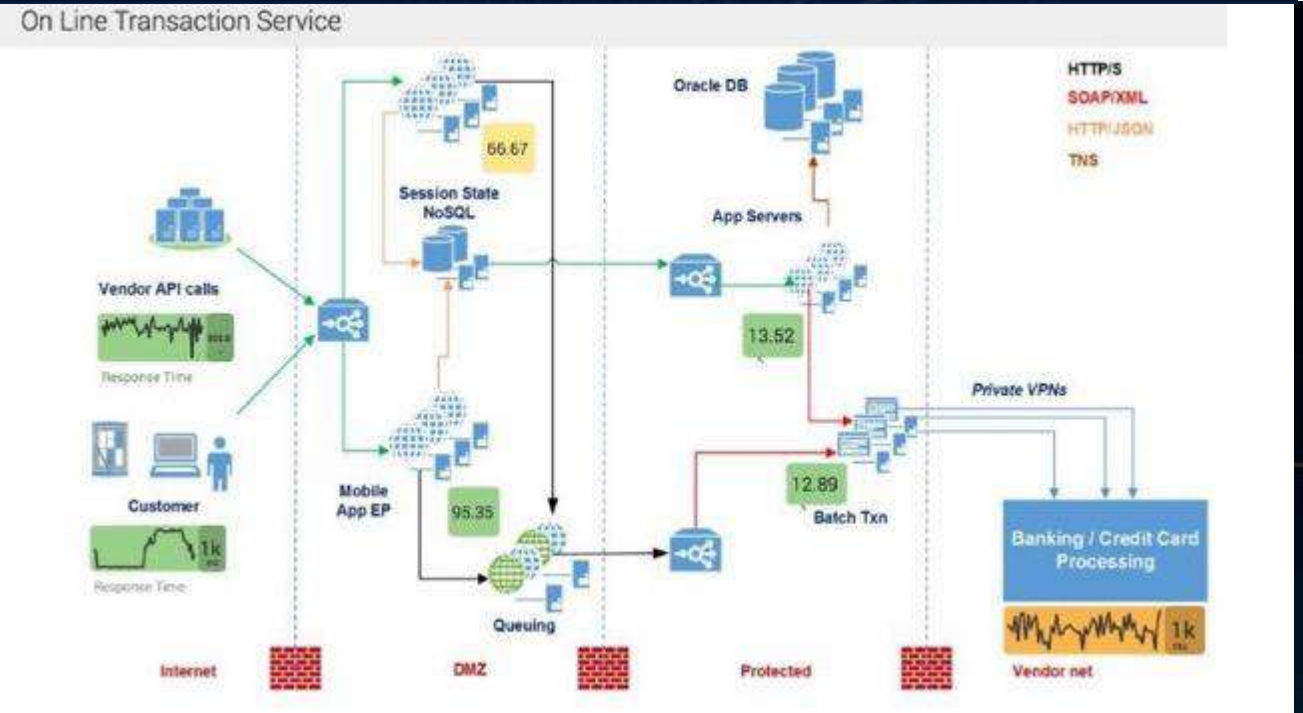
- Make sure you click '*Save As*'
- And save '*Database Deep Dive – <Your Initials>*'

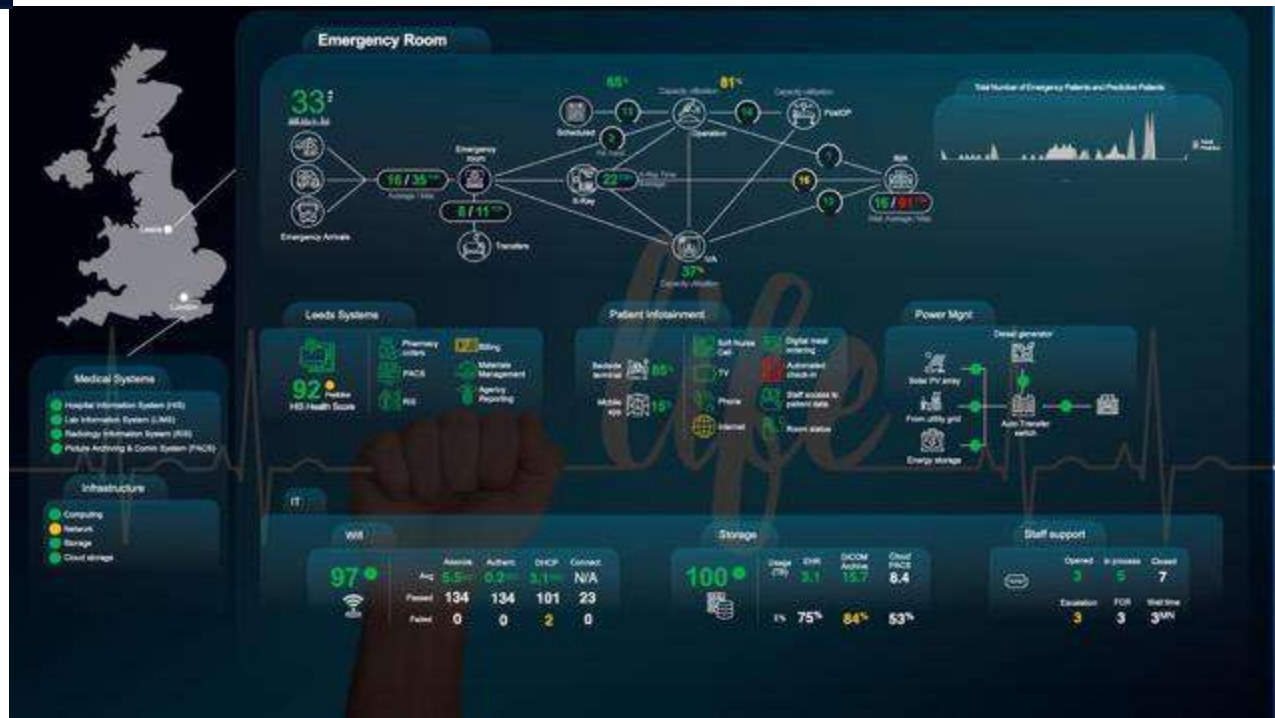


# Glass Tables


Splunk Bank
94
Mobile Banking Health Score
Account services
Account Listing 95 92
Product Application 85 94
Payments & Transfers 80 32
Account Management 80 53
Notification 98
Security 92
Authentication 94
Open Banking 97
Supporting services
Presentation & Authentication layer
Service layer
Data layer
Infrastructure
94 95 85 80 80 92 53 94 95
Firewall
Load Balancer
API gateway
Load Balancer
Microservices
ESB
Database
Core
Mainframe
94
97
98
OpenBanking API


HEALTHCARE SERVICE INTELLIGENCE
CONVERGING DATA
EARLY TREATMENT ZONE
40
QUICK TRIAGE & REGISTRATION
< 5 MINUTES
ED SENIOR ASSESSMENT STREAMING
CLINICAL INITIATIVES NURSE
18
URGENT CARE CENTRE
0
RESUSCITATION/ TRAUMA
ACUTE
SUB-ACUTE
FAST TRACK 2 HOURS
HOME
INPATIENT WARD
HITH, COMPACKS, REHABILITATION FOR CHRONIC CONDITIONS
INPATIENT SHORT STAY UNITS MAU, PECC, SAU
ED SSU
100
50
100
100
100


On Line Transaction Service
HTTP/S
SOAP/XML
HTTP/JSON
TNS
Oracle DB
66.67
Session State NoSQL
App Servers
Vendor API calls
Response Time
13.52
Private VPNs
Customer
Response Time
Mobile App EP
95.35
12.89
Batch Txn
Queuing
Banking / Credit Card Processing
Vendor net
Internet
DMZ
Protected


Emergency Room
33
Emergency Arrivals
16 / 35
8 / 11
Transfers
65
81
37
16 / 91
Leeds Systems
92
Medical Systems
Infrastructure
Patient Infotainment
Power Mgmt
Wifi
97
Storage
100
Staff support
134 134 101 23
0 0 2 0
N/A
8.4
75 84 53
3 5 7
3 3 3

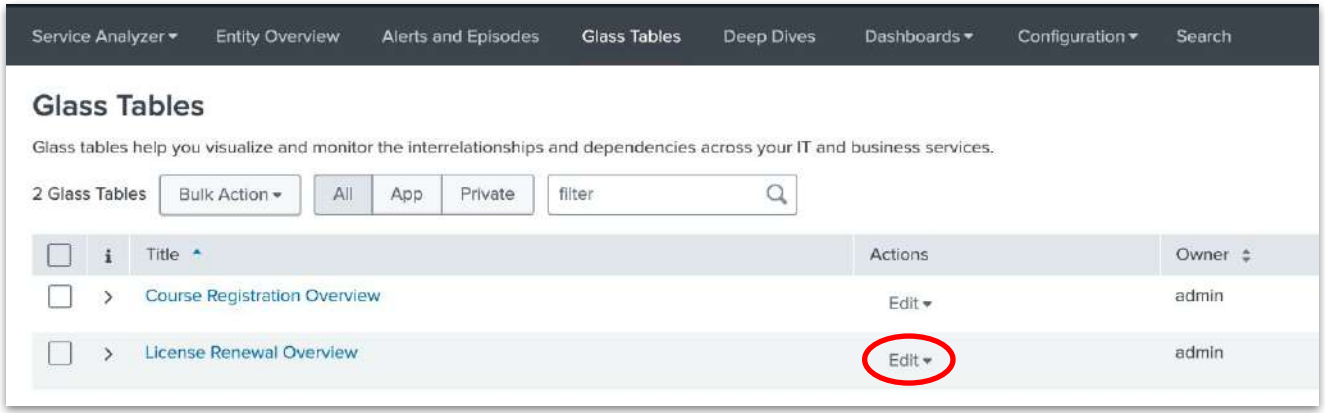
# Glass Table Use Case

- The DMV leaders would like a high-level dashboard showing the key functions and services of the organisation.

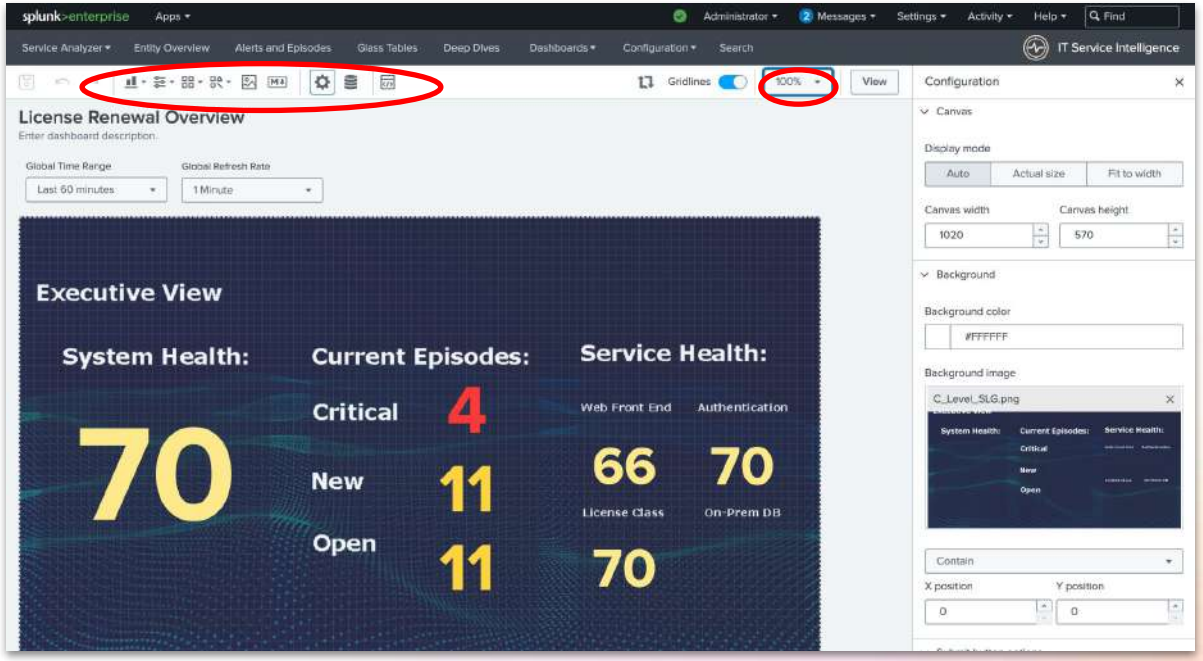
- The objective of this exercise is to complete the existing IT operations dashboard (License Renewal Overview) with the new On-Prem Database service health score, including a drill down to a deep dive.

# Glass Table Lab

- Select *Glass Table menu*
- *Edit 'License Renewal Overview'*

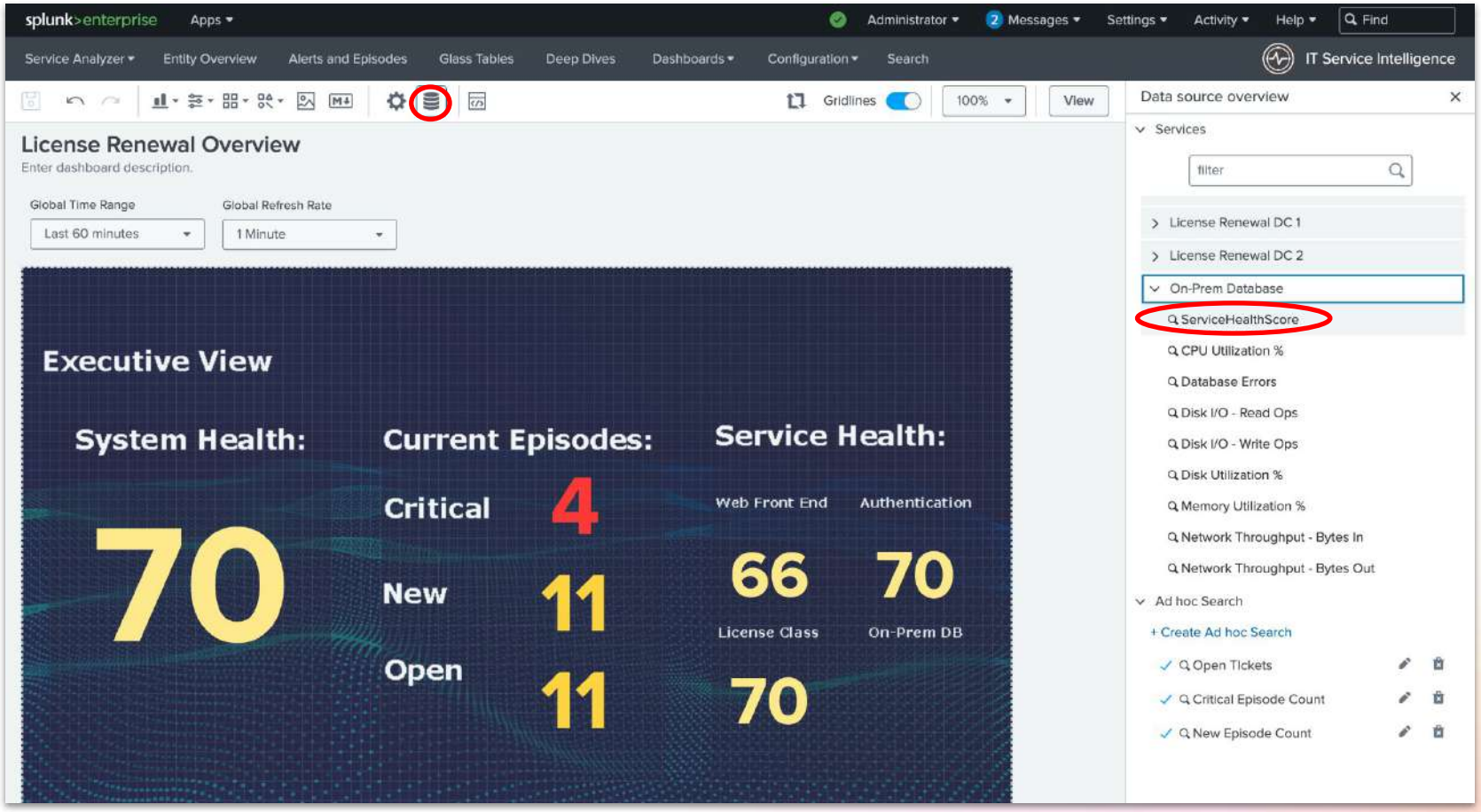



- Investigate the tool palette icons
- *Modify zoom to fit to page*
- *Review the Configuration panel on right*



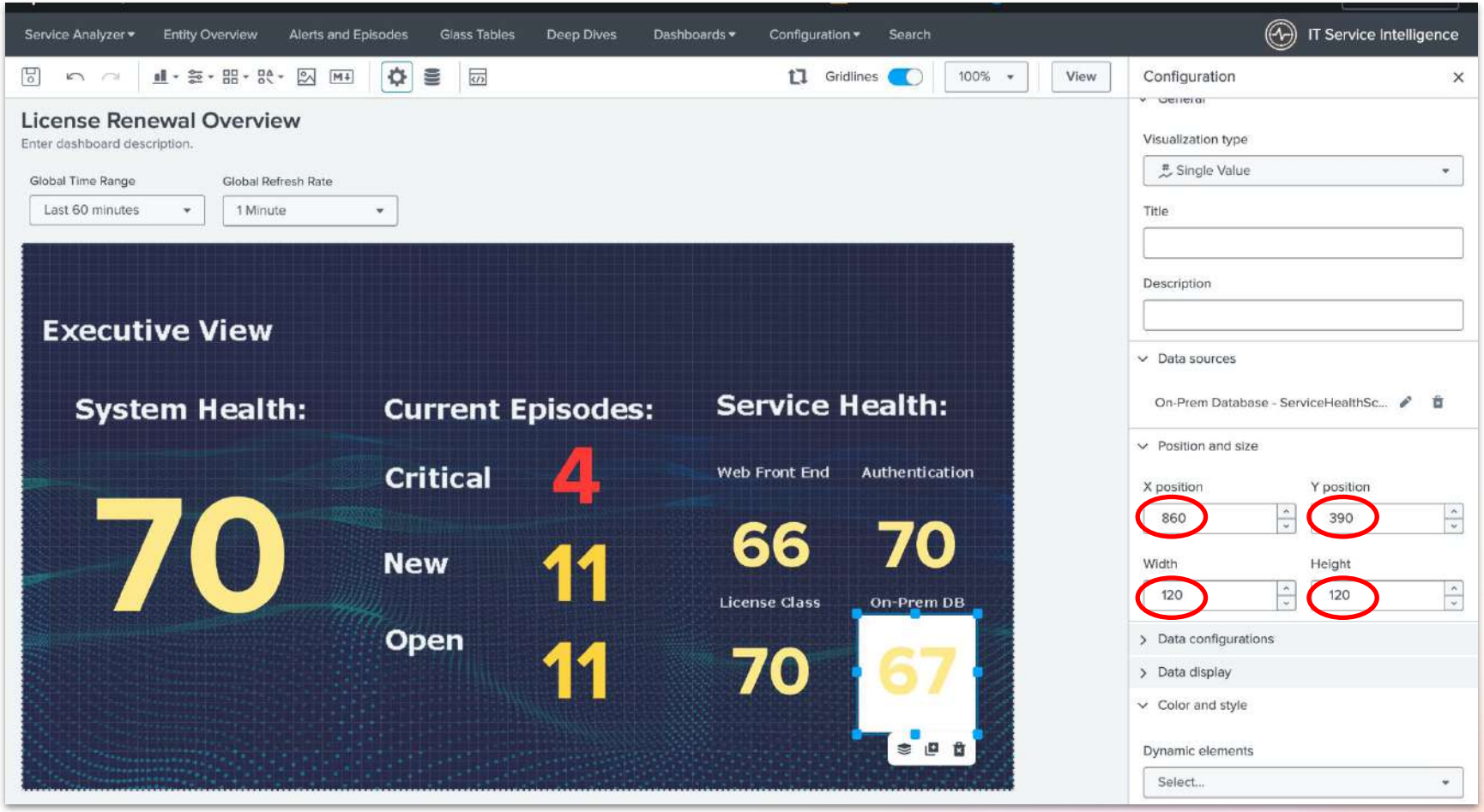
# Glass Table Lab

- Click the “Data Overview” button in the pallet menu
- Select *On-Prem Database Service (scroll down or use the filter box)*
- Click ‘ServiceHealthscore’



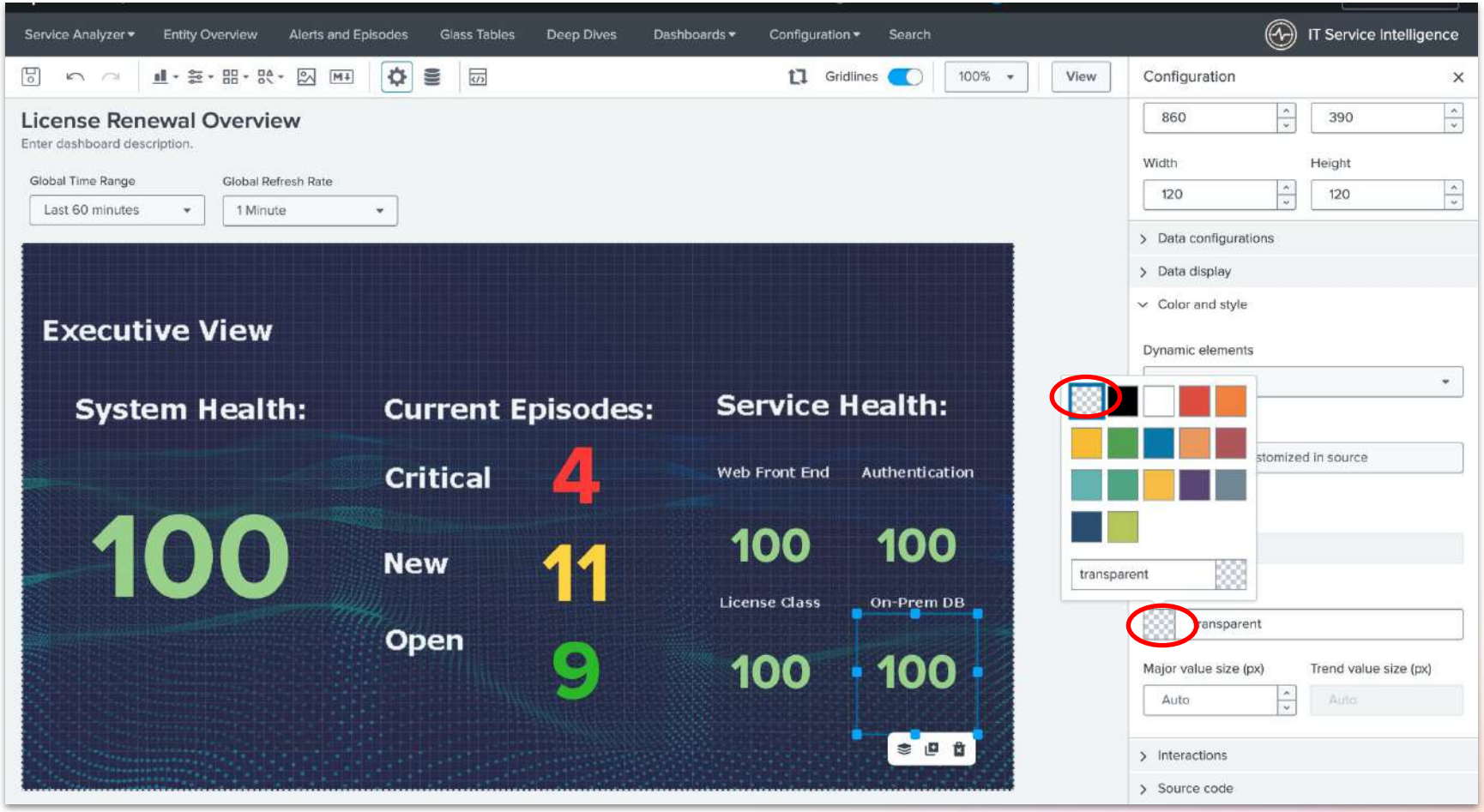
# Glass Table Lab

- Move the Service Health Score to the correct position
- Modify size to appropriate size and investigate options



# Glass Table Lab

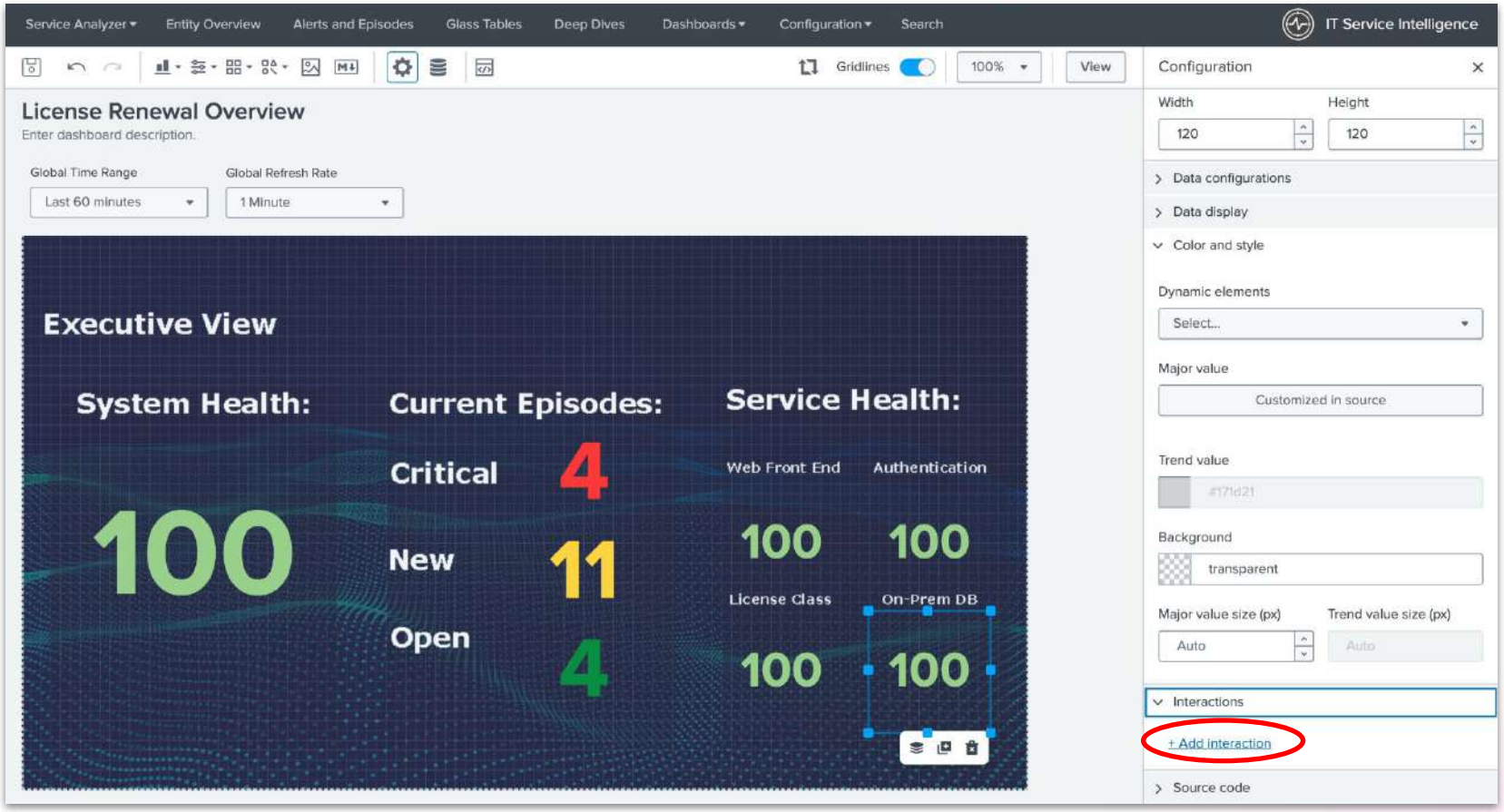
- Change Color and Style so the KPI has a transparent Background



# Glass Table Lab

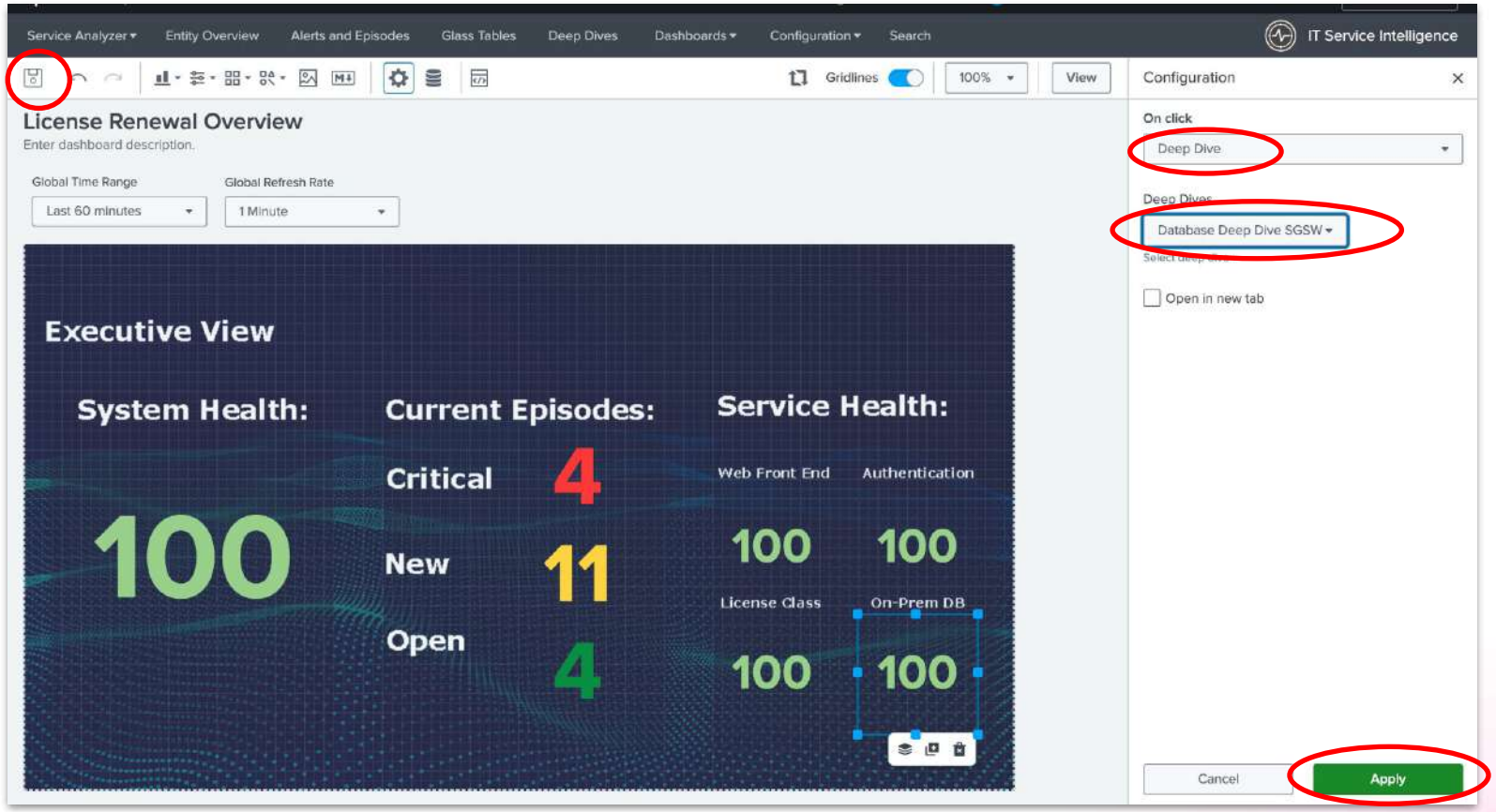
We will now link the database deep dive visualization to this glass table

- Click Add Drilldown



# Glass Table Lab

- Select “Deep Dive” on click
- Now choose your saved Deep Dive
- Click Apply
- Click the Save button and icon once completed



# Next Steps

# Service Decomposition Workshop

# Implementation Methodology

## Service Decomposition

What is the service to be monitored?

What are the components of the service?

What are the metrics/what do you care about?

What are the KPIs per service?

Identify data sources for each KPI

Onboard data into Splunk.

Create Services, Dependencies

Create KPIs, tune thresholds

Modify Deep Dives

Create Glass Tables

Event Clustering

Adaptive Thresholding

KPI Alerting

Predictive Analytics

## Ready for ITSI

# Three things to think about

**1**

Start with a problem worth solving

**2**

Bring subject experts together

**3**

Design before configuring

# 1. Uncovering the Problem Worth Solving

## Critical Services

- What are the top business services in your enterprise?
- How do you measure the customer experience with these services?
- What is the customer experience with these services ?

## Issue Frequency

- How often do customers experience issues with the service?
- When issues arise, who gets involved in resolving them?
- How do teams work together to resolve issues?

## Impact

- What's the average time-to-issue-resolution?
- What's the impact when customers have a bad experience with your services?

# 2. Bring Subject Experts Together

Identify stakeholders and support personnel for the selected service

Create awareness and invite their collaboration to solve the business challenge

# 3. Design Before Configuring

Identify pains, performance indicators and measurement goals for the service

Identify major components and data needed to drive service insights

Connect components into an enterprise process/IT services map

# Thank You

splunk>
a CISCO company