

ITSI for SLED

Hands-On Workshop



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, Splunk> and Turn Data Into Doing are trademarks and registered trademarks of Splunk LLC in the United States and other countries. All other brand names, product names or trademarks belong to their respective owners.

© 2024 Splunk LLC. All rights reserved.

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>

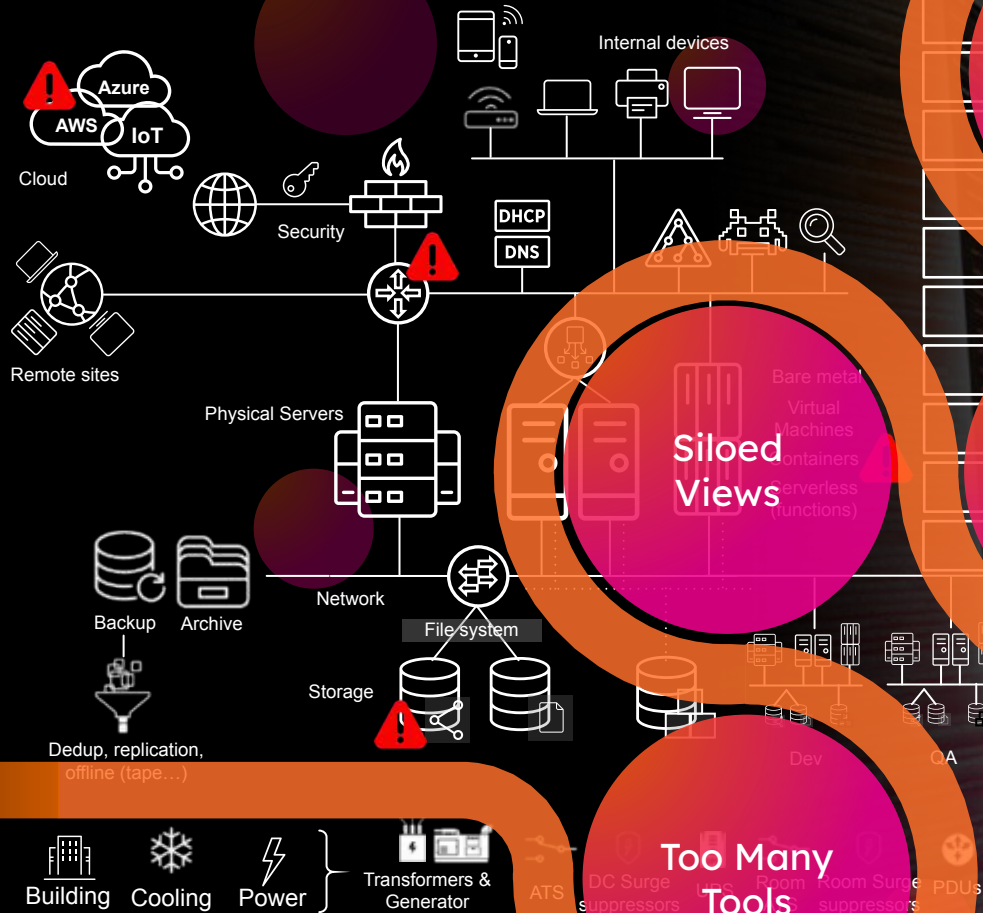
Goal

The screenshot shows the 'ITSI for SLED Workshop' event page. The breadcrumb trail is 'Home > ITSI for SLED Workshop'. The main content area features the event title 'ITSI for SLED Workshop' with a status 'INVITED' and a 'STARTING SOON' badge. Below the title is the 'Splunk IT Service Intelligence' logo. To the right, there is a blue 'Enroll event' button and a 'Request Help' link. A callout box in the top right corner of the page says 'Enroll in today's event'.

ITSI Overview

Complexity obscures the data you need

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



Siloed Views

Long MTTR

Event Noise

Too Many Tools



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

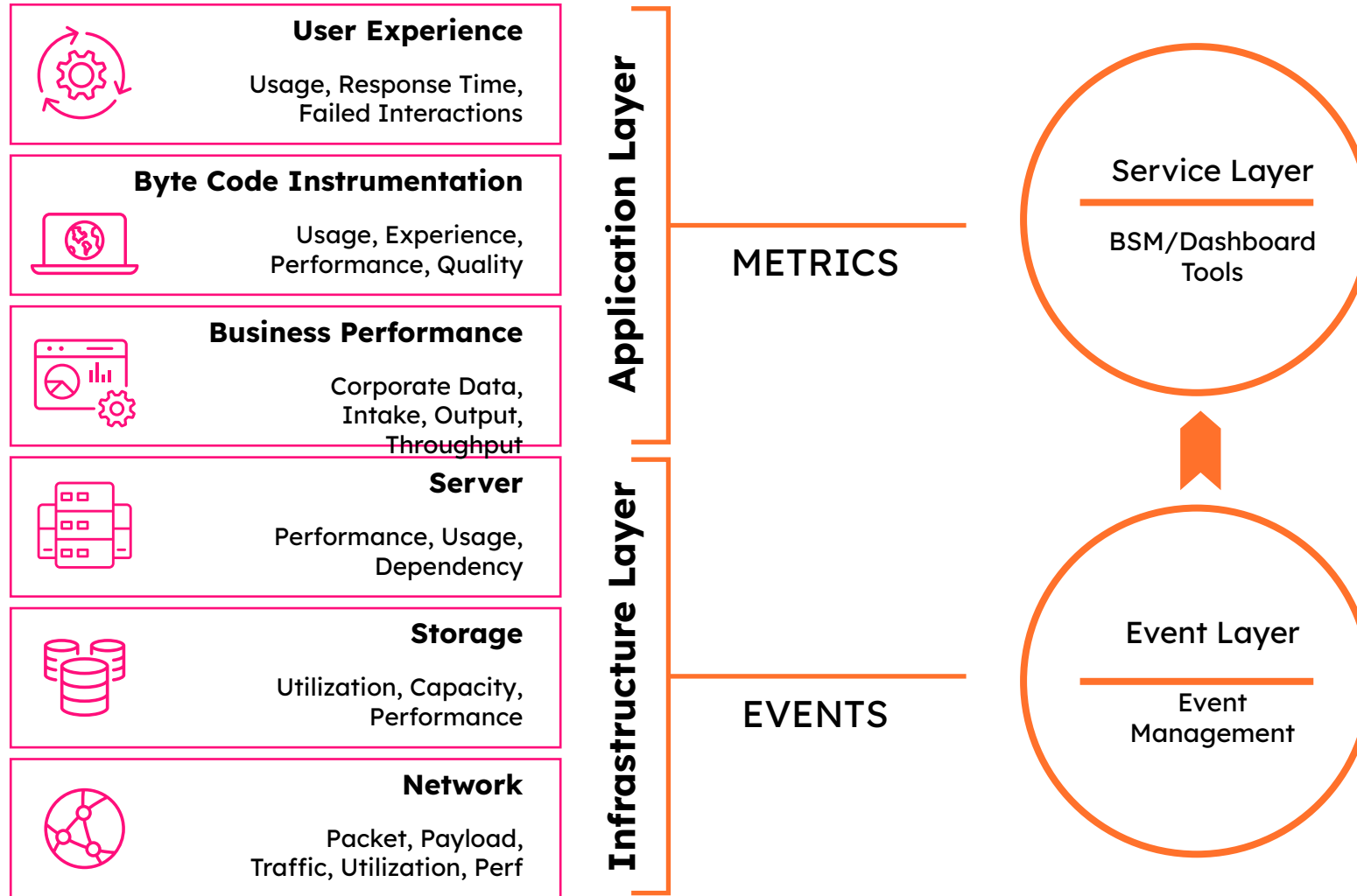
Teams thrash, finger-point, and key employees leave



Struggle to Innovate

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

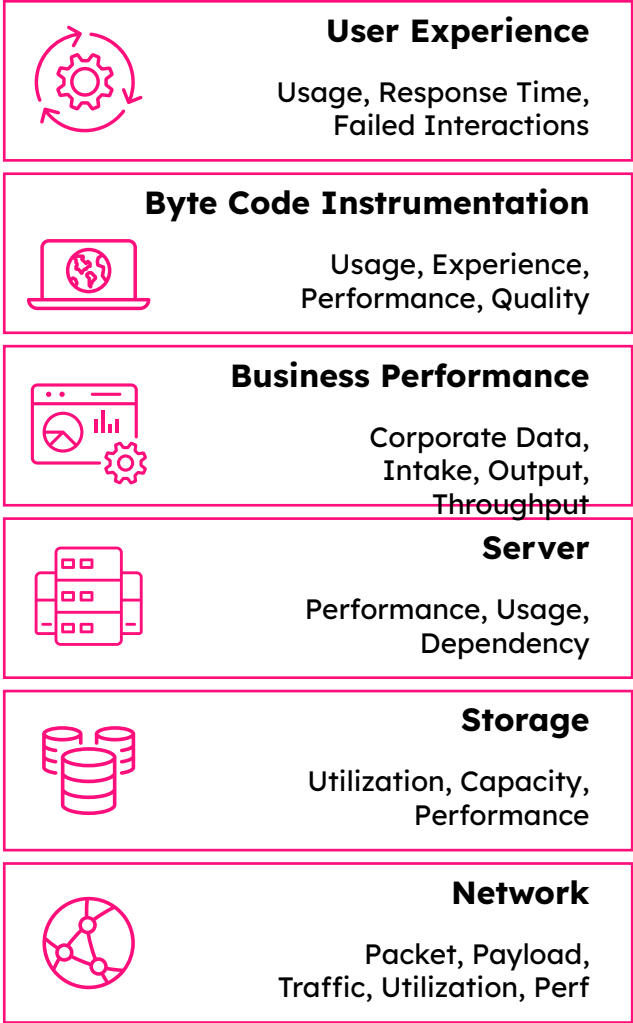
The Old Ways Disappoint



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



Application Layer

Infrastructure Layer

Machine Data

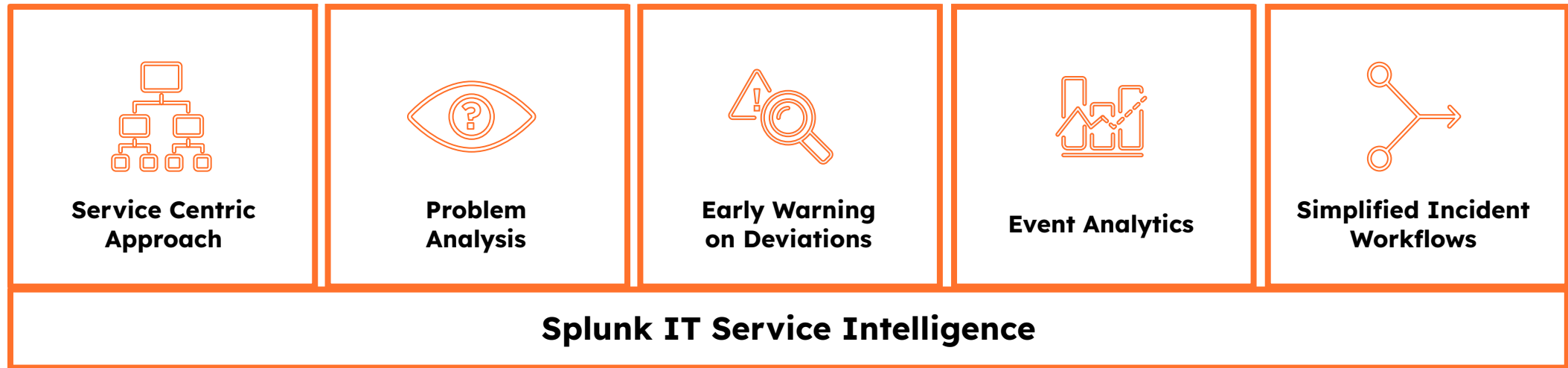


Splunk Approach:

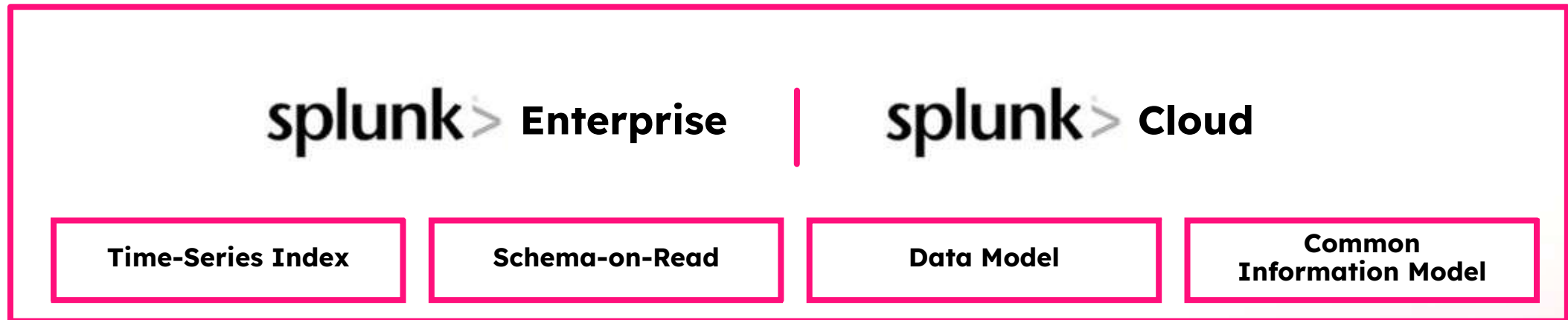
- Repository for **ALL** data
- Data in original raw format
- Machine learning
- Simplified architecture
- Fewer resources to manage
- Collaborative approach

Splunk IT Service Intelligence

Data-driven service monitoring and analytics



Machine Learning



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

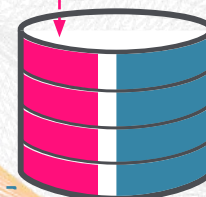


Raw Format, No Normalization

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

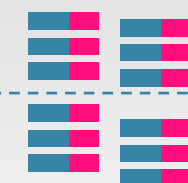


Query

All queries include a time component, data indexed on time

Rapidly return results across all data sources with no configuration

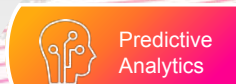
Aggregate events on any metadata **programmatic** declaration



Flexible Visualization



Alert on Any Data



Predictive Analytics

Correlation of any Data Source is Key

Logs were just the first to illustrate the problem...

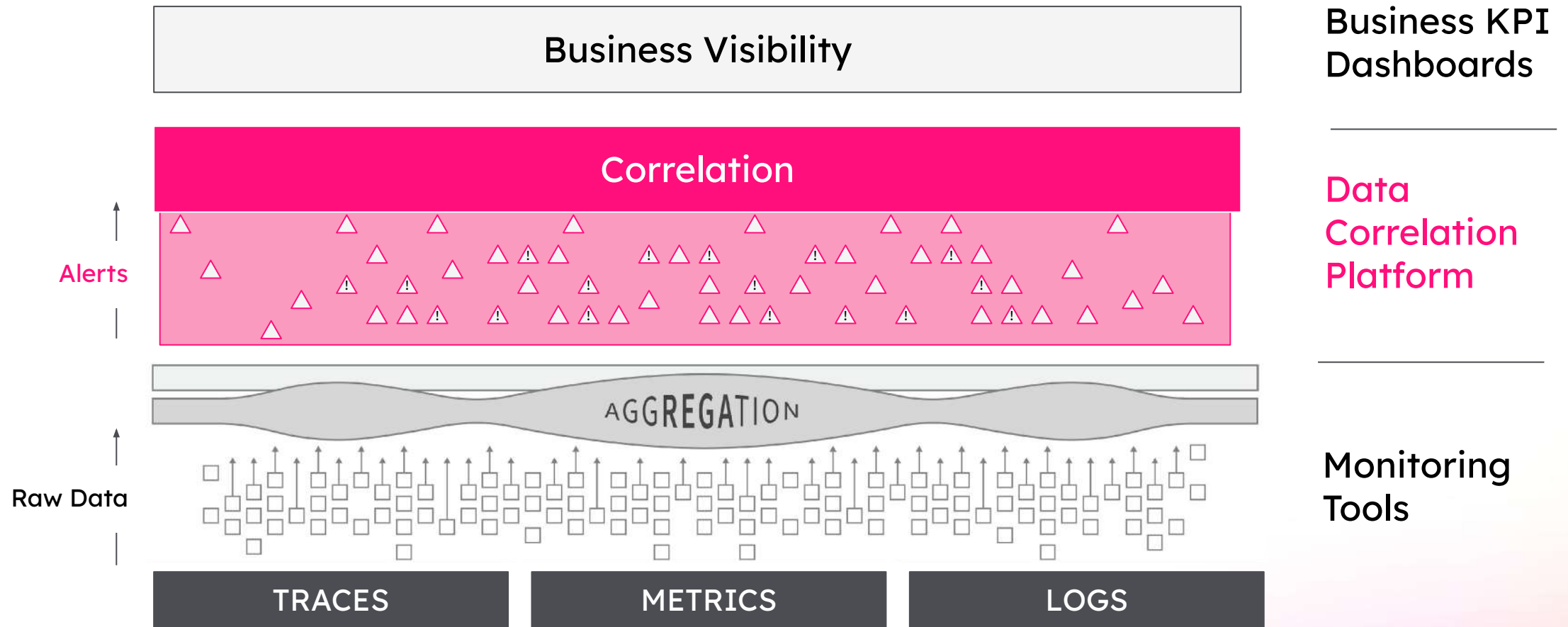
Database Solutions

- **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...



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!

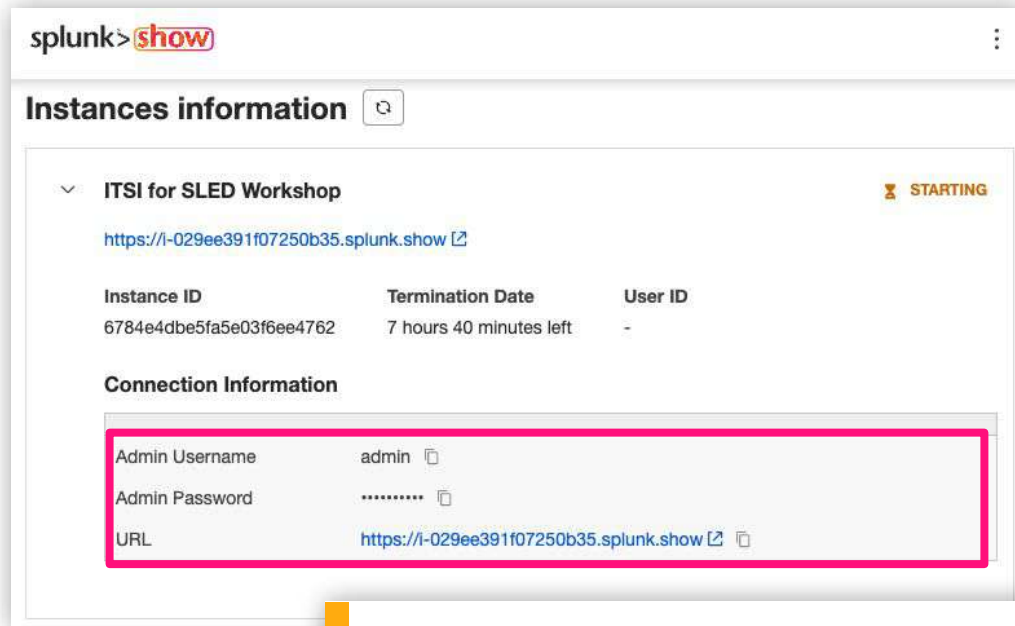
The lab starts on the back of a **service decomposition workshop** which has identified all the missing **database** components.

Login to Splunk

Locate your instance URL and credentials
in the Splunk Show event

<https://show.splunk.com>

Log in to your Splunk instance



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



Login using the credentials
from Splunk Show

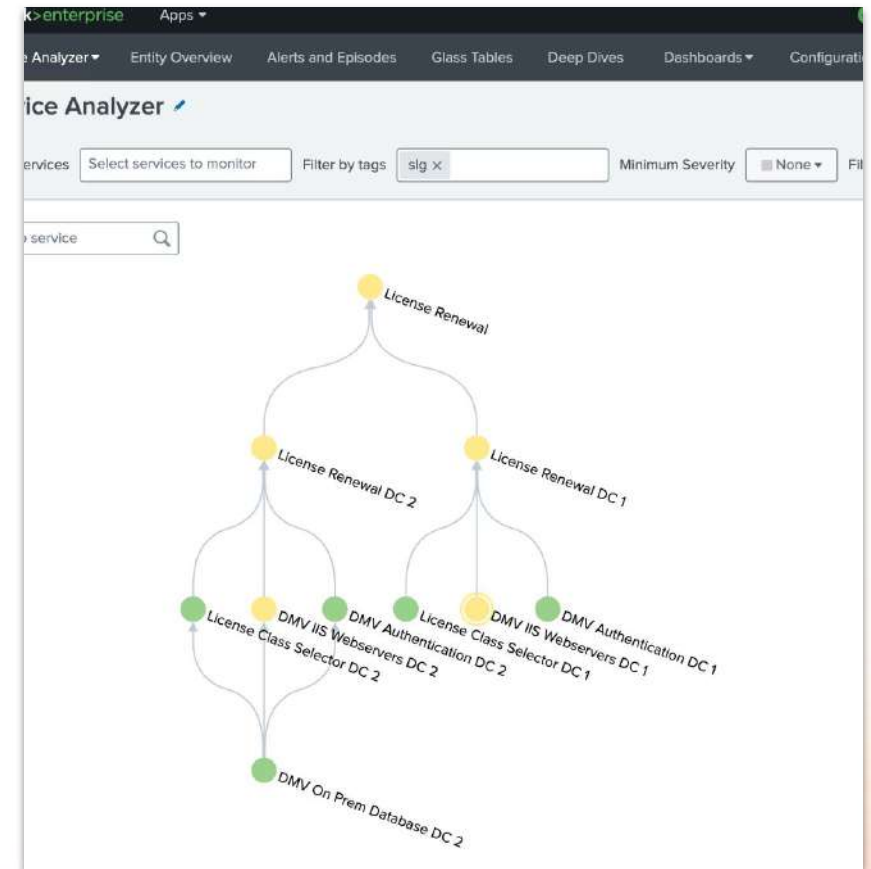
Services Exercise

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.

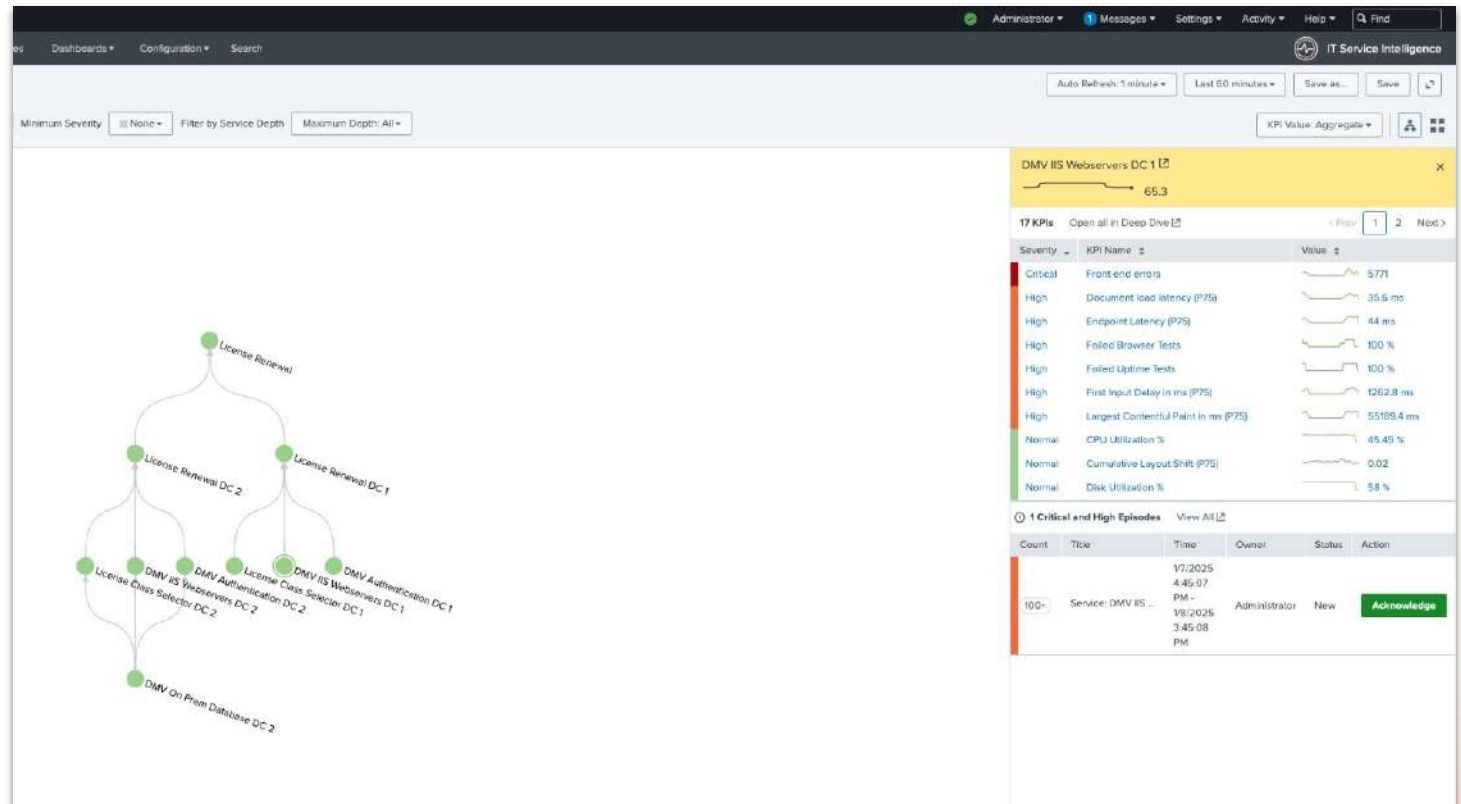
- Click on the different services service and review the KPIs.
- Adjust the time picker to investigate when there was a severity degradation. *(note: there should be issues around an hour before the start of workshop (xx:40 - xx:59)).*



Service Tree

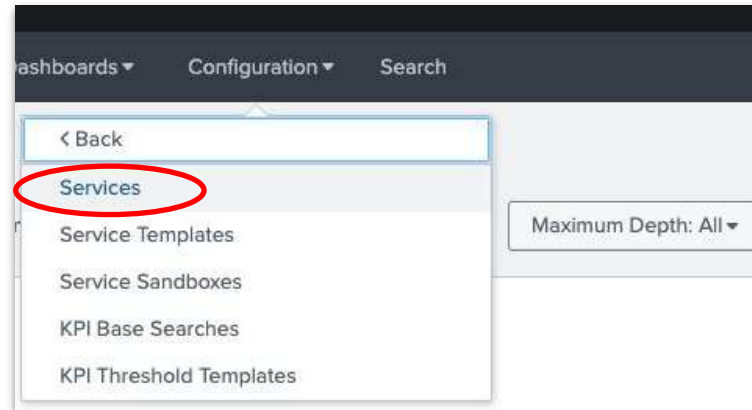
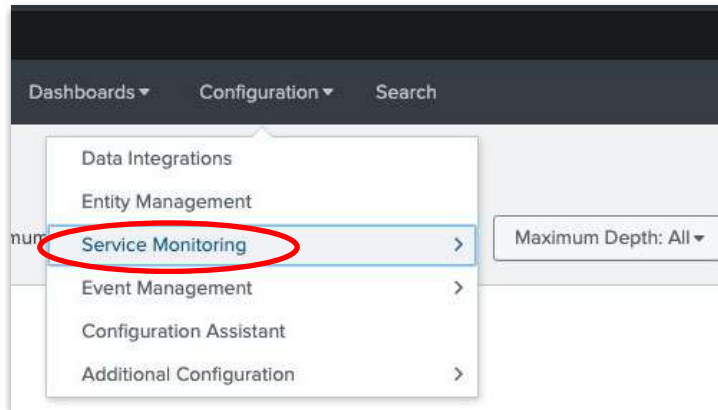
We can see that there is an issue with the Cart Services service.

- 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”

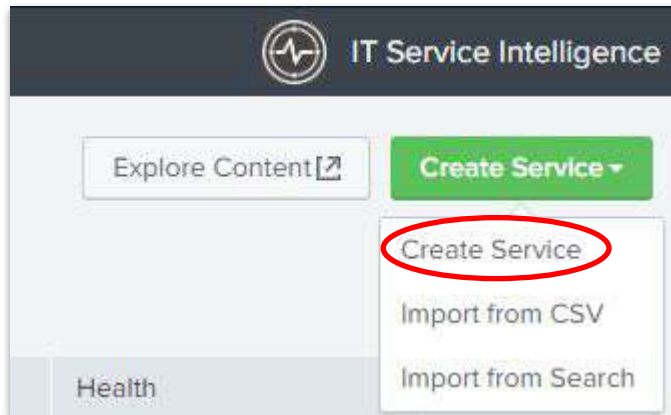


Services Lab

- 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

The screenshot shows the 'Create Service' dialog box. The 'Title' field is 'On-Prem Database'. The 'Description' field is 'optional'. The 'Team' dropdown is 'Global'. The 'Link service to a service template' radio button is selected and circled in red. The 'Link to template' dropdown is 'Workshop On Prem Database' and is circled in red. The 'Workshop On Prem Database Details' section shows '1 Entity Rules', '8 KPIs', and '0 services already linked to this template'. The 'Settings' section has the 'Enable 7 days of backfill for all service KPIs' checkbox checked and circled in red. The 'Create' button is circled in red. A red arrow points down from the right side of the dialog.

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.

On-Prem Database

Workshop On Prem Database

Entities

KPIs

Service Dependencies

Settings

Predictive Analytics

Entity Rules allow for the optional, dynamic filtering of KPIs and can help in root cause analysis. A service need not define any Entity Rules and is not limited to only the entities matching Entity Rules.

Entity Type

matches

*nix

Entity Title

matches

SLG_DC_1_MySQL

+ Add Rule (AND)

+ Add Set of Rules (OR)

Matched Entities

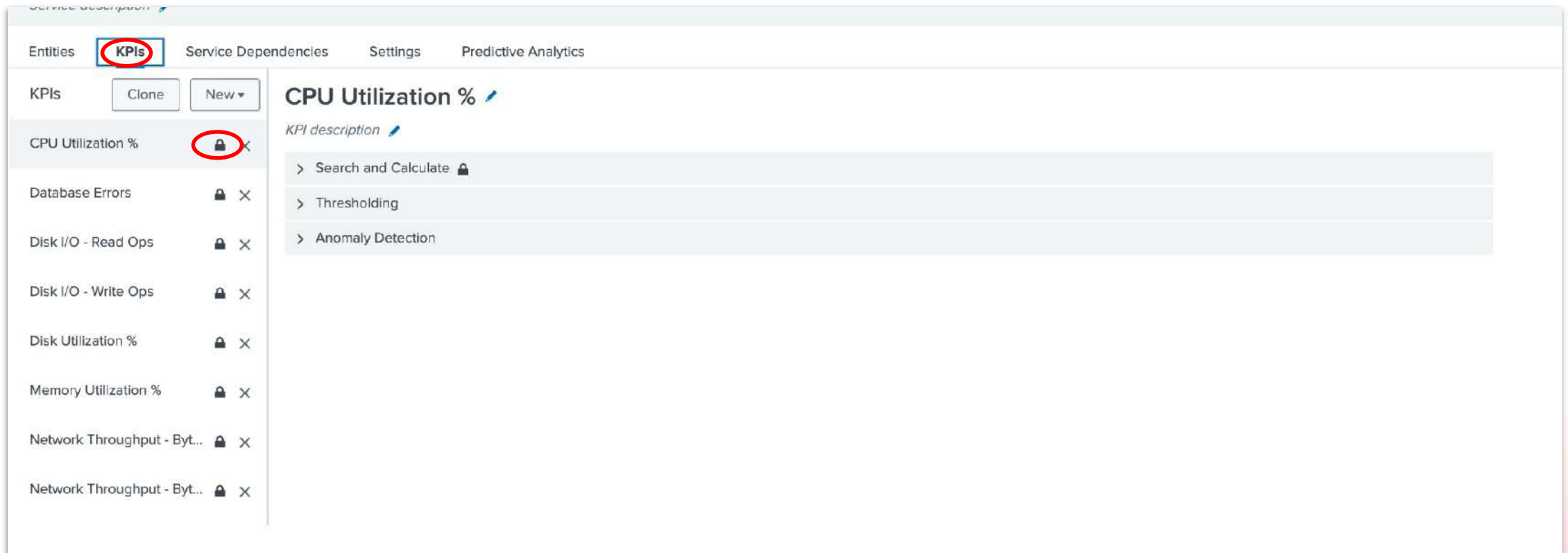
4 Entities

Title	Aliases	Info	Entity Types
SLG_DC_1_MySQL_01	slg_dc_1_mysql_01	10.1.2.101l, linux, '2.6.32-573.8.1.el6.x86_6...	*nix
SLG_DC_1_MySQL_02	slg_dc_1_mysql_02	10.1.2.102l, linux, '2.6.32-573.8.1.el6.x86_6...	*nix
SLG_DC_1_MySQL_03	slg_dc_1_mysql_03	10.1.2.103l, linux, '2.6.32-573.8.1.el6.x86_6...	*nix
SLG_DC_1_MySQL_04	slg_dc_1_mysql_04	10.1.2.104l, linux, '2.6.32-573.8.1.el6.x86_6...	*nix

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

The screenshot shows the 'Settings' tab for a service in the Splunk Services Lab. The 'General' section has a 'Status' toggle set to 'Enabled', which is circled in red. Below it, the 'Team' is set to 'Global' with a 'View Details' link. A warning message states: 'Changing a service's team may break service dependencies. Ask your Splunk administrator to review the logs after saving the change.' The 'Tags' field is empty. The 'Service Health Score' section has a 'Backfill' checkbox, which is crossed out with a large red 'X'. The 'Health Score Calculation' section has a note: 'Tweak the importance of each of the KPIs and see how that reflects on the simulated Service Health Score.' The 'On-Prem Database KPIs' section contains a table with columns for 'KPI Title', 'Simulated Severity', and 'Importance'. The table lists eight KPIs, all with 'Normal' severity. To the right of the table, a green box displays the 'Simulated Health Score' as 100. At the bottom right, there are 'Cancel' and 'Save' buttons, with the 'Save' button circled in red.

KPI Title	Simulated Severity	Importance
Database Errors	Normal	10
Database Queries	Normal	8
Disk I/O - Read Ops	Normal	2
Disk I/O - Write Ops	Normal	2
Disk Space Used %	Normal	10
Memory Used %	Normal	8
Network Throughput - Bytes In	Normal	2
Network Throughput - Bytes Out	Normal	2


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*

<input type="checkbox"/>	>	Course Picker DC 2	Edit ▾	<input checked="" type="checkbox"/> Enabled	Synced with Custom Demo Appserver	3	10	View Health	Global
<input type="checkbox"/>	>	Course Registration	Edit ▾	<input checked="" type="checkbox"/> Enabled	Not linked	0	0	View Health	Global
<input type="checkbox"/>	>	Course Registration DC 1	Edit ▾	<input checked="" type="checkbox"/> Enabled	Not linked	0	0	View Health	Global
<input type="checkbox"/>	>	Course Registration DC 2	Edit ▾	<input checked="" type="checkbox"/> Enabled	Not linked	0	0	View Health	Global
<input type="checkbox"/>	>	DMV Authentication DC 1	Edit ▾	<input checked="" type="checkbox"/> Enabled	Synced with Custom Demo Linux	1	7	View Health	Global
<input type="checkbox"/>	>	DMV Authentication DC 2	Edit ▾	<input checked="" type="checkbox"/> Enabled	Synced with Custom Demo Linux	1	7	View Health	Global

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

DMV Authentication DC 1 

Service description 

Entities

KPIs

Service Dependencies

Settings

Predictive Analytics

Remove selected dependencies

Add dependencies

Services Lab

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

Add dependencies

☐

Network Services

☐

Networking

☐

NTP

☒

On-Prem Database

☐

Order Management☐☐☐☐☐☐☐☐

<input type="checkbox"/>	KPI Title	Service Title
<input checked="" type="checkbox"/>	ServiceHealthScore	On-Prem Database
<input type="checkbox"/>	Database Queries	On-Prem Database
<input type="checkbox"/>	Disk I/O - Read Ops	On-Prem Database
<input type="checkbox"/>	Disk I/O- Write Ops	On-Prem Database
<input type="checkbox"/>	Disk Space Used %	On-Prem Database
<input type="checkbox"/>	Memory Used %	On-Prem Database
<input type="checkbox"/>	Network Throughput - Inbound	On-Prem Database
<input type="checkbox"/>	Network Throughput - Outbound	On-Prem Database

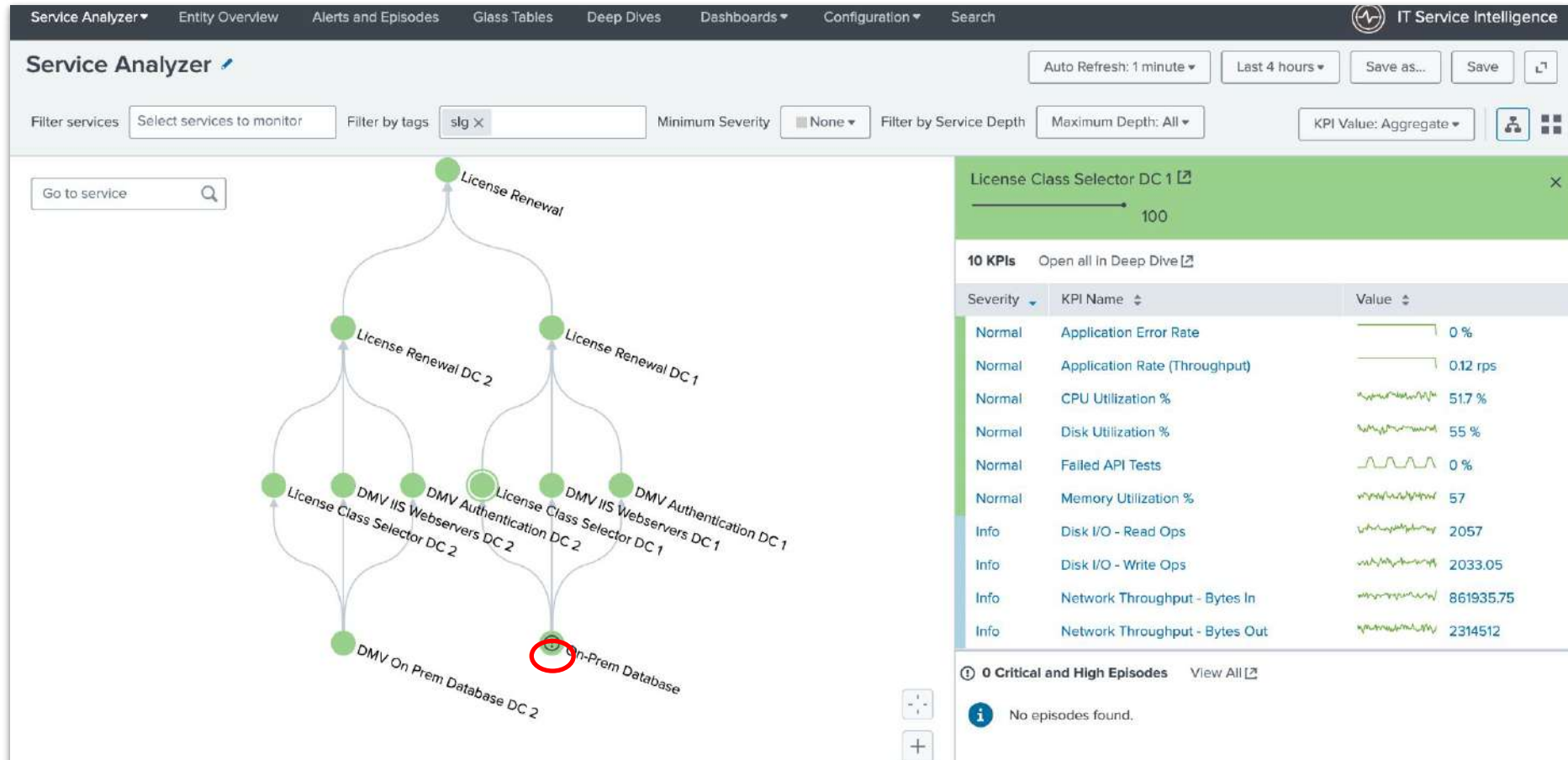
Cancel

Done

- 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.



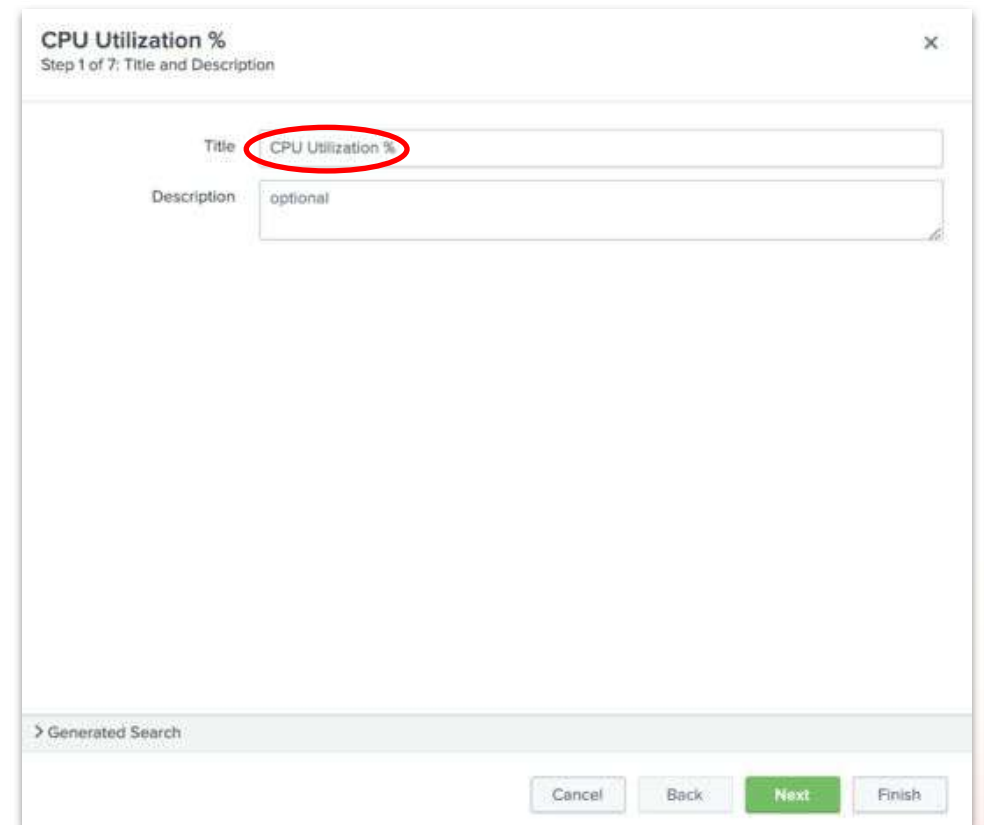
Note: The service health score may be grey until KPIs searches have executed.

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



The screenshot shows a dialog box titled 'CPU Utilization %' with the subtitle 'Step 1 of 7: Title and Description'. It contains two text input fields: 'Title' with the value 'CPU Utilization %' (circled in red) and 'Description' with the value 'optional'. At the bottom, there is a section labeled '> Generated Search' and four buttons: 'Cancel', 'Back', 'Next' (highlighted in green), and 'Finish'.

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 %'

CPU Utilization %
Step 2 of 7: Source

KPI Source ? Data Model Metrics Search Ad hoc Search **Base Search**

Base Search ? **Workshop Linux CPU Base Search**
[Edit Base Search](#)

Metric ? **CPU Utilization %**

> Generated Search

Cancel Back **Next** Finish

- Click the 'Next' button

KPI Lab

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

CPU Utilization %
Step 3 of 7: Entities

⚠ Fields are populated from the selected base search.

Split by Entity ? ☒ Yes ☐ No

Entity Split Field ?

Filter to Entities in Service ? ☒ Yes ☐ No
Service must have entities to filter by entities.

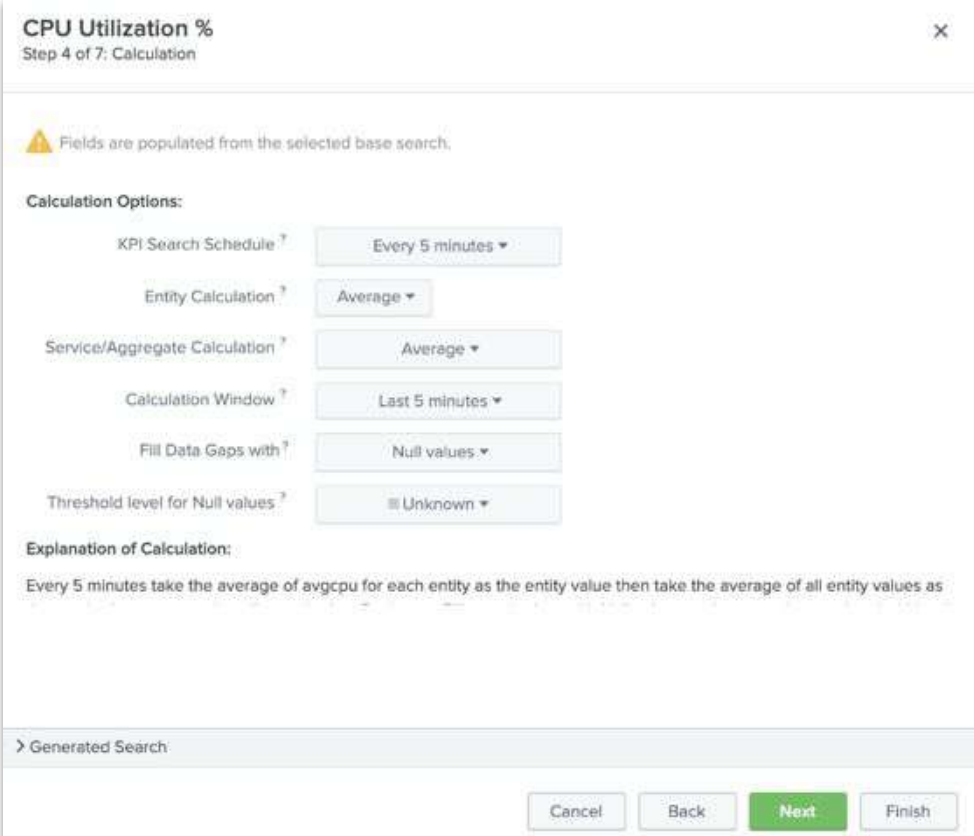
Entity Filter Field ?

> Generated Search

- Click the 'Next' button

KPI Lab

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



CPU Utilization %
Step 4 of 7: Calculation

⚠ Fields are populated from the selected base search.

Calculation Options:

KPI Search Schedule ?	Every 5 minutes ▼
Entity Calculation ?	Average ▼
Service/Aggregate Calculation ?	Average ▼
Calculation Window ?	Last 5 minutes ▼
Fill Data Gaps with ?	Null values ▼
Threshold level for Null values ?	Unknown ▼

Explanation of Calculation:
Every 5 minutes take the average of avgcpu for each entity as the entity value then take the average of all entity values as

> Generated Search

Cancel Back **Next** Finish

- Click the 'Next' button

KPI Lab

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

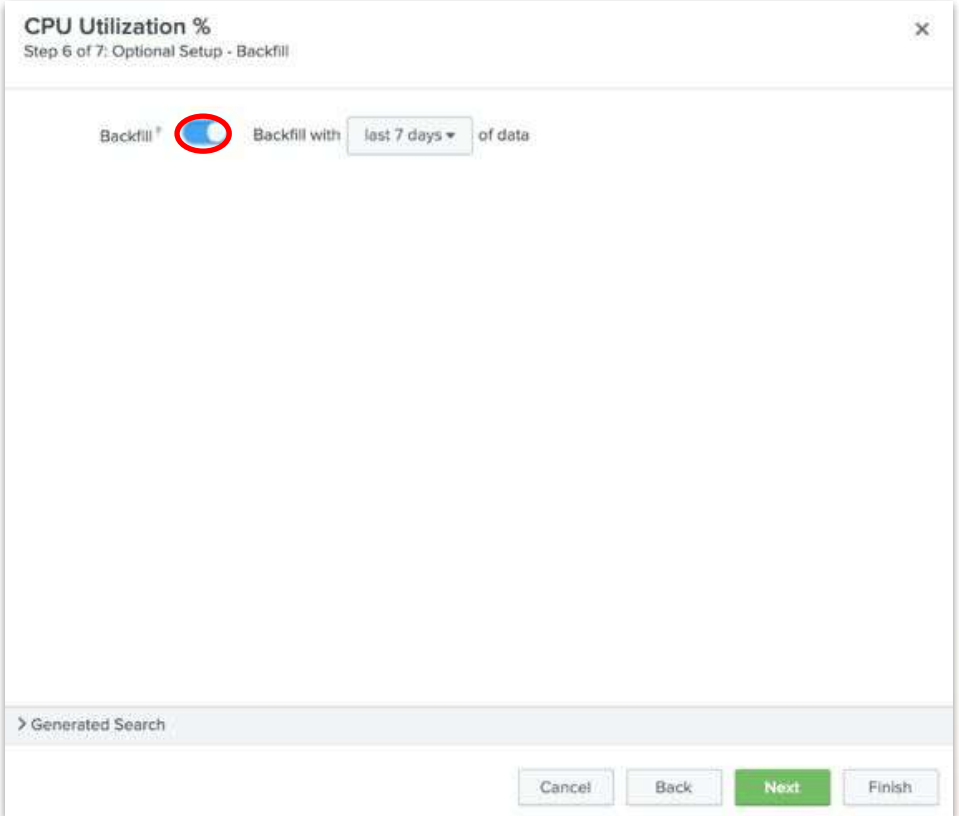
- Click the 'Next' button

The screenshot shows a configuration window titled "CPU Utilization %" with a subtitle "Step 5 of 7: Optional Setup - Unit and Monitoring Lag". A warning icon and text state: "Fields are populated from the selected base search." Below this, there are two input fields: "Unit" and "Monitoring Lag (in seconds)". The "Unit" field is empty, and the "Monitoring Lag" field contains the value "30". A link "Determine Recommended Lag" is visible next to the "Monitoring Lag" field. At the bottom of the window, there is a section labeled "Generated Search" and four buttons: "Cancel", "Back", "Next" (highlighted in green), and "Finish".

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



The screenshot shows the 'CPU Utilization %' configuration window in Splunk, specifically Step 6 of 7: Optional Setup - Backfill. The window has a title bar with a close button. Below the title bar, the text 'CPU Utilization %' is displayed, followed by 'Step 6 of 7: Optional Setup - Backfill'. The main content area shows a 'Backfill' toggle switch, which is currently turned on (blue) and is circled in red. To the right of the toggle, the text 'Backfill with' is followed by a dropdown menu showing 'last 7 days' and 'of data'. At the bottom of the window, there is a section labeled '> Generated Search' and four buttons: 'Cancel', 'Back', 'Next' (highlighted in green), and 'Finish'.

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 = 80
- Click 'Finish' button

CPU Utilisation %
Step 7 of 7: Thresholds

Aggregate Thresholds Per-Entity Thresholds

Aggregate Threshold Values


Critical ▼	90	×
High ▼	85	×
Medium ▼	80	×
Low ▼	70	×

+ Add Threshold

Base Severity

Normal ▼

View data from last 4 hours ▼



> Generated Search

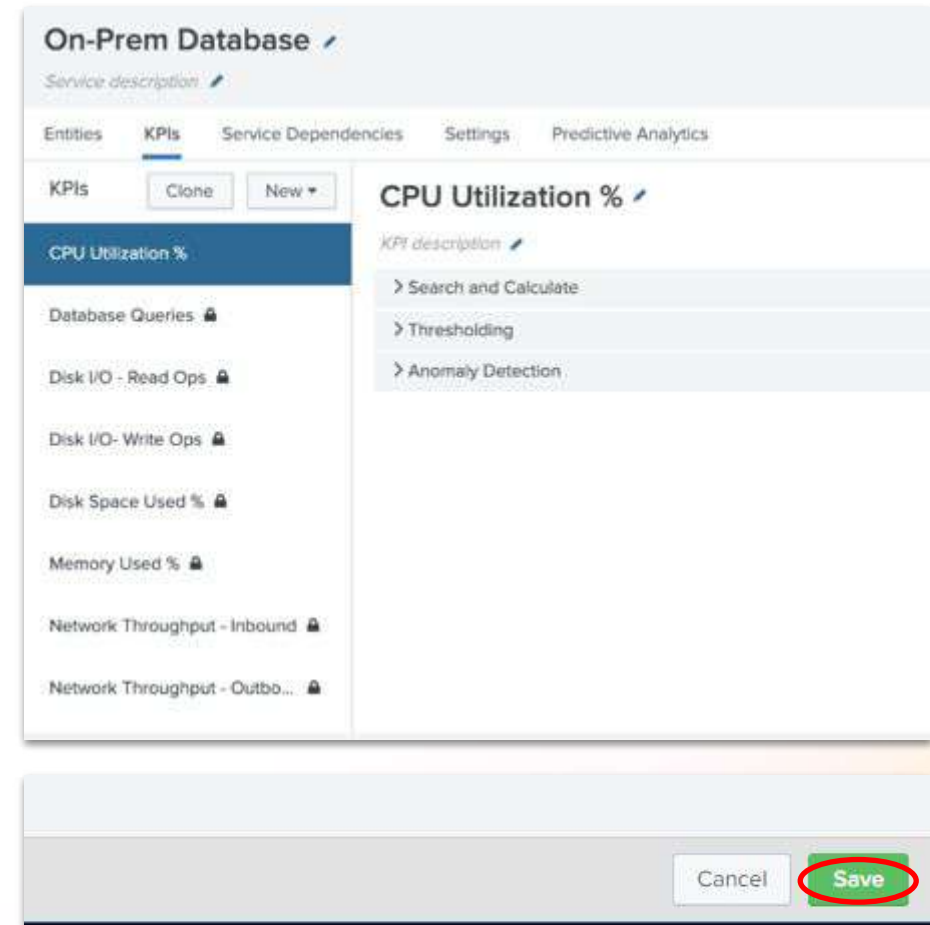
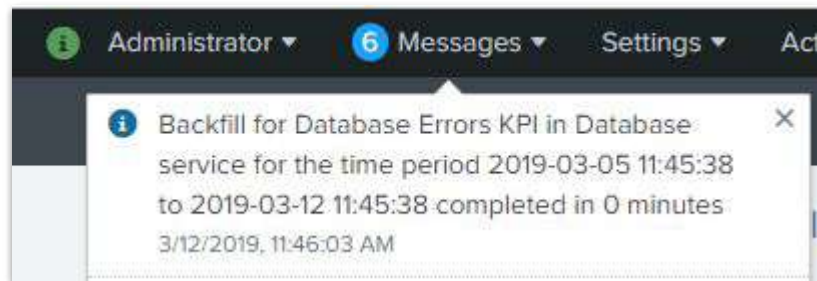
Cancel Back Next Finish

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

On-Prem Database

Service description

Entries KPIs Service Dependencies **Settings** Predictive Analytics

General

Status: Enabled

Team: Global View Details

Changing a service's team may break service dependencies. Ask your Splunk administrator to review the logs if after saving the change.

Service Health Score

Backfill: ☒ Off with last 7 days of data

It is advised that you first backfill the KPIs in this service and all dependent services for at least the time range selected here. Enabling backfill for a KPI does not mean backfill has completed. Wait for a successful backfill completion message for all KPIs before backfilling the service health score.

Health Score Calculation

Tweak the importance of each of the KPIs and see how that reflects on the simulated Service Health Score.

On-Prem Database KPIs

KPI Title	Simulated Severity	Importance
CPU Utilization %	Normal	10
Database Queries	Normal	10
Database Response Time	Normal	10
Disk I/O - Read Ops	Normal	10

Simulated Health Score

On-Prem Database

100

Cancel Save

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*'

The screenshot displays the Service Analyzer interface. On the left, a service tree shows a hierarchy starting from 'On-Prem Database' at the bottom, branching up through 'DMV On Prem Database DC 2', 'License Class Selector DC 2', 'DMV IIS Webservers DC 2', and 'License Renewal DC 2'. A red circle highlights the 'On-Prem Database' node. On the right, the 'On-Prem Database' service details are shown. A red rectangle highlights the 'Open all in Deep Dive' link. Below this, a table lists 8 KPIs with their names and values. At the bottom, a section titled '4 Critical and High Episodes' shows a list of incidents, with the first one highlighted in red.

Service Analyzer

Auto Refresh: 1 minute | Last 4 hours | Save as... | Save

Filter services: Select services to monitor | Filter by tags: slg x | Minimum Severity: None | Filter by Service Depth: Maximum Depth: All | KPI Value: Aggregate

Go to service

License Renewal DC 2 | License Renewal DC 1

DMV IIS Webservers DC 2 | License Class Selector DC 2 | DMV IIS Webservers DC 1 | DMV Authentication DC 1

DMV On Prem Database DC 2 | On-Prem Database

On-Prem Database

8 KPIs | Open all in Deep Dive

Severity	KPI Name	Value
Normal	CPU Utilization %	53.34 %
Normal	Database Errors	0
Normal	Disk Utilization %	12.63 %
Normal	Memory Utilization %	12.25
Info	Disk I/O - Read Ops	2069.24
Info	Disk I/O - Write Ops	2082.74
Info	Network Throughput - Bytes In	831686.5
Info	Network Throughput - Bytes Out	2138118.63

4 Critical and High Episodes | View All

Count	Title	Time	Owner	Status	Action
100+	Src: SLG_DC_1...	1/7/2025 4:07:33 PM - 1/8/2025 6:05:07	Unassigned	New	Acknowledge

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'

Lane Overlay Options

Enable Overlays: **Yes** (circled in red) | No

Overlay Type: Entity ▾

Graph Color: Automatic ▾

Overlay Selection Mode: Static | Dynamic

Selection	Entity Title	Alert Level	sparkline
<input checked="" type="checkbox"/>	mysql-01	Normal	
<input checked="" type="checkbox"/>	mysql-02	Normal	
<input checked="" type="checkbox"/>	mysql-03	Normal	
<input type="checkbox"/>	mysql-04	Normal	

Selected Entities

mysql-01	×
mysql-02	×
mysql-03	×

Buttons: Cancel | **Save** (circled in green)

Deep Dive Lab

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

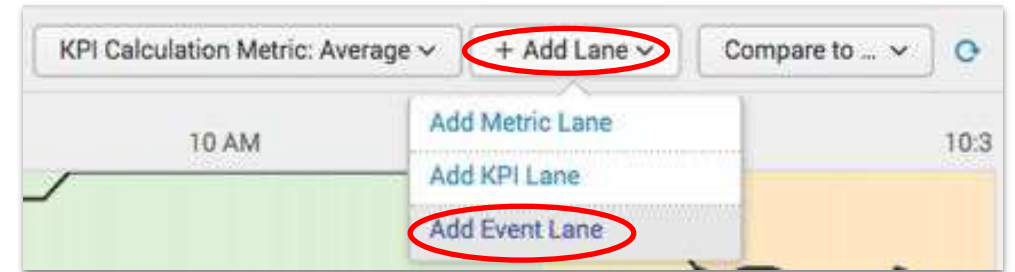
- Hover over the 'Disk Utilization %'
- We can see the individual entities performance right from this view.



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'

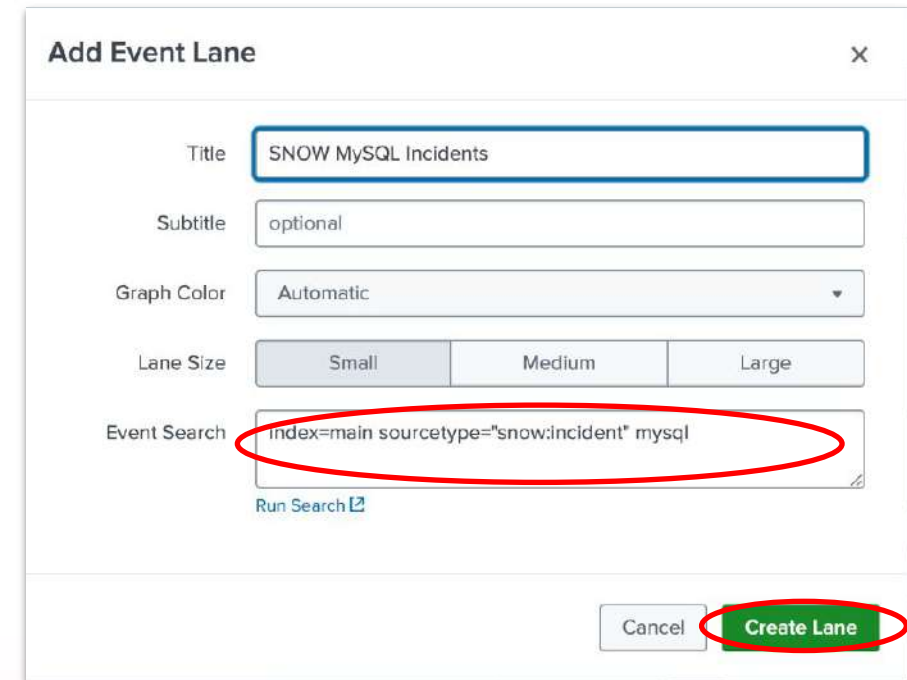
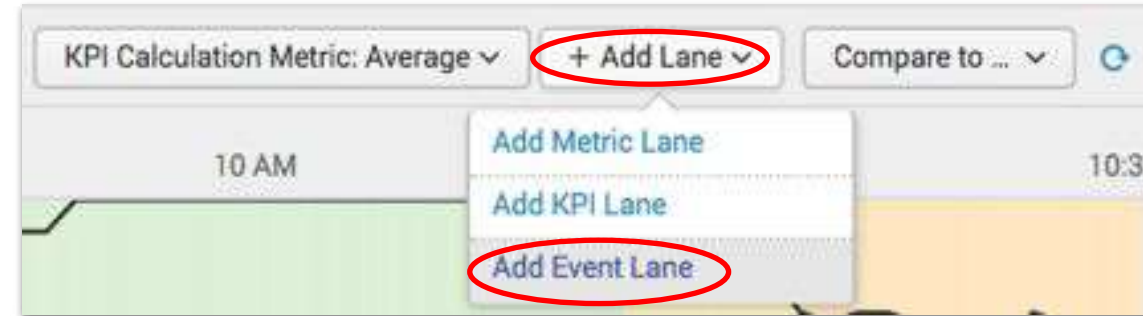


This screenshot shows the 'Add Event Lane' configuration dialog. It has a title field with 'Database Service Errors', a subtitle field with 'optional', a graph color dropdown set to 'Automatic', and three lane size buttons: 'Small' (selected), 'Medium', and 'Large'. The 'Event Search' field contains the query 'index=itsidemo mysql err*' and is circled in red. Below the search field is a 'Run Search' button. At the bottom right, there are 'Cancel' and 'Create Lane' buttons, with the latter circled in red.

Deep Dive Lab

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

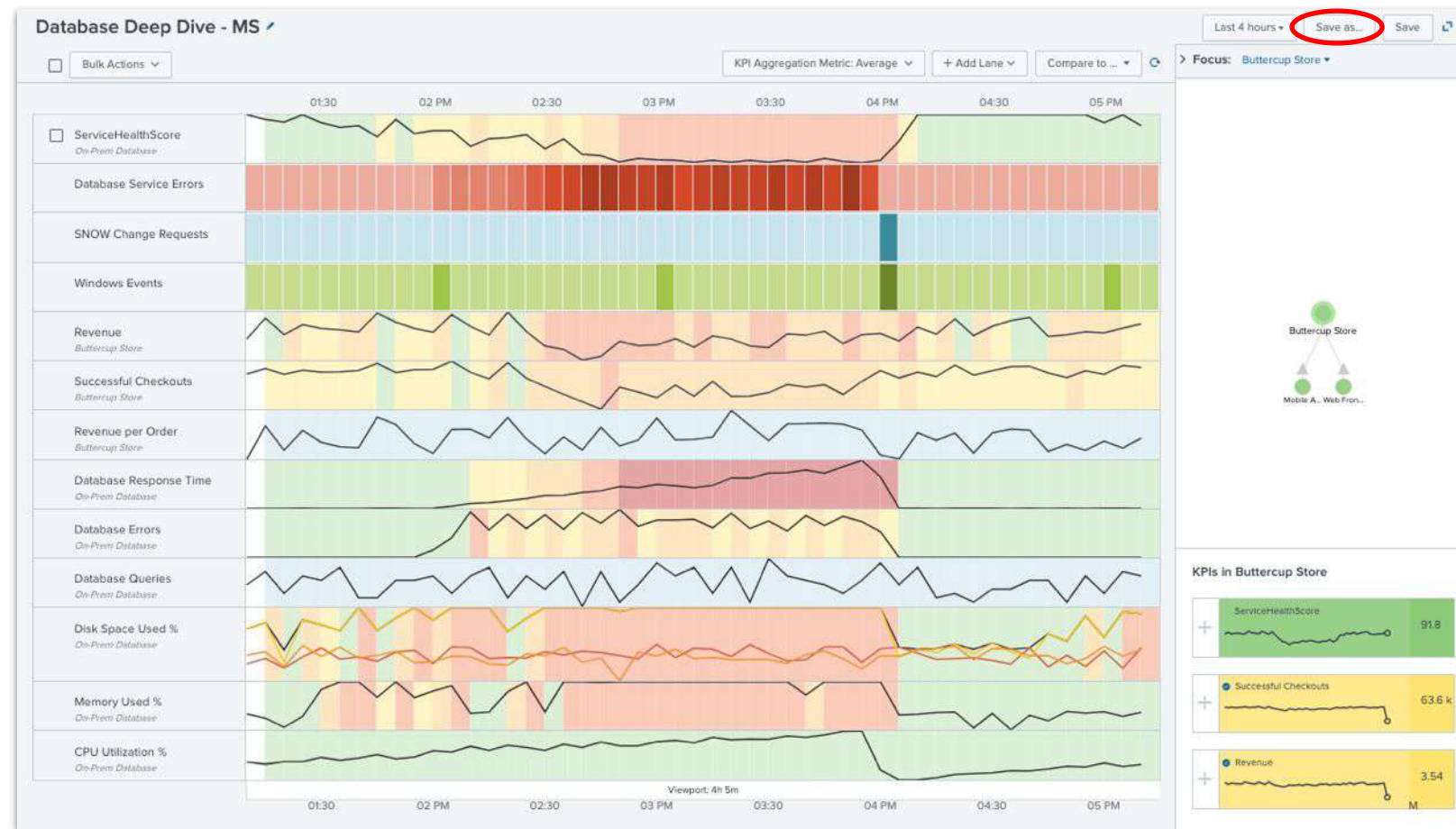
- Select 'Add Lane'
- Click 'Add Event Lane'
- Type 'SNOW MySQL Incidents' as the Title
- Event Search:
 - *'index=main sourcetype="snow:incident" mysql*
- Click 'Create Lane'

A screenshot of the 'Add Event Lane' configuration dialog. The dialog has a title bar 'Add Event Lane' with a close button. It contains several fields: 'Title' with the value 'SNOW MySQL Incidents', 'Subtitle' with the value 'optional', 'Graph Color' with a dropdown set to 'Automatic', 'Lane Size' with three buttons 'Small', 'Medium', and 'Large', and 'Event Search' with the value 'index=main sourcetype="snow:incident" mysql' circled in red. Below the 'Event Search' field is a 'Run Search' link. At the bottom right, there are 'Cancel' and 'Create Lane' buttons, with the latter circled in red.

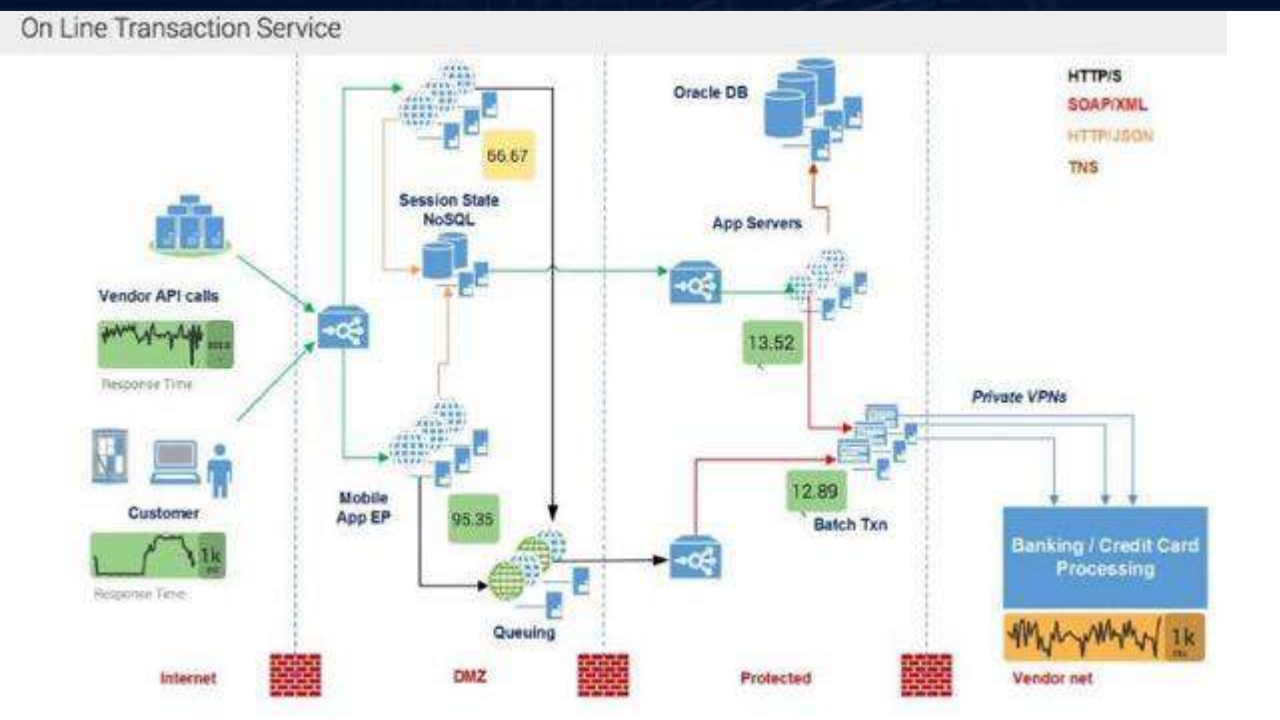
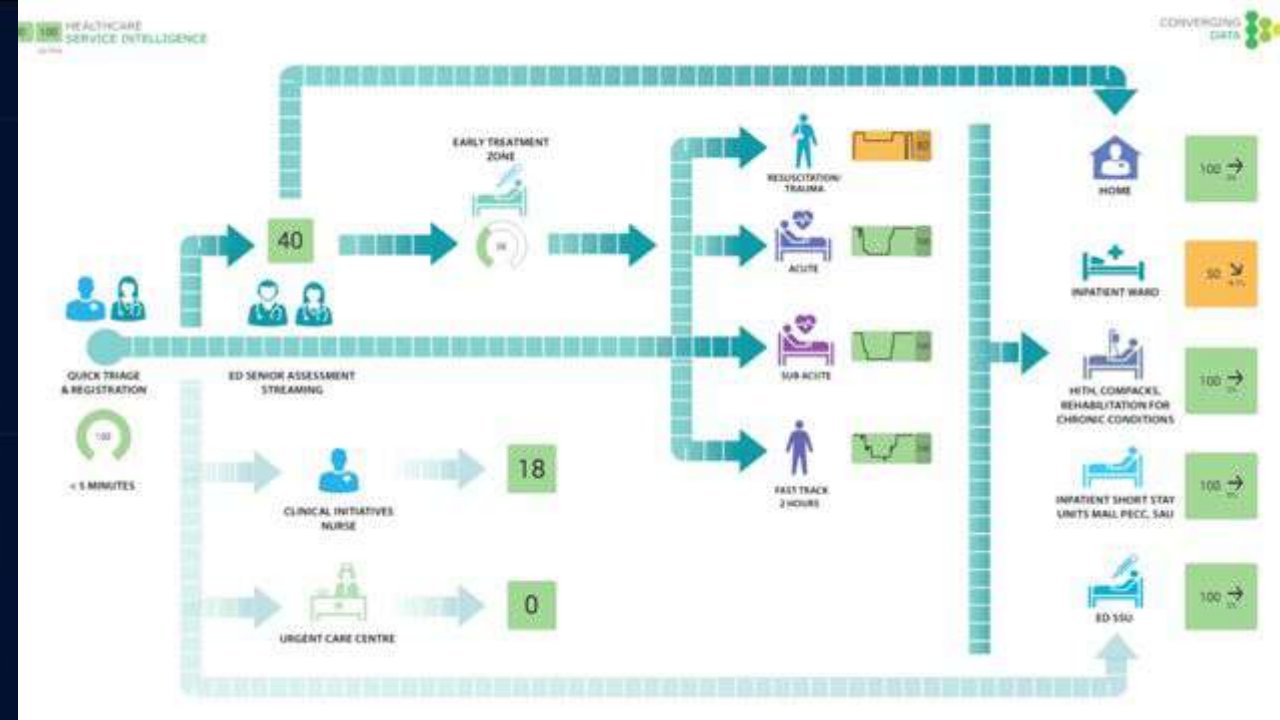
Deep Dive Lab

Once you have finished investigating the Deep Dive dashboard

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



Glass Tables

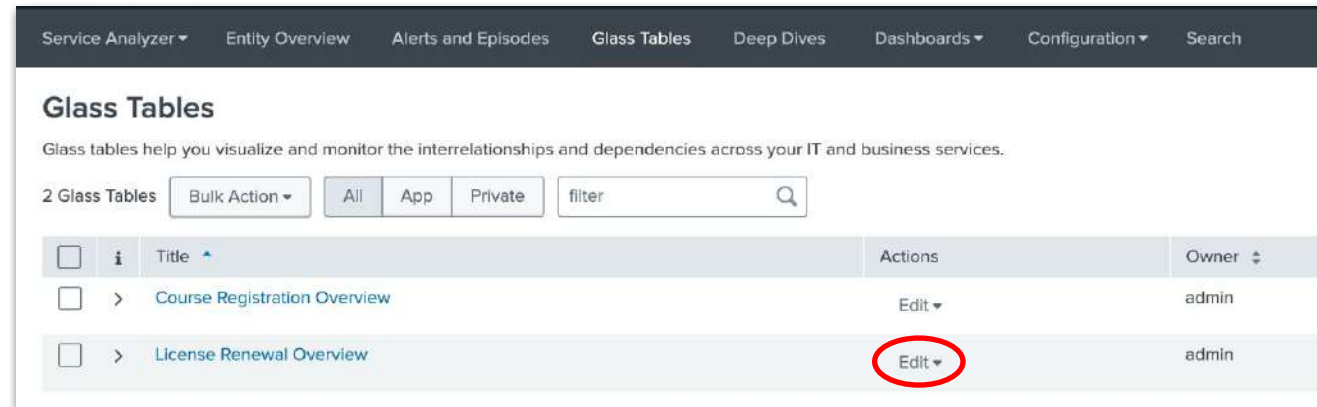


Glass Table Use Case

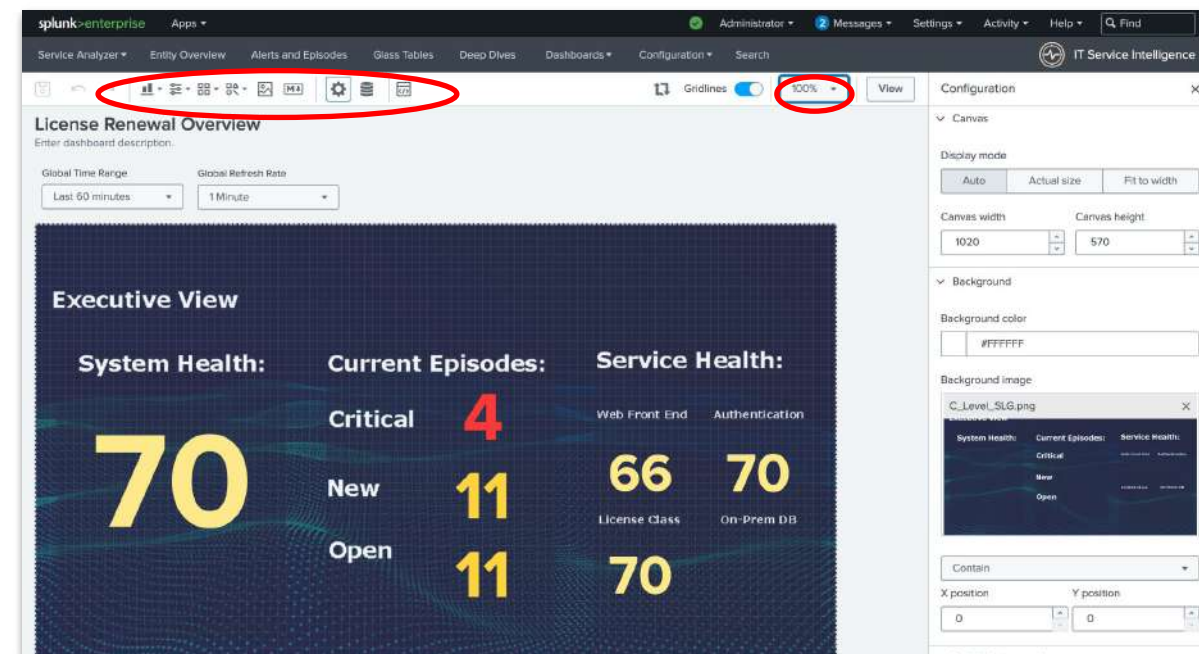
- The DMV leaders would like a high-level dashboard showing the key functions and services of the organisation.
- The objective of this exercise is to complete the existing IT operations dashboard (License Renewal Overview) with the new On-Prem Database service health score, including a drill down to a deep dive.

Glass Table Lab

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

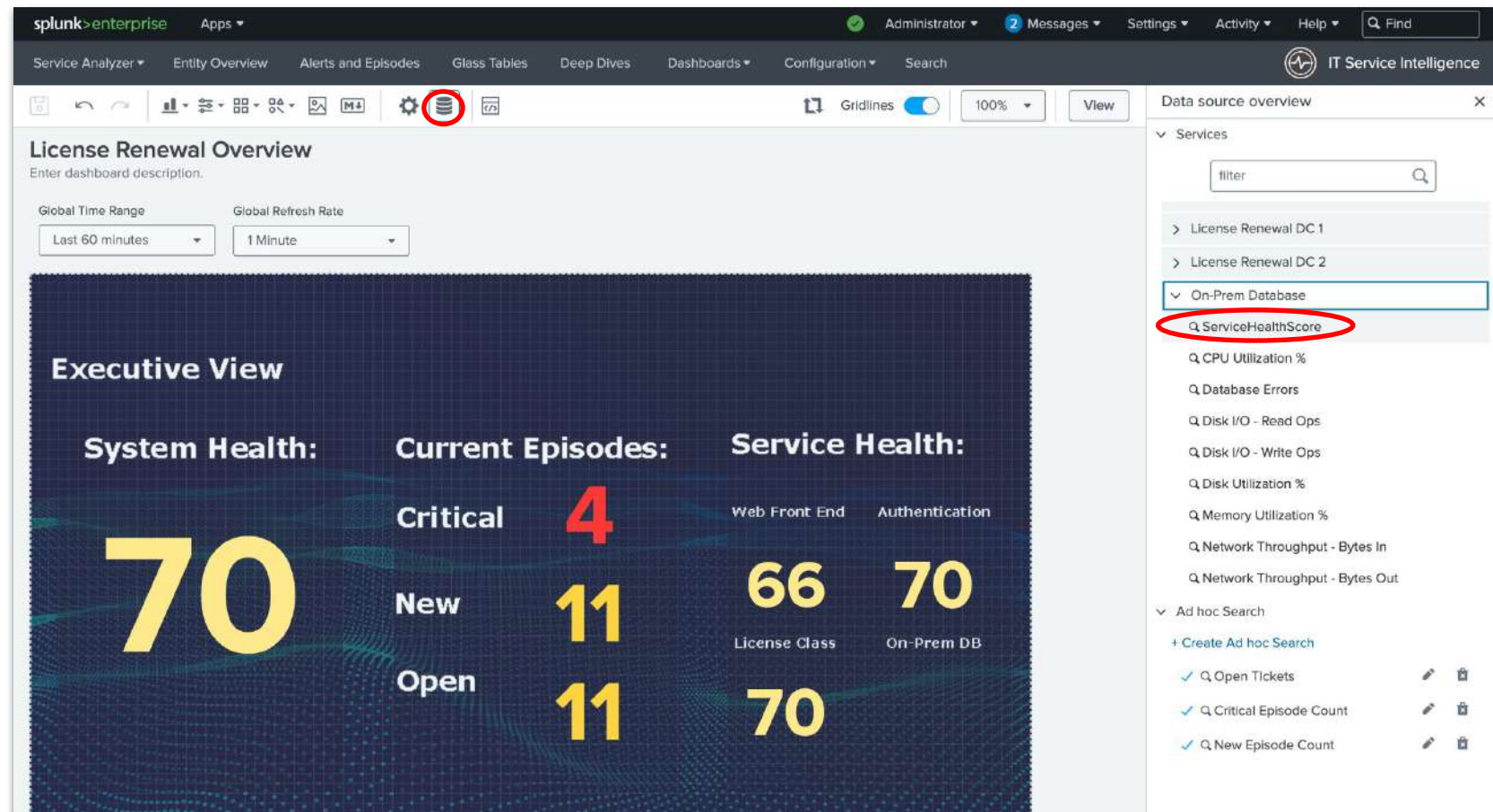


- Investigate the tool palette icons
- Modify zoom to fit to page
- Review the Configuration panel on right



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

The screenshot displays the Splunk Service Analyzer interface. The main dashboard, titled "License Renewal Overview", features an "Executive View" with a dark blue background and a grid pattern. It contains three main sections: "System Health" with a large yellow "70", "Current Episodes" with "Critical 4", "New 11", and "Open 11", and "Service Health" with "Web Front End 66", "Authentication 70", "License Class 70", and "On-Prem DB 67". The "On-Prem DB" score is highlighted with a white box and a blue border. To the right, the "Configuration" panel is open, showing settings for the "On-Prem Database - ServiceHealthSc..." data source. The "Position and size" section has four input fields: "X position" (860), "Y position" (390), "Width" (120), and "Height" (120), all of which are circled in red. The "Visualization type" is set to "Single Value".

Service Analyzer ▾ Entity Overview Alerts and Episodes Glass Tables Deep Dives Dashboards ▾ Configuration ▾ Search

IT Service Intelligence

License Renewal Overview
Enter dashboard description.

Global Time Range: Last 60 minutes ▾ Global Refresh Rate: 1 Minute ▾

Executive View

System Health:	Current Episodes:	Service Health:	
70	Critical	4	Web Front End
	New	11	66
	Open	11	Authentication
			70
		License Class	70
		On-Prem DB	67

Configuration

Visualization type: Single Value ▾

Title:

Description:

Data sources: On-Prem Database - ServiceHealthSc...

Position and size

X position: 860 Y position: 390

Width: 120 Height: 120

> Data configurations

> Data display

Color and style

Dynamic elements: Select... ▾

Glass Table Lab

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

The screenshot displays the Splunk Glass Table Lab interface. The main dashboard, titled "License Renewal Overview", features an "Executive View" with three KPIs: "System Health: 100", "Current Episodes: 4 Critical, 11 New, 9 Open", and "Service Health: 100". The "Service Health" KPI is further detailed with "Web Front End: 100", "Authentication: 100", "License Class: 100", and "On-Prem DB: 100". A configuration panel on the right is open, showing settings for the selected KPI. The "Color and style" section is expanded, and the "transparent" option is selected for the background color. The "transparent" option is also selected for the "Dynamic elements" dropdown. The "Major value size (px)" and "Trend value size (px)" are both set to "Auto".

Service Analyzer Entity Overview Alerts and Episodes Glass Tables Deep Dives Dashboards Configuration Search

IT Service Intelligence

Gridlines 100% View

License Renewal Overview

Enter dashboard description.

Global Time Range: Last 60 minutes Global Refresh Rate: 1 Minute

Executive View

System Health: 100

Current Episodes: Critical 4 New 11 Open 9

Service Health: 100

Web Front End: 100 Authentication: 100

License Class: 100 On-Prem DB: 100

Configuration

Width: 120 Height: 120

Data configurations

Data display

Color and style

Dynamic elements

transparent

Major value size (px): Auto Trend value size (px): Auto

Interactions

Source code

Glass Table Lab

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

- Click Add Drilldown

The screenshot shows the Splunk Glass Table configuration interface for a dashboard titled "License Renewal Overview". The main visualization area displays an "Executive View" with three columns: "System Health", "Current Episodes", and "Service Health".

System Health:	Current Episodes:	Service Health:	
100	Critical	4	Web Front End
	New	11	Authentication
	Open	4	100
		License Class	On-Prem DB
		100	100

The right sidebar contains the "Configuration" panel with various settings. The "Interactions" section at the bottom has a red circle around the "+ Add Interaction" button.

Glass Table Lab

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

The screenshot shows the Splunk IT Service Intelligence (ITSI) Glass Tables interface. The main panel displays the 'License Renewal Overview' dashboard with an 'Executive View' section. The 'Executive View' section contains three columns of data: 'System Health' (100), 'Current Episodes' (Critical: 4, New: 11, Open: 4), and 'Service Health' (Web Front End: 100, Authentication: 100, License Class: 100, On-Prem DB: 100). The right sidebar is open to the 'Configuration' panel. In this panel, the 'On click' dropdown is set to 'Deep Dive'. Below it, the 'Deep Dives' section shows a list of saved deep dives, with 'Database Deep Dive SGSW' selected. At the bottom of the configuration panel, the 'Apply' button is highlighted.

Service Analyzer ▾ Entity Overview Alerts and Episodes Glass Tables Deep Dives Dashboards ▾ Configuration ▾ Search

IT Service Intelligence

License Renewal Overview

Enter dashboard description.

Global Time Range: Last 60 minutes ▾ Global Refresh Rate: 1 Minute ▾

Executive View

System Health:	Current Episodes:	Service Health:	
100	Critical	4	Web Front End
	New	11	Authentication
	Open	4	License Class
			On-Prem DB
		100	100
		100	100

Configuration

On click: Deep Dive ▾

Deep Dives: Database Deep Dive SGSW ▾

Select deep dive: ☐ Open in new tab

Cancel Apply

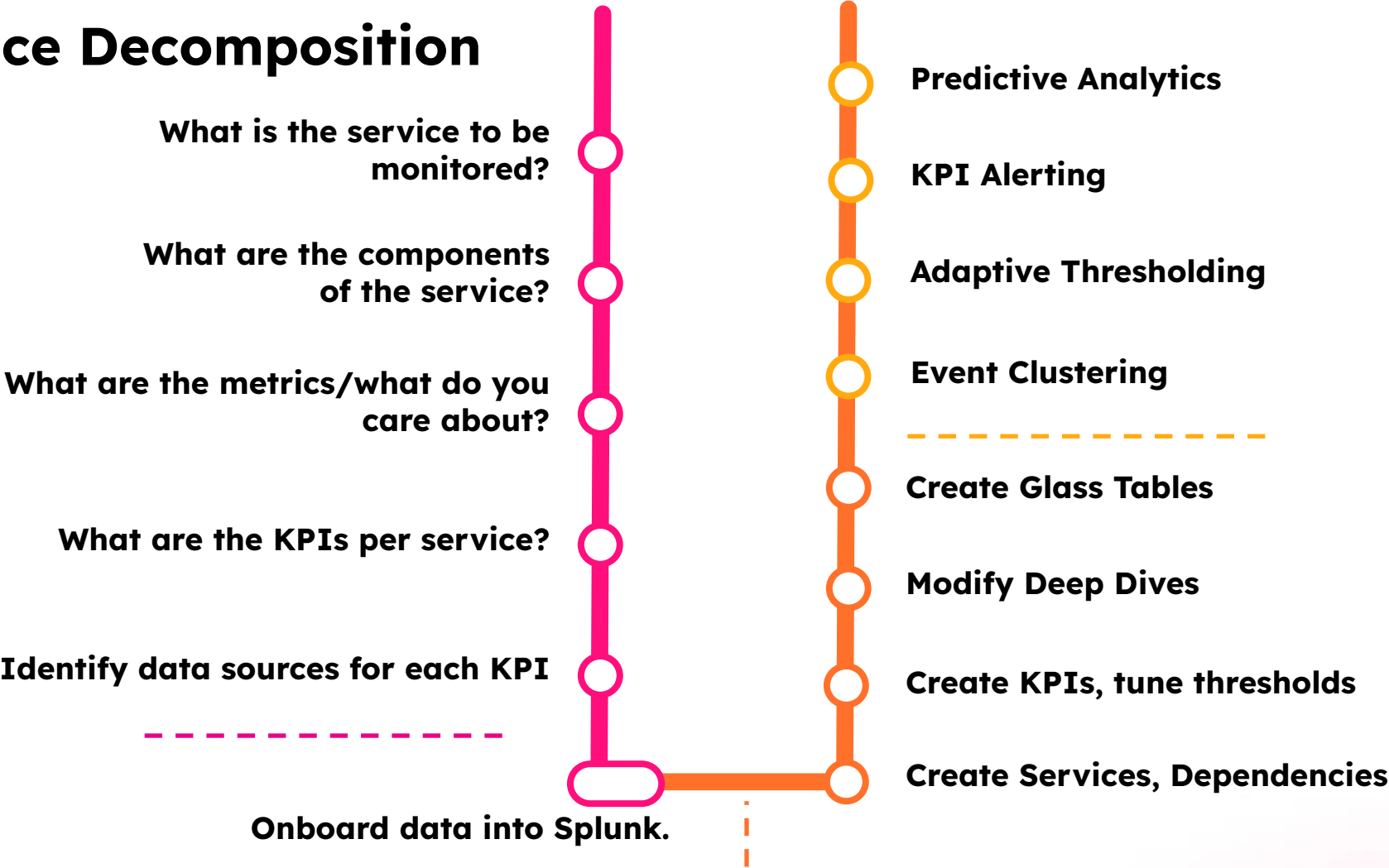


Next Steps

Service Decomposition Workshop

Implementation Methodology

Service Decomposition



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