Welcome we will get started shortly

Splunk IT服务智能(ITSI)在线实操研讨会

徐世文

Sr. Sales Engineer

Agenda

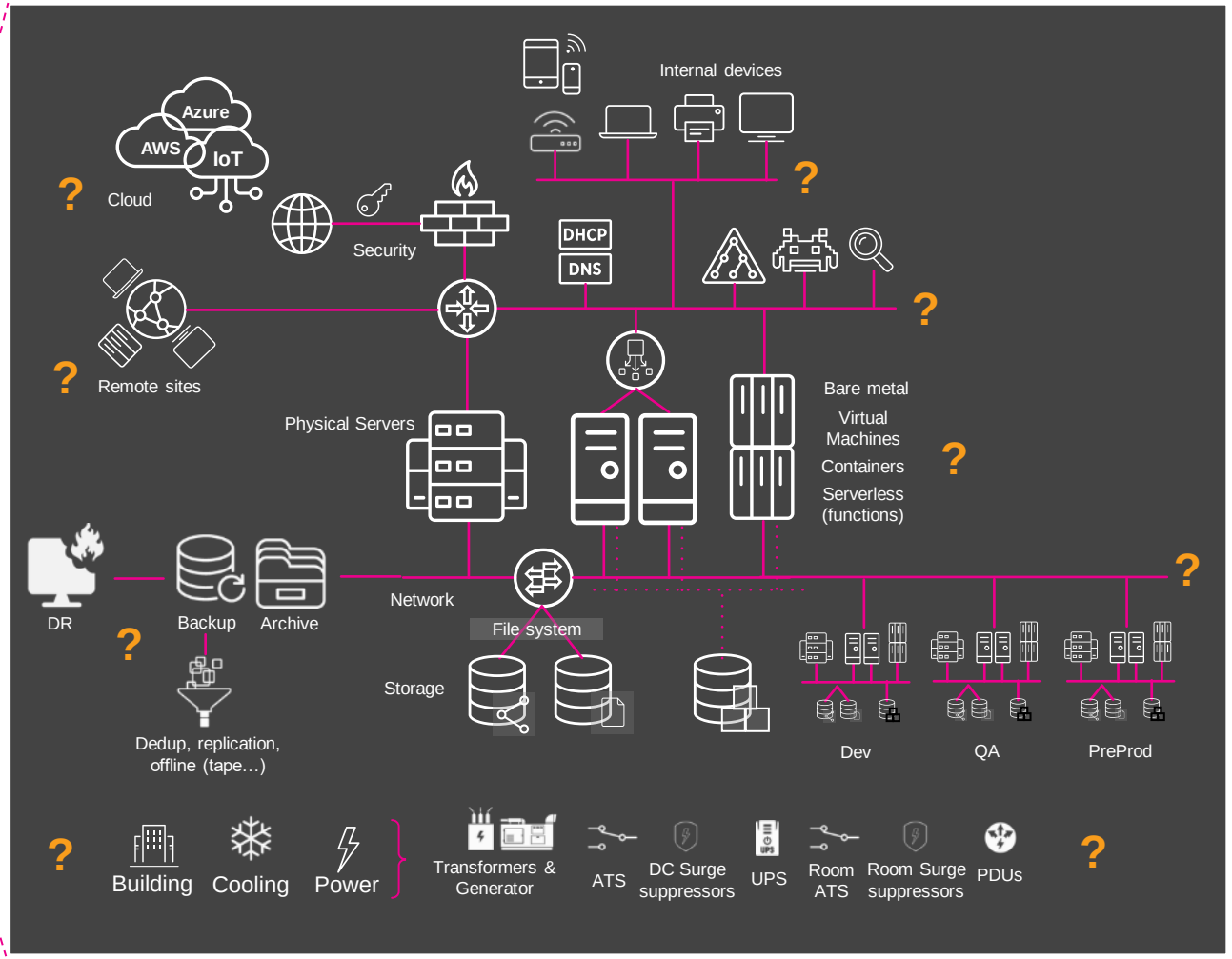
- Problem Statement
- IT Service Intelligence Overview
- Service Creation
- KPIs Creation
- Deep Dives
- Glass Tables
- Machine Learning
- Event Analytics
- Next Steps

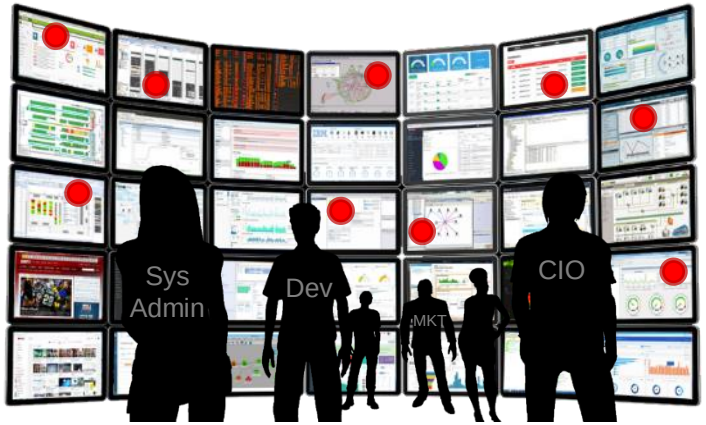
IT Service Intelligence

当出现问题时...

快速找到和修复问题，并确定正确的优先事项对于业务至关重要

- DEV/APPS
- CLOUD
- OFFICE
- DR
- REMOTE
- SECURITY
- STORAGE
- NETWORK
- SERVERS
- BUILDING





臃肿的产品和各类工具

数据孤岛

告警噪音&事件超负荷

很难快速定位根因

对企业影响甚巨

Putting revenue, customer experience, employee effectiveness & innovation at risk

营收损失

Outages and incidents impact the services and apps driving revenues

客户体验糟糕

Customers click away and brand reputation is damaged

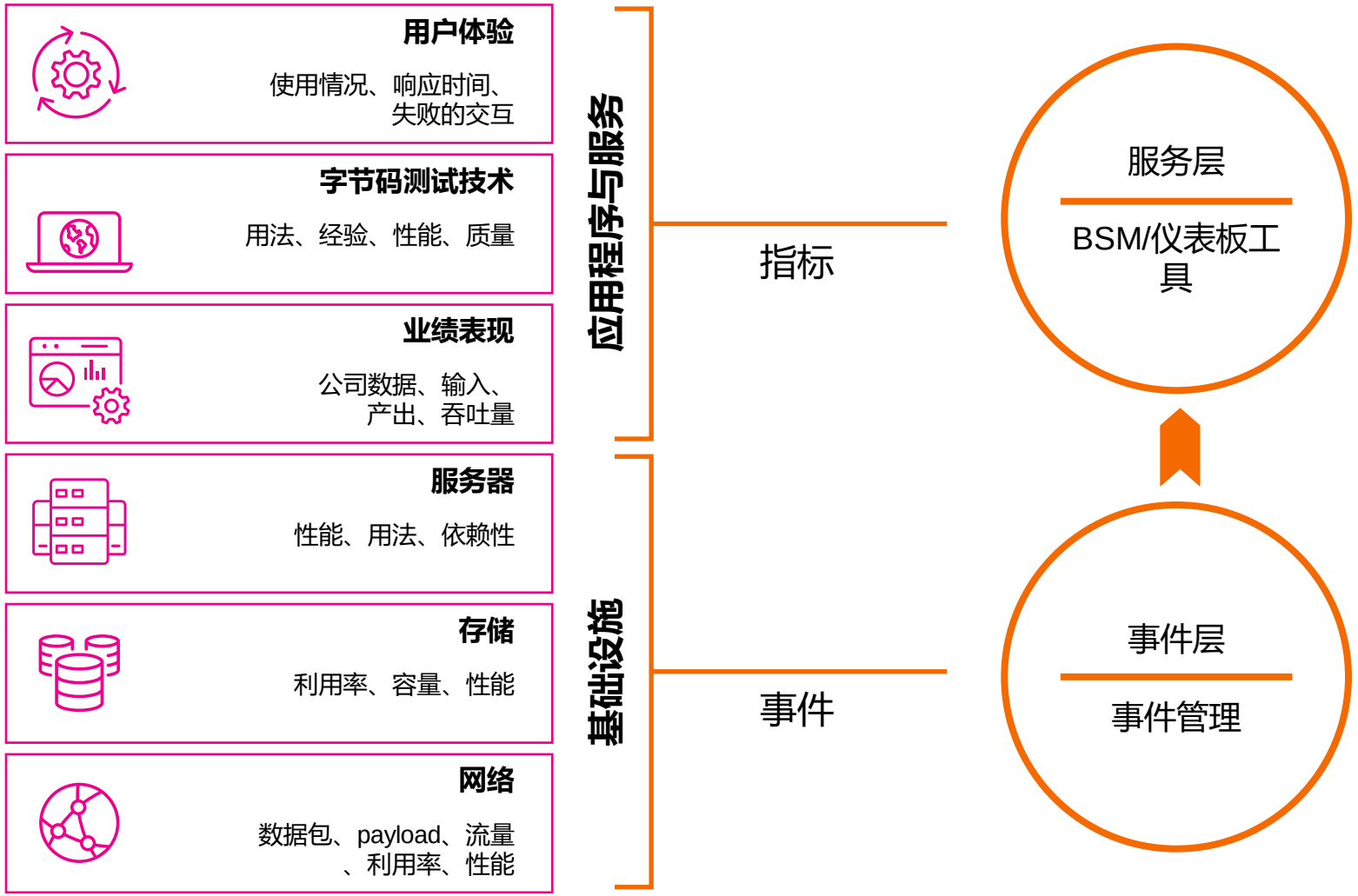
员工效率降低

Teams thrash, finger-point, and key employees leave

难以创新

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

传统IT管理整合方式



挑战

- 许多不同的组件
- 一体化不够成熟
- 数据汇总丢失
- 根本原因定位时间更长
- 端到端视图挑战
- 劳动密集型的管理
- 对数字化业务不够敏感

利用ITSI解决已知的和潜在的问题

用户体验

使用情况、响应时间、失败的交互

字节码测试技术

用法、经验、性能、质量

业绩表现

公司数据、输入、产出、吞吐量

服务器

性能、用法、依赖性

存储

利用率、容量、性能

网络

数据包、payload、流量、利用率、性能

应用程序与服务

基础设施

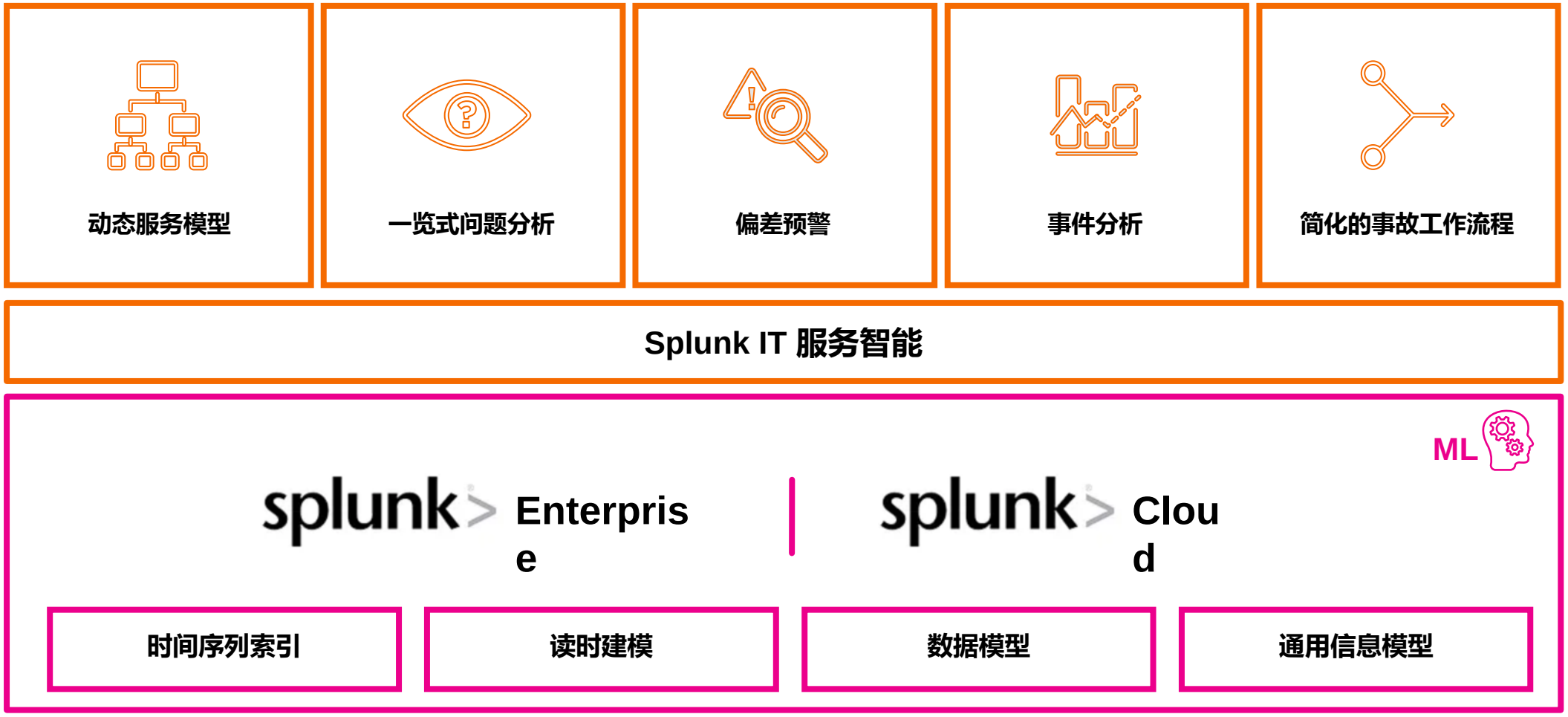
机器数据

Splunk方法:

- 任何类型和数量数据的统一平台
- 完整的原始数据
- 结合机器学习
- 简化的架构
- 更少的管理资源
- 协作方式

Splunk IT服务智能

数据驱动的服务监控和分析

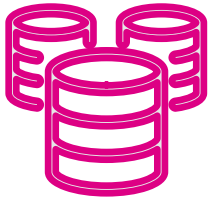


Key Terminology

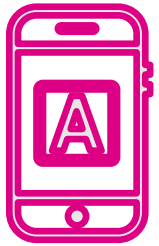
What is a Service

用户认为需要一起监控的一组逻辑技术组件。
服务可以包含IT域的多个层。

Online Store Service

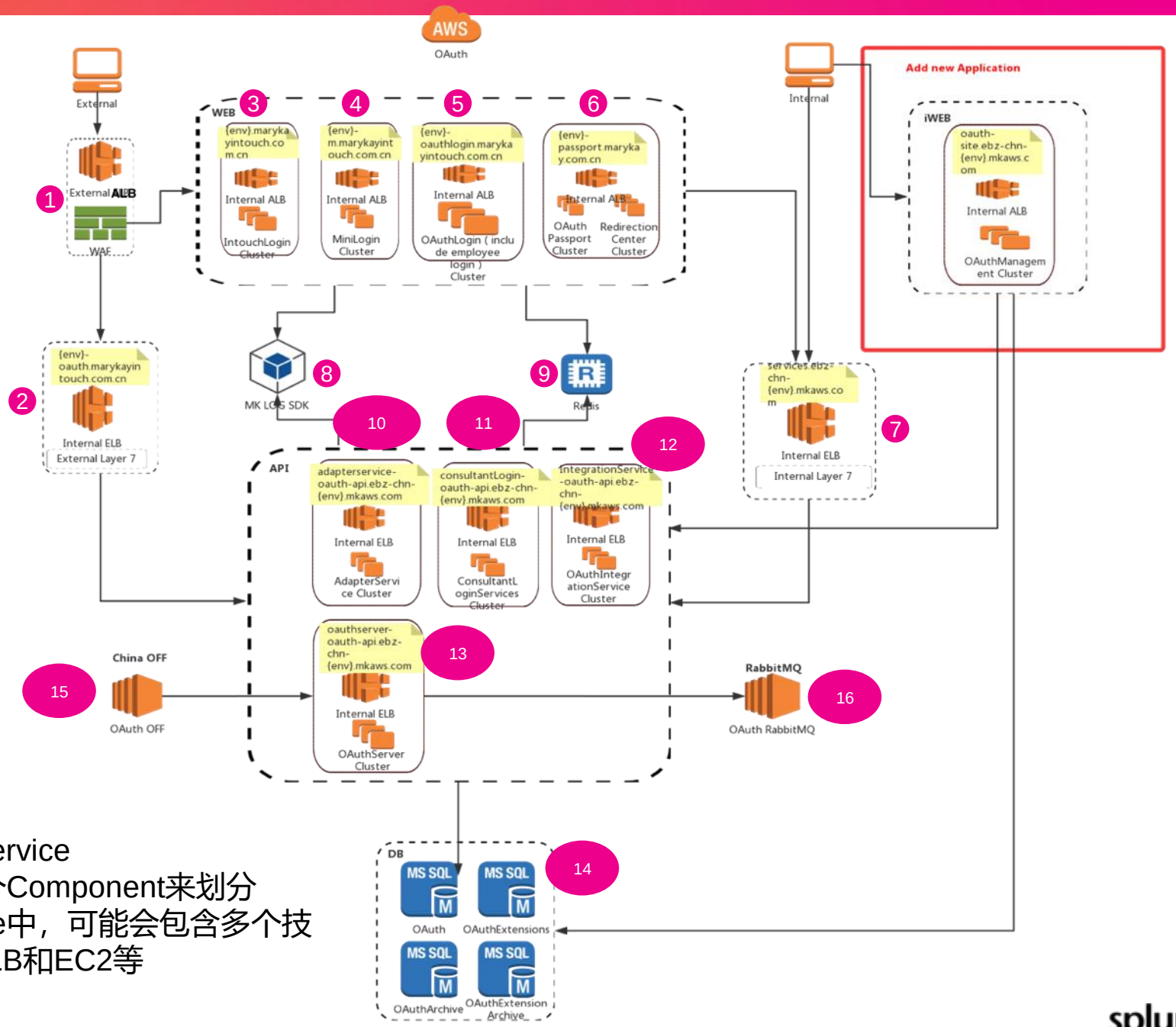


Database Service



Mobile App Service

Call Centre Service



- ●代表一个Service
- Service按一个Component来划分
- 在一个Service中，可能会包含多个技术组件，如ELB和EC2等

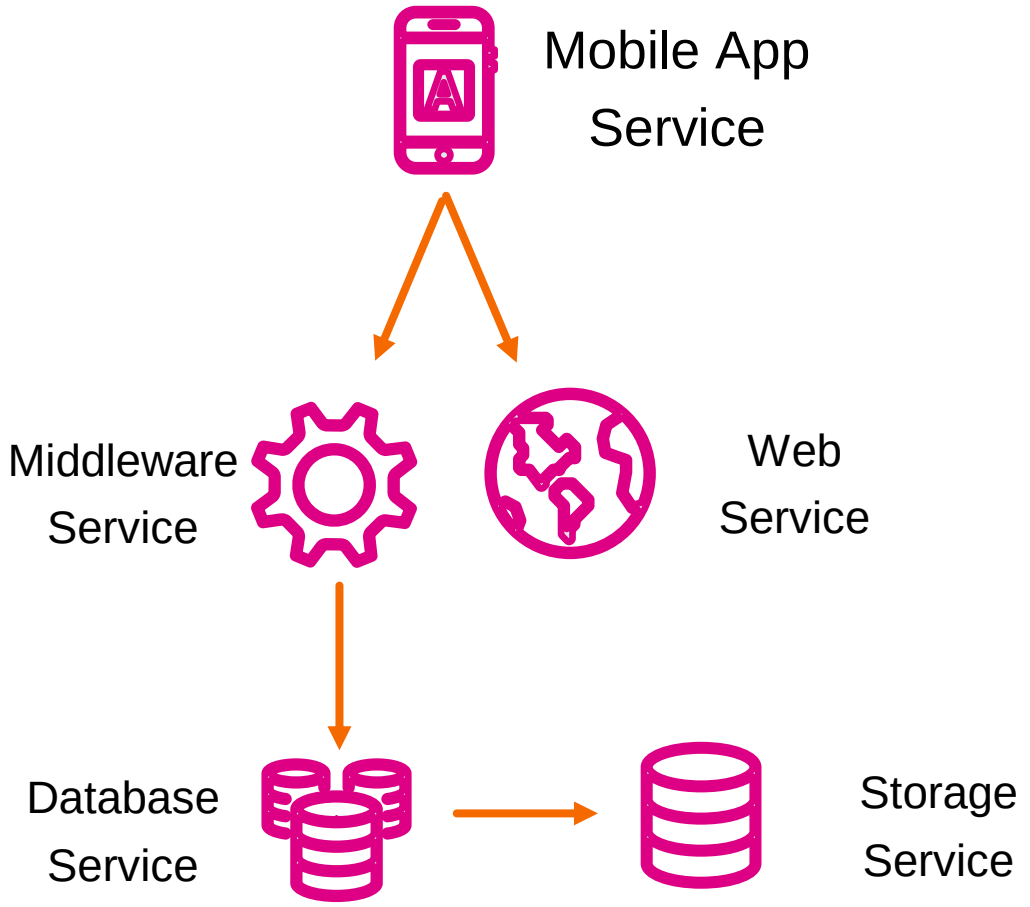
服务可能还依赖其它服务

服务可以是技术服务，还可以是更高层次—业务服务。

Business Services

Application Services

Technical Services

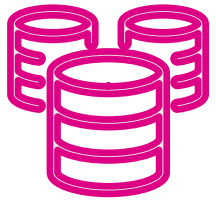


What is a KPI

KPI是ITSI中创建的保存搜索，它可以帮助监控特定值，例如CPU、内存、错误数量等，KPI包含在服务当中。

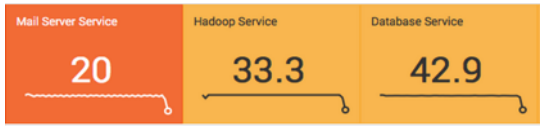
Online Store Service

- Number of visitors
- Revenue
- Transactions per day



Database Service

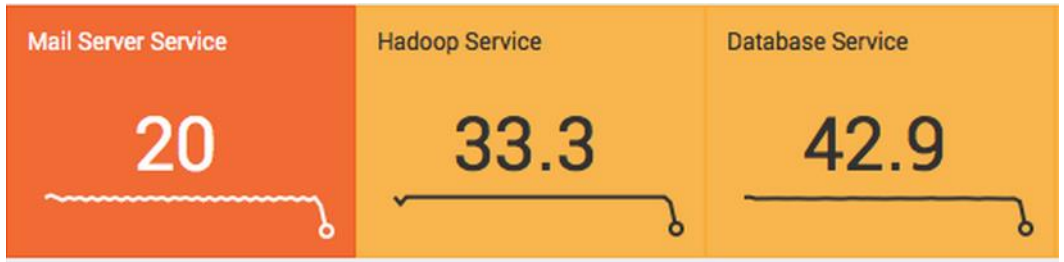
- CPU Utilisation
- Query Response Time
- Storage Free Space



splunk> turn data into doing

What is a Health Score

健康评分用于帮助诊断服务的健康程度，其值从0-100（0表示严重，100表示健康）。该值基于所有的指标的重要性和相关状态（例如绿色、橙色、红色）计算得出。



KPI和健康度评分构成服务监控的手段

What is an Entity

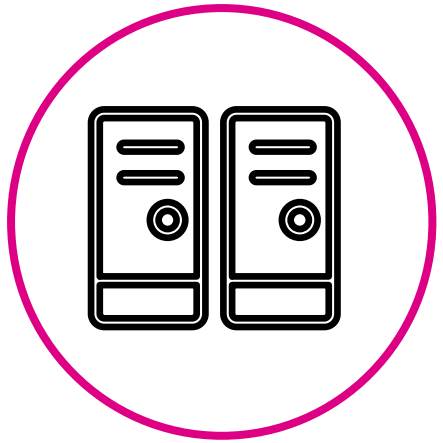
实体可以是一台服务器，或负载均衡设备，防火墙等企业资产，它们所产生的日志、指标数据等被发送到Splunk。
KPI可以通过实体进行筛选，ITSI可以从CMDB或其他来源导入实体

Severity	Entity Name	Value
Critical	mysql-02	0 %
Normal	mysql-01	33.26 %
Normal	mysql-03	30.7 %
Normal	mysql-04	28.05 %

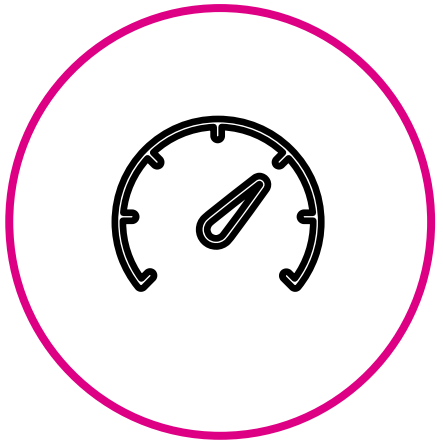
ITSI Service Definition

概况而言，一项服务包括:

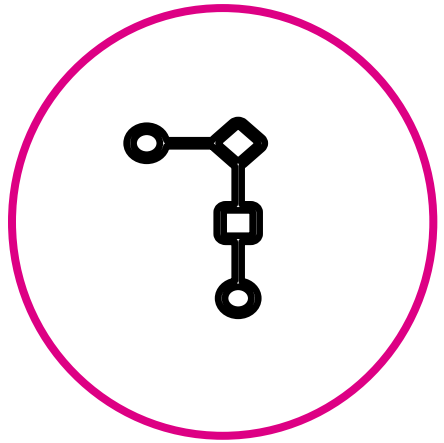
A Service Health Score



0 or More Entities



0 or More KPIs



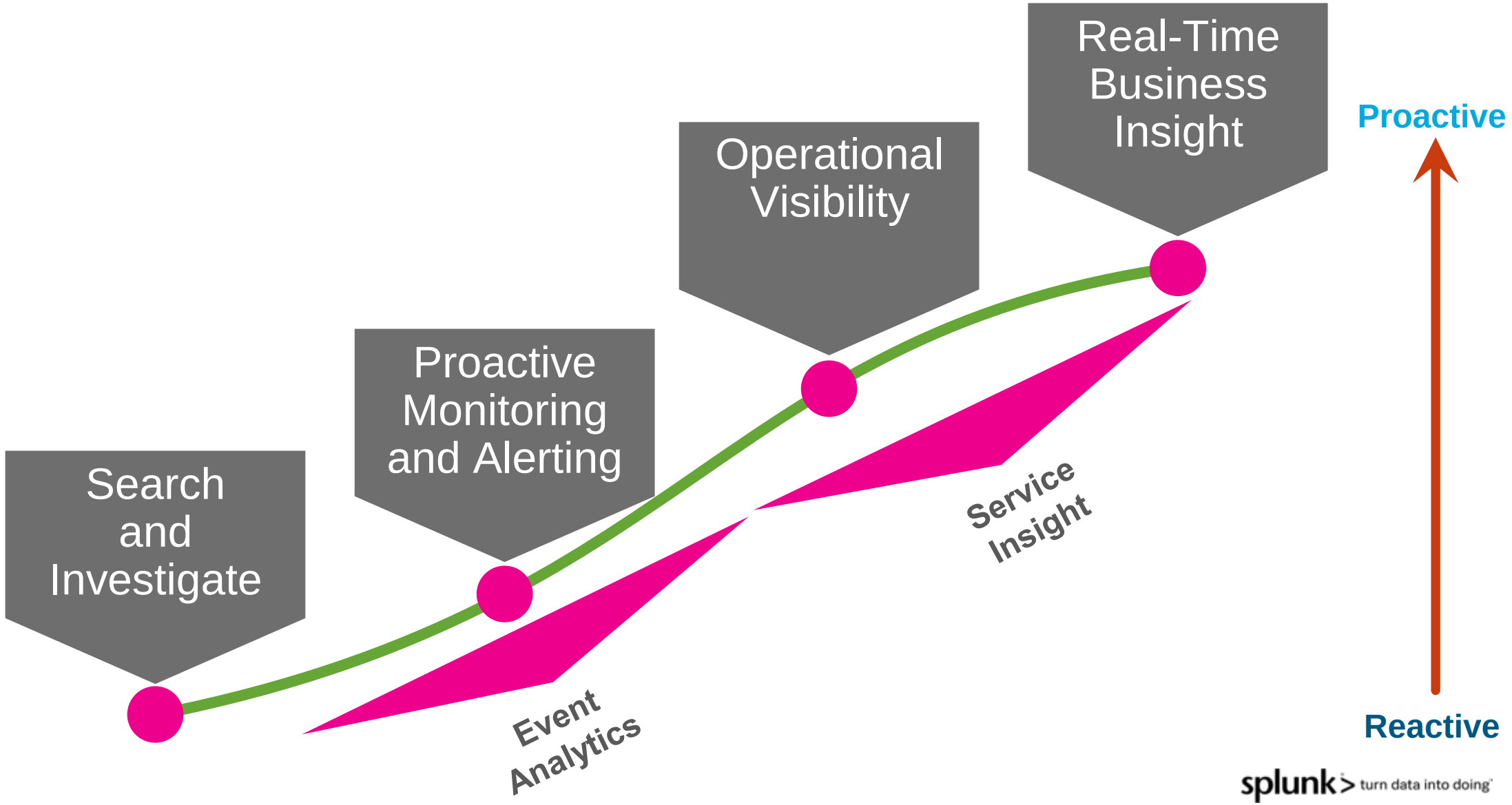
0 or More Dependencies

ITSI Key Terminology

逻辑上组合 在一起的模块	为完成 某个商业目标 聚合在一起的 一组行为	承载服务的 组件	用于评估健康状态 的评分系统
举例	举例	举例	举例
资金受托管理应用， 用户验证系统， 核心业务系统	账户开立， 资格申请， 信息维护&管理	主机，用户， 操作系统	服务健康度， 订单处理成功， 系统延迟
服务 **Service**	**业务流程** **Business Process**	**实体** **Entities**	**关键性能指标** **KPI**

Tips

IT Operations Splunk Journey



ITSI discovery steps

- 发掘并确认客户核心的、关心的high-level 业务服务
- 尝试找到其中最具高可见性、高价值的服务以及依赖关系树（业务流程、承载关系、上下游依赖关系等）
- 针对上述梳理出的服务，定义出黄金KPI，阈值等
- 从KPI确定具体数据源，字段，实时性等

ITSI deep dive

- 首要理解服务的总体任务、目标、现状等
- 先从上往下，然后从下往上验证。尽量保持更低的cost，如数据复用，使用已有工具，降低存储；减少风险，如更可治理、可控、可见性；驱动营收，更快的获得洞察，能持续改进。
- 在白板上画下来，开始工作后给让客户业务专家、相关团队参与进来
- 一次只关注一个层级（one layer），重点讨论每一层级的常见问题和指标(KPI)，不要跳来跳去的
- 服务分解可能是跨部门的工作，需要一个主导发起人
- 如果客户之间出现了分歧，让他们去解决吧——坐下来，放松
- 如果跨不同部门或团队，避免出现“他说了什么”，“什么意思”，让所有的相关人员都参与进来
- 找不到客户合适的业务服务，或没有业务owner的buy-in，请谨慎！

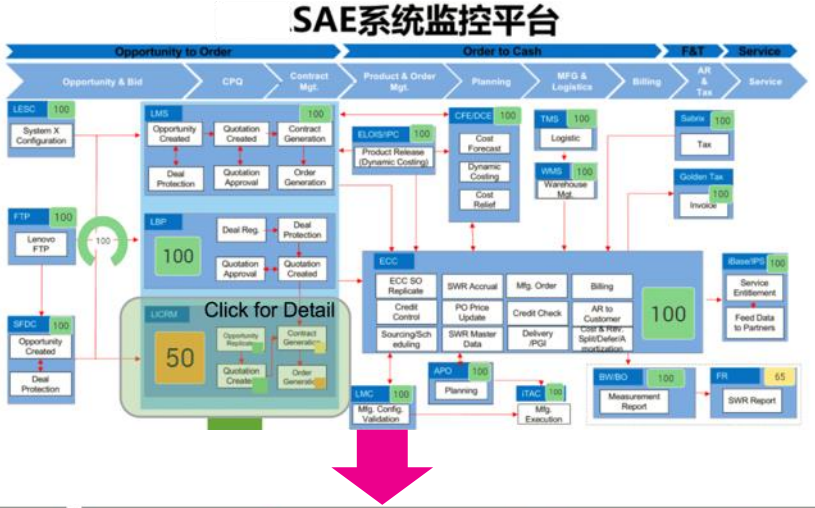
请尽量避免

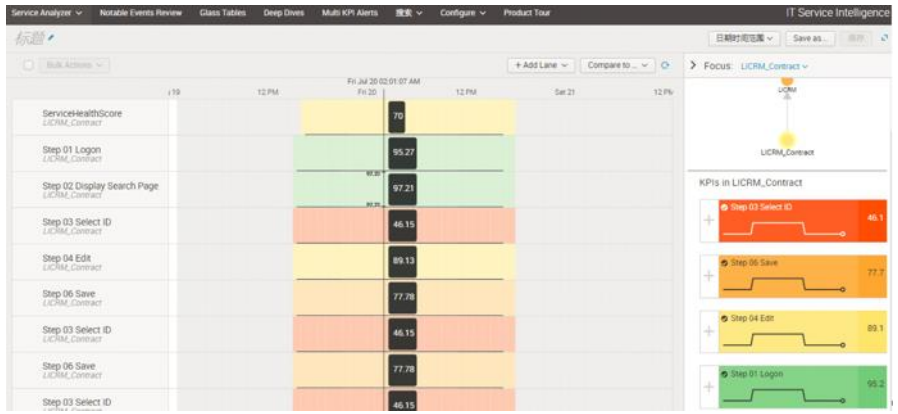
- 倾向于只选择低层次的技术服务（ low-level, technical services）
  - …这对上层管理人员来说可能不是很明显/很有价值
- 只选择传统的（或现有工具现成）KPI
  - 常规KPI: CPU使用量、内存使用量、磁盘使用量…
- 选择在Splunk中没有数据的服务
  - 服务基于KPI, KPI基于Splunk搜索
  - 没有数据就意味着没有KPI，也就意味着没有服务…从0开始会大大增加POC周期，降低客户预期

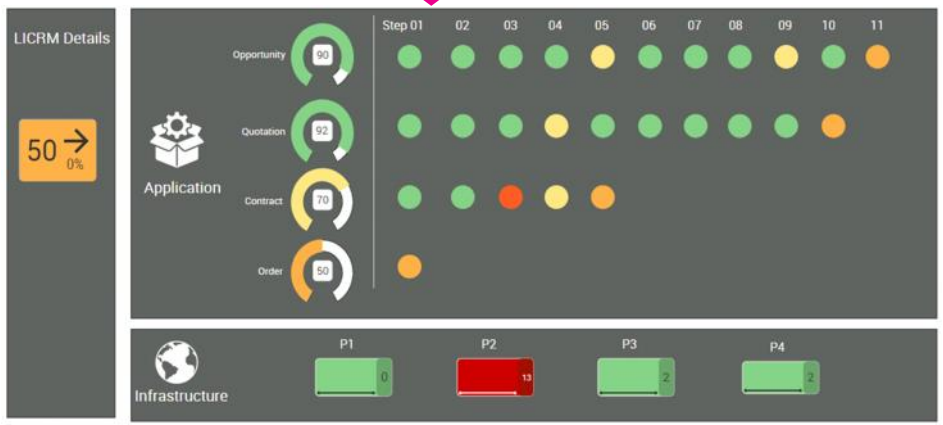
Glass Tables

Glass Tables:

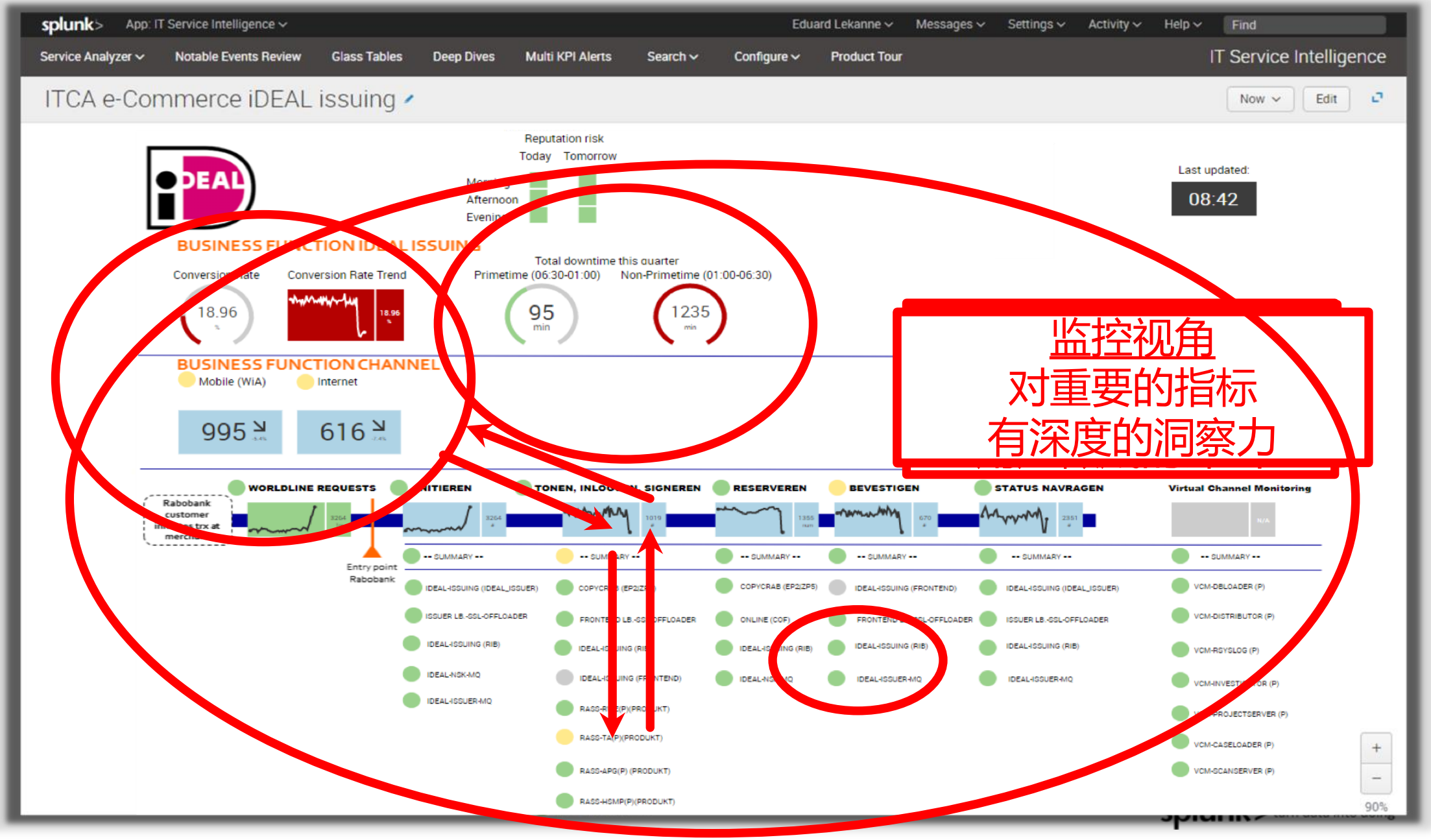
- High-level 业务GT -> 详图GT -> deep dive
- 小部件（ITSI widget）链接到其他仪表板和第三方工具，并非完全替换客户现有的工具或已有内容







splunk> turn data into doing



Workshop Back Story

Workshop Back Story

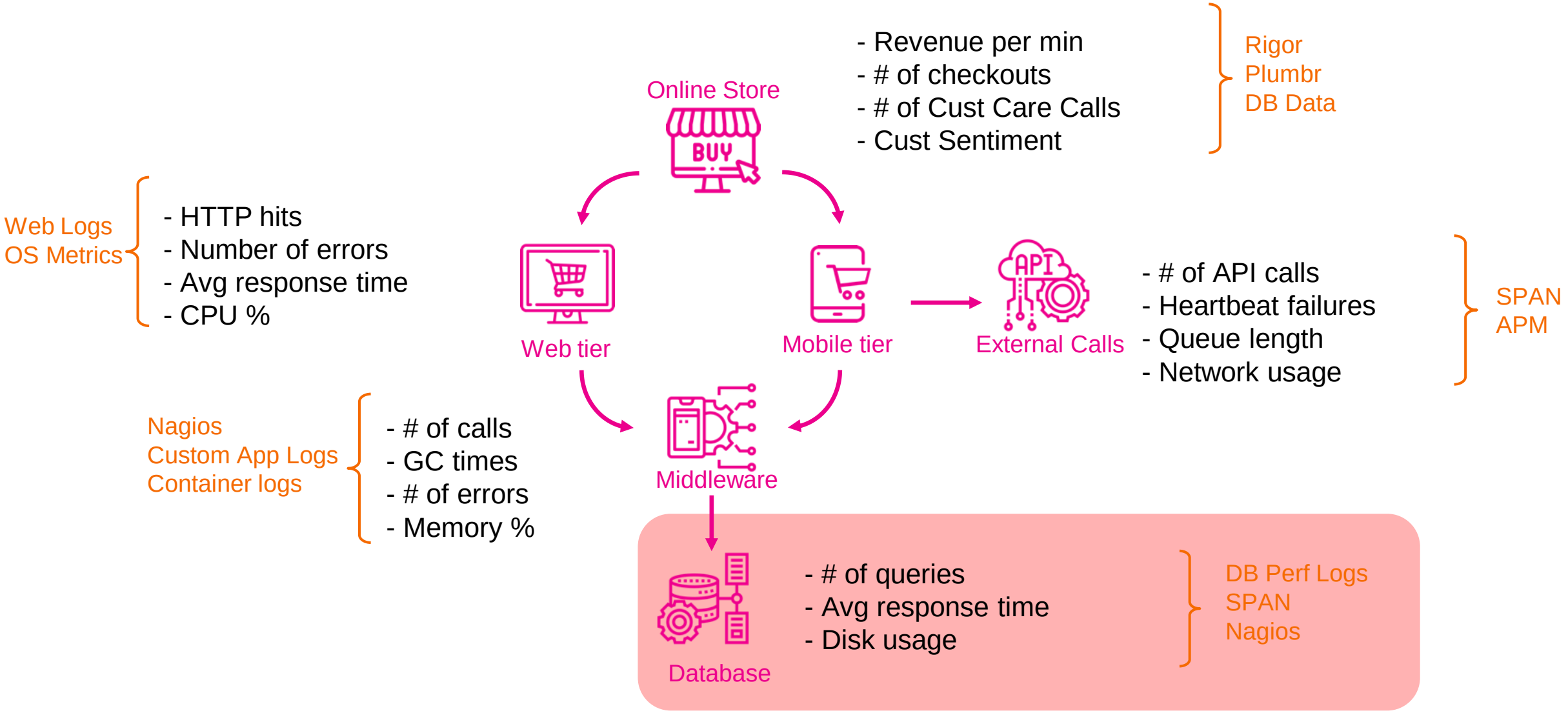
Buttercup Store has just deployed a new Web service, however the engineers forgot to include database monitoring.

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 identify all the missing **database** components.

Business Service Decomposition



Let’s get our hands dirty

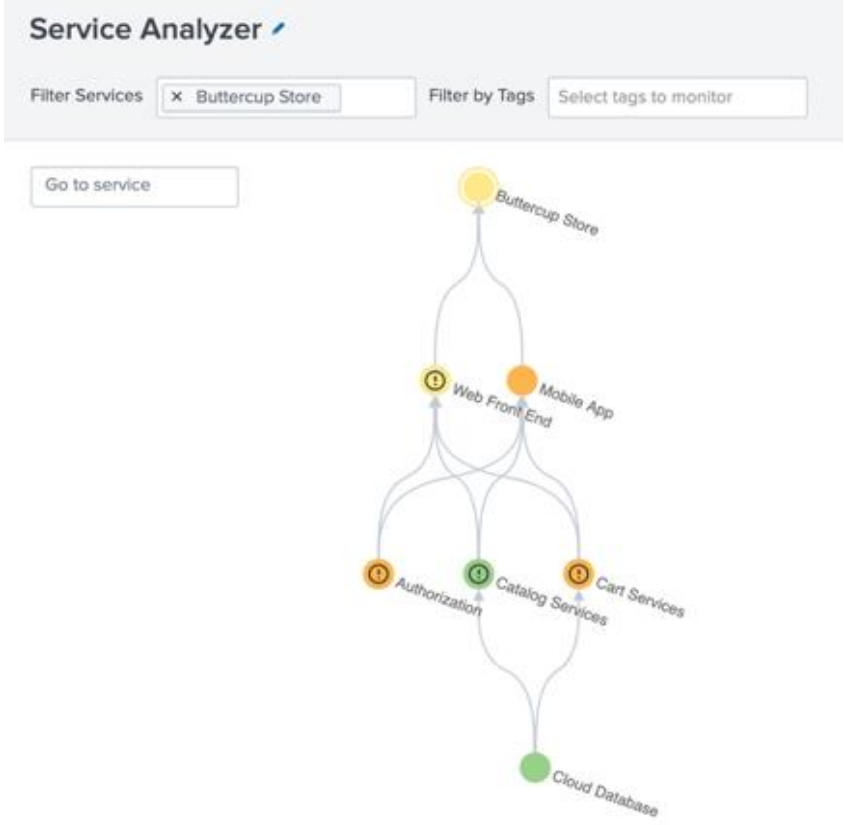
Enter the following URL in your browser : http://<aws_instance>:8000/en-US/

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, CMDB or via a search.



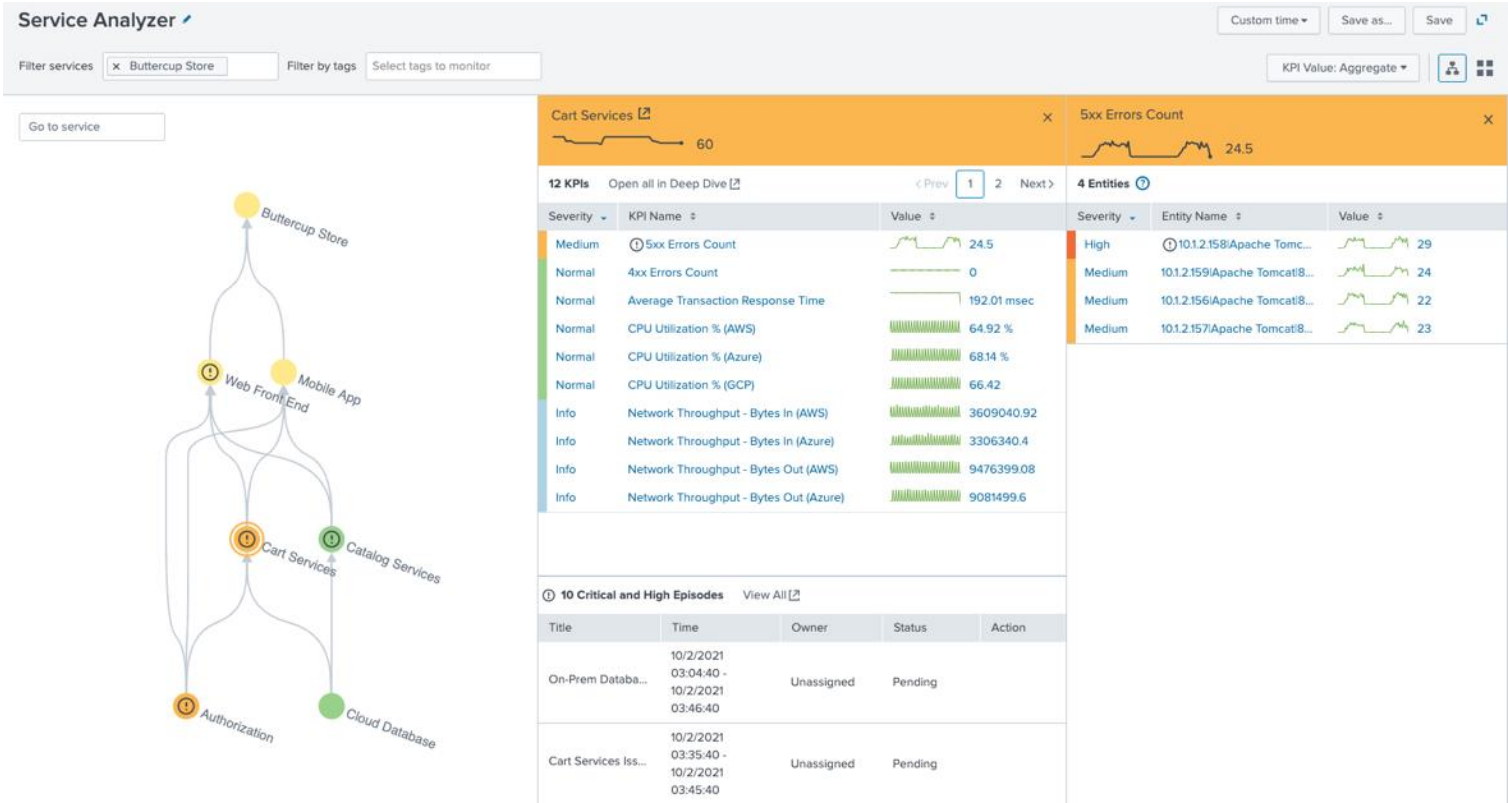
- Click on the Buttercup Store service and review the KPIs, notice that these are all business KPIs.

- 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:10 - xx:20)*.

Service Tree

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

- Click on the effected service (***Cart Services***) to investigate which KPIs have degraded.
- Review the effected entities.
- *Hint : click “5xx Errors”*



Services Lab

During the service decomposition workshop we identified a missing ‘On-Prem Database’ service. We are going to create this new service, we will review the ITSI DB module however we will select a service template.

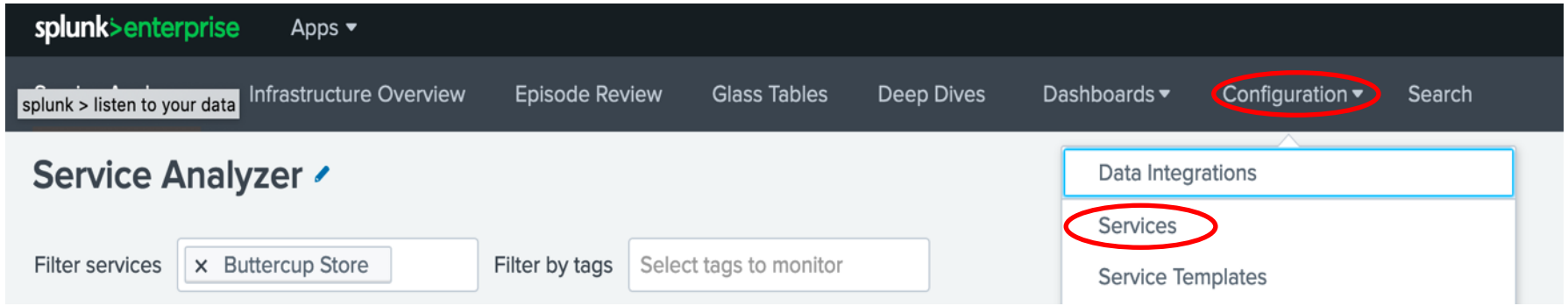
Services could use (technical) KPI’s that comes with these modules:

- OS: Linux, Unix & Windows
- Web server: Apache & Microsoft IIS
- Application server: Tomcat & Websphere
- Database: Microsoft SQL & Oracle
- Storage: Netapp ONTAP & EMC VNX
- Load Balancer: F5 Big IP & Netscaler
- Virtualisation: VMWare & Hyper=V

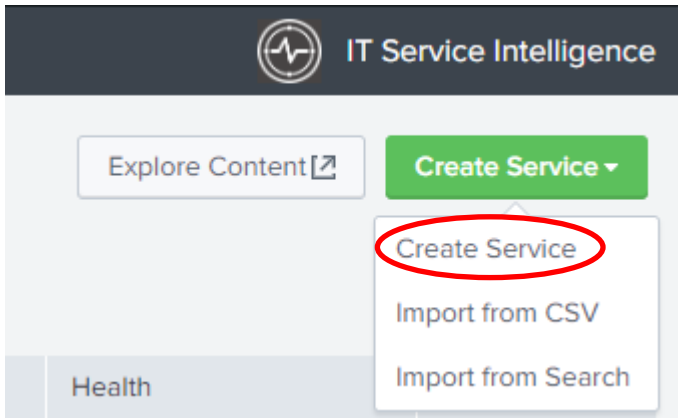
https://docs.splunk.com/Documentation/ITSI/latest/IModules/AboutITSIModules

Services Lab

- Select the Configure menu + Services

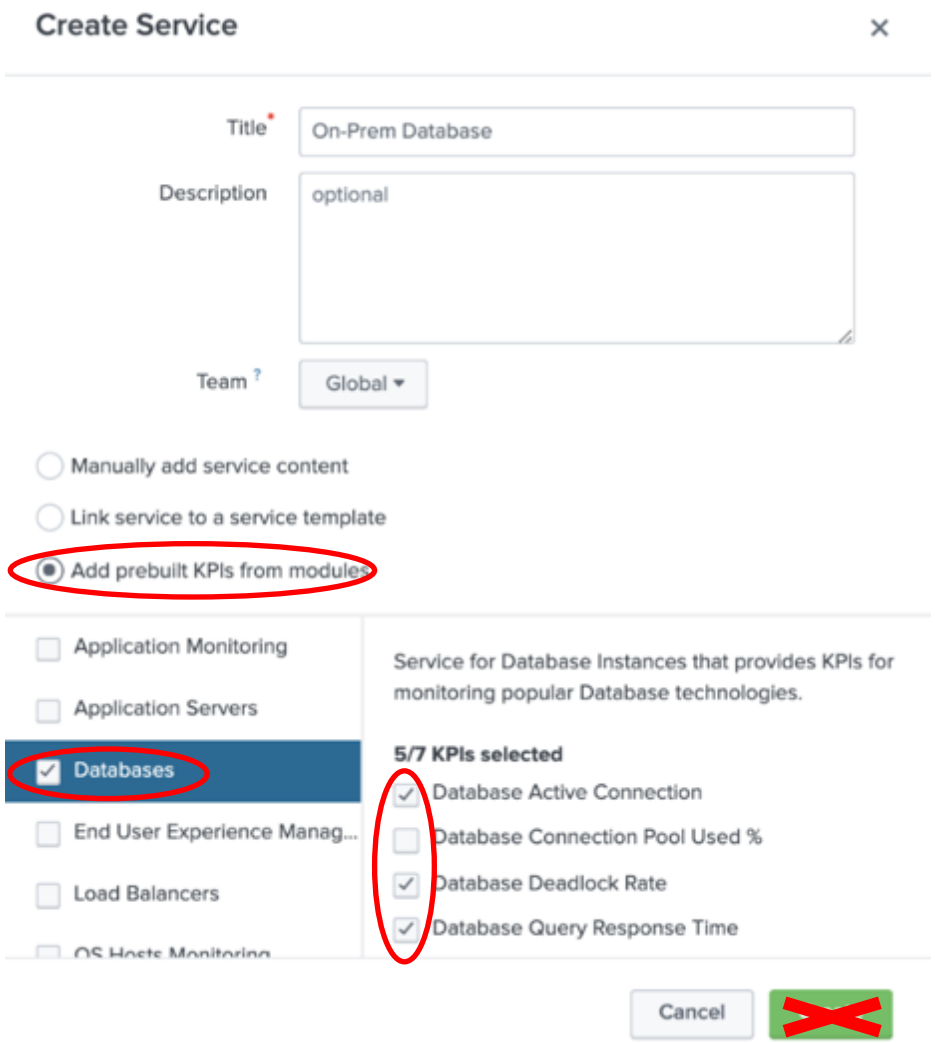


- Click Create Service > Create Service



Services Lab

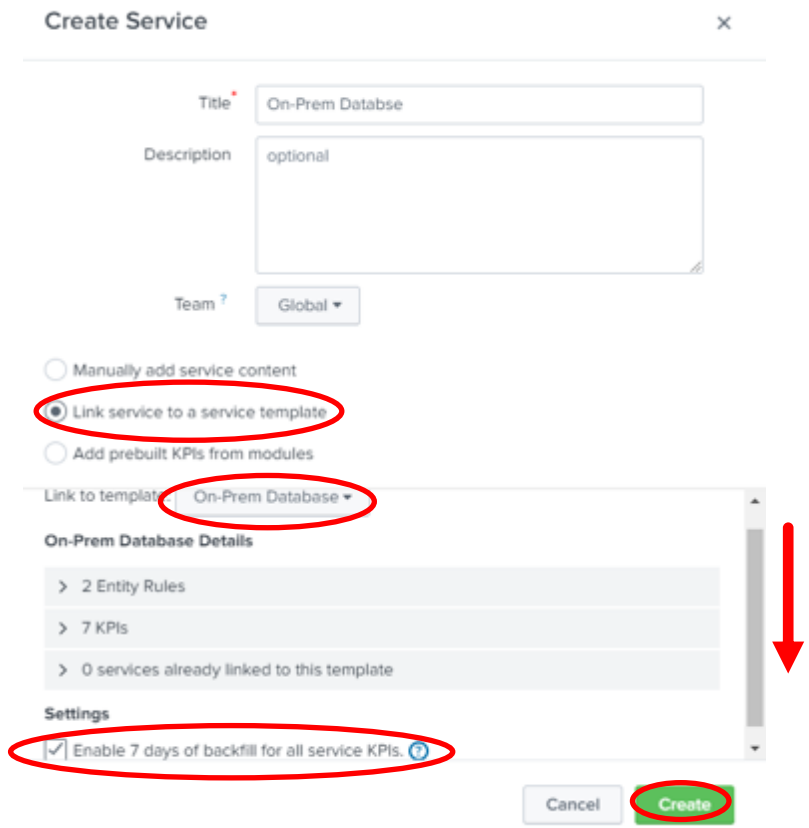
- Name the service ‘On-Prem Database’
- Check ‘**Database**’ in modules list
  - Review the selected KPIs
  - ***Do not hit the ‘Create’ button!***
- ITSI suggests the best KPIs for database monitoring.



Services Lab

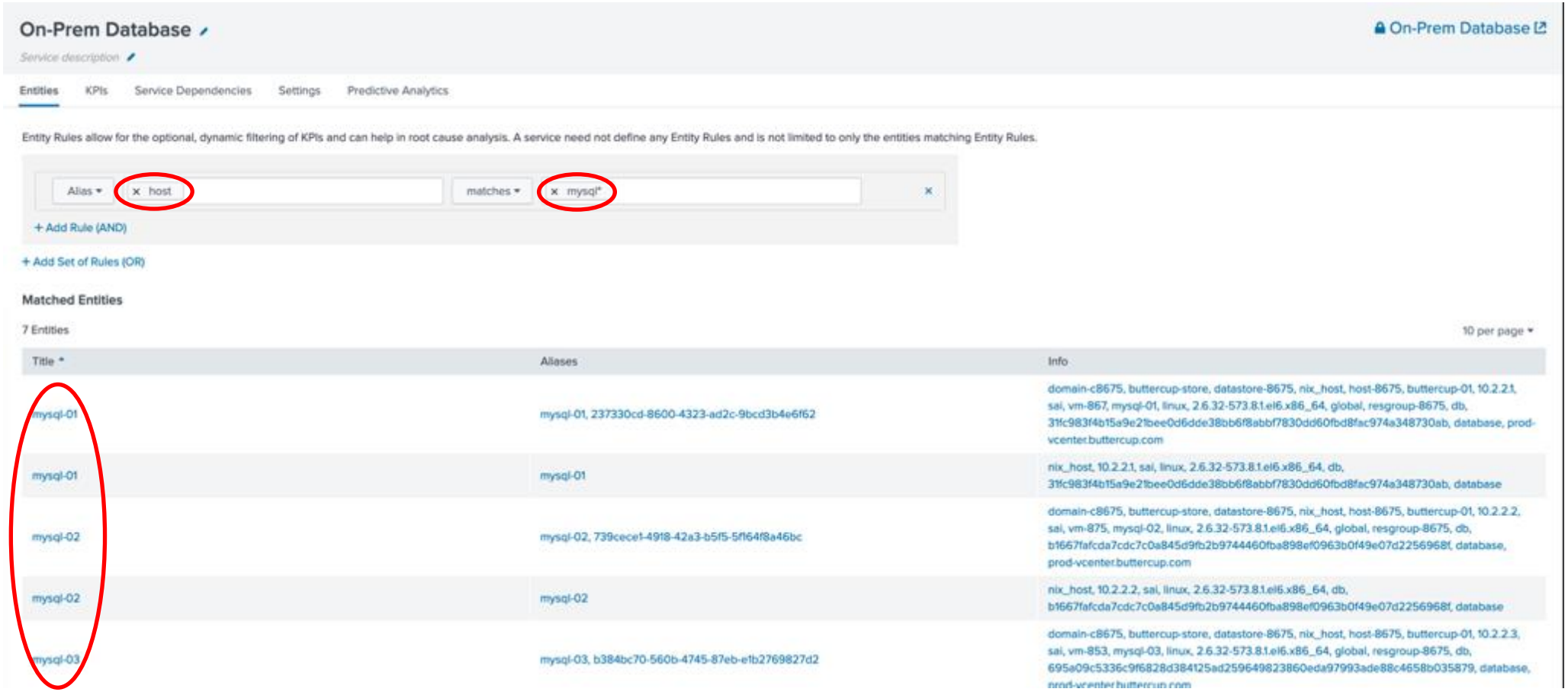
Instead, we are going to utilize the ITSI service templates feature, this will build the service with predefined KPIs.

- Select '*Link service to a service template*' button
- Choose '***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

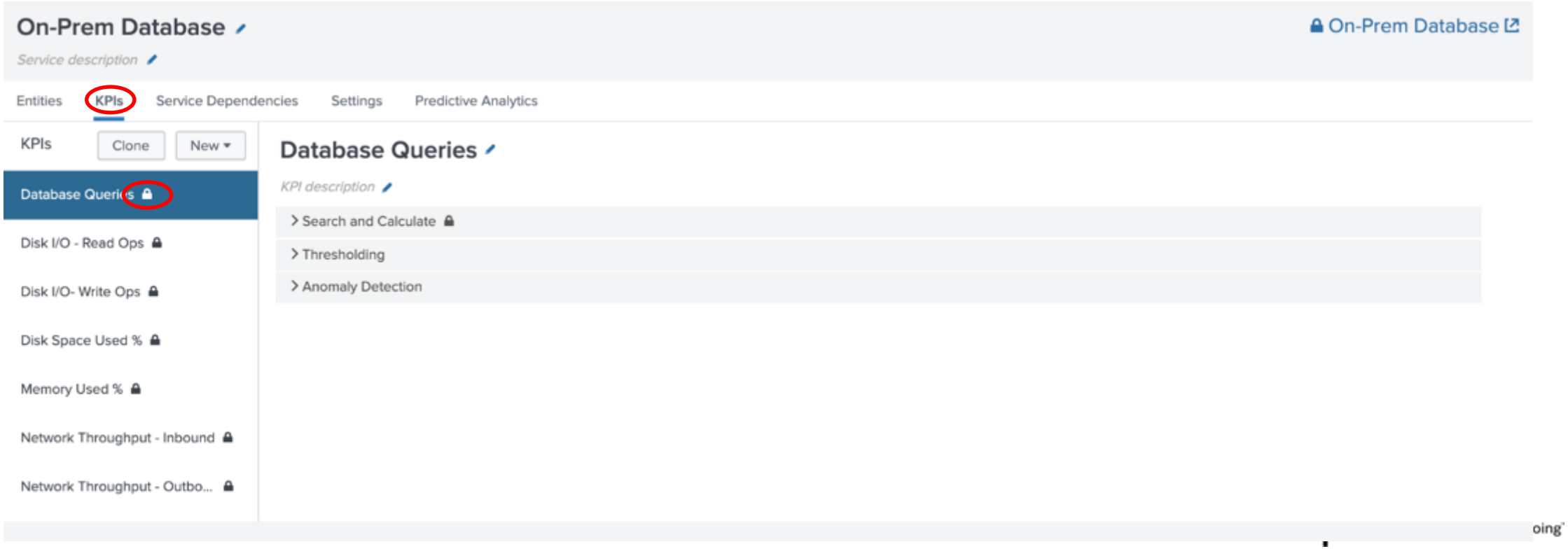
The new ‘On-Prem Database’ service is based on a template, if you review the ‘Entities’ tab we can see that the entities are already filtered.



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.

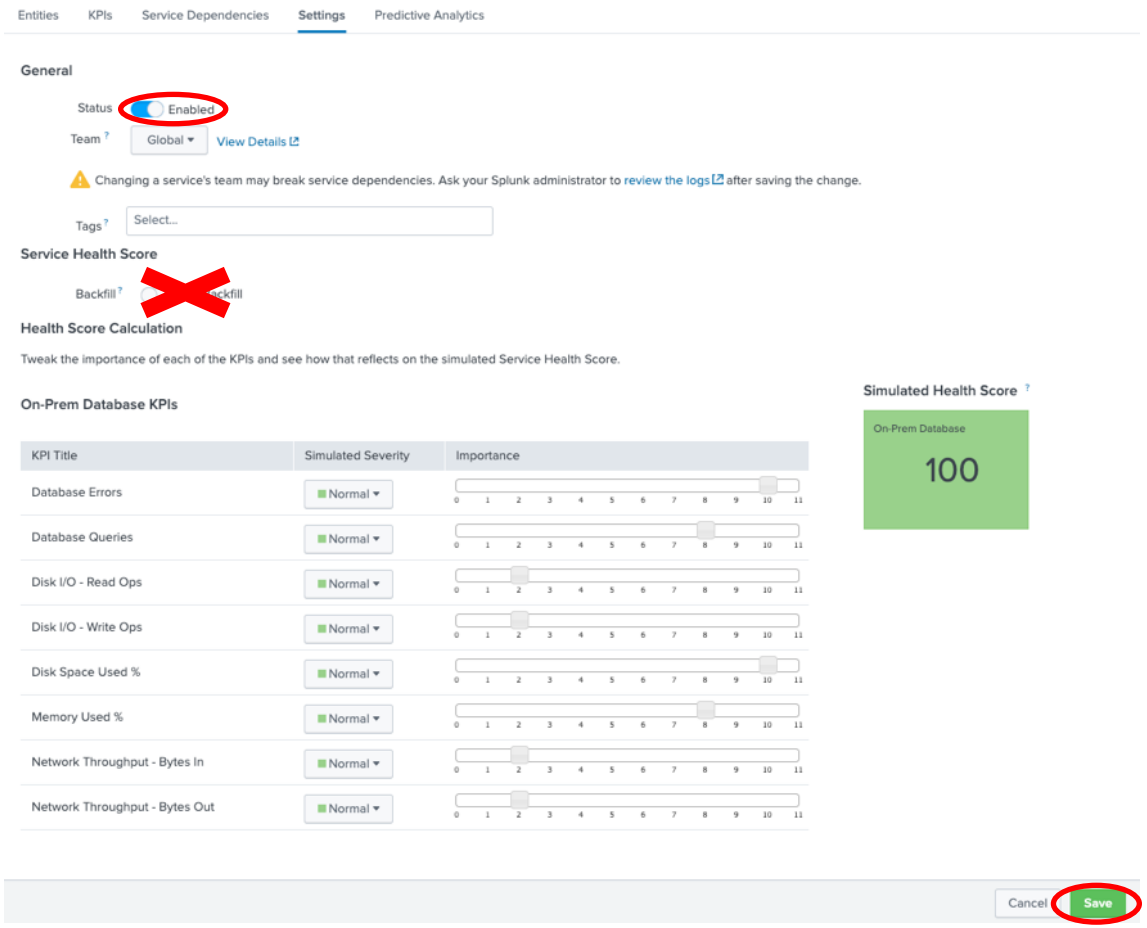


Services Lab

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***

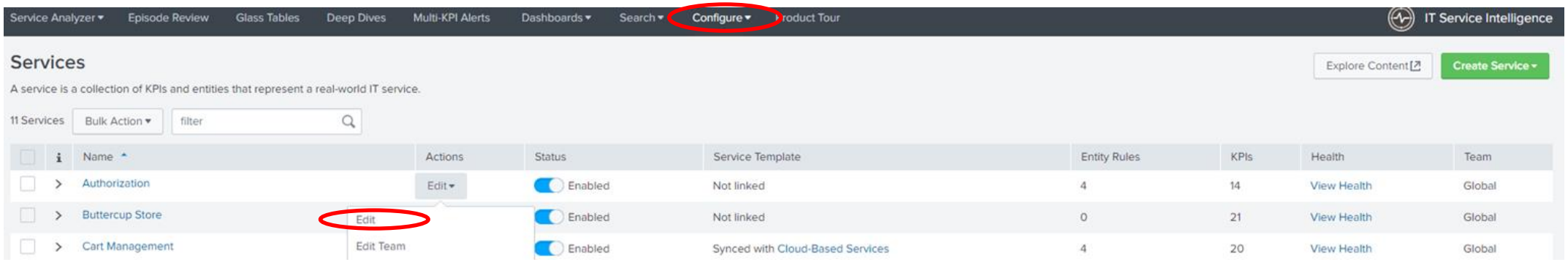
- Click the ‘Save’ button



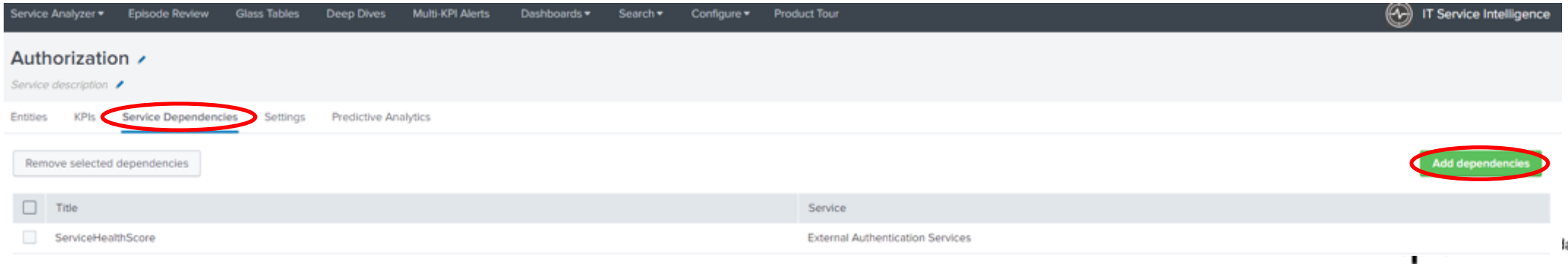
Services Lab

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 *'Authorization' service*



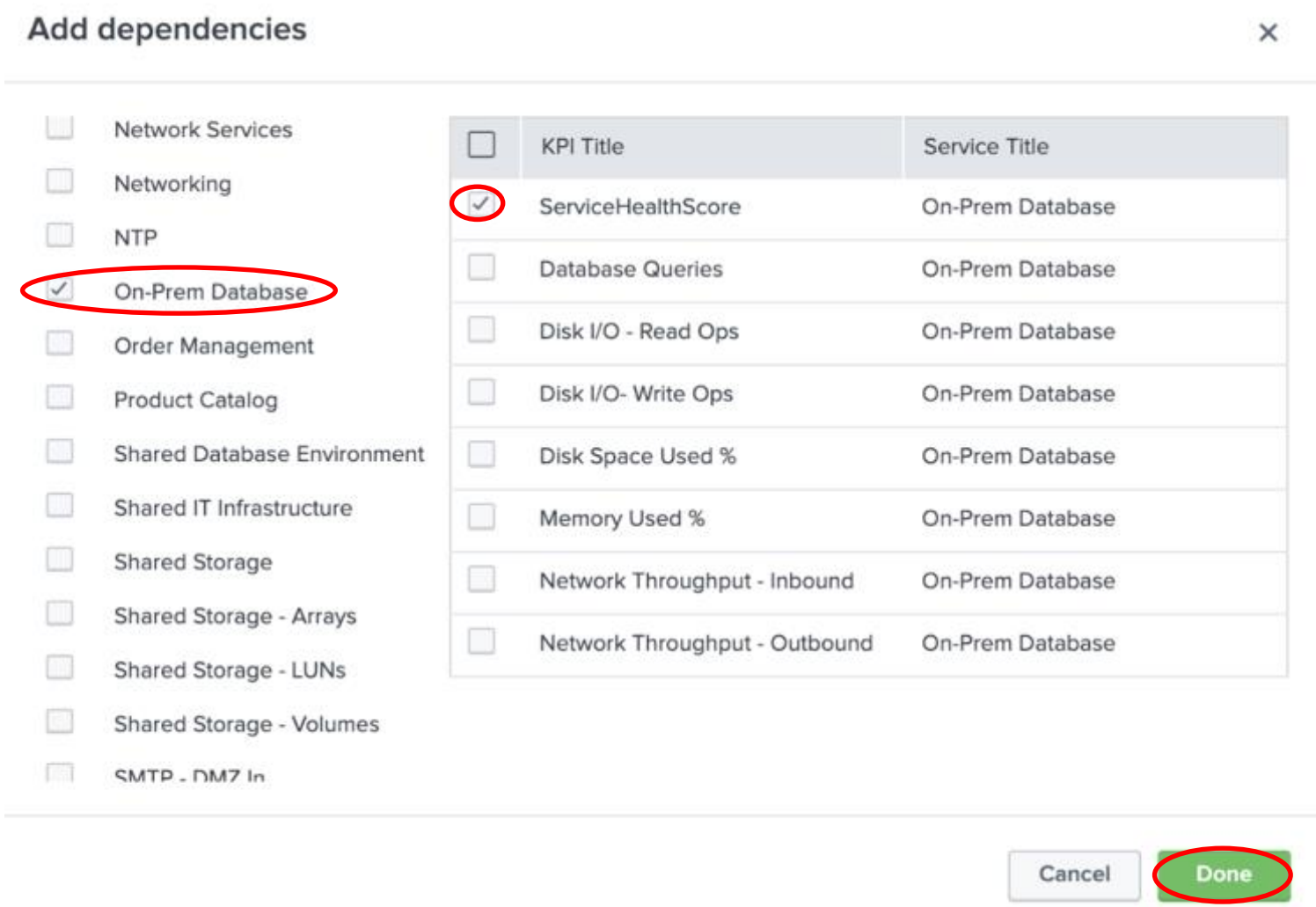
- *Click 'Service Dependencies' tab and then 'Add dependencies'*



lata into doing'

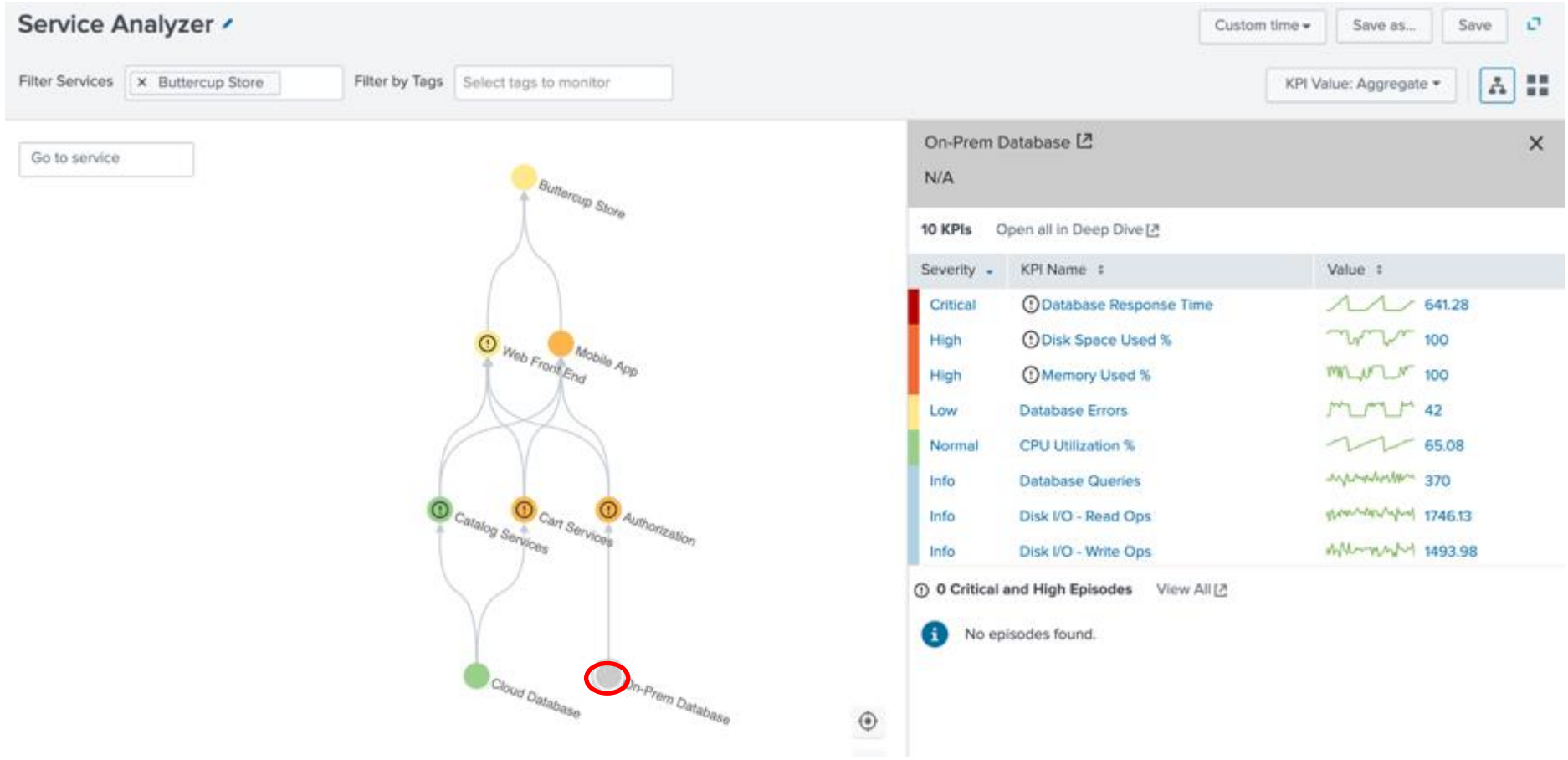
Services Lab

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



Check Service Tree

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



Note : the service health score will be grey until KPIs searches have executed.

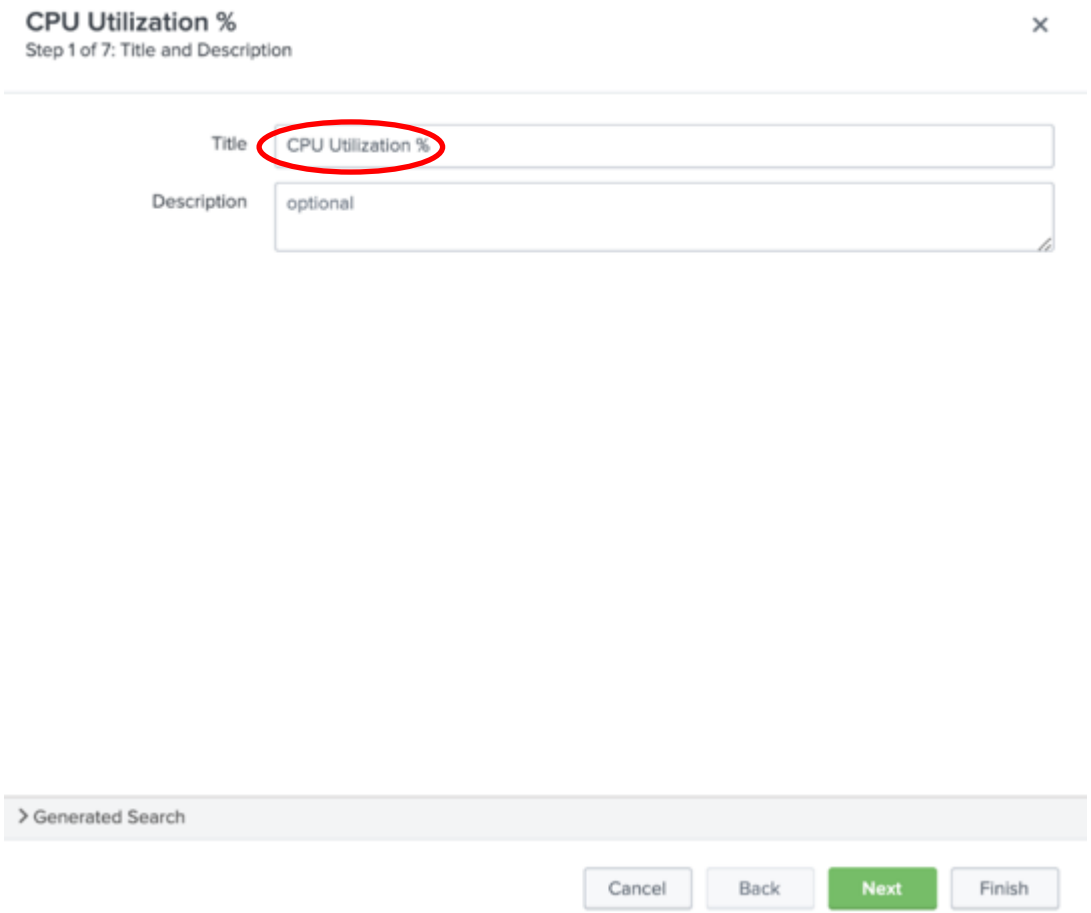
KPI Exercise

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 %’

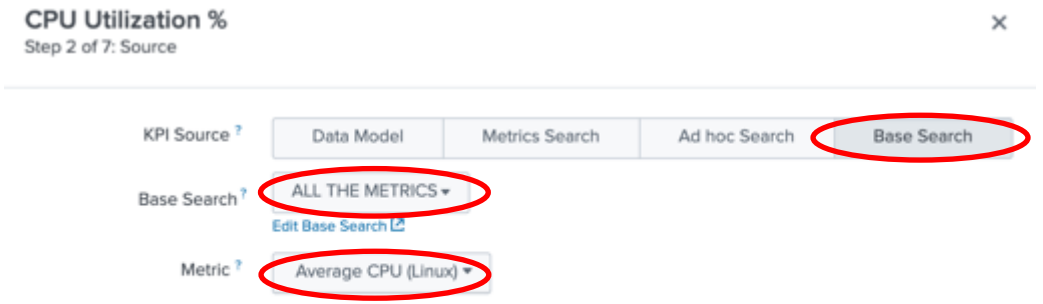
- Click ‘Next’ button



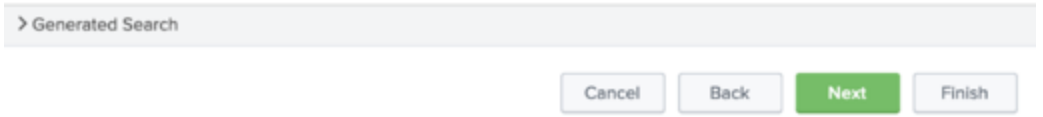
KPI Lab

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 ‘ALL THE METRICS’
- Select ‘Average CPU (Linux)’

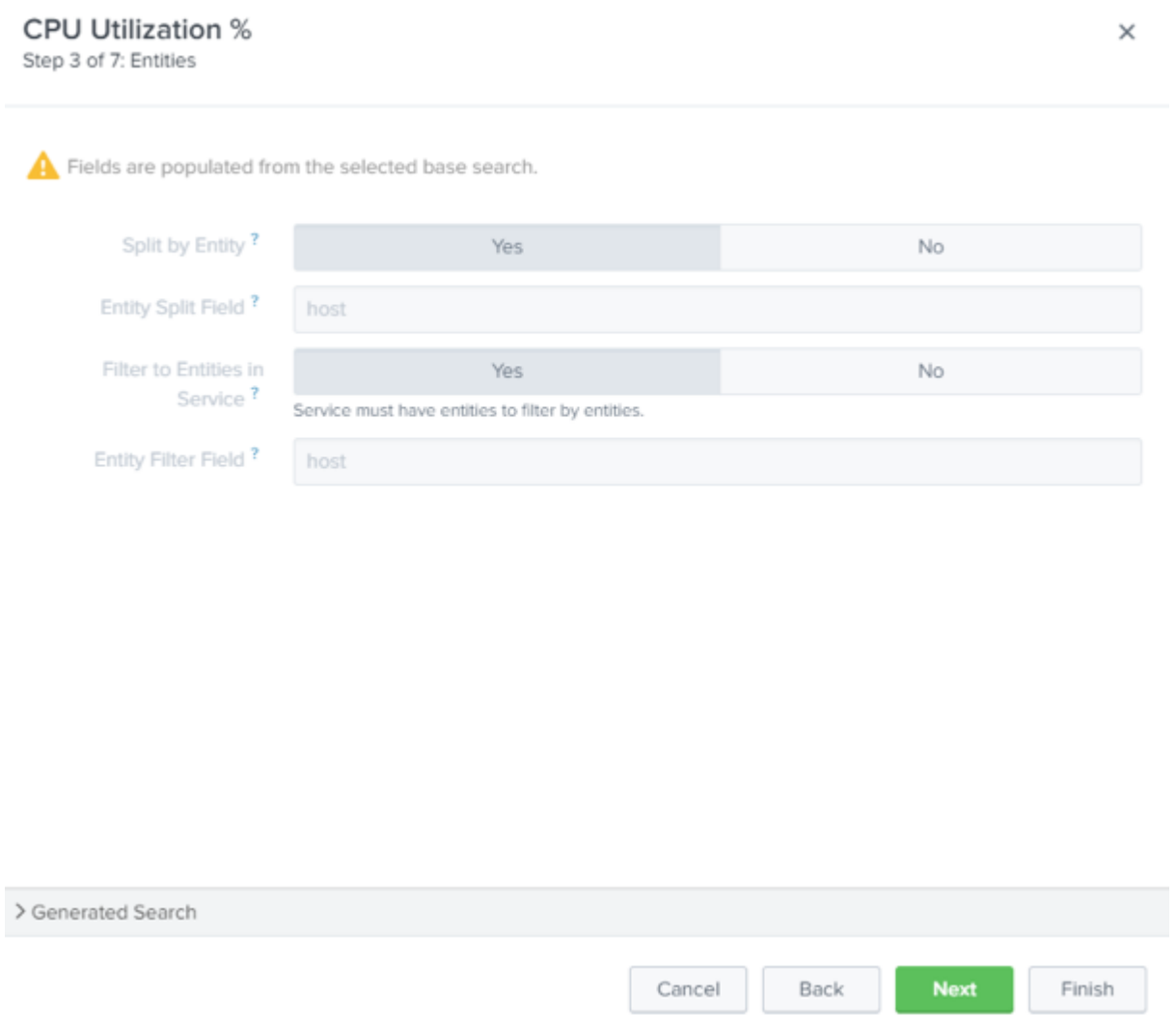


- Click ‘Next’ button



KPI Lab

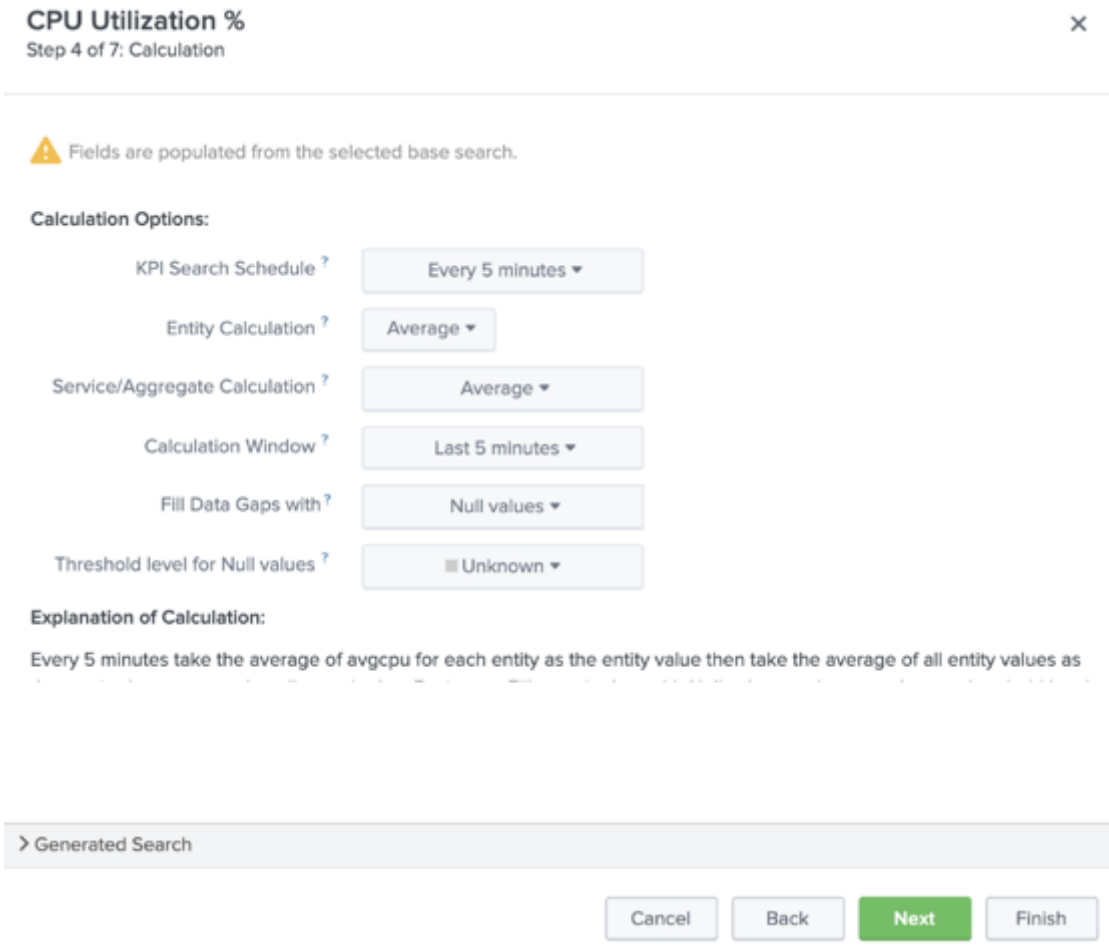
There is no option to split as this KPI is using a base search.



- Click ‘Next’ button

KPI Lab

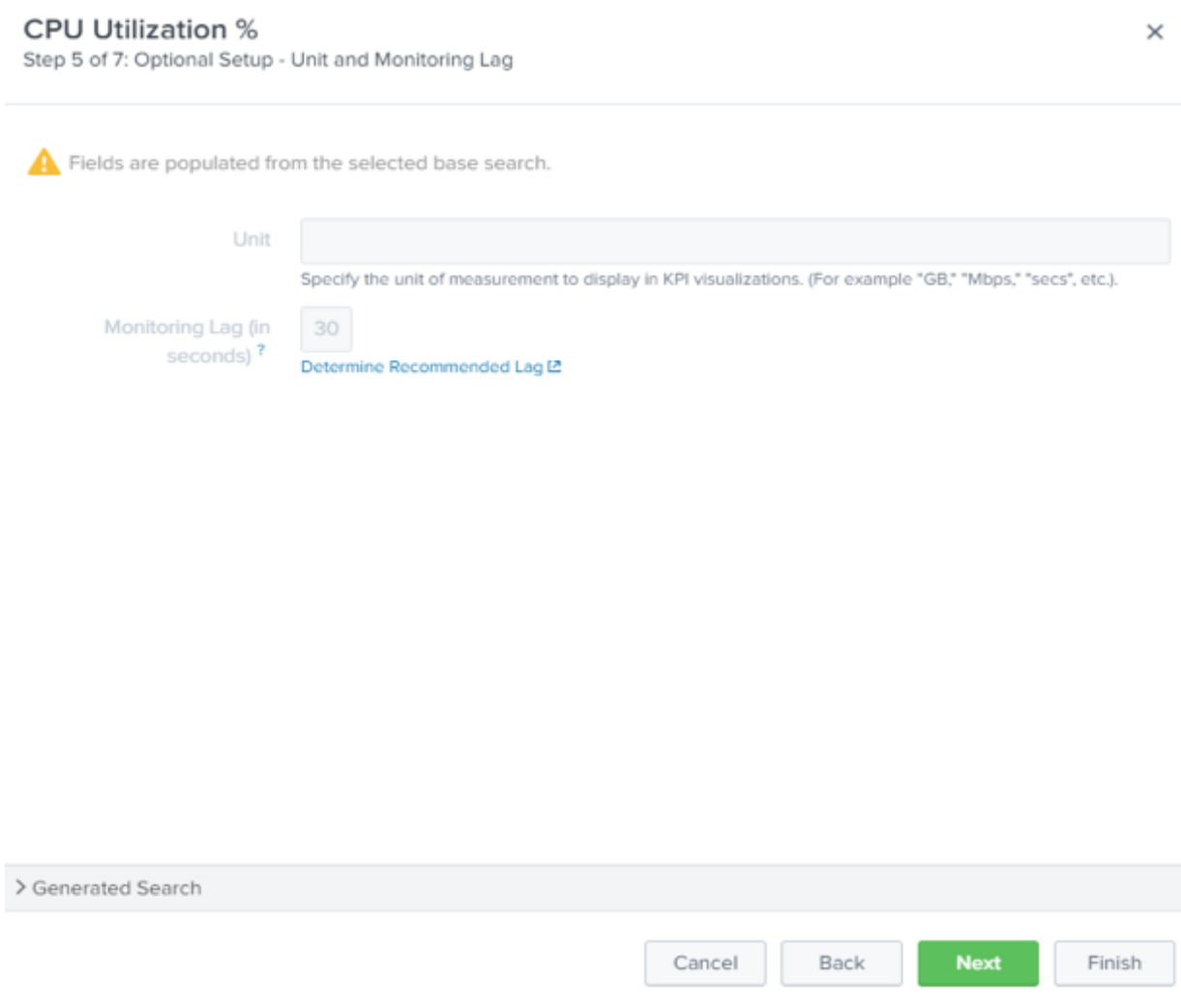
There is no option to configure the calculation as this KPI uses a base search.



- Click ‘Next’ button

KPI Lab

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

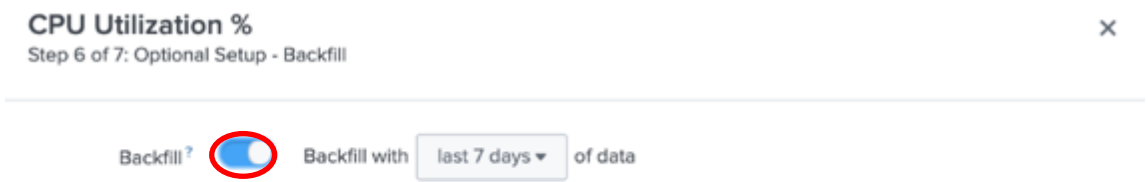


- Click ‘Next’ button

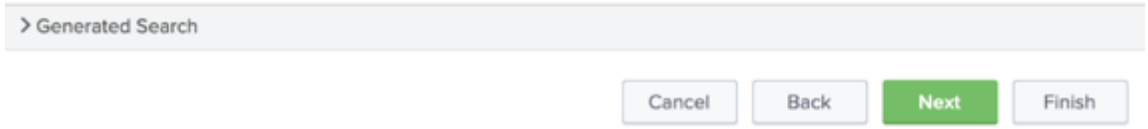
KPI Lab

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



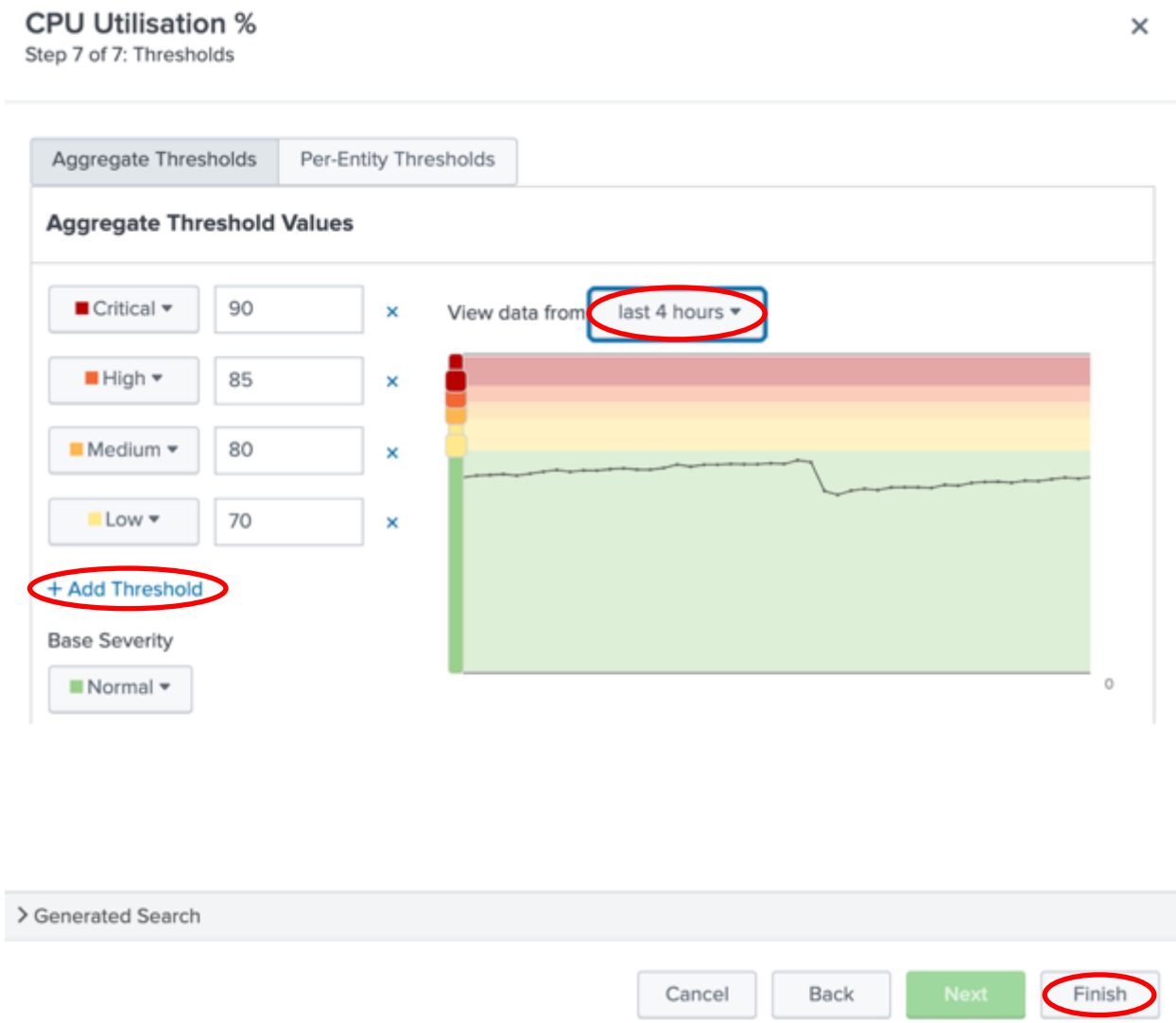
- Click ‘Next’ button



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



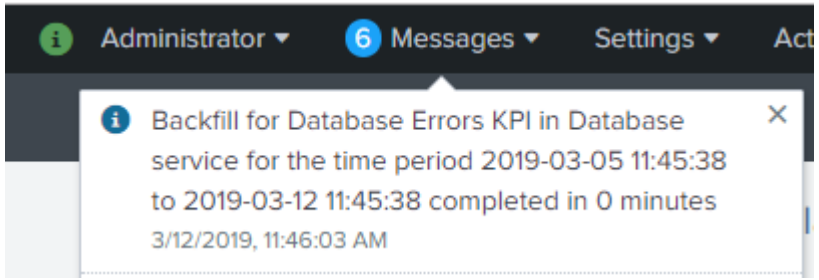
- Click ‘Finish’ button

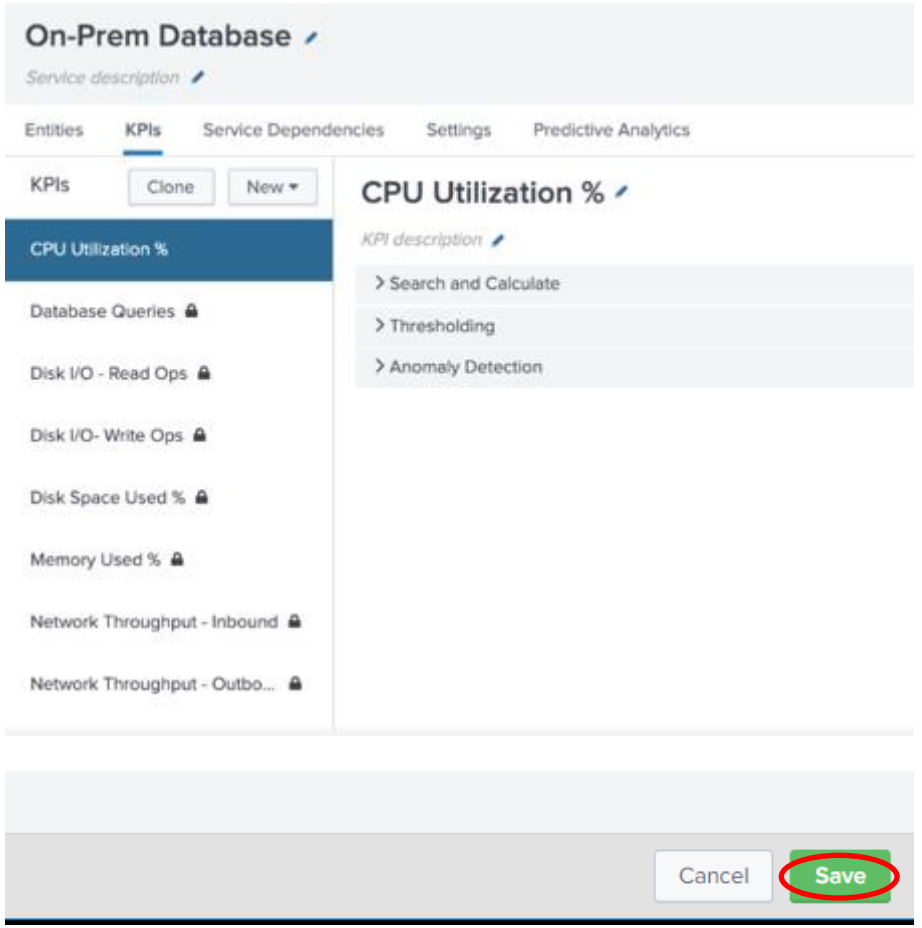
KPI Lab

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

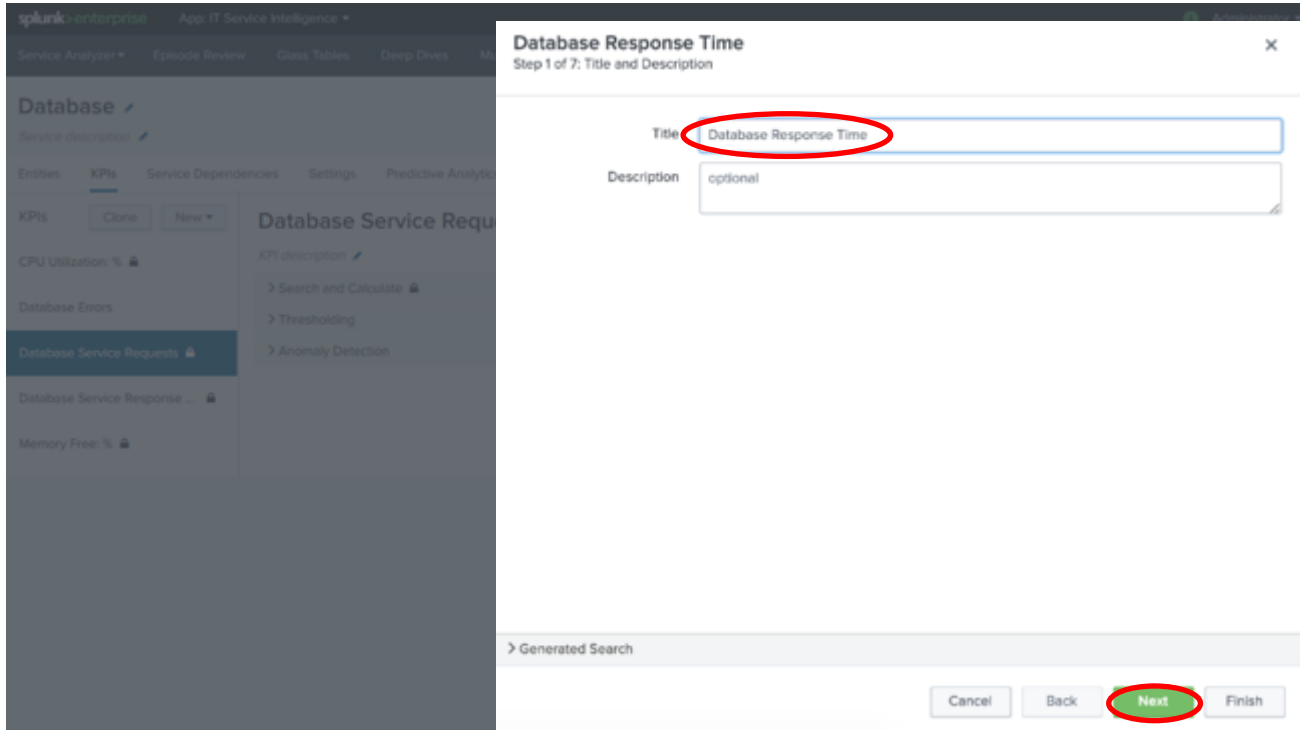




KPI Lab

An important dependency for the new ‘On-Prem Database’ service is response time, in this lab we will add an extra KPI: ‘Database Response Time’. For this KPI we use an ad-hoc search.

- Click Configure > Services
- Click ‘On-Prem Database’ & KPI tab
- Click New KPI > Generic KPI
- Title = ‘Database Response Time’

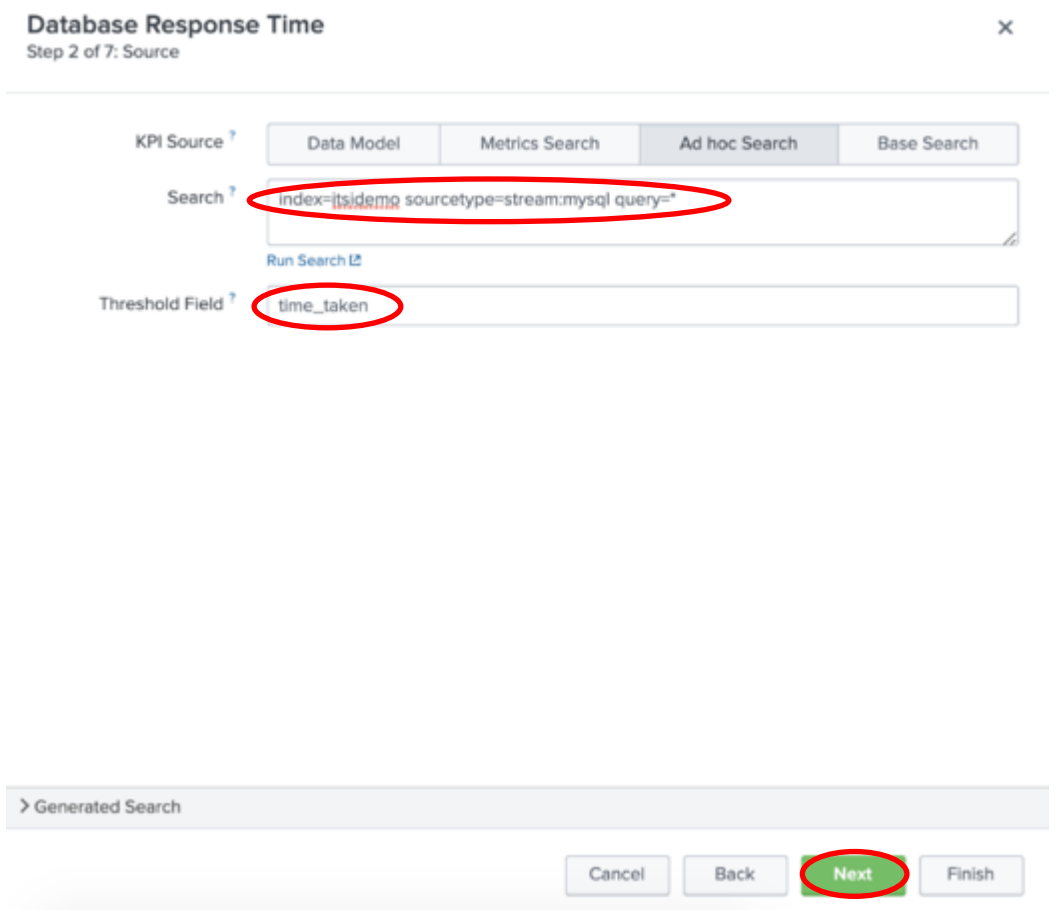


- Click ‘Next’ button

KPI Lab

The new KPI source could be driven by a data model, ad-hoc search or a base search. In this instance we will create the KPI using an ad-hoc search.

- Click ‘Ad-hoc Search’
- Enter the following search:
  - index=itsidemo sourcetype=stream:mysql query=*
- Enter ‘time_taken’ as the threshold field
- Click ‘Run Search’ button to test search

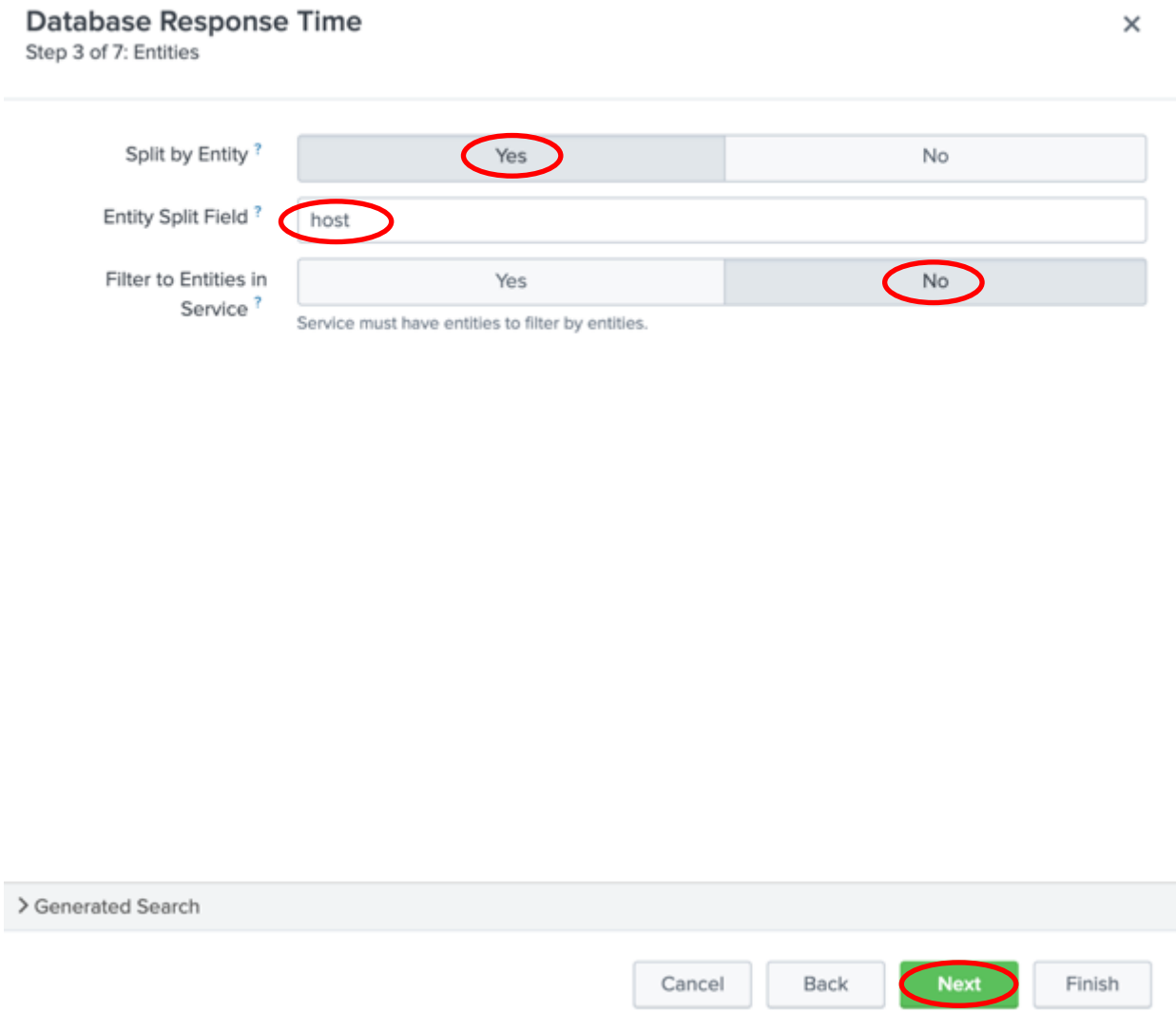


- Click ‘Next’ button

KPI Lab

The database response time KPI will be split via the host.

- Select ‘Yes’ for split by entity
- Enter ‘host’ as the split by field
- Select ‘No’ for filter to entities in Service

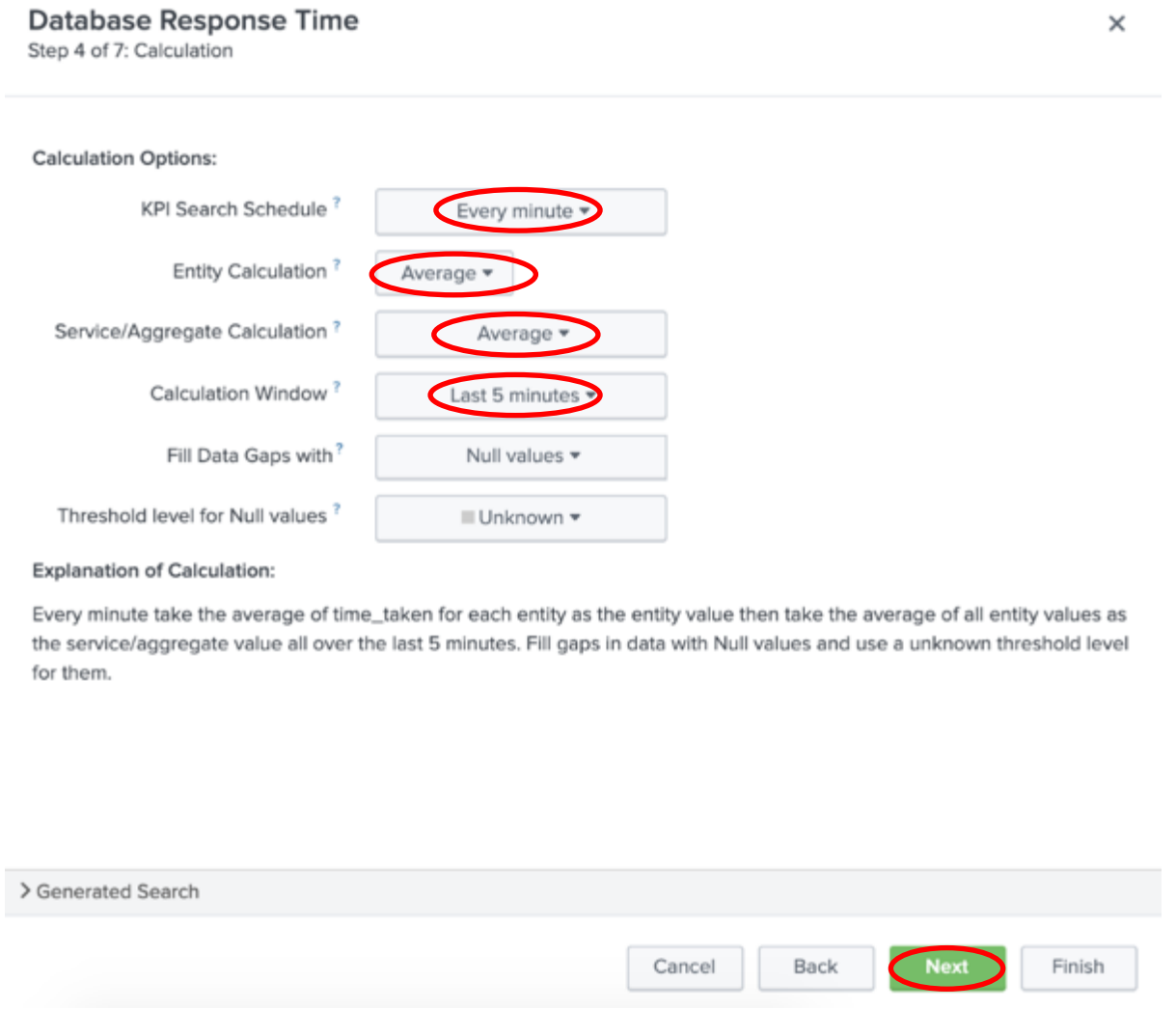


- Click Next

KPI Lab

The database response time KPI will have the following calculation options.

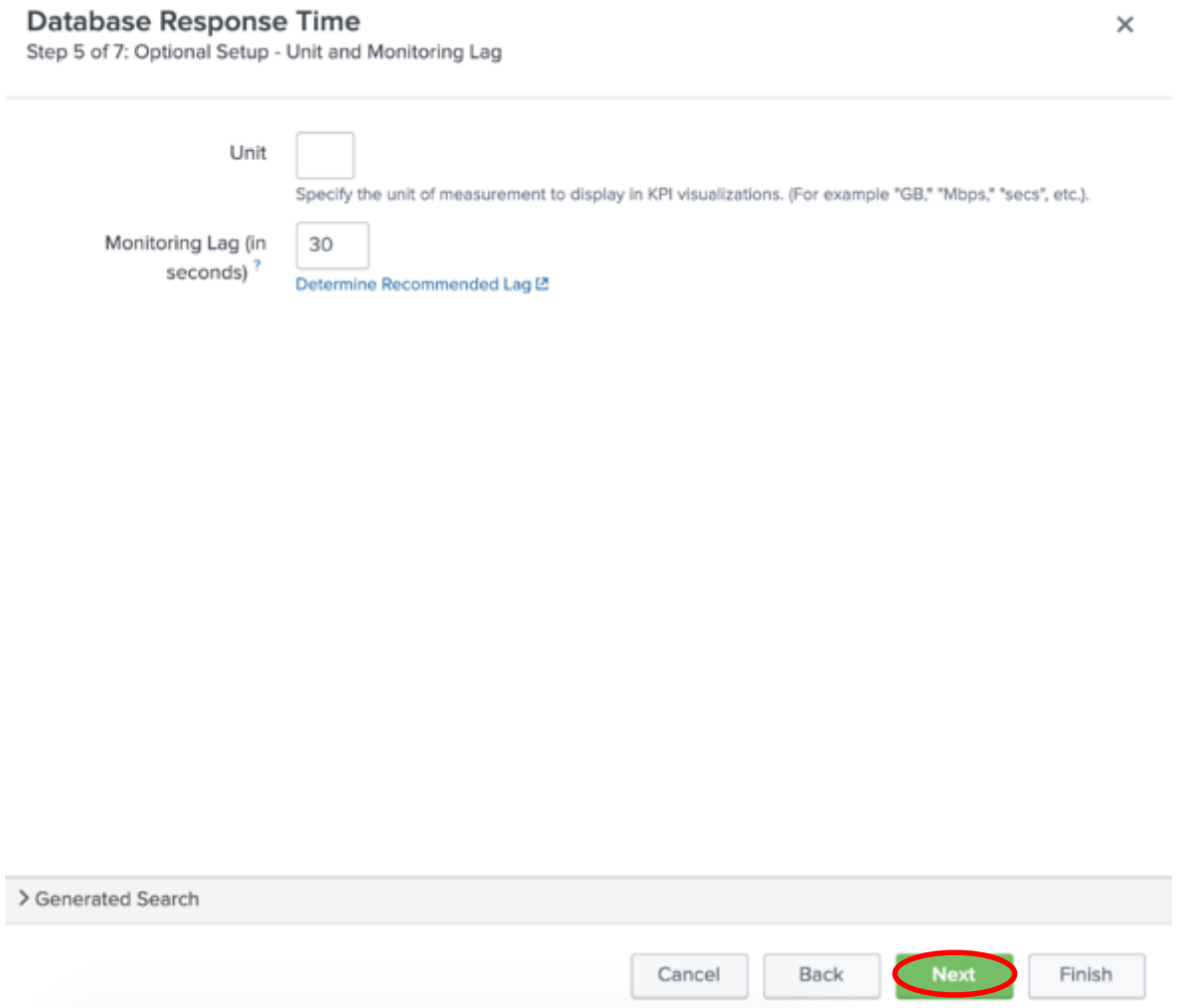
- Schedule = Every minute
- Entity Calculation = Average
- Aggregate Calculation = Average
- Calculation Window = 5 minutes



- Click Next

KPI Lab

We will leave the next screen with the default values.

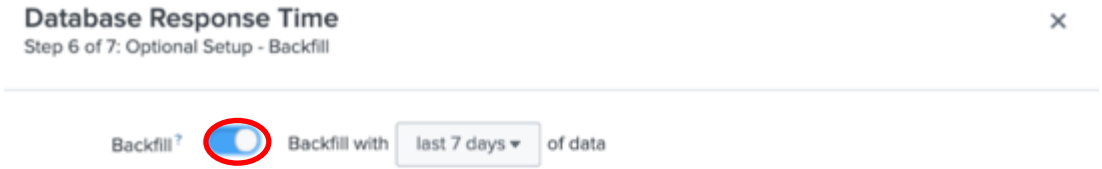


- Click Next

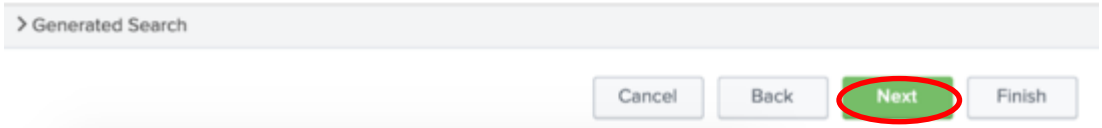
KPI Lab

We want this KPI to use data already ingested in Splunk over the last 7 days. This historical data will be used in the machine learning labs.

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



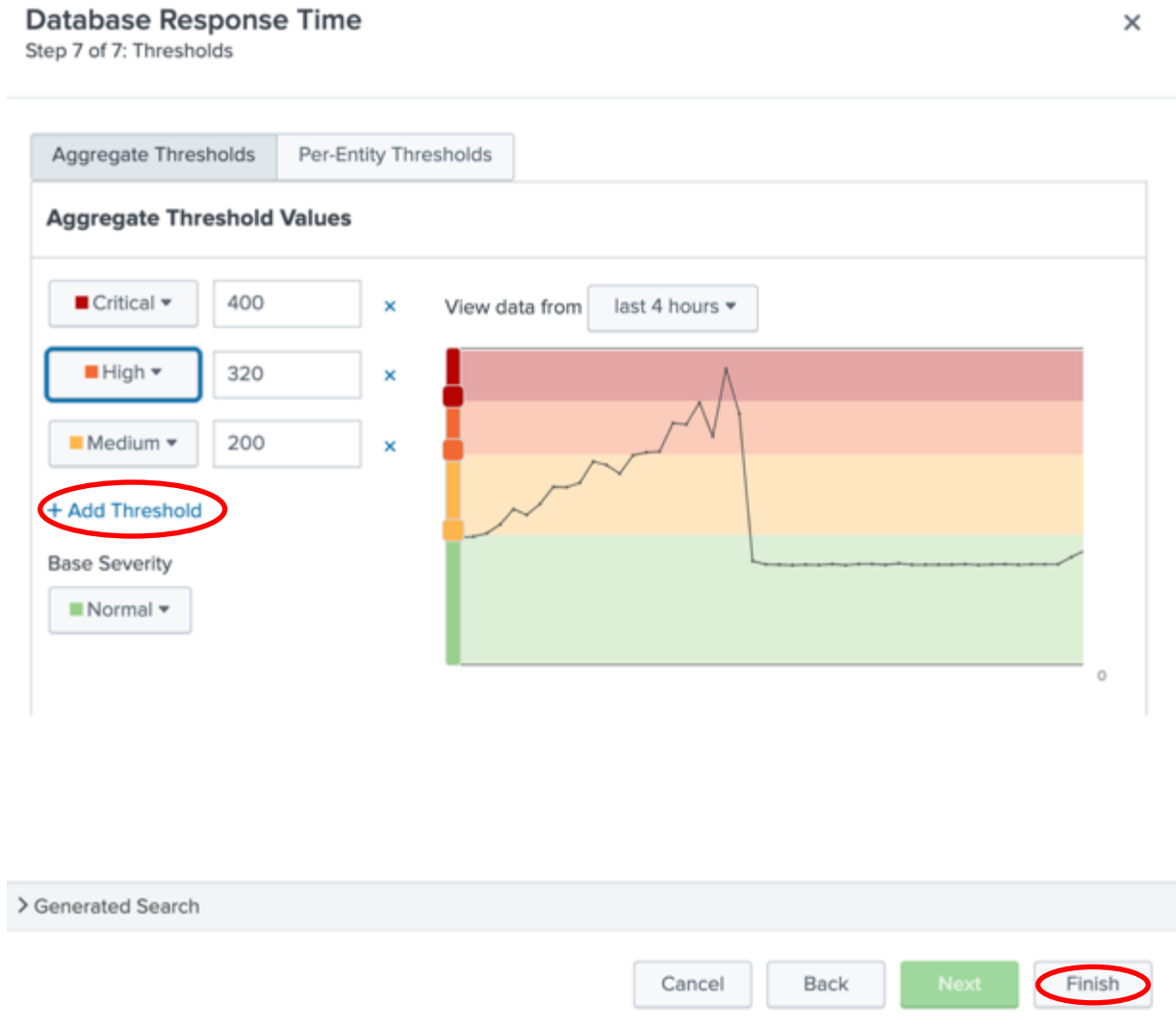
- Click ‘Next’ button



KPI Lab

We need to set some static thresholds for this new KPI

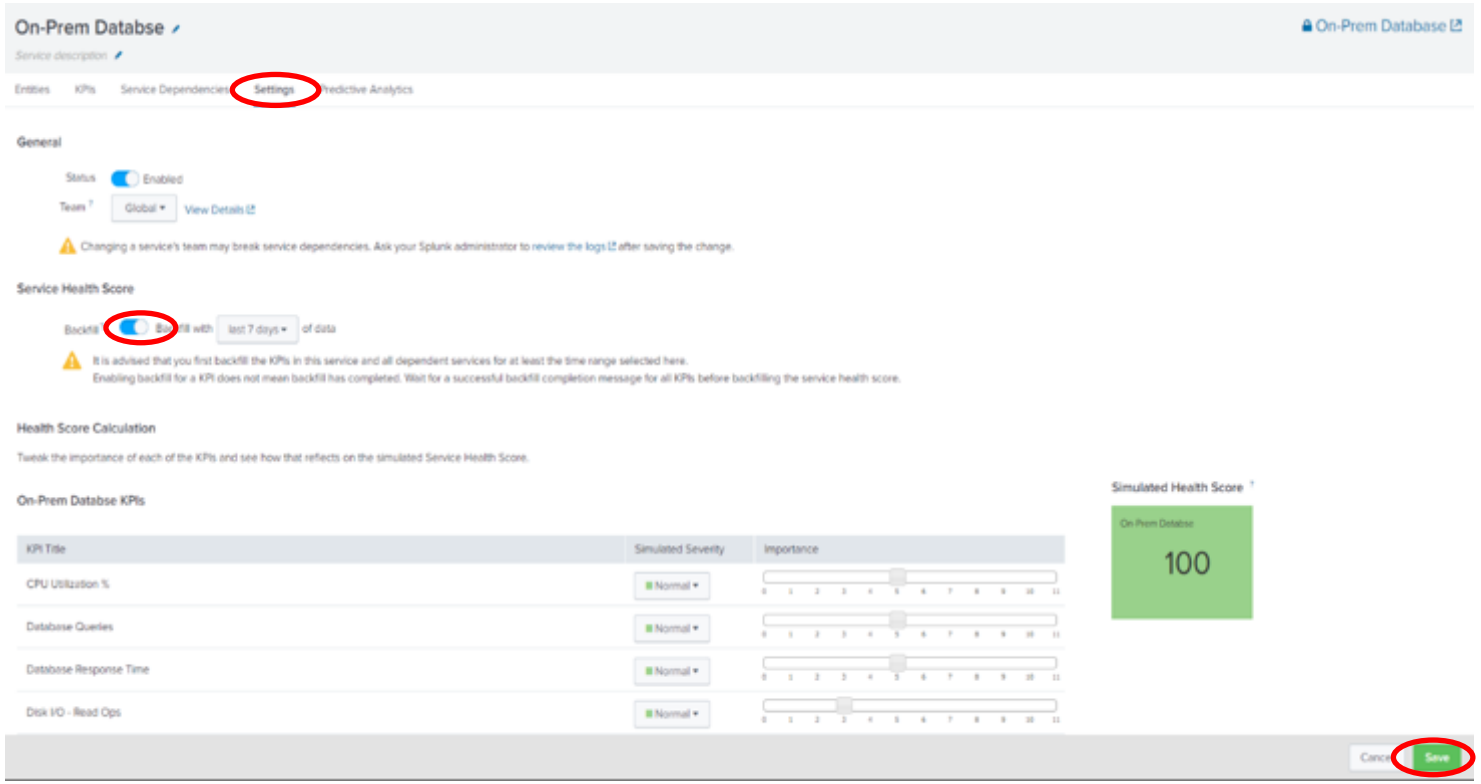
- Increase time to 4 hours
- Add & configure threshold:
  - Critical = 400
  - High = 320
  - Medium = 200
- Click '*Finish*' button
- Do not forget to click '*Save*' button!!



KPI Lab

We have built two new KPIs 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.

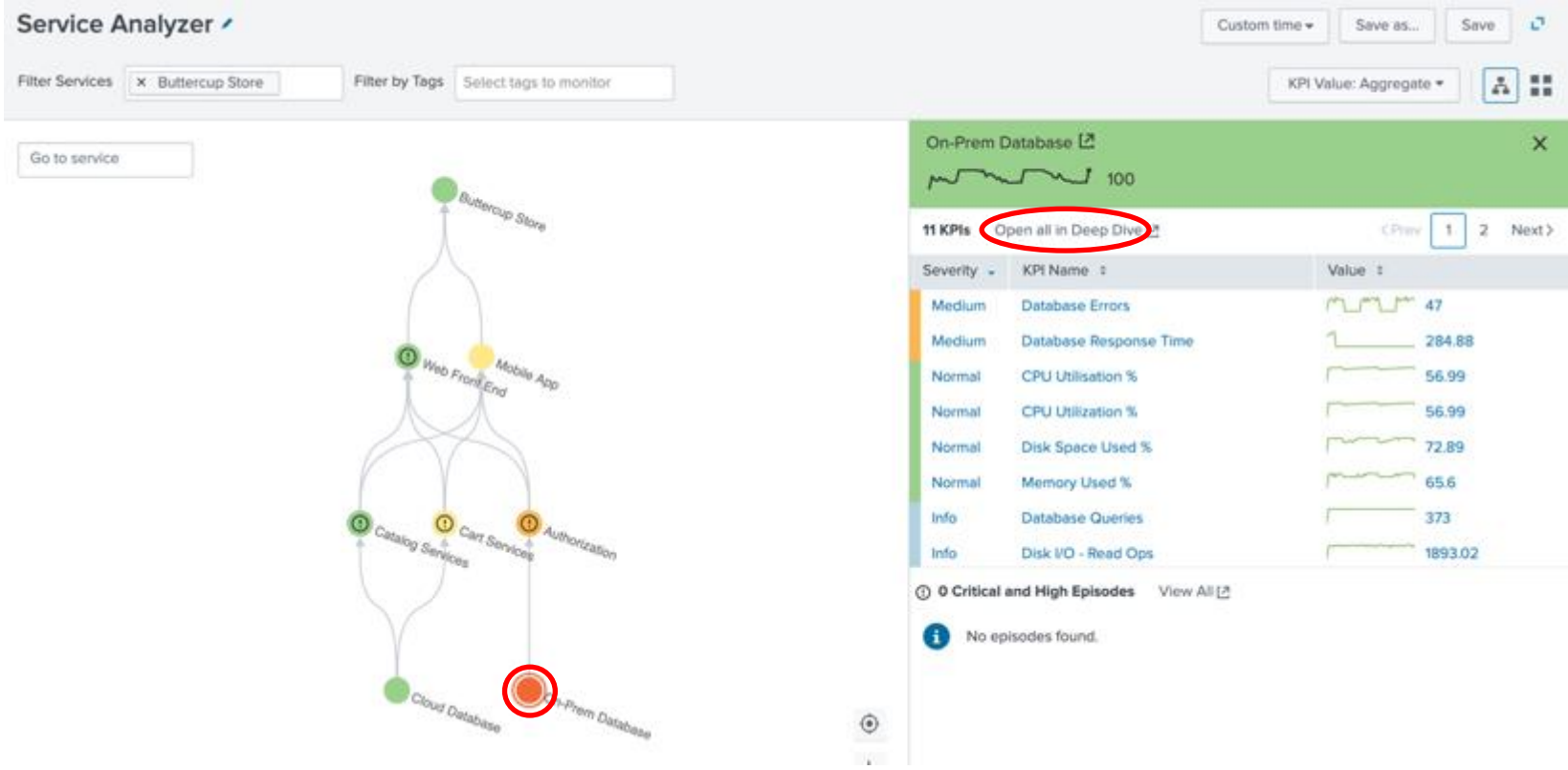
The deep dive capabilities within ITSI brings together multiple data sources into a single visualization. The correlation of data streams enable quick identification of root cause and effect on the business.

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 Lab

- 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

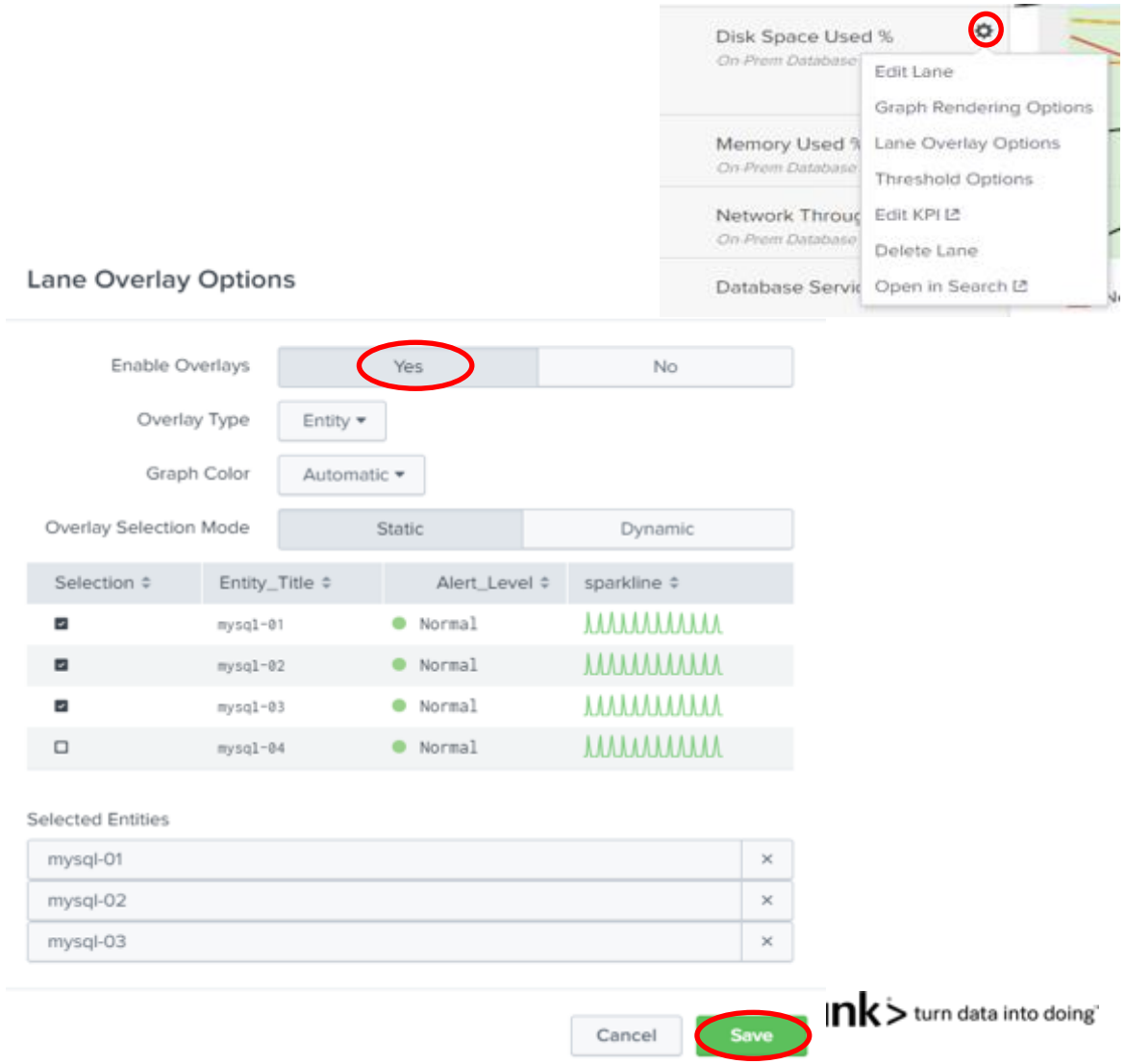
To understand the impact we need to add some business KPI to this deep dive, this will speed up investigations and diagnosis.

- Either navigate up the service tree or change focus to '*Buttercup Store*'
- Click + on the following KPIs;
  - Revenue
  - Successful Checkouts
- Move lanes as per image

Deep Dive Lab

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

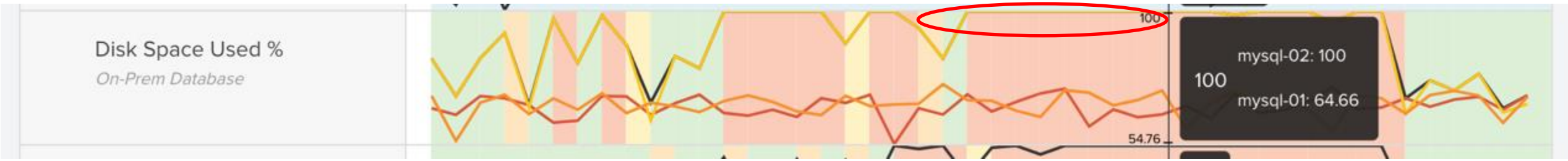
- Select ‘Disk Space used %’
- Select the COG icon next to Disk Space used %
- Select Lane Overlay options
- Select Enable Overlays ‘Yes’
- Click ‘Save’



Deep Dive Lab

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

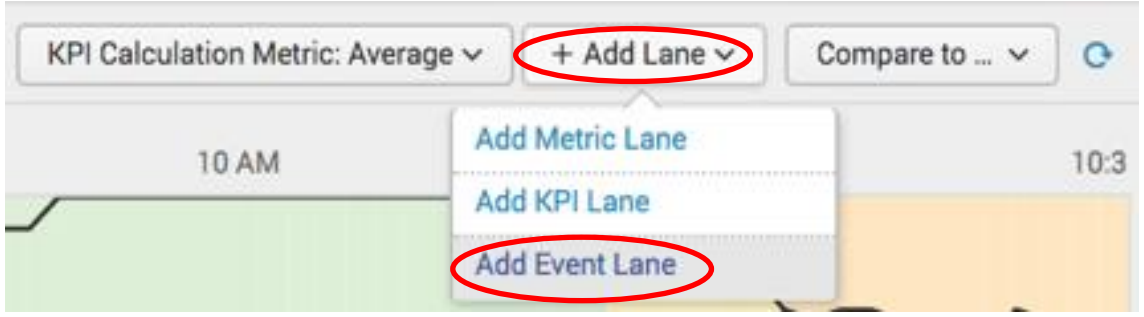
- Hover over the ’Disk Space Used %’
- Notice the “mysql-02’ disk space is running at 100%



Deep Dive Lab

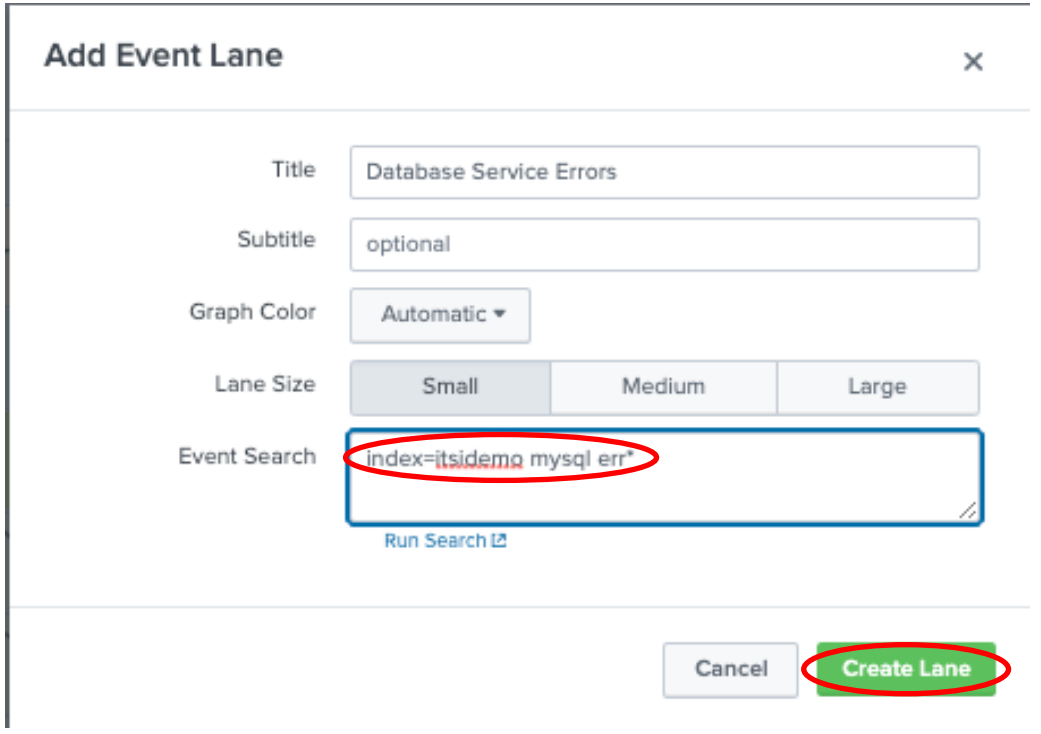
We will now add an event lane to the deep dive, this enables us to dive into the root cause.

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



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

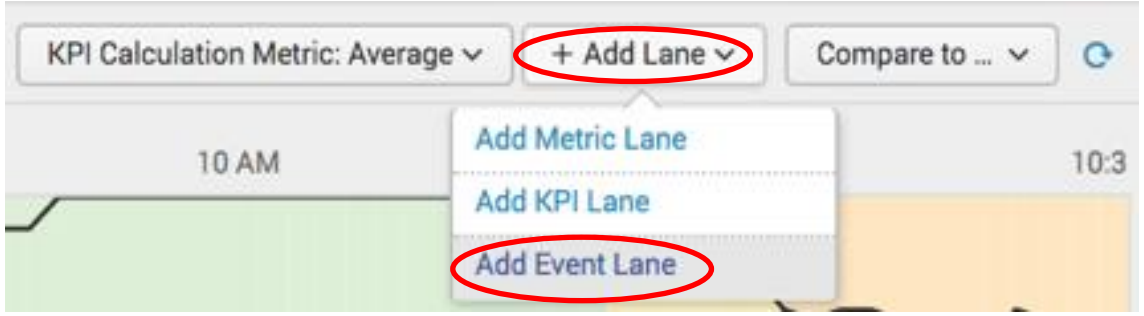
- Click ‘Create Lane’



Deep Dive Lab

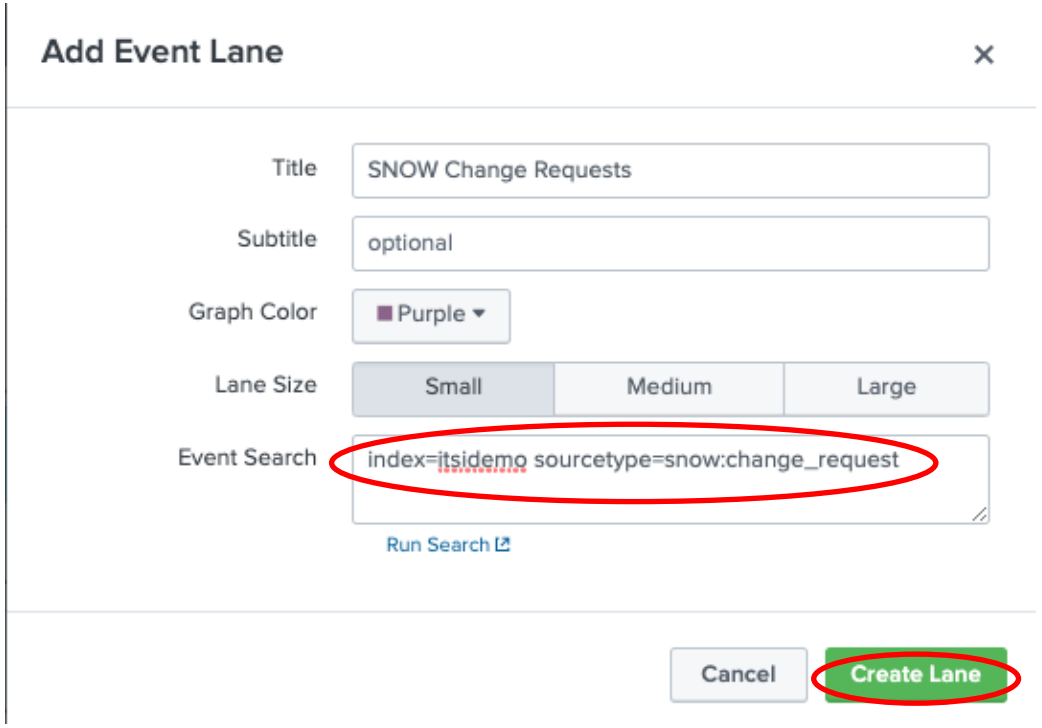
We will add another event lane to the deep dive to show us any change requests for the database service.

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



- Type ‘SNOW Change Requests’ Title
- Event Search:
  - *‘index=itsidemo sourcetype=snow:change_request’*

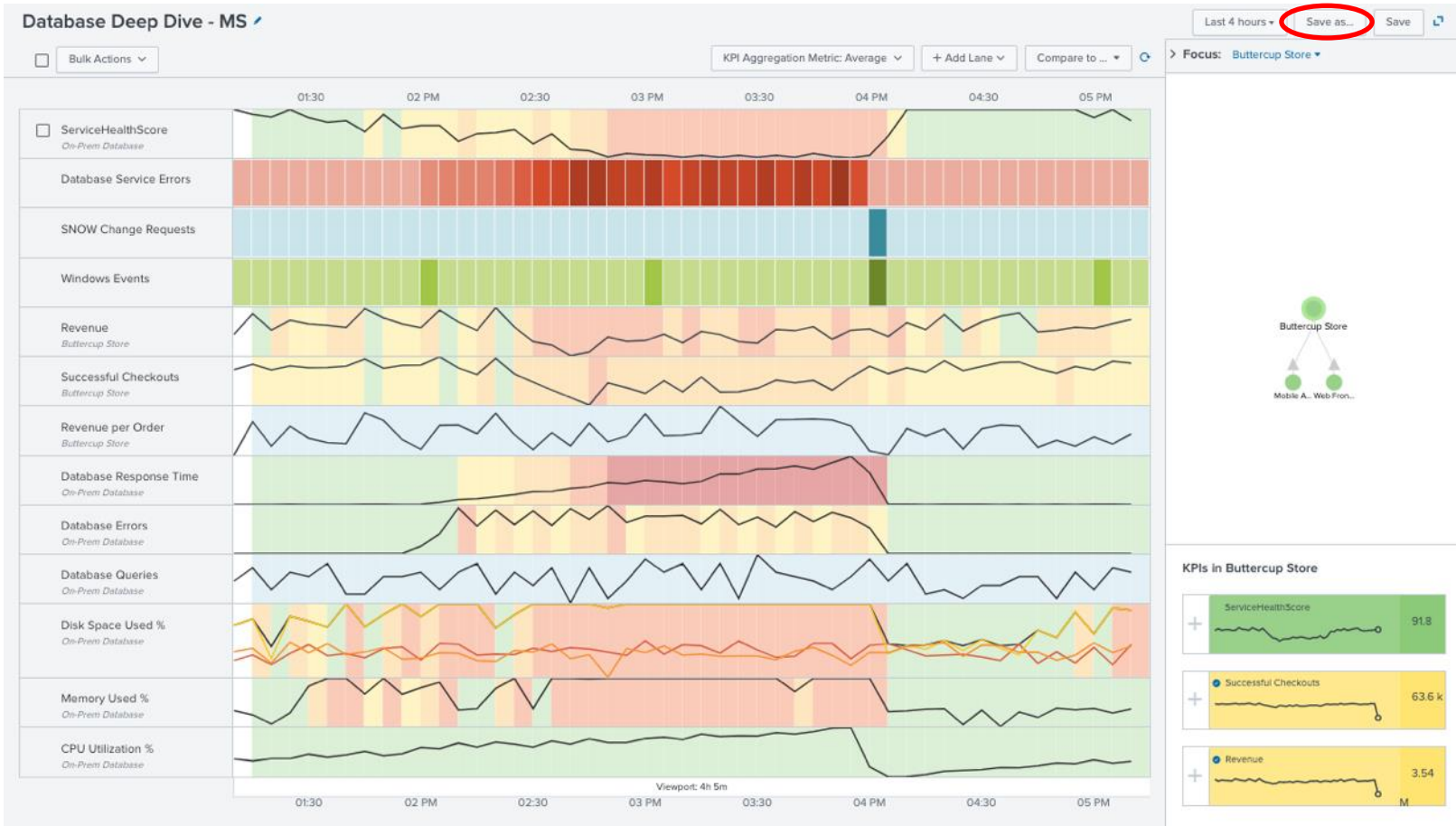
- Click ‘Create Lane’



Deep Dive Lab

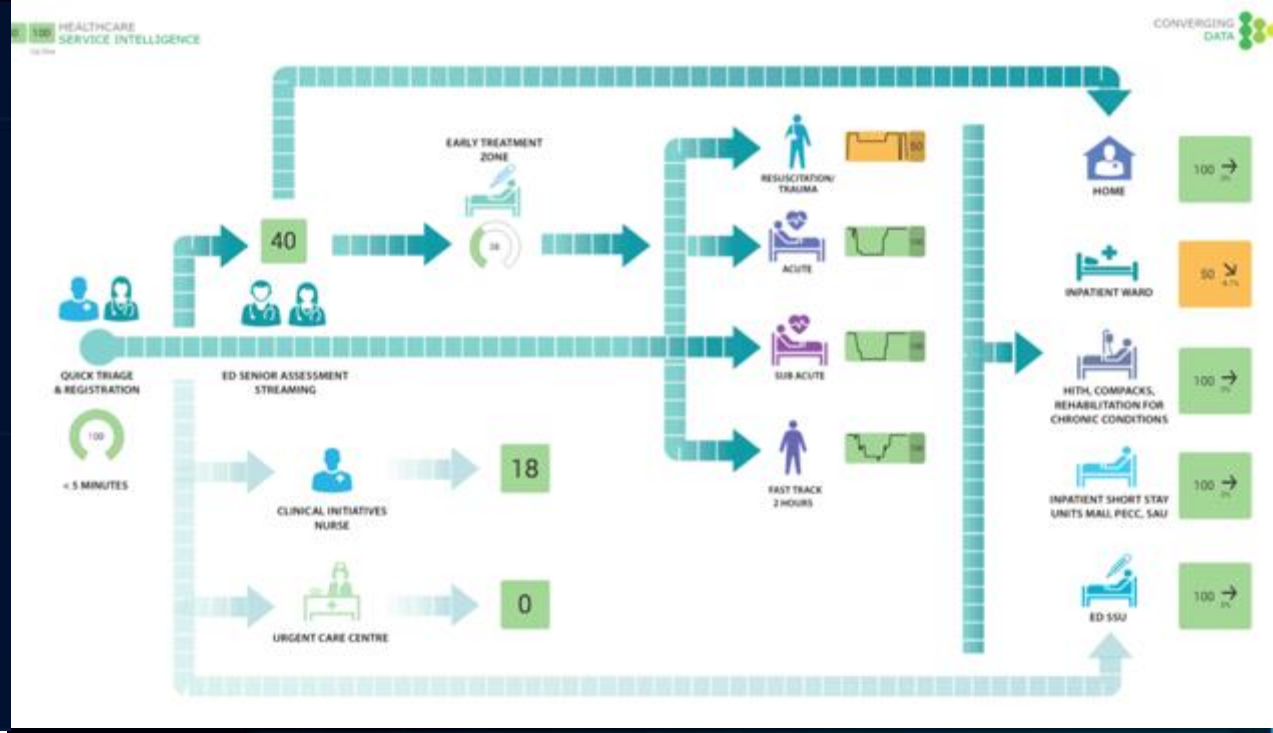
Once you have finished investigating the Deep Dive dashboard

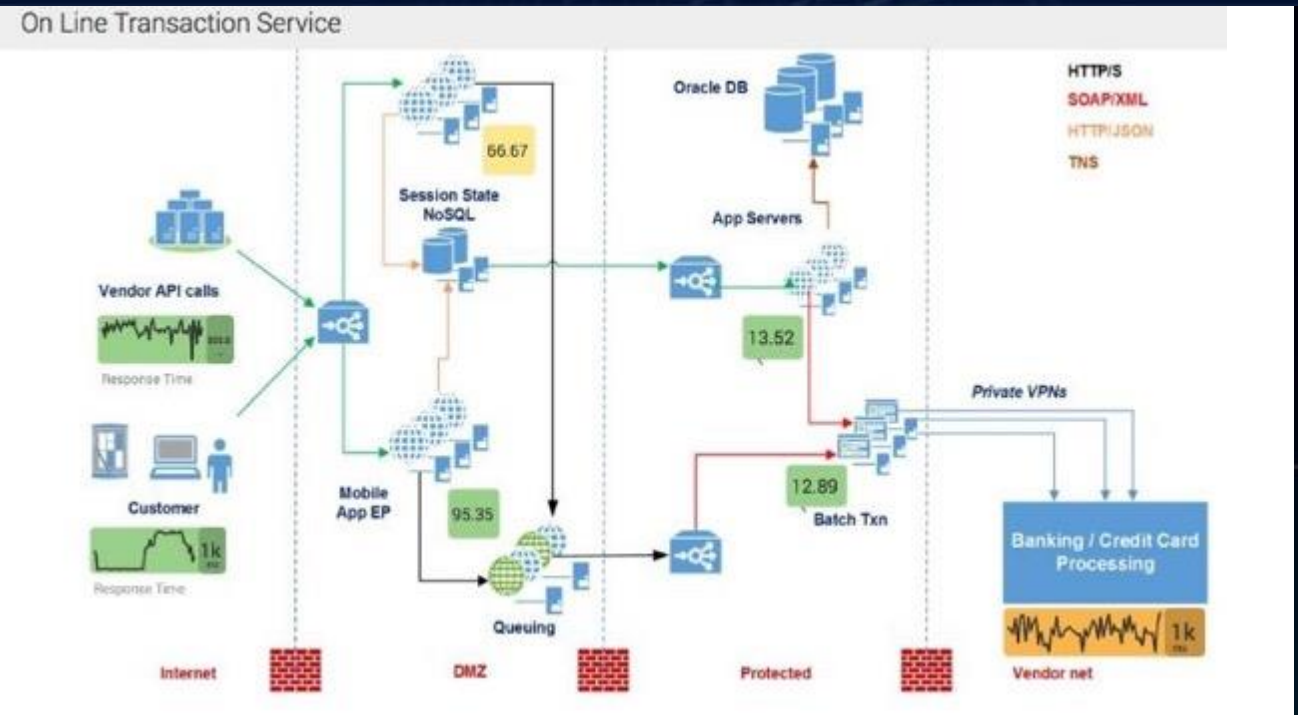
- Make sure you click '*Save As*'
- And save '*Database Deep Dive – <Your Initials>*'



Glass Tables


Splunk Bank
94
Mobile Banking Health Score
Account services
Account Listing
Product Application
Payments & Transfers
Account Management
95
92
85
94
80
32
80
53
Loans
Insurance
Direct Debit
Cheques
Help service
Statement services
Mortgage
Overdraft
Credit cards
Intl transfer
Chat bot
Credit cards
Savings
Standing orders
Intl orders
Live chat
Supporting services
Notification
98
Security
92
Authentication
94
Open Banking
97
Infrastructure
Presentation & Authentication layer
Service layer
Data layer
94
95
85
80
80
92
53
94
95
94
97
98
Firewall
Load Balancer
API gateway
Load Balancer
Microservices
ESB
Database
Core
Mainframe
2 factor
OpenBanking API


HEALTHCARE SERVICE INTELLIGENCE
CONVERGING DATA
EARLY TREATMENT ZONE
40
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
QUICK TRIAGE & REGISTRATION
< 5 MINUTES
ED SENIOR ASSESSMENT STREAMING
CLINICAL INITIATIVES NURSE
18
URGENT CARE CENTRE
0


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
1k
Internet
DMZ
Protected
Vendor net


Emergency Room
33
10 / 35
8 / 11
22
16 / 91
37%
Leeds Systems
92
HIS Health Score
Patient Infotainment
Power Mgnt
Medical Systems
Infrastructure
IT
Wifi
97
Storage
100
Staff support
Opened
In process
Closed
7
Escalation
FCR
Wait time
3
3
3MN

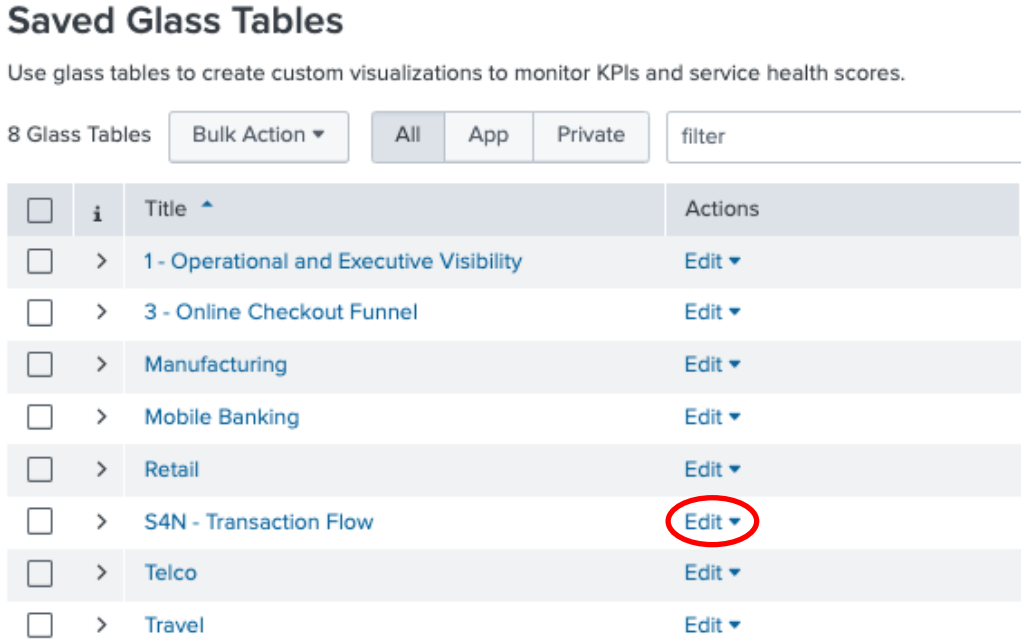
Glass Table Use Case

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

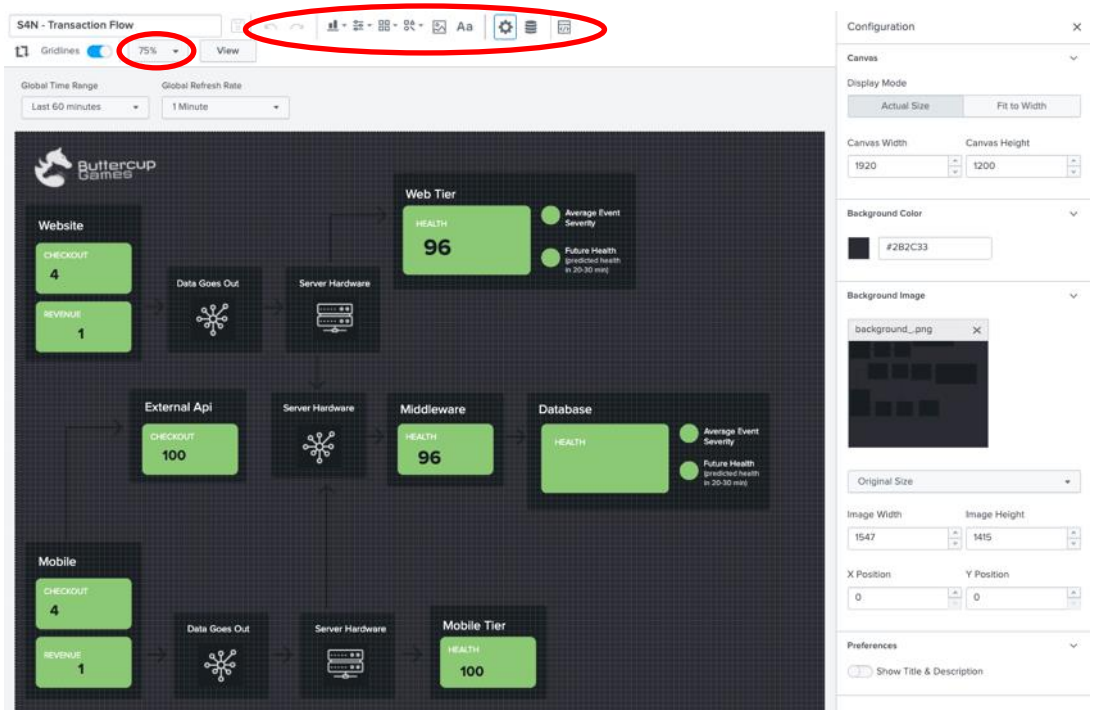
- The objective of this exercise is to complete the existing IT operations dashboard (S4N - Transaction Flow) with the new On-Prem Database service healthscore, including a drill down to a deep dive.

Glass Table Lab

- Select *Glass Table menu*
- *Edit ‘S4N - Transaction Flow’*

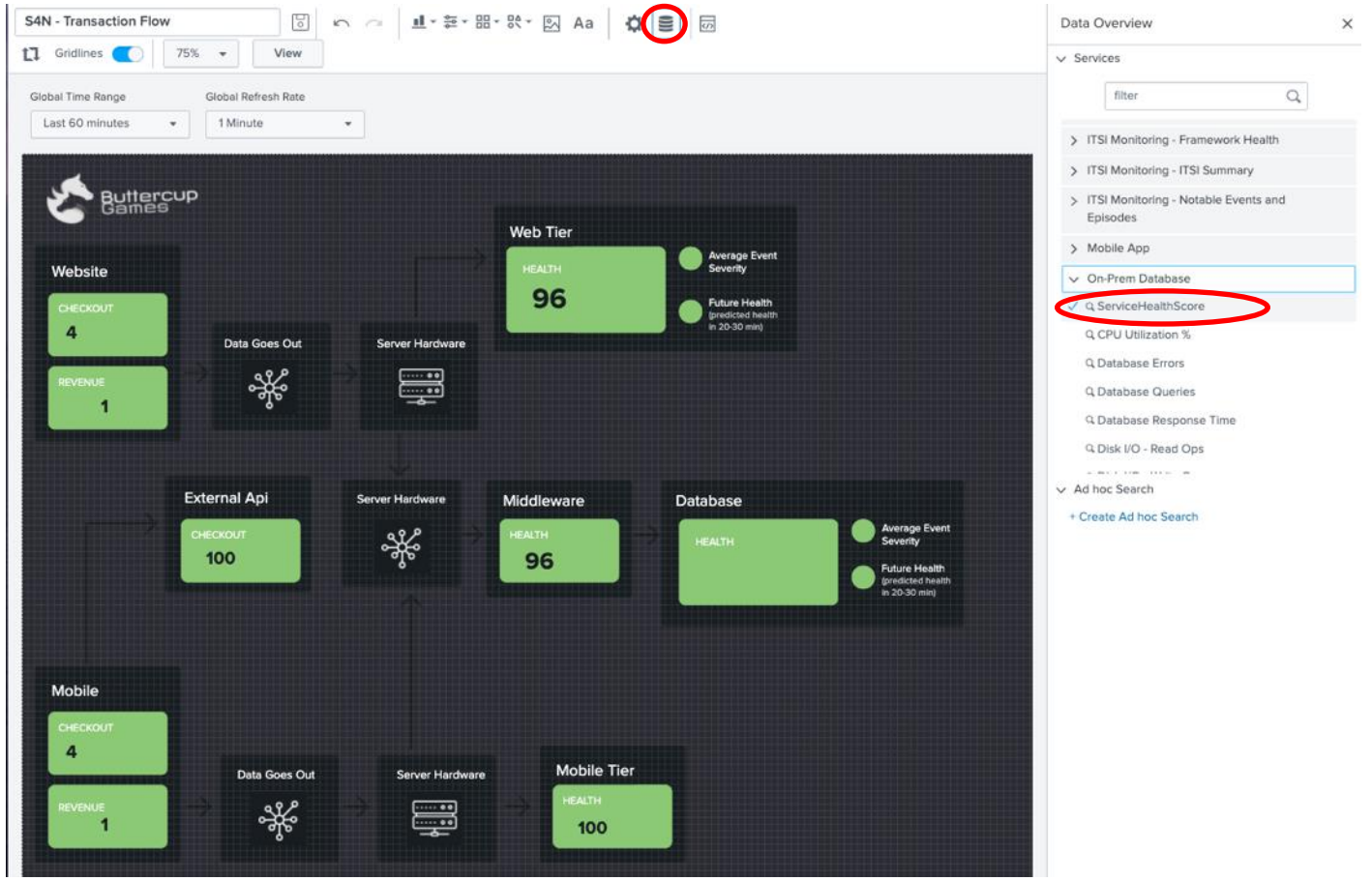


- Investigate the tool pallet icons
- *Modify zoom to fit to page*
- *Review the Configuration panel on right*



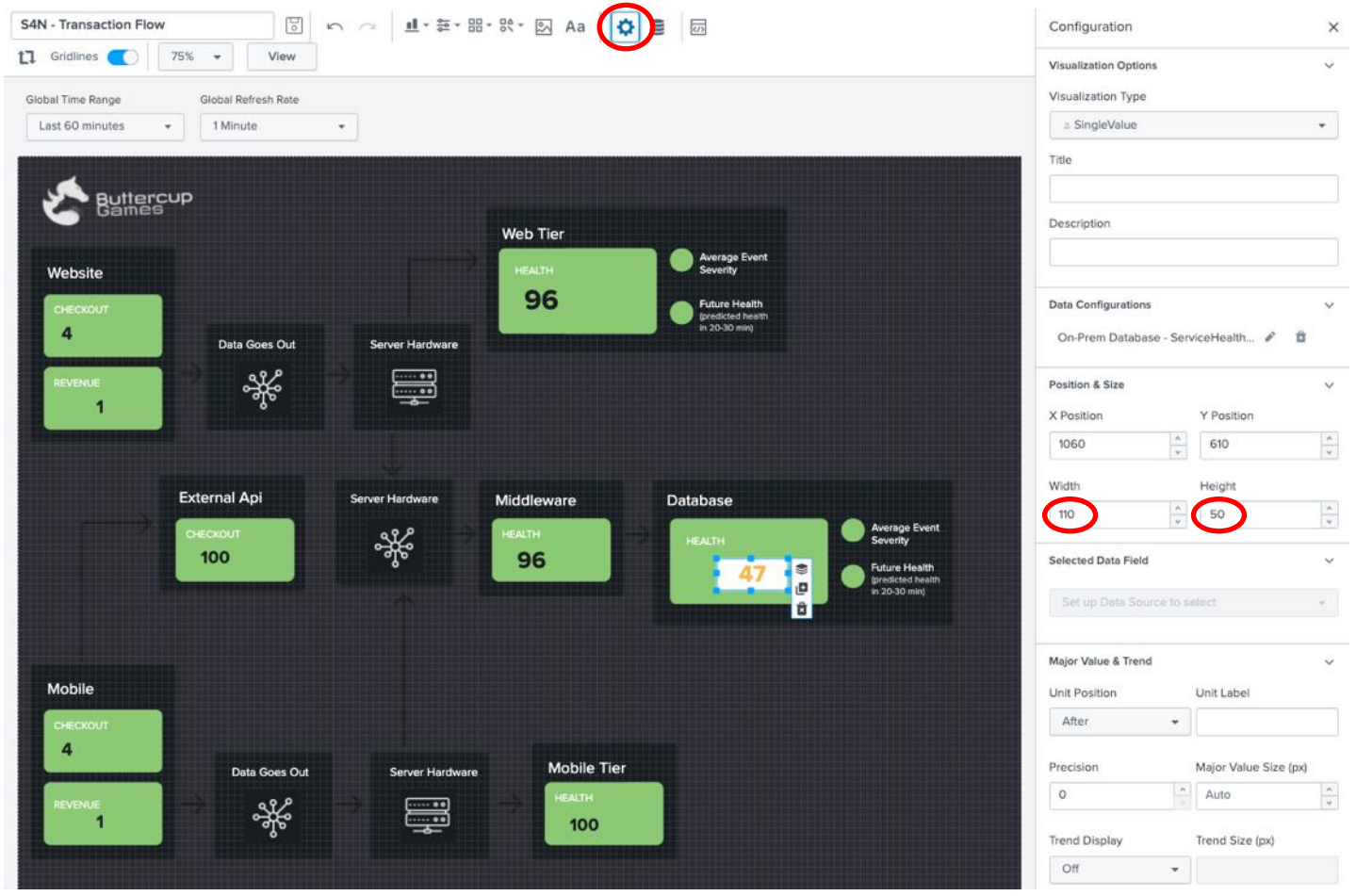
Glass Table Lab

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



Glass Table Lab

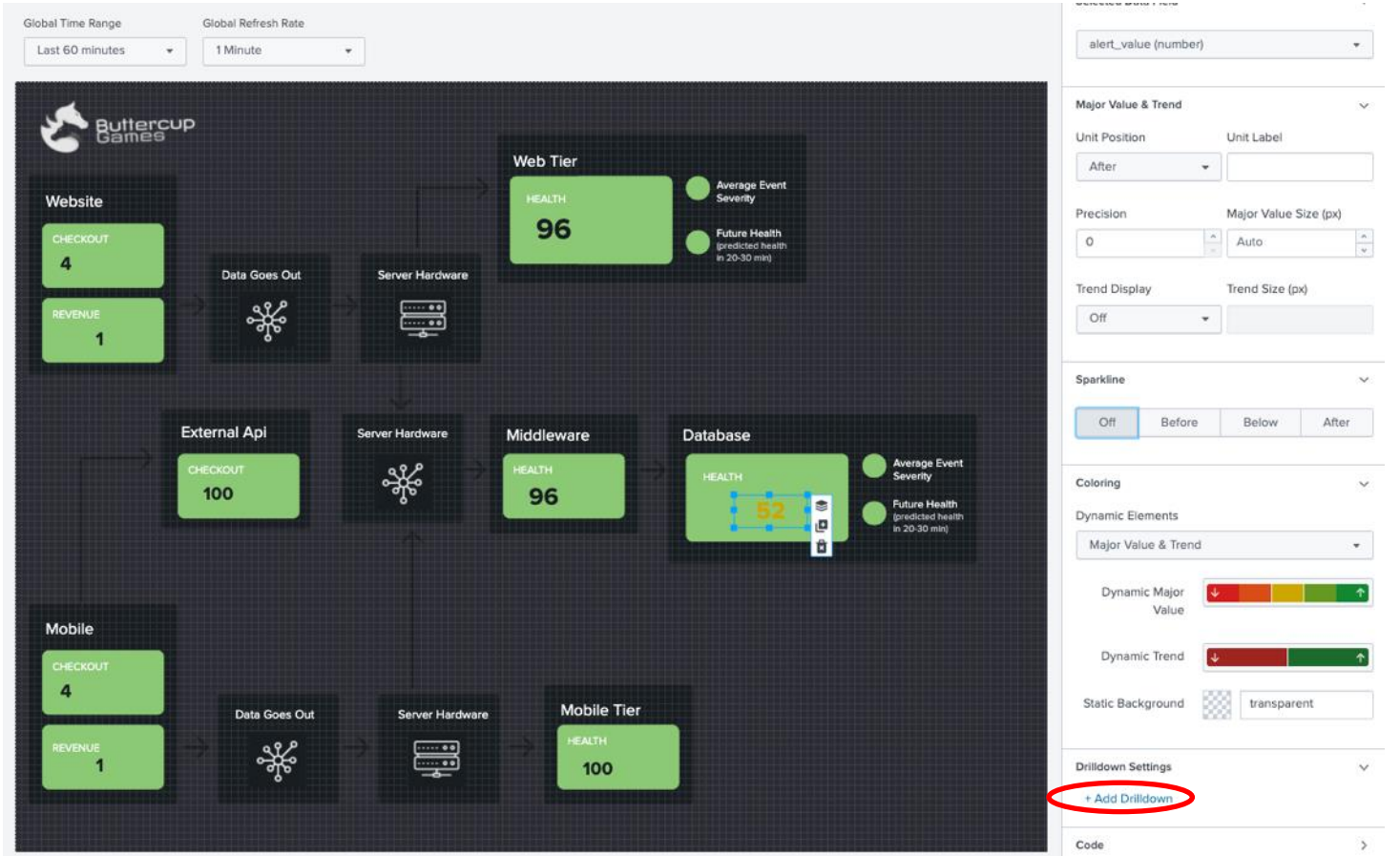
- Move the Service Health Score to the correct position
- Modify size to appropriate size and investigate options



Glass Table Lab

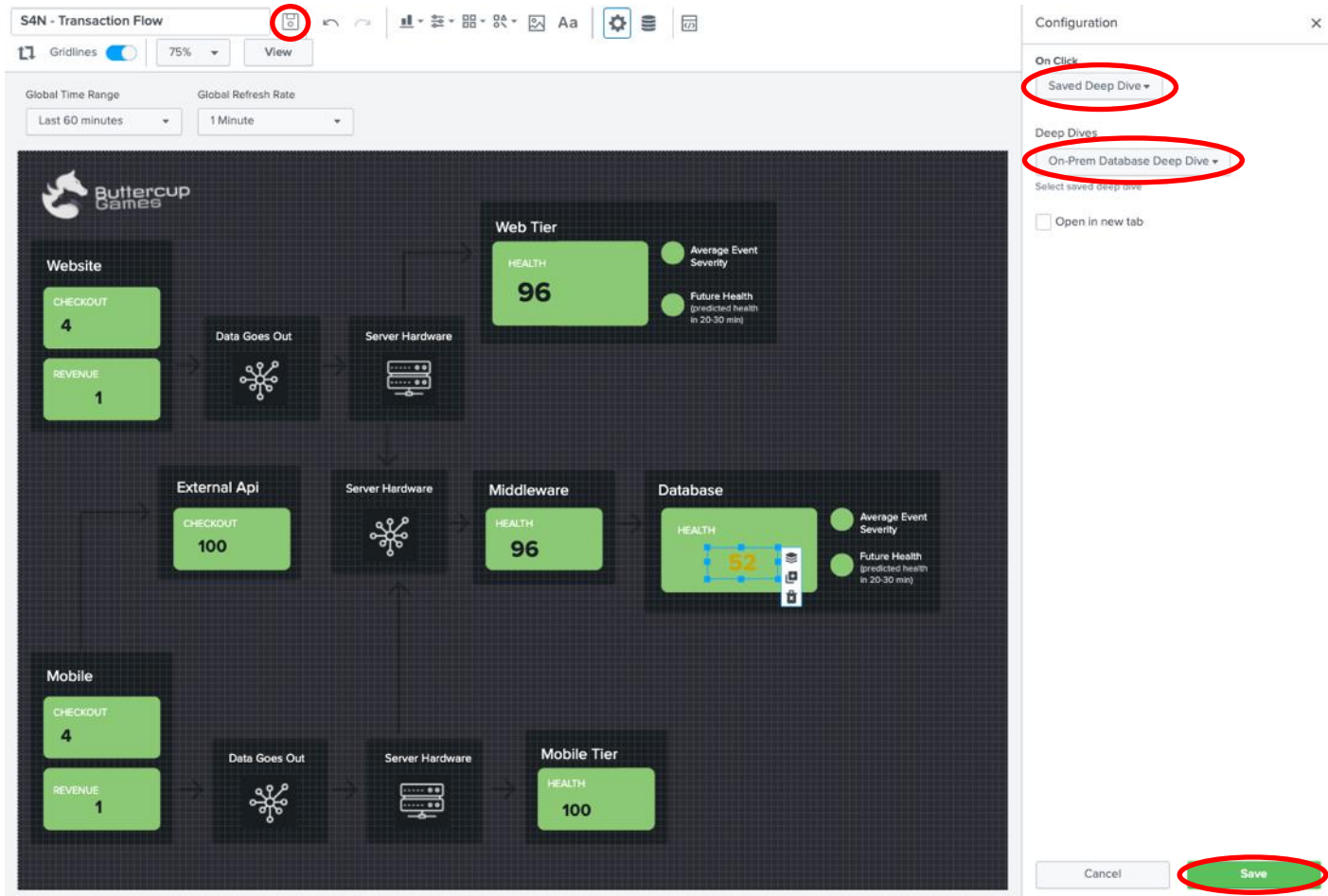
We will now link the database deep dive visualization to this glass table

- Click Add Drilldown



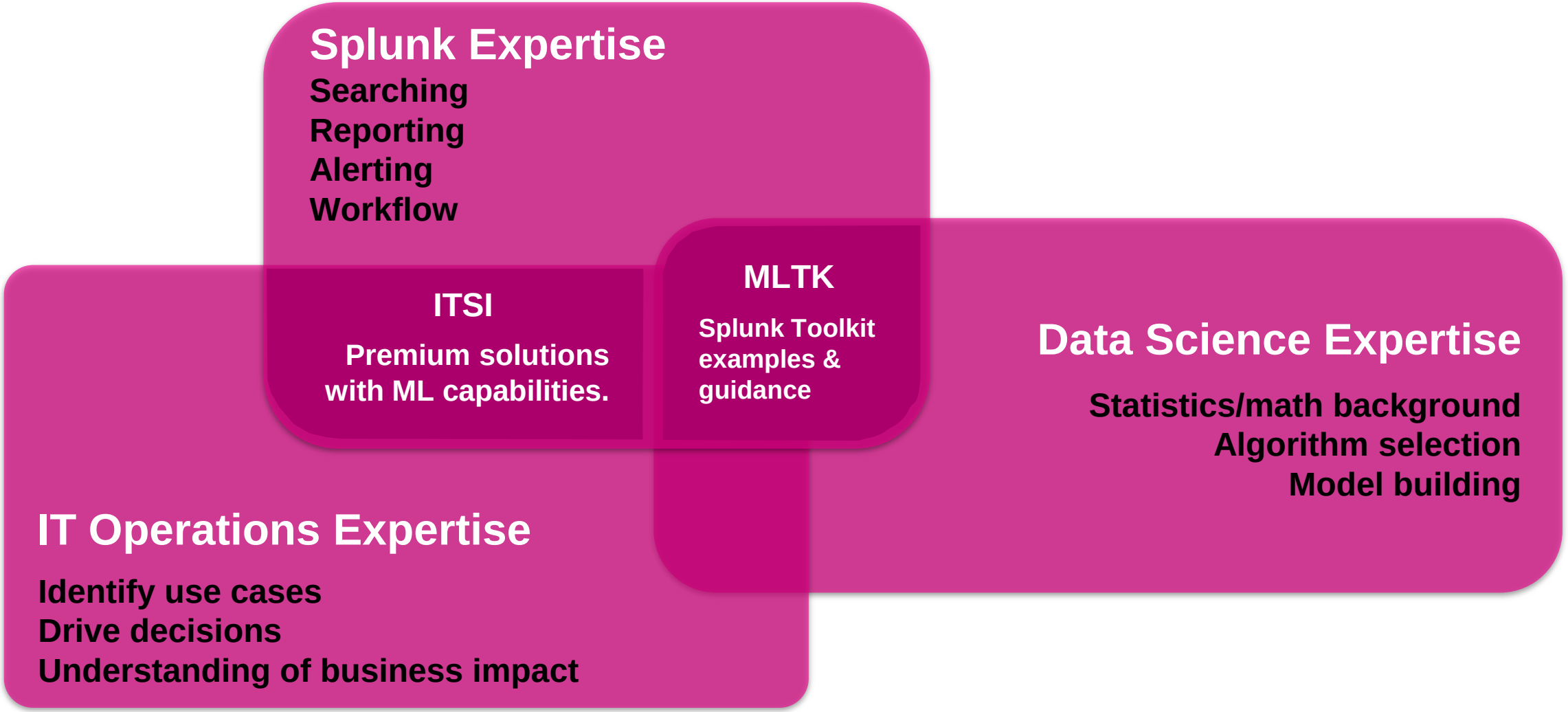
Glass Table Lab

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



Machine Learning

Machine Learning Blend

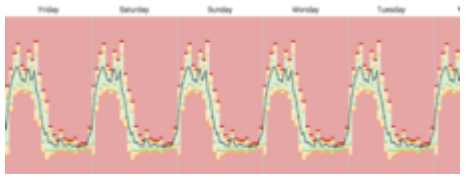


ITSI Machine Learning

Anomaly Detection

Deviation from past behavior
Deviation from peers
Unusual change in features
ITSI Anomaly Detection

Adaptive Thresholds

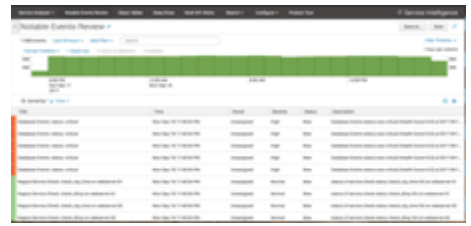


Adaptive Thresholds
What is normal behaviour and what is not normal
Ideal for cyclical and dynamic data

Predictions Analytics

Predict Service Health Score
Predicting events
Trend forecasting
Early warning of failure
Predictive maintenance

Event Clustering



Identify peer groups
Event correlation
Reduce alert noise
ITSI Event Analytics

Machine Learning Use Case

There have been lots of social media comments regarding Buttercup' website availability, especially during the evenings.

Luckily the website data is being ingested by Splunk, this sourcetype is called 'access_combined' and contains lots of information.

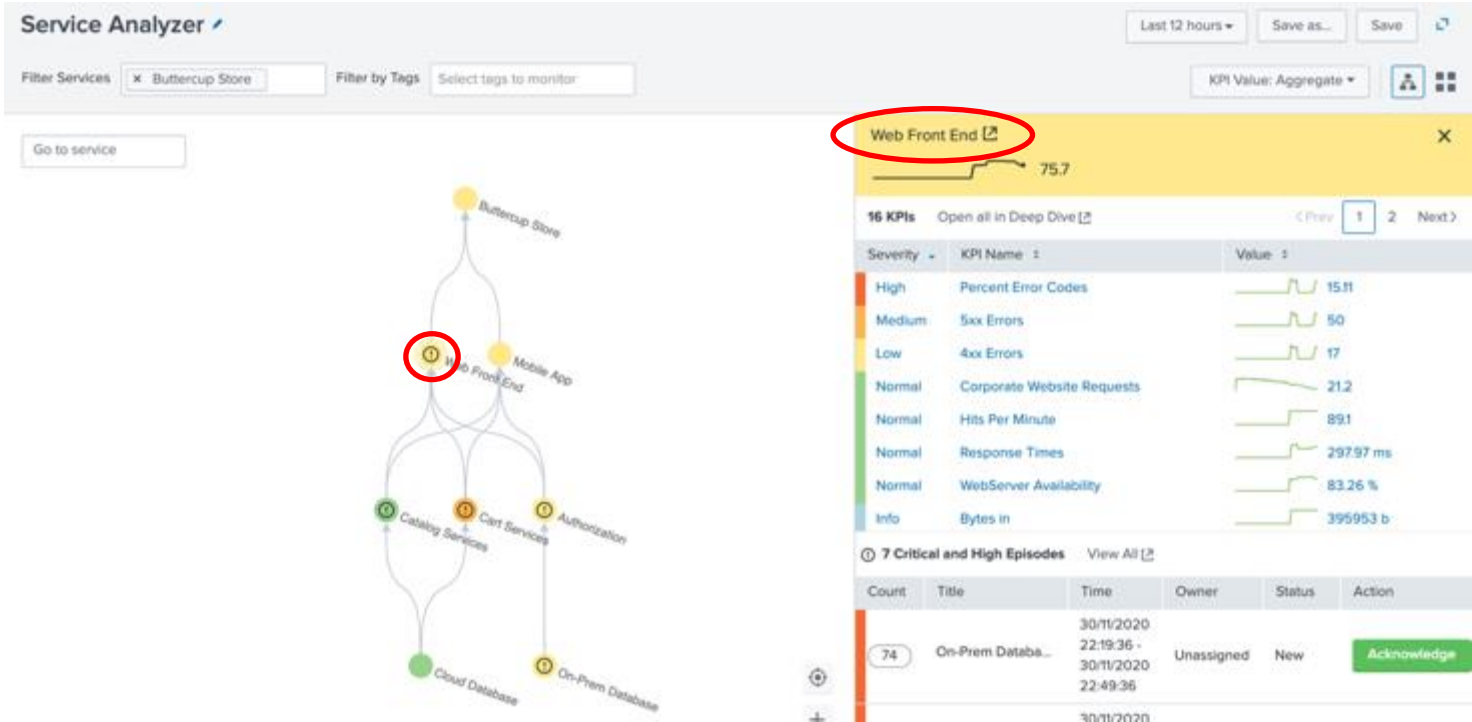
The objective of this exercise to is utilise Splunk ITSI machine learning capabilities to identify normal behaviour for web response time.

We will also look to see if the application servers supporting the website are functioning equally.

Machine Learning Lab

The Corporate Website Request KPI has no thresholding for alerting. In this lab we will configure machine learning to understand what normal looks like and alert us when the KPI falls outside this range.

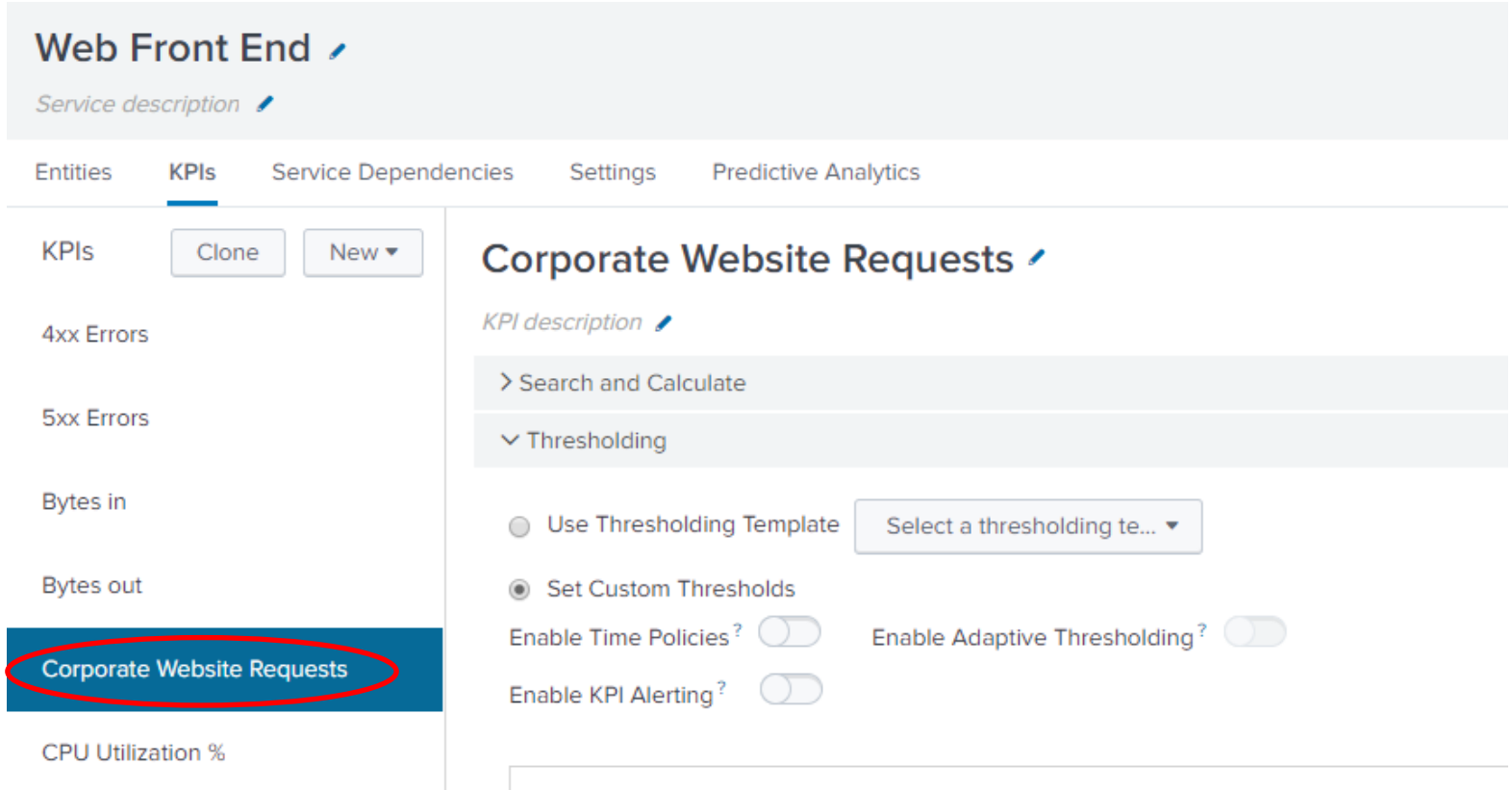
- Go to the '*default*' service analyzer view and expand the tree view
- Click '*Web Front End*' service
- Select the *'Web Front End*' link



Machine Learning Lab

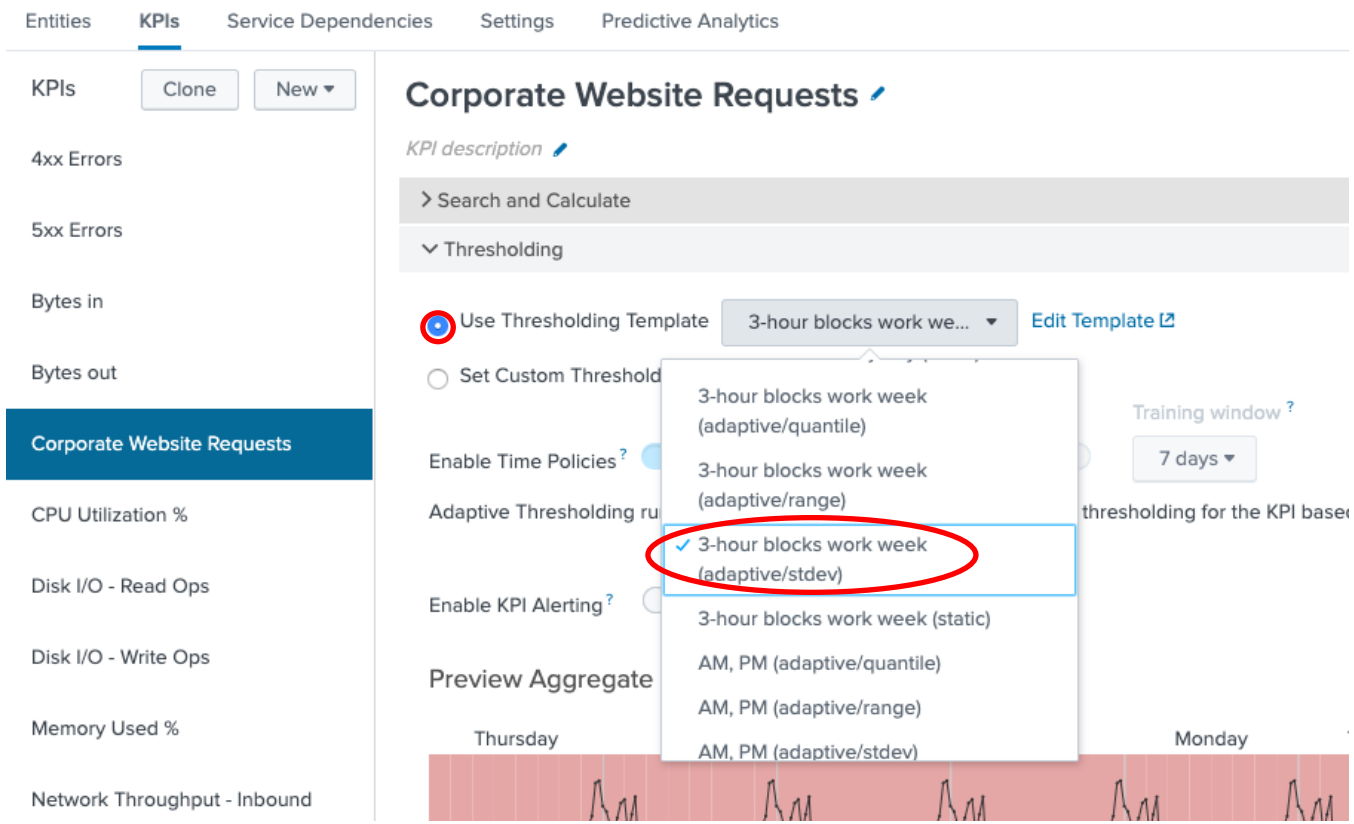
We need to instruct ITSI to use a template for thresholding, we will be using the adaptive standard deviation 3 hour working week template.

- Select the '*Corporate Website Requests*' KPI

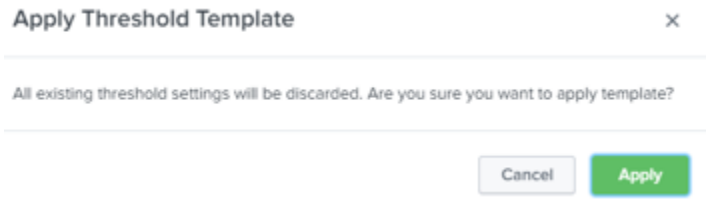


Machine Learning Lab

- Select Thresholding Panel
- Select '*use Thresholding Template*' button
- Review the different options
- Select '*3-hour blocks work week*'
  - *(adaptive/stdev)*



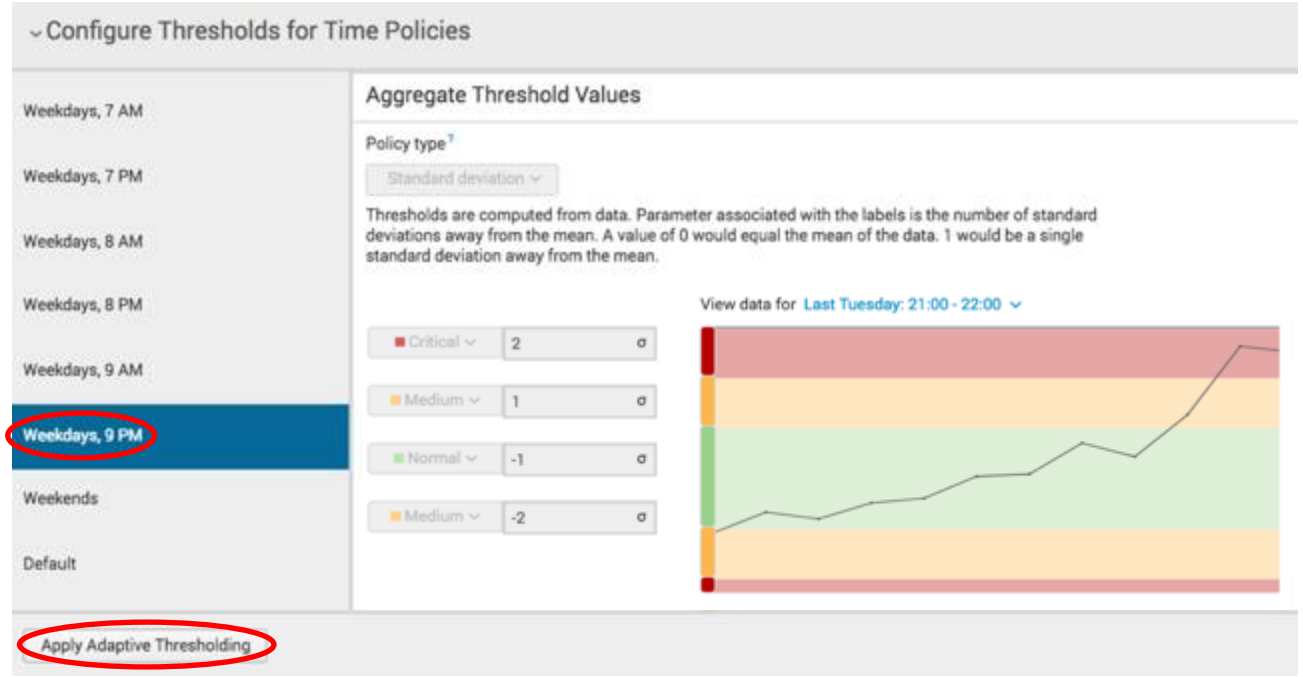
- Click 'Apply' button



Machine Learning Lab

The built-in machine learning has configured thresholds, this is broken into 3-hour time ranges. However we want to use historical data to apply some adaptive thresholding.

- Open the ‘Configuration thresholds for Time Policies’ box
- Review different times
  - Choose ‘*Weekdays, 9am-12am*’
- Click ‘*Apply Adaptive Thresholding*’ button
  - Wait 30 Seconds
- Notice threshold
- Click ‘Save’ button

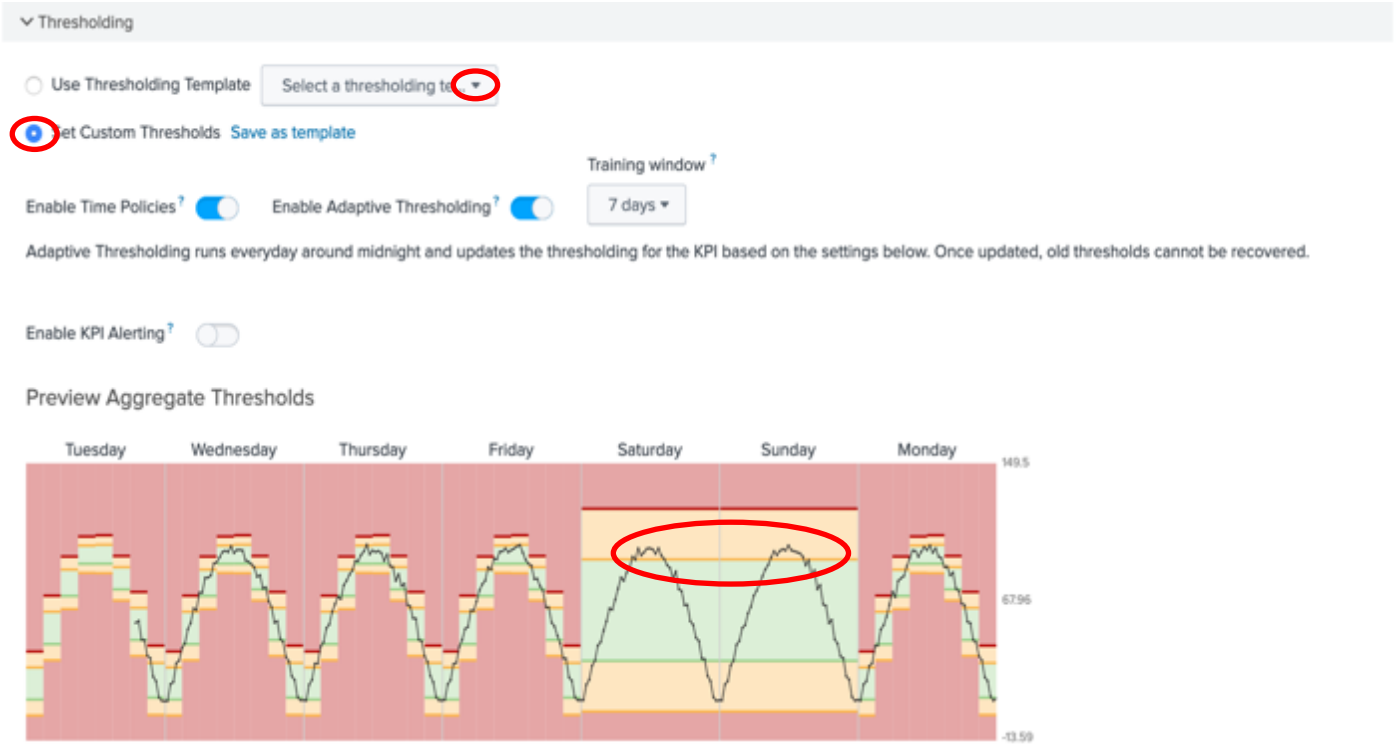


Machine Learning Lab

Internal SLAs do not apply on weekends, tracking is still necessary, but management wants deliberately higher values.

We will now modify the new adaptive thresholds to increase the weekend ranges, this will result in a custom template.

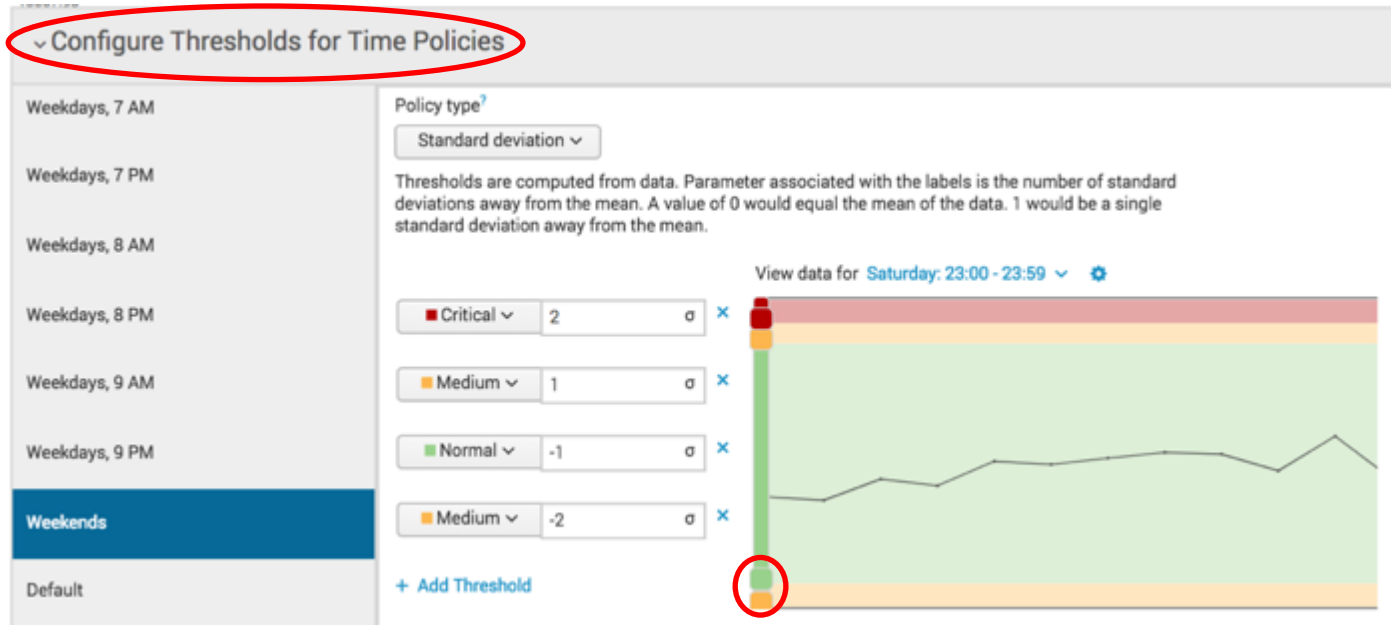
- Click on '*Thresholding*' arrow
- Review the preview window
  - Note weekend range
- Click '*Set Custom Threshold*'



Machine Learning Lab

We will now modify the new adaptive thresholds to increase the weekend ranges, this will result in a custom template.

- Expand '*Configure Thresholds for Time Policies*'
- Click '*Weekends*'
- Move all sliders as shown
- Click '*Apply Adaptive Thresholding*'



Machine Learning Lab

Having changed the sliders as shown and hitting “apply Adaptive thresholding for some reason my result still shows breaches

- Click ‘Save’ button

Machine Learning: Predictive Analytics

What's Prediction Analytics?

It's as Sexy as it sounds

Using historical KPI data and some clever ML algorithms, you can **predict an outage** 20-30 minutes before it happens!

Works best when a service has 5+ good KPIs and 1+ week of historical data

The algorithm looks for recognizable/predictable KPI behavior, which comes before the service's aggregate health score changes.

- For example: before the last outage, CPU usage went up AND garbage collection times increased AND session counts dropped...

Workshop Use Case

The IT operations team are struggling to resolve issues with the company ‘On-Prem Database’ service, typically outages are reported via customers contacting the service desk to complain.

They would like to use machine learning to predict health score degradation 30 minutes before it causes a service outage.

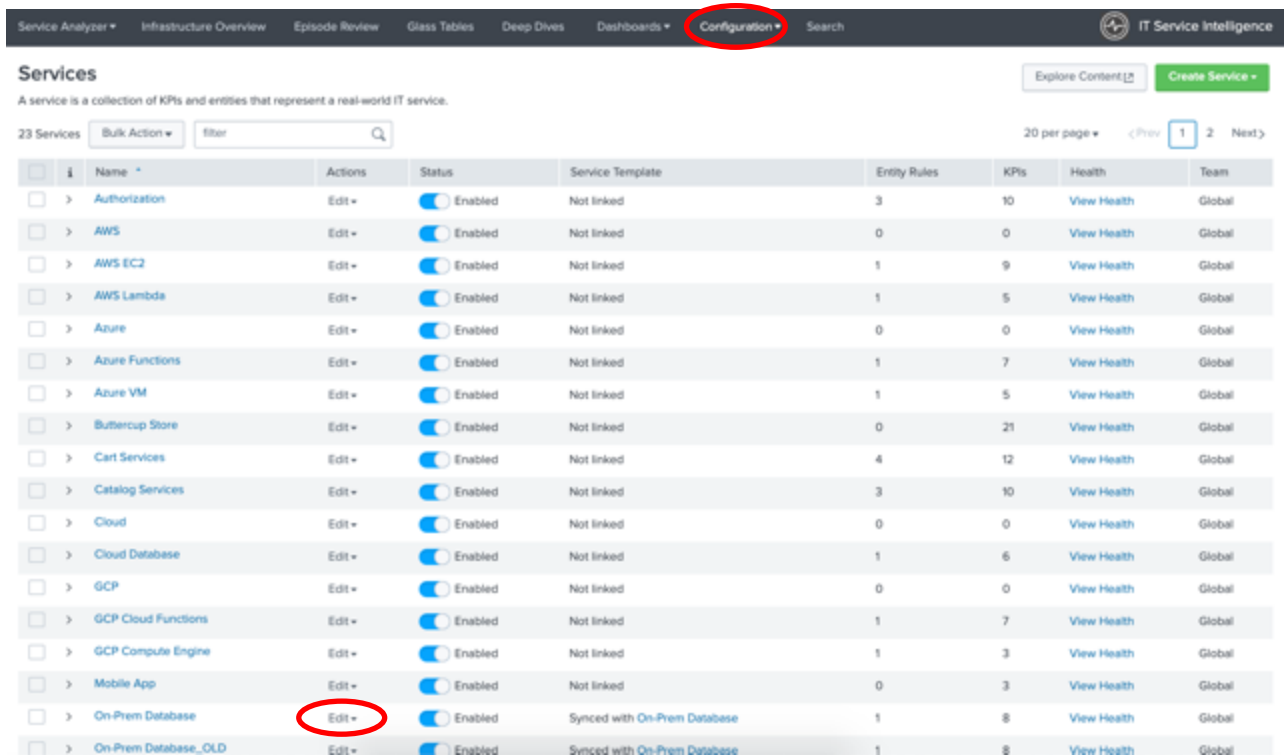
The objective of this lab will be to use the ‘**On-Prem Database**’ health score to build a predictive algorithm model to predict future issues.

- *Extra : this new KPI can be copied on the glass table if time permits.*

Predictive Analytics Lab

We need to use machine learning to build a model for the On-Prem Database service. This model will be used in the second part of this lab.

- Select '*Configuration*' > '*Services*' item
- Click edit '*On-Prem Database*' service
- Select '*Edit*' menu

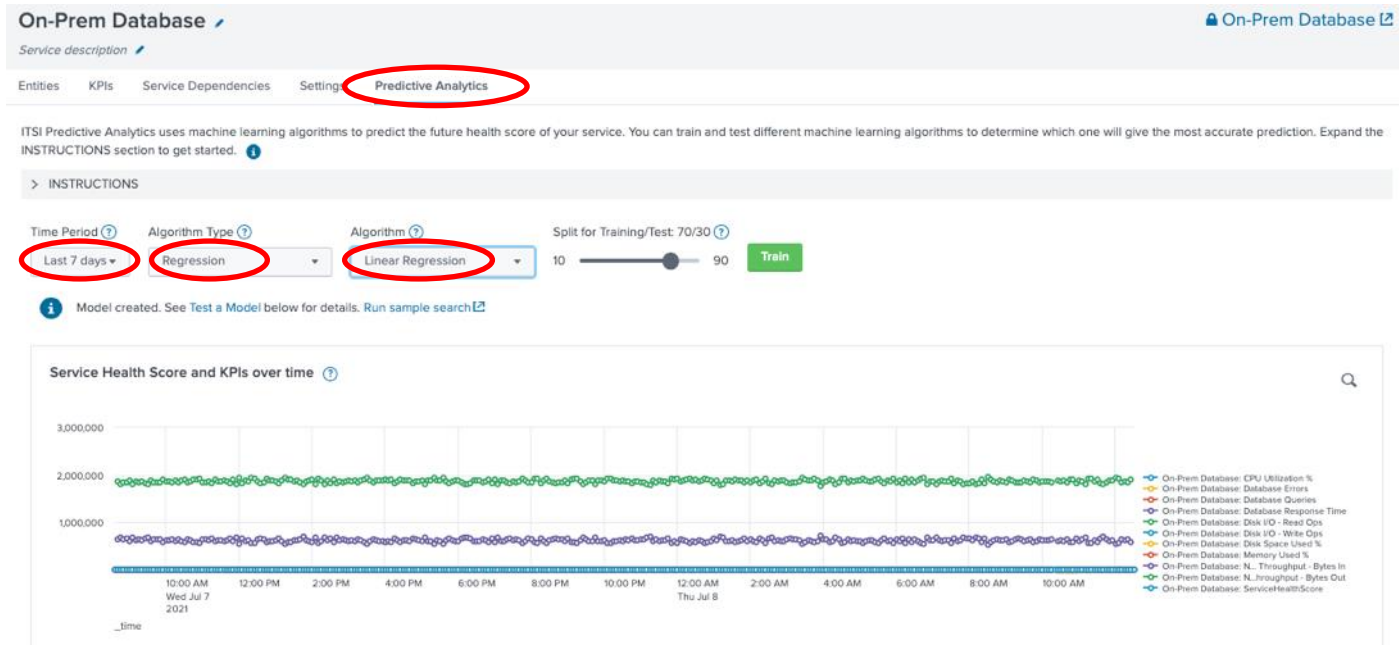


Predictive Analytics Lab

ITSI Predictive Analytics uses machine learning algorithms to predict the future health score of your service. On this screen we will train and test different machine learning algorithms to determine which one will give the most accurate prediction.

- Select '*Predictive Analytics*'
- Time = 7 Days
- Algorithm Type = Regression
- Algorithm = Linear Regression
- Click 'Train' button

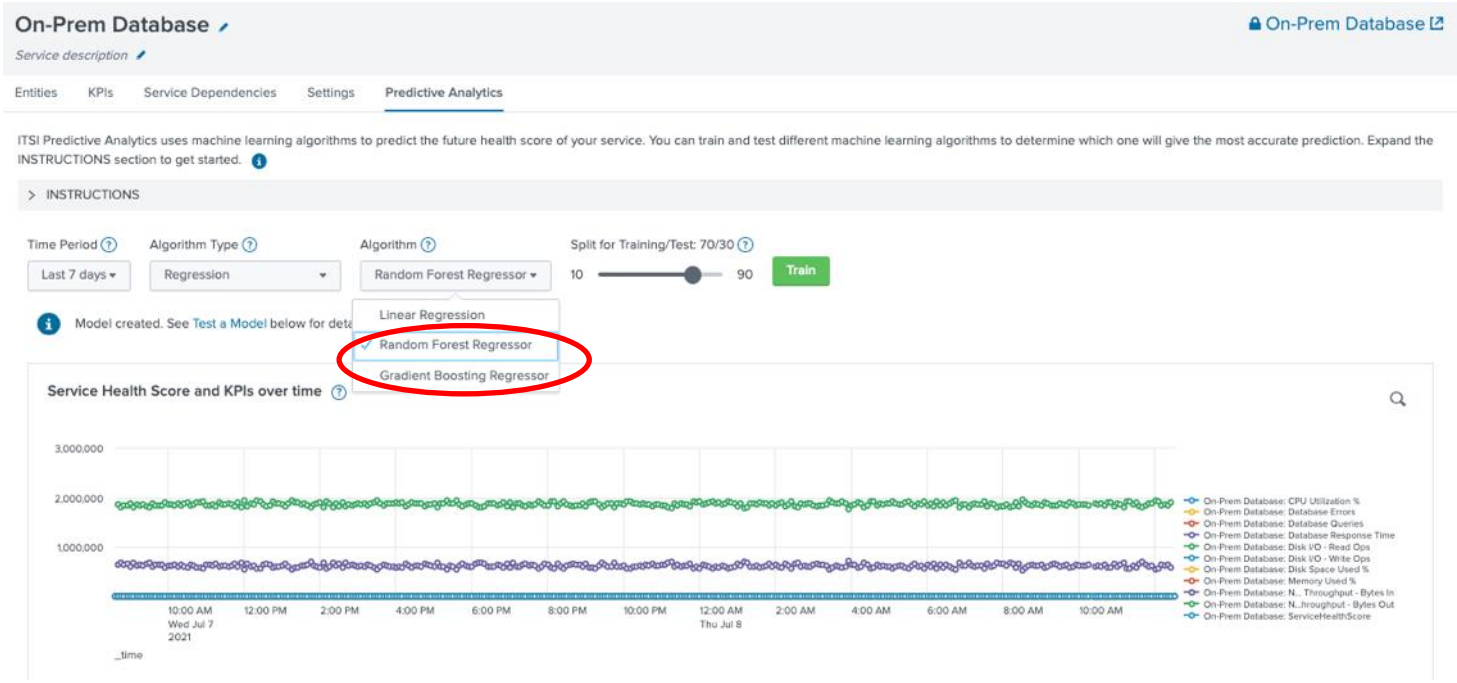
- Once the model has run, investigate results below.
- Click '*Save*'



Predictive Analytics Lab

- Repeat the previous steps for the other two algorithms over 14-day period.
- Random Forest Regressor
- Click *'Train*' button
- Remember '*Save*' button !

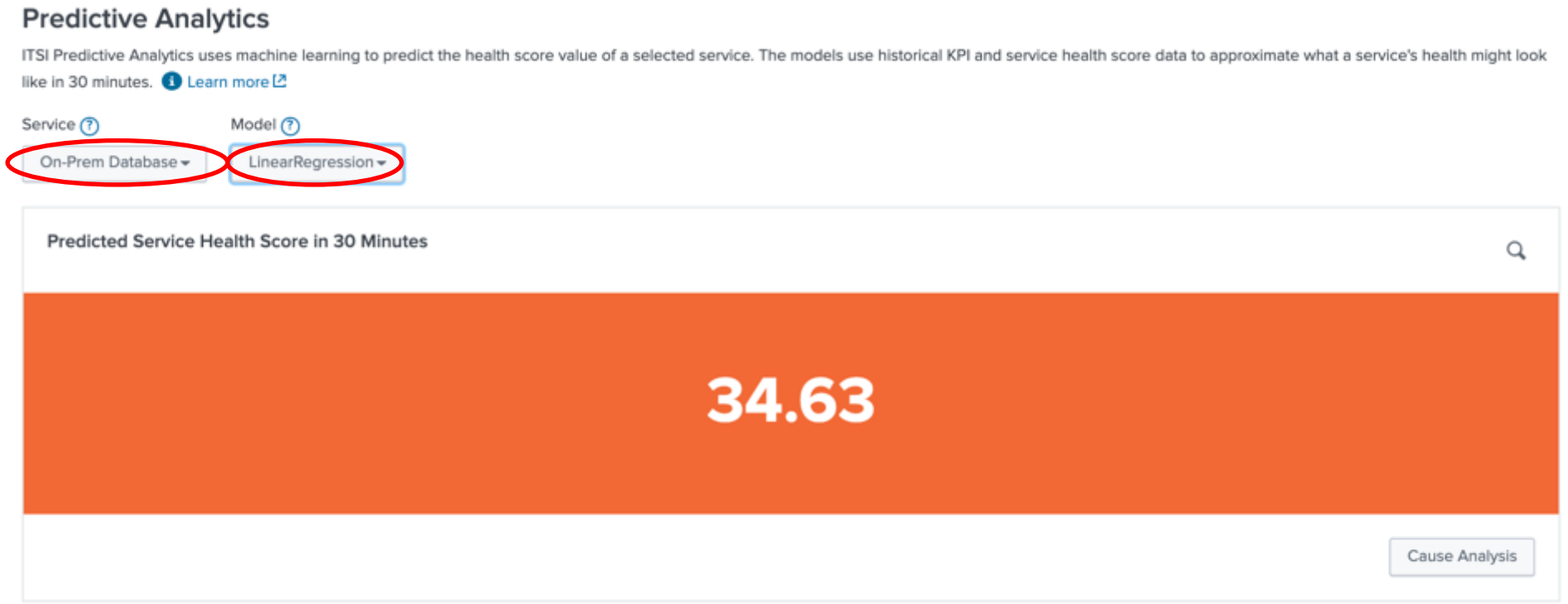
- Gradient Boosting Regressor
- Click *'Train*' button
- Remember '*Save*' button !



Predictive Analytics Lab

In this lab we are going to review the predictive analytics value for the **On-Prem Database** service using the recommended model.

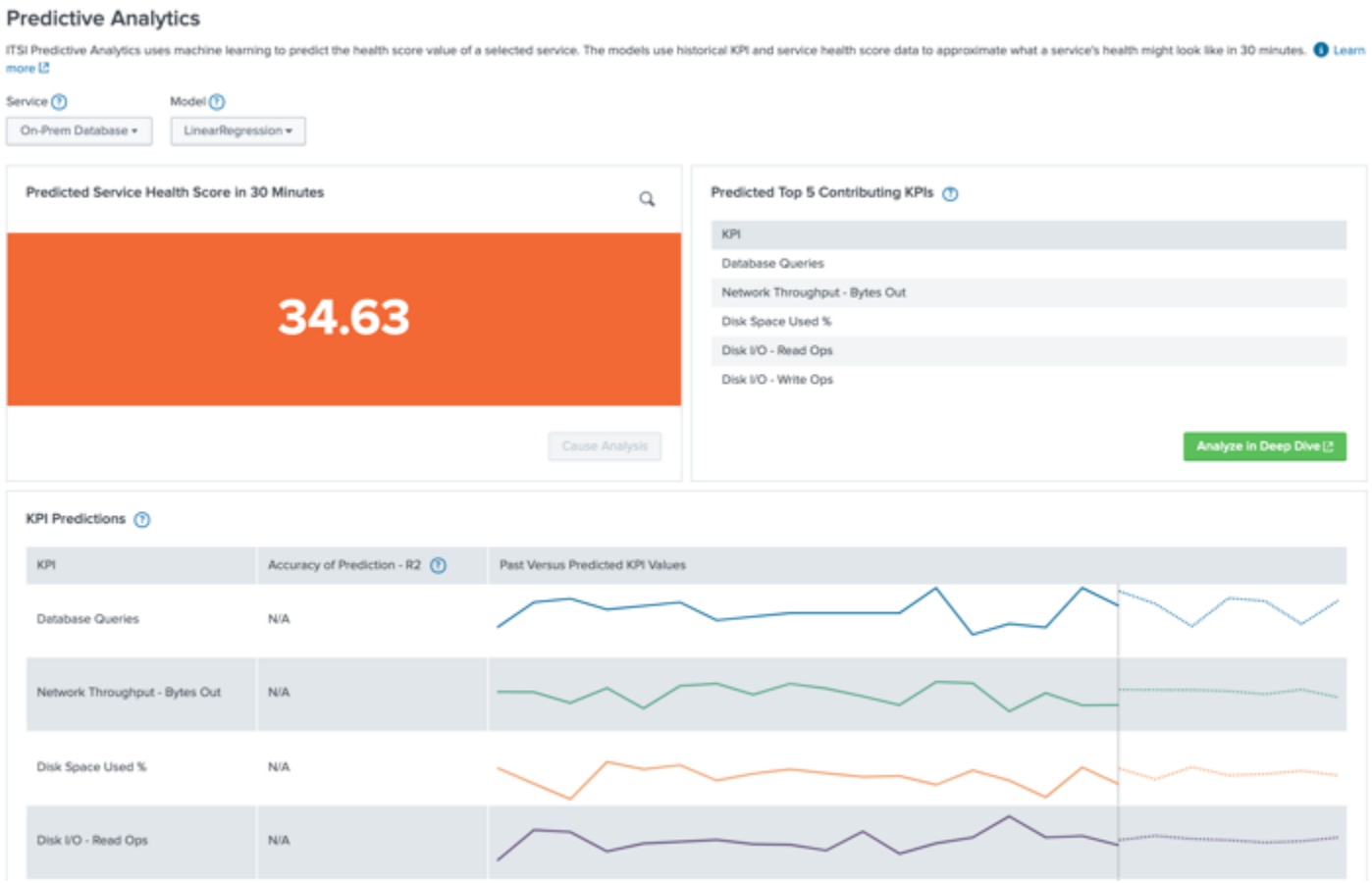
- Select *Dashboards* > *Predictive Analytics*
- *Select the 'On-Prem Database' service*
- *Select the recommended algorithm model*



Predictive Analytics Lab

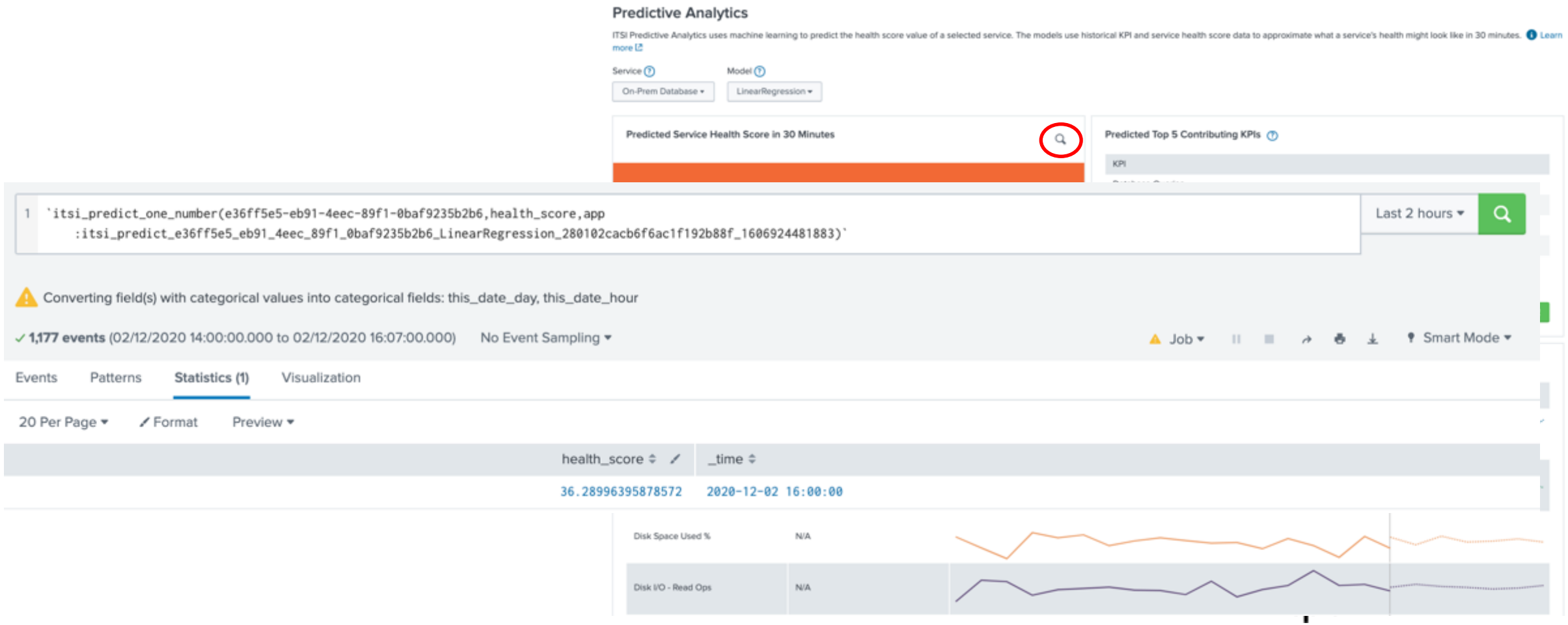
Once we have selected a model ITSI will calculate the future healthscore

- *Click ‘Cause Analysis’ button to review the suggested KPIs*



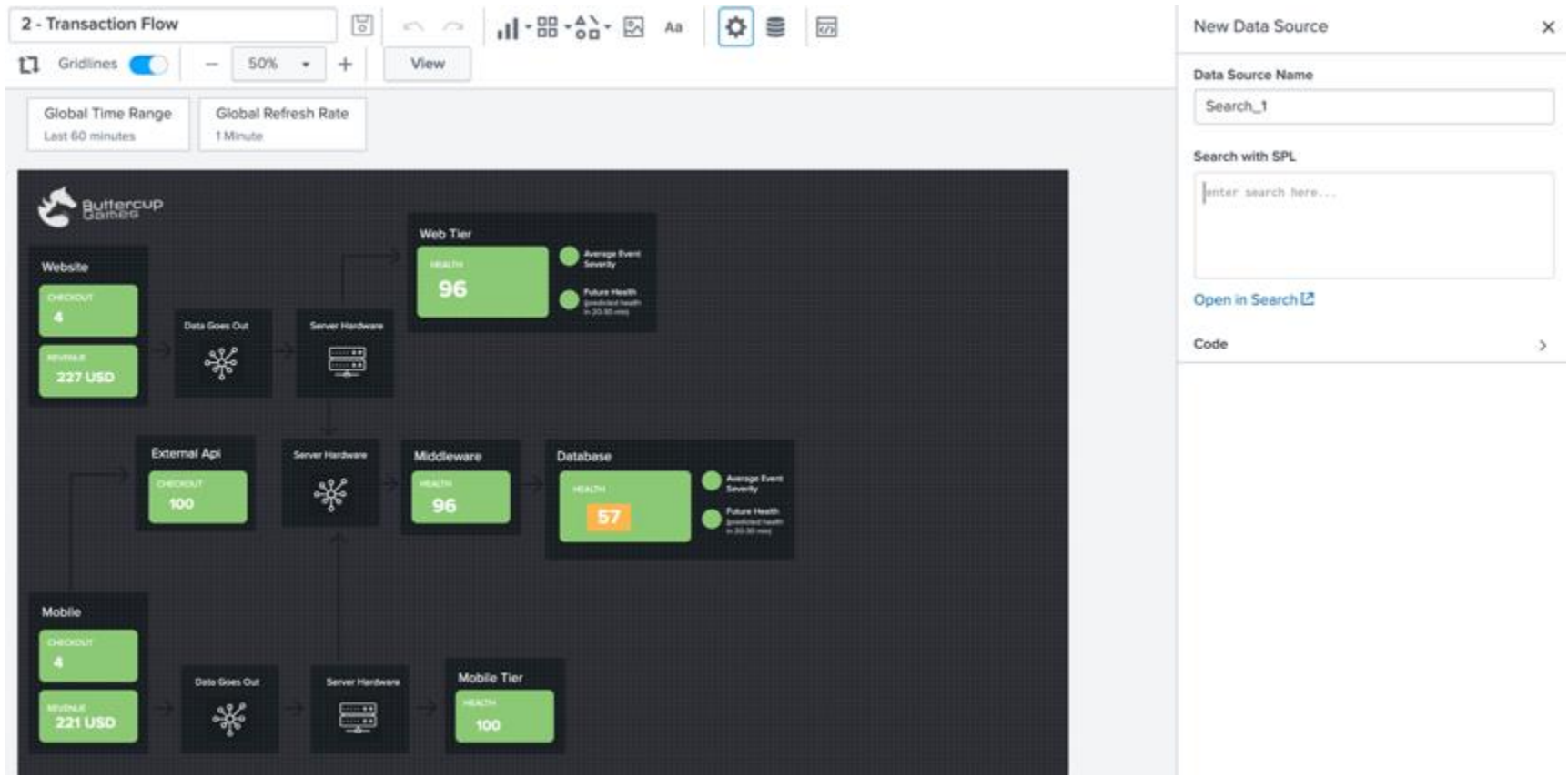
Predictive Analytics Lab

- Click the spyglass to review the SPL
- This SPL can be copied to our glass table, for now save to a notepad



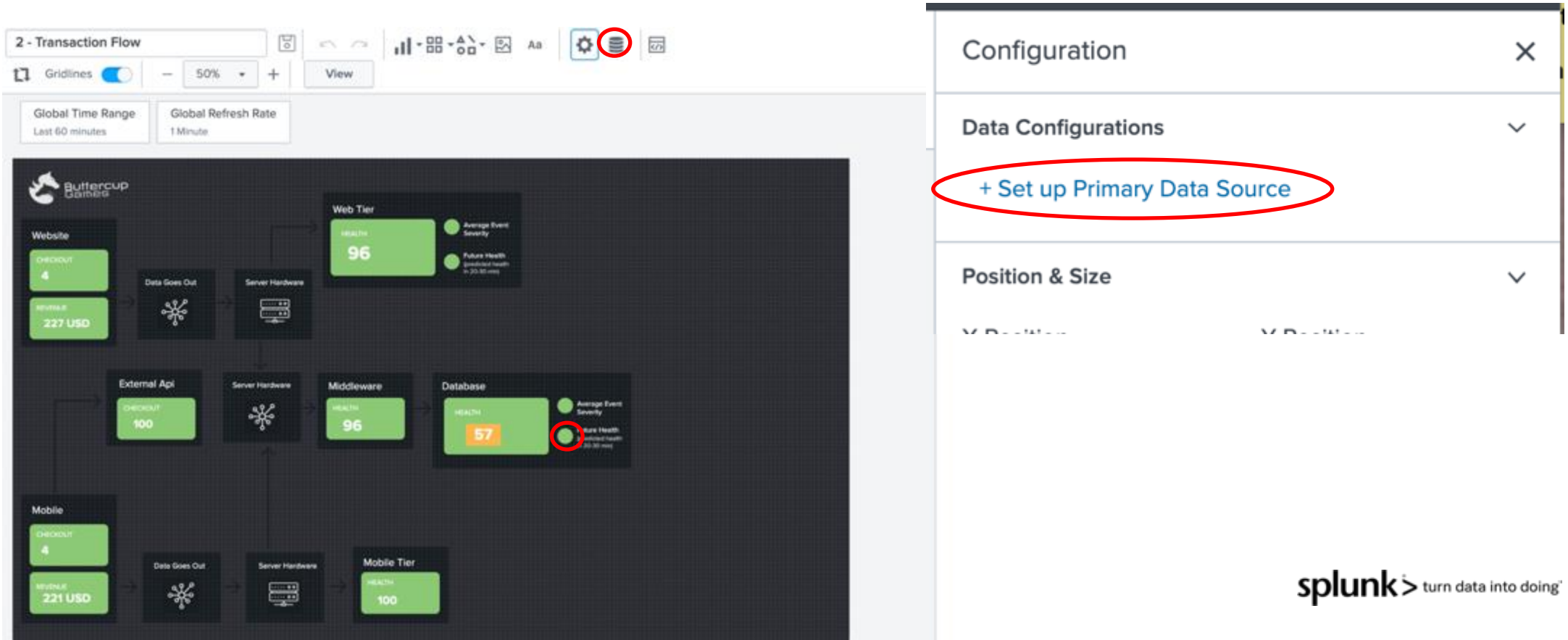
Predictive Analytics Lab

- Select ‘Glass Tables’ > ‘S4N - Transaction Flow’
- Click ‘Edit’ button
- Review the Database Future Health-Score attributes



Predictive Analytics Lab

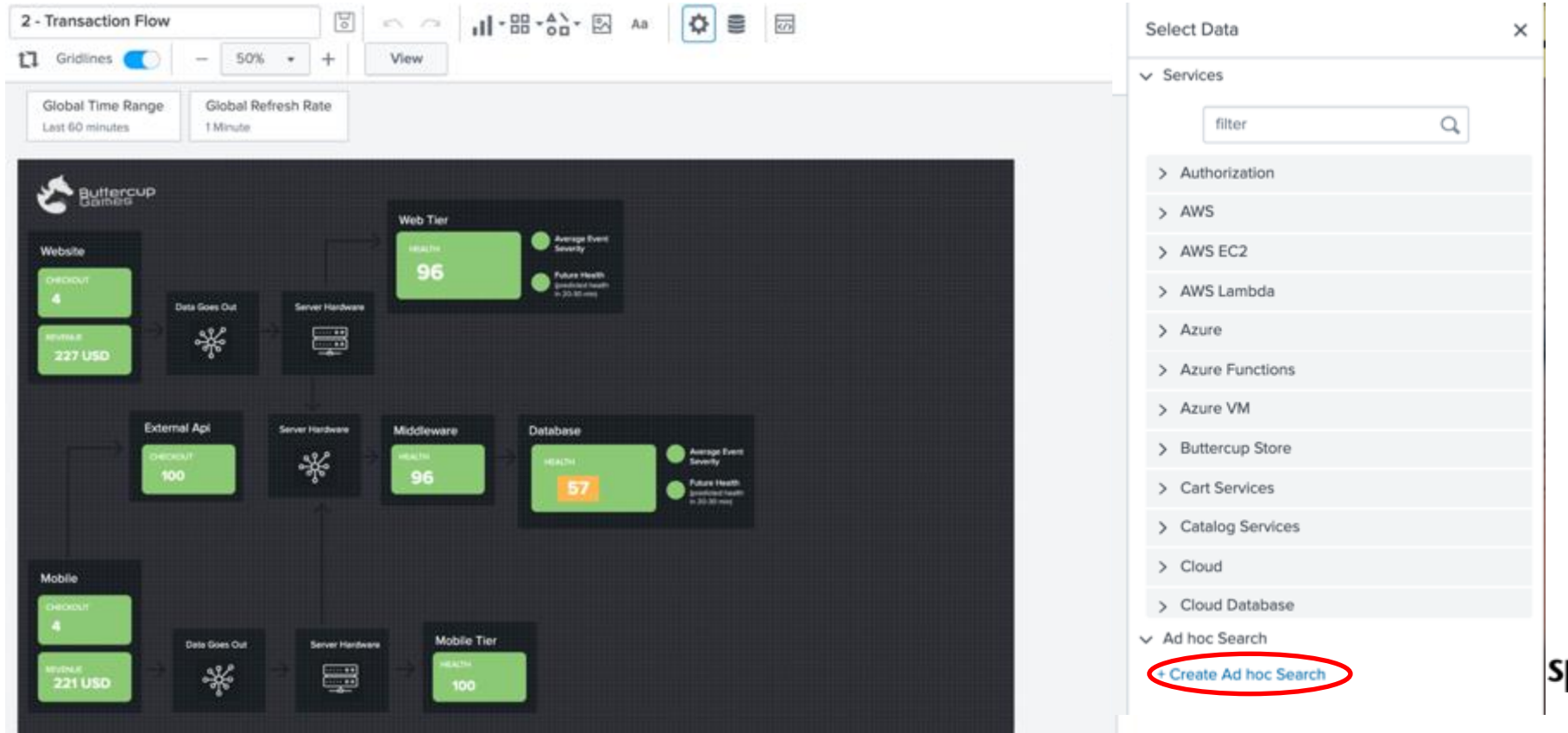
- Select the On-Prem Database Future Health
- Click ‘Set up Primary Data Source'



splunk> turn data into doing

Predictive Analytics Lab

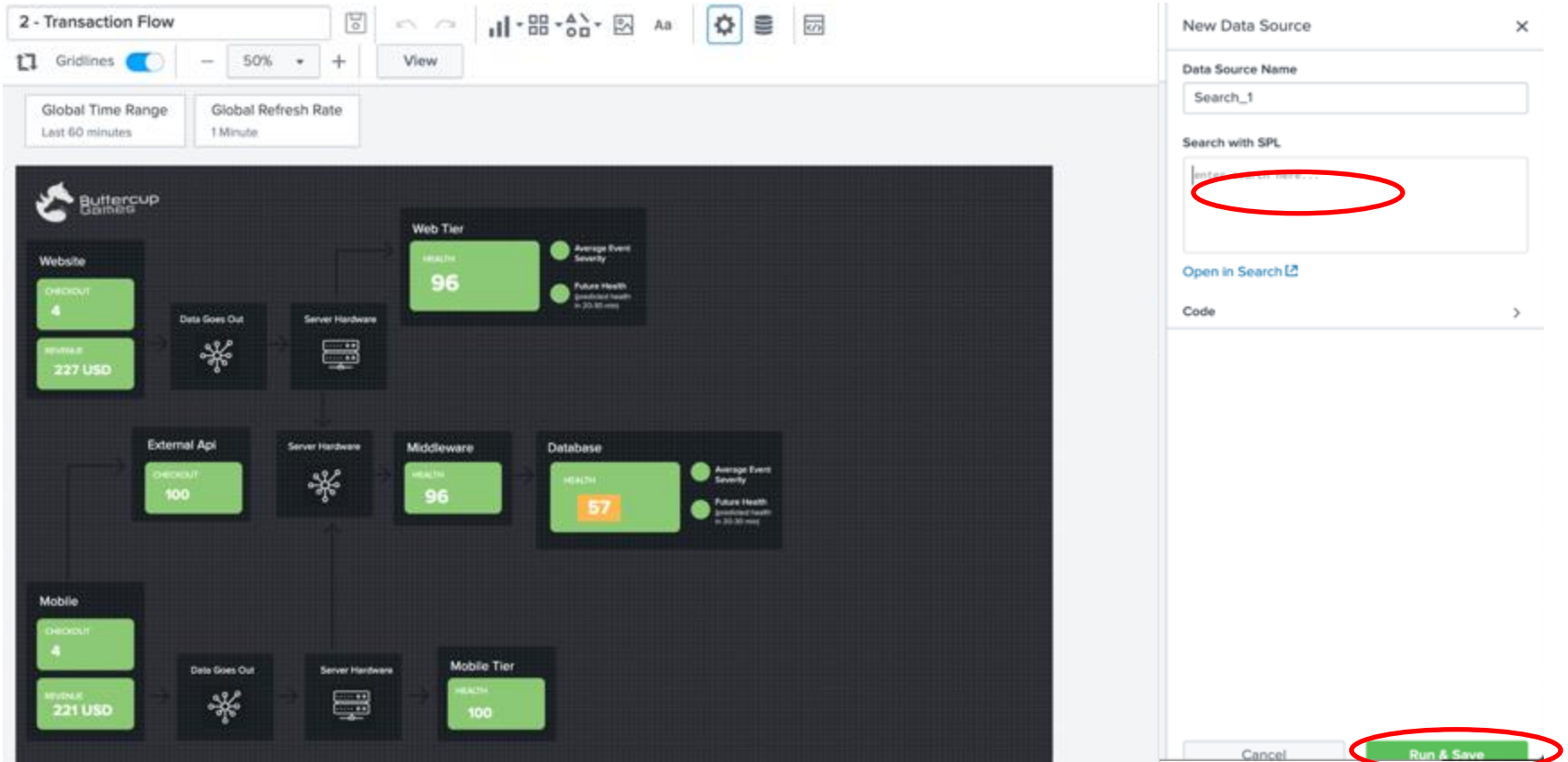
- Select the ‘Create Ad-Hoc Search’



splunk> turn data into doing

Predictive Analytics Lab

- Copy the previous Predictive Analytics SPL
- Click ‘Run & Save’ button



splunk> turn data into doing

Machine Learning: Event Analytics

Event Analytics Lab

The database team has expressed frustration with alerts originating from Nagios. The high volume of alerts is leading to alert fatigue and they lack the contextual information to determine importance.

While the plan is to consolidate monitoring tools, they have asked if we can provide immediate relief using ITSI to group events together and reduce noise.

The same challenges are being expressed by the web team who uses New Relic to monitor the application code.

Event Analytics Lab

In this exercise we will group the database teams Nagios events together based on time and associate them to a service

Clean and prepare “raw” alert events
- SPL

Create Notable Events from alerts
- *Correlation Search*

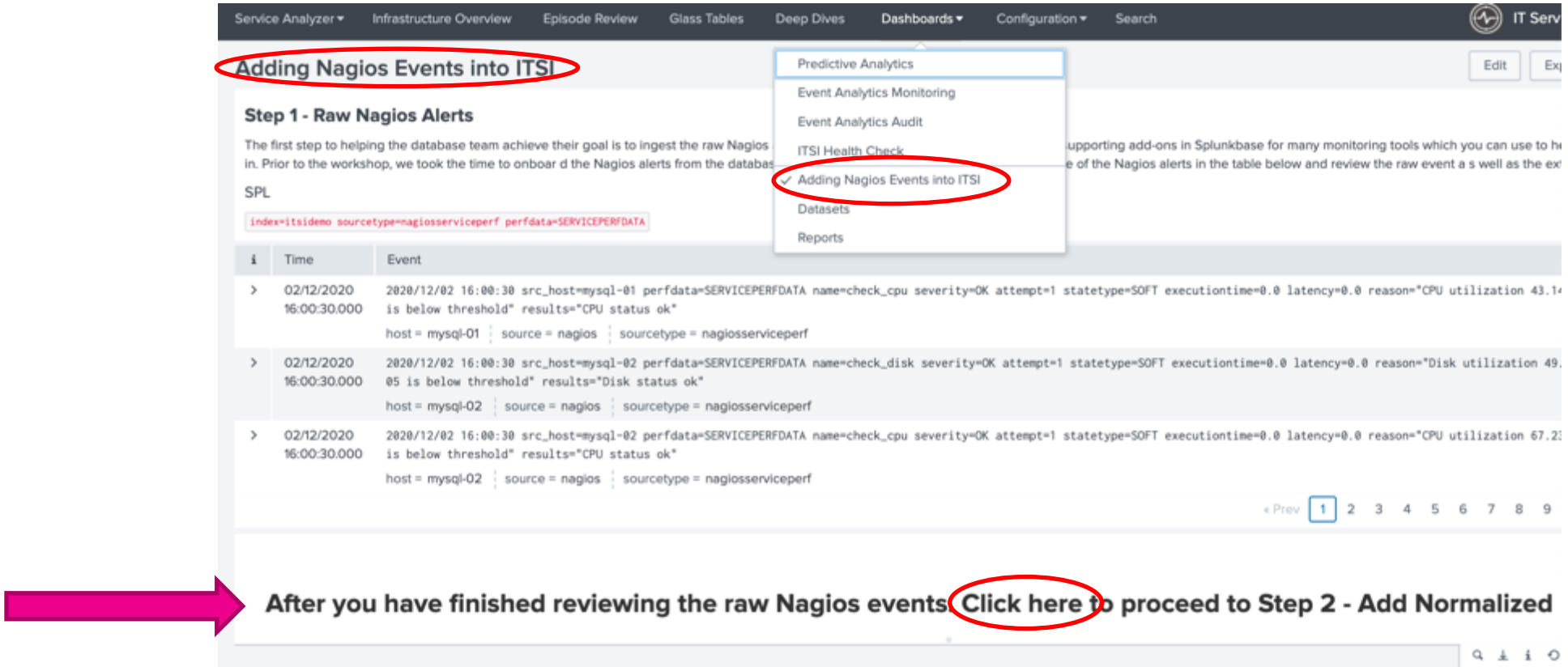
Apply Service Context & Configure Event Grouping
- Notable Event Aggregation Policies

Review episodes

EA Lab Step 1 : Clean and prepare “raw” alert events

Check raw alerts → Normalizing → Filter duplicates → Add Service Context

index=itsidemo sourcetype=nagiosserviceperf perfdata=SERVICEPERFDATA

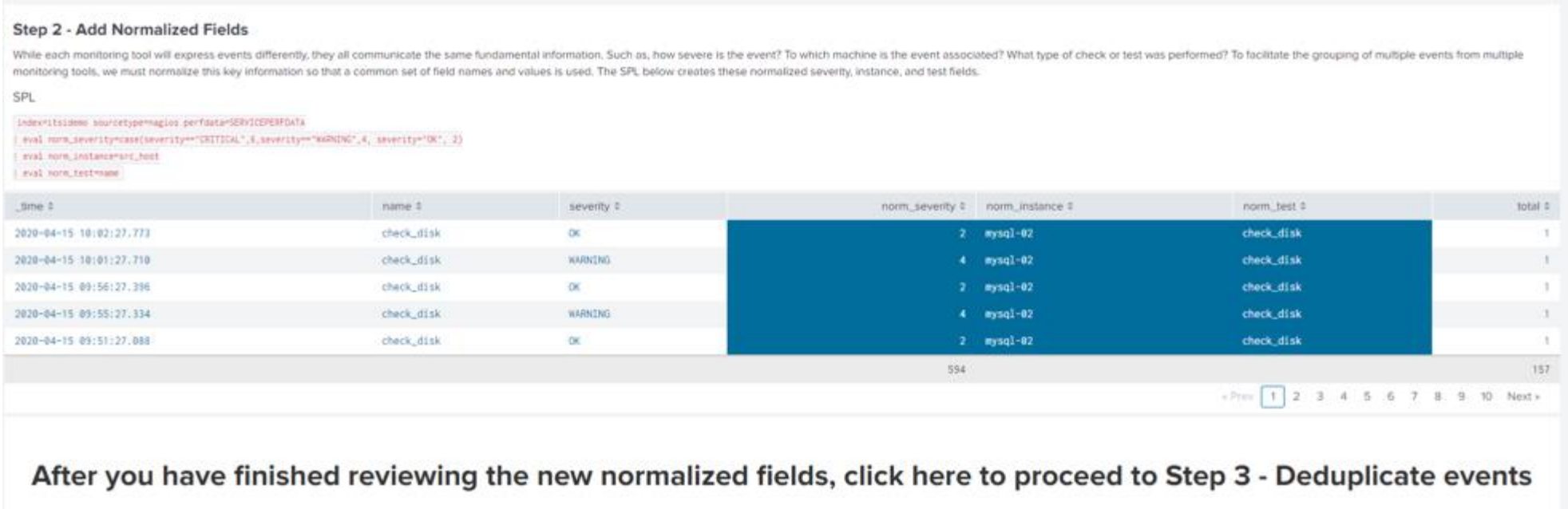


EA Lab Step 2 : Add Normalized Fields

Check raw alerts → **Normalizing** → Filter duplicates → Add Service Context

Goal: Normalize the data to make it possible to correlate data from different sources

```
| eval norm_severity=case(severity=="CRITICAL",6,severity=="WARNING",4, severity="OK", 2)
| eval norm_instance= src_host
| eval norm_test=name
```



Step 2 - Add Normalized Fields

While each monitoring tool will express events differently, they all communicate the same fundamental information. Such as, how severe is the event? To which machine is the event associated? What type of check or test was performed? To facilitate the grouping of multiple events from multiple monitoring tools, we must normalize this key information so that a common set of field names and values is used. The SPL below creates these normalized severity, instance, and test fields.

SPL

```
index=itsidemo sourcetype=nagios perfdata=SERVICEPERFDATA
| eval norm_severity=case(severity=="CRITICAL",6,severity=="WARNING",4, severity="OK", 2)
| eval norm_instance=src_host
| eval norm_test=name
```

_time	name	severity	norm_severity	norm_instance	norm_test	total
2020-04-15 10:02:27.773	check_disk	OK	2	mysql-02	check_disk	1
2020-04-15 10:01:27.710	check_disk	WARNING	4	mysql-02	check_disk	1
2020-04-15 09:56:27.396	check_disk	OK	2	mysql-02	check_disk	1
2020-04-15 09:55:27.334	check_disk	WARNING	4	mysql-02	check_disk	1
2020-04-15 09:51:27.088	check_disk	OK	2	mysql-02	check_disk	1
			594			157

« Prev 1 2 3 4 5 6 7 8 9 10 Next »

After you have finished reviewing the new normalized fields, click here to proceed to Step 3 - Deduplicate events

EA Lab Step 3 : Deduplicate events

Check raw alerts → Normalizing → **Filter duplicates** → Add Service Context

Goal: Removing duplicated events

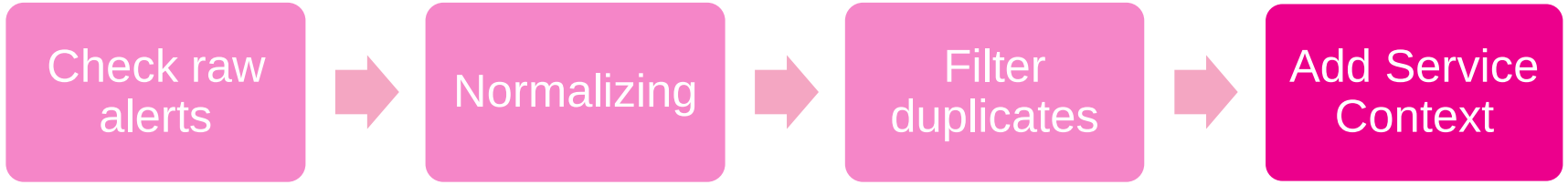
| dedup consecutive=true src_host severity name

_time	name	norm_instance	severity	norm_severity	total
2020-04-15 10:02:27.773	check_disk	mysql-02	OK	2	1
2020-04-15 10:01:27.710	check_disk	mysql-02	WARNING	4	1
2020-04-15 09:56:27.396	check_disk	mysql-02	OK	2	1
2020-04-15 09:55:27.334	check_disk	mysql-02	WARNING	4	1
2020-04-15 09:51:27.088	check_disk	mysql-02	OK	2	1
				102	34

« Prev 1 2 3 4 5 6 7 Next »

Finally, after you have finished reviewing the deduplicated events, click here to proceed to Step 4 - Add Service Context

EA Lab Step 4 - Add Service Context



Goal: Add Service Context makes correlation possible for different alerts in a serv

```
| `apply_entity_lookup(host)`
| `get_service_name(serviceid,service_name)`
```

- Click on the Spyglass

_time	name	norm_instance	severity	norm_severity	service_name
2020-04-15 10:02:27.773	check_disk	mysql-02	OK	2	On-Prem Database
2020-04-15 10:01:27.710	check_disk	mysql-02	WARNING	4	On-Prem Database
2020-04-15 09:56:27.396	check_disk	mysql-02	OK	2	On-Prem Database
2020-04-15 09:55:27.334	check_disk	mysql-02	WARNING	4	On-Prem Database
2020-04-15 09:51:27.088	check_disk	mysql-02	OK	2	On-Prem Database

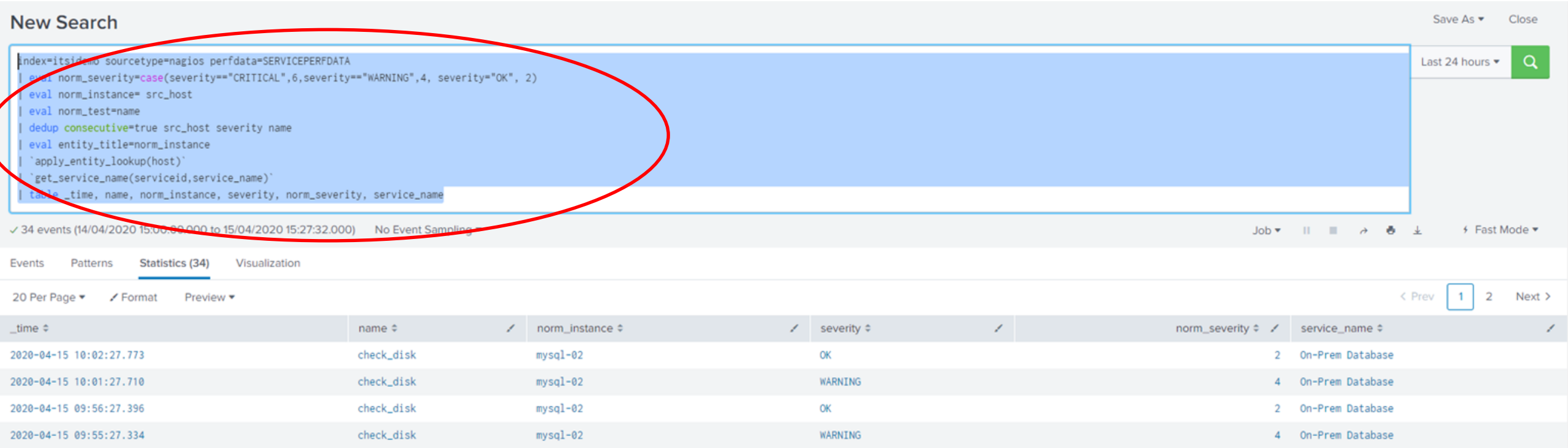
« Prev 1 Open in Search 6 7 Next »

a minute ago

Event Analytics Lab

Check raw alerts → Normalizing → Filter duplicates → Add Service Context

- Select the SPL and copy to clipboard, we will need it in the next exercise



Event Analytics Lab

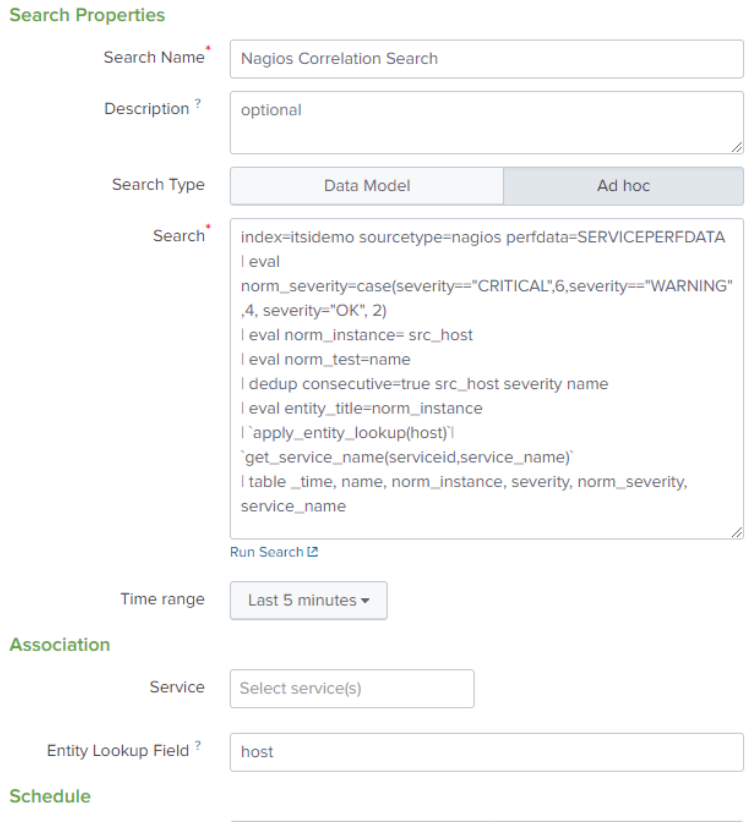
In this exercise we will group the database teams Nagios events together based on time and associate them to a service

Clean and prepare “raw” alert events
- SPL

Create Notable Events from alerts
- *Correlation Search*

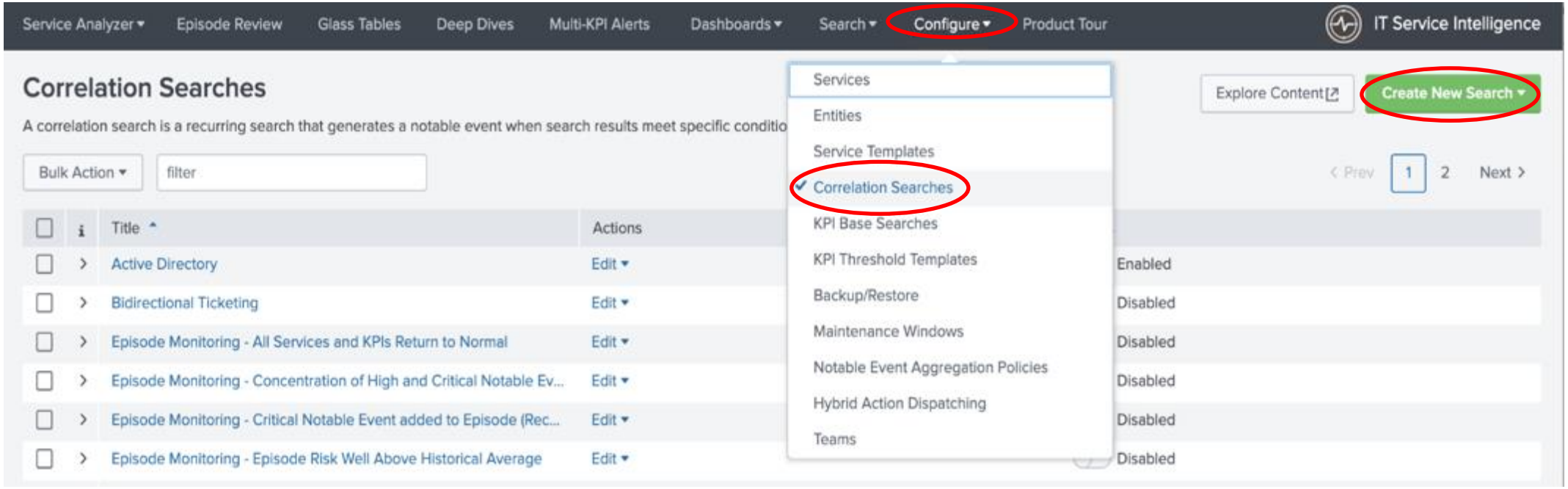
Apply Service Context & Configure Event Grouping
- Notable Event Aggregation Policies

Review episodes



Event Analytics Lab

- Navigate to Configuration -> Correlation Searches
- Create New Search -> Create Correlation Search

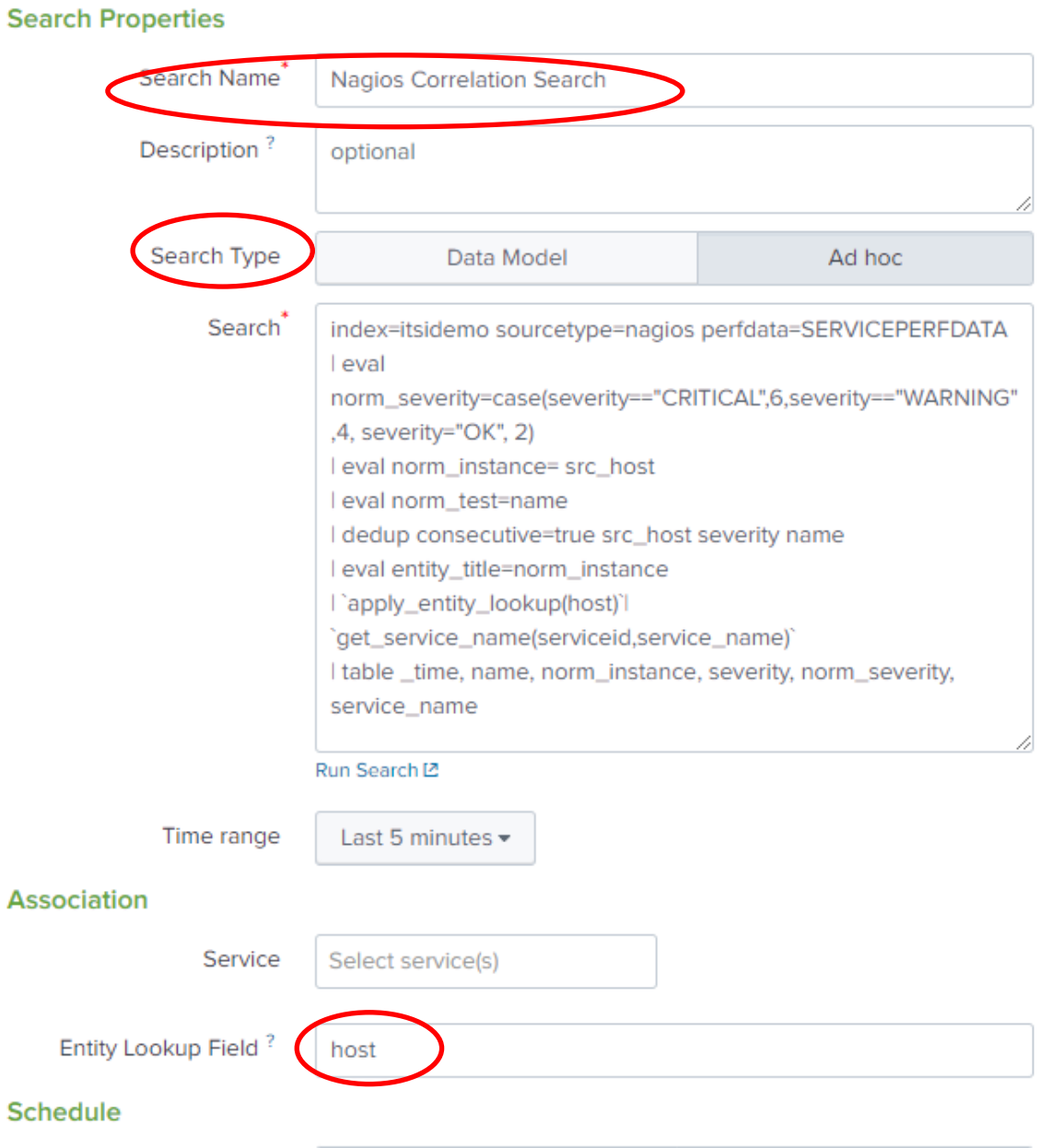


Event Analytics Lab: correlation search

- Name your search
- *Paste the SPL in search:*

```
index=itsidemo sourcetype=nagios perfdata=SERVICEPERFDATA
| eval norm_severity=case(severity=="CRITICAL",6,severity=="WARNING",4, severity="OK", 2)
| eval norm_instance= src_host
| eval norm_test=name
| dedup consecutive=true src_host severity name
| eval entity_title=norm_instance
| `apply_entity_lookup(host)`
| `get_service_name(serviceid,service_name)`
| table _time, name, norm_instance, severity, norm_severity, service_name
```

- *Time range: Last 5 minutes (select 'relative' in time picker)*
- *Run Every: 5 minutes*
- *Entity Lookup Field: host*
- *Scroll down*



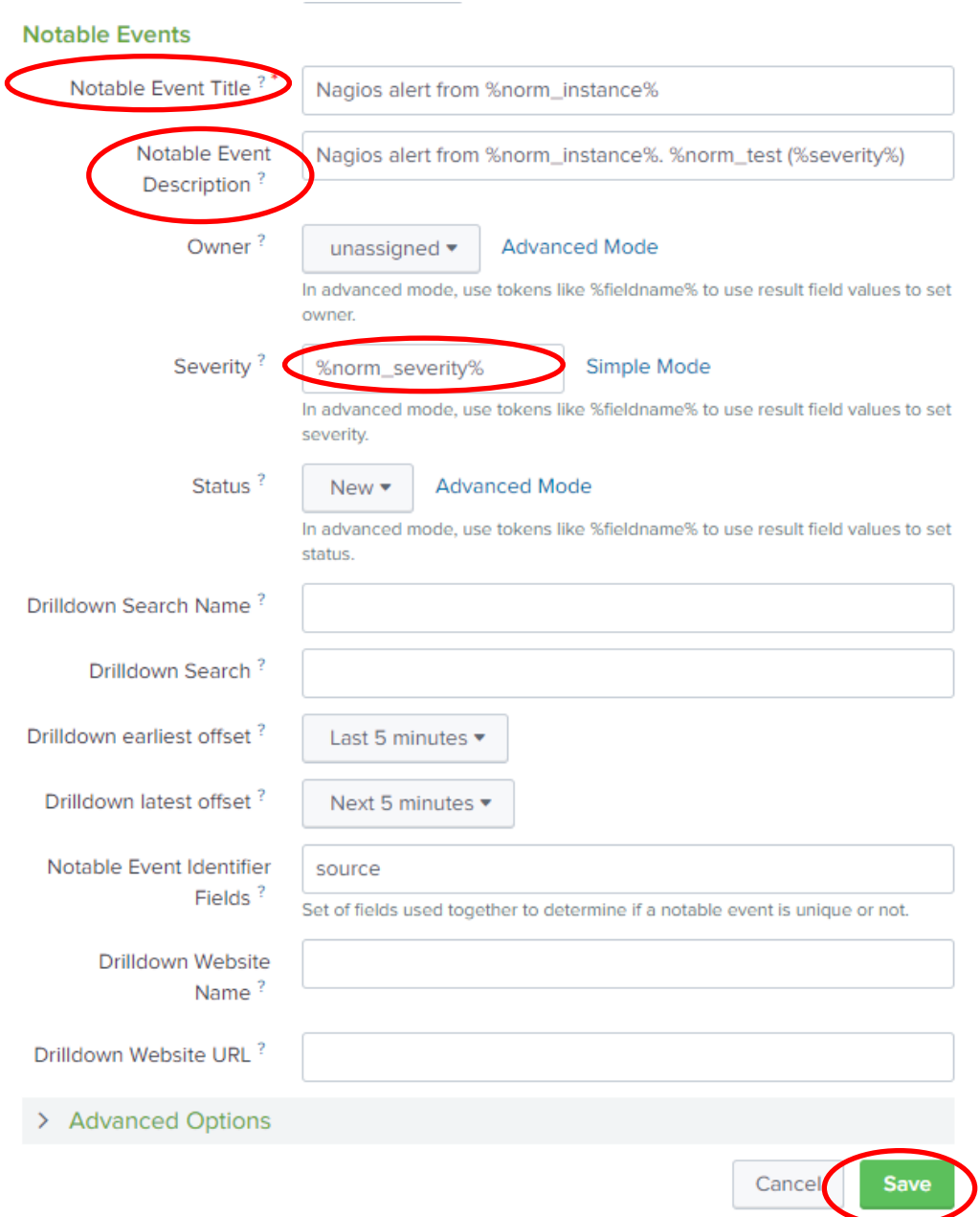
Event Analytics Lab: correlation search

- *Populate Notable Event Title*

  Nagios alert from %norm_instance%
- *Populate Notable Event Desc.*

  Nagios alert from %norm_instance%
  %norm_test% (%severity%)
- *Click Severity: Advanced Mode*
- *Severity: %norm_severity%*

- *Save*



Event Analytics Lab: Notable Event Aggregation Policies

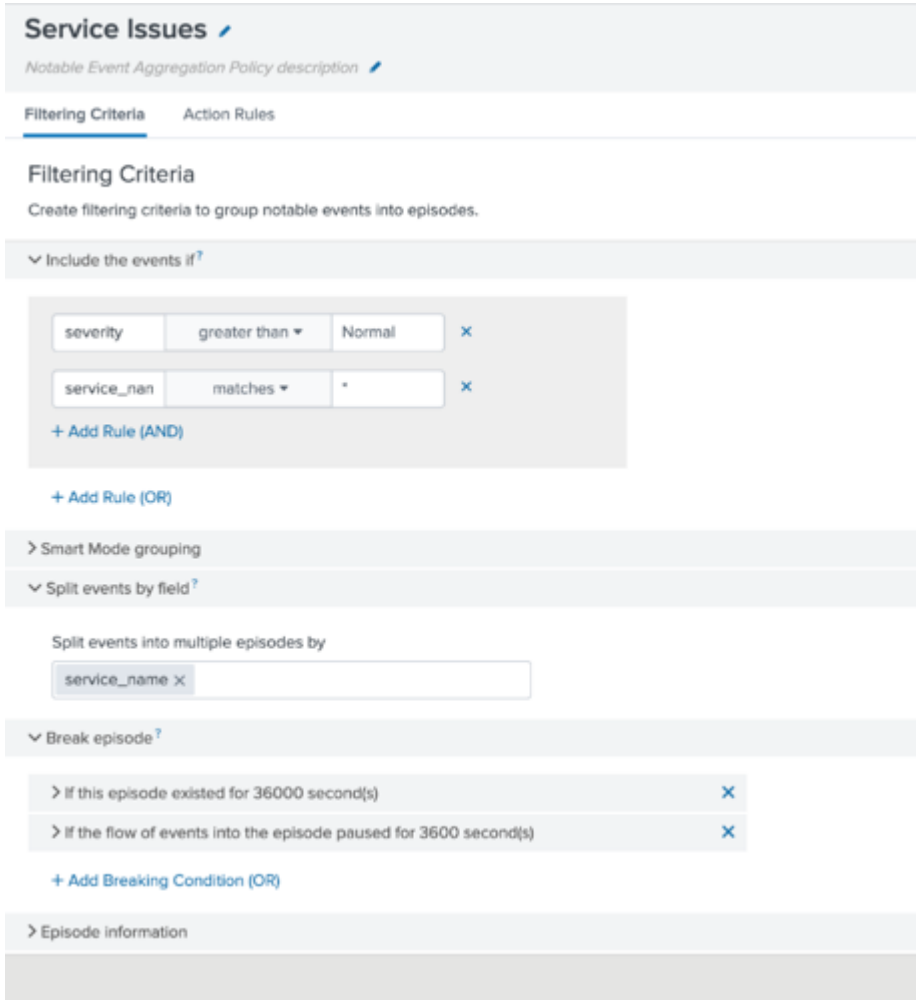
In this exercise we will group the database teams Nagios events together based on time and associate them to a service

Clean and prepare “raw” alert events
- SPL

Create Notable Events from alerts
- *Correlation Search*

Apply Service Context & Configure Event Grouping
- Notable Event Aggregation Policies

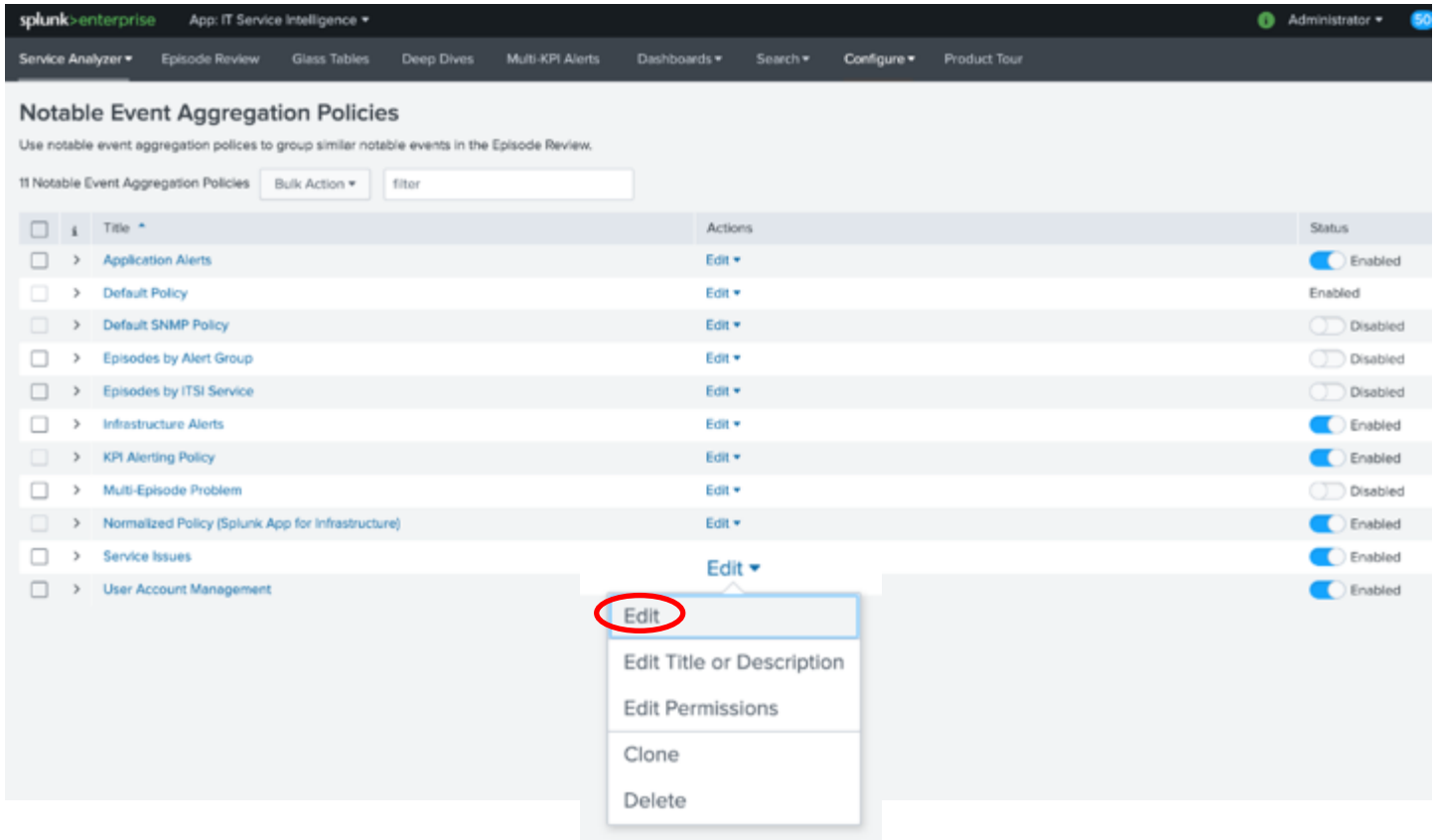
Review episodes



Event Analytics Lab: Notable Event Aggregation Policies

- Navigate to Configure -> Notable Event Aggregation Policies

- Edit *"Service Issues"* policy

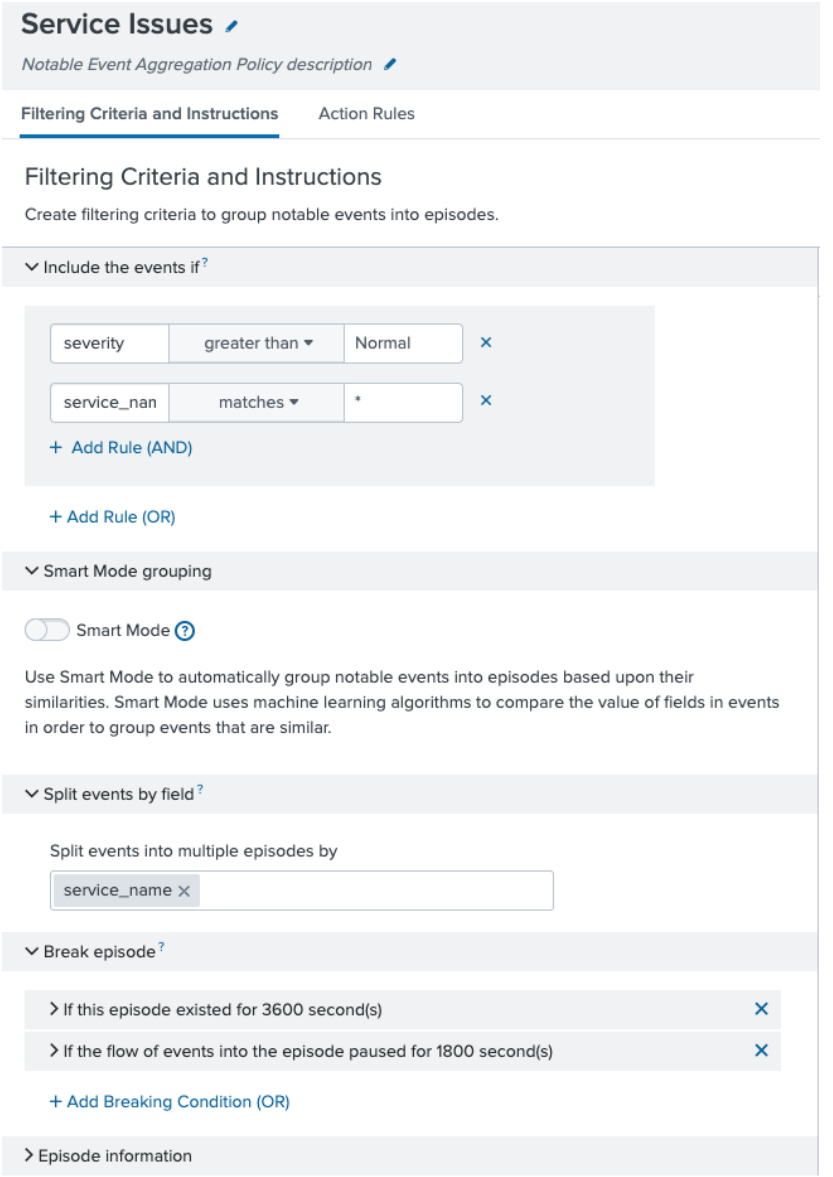


Event Analytics Lab: Notable Event Aggregation Policies

- *Review "Include the events if" configuration*
- *Review "Split events by field" configuration*
- *Review "Break episode" configuration*
- *Modify the "Break episode" configuration*
  - *If the flow of events paused for 3600 seconds*

related notable events.

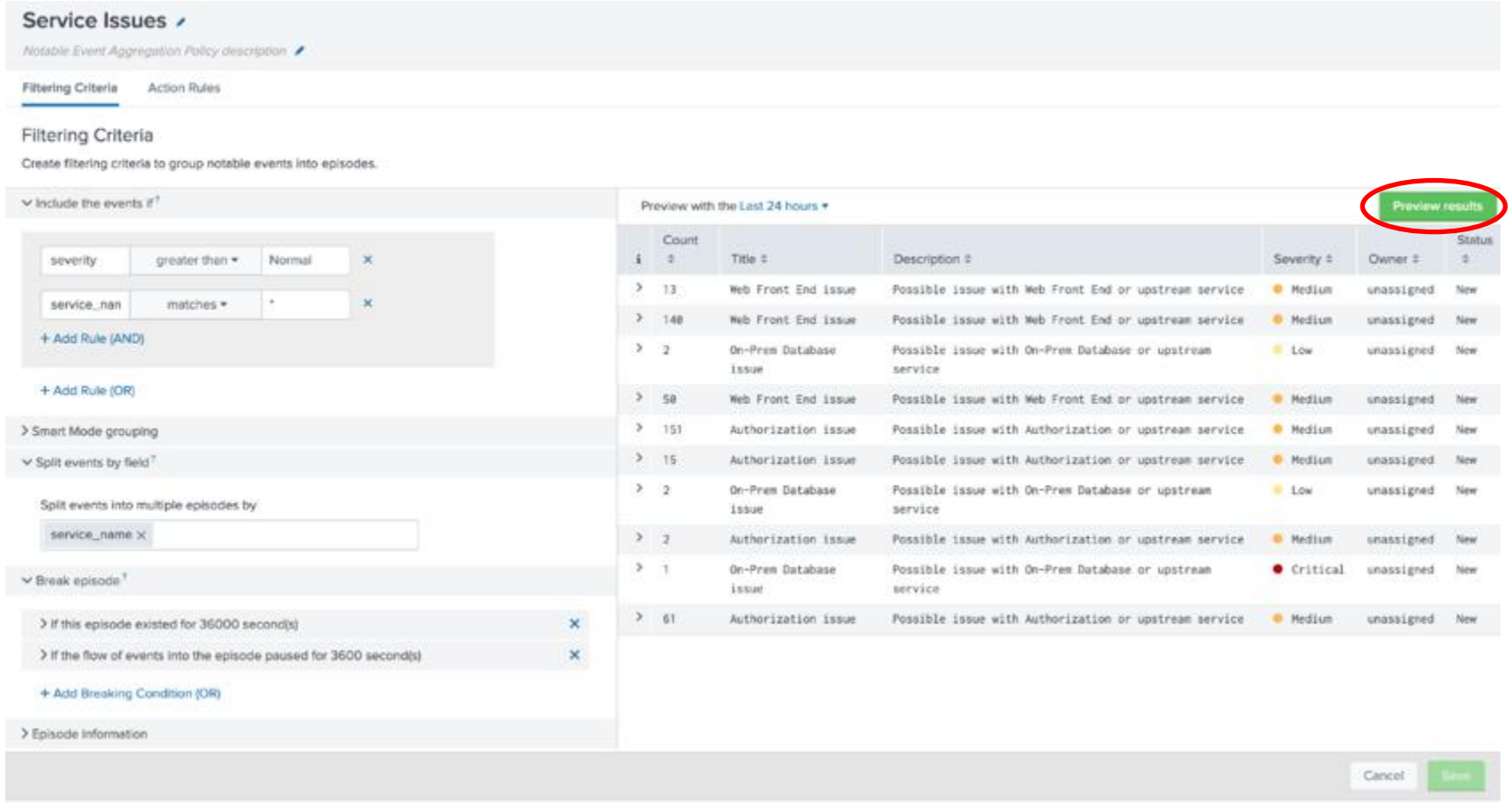
It looks like a policy might already exist which groups notable events together by the affected ITSI Service. That policy is called "Service Issues



Event Analytics Lab: Notable Event Aggregation Policies

The preview result screen show how ITSI is now grouping events together based on your configurations.

- Preview Results
- Click Cancel



Event Analytics Lab

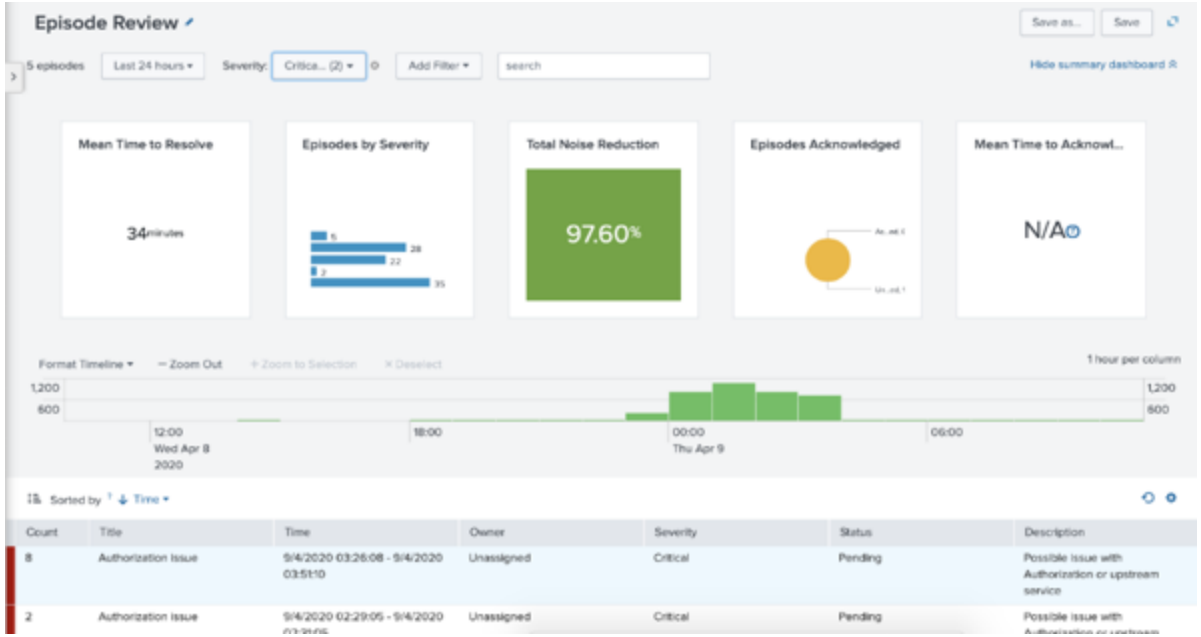
In this exercise we will group the database teams Nagios events together based on time and associate them to a service

Clean and prepare “raw” alert events
- SPL

Create Notable Events from alerts
- *Correlation Search*

Apply Service Context & Configure Event Grouping
- Notable Event Aggregation Policies

Review episodes



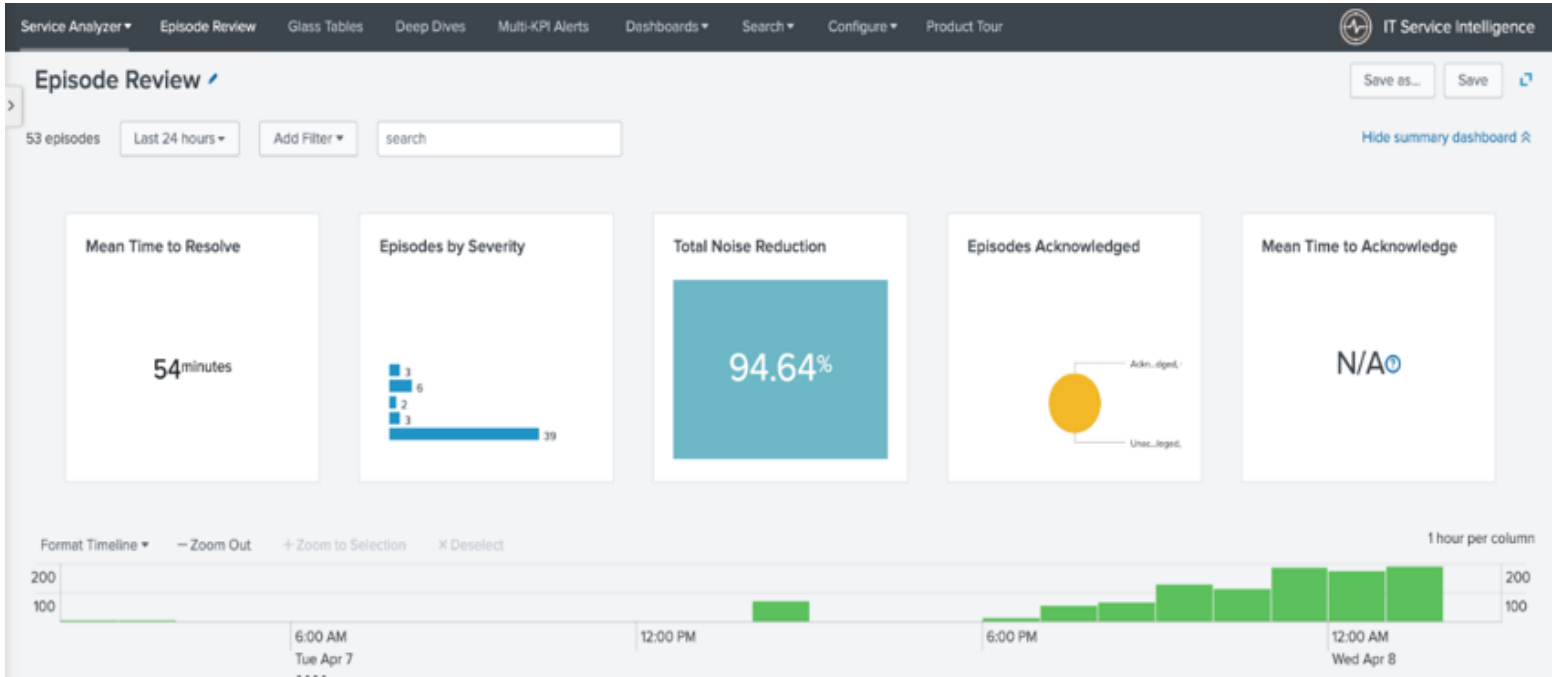
splunk> turn data into doing

Event Analytics Lab: Episode View

When notable events are grouped by aggregation policies, the resulting groups are called episodes, you can think of an episode as event grouping.

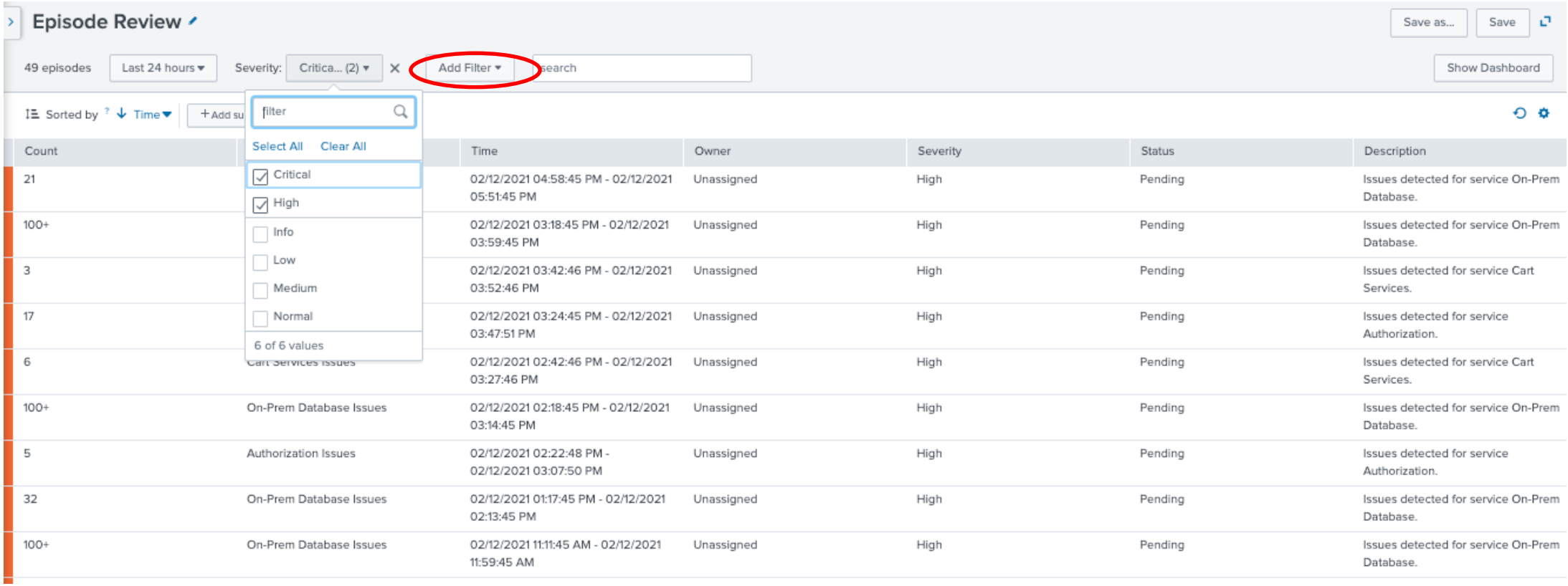
The episode review page provides a great deal of information in a heads-up display and is like the cockpit view for Operations teams.

- Navigate to Episode Review
- Note the Noise Reduction



Event Analytics Lab: Episode View

- Scroll down and review list
- Click the ‘filter’ button
- Select the ‘Severity’ field
- Tick only ‘Critical’ & ‘High’ events



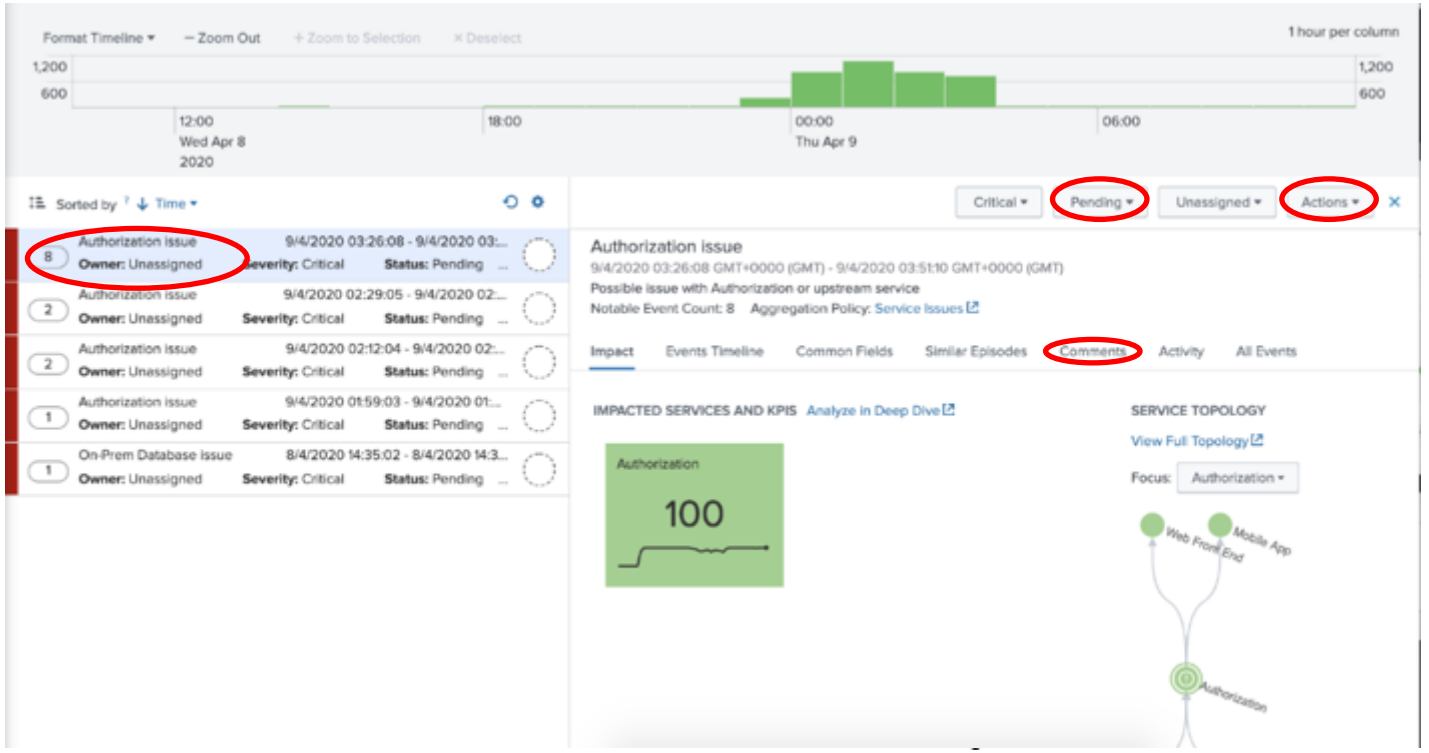
Count		Time	Owner	Severity	Status	Description
21		02/12/2021 04:58:45 PM - 02/12/2021 05:51:45 PM	Unassigned	High	Pending	Issues detected for service On-Prem Database.
100+		02/12/2021 03:18:45 PM - 02/12/2021 03:59:45 PM	Unassigned	High	Pending	Issues detected for service On-Prem Database.
3		02/12/2021 03:42:46 PM - 02/12/2021 03:52:46 PM	Unassigned	High	Pending	Issues detected for service Cart Services.
17		02/12/2021 03:24:45 PM - 02/12/2021 03:47:51 PM	Unassigned	High	Pending	Issues detected for service Authorization.
6	Cart Services Issues	02/12/2021 02:42:46 PM - 02/12/2021 03:27:46 PM	Unassigned	High	Pending	Issues detected for service Cart Services.
100+	On-Prem Database Issues	02/12/2021 02:18:45 PM - 02/12/2021 03:14:45 PM	Unassigned	High	Pending	Issues detected for service On-Prem Database.
5	Authorization Issues	02/12/2021 02:22:48 PM - 02/12/2021 03:07:50 PM	Unassigned	High	Pending	Issues detected for service Authorization.
32	On-Prem Database Issues	02/12/2021 01:17:45 PM - 02/12/2021 02:13:45 PM	Unassigned	High	Pending	Issues detected for service On-Prem Database.
100+	On-Prem Database Issues	02/12/2021 11:11:45 AM - 02/12/2021 11:59:45 AM	Unassigned	High	Pending	Issues detected for service On-Prem Database.

Event Analytics Lab: Episode View

We will now review an episode to better understand the flow of events, and we will then ensure someone has ownership.

- Click on '*Authorization Issue*' episode
- Review the details for each tab
- Add your name to the comments

- Change to '*In Progress*'
- Review possible Actions




FINISH

Thank You