

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

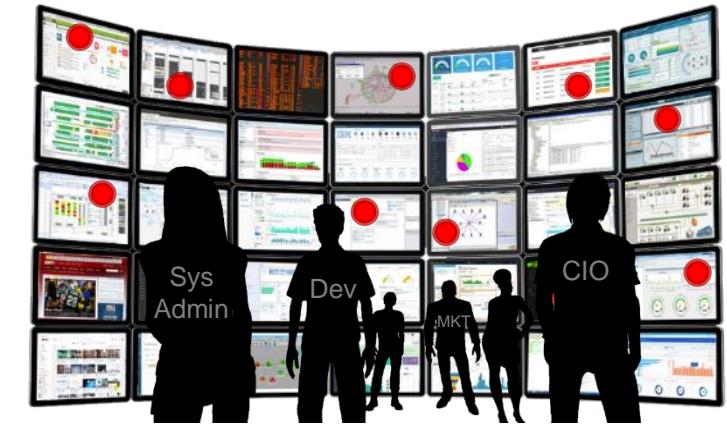
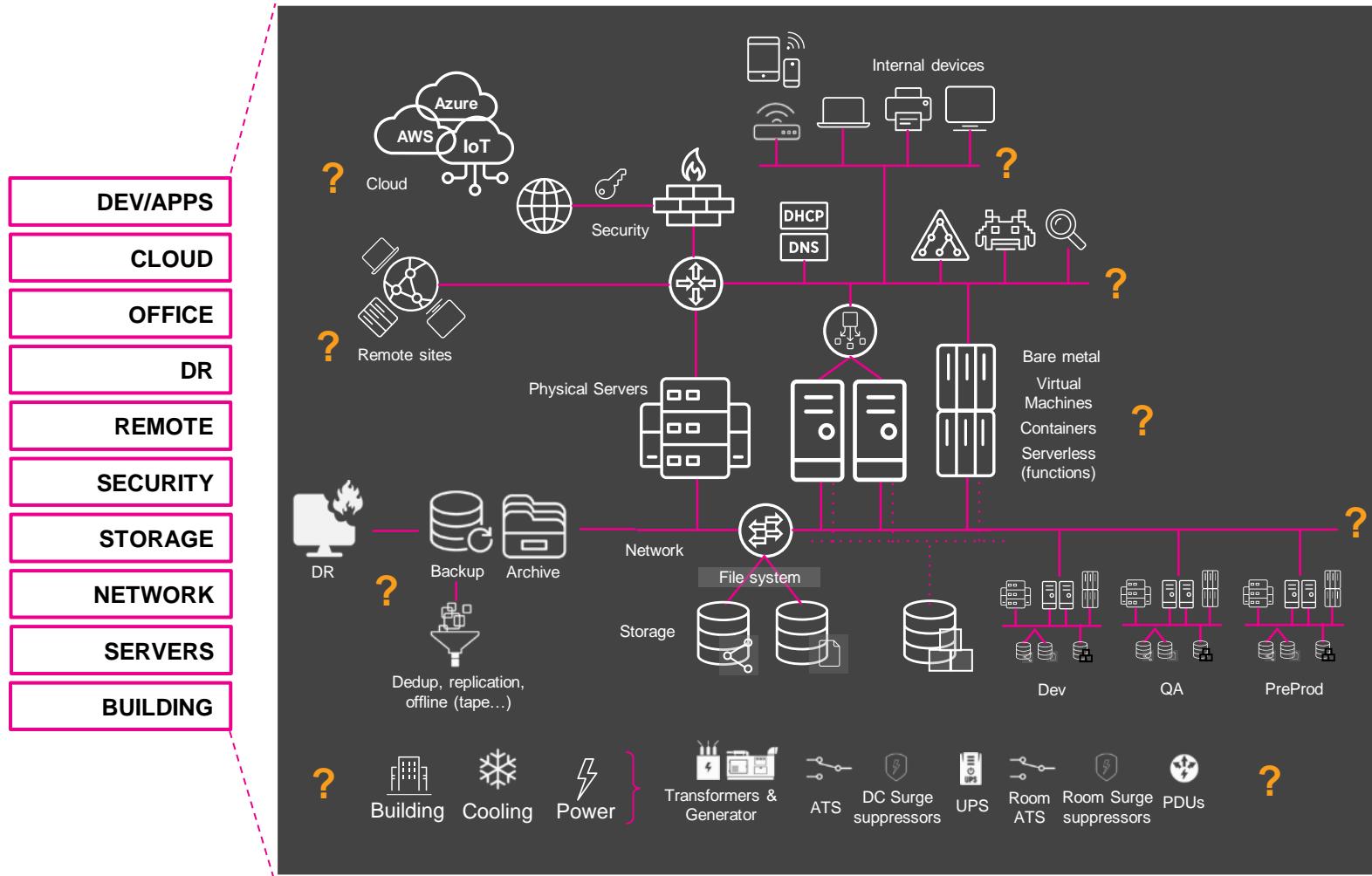
- Problem Statement
- IT Service Intelligence Overview
- Service Creation
- KPIs Creation
- Deep Dives
- Glass Tables
- Machine Learning
- Event Analytics
- Next Steps

# 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



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

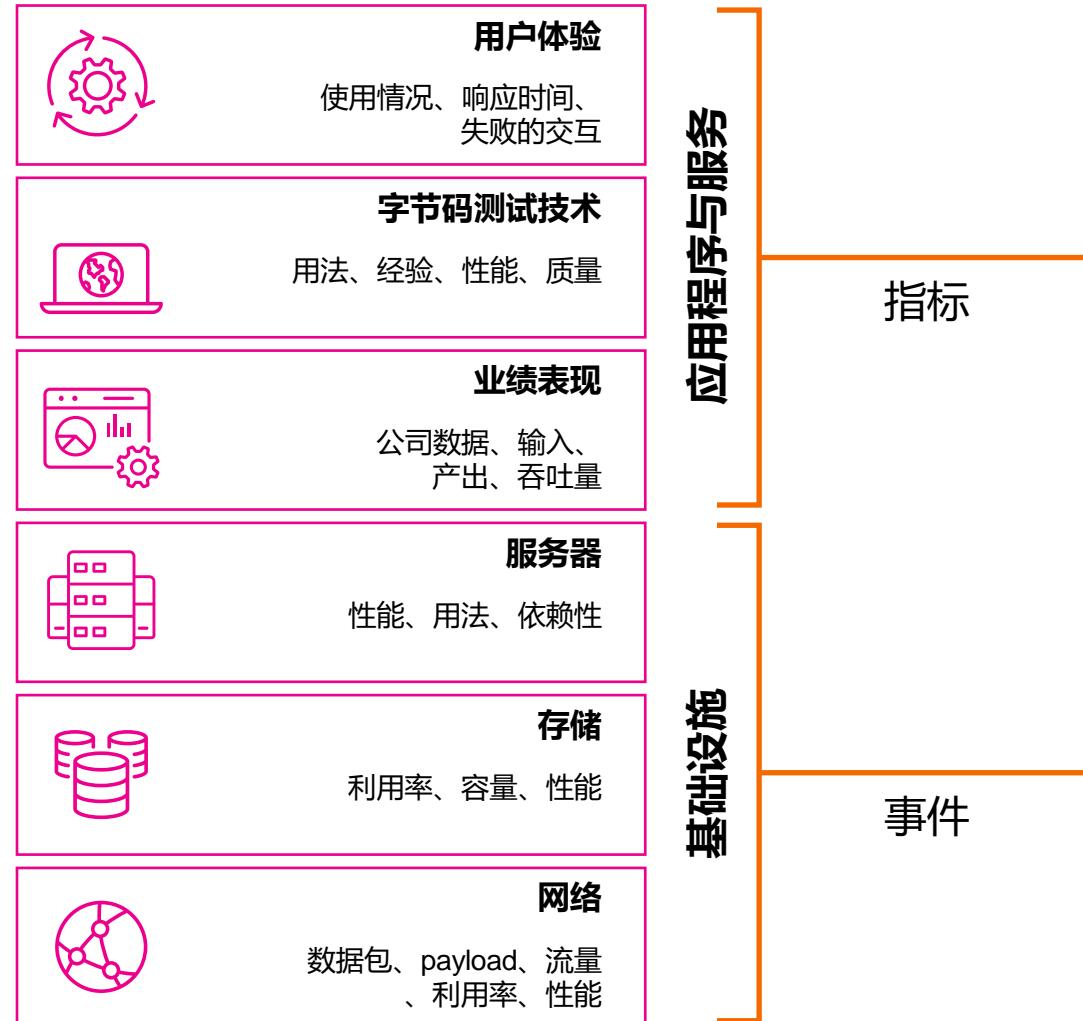
Teams thrash, finger-point, and key employees leave



## 难以创新

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

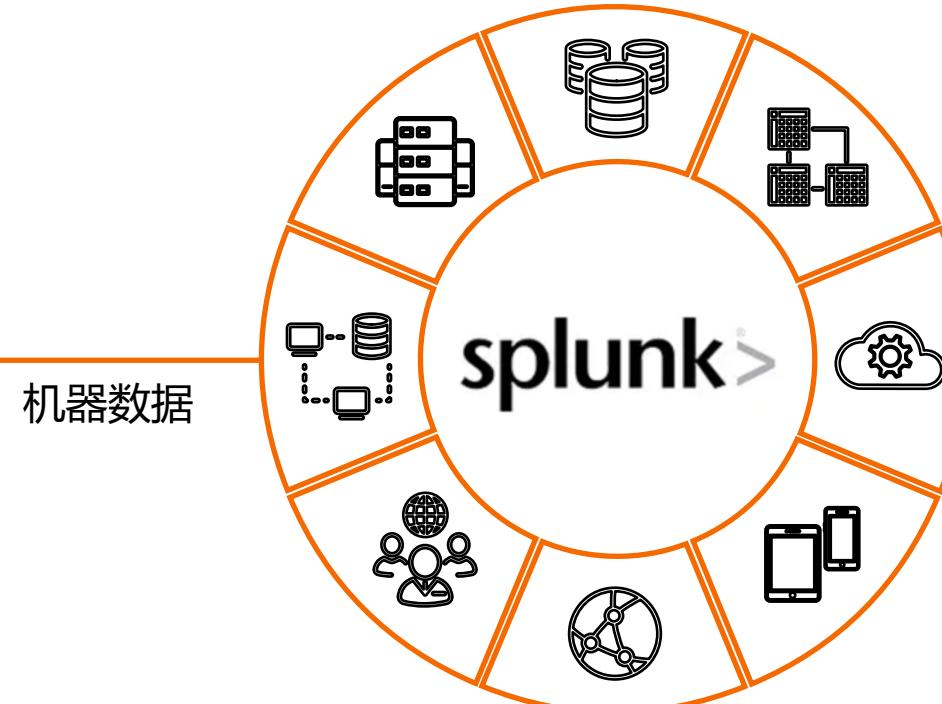
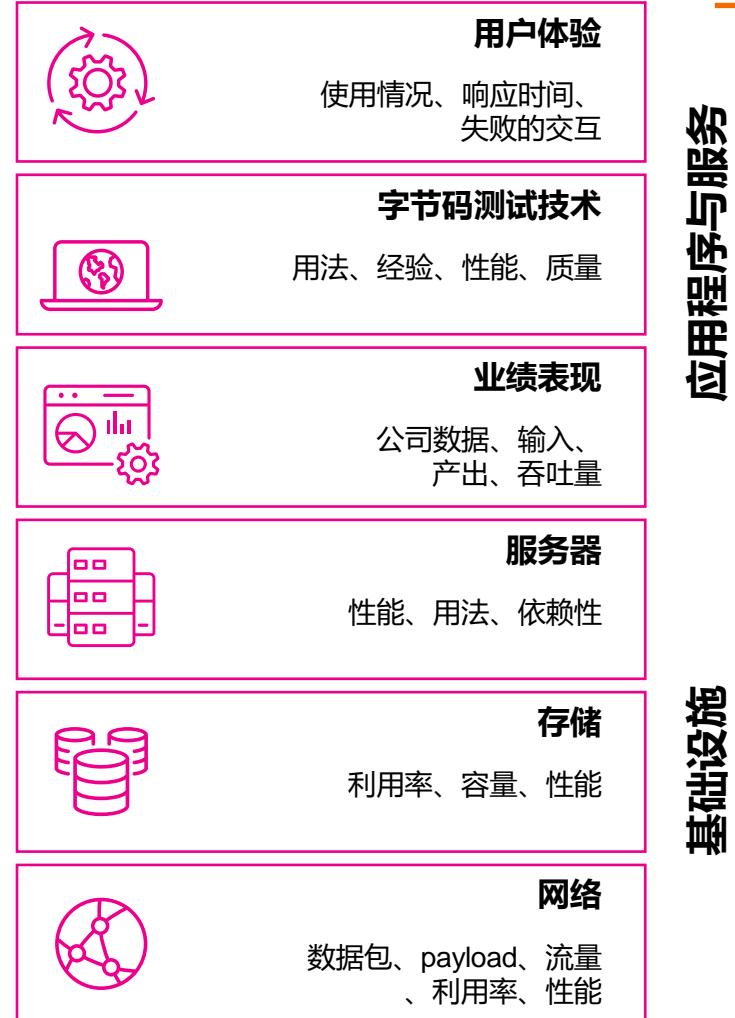
# 传统IT管理整合方式



## 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



## 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



动态服务模型



一览式问题分析



偏差预警



事件分析



简化的事故工作流程

Splunk IT 服务智能

splunk> Enterprise

splunk> Cloud



时间序列索引

读时建模

数据模型

通用信息模型

# Key Terminology

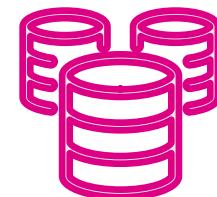
---

# 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



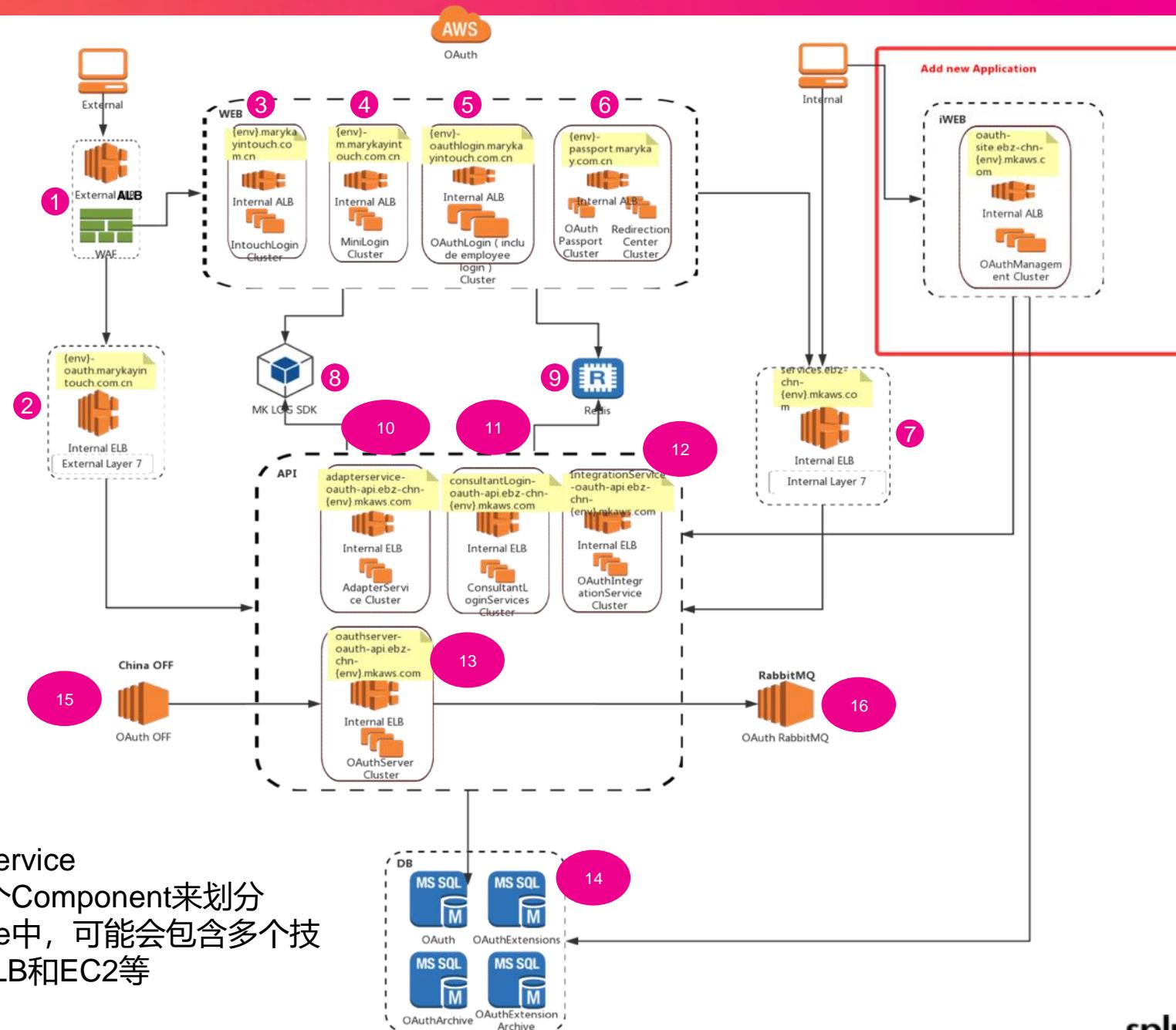
Database  
Service



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

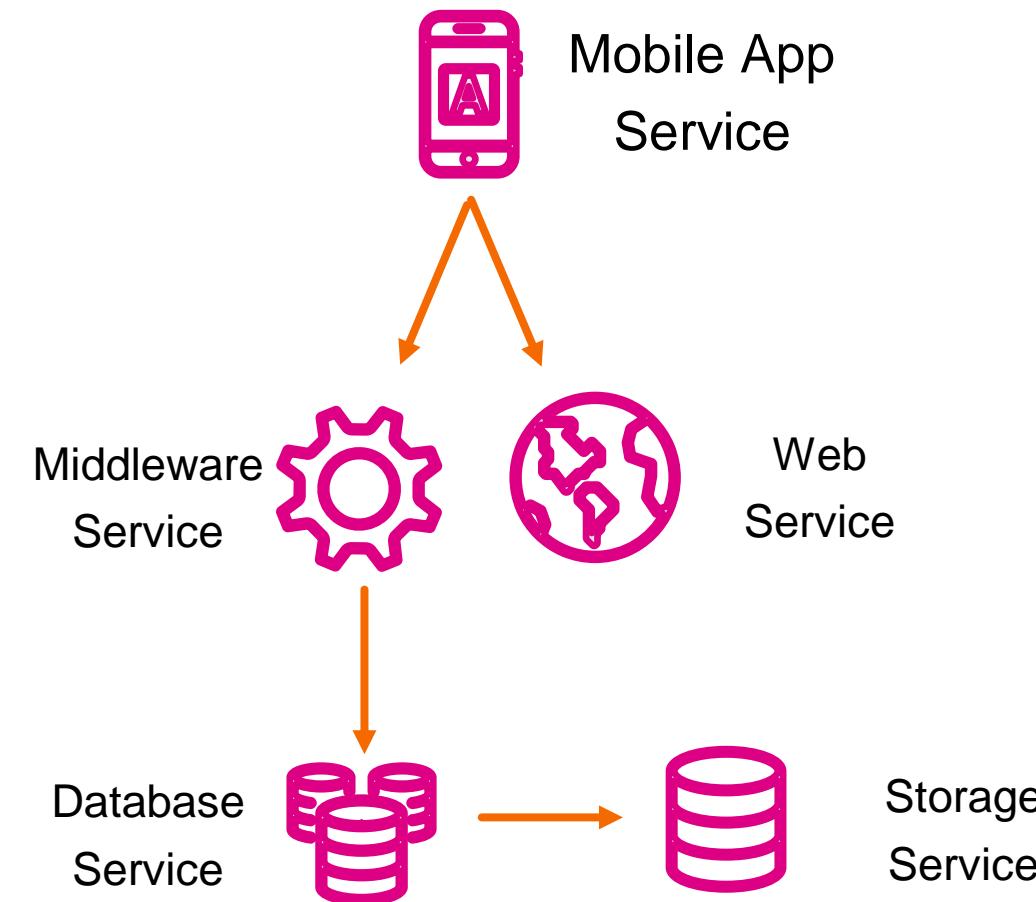
# 服务可能还依赖其它服务

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。



Number of visitors  
Revenue  
Transactions per day



CPU Utilisation  
Query Response Time  
Storage Free Space



# 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

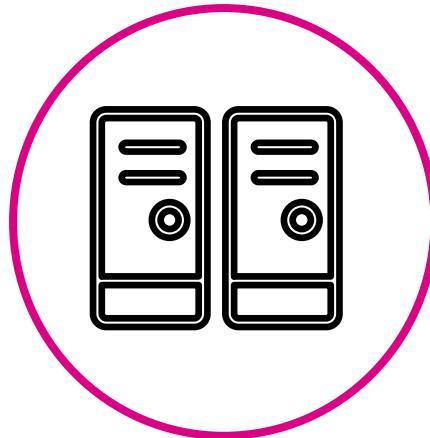


# ITSI Service Definition

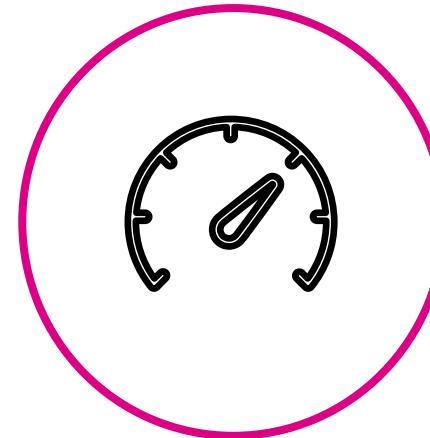
概况而言，一项服务包括：



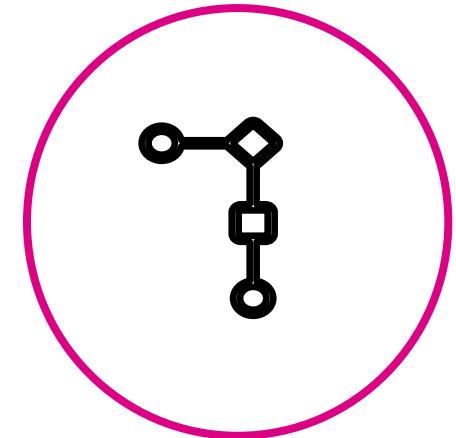
A Service  
Health Score



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

举例

资金受托管理应用，  
用户验证系统，  
核心业务系统

服务  
*Service*

为完成某个商业目标聚合在一起的一组行为

举例

账户开立，  
资格申请，  
信息维护&管理

业务流程  
*Business Process*

承载服务的组件

举例

主机, 用户,  
操作系统

实体  
*Entities*

用于评估健康状态的评分系统

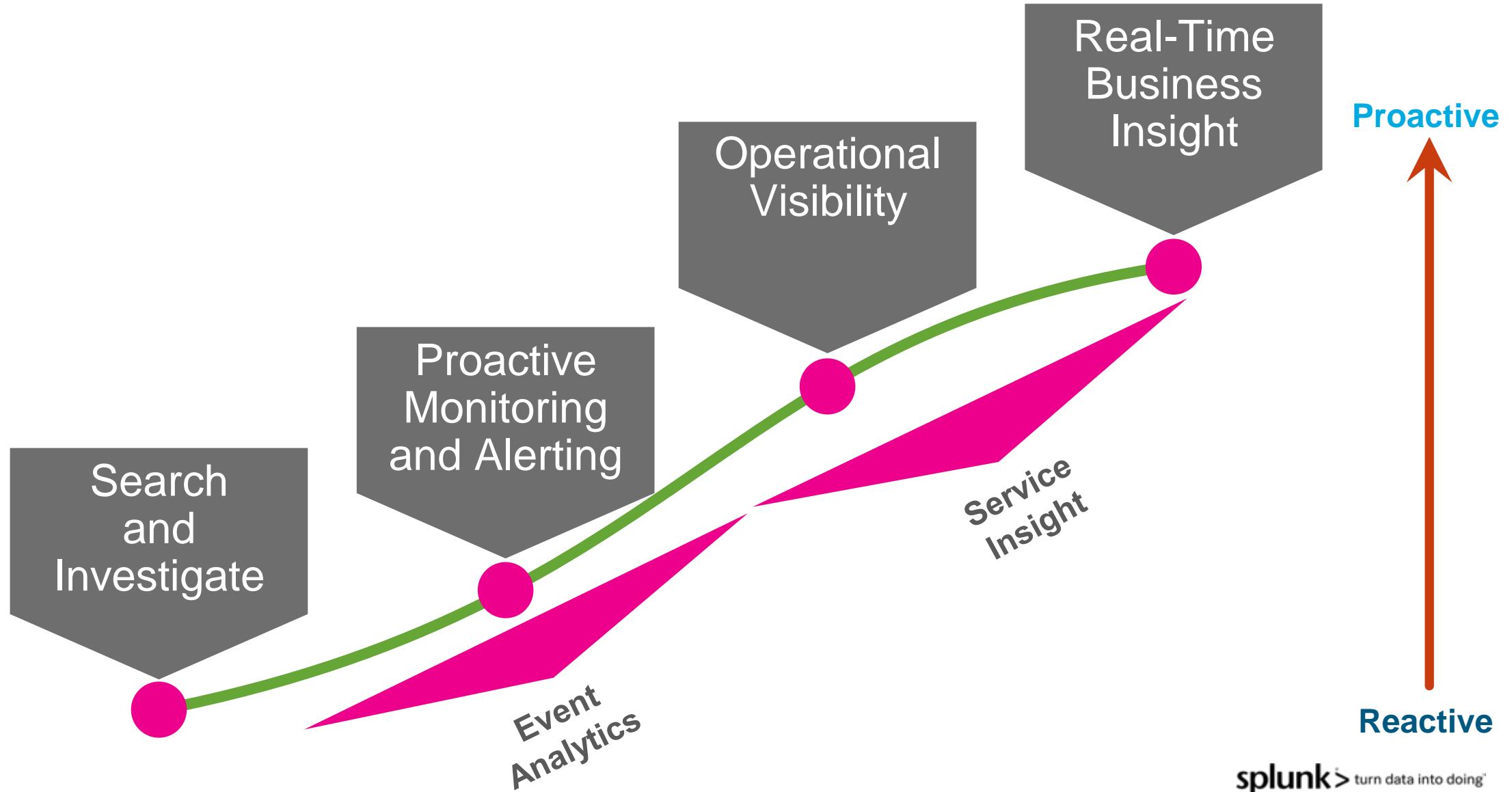
举例

服务健康度，  
订单处理成功，  
系统延迟

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

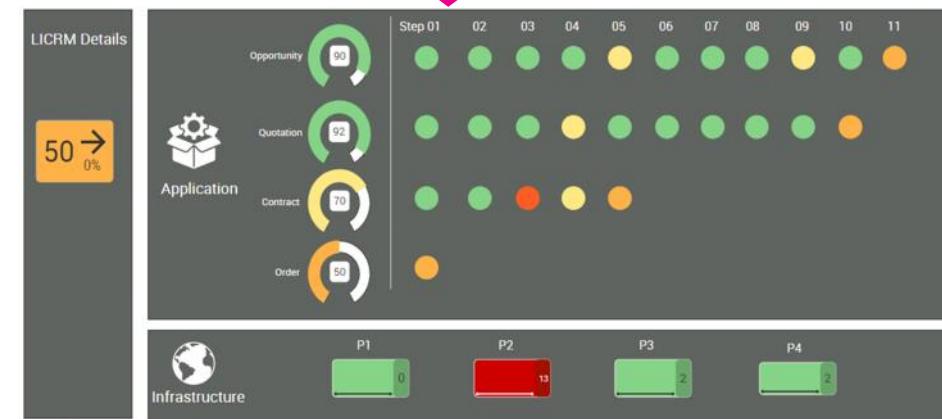
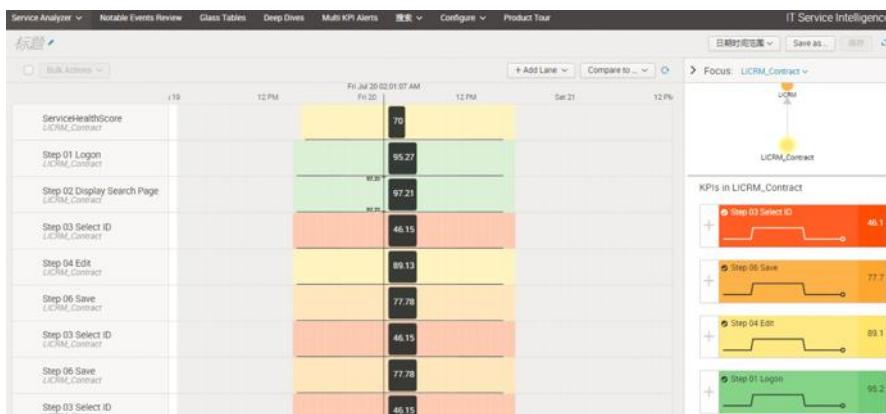
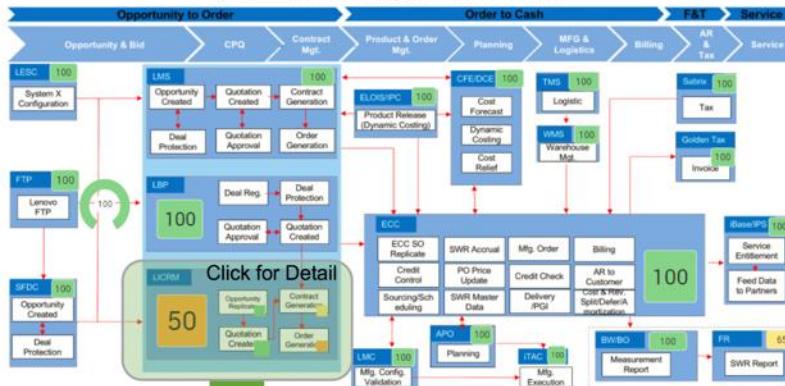
# Glass Tables

## 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



SAE系统监控平台





# Workshop Back Story

# Workshop Back Story

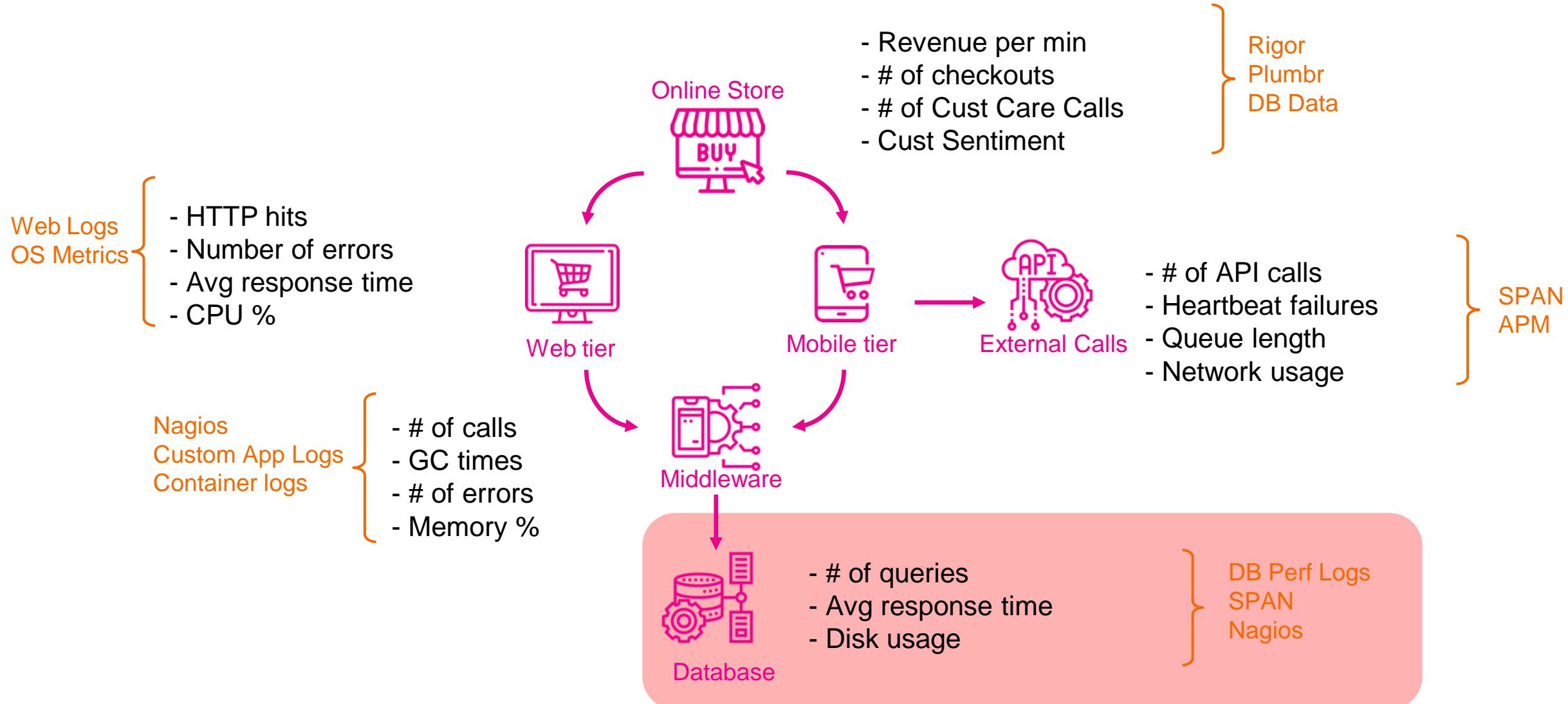
Buttercup Store has just deployed a new Web service, however the engineers forgot to include database monitoring.

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!

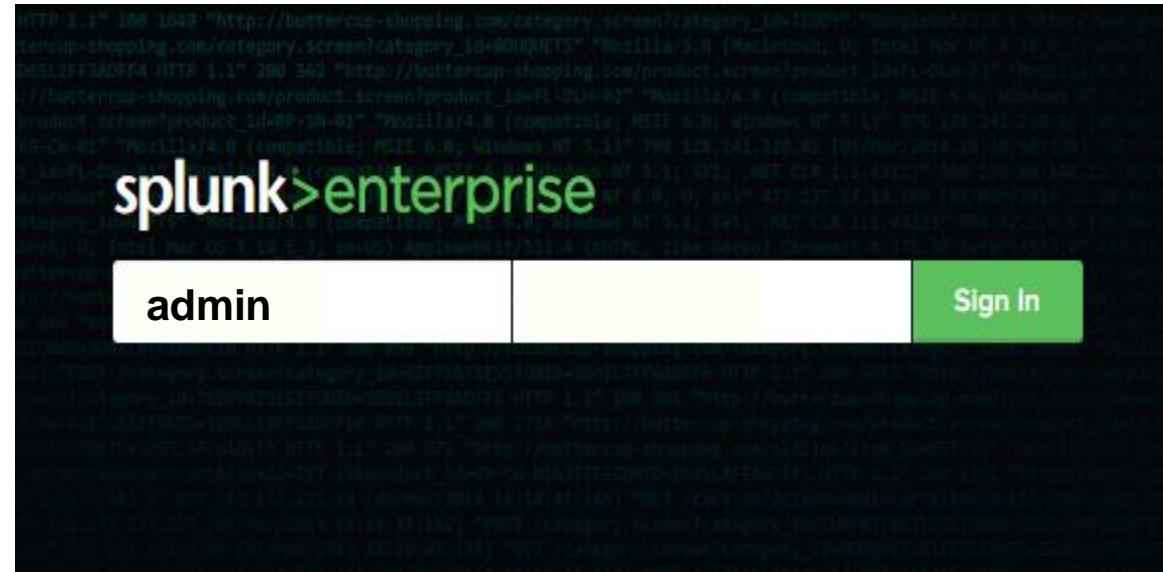
The lab starts on the back of a **service decomposition workshop** which has identify all the missing **database** components.

# Business Service Decomposition



# Let's get our hands dirty

Enter the following URL in your browser : [http://<aws\\_instance>:8000/en-US/](http://<aws_instance>:8000/en-US/)



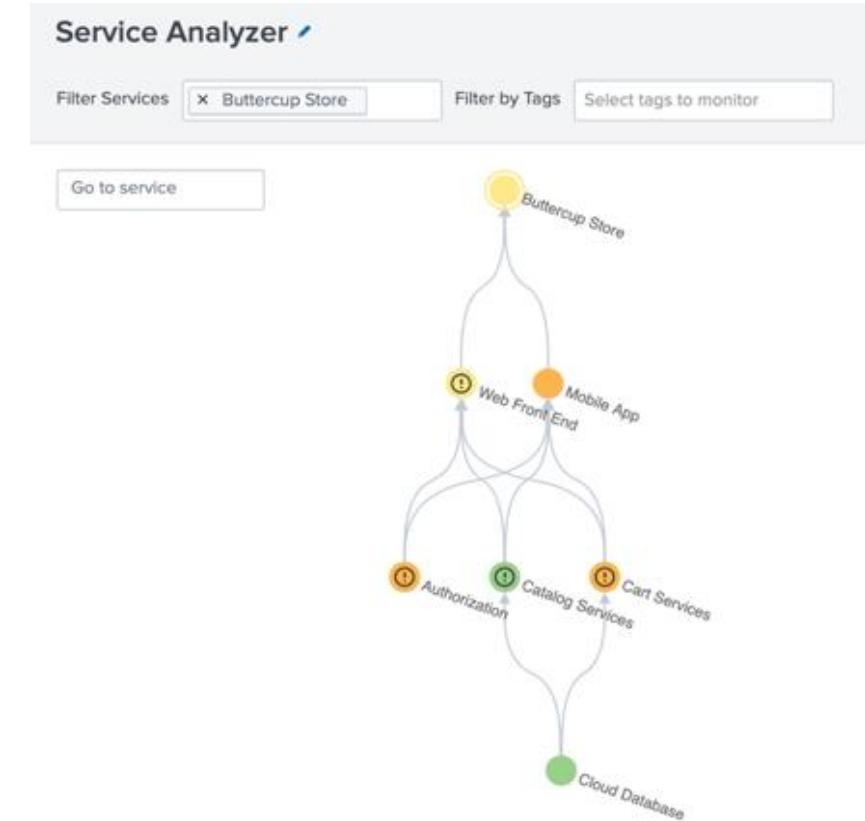
# Services Exercise

# 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.

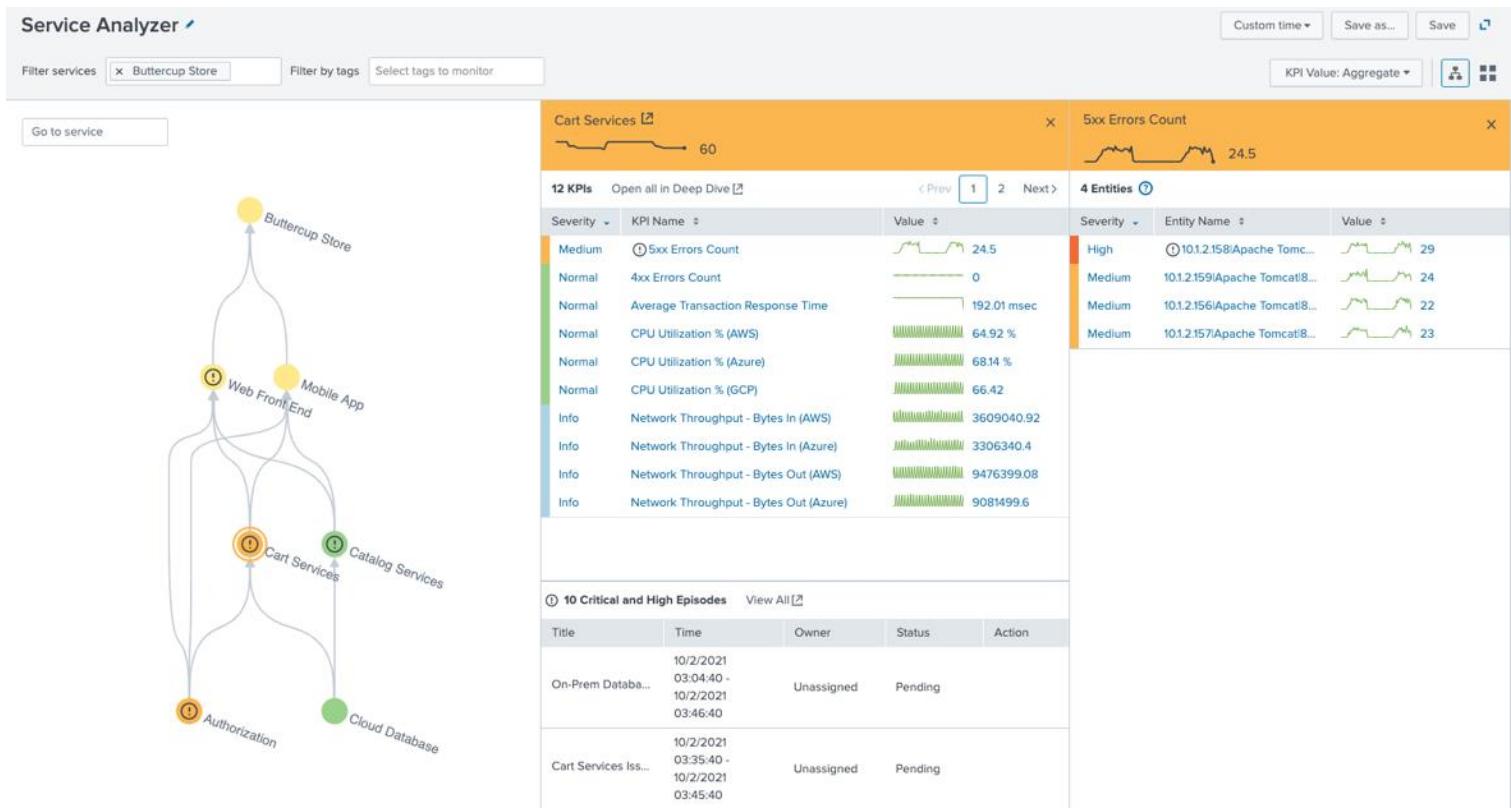
- Click on the Buttercup Store service and review the KPIs, notice that these are all business KPIs.
- Adjust the time picker to investigate when there was a severity degradation. (*note: there should be issues around an hour before the start of workshop (xx:10 - xx:20).*



# 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.

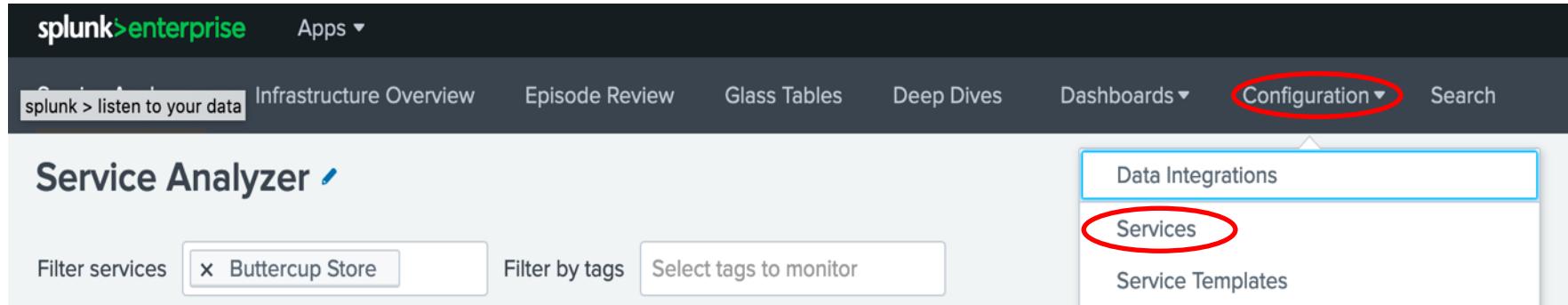
Services could use (technical) KPI’s that comes with these modules:

- 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

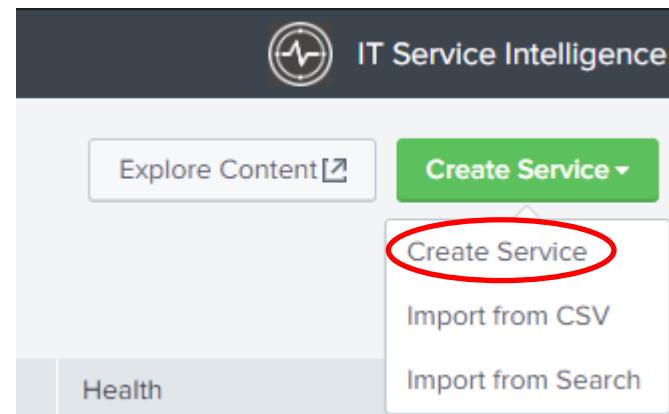
<https://docs.splunk.com/Documentation/ITSI/latest/IModules/AboutITSIModules>

# Services Lab

- Select the Configure menu + Services

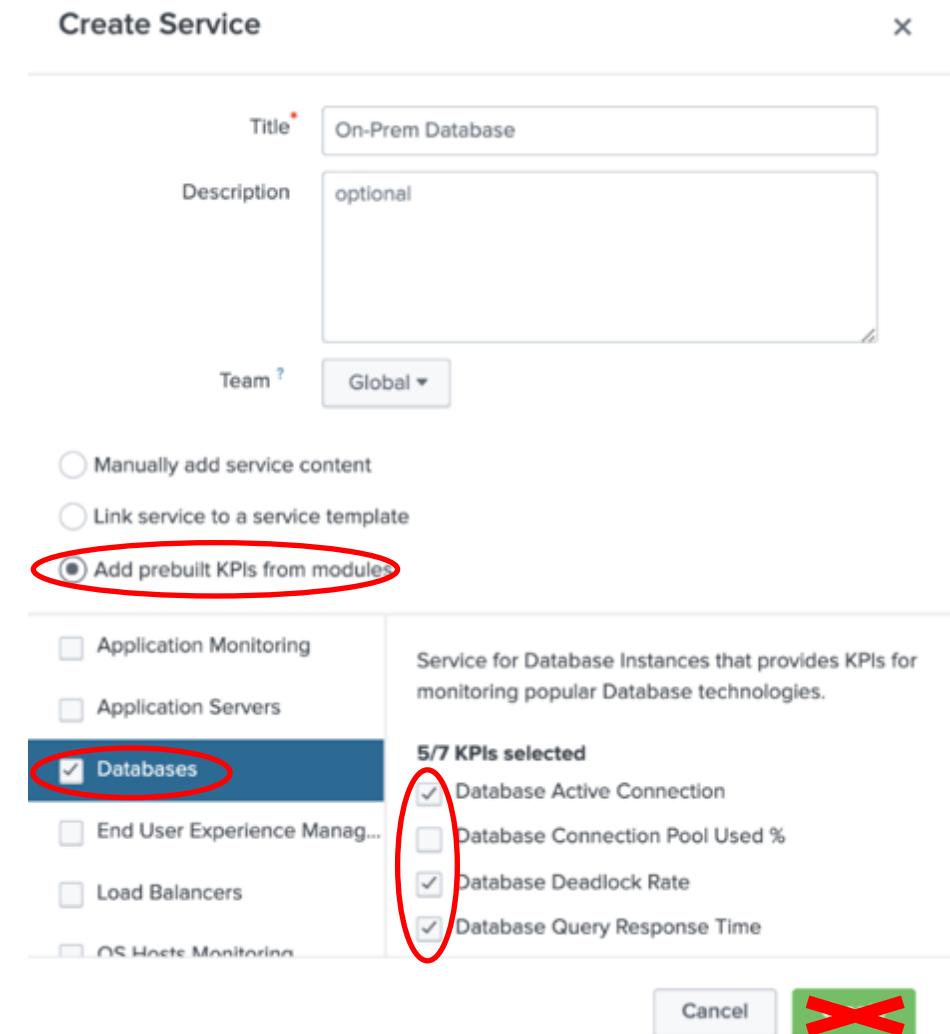


- Click Create Service > Create Service



# Services Lab

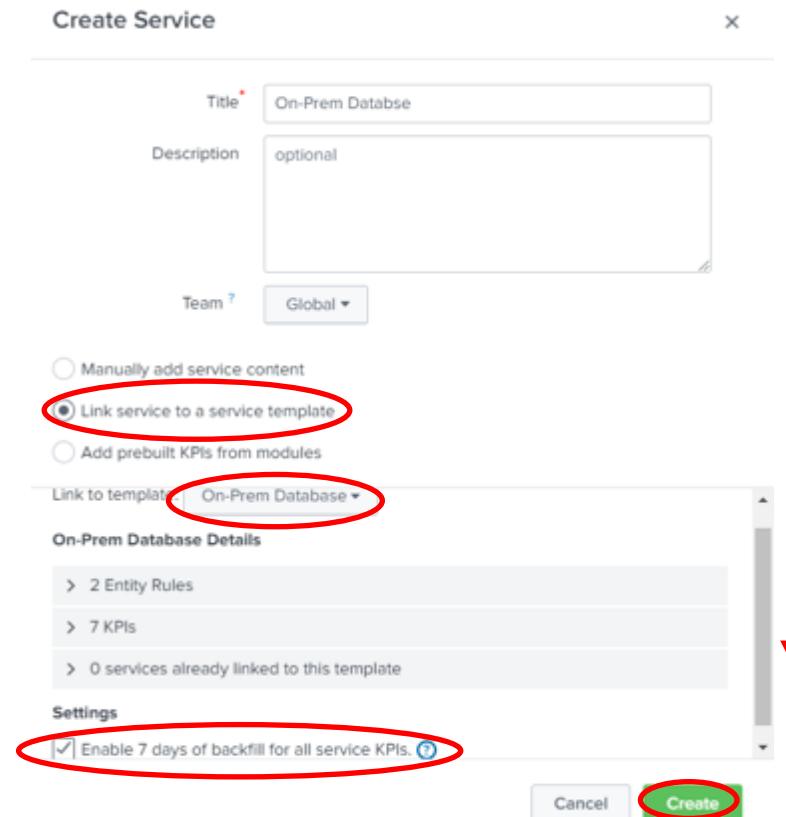
- Name the service ‘On-Prem Database’
- Check ‘Database’ in modules list
  - Review the selected KPIs
  - ***Do not hit the ‘Create’ button!***
- ITSI suggests the best KPIs for database monitoring.



# 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.

On-Prem Database

Service description

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.

Aliases: host  
matches: mysql\*

+ Add Rule (AND)  
+ Add Set of Rules (OR)

Matched Entities

Title	Aliases	Info
mysql-01	mysql-01, 237330cd-8600-4323-ad2c-9bcd3b4e6f62	domain-c8675, buttercup-store, datastore-8675, nix_host, host-8675, buttercup-01, 10.2.2.1, sal, vm-8675, mysql-01, linux, 2.6.32-573.8.1.el6.x86_64, global, resgroup-8675, db, 31fc983f4b15a9e21bee0d6dde38bb6f8abbf7830dd60fbdb8fac974a348730ab, database, prod-vcenter.buttercup.com
mysql-01	mysql-01	nix_host, 10.2.2.1, sal, linux, 2.6.32-573.8.1.el6.x86_64, db, 31fc983f4b15a9e21bee0d6dde38bb6f8abbf7830dd60fbdb8fac974a348730ab, database
mysql-02	mysql-02, 739cece1-4918-42a3-b5f5-5f64f8a46bc	domain-c8675, buttercup-store, datastore-8675, nix_host, host-8675, buttercup-01, 10.2.2.2, sal, vm-875, mysql-02, linux, 2.6.32-573.8.1.el6.x86_64, global, resgroup-8675, db, b1667fafcda7cdc7c0a845d9fb2b974446fbba898ef0963b0f49e07d2256968f, database, prod-vcenter.buttercup.com
mysql-02	mysql-02	nix_host, 10.2.2.2, sal, linux, 2.6.32-573.8.1.el6.x86_64, db, b1667fafcda7cdc7c0a845d9fb2b974446fbba898ef0963b0f49e07d2256968f, database
mysql-03	mysql-03, b384bc70-560b-4745-87eb-efb2769827d2	domain-c8675, buttercup-store, datastore-8675, nix_host, host-8675, buttercup-01, 10.2.2.3, sal, vm-853, mysql-03, linux, 2.6.32-573.8.1.el6.x86_64, global, resgroup-8675, db, 695ea9c5336c9f6828d384125ad259649823860eda97993ade88c4658b035879, database, nnn-vcenter.buttercup.com

# 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.

The screenshot shows the 'On-Prem Database' service configuration page. At the top, there's a navigation bar with tabs: Entities, KPIs (which is the active tab, indicated by a red circle), Service Dependencies, Settings, and Predictive Analytics. Below the navigation bar, there's a sub-navigation bar with tabs: KPIs (active), Clone, and New. A main content area is titled 'Database Queries'. Under 'KPI description', there are three items: 'Search and Calculate' (with a lock icon), 'Thresholding', and 'Anomaly Detection'. To the left of the main content area, there's a sidebar with a list of KPIs: 'Disk I/O - Read Ops' (locked), 'Disk I/O- Write Ops' (locked), 'Disk Space Used %' (locked), 'Memory Used %' (locked), 'Network Throughput - Inbound' (locked), and 'Network Throughput - Outbo...' (locked). The bottom right corner of the screenshot has a small 'oing' logo.

# 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 of the Splunk Services Lab interface. The 'Status' field is set to 'Enabled' (highlighted with a red circle). The 'Backfill' dropdown is set to 'None' (highlighted with a large red X). The 'Simulated Health Score' for 'On-Prem Database' is 100. The 'Save' button at the bottom right is also highlighted with a red circle.

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 '*Authorization*' service

Service Analyzer ▾ Episode Review Glass Tables Deep Dives Multi-KPI Alerts Dashboards ▾ Search ▾ **Configure** ▾ Product Tour

IT Service Intelligence

Services

A service is a collection of KPIs and entities that represent a real-world IT service.

11 Services	Bulk Action ▾	filter							
Name	Actions	Status	Service Template	Entity Rules	KPIs	Health	Team		
Authorization	Edit ▾	Enabled	Not linked	4	14	View Health	Global		
Buttercup Store	Edit	Enabled	Not linked	0	21	View Health	Global		
Cart Management	Edit Team	Enabled	Synced with Cloud-Based Services	4	20	View Health	Global		

Explore Content ▾ Create Service ▾

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

Service Analyzer ▾ Episode Review Glass Tables Deep Dives Multi-KPI Alerts Dashboards ▾ Search ▾ Configure ▾ Product Tour

IT Service Intelligence

Authorization

Service description

Entities KPIs **Service Dependencies** Settings Predictive Analytics

Remove selected dependencies Add dependencies

Title	Service
ServiceHealthScore	External Authentication Services

Data into doing'

# Services Lab

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

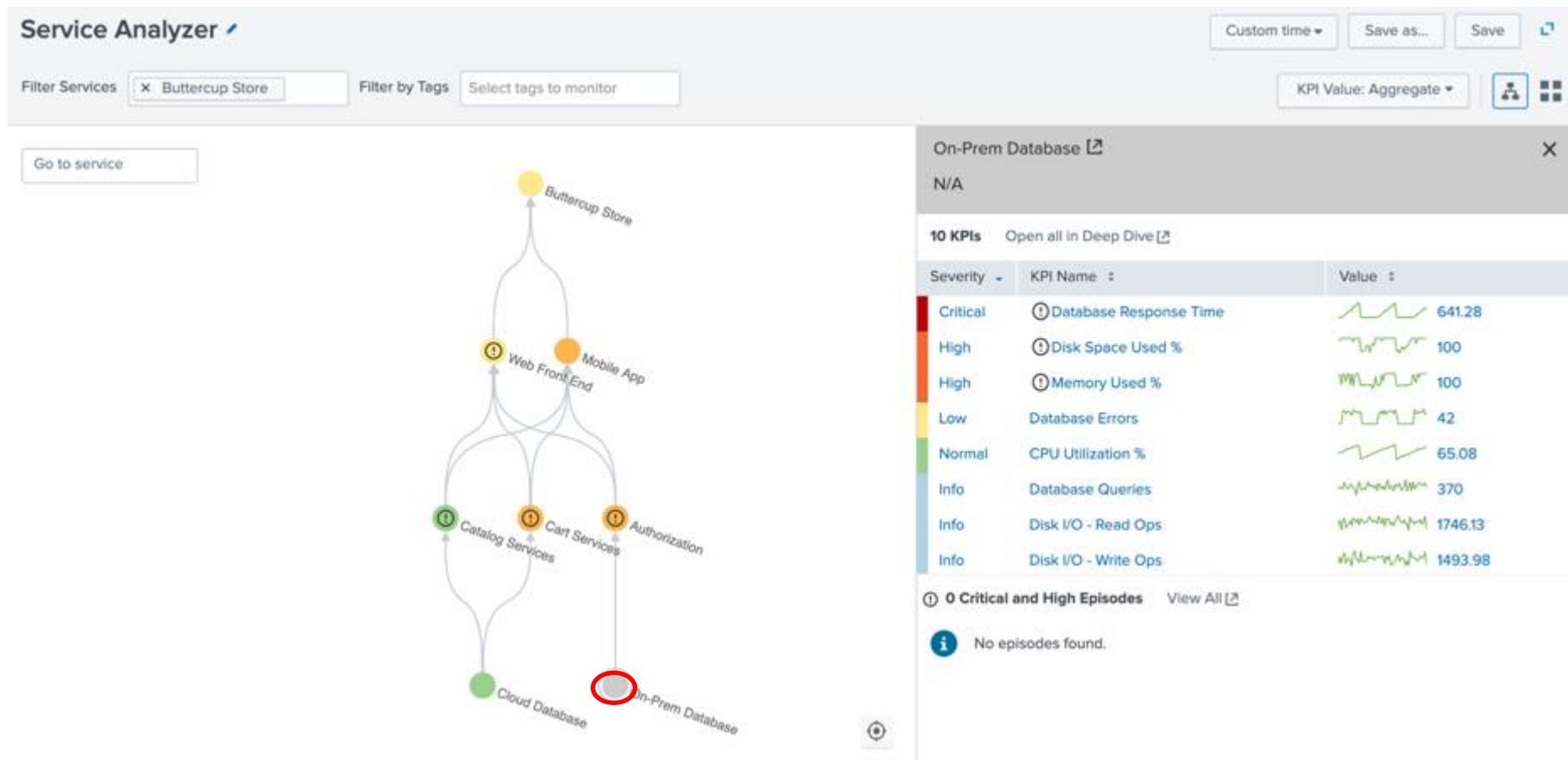
Add dependencies

<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

Network Services  
 Networking  
 NTP  
 On-Prem Database  
 Order Management  
 Product Catalog  
 Shared Database Environment  
 Shared IT Infrastructure  
 Shared Storage  
 Shared Storage - Arrays  
 Shared Storage - LUNs  
 Shared Storage - Volumes  
 SMTP - DMZ In

# 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

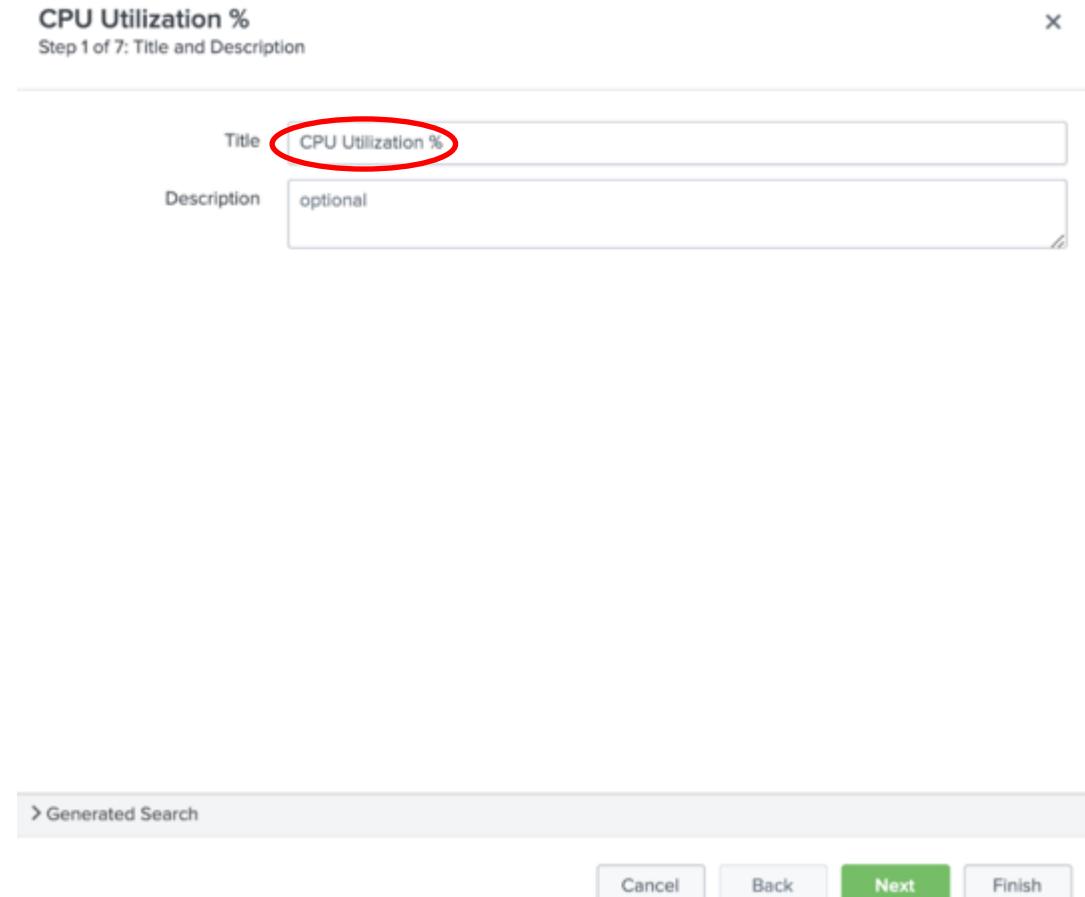
CPU Utilization %  
Step 1 of 7: Title and Description

Title: CPU Utilization %

Description: optional

> Generated Search

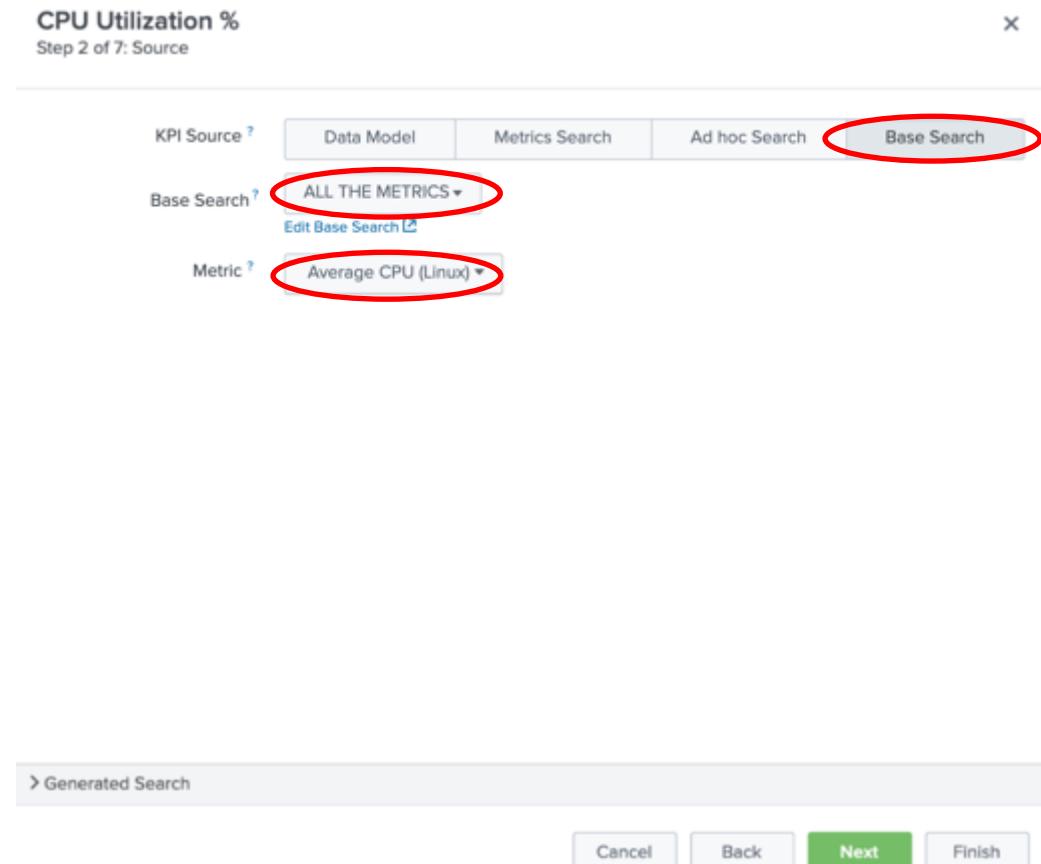
Cancel Back Next Finish



# 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 ‘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.

CPU Utilization %  
Step 3 of 7: Entities

⚠ Fields are populated from the selected base search.

Split by Entity ?	Yes	No
Entity Split Field ?	host	
Filter to Entities in Service ?	Yes	No
Entity Filter Field ?	host	

Service must have entities to filter by entities.

Generated Search

Cancel Back Next Finish

# 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

- Click 'Next' button

› Generated Search

Cancel Back Next Finish

# KPI Lab

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

CPU Utilization %  
Step 5 of 7: Optional Setup - Unit and Monitoring Lag

⚠ Fields are populated from the selected base search.

Unit   
Specify the unit of measurement to display in KPI visualizations. (For example "GB," "Mbps," "secs", etc.).

Monitoring Lag (in seconds) ?  [Determine Recommended Lag](#)

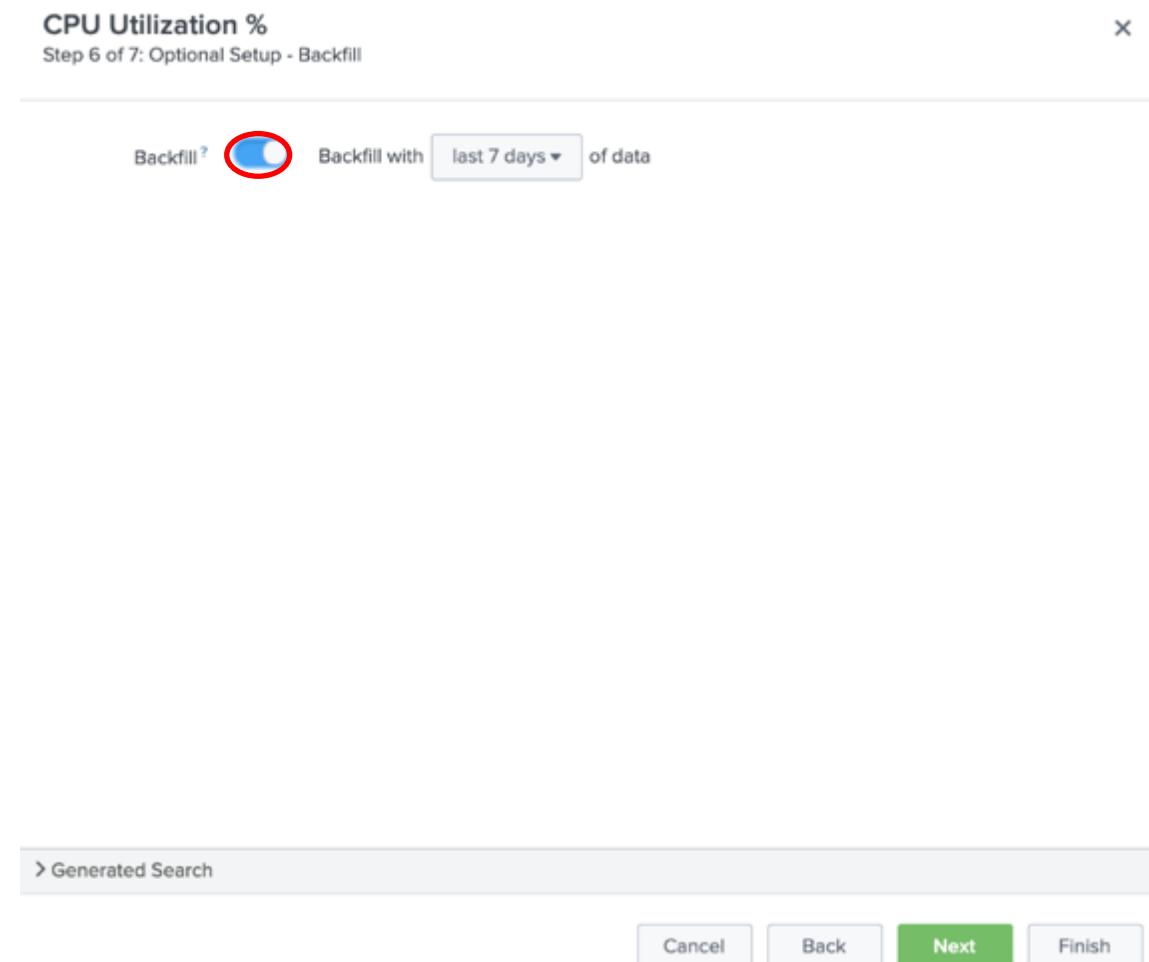
> Generated Search

[Cancel](#) [Back](#) [Next](#) [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

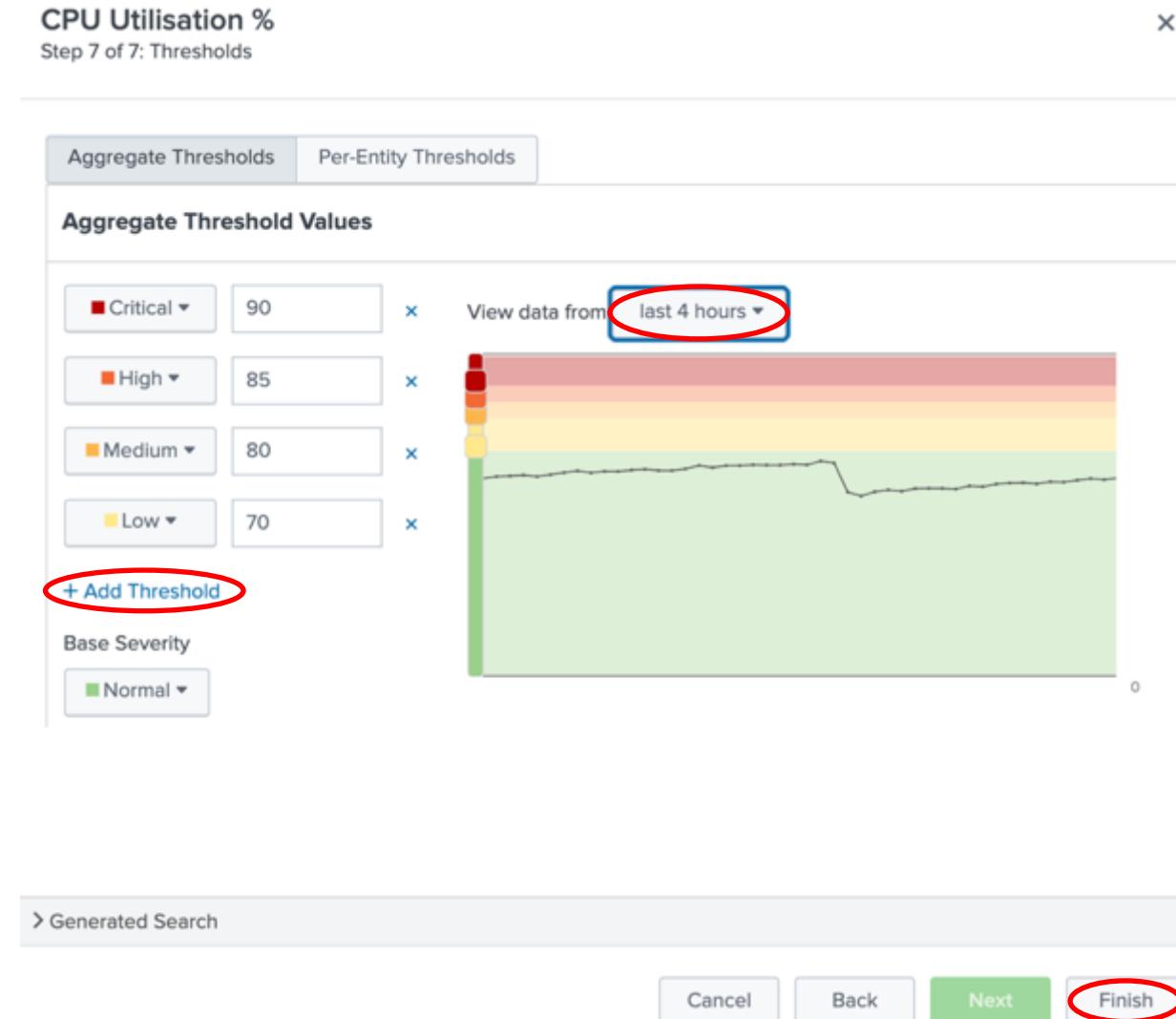


- Click ‘Next’ button

# 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

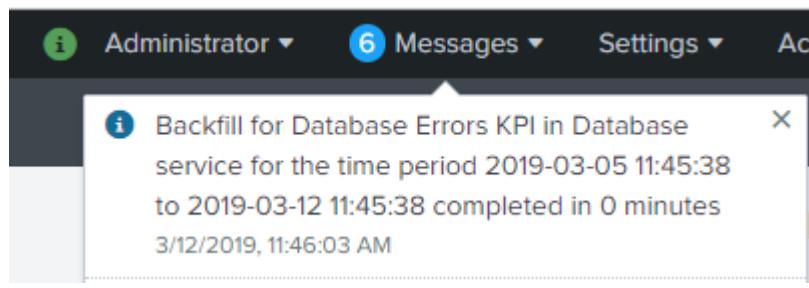


# KPI Lab

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

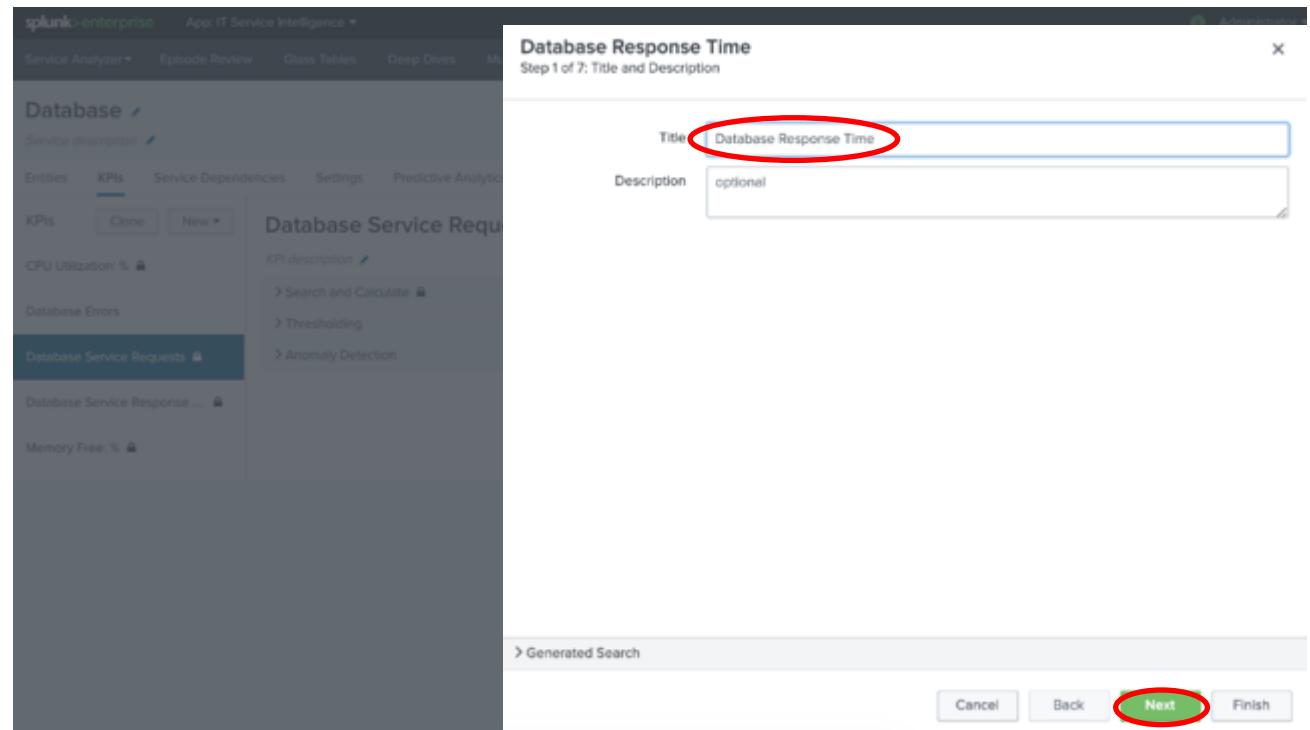


A screenshot of the ADF KPI configuration page for the 'On-Prem Database' service. The 'KPIs' tab is selected. On the left, a list of KPIs includes 'CPU Utilization %' (selected), 'Database Queries', 'Disk I/O - Read Ops', 'Disk I/O- Write Ops', 'Disk Space Used %', 'Memory Used %', 'Network Throughput - Inbound', and 'Network Throughput - Outbo...'. On the right, a detailed view of the 'CPU Utilization %' KPI shows sections for 'KPI description', 'Search and Calculate', 'Thresholding', and 'Anomaly Detection'. At the bottom right of the main panel, there are 'Cancel' and 'Save' buttons, with 'Save' being circled in red.

# 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

Database Response Time  
Step 2 of 7: Source

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

Search ? `index=itsidemo sourcetype=stream:mysql query=*`

Run Search ↗

Threshold Field ? `time_taken`

Generated Search

Cancel Back Next Finish

# 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

Database Response Time  
Step 3 of 7: Entities

Split by Entity ?  Yes  No

Entity Split Field ?

Filter to Entities in Service ?  Yes  No

Service must have entities to filter by entities.

Generated Search

Cancel Back  Next Finish

# 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

Database Response Time  
Step 4 of 7: Calculation

X

Calculation Options:

KPI Search Schedule ?  (circled)

Entity Calculation ?  (circled)

Service/Aggregate Calculation ?  (circled)

Calculation Window ?  (circled)

Fill Data Gaps with ?

Threshold level for Null values ?

Explanation of Calculation:

Every minute take the average of time\_taken for each entity as the entity value then take the average of all entity values as the service/aggregate value all over the last 5 minutes. Fill gaps in data with Null values and use a unknown threshold level for them.

> Generated Search

Cancel Back Next (circled) Finish

# KPI Lab

We will leave the next screen with the default values.

Database Response Time  
Step 5 of 7: Optional Setup - Unit and Monitoring Lag

Unit  Specify the unit of measurement to display in KPI visualizations. (For example "GB," "Mbps," "secs", etc.).

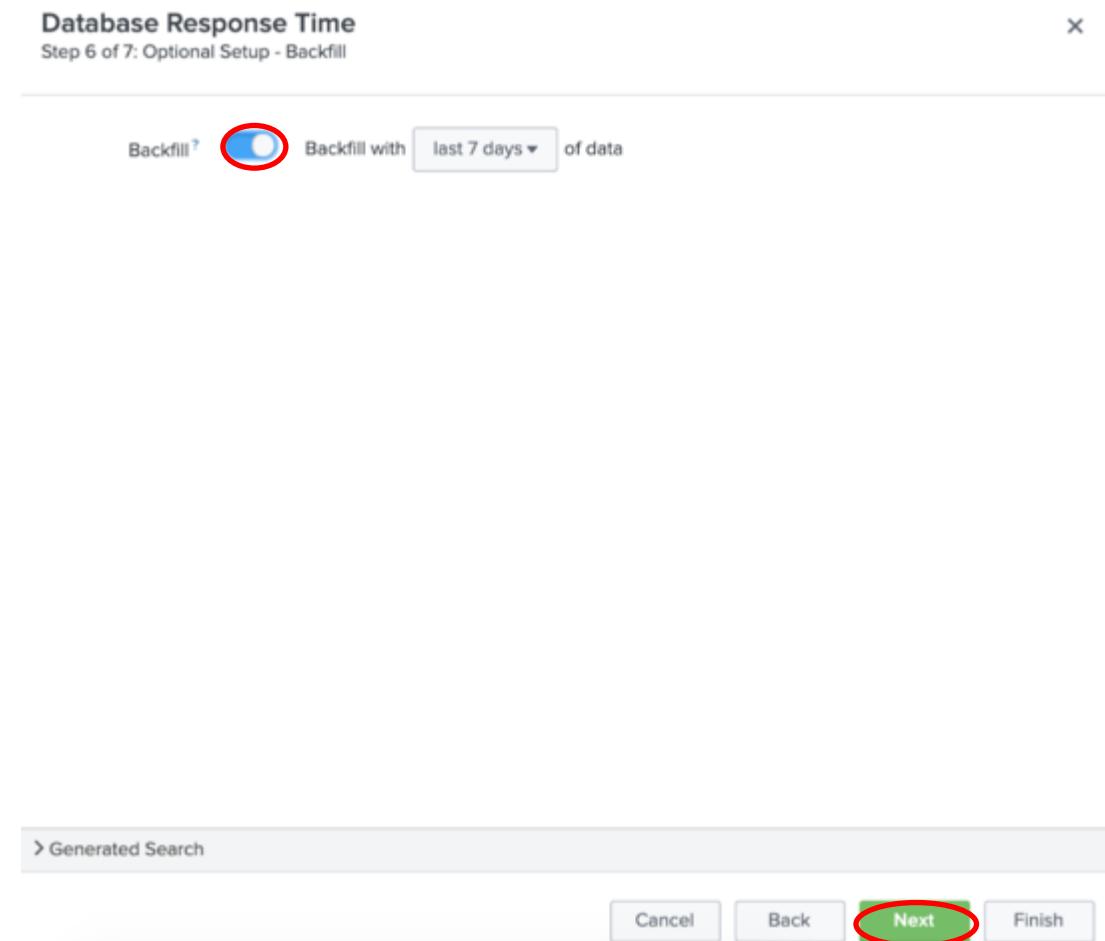
Monitoring Lag (in seconds) ?  Determine Recommended Lag [?](#)

> Generated Search

# 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.

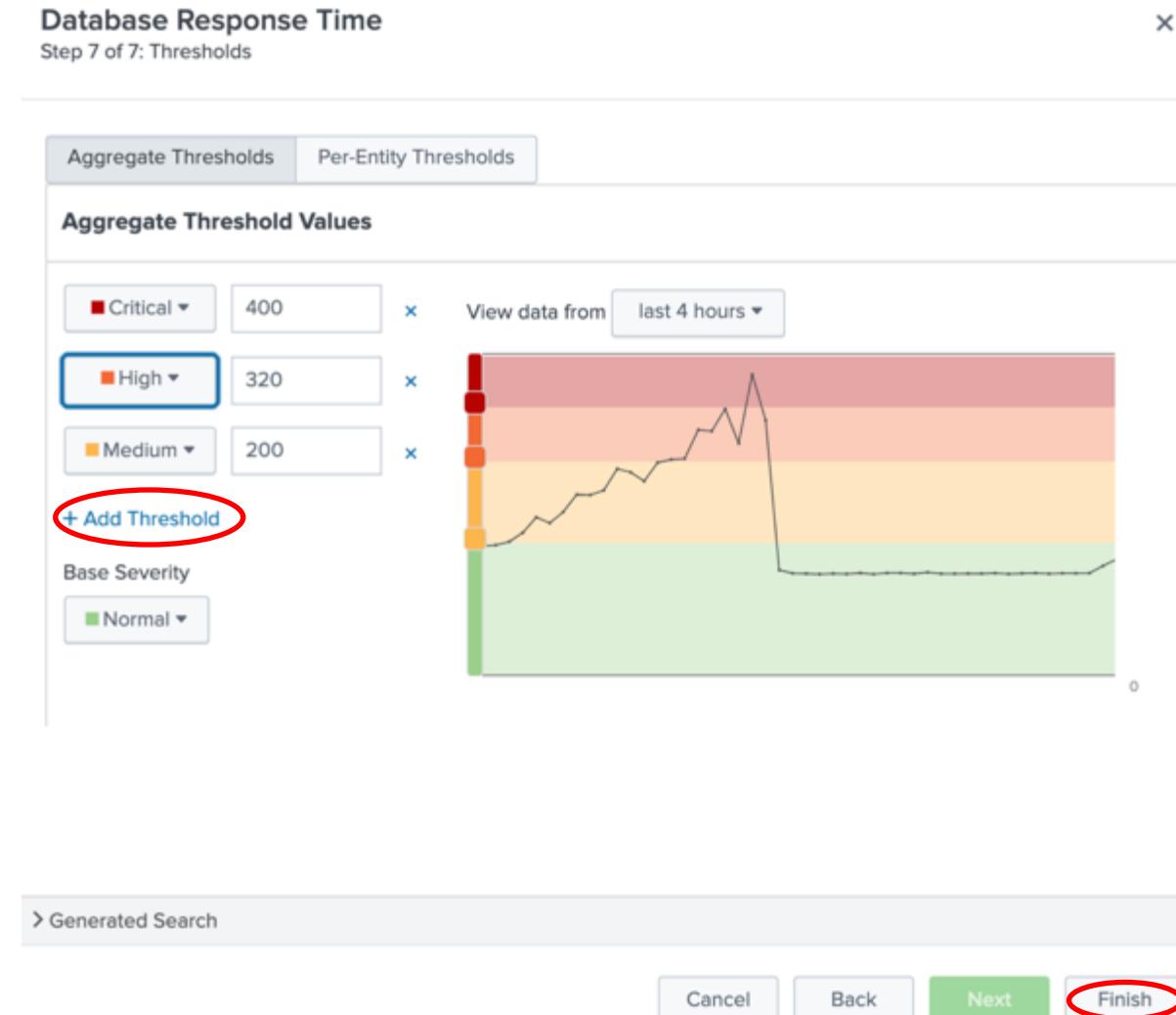
- Click ‘Enable Backfill’ button
- We will leave the backfill period as 7 days
- Click ‘Next’ button



# 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

The screenshot shows the 'On-Prem Database' service configuration page. The 'Settings' tab is highlighted with a red circle. The 'General' section shows the service is enabled and part of the 'Global' team. 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 'Service Health Score' section has a 'Backfill' toggle switch turned on, which is also circled in red. A note below says: '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.' The 'Health Score Calculation' section allows tweaking the importance of KPIs. The 'On-Prem Database KPIs' table lists four KPIs: CPU Utilization %, Database Queries, Database Response Time, and Disk I/O - Read Ops. Each KPI has a dropdown menu for 'Simulated Severity' (set to 'Normal') and a slider for 'Importance'. To the right, a large green box displays the 'Simulated Health Score' as 100. At the bottom right, there are 'Cancel' and 'Save' buttons, with the 'Save' button also circled in red.

# 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.

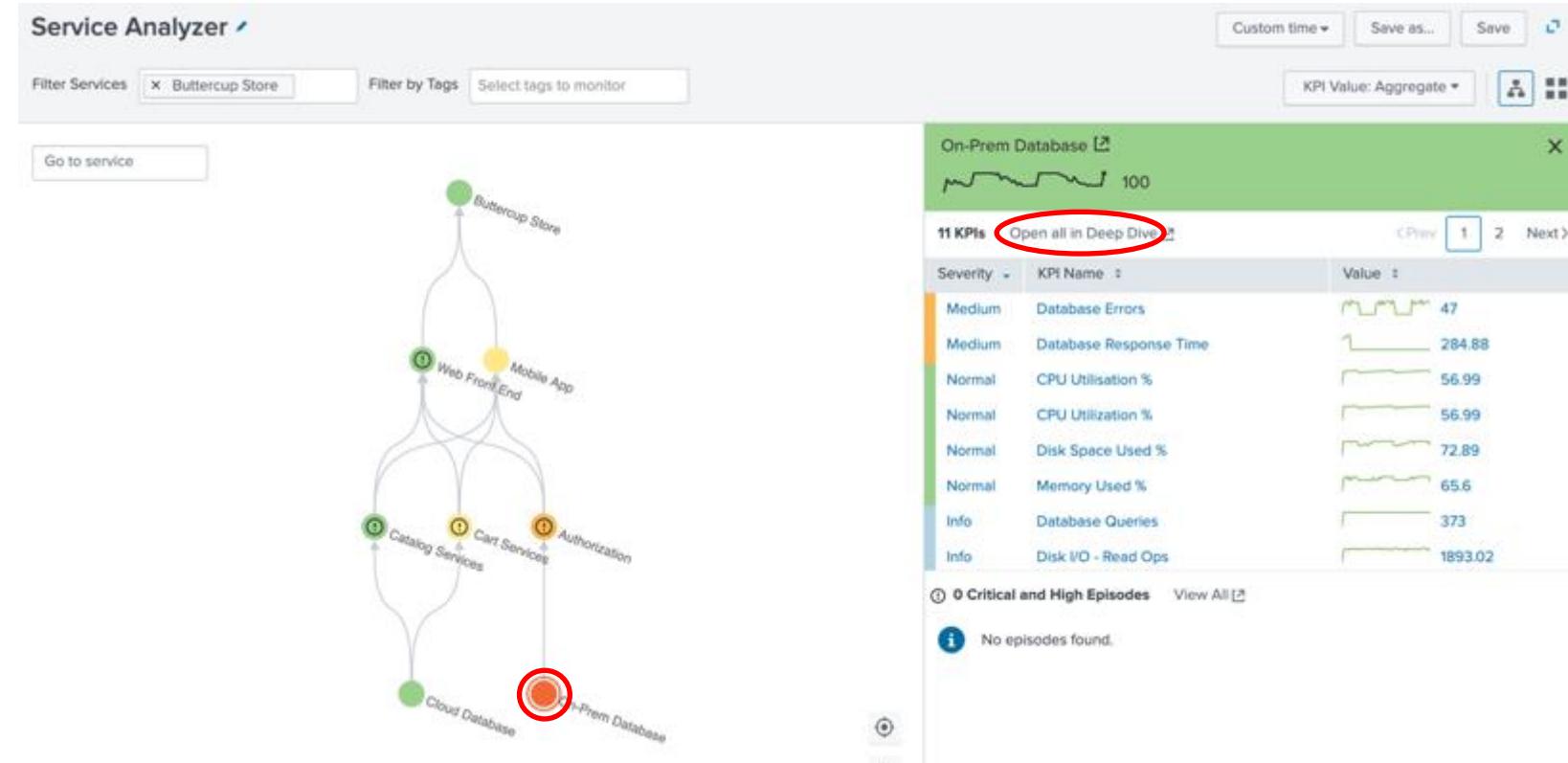
The deep dive capabilities within ITSI brings together multiple data sources into a single visualization. The correlation of data streams enable quick identification of root cause and effect on the business.

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’

The screenshot shows the 'Lane Overlay Options' configuration page. At the top right, a context menu is open for the 'Disk Space Used %' KPI, with the 'Edit Lane' option highlighted by a red circle. The main area contains settings for enabling overlays, overlay type, graph color, and selection mode. Below these are tables for 'Selected Entities' and 'Alert\_Levels'. A large green 'Save' button at the bottom right is also circled in red.

Disk Space Used %

On-Prem Database

Memory Used %

On-Prem Database

Network Throughput

On-Prem Database

Database Services

Edit Lane

Graph Rendering Options

Lane Overlay Options

Threshold Options

Edit KPI

Delete Lane

Open in Search

Lane Overlay Options

Enable Overlays  Yes  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	x
mysql-02	x
mysql-03	x

Cancel  Save

Ink > turn data into doing'

# 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’

A screenshot of a 'Add Event Lane' dialog box. It contains the following fields:

- Title: Database Service Errors
- Subtitle: optional
- Graph Color: Automatic
- Lane Size: Small, Medium, Large (with Small selected)
- Event Search: index=itsidemo mysql err (this field is highlighted with a red circle)

At the bottom right of the dialog box is a green 'Create Lane' button, which is also highlighted with a red circle.

# Deep Dive Lab

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

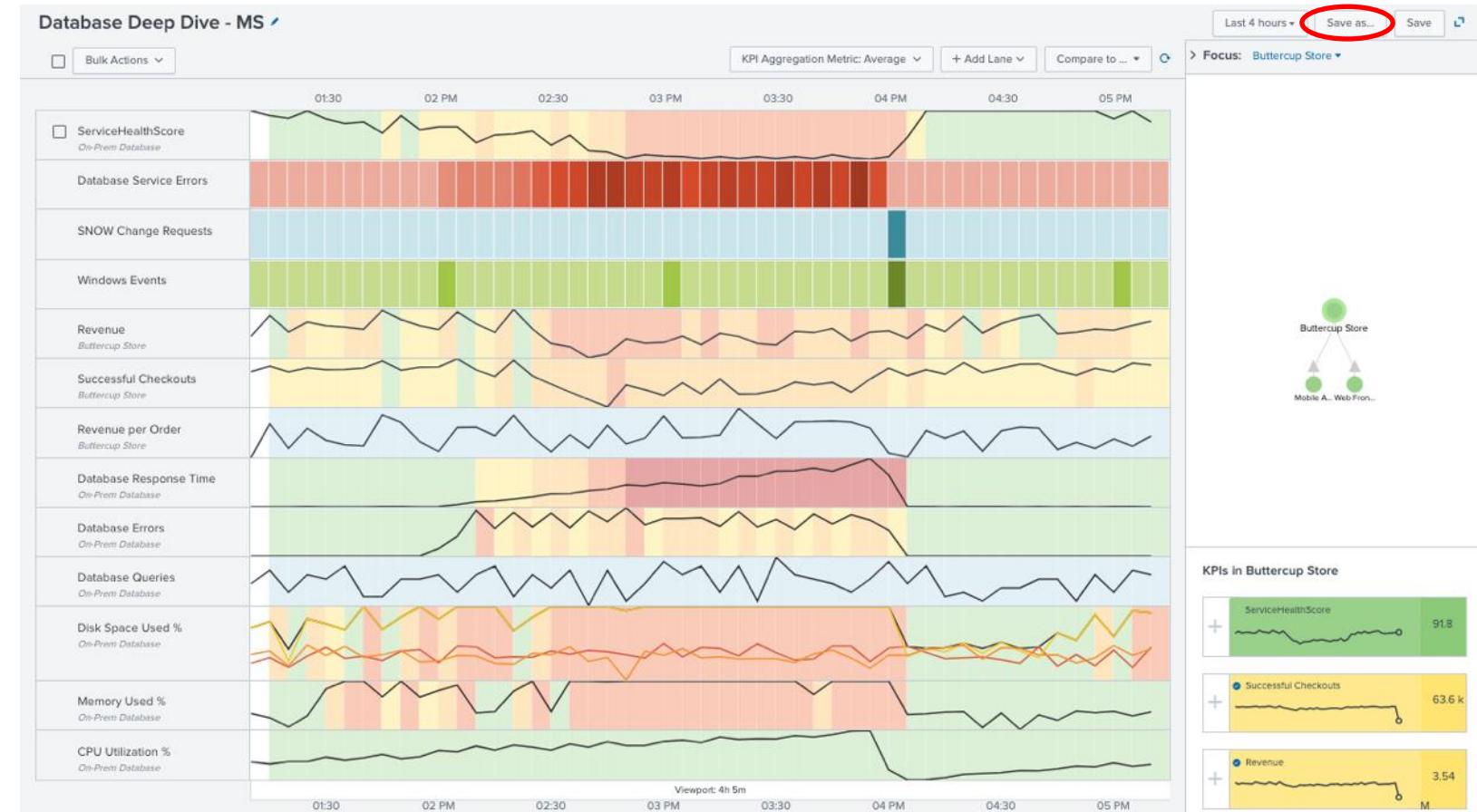
- Select ‘Add Lane’
  - Click ‘Add Event Lane’
- 
- Type ‘SNOW Change Requests’ Title
  - Event Search:
    - *‘index=itsidemo sourcetype=snow:change\_request’*
  - Click ‘Create Lane’

A screenshot of a 'Add Event Lane' dialog box. It has fields for 'Title' (SNOW Change Requests), 'Subtitle' (optional), 'Graph Color' (Purple), 'Lane Size' (Medium selected), and an 'Event Search' field containing the query 'index=itsidemo sourcetype=snow:change\_request'. A red circle highlights the 'Event Search' field. At the bottom right, there are 'Cancel' and 'Create Lane' buttons, with 'Create Lane' also circled in red.

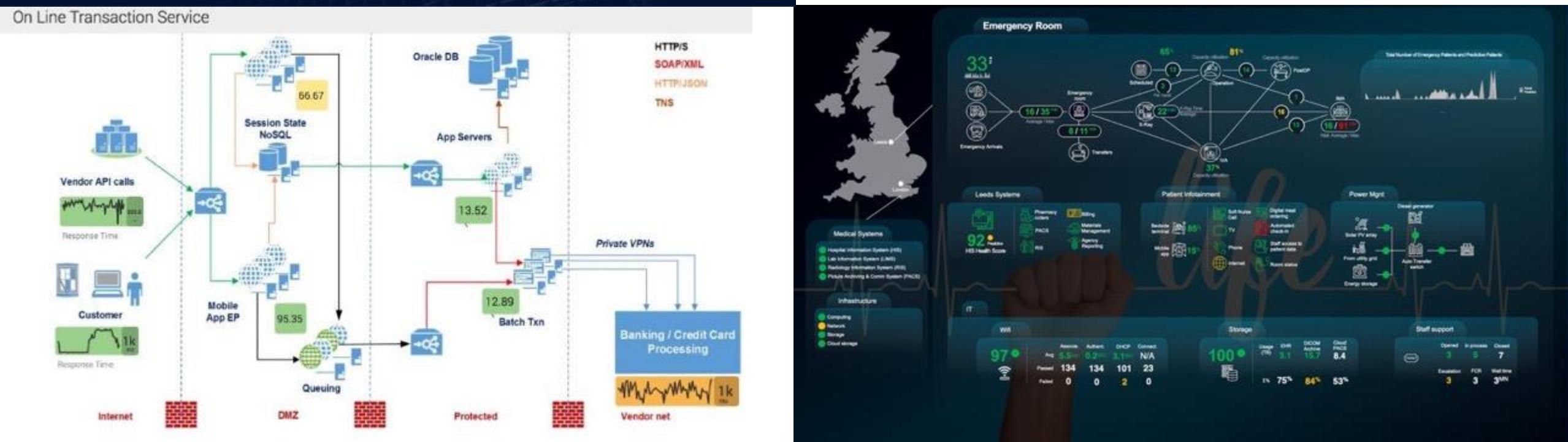
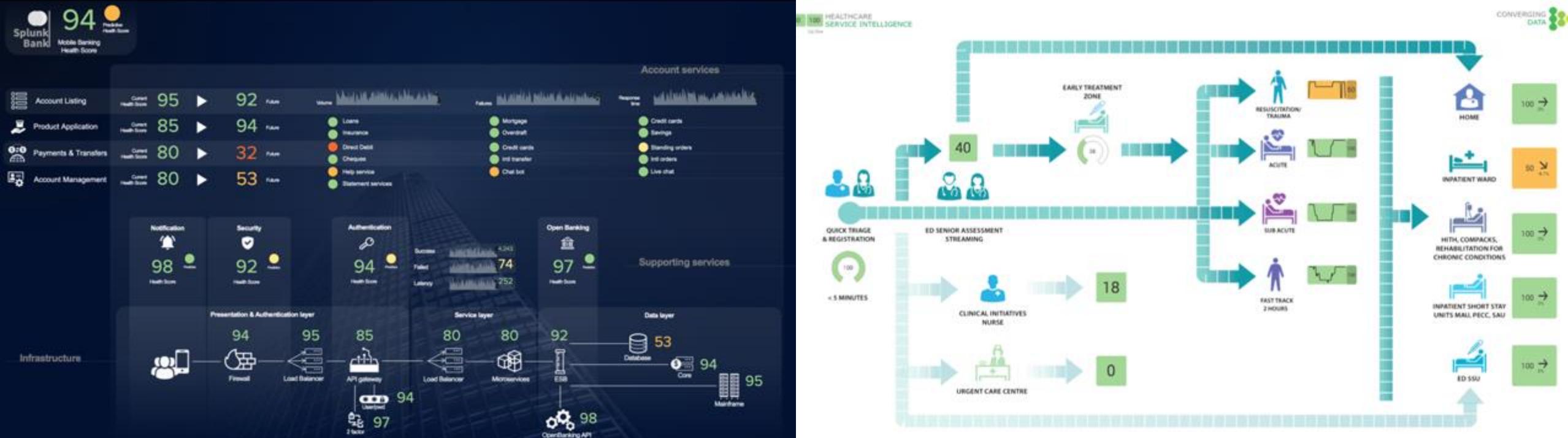
# Deep Dive Lab

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 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*

## Saved Glass Tables

Use glass tables to create custom visualizations to monitor KPIs and service health scores.

8 Glass Tables

Bulk Action ▾

All

App

Private

filter

<input type="checkbox"/>	<i>i</i>	Title ▾	Actions
<input type="checkbox"/>	>	1 - Operational and Executive Visibility	Edit ▾
<input type="checkbox"/>	>	3 - Online Checkout Funnel	Edit ▾
<input type="checkbox"/>	>	Manufacturing	Edit ▾
<input type="checkbox"/>	>	Mobile Banking	Edit ▾
<input type="checkbox"/>	>	Retail	Edit ▾
<input type="checkbox"/>	>	S4N - Transaction Flow	Edit ▾
<input type="checkbox"/>	>	Telco	Edit ▾
<input type="checkbox"/>	>	Travel	Edit ▾

S4N - Transaction Flow

Gridlines  75% View

Global Time Range Global Refresh Rate

Last 60 minutes 1 Minute

Configuration

Canvas

Display Mode

Actual Size Fit to Width

Canvas Width Canvas Height

Background Color #2B2C33

Background Image background.png

Original Size

Image Width Image Height

X Position Y Position

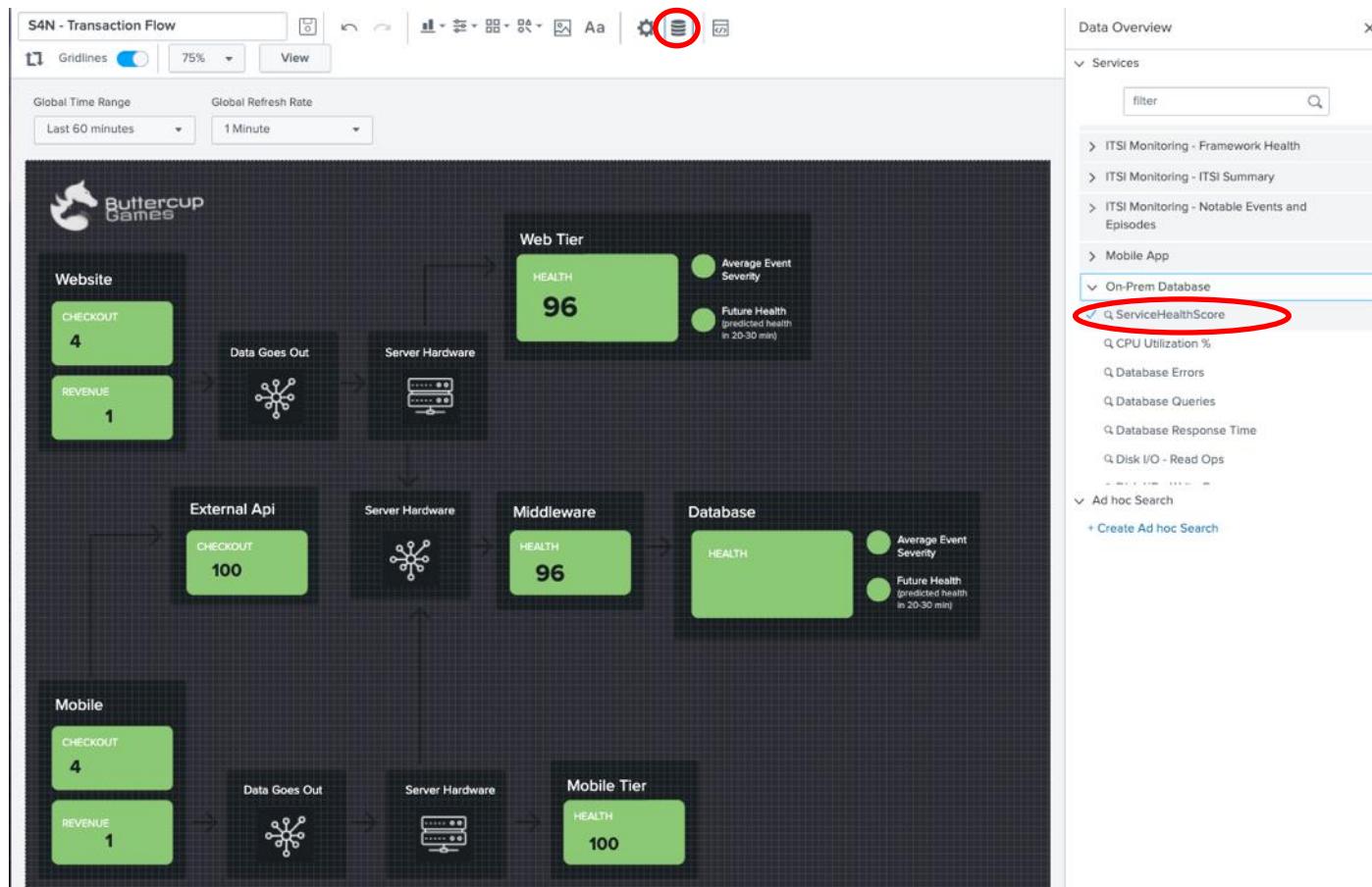
Preferences Show Title & Description

# Glass Table Lab

- Click the “Data Overview”
- Select *On-Prem Database*
- Click Service Healthscore

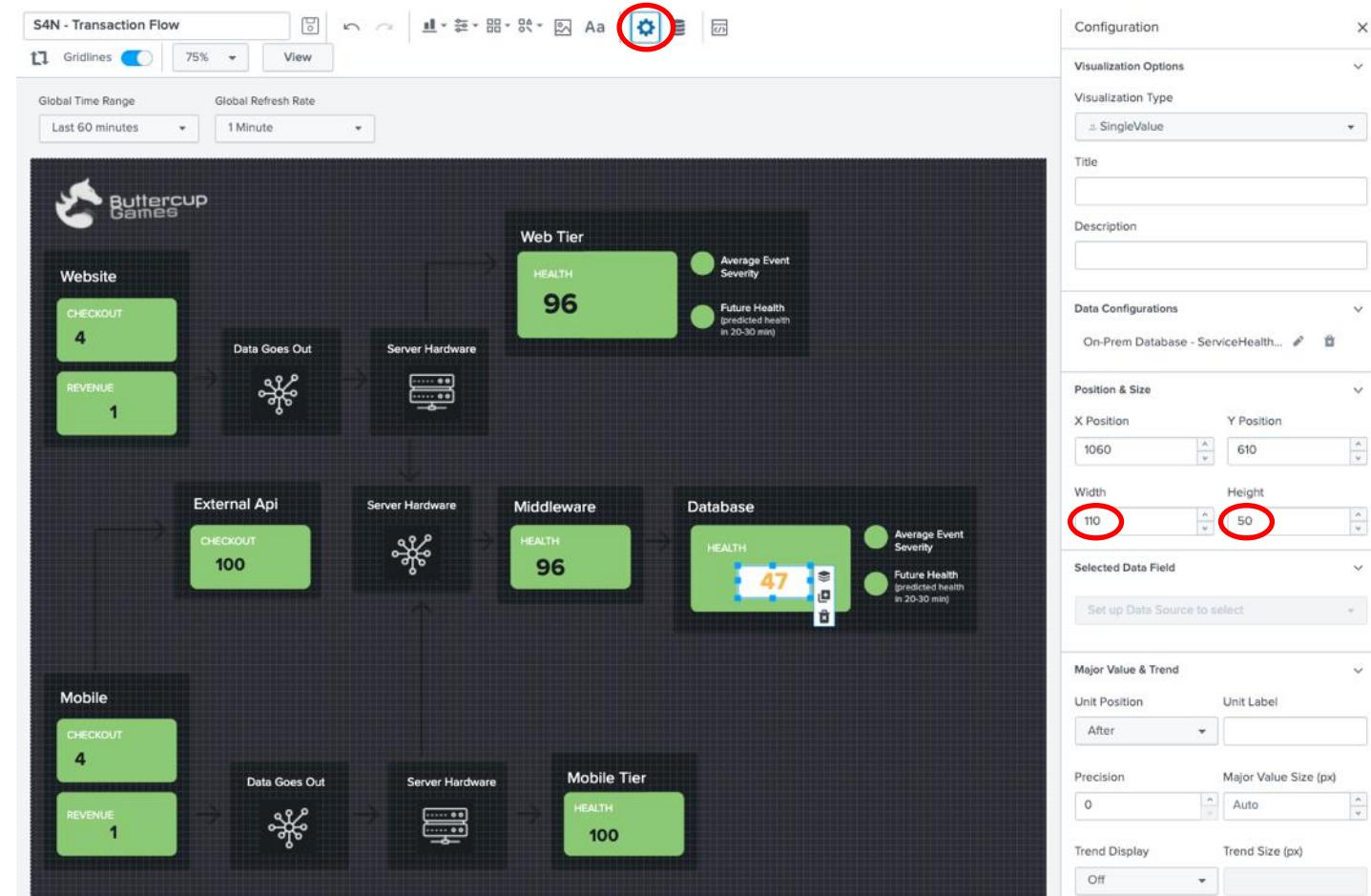


button in the pallet menu  
vice (*scroll down or use the filter box*)



# Glass Table Lab

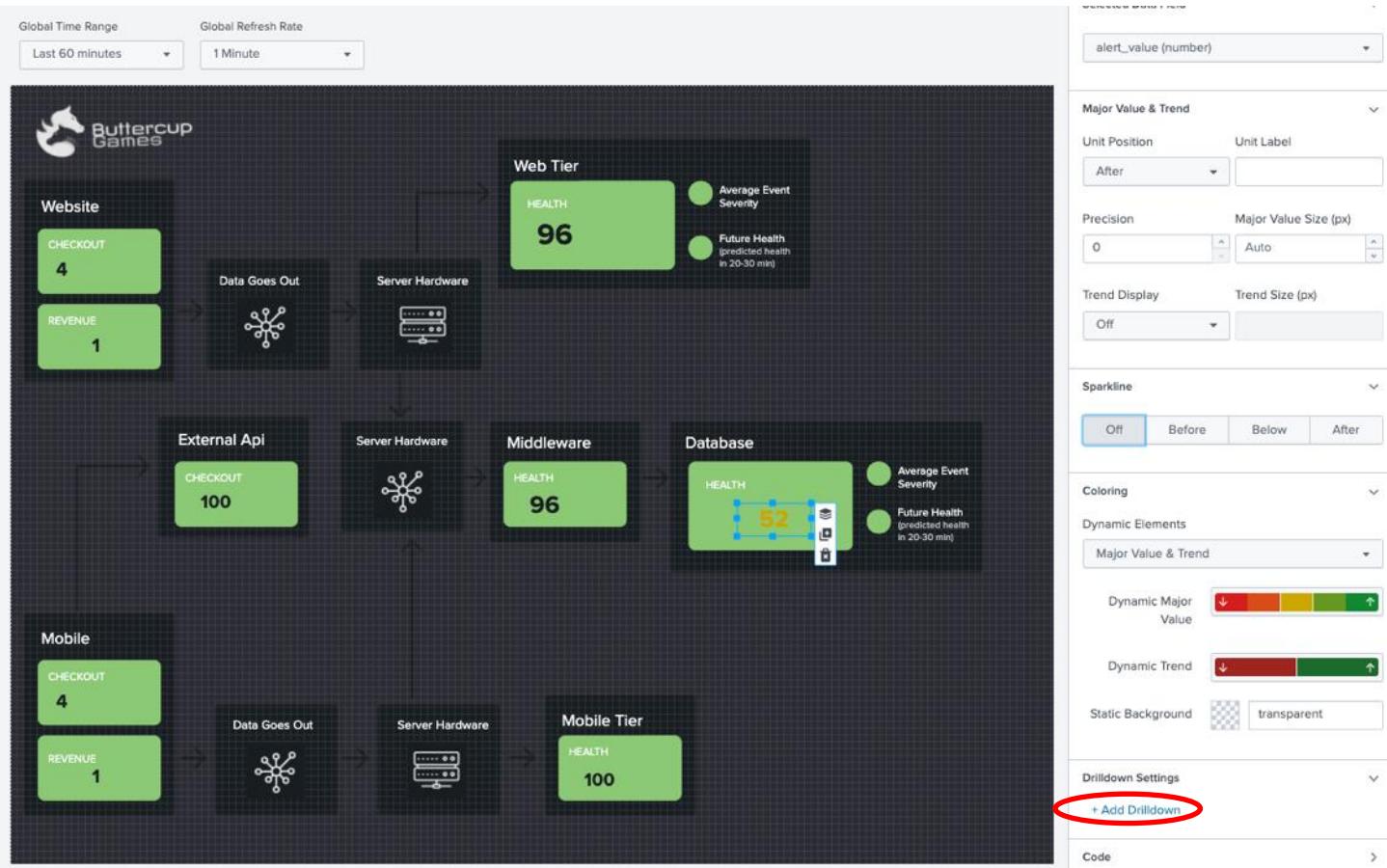
- Move the Service Health Score to the correct position
- Modify size to appropriate size and investigate options



# Glass Table Lab

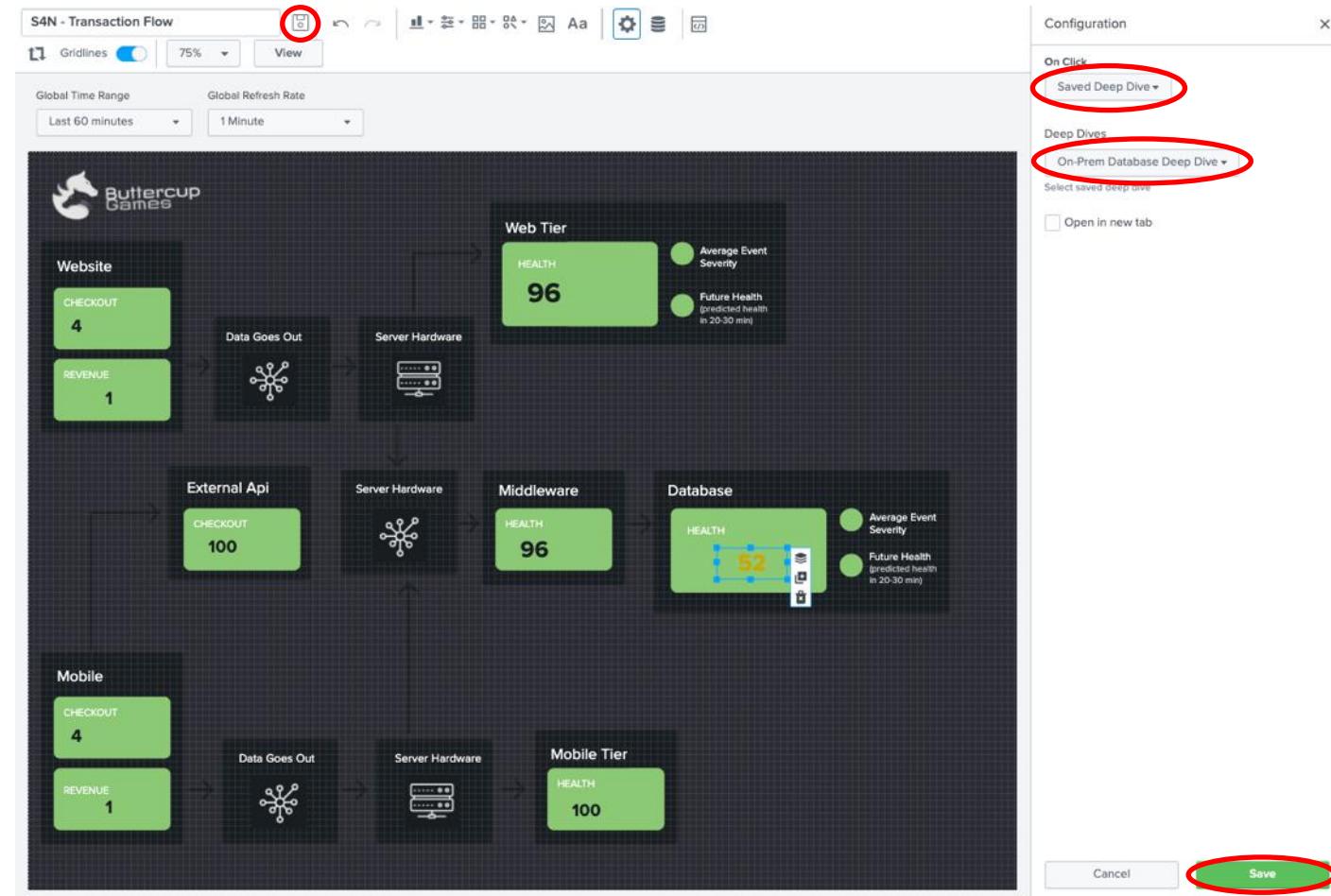
We will now link the database deep dive visualization to this glass table

- 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

## Splunk Expertise

Searching  
Reporting  
Alerting  
Workflow

ITSI  
Premium solutions  
with ML capabilities.

## MLTK

Splunk Toolkit  
examples &  
guidance

## Data Science Expertise

Statistics/math background  
Algorithm selection  
Model building

## IT Operations Expertise

Identify use cases  
Drive decisions  
Understanding of business impact

# ITSI Machine Learning

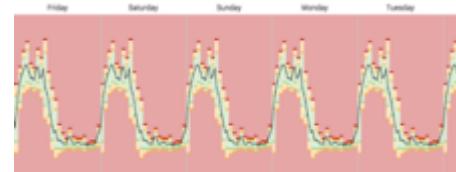
## Anomaly Detection



Deviation from past behavior  
Deviation from peers  
Unusual change in features

### ITSI Anomaly Detection

## Adaptive Thresholds



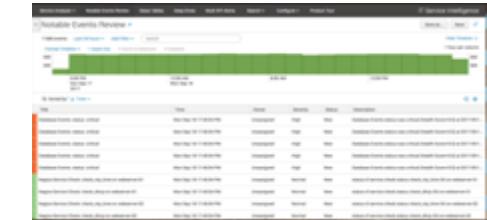
**Adaptive Thresholds**  
What is normal behaviour and what is not normal  
Ideal for cyclical and dynamic data

## 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.

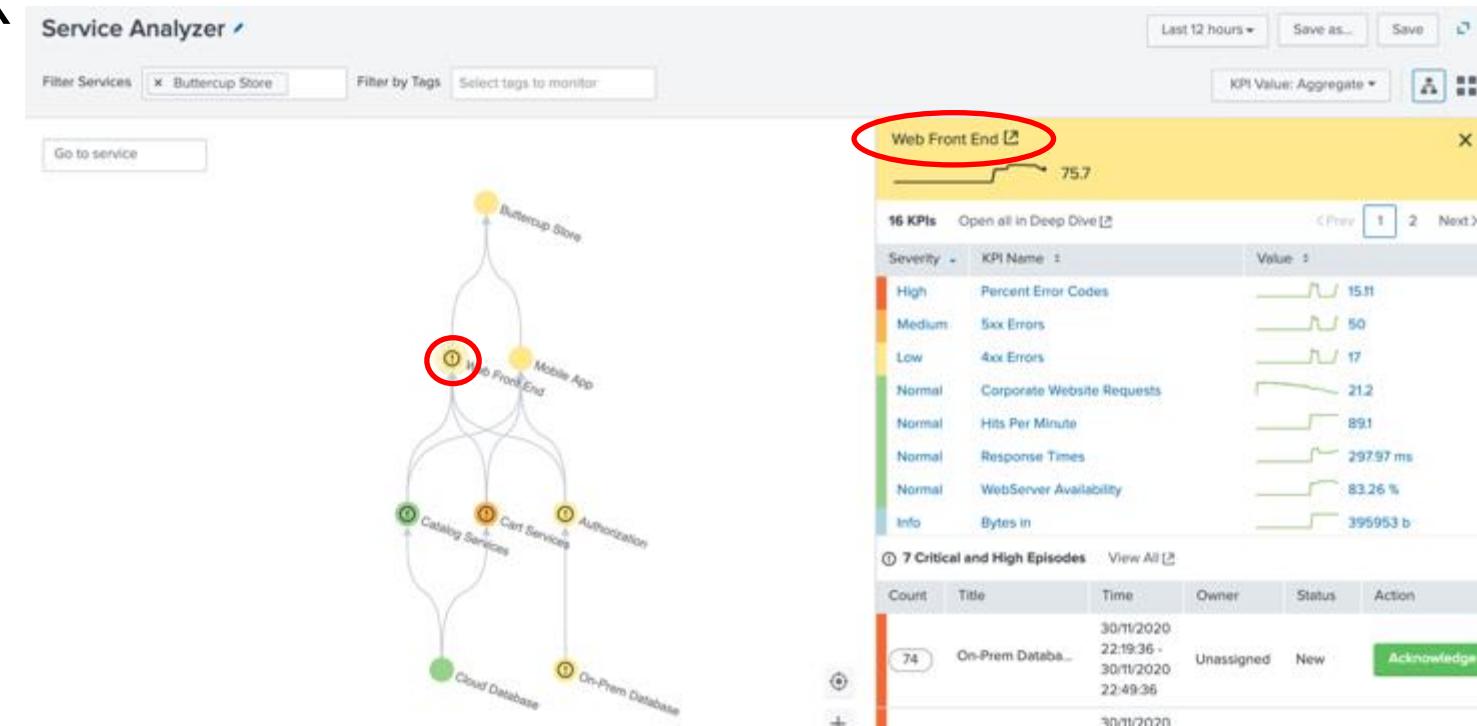
The objective of this exercise to is utilise Splunk ITSI machine learning capabilities to identify normal behaviour for web response time.

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

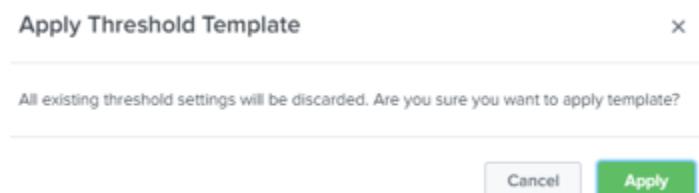
We need to instruct ITSI to use a template for thresholding, we will be using the adaptive standard deviation 3 hour working week template.

- Select the '*Corporate Website Requests*' KPI

The screenshot shows the ITSI interface for the 'Web Front End' service. The top navigation bar includes tabs for Entities, KPIs (which is the active tab), Service Dependencies, Settings, and Predictive Analytics. Below the navigation, there are several KPIs listed: 4xx Errors, 5xx Errors, Bytes in, Bytes out, and Corporate Website Requests. The 'Corporate Website Requests' button is highlighted with a red oval. On the right side, the 'Corporate Website Requests' KPI details are displayed, including its description, search and calculate options, thresholding settings (with 'Set Custom Thresholds' selected), and policy enablement options for time policies, adaptive thresholding, and KPI alerting.

# 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



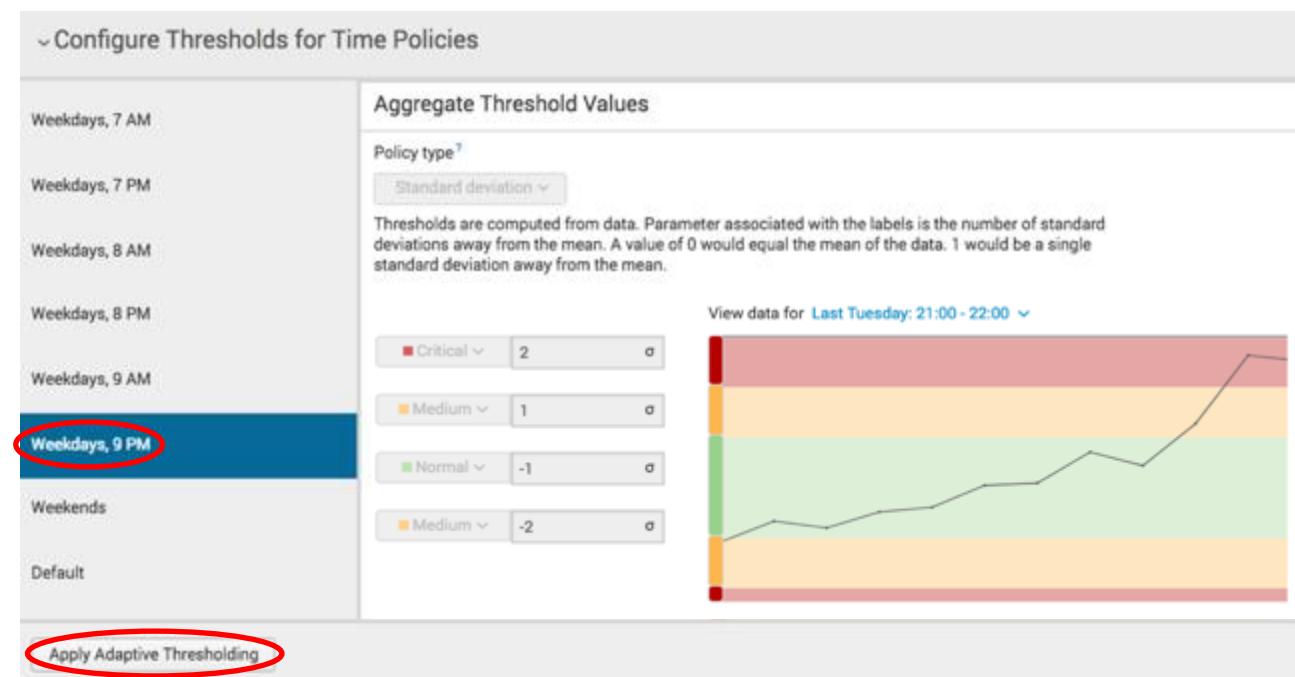
Screenshot of the Splunk interface showing the 'Corporate Website Requests' KPI page. The 'KPIs' tab is selected. On the left, there are several metrics listed: 4xx Errors, 5xx Errors, Bytes in, Bytes out, Corporate Website Requests (which is highlighted in blue), CPU Utilization %, Disk I/O - Read Ops, Disk I/O - Write Ops, Memory Used %, and Network Throughput - Inbound.

The 'Corporate Website Requests' section contains a 'KPI description' field with a link to 'Search and Calculate' and a 'Thresholding' section. Under 'Thresholding', the 'Use Thresholding Template' radio button is selected, and a dropdown menu shows '3-hour blocks work week (adaptive/stdev)' which is circled in red. Other options in the dropdown include 'Set Custom Threshold', '3-hour blocks work week (adaptive/quantile)', '3-hour blocks work week (adaptive/range)', '3-hour blocks work week (static)', 'AM, PM (adaptive/quantile)', 'AM, PM (adaptive/range)', and 'AM, PM (adaptive/stdev)'. A 'Training window' dropdown is set to '7 days'. Below the dropdown, a 'Preview Aggregate' section shows a timeline from Thursday to Monday with AM and PM markers.

# 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.

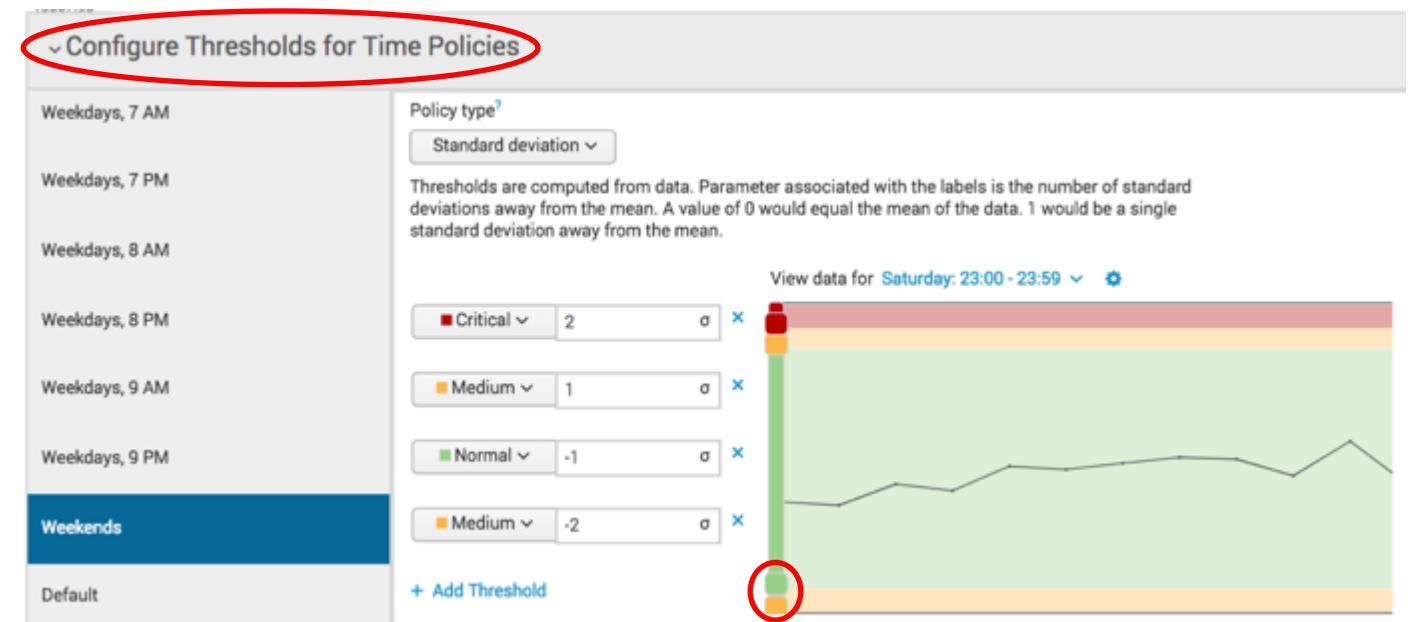
- Click on '*Thresholding*' arrow
- Review the preview window
  - Note weekend range
- Click '*Set Custom Threshold*'



# 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

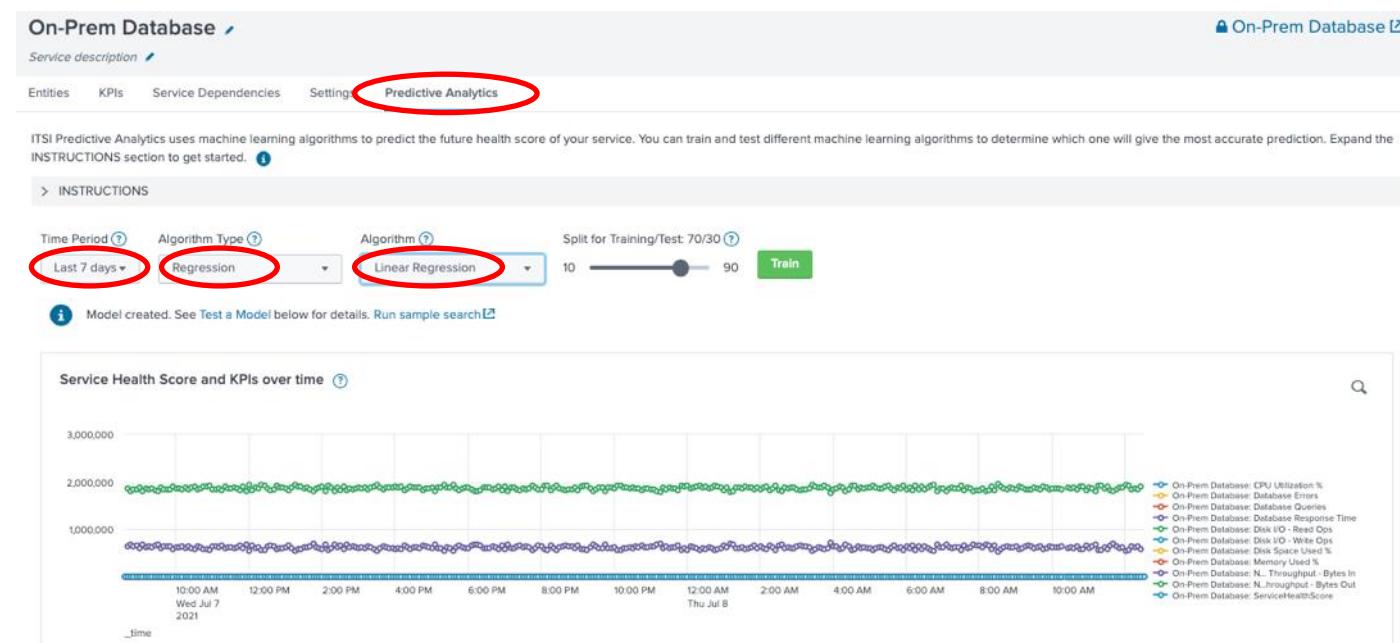
The screenshot shows the IT Service Intelligence web application. The top navigation bar includes links for Service Analyzer, Infrastructure Overview, Episode Review, Glass Tables, Deep Dives, Dashboards, Configuration (which is circled in red), and Search. Below the navigation is a sub-navigation bar with links for Explore Content and Create Service. The main content area is titled 'Services' and contains a table with 23 entries. The table columns are: Actions, Status, Service Template, Entity Rules, KPIs, Health, and Team. The 'On-Prem Database' row is highlighted with a red circle around its 'Edit' button. The table also includes a 'filter' input field and pagination controls at the bottom right.

	Name	Actions	Status	Service Template	Entity Rules	KPIs	Health	Team
<input type="checkbox"/>	Authorization	Edit	Enabled	Not linked	3	10	<a href="#">View Health</a>	Global
<input type="checkbox"/>	AWS	Edit	Enabled	Not linked	0	0	<a href="#">View Health</a>	Global
<input type="checkbox"/>	AWS EC2	Edit	Enabled	Not linked	1	9	<a href="#">View Health</a>	Global
<input type="checkbox"/>	AWS Lambda	Edit	Enabled	Not linked	1	5	<a href="#">View Health</a>	Global
<input type="checkbox"/>	Azure	Edit	Enabled	Not linked	0	0	<a href="#">View Health</a>	Global
<input type="checkbox"/>	Azure Functions	Edit	Enabled	Not linked	1	7	<a href="#">View Health</a>	Global
<input type="checkbox"/>	Azure VM	Edit	Enabled	Not linked	1	5	<a href="#">View Health</a>	Global
<input type="checkbox"/>	Buttercup Store	Edit	Enabled	Not linked	0	21	<a href="#">View Health</a>	Global
<input type="checkbox"/>	Cart Services	Edit	Enabled	Not linked	4	12	<a href="#">View Health</a>	Global
<input type="checkbox"/>	Catalog Services	Edit	Enabled	Not linked	3	10	<a href="#">View Health</a>	Global
<input type="checkbox"/>	Cloud	Edit	Enabled	Not linked	0	0	<a href="#">View Health</a>	Global
<input type="checkbox"/>	Cloud Database	Edit	Enabled	Not linked	1	6	<a href="#">View Health</a>	Global
<input type="checkbox"/>	GCP	Edit	Enabled	Not linked	0	0	<a href="#">View Health</a>	Global
<input type="checkbox"/>	GCP Cloud Functions	Edit	Enabled	Not linked	1	7	<a href="#">View Health</a>	Global
<input type="checkbox"/>	GCP Compute Engine	Edit	Enabled	Not linked	1	3	<a href="#">View Health</a>	Global
<input type="checkbox"/>	Mobile App	Edit	Enabled	Not linked	0	3	<a href="#">View Health</a>	Global
<input type="checkbox"/>	On-Prem Database	<b>Edit</b>	Enabled	Synced with On-Prem Database	1	8	<a href="#">View Health</a>	Global
<input type="checkbox"/>	On-Prem Database_OLD	Edit	Enabled	Synced with On-Prem Database	1	8	<a href="#">View Health</a>	Global

# Predictive Analytics Lab

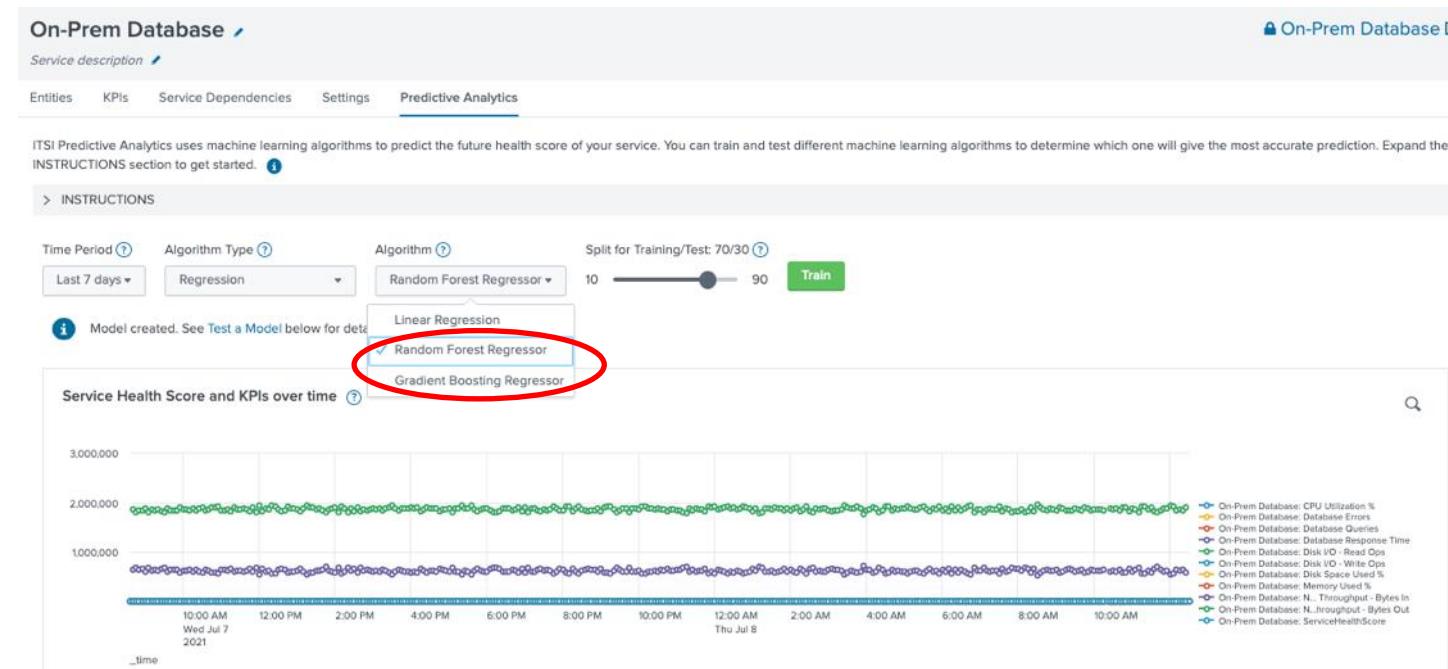
ITSI Predictive Analytics uses machine learning algorithms to predict the future health score of your service. On this screen we will train and test different machine learning algorithms to determine which one will give the most accurate prediction.

- 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**

ITSI Predictive Analytics uses machine learning to predict the health score value of a selected service. The models use historical KPI and service health score data to approximate what a service's health might look like in 30 minutes. [Learn more](#)

Service [?](#) Model [?](#)

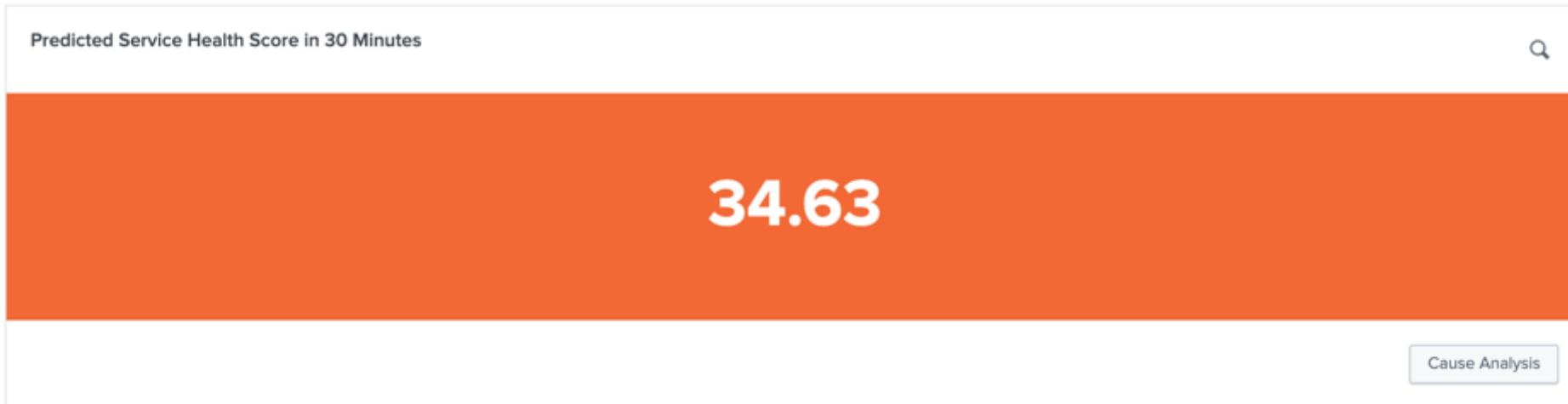
On-Prem Database ▾ LinearRegression ▾

Predicted Service Health Score in 30 Minutes

34.63

Cause Analysis

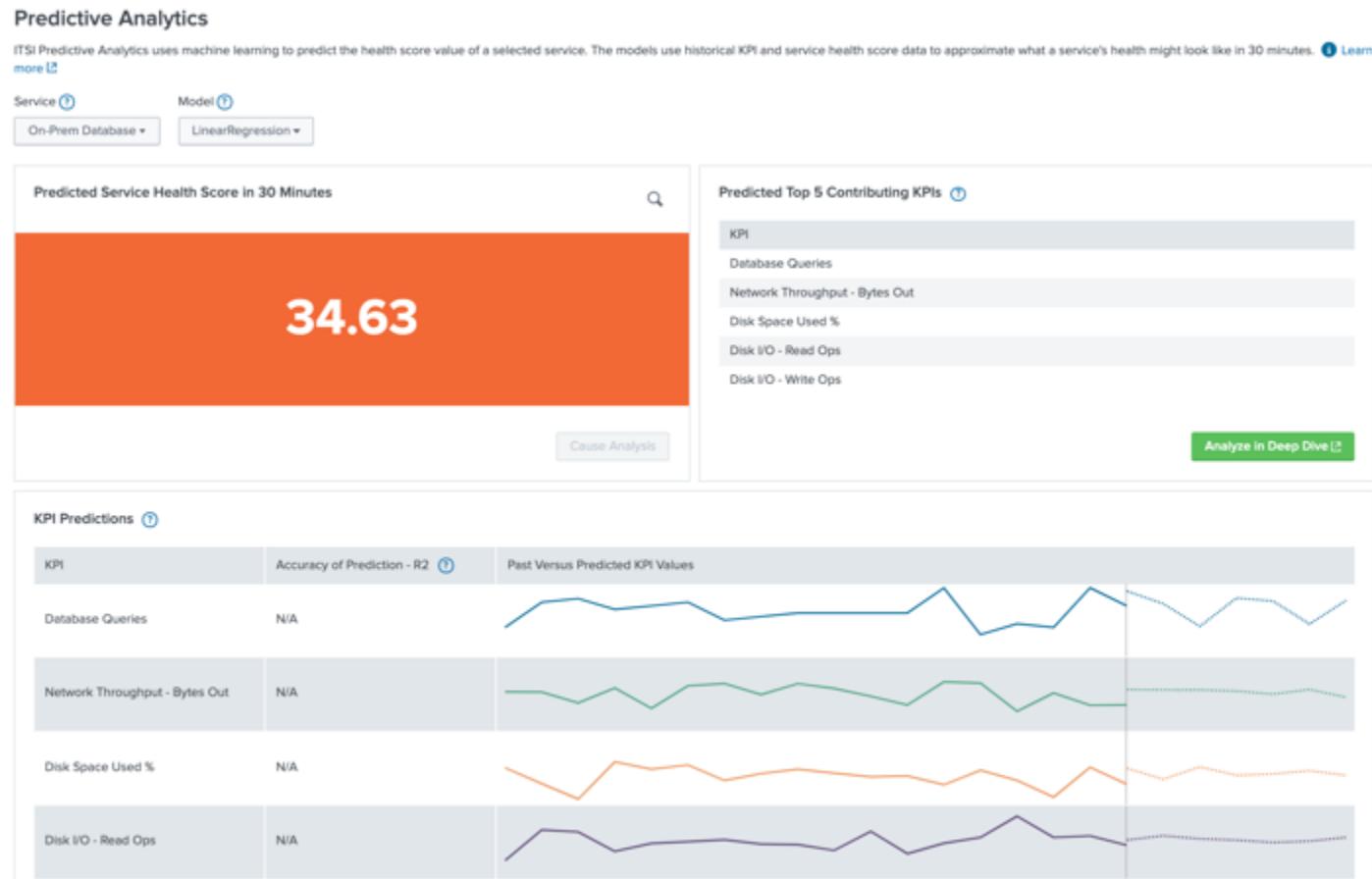
turn data into doing



# 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

ITSI Predictive Analytics uses machine learning to predict the health score value of a selected service. The models use historical KPI and service health score data to approximate what a service's health might look like in 30 minutes. [Learn more](#)

Service [?](#) Model [?](#)  
On-Prem Database ▾ LinearRegression ▾

Predicted Service Health Score in 30 Minutes 

Predicted Top 5 Contributing KPIs [?](#)

KPI 

Last 2 hours ▾ 

```
1 'itsi_predict_one_number(e36ff5e5-eb91-4eec-89f1-0baf9235b2b6,health_score,app  
:itsi_predict_e36ff5e5_eb91_4eec_89f1_0baf9235b2b6_LinearRegression_280102cacb6f6ac1f192b88f_1606924481883)'
```

⚠ Converting field(s) with categorical values into categorical fields: this\_date\_day, this\_date\_hour

✓ 1,177 events (02/12/2020 14:00:00.000 to 02/12/2020 16:07:00.000) No Event Sampling ▾  Job ▾  Smart Mode ▾

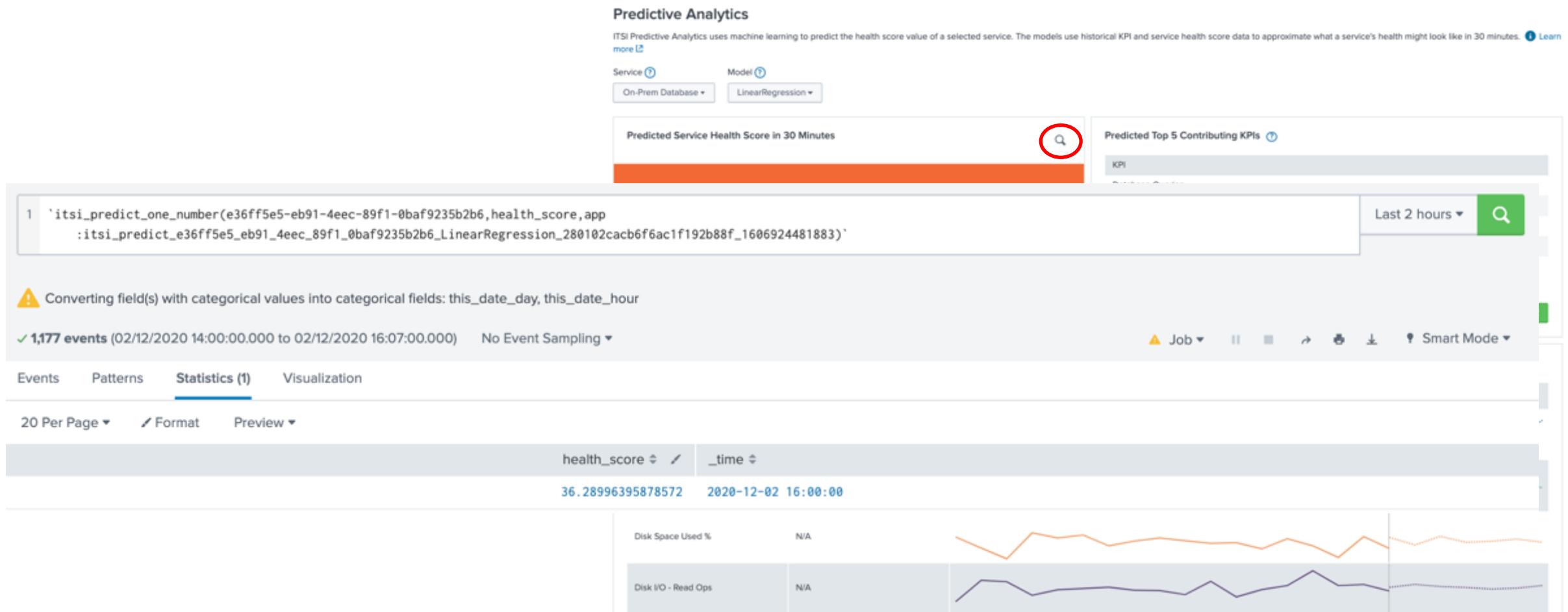
Events Patterns Statistics (1) Visualization

20 Per Page ▾ Format Preview ▾

health\_score ▾ \_time ▾  
36.28996395878572 2020-12-02 16:00:00

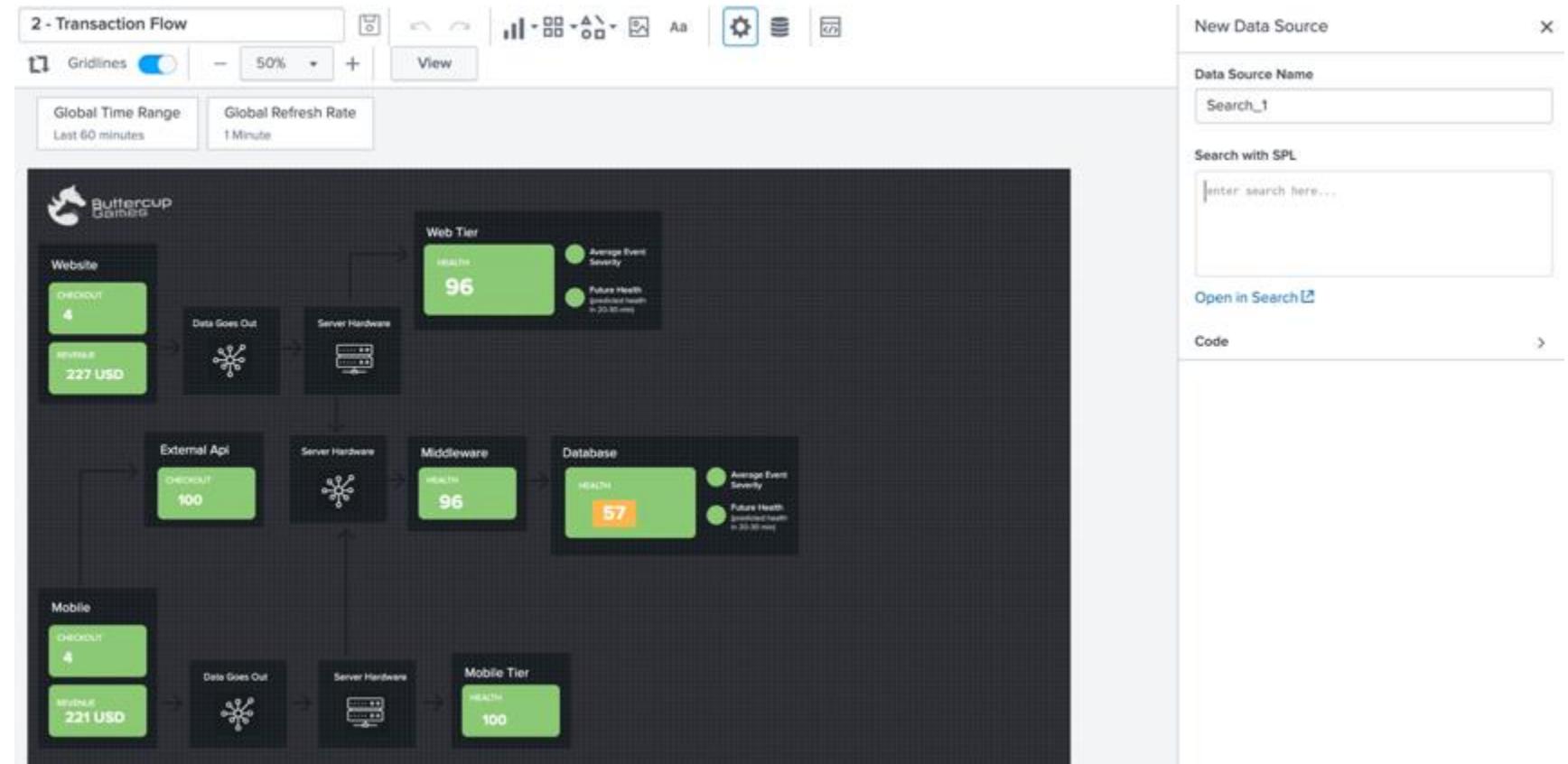
Disk Space Used % N/A 

Disk I/O - Read Ops N/A 



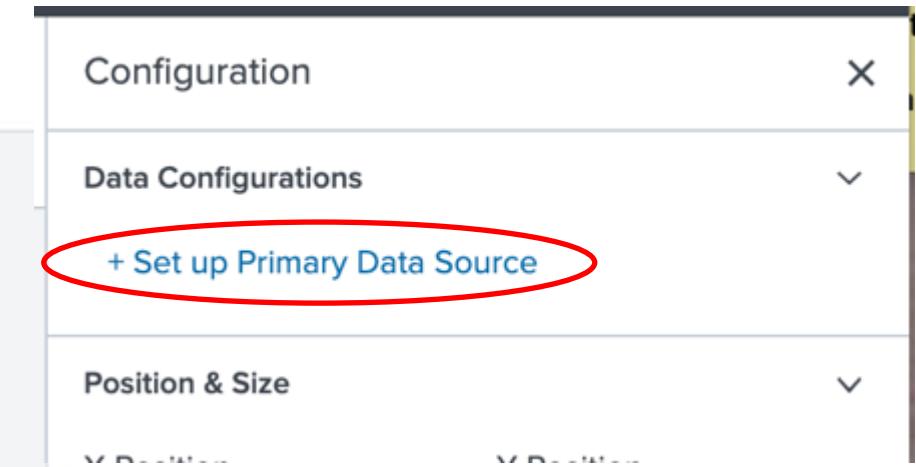
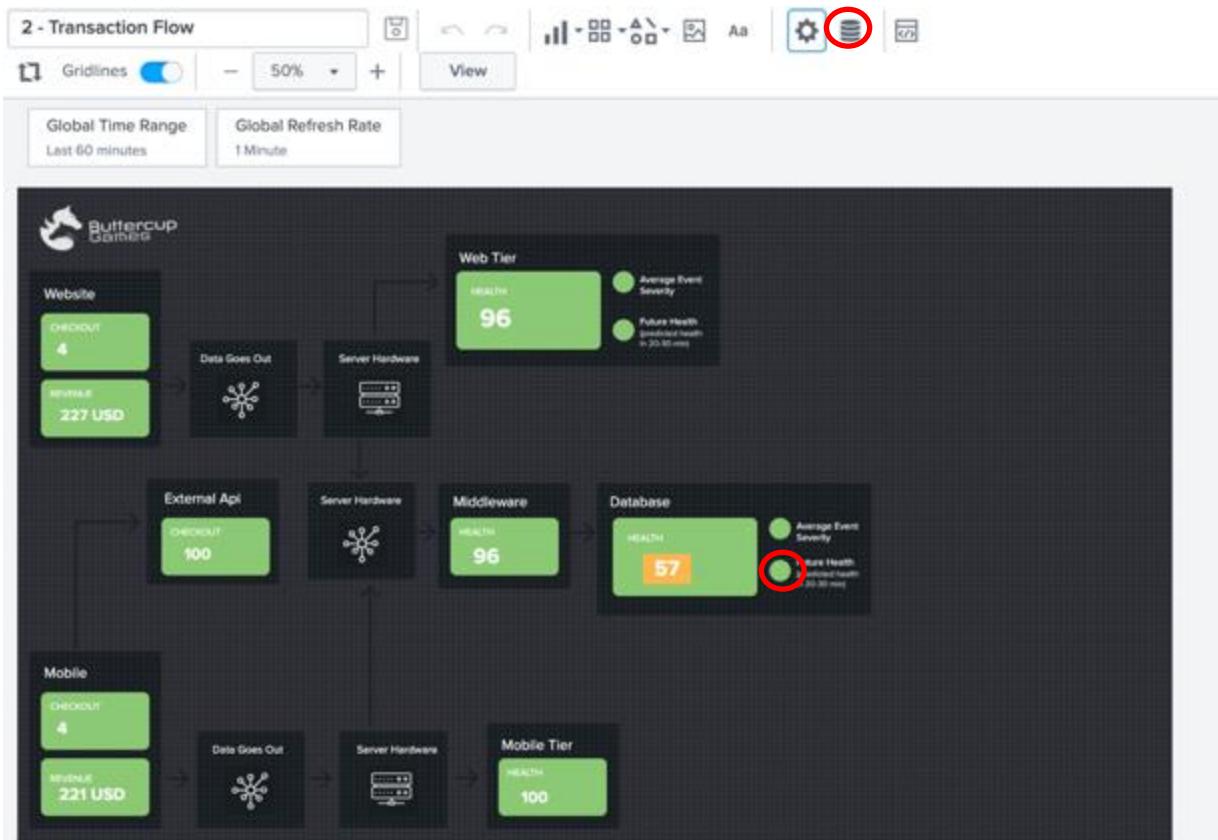
# Predictive Analytics Lab

- 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'



# Predictive Analytics Lab

- Select the 'Create Ad-Hoc Search'

The screenshot displays a Predictive Analytics Lab interface. On the left, a 'Transaction Flow' visualization for 'Buttercup Games' shows a flow from 'Website' to 'Web Tier', then to 'Database', and finally to 'Mobile'. Each stage includes metrics like 'CHECKOUT' counts and 'REVENU' amounts. The 'Web Tier' stage has a 'Health' score of 96. On the right, a 'Select Data' sidebar lists various services under 'Services' and 'Ad hoc Search'. The 'Create Ad hoc Search' option is highlighted with a red oval.

2 - Transaction Flow

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

View

Buttercup Games

Website: CHECKOUT 4, REVENU 227 USD

Data Goes Out, Server Hardware

Web Tier: HEALTH 96 (Average Event Severity: 1.0, Future Health: predicted health in 20.00 ms)

External API: CHECKOUT 100

Server Hardware, Middleware: HEALTH 96

Database: HEALTH 57 (Average Event Severity: 1.0, Future Health: predicted health in 20.00 ms)

Mobile: CHECKOUT 4, REVENU 221 USD

Data Goes Out, Server Hardware

Mobile Tier: HEALTH 100

Select Data

Services

- > Authorization
- > AWS
- > AWS EC2
- > AWS Lambda
- > Azure
- > Azure Functions
- > Azure VM
- > Buttercup Store
- > Cart Services
- > Catalog Services
- > Cloud
- > Cloud Database

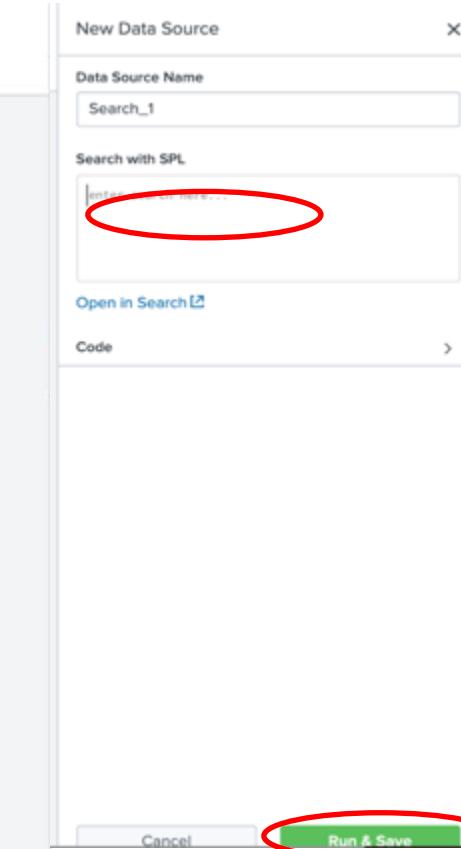
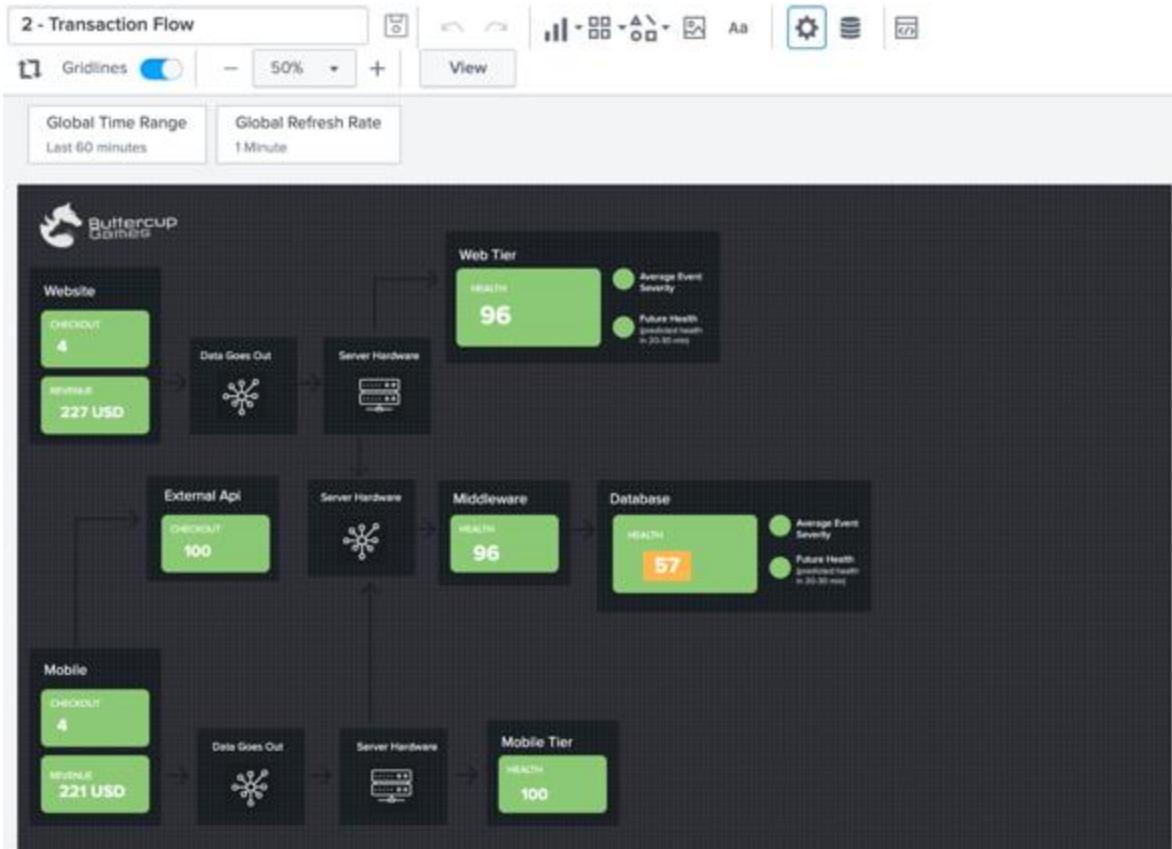
Ad hoc Search

- < Create Ad hoc Search

splunk > turn data into doing

# Predictive Analytics Lab

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



# 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

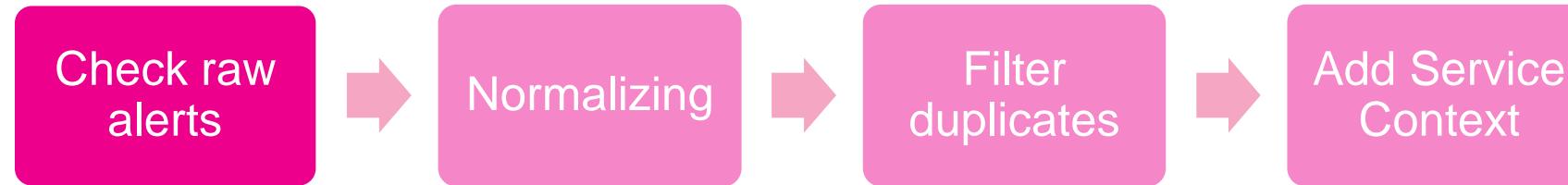
*Apply Service Context & Configure Event Grouping*

- Notable Event Aggregation Policies

*Review episodes*

#	Time	Event
>	09/04/2020 11:49:52.652510	src_host="mysql-02" md_site="SJC" perfdata="SERVICEPERFDATA" name="check_disk" severity="OK" attempt="1" statetype="SOFT" executiontime="0.0" latency="0.0" reason="Disk Space utilization 51.18 is below threshold" results="Disk Space status ok" host = mysql-02   source = nagios   sourcetype = nagios
>	09/04/2020 11:48:52.582663	src_host="mysql-02" md_site="SJC" perfdata="SERVICEPERFDATA" name="check_disk" severity="WARNING" attempt="3" statetype="HARD" executiontime="0.0" latency="0.0" reason="Disk Space utilization 96.3 is above threshold" results="Disk Space status warn" host = mysql-02   source = nagios   sourcetype = nagios
>	09/04/2020 11:47:52.927797	src_host="mysql-02" md_site="SJC" perfdata="SERVICEPERFDATA" name="check_disk" severity="WARNING" attempt="1" statetype="SOFT" executiontime="0.0" latency="0.0" reason="Disk Space utilization 93.09 is above threshold" results="Disk Space status warn" host = mysql-02   source = nagios   sourcetype = nagios

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



**index=itsidemo sourcetype=nagiosserviceperf perftdata=SERVICEPERFDATA**

Service Analyzer Infrastructure Overview Episode Review Glass Tables Deep Dives Dashboards Configuration Search

IT Serv

Adding Nagios Events into ITSI

Step 1 - Raw Nagios Alerts

The first step to helping the database team achieve their goal is to ingest the raw Nagios in. Prior to the workshop, we took the time to onboard the Nagios alerts from the database.

SPL

index=itsidemo sourcetype=nagiosserviceperf perftdata=SERVICEPERFDATA

i	Time	Event
>	02/12/2020 16:00:30	src_host=mysql-01 perftdata=SERVICEPERFDATA name=check_cpu severity=OK attempt=1 statetype=SOFT executiontime=0.0 latency=0.0 reason="CPU utilization 43.1% is below threshold" results="CPU status ok" host = mysql-01   source = nagios   sourcetype = nagiosserviceperf
>	02/12/2020 16:00:30	src_host=mysql-02 perftdata=SERVICEPERFDATA name=check_disk severity=OK attempt=1 statetype=SOFT executiontime=0.0 latency=0.0 reason="Disk utilization 49.6% is below threshold" results="Disk status ok" host = mysql-02   source = nagios   sourcetype = nagiosserviceperf
>	02/12/2020 16:00:30	src_host=mysql-02 perftdata=SERVICEPERFDATA name=check_cpu severity=OK attempt=1 statetype=SOFT executiontime=0.0 latency=0.0 reason="CPU utilization 67.2% is below threshold" results="CPU status ok" host = mysql-02   source = nagios   sourcetype = nagiosserviceperf

Predictive Analytics

Event Analytics Monitoring

Event Analytics Audit

ITSI Health Check

✓ Adding Nagios Events into ITSI

Datasets

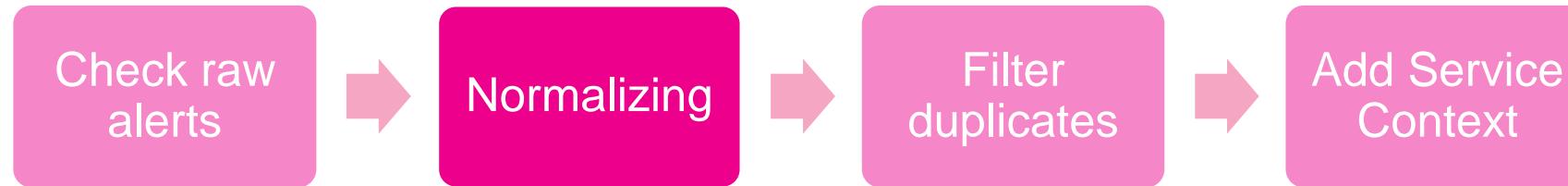
Reports

supporting add-ons in Splunkbase for many monitoring tools which you can use to handle the raw Nagios alerts in the table below and review the raw event as well as the exten

< Prev 1 2 3 4 5 6 7 8 9

After you have finished reviewing the raw Nagios events **Click here** to proceed to Step 2 - Add Normalized

# EA Lab Step 2 : Add Normalized Fields



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

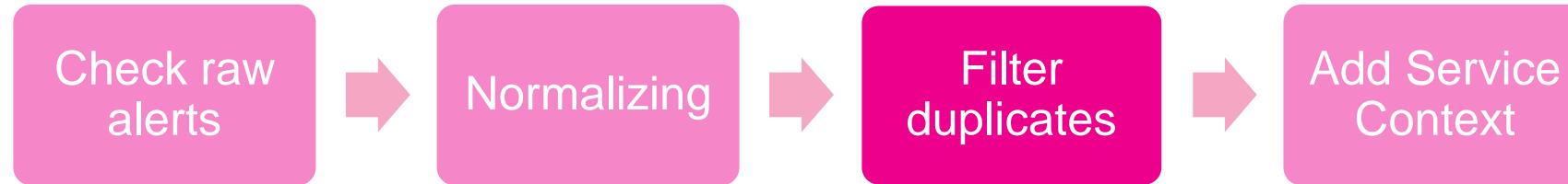
_time	name	severity	norm_severity	norm_instance	norm_test	total
2020-04-15 10:02:27.773	check_disk	OK	2	mysql-02	check_disk	1
2020-04-15 10:01:27.710	check_disk	WARNING	4	mysql-02	check_disk	1
2020-04-15 09:56:27.396	check_disk	OK	2	mysql-02	check_disk	1
2020-04-15 09:55:27.334	check_disk	WARNING	4	mysql-02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



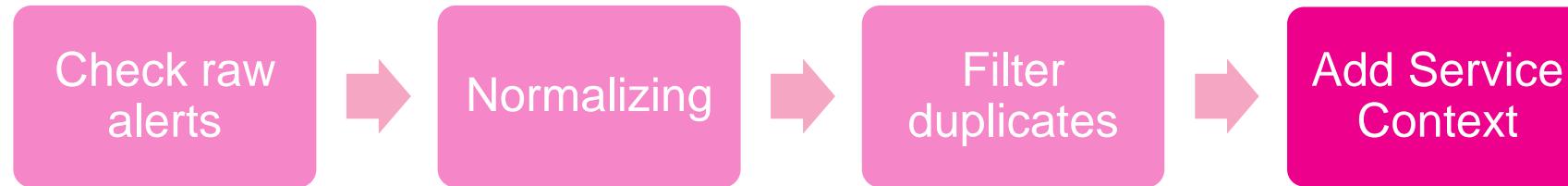
Goal: Removing duplicated events

```
| 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

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



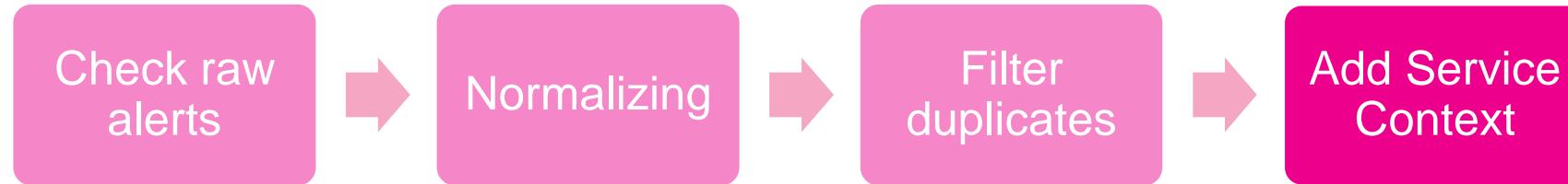
Goal: Add Service Context makes correlation possible for different alerts in a service

```
|`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

# Event Analytics Lab



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

New Search

```
index=itsid:s sourcetype=nagios perftype=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
```

Last 24 hours

34 events (14/04/2020 15:00:00.000 to 15/04/2020 15:27:32.000) No Event Sampling

Save As ▾ Close

Job ▾ II ■ ↻ ⏪ ⏩ ⏴ ⏵ ⏵ Fast Mode ▾

Events Patterns Statistics (34) Visualization

20 Per Page ▾ Format Preview ▾

_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

< Prev 1 2 Next >

# 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*

## Search Properties

Search Name \*

Nagios Correlation Search

Description ?

optional

Search Type

Data Model

Ad hoc

Search \*

```
index=itsidemo sourcetype=nagios perftype=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
```

Run Search ↗

Time range

Last 5 minutes ▾

## Association

Service

Select service(s)

Entity Lookup Field ?

host

## Schedule

# Event Analytics Lab

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

The screenshot shows the Splunk Configuration interface with the following details:

- Top Navigation:** Service Analyzer, Episode Review, Glass Tables, Deep Dives, Multi-KPI Alerts, Dashboards, Search, Configure (highlighted with a red oval), Product Tour.
- Right Sidebar:** IT Service Intelligence icon, Explore Content, Create New Search (highlighted with a red oval).
- Current Page:** Correlation Searches. A message states: "A correlation search is a recurring search that generates a notable event when search results meet specific conditions." Below is a table with columns: Bulk Action, Title, Actions.
- Table Data:**

Bulk Action	Title	Actions
<input type="checkbox"/>	Active Directory	Edit
<input type="checkbox"/>	Bidirectional Ticketing	Edit
<input type="checkbox"/>	Episode Monitoring - All Services and KPIs Return to Normal	Edit
<input type="checkbox"/>	Episode Monitoring - Concentration of High and Critical Notable Events	Edit
<input type="checkbox"/>	Episode Monitoring - Critical Notable Event added to Episode (Rec...	Edit
<input type="checkbox"/>	Episode Monitoring - Episode Risk Well Above Historical Average	Edit
- Left Sidebar (highlighted with a red oval):**
  - Services
  - Entities
  - Service Templates
  - Correlation Searches** (highlighted with a red oval)
  - KPI Base Searches
  - KPI Threshold Templates
  - Backup/Restore
  - Maintenance Windows
  - Notable Event Aggregation Policies
  - Hybrid Action Dispatching
  - Teams
- Pagination:** < Prev, 1, 2, Next >

# Event Analytics Lab: correlation search

- Name your search
- Paste the SPL in search:

```
index=itsidemo sourcetype=nagios perftype=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

**Search Properties**

Search Name *	Nagios Correlation Search
Description ?	optional
Search Type	Data Model

**Search \***

```
index=itsidemo sourcetype=nagios perftype=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
```

**Run Search**

Time range

Last 5 minutes

**Association**

Service

Select service(s)

Entity Lookup Field ?

host

**Schedule**

# 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*

Notable Events

Notable Event Title ?

Notable Event Description ?

Owner ?  Advanced Mode  
In advanced mode, use tokens like %fieldname% to use result field values to set owner.

Severity ?  Simple Mode  
In advanced mode, use tokens like %fieldname% to use result field values to set severity.

Status ?  Advanced Mode  
In advanced mode, use tokens like %fieldname% to use result field values to set status.

Drilldown Search Name ?

Drilldown Search ?

Drilldown earliest offset ?

Drilldown latest offset ?

Notable Event Identifier Fields ?   
Set of fields used together to determine if a notable event is unique or not.

Drilldown Website Name ?

Drilldown Website URL ?

> Advanced Options

# 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*

## Service Issues

Notable Event Aggregation Policy description

Filtering Criteria Action Rules

### Filtering Criteria

Create filtering criteria to group notable events into episodes.

▼ Include the events if<sup>?</sup>

severity greater than Normal

service\_nan matches \*

+ Add Rule (AND)

+ Add Rule (OR)

➤ Smart Mode grouping

▼ Split events by field<sup>?</sup>

Split events into multiple episodes by

service\_name

▼ Break episode<sup>?</sup>

➤ If this episode existed for 36000 second(s)

➤ If the flow of events into the episode paused for 3600 second(s)

+ Add Breaking Condition (OR)

➤ Episode information

# Event Analytics Lab: Notable Event Aggregation Policies

- Navigate to Configure -> Notable Event Aggregation Policies
- Edit "Service Issues" policy

The screenshot shows the Splunk Enterprise interface with the title bar "splunk>enterprise App: IT Service Intelligence". Below the title bar, there are several navigation links: Service Analyzer, Episode Review, Glass Tables, Deep Dives, Multi-KPI Alerts, Dashboards, Search, Configure, and Product Tour. On the far right, there is a user profile icon for "Administrator" and a blue circular badge with the number "50".

The main content area is titled "Notable Event Aggregation Policies" with the sub-instruction "Use notable event aggregation policies to group similar notable events in the Episode Review." Below this, there is a table with 11 rows, each representing a policy. The columns are "Title", "Actions", and "Status".

Title	Actions	Status
Application Alerts	Edit	Enabled
Default Policy	Edit	Enabled
Default SNMP Policy	Edit	Disabled
Episodes by Alert Group	Edit	Disabled
Episodes by ITSI Service	Edit	Disabled
Infrastructure Alerts	Edit	Enabled
KPI Alerting Policy	Edit	Enabled
Multi-Episode Problem	Edit	Disabled
Normalized Policy (Splunk App for Infrastructure)	Edit	Enabled
Service Issues	Edit	Enabled
User Account Management	Edit	Enabled

A modal window is open over the table, centered on the "Service Issues" row. The modal has a light gray background and contains the following options:

- Edit (highlighted with a red circle)
- Edit Title or Description
- Edit Permissions
- Clone
- Delete

# 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.

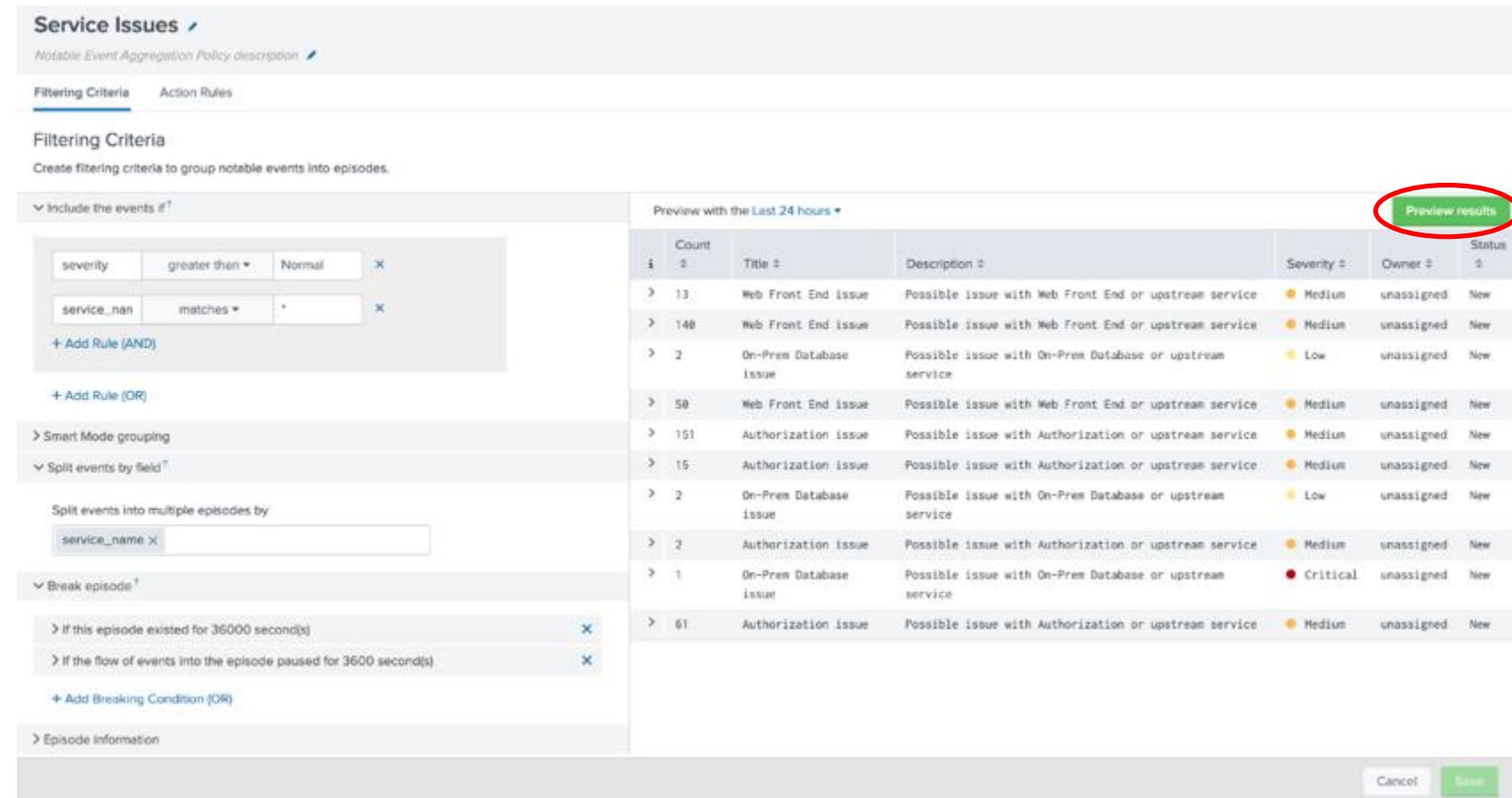
It looks like a policy might already exist which groups notable events together by the affected ITSI Service. That policy is called “Service Issues

The screenshot shows the 'Service Issues' configuration page. It includes sections for 'Filtering Criteria and Instructions' and 'Action Rules'. Under 'Filtering Criteria and Instructions', there are two AND rules: 'severity greater than Normal' and 'service\_nam matches \*'. There is also a Smart Mode grouping section with a toggle switch set to 'Smart Mode'. Under 'Break episode?', there are two conditions: 'If this episode existed for 3600 second(s)' and 'If the flow of events into the episode paused for 1800 second(s)'. The 'Episode information' section is also visible.

# 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



The screenshot shows the 'Service Issues' configuration page for a 'Notable Event Aggregation Policy description'. On the left, there's a 'Filtering Criteria' section with rules for 'severity' (greater than Normal) and 'service\_name' (matches \*). Below it are sections for 'Smart Mode grouping' and 'Break episode' conditions. On the right, a table titled 'Preview with the Last 24 hours' lists various service issues with their counts, titles, descriptions, severity, owner, and status. A green button labeled 'Preview results' is located at the top right of the table area, which is circled in red.

Count	Title #	Description #	Severity #	Owner #	Status
> 13	Web Front End issue	Possible issue with Web Front End or upstream service	Medium	unassigned	New
> 148	Web Front End issue	Possible issue with Web Front End or upstream service	Medium	unassigned	New
> 2	On-Prem Database issue	Possible issue with On-Prem Database or upstream service	Low	unassigned	New
> 58	Web Front End issue	Possible issue with Web Front End or upstream service	Medium	unassigned	New
> 151	Authorization issue	Possible issue with Authorization or upstream service	Medium	unassigned	New
> 15	Authorization issue	Possible issue with Authorization or upstream service	Medium	unassigned	New
> 2	On-Prem Database issue	Possible issue with On-Prem Database or upstream service	Low	unassigned	New
> 2	Authorization issue	Possible issue with Authorization or upstream service	Medium	unassigned	New
> 1	On-Prem Database issue	Possible issue with On-Prem Database or upstream service	Critical	unassigned	New
> 61	Authorization issue	Possible issue with Authorization or upstream service	Medium	unassigned	New

- 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

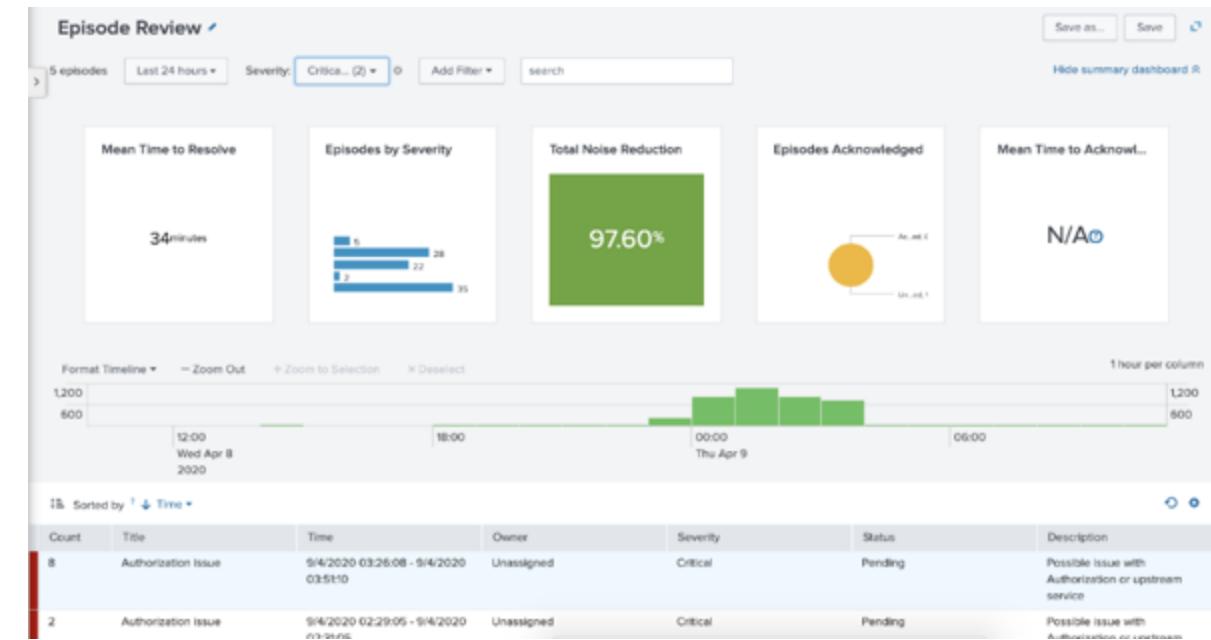
Clean and prepare “raw” alert events

- SPL

*Create Notable Events from alerts*  
• Correlation Search

*Apply Service Context & Configure Event Grouping*  
• Notable Event Aggregation Policies

*Review episodes*

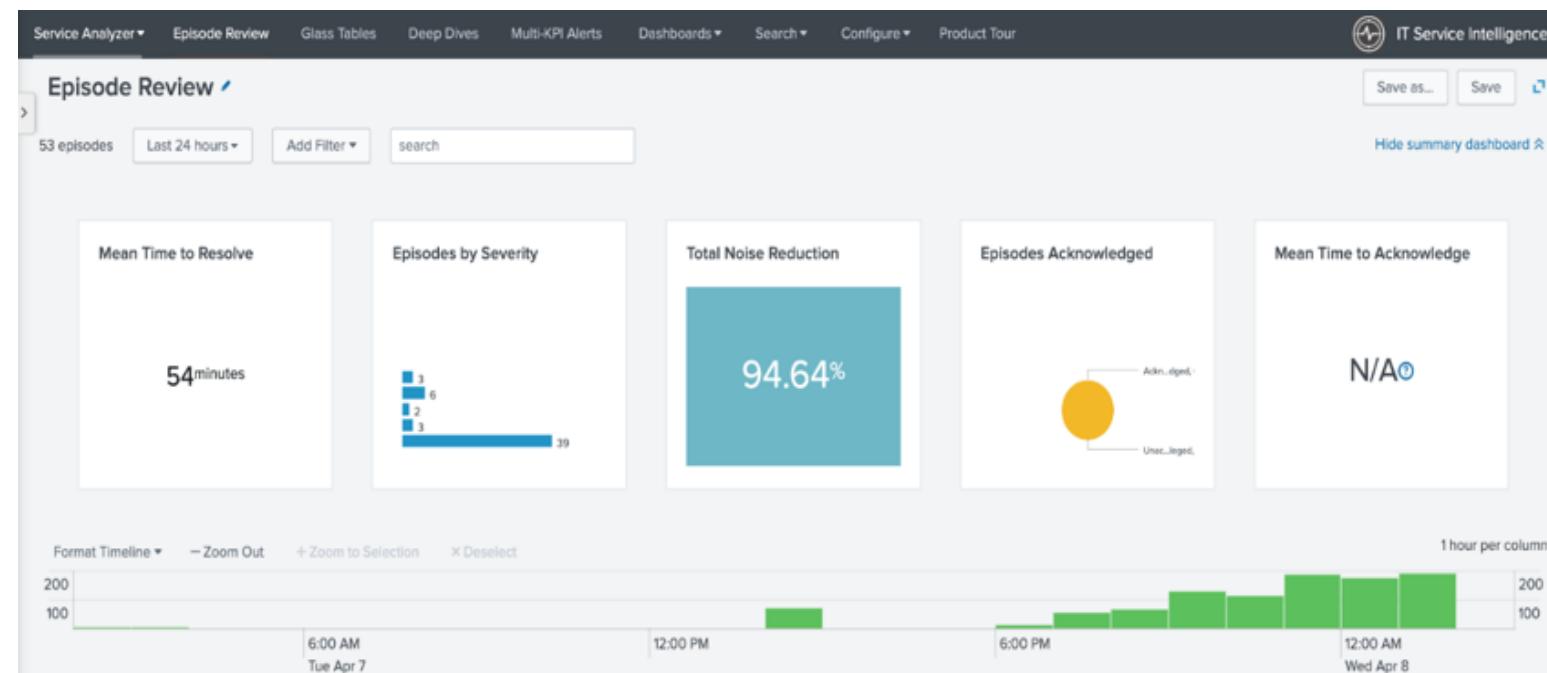


# Event Analytics Lab: Episode View

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

**Episode Review**

49 episodes Last 24 hours Severity: Critical... (2) Add Filter search Show Dashboard

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	02/12/2021 02:42:46 PM - 02/12/2021 03:27:46 PM	Unassigned	High	Pending	Issues detected for service Cart Services.
100+	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	02/12/2021 02:22:48 PM - 02/12/2021 03:07:50 PM	Unassigned	High	Pending	Issues detected for service Authorization.
32	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+	02/12/2021 11:11:45 AM - 02/12/2021 11:59:45 AM	Unassigned	High	Pending	Issues detected for service On-Prem Database.

**Filter**

Select All Clear All

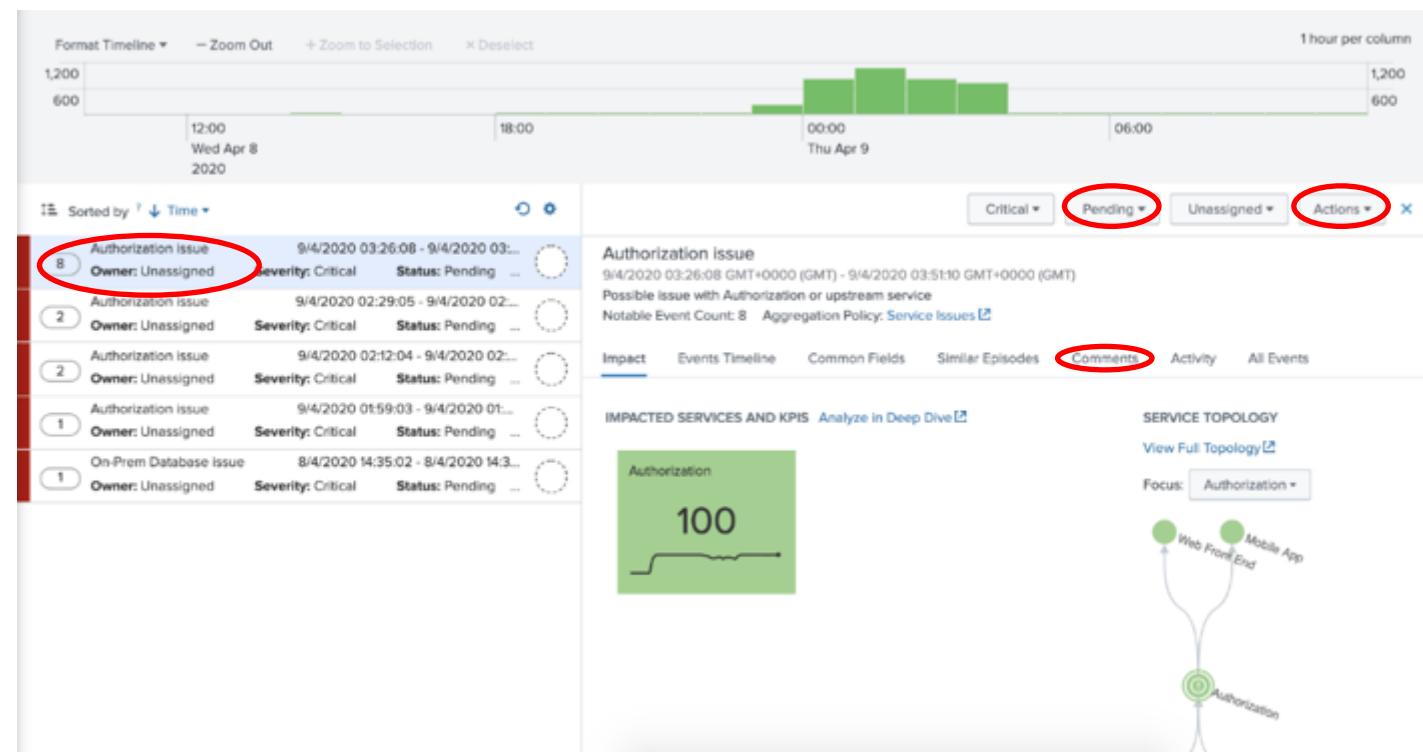
Critical  
 High  
 Info  
 Low  
 Medium  
 Normal  
6 of 6 values

Cart Services Issues

# 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





# Thank You

---

