Splunk ITSI Training

Prachi Saxena

Week 3 – Day1 (3 hours)

Thresholds and Time Policies (Module 9)

- Create KPIs with static and adaptive thresholds
- Use time policies to define flexible thresholds

Anomaly Detection

- Enable anomaly detection
- Work with generated anomaly events

Thresholds and Time Policies (Module 9)

- Create KPIs with static and adaptive thresholds
- Use time policies to define flexible thresholds

Objectives

- Configure KPI thresholds
- Use aggregate and entity level threshold
- Use static and adaptive thresholds
- Apply time policies to thresholds
- Create custom threshold templates

Configuring KPI Thresholds

- Two methods of configuring thresholds
  - Manual: build manual list of level normal, low, high with their values
  - Automatic: thresholds based on daily statistics
- Each KPI has an aggregate threshold map, which indicates the overall alert level for that KPI
  - Separate map in case you have per entity thresholds
- Threshold maps can be statics or adaptive

- Use cases in which different workloads for a KPI occur at regular and expected intervals

KPI Alert Values and threshold maps

- Every Kpi search, creates event in itsi_summary index
- The numeric value is stored in “alert_value”
  - It can be static or unbounded
  - Static = 0 – 100 (memory utilization)
  - Upper bound = purchase events
- Thresholds map “alert_value” to “alert_level”
  - Alert_level is between 2(normal) and 6(critical)
  - **Base severity** is the alert level defined when value is below any defined threshold. i.e: the lowest severity
  - Example:
    - Mem util: < 30 %: normal
      - 31 – 50%: low
      - 51 – 80%:high
      - > 81%: Critical

Threshold: adding them and design

- You can add as many thresholds as needed
- Need to define cut off range for each range
- Anything below first cutoff is base severity
- Anything above top cut off is top severity

- There are no rules for threshold design
  - You can use as many values as needed
  - They can be in any order that makes sense to your use case
- Info Threshold: this is a KPI that does no need threshold
  - It does not play a role in service health
  - In this case, set base severity to “info”

Aggregate Vs Entity

- Entity thresholds are available then your KPI is split by entity
- The aggregate threshold apply to combined values of the entity values
- Per entity thresholds can be copied from aggregate thresholds
- Example: Total number of connections, sum of overall connections may be normal at 1000, but normal for each entity may be different such as 250 per entity.
    - There could be same in case of KPIs such as CPU utilization
- Demo

Time Policies

- It is useful when simple threshold don’t apply and normal for a weekday may differ from weekend
- Each policy is a period of time and set of thresholds
- One default policy applies to all time periods not covered by defined policies
- Demo
  - Add a time policy
  - Configure time policy thresholds
  - Edit Time policy thresholds
  - Time policy preview
- Threshold Templates
  - Adaptive
  - Static
  - Custom

Adaptive Thresholding

- Based on statistical analysis
- Useful if you do not know the expected range of data, it is very dynamic and fluctuate in unpredictable manner
- Need at least 7 days of data to take advantage of it
- Need time policy to be enabled
- Four types:
  - Static
  - Standard Deviation
  - Quantile
  - Range
- Stored in KVStore

Anomaly Detection (module 12)

- Enable anomaly detection
- Work with generated anomaly events
- Predictive Analytics

Anomaly Detection

- Generates alerts based on historic patterns
- Enabled on KPI level
- Uses machine learning to analyse patterns of KPI
- Algorithms used are trending and entity cohesion
- Results in an notable event
  - Anomaly: need min 24 hours of data
  - Cohesion: needs atleast 4 entities
- Not useful is the patterns are difficult to detect, so use when you have established patterns over time and baselines of data
- Results are stored in index=anomaly_detection

Algorithms

Trending

- Applies on aggregate event results over a defined time period
- It compares recent data to historical events
- Anomalously high scores generate an alert as notable event
- Service level alert

Cohesion

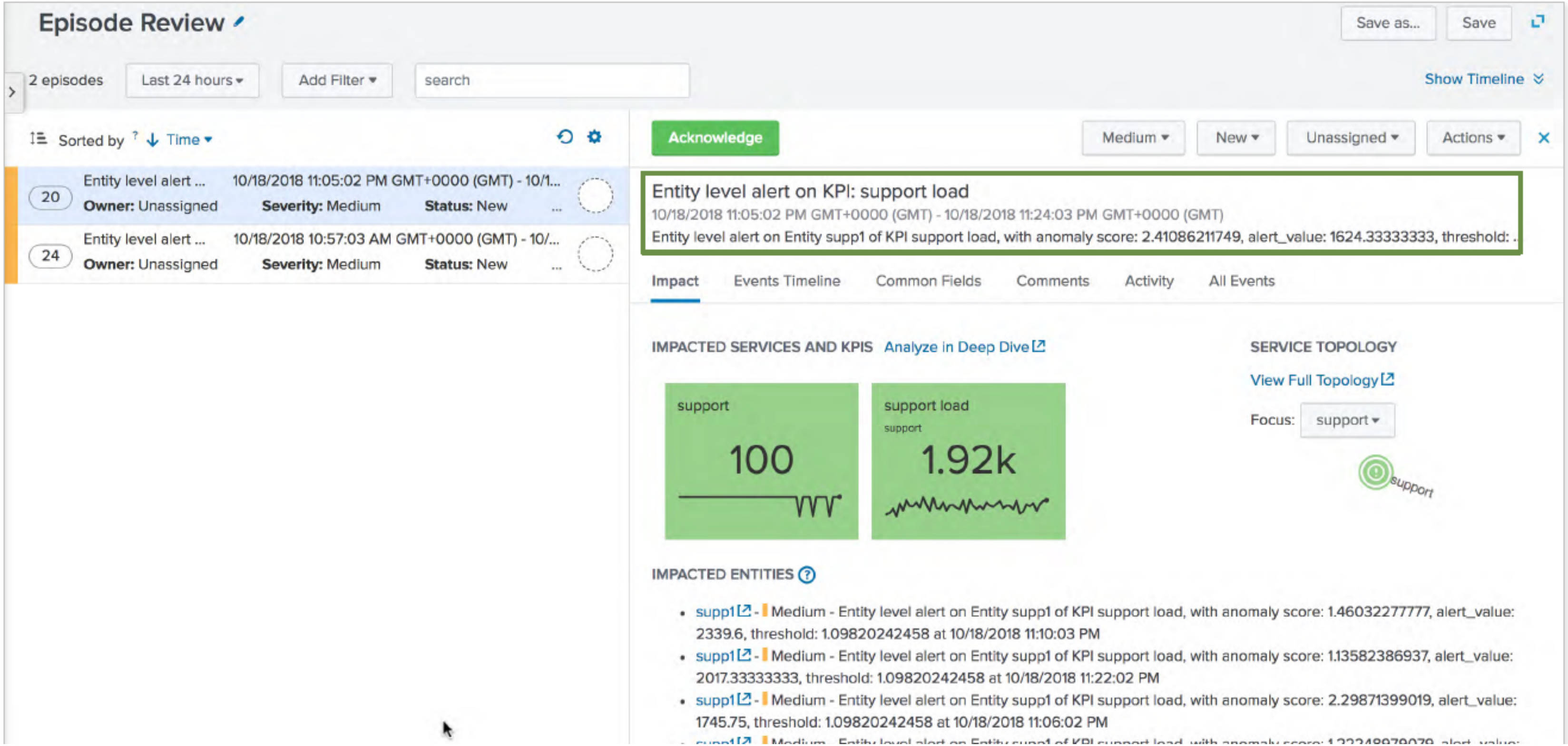
- Examines multiple timeseries (per entity) simultaneously
- KPI must be split by entity
- Min 4 entities to be available
- Alert is generated based on deviation from the typical pattern
- Entity level alert

Use Cases

- It is useful if KPI doesn’t necessarily spike, but instead begins to behave abnormally
- For instance:
  - Online sales volume typically follows a sine wave per day with peak load in the early evening and low load in early morning
  - If instead it “flatlines” at around medium load, this would not set off a status-based alert since it is not spiking, but AD will notice and create a notable event
- Setup: demo

Anomaly Alerts

- After configuring, it takes upto 24 hours for AD to generate alerts
- Anomaly alerts appear as notable event episode
- They can be acknowledged and worked on like other notable event episode



2 episodes

20	Entity level alert ...	10/18/2018 11:05:02 PM GMT+0000 (GMT) - 10/1...		
	Owner: Unassigned	Severity: Medium	Status: New	...
24	Entity level alert ...	10/18/2018 10:57:03 AM GMT+0000 (GMT) - 10/...		
	Owner: Unassigned	Severity: Medium	Status: New	...

Entity level alert on KPI: support load

10/18/2018 11:05:02 PM GMT+0000 (GMT) - 10/18/2018 11:24:03 PM GMT+0000 (GMT)

Entity level alert on Entity supp1 of KPI support load, with anomaly score: 2.41086211749, alert_value: 1624.33333333, threshold: .

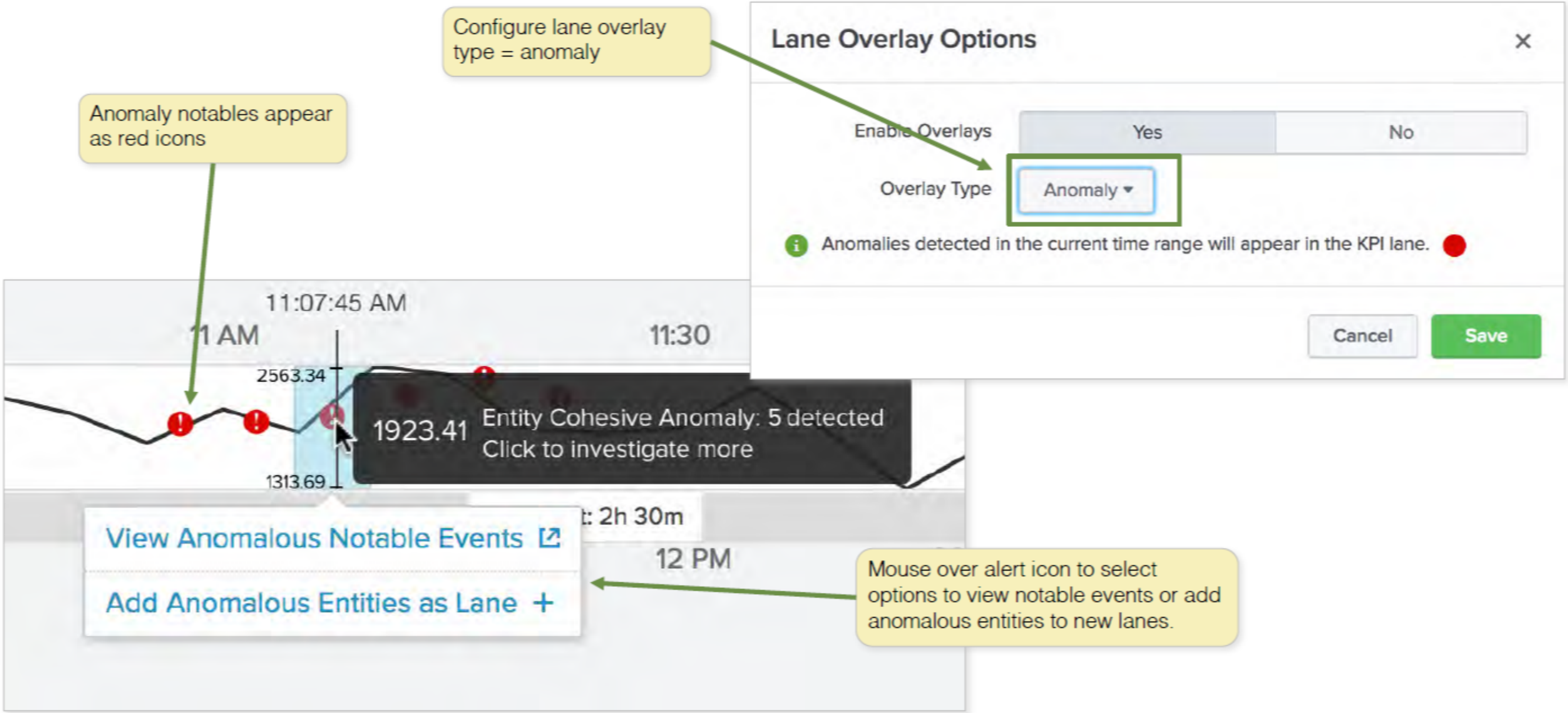
IMPACTED SERVICES AND KPIS

SERVICE TOPOLOGY

Focus: support

IMPACTED ENTITIES

- supp1 - Medium - Entity level alert on Entity supp1 of KPI support load, with anomaly score: 1.46032277777, alert_value: 2339.6, threshold: 1.09820242458 at 10/18/2018 11:10:03 PM
- supp1 - Medium - Entity level alert on Entity supp1 of KPI support load, with anomaly score: 1.13582386937, alert_value: 2017.33333333, threshold: 1.09820242458 at 10/18/2018 11:22:02 PM
- supp1 - Medium - Entity level alert on Entity supp1 of KPI support load, with anomaly score: 2.29871399019, alert_value: 1745.75, threshold: 1.09820242458 at 10/18/2018 11:06:02 PM
- supp1 - Medium - Entity level alert on Entity supp1 of KPI support load, with anomaly score: 1.22248979079, alert_value:


11:07:45 AM
11 AM
11:30
2563.34
1313.69
t: 2h 30m
12 PM
View Anomalous Notable Events
Add Anomalous Entities as Lane +
×
Cancel
Save

Lane Overlay Options

Enable Overlays: ● Yes ○ No

Overlay Type: Anomaly ▾

Anomalies detected in the current time range will appear in the KPI lane. ●

1923.41 Entity Cohesive Anomaly: 5 detected
Click to investigate more

Configure lane overlay type = anomaly

Anomaly notables appear as red icons

Mouse over alert icon to select options to view notable events or add anomalous entities to new lanes.

Memory

- Ad reserves 1 GB of memory
  - Max 600 KPIs for trending analysis
  - 1000 metrics for cohesion analysis (KPI * entities)
- Update the limits from $SPLUNK_home/etc/apps/SA-ITSI-MetricAD/local/commands.conf
  - [MAD] stanza, command.arg.1 = J-Xmx1G
  - Restart splunk

Predictive Analytics

- Provide analysts with tools to anticipate and avoid future service degradation
- Root cause analysis highlights KPIs that contribute to poor SHS
- You need two splunk apps to be installed:
    - Python for Scientific Computing
    - Splunk Machine Learning Toolkit
- Defined on service level with defined time period.
    - Longer time period is better
- Demo:
    - Initial Analysis
    - Select Algorithm
    - Train the model
    - Test the model
    - Configure alert

Model Maintenance

- They are static and need retraining
- Service with have many KPI/ entities generate resource intensive models (20+ kpi or 50+ entities)
- Available and lookup files:
  - Name is _avg,_ss,_worst

Comparison

- Anomaly Detection
  - Configured per-KPI
  - Detect patterns deviation when it happens
  - Can analyse per entity behaviour
  - Create alerts after an anomaly is detected

- Predictive analysis
  - Configured per service
  - Predicts future service health degradation
  - No entity analysis
  - Create alerts indicating service health may deteriorate in the future