Splunk ITSI Training

Prachi Saxena

Week 4 – Day2

Investigating Issues with Deep Dive

- Describe deep dive concepts and their relationships
- Use default deep dives
- Create and customize new custom deep dives
- Add and configure swim lanes
- Custom views
- Describe effective workflows for troubleshooting

What is Deep Dive

- Lane based visualizations used for comparing the various KPIs based on time
- The results are always based on timechart
- The use case is to derive the insights into issues, represented by KPI or service behaviour, based on viewing them in a time-based lane manner
- Use case: during an outage, you can use them to examine and compare alerts levels for KPIs in a service over time

Uses

- You can add, remove or sort lanes as needed
- It can be accesses by service analyzer or glass table
- Admin can modify the views and they would be globally changed
- You can also save deep dives with a name and use as action from glass table
- Default deep dive:
  - Configure as you like and no need to save
  - Changes to deep dives are persistent globally for all users

Concepts

- Lane Types
  - Metric
  - KPI
  - Event
- Bulk Actions:
  - Multi Kpi alert
  - Show state, level or threshold
  - Show/hide entity/ anomaly
  - Delete lanes
- Lane Overlays

Troubleshooting workflows

- Service Analyzer→Service →KPI → Entities
- Service Analyzer → Service → KPI → Deep Dive --> bulk actions or
  - Entity Overlay → View entity or module
- Episode Review → Episode → Deep Dive
- Glass Table → Deep Dive →
  - Enable overlays
  - Identify hosts
  - Drilldown to raw data
- Glass table drilldown to predictive analytics