Splunk ITSI Training

Prachi Saxena

Week 4 – Day1 (3 hours)

Aggregation Policies

- Create new aggregation policies
- Use smart mode

Glass Tables

- Describe glass tables
- Use glass tables
- Design glass tables
- Configure glass table

Aggregation Policies

- Create new aggregation policies
- Use smart mode
- Use aggregation policies to automate notable event response

Aggregation policies

- AP allows to identify groups of notable events that should be processed collectively as episodes
- Default Policy: based on source, any event not covered by any other policy is process by it
- More Example:
  - Based on entity, service, location, age,etc
  - SNMP Policy: for SNMP trapping
  - KPI alerting policy: group events by KPI
  - Normalized policy: group SAI alerts into episode
- Displayed in episode review and automated actions are used on them

Polices

- If you have more than 1 policies, they would always be applied before default policy
- An event can be processed by more than 1 policy
- There is no order in policy processing and actions can also be applied in any order… so try not be create competing action rules
- An event which match with more than 1 policy would appear on more than 1 group in “episode review dashboard”

Grouping

- Each episode can have an owner and status
- Number of events are dynamic
- On resolution, events stop being generated and episode status to be closed
- After closure, any new episodes will create a new group
- Events are added to groups, only once on creation and cannot be changed
- Split rules should not be based on fields like severity, owner or status due to their dynamic nature

- DEMO
    - Select events
    - Split events & episodes
    - Policy Preview
    - Episode information
    - Action Rules

Smart mode

- Usage of machine learning to create episodes from events
- Demo
- Actions:
  - They are executed on local ITSI instance
  - Can be changed to remote by changing “Hybrid Action Dispatching Configuration"

Glass Tables

- Describe glass tables and their relationship to services
- Use glass tables editor to create and edit glass tables
- Design glass tables
- Configure glass table: Kpi, adhoc searches, drilldowns

Glass Tables

- Visualization tool of ITSI to identify the services status in real time
- Uses:
  - Ops dashboard
  - Service and KPI status
  - Health Score displays
  - Custom icons
- Examples: https://conf.splunk.com/files/2016/slides/anatomy-of-a-successful-splunk-it-service-intelligence-deployment.pdf

Scenarios

- You can use it to document the first requirement from users
- Scenario : Monitor Sales and IT Operations
  - Sales: overview of online sales on the website
  - IT: identify IT related issues impact critical sales process like purchase
- Our job: As splunk engineer, you need to create a glass table with given requirements:
  - Identify KPIs
  - Identify adhoc searches

Step 1: Interview your customers

- Sales
  - “Build a status dashboard that updates each minute and shows the last 15 mins overall online sales efficiency, by views and purchases, and the total volume of web content viewed by customers”
  - (customer visits, purchases, volume, conversion rate)

- IT
  - “we want to see website health. Errors encountered… CPU/mem/disk usage per machine
  - We need to see this update every minute and for last 15 mins
  - We want to be alerted if the number of servers in the web farm fall below our service level”

Glass table demo and building it

- Configuration Bar: KPI
- Configuration Bar: adhoc search
- Configuration Bar: General
- Predictive : Dashboard > predictive analytics .. Copy and paster search
- Drilldown:
  - Deep dive (default)