Splunk ITSI Training

Prachi Saxena

Week 3 - Day 2 (3 hours)

Managing Notable Event

- Define key notable events terms and their relationships
- Describe the notable events workflow
- Work with notable events

Correlations and Multi KPI searches

- Define new correlation searches
- Define multi KPI alerts
- Manage notable event storage

Managing Notable Event(Module 3)

- Define key notable events terms and their relationships
- Describe the notable events workflow
- Work with notable events

Key terms

- Episode: collection of related notable events
- Notable event: It is stored alert with a unique ID, time, status, severity, and owner. It is generated as an alert action by
  - Correlation search
  - Multi kpi alert
  - Anomaly detection
- Notable event indicate an issue or problem or disruption of service operation
- Episode Review: a dashboard which is basically service oriented event console
- Notable Event is similar to any ticket in ticketing system
- Individual notable event is immutable
- Notable events are stored in itsi_tracked_alerts
- Episode data is managed in itsi_grouped_alerts and kvstore collection

Event creation methods

- Correlation search are scheduled searches used to create an event when they detect issues
- These events are automatically associated with their respective service
- Impacted services are shown under “impacted services”
- These are setup by ITSI admins based on your requirement
- Role itoa_admin and itoa_analyst can own and modify notable events
- ITSI stores the status of notable events and episodes in the KV store collections called itsi_notable_<object type>.
- By default, notable event metadata is archived after six months to keep the KV store from growing too large. https://docs.splunk.com/Documentation/ITSI/4.6.1/EA/TrimNECollections

Episode Management concepts

- Examples of application-level episodes could be service unavailability, a data issue, an application bug, or disk-usage threshold exceeded.
- Examples of hardware episodes include server issues, network issues, or system issues.
- Each episode can be used as a ticket to track the status of work related activities
- Initial status of episode is “new” and without any ownership
- Analyst need to work in episodes by assigning it to themselves, update status and activity performed or comments and close it
- Analyst can also change the severity
- ITSI uses an indexed real-time search to retrieve notable events from the Splunk platform
- Indexed real-time searches have a delay of about 90 seconds before events get processed.
- Clear notable events: https://docs.splunk.com/Documentation/ITSI/4.6.1/EA/ClearNEs
- We can integrate it with other ticketing systems like service now

Episode Lifecycle

Status	Description
Unassigned	Used by ITSI when an error prevents the episode from having a valid status assignment.
New	Default status. The episode is logged but has not been triaged.
In Progress	The episode is assigned and the owner is investigating the issue.
Pending	The responsibility for the episode shifts temporarily to another entity to provide further information, evidence, or a resolution. An action must occur before the episode can be closed.
Resolved	The owner has addressed the cause of the episode and is waiting for verification. A satisfactory fix is provided to ensure it doesn't occur again.
Closed	It's confirmed that the episode is satisfactorily resolved.

Episode: Analyst Workflow

- Identify the episode to investigate
- Acknowledge the episode(status=in progress, owner=yourself)
- Triage using the severity, status, policy, etc (basically using methods of filter, sort and search)
- Update assignment and status as needed
- Select and investigate episodes (tabs: Impact, common fields, activity, all events, event timeline)
- Take action: Ping, Script, share, create ticket
- Demo

Views

- You can create custom views for the episode review screen
  - Change Title
  - Filters by owner, status, etc
  - Group events, choose color and fields
- Examples: Unassigned events, critical events
- Views are private by default but can be shared in app
- Demo

Correlations and Multi KPI searches (Module 13)

- Define new correlation searches
- Define multi KPI alerts
- Manage notable event storage

Correlation search

- It queries for a condition that needs attention such as disk full
- They are basically scheduled saved searches
  - If the search finds matching events, notable event is created and stored in itsi_tracked_alerts index
  - The notable event contains all result fields from the correlation search
  - Other actions such as script and email can be run
- Pre built:
  - Monitor critical service based on health score
  - Normalized correlation search
  - SNMP Traps
  - Splunk app for infrastructure alerts
- Defining correlation search :demo

Multi KPI alerts

- Multi Kpi alerts generate notable event episodes based on more than one KPI values
  - Multi kpi dashboard: demo
- These KPIs can be from one or more services
- Event creation condition can depend upon
  - Composite score: sum total of two or more KPIs reaches the limi
  - Status over time: one KPI is normal while another is critical
- Example: CPU utilization is high but number if visits are normal

Scoring(Type of MultiKPI alert)

- Composite:
  - Combined health score of all KPIs is added to the alert
  - Notable event is created if the combined score is high or low
  - Example: poor apdex score+high memory and cpu = poor customer experience

- Status over time:
  - Compare two or more KPIs
  - Create notable event based on conditions
  - Example: high number of visits but low purchase

Creating multikpi alert

- Create multi kpi alert demo
- Method 1: Main menu
- Method 2: Correlation searches
- Deep Dive: bulk actions

- Composite alert: the importance mentioned here has no impact on KPI’s normal importance for its service
- Status over time: a trigger condition model is opened for each KPI

Other Concepts

- Multi KPI notable events
- Integrating third party system
  - Ingest alerts from third party sources: https://docs.splunk.com/Documentation/ITSI/4.6.1/EA/ThirdParty
  - Link notable event to a ticket in external system:https://docs.splunk.com/Documentation/ITSI/4.6.1/User/Setupandrunnotableeventactions#Create_a_ticket_in_an_external_ticketing_system
  - Create new tickets in external system: https://docs.splunk.com/Documentation/ITSI/4.6.1/User/Setupandrunnotableeventactions#Create_a_ticket_in_ServiceNow
- Custom notable event actions
  - Add custom actions to action menu : https://docs.splunk.com/Documentation/ITSI/4.6.1/EA/Customactions
  - Build new custom action (python sdk)
  - SDK for ITSI event management: https://docs.splunk.com/Documentation/ITSI/4.6.1/EA/SDKRef

More Concepts

- Assignment list
  - User assignment drop down is created using search
    - IT Service Intelligence – User Realnames – Lookup Gen
    - Default is all uses but can be modified to get filtered users
- They are stored in itsi/local/savedsearches
- Some correlation search config items managed by kvstore too
- Retention period: stored in SA-ITOA/local/itsi_notable_event_retention.conf and default is 6 month

Event Storage