Splunk ITSI Training Plan

Prachi Saxena

Week 5 – Day1

Identify data input options for ITSI

Creating modules

- Add custom data to an ITSI deployment

Creating custom actions

Troubleshooting ITSI

- Maintenance mode
- Troubleshooting

Modules

- Identify data input options for ITSI
- Creating modules
  - Add custom data to an ITSI deployment

ITSI Modules and Content Packs

- Prebuild modules are basically splunk apps which contain range of things which helps in accelerating the service implementation and can be used during planning as well
  - Data models
  - Base searches
  - KPIs
  - Entity discovery searches
  - Visualizations
- Support technologies
  - Operating systems
  - Virtualization servers
  - Application and web servers
  - Databases
  - Loadbalancers
  - End user experience
- Additional ITSI objects are available as content packs which contain services, glass tables, etc
- Module Demo

Module Example: OS

- This is used to build KPIs for servers performance such as Processor, memory and disk
- This depends for data input using splunk_ta_nix
- Entity import is done using sourcetype as *.Version
- Prebuild module dashboard is available as ”OS Host Details”

How to configure modules

- All modules, whether included or downloaded and installed separately, do not require configuration. However, they do require relevant data to be indexed before you can create services based on the KPIs included in the modules.
- Most of the modules have pre-existing config requirements and their respective technology add ons
- URL: https://docs.splunk.com/Documentation/ITSI/4.4.5/IModules/ITSIModuleInstallationandDeployment
- Continuing our example,
  - itsi_os_module_indexes macro is used to identify entities
  - Add ons for windows and nix are used to automatically import entities
- Additional modules are available at splunkbase and can be searched using “ITSI module”
- There used to be an option Configure -> Modules, but it has been removed from version 4.4 onwards

Creating Module

- The modules creation option is not available in latest versions of Splunk ITSI (last version was 4.3.x)
- Demo of module creation

Creating custom actions

- Docs: https://docs.splunk.com/Documentation/ITSI/4.6.1/EA/Customactions
- Create a stanza in alert_actions.conf at SPLUNK_HOME/etc/apps/SA-ITOA
- Open or create a local version of notable_event_actions.conf at SPLUNK_HOME/etc/apps/SA-ITOA
- Add a stanza for the action you want to perform.
  - For example: [itsi_sample_event_action_ping]
- Set disabled = 0 to enable the custom action.
  - For example:[itsi_sample_event_action_ping] disabled = 0
- Example: https://www.splunk.com/en_us/blog/it/tale-of-tinkering-with-splunk-it-service-intelligence-and-notables.html
- Demo
- SDK: https://dev.splunk.com/enterprise/downloads and https://github.com/splunk/splunk-sdk-python/

Troubleshooting ITSI

- Maintenance mode
- Troubleshooting

Maintenance Mode

- Temporary suspend the services and entities for maintenance or planned purposes
  - KPI and notable event episodes are suppressed
  - Once maintenance window is over, KPIs and episodes would be generated again
- Need to configure for a start or stop time
- Demo of creation: Configure → Maintenance Windows
- The Services and KPI are shown in gray color with a maintenance icon
- It can be used to edit the services & entities.
- Always schedule the windows 15 to 30 mins before and after the work. This buffer gives the system an opportunity to catch up with the maintenance state and reduces the chance of ITSI generating false positives during maintenance operations.

Troubleshooting and Best Practices

- Log files:
  - Any log entries with /itsi* source such as itsi_statestore.log, itsi_backfill,log
  - index=_internal source=*itsi* sourcetype=itsi_internal_log
- Unable to add entities:
  - Missing sourcetypes that are used for entity discovery
  - As per our OS example, entity import depend upon “Host_OS Inventory”, populated by “Unix.Version” events. If these are missing, the entity import will not work. https://docs.splunk.com/Documentation/ITSI/4.4.5/IModules/OSModuletroubleshooting#Entity_information_not_populating
  - Also Splunk_TA_nix and/or Splunk_TA_windows need to be installed with supported version
  - Macro itsi_os_module_indexes need to be enabled and configured with correct indexes
  - The version.sh used for nix input should be enabled

Skipped searches

- Too many concurrent searches in your environment may cause some of your searches to be skipped
- ITSI uses realtime_schedule = 0 , so if you have many saved searches, it may cause delayed results and high resource utilization
- Solution:
  - Reduce number of KPI
  - Reduce correlation searches
  - Reduce frequency
  - Increase indexers
  - Monitor long running searches and improve them by removing wildcards, proper filtering
    - | rest /services/search/jobs | search label = Indicator*

Entity

- ITSI Health Check dashboard: https://docs.splunk.com/Documentation/ITSI/latest/User/ITSIHealthCheckdashboard
- Entity Duplication: all entities should have unique names
  - Sometime we have same alias for multiple entities
  - Details available on health check dashboard
  - Resolve it by deleting duplicate and not mapped to any service entities
  - Find stale entities using below search

```
|inputlookup itsi_entities
| fields title
|join type=outer [
        search index=itsi_summary
        |stats count,last(_time) as lastsec by entity_title
        |eval age = round(now() – lastsec) / 86400,1)
        | rename entity_title as title
        | table title count age]
```

Missing KPI events

- If no events are available in itsi_summary
  - Execute alert search for KPI in the KPI edit screen and ensure it returns data
  - If there is no data,
    - Make sure your search syntax is correct
    - You are not using stats command
    - Check the lag settings
    - Don’t use earliest or latest time in search

KV store memory

- KV store is extensively used in ITSI for services, base search, deep dive and glass tables
- It has default limit of 50mb per batch save, which could be used by in bigger installations
- Edit etc/system/local/limits.conf
  - [kvstore]
  - max_size_per_batch_save_mb = < larger value >
  - Restart splunk