Splunk ITSI Training

Prachi Saxena

Day4 (3 hours)

Data Audit and Base Searches

- Use a data audit to identify service key performance indicator
- Design base searches

Implementing Services

- Use a service design to implement services in ITSI
- Creating Service Templates

Lab discussion

Data Audit and Base Searches

- Use a data audit to identify service key performance indicator
- Design base searches

Generating KPI Values

- This is a part of detailed design and is needed to generate the correct numeric value for each KPI
- It is needed to have a detailed understanding of the available events in Splunk
- This is mostly an iterative process and you go back and forth between high- and low-level design
- Each KPI gets its value from calculations executed on filtered set of events

Data Inputs

- ITSI can consume any data available in Splunk Enterprise
- It uses event or metrics data to define KPIs and entities
- Try to have at least 7 days of data before starting ITSI configuration
- There are times when you may have to add new data

KPI search design criteria

- Kpi always measures one value, so you need to define a search which would return one value
  - Use eval or coalesce command
- Required data information
  - Search expression
  - Time span and frequency
  - Type of summarization: avg, count, last
  - Split criteria
- Event Search or Metric searches
- Fieldsummary command

Approaches to Design research

- Use built in modules
  - Useful for common data types
- Run searches in splunk to identify content
  - Useful for unique business KPIs

Note: work with knowledge experts and admins in company

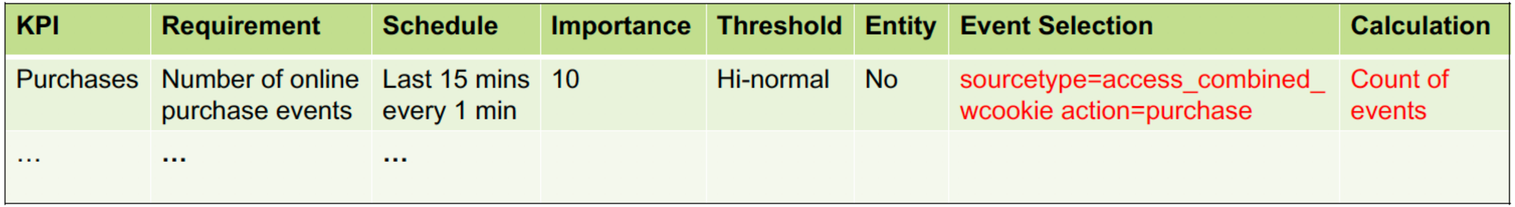
Start with what systems are being used, what software is being used to run that system, how are they implemented

KPI Event selection best practices

- Must return single numeric value
- Use single sourcetype if possible
- Use simple search criteria:
    - Avoid wildcards, datamodel commands and transforming commands
- Use least frequent schedule possible
- Use shortest time span possible
- Decide if the KPI is an overall value,or if it should be split by entity

Optimize the searches

- Create a search with needed fields and filters and test it
- Use search job inspector to check search performance
- Reduce the search execution time as much as possible
- Create template to record it



KPI	Requirement	Schedule	Importance	Threshold	Entity	Event Selection	Calculation
Purchases	Number of online purchase events	Last 15 mins every 1 min	10	Hi-normal	No	sourcetype=access_combined_wcookie action=purchase	Count of events
...	...	...					

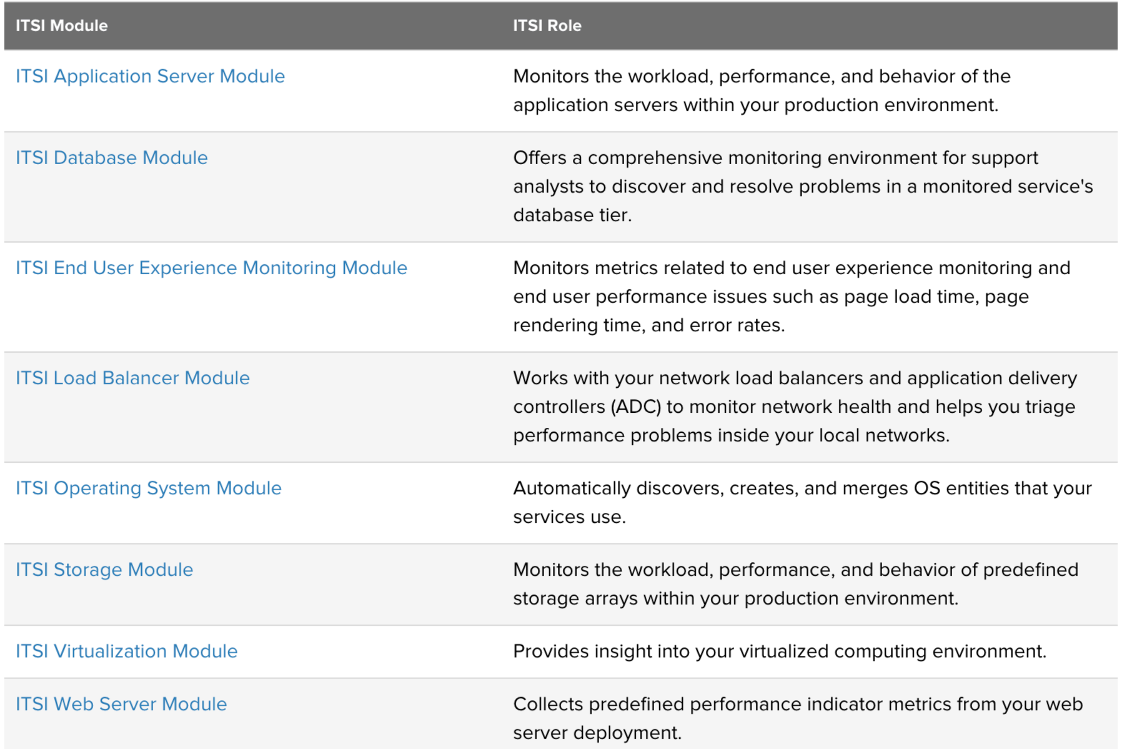
- Use Base searches: use when multiple KPIs share common source and reduce search concurrency

Base searches

- Demo on how to create them
- Changes are published across all KPIs and services
- Selected search expression should be as simple as possible
- They are saved in savdsearches.conf
  - Indicator - Shared - XXXX - ITSI Search

Built in modules

Splunk IT Service Intelligence (ITSI) modules are built from a collection of metrics, entities, and service configurations. They help ITSI users understand and act on the data that comes from monitoring services within ITSI.



ITSI Module	ITSI Role
ITSI Application Server Module	Monitors the workload, performance, and behavior of the application servers within your production environment.
ITSI Database Module	Offers a comprehensive monitoring environment for support analysts to discover and resolve problems in a monitored service's database tier.
ITSI End User Experience Monitoring Module	Monitors metrics related to end user experience monitoring and end user performance issues such as page load time, page rendering time, and error rates.
ITSI Load Balancer Module	Works with your network load balancers and application delivery controllers (ADC) to monitor network health and helps you triage performance problems inside your local networks.
ITSI Operating System Module	Automatically discovers, creates, and merges OS entities that your services use.
ITSI Storage Module	Monitors the workload, performance, and behavior of predefined storage arrays within your production environment.
ITSI Virtualization Module	Provides insight into your virtualized computing environment.
ITSI Web Server Module	Collects predefined performance indicator metrics from your web server deployment.

Reference: https://docs.splunk.com/Documentation/ITSI/4.6.1/IModules/AboutITSIModules

ITSI Modules

- ITSI modules process data collected through the use of Splunk **add-ons**.
- Add-ons collect host, network, and other data from computers that you install them on, and map that data to a data model.
- Add-ons power the data underlying metrics and entities of each module.
- ITSI interacts with modules through configuration files.
- ITSI consumes and processes these files and integrates the information across the app.

ITSI Content Pack

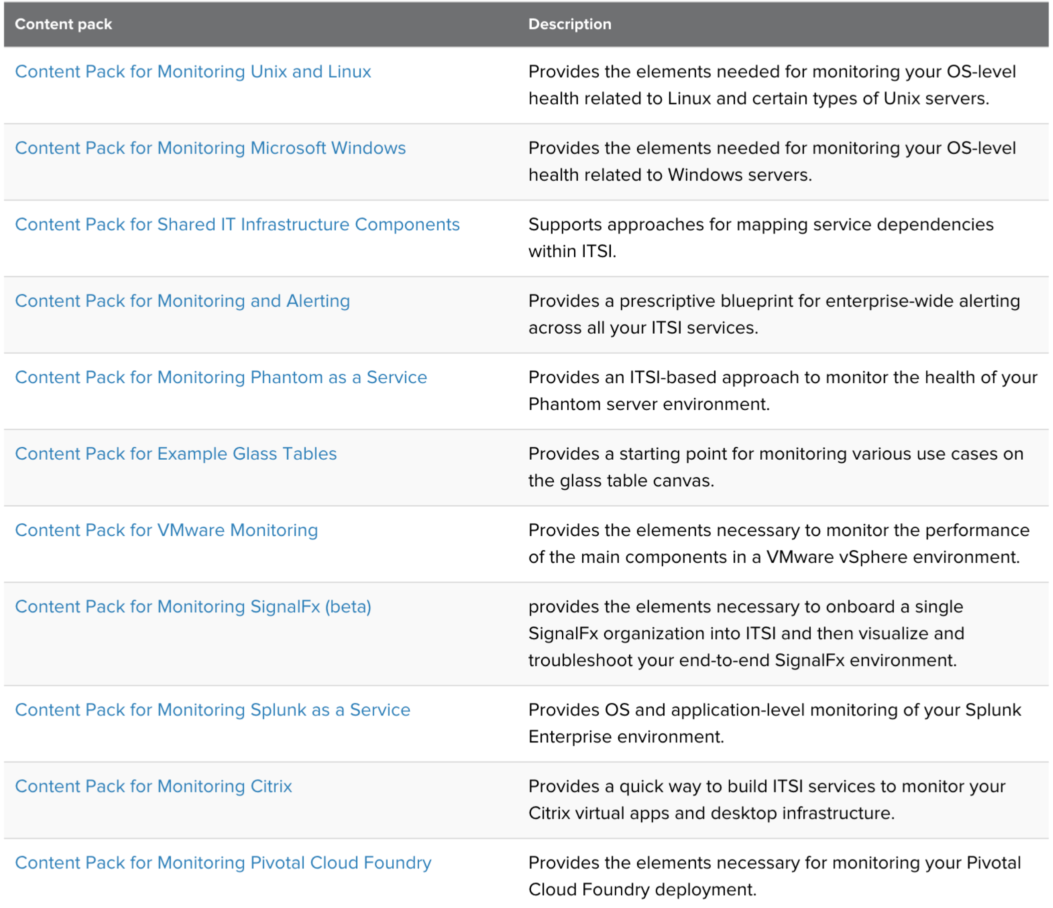
- Splunk IT Service Intelligence (ITSI) content packs provide out-of-the-box content that you can use to quickly set up your ITSI environment.
- A content pack is a backup of **KV store** objects that you restore to your own environment and tune for your specific data sources.
- This content can include preconfigured KPI base searches, service templates, saved glass tables, and other objects for use within
- Most content packs process data collected through the use of Splunk add-ons. Add-ons collect host, network, and other data from computers that you install them on and map that data to a data model. Add-ons power the data underlying the metrics for each content pack.

Difference between CP and Modules

- ITSI currently still supports modules. Modules were introduced in ITSI version 2.0 as a way to deliver out-of-the-box content to customers.
- Like content packs, modules include KPI base searches, KPIs, and entity auto-discovery searches, but not the other elements that content packs provide.
- One key difference is that all module content is immutable, so you can't tailor KPI base searches for maximum performance.
- Due to the limitations of modules, the current best practice is to use the content packs instead.

Content Packs

- At this time, content packs can only be installed in clean ITSI environments because the objects might overwrite existing configurations. Each content pack should only be downloaded and installed once. Do not install newer versions of a content pack on top of an existing version.



Content pack	Description
Content Pack for Monitoring Unix and Linux	Provides the elements needed for monitoring your OS-level health related to Linux and certain types of Unix servers.
Content Pack for Monitoring Microsoft Windows	Provides the elements needed for monitoring your OS-level health related to Windows servers.
Content Pack for Shared IT Infrastructure Components	Supports approaches for mapping service dependencies within ITSI.
Content Pack for Monitoring and Alerting	Provides a prescriptive blueprint for enterprise-wide alerting across all your ITSI services.
Content Pack for Monitoring Phantom as a Service	Provides an ITSI-based approach to monitor the health of your Phantom server environment.
Content Pack for Example Glass Tables	Provides a starting point for monitoring various use cases on the glass table canvas.
Content Pack for VMware Monitoring	Provides the elements necessary to monitor the performance of the main components in a VMware vSphere environment.
Content Pack for Monitoring SignalFx (beta)	provides the elements necessary to onboard a single SignalFx organization into ITSI and then visualize and troubleshoot your end-to-end SignalFx environment.
Content Pack for Monitoring Splunk as a Service	Provides OS and application-level monitoring of your Splunk Enterprise environment.
Content Pack for Monitoring Citrix	Provides a quick way to build ITSI services to monitor your Citrix virtual apps and desktop infrastructure.
Content Pack for Monitoring Pivotal Cloud Foundry	Provides the elements necessary for monitoring your Pivotal Cloud Foundry deployment.

Reference:https://docs.splunk.com/Documentation/ITSICP/current/Config/About

Implementing Services

- Use a service design to implement services in ITSI
- Creating Service Templates

Creating Service

- Manually
- Service Template
- CSV Import

Service Health Score

- Take the latest **alert_severity** for each KPI and map it to a score in this table:

alert_severity	Score
Normal	100
Low	70
Medium	50
High	30
Critical	0

- Then multiply that score times the KPI's importance value—this is the KPI's **weighted alert_level**

$$\left\{ \frac{\Sigma[\text{weighted alert levels}]}{\Sigma[\text{importance weights}]} \right\}$$

The sum of all weighted alert levels, divided by the sum of all importance weights, expressed as a score from 0 (critical) to 100 (normal)

Minimum health indicator KPIs (importance = 11) are treated as 10 for math, but cause the overall score to be no higher than that KPI's alert level

Service health score alert levels

Normal: 81 - 100

Low: 61 - 80

Medium: 41 – 60

High: 21 - 40

Critical: 0 - 20

- Let's say the ship's **Phaser** service has 3 KPIs with the following importance settings and alert levels:

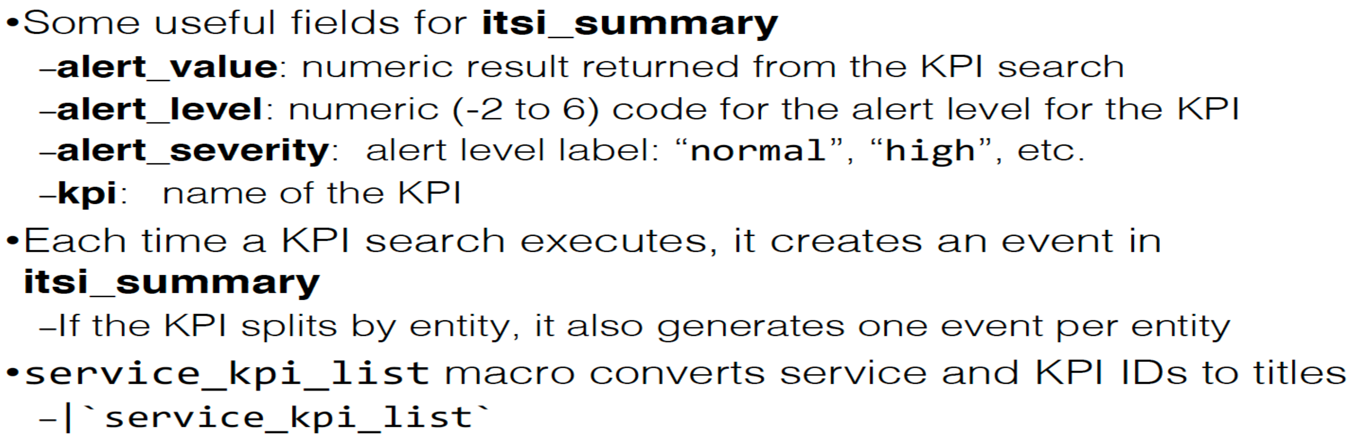
KPI	Alert Severity	Importance
Charge	Normal (100)	10
Available banks	High (30)	5
Targeting	Low (70)	5

- The health score would be:

```
Σ [weighted alert levels] / Σ [importance weights]
  (100*10 + 30*5 + 70*5)  /   (10 + 5 + 5) = 75 (low)
```

Details

- Service and entity definition are store in KVstore
- KPIs are stored as saved searches: Indicator – xxxxxx – ITSI Search
- Events created by KPI execution are stored in itsi_summary index



- Some useful fields for **itsi_summary**
  - **alert_value**: numeric result returned from the KPI search
  - **alert_level**: numeric (-2 to 6) code for the alert level for the KPI
  - **alert_severity**: alert level label: "`normal`", "`high`", etc.
  - **kpi**: name of the KPI
- Each time a KPI search executes, it creates an event in **itsi_summary**
  - If the KPI splits by entity, it also generates one event per entity
- `service_kpi_list` macro converts service and KPI IDs to titles
  - `|`service_kpi_list``