Splunk ITSI Training Plan

Prachi Saxena

Week 2 - Day 2 (2 hours)

Installing and Configuring ITSI

- List ITSI hardware recommendations
- Describe ITSI deployment options
- Identify ITSI components
- Describe the installation procedure

Planning

- Assumptions:
  - Splunk enterprise is already deployed in your environment
  - Data is available in Splunk
  - You have valid licenses
- Do not installed with Splunk Enterprise Security

  https://docs.splunk.com/Documentation/ITSI/4.6.1/Install/Compatibility
- Components:
  - Search Heads
  - Indexers
  - License Servers

Planning

- Splunk Enterprise version compatibility
  - https://docs.splunk.com/Documentation/VersionCompatibility/current/Matrix/CompatMatrix
- Prepare list of services, KPIs and glass tables required
- Prepare list of entities: ip, hostname,type
- User roles and permissions: admin
- Existing hardware performance

```
index=_introspection sourcetype=splunk_resource_usage component=Hostwide
earliest=-5m | timechart avg(data.cpu_user_pct) by host
```

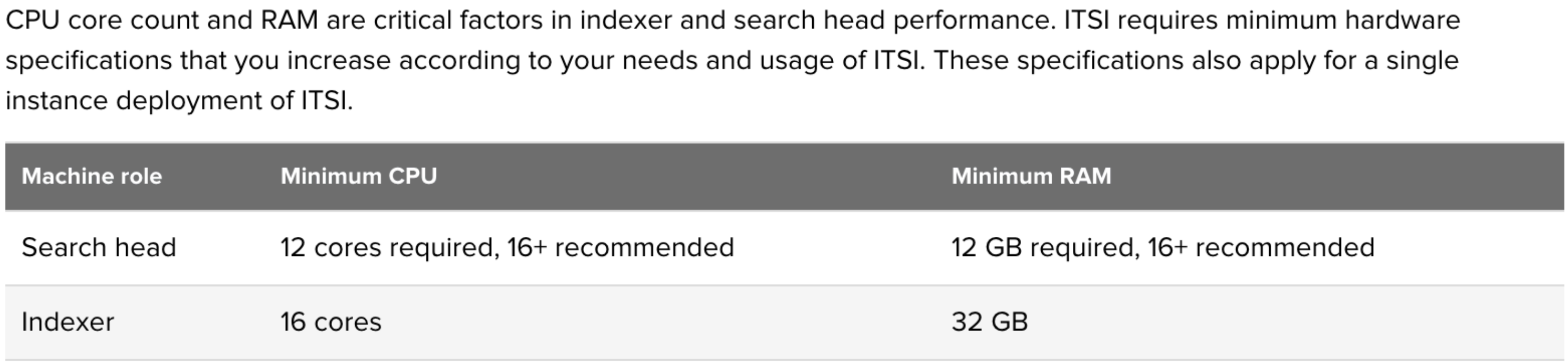
- No skipped searches

Deployment Architecture

- Single instance
- Distributed deployments:
    - Search Head Clustering
    - Indexer Clusters
    - Multi-site indexer clusters
- Licenses:
    - It is requirement to have valid ITSI license
    - This is checked every 24 hours at midnight
    - A warning is generated if ITSI license is not found

Hardware

- Basic Enterprise hardware recommendations to be followed
    - On SH: minimum of 30 GB of free storage in $SPLUNK_HOME



CPU core count and RAM are critical factors in indexer and search head performance. ITSI requires minimum hardware specifications that you increase according to your needs and usage of ITSI. These specifications also apply for a single instance deployment of ITSI.

Machine role	Minimum CPU	Minimum RAM
Search head	12 cores required, 16+ recommended	12 GB required, 16+ recommended
Indexer	16 cores	32 GB

ITSI Performance Considerations

- ITSI performance depends on the ability to perform multiple fast, concurrent searches.
    - Number of entities and KPIS would increase the load on indexer
        - Based on number of scheduled searches and their complexity
    - If ITSI is sharing resources with existing Splunk enterprise(SHs) environment, you might need to increase the resources.
    - Mostly the actual required resources are above base splunk recommendation
    - Need fast storage (SSDs) and higher CPU/MEM on Search heads

ITSI Capacity Planning

- Estimate the number of KPI and searches you would need before working on capacity planning
- Hardware requirement would vary over time and mostly increase with the progress on ITSI deployment and usage
  - https://docs.splunk.com/Documentation/ITSI/4.6.1/Install/Plan#ITSI_capacity_planning
- Main ITSI factors:
  - KPI schedule and run time
  - Number of entities per KPI
  - data volume
  - Concurrent users

- 200 discrete KPIs, a search head cluster is a more stable option
- The limit of a single batch save to a KV store collection is 50 MB.
  - https://docs.splunk.com/Documentation/ITSI/4.6.1/Install/Plan#KV_store_size_limits

Things to remember

- Need Java to be installed: Java 8x - 11.x , 64 bit
- Need MLTK and Python for scientific computing
- Enable forwarding on Search heads
- Enable SSL
- Check the supported version as per your Enterprise version
- Get the latest supported version
- You can't disable real-time searches on either the indexer tier or the search head tier where ITSI is running

Installing ITSI

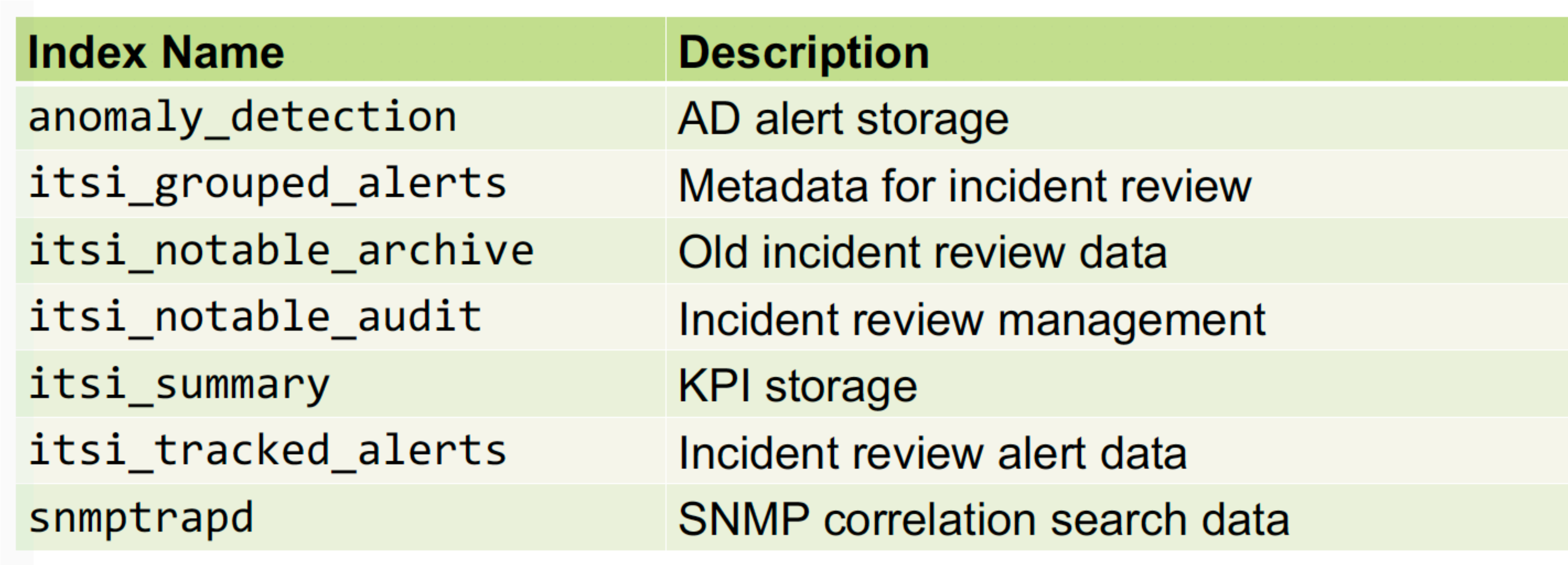
- Commands to install on single server
    - /opt/splunk/bin/splunk stop
    - tar -xvf splunk-it-service-intelligence_445.spl -C /opt/splunk/etc/apps/
    - /opt/splunk/bin/splunk start

- On distributed or cluster environment deploy through the respective management servers

Component locations

- Search Head: all components
- Indexers: SA-IndexCreation, Splunk_TA_Infrastructure
- License Master:
  - SA-ITSI-Licensechecker
  - SA-ITOA
  - SA-UserAccess

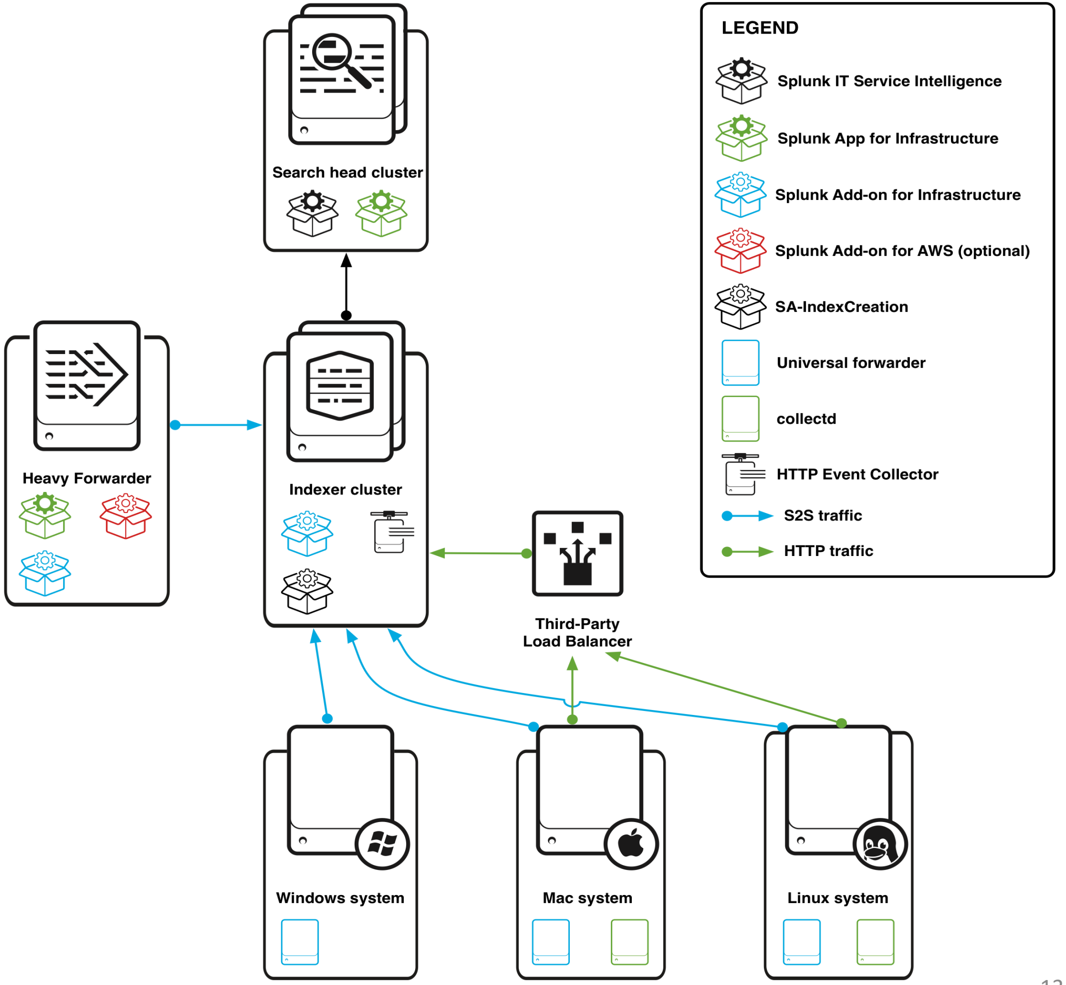
ITSI Indexes



Index Name	Description
anomaly_detection	AD alert storage
itsi_grouped_alerts	Metadata for incident review
itsi_notable_archive	Old incident review data
itsi_notable_audit	Incident review management
itsi_summary	KPI storage
itsi_tracked_alerts	Incident review alert data
snmptrapd	SNMP correlation search data

Distributed deployment Scenarios

- Distributed Search
- Search Head Cluster
- Indexer cluster



ITSI Components

Splunk_app_infrastructure	Newly added Apps and addons
Splunk_Ta_Infrastructure	
vmware_ta_itsi	
DA-ITSI-APPSERVER	Domain add-ons: Modules
DA-ITSI-DATABASE	
DA-ITSI-EUEM	
DA-ITSI-LB	
DA-ITSI-OS	
DA-ITSI-STORAGE	
DA-ITSI-VIRTUALIZATION	
DA-ITSI-WEBSERVER	
SA-ITOA	Entity and service management
SA-ITSI-ATAD	Adaptive threshold management
SA-ITSI-CustomModuleViz	Custom visualization files
SA-ITSI-Licensechecker	Validate ITSI licenses
SA-ITSI-MetricAD	Anomaly detection tools and services
SA-IndexCreation	ITSI summary index configurations
SA-UserAccess	ITSI access control tools
itsi	IT Service Intelligence main application