Splunk ITSI Training Plan

Prachi Saxena

Week 5 - Day 2 (2 hours)

Access Control

Backup and restore

Access Control

- Identify ITSI roles and capabilities
- Describe service level roles and teams
- Modify ITSI Menu options
- Control access to ITSI Views

ITSI Default Roles

Splunk IT Service Intelligence provides four special roles with predefined capabilities:

Role	Description
`itoa_user`	Assign this role to users who need basic read access to ITSI.
`itoa_analyst`	Assign this role to knowledge managers in your organization who will create glass tables, deep dives, and service analyzers and work with episodes in Episode Review.
`itoa_team_admin`	Create team admin roles that inherit from this role. Team admins can create and administer services for ITSI teams to which they are assigned read/write access. This role can also create and manage notable event aggregation policies.
`itoa_admin`	Assign this role to ITSI administrators. Admins create teams for team administrators to administer as well as create objects in the Global team. This role is required to assign access to objects such as glass tables to other ITSI roles. Note that users with the Splunk `admin` role also have the `itoa_admin` role.

https://docs.splunk.com/Documentation/ITSI/4.6.2/Configure/UsersRoles

Role Permissions

- Access level is set for the Service Analyzers, Deep Dives and Glass table by roles.
- Docs: Very detailed level roles information is available below for reference https://docs.splunk.com/Documentation/ITSI/4.4.5/Install/UsersandRoles
- Custom roles can be created based on the existing roles with permissions as needed
  - Itoa_analyst can only read correlation searches, but sometimes you may want to give them “write_correlation_search” capability to let them create multiKPI alerts
  - Go to Settings → Access Controls → Roles

Permissions

- Deep Dive (default)
  - Itoa_user and itoa_analyst, both and read write access… permission name is write_itsi_deep_dive_context
- Service Analyzer (default)
  - Itoa_user has read only and itoa_analyst has read/write access
  - Controlled by write_itsi_homeview
- All other objects such as saved service analyzer, saved deep dive, episode review are owned by users creating them and have role based access
- Permissions are controlled by usual splunk method of Edit → Edit Permissions
  - Read for read only view and Write for read/write permissions

Customize ITSI Menu

- You can customize the default ITSI menu by Settings → User Interface →Navigation Menus
  - Changes are made by modifying default entry and editing XML

Service Level Permissions

- Teams concept is used to manage service level permissions
  - Default = Global Team (managed by itoa_admin)
  - Any ITSI user can view these services, KPIs and notable events

- Create new teams in order to control service permissions and to assign teams ownership to the disparate teams
  - Create new team
  - Use role as itoa_team_admin
  - Add analyst role to the teams
  - Assign services to the team

- Teams can only control services, rest entity, views, base searches, etc are always owned by Global team

User Case for Teams

- Global Team (itoa_admin)
  - Entity, KPI template, base searches and threshold templates
- Department 1: Marketing (itoa_team_admin_1)
  - Marketing Service
- Department 2: Infrastructure (itoa_team_admin_2)
  - OS Service, DB Service, Network Service, Storage Service, etc.
- Department 3: HR (itoa_team_admin_3)
  - Payroll Application service, Recruitment Service

Views and Teams

- Any View such as SA, DD,GT would display the KPIs from services based on the team assignment
- For Notable events as well, you would only view episodes based on the service access for your team
- Service with Global team can be accessed by anyone
- This does not impact raw data access for the services
- Create Team: Configure → Teams
  - Enter Title, select roles based on read / write access
- Create Service with team owner

Backup and restore

- You can configure complete or partial backup based on the job
- Accessed by Configure → Backup/ Restore
- It contains KV Store and configuration files
- They are basically json files and can be moved from one splunk instance to another
- Default backup schedule is daily at 1:00 am system time, it can be modified but not deleted
- Once the backup job is completed, message is display on top
- Partial Backup can have Services, Templates, Teams, deep dives and Glass tables, etc.

Restore

- This backup package can be downloaded when job is completed and can be used for restore
- Restore can be done on same or different systems
- The restore job does the full replacement of the target system ITSI config
- Indexes backup is not included
- Content packs are also installed using the restore method
- Script “kvstore_to_json.py” from SA-ITOA/bin can be used via command line to
  - Perform full/partial backup
  - Bulk update KPIs
  - Bulk update timezone offsets
  - Migrate ITSI objects from one ITSI instance to another
  -