Introduction to Splunk

General Overview

Index

- collects data from virtually any source.
- Like a factory that takes in data as raw materials.
- Inspectors decide how to process the data.
- The data is then labeled with a source type, which is used to break the data into single events.
- These events are time stamped, and entered into the Splunk index, where they can be searched.

Search & Investigate

- Enter a query to find events that contain values.
- You can then analyze and run statistics on the events using the Splunk search language.

Knowledge Objects

- Allow you to affect interpretations of data.
- You can add classification and data enrichment.
- You can also save reports for future use

Monitor & Alert

- Splunk proactively monitors all your infrastructure in real time.
- You can set alerts to monitor specific conditions, and automatically respond.

Report & Analyze

- Collect reports and visualizations into dashboards.

Splunk Web

Apps

- Preconfigured environments that sit on top of your instance
- Extends prebuilt knowledge and capabilities
- Like workstations built to solve specific use case
- Splunk Enterprise has 2 default apps:
    1. Home
        a. Quick place to explore splunk enterprise
        b. Launch and manage other splunk apps
        c. Find documentation
        d. Set a custom dashboard as your home dashboard
        e. Admins can add apps and data

2. Search and Reporting
    a. Default interface for searching and analyzing data
    b. 8 main components
        i. Splunk Bar
        ii. App Bar
        iii. Search bar
            1. Time range picker retrieves events over a certain period
        iv. How to search panel
            1. Documentation
            2. Search tutorial
            3. Data summary button
                a. Breaks down data into 3 types:
                    i. Hosts: name, ip address, domain name of machine of event origin
                    ii. Source: Where the event originated
                    iii. Sourcetype: Classification of data
        v. Table Views
            1. Ui driven way to explore and prepare data
        vi. Search History menu
            1. Allows you to run and view past searches
            2. Can narrow search history by entering search terms into filter window
            3. Can filter searches by time

- Defined by roles

Splunk Roles

- Define what a user can see, do, and interact with
- 3 Roles:
    1. Admin
        a. Most powerful
        b. Install apps
        c. Create Knowledge Objects for all users
    2. Power
        a. Create and share knowledge objects for users of and app
        b. Do real time searches
    3. User
        a. Only see their own knowledge objects and those shared with them

Splunk Bar

- Appears on every page in Splunk enterprise
- Switch between apps
- Edit account
- View system level messages
- manage and edit Splunk configurations
- Monitor progress of search jobs
- Find help

App Bar

- Allows you to navigate applications

Splunk Search Language

- Limiting Search by time gets faster results and is a best practice

After Search Interface

- Search jobs will remain active for 10 minutes after it is run
- Save as menu
    - Allows you to save search as a knowledge object
- Search results tab
    - Populate search result tabs depending on search commands
    - Events Tab
        - Displays events returned for your search
        - Usually default for simple searches
    - Patterns tab
        - Lets you see patterns in your data
    - Statistics tab
    - Visualizations tab
    - Above you can see total events returned
    - Can also select a random sample of events returned
- Search action buttons
    - Edit, inspect, delete, and send to background actions
    - Pause, stop, share, print, and export buttons
    - Can bookmark by hitting the share button
    - Shared search jobs remain active for 7 days
    - Export allows you to save results as raw, csv, xml, or json
- Search mode selector
    - 3 modes:
        1. Fast: cuts down on returned field info; field discovery disabled
        2. Smart: toggles behavior based on search
        3. Verbose: returns as much field and event data as possible
- Timeline

    - Segments decided by time chose in time range picker
    - Can select specific time lists
    - Can zoom in and out
- Event list
- Field sidebar

Transforming commands

- Commands that create statistics or visualizations

Event List

- Text you search for is highlighted
- Returned in reverse chronological order
- Timestamp based on personal time zone
- Selected fields across the bottom of each event.
    - Default fields: host, source, sourcetype
- Can highlight text to add text to search, exclude, or make a new search
- Info button
    - Shows all extracted fields for event
    - Drop down for event actions
    - Link for field actions

Search Terms

- *-wildcard
- Not case sensitive
- Booleans can be used for multiple terms
    - No boolean implies and
    - Order of operations: not, or, and
- Search in quotes for exact terms
- \ escape char
- | pipe

Commands

- Tells Splunk what we want to do with search results
    - Creating charts, statistics, etc.
- Functions
    - Explain how we want to chart, compute and evaluate results
- Arguments
    - Variables we want in functions
- Clauses
    - How we want results grouped or defined

- Start with search terms, then components
- Commands may have functions that perform operations ex. Count function in stats command
- Search command can be used at any time to filter results further

Best Practices

- If command references a specific value, it is case-sensitive
- Time filter your searches
- Index, source, host, and sourcetype are next strongest after time
- The more you tell the search engine, the better results you will get
- Inclusion > exclusion (access denied> NOT access granted)
- When possible, use OR or IN instead of wildcards
- Apply filtering commands as early as possible

Knowledge Objects

- Tools that help users discover and analyze data
- Can be shared with other users based on permissions
- Can be saved and reused by multiple users in multiple apps
- Can be used in a search
- 5 Categories:
    1. Data interpretation
        a. Fields
            i. Automatically extracted based on source type
        b. Field extractions
            i. Manual extractions
        c. Calculated fields
            i. Perform calculations based on values of existing fields
    2. Data classification
        a. Event types
            i. Categorize events based on search terms
        b. Transactions
            i. Groups of conceptually related events
    3. Data enrichment
        a. Lookups
            i. Add other fields and values to events
        b. Workflow actions
            i. Create links within events that have access to external resources
    4. Data normalization

    a. Tags
        i. Designate descriptive names for key value pairs; labels for data
    b. Field Aliases
        i. Normalize data over multiple sources
5. Data models
    a. Hierarchically structured datasets

Knowledge Manager Responsibilities

- Oversee knowledge object creation
- Implement naming conventions
- Normalize event data
- Create data models

<u>Creating Reports and Dashboards</u>

- Simple way to save and share searches
- Todo:
    - Save as, select report
- Good to define report naming conventions
- Can change time range of events in report if turned on
- Find reports in your applications bar
- You can edit description, permissions, schedule or acceleration of reports
- You can also clone, embed, or delete reports with proper permissions
- Change display setting to app in report to display to everyone in the app
- Run as lets you switch between running as user or owner
- Can generate quick reports from the fields in your search

Visualizing data

- Any search with statistical values can be viewed as a chart
    - Hovering over a segment of a chart will show statistic of that segment
    - Can be based on numbers, time, or location
- Many visualizations are interactive
- Can save visualization as report or dashboard panel

Dashboard panel

- Can view and edit dashboards from the dashboard tab in the app bar
- Report or collection of reports displayed as a single pane of glass
- Visualizations tab
    - Can select chart

        - Use format menu to change specifics about the visualization (ex. Legend on the left)
- You can add multiple panels to one dashboard
- You can rearrange panels by clicking on the edit button
    - You can view and edit the xml source of the dashboard
    - Add panel
        - New
        - New from report
        - Clone from dashboard
        - Add a prebuilt panel
    - Add input
    - Toggle dark theme
- There are tools on each panel
    - Edit searches
    - Change visualizations
    - Modify visualization formatting