Intro to Splunk Cheat Sheet

What is Splunk?

- “Splunk turns machine data into answers.”
- Aggregates, processes, analyzes, and helps use data.

Splunk & Your Career

- Search for people who have skill you are considering – see what they can do with the certification you are considering, examine experience levels, jobs, etc.
- Check LinkedIn and job sites.

Course Resume Items

- Installed and maintained small Splunk enterprise environment
- Created alerts, dashboards, and reports from Splunk data
- Onboarded new data sources for Splunk environment

Parts of Splunk

- Data Pipeline: Input > Parsing > Indexing > Searching
- Search Heads: Search management; scheduled searches, alerts, dashboards;
- distributes searches to indexers
- Indexers: Receive, index, store data; search data based on search requests from search head
    - Index: Noun; data repository
    - Index: Verb; processing raw data

- Indexer: Splunk instance that indexes data
- An indexer indexes data and puts it into an index

- Forwarders: Send data onward
  - Universal Forwarder
  - Light Forwarder (deprecated)
  - Heavy Forwarder
  - Installation of Universal Forwarder in large environment may be managed with a
  - deployment tool like SCCM, Ansible, or Chef
- Server roles: Search Head, Cluster Master, License Master, Indexer, Deployment Server, KV Store, SHC Deployer
- Distributed environments: “Horizontal scaling”; separate out the pieces
- Deployment Scales
  - Very small office/department: Might be able to do a non-distributed environment; combined Search Head/Indexer
    - < 20 GB
    - < 100 forwarders
  - Large enterprise: Distributed environment; 10+ Indexers, separate Deployment Server, likely multiple Search Heads
    - 300+ GB
    - 1000s of forwarders
- Clustering: Data replication (availability, fidelity, recovery); redundancy
- Forwarders send data, Indexers turn data into events and place them in indexes, Search Heads send search requests and display data