Introduction to Splunk

Module 3: Parts of Splunk

Natasha Staples

CYBRARY

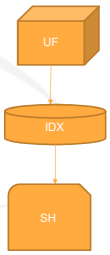
In this video...

- Use whatever you have
- Data pipeline
- Splunk components
- Distributed / Non-distributed / Clustered

CYBRARY

Data Pipeline

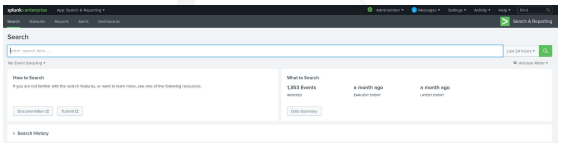
- Input
- Parsing
- Indexing
- Searching



CYBRARY

Search Heads

- Search management
- Scheduled searches, alerts, dashboards
- Distributes searches to indexers



CYBRARY

Indexers

- Receive, index, store data
- Search data based on search requests from search head

CYBRARY

Index…?

- 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.

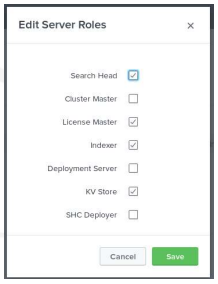
CYBRARY

Forwarders

- Sends data onward
- Universal forwarder
- Light forwarder (deprecated)
- Heavy forwarder

CYBRARY

Other server roles



CYBRARY

Distributed environments

- "Horizontal scaling"
- Separate out the pieces

CYBRARY

Deployment Scales

- Very Small Office / Department
  - <20GB
  - <100 forwarders
- Large Enterprise
  - 300GB+
  - Up to 1000s of forwarders

→ Combined Search Head, Indexer

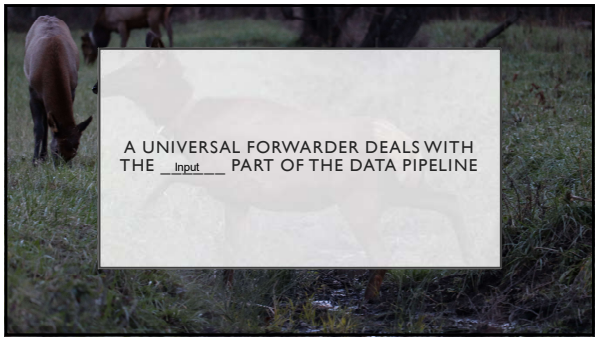
→ Distributed environment with 10+ indexers and separate deployment server and likely multiple search heads

CYBRARY

Clustering

- Data replication
  - Availability
  - Fidelity
  - Recovery

CYBRARY



Review

- Forwarders send data, indexers turn data into events and place them in indexes, search heads send search requests, display data
- A large company will likely need a distributed environment
- Clustering provides redundancy

CYBRARY

Next up: Installation!

CYBRARY