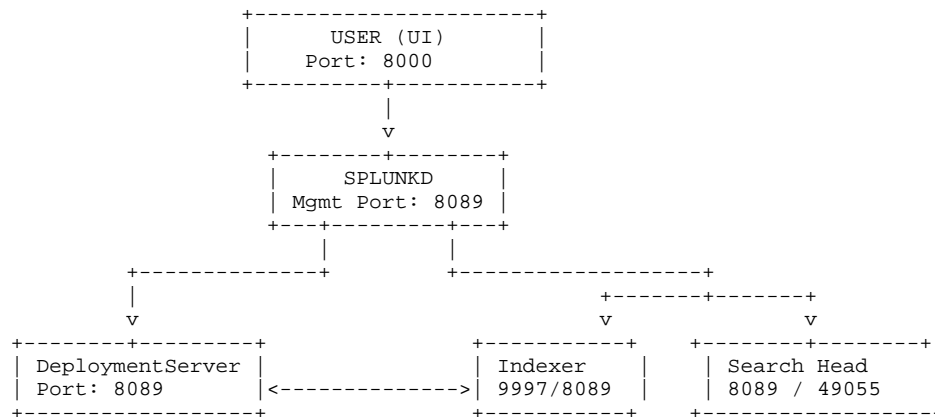


Splunk Ports Cheat Sheet & Connectivity Diagram



Core Splunk Ports

- 8000 – Splunk Web UI
- 8089 – splunkd management port (internal communication)
- 8191 – KV Store (MongoDB)
- 9887 – Indexer cluster replication
- 9997 – Forwarder → Indexer data ingest

Search Head Cluster (SHC)

- 8089 – SHC member communication
- 49055 – Captain election (RAFT)
- 8191 – KV store replication

Indexer Cluster

- 8089 – Cluster Manager → Indexers
- 9887 – Bucket replication

Forwarders

- 9997 – Data forwarding
- 8089 – Connect to Deployment Server
- 514 / 1514 / 6514 – Syslog ingestion (UDP/TCP/TLS)

HTTP Event Collector (HEC)

- 8088 – HEC token ingestion

Syslog

- 514 – Standard syslog
- 1514 – Custom non-privileged syslog
- 6514 – Secure syslog over TLS