Splunk Capacity Planning Template

|  |  |  |
| --- | --- | --- |
| Parameter | Description | Your Systems |
| Daily Data Ingestion | Total volume of data ingested daily into the environment. |  |
| Number of Indexers Needed | Number of indexers calculated based on ingestion rates (typical indexer handles ~300 GB/day in a non-clustered environment). |  |
| Indexer Clustering | For redundancy and data availability. |  |
| Daily Search Loads | Expected search queries per day, influences search head requirements. |  |
| Number of Search Heads Needed | Number of search heads based on concurrent user searches (approx. 150 concurrent searches per search head). |  |
| Search Head Clustering | For high availability and search load distribution across multiple nodes. |  |
| Enterprise Security | Heavy resource consumption due to correlation searches, dashboards, and real-time threat analysis. |  |
| IT Service Intelligence | High data ingestion due to real-time metrics, KPIs, and service correlation for service monitoring. |  |
| Search Concurrency | Number of users running searches concurrently, influencing search head sizing. |  |
| Search Duration | Average length of a search query. |  |
| Storage Requirements | Required storage for raw data retention. Based on data retention policies (e.g., 90 days). |  |
| Storage Requirements (Replicated Data) | Storage for replicated data (based on replication factor). |  |
| Hot Warm Storage | Hot storage is for recent data available for searches; warm is data that is still searchable but older. |  |
| Cold Archived Storage | Long-term storage for rarely accessed data. |  |

**Key Considerations for Each Use Case:**

* **Low Volume Environment**: Ingests minimal data (~300 GB/day), so the system can run efficiently with 1-2 indexers and 1-2 search heads. Clustering is optional, depending on your redundancy needs. **Enterprise Security** and **ITSI** may not be major components but can still operate within the environment.
* **High Volume Environment**: Handles over 2 TB of daily ingestion. This demands more powerful infrastructure, typically 6-8 indexers and 3-4 search heads (plus extra for ES and ITSI). **Search head clustering** and **indexer clustering** are essential for high availability.
* **User-Heavy Environment**: A large number of users performing searches at once requires significant search head power. Planning for search concurrency (up to 500 users) means you'll need about 6-8 search heads, potentially more depending on the intensity of queries. This environment will also see an impact from **Enterprise Security** and **ITSI**, which add to resource usage.

A screenshot of a white sheet

Description automatically generated

A white grid with black text

Description automatically generated

A white rectangular box with black text

Description automatically generated

A white background with black text

Description automatically generated