Splunk License Management - Detailed Guide

Types of Splunk Licenses

1. Enterprise License
   - Full-featured license for production.
   - Based on daily ingest volume (e.g., 5GB/day, 100GB/day).
   - Includes distributed search, clustering, alerting, and advanced features.

2. Free License
   - Up to 500 MB/day indexing.
   - Limited features (no alerting, no authentication).

3. Trial License
   - Time-limited (60 days), full enterprise features.
   - Converts to Free license after expiry unless you apply a purchased one.

4. Developer/Developer Cloud Licenses
   - For learning, testing, non-production purposes.

Licensing Model

- Measured in GB/day of indexed data.
- License usage is calculated daily (midnight to midnight).
- Overuse for more than 5 times in 30 days results in a license violation - searches are disabled until resolved or reset by Splunk support.

License Manager

In distributed environments:
- A License Master centrally manages license usage.
- Other Splunk instances (Search Heads, Indexers) are license slaves.

License Master Responsibilities:

- Validate license pools.
- Track daily ingest volume per indexer.
- Manage license warnings/violations.
- Assign license pools to groups of indexers.

License Pools

License Pools allow partitioning of license volume across groups.

Use Cases:

- Assigning quotas to different departments or use cases.
- Controlling ingestion from specific sources or environments.

Each pool:

- Has a defined daily volume.
- Can have one or more indexers/search heads assigned.

Monitoring License Usage

Splunk provides several tools:

1. Monitoring Console (MC):
   - Navigate to: Settings > Licensing or MC > License Usage
   - View daily usage, pool usage, warnings, and violations.

2. Search Query:

```
   index=_internal source=*license_usage.log* type="Usage"
   | stats sum(b) as bytes by h
   | eval GB=round(bytes/1024/1024/1024,2)
   | sort -GB
```

   - Shows per-host license usage in GB.

3. Alerts:

   - Set alerts for nearing limits (e.g., 80% of quota).
   - Prevent surprise violations.

License Violation Handling

- Violations occur if ingestion exceeds quota 5 times in 30 days.
- In violation state:
  - Search functionality is disabled (except for internal logs).
  - Resolution:
    - Wait for 30-day window to shift.
    - Contact Splunk to reset violation state if critical.
    - Reduce data ingest (filter noisy sources, reduce logs).

Tips for Efficient License Management

- Filter data at UF/HF level (regex, props.conf).
- Deduplicate or throttle logs where possible.
- Use index-time parsing wisely to avoid ingest bloat.
- Monitor and regularly review ingestion by source/type.
- Split ingestion across pools for governance.

License Files

- License files are provided by Splunk in .lic format.
- Upload via: Settings > Licensing > Add License.
- Or use CLI:

```
  splunk add licenses /path/to/file.lic
```