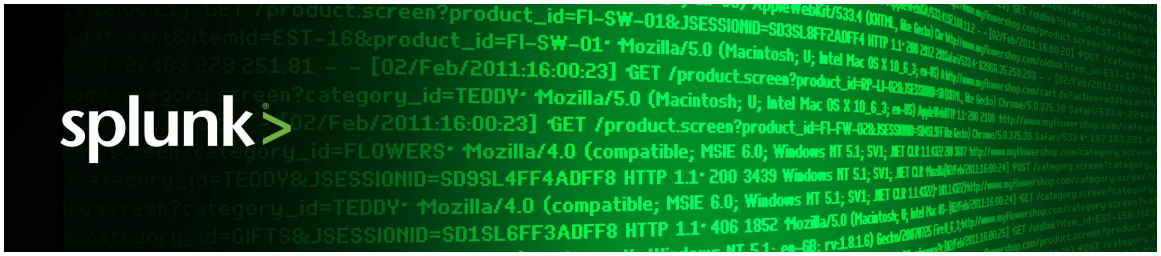

Splunk® Enterprise Knowledge Manager Manual 7.1.2

Develop naming conventions for knowledge objects

Generated: 8/17/2018 3:19 pm

Develop naming conventions for knowledge objects

As a best practice, develop naming conventions for your knowledge objects when it makes sense to do so. If the naming conventions you develop are followed consistently by all of the Splunk users in your organization, you will find that they become easier to use and that their purpose is much easier to discern at a glance.

You can develop naming conventions for just about every kind of knowledge object in your Splunk deployment. Naming conventions can help with object organization, but they can also help users differentiate between groups of reports, event types, and tags that have similar uses. And they can help identify a variety of things about the object that may not even be in the object definition, such as what teams or locations use the object, what technology it involves, and what it is designed to do.

Early development of naming conventions for your Splunk deployment will help you avoid confusion and chaos later on down the road.

Example - Set up a naming convention for reports

You work in the systems engineering group of your company, and as the knowledge manager for your Splunk deployment, it is your job to define a naming convention for the reports produced by your team.

You develop a naming convention that combines:

- **Group**: Corresponds to the working group(s) of the user saving the search.
- **Search type**: Indicates the type of search (alert, report, summary-index-populating).
- **Platform**: Corresponds to the platform subjected to the search.
- **Category**: Corresponds to the concern areas for the prevailing platforms.
- **Time interval**: The interval over which the search runs (or on which the search runs, if it is a scheduled search).
- **Description**: A meaningful description of the context and intent of the search, limited to one or two words if possible. Ensures the search name is unique.

Group	Search type	Platform	Category	Time interval	Description

SEG NEG OPS NOC	Alert Report Summary	Windows iSeries Network	Disk Exchange SQL Event log CPU Jobs Subsystems Services Security	<arbitrary>	<arbitrary>

Possible reports using this naming convention:

- SEG_Alert_Windows_Eventlog_15m_Failures
- SEG_Report_iSeries_Jobs_12hr_Failed_Batch
- NOC_Summary_Network_Security_24hr_Top_src_ip