The search command in Splunk allows users to retrieve events from indexes or filter the results of a previous search command in the pipeline. It can be used in a subsearch and can be applied to transform, filter, and report on the retrieved events. The search command supports IPv4 and IPv6 addresses and subnets that use CIDR notation. The syntax for the search command is logical-expression, with required arguments including keywords, time-opts, search-modifier, not, index-expression, comparison-expression, time-opts, comparison operators, field-value pairs, and index expression options. Comparison operators can be used to compare string values, numerically compare two numbers, or lexicographically compare other values. The search-modifier allows users to search for events from specified fields or field tags, such as hosts, sources, source types, saved searches, and event types. The search command is implied at the beginning of any search and can be used later in the search pipeline to filter results from previous commands.

Logical expression options

<comparison-expression>

Syntax: <field><comparison-operator><value> | <field> IN (<value-list>)

Description: Compare a field to a literal value or provide a list of values that can appear in the field.

<index-expression>

Syntax: "<string>" | <term> | <search-modifier>

Description: Describe the events you want to retrieve from the index using literal strings and search modifiers.

<time-opts>

Syntax: [<timeformat>] (<time-modifier>)...

Description: Describe the format of the starttime and endtime terms of the search. See Time options.

Comparison expression options

<comparison-operator>

Syntax: = | != | < | <= | > | >=

Description: You can use comparison operators when searching field/value pairs. Comparison expressions with the equal ( = ) or not equal ( != ) operator compare string values. For example, "1" does not match "1.0". Comparison expressions with greater than or less than operators < > <= >= numerically compare two numbers and lexicographically compare other values. See Usage.

<field>

Syntax: <string>

Description: The name of a field.

<value>

Syntax: <literal-value>

Description: In comparison-expressions, the literal number or string value of a field.

<value-list>

Syntax: (<literal-value>, <literal-value>, ...)

Description: Used with the IN operator to filter events by specifying two or more values. For example use error IN (400, 402, 404, 500) instead of error=400 OR error=402 OR error=404 OR error=500. You can also use a wildcard character ( \* ) to specify values that are similar, such as error IN (40\*).

See the "Multiple field-value comparisons with the IN operator" section in Usage.

Index expression options

<string>

Syntax: "<string>"

Description: Specify keywords or quoted phrases to match. When searching for strings and quoted strings (anything that's not a search modifier), Splunk software searches the \_raw field for the matching events or results.

<search-modifier>

Syntax: <sourcetype-specifier> | <host-specifier> | <hosttag-specifier> | <source-specifier> | <savedsplunk-specifier> | <eventtype-specifier> | <eventtypetag-specifier> | <splunk\_server-specifier>

Description: Search for events from specified fields or field tags. For example, search for one or a combination of hosts, sources, source types, saved searches, and event types. Also, search for the field tag, with the format: tag::<field>=<string>.

Read more about searching with default fields in the Knowledge Manager manual.

Read more about using tags and field aliases in the Knowledge Manager manual.

<sourcetype-specifier>

Syntax: sourcetype=<string>

Description: Search for events from the specified sourcetype field.

<host-specifier>

Syntax: host=<string>

Description: Search for events from the specified host field.

<hosttag-specifier>

Syntax: hosttag=<string>

Description: Search for events that have hosts that are tagged by the string.

<eventtype-specifier>

Syntax: eventtype=<string>

Description: Search for events that match the specified event type.

<eventtypetag-specifier>

Syntax: eventtypetag=<string>

Description: Search for events that would match all eventtypes tagged by the string.

<savedsplunk-specifier>

Syntax: savedsearch=<string> | savedsplunk=<string>

Description: Search for events that would be found by the specified saved search.

<source-specifier>

Syntax: source=<string>

Description: Search for events from the specified source field.

<splunk\_server-specifier>

Syntax: splunk\_server=<string>

Description: Search for events from a specific server. Use "local" to refer to the search head.

Time options

For a list of time modifiers, see Time modifiers for search.

<timeformat>

Syntax: timeformat=<string>

Description: Set the time format for starttime and endtime terms.

Default: timeformat=%m/%d/%Y:%H:%M:%S.

<time-modifier>

Syntax: starttime=<string> | endtime=<string> | earliest=<time\_modifier> | latest=<time\_modifier>

Description: Specify start and end times using relative or absolute time.

You can also use the earliest and latest attributes to specify absolute and relative time ranges for your search. For more about this time modifier syntax, see Specify time modifiers in your search in the Search Manual.

starttime

Syntax: starttime=<string>

Description: Events must be later or equal to this time. Must match timeformat