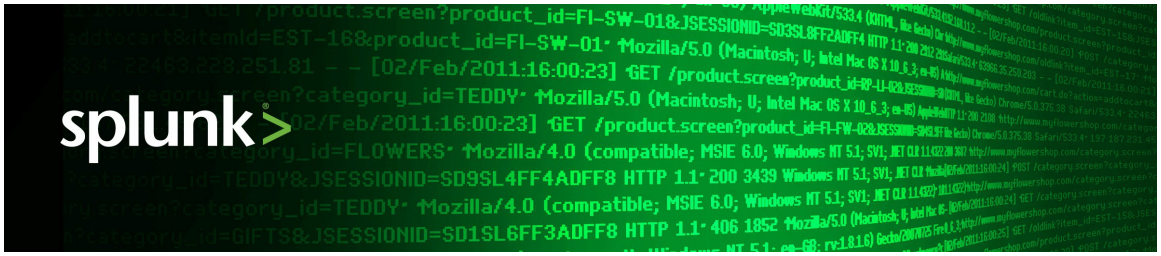

Splunk® Investigate Search Reference Current

search command examples

Generated: 10/09/2019 11:53 pm

search command examples

The following are basic examples for using the `search` command.

1. Field-value pair matching

This example shows field-value pair matching for specific values of source IP (src) and destination IP (dst).

```
search src="10.9.165.*" OR dst="10.9.165.8"
```

2. Using boolean and comparison operators

This example shows field-value pair matching with boolean and comparison operators. This example searches for events with code values of either 10, 29, or 43 and any `host` that is not "localhost", and an `xqp` value that is greater than 5.

```
search (code=10 OR code=29 OR code=43) host!="localhost" xqp>5
```

An alternative is to use the IN operator, because you are specifying multiple field-value pairs on the same field. The revised search is:

```
search code IN(10, 29, 43) host!="localhost" xqp>5
```

3. Using wildcards

This example shows field-value pair matching with wildcards. This example searches for events from all of the web servers that have an HTTP client and server error status.

```
search host=webserver* (status=4* OR status=5*)
```

An alternative is to use the IN operator, because you are specifying two field-value pairs on the same field. The revised search is:

```
search host=webserver* status IN(4*, 5*)
```

4. Using the IN operator

This example shows how to use the IN operator to specify a list of field-value pair matchings. In the events from an access.log file, search the `action` field for the

values `addtocart` or `purchase`.

```
search sourcetype=access_combined_wcookie action IN (addtocart,
purchase)
```

5. Using the NOT or != comparisons

Searching with the boolean "NOT" comparison operator is not the same as using the "!=" comparison.

The following search returns everything except fieldA="value2", including all other fields.

```
search NOT fieldA="value2"
```

The following search returns events where fieldA exists and does not have the value "value2".

```
search fieldA!="value2"
```

If you use a wildcard for the value, `NOT fieldA=*` returns events where fieldA is null or undefined, and `fieldA!=*` never returns any events.