**Splunk Lookups**

Lookup tables use information in your events to determine how to add other fields from external data sources such as static tables (CSV files)

*Example:*

An example of this functionality would be a CSV lookup that takes the http\_status value in an event, matches that value with its definition in a CSV file, and then adds that definition to the event as the value of a newstatus\_description field. So if you have an event where http\_status = 503 the lookup would addstatus\_description = Service Unavailable, Server Error to that event.

**Steps in managing Lookup**

* List existing lookup tables or upload a new file.
* Edit existing lookup definitions or define a new file-based or external lookup.
* Edit existing automatic lookups or configure a new lookup to run automatically.

***Adding Lookup via UI***

<http://docs.splunk.com/Documentation/Splunk/latest/Knowledge/Usefieldlookupstoaddinformationtoyourevents>

***Configure Lookup via backend***

<http://docs.splunk.com/Documentation/Splunk/6.4.1/Knowledge/ConfigureCSVlookups#Prefilter_large_CSV_lookup_tables>

***Steps***

1. Add your lookup to anyone of the below place

$SPLUNK\_HOME/etc/system/lookups

$SPLUNK\_HOME/etc/apps/<app\_name>/lookups

1. Define your lookup in transforms

If you want the lookup to be available globally, add its lookup stanza to the version of transforms.conf in $SPLUNK\_HOME/etc/system/local/.

If you want the lookup to be specific to a particular app, add its stanza to the version of transforms.conf in $SPLUNK\_HOME/etc/apps/<app\_name>/local/.

The CSV lookup stanza names the lookup table and provides the name of the CSV file that the lookup uses. It uses these required attributes.

**[<lookup\_name>]** The name of the lookup.

**filename = <string>**The name of the CSV file that the lookup references.

**Custom your transform based on your requirement**

[mylook]

filename = mytable.csv

max\_matches = 1

min\_matches = 1

default\_match = nothing

filter = id<500 AND color="red"

match\_type = WILDCARD(msgId,msg)

case\_sensitive\_match=false

1. Make your lookup automatic using props

When you create a lookup configuration in transforms.conf, you invoke it by running searches that reference it. However, you can optionally create an additional props.conf configuration that makes the lookup "automatic." This means that it runs in the background at search time and automatically adds output fields to events that have the correct match fields.

**[<stanza name>]**

**LOOKUP-<class> = $TRANSFORM <match\_field\_in\_lookup\_table> AS <match\_field\_in\_event>OUTPUT|OUTPUTNEW <output\_field\_from\_lookup\_table> AS <output\_field\_in\_event>**

If you do not include an OUTPUT|OUTPUTNEW clause, Splunk software adds all the field names and values from the lookup table to your events. When you use OUTPUTNEW, Splunk software can add only the output fields that are "new" to the event. If you use OUTPUT, output fields that already exist in the event are overwritten.

**Lookup commands**

**lookup**

http://docs.splunk.com/Documentation/Splunk/6.4.1/SearchReference/Lookup

sourcetype=access\_\* | lookup status\_desc status OUTPUT description | stats count by description

**inputlookup**

http://docs.splunk.com/Documentation/Splunk/6.4.1/SearchReference/Inputlookup

| inputlookup append=t usertogroup

| inputlookup kvstorecoll\_lookup where (CustID>500) AND (CustName="P\*") | stats count

**outputlookup**

<http://docs.splunk.com/Documentation/Splunk/6.4.1/SearchReference/Outputlookup>

| outputlookup users.csv

**inputcsv**

| inputcsv students.csv WHERE (age>=13 age<=19) AND NOT age=16 | stats count

http://docs.splunk.com/Documentation/Splunk/6.4.1/SearchReference/Inputcsv

**outputcsv**

| outputcsv mysearch

http://docs.splunk.com/Documentation/Splunk/6.4.1/SearchReference/Outputcsv

**Difference between lookup and csv**

There is a major difference. outputlookup will use the defined transforms or the filename you give it and put the CSV file in the lookups folder of the current App context. You can use this lookup in other commands using the lookup command. Changes to the lookup are replicated on the SHC.

outputcsv just dumps the CSV to the file system in $SPLUNK\_HOME/var/run/splunk/. You can't use it later, and changes are not replicated in a SHC.