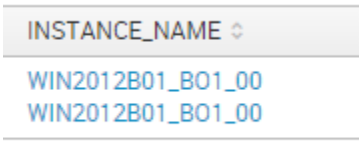
Duplicate instance name in Splunk

Problem:

source!=audittrail EVENT_TYPE=SM51 | dedup INSTANCE_NAME | sort+INSTANCE_NAME | fields INSTANCE_NAME | table INSTANCE_NAME



INSTANCE_NAME
WIN2012B01_BO1_00
WIN2012B01_BO1_00

Condition:

- Distributed Splunk Environment where search head and indexer are running on different systems

Cause:

Sourcetype SAP_ABAP has not been configured in search head properly.

Solution:

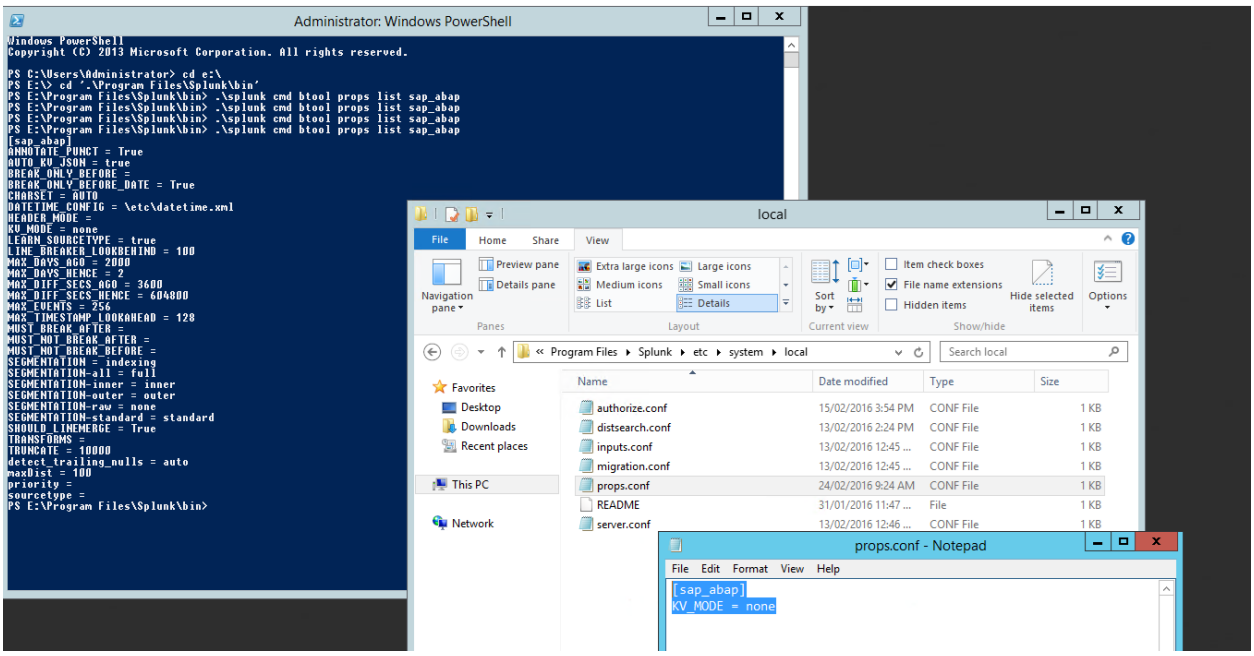
- Locate props.conf in SPLUNK_HOME\etc\system\local

If the file does not exist, please create it

- Add attribute KV_MODE = none to sourcetype.

[sap_abap]

KV_MODE = none



- Restart the search head
- The above query should return one result

Reference

http://docs.splunk.com/Documentation/Splunk/6.2.2/admin/Propsconf

```
KV_MODE = [none|auto|auto_escaped|multi|json|xml]
* Used for search-time field extractions only.
* Specifies the field/value extraction mode for the data.
* Set KV_MODE to one of the following:
        * none: if you want no field/value extraction to take place.
        * auto: extracts field/value pairs separated by equal signs.
        * auto_escaped: extracts fields/value pairs separated by equal signs and honors \" and \\
          as escaped sequences within quoted values, e.g field="value with \"nested\" quotes"
        * multi: invokes the multikv search command to expand a tabular event into multiple events.
        * xml : automatically extracts fields from XML data.
        * json: automatically extracts fields from JSON data.
* Setting to 'none' can ensure that one or more user-created regexes are not overridden by
  automatic field/value extraction for a particular host, source, or source type, and also
  increases search performance.
* Defaults to auto.
* The 'xml' and 'json' modes will not extract any fields when used on data that isn't of the
  correct format (JSON or XML).
```