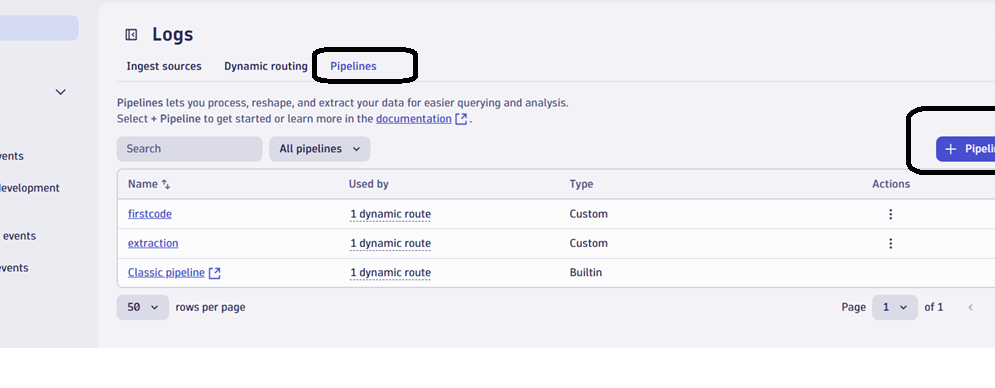
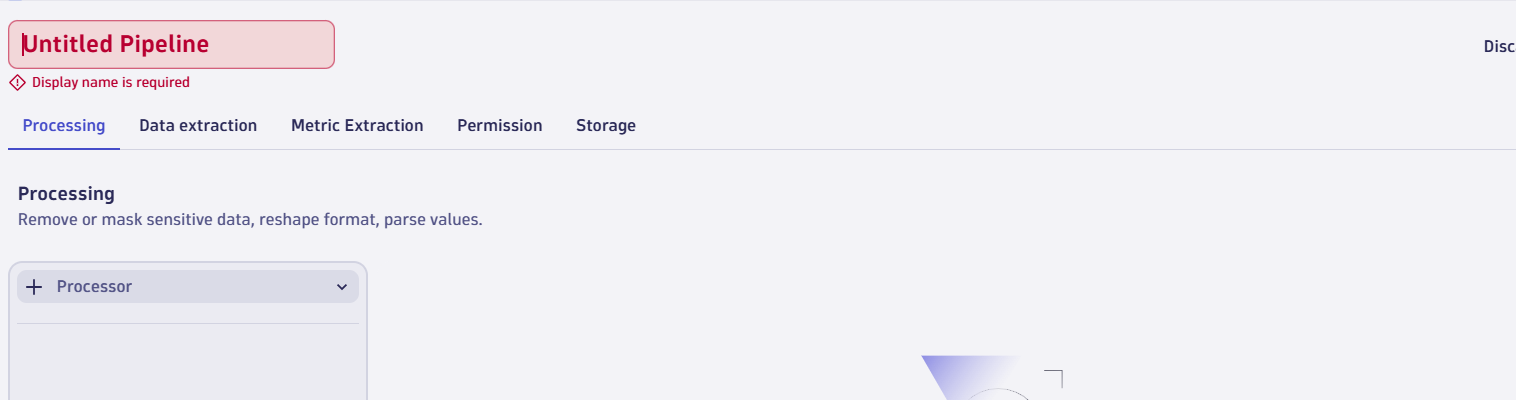
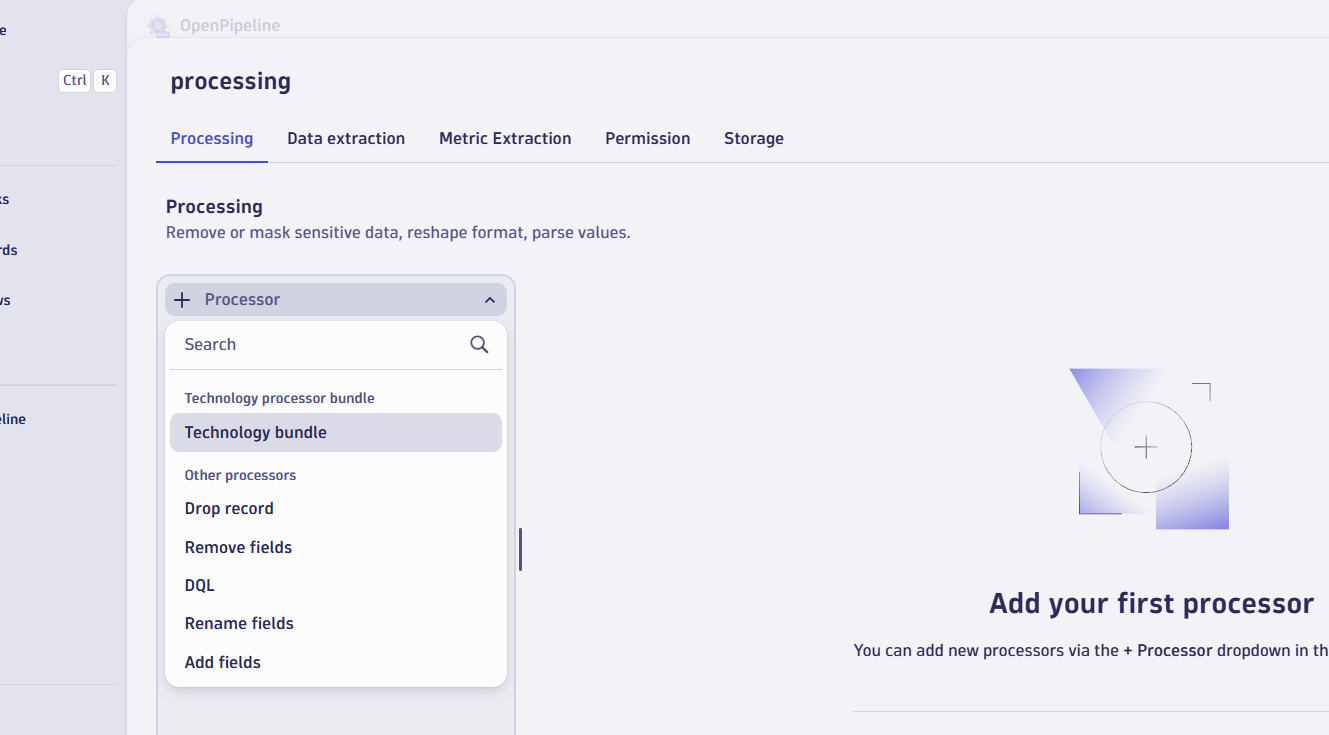
Lab:

1. Go to OpenPipeline  and find the pipeline for the record source (or create a new pipeline).
2. Select the stage.







configure a DQL processor in the Processing stage with a DQL processor definition copied from one of the following:

Provide a name and , DQL section

parse content, "

'['

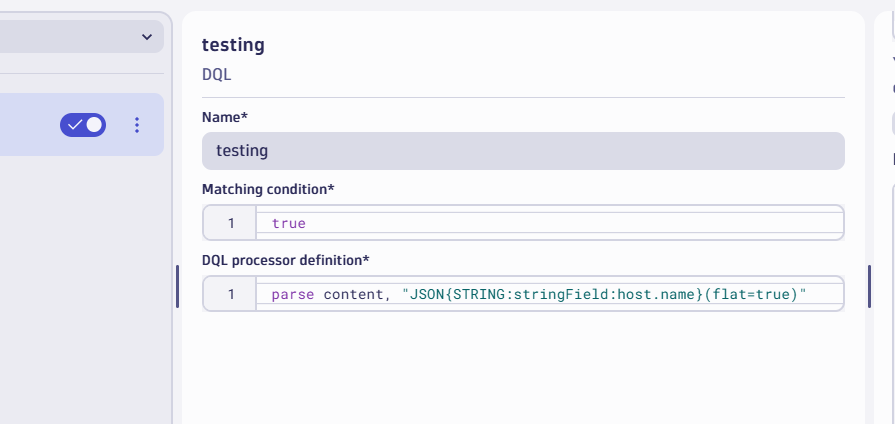
TIMESTAMP('yyyy-MM-dd HH:mm:ssZ'):timestamp

']'

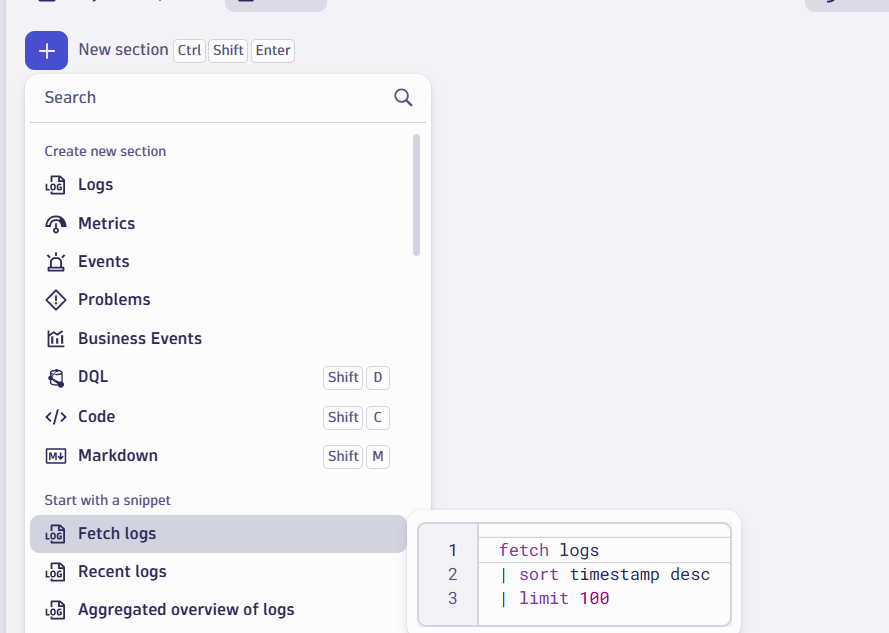
SPACE

LD:message

"



sample data copy from notebook section: Open new tab



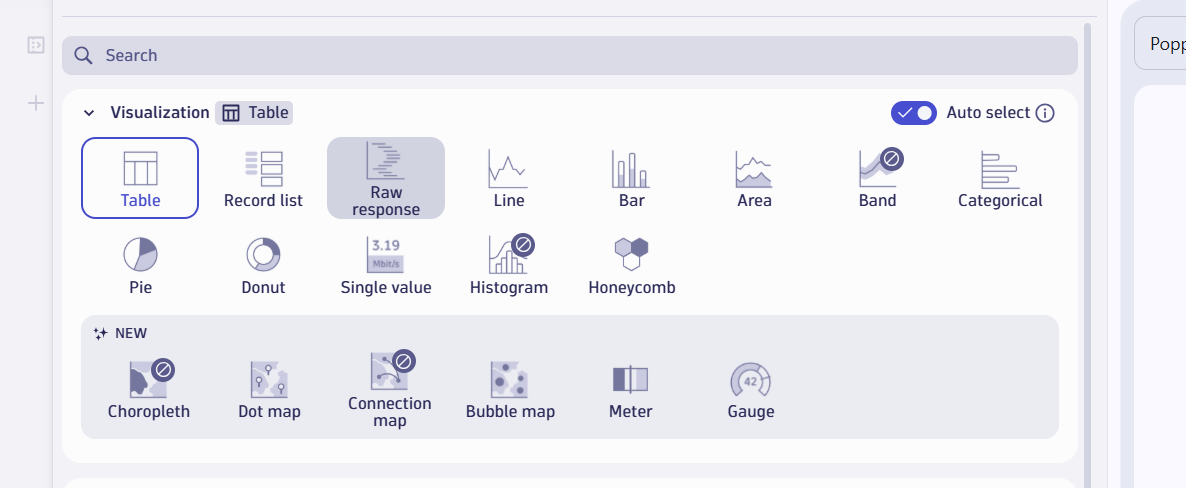
Fetch only one record

fetch logs

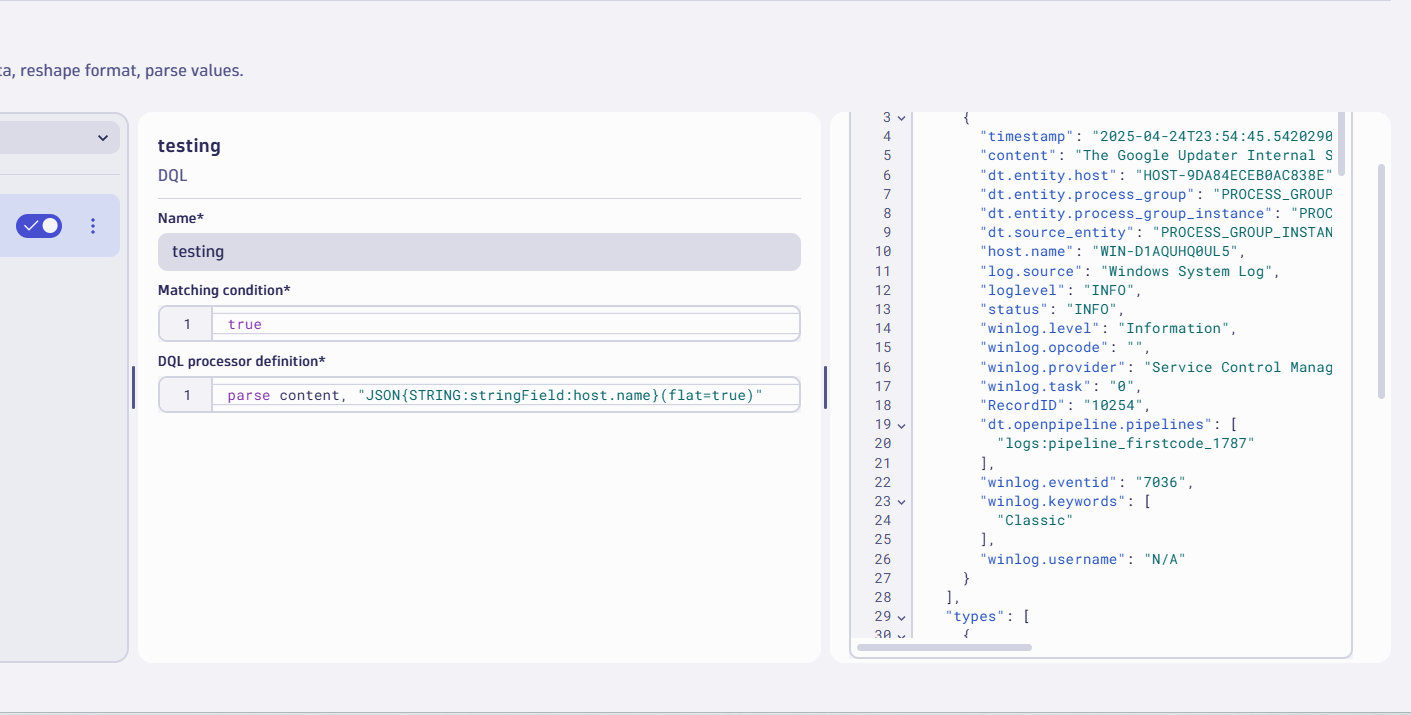
| sort timestamp desc

| limit 1

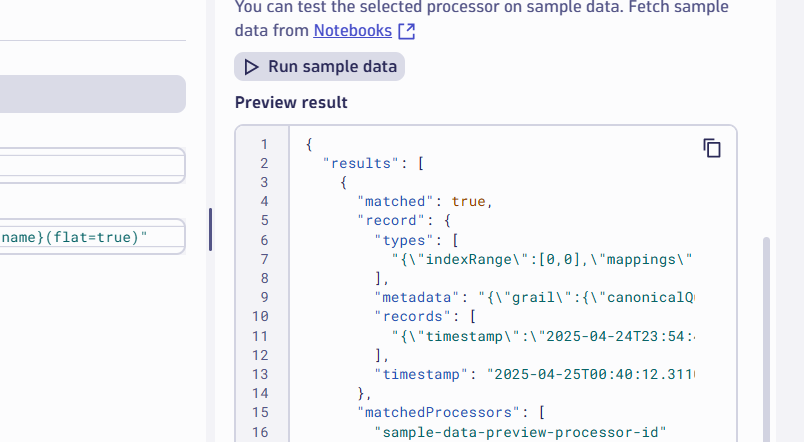
Convert data in raw format



Copy the sample to openpipeline



Click on “Run sample data



Run other query also and check

parse content, "JSON:parsedJson"

| fieldsAdd new.field1 = parsedJson[RecordID],

new.field2 = parsedJson[host.name],

new.field3 = parsedJson[winlog][provider],

new.field4 = parsedJson[winlog][username]

| fieldsRemove parsedJson