

Loading Musicbrainz in Splunk

Refer to the https://musicbrainz.org/doc/MusicBrainz_Database for the Original setup

First part - Install and setup "Splunk DB Connect"

Afterwards, make sure JAVA is configed:

● JRE Status:

JRE Installation Path (JAVA_HOME)
Only Java SE 8 is supported. [Learn More](#)

JVM Options
Java Virtual Machine parameters. [Learn More](#)

RPC Server Port
DB Connect RPC server port. [Learn More](#)

RPC Server SSL

add the [Postgres JDBC](#) driver and check the Config:

Settings		
General Settings Drivers Usage Collection		
Driver	Installed?	Version Number
AWS RDS Aurora	✓	5.1
DB2	✗	-
MS-SQL Server Using MS Generic Driver	✗	-
MS-SQL Server Using MS Generic Driver With Kerberos Authentication	✗	-
MS-SQL Server Using MS Generic Driver With Windows Authentication	✗	-
Hive	✗	-
HyperSQL	✗	-
Informix	✗	-
MemSQL	✓	5.1
MS-SQL Server Using TDS Driver	✗	-
MS-SQL Server Using TDS Driver With Windows Authentication	✗	-
MySQL	✓	5.1
Oracle	✗	-
Oracle Service	✗	-
Postgresql	✓	9.4
AWS RedShift	✗	-
Spark SQL	✗	-
Sybase ASE (jConnect)	✗	-
Sybase IQ (jConnect)	✗	-
Sybase SQL Anywhere (jConnect)	✗	-
Teradata	✗	-

Now, the core part is done.

Then setup Identities and Connection - this is pretty basic



Remember to make sure the Databases You are connecting to are listening on 0.0.0.0 and NOT 127.0.0.1 - The 127.0.0.1 is typically default for Postgres and MySQL

splunk>

App: Splunk DB Connect

Explorer

Operations

Health

Settings

Search

RPC Service: Up

Filter by name

Splunk DB Connect

Identities

confluence

musicbrainz

Connections

confluence

musicbrainz

Connection: musicbrainz

Edit

Query

Valid connection

Status

Enabled

Disabled

Connection Name

musicbrainz

App

Splunk DB Connect

Host

77.243.52.155

Database Types

Postgresql

Default Database

musicbrainz

JDBC URL Format

jdbc:postgresql://77.243.52.155:5432/n

Identity

musicbrainz

Port

5432

Fetch Size

Enable SSL

Readonly

Clone

Delete

The number of rows to return at a time from the database. Default is 300.

This is a DB driver flag, and may not be supported for all JDBC drivers.

This is a DB driver flag and cannot always guarantee read-only access. Use a read-only database user account to ensure that data cannot be altered.

Generated JDBC URL:

jdbc:postgresql://77.243.52.155:5432/musicbrainz?user=musicbrainz&password=hu8jmn3

Permissions

Sharing

App

All Apps

	Read	Write
Everyone		
admin		
can_delete		
db_connect_admin		
db_connect_user		
power		
sc_admin		
splunk-system-role		
user		

Collapse Permissions

Cancel

Validate

Save

Referring to the previous ELK setup, we use the same query:

```

SELECT DISTINCT * FROM (
SELECT
    release_group.gid AS album_id,
    release_group.type AS album_primary_type_id,
    release_group_primary_type.name AS album_primary_type_name,
    release.name AS release_name,
    artist.name AS artist_name,
    artist.gid AS artist_gid,
    artist_credit.id AS artist_credit_id,
    artist.type AS artist_type_id,
    artist_type.name AS artist_type_name,
    artist.begin_date_year AS artist_begin_date_year,
    area.name AS artist_country_name,
    release_country.date_year AS release_year,
    release_country.date_month AS release_month,
    release_country.date_day AS release_day
FROM
    musicbrainz.artist
INNER JOIN musicbrainz.artist_credit_name
    ON artist_credit_name.artist = artist.id
INNER JOIN musicbrainz.artist_credit
    ON artist_credit.id = artist_credit_name.artist_credit
INNER JOIN musicbrainz.release_group
    ON release_group.artist_credit = artist_credit.id
INNER JOIN musicbrainz.release
    ON release.release_group = release_group.id
INNER JOIN musicbrainz.release_country
    ON release.id = release_country.release
INNER JOIN musicbrainz.artist_type
    ON artist.type = artist_type.id
INNER JOIN musicbrainz.area
    ON artist.area = area.id
INNER JOIN musicbrainz.release_group_primary_type
    ON release_group_primary_type.id = release_group.type
WHERE
    ((release_country.date_year IS NOT NULL) AND
    (release_country.date_month IS NOT NULL) AND
    (release_country.date_day IS NOT NULL))
) As Dummy2

```

To get a preview:

Editor Mode

Max Rows 100 Format SQL Save As Execute

```

1 SELECT Distinct * FROM (
2 SELECT
3     release_group.gid AS album_id,
4     release_group.type AS album_primary_type_id,
5     release_group.primary_type.name AS album_primary_type_name,
6     release.name AS release_name,
7     artist.name AS artist_name,
8     artist.gid AS artist_gid,
9     artist_credit.id AS artist_credit_id,
10    artist.type AS artist_type_id,
11    artist.type.name AS artist_type_name,
12    artist.begin_date_year AS artist_begin_date_year,
13    area.name AS artist_country_name,
14    release_country.date_year AS release_year,
15    release_country.date_month AS release_month,
16    release_country.date_day AS release_day
17 FROM
18     musicbrainz.artist
19 INNER JOIN musicbrainz.artist_credit_name
20     ON artist_credit_name.artist = artist.id
21 INNER JOIN musicbrainz.artist_credit
22     ON artist_credit.id = artist_credit_name.artist_credit
23 INNER JOIN musicbrainz.release_group
24     ON release_group.artist_credit = artist_credit.id
25 INNER JOIN musicbrainz.release
26     ON release.release_group = release_group.id
27 INNER JOIN musicbrainz.release_country
28     ON release.id = release_country.release
29 INNER JOIN musicbrainz.artist_type
30     ON artist.type = artist_type.id
31 INNER JOIN musicbrainz.area
32     ON artist.area = area.id
33 INNER JOIN musicbrainz.release_group_primary_type
34     ON release_group.primary_type.id = release_group.type
35 WHERE
36     ((release_country.date_year IS NOT NULL) AND
37     (release_country.date_month IS NOT NULL) AND
38     (release_country.date_day IS NOT NULL))
39 ) AS Dummy2

```

100 rows

10 per Page

< prev

1

2

3

4

5

6

7

8

9

10

next >

	album_id	album_primary_type_id	album_primary_type_name	release_name	artist_name	artist_gid	artist_credit_id	artist_type_id	artist_type_name	artist_begin_date_year
1	00000519-f708-35a3-be4e-cbe552ece701	1	Album	So Alone	Johnny Thunders	3b14b1a7-2235-4fcf-a718-383beb79e856	4645	1	Person	195
2	00000519-f708-35a3-be4e-cbe552ece701	1	Album	So Alone	Johnny Thunders	3b14b1a7-2235-4fcf-a718-383beb79e856	4645	1	Person	195
3	000079f9-f34c-3713-97c0-b22ca5010087	2	Single	The X-Files Theme (remix)	Mark Snow	a1d3685a-c61d-49aa-a294-bcfc29e516b5	2483	1	Person	194
4	000079f9-f34c-3713-97c0-b22ca5010087	2	Single	The X-Files Theme	Mark Snow	a1d3685a-c61d-49aa-a294-bcfc29e516b5	2483	1	Person	194
5	000079f9-f34c-3713-97c0-b22ca5010087	2	Single	The X-Files Theme	Mark Snow	a1d3685a-c61d-49aa-a294-bcfc29e516b5	2483	1	Person	194
6	0000aae9-737f-31bf-a9f0-6b7c3297ab1d	1	Album	Hier kommt Ärger!	Betontod	9ae757bc-89bb-45b7-800c-00959ea371dd	169642	2	Group	195
7	0000bbd3-8d64-4edc-88ac-f4c7b701849f	2	Single	Sea of Flags	Jessica Mauboy	18f719e7-e9b4-4216-8869-9083ebc23f7d	571185	1	Person	196
8	0000d1ef-cbe5-398e-846f-7eff1a364cef	2	Single	It's My Life	No Doubt	fb42a255-1d57-4d31-ac11-65b671c19958	464	2	Group	198
9	0000d1ef-cbe5-398e-846f-7eff1a364cef	2	Single	It's My Life / Bathwater (The Remixes)	No Doubt	fb42a255-1d57-4d31-ac11-65b671c19958	464	2	Group	198
10	0000d1ef-cbe5-398e-846f-7eff1a364cef	2	Single	It's My Life	No Doubt	fb42a255-1d57-4d31-ac11-65b671c19958	464	2	Group	198

Where [Logstash](#) only gave us the possibility to "bulk" upload the Query result to Elasticsearch - "[Splunk DB Connect](#)" gives us 3 options:



This is where Splunk in my Opinion "runs over" the ELK stack - There are more GUI and both inputs (as Logstash) and on-the-fly lookup 😊

DB Inputs

DB Inputs are "equal" to the Logstash approach, load the Query result into Splunk as "log lines":

DB Input: Releases

Name Input

Status

Enabled Disabled

Name

Releases

Description

App

Splunk DB Connect

Connection

musicbrainz

Valid connection

Set Parameters

Input Type

Batch Input

Max Rows to Retrieve

100000

Error on integer between 1 and 1000000.

Fetch Size

The number of rows to return at a time from the database. Default is 300.

Timestamp

Current Index Time

Choose Columns

Output Timestamp Format

yyyy-MM-dd HH:mm:ss

Execution Frequency

40 s ***

Enter seconds or a valid cron string.

Metadata

Source

releases

Source type

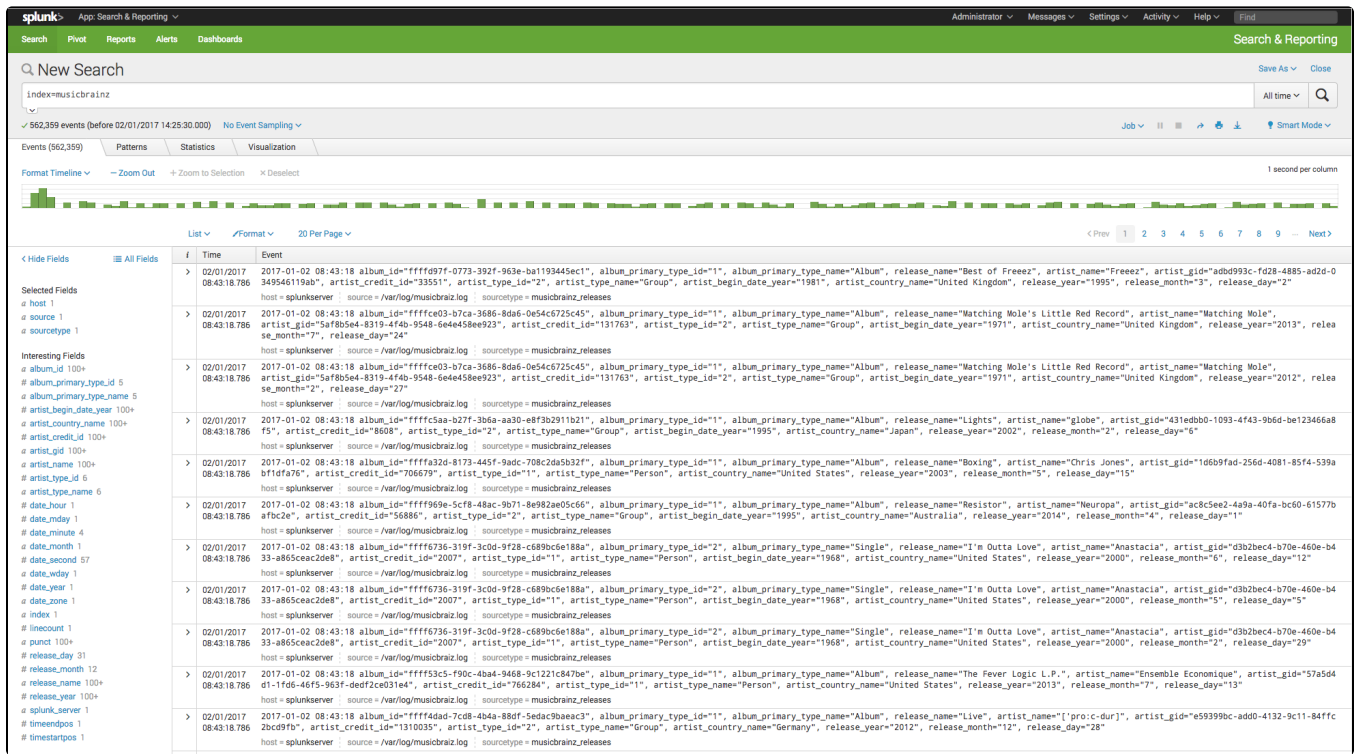
musicbrainz_releases

Index

releases

Select Resource Pool

Gives the loglines:



DB Outputs

DB Lookups