Import Logger Event Data Into Recon

1. Install VSQL Client Driver on Logger

Download the VSQL Client Tar package.

https://www.vertica.com/download/vertica/client-drivers/

Extract the tar package

```
tar xvfz vertica-client-[version] [OS].tar.gz -C /
```

Modify the profile

```
cd ~
vi .bashrc
```

Include /opt/vertica/bin into the PATH environment variable

```
# User specific aliases and functions

alias rm='rm -i'
alias cp='cp -i'
alias mv='mv -i'

# Source global definitions
if [ -f /etc/bashrc ]; then
        . /etc/bashrc
fi
export PATH=/opt/vertica/bin:$PATH
```

Save the .bashrc file, reload the profile

```
source .bashrc
```

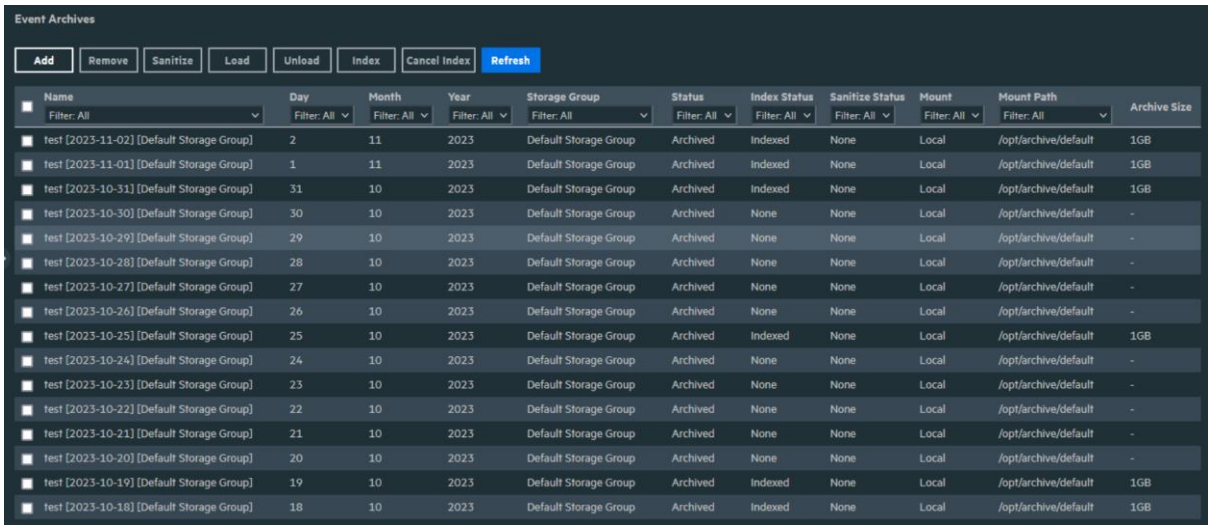
Verify VSQL is installed correct.

```
[root@logger ~]# vsql --version
vsql version 23.04.0000, built for Linux64, contains support for command-line
editing
```

2. Archive Live Logger Data

Configure event archives on logger.

Following screen shot show the archives from 2023-10-18 to 2023-11-2 for Default Storage Group. The archives are stored in /opt/archive/default



Name	Day	Month	Year	Storage Group	Status	Index Status	Sanitize Status	Mount	Mount Path	Archive Size
test [2023-11-02] [Default Storage Group]	2	11	2023	Default Storage Group	Archived	Indexed	None	Local	/opt/archive/default	1GB
test [2023-11-01] [Default Storage Group]	1	11	2023	Default Storage Group	Archived	Indexed	None	Local	/opt/archive/default	1GB
test [2023-10-31] [Default Storage Group]	31	10	2023	Default Storage Group	Archived	Indexed	None	Local	/opt/archive/default	1GB
test [2023-10-30] [Default Storage Group]	30	10	2023	Default Storage Group	Archived	None	None	Local	/opt/archive/default	-
test [2023-10-29] [Default Storage Group]	29	10	2023	Default Storage Group	Archived	None	None	Local	/opt/archive/default	-
test [2023-10-28] [Default Storage Group]	28	10	2023	Default Storage Group	Archived	None	None	Local	/opt/archive/default	-
test [2023-10-27] [Default Storage Group]	27	10	2023	Default Storage Group	Archived	None	None	Local	/opt/archive/default	-
test [2023-10-26] [Default Storage Group]	26	10	2023	Default Storage Group	Archived	None	None	Local	/opt/archive/default	-
test [2023-10-25] [Default Storage Group]	25	10	2023	Default Storage Group	Archived	Indexed	None	Local	/opt/archive/default	1GB
test [2023-10-24] [Default Storage Group]	24	10	2023	Default Storage Group	Archived	None	None	Local	/opt/archive/default	-
test [2023-10-23] [Default Storage Group]	23	10	2023	Default Storage Group	Archived	None	None	Local	/opt/archive/default	-
test [2023-10-22] [Default Storage Group]	22	10	2023	Default Storage Group	Archived	None	None	Local	/opt/archive/default	-
test [2023-10-21] [Default Storage Group]	21	10	2023	Default Storage Group	Archived	None	None	Local	/opt/archive/default	-
test [2023-10-20] [Default Storage Group]	20	10	2023	Default Storage Group	Archived	None	None	Local	/opt/archive/default	-
test [2023-10-19] [Default Storage Group]	19	10	2023	Default Storage Group	Archived	Indexed	None	Local	/opt/archive/default	1GB
test [2023-10-18] [Default Storage Group]	18	10	2023	Default Storage Group	Archived	Indexed	None	Local	/opt/archive/default	1GB

Note: You must make sure the archiving job is executed continuously every day during the whole time frame. If there is a break during the time frame, for example, archiving job is not run on Oct 17th . In this case, the logger data migration will NOT be successful.

3. Execute the Construct Mounts Instructions Script on logger

Copy the script /opt/arcsight-db-tools/scripts/loggerToReconConstructMounts.sh from Vertica host to logger host, then execute

```
./loggerToReconConstructMounts.sh $<INSTALL LOGGER PATH>
```

In following example, the logger software is installed on host 10.0.0.4 under /opt/logger folder.

```
[root@logger opt]# ./loggerToReconConstructMounts.sh /opt/logger
=====================================================================
**       Instructions to create the mount on Vertica side         **
=====================================================================

Getting the instructions for /opt/archive/default
Before mounting the archive on all nodes in the database, ensure that you configure the
following folder as an NFS server: [/opt/archive/default]
mkdir -p /opt/LOGGER_10004/opt/archive/default
mount -t nfs 10.0.0.4:/opt/archive/default /opt/LOGGER_10004/opt/archive/default



IMPORTANT: The dbuser must be able to access to the data. Please check, and update as needed,
the ownership of the archive directory.
setfacl -R -m u:DB_USER:rwX /opt/LOGGER_10004
NOTE: If it is a multi-node installation please run the following command on each Vertica
node.
/opt/vertica/bin/vsql -U DB_USER -w DB_PASSWORD -c "SELECT
default_secops_adm.AddLoggertoKnownHosts ('10.0.0.4','/home/dbadmin/known_loggers', true);"
```

Above script does NOT execute any command, it just generate the command need to be executed on vertica DB host and logger host.

Following command need to run from vertica host:

```
mkdir -p /opt/LOGGER_10004/opt/archive/default
mount -t nfs 10.0.0.4:/opt/archive/default /opt/LOGGER_10004/opt/archive/default
```

Following command need to run on logger host (Note: there is a critical error in the output of above script, this setfacl command MUST run on the logger host, and the folder should be the logger archiving folder (/opt/archive/logger in this example)

```
setfacl -R -m u:DB_USER:rwX /opt/archive/logger
```

4. Create NFS share on logger and set the right permission

On logger, install nfs package

```
yum install nfs-utils
```

Create /etc/exports file with following content (/opt/archive/default in the logger archive folder in this example)

```
/opt/archive/default  *(rw,sync,no_all_squash,root_squash)
```

Export NFS share

```
exportfs -r
```

Check NFS share

```
[root@logger opt]# showmount -e
Export list for logger.arcsight.example.com:
/opt/archive/default *
```

Allow dbadmin user from vertica host to visit archive files (The user id of dbadmin user is 1999 in following example)

```
setfacl -R -m u:1999:rwX /opt/archive/logger
```

5. Execute the Instructions in ArcSight Database

Create logger migration schema in Vertica DB

```
[root@intelligence ~]# /opt/arcsight-db-tools/scripts/logger_migration_preconfig.sh
NOTICE 4185:  Nothing was dropped
CREATE LIBRARY
CREATE FUNCTION
CREATE FUNCTION
CREATE FUNCTION
CREATE FUNCTION
CREATE FUNCTION
CREATE FUNCTION
GRANT PRIVILEGE
WARNING 6978:  Table "logger_migration_data" will include privileges from schema
"default_secops_adm"
CREATE TABLE
NOTICE 8778:  Duplicate column name; nothing was done
ALTER TABLE
NOTICE 8778:  Duplicate column name; nothing was done
ALTER TABLE
NOTICE 8778:  Duplicate column name; nothing was done
ALTER TABLE
NOTICE 8778:  Duplicate column name; nothing was done
ALTER TABLE
NOTICE 8778:  Duplicate column name; nothing was done
ALTER TABLE
NOTICE 8778:  Duplicate column name; nothing was done
ALTER TABLE
NOTICE 8778:  Duplicate column name; nothing was done
ALTER TABLE
NOTICE 8778:  Duplicate column name; nothing was done
ALTER TABLE
WARNING 6978:  Table "logger_connection" will include privileges from schema
"default_secops_adm"
CREATE TABLE
NOTICE 8778:  Duplicate column name; nothing was done
ALTER TABLE
WARNING 6978:  Table "logger_audit_log" will include privileges from schema
"default_secops_adm"
CREATE TABLE
WARNING 6978:  Table "logger_udx_settings" will include privileges from schema
"default_secops_adm"
```

```
CREATE TABLE

NOTICE 8778:  Duplicate column name; nothing was done

ALTER TABLE

WARNING 6978:  Table "logger_deletion_events_data" will include privileges from schema
"default_secops_adm"

CREATE TABLE

WARNING 6978:  Table "logger_metadata_migrations" will include privileges from schema
"default_secops_adm"

CREATE TABLE

COMMIT
```

Mount the NFS share exported by logger host, following command are generated in step 3, you can just copy it.

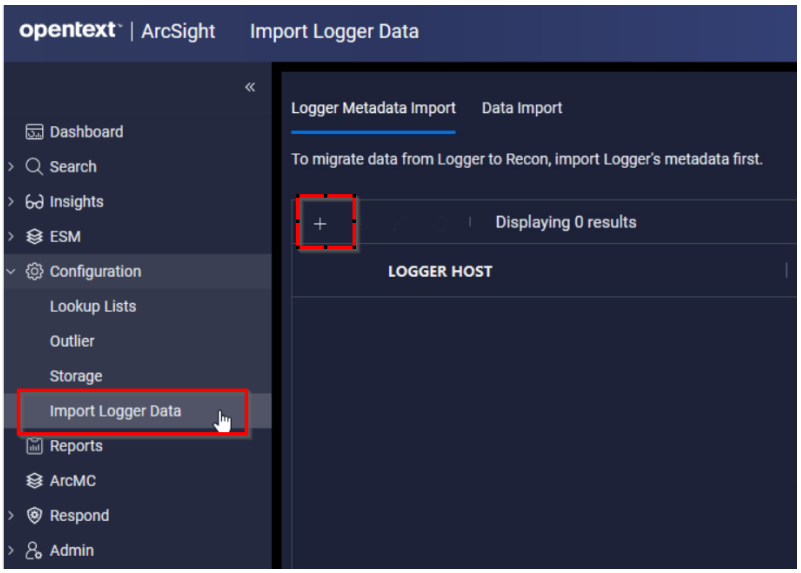
```
mkdir -p /opt/LOGGER_10004/opt/archive/default

mount -t nfs 10.0.0.4:/opt/archive/default /opt/LOGGER_10004/opt/archive/default
```

Verify if dbadmin user is able to read the archiving files

```
[root@intelligence ~]# su - dbadmin

[dbadmin@intelligence ~]$ cd /opt/LOGGER_10004/opt/archive/default/648518346341351424/

[dbadmin@intelligence 648518346341351424]$ cd 20231017

[dbadmin@intelligence 20231017]$ ls

ArcSight_Data_1_0504403158265495598.dat  ArcSight_Metadata_1_504403158265495598.csv.gz
ArcSight_Metadata_Archive_0504403158265495598.xml.gz

[dbadmin@intelligence 20231017]$ cat ArcSight_Data_1_0504403158265495598.dat
```

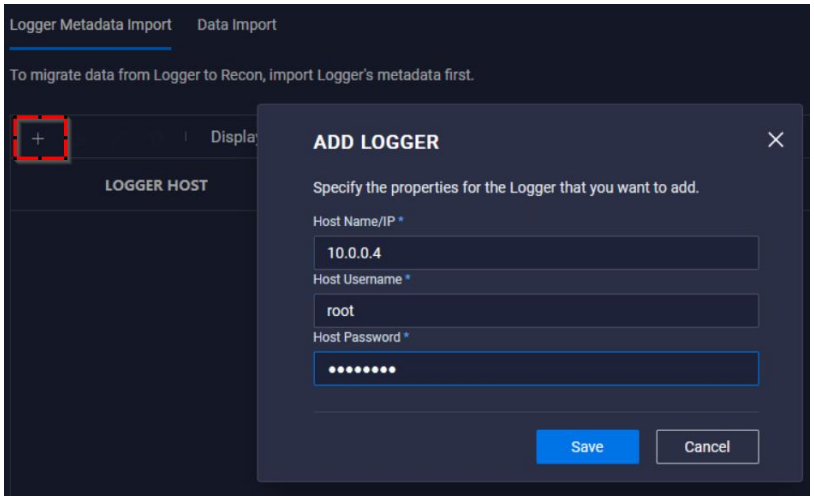
6. Import Metadata for Logger Events

Login to Recon UI, Choose Configuration => Import Logger Data

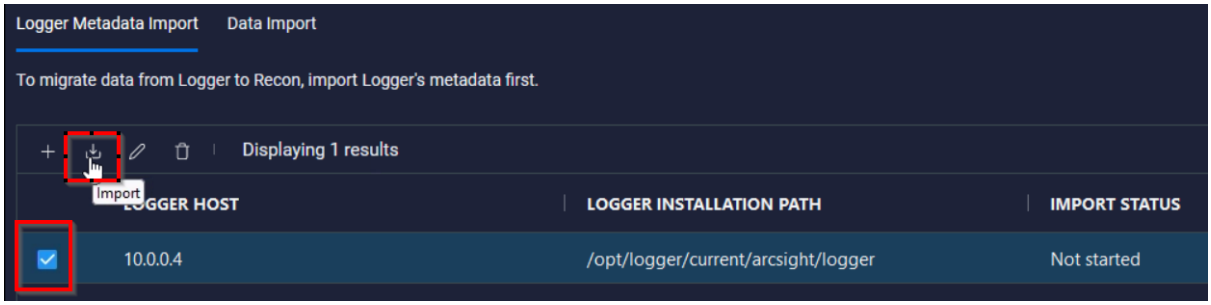


Under Logger Metadata Import, click “+” to add logger host

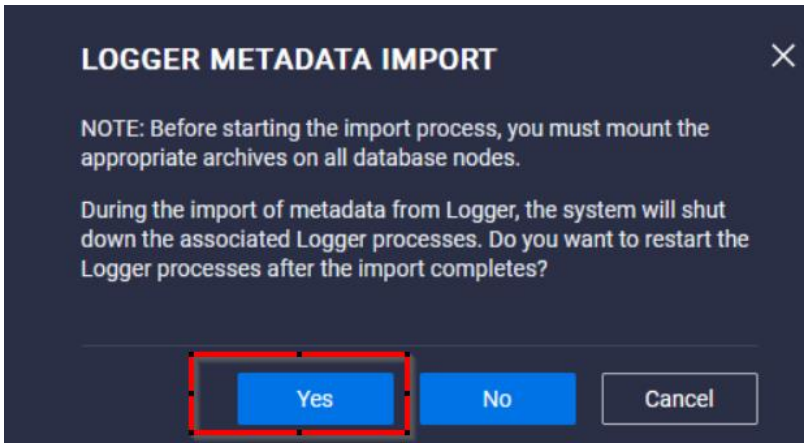
Note: You need to set the OS username/password for logger, NOT logger UI credential



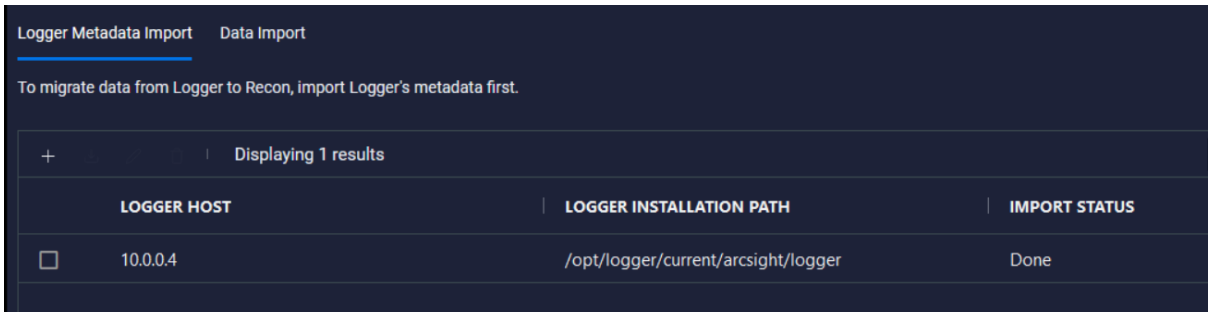
After adding the logger host, select the entry, then click the import button



During metadata importing, the logger process will be stopped, click the YES button to automatically start logger after metadata import.

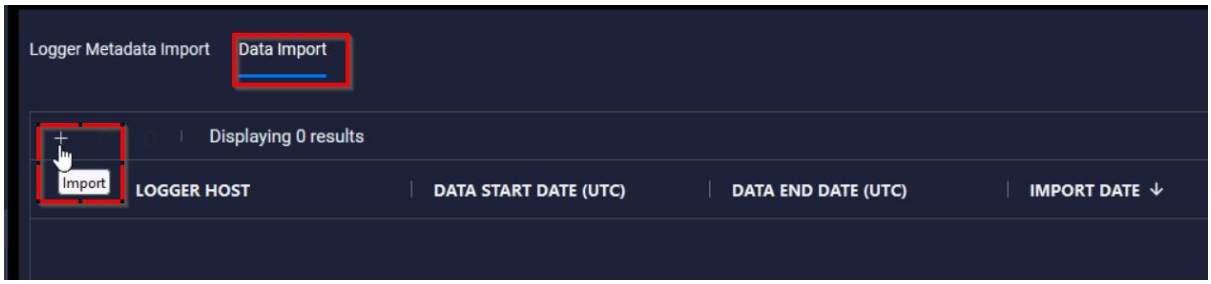


Refresh the UI to check the metadata importing status

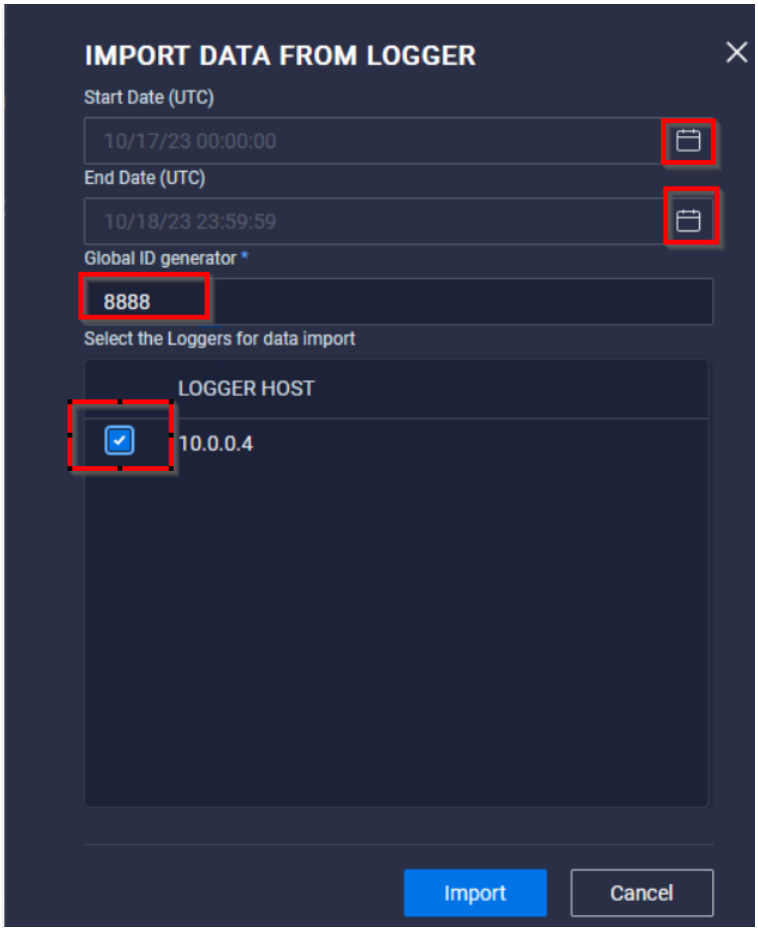


7. Import Logger Events

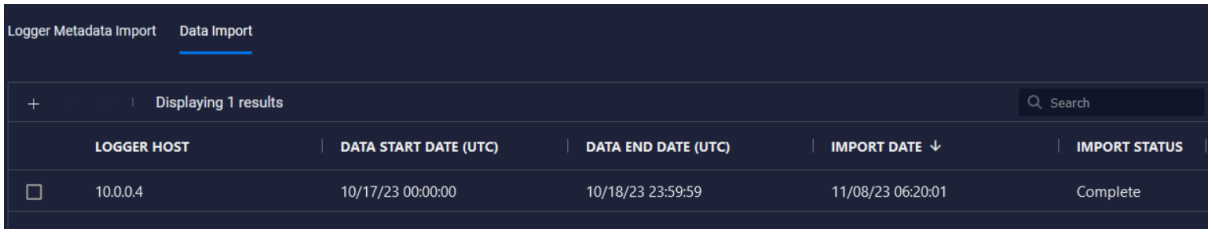
Start the Logger Data Import



Click the calendar icon to set the start date and end date, set the Global ID for all imported logger events



Import status begin with “Initialize” then “Complete”. If the status is not complete, check the logs for troubeleshooting.


Logger Metadata Import
Data Import
Displaying 1 results
Search
LOGGER HOST
DATA START DATE (UTC)
DATA END DATE (UTC)
IMPORT DATE
IMPORT STATUS
10.0.0.4
10/17/23 00:00:00
10/18/23 23:59:59
11/08/23 06:20:01
Complete

8. Troubleshooting Logger Migration

Check the logger data migration logs on Vertica host

```
[root@intelligence ~]# cd /opt/vertica/udfs/datamigration/logs/

[root@intelligence logs]# ls

logger_to_recon_migration_10.0.0.4_from_2023-10-17T00:00:00.000Z_to_2023-10-
18T23:59:59.999Z.log

[root@intelligence logs]# more logger_to_recon_migration_10.0.0.4_from_2023-10-
17T00:00:00.000Z_to_2023-10-18T23:59:59.999Z.log

[2023-11-08 06:20:01,690][INFO] Migration from 2023-10-17T00:00:00.000Z to 2023-10-
18T23:59:59.999Z.

[2023-11-08 06:20:01,692][INFO] Timerange in milliseconds: [1697500800000, 1697673599999].

[2023-11-08 06:20:01,693][INFO] Logging the status of the "Data Migration" process...

[2023-11-08 06:20:01,720][INFO] Getting the ID of the "Data Migration" process...

Setting ArcSight system version to 7.2.0.0000.0 as indicated on commandline/through system
properties.

ARCSIGHT_HOME=/opt/vertica/udfs/datamigration

AbandonedObjectPool is used (org.apache.commons.dbcp.AbandonedObjectPool@5680a178)

   LogAbandoned: true

   RemoveAbandoned: true

   RemoveAbandonedTimeout: 300

[2023-11-08
06:20:02,227][INFO] >>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>
>>>>>>>>>>>>>>>>

[2023-11-08 06:20:02,228][INFO]                      Starting Events Migration from Logger to
Recon

[2023-11-08
06:20:02,228][INFO] >>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>
>>>>>>>>>>>>>>>>

[2023-11-08 06:20:02,228][INFO] Checking if there are archives to load...

[2023-11-08 06:20:02,369][INFO] Loading the archive
[/opt/LOGGER_10004/opt/archive/default/648518346341351424//20231016].

[2023-11-08 06:20:02,408][INFO] Archive 20231016 is empty.  No events have been loaded.

[2023-11-08 06:20:02,511][INFO] Loading the archive
[/opt/LOGGER_10004/opt/archive/default/648518346341351424//20231018].

[2023-11-08 06:20:02,987][INFO] Loading the archive
[/opt/LOGGER_10004/opt/archive/default/648518346341351424//20231017].

[2023-11-08 06:20:03,227][INFO] The Following Archives were Loaded:

[2023-11-08 06:20:03,227][INFO] 0504403158265495597

[2023-11-08 06:20:03,227][INFO] 0504403158265495599

[2023-11-08 06:20:03,227][INFO] 0504403158265495598
```

```
[2023-11-08
06:20:03,247][INFO] >>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>
>>>>>>>>>>>>>>>>

[2023-11-08 06:20:03,247][INFO]                     Getting the projection of events to
migrate

[2023-11-08
06:20:03,247][INFO] >>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>
>>>>>>>>>>>>>>>>

[2023-11-08 06:20:03,247][INFO] A total of 38,784 will be migrated.

[2023-11-08 06:20:03,247][INFO] Updating the migration status...

[2023-11-08
06:20:03,292][INFO] >>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>
>>>>>>>>>>>>>>>>

[2023-11-08 06:20:03,292][INFO]                                Sending events to Vertica

[2023-11-08 06:20:03,292][INFO]                                     Iteration 1 of 4

[2023-11-08
06:20:03,292][INFO] >>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>
>>>>>>>>>>>>>>>>

[2023-11-08 06:20:03,292][INFO] Loading the chunks in the specified time range...

[2023-11-08 06:20:03,355][INFO] Metadata fetching took 0 seconds.

[2023-11-08 06:20:03,363][INFO] Starting the parsing and event insertion from Logger
[10.0.0.4] to Vertica.

[2023-11-08 06:20:03,363][INFO] Processing the events...

[2023-11-08 06:20:07,990][INFO] Progress:29%. Event written in Vertica: 11,513. Total Events
processed: 11,513

[2023-11-08 06:20:09,369][INFO] Updating the migration status...

[2023-11-08
06:20:09,807][INFO] >>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>
>>>>>>>>>>>>>>>>

[2023-11-08 06:20:09,807][INFO]                                Sending events to Vertica

[2023-11-08 06:20:09,807][INFO]                                     Iteration 2 of 4

[2023-11-08
06:20:09,807][INFO] >>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>
>>>>>>>>>>>>>>>>

[2023-11-08 06:20:09,807][INFO] Loading the chunks in the specified time range...

[2023-11-08 06:20:09,854][INFO] Metadata fetching took 0 seconds.

[2023-11-08 06:20:09,856][INFO] Starting the parsing and event insertion from Logger
[10.0.0.4] to Vertica.

[2023-11-08 06:20:09,857][INFO] Processing the events...

[2023-11-08 06:20:14,576][INFO] Progress:59%. Event written in Vertica: 11,480. Total Events
processed: 22,993

[2023-11-08 06:20:15,861][INFO] Updating the migration status...

[2023-11-08
06:20:16,302][INFO] >>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>
>>>>>>>>>>>>>>>>

[2023-11-08 06:20:16,303][INFO]                                Sending events to Vertica

[2023-11-08 06:20:16,303][INFO]                                     Iteration 3 of 4

[2023-11-08
06:20:16,303][INFO] >>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>
>>>>>>>>>>>>>>>>

[2023-11-08 06:20:16,303][INFO] Loading the chunks in the specified time range...

[2023-11-08 06:20:16,341][INFO] Metadata fetching took 0 seconds.
```

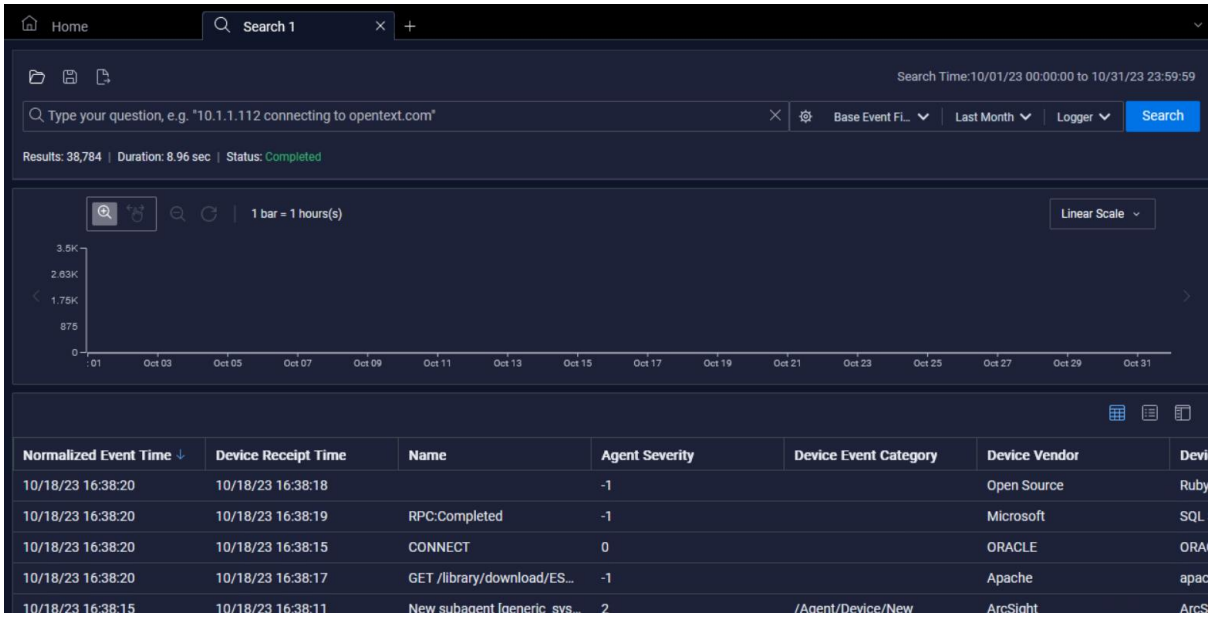
```
[2023-11-08 06:20:16,342][INFO] Starting the parsing and event insertion from Logger
[10.0.0.4] to Vertica.

[2023-11-08 06:20:16,342][INFO] Processing the events...

[2023-11-08 06:20:21,775][INFO] Progress:89%. Event written in Vertica: 11,609. Total Events
processed: 34,602

[2023-11-08 06:20:23,344][INFO] Updating the migration status...

[2023-11-08
06:20:23,780][INFO] >>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>
>>>>>>>>>>>>>>>>

[2023-11-08 06:20:23,780][INFO]                                Sending events to Vertica

[2023-11-08 06:20:23,780][INFO]                                     Iteration 4 of 4

[2023-11-08
06:20:23,780][INFO] >>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>
>>>>>>>>>>>>>>>>

[2023-11-08 06:20:23,780][INFO] Loading the chunks in the specified time range...

[2023-11-08 06:20:23,814][INFO] Metadata fetching took 0 seconds.

[2023-11-08 06:20:23,815][INFO] Starting the parsing and event insertion from Logger
[10.0.0.4] to Vertica.

[2023-11-08 06:20:23,815][INFO] Processing the events...

[2023-11-08 06:20:26,251][INFO] Progress:100%. Event written in Vertica: 4,182. Total Events
processed: 38,784

[2023-11-08 06:20:27,816][INFO] Updating the migration status...

[2023-11-08
06:20:28,249][INFO] >>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>
>>>>>>>>>>>>>>>>

[2023-11-08 06:20:28,249][INFO]                       Ending Events Migration from Logger to
Recon

[2023-11-08
06:20:28,249][INFO] >>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>
>>>>>>>>>>>>>>>>

[2023-11-08 06:20:28,249][INFO] Checking the last chunkid migrated...

[2023-11-08 06:20:28,281][INFO] Checking if there are archives to unload...

[2023-11-08 06:20:28,638][INFO] The Archives previously loaded have been unloaded correctly

[2023-11-08 06:20:28,638][INFO] A total of 38,784 events have been migrated.

[2023-11-08 06:20:28,638][INFO] Updating the migration status...

[2023-11-08 06:20:28,692][INFO] Updating the status of the process on Vertica side...

[2023-11-08 06:20:28,725][INFO] Status updated successfully.

[2023-11-08 06:20:28,727][INFO] Logger Data Migration procedure ended successfully. Exiting...

[2023-11-08 06:20:28,730][INFO] The script execution took 27 seconds.
```

9. Search Logger Events on Recon

Once logger data import complete, you can search the logger events in Recon UI.

Click the “Recon” button next to “Search” button, switch to “Logger”

Following is the search result with empty search condition (means all events)



Notice the time series bar chart is not updated for logger data search (at least in ArcSight 2023.3 version)