arcsight コマンドの arcdt runsql の使い方例

2023 年 3 月 16 日　ArcSight Support

arcsight コマンドの arcdt runsql にて ESM の MySQL データベースからデータを抽出することが可能です。この資料はその使い方の例を説明したものです。

以下、OS の arcsight ユーザーでのご実行をお願い致します。

1. 次の様な SQL のファイルを作成します。

```
[arcsight@esm003jp bin]$ cat /tmp/test1.sql
select count(*) from arc_event
```

2. 次にこのファイルを使用して arcsight コマンドの arcdt runsql を実行します。

2.1 “-type EndTime” 終了時刻の場合

```
[arcsight@esm003jp ~]$ cd /opt/arcsight/manager/bin/
[arcsight@esm003jp bin]$ ./arcsight arcdt runsql -f /tmp/test1.sql -type EndTime -ss 2023-02-01-00
-00-00-000-JST -se 2023-02-02-00-00-00-000-JST

Assuming ARCSIGHT_HOME: /opt/arcsight/manager
Assuming JAVA_HOME: /opt/arcsight/java/esm/current/jre

ArcSight Diagnostics Tool starting ...

RunSQL sessionId: 524288002

executing sql statement: set arc_logger_usersessionId =524288002;
Input startDate and endDate values:
startDate: Wed Feb 01 00:00:00 JST 2023    1675177200000
endDate: Thu Feb 02 00:00:00 JST 2023    1675263600000
RunSQL sessionId: 524288002
Running SQL: select count(*) from arc_event

count(*)
--------
  11919



[arcsight@esm003jp bin]$
```

ここで、”-type EndTime”　は終了時刻の指定で、”-ss”は範囲開始、”-se”は範囲終了の指定になります。次ページ以降のようにマネージャ受信時刻を使用されたい場合は、”-type mrt”となり、イベント ID”-type EventId”とすることも可能です。

2.2 ”-type mrt” マネージャ受信時刻の場合

```
[arcsight@esm003jp bin]$ ./arcsight arcdt runsql -f /tmp/test1.sql -type mrt -ss 2023-02-01-00-20-00-000-JST -se 2023-02-02-23-00-00-000-JST

Assuming ARCSIGHT_HOME: /opt/arcsight/manager
Assuming JAVA_HOME: /opt/arcsight/java/esm/current/jre

ArcSight Diagnostics Tool starting ...

RunSQL sessionId: 524288063

executing sql statement: set arc_logger_usersessionId =524288063;
Input startDate and endDate values:
startDate: Wed Feb 01 00:20:00 JST 2023    1675178400000
endDate: Thu Feb 02 23:00:00 JST 2023    1675346400000
RunSQL sessionId: 524288063
Running SQL: select count(*) from arc_event

count(*)
--------
  14528



[arcsight@esm003jp bin]$
```

2.3 ”-type EventId” イベント ID の場合

```
[arcsight@esm003jp bin]$ ./arcsight arcdt runsql -f /tmp/test1.sql -type EventId -ss 900001 -se 900010

Assuming ARCSIGHT_HOME: /opt/arcsight/manager
Assuming JAVA_HOME: /opt/arcsight/java/esm/current/jre

ArcSight Diagnostics Tool starting ...

RunSQL sessionId: 524288112

executing sql statement: set arc_logger_usersessionId =524288112;
RunSQL sessionId: 524288112
Running SQL: select count(*) from arc_event

count(*)
--------
     10



[arcsight@esm003jp bin]$
```

3. テーブルのカラムを指定することによりデータの抽出が可能です。

```
[arcsight@esm003jp bin]$ cat /tmp/test2.sql
select event_id, end_time, manager_receipt_time, message from arc_event limit 10
[arcsight@esm003jp bin]$ ./arcsight arcdt runsql -f /tmp/test2.sql -type EndTime -ss 2023-02-01-00
-20-00-000-JST -se 2023-02-02-23-00-00-000-JST

Assuming ARCSIGHT_HOME: /opt/arcsight/manager
Assuming JAVA_HOME: /opt/arcsight/java/esm/current/jre

ArcSight Diagnostics Tool starting ...

RunSQL sessionId: 524288020

executing sql statement: set arc_logger_usersessionId =524288020;
Input startDate and endDate values:
startDate: Wed Feb 01 00:20:00 JST 2023    1675178400000
endDate: Thu Feb 02 23:00:00 JST 2023    1675346400000
RunSQL sessionId: 524288020
Running SQL: select event_id, end_time, manager_receipt_time, message from arc_event limit 10

event_id | end_time              | manager_receipt_time    | message
---------+-------------------------+-------------------------+--------
  900001 | 2023-02-01 18:32:32.451 | 2023-02-01 18:32:32.461 |
  900002 | 2023-02-01 18:32:32.594 | 2023-02-01 18:32:32.594 |
  900003 | 2023-02-01 18:33:11.587 | 2023-02-01 18:33:11.587 |
  900004 | 2023-02-01 18:33:11.588 | 2023-02-01 18:33:11.588 |
  900005 | 2023-02-01 18:33:11.738 | 2023-02-01 18:33:11.738 |
  900006 | 2023-02-01 18:33:11.739 | 2023-02-01 18:33:11.739 |
  900007 | 2023-02-01 18:33:31.324 | 2023-02-01 18:33:31.324 |
  900008 | 2023-02-01 18:33:32.255 | 2023-02-01 18:33:32.255 |
  900009 | 2023-02-01 18:33:32.252 | 2023-02-01 18:33:32.252 |
  900010 | 2023-02-01 18:33:32.256 | 2023-02-01 18:33:32.256 |



[arcsight@esm003jp bin]$
```

4. 次の様にテーブルの情報取得が可能です。（arc_event テーブルの例）

```
[arcsight@esm003jp bin]$ cat /tmp/test3.sql
desc arc_event
[arcsight@esm003jp bin]$ ./arcsight arcdt runsql -f /tmp/test3.sql

Assuming ARCSIGHT_HOME: /opt/arcsight/manager
Assuming JAVA_HOME: /opt/arcsight/java/esm/current/jre

ArcSight Diagnostics Tool starting ...

RunSQL sessionId: 524288059

executing sql statement: set arc_logger_usersessionId =524288059;
Input startDate and endDate values:
startDate: Thu Jun 30 09:00:00 JST 2011    1309392000000
endDate: Fri Sep 30 10:00:00 JST 2011    1317344400000
RunSQL sessionId: 524288059
Running SQL: desc arc_event

COLUMN_NAME             | COLUMN_TYPE   | IS_NULLABLE | COLUMN_KEY | COLUMN_DEFAULT
| EXTRA
-------------------------+--------------+-------------+------------+------------------------+----------------------------
--
event_id               | bigint(20)    | NO        |          |                  |
end_time               | timestamp(3)  | NO        |          | CURRENT_TIMESTAMP(3)    | on update
CURRENT_TIMESTAMP(3)
manager_receipt_time      | timestamp(3)  | NO        |          | 0000-00-00 00:00:00.000 |
cat_descriptor_id        | bigint(20)    | YES       |          |                  |
dvc_descriptor_id        | bigint(20)    | YES       |          |                  |
agt_descriptor_id        | bigint(20)    | YES       |          |                  |
agt_receipt_time         | datetime(3)   | YES       |          |                  |
base_event_count         | bigint(20)    | YES       |          |                  |
dest_trans_address       | varbinary(16) | YES       |          |                  |
dest_address             | varbinary(16) | YES       |          |                  |
dest_geo_id              | bigint(20)    | YES       |          |                  |
dest_port               | int(11)       | YES       |          |                  |
dest_trans_port          | int(11)       | YES       |          |                  |
dest_zone               | bigint(20)    | YES       |          |                  |
name                   | varchar(512)  | YES       |          |                  |
event_type              | tinyint(4)    | YES       |          |                  |
generator               | bigint(20)    | YES       |          |                  |
priority               | int(11)       | YES       |          |                  |
raw_event               | varchar(4000) | YES       |          |                  |
（後略）
```

SQL にカラムを指定されたい場合は、こちらの COLUMN_NAME をご指定ください。

5. MySQL へのログイン

次の様にして MySQL に直接ログインすることが可能ですが、何らかの問題（リソースがコンソールから削除できなくなった）などがない場合は直接 MySQL データベースにログインすることはお勧めしておりません。また、MySQL ログインする場合は、念のため manager サービスを停止されることをお勧めします。

```
[arcsight@esm003jp bin]$ cd /opt/arcsight/logger/current/arcsight/bin/
[arcsight@esm003jp bin]$ ./mysql -u arcsight -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 204
Server version: 5.7.33 Source distribution

Copyright (c) 2000, 2021, Oracle and/or its affiliates.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> use arcsight
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
mysql> desc arc_resource;
+-------------------+--------------+------+-----+-------------------------+-------+
| Field             | Type         | Null | Key | Default                 | Extra |
+-------------------+--------------+------+-----+-------------------------+-------+
| id                | varchar(37)  | NO   | PRI | NULL                    |       |
| name              | varchar(200) | NO   | MUL | NULL                    |       |
| alias             | varchar(200) | YES  |     | NULL                    |       |
| description       | varchar(4000)| YES  |     | NULL                    |       |
| resource_type     | int(5)       | NO   | MUL | NULL                    |       |
| lastmodified      | bigint(20)   | NO   |     | NULL                    |       |
| version_id        | varchar(25)  | YES  |     | NULL                    |       |
| content_version_id | varchar(25) | YES  |     | NULL                    |       |
（後略）
```

なお、arc_event テーブルに関しては MySQL に定義されておりますが、イベントデータはストレージデバイスとして PostgreSQL に格納されており、MySQL からは直接はイベントデータの抽出ができませんのでご注意ください。

以上