MySQL クライアントで arc_event テーブルにアクセスする方法

2023 年 3 月 16 日

ArcSight Support

MySQL の arc_event テーブルのイベントデータは InnoDB に格納されていないため、アクセスは自動でなく事前準備が必要となっています。

MySQL で arc_event テーブルからイベントデータを選択すると、次のエラーが発生します。

```
mysql> select event_id, name from arc_event limit 10;
ERROR 3232 (HY000): 5005: invalid user session: [20]
mysql>
```

以下は、MySQL クライアントで arc_event テーブルを照会するサンプル手順です。（実行は OS の arcsight ユーザーでお願い致します。）

１．ダミーファイルの作成

```
$ touch /tmp/dummy.sql
```

２．ArcSight arcdt runsql コマンドを実行します

```
$ /opt/arcsight/manager/bin/arcsight arcdt runsql -f /tmp/dummy.sql -type EndTime -ss 1900-01-01-00-00-00-000-JST -se 2023-02-15-00-00-00-000-JST
```

３．２の実行結果から sessionId（arc_logger_usersessionId）を取得します

```
$ /opt/arcsight/manager/bin/arcsight arcdt runsql -f /tmp/dummy.sql -type EndTime -ss 1900-01-01-00-00-00-000-JST -se 2023-02-17-00-00-00-000-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: Mon Jan 01 00:00:00 JST 1900    -2209021200000
endDate: Fri Feb 17 00:00:00 JST 2023    1676559600000
RunSQL sessionId: 524288002

$
```

４．MySQL にログインし、ステップ３で取得した sessionId（arc_logger_usersessionId）を設定してクエリを実行します

```
$ /opt/arcsight/logger/current/arcsight/bin/mysql -D arcsight -uarcsight -p
Enter password:
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 128
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> set arc_logger_usersessionId =524288002;
Query OK, 0 rows affected (0.00 sec)

mysql> select event_id, name from arc_event limit 10;
+----------+--------------------------+
| event_id | name                     |
+----------+--------------------------+
|   600001 | Group [Asset] updated    |
|   600002 | ConfigurationItem updated |
|   600003 | ActiveList entry expired  |
|   600004 | ActiveList entry expired  |
|   600005 | ActiveList entry expired  |
|   600006 | ActiveList entry expired  |
|   600007 | ActiveList entry expired  |
|   600008 | ActiveList entry expired  |
|   600009 | ActiveList entry expired  |
|   600010 | ActiveList entry expired  |
+----------+--------------------------+
10 rows in set (0.25 sec)

mysql>
```

以上