ESM administration from Oracle to MySQL

Kerry Adkins

#HPProtect
Objectives

After attending this presentation you will:

• Understand how to access MySQL and postgres DB for CORR-E
• Learn about existing utilities to access the data
• Be aware of some known issues
• Learn a few best practices
What is CORR-E?
CORR-Engine as database

ESM Manager → CORR-Engine Comm Layer → CORR-Engine

Events → ArcSight Event Store → InnoDB Storage Engine

Resources and data → MySQL

© Copyright 2014 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.
MySQL Storage Engines

• The CORR-Engine relies on MySQL’s pluggable storage engine architecture
  - Allows for different types of data handling
    
  **ArcSight’s high performance event storage and retrieval**

• InnoDB – Built-in transactional support, allowing updates and deletes
  - Multiversion concurrency control (same as Oracle)

  **Used for ESM resources (rules, channels, …) and trend data, active/session list data, annotations**

• MySQL seamlessly handles the joins (e.g.: events and cases, actors)

• Patent-pending technology superstore (single database with row and column store)
Commands
Accessing CORR-E – logs & commands

• Getting to the database:
  Commands are: mysql and psql

• Log files
  MySQL – centralized in ArcSight’s logger directory

• DB commands:
  show database;
  ‘use arcsight’ (only one instance allowed)
  show tables;
  desc (tablename);
  show processlist; and show full processlist;
  export_system_tables
    Moved from db to manager/bin and requires ESM shutdown!
Accessing data
Manipulating data warnings

• Do not make direct changes to the database without support approval
  - MySQL = Corrupt or broken data
  - Postgres = broken ESM functionality

• Error: Querying the event table requires a session
  - Use the arcdt script
  - Read the ‘ESM Admin Guide’ for parameters and usage

• Show create table <tablename>
  - Storage type and character set parameters

• Use Limit to restrict row count return
  - Select <column> from <tablename> limit 10;
Known issues
Known issues – fixed 6.0c patch 2 and 6.5c and 6.5C SP1

Don’t use this command, it can corrupt MySQL/innodb tables
/sbin/service arcsight_services stop all

Instead use the following:
• /sbin/service arcsight_services stop arcsight_web
• /sbin/service arcsight_services stop manager
• /sbin/service arcsight_services stop logger
• /sbin/service arcsight_services stop mysqld

Strongly recommended by Support to stop each component individually
Known issues – space

There have been cases where arc_system_data fills, the culprits usually are:

- **Trends, Session lists, Active lists**
- **Possible actions:**
  - Run SQL to find large tables
  - Truncate
  - Create from / rename
  - Insert into / select *
Patches and release notes

Same as Oracle versions – **Always review the Release Notes for bugs fixed, open issues, for example 6.5 SP1:**

NGS-4790

To resolve a "database full" condition, you can free up space by doing the following:

- Delete any unused trends. Deleting the trend frees up any data in the table associated with this trend.
- Reduce the retention period of specific trends. By default, trends retain 180 days of data. You can set this retention time on a per-trend basis. Any data falling outside this range will be removed the next time the trend runs.
- Examine the contents of your session lists. Data is not usually removed from session lists. Running "bin/arcsight dropSLPartitions -h" will explain how to remove data older than a specified time. Note that this will apply to ALL session lists on your system.
DB dos and don’ts

• Oracle best practices:
  - See http://protect724.hp.com/docs/DOC-1466

• CORR-E don’ts:
  - Don’t make changes to the my.cnf file (MySQL configuration)
    • Customers have lost all data by adding parameters
    • Customers have encountered unrecoverable corruption – also lost data

• CORR-E dos:
  • Open a support ticket and ask about any parameters you want to add or change first!
Sites for more information

Protect 724

ArcSight Resources – webinars, tools, interesting stuff:
https://protect724.hp.com/community/arcsight/arcsight-resources

Product documentation:
https://protect724.hp.com/community/arcsight/productdocs
For more information

Attend these sessions

• TB3259 HP ArcSight ESM Health Check
• TB3012 Correlating Efficiently Tips, Tricks and Troubleshooting
• TB3273 Practical Examples of Big Data, Security Analytics and Visualization
Please give me your feedback

Session TT3156  Speaker Kerry Adkins

Please fill out a survey.

Hand it to the door monitor on your way out.

Thank you for providing your feedback, which helps us enhance content for future events.
Thank you
Make it matter.
Detailed information for hands-on practice
## Accessing the databases

<table>
<thead>
<tr>
<th>Command</th>
<th>Oracle</th>
<th>MySQL</th>
</tr>
</thead>
</table>
| Connect to db as default user                | arcdbutil sql / as sysdba  
Or sqlplus / as sysdba | /opt/arcsight/logger/current/arcsight/bin/mysql -u root -p          |
| Connect to db as schema owner                | arcdbutil sql arcsight  
Or sqlplus arcsight          | /opt/arcsight/logger/current/arcsight/bin/mysql -u arcsight -p        |
| Connect to Postgres                          | N/A                     | /opt/arcsight/logger/current/arcsight/bin/psql rwdb web               |

**DANGER!** Do not manipulate MySQL or postgresql in any way unless expressly advised by HP. Configuration changes or data changes at this level may result in catastrophic loss of data.
## Log files

<table>
<thead>
<tr>
<th>files</th>
<th>Oracle</th>
<th>MySQL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Oracle alert log 10g</td>
<td>$ORACLE_HOME/admin/arcsight/bdump/alert_arcsight.log</td>
<td>/opt/arcsight/logger/data/mysql/mysql.log</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Oracle alert log 11g</td>
<td>$ORACLE_BASE/diag/rdbms/arcsight/arcsight/trace/alert_arcsight.log</td>
<td>Same as above</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Datafiles</td>
<td>SQL&gt; select file_name from dba_data_files;</td>
<td>mysql&gt; SELECT @@datadir;</td>
</tr>
<tr>
<td></td>
<td>select file_name from dba_temp_files;</td>
<td>+---------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>+---------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>+---------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1 row in set (0.00 sec)</td>
</tr>
</tbody>
</table>
show databases – Lists the schemas/databases available

Oracle command to show schemas:
SQL> select username from dba_users;

Oracle has a database that can have many schemas or users.

In MySQL database = schema

You cannot create multiple ArcSight installs on CORR-E.
use database_name – Selects the db to connect to

**Oracle command:**
sqlplus <schema name>

Our default is ArcSight
show tables; – Lists tables in the db/schema

**Oracle command:**

SQL> select table_name from dba_tables where owner='ARCSIGHT';
desc table_name; – Describes columns/sizes in table

**Oracle command:**
SQL> desc table_name

**MySQL command:**
mysql> desc table_name;
show processlist – Shows active processes in DB

**Oracle command:**
arcdbutil sql arcsight
SQL> @dbsessions

Our internal script dbsessions.out

**MySQL command:**
mysql> use arcsight;
mysql> show processlist;
mysql> show full processlist;*

Both show what users are connected and what is running.

*Show full processlist will show actual queries running
## Export system tables – CORR-E - ESM service down

<table>
<thead>
<tr>
<th>command</th>
<th>Oracle</th>
<th>MySQL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Getting a system dump, referred to as export system tables</td>
<td>$ARCSIGHT_HOME/bin/arcsight export_system_tables &lt;schema&gt;/&lt;password&gt;@ORACLE_SID</td>
<td>/sbin/service arcsight_services stop manager</td>
</tr>
<tr>
<td></td>
<td>Example: /opt/arcsight/db/bin/arcsight export_system_tables arcsight/arcsight@arcsight</td>
<td>Execute the following command from /opt/arcsight/manager/bin to export the tables: ./arcsight</td>
</tr>
<tr>
<td></td>
<td>Output file is in $ARCSIGHT_HOME/arcsight.dmp</td>
<td>export_system_tables &lt;MySQL_username&gt; &lt;MySQL_password&gt; &lt;MySQL_databasem&gt;</td>
</tr>
<tr>
<td></td>
<td>&lt;Oracle ESM can stay up for export_system_tables&gt;</td>
<td>Example: /arcsight export_system_tables arcsight arcsight</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Output file is: /opt/arcsight/manager/tmp/arcsight_dump_system_tables.sql</td>
</tr>
<tr>
<td></td>
<td></td>
<td>start the Manager: /sbin/service arcsight_services start manager</td>
</tr>
</tbody>
</table>
Accessing data
Manipulating data warnings

If you make changes directly through MySQL – You could corrupt, change, irreparably damage your configuration (ie reports, connector information, trends, etc)

If you make changes through Postgres – You could corrupt, change, irreparably damage the metadata that allows access to the CORR-E storage
How to query arc_event table?

mysql> select * from arcsight.events where arc_deviceHostName = 'esm6c.hp.local' limit 1;
Gets ERROR 1641 (HY000): 5005: invalid user session: [20]

We have to set a session before running a command:
set arc_logger_usersessionId =524299997;

... but instead of going into that detail we have a utility! arcdt
CORR-E utility: arcdt

ArcSight Diagnostics tool – arcdt - runs sql commands

/opt/arcsight/manager/bin/arcsight arcdt.

Example: ./arcsight arcdt runsql \(\text{-f} \) /tmp/test.sql

Output will come to the screen
CORR-E utility: arcdt

Preferred method for accessing the Database in CORR-E

As tables are stored in either CORR-E storage OR innodb you will use different parameters for the arcdt command. All the parameters are listed in the 6.5 Admin guide on page 105-107 – too many to list here

https://protect724.hp.com/docs/DOC-9255

> Oracle equivalent of arcdt runsql = sqlp
CORR-E utility: arcdt simple command

```
[arcsight@esm60c bin]$ ./arcsight arcdt runsql -f /tmp/m.sql

Assuming ARCSIGHT_HOME: /opt/arcsight/manager
Assuming JAVA_HOME: /opt/arcsight/manager/jre

ArcSight Diagnostics Tool starting ...

RunSQL sessionId: 524407465

executing sql statement: set arc_logger_userSessionId =524407465;
Input startDate and endDate values:
startDate: Wed Jun 29 17:00:00 PDT 2011       1309392000000
endDate: Thu Sep 29 18:00:00 PDT 2011       1317344400000
RunSQL sessionId: 524407465
Running SQL: select count(*) from arc_resource where resource_type = 32

count(*)
-------
   1

[arcsight@esm60c bin]$ 
```
How to query arc_event table: Oracle

Note: Use end_time as oracle stores in partitions via end_time

This will select count for the day of 1/2/2014
SQL> select count(*) from arc_event where
  end_time < to_date('2014-01-01','YYYY-MM-DD') and end_time >= to_date('2014-01-02','YYYY-MM-DD');

Or with Oracle as we have partitions, you can count by partition:
SQL>select count(*) from arc_event partition (arc_event_20140102);

Or with seconds included:
SQL>select count(*) from arc_event where
  end_time <= to_date('2014-01-02 00:00:00','YYYY-MM-DD HH24:MI:SS')
  and end_time > to_date('2014-01-02 23:59:59','YYYY-MM-DD HH24:MI:SS');
To count the number of events in ESM CORRE you need to run a SQL command.

1. Create a file /opt/arcsight/manager/sample.txt with the following statement:

   `select count(*) from arcsight.events;`
How to query arc_event table pt 3

2. Run this command. Replace the date format with the dates you will like to query (See example):

```
/opt/arcsight/manager/bin/arcsight arcdt runsql -f /opt/arcsight/manager/sample.txt
-type EndTime -ss yyyy-mm-dd-00-00-00-000-UTC -se yyyy-mm-dd-00-00-00-000-UTC
```
(all on 1 line)

For example:

```
/opt/arcsight/manager/bin/arcsight arcdt runsql -f /opt/arcsight/manager/sample.txt
-type EndTime -ss 2014-01-01-00-00-00-000-UTC -se 2014-01-02-00-00-00-000-UTC
```

will count all events from 2014/01/01 00 hour to 2014/01/02 00 hour.
How to tell where table is stored

**Oracle command:**

SQL> select table_name, tablespace_name
from dba_tables
where table_name='ARC_EVENT';

**MySQL command:**

mysql>show create table <tablename>

The end will show storage and character set parameter. For example:

mysql>show create table arcsight.events;

  ENGINE=ARC_LOGGER DEFAULT CHARSET=utf8 COLLATE=utf8_bin |

mysql>show create table arc_resource;

  ENGINE=InnoDB DEFAULT CHARSET=utf8 COLLATE=utf8_bin |
Limiting result sets

**MySQL**

Doesn't support the standard. Alternative solution:

```sql
SELECT columns
FROM tablename
ORDER BY key ASC
LIMIT n;
```

**Oracle**

Supports ROW_NUMBER;

```sql
SELECT * FROM ( SELECT
ROW_NUMBER() OVER (ORDER BY key ASC) AS rownumber, columns FROM tablename)
WHERE rownumber <= n;
```
Known issues
Sample SQL – Finding large trend tables

To find the 5 largest trend tables:

```sql
SELECT concat(table_schema,'.',table_name) as Database_Tablename, table_rows as Rows,
concat(round(data_length/(1024*1024),2),'M') DATA, concat(round(index_length/(1024*1024),2),'M') idx,
concat(round((data_length+index_length)/(1024*1024),2),'M') total_size, round(index_length/data_length,2)
idxfrac
FROM information_schema.TABLES
where table_name like '%arc_trend%'
order by data_length+index_length DESC limit 5;
```
Truncate notification tables

Sometimes notification tables fill due to Rules or Datamonitorors getting too many hits and ESM doesn’t start or logging into the console is really slow. If you are OK in losing all your notifications, you can use the following SQL to remove them:

First you would shut the ESM service down then login to MySQL or use arcsight arcdt

mysql> set foreign_key_checks=0;
mysql> truncate table arc_notification_history;
mysql> truncate table arc_notification_registry;
mysql> set foreign_key_checks=1;

Last bring ESM back up.
Instead of delete – Create/rename

If you are deleting many rows from a large table, you may exceed the lock table size for an InnoDB table. To avoid this issue, or simply to minimize the time that the table remains locked, the following strategy (which does not use DELETE at all) might be helpful:

Login to MySQL or use arcsight arcdt
CREATE TABLE arc_notification_history_copy LIKE arc_notification_history;
Use RENAME TABLE to atomically move the original table out of the way and rename the copy to the original name:
RENAME TABLE arc_notification_history TO arc_notification_history _old, arc_notification_history _copy TO arc_notification_history;
Drop the original table:
DROP TABLE arc_notification_history _old;
<repeat for arc_notification_registry>
If you are not deleting all rows from large table

Select the rows not to be deleted into an empty table that has the same structure as the original table

```
INSERT INTO table_copy SELECT * FROM table WHERE ... ;
```

Use RENAME TABLE to atomically move the original table out of the way and rename the copy to the original name:

```
RENAME TABLE t TO table_old, table_copy TO table;
```

Drop the original table:

```
DROP TABLE table_old;
```