



ESM Oracle to MySQL mapping

Kerry Adkins

Mar/Apr 2014

Objectives

After attending this presentation you should be able to:

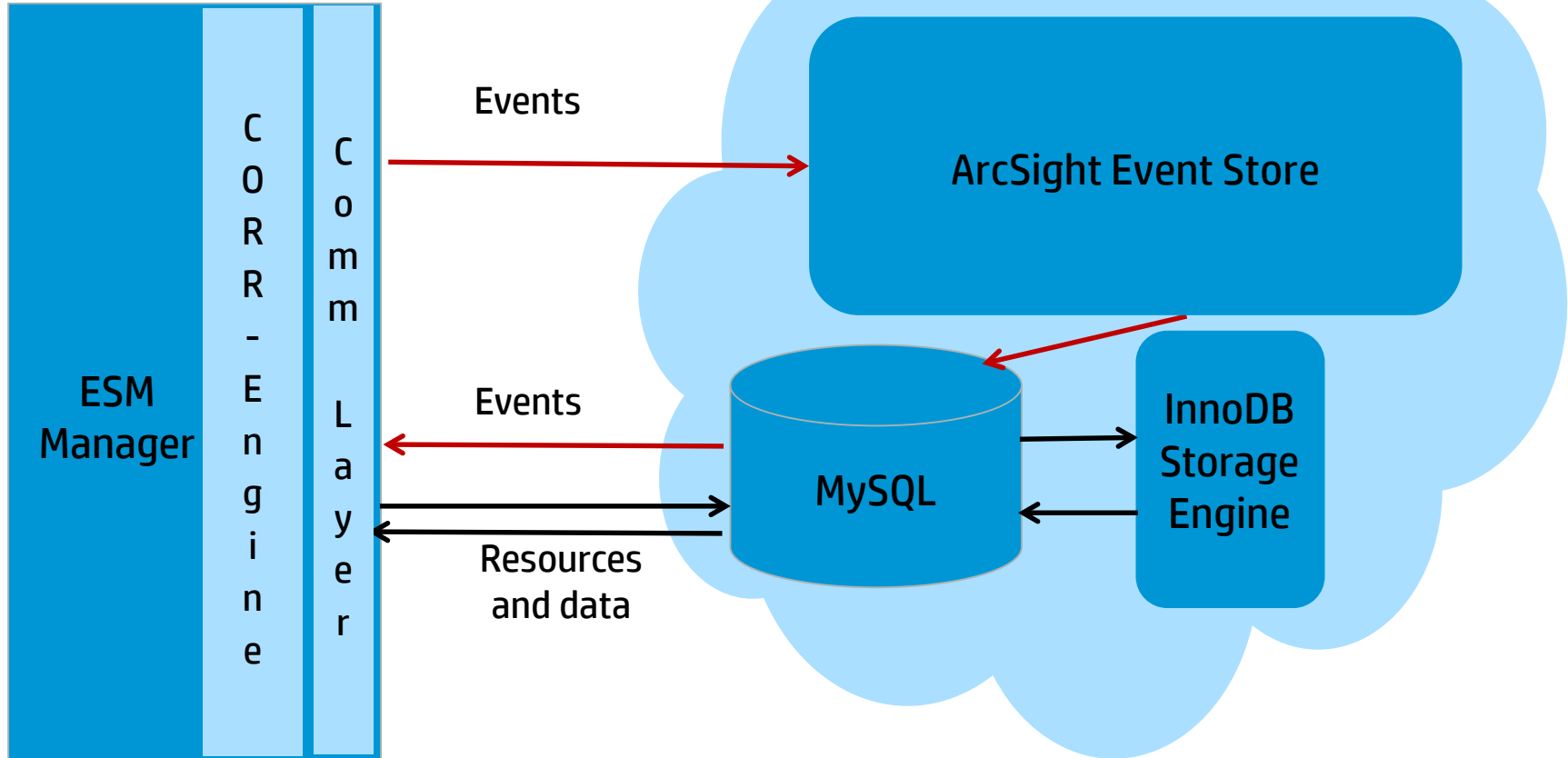
- Understand how to access MySQL DB for CORR-E utilities, etc
- Mappings of Oracle commands to MySQL
- Utilities and getting at the data in CORR-E
- Known Issues & a few Best Practices



What is CORR-E



CORR-Engine as Database



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, ...) & 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 the Databases

Command	Oracle	MySql
Connect to db as default user	arcdbutil sql / as sysdba Or sqlplus / as sysdba	<code>/opt/arc sight/logger/current/arc sight/bin/mysql -u root -p</code>
Connect to db as schema owner (default arcsight)	arcdbutil sql arcsight Or sqlplus arcsight	<code>/opt/arc sight/logger/current/arc sight/bin/mysql -u arcsight -p</code>
Connect to Postgres	N/A	<code>/opt/arc sight/logger/current/arc sight/bin/psql rwdb web</code>



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

files	Oracle	MySQL
Oracle alert log 10g	\$ORACLE_HOME/admin/arcsight/bdum/alert_arcsight.log	<i>/opt/arcsight/logger/data/mysql/mysql.log</i>
Oracle alert log 11g	\$ORACLE_BASE/diag/rdbms/arcsight/arcsight/trace/alert_arcsight.log	Same as above
Datafiles	SQL> select file_name from dba_data_files; select file_name from dba_temp_files;	mysql> SELECT @@datadir; +-----+ @@datadir +-----+ /opt/arcsight/logger/current/./data/mysql/ +-----+ 1 row in set (0.00 sec)

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.

```
arcsight@esm6:~$ /opt/arcsight/logger/current/arcsight/bin/mysql -u root -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 8816
Server version: 5.1.54 Source distribution

Copyright (c) 2000, 2010, Oracle and/or its affiliates. All rights reserved.
This is commercial software, and use of this software is governed
by your applicable license agreement with MySQL

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

mysql> show databases;
+-----+
| Database |
+-----+
| information_schema |
| arcsight |
| arcsight_report_repository |
| mysql |
| test |
+-----+
5 rows in set (0.00 sec)

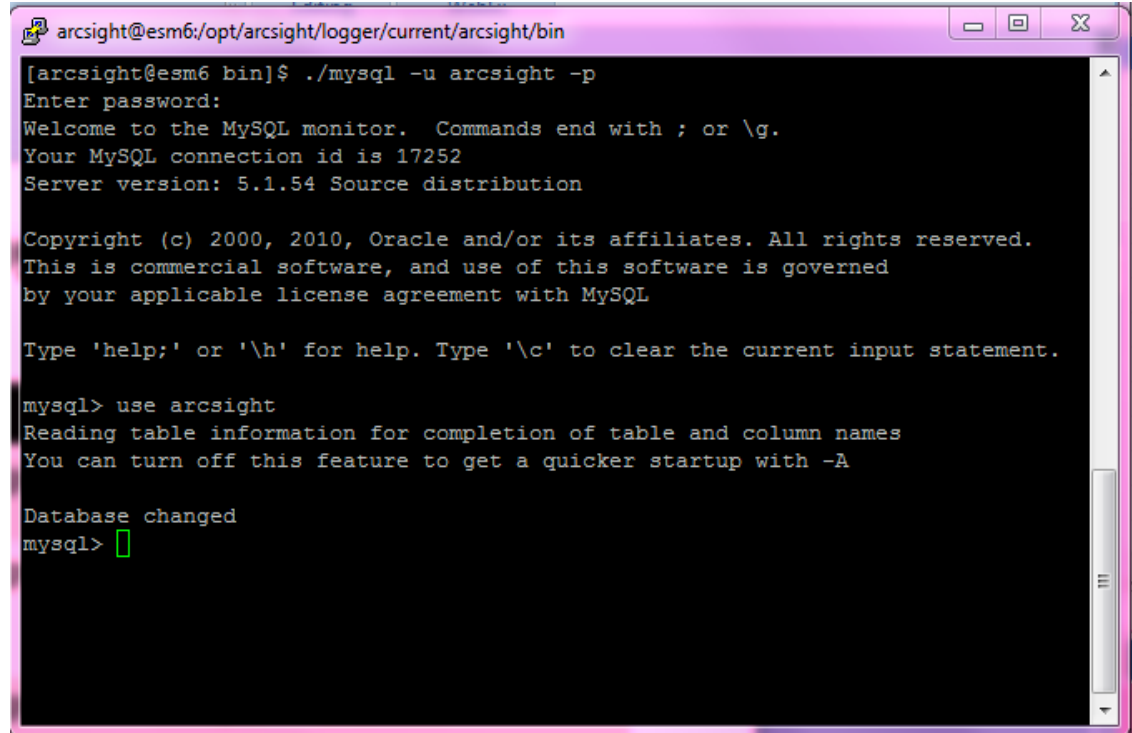
mysql> 
```



use database_name – selects the db to connect to

Oracle command:
sqlplus <schema name>

Our default is arcsight

A terminal window with a black background and white text. The window title is "arcsight@esm6:/opt/arcsight/logger/current/arcsight/bin". The prompt is "[arcsight@esm6 bin]\$". The user enters the command "./mysql -u arcsight -p". The terminal shows the MySQL prompt "mysql>" and the user enters "use arcsight". The terminal output includes: "Reading table information for completion of table and column names", "You can turn off this feature to get a quicker startup with -A", and "Database changed". The prompt "mysql>" is followed by a green cursor.

```
arcsight@esm6:/opt/arcsight/logger/current/arcsight/bin
[arcsight@esm6 bin]$ ./mysql -u arcsight -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 17252
Server version: 5.1.54 Source distribution

Copyright (c) 2000, 2010, Oracle and/or its affiliates. All rights reserved.
This is commercial software, and use of this software is governed
by your applicable license agreement with MySQL

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

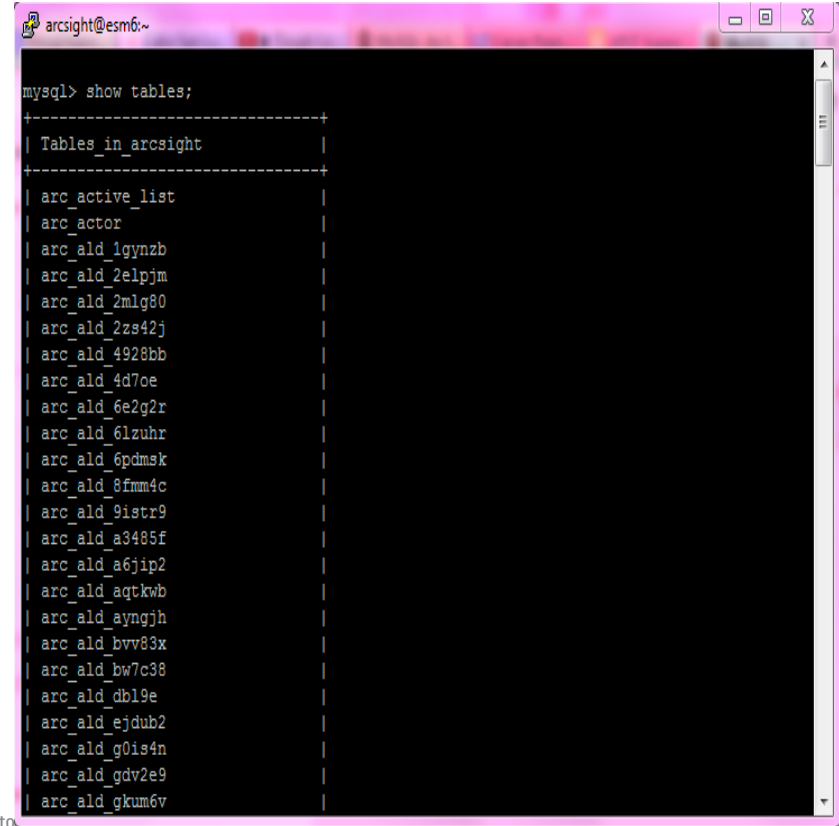
Database changed
mysql> █
```



show tables; - lists tables in the db/schema

Oracle command:

SQL> select table_name from dba_tables
where owner='ARCSIGHT';



```
arc_sight@esm6:~$ mysql> show tables;
+-----+
| Tables_in_arc_sight |
+-----+
| arc_active_list     |
| arc_actor           |
| arc_ald_1gyznzb     |
| arc_ald_2elbjm      |
| arc_ald_2mlg80      |
| arc_ald_2zs42j      |
| arc_ald_4928bb      |
| arc_ald_4d7oe       |
| arc_ald_6e2g2r      |
| arc_ald_6lzuhz      |
| arc_ald_6pdmsk      |
| arc_ald_8fmm4c      |
| arc_ald_9istr9      |
| arc_ald_a3485f      |
| arc_ald_a6jip2      |
| arc_ald_aqtkwb      |
| arc_ald_ayngjh      |
| arc_ald_bvv83x      |
| arc_ald_bw7c38      |
| arc_ald_db19e       |
| arc_ald_ejdub2      |
| arc_ald_g0is4n      |
| arc_ald_gdv2e9      |
| arc_ald_gkum6v      |
+-----+
```



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

Both show what users are connected and what is running.

MySql command:

```
mysql> use arcsight;
```

```
mysql> show processlist;
```

```
mysql> show full processlist;*
```

*Show full processlist will show actual queries running



Export System Tables – CORR-E - ESM service down

command	Oracle	MySql
Getting a system dump, referred to as export system tables	<pre>\$ARCSIGHT_HOME/bin/arcsight export_system_tables <schema>/<password>@ORACLE_SID</pre> <p>Example: /opt/arcsight/db/bin/arcsight export_system_tables arcsight/arcsight@arcsight</p> <p>Output file is in \$ARCSIGHT_HOME/arcsight.dmp</p> <p><Oracle ESM can stay up for export_system_tables></p>	<pre>/sbin/service arcsight_services stop manager Execute the following command from /opt/arcsight/manager/bin to export the tables: ./arcsight export_system_tables <mysql_username> <mysql_password> <mysql_dabatbase> Example: /arcsight export_system_tables arcsight arcsight arcsight Output file is: /opt/arcsight/manager/tmp/arcsight_dump_system_tables.sql start the Manager: /sbin/service arcsight_services start manager</pre>



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 **pgsql** – you could corrupt, change, irreparably damage the metadata that allows access to the CORR-E storage



How to query arc_event table ?

<http://support.openview.hp.com/selfsolve/document/KM00598676>

```
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;
```



CORR-E utility: arcdt

➤ **ArcSight Diagnostics tool – arcdt - runs sql commands**

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

Example: ./arcsight arcdt runsql -f /tmp/test.sql

Output will come to the screen



CORR-E utility: arcdt

➤ Preferred method for accessing the Database in CORR-E

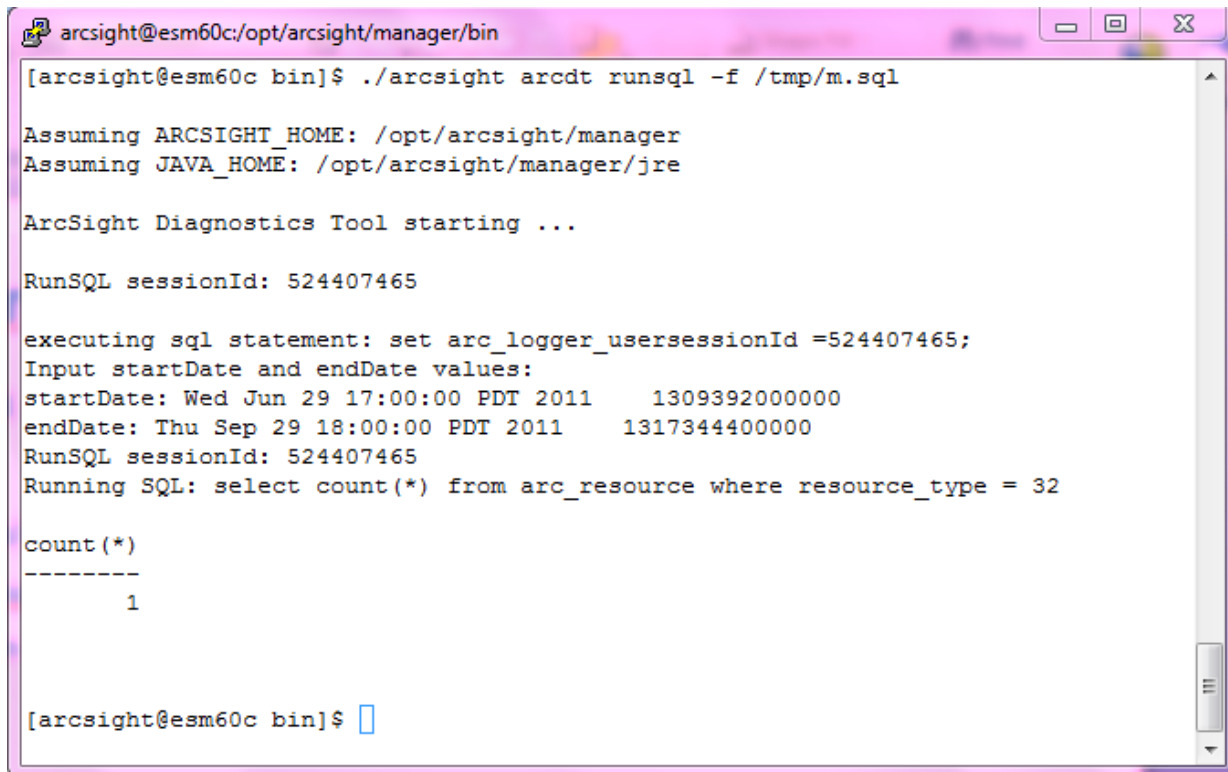
As tables are stored in either CORR-E storage OR innodb you will use different parameters for the arcdt command. All the parameters are listed in the 6.5 Admin guide on page 105-107 – too many to list here

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

> Oracle equivalent of arcdt runsql = sqlp



CORR-E utility: arcdt simple command



```
arcsight@esm60c:/opt/arcsight/manager/bin
[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 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 |
```



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('2014-01-02','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');
```



How to query arc_event table pt 2

<http://support.openview.hp.com/selfsolve/document/KM00598676> contents:

- 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 2014-01-02-00-00-00-000-UTC -se 2014-01-02-00-00-00-000-UTC
```

will count all events from 2014/01/02 00 hour to 2014/01/02 00 hour.



Limiting result sets

MySql

Doesn't support the standard. Alternative solution:

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

Oracle

Supports ROW_NUMBER;

```
SELECT * FROM ( SELECT  
ROW_NUMBER() OVER (ORDER BY key ASC) AS rownumber, columns FROM tablename)  
WHERE rownumber <= n;
```



Known Issues



Known Issues – 6.0c – fixed patch 2 and 6.5

Don't use 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
```



Known Issues – space

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

Trends

Session lists

Active lists



Sample SQL - Finding Large trend tables

To find the 5 largest trend tables:

```
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 Datamonitors 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;
```



Expanding storage space

**Oracle command:
arcsight database xts**

MySQL

In 6.0 there are files you can edit, but this can be dangerous if you use a smaller size, it can corrupt your data

Recommended step is to upgrade to 6.5 and use the Command Center to expand space.



ESM 6.5C Command Center – modify storage 6.5c only

Event Storage

Storage Groups

- Create New
- Edit Existing
- Control Archive location

Retention

- Specific to Storage group

Storage Mapping

- Segment your data

The screenshot displays the ArcSight Command Center Administration interface. The top navigation bar includes 'Dashboards', 'Search', 'Reports', 'Cases', 'Applications', and 'Administration'. The 'Administration' section is active, showing 'Storage and Archive' settings. The 'Storage' tab is selected, with sub-tabs for 'Storage Mapping', 'Alerts', and 'Archive Jobs'. The 'Archiving' status is 'On', and the 'Schedule Time' is set to '01:00'. A table lists storage groups with columns for Name, Retention Period, Current Size, Maximum Size, Follow Schedule, and Archive Location. The table includes rows for 'Default Storage Group', 'Internal Event Storage Group', and 'MyStorage Group', along with a 'Total' row. Below the table, there is a note about name changes and a section for 'System Storage' showing 'Current Size' (102.0 MB) and 'Maximum Size' (10.0 GB).

Storage and Archive

Storage Mapping Alerts Archive Jobs

New... Edit

Archiving Status: On

Schedule Time 01:00

Storage Group Name	Retention Period	Current Size	Maximum Size	Follow Schedule	Archive Location
Default Storage Group	30	1.0	12.0	<input checked="" type="checkbox"/>	/opt/arcSight/logger/data/archi...
Internal Event Storage Group	365	1.0	5.0	<input checked="" type="checkbox"/>	/opt/arcSight/logger/data/archi...
MyStorage Group	13	1.0	5.0	<input checked="" type="checkbox"/>	/opt/arcSight/logger/data/archi...
Total		3.0	22.0		

Note: The name cannot be changed.

Allocated Size 42.0 GB Edit

Maximum Size 53.2 GB

System Storage

Current Size 102.0 MB

Maximum Size 10.0 GB



Space ...Challenges

Support to have a KCS article to manually expand space

6.5 Command Center doesn't allow System Storage changes (bug)

Jira filed for a script [NGS-4551](#)



Best Practices



Patches and Release Notes

•**Same as Oracle versions – ALWAYS review the Release Notes for bugs fixed and tuning tidbits, for example 6.0C patch 2 release notes:**

-NGS-4082

If the buffer pool is too small, it can cause slow channel performance or prevent logging in to the Console. If you get an error message like this:

```
[ERROR][default.com.arcsight.common.persist.mysql.MySqlNotificationBroker][purgeOldNotifications]  
java.sql.SQLException: The total number of locks exceeds the lock table size
```

...you can solve the problem by editing the file:

```
/opt/arcsight/logger/data/mysql/my.cnf to set innodb_buffer_pool_size = 512M  
(the default was 128).
```

Then restart all services.



DB Don't and Do's

•Oracle Best Practices:

–Search Protect 724 <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 with by adding parameters
- Customers have encountered unrecoverable corruption – also lost data

CORR-E do's:

- Open a support ticket and ask about any parameters you want to add or change first!



Places to go 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>



Thank you

