ACID: Managing Alert Databases (Purging and Archiving)

Depending on a number of factors (e.g. rules set, number of sensors) the Alert database generated by Snort will eventually grow quite sizable. This sheer number of alerts makes any type of analysis, both human or via automation (e.g. ACID), quite cumbersome and slow. Therefore, several strategies need to be employed to decrease the size of the effective Alert database.

Purging (Deleting,Trimming) Alerts

The most obvious strategy to help mitigate the size of the Alert DB is simply to delete alerts. This action is quite appropriate and convenient when dealing with alerts that are false positives. Alerts can be deleting by following these steps:

1. Run the query which contains the alerts to be selectively deleted.
2. At the bottom of the query results will be an 'Action' box.

   From the left-most 'Action' combo-box choose 'Delete'.

   The text-box following the combo-box should be left blank

   Finally, the alerts which will be deleted need to be specified. This selection is achieved by choosing one of the three 'Action' buttons.

   - *Selected*: delete those alerts which have been checked (note the check boxes in the extreme left-hand column)
   - *ALL on Screen*: delete all alerts currently displayed on the screen
   - *Entire Query*: delete all alerts in this query/report

Archiving Alerts

Another strategy to shrink the size of the active database is to archive the already analyzed alerts into a separate database. In this manner, the "current" active database will remain manageable, but the already analyzed alerts are still preserved. Alerts can be archived by following these steps:

1. In preparation to archive alerts, a separate database must be created. This archive database must be the same schema version as the one from which alerts will be copied. Therefore, use the appropriate `create_mysql/create_postgresql` script from the Snort distribution.
2. Update the `$archive_dbname, $archive_host, $archive_user, $archive_password, $archive_port` variables in the ACID configuration file `acid_conf.php` to reference the archive database
3. Run the query which contains the alerts to be archived
4. At the bottom of the query results will be an 'Action' box.

   From the left-most 'Action' combo-box choose 'Archive'. There are two types of archiving: "Archive -- copy", and "Archive -- move". The former action merely archives the specified alerts into the appropriate database, while the latter archives the alert into the alert database and then deletes these alerts from the current alert DB.

   The text-box following the combo-box should be left blank

   Finally, the alerts which will be archived need to be specified. This selection is achieved by choosing one of the three 'Action' buttons.

   - *Selected*: archives those alerts which have been checked (note the check boxes in the extreme left-hand column)
   - *ALL on Screen*: archives all alerts currently displayed on the screen
   - *Entire Query*: archives all alerts in this query/report