Device SubSection Data Retention Options

With the release of Open-AudIT 3.1.0 we have massively expanded the options around keeping and processing data from devices.

SubSections of a device within Open-AudIT refers to the many tables that hold specific data types - software, netstat ports, processors, memory, disks, users, groups, etc, etc.

These options exist (for now at least) in the Configuration of Open-AudIT. The items of interest are create_change_log* . and delete_noncurrent*.

We previously had these options for a couple of select couple of Subsections, but have expanded these to cover every subsection.

Create Change Logs

The items named create_change_log_* use the database table names to specify which subsection they apply to - so create_change_log_software and create_change_log_memory are both valid examples. You can override ALL items by setting create_change_log to "n" - this will stop any change logs being generated, regardless of the individual table setting. So if a device has a piece of software added (for example), a correspond change log would not be inserted if create_change_log_software was set to "n". This is set to "y" by default. This matches how Open-AudIT has always worked.

Special Items

We have also introduced three special configuration items for Netstat Ports. Because ports above 1024 are mostly designed to be dynamic, we now provide three options to keeping this data. **create_change_log_netstat_registered**, **create_change_log_netstat_well_known** and **create_change_log_netstat_dynamic**. These options correspond to the ports 0-1023, 1024-49151 and 49152-65535.See https://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers. In particular, Windows DNS servers open a LOT of ports high in the range that are (in my opinion) silly to keep track of, see here and here. By default, only create_change_log_netstat_registered is set to "y". We may add to these options in the future for other subsection, if required.

Delete NonCurrent Items

Along similar lines, the configuration items for delete_noncurrent* use the database table names to specify which subsection they apply to. If set to "y", then no historical entries will be kept for that table, only the "current" items as at the last audit (or discovery). Again, these individual items can be overridden by the global "delete_noncurrent" item. If set to "y", it will remove all noncurrent items from all tables. This is set to "n" by default. This matches how Open-AudIT has always worked.

Hopefully these options provide some customisability for you to only keep the data you actually need.

Onwards and upwards.

Mark Unwin.