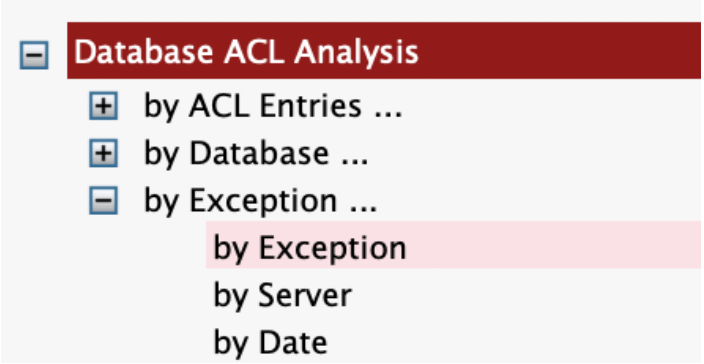
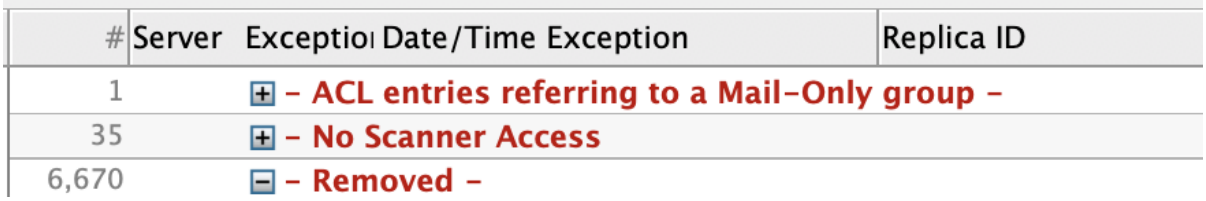
Analyzing ACLs: Identifying Mail-Only groups used in database ACLs

Go to the "Database ACL Analysis – by Exception" view:



Databases are categorized by exception - one possible category being "- ACL entries referring to a Mail-Only group -":



If you don't see such a category after a scan, then none of the scanned database ACLs contain any Mail-Only groups.

If a mail-only group is added to a database ACL, the members of that group are NOT granted access to the database via that ACL entry. This can lead to a case where a group of users doesn't have as much access as they're supposed to have, or even worse, they have more access than they should. For example, if a mail-only group is used to indicate that a group should have no access to a database, the database ACL will ignore that entry and users might have access anyway!

Note that exceptions are not cleared from this view if they are resolved in the respective database – they remain in the SecurityInsider database with the date/time stamp of when the problem was last encountered for documentation purposes; you can simply manually delete (all or selected) exception documents if you do not wish to keep a history of (certain) exceptions.