Retrieve Zombie Attachments

Files uploaded to RiskVision as evidence, documents stored in the Document Repository, or attachments on RiskVision objects like entities and tickets, will appear in 3 places:

- **User Interface:** You will see the document and its link within the UI where the file was uploaded.
- **RiskVision Database:** The file will have a record in the database that contains metadata such as the name and upload date. The file will also point to where it is stored on the RiskVision file system.
- **RiskVision's File System:** After being uploaded to RiskVision, the file is stored in the RiskVision server's data folder.

Files uploaded to RiskVision should always exist in each of the above 3 places. However, there are situations in which a file may be deleted through the UI and as a result be deleted from the database, but not from the file system. This would result in unneeded files residing in the file system. These files, referred to here as zombie attachments, can cause undue strain on the system by taking up memory and storage. In order to better maintain the system, RiskVision provides a way to identify and access the zombie attachments in the file system so they can be deleted.

Zombie database records may also exist. Zombie database records represent records in the database that don't have related files in the file system. There should not be any such records, and the zombie database report will provide proof that there are none. If such records exist, please contact Resolver Support.

The below steps will extract the zombie attachments as two separate .CSV reports: one for database zombies, and another for file system zombies. The database report contains the following columns:

- **Attachment ID:** The ID number of the attachment.
- **Path ID:** The ID of the file path for an object in the file system.
- **Owning Object ID:** The ID number of the object that the attachment is attached to.
- **File Name:** The file name of the attachment.
- **File Version:** The version number of the attachment.
- **Who Uploaded:** The RiskVision user name of the user who uploaded the attachment.
- **Content Type:** The type of file the attachment is.

The file system report contains the following columns:

- **Path ID:** The ID of the file path for an object in the file system.
- **Hash Filename:** The name of the attachment in the file system.
- **RiskVision Object Type:** The object type of the zombie attachment.
- **File Size (Kb):** The attachment's file size in kilobytes.
- **Last Modified:** The date and time that the attachment was last modified.
- **File Path:** The location of the attachment in the file system.

> The **RISKVISION_HOME\config\agiliance.properties** file contains a `com.agiliance.attachments.extractor.tool.encryptionCheck.excludedContentTypes` property to exclude certain file types from being extracted by the below steps. This property stores file types to be excluded as a comma-separated list and it excludes network paths and web links by default. Ensure that you check this property so the tool only extracts what you want it to.

To access zombie attachments:

1. Open the command prompt in administrator mode and navigate to the **RISKVISION_HOME\install\toolbox\bin\**.
2. Run the `attachmentExtractionTool.cmd` command.
3. **Optional:** The following options can be used in the command line to modify how the zombie attachments are extracted:
    - **{f,-force-pre-process}:** Reloads the file system after changes have been made.
    - **{v,-verbose}:** Produces additional information on the files in the file path, including whether or not they are zombie attachments.
    - **{w,-show-object-types}:** Shows all the available RiskVision object types.

  - **{t,-object-types}:** Extracts zombie attachments of the specified object type(s). The user must enter a comma separated list of RiskVision object types, a total list of which can be viewed by using the above **-w** command. For example, `attachmentExtractionTool.cmd -t ComputerSystem,OperatingSystem,Asset`. Entering no values will only extract entities of the **Application** object type. Entering `attachmentExtractionTool.cmd -t All` will extract all zombie attachments from the database and file system, regardless of object type. This command is useful for focusing on specific object types in a smaller report after running a full report of all zombie records.

  - **{y,-copy-zombie-attachments}:** Copies the zombie attachments from the file system to the **RISKVISION_HOME\install\toolbox\bin\ZOMBIE_ATTACHMENTS\Copied_ZOMBIE_ATTACHMENTS** folder. If the user uses this command, the attachments will only be copied and will still remain in the file system. This command will not affect any attachments in the database.

  - **{o,-output-dir}:** Creates a folder to store the extracted attachments. By default, the attachments will be saved to the **ZOMBIE_ATTACHMENTS** folder under the current directory.

  - **{h,-help}:** Lists all the optional commands available in the `attachmentExtractionTool.cmd` command.

4. The file system and database zombie attachments will be extracted as two separate .CSV files under the **RISKVISION_HOME\install\toolbox\bin\ZOMBIE_ATTACHMENTS** folder.