Use the following procedure to list the files on disk which are currently in the resident state and to narrow down the list by the number of allocated disk blocks.

Note: This method potentially detects a false positive issue such when the block allocation was round up to the next block size boundary which is equal to the stub file size, when the file was originally created as the sparse file, or when the file is small enough to fit in inode in case the stub file size is set to 0. This method may not be able to detect a file in case the stub file size setting has been changed during the life of the file.

Related Alert:
> https://www.ibm.com/support/pages/node/6415807

Prerequisites:
- Complete the check and recovery using the script procedure in the separate zero-check.README.
- Download the show_reg_stub.policy file from Fix Central.

Policy Procedure:
> 1. Determine the IBM Spectrum Scale file system under the management of IBM Spectrum Archive EE, by running "mmlsfs all -ziBT" command. This procedure should only be performed on DMAPI-enabled file systems.

> Example of result:

```
# mmlsfs all -ziBT

File system attributes for /dev/fs1:
===================================
flag        value              description
------------------ ----------------------- ----------------------------------
 -i        4096              Inode size in bytes
 -B         262144             Block size
 -z         Yes              Is DMAPI enabled?
 -T         /ibm/fs1           Default mount point
```

> 2. Identify the current setting of stub file size of the file system, by running "dsmmigfs query -D" command with the default mount point from step 1.

Example of result:

```
# dsmmigfs query -D /ibm/fs1
IBM Spectrum Protect
Command Line Space Management Client Interface
 Client Version 8, Release 1, Level 11.0
 Client date/time: 03/01/2021 18:47:27
(c) Copyright by IBM Corporation and other(s) 1990, 2020. All Rights Reserved.

File System Name:   /ibm/fs1
High Threshold:      90
Low Threshold:      80
Premig Percentage:   10
Quota:         10240
Stub Size:      262144
Read Starts Recall:   no
Preview Size:      0
Server Name:       SERVER_A
Max Candidates:     100
Max Files:      0
Read Event Timeout:   600
Stream Seq:      0
Min Partial Rec Size:  0
Min Stream File Size:  0
Min Mig File Size:   0
Inline Copy Mode:    MIG
Preferred Node:    spectrumscale      Node ID: 1
Owner Node:       spectrumscale      Node ID: 1
```

3. Remove the list.show_reg_stub file under /tmp directory, if it exists.

4. Run the sample policy (show_reg_stub.policy) by using mmapplypolicy command.   If the stub file size for the file system is set to non-0 value at step 2, then specify the value as STUBSIZE_IN_BYTES.

Example:

```
# mmapplypolicy mountpoint -P show_reg_stub.policy -I defer -f /tmp -M STUBSIZE_IN_BYTES=0
```

NOTE: The *mountpoint* parameter of mmapplypolicy command should be substituted with the actual mount point. See example in step 1.
The example assumes the show_reg_stub.policy file is in the current directory. If it is placed in a different directory, specify the full path filename.

5. Find the list.show_reg_stub file under /tmp directory. Each line of file consists of 5 numbers followed by the double dash and the file name. The first 3 numbers are the file identifiers. The 4th and 5th numbers are the amount of allocated disk blocks and the logical file length, both in bytes.

Example of result:

```
 36426 182015648 0  0 1048576 -- /ibm/fs1/suspiciousfile
```

The listed files that are potentially affected by this problem are those whose allocated disk blocks match the stub file size.

Check the content of listed file by reading the file using an application to determine if a recovery is required or if it is a false positive. Contact IBM Support with the list.show_reg_stub file and all the files under the metadata directory, for the further analysis to see if the original data is still available and recoverable on the tape.

6. Rename /tmp/list.show_reg_stub file before applying the policy procedure to other file system.

7. Repeat step 2 through 6 for each DMAPI-enabled file system.