

# My Experiences Activating the FSEXEC Resource Class

Joel Tilton  
RACF Engineer  
Mainframe Evangelist  
October 2018

# About Joel Tilton, CISSP



- Joel Tilton is a former employee of IBM, where he got his start with mainframes, who continues to champion mainframe security issues and solutions.
- Over 20+ years technical IT experience, the majority of which was gained in hands-on technical roles, performing a variety of duties in diverse and complex environments.
- The majority of Joel's experience is focused on IBM mainframe systems, where he performs as a Technician and Project Manager. Joel's specialist subject is IT Security, in particular z/OS and associated subsystems (CICS, DB2, MQ, zSecure, etc.) security with RACF.
- Joel is also an active member of the Tampa Bay RUG (RACF User Group) which meets jointly with the NY RUG. Joel has a true passion for security and the mainframe. Long live the mainframe!
- <https://www.linkedin.com/in/joeltilton>
- [RACFEngineer@gmail.com](mailto:RACFEngineer@gmail.com)
- 702-483-RACF(Google Voice) ← Because it's cool!

# Disclaimers

- All products, trademarks, and information mentioned are the property of the respective vendors.
- Mention of a product does not imply a recommendation.
- Always test new profiles on a non-production system.
- Only you can prevent IPLs...
- The views expressed are his own personal views, and are not endorsed or supported by, and do not necessarily express or reflect, the views, positions or strategies of his employer



# Agenda

- FSEXEC – Available with z/OS 2.2
- SETR CLASSACT & More
- Securing the Unknown
- Wherefore art thou SMF?
- Calls to FSEXEC in One Month
- What “thingy” typically calls FSEXEC ?
- Suggestion, Start Small
- RFEs
  - Because IBM developers need work! 😊
- Wrap Up



# FSEXEC – How It Works

- Think of it as “Front Door” Access Check
  - Without access I’m stopped at the door by the bouncer
  - Do NOT Pass Go; Do Not Collect \$200
- Superuser, auditor, or read-only auditor privilege does **NOT** override FSEXEC denial of access.
- RACLIST Required
- FSEXEC restriction does not apply to file systems mounted with the '-s nosecurity' option.
  - So verify how your file systems are mounted!
- [https://www.ibm.com/support/knowledgecenter/en/SSLTBW\\_2.3.0/com.ibm.zos.v2r3.icha700/reaiazotfs.htm](https://www.ibm.com/support/knowledgecenter/en/SSLTBW_2.3.0/com.ibm.zos.v2r3.icha700/reaiazotfs.htm)

# Class Activation

- **SETR CLASSACT(fsexec) AUDIT(fsexec)  
GENERIC(fsexec) RACLIST(fsexec)**
  - GENERIC ( ) means GENCMD ( ) too
  - However NOGENERIC does not include NOGENCMD!
  - When in doubt always code GENERIC & GENCMD
    - Thanks to Julie Bergh for that tip!
- **RDEFINE RACGLIST FSEXEC OWNER ( )**
  - IPL will not refresh in-storage RACF profiles
  - Ensure Sysplex Consistency for RACF
  - By Product...Performance Improvement
  - **SETR classact(RACGLIST) audit(RACGLIST)**
  - **SETR RACLIST(...) REFRESH**
    - Builds RACGLIST profiles

# Securing the Unknown

- Everything is going great when we have
  - SMF
  - ICH4o8l
    - Well maybe not “great” when we get security violations
    - At least we have a “hint” of where is the problem
- But what would we do if none of these are available?
- There’s always exits
  - But do we have the time or expertise?
- How do you secure a resource when you can’t find any bread crumbs?



# Wherefore art thou SMF?

- Where oh where has my SMF gone?
- AUDIT(ALL(READ)) but still don't get SMF?
  - RACROUTE ... LOG=NONE
    - Alas the software has decided the security engineer doesn't get to control logging! ☹️
- Never give up, never surrender!
- PMR IBM to death of course 😊
  - I Love the smell of Sev 2 PMRs in the morning!
  - But IBM takes time to build fixes ☹️
  - So PMR is the "long game"



# Wherefore art thou SMF?

- If you really want a Nor'easter of SMF....
- SETR LOGOPTIONS(ALWAYS(class\_name))
  - Check with your systems programmer first!
  - And still duck if SMF starts dumping like crazy...
  - I still remember the day when some did this:
    - RALT PROGRAM \*\* AUDIT(ALL(READ))
      - BONUS QUESTION: Why did that cause pain?
      - HINT: SYS1.TCPIP.SEZALOAD



# 50,766,830 FSEXEC Calls – 1 Month

```

IBM Security zSecure ACCESS summary
Command ==>
Access monitor records - Classes like FSEXFC
Occurrence Class First occurrence Last occurrence
50766830 FSEXEC 9Sep2018 00:42 30Oct2018 08:27
Occurrence Profile key used
50766830
Occurrence Intent Type RetAll AccRC
50766830 UPDATE Fast 4
Occurrence Resource
4 SYSP.PGRP.OMVS.BFORGE.AGTBAS.DIR
17 SYSP.PGRP.OMVS.CERT.GCU.DIR
43 SYSP.PGRP.OMVS.CICS.ZFS.DIR
148 SYSP.PGRP.OMVS.CTG.ZFS.DIR
168 SYSP.PGRP.OMVS.DB2B10.M1.DIR
2397730 SYSP.PGRP.OMVS.DOVETAIL.USERLOGS.DIR
7403777 SYSP.PGRP.OMVS.DOVETAIL.V5R1M1.DIR
1031 SYSP.PGRP.OMVS.DTCDIRS.BOX.SERVER.DIR
255 SYSP.PGRP.OMVS.DTCDIRS.PKISERV.DIR
48 SYSP.PGRP.OMVS.DTCDIRS.DIR
1001 SYSP.PGRP.OMVS.DTCDIRS.WMB.DIR
62449 SYSP.PGRP.OMVS.JAVA.DIR
16366 SYSP.PGRP.OMVS.JAVA.1.DIR
11618 SYSP.PGRP.OMVS.JAVA.DIR
354726 SYSP.PGRP.OMVS.JAVA.DIR
362821 SYSP.PGRP.OMVS.MPT.DIR
1608 SYSP.PGRP.OMVS.MQM.PB.DIR
163003 SYSP.PGRP.OMVS.NONSP.DIR
257 SYSP.PGRP.OMVS.SYSTEMS.DIR
96 SYSP.PGRP.OMVS.WAS.ZOSCONN.V3R0.DIR
6565 SYSP.PGRP.OMVS.WASIHS.DIR
15106 SYSP.PGRP.OMVS.WAS.BBO.SBBOHFS.DIR
3373 SYSP.PGRP.OMVS.WAS.BBO.SHAPHFS.DIR
108 SYSP.PGRP.OMVS.WAS.BBO.SIWOHFS.DIR
2 SYSP.P001.OMVS.BMC.DIR
108 SYSP.P001.OMVS.DYNATR.AGENT.DIR
26 SYSP.P001.OMVS.MQSI.DIR
78 SYSP.P001.OMVS.DIR
4 SYSP.P001.OMVS.WAS.ZOSCONN.CONFIG.DIR
8 SYSP.P001.OMVS.WAS.DMGR.CONFIG.DIR
26 SYSP.P003.OMVS.MQSI.DIR
8 SYSP.P003.OMVS.DIR
4 SYSP.P003.OMVS.WAS.ZOSCONN.CONFIG.DIR
39619 SYS1.OMVS.PMVS21.ROOT
45 SYS1.OMVS.PMVS31.BBLZFS
39162297 SYS1.OMVS.PMVS31.ROOT
301947 SYS1.P001.OMVS.ETC.DIR
460340 SYS1.P003.OMVS.ETC.DIR

```

# So Who Typically Accesses FSEEXEC?

- Batch UserIDs
- Every SFTP UserID
- Started Tasks
- Anything Using z/OS UNIX
- That's a BIG access list in some cases

# Suggestion – Start Small

- Start with securing of /tmp & /var/tmp
  - A First Step
  - Prevent Trojan Horses
- Interestingly enough that means
  - Creating a new mount point
- Profiles in FSEEXEC are the underlying name of MVS dataset name that contains the mounted zFS file system
- Based on analysis, can't really set up a profile just for /tmp today
  - /tmp is a part of / i.e. root file system
- Befriend the managers of your systems programmers!

# RFEs – Please Vote

- To my knowledge, no caching
- Reduce CPU time for UNIX file security especially if you have FSACCESS on (116261)
  - Uncommitted Candidate → 20 Votes
  - 20 Votes



# UNIXPRIV

## SUPERUSER.FILESYS.DIRSRCH

- Users with READ access to SUPERUSER.FILESYS.DIRSRCH profile in the UNIXPRIV class can list files in a directory
- Security improvement
  - So having access to the data itself is no longer necessary?
  - Should those of us administering permission bits only need READ to SUPERUSER.FILESYS.DIRSRCH \*instead of\* SUPERUSER.FILESYS?
  - It Depends. Your Mileage May Vary.
- Available with z/OS 2.2

# Summary

- Turning on FSEXEC is not hard
- Trying to secure individual UNIX directories will be the challenge
  - /tmp only? Need to change to its own mount point
- 50 million calls to RACF in a month
  - 39 million for root file system
- Start small and grow
- Vote for RFEs!
- Your Mileage May Vary



# Questions?

