

Practical Steps to Implement a New Resource Class

Joel Tilton
RACF Engineer
Mainframe Evangelist
March 2017

About Joel Tilton

- 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
- 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

- Where to start
- Wherefore art thou SMF?
- My Country for an ICH₄o8l?
- Real World Example: zEDC FACILITY Resource
- ISV Software has a solution
- Endless Possibility
- Security Analytics
- Not a replacement for SMF
- Summary



ABSTRACT

- Have you ever had to define RACF rules for a new resource class or a new piece of software when the info you needed to do it easily just wasn't available?
- In this presentation Joel describes the commonly used "standard" techniques and explains why they sometimes don't work.
- He then shows an improved technique using commonly available reporting/analytic tools and a real-life example of how he applied it in real life

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



My Country for an ICH4o8l

- So we can not find SMF
- We can not find ICH4o8l
- Thanks to some design that thinks the RACF profiles / SETR options should not be the decision makers for logging
 - Why on Earth do software developers ever think this is a good idea!
 - Oh wait some customers are annoyed by too much logging!
- Sometimes this is a good thing
 - SDSF
 - Imagine all the SAF calls made just to build your SDSF menu options
- But without any trail at all what do we do next?
- What do I grant access to?
 - READ UPDATE CONTROL ALTER ?????????????????????????????????
- Thoughts?

A Real World Example - zEDC

- FACILITY FPZ.ACCELERATOR.COMPRESSION
 - zEDC: hardware accelerated 100% CPU FREE DASD Compression
 - zEDC SAF check for problem state callers
- The profile didn't exist a year ago
- And then someone defined the profile with UACC(NONE) AUDIT(FAILURES(READ)) a few months ago
 - Which is "typical" but I'd like to do a one year analysis of all SAF checks for FPZ.ACCELERATOR.COMPRESSION
 - So I can set up the access to ensure everything that needs access has access
- Set AUDIT(ALL(READ)) and wait for the next ICH4081 message? I think not.....

Enter ISV Software

- IBM Security zSecure
 - Access Monitor a part of zSecure admin
 - <http://www-03.ibm.com/software/products/en/zsecure-admin>
- Vanguard Integrity Professionals
 - Vanguard Cleanup
 - <https://www.go2vanguard.com/mainframe-security-software/administration/cleanup/>

The Concept

- Utilize RACF exit points
 - ICHRCX02, ICHRDY02, ICHRFX04, ICHRIX02
 - Deployed by STC using Dynamic Exit Services
 - Code DIRECT BRANCH parm for best performance
 - Intercepts all AUTH, FASTAUTH & VERIFY events
- Catching the SAF call and buffering data at the time we call RACF
 - 32 – 16 MB Buffers – and now up to 32 – 1 GB Buffers!
- So we can find security calls today and not wait for SMF to generate assuming you can even get SMF (LOG=NONE)
 - I generally like at least 3 months of data; yearly roll ups available
- This gives us a real opportunity to do analytics

The Benefit

- I can now find Unknown Unknowns
- I would say we have actually solved the Unknown Unknown problem
- Using SAF & the RACF Exits you can find all calls ever made for all security decisions
 - No waiting for SMF to accumulate
 - No scanning through syslog for ICH408i
 - Software products make this data manageable
 - Some assembly required
 - Batch jobs, GDGs, not rocket science
 - And modern Virtual Tape Systems now do MIGRAT2 at MIGRAT1 speeds!
 - Only downside so far
 - RACROUTE REQUEST=LIST,GLOBAL=NO (Legacy...no benefit)

Find ALL SAF Calls Easily

IBM Security zSecure ACCESS summary

Command ==> All access monitor records, No profile found 13 Mar 2017 18:48

Occurrence	Class	First occurrence	Last occurrence
7258	\$OMCAN	25Apr2016 16:47	25Apr2016 16:47
1	\$BBS	16Mar2016 14:34	26Feb2017 12:32
1	\$CDTSCTL	21Nov2016 07:15	21Nov2016 07:15
100199	\$CDTSRTE	1Mar2016 12:50	1Mar2017 10:00
3130667	\$CHGMAN	1Mar2016 16:12	1Mar2017 09:30
39682150	\$C4RVFY	1Mar2016 11:13	1Mar2017 09:57
153296	\$DTRKRTE	1Mar2016 12:50	1Mar2017 10:00
1	\$FTPCNTL	21Oct2016 17:46	21Oct2016 17:46
1	\$MQCHNL	21Jun2016 11:08	21Jun2016 11:08
889	\$VPS	28Jul2016 14:49	23Feb2017 17:29
51	\$XACT	14Apr2016 23:02	14Feb2017 00:02
6	ACCTNUM	4Mar2016 20:57	9Jan2017 14:30
105337	APPCPORT	23Mar2016 19:47	29Sep2016 01:00
1	APPCSI	11Dec2016 15:31	11Dec2016 15:31
13	CDT	18Jun2016 13:30	10Jan2017 21:57
1	CFIELD	15Jul2016 17:19	15Jul2016 17:19
1	DIGTCERT	27Oct2016 16:18	27Oct2016 16:18
1	FIBROLE	23Jun2016 14:26	23Jun2016 14:26
109868439	FACILITY	1Mar2016 10:00	1Mar2017 10:00
151999	FIELD	2Mar2016 15:53	28Feb2017 19:11
39643491k1	FSACCESS	21Apr2016 13:33	1Mar2017 10:00
5	G\$ATPTRN	20May2016 12:41	7Feb2017 13:20
25	G\$DTCTRN	27Jun2016 20:26	3Nov2016 15:14
4	G\$NSCTRN	7Jun2016 12:01	7Feb2017 16:50
8	G\$PTSTRN	29Jun2016 15:12	30Aug2016 13:08
2	GLOBAL	10Oct2016 23:46	13Oct2016 15:45
12	GTERMINL	24May2016 20:36	23Feb2017 15:16
8	GXFACILI	1Sep2016 18:19	1Sep2016 18:19
62196	LOGSTRM	17Mar2016 18:16	1Mar2017 09:45
1	NETSPAN	27Apr2016 07:28	27Apr2016 07:28
1	NODES	3Jun2016 15:27	3Jun2016 15:27
8	OPERCMD5	1Apr2016 12:36	9Oct2016 00:02
2	PA@EL	20Mar2016 01:15	21Mar2016 20:04
15	PROGRAM	21Mar2016 19:13	24Jan2017 18:47
13	PTKTDATA	28Sep2016 22:13	30Nov2016 11:03
2	RACFVARS	21May2016 22:15	16Jul2016 04:03
8	RACGLIST	23Mar2016 19:47	12Jan2017 14:23
764685	RDATA LIB	18Mar2016 21:58	1Mar2017 10:00

*ZSECURE SDSF WORK -WORK UDLIST

4B :00.1

Easy Analysis for RC 04

IBM Security zSecure ACCESS summary

Command ==>

```
All access monitor records, No profile found      13 Mar
Occurrence Class      First occurrence Last occurrence
 109868439 FACILITY    1Mar2016 10:00  1Mar2017 10:00
Occurrence Profile key used
 109868439
Occurrence Intent      Type      RetAll AccRC
 2320868  READ      Fast      4
Occurrence Resource
 1040 ERBSDS.MON3DATA
 186703 FPZ.ACCELERATOR.COMPRESSION
 21 IXCNOTE.$$TM.JES2
***** Bottom of Data *****
```

IBM Security zSecure ACCESS summary

Command ==>

```
All access monitor records, No profile found      13 Mar
Occurrence Class      First occurrence Last occurrence
 109868439 FACILITY    1Mar2016 10:00  1Mar2017 10:00
Occurrence Profile key used
 109868439
Occurrence Intent      Type      RetAll AccRC
 2320868  READ      Fast      4
Occurrence Resource
 186703 FPZ.ACCELERATOR.COMPRESSION
Occurrence Userid      Name
 93      MESSAGE BROKER
 1665    SCHEDULER ID
 8638    SCHEDULER ID
 1861    SCHEDULER ID
 1203    SCHEDULER ID
 1195    SCHEDULER ID
 75      SCHEDULER ID
 75      SCHEDULER ID
 795     SCHEDULER ID
```

Lots of Useful SAF Flags

```

IBM SECURITY zSecure ACCESS Summary                                     L11E 1 C
Command ==>                                                         Scroll==>
Access monitor records for Classes like FACILIT 13 Mar 2017 19:59

Access summary
Security complex name
RACF userid                                MESSAGE BROKER
Access intent                              READ
Record type                               Fast
System name
SAF resource class                         FACILITY
SAF resource name                         FPZ.ACCELERATOR.COMPRESSION
Timestamp of last occurrence               23Feb2017 14:39
Access count                               93

Request flags                             Define flags
RACFIND                                    Command
Limit to generics                          No          Use internal RACROUTE AUTH
Private/CSA (no global)                    No          Verify
Retrieval of access allowed                 Propagated

Access time effect
RACF class and profile                     FACILITY
RACF Profile type used                     missing
Access allowed                             NONE
RACF return code                           4

Access flags (common)
Obtained generic                           No
Undefined user                             No
Global access table used                   No
Special authority used                     No
Operations authority used                  No

Access flags (rare)
Privileged/trusted user                    No
Group used                                  No
Installation exit used

Access-time user attributes
User systemwide SPECIAL                    No
User systemwide OPERATIONS                 No
***** Bottom of Data *****

```


Imagine the Possibilities

- Live troubleshooting of security issues that have no SMF or ICH408I message
- C2PACMON will take a MODIFY command to release its “current” logging dataset
 - Then that data set from today’s accumulated SAF calls can be analyzed
- Think about what that means.....
- Without any SMF or ICH408I I can troubleshoot security problems that I didn’t know existed

Analyze & Quantify Security

- Senior Management Likes Numbers
- Quote how many calls there were to RACF
 - Break down by Class, UserID, Jobname
- Analyze volume of SAF calls
 - Why so many for XYZ class? Performance!
- Analyze why access is still in place if its not being used



Not a replacement for SMF

- These are security analytic tools
- Not a replacement for
 - SMF
 - Real time security monitoring by a SIEM
- They will help you:
 - Find things you did not know existed
 - Find new things to secure
 - Find existing profiles that perhaps need logging set
 - Clean up stale Access Entries.
 - If not used in more than a year why is it still there?

Summary

- Try not. Do...or do not. There is no try!
 - Master Yoda
- You've been show how to roll out RACF protection for a new resource class or piece of software when the standard techniques aren't sufficient
- You've also been shown the thought process behind the advanced techniques.
- We hope this adds a useful tool to your toolbox



Questions?

