

IDUG

2024 NA Db2 Tech Conference

Considerations for Migrating Db2 Security to RACF

Ray Overby <u>roverby@rocketsoftware.com</u> Jørn Thyssen <u>jthyssen@rocketsoftware.com</u> Rocket Software

Session Code: SEC2 | Platform: z/OS

Agenda

- Native Db2 Security
- Why use RACF for Db2 security
- Migration process to convert to RACF security
- Best practices for your Db2 security
- Helpful tools to use when using RACF security

Db2 security



https://www.ibm.com/do cs/en/db2-forzos/13?topic=securingdb2

Db2 native security

- Original implementation
 - In effect if DSNZPARM SECURE=YES
- Managed through GRANTs and REVOKEs
- Stored in 13 SYSIBM.SYSxxxAUTH tables
 - System level privileges, object level privileges, column privileges, ...
 - <u>https://www.ibm.com/docs/en/db2-for-zos/12?topic=catalog-tables-privilege-records</u>
- Security managed by SYSADM, SYSCTRL, ACCESSCTRL, install SECADM
 or users with WITH GRANT option or ownership of object or ...
- Db2 z/OS V10 introduced SEPARATE_SECURITY
 - Prevents SYSADM and SYSCTRL from issuing GRANT/REVOKE

Db2 native security

• Db2 Vendor tools all support native security

DB2 Admin Command ===>		DS	SAD Sys	stem Pi	riv	'i 1	eg	jes	Αι	ıth	or	iza	ti	ons	5	S S	lov	v 1 577	L t	0	8 ^	of CS	₹8 SR	\$
Commands: RE Line command R - Revoke I - Interpr RE - Grante ? - Show al	VOKE GRA s: GR - Gra etation e role R l line co	NT nt R - mma	SYSAU - Grant ands	JTH RM	MIM le		BSDS	C	RE4	ATE A L T	ΗΣH		SHOND			5×540	SYSCE	SYSOP		EXPL<	SQL40	SYDB4		AUCEV
Sel Grantor	Grantee *	G T *	Grant *	date	H G *			B A *	B S C C	A S *	A B *	R E	A C *	Ğ T * *		M *	R L *	R *	S МШ*	A H N *	М	A D M *	1 00*	SC*
SYSIBM SSUSER1 SSUSER1 SSUSER1 SSUSER1 SSUSER1 SSUSER2 SSUSER1 ****	SYSOPR PDZTEAM PDBUILD PDZT1 PDZT2 SSUSER2 SSUSER1 ROLE1	- ***	1985-0 2023-0 2023-0 2023-0 2023-0 2023-0 2023-0 2023-0 2023-0 2023-0	04-01 08-01 08-01 08-01 08-01 08-01 08-01 08-01 08-01 04-08 ** END	- SSSSSS		-)B2	- 2 D	 AT4							- - - - - - - - - - - - - - - - - - -		G						

Db2 native security

- A couple of vendors have built capabilities to do RACF-like administration of native Db2 security
 - Set-up desired auth through users, roles, objects, applications with wildcard support & optional expiry
 - GRANT/REVOKE auth in Db2 based on desired auths

- Manage Pending	P	rivileges Row 1 to 13 of 29 Scroll ===> PAGE
DISFAILED roup GP - Group ID ? - Show all	pr li	ivilege I - Interpret ne commands
Privilege Name *	P *	Statement *
>		>
READTAB	Ν	GRANT SELECT, UNLOAD ON TABLE
READTAB	Ν	GRANT SELECT, UNLOAD ON TABLE
READTAB	Ν	GRANT SELECT, UNLOAD ON TABLE
READTAB	N	GRANT SELECT, UNLOAD ON TABLE
UPDATETAB	Ŷ	GRANT DELETE, INSERT, UPDATE O
UPDATETAB	Y	REVOKE DELETE, INSERT, UPDATE
UPDATETAB	Y	GRANT DELETE, INSERT, UPDATE O
UPDATETAB	Y	REVOKE DELETE, INSERT, UPDATE
UPDATETAB	Y	GRANT DELETE, INSERT, UPDATE O
UPDATETAB	Y	REVOKE DELETE, INSERT, UPDATE
UPDATETAB	Y	GRANT DELETE, INSERT, UPDATE O
UPDATETAB	Y	REVOKE DELETE, INSERT, UPDATE
EXECPRIV	N	GRANT EXECUTE ON FUNCTION AD
	- Manage Pending DISFAILED roup GP - Group ID ? - Show all Privilege Name * READTAB READTAB READTAB READTAB UPDATETAB UPDATETAB UPDATETAB UPDATETAB UPDATETAB UPDATETAB UPDATETAB UPDATETAB	- Manage Pending P DISFAILED roup GP - Group pr ID ? - Show all lin Privilege Name P *

Why use RACF for Db2 security – Organizational benefits

- Who is performing Db2 security now?
 - Db2 systems programmers or DBAs
 - Security is not their primary function
- Support for ESM based security was added to Db2 V6 as an alternative to Db2 native security



Why use RACF for Db2 security – Organizational benefits

- Moving Db2 security from where it is today to mainframe security
 - Primary responsibility is Security and Compliance
 - Adherence to security principles
 - Individual accountability
 - Auditability
 - Separation of function
 - Least privilege
- May satisfy an audit requirement
- Align Db2 security with all other mainframe resources

Why use RACF for Db2 security – Technical advantages

- There are several technical advantages
- But: Db2 for z/OS engine and vendor tooling have delivered features and enhancements to reduce this

Why use RACF for Db2 security – Technical advantages

- Security rules are defined outside Db2 in a single system (RACF)
 - Multiple Db2 subsystems can be protected by the same RACF
 - Db2 subsystem does not need to be started to query auth
- Rules can be defined before object exist
 - Also possible with tools that add RACF-like administration of Db2 native security
- Rules persist when an object is dropped
 - Db2 vendor tools supports recreating native authorizations, e.g.,
 - for complex Db2 changes that require drop/recreate
 - Recovery of dropped objects

Why use RACF for Db2 security – Technical advantages

- Eliminates revoke of dependent privileges when a privilege is revoked from a Db2 user
 - Db2 now has ZPARM REVOKE_DEP_PRIV=YES|NO|SQLSTMT
 - for REVOKE_DEP_PRIV=SQLSTMT:
 - REVOKE ... NOT INCLUDING DEPENDENT PRIVILEGES
- A single rule can cover multiple objects
 - RACF Generics (wildcards)
 - RACFVARS
 - Grouping class profiles

Differences between RACF and native Db2 security – some highlights

- Long list of differences and considerations https://www.ibm.com/docs/en/db2-for-zos/13?topic=module-specialconsiderations
- Implicit databases
 - RACF only checks for access against DSNDB04
- Updatable views
- Ownership privileges still apply
- Grants are still possible
- Db2 object names with special characters, blanks, or mixed case
 - Default RACF classes do not allow mixed case
- Db2 objects with long names
- ... review the doc to see if any of these apply to you

Conversion to RACF security

- Step 1 optional, but recommend: Review and cleanup
- Step 2 prepare and customize Db2 RACF exit
- Step 3 Loop: Define, protect, activate, and test
 - Step 3A define RACF classes
 - Step 3B define RACF resources to protect Db2 objects and privileges
 - Step 3C activate and refresh classes
 - Step 3D restart Db2
 - Step 3E test & debug
- Step 4 revoke grants



This Photo by Unknown Author i licensed under <u>CC</u> <u>BY-SA</u>

Review and cleanup

- Optional, but highly recommend
 - Can reduce conversion work significantly
- Review local modifications to Db2 sign-on exit
- Review who have install SYSADM, SYSOPR, SECADM, or high-level database management privileges
- Grants "WITH GRANT OPTION" won't translate properly to RACF
 - ... and you probably don't want to translate them
 - Partially defeats the purpose of migrating to RACF security



<u>This Photo</u> by Unknown Author is licensed under <u>CC BY-SA</u>

Review and cleanup, cont'ed

• Grants to PUBLIC

- will translate to RACF UACC(READ)
- Auditors don't like UACC >= READ
- Look for orphaned grants where GRANTEE does not exist in RACF
 REVOKE
- Look for orphaned objects where owner does not exist in RACF
 - TRANSFER OWNERSHIP

Prepare and customize Db2 RACF exit

- RACF exit source code: DSNXRXAC in hlq.SDSNSAMP
- Assemble and link: Step 3 (JEX0003) in DSNTIJEX
 - Creates load module DSNX@XAC
- Have a copy of both versions of DSNX@XAC so you can switch between native and RACF security easily
- Have processes in place to review and deploy updates to DSNXRXAC delivered through Db2 maintenance or new Db2 versions

Db2 RACF exit options

&CLASSOPT - scope

- 1 single-subsystem scope
 - The class names identify with the SSID, e.g., class name M<ssid>TB1
- 2 multiple-subsystem scope
 - Same class is used for all Db2s; resource name includes the SSID
 - Example: class name MDSNTB, resource name <ssid>.<something>

• Considerations:

- Centralized security team
- Number of classes
- POSITs
- Class sizes
- Class options, e.g., ASIS
- Class refresh disruptiveness

VIEW SSUSER1 Command ===>	.SDSNSAM	P (DSNXRXAC	C) - 01.00 R	ecovery p	rocessed ==> <mark>CSR</mark>
*****	******	*****	**** Top of Data **************		****
000001 DSNX@XAC TI	TLE 'RAC	F/DB2 Exte	ernal Security Module - Symbols'		
000002 SY:	SSTATE A	RCHLVL=1		@L 3A	0002000
000003 *					0003000
000004 * Global SE	T Symbol	s: See \$SE	T for a description		0004000
000005 *					0005000
000006	GBLC	&CLASSNMT	,&CHAROPT,&CLASSOPT,&ERROROPT	@09C	0006000
000007		&PCELLCT,	&SCELLCT, &XAPLDBCK		0007000
000008 &CLASSOPT		'2' 1	Use Classification Model I		0008000
000009 .*			(One set of classes for EACH s	ubsys)	0009000
000010 .*		2	! - Use Classification Model II		0010000
000011 .*			(One set of classes for ALL su	bsys)	0011000
000012 &CLASSNMT		'DSN' 🛛)B2 Subsystem Name (Up to 4 chars)		0012000
000013 &CHAROPT		'1' C	ne character suffix (0-9, #, @ or	\$)	0013000
000014 &PCELLCT	SETA	50 P	Primary Cell Count		0014000
000015 &SCELLCT	SETA	50 S	Gecondáry Cell Count		0015000
000016 &ERROROPT		'1' 1	Defer to DB2 authorization if	@L 3C	0016000
000017 .*			exit abends, sets terminating	@09A	0017000
000018 .*			return code(12), or sets an	@09A	0018000
.*			unexpected return code.	@09A	0019000
000020 .*		2	! - Terminate DB2 if	@09A	0020000
000021 .*			exit abends, sets terminating	@09A	0021000
000022 .*			return code(12), or sets an	@09A	0022000
000023 .*			unexpected return code.	@09A	0023000
000024 *					0024000
000025 &SERVICELEV	L SETC	'PH24314'	Release/APAR number (up to 7 ch	ars) @LGC	0025982
000026 *			This symbol is for IBM use onl	y.	0026000
000027 *					0026500
000028					0027000
000029 TT	F 'RAC	F/DB2 Exte	rnal Security Module - Prolog'		0028000

For DSGs the group attach name is used

Db2 RACF exit options, cont'ed

&CLASSNMT (for &CLASSOPT=2 only) – class name root

- Default is DSN, e.g., MDSNTB
- &CHAROPT (ignored for &CLASSMNT=DSN) class name suffix
 Default is 1: M<ssid>TB1

<u>F</u> ile	<u>E</u> dit	E <u>d</u> it_S	ettings	<u>M</u> enu	<u>U</u> til	lities	<u>C</u> ompile	ers	<u>T</u> est	<u>H</u> e]p			
VIEW	SSU	SER1.SI	DSNSAMF	(DSNXRXA	4C) -	- 01.00					Recove	ry pi	rocessed
Command	===>	de els sis sis sis sis s			to all a de alla al		6 8 1	allo allo allo allo a			Scro		==> <u>CSR</u>
000001	R R R R R R R R	*****			******	re lop	οτ υατα	*****		*****	36 36 36 36 36 36 36	*****	* ** ** ** ** ** ** ** **
000001	DSNX@XA		RACE	TOBZ EXT	cerna	ai secu	гіту моа	iuie	– sym	pois			00000000
000002	*	5155	TATE AR	CHLVL=1								eL 3A	00020000
000003	* Cloba	1 CET (Symbole	. 500 49	SET 4	For a d	occripti	00					00030000
000004	* GTODA	I SET .	Symbols	. see .		or a u	escripti	OII					00040000
000000			CRLC	&CLASSNA	MT 8.0	HARODT	&CLASSO	DT &	ERROR	OPT		anac	00050000
000007					T AS	FLICT	AXADI DBC	к, с	LIKIKOIK	OF 1		ausc	00070000
000008	&CL 4550	РТ	SETC	2	1 -		assifica	tion	Mode	ТГ			00080000
000009	*			-	-	(One s	et of cl	asse	s for	FACH	subsvs	`	00090000
000010					2 -	Use Cl	assifica	tion	Mode	1 TT	546595	,	00100000
000011	*					(One s	et of cl	asse	s for	ALLS	ubsvs)		00110000
000012	&CLASSN	мт	SETC	'DSN'	DB2	Subsys	tem Name	(Up	to 4	chars	5		00120000
000013	&CHAROP	Т	SETC	'1'	One	charac	ter suff	ix 0	0-9.	#. @ o	r \$)		00130000
000014	&PCELLC	Ť		50	Prin	nary Ce	11 Count						00140000
000015	&SCELLC	т	SETA	50	Seco	ondáry	Cell Cou	int					00150000
000016	&ERRORO	РТ		'1'	1 -	Defer	to DB2 a	utho	rizat	ion if		@L 3C	00160000
000017						exit a	bends, s	ets -	termi	nating		@09A	00170000
000018						return	code (12	!), o	r set	s an T		@09A	00180000
000019						unexpe	cted ret	urn	code.			@09A	00190000
000020					2 –	Termin	ate DB2	if				@09A	00200000
000021	.*					exit a	bends, s	ets	termi	nating	'	@09A	00210000
000022	- **					return	code(12	!), o	r set	s an		@09A	00220000
000023	. **					unexpe	cted ret	urn	code.			@09A	00230000
000024	*			1000			(00240000
000025	&SERVIC	ELEVEL		PH24314	4	erease	ZAPAR nu	mber	cup	το 7 c	nars)	algc	00259820
000026	W					ints s	ymbol is	for	TBW	use on	ly.		00260000
000027													00265000
000028			EJECI			1				7 1			00270000
000029			E RACI	-/DB2 EXT	cerna	ai Secu	rity Mod	iure	– Pro	rog			00280000

Db2 RACF exit options, cont'ed

• & ERROROPT – error option

- What to do if exit initialization fails, unexpected return codes during authorization checking, or if # abends exceed "AUTH EXIT LIMIT"
- 1 fallback to Db2 native auth
- 2 stop Db2
- & PCELLCT, & SCELLCT work cells

<u>F</u> ile	<u>E</u> dit E <u>c</u>	11t_Se	ettings	<u>M</u> enu	Util	ities	<u>C</u> ompiler	s <u>l</u> est	<u>H</u> e Ip		
VIEW	SSUSE	R1.SC	SNSAMP	(DSNXRX/	4C) -	01.00			Reco	overy p	rocessed
Command	d ===>	e ale ale ale ale al					C D I I	a de alle alle alle alle alle alle alle	Sc	roll ==	==> <u>CSR</u>
	DCNNGNAC	*****	IN N N N N N N	××××××××	*****	* lop	of Data *		**********	*******	*******
000001	DSNX@XAC		RACE	JDB2 EXT	cerna	i secu	rity Modu	ie – sym	1DO I S	a 1 a 4	00000000
000002		51551	ALE AR	CHLVL=1						@L 3A	00020000
000003	* Clobal	CET C	Symbole	. 500 49	CCT f	on a d	occriptio				00030000
000004	* GIUDAI	SET 3	symbols	. See 33		or a u	escriptio				00040000
000000			CRLC	CLASSNI	MT &C	HARODT	&CLASSOR		OPT	anoc	00050000
000007			GBLC		TASC	FLICT		, activition	OF 1	eosc	00070000
000008	&CLASSOPT		SETC	2'	1 -		assificat	ion Mode	л т		00080000
000009	*			-	-	(One s	et of cla	sses for	FACH subs	(VS)	00090000
000010					2 -	Úse Cl	assificat	ion Mode	1 TT		00100000
000011	ste					(One s	et of cla	sses for	ALL subs	/s)	00110000
000012	&CLASSNMT		SETC	'DSN'	DB2	Subsys	tem Name	(Up to 4	chars)		00120000
000013	&CHAROPT		SETC	'1'	One	charac	ter suffi	x (0-9.	#. @ or \$)		00130000
000014	&PCELLCT			50	Prim	ary Ce	11 Count				00140000
000015	&SCELLCT			50	Seco	ndáry	Cell Coun	t			00150000
000016	&ERROROP1			'1'	1 -	Defer 🕆	to DB2 au	thorizat	ion if	@L3C	00160000
000017						exit a	bends, se	ts termi	nating	@09A	00170000
000018						return	code(12)	, or set	s an 🕺	@09A	00180000
000019						unexpe	cted retu	rn code.		@09A	00190000
000020					2 –	Termin	ate DB2 i	f .		@09A	00200000
000021						exit a	pends, se	ts termi	nating	@09A	00210000
000022	- ³⁶					return	code(12)	, or set	s an	@09A	00220000
000023	· **					unexpe	cted retu	rn code.		@09A	00230000
000024	*					-	(2 01 00	00240000
000025	&SERVICEL	EVEL		PH24314	4 R	e lease	APAR num	per (up	to / chars) @LGC	00259820
000026	26					ints s	ymbol is	TOP IBM	use only.		00260000
000027											00265000
000028			EJECI			1	and data and the state	1- D	1		00270000
000029			RACE	/DBZ EXT	cerna	i secu	rity Modu	re – Pro			00280000

Db2 RACF exit modifications?

- Is possible, but we recommend against it
- Use cases:
 - Create new Db2 authorizations tailored to organization
 - Example: R/O access to all tables

<u>F</u> ile	<u>E</u> dit	E <u>d</u> it_Se	ettings	<u>M</u> enu	<u>U</u> tilities	<u>C</u> ompilers	<u>T</u> est	<u>Н</u> е]р		
VIEW Command	SSL d ===>	SER1.SE	DSNSAMP	(DSNXRX	AC) - 01.0	0			Recovery pr Scroll ==	rocessed ==> <u>CSR</u>
*****	******	******	******	*******	erer lop	of Data ***	******	******	*********	*********
000001	DSNX@XA		RACE	/DB2 Ex	ternal Sec	urity Module	– Sym	bols		
000002		SYSS	IAIE AR	CHLVL=1					@L 3A	00020000
000003	*	1								00030000
000004	🚆 Globa	U SEL S	symbols	: See \$	SEI TOP a	description				00040000
000005	*									00050000
000006			GBLC	&CLASSNI	MI , &CHAROP	I, ACLASSOPT,	WERROR	OPT	@09C	00060000
000007			GBLA	&PCELLC	, SCELLCI	&XAPLDBCK				00070000
000008	&CLASSC	I PI	SEIC	2	I - Use C	Tassificatio	n Mode	1 I I		00080000
000009	· 2				Cone	set of class	es tor	- EACH	subsys)	00090000
000010	- 2				2 - Use C	lassificatio	n_Mode	1.tt -		00100000
000011				I DON!	DDD Cube	set of class	es ror	ALL S	ups ys J	00110000
000012	&CLASSN		SEIC	DSN	DBZ SUDSY	stem Name (U	p to 4	"cnars	2 62	00120000
000013	&CHAROP	1	SEIC		One chara		(0-9,	<i>#</i> , œ 0	n 3)	00130000
000014	&PCELLC		SETA	20	Primary C					00140000
000015	&SCELLC		SETA	50.	Secondary	te DB2 auth	andaat	ion if	al 20	00150000
000016	WERKURU	JP I		1	I - Derer	LO DB2 auth	orizat	ion ii		00160000
000017	· 2				exit	abends, sets	cermin	nating	accord accord	00170000
000018	·				recuri		or set	s an	acos A	00180000
000019	- 2				2 Tormi	ected return	code.		accord accord	00190000
000020					2 - Termin	abonds sots	tormi	nating	009A	00200000
000021					rotur	n code(12)	or set	s an	@09A	00220000
000022					upovp	actod roturn	code	s all	anga	00220000
000023	*				unexp	ecceu-recurn	coue.		@U9A	00230000
000024	8.SERVITO	EL EVEL		'DH2/21	I' Roloss	ADAR numbe	n (un	to 7 c	hars) alco	00259820
000025	*			F1124514	This	symbol is fo	r TBM			00260000
000027					11113	Symbol 13 10	T T DIVI	use on	·y·	00265000
000028										00270000
000029		TTTLE	'RACE	/DB2 Ext	ternal Sec	urity Module	- Pro	log'		00280000
000025					cernal see	in rey nodu re				

Relevant Db2 DSNZPARMs

• AUTHEXIT_CHECK

- "DB2" use package owner for autobind, BIND, and REBIND instead of primary auth id
- <u>"PRIMARY"</u> (default)
- AUTHEXIT_CACHEREFRESH
 - "ALL" Db2 refreshes the internal plan and package auth cache, routine auth cache, and DSC when user profile or resource access is changed in RACF
 - Listens to type 62, 71 and 79 ENF signals from RACF
 - Does not support RACFVARS
 - <u>"NONE"</u> (default)
 - Can lead to incorrect access to objects
- AEXITLIM
 - Number of abends before security exit shuts down
 - Default is 10

Big bang or piecemeal?

• Db2 supports RACF and native security concurrently

- Actually, you can't turn off native security ...
- Declined: <u>https://ibm-data-and-ai.ideas.ibm.com/ideas/DB24ZOS-I-443</u>
- If the RACF exit is active, but a class is not active, or the class is active, but the resource is not defined
 - Fallback to Db2 native security
 - Also: auth exit failures
- Allows both big bang and piecemeal conversion



Big bang or piecemeal?

 Example: start with administrative privileges DSNADM and MDSNSM; then move on to object specific classes

• Example

- Piecemeal for lower environments while gaining experience
- Big bang for higher environments to reduce conversion time

Define RACF classes

 Classes predefined in RACF for &CLASSOPT=2 + &CLASSMNT=DSN but need to be activated

Admin	Grouping classes	5	Member classes					
DSNADM	GDSNBP	GDSNSG	MDSNBP	MDSNSG				
	GDSNCL	GDSNSM	MDSNCL	MDSNSM				
	GDSNDB	GDSNSP	MDSNDB	MDSNSP				
	GDSNJR	GDSNSQ	MDSNJR	MDSNSQ				
	GDSNPK	GDSNTB	MDSNPK	MDSNTB				
	GDSNPN	GDSNTS	MDSNPN	MDSNTS				
	GDSNSC	GDSNUF	MDSNSC	MDSNUF				
		GDSNUT		MDSNUT				

DSNR checking not affected by conversion

Defining resources

- Mapping all objects to resources 1:1 will be very inefficient
 - will lead to definition of 100k or even millions of resources
 - Will negatively impact RACF performance
 - SETROPTS ... REFRESH will be too disruptive
 - Will negatively impact managing security
 - Add multiple member profiles to grouping class profile
 - Use generic profiles if all grants map to a single level of access
 - Create RACF groups for multiple users with same access level and permit group instead of users



This Photo by Unknown Author is licensed under CC BY-SA

Back-stop profiles & warning

- <ssid>.** or ** with UACC(NONE)
 - Will prevent Db2 from falling back to Db2 security if a resource is undefined
- You can define profiles with RDEFINE ... WARNING on sandbox
 - This will allow access, but issue ICH4081

Audit considerations



- Define administrative resources in classes DSNADM and MDSNSM with AUDIT(ALL)
- Define other resources with AUDIT(FAILURES)
- Consider audit record volumes if you use AUDIT(ALL) for other objects
 - You can restrict AUDIT(ALL) to resources for I/U/D or DDL activity

Activate and refresh classes

• Activate the class in RACF

• Class must be RACLIST'ed

• Refresh class

Start Db2 with RACF exit

• Stop Db2

- Copy the RACF exit to your SDSNEXIT library
- Restart Db2

Look for IRR9xx on SYSLOG

IRR908I RACF/DB2 EXTERNAL SECURITY MODULE FOR DB2 SUBSYSTEM DSAD HAS A MODULE VERSION OF PH24314 AND A MODULE LENGTH OF 00007EA0. IRR909I RACF/DB2 EXTERNAL SECURITY MODULE FOR DB2 SUBSYSTEM DSAD IS USING OPTIONS: &CLASSOPT=2

> &CLASSNMT=DSN &CHAROPT=1 &ERROROPT=1 &PCELLCT=50 &SCELLCT=50

https://www.ibm.com/docs/en/db2-for-zos/13?topic=module-db2racf-access-control-messages

IRR910I SUBSYST	RACF/DB2 EM DSAD	EXTERNAL	SECURITY	MODULE FC	DR DB2
	INITIATEI	RACLIST	FOR CLAS	SES:	
	MDSNDB	MDSNPK	MDSNPN	MDSNBP	MDSNCL
	MDSNTS	MDSNSG	MDSNTB	MDSNSM	MDSNSC
	MDSNUT	MDSNUF	MDSNSP	MDSNJR	MDSNSQ
	MDSNGV	DSNADM			
IRR911I	RACF/DB2	EXTERNAL	SECURITY	MODULE FC	DR DB2
SUBSYST	EM DSAD				
	SUCCESSFU	JLLY RACL	ISTED CLA	SSES:	
	MDSNDB	MDSNPK	MDSNPN	MDSNBP	MDSNCL
	MDSNTS	MDSNSG	MDSNTB	MDSNSM	MDSNSC
	MDSNUT	MDSNUF	MDSNSP	MDSNJR	MDSNSQ
	MDSNGV	DSNADM			
IRR916I	RACF/DB2	EXTERNAL	SECURITY	MODULE WA	AS ASSEMBLED
WITH AN	HRF7730 (OR LATER N	MACRO LIB	RARY.	
ROLES A	S BACE CRI	TTERTA ARE	C STIPPORT	ED	



Debugging

- Db2 trace IFCID 314 Authorization Exit Parameters
 - -START TRACE(PERF) CLASS(22)
 - If you turn on IFCID 410 a record is only cut for RC 04
 - You get one record per access attempt
- Db2 trace IFCID 140 Audit Auth Failures
 - -START TRACE(AUDIT) CLASS(1)
- RACF SMF80 records
- IBM SAF trace (GTF) or equivalent vendor tooling
- Modify exit

<u>This Photo</u> by Unknown Author is licensed under <u>CC</u> <u>BY-SA</u>

Debugging – IFCID 314 Auth exit parameters

 User SSUSER6 attempt to run SQL: SELECT * FROM NETBANK.GLWDPT

EXIT EXIT	RETURN CODE: REASON CODE:	8 0 This Photo by Unknown
	AUTH ID UNQUALIFIED OBJECT NAM OBJECT OWNER RELATED INFO 1	: SSUSER6 : GLWTDPT : NETBANK : NETBANK NETBANK
SSUSER6 SSUSER6 ADB	TSO IRELATED INFO 2 SSUSER6 BLANK N/P	EXIT PARM
	IADDRESS EXPL : X 7296CAD8 EXIT RETURN CODE: IADDRESS WORK AREA: X 726A38000' EXIT REASON COD IAUTH ID : SSUSER6 UNQUALIFIED OBJECT NAME: GLWTDPT IOBJECT OWNER : NETBANK RELATED INFO 1 : NETBANK IRELATED INFO 2 : NETBANK ILENGTH WORK AREA : 4096	$\{ XAPLV13R1M5 j 8V \\ nSSUSER6 DSAD] = 0 \\ = 0 k = 0 \qquad = 0 \qquad 0 \qquad$
	ACEE UTOKEN : & { PARAMETER LIST : 0000 216A0100 E7C1D7D3 E5F1F3D9 F1D4F540 D 0020 008FB770 E2E2E4E2 C5D9F640 0002C4E2 C 0040 7E96DC92 7E96DD14 00000000 7E96CC20 0	V13R1M503
	0060 0000000 0000000 0000000 0000000 0000000 0000000 0000000 000000000 000000000 0000	00000 00000E5 F1F3D9F1 D4F5F0F3V13R1M503 00000 0000000 0000000 00000000V13R1M503 00004 04040000 04040000 04040000 00000 0000000 0000000 00000000

Debugging – IFCID 140 Audit Auth failures

User SSUSER6 attempt to run SQL: SELECT * FROM NETBANK.GLWDPT

LOCATI GRO MEMB SUBSYST DB2 VERSI PRIMAUTH ORIGAUTH PLANNAME	CON: SSOID DUP: N/A BER: N/A TEM: DSAD CON: V13 CONNECT CORRNAME CORRNAME	INSTANCE CONNTYPE	END_USER RECORD TIME TCB CPU TIME	BM OMEGA RECO WS_NAMI DESTNO	AMON ORD E ACE	FOR TRACI	DB2 PERFORMAN E - SHORT DESCRIPTION	TRANSACT	5R5MO) REQ	UESTED F ACTUAL F PAGE D	PAGE: 1-2 FROM: NOT S TO: NOT S FROM: 05/03 DATE: 05/03	PECIFIED PECIFIED /24 08:49:5 /24	53.18
SSUSER6 SSUSER6 ADB	TSO SSUSER6 'BLANK'	DF0990F37DF9 TS0	SSUSER6 08:50:10.20843146 N/P	TSO 8	2	140	AUDIT AUTH FAILURES	SSUSER6 NETWORKID:	ROCKNET1	LUNAME :	DSADDB2	LUWSEQ:	6
	*** Long AUTH CHE SOURCE SOURCE TARGET C TARGET C *** End	name sectio CKED : SSUS DJECT : GLWT DWNER : NETB DBJECT : 'BLA DWNER : 'BLA of long name	n: ER6 DPT ANK NK' NK' S										
	REASON PRIV CHE OPTIONS AUTH ID	: CKED : SELE : X'04 TYPE : PRIM	0 CT 0000000000000000' IARY OR SECONDARY	AUTH ID		STATI OBJE RID (MNT LENGTH: CT : TA DF ROW : N/	48 BLE OR VIEW P	RETCOD SECLAB	EL ROW	: : N/P	8	
	SQL STAT	TEMENT : ◎ FROM "NETBA	NK"."GLWTDPT" FOR	FETCH (ONLY								
	ACEE UTO	OKEN (STRING)	: & {					S01TCP42	2 SS	USER6 PC	DUSER		
	ACEE UTC 50012006 00000000	0KEN (IN HEX) 00001C0000000 0E2E2E4E2C5D9	: 000000000000000000000000000000000000	00000000 040	0000	00000	00000000000000	000000000000000000000000000000000000000	00000000000	000000E	2F0F1E3C3D	7F4F2000000	000

Debugging – ICH408I message

 User SSUSER6 attempt to run SQL: SELECT * FROM NETBANK.GLWDPT

ICH408I USER(SSUSER6) GROUP(PDUSER) NAME(SELF SERVICE USER 6)
DSAD.NETBANK.GLWTDPT.SELECT CL(MDSNTB)
INSUFFICIENT ACCESS AUTHORITY
FROM DSAD.** (G)
ACCESS INTENT(READ) ACCESS ALLOWED(NONE)

Debugging – SMF 80

 User SSUSER6 attempt to run SQL: SELECT * FROM NETBANK.GLWDPT

SMF record RACF processing and audit records

-

Description SSUSER6 RACF ACCESS violation: (READ, NONE) on MDSNTB DSAD.NETBANK.GLWTEMP.SELECT

80

Record identification Jobname + id: SSUSER6 SMF date/time: Fri 3 May 2024 12:18:28.28 SMF system: SS01 record type:

Event identification RACF event description RACF event qualifier RACF descriptor for event RACF reason for logging SAF authority used Access intent Access allowed Unix Audit Function Code Unix Access Intent Unix Access Allowed Unix Access Used RACF command Audit/message logstring Audit/message logstring

Command ===>

Resource access (Failure:Insufficient authority) Violation Resource Normal READ NONE

record no: CKR4SM01 698

A.50.GCV SSUSER6 DSAD T Y Y N Y N N GLWTEMP 050 MDSNTB DSAD.NETBANK.GLWTEMP.SELECT

Object identification SAF resource class SAF profile key SAF resource name Volume serial Resource token Pathname Failing job name

Object ownership Profile owner id

Installation data

MDSNTB DSAD.** DSAD.NETBANK.GLWTEMP.SELECT

SSUSER1 SELF SERVICE USER 1

Subject identification User: SSUSER6 Group: PDUSER Name: SELF SERVICE USER 6 SERVAUTH POE:

Terminal: S01TCP47 Appl: Security label:

Token: User:SSUSER6; Group:PDUSER; Flags:(Pre 1.9); Session:TSO; Port:TERMINAL(S01TCP47)

Cleanup grants – backup first

- Make a backup copy of grants
- Options:
 - 1. Db2 UNLOAD of relevant SYSIBM.SYSxxxAUTH tables
 - Difficult to query
 - 2. Copy all SYSIBM.SYSxxxAUTH tables to new schema
 - Vendor tooling that allow "catalog copy"
 - 3. Db2 V13 FL505: enable temporal history on SYSIBM.SYSxxxAUTH
 - Vendor tooling that exploit FL505: "show authorizations as of June 1, 2024"
- NEW

4. Vendor tooling that can generate GRANTs from catalog

Cleanup grants - revoke

• Revoke the authorizations that are no longer used

- Strongly recommended for security reasons
- Db2 can fallback
 - All classes not implemented
 - No backstop profiles
 - Db2 auth exit failures
 - Processing GRANTs

• Vendor tooling typically support mass revokes

- You cannot revoke implicit privileges
 - Ownership
 - Package



Conversion tools & support



• RACFDB2

2002 edition is still available:

https://public.dhe.ibm.com/eserver/zseries/zos/racf/racfdb2/

- No compression of profiles
- Updates/improvements discussed on IDUG-L in 2020: <u>https://community.idug.org/discussion/6581994178556524276/migrating-from-db2-internal-security-to-db2-external-security-racf</u>
- Build your own tools
- Consultants
 - E.g., Rocket Software 😳

Helpful tools for DBAs when using RACF security

- Before: the security admin had to learn a new tool to manage Db2 native security
- Now: the DBA must learn a new tool to answer questions like:
 - Why do I get a sqlcode -551?
 - What profile provides UPDATE access to this object?
 - What access does this user have?
- Options:
 - 1. RACF commands (see appendix for samples)
 - 2. Vendor tools for RACF administration
 - 3. Db2 vendor tools with RACF support



Helpful tools for DBAs when using RACF security

- Vendor tooling generic RACF administration tools
 - Example: IBM zSecure Administration

Command ===>	General resource overview	
Class MDSNTB Class Profile key MDSNTB DSAD.SYSIBM.*.SELE MDSNTB DSAD.**	CT G NONE G NONE CT G NONE CT G NONE CT CT C	Owner S/F W SgF ID(*) Complex <u>SSUSER1</u> <u>R</u>
zSecure Suite G Command ===> Class MDSNTB	eneral resource overview	
Identification Class Profile name Type Volume serial list	MDSNTB DSAD.SYSIBM.*.SELECT GENERIC	RSPLEXRS
Owner Installation data Application data	<u>SSUSER1</u> SELF SERVICE USER 1	
User Access ACL id When SSUSER6 READSSUSER6	RI Name SELF SERVICE	DfltGrp RvC InstData USER 6 PDUSER
Safeguards User to notify of violation Audit access success/failures Global audit success/failures Mandatory Access Control Security label Security level Categories list	Other permissions Allow all accesses WARNING Universal access authority Resource level Statistics Creation date	No NONE O 15Jan24

Helpful tools for DBAs when using RACF security

• Vendor tooling – Db2 specific





IDUG

2024 NA Db2 Tech Conference



Ray Overby

roverby@rocketsoftware.com

Jørn Thyssen jthyssen@rocketsoftware.com

Session Code SEC2



Please fill out your session evaluation!



Appendix: helpful RACF commands

- Activate & raclist class
 - SETROPTS CLASSACT(MDSNTB) RACLIST(MDSNTB)
- Refresh class after changes
 - SETROPTS RACLIST(MDSNTB) REFRESH
- Define profile
 - RDEFINE MDSNTB DSAD.SYSIBM.*.SELECT UACC(NONE) OWNER(<owner>) AUDIT(FAILURES(READ))
 - Requires refresh to take effect
- Delete profile
 - RDELETE MDSNTB DSAD.SYSIBM.*.SELECT
 - Requires refresh to take effect

Appendix: helpful RACF commands, cont'ed

• Search

- Search for all profiles:
 - SEARCH ALL CLASS(MDSNTB)
- Search for all profiles for subsystem DSAD
 - SEARCH ALL CLASS(MDSNTB) MASK(DSAD)
 - SEARCH ALL CLASS(MDSNTB) FILTER(DSAD.**)
- Search for all profiles for tables in schema SYSIBM for any subsystem
 - SEARCH ALL CLASS(MDSNTB) FILTER(*.SYSIBM.**)

Appendix: helpful RACF commands, cont'ed

• List profile

- List all information about profile
 - RLIST MDSNTB DSAD.** ALL
- List user
 - LU <userid>
- List group
 - LG <group>

Appendix: helpful RACF commands, cont'ed

• Permit access

- PERMIT AC(READ) CL(MDSNTB) DSAD.SYSIBM.*.SELECT ID(JORN)
- Requires refresh to take effect
- Revoke access
 - PERMIT CL(MDSNTB) DSAD.SYSIBM.*.SELECT ID(JORN) DELETE
 - Requires refresh to take effect