

THINGS I CAN DO UP TO 7.5,
CAN'T FROM 7.6

THINGS I CAN'T DO UP TO 7.5,
CAN FROM 7.6



DISCLAIMER: The content of this presentation is intended to provide ideas for developing your own strategy. It focuses deliberately on security-related topics.



Guy Marmorat
gmarmorat@resiliane.com



Steve Bradshaw
steve.bradshaw@rowtonit.com



How to discover what was
added / changed / removed
by Version 7.6?

How to discover what was added/changed/removed by version 7.6?

- Every version has its own MTU guide (Memo To Users)
- Detailed description of all the changes compared to the previous version (68 pages at 2026-07)

Who should read this memorandum

The IBM i 7.6 Memo to Users contains information that is **critical** for several audiences.

This memorandum has four sections:

- **Read this first** provides information to be considered before you install IBM i 7.6. This section is intended for system and application programmers and for the person responsible for system management.
- **IBM i Operating system** contains new release changes to basic operating system functions. This section includes changes to systems management functions, such as configuration and tailoring the system, and changes **that could affect the way things operate or appear in the new release**. This section is intended for all users of the IBM i.
- **Options** provides information about new release changes that affect specific program options of the operating system. This section is intended for all users of the IBM i.
- **Licensed programs** contains new release changes that might affect existing applications. These changes might also affect applications that are saved on an IBM i 7.6 system to be restored on a previous release server. This section is intended for application programmers and system programmers who use the IBM i and its licensed programs, as well as for businesses with complex networks or application development businesses that have systems at different releases.



How to discover what was added/changed/removed by version 7.6?

Luckily 7.6 has also its Redbook (234 pages)

www.redbooks.ibm.com/abstracts/sg248588.html

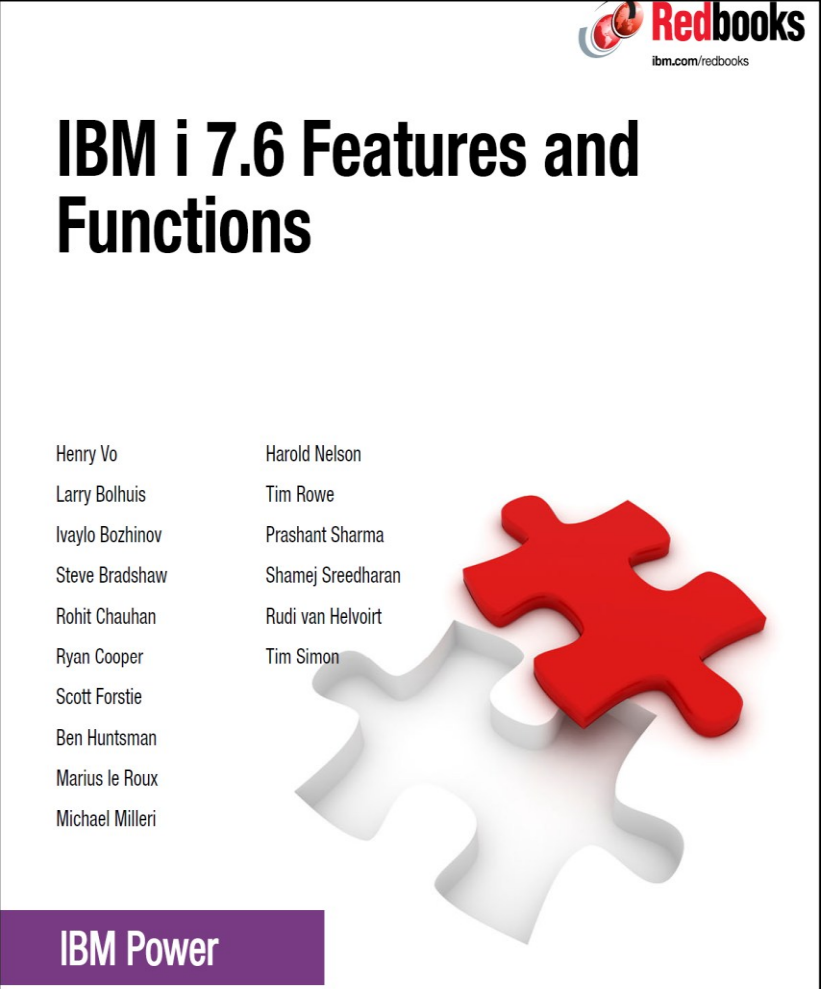
Webpage for new features

www.ibm.com/docs/en/i/7.6.0?topic=documentation-overview-whats-new

Security Reference Guide updated (“What’s new” section + special marks)

www.ibm.com/docs/en/i/7.6.0?topic=reference-pdf-file-security

Command	Referenced object	Authority needed	
		For object	For library
ENDLINRCY	Line description	*OBJOPR	*EXECUTE
PRTCMNSEC ^{2, 3}			
RSMLINRCY	Line description	*OBJOPR	*EXECUTE
WRKLIND ^{1, 4}	Line description	*OBJOPR	*EXECUTE
¹ To use individual operations, you must have the authority required by the individual operation.			
² To use this command, you must have *IOSYSCFG special authority.			
³ To use this command, you must have *ALLOBJ special authority.			
⁴ To use this command, you must have *IOSYSCFG special authority or be authorized to the QIBM_IOSYSCFG_VIEW function ID.			



How to discover what was added/changed/removed by version 7.6 TR2?

MTU is updated
(“What’s new” Section)

Webpage IBM i 7.6 - TR2 Enhancements

7.6	2025-04-18	7.2 months
7.6 TR1	2025-11-21	7.8 months
7.6 TR2	2025-07-14	

www.ibm.com/support/pages/ibm-i-76-tr2-enhancements

IBM

Support Downloads Documentation Forums Cases Monitoring Manage support account

IBM Support

Search support or find a product

IBM i 7.6 - TR2 Enhancements

News

Abstract

IBM i 7.6 - TR2 Software Enhancements

Content

You are in: IBM i Technology Updates > IBM i 7.6 - TR2 Enhancements

www.ibm.com/docs/en/ssw_ibm_i_76/pdf/rzaq9.pdf

What's new

The following revisions or additions have been made to the Memorandum to Users documentation since the first IBM i 7.6 publication. These entries will be found only in the English version of the memo to users.

What's new

The updates for each Memo to Users entry were made at the specified time frame for the section. The actual release date of some changes documented may not be until the next Technical Refresh (TR) date. Check dates on the PTF specified for each entry to verify release dates.

July 2026

New entries added:

"Managing master keys" on page 39

"QIBM_QUERY_CONVERT_BLANK_TO_0 environment variable" on page 25

"Column cannot be defined as NOT NULL DEFAULT NULL" on page 25

"SQL INTERPRET function error enforcement" on page 25

"SQL syntax error enforcement: common table expression with VALUES INTO statement" on page 25

"Automated removal of historical data from /QIBM/UserData/OS400/SQE directory" on page 26

"Changes to authority required for QSYS2.CHANGE_MIGRATION_MANAGER procedure" on page 34

"NVMe Locking Policy - password length minimum change" on page 39

"Enhanced cluster security" on page 38

"Reduced Processor on Demand Data in MATMATR (FW1120+)" on page 40

"Resource Group ID Support in MI Instructions" on page 40

Updated entries:

"Usage of Cluster functionality with Multi-Factor Authentication (MFA) Enabled Users" on page 38

November 2025

New entries added:

"Change to Database file delete processing" on page 25

How to discover what was removed by version 7.6?

Removed in 7.5

- User profiles « Content Manager OnDemand »: QRDARSADM, QRDARS400n
- Service Tools User IDs : 22222222, 11111111

Removed in 7.6

- System user profiles : QMGTC, QIBMHELP, QPM400
- Library QGDDM
- Objects related to OptiConnect
- Objects and Services related to PPP and some TCP servers
- Functions IDs

Server	EXIST_V7R5	EXIST_V7R6	Reserved
*BOOTP ...	1	0	Bootstrap Protocol
*CIMOM ...	1	0	CIM OBJECT MANAGER
*DHCP ...	1	0	Dynamic Host Configuration Protocol
*DNS ...	1	0	Domain Name System
*MGTC ...	1	0	Management Central
*QOS ...	1	0	Quality of Service
*ROUTED ...	1	0	Router Daemon

Function Product ID	EXIST_V7R5	EXIST_V7R6	COUNT
QIBM_QYCM_CIMOM	1	0	11
QIBM_QYPS_MGTCTRL	1	0	1
QIBM_XD1_OPNAV	1	0	75

Decision for an upgrade to 7.6

- Evaluate the benefits
- Read the new features
- Evaluate the effort
- Read the changes (MTU)
- Evaluate the risk
- Read the changes (MTU)
- Run « Pre-Upgrade Verification Tool for IBM i »

NEW_WITH_NO_IMPACT	Net new feature that requires a specific setting to be triggered			
REMOVAL	Objects and ressources that are not used anymore by IBM			
CHANGE	Change in a setting that may impact your existing applications			
RESTRICTION	Restrictions that may impact your existing applications			
		public authority reduced		
		new authority required		
		new special authority required		
		new function usage resgistration required		
		...		

RISK	COUNT	CONTRIBUTION	COUNT
high	1	huge	2
medium	25	high	9
low	11	medium	25
N/A	24	low	25

CATEGORY	SUB_CATEGORY	COUNT
CHANGE		9
NEW_WITH_NO_IMPACT		22
REMOVAL		3
RESTRICTION	*OBJMGT required	1
RESTRICTION	*OBJOPR required	1
RESTRICTION	*READ required	1
RESTRICTION	*SAVSYS removed from QPGMR	1
RESTRICTION	*USE required	1
RESTRICTION	system file no longer updateable	1
RESTRICTION	FCNUSG	2
RESTRICTION	PUBAUT	1
RESTRICTION	PUBAUT & OWNERSHIP	1
RESTRICTION	SPCAUT	5
RESTRICTION	SPCAUT or FCNUSG	12

27

Planning for an upgrade to 7.6

Tasks

- Copy production Lpar to test Lpar; upgrade to 7.6; simulate normal activities; **monitor the failures**
- Try to **predict what could break in 7.6 using auditing features**

NEW_WITH_NO_IMPACT	Net new feature that requires a specific setting to be triggered		
REMOVAL	Objects and ressources that are not used anymore by IBM		
CHANGE	Change in a setting that may impact your existing applications		
RESTRICTION	Restrictions that may impact your existing applications		
		public authority reduced	
		new authority required	
		new special authority required	
		new function usage resgistration required	
		...	

CATEGORY	SUB_CATEGORY	COUNT
CHANGE		9
NEW_WITH_NO_IMPACT		22
REMOVAL		3
RESTRICTION	*OBJMGT required	1
RESTRICTION	*OBJOPR required	1
RESTRICTION	*READ required	1
RESTRICTION	*SAVSYS removed from QPGMR	1
RESTRICTION	*USE required	1
RESTRICTION	system file no longer updateable	1
RESTRICTION	FCNUSG	2
RESTRICTION	PUBAUT	1
RESTRICTION	PUBAUT & OWNERSHIP	1
RESTRICTION	SPCAUT	5
RESTRICTION	SPCAUT or FCNUSG	12

Planning for an upgrade to 7.6 – Why these restrictions?

Critical phase of an attack/malicious act =



Is it ok that a user with no authority can:

- List all the shares
- Display all RDB entries
- Check the DDM attributes
- Check the TELNET, FTP attributes
- Check the TCP, Domain, Hosts, routes
- Display the activity on ports/IPs
- Display RCAC rules
- Display system values
- And more....

NEW_WITH_NO_IMPACT	Net new feature that requires a specific setting to be triggered
REMOVAL	Objects and ressources that are not used anymore by IBM
CHANGE	Change in a setting that may impact your existing applications
RESTRICTION	Restrictions that may impact your existing applications
	public authority reduced
	new authority required
	new special authority required
	new function usage resgistration required
	...

CATEGORY	SUB_CATEGORY	COUNT
CHANGE		9
NEW_WITH_NO_IMPACT		22
REMOVAL		3
RESTRICTION	*OBJMGT required	1
RESTRICTION	*OBJOPR required	1
RESTRICTION	*READ required	1
RESTRICTION	*SAVSYS removed from QPGMR	1
RESTRICTION	*USE required	1
RESTRICTION	system file no longer updateable	1
RESTRICTION	FCNUSG	2
RESTRICTION	PUBAUT	1
RESTRICTION	PUBAUT & OWNERSHIP	1
RESTRICTION	SPCAUT	5
RESTRICTION	SPCAUT or FCNUSG	12

Typical actions to perform in pre-upgrade steps (not exhaustive)

Identify all customized system objects

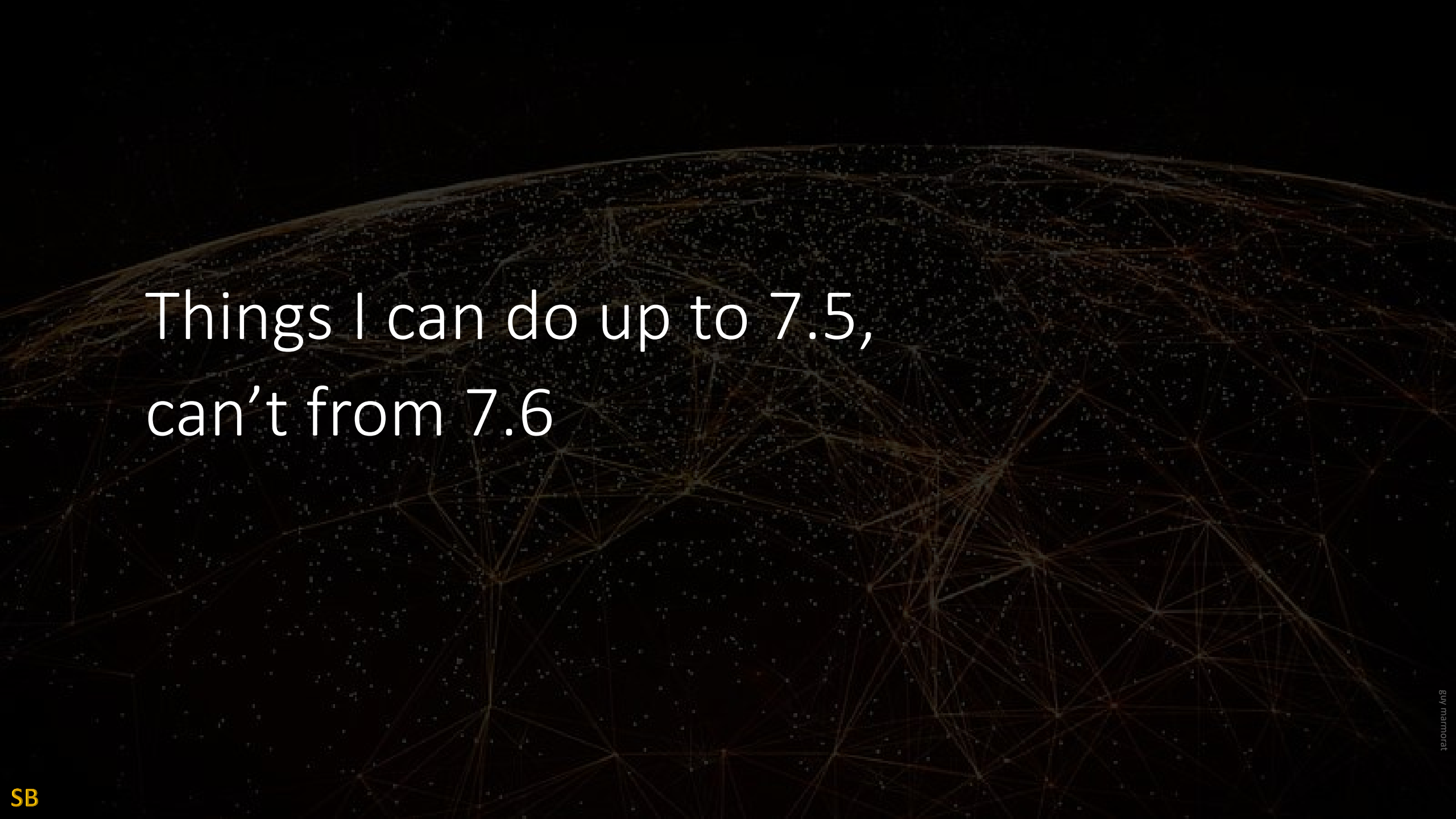
- Commands
- Authorities on system objects
- User objects in QSYS
- Messages
-

```
764 -- default values have been changed
765 SELECT OBJLIB, OBJNAME, OBJTEXT, APAR_ID, USER_CHANGED, CHANGE_TIMESTAMP, objdefiner, objowner
766 FROM TABLE(QSYS2.OBJECT_STATISTICS('*ALL', '*CMD')) os
767 WHERE APAR ID = 'CHGDFT' and (objdefiner in ('*IBM', 'QLPINSTALL', 'QSYS') or objowner in ('QSYS'));
```

OBJLIB	OBJNAME	OBJTEXT	APAR_ID	USER_CHANGED	CHANGE_TIMESTAMP	OBJDEFINER	OBJOWNER
QMGTOOLS	CMPPTF	-	CHGDFT	YES	2026-07-31 12:05:26.000000	QSYS	QSYS
QMGTOOLS	CMPVER	Compare version CMD	CHGDFT	YES	2026-07-31 12:05:26.000000	QSYS	QSYS
QMGTOOLS	FTPMSD	FTP MSD command	CHGDFT	YES	2026-07-31 12:05:26.000000	QSYS	QSYS
QSYS	SAVOBJ	Save Object	CHGDFT	YES	2026-08-21 16:47:43.000000	*IBM	QSYS

```
769 -- allow limited cap. have been changed
770 select command_library, command_name, text_description, allow_limited_user, USER_CHANGED, CHANGE_TIMESTAMP, objdefiner, objowner
771 from qsys2.command_info
772 join TABLE(QSYS2.OBJECT_STATISTICS('*ALL', '*CMD')) os on objname = command_name and objlib = command_library
773 where allow_limited_user <> 'NO' and command_name not in ('STRPCO', 'DSPJOB', 'DSPJOBLOG', 'DSPMSG', 'SIGNOFF', 'SNDMSG', 'WRKMSG') and
774 (objdefiner in ('*IBM', 'QLPINSTALL', 'QSYS') or objowner in ('QSYS')) ;
```

COMMAND_LIBRARY	COMMAND_NAME	TEXT_DESCRIPTION	ALLOW_LIMITED_USER				
Command Library	Command Name	Text Description	Allow Limited User				
				USER_CHANGED	CHANGE_TIMESTAMP	OBJDEFINER	OBJOWNER
QSQL	STRSQL	Start SQL Interactive Session	YES	NO	2026-08-21 16:59:18.000000	*IBM	QSYS
QSYS	UPDDTA	Update Data with Temp Program	YES	NO	2026-08-21 16:59:24.000000	*IBM	QSYS



Things I can do up to 7.5,
can't from 7.6

Predicting failures in 7.5: Example

QSYS2.SECURITY_INFO view

From the
MTU

The caller of the QSYS2.SECURITY_INFO view must have `*SECADM` or `*AUDIT` special authority. An SQL error SQLCODE -443, SQLSTATE '42502' will be returned if the user has insufficient authority. In prior releases, no authority was required to query the view.

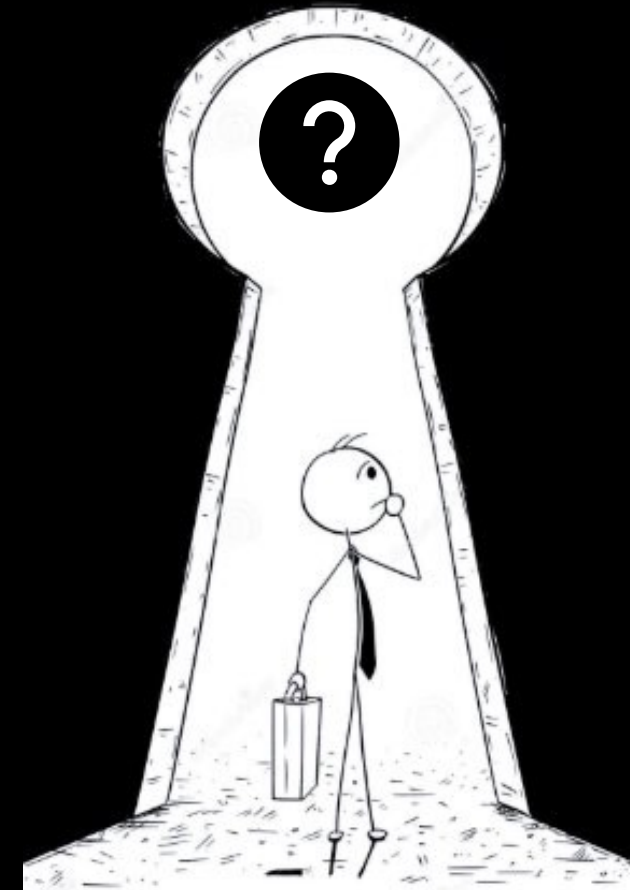
QUICK FIRE QUESTION 1mn:

➤ How will you predict this failure?



Options:

- QAUDJRN-ZR entries
- Authority Collection
- Database Monitor
- Plan cache
- SQL exit points
- Others?



Predicting failures in 7.5: example

```
47 -- check the journal entries with a failure prediction on 7.6
48 select jrn.SYSTEM_NAME, jrn.ENTRY_TIMESTAMP, entry_type_detail, job_name, job_number, program_library, program_name,
49 remote_address, jrn.user_name, jrn.library_name, system_object_name, jrn.object_type
50 from table(SYSTOOLS.AUDIT_JOURNAL_ZR (STARTING_RECEIVER_NAME => '*CURCHAIN', STARTING_TIMESTAMP => current date - 1 days)) jrn
51 join rslaud.audit_sql_service_for_v7r6 aud on jrn.library_name = aud.service_schema_name and jrn.object_name = aud.system_object_name and jrn.object_type = aud.object_type
52 where not exists (select 1 from systools.special_authority_data_mart spa where spa.authorization_name = jrn.user_name and special_authority not in ('*SECADM', '*AUDIT')) ;
53
```

SYSTEM_NAME	ENTRY_TIMESTAMP	ENTRY_TYPE_DETAIL	JOB_NAME	JOB_NUMBER	PROGRAM_LIBRARY	PROGRAM_NAME	REMOTE_ADDRESS	USER_NAME	LIBRARY_NAME	SYSTEM_OBJECT_NAME	OBJECT_TYPE
IUG6	2026-08-06 14:2...	Read of a...	QZDASOINIT	023377	QSYS	QZDASOINIT	10.24...	GM_BASIC	QSYS2	SEC_INFO	*FILE

Object Auditing

```
88 -- check the autcol entries with a failure prediction on 7.6
89 select distinct cast(check_timestamp as timestamp(0)) as check_timestamp, aut.authorization_name, job_name, job_number, object_schema, object_name, system_object_type
90 from qsys2.authority_collection_object aut
91 join rslaud.audit_sql_service_for_v7r6 aud on aut.system_object_schema = aud.service_schema_name and aut.system_object_name = aud.system_object_name and aut.system_object_type = aud.object_type
92 where check_any_authority = 0 and cached_authority = 0
93 and not exists (select 1 from systools.special_authority_data_mart spa where spa.authorization_name = aut.user_name and special_authority not in ('*SECADM', '*AUDIT'))
94 order by authorization_name ;
```

CHECK_TIMESTAMP	AUTHORIZATION_NAME	JOB_NAME	JOB_NUMBER	OBJECT_SCHEMA	OBJECT_NAME	SYSTEM_OBJECT_TYPE
2026-08-06 14:36:17	GM_BASIC	QZDASOINIT	023377	QSYS2	SECURITY_INFO	*FILE

Authority Collection

+
Adopted
Authority

```
128 -- check the dxmon entries with a failure prediction on 7.6
129 select distinct qctime, qsys, qqjob, qqcl03 client_ip, qvc102 current_user, qvc3001 SQL_app, qq1000 SQL_string from RSLAUD.DEM_SQLSRV dbm
130 join rslaud.audit_sql_service_for_v7r6 aud on upper(qq1000) like '%' concat aud.service_schema_name concat '%' concat aud.service_name
131 where not exists (select 1 from systools.special_authority_data_mart spa where spa.authorization_name = qvc102 and special_authority not in ('*SECADM', '*AUDIT'))
132 order by qvc102 ;
```

QQTIME	QSYS	QQJOB	CLIENT_IP	CURRENT_USER	SQL_APP	SQL_STRING
Created Time	System Name	Job Name				
2026-08-06 14:5...	IUG6	QZDASOINIT	10.242.2.131	GM_BASIC	IBM i Access Client Solutions - Run SQL Scripts	select * from QSYS2.SECURITY_INFO

Database Monitor

Monitoring real failures in 7.6: example

QSYS2.SECURITY_INFO view

From the
MTU

The caller of the QSYS2.SECURITY_INFO view must have `*SECADM` or `*AUDIT` special authority. An SQL error SQLCODE -443, SQLSTATE '42502' will be returned if the user has insufficient authority. In prior releases, no authority was required to query the view.

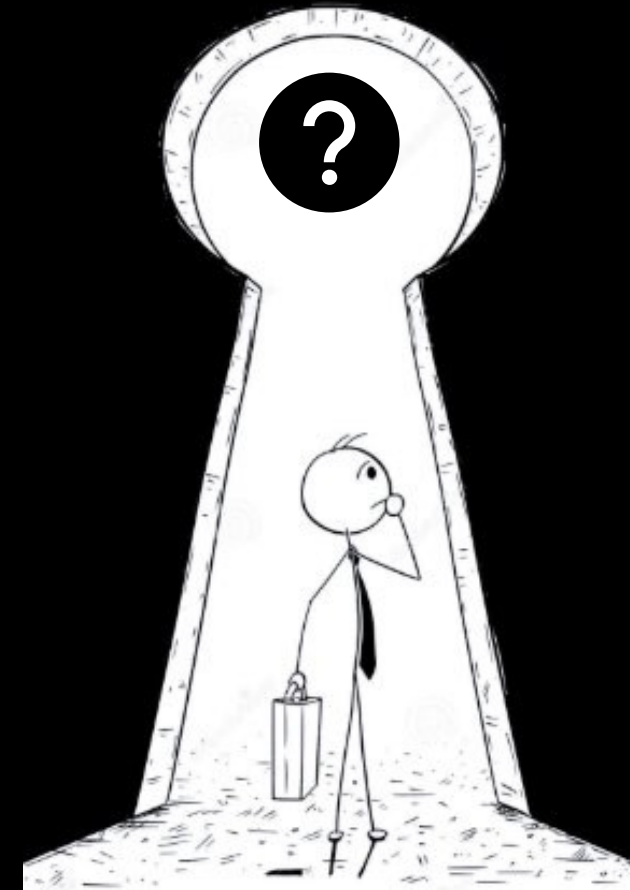
QUICK FIRE QUESTION 1mn:

➤ How will you monitor this failure?



Options:

- QAUDJRN-AF entries - violation_type = 'K'
- QAUDJRN-GR entries – entry_type = 'F' and function_registration_operation = 'USAGE FAILURE'
- Message Watcher
- QSYS2.SQL_ERROR_LOG
- Others?



Monitoring real failures in 7.6: example

No information about which special authority is missing. Clean the false positive and/or add more criteria

```
150 -- check the journal entries with a real failure on 7.6
151 select jrn.SYSTEM_NAME, jrn.ENTRY_TIMESTAMP, job_name, job_number, program_library, program_name,
152 remote_address, jrn.user_name, object_library, object_name, jrn.object_type, violation_type_detail
153 from table(SYSTOOLS.AUDIT JOURNAL_AF (STARTING_RECEIVER_NAME => '*CURCHAIN', STARTING_TIMESTAMP => current date - 1 days)) jrn
154 where violation_type = 'K'
```

AF journal entries

SYSTEM_NAME	ENTRY_TIMESTAMP	JOB_NAME	JOB_NUMBER	PROGRAM_LIBRARY	PROGRAM_NAME	REMOTE_ADDRESS	USER_NAME	OBJECT_LIBRARY	OBJECT_NAME	OBJECT_TYPE	VIOLATION_TYPE_DETAIL
IUG6	2026-08-06 15:0...	QPADEV0007	023412	QSYS	QCMD	10.24...	GM_BASIC	QSYS	QSYRTVSA	*PGM	Special authority violation

```
188 -- start watch process focusing on message CPF503E with proper filters
189 cl: STRWCH SSNID(SPCAUT_1)
190     WCHPGM(RSLAUD/SPCAUT_AF)
191     WCHMSG((CPF503E SECURITY_INFO *MSGDTA *ALL))
192     WCHMSGQ((*JOBLOG))
193     WCHJOB((*ALL/*ALL/*ALL))
194     RUNPTY(20) ;
195
196 -- check the resulting table
197 select distinct cast(log_timestamp as timestamp(0)) as log_timestamp, session_id, job_name, job_user, job_number, message_id, message_queue
198 from rslaud.spcaut_failures ;
```

Message Watcher

LOG_TIMESTAMP	SESSION_ID	JOB_NAME	JOB_USER	JOB_NUMBER	MESSAGE_ID	MESSAGE_QUEUE
2026-08-06 15:13:33	SPCAUT_1	QPADEV0007	GM_BASIC	023412	CPF503E	*JOBLOG

SQLCODE	SQLSTATE	SQL	LIBRARY	PROGRAM	MOST	MOST	CURRENT	CURRENT	CURRENT
BEING	CORRESPONDING	STATEMENT	CONTAINING	ENCOUNTERING	RECENT	RECENT	USER	CLIENT_APPLNAME	CLIENT_PROGRAMID
LOGGED	TO	TEXT	NAME	SQLCODE	OCCURRENCE	JOB	SPECIAL REGISTER		
-443 42502		CREATE OR REPLACE TABLE QTEMP . SEC_INFO AS (SELECT * FROM QSYS2 . SECU...	QGPL	RUN_SECINF	2026-08-11...	023655/GM_BASIC/QPADEV...	GM_BASIC		
-443 42502		CREATE OR REPLACE TABLE QTEMP . SEC_INFO AS (SELECT * FROM QSYS2 . SECU...	QGPL	RUN_SECINF	2026-08-11...	023655/GM_BASIC/QPADEV...	GM_BASIC		
-443 42502		create or replace table qtemp/sec_info as	(sele... QSQL	QSQIMAIN	2026-08-11...	023655/GM_BASIC/QPADEV...	GM_BASIC	-	STRSQL
-443 42502		create or replace table qtemp/sec_info as	(sele... QSQL	QSQIMAIN	2026-08-11...	023655/GM_BASIC/QPADEV...	GM_BASIC	-	STRSQL
-443 42502		create or replace table qtemp.sec_info as (select * from qsys2.security_i...	QSYS	QSQSCHM	2026-08-11...	023647/QUSER_NC/QZDASO...	GM_BASIC	-	RUNSQL
-443 42502		create or replace table qtemp.sec_info as (select * from qsys2.security_i...	QSYS	QSQSCHM	2026-08-11...	023647/QUSER_NC/QZDASO...	GM_BASIC	-	RUNSQL
-443 42502		select * from qsys2.security info	QSYS	QZDASRV	2026-08-11...	023647/QUSER_NC/QZDASO...	GM_BASIC	IBM i Access C...	file:/C:/Users/P

SQL_ERROR_LOG

Non-changeable system user profiles

PREVIOUS_SYSTEM_USRPRF	NEW_SYSTEM_USRPRF
QPGMR	QPGMR_NC
QSECOFR	QSECOFR_NC
QSYSOPR	QSYSOPR_NC
QUSER	QUSER_NC

- They run system processes (Job_user)
- They can't be changed
- They can't have a password, neither a TOTP code
- They can't be added with "denied" to QIBM_RUN_UNDER_USER_NO_AUTH.

JOB_NAME_SHORT	JOB_USER_V7R5	JOB_USER_V7R6
QMRDBJNFY	QUSER	QUSER_NC
QNPFSERVD	QUSER	QUSER_NC
QNPFSERVS	QUSER	QUSER_NC
QPWFSERV	QUSER	QUSER_NC
QPWFSERVSD	QUSER	QUSER_NC
QPWFSERVSO	QUSER	QUSER_NC
QPWFSERVSS	QUSER	QUSER_NC
QPWFSERVS2	QUSER	QUSER_NC
QFWTLSTN	QUSER	QUSER_NC
QSCCLICEV	QUSER	QUSER_NC
QSCWCHMS	QUSER	QUSER_NC
QSERVER	QPGMR	QPGMR_NC
QTFPJTCP	QUSER	QUSER_NC
QZDAINIT	QUSER	QUSER_NC
QZDASOINIT	QUSER	QUSER_NC
QZDASRVSD	QUSER	QUSER_NC
QZDASSINIT	QUSER	QUSER_NC
QZHQSRVD	QUSER	QUSER_NC
QZHQSSRV	QUSER	QUSER_NC
QZLSFILE	QUSER	QUSER_NC
QZLSFILET	QUSER	QUSER_NC
QZLSSERVER	QPGMR	QUSER_NC
QZRCRSVS	QUSER	QUSER_NC
QZRCRSVSD	QUSER	QUSER_NC
QZSCRSVS	QUSER	QUSER_NC
QZSCRSVSD	QUSER	QUSER_NC
QZSOSGND	QUSER	QUSER_NC
QZSOSIGN	QUSER	QUSER_NC
QZSOSMAPD	QUSER	QUSER_NC

JOB_NAME_SHORT	JOB_USER_V7R5	JOB_USER_V7R6
QACSOTP	QUSER	QUSER
QDBMSRVR	QUSER	QUSER
QIWVPPJT	QUSER	QUSER
QLZPSERV	QUSER	QUSER
QNMAPPINGD	QUSER	QUSER
QNMAREXECD	QUSER	QUSER
QNPSEVR	QUSER	QUSER
QRWTSRVR	QUSER	QUSER
QSCWCHPS	QUSER	QUSER
QSQRVR	QUSER	QUSER
QSYSSCD	QPGMR	QPGMR
QZBSEVTM	QUSER	QUSER
QZRCRSVR	QUSER	QUSER
QZSCRSVR	QUSER	QUSER

www.ibm.com/docs/en/ssw_ibm_i_76/pdf/rzaq9.pdf

QPGMR	Programmer profile	– USRCLS: *PGMR – SPCAUT: *ALLOBJ ¹, *SAVSYS, *JOBCTL – PTYLMT: 3 – ACGCDE: *BLANK
QPGMR_NC	Programmer profile that can't be changed	– USRCLS: *PGMR – SPCAUT: *ALLOBJ ¹, *SAVSYS, *JOBCTL – PTYLMT: 3 – ACGCDE: *BLANK

QSECOFR	Security officer profile	– PWDEXP: *YES – USRCLS: *SECOFR – SPCAUT: *ALLOBJ, *SAVSYS, *JOBCTL, *SECADM, *SPLCTL, *SERVICE, *AUDIT, *IOSYSCFG – UID: 0 – PASSWORD: QSECOFR
QSECOFR_NC	Security officer profile that can't be changed	– USRCLS: *SECOFR – SPCAUT: *ALLOBJ, *SAVSYS, *JOBCTL, *SECADM, *SPLCTL, *SERVICE, *AUDIT, *IOSYSCFG

Non-changeable system user profiles

Check existing authorities from the changeable user profiles on objects

Check existing authorities on the changeable user profiles

```
312 -- collect authorizations that the previous user profile has, but not the new one (on other objects)
313 SELECT previous_system_usrprf, a.object_schema, a.object_name, a.object_type, a.object_authority, a.owner, a.object_owner,
314 a.object_operational, a.object_management, a.object_existence, a.object_alter,
315 a.object_reference, a.data_read, a.data_add, a.data_update, a.data_delete, a.data_execute,
316 a.authorization_list, a.primary_group, a.authorization_list_management, os.objdefiner
317 from rslaud.old_new_system_usrprf
318 join qsys2.object_privileges a on previous_system_usrprf = a.authorization_name
319 join TABLE(qsys2.object_statistics('*ALLUSR', '*ALL')) os on a.object_schema = os.objlib and a.object_name = os.objname and a.object_type = os.objtype
320 and os.objdefiner not in ('*IBM', 'QDPINSTALL', 'QSYS') and os.objowner <> 'QSYS'
321 LEFT EXCEPTION JOIN qsys2.object_privileges b ON new_system_usrprf = b.authorization_name and
322 a.object_schema = b.object_schema and a.object_name = b.object_name and a.object_type = b.object_type and
323 a.object_authority = b.object_authority AND
324 a.authorization_list IS NOT DISTINCT FROM b.authorization_list AND
325 a.primary_group IS NOT DISTINCT FROM b.primary_group AND
326 a.owner = b.owner AND a.authorization_list_management = b.authorization_list_management AND
327 a.object_owner = b.object_owner AND
328 a.object_operational = b.object_operational AND a.object_management = b.object_management AND
329 a.object_existence = b.object_existence AND a.object_alter = b.object_alter AND
330 a.object_reference = b.object_reference AND a.data_read = b.data_read AND
331 a.data_add = b.data_add AND a.data_delete = b.data_delete AND
332 a.data_update = b.data_update AND a.data_execute = b.data_execute
333 order by previous_system_usrprf, a.object_schema, a.object_name, a.object_type;
```

	OBJECT_SCHEMA	OBJECT_NAME	OBJECT_TYPE	OBJECT_AUTHORITY	OWNER	OBJECT_OWNER	OBJECT_OPERATIONAL	OBJECT_MANAGEMENT	OBJECT_EXISTENCE	OBJECT_ALTER	OBJECT_REFERENCE	DATA_READ
PREVIOUS_SYSTEM_USRPRF	Object Schema	Object Name	Object Type	Object Authority	Owner	Object Owner	Object Operational	Object Management	Object Existence	Object Alter	Object Reference	Data Read
QPGMR	ERPPGM	ERPMENU	*PGM	*USE	QDFTOWN	NO	YES	NO	NO	NO	NO	YES
QPGMR	LIBHTTP	EXAMPLE1	*PGM	*ALL	QPGMR	YES	YES	YES	YES	YES	YES	YES
QPGMR	LIBHTTP	EXAMPLE10	*PGM	*ALL	QPGMR	YES	YES	YES	YES	YES	YES	YES
QPGMR	LIBHTTP	EXAMPLE11	*PGM	*ALL	QPGMR	YES	YES	YES	YES	YES	YES	YES
QPGMR	LIBHTTP	EXAMPLE12	*PGM	*ALL	QPGMR	YES	YES	YES	YES	YES	YES	YES

```
292 -- collect authorizations that the previous user profile has, but not the new one (on other objects)
293 SELECT previous_system_usrprf, a.authorization_user, a.object_authority, a.object_operational, a.object_management, a.object_existence, a.object_alter,
294 a.object_reference, a.data_read, a.data_add, a.data_update, a.data_delete, a.data_execute,
295 a.authorization_list, a.primary_group, a.authorization_list_management, os.objdefiner
296 from rslaud.old_new_system_usrprf
297 join TABLE(qsys2.object_privileges('QSYS', previous_system_usrprf)
298 on previous_system_usrprf = previous_system_usrprf
299 LEFT EXCEPTION JOIN TABLE (qsys2.object_privileges('QSYS', new_system_usrprf)
300 ON a.object_authority = b.object_authority AND
301 a.authorization_list IS NOT DISTINCT FROM b.authorization_list AND
302 a.primary_group IS NOT DISTINCT FROM b.primary_group AND
303 a.owner = b.owner AND a.authorization_list_management = b.authorization_list_management AND
304 a.object_owner = b.object_owner AND
305 a.object_operational = b.object_operational AND a.object_management = b.object_management AND
306 a.object_existence = b.object_existence AND a.object_alter = b.object_alter AND
307 a.object_reference = b.object_reference AND a.data_read = b.data_read AND
308 a.data_add = b.data_add AND a.data_delete = b.data_delete AND
309 a.data_update = b.data_update AND a.data_execute = b.data_execute;
```

PREVIOUS_SYSTEM_USRPRF	AUTHORIZATION_USER	OBJECT_AUTHORITY	OWNER	OBJECT_OWNER	OBJECT_OPERATIONAL	OBJECT_MANAGEMENT	OBJECT_EXISTENCE	OBJECT_ALTER	OBJECT_REFERENCE	DATA_READ
QSECOFR	QSECOFR	*ALL	QSYS	NO	YES	YES	YES	YES	YES	YES
QSYSOPR	*PUBLIC	*USE	QSYS	NO	YES	NO	NO	NO	NO	YES
QSYSOPR	GM	*USE	QSYS	NO	YES	NO	NO	NO	NO	YES

Actions requiring now *IOSYSCFG special authority or QIBM_IOSYSCFG_VIEW function usage *ALLOWED

- Prompting current value or displaying values: *IOSYSCFG or QIBM_IOSYSCFG_VIEW required
- Making changes: *IOSYSCFG required
- **Prior to 7.6:** Some read-access and change-access to sensitive configuration informations are protected by Object Level Security only
- **From 7.6** : Better protecting read-access and change-access to sensitive configuration informations
 - Configuration commands (DSPCFGL, WRKDEVD, WRKLIND, WRKCTLD, ...) → 7.5 = read-access to public
 - DDM/RDB config commands (WRKDDMF, WRKRDBDIRE, CHGDDMTCPA, ...) → 7.5 = read-access to public
 - System values (QCFGMSGQ, QSSLCSL, QSSLCSLCTL, QSSLPCL) → 7.5 = read-access to public like any system value
 - Network attributes (JOBACN, DDMACC, PCSACC, ALWADDCLU) → 7.5 = read-access to public like any network attribute
 - TCP/IP commands and APIs (CFGTCP, NETSTAT, CHGTCPA, CHGTCPDMN, CHGTCPSVR, CHGUSRSNMP, CHGTELNA, ...)
 - Tape commands (DSPTAPCTG, DSPTAPSTS, CHGTAPF, ...)
 - SQL Services (ASP_INFO, NETSTAT_INFO, NETSTAT_JOB_INFO, RDB_ENTRY_INFO, SERVER_SHARE_INFO, TELNET_SERVER_ATTRIBUTES, ...)
 - Db2 Mirror SQL services (MIRROR_CLUSTER_INFO, MIRROR_INFO, NRG_INFO, RDMA_LINK_INFO, ...)
- CHGFTPA was already protected with *IOSYSCFG since We could not remember; so we asked Bob, it said since V4R5

Displaying System Values

- **Prior to 7.6:** Public read-access to all system values (except values related to auditing which require *AUDIT)
- **From 7.6 :** Public read-access to all system values (except values related to auditing which require *AUDIT and values related to SSL which require *IOSYSCFG or QIBM_IOSYSCFG_VIEW)

	SYSTEM_VALUE_NAME	TEXT_DESCRIPTION	SYSTEM_VALUE_V7R5	SYSTEM_VALUE_V7R6	SHIPPED_DEFAULT_VALUE_V7R6
CATEGORY	System Value	Text	System Value	System Value	Shipped Default Value
Category	Name	Description	Value	Value	Value
*MSG	QCFGMSGQ	Configuration message queue	QSYS/QSYSOPR	*NOTAVL	QSYS/QSYSOPR
*SEC	QAUDCTL	Auditing control	*NOTAVL	*NOTAVL	*NONE
*SEC	QAUDENDACN	Auditing end action	*NOTAVL	*NOTAVL	*NOTIFY
*SEC	QAUDPRCLVL	Force auditing data	*NOTAVL	*NOTAVL	*SYS
*SEC	QAUDLVL	Security auditing level	*NOTAVL	*NOTAVL	*NONE
*SEC	QAUDLVL2	Security auditing level extension	*NOTAVL	*NOTAVL	*NONE
*SEC	QCRTOBJAUD	Create object auditing	*NOTAVL	*NOTAVL	*NONE
*SEC	QSSLCSL	Secure sockets layer cipher specifi...	*AES_128_GCM_SHA256	... *NOTAVL	*AES_128_GCM_SHA256..
*SEC	QSSLCSLCTL	Secure sockets layer cipher control	*OPSYS	*NOTAVL	*OPSYS
*SEC	QSSLPLCL	Secure sockets layer protocols	*OPSYS	*NOTAVL	*OPSYS

Object Name	Object Type	SQL Object Type	Authorization Name	Object Authority	Object Operational	Data Read	Data Execute	Text Description
DSPSYSVAL	*CMD	-	*PUBLIC	*USE	YES	YES	YES	Display System
SYSTEM_VALUE_INFO	*FILE	VIEW	*PUBLIC	USER_DEFINED	YES	YES	NO	-

	SYSTEM_VALUE_NAME	TEXT_DESCRIPTION	SHIPPED_DEFAULT_VALUE_V7R5	SHIPPED_DEFAULT_VALUE_V7R6
CATEGORY	System Value	Text	Shipped Default Value	Shipped Default Value
Category	Name	Description	Value	Value
*SEC	QPWDLVL	Password level	0	3
*SEC	QPWDRULES	Password rules	*PWDSYSVAL	

Displaying System Values using SECURITY_INFO

- **Prior to 7.6:** SECURITY_INFO public read-access
DSPSECA public read-access
DSPSECAUD requires *AUDIT
- **From 7.6** : Requires *AUDIT or *SECADM to run this service and DSPSECA

```
505 -- security_info protected with *AUDIT or *SECADM from 7.6
506 set session authorization gm_basic;
507 select * from qsys2.security_info ;
508 SELECT text_description, system_value FROM QSYS2.system_value_info where system_value_name like 'QPWD%'
509
510
511
```

SECURITY_LEVEL	PENDING_SECURITY_LEVEL	PASSWORD_LEVEL	PENDING_PASSWORD_LEVEL	ADDITIONAL_SIGNON_FACTOR
Security Level	Pending Security Level	Password Level	Pending Password Level	Additional Signon Factor

ERROR: [SQL0443] *AUDIT OR *SECADM SPECIAL AUTHORITY REQUIRED Cause : Either a trigger program

TEXT_DESCRIPTION	SYSTEM_VALUE
Text	System
Description	Value
Maximum sign-on attempts allowed	5
Duplicate password control	0
Limit adjacent digits in password	0
Limit repeating characters in password	0
Limit password character positions	0
Require digit in password	0
Minimum password length	6
Maximum password length	8
Limit characters in password	*NONE
Password validation program	*NONE
Password expiration interval	*NOMAX
Action to take for failed signon attempts	2
Maximum spooled files	9999
Password level	3
Password rules	*LMTPRFNAME...
Block password change	*NONE
Password expiration warning	7

Manipulating Shares

Case: Reinforce authority required to create/change/remove a NetServer File share

- **Prior to 7.6:** The owner of a directory can manipulate the corresponding share without additional controls
- **From 7.6 :** The owner of a directory needs to be registered in function QIBM_QZLS_NETSVR_SHARE in order to manipulate the corresponding share

```
867 cl: extdir '/ibmi_tmp' ;
868 cl: CALL QZLSADFS PARM(testADDSHARE '/ibmi_tmp' x'00000009' x'00000000' 'Root in Read/Write mode' x'00000002' x'FFFFFFF' x'00000000' ) ;
869 cl: CALL QZLSRMS PARM(testADDSHARE x'00000000') ;
870
```

[08/30/2026, 10:09:54 PM] Run Selected...

CALL QZLSADFS PARM(testADDSHARE '/ibmi_tmp' x'00000009' x'00000000' 'Root in Read/Write mode' x'00000002' x'FFFFFFF' x'00000000')

CPF684: User does not have the correct authority for API QZLSADFS.

✗ The highlighted statement did not complete successfully.

Message ID : CPF684 Severity : 40
Message type : Escape
Date sent : 30/08/26 Time sent : 21:09:49

Message : User does not have the correct authority for API QZLSADFS.
Cause : Error occurred for reason code 4. See explanation of the reason codes below:

- 1 - User does not have *IOSYSCFG special authority.
- 2 - User does not have *IOSYSCFG and *SECADM special authority.
- 3 - File system directory or output queue does not exist and the user does not have *IOSYSCFG special authority.
- 4 - User does not have *IOSYSCFG special authority or is not the owner of the file system directory or output queue with authority to the QIBM_QZLS_NETSVR_SHARE function usage identifier.
- 5 - User does not have *IOSYSCFG special authority or authority to the QIBM_IOSYSCFG_VIEW function usage identifier.

CHGFCNUSG FCNID(QIBM_QZLS_NETSVR_SHARE) USER(GM_BASICLM) USAGE(*ALLOWED)
CPC221D: Function QIBM_QZLS_NETSVR_SHARE usage information changed.
✓ Statement ran successfully (162 ms)

Things I can't do up to 7.5, can from 7.6

Some of these features are also included in 7.5 TR8

MFA

Case: I need to reinforce authentication for some users with a second factor (in a single step)

- **Prior to 7.6:** There is no (easy) way to do it, even when buying a 3rd-party solution
- **From 7.6 :** Use the IBM native solution or/and use a 3rd-party solution for additional scenarios
 - Multi-Factor Authentication (MFA) is free and built into the operating system
 - Enabling MFA activates the feature; it is enabled on a per-user basis rather than at system level
 - It can be enabled within the operating system and/or within SST (using independent layers and configurations)
 - It supports only the TOTP (Time-based One-Time Password – RFC 6238) protocol
 - No infrastructure changes are required (in compliance with RFC 6238)
 - Further improvements are planned
 - Understanding "persistence" is essential for optimal use.

Many resources available to help you implement it:

IBM documentation	www.ibm.com/docs/en/i/7.6.0?topic=security-multi-factor-authentication-mfa
IBM Redbook	www.redbooks.ibm.com/abstracts/sg248588.html
IBM quick "How To"	www.ibm.com/support/pages/ibm-i-%E2%80%93-enabling-multifactor-authentication-mfa-technical-guide
Common - iSee	https://learn.common.org/products/isee-integrated-multi-factor-authentication?packages%5B%5D=46368&in_package=46368&sort_by=package_order&ref=package&ref_id=46368
Fortra	https://www.youtube.com/watch?v=wYTxJEkeo6Q
I.Gayte.It - Resiliane	https://i.gayte.it/en/securit-i-2025-replays/

From the Redbook:
« Refer to this IBM i 7.6 doc information as the list of connection protocols that support MFA will likely continue to change over time. »

ASP 1 Encryption

Case: I need to encrypt my data at rest

- **Prior to 7.6:** Only Basic ASPs (2-32) and iASPs (33-225) can be encrypted at 7.5 and below
- **From 7.6** : Included at no cost

- Included in the operating system
- Works on internal IBM i storage
- Helps you meet compliance requirements
- Can be started or stopped whilst system in use
- Requires SS1 Option 45 - Encrypted ASP Enablement
- Encryption uses AES with 256 bit key in CBC mode.

Install Licensed Programs

System: JEDI76

Type options, press Enter.
1=Install

Option	Licensed Program	Product Option	Description
—	5770SS1	38	PSF for IBM i Any Speed Printer Support
—	5770SS1	39	International Components for Unicode
—	5770SS1	41	HA Switchable Resources
—	5770SS1	42	HA Journal Performance
—	5770SS1	43	Additional Fonts
—	5770SS1	44	Encrypted Backup Enablement
1	5770SS1	45	Encrypted ASP Enablement
—	5770SS1	47	IBM Advanced Data Security for i
—	5770SS1	48	Db2 Data Mirroring
—	5761AP1	*BASE	IBM Advanced DBCS Printer Support for i
—	5761AP1	1	Adv DBCS Printer Support - IPDS
—	5770BR2	*BASE	IBM Backup, Recovery and Media Services for i

F3=Exit

F11=Display status/release

F12=Cancel

F19=Display trademarks

More...

ASP 1 Encryption

Case: I need to encrypt my data at rest

- **Prior to 7.6:** You must use external storage, such as an IBM Flash System FS5nnn SAN
- **From 7.6** : Included at no cost

- Enabling ASP 1 Encryption
- STRSST
- Work with Disk Configuration
- Work with Encryption
- Start Encryption on ASPs

Confirm Start Encryption on ASPs

Data will be encrypted on the selected ASPs.
For independent ASPs, data will be encrypted when they are varied on.

Note: Do not stop encryption on the ASPs until this operation has completed. Do not change the data encryption key on the ASPs until this operation has completed.

Press Enter to confirm your choices to start encryption.
Press **F12** to return to change your choices.

Option	ASP	-----Protected-----	Size	%Used	---Unprotected---	Size	%Used	Status
1	1		3200000	19.39%		0	0.00%	Encrypting

F12=Cancel

ASP 1 Encryption

Case: I need to encrypt my data at rest

- **Prior to 7.6:** If you need to store sensitive data in ASP1, encrypt it at the object level
- **From 7.6** : Included at no cost

Things to consider

- The Encryption Keys are stored in the LIC
- You should take a SAVSYS or Go Save 21 after
- Do not IPL server whilst starting/stopping encryption
- There is a performance overhead (circa 20%)
- If you are moving from HDD to NVMe I doubt you'll notice
- If i/o performance is vital consider alternatives
- NVMe Key Management (requires HMCs)
- External Storage

*IOSYSCFG special authority versus QIBM_IOSYSCFG_VIEW function usage

Case: Grant read-only authorities to users who need to view configurations without modifying them.

- **Prior to 7.6:** Giving *IOSYSCFG special authority to the user
- **From 7.6 :** Registering the user in function QIBM_IOSYSCFG_VIEW with usage *ALLOWED

New function ID QIBM_IOSYSCFG_VIEW allows to grant/deny access to these commands/api/services in a read-only mode:

- Configuration commands (DSPCFGL, DSPDEVD, DSPLIND, WRKCTLD, ...)
- DDM/RDB config commands (WRKDDMF, WRKRDBDIRE, CHGDDMTCPA, ...)
- System values (QCFGMSGQ, QSSLCSL, QSSLCSLCTL, QSSLPCL)
- Network attributes (JOBACN, DDMACC, PCSACC, ALWADDCLU)
- TCP/IP commands and APIs (CFGTCP, NETSTAT, CHGTCPA, CHGTCPDMN, CHGTCPSVR, CHGUSRSNMP, CHGFTPA, CHGTELNA, ...)
- Tape commands (DSPTAPCTG, DSPTAPSTS, ...)
- SQL Services (ASP_INFO, NETSTAT_INFO, NETSTAT_JOB_INFO, RDB_ENTRY_INFO, SERVER_SHARE_INFO, TELNET_SERVER_ATTRIBUTES, ...)
- Db2 Mirror SQL services (MIRROR_CLUSTER_INFO, MIRROR_INFO, NRG_INFO, RDMA_LINK_INFO, ...)



*IOSYSCFG special authority versus QIBM_IOSYSCFG_VIEW function usage

Case: Grant read-only authorities to users who need to view configurations without modifying them.

- Prior to 7.6: Giving *IOSYSCFG special authority to the user
- From 7.6 : Registering the user in function QIBM_IOSYSCFG_VIEW with usage *ALLOWED

New function ID QIBM_IOSYSCFG_VIEW allows to grant/deny access to these commands/api/services in a read-only mode:

FUNCTION_ID	DEFAULT_USAGE	ALLOBJ_INDICATOR	USAGE	USER_NAME	USER_TYPE
Function ID	Default Usage	Allobj Indicator	Usage	User Name	User Type
QIBM_IOSYSCFG_VIEW	DENIED	NOT USED	ALLOWED	GM	USER
QIBM_IOSYSCFG_VIEW	DENIED	NOT USED	DENIED	GM_ALLOBJ	USER

```
chgftpa
*IOSYSCFG authority or QIBM_IOSYSCFG_VIEW functional usage required to use
CHGFTPA.
Current values could not be retrieved.
```

```
Message ID . . . . . : TCP8051      Severity . . . . . : 40
Message type . . . . . : Diagnostic
Date sent . . . . . : 06/08/26      Time sent . . . . . : 21:35:30
```

```
Message . . . . . : *IOSYSCFG authority or QIBM_IOSYSCFG_VIEW functional usage
                    required to use CHGFTPA.
Cause . . . . . : *IOSYSCFG special authority or QIBM_IOSYSCFG_VIEW
                    functional usage is required to use the CHGFTPA API or command.
Recovery . . . . . : Ask the security administrator to grant your user profile
                    *IOSYSCFG special authority or QIBM_IOSYSCFG_VIEW functional usage.
```

Protecting against impersonations

Case: I am allowed to run a process under a user I have authority on.

- **Prior to 7.6:** There is no (easy) way to protect us against this potential usurpation/impersonation
- **From 7.6 :** Register the target user in function QIBM_RUN_UNDER_USER_NO_AUTH with *DENIED usage

```
531 set session authorization gm_openbar ;
```

***ALLOBJ required**

```
[ 08/10/2026, 05:49:41 PM ] Run Selected...
set session authorization gm_openbar
Statement ran successfully (148 ms)
```

```
542 cl: sbmjob cmd(chgusrprf gm_basiclm spcaut(*allobj) lmtcpb(*no)) user(gm_openbar) job(aieaieaie)
```

***USE authority required on the target user**

```
sbmjob cmd(chgusrprf gm_basiclm spcaut(*allobj) lmtcpb(*no)) user(gm_openbar) job(aieaieaie)

CPC1221: Job 023577/GM_OPENBAR/AIEAIEAIE submitted to job queue QBATCH in library QGPL.
Statement ran successfully (154 ms)
```

```
[ 08/14/2026, 02:45:18 PM ] Run Selected...
CHGFCNUSG FCNID(QIBM_RUN_UNDER_USER_NO_AUTH) USER(GM_OPENBAR) USAGE(*DENIED)

CPC221D: Function QIBM_RUN_UNDER_USER_NO_AUTH usage information changed.
✓ Statement ran successfully (150 ms)
```

```
[ 08/14/2026, 02:46:30 PM ] Run Selected...
set session authorization gm_openbar
✗ SQL State: 28000
Vendor Code: -552
Message: [SQL0552] Not authorized to SET SESSION_USER. Cause . . . . . : The operation cannot be performed without the required authority.
```

```
[ 08/14/2026, 02:47:36 PM ] Run Selected...
sbmjob cmd(DLTLIB LIB(XXXX)) user(gm_openbar) job(ouille)

CPF4AF1: Operation not allowed for user profile GM_OPENBAR.
CPD1616: Not authorized to user profile GM_OPENBAR.
CPF1338: Errors occurred on SEMJOB command.
```

Protecting against impersonations

Case: I am allowed to run a process under a user I have authority on.

- **Prior to 7.6:** There is no (easy) way to protect us against this potential usurpation/impersonation
- **From 7.6 :** Register the target user in function QIBM_RUN_UNDER_USER_NO_AUTH with *DENIED usage

IBM Navigator for i

Dashboard

Users

Actions

Details: Basic All

Profile Type	Name	Profile Status	Impersonation	MFA Authentication	MFA Key Exists
User	BADLAD	*ENABLED	DENIED	NO	NO
User	FTPIBLOCK	*ENABLED	DENIED	NO	NO
User	FTPOBLOCK	*ENABLED	DENIED	NO	NO
User	GM	*ENABLED	ALLOWED	NO	NO
User	GM_OPENBAR	*DISABLED	ALLOWED	NO	NO

IBM Navigator for i

FTPOBLOCK - Properties

User: FTPOBLOCK

Description: Test FTP outbound Blocked

Class: User

Password:

Additional Authentication Options:

☒ Deny Impersonation ⓘ

Impersonation

When the value of Impersonation is DENIED for a profile, the operating system will restrict the ability to impersonate this user profile without authentication. The system will block any attempt to swap to this user profile without specifying a password. This is controlled by setting the function usage ID QIBM_RUN_UNDER_USER_NO_AUTH to DENIED for this profile.

Protecting against impersonations (auditing)

```
589 -- review function ID and usage
590 SELECT fu.user_name, fu.usage, fu.user_type, fi.default_usage, fi.allobj_indicator, fi.function_id, fi.function_name_message_text
591 FROM QSYS2.FUNCTION_INFO fi left join QSYS2.FUNCTION_USAGE fu on fu.function_id = fi.function_id
592 where fu.function_id = 'QIBM_RUN_UNDER_USER_NO_AUTH'
593 order by user_name ;
594
```

USER_NAME	USAGE	USER_TYPE	DEFAULT_USAGE	ALLOBJ_INDICATOR	FUNCTION_ID	FUNCTION_NAME_MESSAGE_TEXT
User Name	Usage	User Type	Default Usage	Allobj Indicator	Function ID	Function Name Message Text
GM_OPENBAR	DENIED	USER	ALLOWED	NOT USED	QIBM_RUN_UNDER_USER_NO_AUTH	Run under a user without authentication

Default is ***ALLOWED** and **NOT-CHANGEABLE**
(idea under consideration)

```
595 -- monitor changes in function QIBM_RUN_UNDER_USER_NO_AUTH
596 select jrn.ENTRY_TIMESTAMP, job_name, user_name, program_name,
597 remote_address, function_name, function_registration_operation, user_profile_name, usage_setting, previous_usage
598 from table(SYSTOOLS.AUDIT_JOURNAL_GR (STARTING_RECEIVER_NAME => '*CURCHAIN', STARTING_TIMESTAMP => current date)) jrn
599 where entry_type = 'F' and function_name = 'QIBM_RUN_UNDER_USER_NO_AUTH'
600 and function_registration_operation = 'CHANGE USAGE' and usage_setting <> previous_usage ;
601
```

ENTRY_TIMESTAMP	JOB_NAME	USER_NAME	PROGRAM_NAME	REMOTE_ADDRESS	FUNCTION_NAME	FUNCTION_REGISTRATION_OPERATION	USER_PROFILE_NAME	USAGE_SETTING	PREVIOUS_USAGE
2026-08-14 13:...	QZDASOINIT	GM	QCMDExC1	10.24...	QIBM_RUN_UNDER_U...	CHANGE USAGE	GM_OPENBAR	REMOVED	UNKNOWN
2026-08-14 13:...	QZDASOINIT	GM	QCMDExC1	10.24...	QIBM_RUN_UNDER_U...	CHANGE USAGE	GM	REMOVED	UNKNOWN
2026-08-14 13:...	QZDASOINIT	GM	QCMDExC1	10.24...	QIBM_RUN_UNDER_U...	CHANGE USAGE	GM_OPENBAR	DENIED	UNKNOWN

```
602 -- monitor failures in function QIBM_RUN_UNDER_USER_NO_AUTH
603 select jrn.ENTRY_TIMESTAMP, job_name, user_name, program_name,
604 remote_address, function_name, function_registration_operation, user_profile_name
605 from table(SYSTOOLS.AUDIT_JOURNAL_GR (STARTING_RECEIVER_NAME => '*CURCHAIN', STARTING_TIMESTAMP => current date)) jrn
606 where entry_type = 'F' and function_name = 'QIBM_RUN_UNDER_USER_NO_AUTH'
607 and function_registration_operation = 'USAGE FAILURE';
```

ENTRY_TIMESTAMP	JOB_NAME	USER_NAME	PROGRAM_NAME	REMOTE_ADDRESS	FUNCTION_NAME	FUNCTION_REGISTRATION_OPERATION	USER_PROFILE_NAME
2026-08-14 13:...	QZDASOINIT	GM	QZDASOINIT	10.24...	QIBM_RUN_UNDER...	USAGE FAILURE	GM_OPENBAR
2026-08-14 13:...	QZDASOINIT	GM	QCMDExC1	10.24...	QIBM_RUN_UNDER...	USAGE FAILURE	GM_OPENBAR
2026-08-14 13:...	QZDASOINIT	GM	QZDASOINIT	10.24...	QIBM_RUN_UNDER...	USAGE FAILURE	GM_OPENBAR
2026-08-14 13:...	QZDASOINIT	GM	QCMDExC1	10.24...	QIBM_RUN_UNDER...	USAGE FAILURE	GM_OPENBAR

```
609 -- monitor predicted failures in function QIBM_RUN_UNDER_USER_NO_AUTH
610 cl: CHGUSRAUD USRPRF(GM_OPENBAR) AUDLVL(*AUTWARN) ;
611 cl: CHGFCNUSG FCNID(QIBM_RUN_UNDER_USER_NO_AUTH) USER(GM_OPENBAR) USAGE(*NONE) ;
612
613 set session authorization gm_openbar ;
614 set session authorization gm;
615
616 select jrn.ENTRY_TIMESTAMP, job_name, user_name, program_name,
617 remote_address, function_name, function_registration_operation, user_profile_name
618 from table(SYSTOOLS.AUDIT_JOURNAL_GR (STARTING_RECEIVER_NAME => '*CURCHAIN', STARTING_TIMESTAMP => current date)) jrn
619 where entry_type = 'F' and function_name = 'QIBM_RUN_UNDER_USER_NO_AUTH'
620 and function_registration_operation = 'USAGE WARNING';
```

ENTRY_TIMESTAMP	JOB_NAME	USER_NAME	PROGRAM_NAME	REMOTE_ADDRESS	FUNCTION_NAME	FUNCTION_REGISTRATION_OPERATION	USER_PROFILE_NAME
2026-08-14 13:...	QZDASOINIT	GM_BASICLM	QCMDExC1	10.2...	QIBM_RUN_UNDER...	USAGE WARNING	GM_OPENBAR
2026-08-14 13:...	QZDASOINIT	GM_BASICLM	QCMDExC1	10.2...	QIBM_RUN_UNDER...	USAGE WARNING	GM_OPENBAR
2026-08-14 13:...	QZDASOINIT	GM_BASICLM	QCMDExC1	10.2...	QIBM_RUN_UNDER...	USAGE WARNING	GM_OPENBAR
2026-08-14 13:...	QZDASOINIT	GM_BASICLM	QCMDExC1	10.2...	QIBM_RUN_UNDER...	USAGE WARNING	GM_OPENBAR
2026-08-14 13:...	QZDASOINIT	GM	QZDASOINIT	10.2...	QIBM_RUN_UNDER...	USAGE WARNING	GM_OPENBAR
2026-08-14 14:...	QZDASOINIT	GM	QZDASOINIT	10.2...	QIBM_RUN_UNDER...	USAGE WARNING	GM_OPENBAR

New Configure Host Server Command

Case: Allows administrators to enable, disable, or restrict non-secure (unencrypted) connections to host servers

- **Prior to 7.6:** Create your own utility based on Exit Programs and TCP Port Restrictions (CFGTCP option 4)
- **From 7.6 :** Require some or all to only accept Secure connections
*SECLOOP can be specified to allow non-secure connections ONLY from *LOOPBACK interface

Configure Host Server (CFGHOSTSVR)

IBM i

- Enable, disable, or allow loopback for non-secure connections on the supported host servers
 - Central, Database, Data Queue, File, Network Print, Remote Command, and Signon
- Provides architected and auditable way to comply with port scan audits by disabling non-secure ports
 - Currently administrators add a TCP port restriction as a circumvention
 - This prevents non-TLS applications from using the host servers over loopback
- Configure the type of connections allowed for each host server (CNNTYPE)
 - *SECURE - Only TLS/Secure connections allowed. Insecure port not started
 - *SECLOOP - TLS/Secure connections and insecure loopback connections allowed
 - Insecure port is not listening on the external interfaces
 - *ALL – All insecure and secure connections allowed

```
Configure Host Server (CFGHOSTSVR)

Type choices, press Enter.

Configuration . . . . . > *CNNTYPE      *CNNTYPE, *LISTEN
Server type   . . . . . > *RMTCMD      *ALLCFG, *CENTRAL...
               + for more values
Connection type . . . . . *SECURE      *SAME, *ALL, *SECLOOP...
```

Universal Authentication Exit Point

- QIBM_QSY_AUTH
- **Universal !!!!!!!!!!!!!**
- Activated user per user
- Independant from MFA
- Can enforce **ANY** authentication from **ANY** user (service accounts)
- Can trigger additional MFA
- When *TOTP + *REGFAC, *TOTP first and then exit pgm

NIST 800-63B-4
SMS, HOTP and TOTP
not compatible with
AAL3 requirements

User profile	:	GM_REGFAC
Previous sign-on	:	14/08/26 14:45:03
Authentication attempts not valid	:	0
Status	:	*ENABLED
Date password last changed	:	14/08/26 14:44:32
Password is *NONE	:	*NO
Password expiration interval	:	*SYSVAL
Password set expired by command	:	*NO
Block password change	:	*SYSVAL
Local password management	:	*YES
TOTP key exists	:	No
Date TOTP key last changed	:	
Authentication methods	:	*REGFAC ←
TOTP optional interval	:	*NONE
Maximum sign-on attempts	:	*SYSVAL

Can be used to build a comprehensive
inventory of authentication categories

New Platform KeyStore (PKS) for iSCSI CHAP authorization

Case: Reduce risk of unauthorized access to data stored on (VTL) virtual tape devices

- **Prior to 7.6:** Required separate TKLM solution
- **From 7.6** : Integrated into HMC / LPAR management

3.9.11 Using Platform KeyStore (PKS) for iSCSI CHAP authorization credentials

The Power Platform KeyStore (PKS) feature on IBM Power10-based servers provides an encrypted, non-volatile storage area designed to enhance data protection. PKS enables logical partitions (LPARs) to securely store sensitive information with partition-specific access controls managed through PowerVM. PowerVM also supports automatic, encrypted migration of PKS data during Live Partition Mobility (LPM) operations, ensuring the security and integrity of iSCSI CHAP credentials as IBM i LPARs move between systems.

With IBM i 7.6, administrators can configure the encrypted PKS to store iSCSI Challenge Handshake Authentication Protocol (CHAP) credentials. With this capability, organizations that use iSCSI-attached Virtual Tape Libraries (VTLs) can safeguard authentication data more effectively, reducing the risk of unauthorized access to virtual tape devices and their contents.

The following requirements must be met:

- ▶ Power 10 + FW10xx and IBM i 7.6
- ▶ iSCSI D-mode with CHAP configuration as plaintext requires FW1050 + PKS
- ▶ iSCSI D-mode with CHAP configuration as a PKS label requires FW1060+
- ▶ PKS Must be enabled for the partition

Use HMC partition properties to enable PKS. This configuration sets PKS as the default method for iSCSI target configurations when they are added or modified. Enhancements to the iSCSI Configuration SQL Services display the storage state of CHAP authentication data so that users can opt out of using PKS for specific target configurations, if needed.

Managing Master Key

Case: Protect against theft or cloning of IBM i Disk Units

- Prior to 7.6: The Save/Restore was set to a default value
- From 7.6 : You must set the Save/Restore key before you set any other master keys
 - NOTE: If you do this, you must protect the Save/Restore Key or your system will not IPL!

Managing master keys

The save/restore master key is no longer set to a default value. Users must explicitly set the key before any of the system master keys can be set. If the save/restore master key is cleared, a subsequent IPL will not complete until the save/restore key is recovered using the Remote Key Agent utility.

QAUDJRN Authentication Entries

PW = Authentication violations (requires *AUTFAIL)

```
729 -- using QAUDJRN, check for signon violations (starting with 7.4 TR4 7.3 TR10)
730 SELECT entry_timestamp, job_name, job_user, program_name, remote_address, AUDIT_USER_NAME,
731 VIOLATION_TYPE, VIOLATION_TYPE_DETAIL
732 FROM TABLE (SYSTOOLS.AUDIT_JOURNAL_PW (STARTING_RECEIVER_NAME => '*CURCHAIN',
733 STARTING_TIMESTAMP => current date - 0 days)) jrn ;
```

New types: F, G, K, O, T
TOTP & Exit point

ENTRY_TIMESTAMP	JOB_NAME	JOB_USER	PROGRAM_NAME	REMOTE_ADDRESS	AUDIT_USER_NAME	VIOLATION_TYPE	VIOLATION_TYPE_DETAIL
2026-08-21 14:...	QZDASOINIT	QUSER_NC	QZDASOINIT	127.0...	GM_TOTP	O	Time-based one-time password (TOTP) specified on CHKTOTP command not valid
2026-08-21 14:...	QZDASOINIT	QUSER_NC	QZDASOINIT	127.0...	GM_TOTP	O	Time-based one-time password (TOTP) specified on CHKTOTP command not valid
2026-08-21 14:...	QZDASOINIT	QUSER_NC	QZDASOINIT	127.0...	GM_TOTP	O	Time-based one-time password (TOTP) specified on CHKTOTP command not valid
2026-08-21 14:...	QZSOSIGN	QUSER_NC	QZSOSIGN	10.24...	GM_TOTP	P	Password not valid
2026-08-21 14:...	QINTER	QSYS	QLESPI	-	GM_TOTP	T	Time-based one-time password (TOTP) not valid
2026-08-21 14:...	QINTER	QSYS	QLESPI	-	GM_TOTP	T	Time-based one-time password (TOTP) not valid
2026-08-21 14:...	QPADEV0005	GM_TOTP	QCMD	10.24...	GM_TOTP	K	Password specified on CHKTOTP command not valid
2026-08-21 14:...	QPADEV0005	GM_TOTP	QCMD	10.24...	GM_TOTP	O	Time-based one-time password (TOTP) specified on CHKTOTP command not valid
2026-08-21 14:...	QZSOSIGN	QUSER_NC	QZSOSIGN	10.24...	GM_TOTP	T	Time-based one-time password (TOTP) not valid
2026-08-21 14:...	QZSOSIGN	QUSER_NC	QZSOSIGN	10.24...	GUTMARMO	U	User name not valid

VP = Network activity (requires *NETFAIL/*NETCMN)

```
735 -- using QAUDJRN, check for signon violations (NetServer)
736 SELECT entry_timestamp, job_name, job_user, program_name, remote_address, AUDIT_USER_NAME, computer_name,
737 ENTRY_TYPE_DETAIL, share_authorization_list, share_action, permissions, share_name, path_name, jrn.*
738 FROM TABLE (SYSTOOLS.AUDIT_JOURNAL_VP (STARTING_RECEIVER_NAME => '*CURCHAIN',
739 STARTING_TIMESTAMP => current date - 0 days)) jrn
740 where entry type in ('P', 'D', 'A', 'U');
```

New type: U
Invalid User

ENTRY_TIMESTAMP	JOB_NAME	JOB_USER	PROGRAM_NAME	REMOTE_ADDRESS	AUDIT_USER_NAME	COMPUTER_NAME	ENTRY_TYPE_DETAIL
2026-08-21 14:...	QZLSSERVER	QUSER_NC	QZLSSERVER	10.24...	GM	::ffff:10.2...	Password error
2026-08-21 15:...	QZLSSERVER	QUSER_NC	QZLSSERVER	10.24...	GM	::ffff:10.2...	Password error
2026-08-21 15:...	QZLSSERVER	QUSER_NC	QLESPI	-	BRAD	::ffff:10.2...	Unknown user attempt to connect or guest...
2026-08-21 15:...	QZLSSERVER	QUSER_NC	QZLSSERVER	10.24...	GM_TOTP	::ffff:10.2...	Password error
2026-08-21 15:...	QZLSSERVER	QUSER_NC	QZLSSERVER	10.24...	GM_TOTP	::ffff:10.2...	Password error
2026-08-21 15:...	QZLSSERVER	QUSER_NC	QZLSSERVER	10.24...	GM_TOTP	::ffff:10.2...	Password error
2026-08-21 15:...	QZLSSERVER	QUSER_NC	QZLSSERVER	10.24...	GM_TOTP	::ffff:10.2...	NetServer user disabled

CP = Changes to user profiles (requires *SECURITY/*SECCFG)

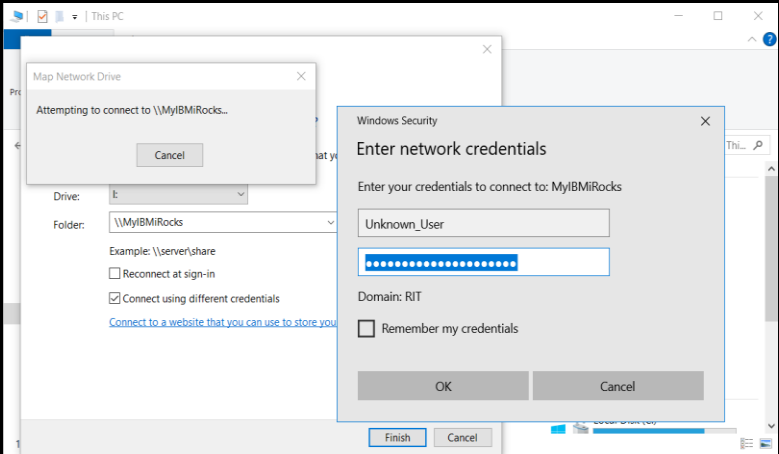
```
742 -- using QAUDJRN, check for TOTP/REGFAC changes on users
743 SELECT entry_timestamp, job_name, user_name, command_type, user_profile, previous_totp_key_exists, totp_key_exists,
744 previous_authentication_methods, authentication_methods, maximum_signon_attempts
745 FROM TABLE (SYSTOOLS.AUDIT_JOURNAL_CP (STARTING_RECEIVER_NAME => '*CURCHAIN',
746 STARTING_TIMESTAMP => current date - 0 days)) jrn ;
```

New type: KEY
TOTP & Exit point

ENTRY_TIMESTAMP	JOB_NAME	USER_NAME	COMMAND_TYPE	USER_PROFILE	PREVIOUS_TOTP_KEY_EXISTS	TOTP_KEY_EXISTS	PREVIOUS_AUTHENTICATION_METHODS	AUTHENTICATION_METHODS	MAXIMUM_SIGNON_ATTEMPTS
2026-08-21 14:...	QPADEV0005	GM	CRT	GM_TOTP	-	-	-	*REGFAC	*SYSVAL
2026-08-21 14:...	QZDASOINIT	GM_TOTP	KEY	GM_TOTP	NO	YES	-	-	-
2026-08-21 14:...	QPADEV0005	GM	CHG	GM_TOTP	-	-	*REGFAC	*REGFAC *TOTP	-
2026-08-21 14:...	QPADEV0005	GM	CHG	GM_TOTP	-	-	-	-	3

QAUDJRN NetServer Authentication Entries (Unknown User)

Previously, if a user that didn't exist on IBM i tried to connect to NetServer, this was the only way you could tell. It was not logged as a VP entry in the Audit Journal



IBM Navigator for i

Dashboard

Home

Work Management

Configuration and Ser

System

Monitors

My Work

Network

Security

IBM i NetServer Status

IBM i Support for Windows Network Neighborhood

Started: 15/05/2025, 16:30:15 BST

Status since: 15/05/2025, 16:30:15 BST

File opens: 0

Print jobs queued: 0

Sessions started: 0

Sessions disconnected automatically: 0

Sessions ended: 0

Unknown user attempts: 9

Password violations: 0

Average response time: 0 milliseconds

Bytes sent: 5 kilobytes

Bytes received: 9 kilobytes

Refresh Now

Reset Status

VP = Network activity (requires *NETFAIL/*NETCMN)

```
735 -- using QAUDJRN, check for signon violations (NetServer)
736 SELECT entry_timestamp, job_name, job_user, program_name, remote_address, AUDIT_USER_NAME, computer_name,
737 ENTRY_TYPE_DETAIL, share_authorization_list, share_action, permissions, share_name, path_name, jrn.*
738 FROM TABLE (SYSTOOLS.AUDIT_JOURNAL_VP (STARTING_RECEIVER_NAME => '*CURCHAIN',
739 STARTING_TIMESTAMP => current date - 0 days)) jrn
740 where entry type in ('P', 'D', 'A', 'U');
```

New type : U
Invalid User

ENTRY_TIMESTAMP	JOB_NAME	JOB_USER	PROGRAM_NAME	REMOTE_ADDRESS	AUDIT_USER_NAME	COMPUTER_NAME	ENTRY_TYPE_DETAIL
2026-08-21 14:...	QZLSSERVER	QUSER_NC	QZLSSERVER	10.24...	GM	::ffff:10.2...	Password error
2026-08-21 15:...	QZLSSERVER	QUSER_NC	QZLSSERVER	10.24...	GM	::ffff:10.2...	Password error
2026-08-21 15:...	QZLSSERVER	QUSER_NC	QLESPI	-	BRAD	::ffff:10.2...	Unknown user attempt to connect or guest...
2026-08-21 15:...	QZLSSERVER	QUSER_NC	QZLSSERVER	10.24...	GM_TOTP	::ffff:10.2...	Password error
2026-08-21 15:...	QZLSSERVER	QUSER_NC	QZLSSERVER	10.24...	GM_TOTP	::ffff:10.2...	Password error
2026-08-21 15:...	QZLSSERVER	QUSER_NC	QZLSSERVER	10.24...	GM_TOTP	::ffff:10.2...	Password error
2026-08-21 15:...	QZLSSERVER	QUSER_NC	QZLSSERVER	10.24...	GM_TOTP	::ffff:10.2...	NetServer user disabled

QAUDJRN NetServer Entries

Case: I need to reduce the NetServer exposure, and therefore audit activities.

- **Prior to 7.6:** There is no direct way to audit access to shares
- **From 7.6 :** Add * NETSMBSVR to QAUDLVL and check VP entries

```
752 -- using QAUDJRN, check NetServer activities
753 SELECT entry_timestamp, job_name, job_user, program_name, remote_address, AUDIT_USER_NAME, computer_name,
754 ENTRY_TYPE_DETAIL, share_authorization_list, share_action, permissions, share_name, path_name
755 FROM TABLE (SYSTOOLS.AUDIT_JOURNAL_VP (STARTING_RECEIVER_NAME => '*CURCHAIN',
756 STARTING_TIMESTAMP => current_date - 0 days)) jrn
757 where entry_type in ('C', 'E', 'S');
```

New types : C, E, S

ENTRY_TIMESTAMP	JOB_NAME	JOB_USER	PROGRAM_NAME	REMOTE_ADDRESS	AUDIT_USER_NAME	COMPUTER_NAME	ENTRY_TYPE_DETAIL	SHARE_AUTHORIZATION_LIST	SHARE_ACTION	PERMISSIONS	SHARE_NAME	PATH_NAME
2026-08-21 14:...	QPADEV0005	GM	TZLSFSHR	10.24...	GM	-	Share modified	-	ADD	*RW	ERPFSDOC	/erpifsdoc
2026-08-21 14:...	QPADEV0005	GM	TZLSFSHR	10.24...	GM	-	Share modified	-	ADD	*R	ROOT	/
2026-08-21 14:...	QPADEV0005	GM	TZLSFSHR	10.24...	GM	-	Share modified	-	CHANGE	*RW	ROOT	/
2026-08-21 14:...	QZLSSERVER	QUSER_NC	QLESPI	-	GM	::ffff:10.24...	Server or share connection established	-	-	*RW	*SERVER	-
2026-08-21 14:...	QZLSSERVER	QUSER_NC	QLESPI	-	GM	::ffff:10.24...	Server or share connection established	-	-	*RW	ERPFSDOC	-
2026-08-21 15:...	QZLSSERVER	QUSER_NC	QLESPI	-	GM	::ffff:10.24...	Server or share connection ended	-	-	-	ERPFSDOC	-
2026-08-21 15:...	QZLSSERVER	QUSER_NC	QLESPI	-	GM	::ffff:10.24...	Server or share connection ended	-	-	-	*SERVER	-
2026-08-21 15:...	QZLSSERVER	QUSER_NC	QLESPI	-	GM	::ffff:10.24...	Server or share connection established	-	-	*RW	*SERVER	-
2026-08-21 15:...	QZLSSERVER	QUSER_NC	QLESPI	-	GM	::ffff:10.24...	Server or share connection established	-	-	*RW	ERPFSDOC	-
2026-08-21 15:...	QZLSSERVER	QUSER_NC	QLESPI	-	GM	::ffff:10.24...	Server or share connection ended	-	-	-	ERPFSDOC	-
2026-08-21 15:...	QZLSSERVER	QUSER_NC	QLESPI	-	GM	::ffff:10.24...	Server or share connection ended	-	-	-	*SERVER	-

CVE - Common Vulnerabilities and Exposures

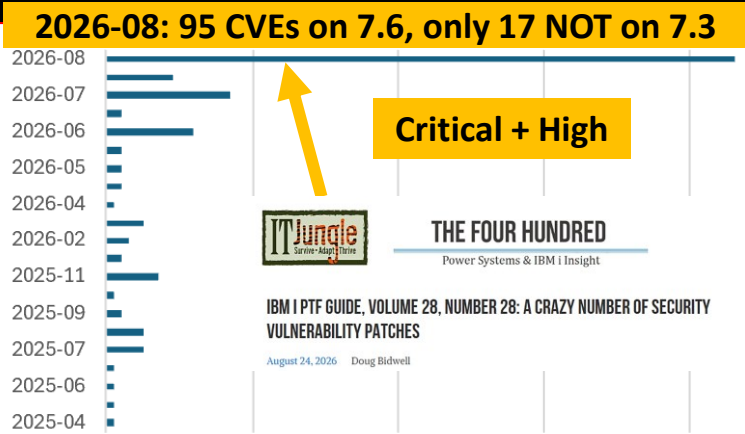
- **Prior to 7.6 TR2 & 7.5 TR8** : No automatic way to query CVEs – reading security alerts and website
- **From 7.6 TR2 & 7.5 TR8** : From the partition access directly the CVE database for the selected version and present the extracted information from the IBM pages in a readable manner

SELECT * FROM TABLE (SYSTOOLS.CVE_INFO())

VERSION	FIRST_PUBLISHED	LAST_PUBLISHED	PERIOD_YEARS	CRIT_COUNT	HIGH_COUNT	MEDIUM_COUNT	LOW_COUNT	CRIT_AVERAGE	HIGH_AVERAGE	MEDIUM_AVERAGE	LOW_AVERAGE
7.3	2018-08-08	2026-08-21	8.03	51	307	401	122	6.35	38.23	49.93	15.19
7.4	2019-12-19	2026-08-21	6.67	24	248	272	85	3.59	37.18	40.77	12.74
7.5	2022-05-23	2026-08-21	4.24	21	210	202	46	4.95	49.52	47.64	10.84
7.6	2025-04-17	2026-08-21	1.34	15	152	115	24	11.19	113.43	85.82	17.91

```
382 -- check the ones that adress a specific category of vuln
383 SELECT * FROM TABLE (SYSTOOLS.CVE_INFO(7.6))
384 WHERE lower(description) like '%privilege escalation%';
385 SELECT * FROM TABLE (SYSTOOLS.CVE_INFO(7.6))
386 WHERE lower(description) like '%unqualified library call%';
387 SELECT * FROM TABLE (SYSTOOLS.CVE_INFO(7.6))
388 WHERE lower(description) like '%openssh%';
```

CVE_ID	SCORE	PUBLISH_DATE	TITLE	IBM_SUPPORT_URL	SUMMARY
CVE-2026-18509	High	2026-08-12	IBM i is Affected By A Privilege Escalation Vulnerability [CVE-2026-18509]	https://www.ibm.com/s...	IBM i is vulnerable to
CVE-2026-18713	High	2026-08-11	IBM i is Affected By Multiple Vulnerabilities in Navigator for i	https://www.ibm.com/s...	IBM i is vulnerable to
CVE-2026-18683	High	2026-08-11	IBM i is Affected By Multiple Vulnerabilities in Navigator for i	https://www.ibm.com/s...	IBM i is vulnerable to
CVE-2026-18669	High	2026-08-11	IBM i is Affected By A Privilege Escalation Vulnerability [CVE-2026-18669]	https://www.ibm.com/s...	IBM i is vulnerable to
CVE-2026-2311	Medium	2026-04-15	IBM i is affected by a privilege escalation vulnerability in Web Administration GUI [CVE-2026-2311]	https://www.ibm.com/s...	Web Administration GUI
CVE-2025-36367	High	2025-10-31	IBM i is affected by a privilege escalation in IBM i SQL services [CVE-2025-36367]	https://www.ibm.com/s...	IBM i is vulnerable to
CVE-2025-33109	High	2025-07-24	IBM i is vulnerable to a privilege escalation due to an invalid database authority check [CVE-2025-...	https://www.ibm.com/s...	IBM i contains a privil
CVE-2025-33103	High	2025-05-17	IBM i is vulnerable to a privilege escalation vulnerability in IBM TCP/IP Connectivity Utilities fo...	https://www.ibm.com/s...	IBM i contains a privil
CVE-2025-2947	High	2025-04-17	IBM i is vulnerable to a privilege escalation due to incorrect profile swapping in an OS command [C...	https://www.ibm.com/s...	IBM i contains a privil



THIS IS A POSITIVE THING



CVE - Common Vulnerabilities and Exposures (Customisation)

select routine_definition from qsys2.sysroutines
where specific_schema = 'SYSTOOLS' and routine_name = 'CVE_INFO'

```
BEGIN
RETURN SELECT
CVE_ID , CVE_BASE_SCORE ,
DATE ( TIMESTAMP_FORMAT ( CHAR ( CVE_PUBLISH_DATE ) , 'YYYY-MM-DD' ) ) ,
CVE_TITLE , CVE_URL , CVE_SUMMARY ,
CVE_DESCRIPTION , CVE_LICPGM , CVE_PRODUCT ,
IBMI_RELEASE ,
DATE ( TIMESTAMP_FORMAT ( CHAR ( CVE_MODIFICATION_DATE ) , 'YYYY-MM-DD' ) ) ,
CVE_X_FORCE_URL , CVE_FIELD_VULNERABILITY_DETAILS ,
CVE_AFFECTED_PRODUCTS
FROM JSON_TABLE (
SYSTOOLS_HTTPGETCLOB (
'https://www.ibm.com/support/pages/securityapp/api/search?q=IBM%20i' , '' ) ,
'lax $.results[*]'
)
COLUMNS (
CVE_ID VARCHAR ( 20 ) CCSID 1208 PATH '$.field_cve_id' ,
CVE_BASE_SCORE VARCHAR ( 20 ) CCSID 1208 PATH '$.field_cvss_base_score' ,
CVE_PUBLISH_DATE VARCHAR ( 200 ) CCSID 1208 PATH '$.field_pub_date' ,
CVE_TITLE VARCHAR ( 2000 ) CCSID 1208 PATH '$.title' ,
CVE_URL VARCHAR ( 200 ) CCSID 1208 PATH '$.field_published_url' ,
CVE_SUMMARY VARCHAR ( 2000 ) CCSID 1208 PATH '$.field_summary' ,
CVE_DESCRIPTION VARCHAR ( 5000 ) CCSID 1208 PATH '$.field_cvss_desc' ,
CVE_LICPGM VARCHAR ( 7 ) CCSID 1208 PATH '$.field_offering_pid_number' ,
CVE_PRODUCT VARCHAR ( 50 ) CCSID 1208 PATH '$.field_product' ,
CVE_AFFECTED_PRODUCTS VARCHAR ( 7000 ) CCSID 1208 PATH '$.field_affected_products' ,
CVE_MODIFICATION_DATE VARCHAR ( 200 ) CCSID 1208 PATH '$.modified_date' ,
CVE_X_FORCE_URL VARCHAR ( 100 ) CCSID 1208 PATH '$.fi
CVE_FIELD_VULNERABILITY_DETAILS CLOB ( 102400 ) CCSID
'$.field_vulnerability_details'
)
)
WHERE CVE_AFFECTED_PRODUCTS LIKE '%' CONCAT IBMI_RELE
END
GM
```

Official IBM API page that lists
all the Security bulletins related to IBM

« Readable » page

<https://www.ibm.com/support/pages/bulletin/search/?q=IBM%20i>

- Gather the associated PTFs
- Check if the PTF has already been applied



CVE_ID	SCORE	TITLE	PUBLISH_DATE	PTF_NUMBER	PTF_LOADED_STATUS
CVE-2026-29063	Critical	IBM i is Affected by Use of Hard-coded Cryptographic Key, Cross-site Scripting, and Protot...	2026-04-02	SJ09013	PERMANENTLY APPLIED
CVE-2026-31789	Critical	IBM i is Affected By NULL Pointer Dereference, Use After Free, and Out-of-Bounds Write Vuln...	2026-06-08	SJ09833	PERMANENTLY APPLIED
CVE-2026-34182	Critical	IBM i is Affected By Multiple Vulnerabilities in OpenSSL	2026-07-14	SJ10651	APPLIED
CVE-2026-8633	Critical	IBM i is Affected By Denial of Service, HTTP Request Smuggling, and Remote Code Execution ...	2026-06-22	SJ10122	APPLIED
CVE-2026-16860	Critical	IBM i is Affected By Remote Code Execution Vulnerability [CVE-2026-16860]	2026-08-11	SJ10879	-
CVE-2026-17083	Critical	IBM i is Affected By Multiple Vulnerabilities in the Debug Server	2026-08-11	SJ10899	-
CVE-2026-17218	Critical	IBM i is Affected By Remote Code Execution Vulnerability in Line Printer Daemon [CVE-2026-...	2026-08-11	SJ10872	-
CVE-2026-17276	Critical	IBM i is Affected By Multiple Vulnerabilities in Navigator for i	2026-08-11	SJ10887	-

Reading Database Changes at Record Level from Database Journal

- **Prior to 7.6 TR2 & 7.5 TR8** : DSPJRN, RCVJRNE, RTVJRNE, QjoRetrieveJournalEntries, QSYS2.DISPLAY_JOURNAL
- **From 7.6 TR2 & 7.5 TR8** : CREATE_DATA_JOURNAL_READER a smart agent used for presenting and filtering columns - No more `interpret(SUBSTR(entry_data ,1, 20) as char(20))`

```
369 -- create data-journal reader table function for all the registered sensitive files
370 select tb.*;
371 QSYS2.CREATE_DATA_JOURNAL_READER(LIBRARY_NAME => system_table_schema, FILE_NAME => system_table_name, OUTPUT_LIBRARY => 'RSLAUD') data_journal_reader_created
372 from rslaud.tables_to_audit tb ;
373
```

SYSTEM_TABLE_SCHEMA	SYSTEM_TABLE_NAME	INITIAL_OBJECT_AUDIT	DATA_JOURNAL_READER_CREATED
System	System		
Table	Table		
Schema	Name		
ERPPFILE	GLFCLIE	*ALL	1
ERPPFILE	GLFCUENTA	*ALL	1
ERPPFILE	GLFTFANS	*NONE	1
XKERPDATA	GLFCLIE	*CHANGE	-1

```
381 -- using data-journal reader, check for updates made by a program outside of the ERP application to a sensitive file and a sensitive column
382 SELECT ub.entry_timestamp, ub.user_name, 'UPDATE' operation, ub.clicomp, ub.clinumero, ub.clinombr,
383 ub.clitipo CLITIPO_before, up.clitipo CLITIPO_after, ub.clistat CLISTAT_before, up.clistat CLISTAT_after,
384 ub.job_name, ub.program_library, ub.program_name
385 FROM TABLE (RSLAUD.DISPLAY_JOURNAL_ERPPFILE_GLFCLIE(JOURNAL_ENTRY_TYPES => 'UB',
386 STARTING_RECEIVER_NAME => '*CURCHAIN', STARTING_TIMESTAMP => current_timestamp - 150 minutes)) ub
387 join TABLE (RSLAUD.DISPLAY_JOURNAL_ERPPFILE_GLFCLIE(JOURNAL_ENTRY_TYPES => 'UP',
388 STARTING_RECEIVER_NAME => '*CURCHAIN', STARTING_TIMESTAMP => current_timestamp - 150 minutes)) up
389 on ub.sequence_number+1 = up.sequence_number
390 where ub.program_library not in ('ERPPGM', 'ERPPTF')
391 and not (ub.job_name = 'QZDASOINIT' and ub.remote_address = '123.456.789' and ub.user_name = 'ERPSRVUSER')
392 and (ub.clitipo <> up.clitipo or ub.clistat <> up.clistat);
393
```

ENTRY_TIMESTAMP	USER_NAME	OPERATION	CLICOMP	CLINUMERO	CLINOMBR	CLITIPO_BEFORE	CLITIPO_AFTER	CLISTAT_BEFORE	CLISTAT_AFTER	JOB_NAME	PROGRAM_LIBRARY	PROGRAM_NAME
2026-08-02 15:10...	GM	UPDATE	001	5915000000000001	John Ford (Jr.)	EEEE	EEEE	Y	Y	QZDASOINIT	QSYS	QZDASOINIT
2026-08-02 15:10...	GM	UPDATE	002	4915000000000001	Petros CHRISTOFIDES	EEEE	EEEE	Y	Y	QZDASOINIT	QSYS	QZDASOINIT
2026-08-02 15:10...	GM	UPDATE	001	5915000000000001	John Ford (Jr.)	EEEE	EEEE	Y	Y	QZDASOINIT	QSYS	QZDASOINIT
2026-08-02 15:10...	GM	UPDATE	002	4915000000000001	Petros CHRISTOFIDES	EEEE	EEEE	Y	Y	QZDASOINIT	QSYS	QZDASOINIT

Powerful at filtering and presenting!!!

Filtering at database file field level

Filtering at journal context field level

- Don't forget to :
 - Manage the retention
 - Manage the change in the file structure
 - Don't miss any period of time when scheduled (no *CONTINUE value)

New QIBM_QZLS_NETSVR_SHARE function ID

Case: Give us the ability to manage NetServer File shares, without giving additional privileges

- **Prior to 7.6:** You had to give user(s) *IOSYSCFG special authority to manage file shares
- **From 7.6 :** Add user(s) to QIBM_QZLS_NETSVR_SHARE function without giving them *IOSYSCFG

IBM i NetServer

The IBM i NetServer APIs that retrieve server configuration information require either *IOSYSCFG special authority or QIBM_IOSYSCFG_VIEW function usage authority. Consider the following updates:

- ▶ Creating, modifying, or removing an IBM i NetServer share without *IOSYSCFG special authority now requires ownership of the shared object and QIBM_QZLS_NETSVR_SHARE function usage authority.

New Service tools server configuration entry service

Case: Enable Programmatic administration of (SST/DST) Console LAN Adapter

- **Prior to 7.6:** Manual interactive configuration via SST / DST required
- **From 7.6** : This can be done via an IBM i program or SQL statement
 - Note: *IOSYSCFG and SST Linked profile required

View

```
SELECT * FROM QSYS2.SERVICE_TOOLS_SERVER_CONFIGURATION_ENTRY_INFO;
```

Add

```
CALL QSYS2.ADD_SERVICE_TOOLS_SERVER_CONFIGURATION_ENTRY (  
    PARTITION_UUID => BX'52C417A870DD4487986B33F74CE9FE47',  
    RESOURCE_NAME  => 'STS',  
    IPV4_ADDRESS   => '1.2.35.56',  
    GATEWAY_ADDRESS => '1.2.35.0',  
    SUBNET_MASK    => '255.255.255.0',  
    IPV6_ADDRESS   => '2001:db8:3333:4444:5555:6666:7777:9999');
```

Change

```
CALL QSYS2.CHANGE_SERVICE_TOOLS_SERVER_CONFIGURATION_ENTRY (  
    PARTITION_UUID => BX'52C417A870DD4487986B33F74CE9FE47',  
    IPV4_ADDRESS   => '1.2.37.56',  
    GATEWAY_ADDRESS => '1.2.37.0');
```

Remove

```
CALL QSYS2.REMOVE_SERVICE_TOOLS_SERVER_CONFIGURATION_ENTRY (  
    PARTITION_UUID => BX'52C417A870DD4487986B33F74CE9FE47');
```

Nice little additions

- **From 7.6 TR2 & 7.5 TR8 :**
Scalar function qcmdexc can write the command to the joblog

```
-- proc qcmdexc
begin
declare run_cmd varchar(1000);
set run_cmd = 'CHGOBJAUD OBJ(QSYS2/SEC_INFO) OBJTYPE(*FILE) OBJAUD(*ALL)';
call qsys2.qcmdexc(run_cmd);
call systools.lprintf ('cmd = ' concat run_cmd);
end ;

-- scalar function qcmdexc
create or replace table qtemp.run_cmd as
(select 'CHGOBJAUD OBJ(' concat service_schema_name concat '/' concat system_object_name concat
') OBJTYPE(' concat object_type concat ' ' OBJAUD(*ALL)' run_cmd, 0 run_cmd_status
from rslaud.audit_sql_service_for_v7r6)
with data on replace delete rows ;
update qtemp.run_cmd set run_cmd_status = qcmdexc(run_cmd, 'VERBOSE');

select qsys2.qcmdexc('CHGUSRPRF USRPRF(BRAD) PASSWORD(''strong_and_secret_pwd'')', 'VERBOSE' ) runcmd_status
from sysibm.sysdummy1 ;
```

024228/QUSER_NC/QZDASOINIT Job Log - iug6

Message ID	Message
-	QCMDEXC success: CHGUSRPRF USRPRF(BRAD) PASSWORD('strong_and_secret_pwd')
CPC2205	User profile BRAD changed.
-	QCMDEXC success: CHGOBJAUD OBJ(QSYS2/SEC_INFO) OBJTYPE(*FILE) OBJAUD(*ALL)
CPC2224	Object auditing value changed for SEC_INFO in QSYS2 type *FILE.
CPC2191	Object QCMPO00001 in QTEMP type *PGM deleted.
-	cmd = CHGOBJAUD OBJ(QSYS2/SEC_INFO) OBJTYPE(*FILE) OBJAUD(*ALL)
CPC2224	Object auditing value changed for SEC_INFO in QSYS2 type *FILE.

Automatic clean-up based on retention days

VARIABLE_ SCHEMA	VARIABLE NAME	LONG_COMMENT	VARIABLE_ VALUE
SYSIBMADM	QIBM_SELF_BY_DAYS	SQL ERROR LOGGING FACILITY PRUNING VARIABLE BY DAYS	365
SYSIBMADM	QIBM_SOEDEBUG_BY_DAYS	SQL DIRECTORY PRUNING VARIABLE BY DAYS	90
SYSIBMADM	QIBM SYSIXADV BY DAYS	SYSIXADV PRUNING VARIABLE BY DAYS	365
SYSIBMADM	QIBM_SYSTEM_LIMITS_ASP_BY_DAYS	SYSTEM LIMITS PRUNING VARIABLE FOR ASP BY DAYS	90
SYSIBMADM	QIBM_SYSTEM_LIMITS_JOB_BY_DAYS	SYSTEM LIMITS PRUNING VARIABLE FOR JOB BY DAYS	90
SYSIBMADM	QIBM_SYSTEM_LIMITS_OBJECT_BY_DAYS	SYSTEM LIMITS PRUNING VARIABLE FOR OBJECT BY DAYS	90
SYSIBMADM	QIBM_SYSTEM_LIMITS_SYSTEM_BY_DAYS	SYSTEM LIMITS PRUNING VARIABLE FOR SYSTEM BY DAYS	90

THANK YOU
FOR
YOUR ATTENTION!



Guy Marmorat
gmarmorat@resiliane.com



Steve Bradshaw
steve.bradshaw@rowtonit.com