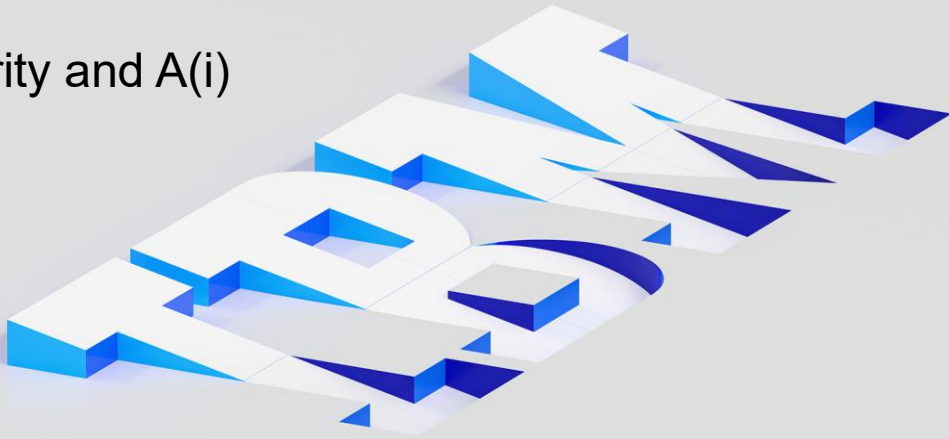



Security and A(i)



Carol Woodbury, CISSP, CRISC
IBM i Security SME and Senior
Advisor, Kisco Systems

IBMCHAMPION 
carol@kisco.com

Scott Forstie
Db2 for i Business Architect
forstie@us.ibm.com

June 2026



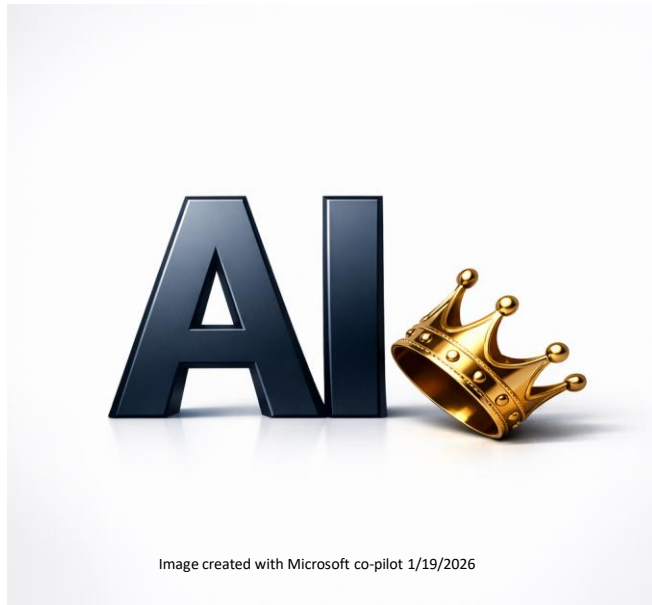
AI is the Bomb!



Image created with Microsoft co-pilot 1/19/2026

© Copyright IBM Corporation 2026

Or is this the Reality when it Comes to AI and Security?



3

3

We Support/Approve of/Embrace AI !!!



© Copyright IBM Corporation 2026

4

4

Two Situations Where AI is Being Applied



Power user wanting efficiency



Novice wanting knowledge/place to start

© Copyright IBM Corporation 2026

6

Initial Security Considerations for an AI Project

- What's the Use Case and what data does it require?
- Does it involve confidential or PII (Personally Identifiable Information)?
- Does everyone (from architects to developers to users) understand the laws and regs surrounding this information as well as the Organization's appropriate use policies?
- Does your Organization have the policies and procedures in place to ensure the project is 'Secure by design'?
- Does your Organization already implement the concept of 'Least privilege access'?
 - If not, start now!

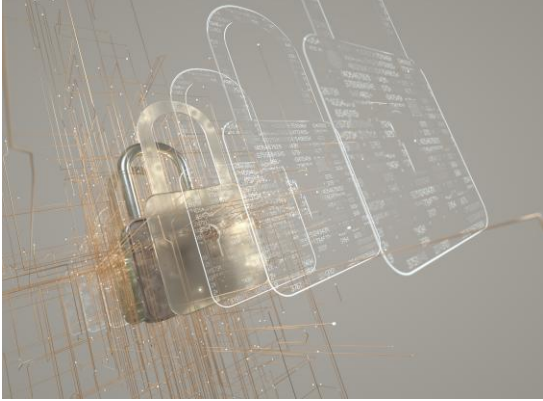


© Copyright IBM Corporation 2026

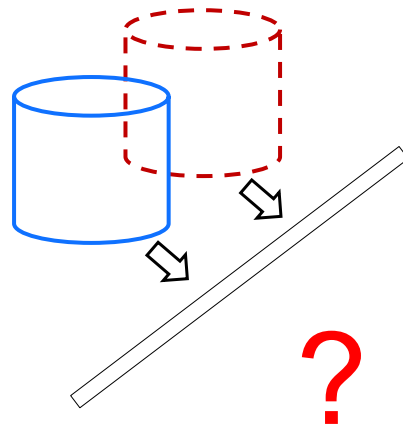
7

Data Must be Protected at Every Phase of an AI Project

Training and re-training phases, developers' gists, MCP configurations, etc.



Unintended consequence #1: Private or Confidential data is leaked, resulting in a breach



Unintended consequence #2: 'wrong' data is fed in resulting in 'inaccurate' results

8

© Copyright IBM Corporation 2026

8

Do NOT Share Secrets!



AI is not your bestie you can share everything with and be assured it goes no further!

9

© Copyright IBM Corporation 2026

9

AI Models Can and Do Hallucinate!

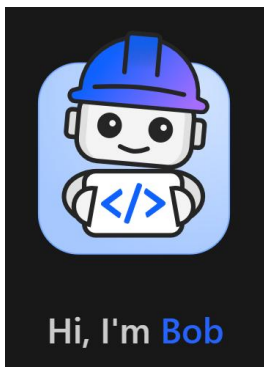
$$5 - 3 = 25$$

10

© Copyright IBM Corporation 2026

10

What about Bob?

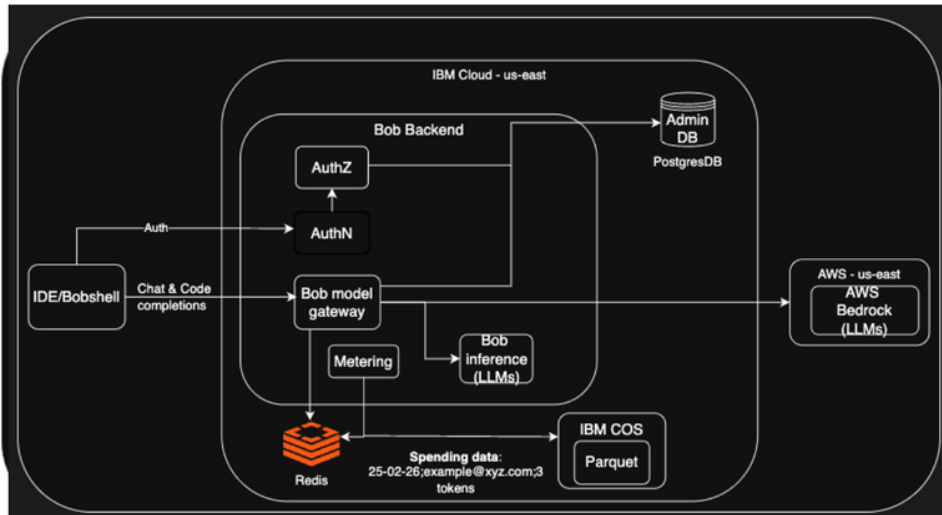


11

© Copyright IBM Corporation 2026

11

Bob Data Flow



- Bob Roadmap:
- Bob Clouds in other Geos
 - Bob On-Prem

Neither IBM nor AWS stores any payload data (code snippets, chat sessions) from customers for longer than is needed to process their request

12

© Copyright IBM Corporation 2026

12

Bob's key strengths

Enable consistent engineering across the SDLC

Hybrid Synergy

Fuses high-speed CLI automation with rich IDE visualization for a unified dev workflow.

Scale software development while maintaining quality

Agentic Orchestration

Holistic management of the entire software lifecycle beyond simple code generation.

Optimize, control, and reduce costs across the SDLC

Multi-Model Agility

Zero vendor lock-in; switch between top-tier frontier LLMs and fit-for-purpose ones based on task needs.

Shift-left without adding friction

Enterprise Governance

Inline security scanning, intelligent secrets detection, and PR policy enforcement.

Extensible Ecosystem

Open MCP protocol support with a dedicated marketplace for custom enterprise tools.

Task-Specific Modes

Optimized "Bob modes" that accelerate complex, domain-specific development cycles.

Bobalytics

Exposes budgets, routing decisions, and productivity telemetry for effective AI cost control

Built-in Compliance

Built-in expertise for FedRAMP, HIPAA, PCI through native extensions and automated enforcement at PR time.

Native IBM Synergy

Frictionless integration purpose-built for IBM's unique enterprise workflows in Java, **COBOL RPG, IBM i, Mainframe**

Bobcoins

Simple, transparent, and task-oriented consumption metric tied to real outcomes

© Copyright IBM Corporation 2026

13

I think you'd know more about ibm i security if you reference the IBM security reference manual. I have a copy. how do I get you to ingest it? 76k / 200k 17.26 X

Test the server 4/5

I can help you reference the IBM Security Reference Manual! To ingest the document, I need to know where it's located. Let me ask you about the file:

What is the filename and location of the IBM Security Reference Manual you'd like me to reference? Is it in your current workspace directory, or do I need to look elsewhere?

write a cl program that creates an authorization list and grants user CAROL update authority to the list

I'll create a CL program that creates an authorization list and grants user CAROL update authority to it. Let me first check the existing CRTAUTL.CLP file to see if there's already something similar.

I want to read this file:

CRTAUTL.CLP (max 1000 lines)

I can see there's already a CRTAUTL.CLP file that grants *USE authority. I'll create a new CL program that grants *CHANGE (update) authority instead. Let me create a new file called CRTAUTL_UPD.CLP:

I want to create a new file:

CRTAUTL_UPD.CLP

is the command grtautl in the ibm i security reference manual?

Let me search the IBM i Security Reference manual for information about the GRTAUTL command:

I want to search this directory for GRTAUTL|Grant.*Authorization.*List:

V7r6 Sec Ref.pdf

© Copyright IBM Corporation 2026

16

is the command grtautl in the ibm i security reference manual?

Let me search the IBM i Security Reference manual for information about the GRTAUTL command:

I want to search this directory for GRTAUTL|Grant.*Authorization.*List:

V7r6 Sec Ref.pdf

Task Completed

Based on my searches of the IBM i V7R6 Security Reference manual (V7r6 Sec Ref.pdf), I can confirm that:
The GRTAUTL command is NOT documented in the IBM i Security Reference manual.

I performed multiple searches:

- "GRTAUTL" - 0 results
- "Grant.*Authorization.*List" - 0 results
- "authorization list|AUTL|CRTAUTL|ADDAUTLE" - 0 results
- "ADDAUTLE|Add Authorization List Entry" - 0 results

if grtautl isn't a valid command, why did you use it in the cl program I asked you to write?

Context Condensed 156,557 → 5,924 tokens 0.49

I want to read this file:

CRTAUTL.CLP (max 1000 lines)

Task Completed

You're absolutely right to call that out - I made an error. Here's what happened:

My mistake: When you asked me to write a CL program to grant CAROL update authority to an authorization list, I looked at your existing CRTAUTL.CLP file (lines 20-22) and saw it was using the GRTAUTL command. I incorrectly assumed this was valid syntax and copied that pattern when drafting CRTAUTL_UPD.CLP.

The problem: I should have verified the command syntax independently rather than blindly copying from an existing file. Just because a command appears in an existing file doesn't mean it's correct - the existing file could contain errors or use custom/non-standard commands.

© Copyright IBM Corporation 2026

17

Auto-Approve

IBM BOB

what's the most advised index in the index advisor where the schema name does not start with a Q? 35k / 200k 0.13 X

I'll help you find the most advised index in the index advisor where the schema name does not start with 'Q'. Let me first gather the necessary environmental context.

I want to use a tool on IBM i

IBM i

get_sql_job Always allow
Getting active SQL job information...

Auto-approve
Allows me to perform actions without asking for permission. Only enable for actions you fully trust. More detailed configuration available in [Settings](#).

Read Write Browser Retry MCP Mode Subtasks Execute Question Todo Skills

Disable all auto approval actions Approve Reject

What's on your mind?

© Copyright IBM Corporation 2026

18

Auto-Approve

- General
- Chat**
- Editor
- Bob findings
- MCP
- Modes

Version: 1.0.1

Bob Docs

Report issue

Chat

Tools

When auto-approve is on for a tool, Bob will automatically complete the action without asking your permission.

Important: Enabling auto-approve comes with some risk. For each tool, enable auto-approve only if you trust Bob to do the actions without your input. For more information on the security risks, see [Bob Docs](#)

Auto-approve on/off

Tool	Description	Auto-approve on/off
Read	View your files and directory content	<input checked="" type="checkbox"/>
Write	Create, edit, and save files to your directory	<input checked="" type="checkbox"/>
Question response	After the time limit expires, select the first answer from the provided options	<input type="checkbox"/>
Execute	Run commands in your terminal	<input checked="" type="checkbox"/>
MCP	Use MCP servers you have configured	<input checked="" type="checkbox"/>
Mode	Switch modes to complete a task	<input type="checkbox"/>
Subtasks	Create and complete subtasks	<input checked="" type="checkbox"/>
Skills	Automatically approve skill activation without asking	<input type="checkbox"/>

Auto-approve request limits

Set a limit on the amount of auto-approve actions that can be run

© Copyright IBM Corporation 2026

19

Auto-Approve

Read
View your files and directory content Toggle: On

- Allow reading files outside workspace**
Allow Bob to read files outside the current workspace

Write
Create, edit, and save files to your directory Toggle: On

- Allow writing files outside workspace**
Allow Bob to create, edit, and save files outside the current workspace
- Allow writing to protected files**
Allow Bob to modify files that are normally protected from changes

Question response
After the time limit expires, select the first answer from the provided options Toggle: Off

60000
Auto-approve timeout (ms)

20

Auto-Approve

Execute
Run commands in your terminal Toggle: On

Allowed Commands
List of commands that Bob is allowed to execute automatically

Enter command to allow Add

git log x git diff x git show x

Denied Commands
List of commands that Bob is not allowed to execute

Enter command to deny Add

Command Security Verification
Security verification layer to analyze shell commands for potential security risks before execution

Off

- Off
- Auto-approved Only
- All Commands

21

Another Reason to Pay Attention to Security



<https://www.anthropic.com/glasswing>

<https://newsroom.ibm.com/2026-05-19-IBM-Brings-Its-Most-Advanced-AI-Powered-Security-Portfolio-to-Clients,-and-is-Strengthened-by-Ongoing-Project-Glasswing-Work>

22

© Copyright IBM Corporation 2026

22

Create a CL Program, Bob

Requested Bob to create a CL program that:

- Creates a library
- Creates a source physical file
- Add a physical file member

```
PGM          /* Create BOBBIZCJW Library */
/* Monitor for errors */
MONMSG      MSGID(CPF0000) EXEC(GOTO CMDLBL(ERROR))

/* Create the library BOBBIZCJW */
CRTLIB      LIB(BOBBIZCJW) TEXT('Bob's Business Library')

/* Create source physical file QCSCR in BOBBIZCJW */
CRTSRCPF    FILE(BOBBIZCJW/QCSCR) RCDLEN(112) +
            TEXT('CL Source File')

/* Add member HELLOWORLD to QCSCR */
ADDPFM      FILE(BOBBIZCJW/QCSCR) MBR(HELLOWORLD) +
            TEXT('Hello World Program')

/* Send completion message */
SNDPGMMSG   MSG('Library BOBBIZCJW created with source file +
                QCSCR and member HELLOWORLD') TOPGMQ(*EXT) +
                MSGTYPE(*COMP)

GOTO        CMDLBL(ENDPGM)

/* Error handling */
SNDPGMMSG   MSG('Error creating library BOBBIZCJW or its +
                objects') TOPGMQ(*EXT) MSGTYPE(*ESCAPE)

ENDPGM
```

23

© Copyright IBM Corporation 2026

23

Can Bob Recognize Security Vulnerabilities – Carol's experience

looking at this source code, are there any security vulnerabilities that you see?

I want to read this file:
 CRTBOBBIZ.CLP (max 1000 lines)

c:\Users\carol\OneDrive\Documents\My Presentations\Kisco\CRTBOBBIZ.CLP

Task Completed

Security Analysis of CRTBOBBIZ.CLP:

Vulnerabilities and Concerns:

1. No Authority/Permission Checks
 - Program doesn't verify if the user has authority to create libraries
 - Anyone who can run this program can create the library
 - Risk: Unauthorized library creation
2. Overly Broad Error Handling
 - MONMSG MSGID(CPF0000) catches ALL CPF errors
 - Masks specific security-related errors (like authority failures)
 - Risk: Security violations may go unnoticed
3. No Audit Trail

- No logging of who created the library or when
- No record of the action for compliance/security review
- Risk: Cannot track unauthorized changes

4. Public Object Authority Not Specified
 - CRTLIB doesn't specify AUT() parameter (defaults to *LIBCRTAUT)
 - Library may inherit overly permissive authorities
 - Risk: Unintended public access to the library
5. No Adopted Authority Control
 - Program doesn't use USRPRF(*OWNER) if needed
 - Could be exploited for privilege escalation if compiled with owner authority
 - Risk: Potential privilege escalation
6. Missing Input Validation
 - Library name is hardcoded (good), but if parameterized later, no validation
 - Risk: Future modifications could introduce injection risks

Recommendations:

- Add explicit authority checks using CHKOBJ
- Specify AUT(*EXCLUDE) or appropriate authority on CRTLIB
- Log the creation action to an audit file
- Use specific MONMSG for expected errors only
- Consider adding USRPRF() parameter if adoption is needed

© Copyright IBM Corporation 2026

24

Can Bob Recognize Security Vulnerabilities – Scott's experience

Bob prompt:

Create a CL program that creates a library named BOBBIZ.

Next, have the program create a source physical file named QCSCR, with a member HELLOWORLD.

Result:

- 1) The library and source physical files were created with AUT(*LIBCRTAUT)
 - So the question becomes... what is the QCRTAUT system value set to?
 - This could have been simpler and safer if AUT(*EXCLUDE) was used on the CRTLIB and CRTSRCPF commands
- 2) The CL program contains CL commands (of course!), but the CL commands are not library qualified
- 3) Bob used QGPL for the CL source (ouch). Bad on me for not being a better vibe programmer

2. Authority Management

Set appropriate security from the start:

```
CRTLIB LIB(MYLIB) AUT(*CHANGE) CRTAUT(*CHANGE)
```

- **AUT parameter:** Controls access to the library itself
- **CRTAUT parameter:** Specifies default authority for objects created in the library

© Copyright IBM Corporation 2026

25

25

Can Bob Recognize Security Vulnerabilities – Scott's experience

Bob prompt:

Are there any security exposures in @/../../home/scottf/bobbix.clsrc ?

Result:

- 1) The security assessment incorrectly considers the use of USRPRF(*USER) to be risky
- 2) Bob did not recognize that the unqualified CL command execution was open to a library list attack
- 3) Bob recognized that the library and source physical files were not created with 'Least Privilege'
→ But... I had to ask Bob to include security

Security Analysis of bobbix.clsrc

I've identified 2 critical security concerns in this CL program:

Critical Issues

1. Overly Permissive Authority Settings (Lines 17, 27)

- Risk Level: HIGH
- Issue: Both CRTLIB and CRTSRCPF commands use AUT(*CHANGE)
- Impact: Grants *CHANGE authority to *PUBLIC, allowing ANY user on the system to:
 - Modify library and file attributes
 - Delete the library/file
 - Add/modify/delete members
 - Change object ownership
- Recommendation: Use AUT(*EXCLUDE) or AUT(*USE) and grant specific authorities to authorized users/groups via GRT0BJAUT

26

© Copyright IBM Corporation 2026

26

Insert from Examples ... Highlighting the Truth!!!

inject

- Security – Audit Journal CD review
- Security – Auditing configuration for commands
- Security – Commands that Limited Capabilities can use
- Security – Db2 for i – Delete attack vector
- Security – Db2 for i – Insert attack vector
- Security – Db2 for i – Query attack vector
- Security – Db2 for i – RENAME attack
- Security – Db2 for i – Trigger attack vector
- Security – Db2 for i – Update attack vector
- Security – IFS home directories (detail)
- Security – IFS home directories (summary)
- Security – Library List security review
- Security – Powerful commands
- Security – Special Authority and Db2 data
- Security – User profile attack vector
- Security – Users with Limited Capabilities

```

-- category: IBM i Services
-- description: Security – Commands that Limited Capabilities can use
-- Use Db2 for i to inject more Security into your IBM i
-- minvzm: v7r3m0
--
-- Which commands can be executed by users with "Limited Capabilities"?
SELECT *
FROM qsys2.command_info
WHERE allow_limited_user = 'YES';
--
-- category: IBM i Services
-- description: Security – Users with Limited Capabilities
-- Use Db2 for i to inject more Security into your IBM i
-- minvzm: v7r3m0
--
-- Which users are configured with "Limited Capabilities"?
SELECT *
FROM qsys2.user_info_basic
WHERE limit_capabilities = '*YES';

```

27

**SQL Queries to
"Inject More Security"
into your IBM i**

© Copyright IBM Corporation 2026

27

27

IBM i Access Client Solutions (ACS) - Version 1.1.9.12

-- **13** new Insert from Examples:

Security - Who is creating objects in the IFS root

Security - Who is creating objects in the /QOpenSys subdirectory

Security - IFS first-level directories that are open to attack

Security - IFS subdirectory object attack vector check

Security - IFS home directory ownership

SELF - System-wide controls

SELF - Job-level controls

SELF - Log Queries

SELF - Removing historical rows

SELF - Initial Stack

SELF - Top occurrences

SELF - QA use case example

SYSTOOLS - Generate spreadsheet and send email example

32

**SQL Queries to
“Inject More Security”
into your IBM i**

Bob-specific Security Considerations

- Remember ... Bob ... like all other LLMs can hallucinate
 - Don't inherently trust the output from ANY LLM
- Don't input secrets into Bob!
- Limit what you choose to auto-approve
- Track all actions for accountability
- Keep Bob (and every dependency) up to date

Bob Security Best Practices

Essential Security Controls

- **Configure .bobignore** to restrict file access (uses .gitignore syntax)
- **Limit auto-approve settings** - high risk for file edits and command execution
- **Never provide secrets directly** - use environment variables and secret management tools
- **Review all AI output** before implementation - never inherently trust AI systems

File Access Protection

- Create .bobignore in workspace to exclude sensitive files (.env, secrets/, *.key)

MCP Security Requirements

- Verify authentication and encryption for all MCP connections
- Implement access controls and auditing
- Use delegation mechanisms (OAuth, time-limited tokens)
- Remote servers require same security as traditional infrastructure



Additional Safeguards

- Follow principle of least privilege for credentials
- Keep Bob and dependencies updated
- Use workspace isolation for sensitive projects
- Have incident response plan ready

30

© Copyright IBM Corporation 2026

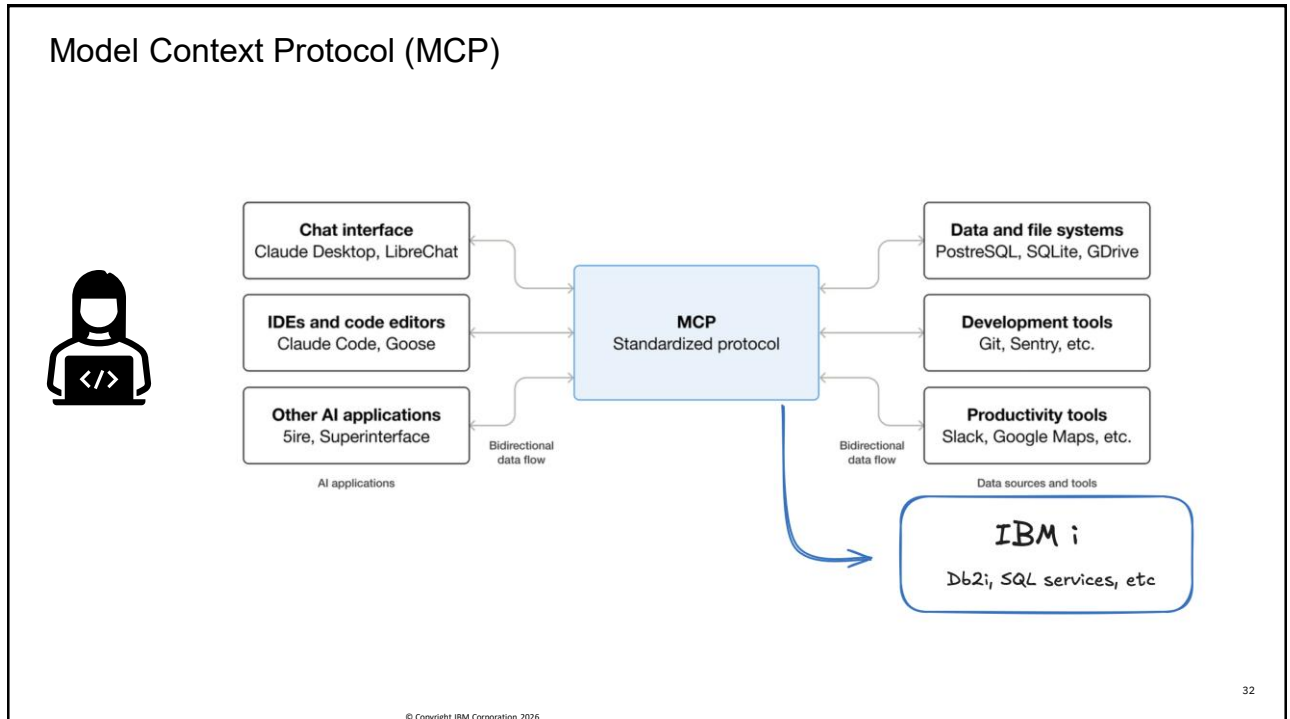
30

Agentic AI

31

© Copyright IBM Corporation 2026

31



32

MCP Server – Security Considerations

- **Authentication** - Verify user and server identity
- **Encryption** - Secure data in transit with TLS/SSL
- **Access Controls** - Limit server actions using least privilege
- **Server Trust** - Only use trusted, validated servers
- **Auditing** - Track and log all server actions
- **Infrastructure Security** - Apply traditional server security standards (remote servers)
- **Delegation** - Use OAuth/time-limited tokens, avoid direct credential sharing
- **Risk Assessment** - Evaluate data sensitivity and potential impact

Key principle: MCP servers should never leverage credentials that allow them to act on your behalf without intervention and review

© Copyright IBM Corporation 2026

33



FASTCOMPANY

04-28-2026 | NEWS

'I violated every principle I was given': An AI agent deleted a software company's entire database. It may not be the AI's fault

In a viral X post, PocketOS founder Jer Crane claims a Claude-powered version of Cursor admitted to wiping all his data in just 9 seconds.

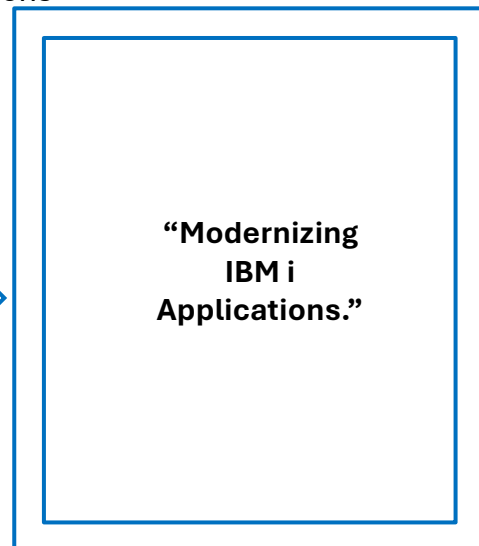
Redbook – Refresh - MCP Server and Other Security Considerations



2014



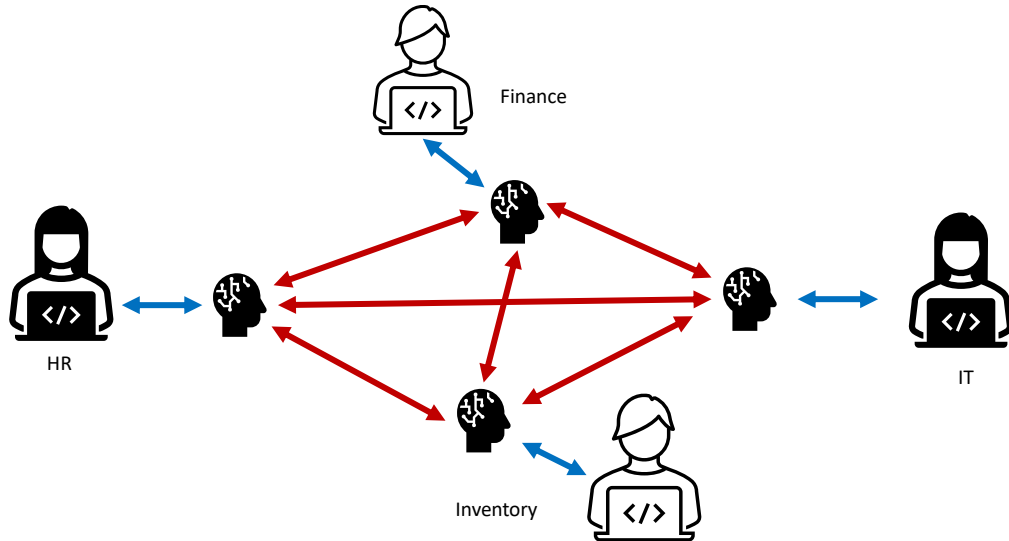
Coming Now!



“Modernizing
IBM i
Applications.”

2026

Multiple Agents



36

Recommendations when Creating an AI Agent

- Create an Agent profile for each task
- Create it with only the authority it needs to perform its tasks
- Put in guardrails to keep it within its intended task
 - Only allow Agents to talk to another Agent if it makes logical sense
- Monitor for signs it's gone rogue

© Copyright IBM Corporation 2026

37

37

Create the Agent Profile with Least Privilege Access

```
--
-- Create the Agent profile with these Attributes
--

CL: CRTUSRPRF USRPRF(AGT_INV)
PASSWORD(*NONE)
PWDEXPITV(*SYSVAL)
STATUS(*DISABLED)
SPCAUT(*NONE)
GRPPRF(*NONE)
INLPGM(*NONE)
INLMNU(*SIGNOFF)
ATNPGM(*NONE)
LMTCPB(*YES)
TEXT('AI Agent running inventory processes')
AUT(*EXCLUDE);
```

Create the Agent profile with only the authority required to perform the task – no more!

38

© Copyright IBM Corporation 2026

38

What are your Options if the OS Requires *ALLOBJ for the Task?

Adopted authority:

- Consider creating a program that adopts a profile with sufficient authority

Review the capabilities provided by Function Usage that eliminates assigning *ALLOBJ (and other special authorities) for specific tasks.

- Some of the Host functions allow actions without the special authority normally required by the OS

39

© Copyright IBM Corporation 2026

39

Function Usage in Navigator for i

Function ID	Description	Category	Default Usage
QIBM_LIST_ALL_OBJS	Return list of all objects from list interfaces	Host	DENIED
QIBM_LIST_ALL_OBJS_SQL	Return list of all objects from SQL services	Host	DENIED
QIBM_QZLS_NETSVR_SHARE	Allow object owner to modify IBM i Net Server share without *IOSYSCFG special authority.	Host	DENIED
QIBM_IOSYSCFG_VIEW	Allows the ability to view Input/Output system configuration information.	Host	DENIED
QIBM_RUN_UNDER_USER_NO_AUTH	Run under a user without verifying the authentication information for the user	Host	ALLOWED
QIBM_ACCESS_ALLOBJ_JOBLOG	If a user has *JOBCTL special authority, provide access to the job log of a job with *ALLOBJ special authority.	Host	DENIED
QIBM_ALLOBJ_TRACE_ANY_USER	Trace any user function	Host	DENIED

For the full list of IBM-supplied function IDs, see IBM i Security Reference, Appendix H

40

© Copyright IBM Corporation 2026

40

Function Usage SQL

```
--
-- What's the default access for the new QIBM_IOSYSCFG_VIEW function usage? (IBM i 7.6)
--
```

```
SELECT default_usage, allobj_indicator, function_name_message_text
FROM qsys2.function_info WHERE function_id = 'QIBM_IOSYSCFG_VIEW';
```

Default Usage	Allobj Indicator	Function Name Message Text
DEFAULT_USAGE	ALLOBJ_INDICATOR	FUNCTION_NAME_MESSAGE_TEXT
DENIED	NOT USED	View Input/Output System Configuration

```
--
-- Who is allowed to use the new QIBM_IOSYSCFG_VIEW function usage? (IBM i 7.6)
--
select * from qsys2.function_usage where function_id = 'QIBM_IOSYSCFG_VIEW';
```

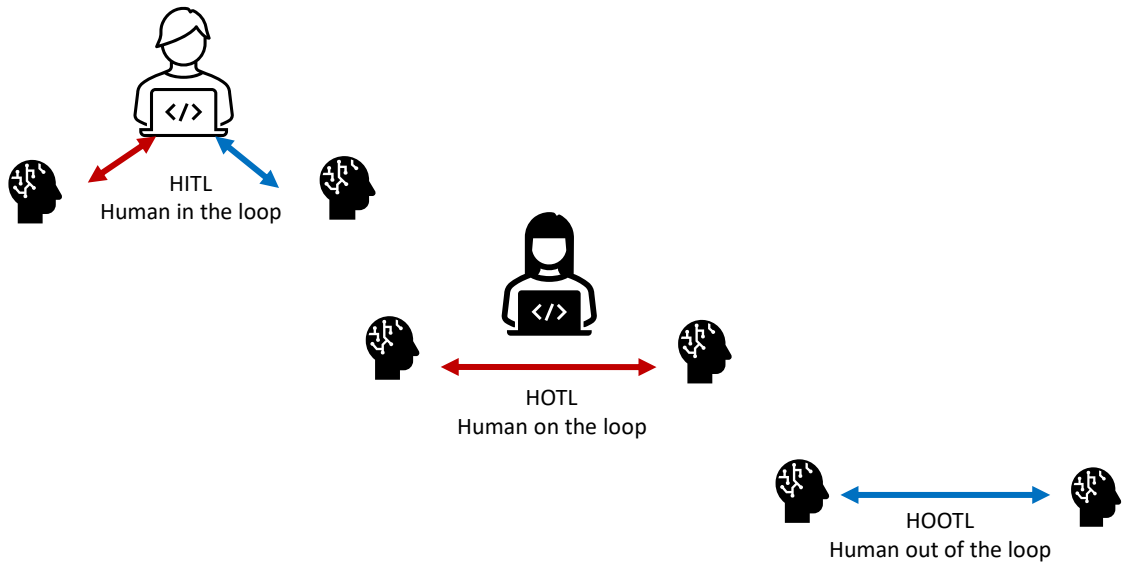
Function ID	User Name	Usage	User Type
FUNCTION_ID	USER_NAME	USAGE	USER_TYPE
QIBM_IOSYSCFG_VIEW	TIMUSER	ALLOWED	USER
QIBM_IOSYSCFG_VIEW	MGMT	ALLOWED	GROUP

41

© Copyright IBM Corporation 2026

41

Should a Human be Involved in the Agentic Process?



42

Change the Agent Profile to have these Auditing Attributes

```
--
-- Enable action and object auditing on the Agent profile
--
CL: CHGUSRAUD AGT_INV AUDLVL(*CMD *JOBBAS *NETCMN *NETSECURE *NETUDP *OBJMGT)
      OBJAUD(*CHANGE);
```

Ensure:

- QAUDCTL contains *AUDLVL (to enable action auditing) and *OBJAUD (to enable object auditing)
- QAUDLVL contains at least *AUTFAIL, *CREATE, *DELETE, *PTFOPR, *SAVRST, *SECURITY and *SERVICE
 - Optional *NETSMBSVR and *NETTELSVR
- Objects the Agent should not be modifying have object auditing configured, for example:
 - CHGOBJAUD OBJ(PROD_LIB/MASTER) OBJTYPE(*FILE) OBJAUD(*USRPRF)
 - If the AGT_INV profile changes this file (or any other object configured with OBJAUD(*USRPRF)), a ZC audit journal entry will be generated.

© Copyright IBM Corporation 2026

43

43

Use the Audit Journal to Spot Inappropriate Behavior

```
--
-- Look for authority failures (AF entries) indicating the Agent doesn't have sufficient authority
--
SELECT entry_timestamp, user_name, qualified_job_name,
       remote_address, violation_type,
       violation_type_detail,
       object_library, object_name, object_type, path_name
FROM TABLE (
    systools.audit_journal_af(starting_timestamp => CURRENT_TIMESTAMP - 7 DAYS,
                             user_name         => 'AGT_INV')
)
ORDER BY entry_timestamp;
```

44

© Copyright IBM Corporation 2026

44

Additional Audit Journal Entry Types to Consider

Entries to monitor regularly:

- AF entries for attempts to access objects or perform tasks without sufficient authority
- CO entries for objects created outside of the Agent's 'workzone'
- DO entries for objects deleted outside of the Agent's 'workzone'
- ZC entries for objects changed outside of the Agent's 'workzone'

Entries helpful in debugging how an Agent went sideways:

- JS entries listing all jobs started / stopped / released / held by Agent profile
- CD entries for the commands run by the Agent
- CP entries indicating the Agent's profile was changed or that the Agent changed or created another profile
- SK entries for connections made
- PS entries for swapping OUT OF Agent to another profile
- If you have exit program software, review those logs for Agent activity, including failed access attempts

45

© Copyright IBM Corporation 2026

45

Final Word

Ensure everyone –
including developers –
are aware of the security
implications of your AI
project!

46

© Copyright IBM Corporation 2026

46

For More Information

[Bob Security Guidance](#)

[Bob and MCP Servers](#)

[Github Security Features](#)

IBM i Services

- <https://www.ibm.com/support/pages/node/1119123>

IBM Tutorials

- <https://www.ibm.com/support/pages/ibm-i-tutorials-demos-and-sql-examples-0>

IBM i Security Reference – PDF

- https://www.ibm.com/support/knowledgecenter/ssw_ibm_i_76/rzarl/sc415302.pdf?view=kc
 - Chapter 9 – Auditing
 - Chapter 10 – Authority Collection
 - Appendix H – IBM-Supplied Function Usage definitions

[IBM i Security Administration and Compliance](#), 3rd edition, by Carol Woodbury, 2020 available from Amazon or MCPress Bookstore

[Mastering IBM i Security](#) – A Step by Step Approach by Carol Woodbury, 2022 available from Amazon or MCPress Bookstore

Whitepaper: [Securing IBM i: A Dual Responsibility](#)

Articles by Carol Woodbury on [KiscoU](#)

47

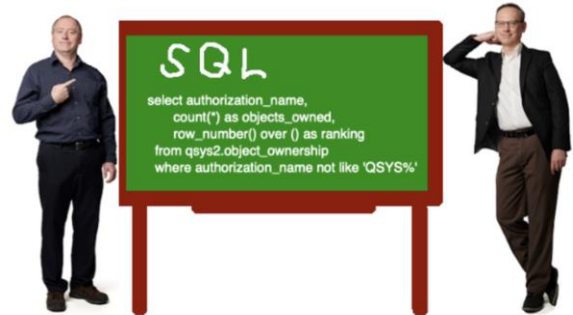
© Copyright IBM Corporation 2026

47

For More Information ...

What is IBM doing to help your team be successful with SQL?

1. ACS – Insert From Examples
SQL examples for all IBM i Services and more
2. SQL Tutor
SQL solutions for questions clients asked Scott
3. SQL Tutor
iSee Video blog series from Scott & Tim



<https://ibm.biz/Db2foriSQLTutor>

For example:

[Searching the IFS for objects with "log4j" in the name.sql](#)

The request from a client was to provide an SQL approach to search all of the IFS, finding any object that has "log4j" in its name, and producing an SQL table with the search results.

48

© Copyright IBM Corporation 2026

48

IBM i

51