Audit Journaling with Navigator for i

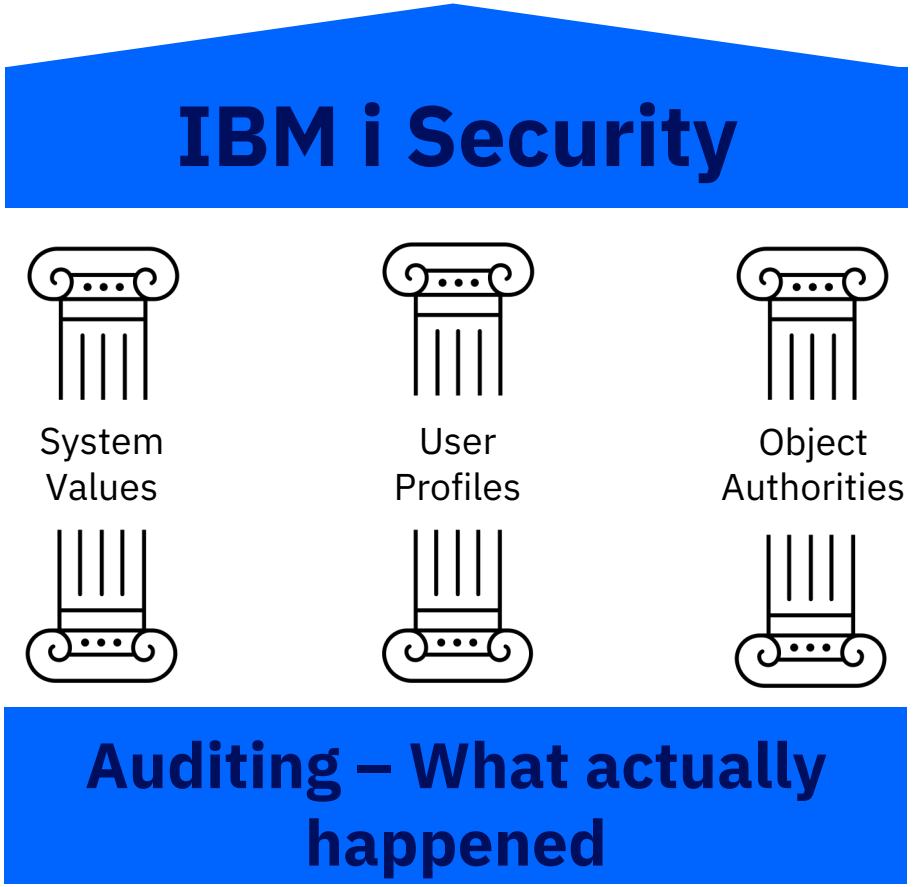
Tim Rowe – timmr@us.ibm.com
STSM – IBM i Business Architect

The Pillars of IBM i Security

The IBM i Security model is based on three pillars:

- System Values
- User Profiles
- Object Authorities

All three parts are key to understanding a system's true security posture

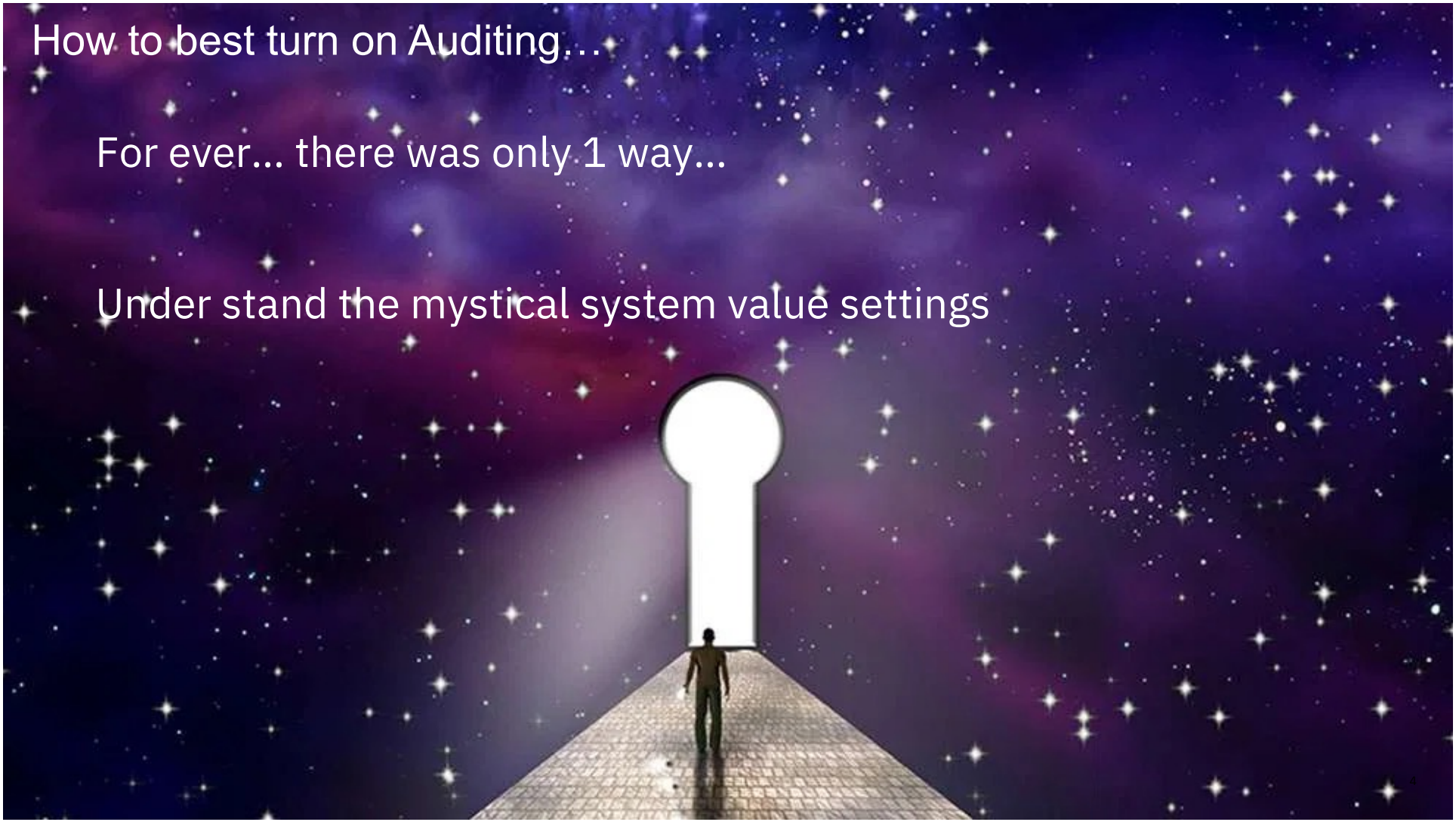


System Auditing

The IBM i has robust auditing capabilities built-in – Turn them ON!
Use Change Security Auditing (CHGSECAUD) command to set them up
IBM Recommends:

- QAUDCTL at: *AUDLVL, *OBJAUD, and *NOQTEMP
- QAUDLVL at: *AUTFAIL, *OBJMGT, *PGMFAIL, *SAVRST, *SERVICE, *SECURITY, and *SYSMGT
- Be careful with “noisy” options (*CREATE, *DELETE, *JOBDTA, *PRTDTA, *SPLFDTA)
  - Don’t want to hide the important messages in a huge pile of hay!

Do not put your Audit Journal Receivers in QSYS or QGPL – use their own secured library
Use command auditing to record the actions of privileged users – CHGUSRAUD AUDLVL(*CMD)
Integrate with a central SIEM (Splunk, QRadar, ArcSight) using the Syslog Reporting Manager


How to best turn on Auditing…
For ever… there was only 1 way…
Under stand the mystical system value settings

Audit Journaling Before

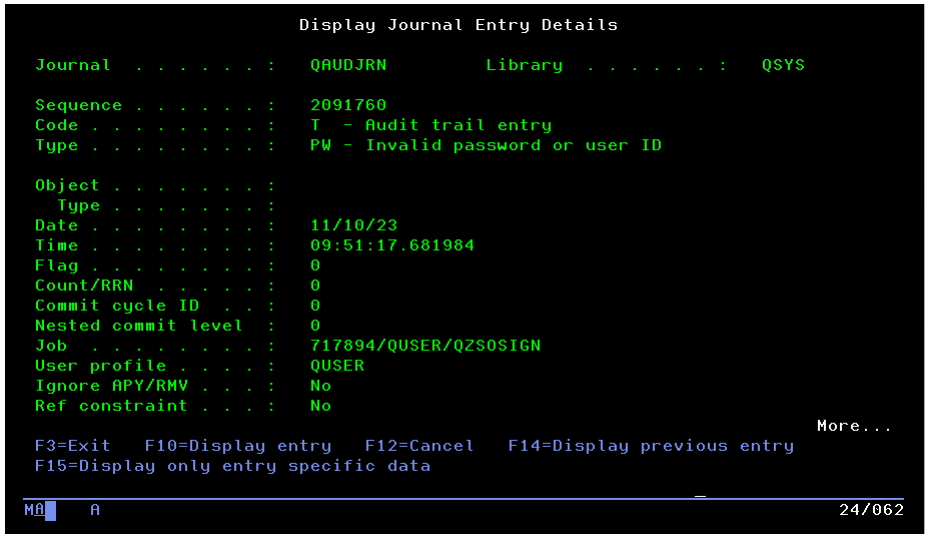
IBM i
continuous innovation
continuous integration

Configuration

- Multiple system values with multiple values
  - QAUDCTL
  - QAUDLVL
  - QAUDLVL2
  - …
- Set up journal and journal receivers

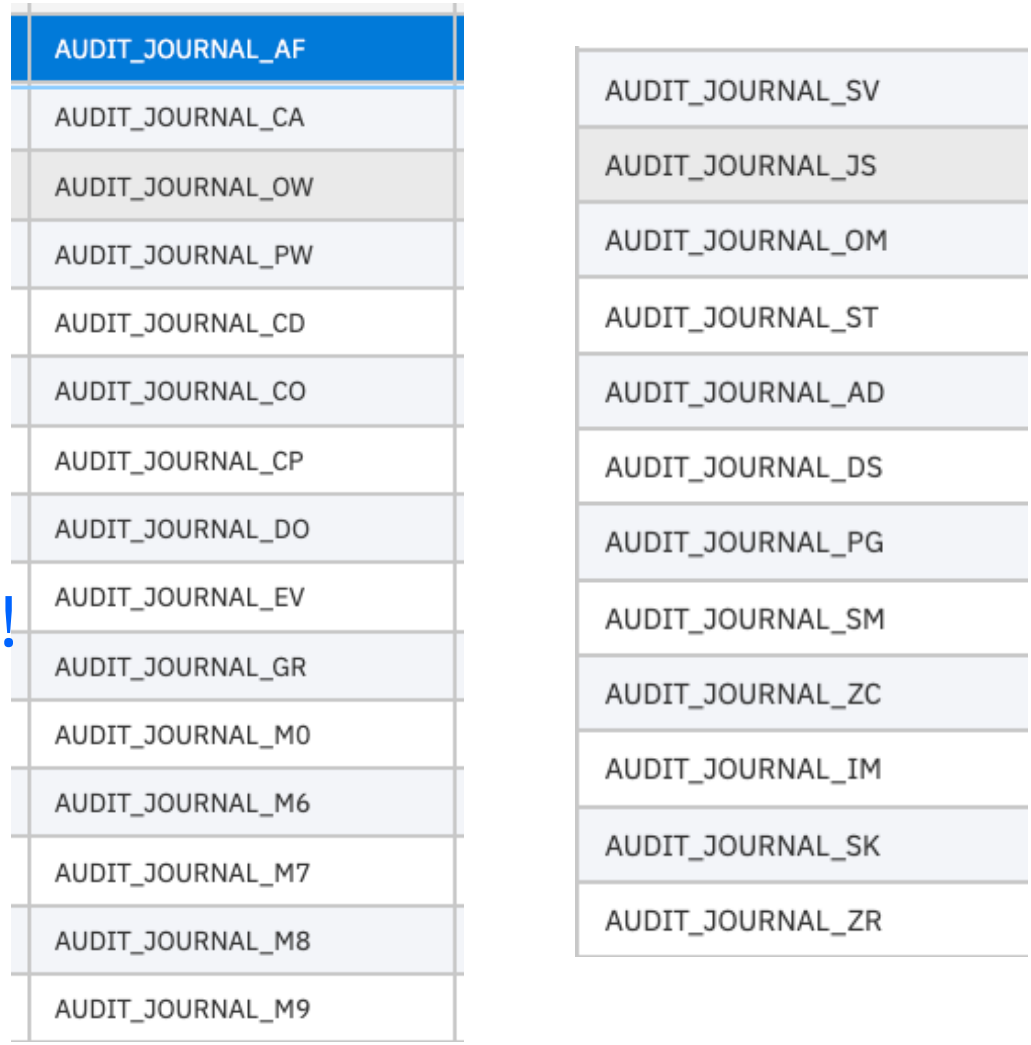
Viewing data

- Difficult to understand
- Hard to analyze all data at once
- Green screen (CPYAUDJRN, DSPJRN)

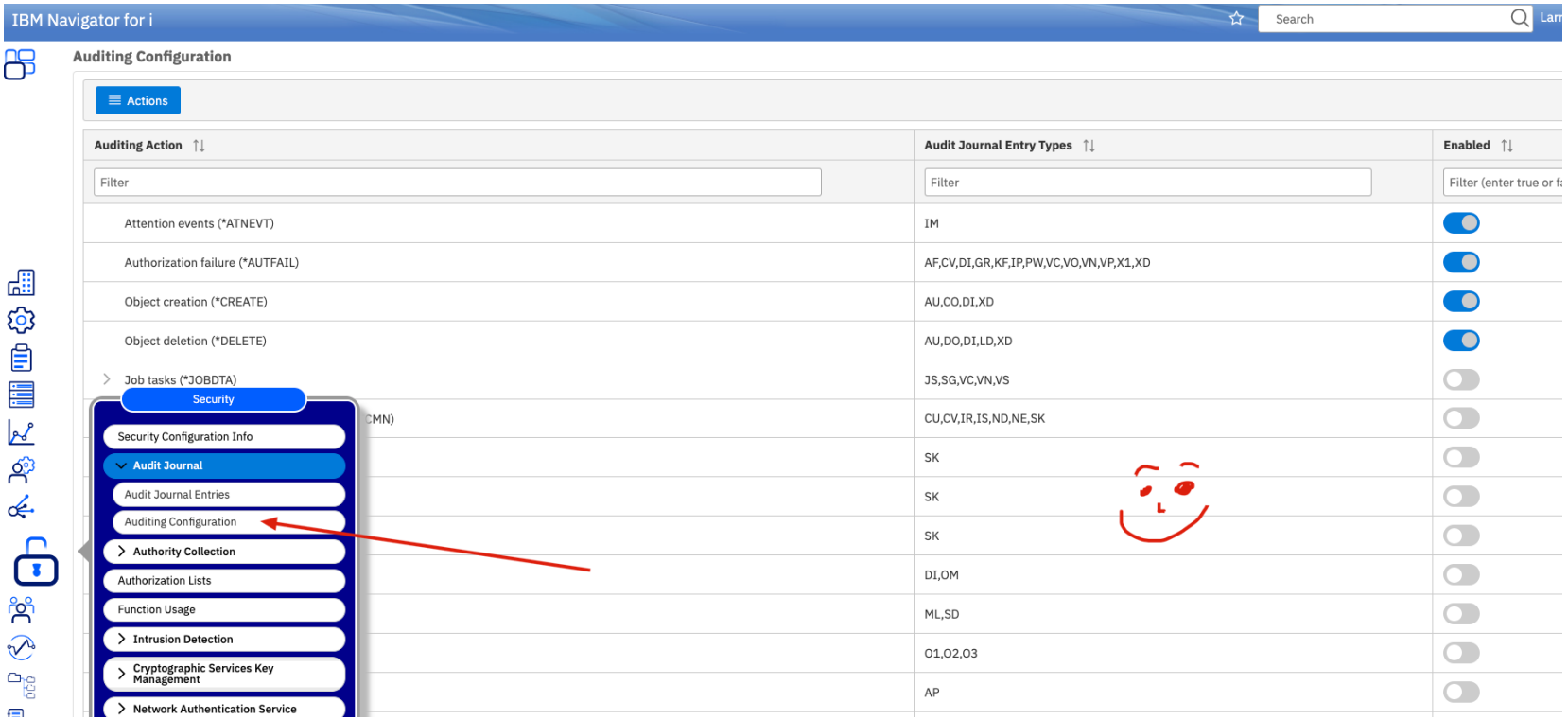


So many helper functions

And More coming!



Use Navigator

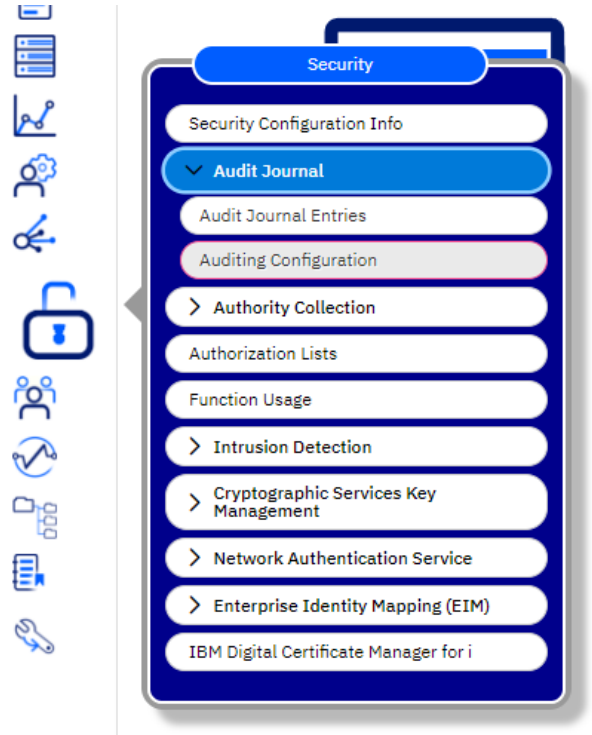


Audit Journaling Now

IBM i
continuous innovation
continuous integration

Configuring and viewing data is conveniently in one place

Based on the SYSTOOLS.AUDIT_JOURNAL_XX support



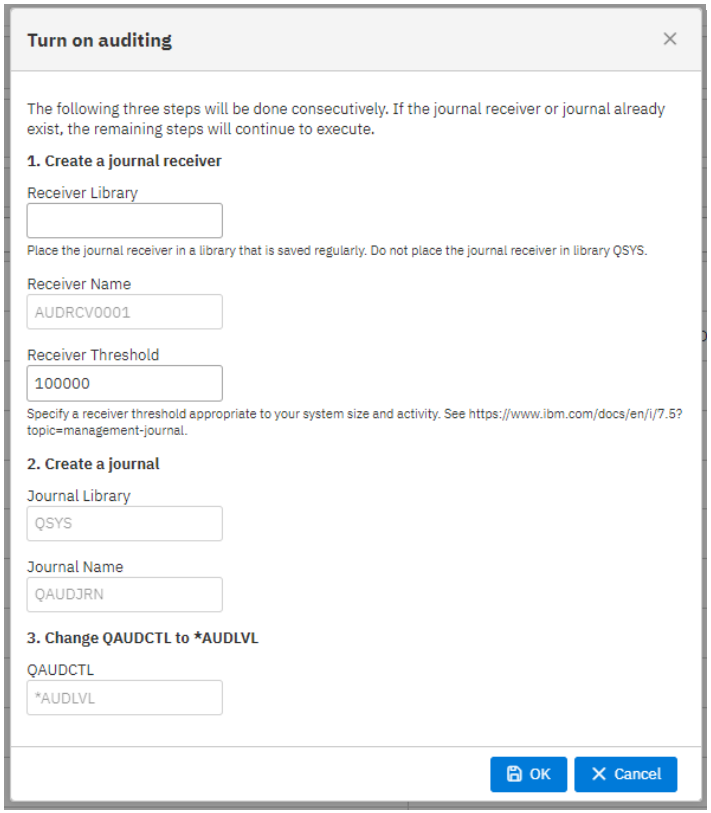
Audit Journaling Configuration

IBM i
continuous innovation
continuous integration

What if I've never set up auditing on my system before?

Navigator will handle the configuration for you

- Creates a journal receiver in the specified library
- Creates the QSYS/QAUDJRN journal
- Changes the QAUDCTL system value to *AUDLVL



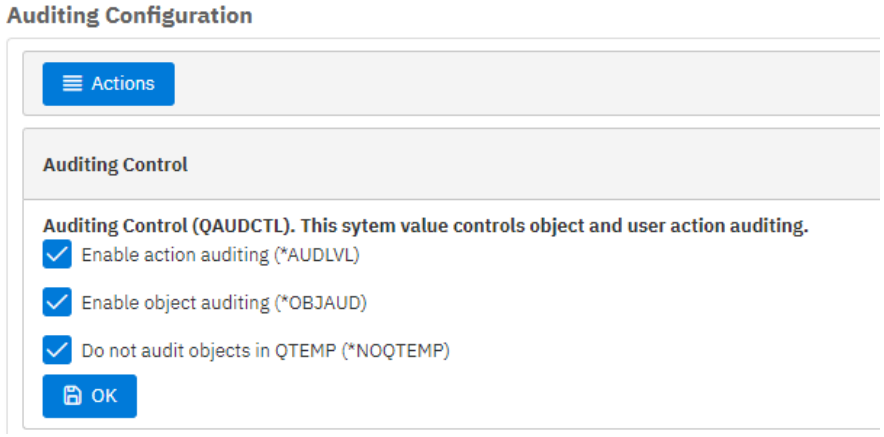
Audit Journaling Configuration

IBM i
continuous innovation
continuous integration

How do I control what is audited?

Navigator allows you to set the QAUDCTL system value

- Check *AUDLVL to enable action auditing (password failures, objects created, etc)
- Check *OBJAUD to enable auditing on specified objects
- Check *NOQTEMP to disable auditing objects in QTEMP

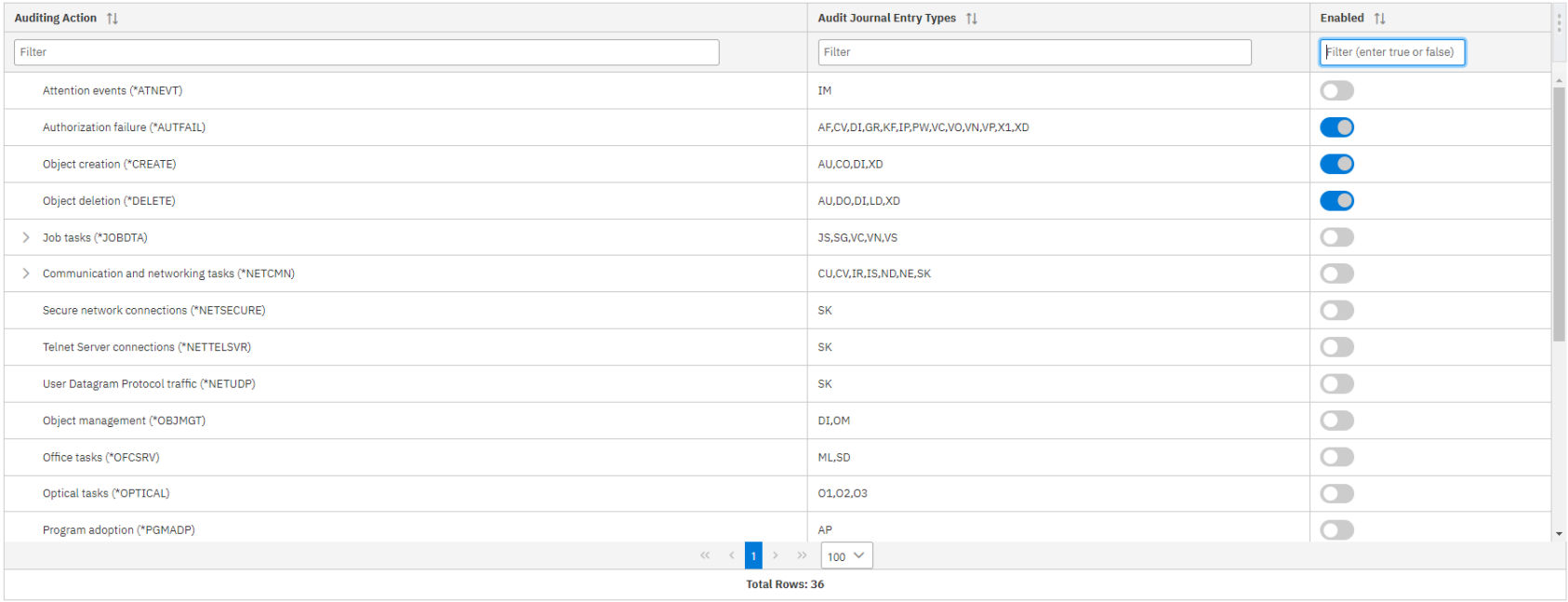


Audit Journaling Configuration

IBM i
continuous innovation
continuous integration

How do I control what is audited?

Navigator allows you to set the QAUDLVL/QAUDLVL2 system values



Auditing Action	Audit Journal Entry Types	Enabled
Filter	Filter	Filter (enter true or false)
Attention events (*ATNEVT)	IM	
Authorization failure (*AUTFAIL)	AF,CV,DI,GR,KF,IP,PW,VC,VO,VN,VP,X1,XD	
Object creation (*CREATE)	AU,CO,DI,XD	
Object deletion (*DELETE)	AU,DO,DI,LD,XD	
Job tasks (*JOBDTA)	JS,SG,VC,VN,VS	
Communication and networking tasks (*NETCMN)	CU,CV,IR,IS,ND,NE,SK	
Secure network connections (*NETSECURE)	SK	
Telnet Server connections (*NETTELSVR)	SK	
User Datagram Protocol traffic (*NETUDP)	SK	
Object management (*OBJMGT)	DI,OM	
Office tasks (*OFCSRV)	ML,SD	
Optical tasks (*OPTICAL)	O1,O2,O3	
Program adoption (*PGMADP)	AP	

« ‹ 1 › » 100

Total Rows: 36

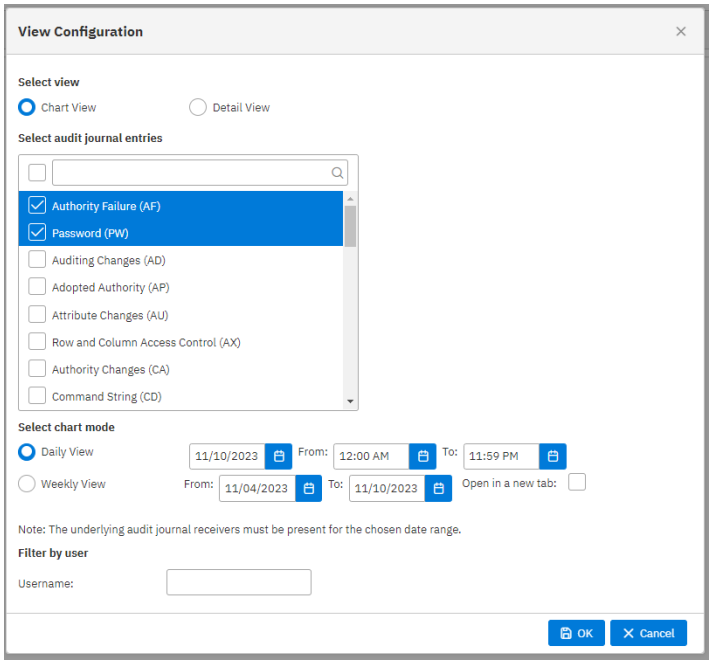
View Audit Journal Data

IBM i
continuous innovation
continuous integration

How do I view the audit journal data?

Navigator provides flexibility for how you want to view and analyze audit journal data

- Chart view – graphical representation
  - Daily view – bar graph of audit entries for the day
  - Weekly view – line graph for audit entries of a week
- Detail view – table view for one audit entry

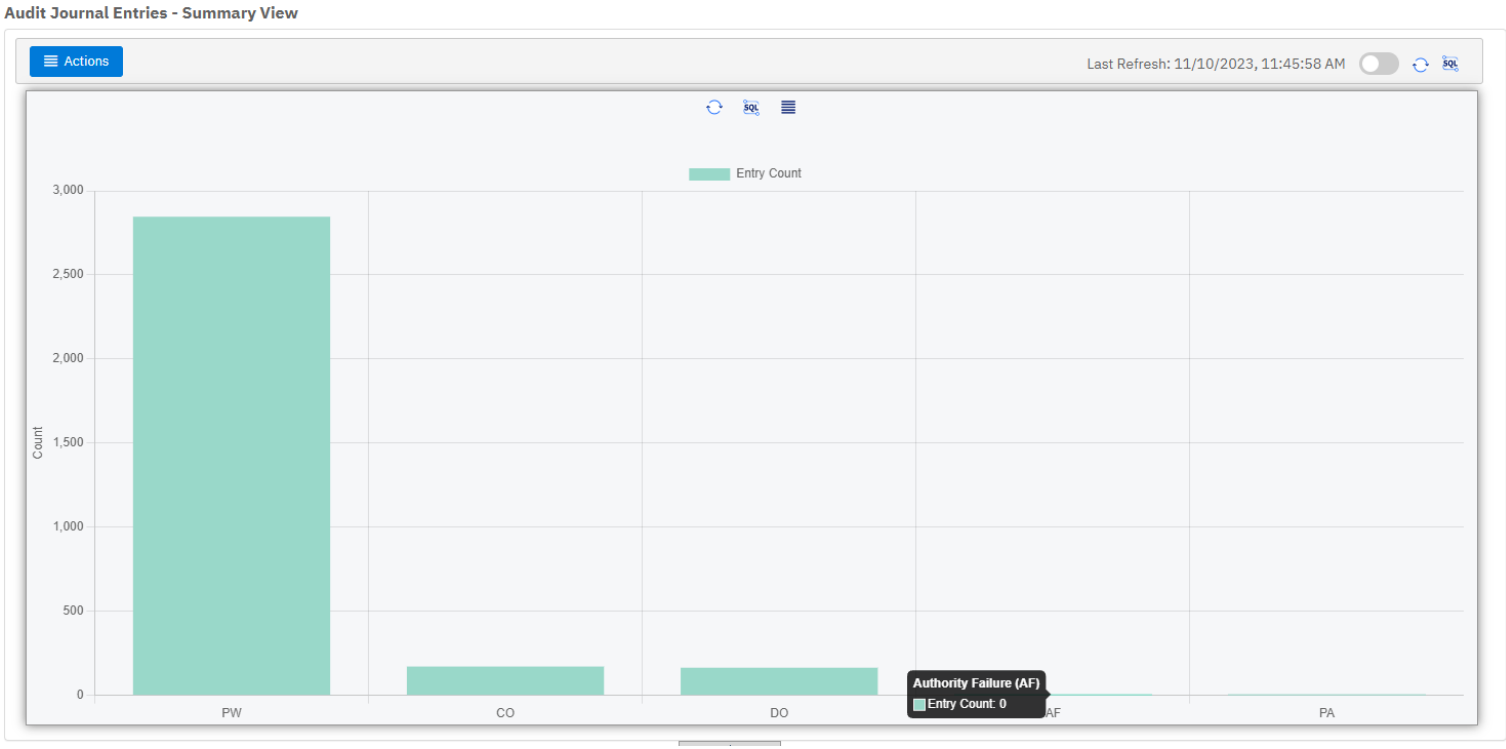


View Audit Journal Data

IBM i
continuous innovation
continuous integration

Daily View

- Helpful for monitoring your system's activity

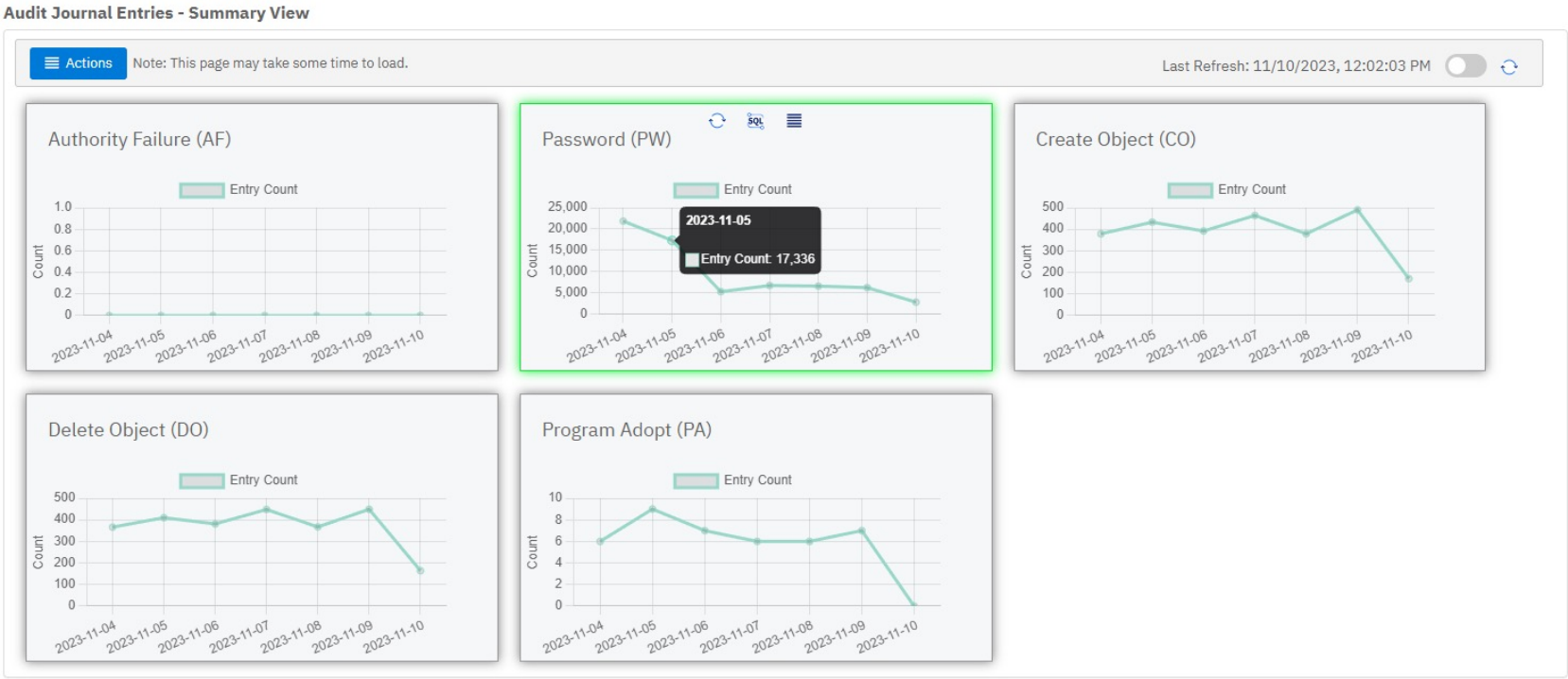


View Audit Journal Data

IBM i
continuous innovation
continuous integration

Weekly View

- Helpful for seeing trends over time



View Audit Journal Data

IBM i
continuous innovation
continuous integration

Detail View

- Filter and sort through data to understand what happened when an audit entry was created

Password (PW) Detail View

Actions | Weekly Summary View > Detail View | Filters

Timestamp	Qualified Job Name	Program Library	Program Name	Violation Type	Violation Type Detail	User Name
Filter	Filter	Filter	Filter	A, C, D, E, P, Q, R, S, U, X, Y, Z	Filter	Filter
2023-11-04 11:46:06.862896	198060/QUSER/QP0ZSPWT	QSYS	QP0ZPCP2	U	User name not valid	ROOT
2023-11-04 11:46:09.069328	198064/QUSER/QP0ZSPWT	QSYS	QP0ZPCP2	U	User name not valid	ROOT
2023-11-04 11:46:11.123232	198066/QUSER/QP0ZSPWT	QSYS	QP0ZPCP2	U	User name not valid	ROOT
2023-11-04 11:46:17.048880	198068/QUSER/QP0ZSPWT	QSYS	QP0ZPCP2	U	User name not valid	ROOT
2023-11-04 11:46:26.245840	198070/QUSER/QP0ZSPWT	QSYS	QP0ZPCP2	U	User name not valid	ROOT
2023-11-04 11:46:31.499296	198074/QUSER/QP0ZSPWT	QSYS	QP0ZPCP2	U	User name not valid	ROOT
2023-11-04 11:46:33.458416	198076/QUSER/QP0ZSPWT	QSYS	QP0ZPCP2	U	User name not valid	ROOT

1 2 3 4 5 | 100

Total Rows: 61454

Performance Enhancements with Data Mart

IBM i
continuous innovation
continuous integration

- Large systems generate tons of audit journal entries which can be hard to manage
- Data mart will allow you to preload audit journal data so it can be quickly managed in the GUI
- Allows you to create a historical record of audit journal data
- Available in 7.4 TR 10 and 7.5 TR 4

Data Mart – Under the Covers

IBM i
continuous innovation
continuous integration

- MANAGE_AUDIT_JOURNAL_DATA_MART procedure
- Requires *AUDIT and object authority to the data mart library and tables

```
CALL QSYS2.MANAGE_AUDIT_JOURNAL_DATA_MART(
   JOURNAL_ENTRY_TYPE => 'PW',
   DATA_MART_LIBRARY => 'AECIESLA',
   STARTING_TIMESTAMP => CURRENT TIMESTAMP - 1 MONTH,
   ENDING_TIMESTAMP => CURRENT TIMESTAMP,
   DATA_MART_ACTION => 'CREATE'
);
```

Data Mart – Under the Covers

IBM i
continuous innovation
continuous integration

- AUDIT_JOURNAL_DATA_MART_INFO view
  - Metadata table for the most recent call to the manage procedure
  - Contains one row for each unique library and journal entry type pair

```
SELECT DATA_MART_LIBRARY, JOURNAL_ENTRY_TYPE,
    BUILD_START, BUILD_END, BUILD_JOB
  FROM QSYS2.AUDIT_JOURNAL_DATA_MART_INFO;
```

Data Mart Library DATA_MART_LIBRARY	Journal Entry Type JOURNAL_ENTRY_TYPE	Build Start BUILD_START	Build End BUILD_END	Build Job BUILD_JOB
AECIESLA	PW	2024-01-30 15:07:48.171775	2024-01-30 15:08:46.290754	937634/QUSER/QZDASOINIT
SCOTTF	CO	2024-01-30 15:09:52.163365	2024-01-30 15:09:54.084227	937634/QUSER/QZDASOINIT
SCOTTF	DO	2024-01-30 15:09:57.015882	2024-01-30 15:09:58.424444	937634/QUSER/QZDASOINIT
TIMMR	AF	2024-01-30 15:06:41.279314	2024-01-30 15:06:53.040439	937634/QUSER/QZDASOINIT
TIMMR	PW	2024-01-30 15:06:34.119496	2024-01-30 15:06:34.366154	937634/QUSER/QZDASOINIT

Data Mart - Navigator

IBM i
continuous innovation
continuous integration

- Security -> Audit Journaling -> Manage Data Mart

Manage Audit Journal Data Mart

Actions

Data Mart Library	Journal Entry Type	Status	Audit Journal Starting Timestamp	Audit Journal Ending Timestamp
Filter	Filter	Filter	Filter	Filter
AECIESLA	Password (PW)	Built	2024-01-23 15:07:48.150079	2024-01-30 15:07:48.150079
SCOTTF	Create Object (CO)	Built	2024-01-25 15:09:52.139004	2024-01-30 15:09:52.139004
SCOTTF	Delete Object (DO)	Built	2024-01-25 15:09:57.009925	2024-01-30 15:09:57.009925
TIMMR	Authority Failure (AF)	Built	2024-01-28 15:06:41.273382	2024-01-29 15:06:41.273382
TIMMR	Password (PW)	Built	2024-01-28 15:06:34.111383	2024-01-29 15:06:34.111383

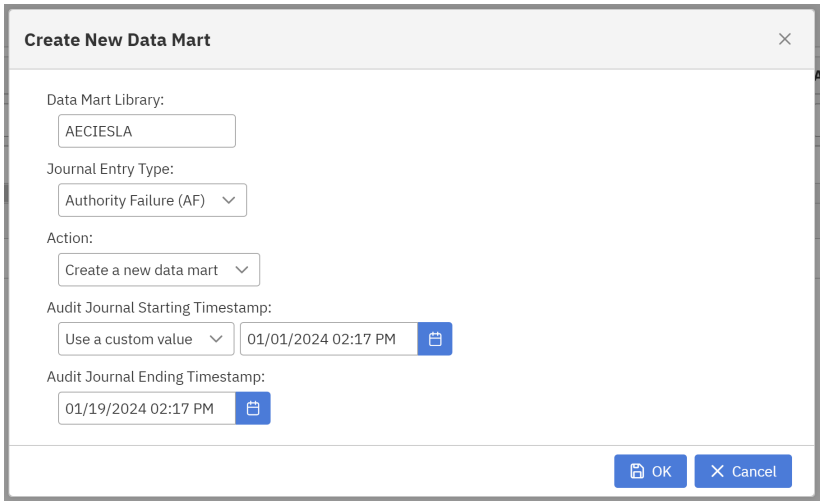
« ‹ 1 › » 100

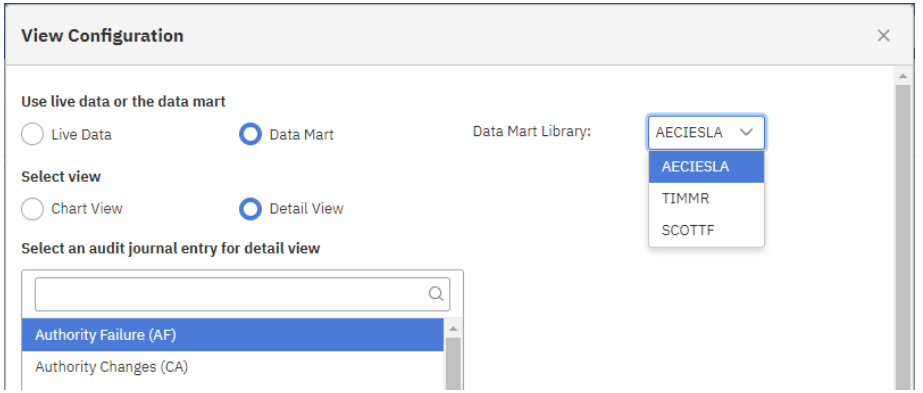
Total Rows: 5

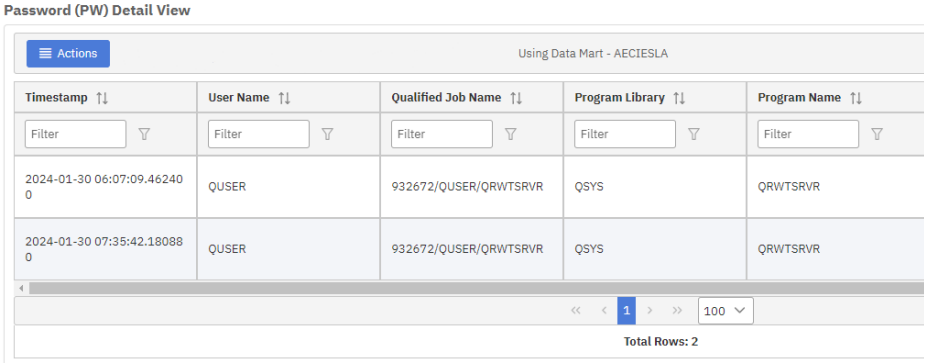
Data Mart - Navigator

IBM i
continuous innovation
continuous integration

- Can be used for chart view and detail view
- Build occurs in the background





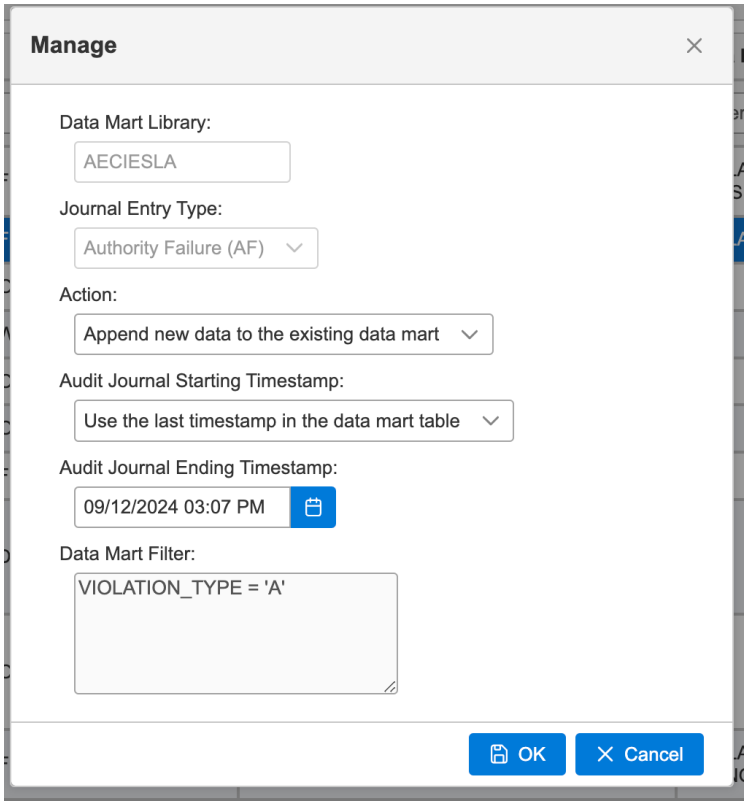


What's coming next to Data Mart

IBM i
continuous innovation
continuous integration

Filtering

- New parameter on the MANAGE_AUDIT_JOURNAL_DATA_MART procedure
- Provide filter criteria when creating a data mart table to limit the type of entries
  - Violation type
  - User profile
  - IP address
  - etc



Audit Journaling in Navigator for i

IBM i
continuous innovation
continuous integration

- Available in 7.4 and 7.5
- SQL Services available: https://www.ibm.com/support/pages/node/6442047
- For more information on Navigator: https://www.ibm.com/support/pages/node/6483299

Special notices

IBM i
continuous innovation
continuous integration

This document was developed for IBM offerings in the United States as of the date of publication. IBM may not make these offerings available in other countries, and the information is subject to change without notice. Consult your local IBM business contact for information on the IBM offerings available in your area.

Information in this document concerning non-IBM products was obtained from the suppliers of these products or other public sources. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

IBM may have patents or pending patent applications covering subject matter in this document. The furnishing of this document does not give you any license to these patents. Send license inquires, in writing, to IBM Director of Licensing, IBM Corporation, New Castle Drive, Armonk, NY 10504-1785 USA.

All statements regarding IBM future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.

The information contained in this document has not been submitted to any formal IBM test and is provided "AS IS" with no warranties or guarantees either expressed or implied.

All examples cited or described in this document are presented as illustrations of the manner in which some IBM products can be used and the results that may be achieved. Actual environmental costs and performance characteristics will vary depending on individual client configurations and conditions.

IBM Global Financing offerings are provided through IBM Credit Corporation in the United States and other IBM subsidiaries and divisions worldwide to qualified commercial and government clients. Rates are based on a client's credit rating, financing terms, offering type, equipment type and options, and may vary by country. Other restrictions may apply. Rates and offerings are subject to change, extension or withdrawal without notice.

IBM is not responsible for printing errors in this document that result in pricing or information inaccuracies.

All prices shown are IBM's United States suggested list prices and are subject to change without notice; reseller prices may vary.

IBM hardware products are manufactured from new parts, or new and serviceable used parts. Regardless, our warranty terms apply.

Any performance data contained in this document was determined in a controlled environment. Actual results may vary significantly and are dependent on many factors including system hardware configuration and software design and configuration. Some measurements quoted in this document may have been made on development-level systems. There is no guarantee these measurements will be the same on generally-available systems. Some measurements quoted in this document may have been estimated through extrapolation. Users of this document should verify the applicable data for their specific environment.

Special notices (cont.)

IBM i
continuous innovation
continuous integration

Revised December 2, 2010