

Audit Journaling with Navigator for i

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

© Copyright IBM Corporation 2024

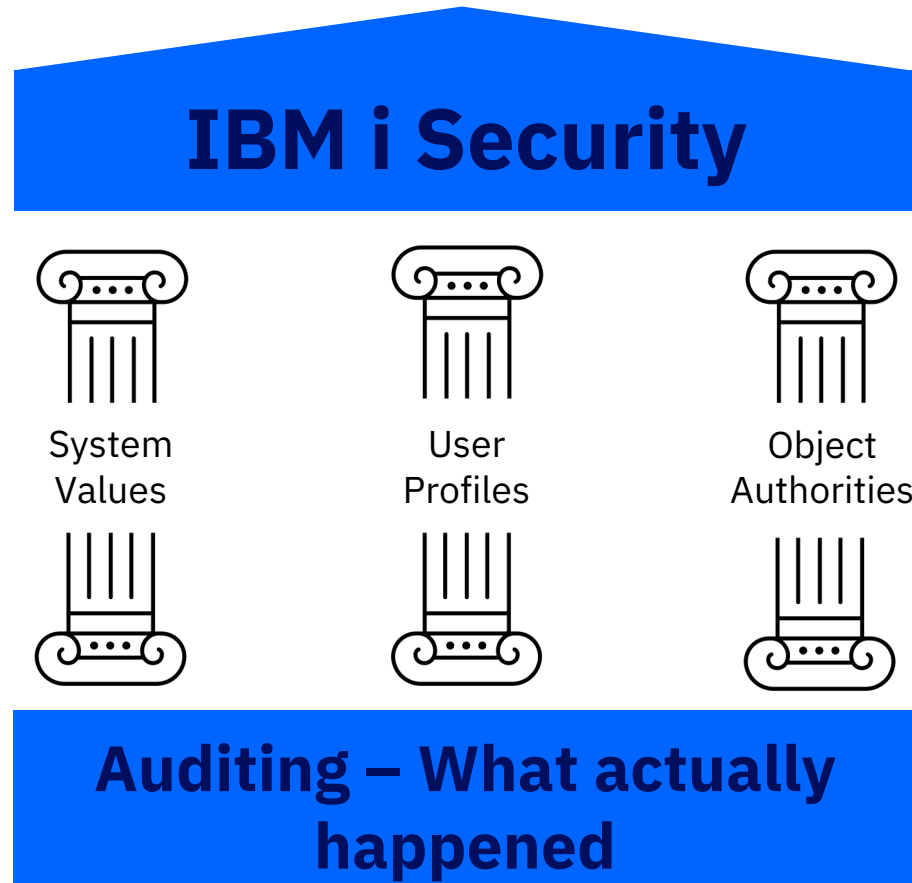


The Pillars of IBM i Security

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, *JOBDDTA, *PRTDDTA, *SPLFDDTA)
 - 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

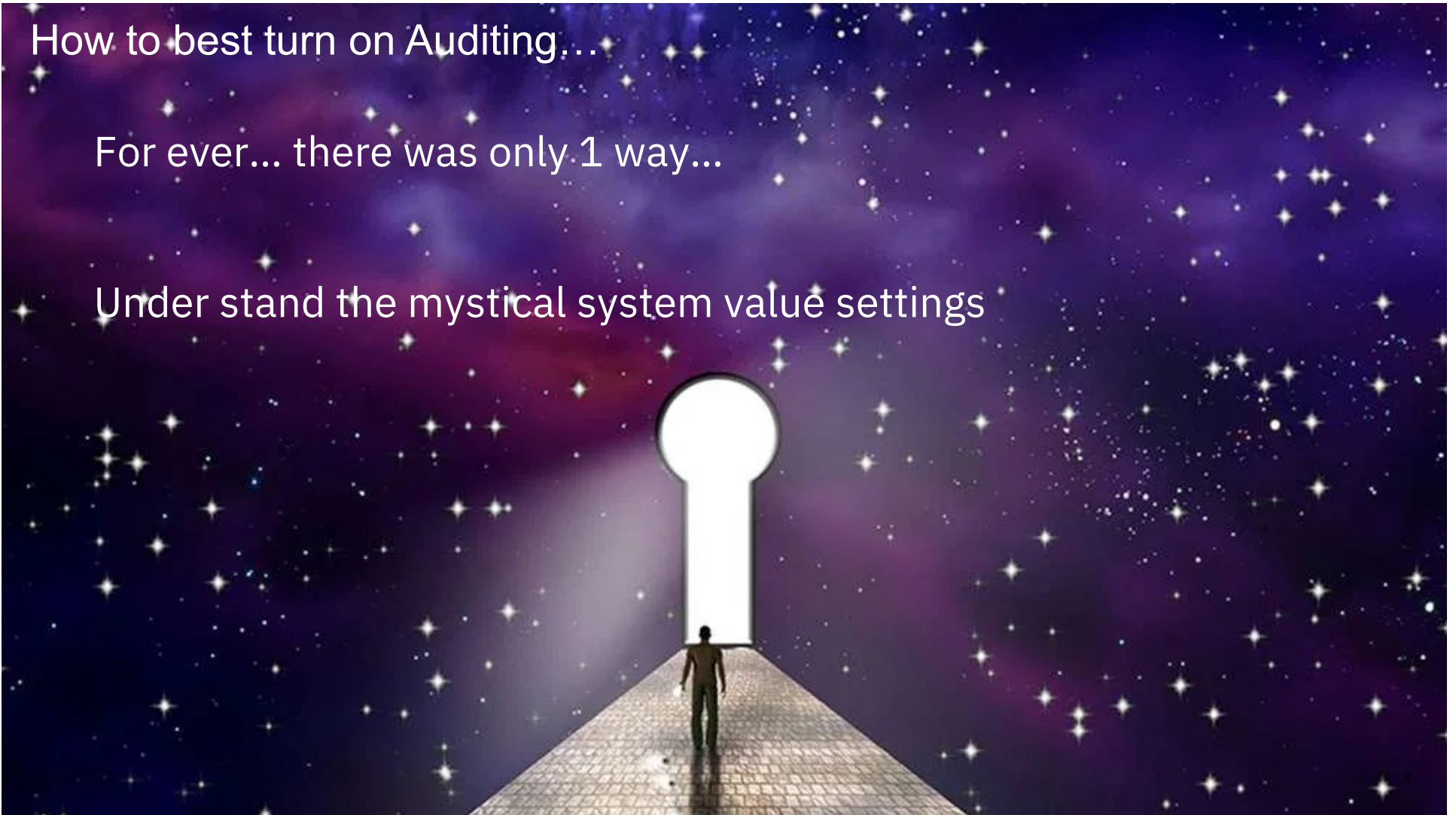
Use command auditing to record the actions of privileged users – CHGUSRAUD AUDLVL(*CMD)

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

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)

```

Display Journal Entry Details

Journal . . . . . : QAUDJRN      Library . . . . . : QSYS
Sequence . . . . . : 2091760
Code . . . . . : T - Audit trail entry
Type . . . . . : PW - Invalid password or user ID

Object . . . . . :
  Type . . . . . :
Date . . . . . : 11/10/23
Time . . . . . : 09:51:17.681984
Flag . . . . . : 0
Count/RRN . . . . . : 0
Commit cycle ID . . . . . : 0
Nested commit level . . . . . : 0
Job . . . . . : 717894/QUSER/QZS0SIGN
User profile . . . . . : QUSER
Ignore APY/RMV . . . . . : No
Ref constraint . . . . . : No

More...

F3=Exit  F10=Display entry  F12=Cancel  F14=Display previous entry
F15=Display only entry specific data

MA  A 24/062
  
```

So many helper functions

And More coming!

AUDIT_JOURNAL_AF
AUDIT_JOURNAL_CA
AUDIT_JOURNAL_OW
AUDIT_JOURNAL_PW
AUDIT_JOURNAL_CD
AUDIT_JOURNAL_CO
AUDIT_JOURNAL_CP
AUDIT_JOURNAL_DO
AUDIT_JOURNAL_EV
AUDIT_JOURNAL_GR
AUDIT_JOURNAL_M0
AUDIT_JOURNAL_M6
AUDIT_JOURNAL_M7
AUDIT_JOURNAL_M8
AUDIT_JOURNAL_M9

AUDIT_JOURNAL_SV
AUDIT_JOURNAL_JS
AUDIT_JOURNAL_OM
AUDIT_JOURNAL_ST
AUDIT_JOURNAL_AD
AUDIT_JOURNAL_DS
AUDIT_JOURNAL_PG
AUDIT_JOURNAL_SM
AUDIT_JOURNAL_ZC
AUDIT_JOURNAL_IM
AUDIT_JOURNAL_SK
AUDIT_JOURNAL_ZR

Use Navigator

IBM Navigator for i

Auditing Configuration

Actions

Auditing Action ↑↓	Audit Journal Entry Types ↑↓	Enabled ↑↓
Filter	Filter	Filter (enter true or false)
Attention events (*ATNEVT)	IM	<input checked="" type="checkbox"/>
Authorization failure (*AUTFAIL)	AF,CV,DI,GR,KF,IP,PW,VC,VO,VN,VP,X1,XD	<input checked="" type="checkbox"/>
Object creation (*CREATE)	AU,CO,DI,XD	<input checked="" type="checkbox"/>
Object deletion (*DELETE)	AU,DO,DI,LD,XD	<input checked="" type="checkbox"/>
> Job tasks (*JOBDTA)	JS,SG,VC,VN,VS	<input type="checkbox"/>
Security	CU,CV,IR,IS,ND,NE,SK	<input type="checkbox"/>
Security Configuration Info	CMN)	<input type="checkbox"/>
> Audit Journal	SK	<input type="checkbox"/>
Audit Journal Entries	SK	<input type="checkbox"/>
Auditing Configuration	SK	<input type="checkbox"/>
> Authority Collection	DI,OM	<input type="checkbox"/>
Authorization Lists	ML,SD	<input type="checkbox"/>
Function Usage	O1,O2,O3	<input type="checkbox"/>
> Intrusion Detection	AP	<input type="checkbox"/>
> Cryptographic Services Key Management		
> Network Authentication Service		

© Copyright IBM Corporation 2024

7

Audit Journaling Now

Configuring and viewing data is conveniently in one place

Based on the SYSTOOLS.AUDIT_JOURNAL_XX support



Audit Journaling Configuration

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

Turn on auditing ✕

The following three steps will be done consecutively. If the journal receiver or journal already exist, the remaining steps will continue to execute.

1. Create a journal receiver

Receiver Library

Place the journal receiver in a library that is saved regularly. Do not place the journal receiver in library QSYS.

Receiver Name

Receiver Threshold

Specify a receiver threshold appropriate to your system size and activity. See <https://www.ibm.com/docs/en/i/7.5?topic=management-journal>.

2. Create a journal

Journal Library

Journal Name

3. Change QAUDCTL to *AUDLVL

QAUDCTL

Audit Journaling Configuration

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

Auditing Configuration

Actions

Auditing Control

Auditing Control (QAUDCTL). This system value controls object and user action auditing.

- Enable action auditing (*AUDLVL)
- Enable object auditing (*OBJAUD)
- Do not audit objects in QTEMP (*NOQTEMP)

OK

Audit Journaling Configuration



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	<input type="checkbox"/>
Authorization failure (*AUTFAIL)	AF,CV,DI,GR,KF,IP,PW,VC,VO,VN,VP,X1,XD	<input checked="" type="checkbox"/>
Object creation (*CREATE)	AU,CO,DI,XD	<input checked="" type="checkbox"/>
Object deletion (*DELETE)	AU,DO,DI,LD,XD	<input checked="" type="checkbox"/>
> Job tasks (*JOBDTA)	JS,SG,VC,VN,VS	<input type="checkbox"/>
> Communication and networking tasks (*NETCMN)	CU,CV,IR,IS,ND,NE,SK	<input type="checkbox"/>
Secure network connections (*NETSECURE)	SK	<input type="checkbox"/>
Telnet Server connections (*NETTELSVR)	SK	<input type="checkbox"/>
User Datagram Protocol traffic (*NETUDP)	SK	<input type="checkbox"/>
Object management (*OBJMGT)	DI,OM	<input type="checkbox"/>
Office tasks (*OFCSRVR)	ML,SD	<input type="checkbox"/>
Optical tasks (*OPTICAL)	O1,O2,O3	<input type="checkbox"/>
Program adoption (*PGMADP)	AP	<input type="checkbox"/>

Total Rows: 36

View Audit Journal Data

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 Configuration

Select view
 Chart View Detail View

Select audit journal entries

[Search]

Authority Failure (AF)
 Password (PW)
 Auditing Changes (AD)
 Adopted Authority (AP)
 Attribute Changes (AU)
 Row and Column Access Control (AX)
 Authority Changes (CA)
 Command String (CD)

Select chart mode
 Daily View From: 11/10/2023 From: 12:00 AM To: 11:59 PM
 Weekly View From: 11/04/2023 To: 11/10/2023 Open in a new tab:

Note: The underlying audit journal receivers must be present for the chosen date range.

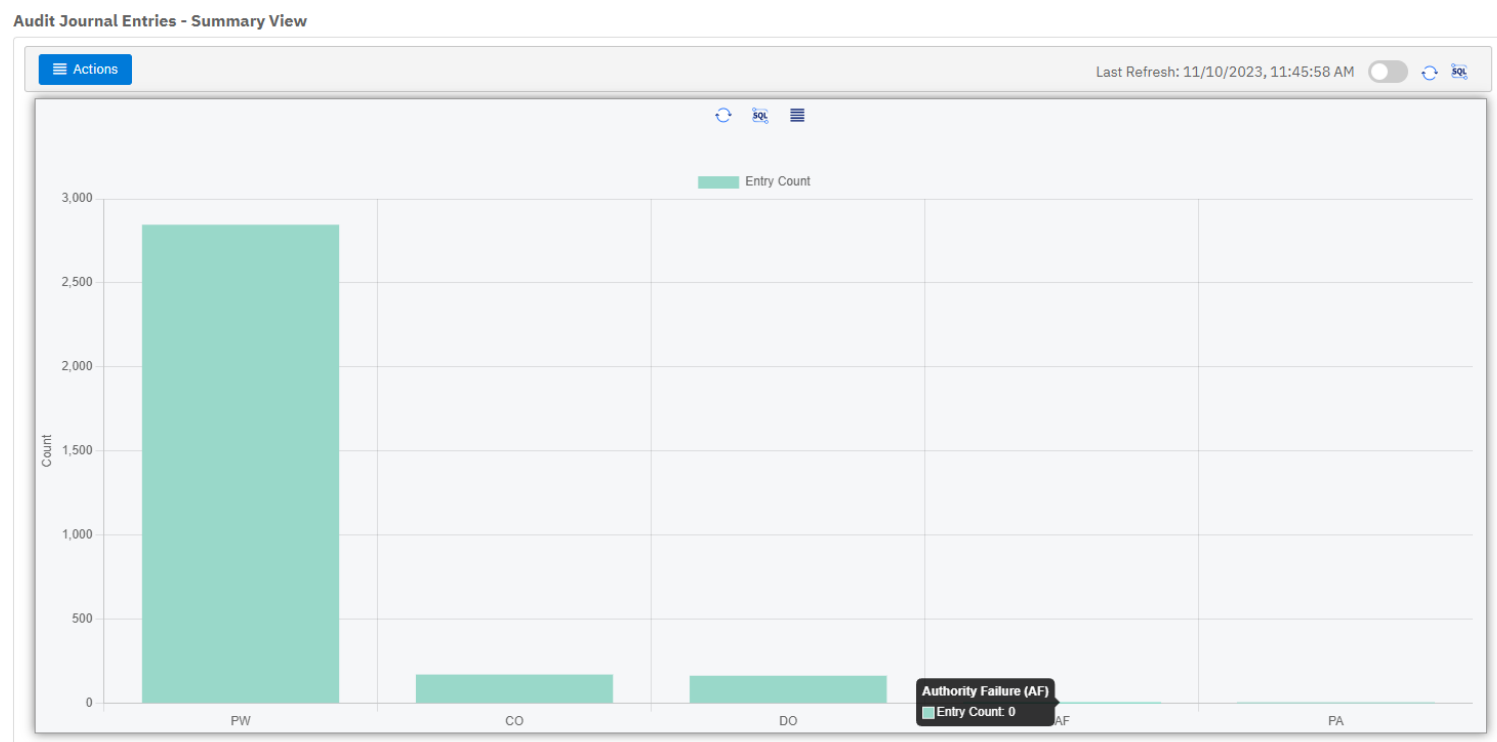
Filter by user
 Username:

OK Cancel

View Audit Journal Data

Daily View

- Helpful for monitoring your system's activity

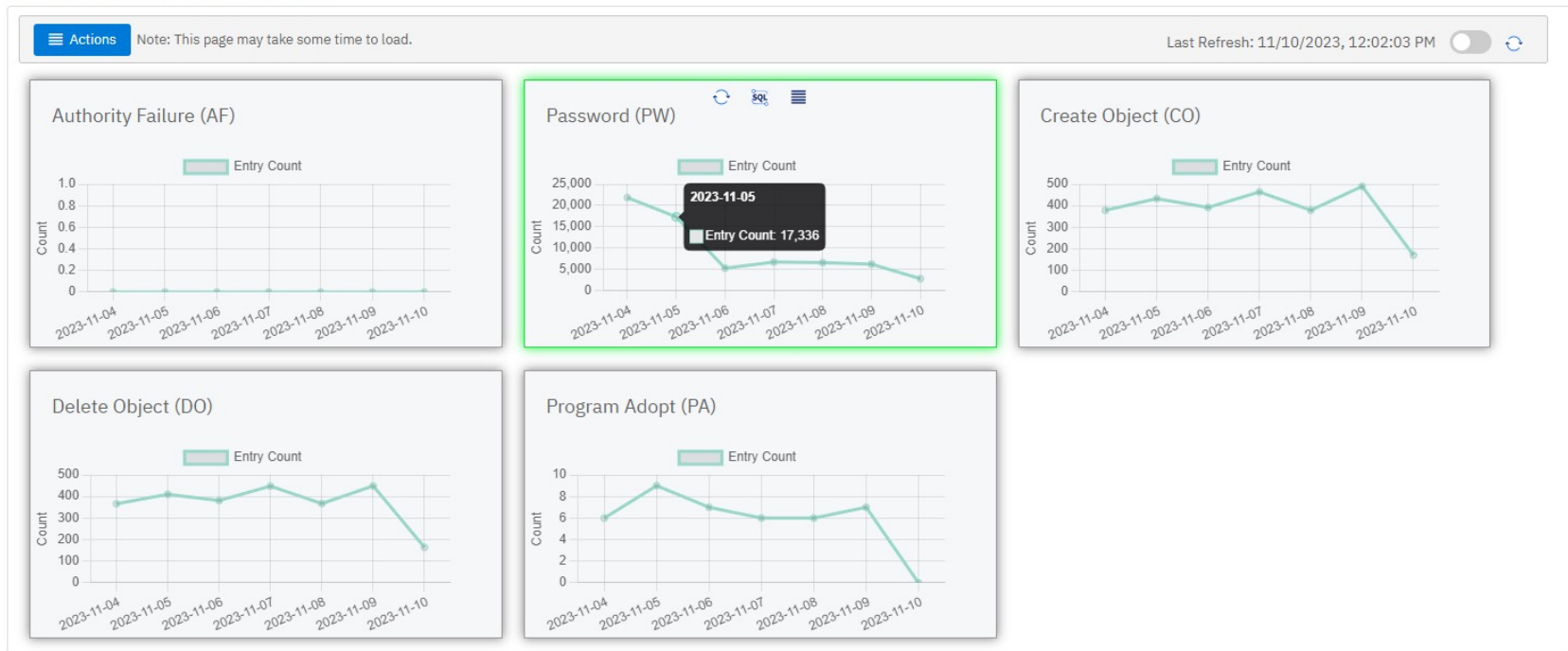


View Audit Journal Data

Weekly View

- Helpful for seeing trends over time

Audit Journal Entries - Summary View



View Audit Journal Data

Detail View

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

Password (PW) Detail View

Timestamp ↑↓	Qualified Job Name ↑↓	Program Library ↑↓	Program Name ↑↓	Violation Type ↑↓	Violation Type Detail ↑↓	User Name ↑↓
<input type="text" value="Filter"/>	<input type="text" value="Filter"/>	<input type="text" value="Filter"/>	<input type="text" value="Filter"/>	A, C, D, E, P, Q, R, S, U, X, Y, Z	<input type="text" value="Filter"/>	<input type="text" value="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

Total Rows: 61454

Performance Enhancements with Data Mart

- 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

- `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

- 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	Journal Entry Type	Build Start	Build End	Build Job
DATA_MART_LIBRARY	JOURNAL_ENTRY_TYPE	BUILD_START	BUILD_END	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



- Security -> Audit Journaling -> Manage Data Mart

Manage Audit Journal Data Mart

Data Mart Library	Journal Entry Type	Status	Audit Journal Starting Timestamp	Audit Journal Ending Timestamp
<input type="text" value="Filter"/>	<input type="text" value="Filter"/>	<input type="text" value="Filter"/>	<input type="text" value="Filter"/>	<input type="text" value="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

Navigation: << < 1 > >> 100

Total Rows: 5

Data Mart - Navigator

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

Create New Data Mart ✕

Data Mart Library:

Journal Entry Type:

Action:

Audit Journal Starting Timestamp:

Audit Journal Ending Timestamp:

View Configuration ✕

Use live data or the data mart
 Live Data Data Mart Data Mart Library:

Select view
 Chart View Detail View

Select an audit journal entry for detail view

Password (PW) Detail View

Using Data Mart - AECIESLA

Timestamp ↑↓	User Name ↑↓	Qualified Job Name ↑↓	Program Library ↑↓	Program Name ↑↓
Filter	Filter	Filter	Filter	Filter
2024-01-30 06:07:09.462400	QUSER	932672/QUSER/QRWTSRVR	QSYS	QRWTSRVR
2024-01-30 07:35:42.180880	QUSER	932672/QUSER/QRWTSRVR	QSYS	QRWTSRVR

Total Rows: 2

What's coming next to Data Mart

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

The screenshot shows a 'Manage' dialog box with the following fields and options:

- Data Mart Library:** AECIESLA
- Journal Entry Type:** Authority Failure (AF) (dropdown)
- Action:** Append new data to the existing data mart (dropdown)
- Audit Journal Starting Timestamp:** Use the last timestamp in the data mart table (dropdown)
- Audit Journal Ending Timestamp:** 09/12/2024 03:07 PM (calendar icon)
- Data Mart Filter:** VIOLATION_TYPE = 'A' (text area)

Buttons at the bottom: OK, Cancel

Audit Journaling in Navigator for i

- 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



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, the IBM logo, ibm.com AIX, AIX (logo), AIX 5L, AIX 6 (logo), AS/400, BladeCenter, Blue Gene, ClusterProven, Db2, ESCON, i5/OS, i5/OS (logo), IBM Business Partner (logo), IntelliStation, LoadLeveler, Lotus, Lotus Notes, Notes, Operating System/400, OS/400, PartnerLink, PartnerWorld, PowerPC, pSeries, Rational, RISC System/6000, RS/6000, THINK, Tivoli, Tivoli (logo), Tivoli Management Environment, WebSphere, xSeries, z/OS, zSeries, Active Memory, Balanced Warehouse, CacheFlow, Cool Blue, IBM Systems Director VMControl, pureScale, TurboCore, Chiphopper, Cloudscape, Db2 Universal Database, DS4000, DS6000, DS8000, EnergyScale, Enterprise Workload Manager, General Parallel File System, , GPFS, HACMP, HACMP/6000, HASM, IBM Systems Director Active Energy Manager, iSeries, Micro-Partitioning, POWER, PowerExecutive, PowerVM, PowerVM (logo), PowerHA, Power Architecture, Power Everywhere, Power Family, POWER Hypervisor, Power Systems, Power Systems (logo), Power Systems Software, Power Systems Software (logo), POWER2, POWER3, POWER4, POWER4+, POWER5, POWER5+, POWER6, POWER6+, POWER7, System i, System p, System p5, System Storage, System z, TME 10, Workload Partitions Manager and X-Architecture are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. If these and other IBM trademarked terms are marked on their first occurrence in this information with a trademark symbol (® or ™), these symbols indicate U.S. registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries.

A full list of U.S. trademarks owned by IBM may be found at: <http://www.ibm.com/legal/copytrade.shtml>.

Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.

AltiVec is a trademark of Freescale Semiconductor, Inc.

AMD Opteron is a trademark of Advanced Micro Devices, Inc.

InfiniBand, InfiniBand Trade Association and the InfiniBand design marks are trademarks and/or service marks of the InfiniBand Trade Association.

Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

IT Infrastructure Library is a registered trademark of the Central Computer and Telecommunications Agency which is now part of the Office of Government Commerce.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Linear Tape-Open, LTO, the LTO Logo, Ultrium, and the Ultrium logo are trademarks of HP, IBM Corp. and Quantum in the U.S. and other countries.

Linux is a registered trademark of Linus Torvalds in the United States, other countries or both.

Microsoft, Windows and the Windows logo are registered trademarks of Microsoft Corporation in the United States, other countries or both.

NetBench is a registered trademark of Ziff Davis Media in the United States, other countries or both.

SPECint, SPECfp, SPECjbb, SPECweb, SPECjAppServer, SPEC OMP, SPECviewperf, SPECcapc, SPECchpc, SPECjvm, SPECmail, SPECimap and SPECsfs are trademarks of the Standard Performance Evaluation Corp (SPEC).

The Power Architecture and Power.org wordmarks and the Power and Power.org logos and related marks are trademarks and service marks licensed by Power.org.

TPC-C and TPC-H are trademarks of the Transaction Performance Processing Council (TPPC).

UNIX is a registered trademark of The Open Group in the United States, other countries or both.

Other company, product and service names may be trademarks or service marks of others.

Revised December 2, 2010