z/OS 3.1 IBM Education Assistant

Solution Name: SETROPTS APPLAUDIT for successful logons

Solution Element(s): RACF

July 2023

Agenda

- Trademarks
- Objectives
- Overview
- Usage & Invocation
- Interactions & Dependencies
- Upgrade & Coexistence Considerations
- Installation & Configuration
- Summary
- Appendix

Trademarks

- See url http://www.ibm.com/legal/copytrade.shtml for a list of trademarks.
- Additional Trademarks:
  - “None”

Objectives

- Understand the current SETROPTS APPLAUDIT function
- Understand the various reasons that cause VERIFYs to be logged
- Understand what's under the administrator's control and what's under the application's control
- Understand how APPLAUDIT logging interacts with APPL class authorization logging
- Understand how to extend APPLAUDIT to UNIX applications
- Understand the RACF subsystem address space requirement

Overview

- Who (Audience)
  - Security administrators
  - Security auditors
- What (Solution)
  - Ability to satisfy regulatory requirements by logging successful logons and logoffs, with controls at the application level
- Wow (Benefit / Value, Need Addressed)
  - Ability to log these extremely critical actions
  - Additional help while performing forensic research on attacks
  - Prove compliance to regulations such as PCI-DSS

Usage & Invocation

- The existing SETROPTS APPLAUDIT function is used to log the start (‘signon’) and end (‘signoff’) of APPC transactions
- However, it actually works for other applications (e.g. TSO)
- We are formally testing, documenting, and supporting this behavior in z/OS 3.1.
- Some customers are aware of this and are using the function. Thus, we do not change its behavior without a compatibility switch.
- A new RACF class named OPTAUDIT is used to define ‘switch profiles’ that modify the behavior of RACF logging functions.
- Defining the APPLAUDIT.FOR.UNIX profile in the OPTAUDIT class and RACLISTing the class extends this support to UNIX applications, which are not currently supported.
- The RACF subsystem must be implemented in order to use this support. It contains the support to recognize the new profile, and react to changes for this, and future ‘switch profiles’.

When are VERIFYs logged?

- When SETROPTS AUDIT(USER) is active, and a password or phrase is changed, the request is logged
- When the (non-UNIX) application making the RACROUTE VERIFY call specifies LOG=ALL, the request is logged
- When the (non-UNIX) application making the RACROUTE VERIFY call specifies (or defaults to) LOG=ASIS, logging is at the discretion of RACF, and the customer
  - RACF: On failures, and on successful PassTicket evaluations and MFA fallbacks, the request is logged
  - Customer:
    - When SETROPTS APPLAUDIT is enabled, and the APPL class profile's logging options say to log successes, the request is logged. With APPLAUDIT.FOR.UNIX defined in the (new) OPTAUDIT class, the same is true for UNIX applications.
- When the application specifies LOG=NONE, no record is created **except** for password changes as in the first bullet.

When are VERIFYs logged? …

Session type/LOG=	LOG=NONE	LOG=ASIS	LOG=ALL
non-UNIX	No logging unless password change ([1])	• Failures • Password change • PassTicket authentication • MFA with password fallback • **APPLAUDIT ([2]) (causes reason=APPLAUDIT)**	Everything is logged
UNIX (SESSION=OMVS SRV or initACEE)	No logging unless password change	• Password change • Password failure • User revoked • MLQUIET error • SECLABEL error • **APPLAUDIT (when switch profile exists)**	• Password change • Password error • User revoked • MLQUIET error • SECLABEL error

Notes:

1. Password change assumes SETROPTS AUDIT(USER) is in effect
2. APPLAUDIT assumes RACLISTed APPL profile requests logging
3. ENVIR=CHANGE is not logged. ENVIR=DELETE (logoff) is reflected above, though many of the keyword combinations are n/a for DELETE.

What about the APPL check logging?

- The APPL profile logging options now come into play for both the APPL profile access check (driven internally by RACROUTE VERIFY), and the logon itself (via SETROPTS APPLAUDIT)
- When RACROUTE VERIFY performs the APPL authorization check, it specifies LOG=NOFAIL, so that only successes may be logged (as an Event Code 2 ACCESS record)
  - Failures are logged as an Event code 1 (JOBINIT) with a qualifier of 5 (“INVAPPL” in SMF Unload output), regardless of APPL profile options.

    ICH408I USER(TSOUSR4) GROUP(SYS1) NAME(T.S. USER)

    LOGON/JOB INITIATION - NOT AUTHORIZED TO APPLICATION TSOIM13
- Thus, turning on success logging can result in both an ACCESS and JOBINIT record for a single logon
  - The APPL authorization check, and thus successful ACCESS logging, is only driven when there is no matching ACEE found in the VLF cache. So, your mileage may vary.
  - The VLF cache is completely purged when the APPL class is RACLIST REFRESHed

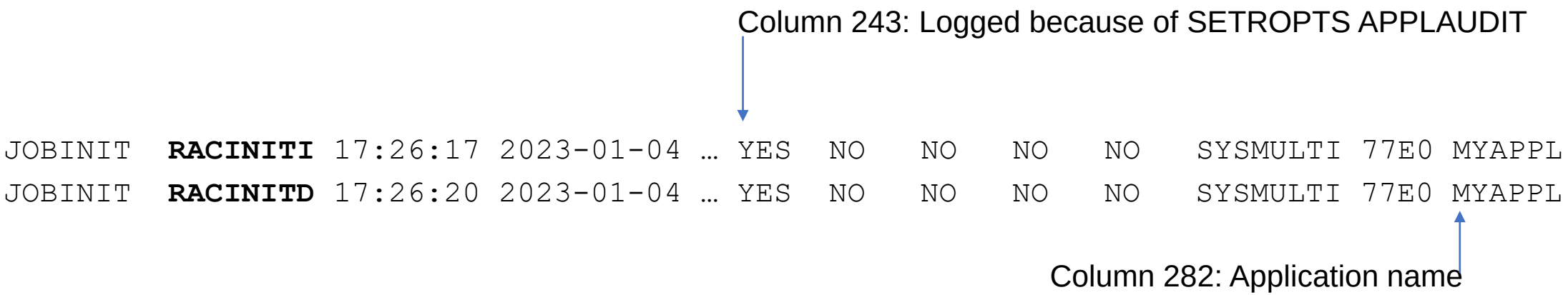
Usage & Invocation … Eligible applications

- Only applications that provide an application name to SAF are eligible for APPLAUDIT
- An application provides a name by:
  - Using the APPL= keyword of RACROUTE REQUEST=VERIFY/X
  - Providing a value for the APPL_id parameter of the initACEE callable service (IRRSIA00)
  - Using one of the UNIX services that take an application name and call one of the SAF services above: __passwd_applid(), __login__applid() and pthread_security_applid_np ()

- The application must specify (or take the default of) LOG=ASIS on RACROUTE REQUEST=VERIFY or VERIFYX.
- If the application specifies LOG=ALL, it is logged for that reason and APPLAUDIT is irrelevant

Usage & Invocation … What you get

- SMF Type 80 Event Code 1 (“JOBINIT”) records for the logon to and logoff from the application.
- For example, for logon, SMF Unload shows:



- Note that the profile logging also results in an SMF 80 Event Code 2 (“ACCESS”) record for successful access to the APPL profile at logon.
  - This check is bypassed when a VLF cache match is found for the user in the IRRACEE VLF class, so the ACCESS record will not always accompany the RACINITI/RACINITD records.

Usage & Invocation … How to enable it

- Make sure the RACF subsystem address space is running
- Issue `SETROPTS APPLAUDIT` from a user with the AUDITOR attribute
- Enable success logging in the APPL class profile. For example:
  - `RALTER APPL MYAPPL GLOBALAUDIT(ALL(READ))`
- RACLIST the APPL class if it is not already (RACLIST is not required for basic APPL protection, but is for APPLAUDIT):
  - `SETROPTS RACLIST(APPL)`
- To extend the support to UNIX applications (those that specify SESSION=OMVSSRV, including all callers of initACEE):
  - `RDEFINE OPTAUDIT APPLAUDIT.FOR.UNIX`
    - This **must** be a discrete profile
    - Its mere existence is the only significance of the profile: UACC, access list, logging options, etc. have no meaning/effect.
  - `SETROPTS CLASSACT(OPTAUDIT) RACLIST(OPTAUDIT)`

Usage & Invocation … OPTAUDIT class

ICHERCDE macro keyword
CLASS=OPTAUDIT
POSIT=609
CASE=UPPER
DFTRETC=4
DFTUACC=NONE
EQUALMAC=NO
FIRST=NONATNUM
OTHER=ANY
GENLIST=DISALLOWED
GENERIC=ALLOWED
ID=1
KEYQUAL=0
MAXLNTH=246
OPER=NO
PROFDEF=YES
RACLIST=ALLOWED
RACLREQ=YES (RACLIST required)
RVRSMAC=NO
SIGNAL=YES (ENF signal issued for changes)
SLBLREQ=NO

Usage & Invocation … RACF subsystem

- The subsystem now houses an ENF 62 listener
  - ENF 62 is issued by RACF when a RACLIST event occurs on a RACF class
- The listener will respond to a change in the OPTAUDIT class by seeing if APPLAUDIT.FOR UNIXPRIV is defined, and turning ON or OFF the RCVTAAUX bit, as appropriate.
  - RACROUTE REQUEST=VERIFY/X checks this bit to see if UNIX application logging is enabled.
- The ENF listener will only set RCVTAAUX if SETROPTS APPLAUDIT is enabled (RCVTAAPL)
  - So, it is important to enable SETROPTS APPLAUDIT prior to defining and activating APPLAUDIT.FOR.UNIX
  - If this was done in the wrong order, you will not observe the SMF records being created. This can be rectified by issuing SETROPTS RACLIST(OPTAUDIT) REFRESH.
- If the RACF subsystem is down when the OPTAUDIT class is RACLIST REFRESHed, RCVTAAUX will continue to retain its old value. It will be refreshed when the address space is started again.

Usage & Invocation … RACF subsystem …

- Status message for ENF listener issued when the subsystem starts up

```
IRRG010I (<) RSWJ SUBSYSTEM PROCESSING OF PARAMETER LIBRARY MEMBER
       IRROPTPW IS COMPLETE.
IRRG010I (<) RSWJ SUBSYSTEM PROCESSING OF PARAMETER LIBRARY MEMBER
       IRROPTW3 IS COMPLETE.
IRRC070I (<) RSWJ SUBSYSTEM XCF SERVER ESTABLISHED AS
       IRRRACF.NODE1.SYS1.
IRRC093I (<) RSWJ SUBSYSTEM ENF 62 LISTENER IS ESTABLISHED.
IRRC093I (<) RSWJ SUBSYSTEM ENF 86 LISTENER IS ESTABLISHED.
IRRB002I (<) INITIALIZATION COMPLETE FOR RSWJ SUBSYSTEM.
```

- And at shutdown

```
IRRB069I (<) RSWJ SUBSYSTEM STARTING SHUTDOWN PROCESSING.
IRRC055I (<) RACF REMOTE SHARING TCP LISTENER IS TERMINATING.
IRRC094I (<) RSWJ SUBSYSTEM ENF 86 LISTENER IS REMOVED.
IRRC094I (<) RSWJ SUBSYSTEM ENF 62 LISTENER IS REMOVED.
IRRB005I (<) RSWJ SUBSYSTEM TERMINATION IS COMPLETE.
IEF352I ADDRESS SPACE UNAVAILABLE
$HASP250 RSWJ PURGED -- (JOB KEY WAS DCAA97BD)
```

Usage & Invocation … RCVT

- The listener will turn ON or OFF an RCVT bit depending on the existence of a switch

Offset (dec)	Offset (Hex)	Type	Len	Name(Dim)	Description
…					
502	1F6	BITSTRING	4	RCVTOPTS	Options implemented using switch profiles
	1… ….			RCVTAAUX	SETROPTS APPLAUDIT is extended to UNIX applications
					Room for future switch profile options
506	1FA	CHARACTER	90	*	Reserved
…					

Usage & Invocation … Managing OPTAUDIT profiles

- SETROPTS APPLAUDIT and other system-level logging options require the AUDITOR attribute
- Consider allowing your auditors to manage the OPTAUDIT class
  - ALTUSER AUDGUY CLAUTH(OPTAUDIT)
  - CONNECT AUDGUY GROUP(AUDGRP) SPECIAL
  - RDEFINE OPTAUDIT APPLAUDIT.FOR.UNIX OWNER(AUDGRP)

Extending APPLAUDIT to UNIX applications

- Unix applications (those that specify SESSION=OMVSSRV) are currently only logged under specific circumstances.
- Note the following doc under TOKENBLD and VERIFY/X under the SESSION= keyword for OMVSSRV:

> An OMVS server application.
> When OMVSSRV is specified, user profile statistics are updated daily at most. **Audit records are only created when** one of the following conditions are met:
> - An incorrect password or password phrase is specified.
> - The user ID has been revoked.
> - A new password or password phrase was provided.
> - A security label error occurred

Interactions & Dependencies

- Software Dependencies
  - Conforming applications as described previously
- Hardware Dependencies
  - None
- Exploiters
  - Many applications (e.g. TSO) are already eligible.
  - Possibly, ISV products.

Upgrade & Coexistence Considerations

- To exploit this solution, all systems in the Plex must be at the new z/OS level: No
- SETROPTS APPLAUDIT works on all supported releases today!
  - There are two minor behavior changes only on 3.1, visible only if you were using the undocumented function:
    - The application name will also appear in the ‘logoff’ record (RACROUTE REQUEST=VERIFY,ENVIR=DELETE). This helps to match the logon and logoff.
    - When an application specifies LOG=ALL, it was possible on earlier releases for the SMF record to identify APPLAUDIT as the reason for logging, even though it wasn’t. On 3.1, APPLAUDIT will never be the reason for logging when LOG=ALL.
- The UNIX enablement is new, and only works on 3.1.
  - It’s fine to define APPLAUDIT.FOR.UNIX on a 3.1 system sharing with a downlevel system. It will not be recognized on the downlevel system.

Installation & Configuration

- List anything that a client needs to be aware of during installation and include **examples** where appropriate - clients appreciate these:
  - Make sure the RACF subsystem address space is implemented

Summary

- SETROPTS APPLAUDIT is only documented/supported for APPC
- But it works for other (non-UNIX) applications
- We are formally testing and documenting the full function in z/OS 3.1
- We also extend it to UNIX applications with a new switch profile named APPLAUDIT.FOR.UNIX in a new RACF class named OPTAUDIT
- The RACF subsystem address space is required to detect creation of this profile and subsequent changes (delete/disablement) to it
- An ENF listener in the RACF subsystem sets the RCVTAAUX bit, so programs can easily detect whether the UNIX support is enabled

Appendix

- Publications:
  - z/OS Security Server RACF Auditor’s Guide
  - z/OS Security Server RACF Command Language Reference
  - z/OS Security Server RACF System Programmer’s Guide
  - z/OS Security Server RACF Macros and Interfaces
  - z/OS Security Server RACF Data Areas
  - z/OS Security Server RACF Callable Services
  - z/OS Security Server RACF RACROUTE Macro Reference
  - z/OS Security Server RACF Messages and Codes