5 Minute Madness
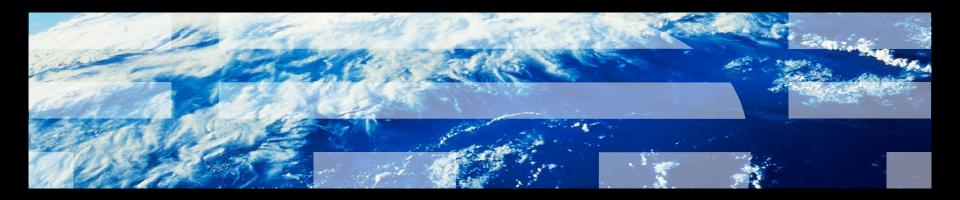
NY/Tampa/Dallas/RACF RACF® User Group

Mark Nelson, CISSP®, CSSLP®,IBM®

17 May, 2023

Recent Statements of Direction

Recent Statements of Direction

- Validated Boot for z/OS

  IBM plans to deliver a solution providing Validated Boot, also known as Secure Boot or Boot Integrity Validation, capability for z/OS IPLs and is designed to meet the requirements for achieving the National Information Assurance Partnership (NIAP) OS Protection Profile ~~4.2.1~~ 4.3 Certification.

- Encryption of tape data sets

  IBM intends to enhance pervasive encryption to perform encryption within the access methods for tape data sets. It is expected to be transparent to the application program unless it uses EXCP. This new data set encryption support is intended to be independent of any encryption that occurs in the tape subsystem.

UNMAP and Erase-on-Scratch

Erase on Scratch (EoS) : Enablement

- EoS was introduced with RACF 1.7 and MVS/XA DFP 2.1.0 (1985)

- Designed to address two threats:

    1. Applications which allocate data sets and read the residual data on the DASD space formerly occupied by a prior data set.

    2. Reading of data by having physical access to the storage device

- Performance improvements

    - z/OS V2.1 (up to 255 tracks erased per I/O)
    - z/OS V2.2 (up to 12,240 tracks erased per I/O)

- But there is still a significant performance impact for large data sets

Erase-on-Scratch: RACF Basics

– SETROPTS ERASE(ALL)

- Instructs DFSMSdfp to erase all scratched data sets, _including temporary data sets_, regardless of the erasure indicator in the data set profile

– SETROPTS ERASE(seclevel-name)

- Instructs DFSMSdfp to erase all scratched data sets that have a security level equal to or greater than seclevel-name

– SETROPTS SETROPTS ERASE or ERASE(NOSECLEVEL)

- RACF instructs DFSMSdfp to erase a scratched data set if the erasure indicator in the data set profile is on

– SETROPTS NOERASE

- No erase-on-scratch processing is to be performed, even if the data set erasure indicator is on in the data set profile

Erase-on-Scratch: The New Stuff

– DFSMSdfp APAR OA61492 introduces UNMAP support for DS8900 solid state drives (SSDs) which have DS8900 firmware release 9.3.2 installed

  – UNMAP provides *very substantial performance benefits* over traditional EoS.

  – Applies to data sets which have the ERASE indicator specified in the RACF profile or temporary data sets

  – *Does not apply to any data set in any form of Copy Services relationship*

– UNMAP is enabled by the presence of a FACILITY class profile named STGADMIN.SMS.DADSM.UNMAP.PREFER

  • If the profile above is present, and the data set is marked for erasure by either the data set profile and/or the SETROPTS ERASE setting and the data set resides on a SSD enabled for EoS, the storage will be UNMAPed instead of ERASEd.

  • Otherwise, traditional (X'00' overwrite) will be performed.

  • For temporary data sets, if the profile above is present and ERASE(ALL) is not in effect, when the data set is deleted its space will be UNMAPped. If the UNMAP is not successful, the data set will not be overwritten with X'00's

Erase-on-Scratch: The New Stuff – Where to Learn More

– https://www.ibm.com/support/pages/apar/OA61492

  – … and subsequent APAR https://www.ibm.com/support/pages/apar/OA63169

– SHARE presentation "Watson and Walker's 2023 zRoadshow", SHARE Atlanta 2023 Proceedings

– "Latest on Erase-on-Scratch and SSDs and the UNMAP Function", upcoming article Cheryl Watson's Tuning Letter, 2023, No.1

– DFSMS Storage Administration, https://www-40.ibm.com/servers/resourcelink/svc00100.nsf/pages/zOSV2R5sc236860/$file/idas200_v2r5.pdf

– DFSMS Using Data Sets: https://www-40.ibm.com/servers/resourcelink/svc00100.nsf/pages/zOSV2R5sc236855/$file/idad400_v2r5.pdf

– Requirement to extend support to data sets engaged in Copy Services relationship: https://ibm-sys-storage.ideas.ibm.com/ideas/DS80-I-198

5 Minute Madness

NY/Tampa/Dallas/RACF RACF® User Group

Mark Nelson, CISSP®, CSSLP®, IBM®

17 May, 2023