IBM Education Assistance

Solution Name: Elimination of user key common storage –

OA53355 / OA56180 / OA57908

Element(s)/Component(s): VSM / RSM

Agenda

- Trademarks
- Session Objectives
- Overview
- Installation
- Usage & Invocation
- Installation – Next steps
- Migration & Coexistence Considerations
- Session Summary
- Appendix

Trademarks

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

Session Objectives

- Reminder of the elimination of user key common storage
- Discuss how the VSM ALLOWUSERKEYCSA, ALLOWUSERKEYCADS and NUCLABEL ENABLE(IARXLUK2) settings affect potential impact
- Explain the use of 3 New Function APARs to help find current usage of user key common
  - Migration health check
  - SMF 30 records
  - SLIP trap
  - RSM Trace Function Option
- Introduce the Restricted Use CSA and explain how it can be used to provide increased data security

Overview

- Who (Audience)
  - All z/OS installations that may still be using user key CSA.
- What (Solution)
  - Tools are provided in service releases to enable the detection of any use of user key common storage.
- Wow (Benefit / Value, Need Addressed)
  - The functionality provided here can be used in all releases to help find the users of the user key common storage so they can be eliminated to ensure a more secure system.
  - Storage isolation can be used to limit the users with access to user key common storage. This option will be a separately orderable paid feature in z/OS 2.4.

Overview

As originally announced in July 2017

- Removal of support of YES setting for VSM ALLOWUSERKEYCSA DIAGxx parmlib parameter: z/OS V2.3 will be the last release of z/OS to support the YES setting for the ALLOWUSERKEYCSA DIAGxx parmlib parameter. If you run any software that requires the setting of this parameter to YES, the software will need to be changed to no longer require the setting of this parameter to YES. All IBM provided software should not require this setting. If you have any other non-IBM provided software that requires this setting, contact the owner of the software regarding this usage.
- Removal of support for obtaining user key CSA/ECSA storage: z/OS V2.3 will be the last release of z/OS to support the usage of the GETMAIN, CPOOL, and STORAGE OBTAIN interfaces to obtain user key (8-15) CSA/ECSA storage. If you have any software that obtains user key CSA/ECSA storage, the software will need to be changed to no longer require this capability.
- Removal of support for changing ESQA storage to user key: z/OS V2.3 will be the last release of z/OS to support the usage of the CHANGKEY interface to change ESQA storage to user key (8-15). If you have any software that changes ESQA storage to user key, the software will need to be changed to no longer require this capability.
- Removal of support for creating SCOPE=COMMON data spaces in user key: z/OS V2.3 will be the last release of z/OS to support the usage of the DSPSERV CREATE interface to create a SCOPE=COMMON data space in user key (8-15). If you have any software that creates a SCOPE=COMMON data space in user key, the software will need to be changed to no longer require this capability.

Overview

- Invocations to change
  - Using the STORAGE, GETMAIN or CPOOL service to obtain common ECSA/CSA storage (subpool 227, 228, 231, 241) that specifies a key of 8-15.
  - Using the DSPSERV service to allocate a SCOPE=COMMON data space in a key of 8-15.
  - Using the CHANGEKEY service to change the storage key of common storage to a key of 8-15.

Overview

To aid in finding all instances of user key common usage OA53355, OA56180 and OA57908 have introduced the ability to audit the usage of user key common

- Health check ZOSMIGV2R3_NEXT_VSM_USERKEYCOMM will trigger an exception when usage of user key common has been detected
- SMF Type 30 records are enhanced to identify jobs/steps that use user key common storage
- An instruction fetch SLIP can be set to trace any of the following accesses of user key common
  - Obtain user key common storage
  - Build a user key CADS
  - Change common storage to a user key
  - Release user key common storage
  - ChangeAccess user key common storage *
  - Protect/Unprotect user key common storage *
- RSM Function Trace Option RUCSAFLT identifies access attempts of user key common storage *

* these require the definition of a Restricted Use CSA (RUCSA) in order to detect

Installation

- If successfully running with the VSM ALLOWUSERKEYCSA and ALLOWUSERKEYCADS set to NO, and (at v2r3) the NUCLABEL ENABLE(IARXLUK2) specified then there's no need to do anything further.
- Apply PTFs for OA53355, OA56180 and OA57908 to your current systems.
- Activate the ZOSMIGV2R3_NEXT_VSM_USERKEYCOMM health check
  - Run long enough to execute all of your normal processing.
  - The health check will detect attempts to obtain, free or access user key CSA, change the key of ESQA storage to a user key, and creation of user key SCOPE=COMMON data spaces.
  - If no user key CSA activity is ever detected then there's no need to continue. Consider changing VSM ALLOWUSERKEYCSA and ALLOWUSERKEYCADS to NO and (at v2r3) specifying NUCLABEL ENABLE(IARXLUK2).
- Size the RUCSA area
  - The RUCSA is a new, optional area of storage located between CSA and PVT that exclusively contains user key common storage.
  - After running a typical system workload
    - Use RMF Monitor I VSTOR (or equivalent) report to determine amount of userkey CSA storage
    - Or use new fields defined in APAR (GDA_RUCSA_HWM and GDA_ERUCSA_HWM)
- Define the RUCSA area and IPL
  - Parmlib system parameter RUCSA=([xM],[yM]) defines the amount of storage (below and above the line, but not for userkey CADS) to be set aside for user key common requests.
  - Can only be defined at IPL
  - Once defined, all requests for user key common storage will come from this area.

Usage & Invocation

- Once the health check indicates an instance of user key common usage, the SMF records can be interrogated to determine who used it.

  SMF type 30 records have been enhanced to report all attempted use of user key common storage.
  - SMF30_RaxFlags flag byte
    - SMF30_UserKeyCommonAuditEnabled x'80' - Auditing of user key common was active
    - SMF30_UserKeyCsaUsage x'40' - Attempts to obtain user key CSA were made
    - SMF30_UserKeyCadsUsage x'20' - Attempts were made to create a user key CADS
    - SMF30_UserKeyChangKeyUsage x'10' - Attempts were made to change CSA to a user key
    - SMF30_UserKeyRuCsaUsage x'08' - Attempts were made to obtain, reference, free or change the attributes of storage in the RUCSA

Usage & Invocation

- The following SLIP trap can be enabled to produce GTF trace records to help identify the users of user key common
  - SLIP SET,IF,A=TRACE,ID=UKEY,NUCEP=(IARXLUK4,0,1),TRDATA=(STD,REGS,0R?,+7.+5R?,+FF),END
  - In the resulting GTF trace entry
    - See documentation of OA56180 for an explanation of the output values.

Usage & Invocation

- The RSM Component Trace with Function Option RUCSAFLT can be activated to trace access attempts of storage located in the RUCSA area.
  - The resulting trace records will include the faulting VSA and faulter's PSWE
  - If a dump is required to determine the software in question
    - Run with NUCLABEL ENABLE(IARFSRCF) set in the active DIAGxx
      - This will cause an ABENDC0D RSN05005C00 on any fault in the RUCSA when not SAF-authorized to access the RUCSA
    - SLIP on the ABEND to produce an SVC dump

```
SLIP SET,ID=C0DA,C=C0D,A=SVCD,RE=05005C00,SDATA=(ALLNUC,LPA,LSQA,PSA,RGN,SQA,
   ALLPSA,NUC,TRT,CSA,SUM,SWA),END
```

Installation – next steps

- Eliminate detected uses of user key common wherever possible
  - The use of the RUCSA area will be a separately orderable paid feature in z/OS 2.4
- Authorize the users that still require use of user key common
  - Permit SAF READ authority to FACILITY class resource IARRSM.RUCSA

```
RDEFINE FACILITY IARRSM.RUCSA UACC(NONE)
PERMIT IARRSM.RUCSA CLASS(FACILITY) ID(userid) ACCESS(READ)
```

- Change DIAGxx specifications for ALLOWUSERKEYCSA and ALLOWUSERKEYCADS to NO and (at v2r3) specify NUCLABEL ENABLE(IARXLUK2). ReIPL.
- Only SAF-authorized users can now obtain or access user key storage
  - Unauthorized users will be ABENDed
    - ABEND0C4-10 for access failures
    - ABENDBxx-5C for obtain/free requests
    - ABEND6C5-xx0340xx for IARVSERV CHANGEACCESS
    - ABEND18A-xx0705xx for PGSER PROTECT
    - ABEND18A-xx0805xx for PGSER UNPROTECT

Migration & Coexistence Considerations

- Consider lowering the CSA by same amount as the specified RUCSA value – system may not IPL if there is not enough PVT
  - No different than when you specify too much CSA
- Enable health check ZOSMIGV2R3_NEXT_VSM_USERKEYCOMM in order to identify user key common storage usage
  - Indicates whether any user key common storage usage has been detected

Session Summary

- Standard support for the use of user key common storage has been removed in V2R4.
- For those impacted sites several methods have been created to help find the usage including
  - Migration health check
  - SMF30 records
  - Common instruction for SLIP invocations
  - RSM Trace Function Option RUCSAFLT
- A new memory area, the RUCSA, has been created to allow enhanced security for usage that can’t be eliminated.

Appendix

- References

  - 'Prepare for the removal of support for user key common areas' section of the z/OS Migration book

  - Use the closing information for OA53355, OA56180 and OA57908
    - Pub updates for OA56180 http://publibz.boulder.ibm.com/zoslib/pdf/OA56180.pdf

  - z/OS MVS Product Management for information regarding product registration at z/OS 2.4 and above.