zedTALKS

May 2016 RACF Options Survey Responses

Presented by

Richard K. Faulhaber

rkf@newera.com twitter: @faulhaber_rk

April 2016 RACF Password Environment Survey Responses

AE2

z/Auditing Essentials

VOLUME 2

Taming RACF – SETROPTS

http://www.newera-info.com/eBooks.html

z/Auditing Essentials

VOLUME 2

Mastering CA ACF2 – GSO

z/Auditing Essentials

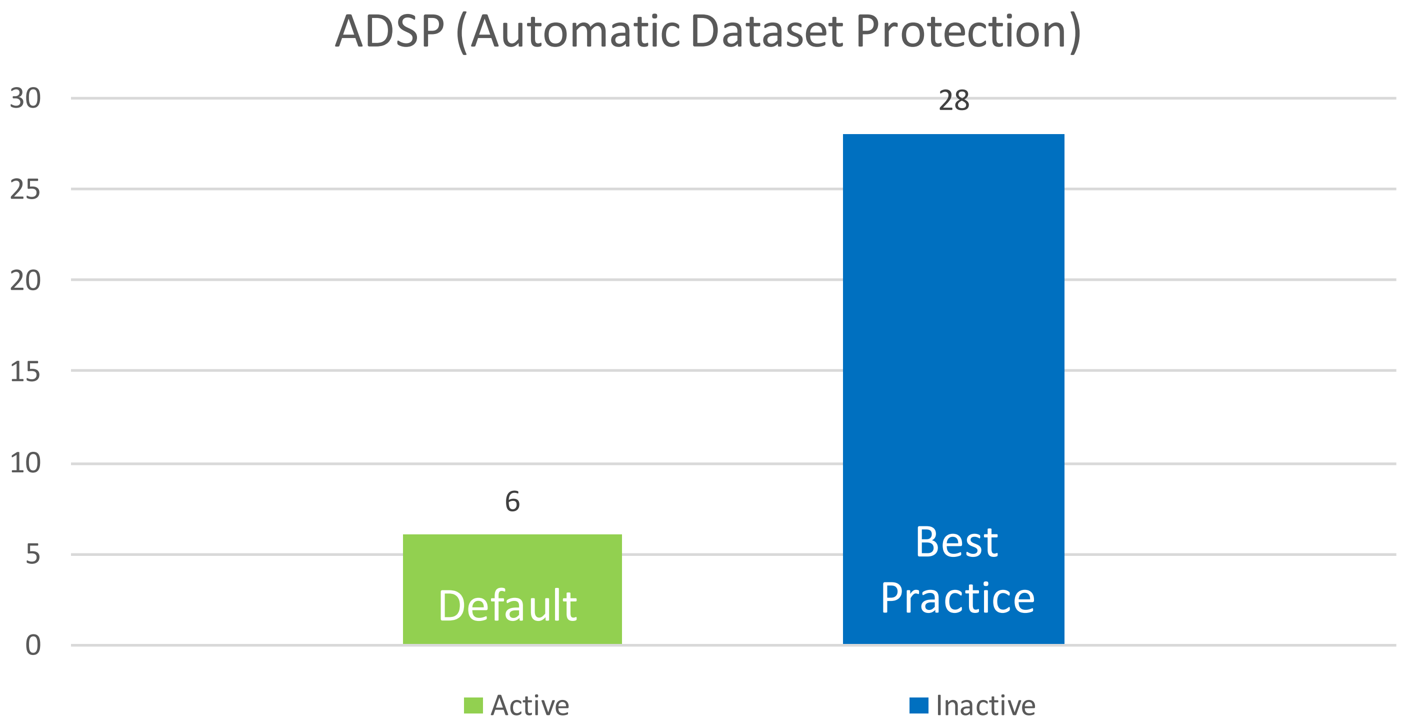
VOLUME 2

Controlling CA Top Secret

May 2016 RACF Options Survey Responses

Is the Automatic Dataset Protection option active (ADSP) or inactive (NOADSP)?

- Specifies that data sets created by users who have the ADSP attribute is RACF-protected automatically.
- Best Practice: ADSP should be turned OFF.
- The Point: Much less efficient than using generic profiles, which can be used to protect more than one dataset.



- Per IBM: “Because ADSP forces the creation of a discrete profile for each data set created by users who have the ADSP attribute, you should normally specify NOADSP if you specify GENERIC.”

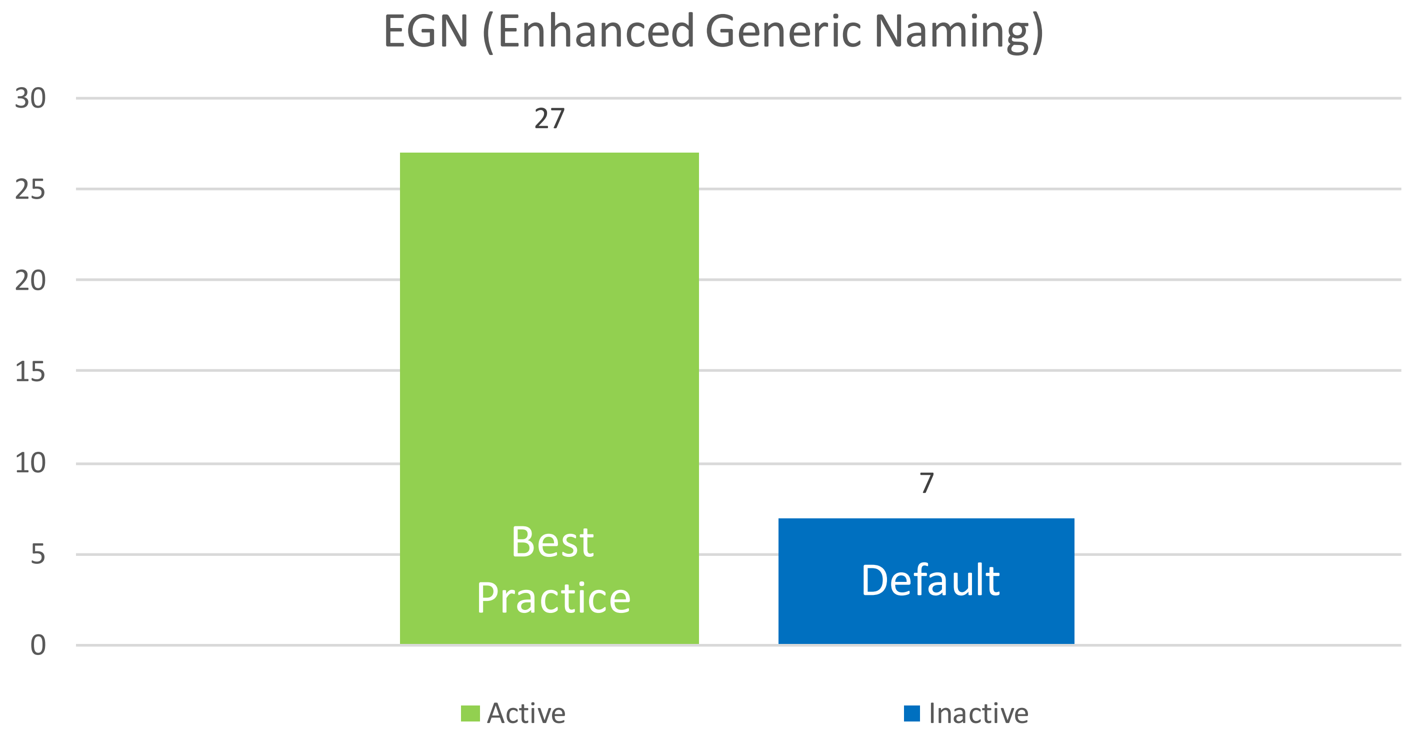
May 2016 RACF Options Survey Responses

Is the Enhanced Generic Naming option active (EGN) or inactive (NOEGN)?

- EGN allows the use of the generic character ** (as well as * and %) when defining dataset profile names and entries in the global access checking table.

- Best Practice: Should be turned on (and never turned off).

- The Point: "EGN should be enabled in order to take advantage of the more granular implementation of dataset protection available in RACF."



- Per IBM: "**Guideline:** Do *not* deactivate enhanced generic naming **after** data set profiles have been created while enhanced generic naming was active."

(Source: https://www.ibm.com/support/knowledgecenter/SSLTBW_2.1.0/com.ibm.zos.v2r1.icha700/icha700_Activating_enhanced_generic_naming_for_the_DATASET_class__EGN_option_.htm)

May 2016 RACF Options Survey Responses

EGN (Enhanced Generic Naming)

- Per IBM: “**Guideline:** Do *not* deactivate enhanced generic naming **after** data set profiles have been created while enhanced generic naming was active.”

  (Source: https://www.ibm.com/support/knowledgecenter/SSLTBW_2.1.0/com.ibm.zos.v2r1.icha700/icha700_Activating_enhanced_generic_naming_for_the_DATASET_class__EGN_option_.htm)

Important:
If you protect data sets with generic profiles while EGN is active and then deactivate this option, your resources can no longer be protected. Table 1 and Table 2 show examples of generic profiles created with enhanced generic naming active.
(Tables found on this page: https://www.ibm.com/support/knowledgecenter/en/SSLTBW_2.1.0/com.ibm.zos.v2r1.icha400/ich2a40030.htm#ich2a400-gen31__egn1)

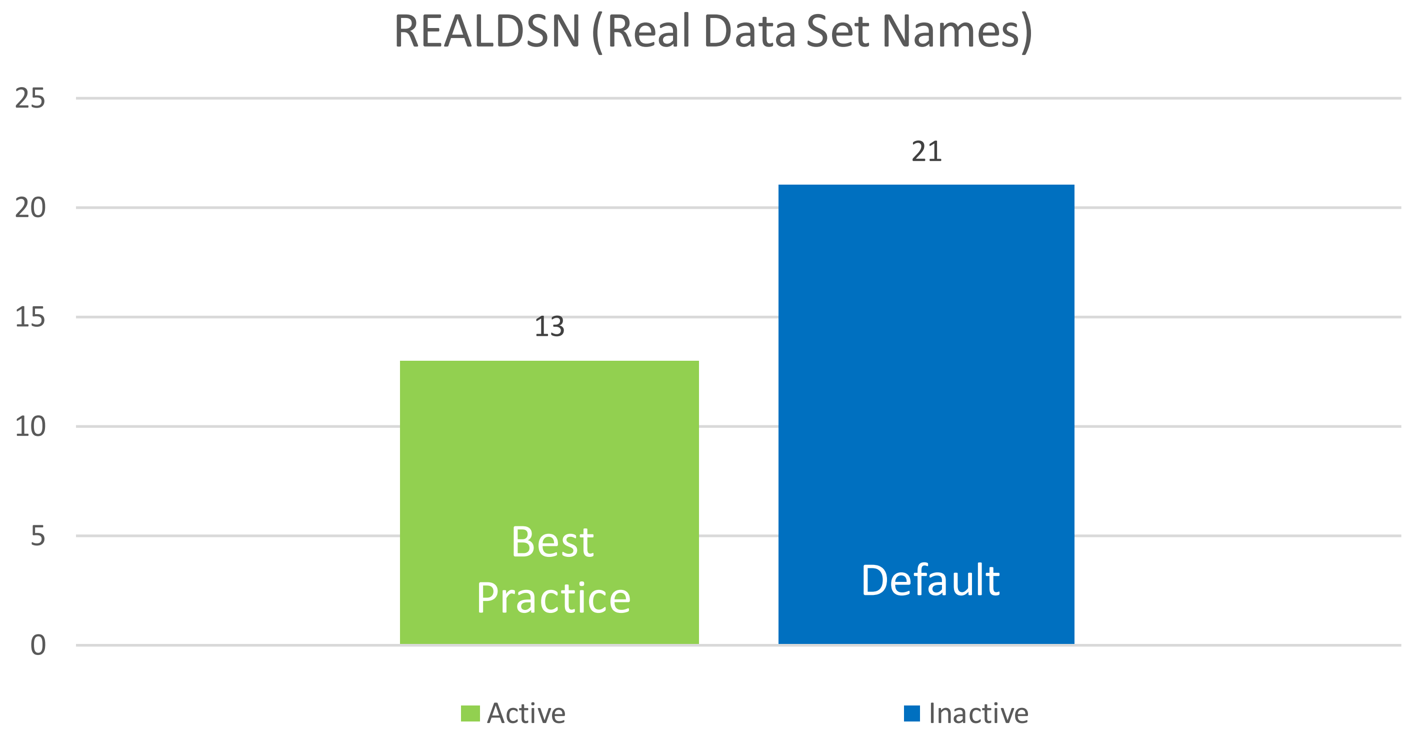
Some of these profiles do not provide RACF protection when the option is deactivated. If a data set is unprotected when EGN is deactivated, you can protect the data set with a discrete profile - as described in Naming considerations for resource profiles z/OS Security Server RACF Command Language Reference
(Link: https://www.ibm.com/support/knowledgecenter/en/SSLTBW_2.1.0/com.ibm.zos.v2r1.icha400/names.htm#names)
- either before or after the option is deactivated, or with a generic profile after the option is deactivated.

Source: (https://www.ibm.com/support/knowledgecenter/SSLTBW_2.1.0/com.ibm.zos.v2r1.icha400/setropts.htm)

May 2016 RACF Options Survey Responses

- REALDSN causes the REAL dataset name to appear in both logs and messages even if the dataset resource name is changed.
- Best Practice: "**REALDSN should be ACTIVE** to make it easier to monitor who is doing what to which resources."
- The Point: Enabling REALDSN makes it easier to monitor and audit what is actually taking place on your system(s).

Is the Real Data Set Names option active (REALDSN) or inactive (NOREALDSN)?



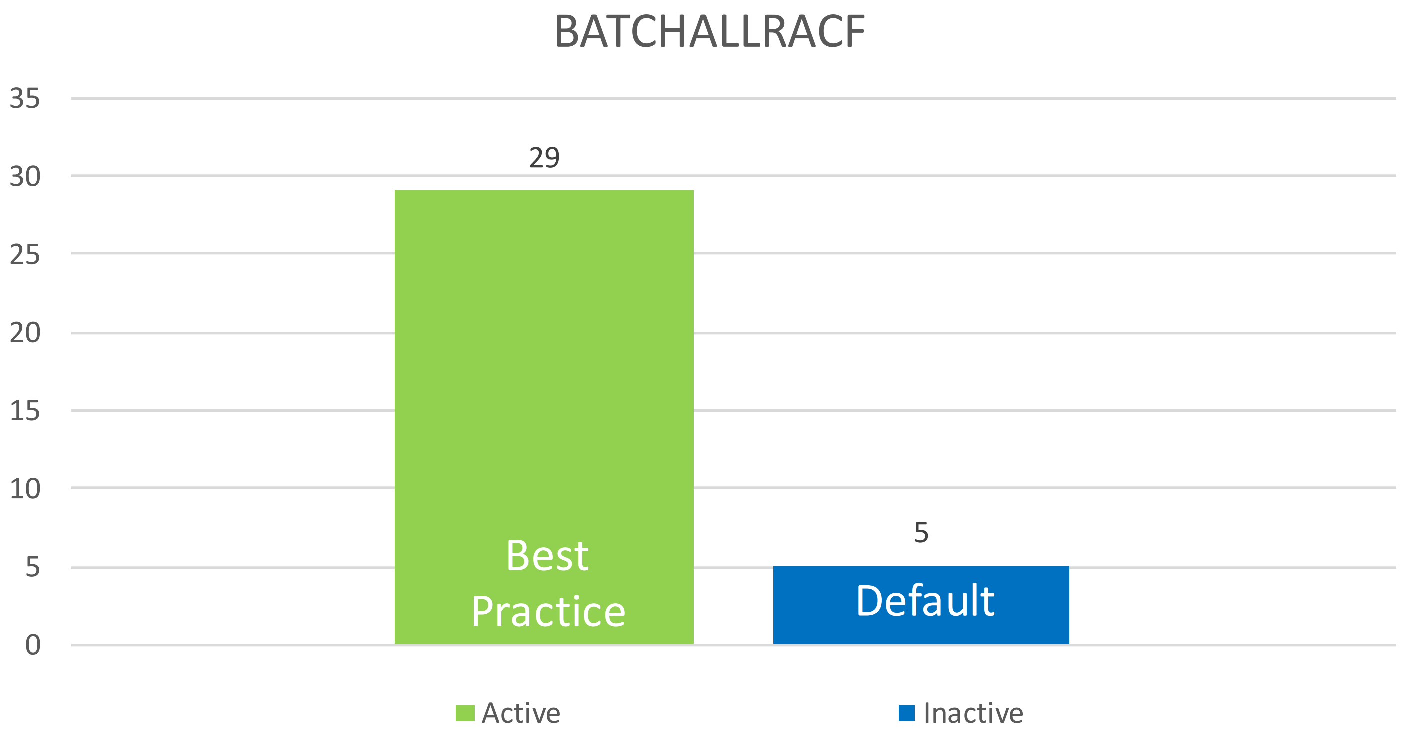
May 2016 RACF Options Survey Responses

Is the JES-BATCHALLRACF option active (BATCHALLRACF) or inactive (NOBATCHALLRACF)?

- BATCHALLRACF causes JES to test for a user ID and password on the job statement or for propagated RACF identification info for all batch jobs. If the test fails, JES fails the job.

- Best Practice: BATCHALLRACF should be enabled.

- The Point: It is important to turn this on so that batch jobs are controlled by RACF. Not doing so represents a security risk, allowing the activities of a would be hacker to be "invisible" to RACF.



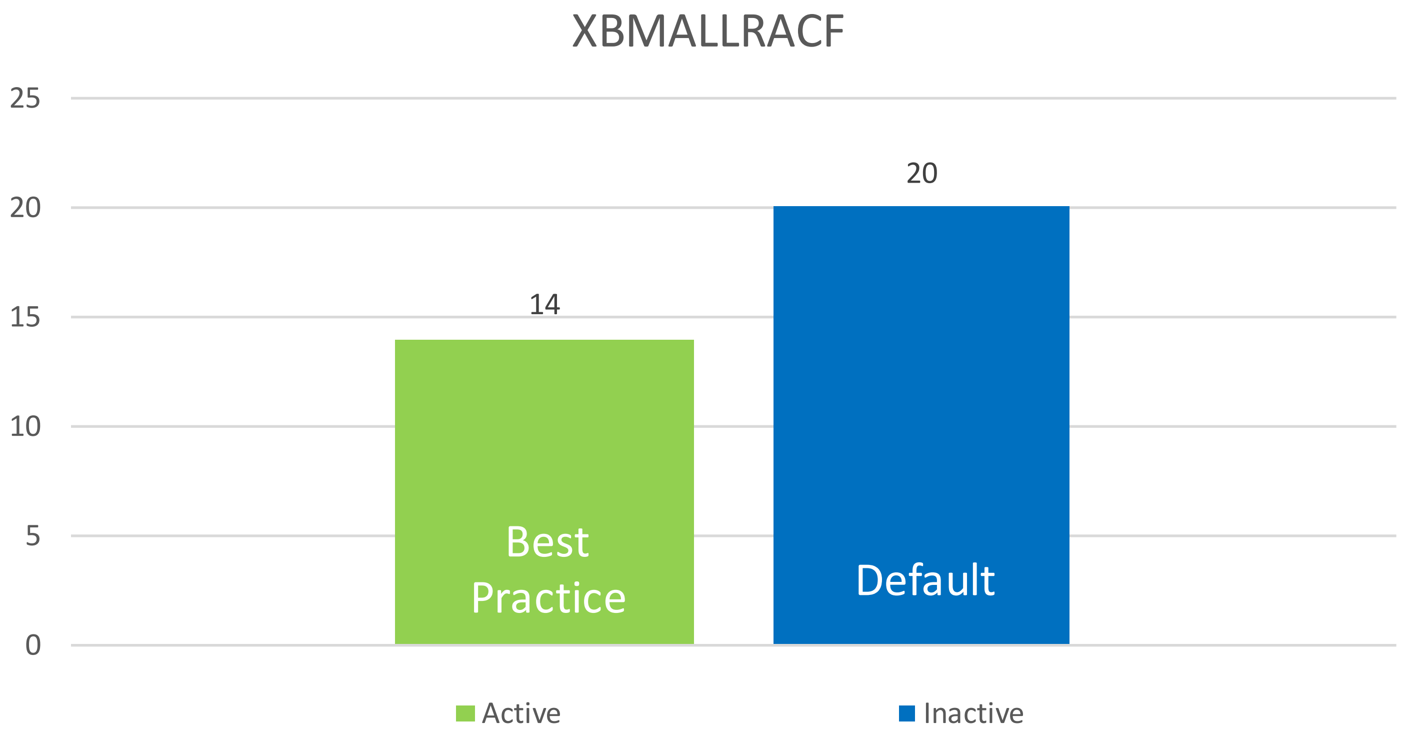
May 2016 RACF Options Survey Responses

- XBMALLRACF causes JES to test for user ID and password on the JOB statement or JES-propagated RACF ID info for all jobs run with an XBM. Only valid for XBM (eXecution Batch Monitor) jobs through JES2.

- Best Practice: Should be switched on.

- The Point: Should be turned on as it could potentially be exploited by a hacker. Even though it is only used by JES2 for XBM jobs, it should probably be turned on anyway in case the issue is raised in an audit.

Is the JES-XBMALLRACF option active (XBMALLRACF) or inactive (NOXBMALLRACF)?



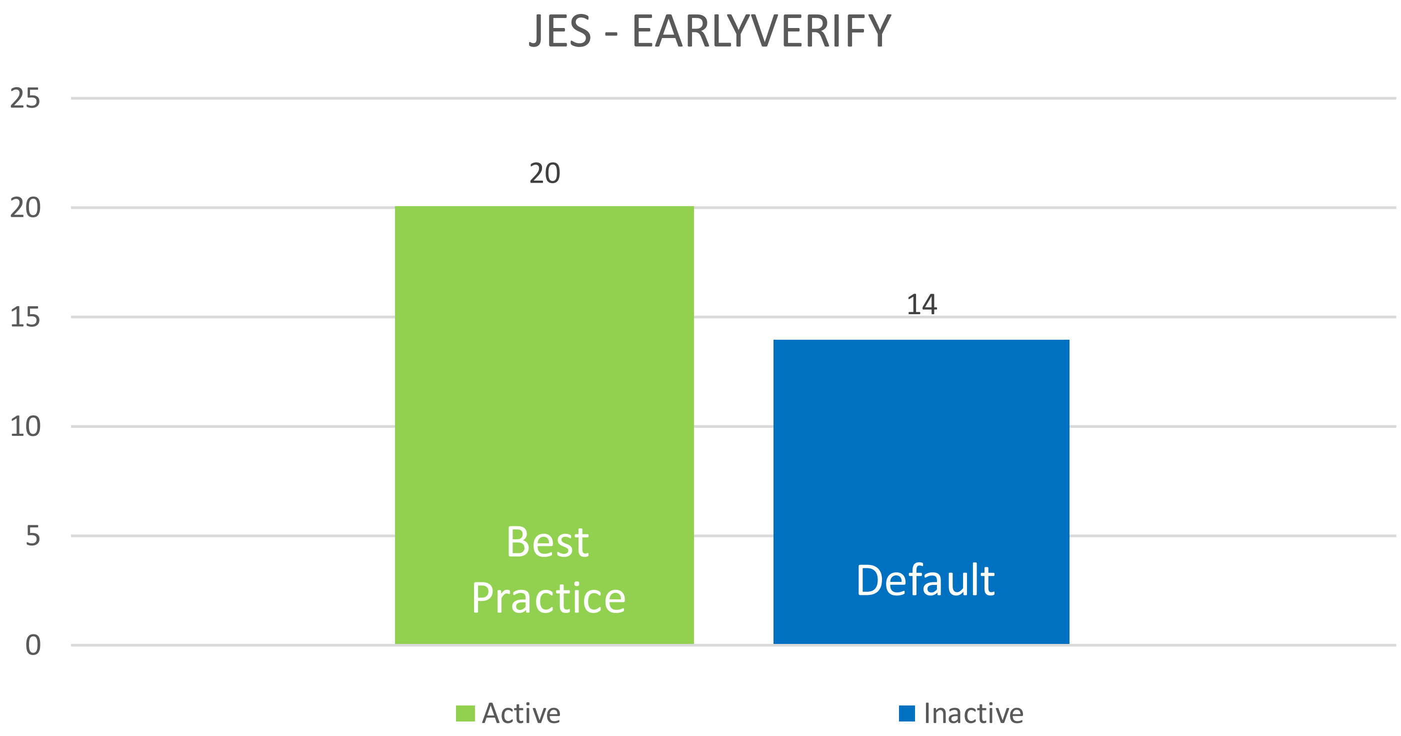
May 2016 RACF Options Survey Responses

Is the JES-EARLYVERIFY option active (EARLYVERIFY) or inactive (NO EARLYVERIFY)?

- This setting is ignored. Of historical significance, only.

- Best Practice: Should be turned on purely to avoid confusion during audits.

- The Point: Per IBM's own documentation, this setting is ignored. Though that is the case, it should be switched on to avoid confusion during audits.



- Per IBM: "Early verification is always done, even if the SETROPTS command has been issued with JES(NOEARLYVERIFY) specified."

Source: (https://www.ibm.com/support/knowledgecenter/SSLTBW_2.1.0/com.ibm.zos.v2r1.icha700/early.htm)

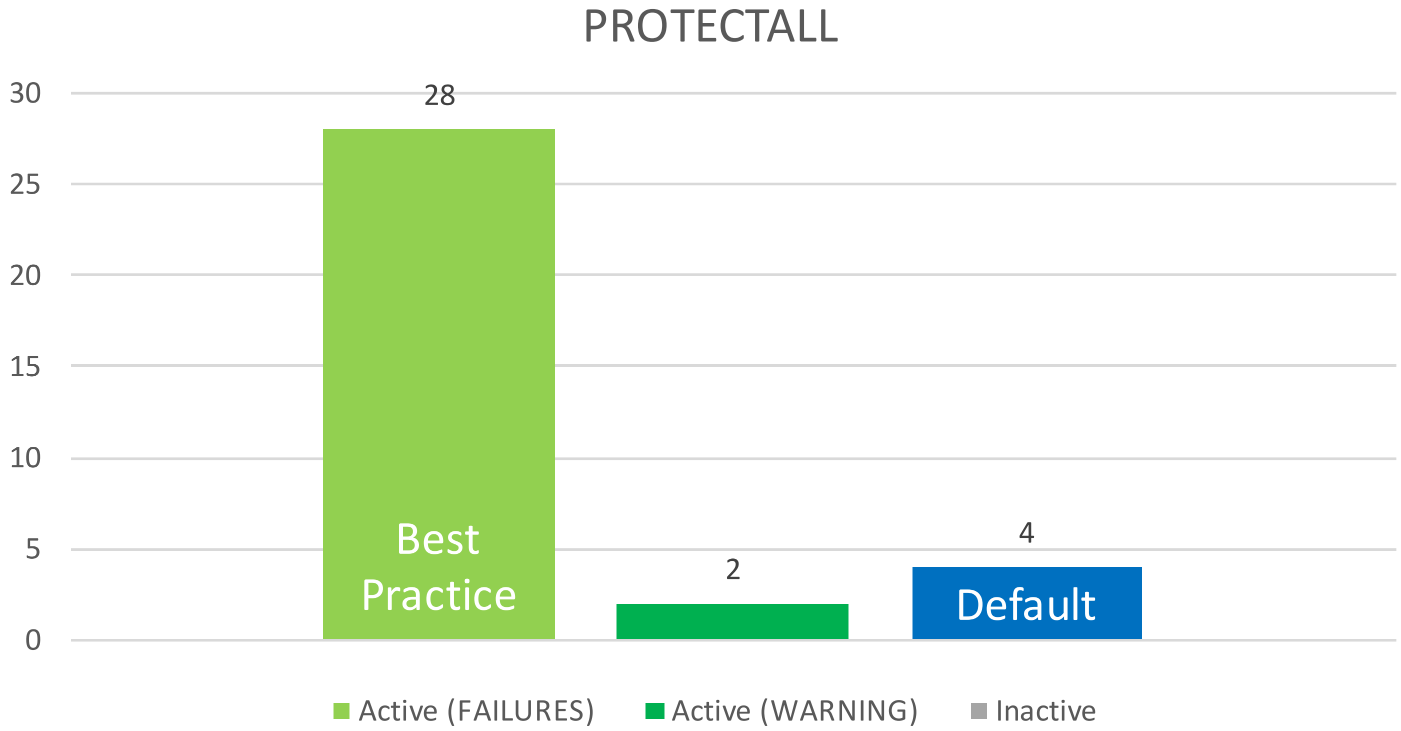
May 2016 RACF Options Survey Responses

- PROTECTALL causes the system to automatically reject requests to create or access datasets that are not RACF-protected.

- Best Practice: Should be active and set to FAIL.

- The Point: PROTECTALL(FAILURES) should be active. When it is disabled, all users, groups, etc… would have unrestricted access to all datasets, unless they are specifically denied.

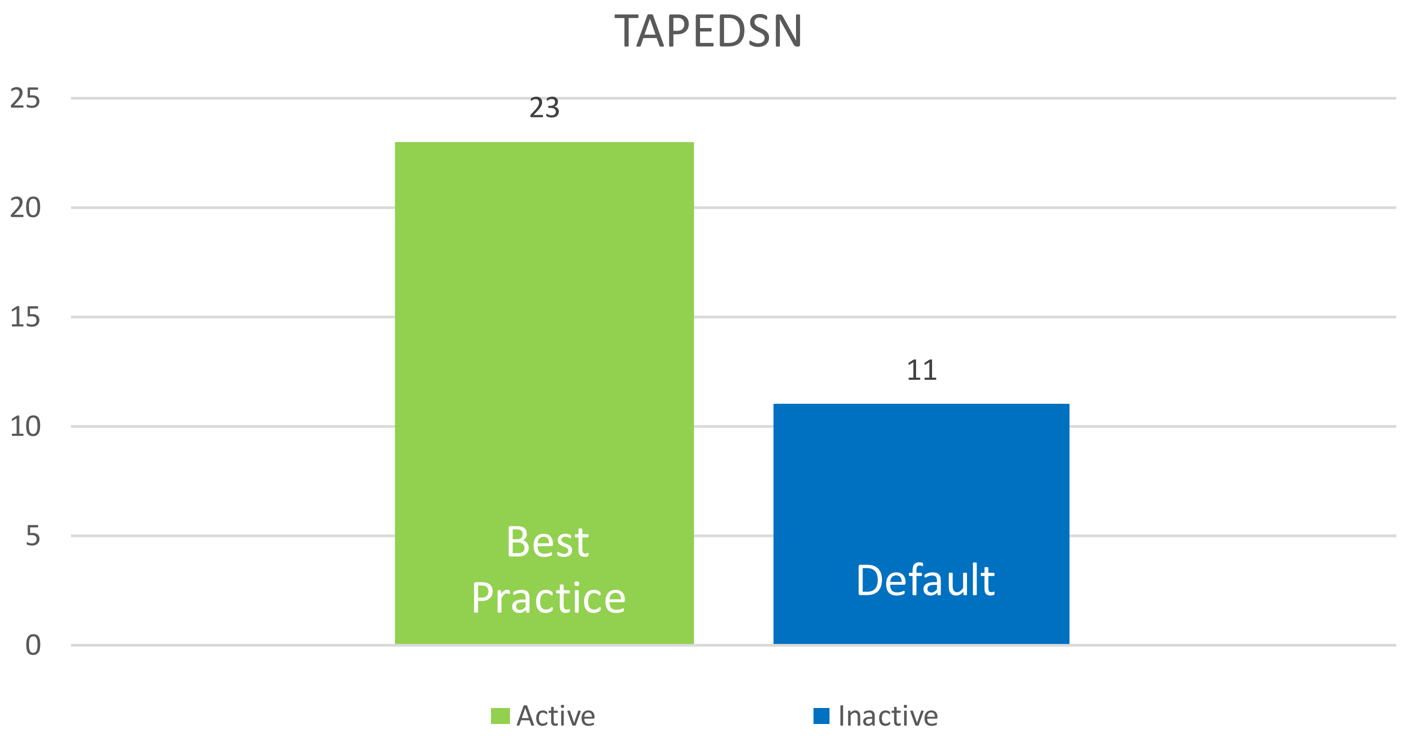
Is the PROTECTALL option active (PROTECTALL) or inactive (NOPROTECTALL)?
If it is active, is the sub-parm set for FAILURES or WARNING?



May 2016 RACF Options Survey Responses

Is the Tape Dataset Protection option active (TAPEDSN) or inactive (NOTAPEDSN)?

- TAPEDSN causes RACF to protect individual tape datasets as well as tape volumes.
- Best Practice: TAPEDSN should be active.
- The Point: TAPEDSN should be set active so as to close a potential security weakness that a hacker could exploit.



- Per IBM: “**Guideline:** If you use a tape management system, such as DFSMSrmm, do not enable TAPEDSN. For more information, see Using DFSMSrmm with RACF.”
  https://www.ibm.com/support/knowledgecenter/en/SSLTBW_2.1.0/com.ibm.zos.v2r1.icha700/usermm.htm

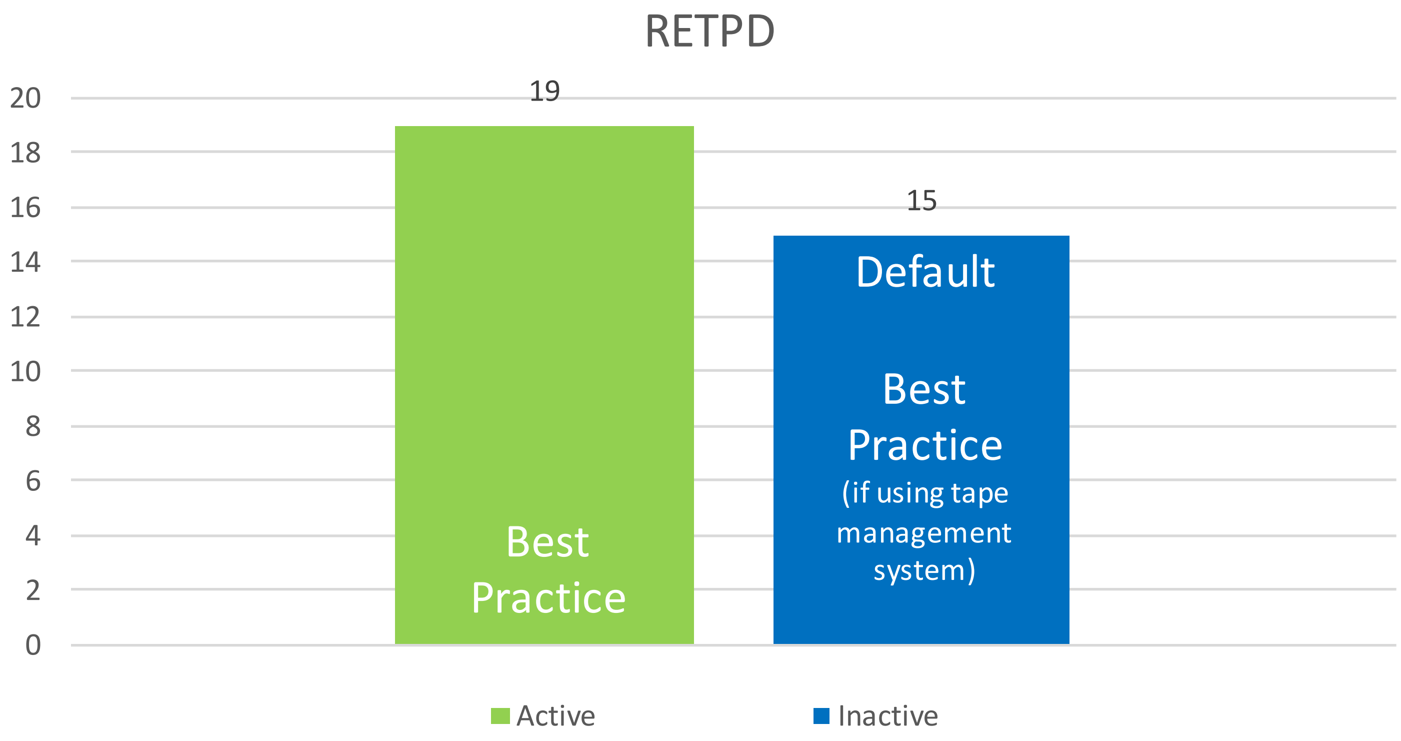
May 2016 RACF Options Survey Responses

Is the Security Retention Period option set? If so, what is its numeric value?

- RETPD with its value establishes the number of days RACF protection remains in effect for a tape dataset. Value may be 0 through 65533, or 99999 for never expire.

- Best Practice: RETPD(0) is ok if a tape management system is being used. Never expire (99999) is common as it is the DISA STIG requirement.

- The Point: If this value is set to the default, 0, the function is turned off so that it can be managed by a tape management system. TAPEDSN must be activated, otherwise the value of RETPD is meaningless.

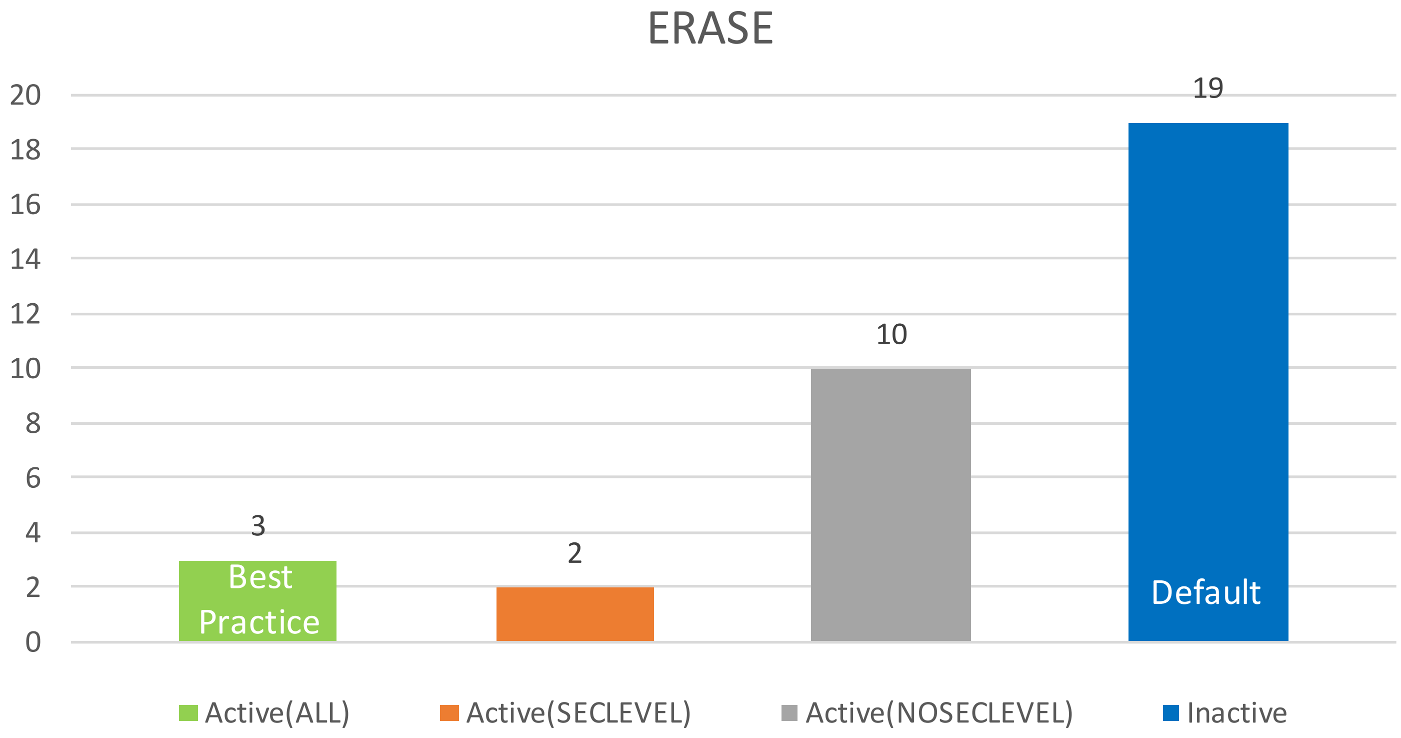


Values: 5 -> 9999
3 -> 99999 [never expire]
4 -> 0 [inactive]

May 2016 RACF Options Survey Responses

- Determines how data management is to erase contents of deleted datasets, and scratched or released DASD extents, by overwriting contents with zeroes.
- Best Practice: Should be set to ERASE(ALL) unless this causes performance issues. In that case, it can be applied at a more granular level.
- The Point: It is important to have this enabled so that confidential datasets cannot be read by unauthorized users even after they have been deleted.

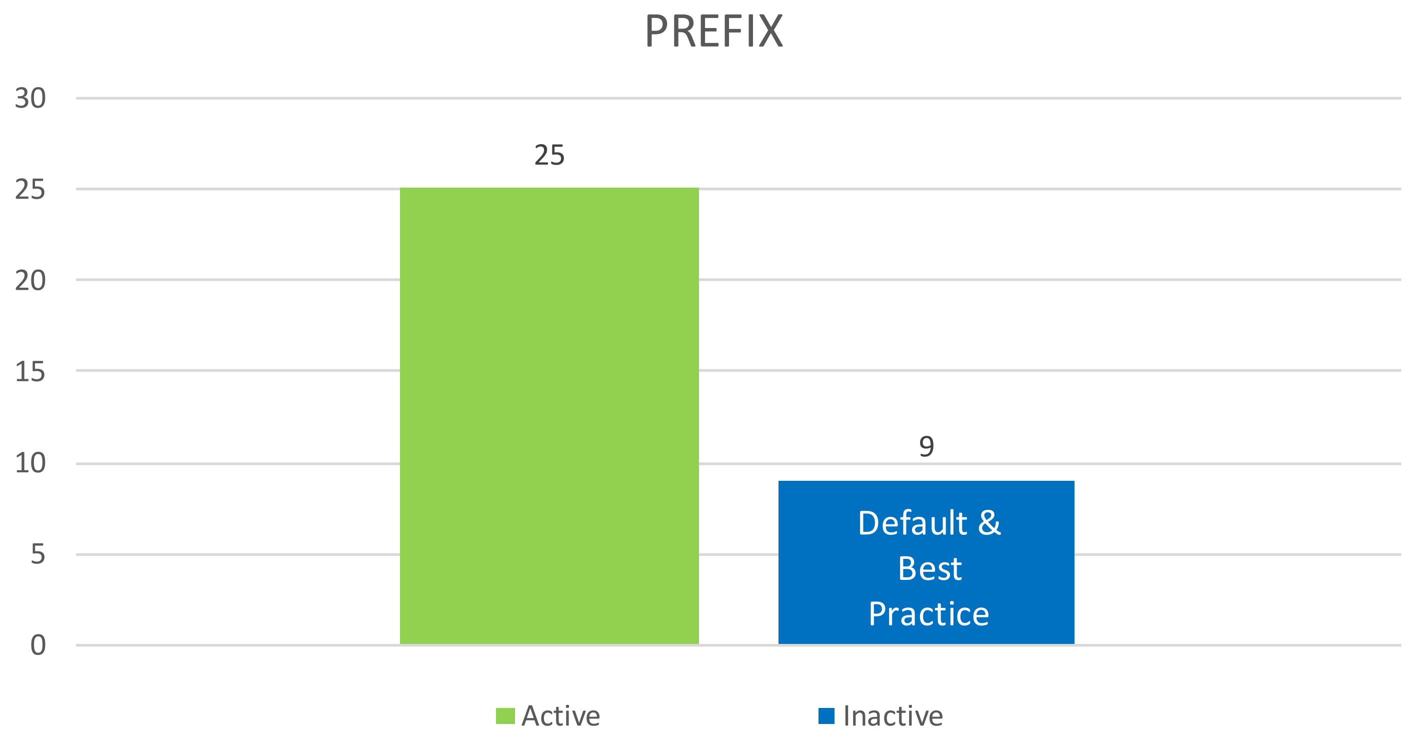
Is the Erase On Scratch option set to active (ERASE) or inactive (NOERASE)?
If it is active, which sup-operand is set? ALL, SECLEVEL, or NOSECLEVEL?



May 2016 RACF Options Survey Responses

- Activates RACF protection for datasets with single-qualifier names. Specifies the prefix to be used as the prefix (1-8 characters) to be used as the HLQ in the internal form of the names.
- Best Practice: Should be turned off. (NOPREFIX).
- The Point: Though AE2 may suggest that it “represents extremely bad practice” to create single level dataset names, some site standards may prefer it, in some cases.

Is the Single Level Name option set to active (PREFIX) or inactive (NOPREFIX)?



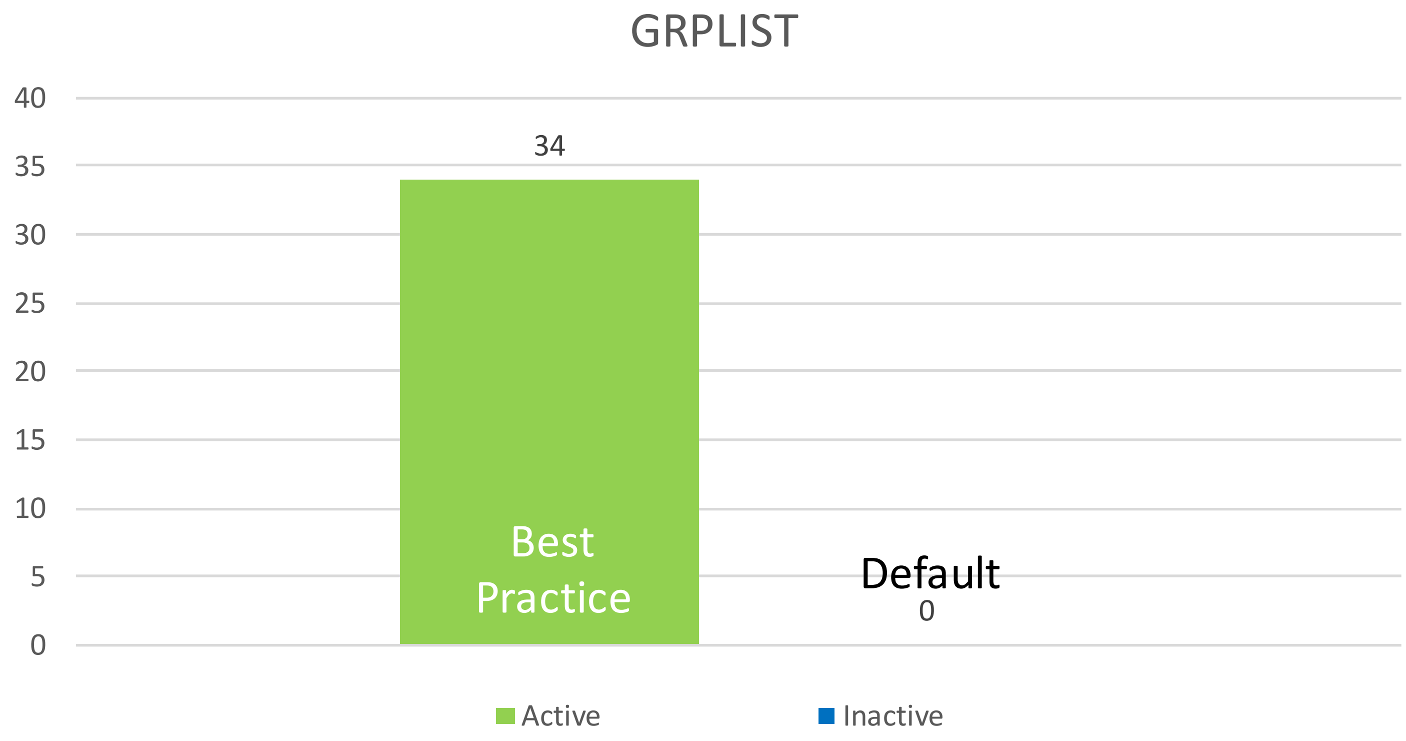
May 2016 RACF Options Survey Responses

- If list-of-groups checking is active, then regardless of which group the user is logged on to, RACF recognizes the user's group-related authorities in other connect groups. If a user is in more than one group and tries to access a resource, RACF uses the highest authority allowed by the user's list of groups and the resource's access list.

- Best Practice: Should be active.

- The Point: The GRPLIST option makes managing a user's access to resources much simpler.

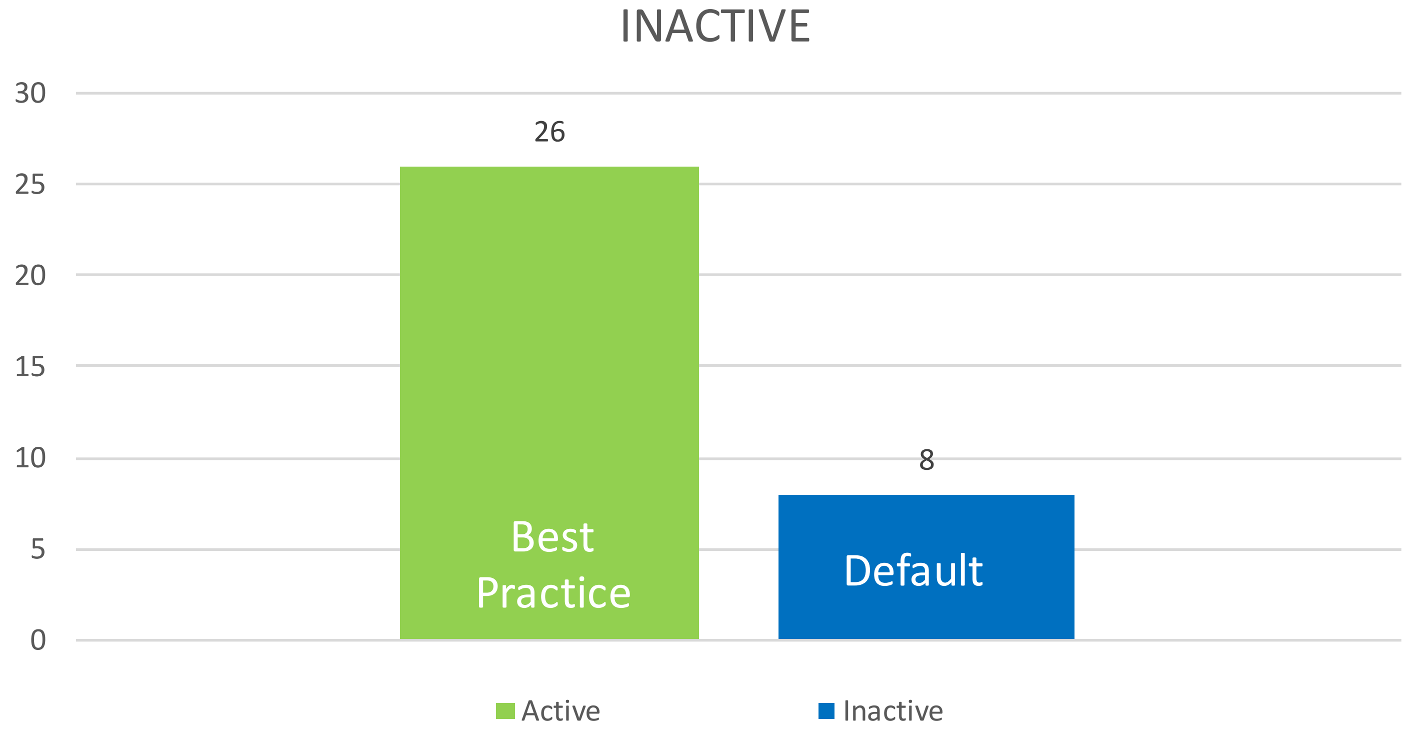
Is the List of Groups Access Checking option set to active (GRPLIST) or inactive (NOGRPLIST)?



May 2016 RACF Options Survey Responses

- Specifies the number of days (1-255) a user ID can remain unused and still be considered valid.
- Best Practice: INACTIVE should be enabled. Value of 1-35 is acceptable. 30 days is common.
- The Point: INACTIVE may not guarantee an unused USERIDs cannot be used. It does ensure that manual intervention by an Admin is required before that is allowed.

Is the Inactive UserIDs Automatically Revoked option set with INACTIVE or NOINACTIVE? If it is set with INACTIVE, for how many days is the unused-userid-interval set?

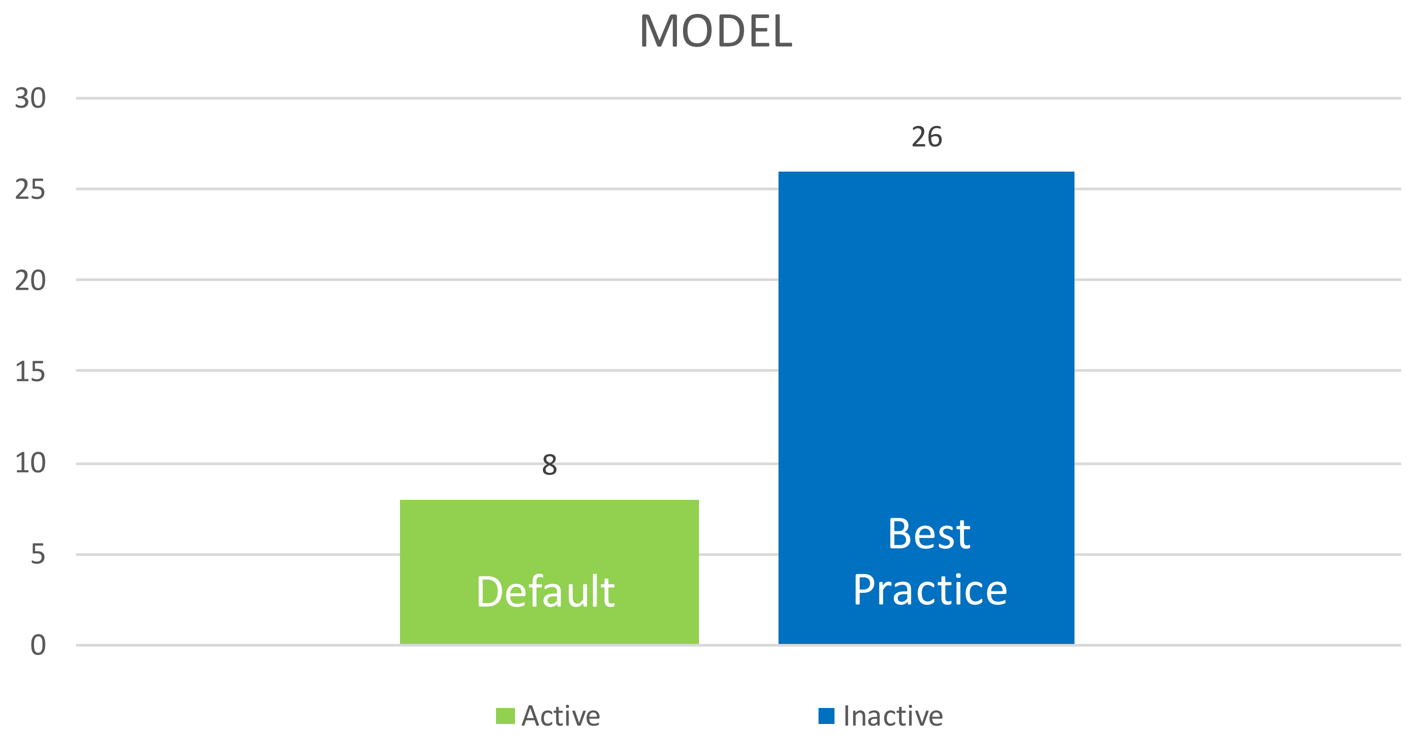


Values: 3 -> 120 days
1 -> 100 days
8 -> 90 days
4 -> 60 days
3 -> 45 days

May 2016 RACF Options Survey Responses

- Allows for the creation of new dataset profiles based on existing (model) profiles.
- Best Practice: Modelling should not be in effect.
- The Point: Dataset modeling is considered out of date and is not recommended. Because it allows for copying info from an existing (model) profile, it is not as rigorous a method of security as is having to make individual decisions each time a DATASET resource definition is created in the RACF database.

Is the Dataset Modeling option set to active (MODEL) or inactive (NOMODEL)? If active, please specify in the comments how the sup-operands are set.



April 2016 RACF Password Environment Survey Responses

RACF Survey for June 2016… RACF Data Processing Options:

PASSWORD_IS_IN_EFFECT_FOR_THE_SWITCH
PASSWORD_IS_IN_EFFECT_FOR_THE_STATUS
SECLEVELAUDIT
SECLABEL_AUDIT
SECLABEL_CONTROL
GENERIC_OWNER_ONLY
COMPATIBILITY_MODE
MULTI-LEVEL_QUIET
MULTI-LEVEL_STABLE
NO_WRITE-DOWN
MULTI-LEVEL_ACTIVE
CATALOGUED_DATA_SETS_ONLY

USER-ID_FOR_JES_NJEUSERID
USER-ID_FOR_JES_UNDEFINEDUSER
PARTNER_LU-VERIFICATION_SESSIONKEY
APPLAUDIT
ADDCREATOR
KERBLVL
MULTI-LEVEL_FILE_SYSTEM
MULTI-LEVEL_INTERPROCESS_COMMUNICATIONS
MULTI-LEVEL_NAME_HIDING
SECURITY_LABEL_BY_SYSTEM
PRIMARY_LANGUAGE_DEFAULT
SECONDARY_LANGUAGE_DEFAULT

Q&A

Richard K. Faulhaber
rkf@newera.com   twitter: @faulhaber_rk

THE z EXCHANGE
Reaching Out to the z Community Worldwide

zed TALKS

NEWERA