RSH CONSULTING

RSH RACF TIPS

For Administrators, Auditors, and Technicians

Volume 9
Issue 4
October
2015

RSH RACF Overview

Many of today's IT security practitioners, CISOs, auditors, and system managers are not familiar with the IBM mainframe and RACF. This lack of understanding and appreciation of the effort and skills required to enhance and maintain RACF controls is creating serious challenges for those of us who are tasked with protecting mainframes. To help everyone address this issue, RSH prepared a brief overview of RACF that you can distribute within your organization to raise awareness and win support for your initiatives. You can obtain a copy from our website's RACF Center webpage.

SUPERUSER.FILESYS.DIRSRCH

Users with READ access to UNIXPRIV resources SUPERUSER.FILESYS.CHANGEPERMS and SUPERUSER.FILESYS.CHOWN can administer Unix file and directory security controls without having to be given full Unix Superuser authority. Access should be permitted to administrators who are tasked with maintaining Unix security but do not require access to the Unix objects themselves.

To use either of these authorities, administrators also require read (r) and search (x) access to all directories. There are three ways to grant this access. One is to create an extended Access Control List (ACL) for every directory with an entry giving administrators r-x access. This entry should be paired with a default ACL entry to ensure new directories were given the same entry. This can be achieved with commands like the following.

setfacl -m g:RACFADM:r-x $(find / -type d)
setfacl -m d:g:RACFADM:r-x $(find / -type d)

The default ACL will ensure most new directories get the required permissions, but it is not 100% reliable. Corrections will be needed on occasion.

Another option is to give administrators RACF System AUDITOR authority. AUDITOR grants r-x access to all directories. However, it also enables users to examine RACF controls and change SETROPTS audit options. ROAUDIT, available in z/OS 2.2, can be used to provide directory access without allowing changes to SETROPTS.

The third option is to permit administrators READ access to resource SUPERUSER.FILESYS in the UNIXPRIV class. This will give them r-x to all directories, but it also gives them read (r--) access to every file, which may not be appropriate.

An enhancement proposed by RSH resulted in a fourth option becoming available in z/OS 2.2. IBM has created a new UNIXPRIV resource named SUPERUSER.FILESYS.DIRSRCH. READ access grants r-x to all directories. It was designed to be paired with CHANGEPERMS and CHOWN.

For more on protecting z/OS Unix, attend RSH's RACF - Securing z/OS Unix course.

Clear an ID's Password History

ALTUSER's new PWCLEAN operand, introduced with APAR OA43999, was intended to help you clear excess entries from a user's password history in the event you reduced the number of past passwords RACF is to store by setting a new SETROPTS PASSWORD(HISTORY(n)) value. PWCLEAN also removes the entire history for a PROTECTED ID. To clear a user's history, just:

ALTUSER *userid* NOPASSWORD
ALTUSER *userid* PWCLEAN
ALTUSER *userid* PASSWORD(*newpswd*)

The End of Masked Passwords

If you are thinking of implementing the new KDFAES password encryption algorithm introduced with APAR OA43999 or plan to upgrade to z/OS 2.2 in the future, read on.

Before DES encryption was introduced in RACF 1.6 (1984), all passwords were hashed using a proprietary IBM masking algorithm that was not cryptographically robust. Masking scrambled the password, but unlike DES, it did not factor in the USERID. With masking, two users with the same password would have the same hash value.

DES was introduced as an option, activated by removing an IBM-supplied ICHDEX01 password

encryption exit that came pre-installed as a Link Pack Area (LPA) module. The IBM-supplied exit simply directed RACF to continue to mask new passwords and to use masking to verify existing ones. It was recognizable in DSMON's RACF Exits report as having a length of 232 bytes.

Once the exit was removed, RACF used DES to encrypt new passwords. For verification, RACF first checked the password using DES, and if that failed, RACF checked it using masking. This process facilitated a non-disruptive migration to DES. When RACF 2.1 was released in 1994, IBM no longer pre-installed the exit in LPA (it was still provided in SYS1.LINKLIB), and DES became the default for new installations. The password verification process remained unchanged.

There is a slight risk associated with this two-step password verification process. The hashed value of a DES-encrypted password could match the hashed value of an entirely different masked password. An assailant who obtains a copy of the RACF database might be able to calculate viable masked passwords for a few IDs. In view of this risk, it has long been regarded a 'best practice' to implement an installation ICHDEX01 exit that directs RACF to only authenticate passwords using DES. Few installations have implemented such an exit. Our 2012 survey on exits found only 1 of 54 installations had an ICHDEX01 exit.

Installations that originally installed a pre-2.1 release of RACF and did not reset all passwords after activating DES, or those still using IBM's exit, are likely to have IDs with masked passwords. Be advised of the following and take appropriate action to avoid logon failures for these IDs.

When KDFAES is activated, RACF will no longer validate masked passwords. You must convert all masked passwords to DES before activation.

When z/OS 2.2 is installed, RACF will no longer validate masked passwords by default, and IBM's ICHDEX01 exit module will no longer be provided. Installations that wish to continue support for masked passwords must code and install their own ICHDEX01 exit. Rather than installing an exit, we recommend converting all passwords to DES. This will facilitate future activation of KDFAES.

Call us if you suspect you have IDs with masked passwords as we can help with remediation.

TSO IDs - 7 Characters or Less

Prior to RACF becoming the repository for TSO user logon information such as logon PROCs and Account Numbers, TSO users were defined in a PDS usually named SYS1.UADS (User Access Data Set). UADS still exists in most systems and can still be used to define TSO IDs. Hence, even though most installations store logon information in user TSO segments in RACF, IBM continues to accommodate the UADS architecture.

With UADS, logon information for each TSO user is stored in one or more PDS members. Member names start with the user's USERID and are followed by a numeric suffix character. Suffix numbering begins with zero and is incremented by one for each additional member. For example, the first member for IBMUSER would be named IBMUSER0, the next IBMUSER1, and so on. Since member names are limited to 8 characters, TSO USERIDs can at most be 7 characters in length to allow a space for the suffix character.

RACF will allow you to add a TSO segment to an 8-character ID, but the ID cannot be used for TSO logon. The segment is also ignored if the ID executes TSO in batch with program IKJEFT01.

RSH News

During RSH RACF training, attendees examine RACF options and profiles in their own systems and get on-the-spot advice for addressing any concerns they uncover.

Upcoming ***RSH RACF Training*:**

- RACF - Audit & Compliance Roadmap
  November 10-13, 2015 - Boston, MA
- RACF - Intro and Basic Administration
  December 7-11, 2015 - WebEx
- RACF - Securing z/OS Unix - *Expanded*
  February 8-12, 2016 - WebEx

RSH will be giving presentations at the upcoming RUGONE and KOIRUG meetings.

Many thanks to all who participate in our surveys!