UACC

VANGUARD
INTEGRITY PROFESSIONALS
CYBERSECURITY EXPERTS

How to use Vanguard security products to remove UACCs greater than NONE or READ to create a more secure mainframe RACF database without risking an operational outage due to removing required access.

NOTE: This process is not to be used for Grouping/ Member Classes. Those will be covered in another White Paper.

UACC Permissions

According to over 300 audits of different RACF databases and environments, a recurring problem is that too many data sets have RACF UACC (Universal Access) permissions with READ or greater.

The Issue

Most organizations have no idea who or what processes rely upon the UACC permission in order to gain access to a needed resource. Additionally even with AUDIT(ALL) specified on the profile, it is nearly impossible, very time consuming and very CPU intensive to gather 365 days or more worth of SMF data in order to even begin the process of determining who or what process gained access to a resource (including Datasets) via a Universal Access.

The Problem

With the increased scrutiny by auditors of security on the mainframe and the realization that UACC access provides ALL users (authenticated and not authenticated) access to resources, the removal of this UACC permissions has become a requirement that requires resolution.

The Solution

There is one fool proof method to identify and remediate all UACC access in a RACF database. Vanguard Administrator and Vanguard Offline can be used to find and remediate the UACC accesses while Vanguard Policy Manager can be used to maintain the RACF database once remediated. After all, fixing the database only provides relief until someone modifies it and changes the profiles back to an undesirable state.

The How (The technical details of how to resolve this problem)

With the Vanguard Offline and Vanguard Administrator solution, it is possible to determine any and all access to all resource via a UACC and then remove that access Here is how the process works:

UACC

VANGUARD
INTEGRITY PROFESSIONALS
CYBERSECURITY EXPERTS

First:

You must install the Vanguard Cleanup product and allow it to collect data for a period of time. The length of time depends on the customer installations desire for complete reporting. 365 days is a recommended value but a smaller amount of time can be used as long as end of year processing has been completed.

Second:

Go into Vanguard Administrator and either against a current Vanguard Extract File or the LIVE database, go into option 3: Security Server Reports and then Option 10: Universal Access. On the next panel specify the Level of UACC of N and GT (for Greater Then) , this will result in a report of all UACCs greater than NONE. You should do this BY CLASS (No need to try and boil the ocean) so add further Masking below to do one class at a time (such as specifying DATASET on the CLASS Line), you will also need to do DISCRETE and GENERIC Datasets separately. It is recommended that GENERIC datasets be done first. Do this ONLINE as we will use QuickGen to create the commands in the next step, so specify O on the BATCH/One-Line. Generate Heading should be set to N.

Third:

Create the commands to change the UACC on all results to NONE. Once the report comes back online, Type QG on the command line and then specify either one of the following on line 1:

For the DATASET CLASS for GENERIC profiles:

ALTDSD '&PROFILE' UACC(NONE) &TYPE For the DATASET CLASS for DISCRETE profiles: ALTDSD '&PROFILE' UACC(NONE) For NON DATASET CLASSES RALTER &CLASS &PROFILE UACC(NONE)

Then on the command line type : GEN This will create a temporary file of all the commands you will needs for testing, that you should now copy to a permanent file (call it anything you want, it can be a flat file or a member in a PDS, but remember the name of this file). This file will be later in this document as the COMMANDFILE.

NOTE: DO NOT ISSUE the VRAEXEC, VRABATCH or VRASCHED command or in any way submit this set of commands to your RACF database as: YOU DO NOT WANT to remove access yet. DON'T DO IT.

Fourth:

Now that we have the commands to change the UACC to NONE, we need to find out what the effect of the commands will have given actual accesses (those captured by the Vanguard Cleanup Started task from the First Step) that occurred to the production RACF database so that we can find what users will lose access, given the changes.

What we do here in Targeted Impact Analysis Option 4 is take every access Request from that Offline HMF that could be affected by the Commands in the COMMANDFILE and test them against the Test RACF database (the Offline version) and store the results (no we don't use RACF to do this, it is all Vanguard Processing) and then we execute the Commands in the COMMANDFILE against the Test RACF database (the Offline version) and then rerun the Same set of Access Requests against the now modified test RACF database (now having the effect of the COMMANDFILE run against it) and then we compare the two resultant sets of access. Any difference found is directly due to the effect of the commands in the COMMANDFILE and ONLY those commands.

To accomplish this go into Vanguard Offline, Specifying Option 7 for Targeted Impact Analysis reports and then chose Option 4.

On the Option 4 panel, you will need to provide the COMMANDFILE name on the Command Input Dataset Line and you will specify the name of the offline copy of the RACF database (Option 4, will delete, define and create the copy at run time of the RACF database based on the system it executes upon). The History Master File is determined based on the VCLOPT00 and MUST point to your production Offline History Master File (This can be found in VCLOPT00 specified as VOFMAST). Next, On the Targeted Impact Analysis Screen you will see a CREATE EXTRACT FILE option, please specify this as YES, provide it a meaningful name as this flat file dataset will be used later. This file will be used later as RESULTSET in this white paper. Hit Enter to get to the next screen where it allows for specification of one or more Offline HMFs. If you are running Offline on multiple systems against different Offline HMFs within a SYSPLEX against the same RACF database, you should specify the names of the other HMFs here. Hit Enter and then submit the generated JCL after making any necessary JOBCARD modifications. The Job may run awhile depending on the size of the RACF database and more importantly the number of access requested contained in the Vanguard Offline History Master File.

UACC

VANGUARD
INTEGRITY PROFESSIONALS
CYBERSECURITY EXPERTS

Fifth:

Now it is time to see the effect of the COMMANDFILE and generate permits for users that would lose access due to their use of the UACC to gain access to resources. Once the batch FILE from the previous step is completed, go back into Vanguard Offline and chose Option 6: Target Impact Analysis Report Online and then option 7 Impact Detail – All Access Changes (which if you only issued commands that will lower UACC access, then all records reflected will be denied access as lowering a UACC cannot provide additional Access).

Once you view the report, first make sure that *UNDEF* does not show in the USER column. This would indicate that one or more unauthenticated users gained access to resources via a UACC. It is not possible to generate commands to permit these users as they are UNKNOWN. This should not be the case, but if there are *UNDEF* users then these MUST be investigated first to ensure that these unknown users or processes (usually an STC) do not lose access.

On the command line put a Q for QUICKGEN and on line 1: Type one of the following:

For the generic profile datasets:
PE '&AUTHPROF' CLASS(&CLASS) ID (&USERID) ACCESS(&LACCREQ) GEN

For discrete profile datasets:
PE '&AUTHPROF' CLASS(&CLASS) ID (&USERID) ACCESS(&LACCREQ)

For General Resource class members:
PE '&AUTHPROF' CLASS(&CLASS) ID (&USERID) ACCESS(&LACCREQ

Take the resultant set of commands and save them as a new set of commands, this file will be the PERMITTOREMOVEUACC referred to below.

Last:

Now, once you are ready to actually remediate your RACF database by changing the UACCs, take the PERMITTOREMOVEUACC commands and the COMANDFILE and run them against your RACF database back to back running the PERMITTOREMOVEUACC first. You can do this in a batch job or online.

TO PREVENT UACCs being changed in the future. Vanguard Policy Manager should be implemented on the target system to prevent undesirable changes from being reintroduced back into the RACF database by well-intentioned Administrators. Install Policy Manager on the system and then implement the following Best Practice Policy.

BP.UACC.NONE.REQUIRED

This best practice policy is easily implemented by simply selecting the Policy under the Policy Manager Option 1 Best Practices. It will interrogate every command issued to the RACF database and prevent any Administrator from issuing a command that creates or alters a profile to elevate the UACC above NONE.

Vanguard Policy Manager contains a number of other best practices and user defined policies that can be used to ensure that the site's implementation of security is adhered to by even the most authorized system special users. See the Policy Manager manual for more details.

Why Vanguard to Secure Your Enterprise?

Almost half of the Fortune 1000 companies in the world spanning banking, retail, insurance, as well as numerous government agencies trust Vanguard with their enterprise security.

About Vanguard Security Solutions

Vanguard offers the most advanced and integrated portfolio of enterprise security products and services in the world. The portfolio was the first to offer fully automated baseline configuration scanner for Mainframe DISA STIGs— the Gold Standard for Security.

For More Information

To learn more about Vanguard Security Solutions please call 702.794.0014 or visit www.go2vanguard.com

Corporate Headquarters

6625 S. Eastern Avenue—Suite 100
Las Vegas, NV 89119-3930