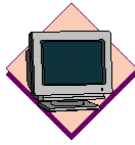


BY LINDA DOCKSTADER



INTRODUCING ACCESS CONTROL FOR VSE/ESA 2.1

VSE/ESA 2.1 comes equipped with a substantial and sophisticated security feature. Here's an introductory look.

BUILT-IN SECURITY IN VSE/ESA 2.1

VSE/ESA 2.1 has a built-in security feature, called Access Control, for restricting access to files, jobs, libraries, and so on. This is included with the operating system at no extra charge. (Note that Access Control is unavailable for VSE/ESA 2.1 in unattended node support configuration — environment “C”.)

Access Control security in VSE/ESA 2.1 starts at IPL time, when you enter the SEC= parameter in the SYS IPL command. The options for this parameter are NO (which is the default), YES, and YES,NOTAPE. The default of SEC=NO means there will be no Access Control in this VSE system during the time this IPL is active. Using the parameter SEC=YES enables the built-in Access Control feature. It also enables ACLR if you have it installed. SEC=YES,NOTAPE activates Access Control, but removes tape files from protection. You can use Access Control to secure the following:

- libraries;
- sublibraries;
- members;
- standard-labeled single-file tapes;
- non-VSAM disk files;
- ACB macro-accessed VSAM KSDS, ESDS, RRDS, and VRDS files;
- certain VSAM managed SAM files; and
- jobs.

Note that Access Control doesn't provide protection for files on diskette. Access Control uses label information so unlabeled tapes, non-standard labeled tapes, and multfile tape volumes cannot be protected. The system libraries IJSYSRS and IJSYSRS.SYSLIB have a special default access right (UACC=CON) to provide for any period when label information may not be available, such as during IPL.

In addition to the label requirements, when using Access Control to secure your tape data sets there are also some restrictions placed on the console operator. You may find you cannot live with these

proscriptions. You may choose instead to use a tape data set management software package. In that case, you can still make use of Access Control's other features while removing your tape files from its grasp. Just use the YES,NOTAPE option. When Access Control is in place, VSE/ICCF security defers to Access Control. This means that each VSE/ICCF user must have an entry in the Access Control table to run jobs in the interactive partitions. Without VSE/ESA Access Control, VSE/ICCF provides its own security in the usual manner.

VSE/ESA 2.1 Access Control secures your resources by referring to a table you assemble (called DTSECTAB). A default table is shipped with the operating system. You can modify this table to meet your specific security needs.

ACCESS RIGHTS

VSE/ESA 2.1 Access Control secures your resources by referring to a table you assemble (called DTSECTAB). A default table is shipped with the operating system. You can modify this table to meet your specific security needs. DTSECTAB holds user profiles in which you specify user ID, password, access class, and access rights. It also holds resource profiles in which you specify resource type, name, and access class.

Access Control checks user ID and password to establish identification. It works in the usual way, i.e., if user ID and password don't match, access is denied. A user is established as a system administrator by including the parameter AUTH=YES, which status allows full

access to all resources and offers master console authorization. If the AUTH= parameter is not specified, the default of AUTH=NO takes effect.

Upon a user ID match, Access Control then provides a deeper level of security by analyzing this user's access rights. Access rights can be confusing because they provide multiple levels of protection for a variety of resources. In general, the access rights are ALT (alter), UPD (update), READ (read only), and CON (connect). Access rights for files are simple when compared to those of libraries. Files can be created, renamed, and deleted, and the contents added, changed, and deleted with the access rights ALT or UPD. Access right READ allows read-only access to the file in question. As you can imagine, access right CON doesn't apply to files.

For libraries, sublibraries, and members, access rights are a bit more complicated. The following applies:

1. When you restrict access to a library, you also protect all sublibraries and members.
2. If you don't restrict access to a library, sublibraries and members are unprotected as well.
3. The access right ALT allows creation and deletion, and in some cases renaming. ALT implies UPD.
4. UPD allows the user to read and change the contents. UPD implies READ.
5. READ allows read-only access. READ implies CON.
6. CON allows connection to libraries and sublibraries. It doesn't apply to members.

In addition, access rights fall into two major categories, Universal Access Rights and Access Control Class rights. Universal Access Rights apply only to libraries, sublibraries, and members thereof.

You define this right with the UACC= parameter in the DTSECTAB macro. For example, if you wanted all users to have read-only access to a specific library, define that library in DTSECTAB with a TYPE=LIBRARY and include the parameter UACC=READ. All users could then read, but not update or otherwise change, that specific library. Note that system libraries IJSYSRS and IJSYSRS.SYSLIB have a default of UACC=CON so that they may be accessed at times when label information is unavailable.

Access Control Class rights are somewhat more complicated. Once the user ID and password are matched, the access rights defined for this user ID are compared against those specified for the requested resource.

There must be a match for access to the resource to be granted. Note that if the resource is not listed in DTSECTAB this analysis cannot take place, and the resource is considered unprotected.

When you define the resource profile in DTSECTAB, you can assign one or more access control classes (from 1 to 32) to the resource. Then, when you define the user profile, you use the ACC= parameter to grant access to the various classes. For example, to grant a user read-only access to a file, you might define that file with a resource profile containing ACC=(5,6,7) and define the user profile with the parameter ACC=(5,READ). Other users with rights to access control classes 5, 6, and 7 can also access this file. You can find complete information on access rights and the DTSECTAB macro in IBM's publication *VSE/ESA Guide to System Functions*.

LOGGING AND REPORTING

In addition to Access Control, which comes with the VSE/ESA operating system, IBM offers an optional program called VSE/Access Control — Logging and Reporting (ACLR). ACLR logs security activity and supplies useful reports. With this product, you can keep and report historical data on resource usage and unauthorized access attempts.

In a manner similar to CICS system journaling, ACLR records security events to one of two log data sets, IJSYSL1 and IJSYSL2. These two logs alternate when full, sending messages to the system console. You offload the log files to a labeled tape via a batch job using the SAVE control statement. (You may save the files to disk if you choose, but it isn't recommended.) Label and extent information for log data sets must define sequential VSE files, not within VSAM-managed space, and specify an explicit volume serial number. This information must be available to the system when Access Control starts at IPL time. Therefore, the information must be contained in Standard Labels.

The logging portion of ACLR loads into the SVA and begins execution at IPL time. When a recognized security event occurs, ACLR logs the event into a log queue in main storage, then writes the event record to the log data set at a later time.

There are two ways to record access events, either record violations only, or record all attempts at resource access by class. The latter may be useful to pinpoint your resource usage, but keep in mind that it may become a performance drain. Recording all resource access attempts will greatly increase the main performance issue in ACLR, that is, the number of "hits" per second. It also may impact your I/O rates and queue space needs. In any case, all accesses

by security administrators (AUTH=YES on user ID profile) are always logged, and accesses of resources with universal access (UACC=) are not logged. The reporting feature of ACLR is a versatile batch job to accomplish log data set initialization, saving logs to tape, and producing versatile reports. This job runs in a VSE static partition or a VSE/ICCF Interactive partition, and needs access to a Sort/Merge utility. The logs are initialized when you first install ACLR, or after a hardware failure. You need to save logs to tape on a regular schedule. Consider including historical log tapes in your off-site storage plan.

The reporting function produces diverse reports sorted by such categories as user ID, resource type, resource name, etc. For report runs, the control statement can be continued up to 19 lines. There may be up to 255 separate control statements per report run.

For more information, see IBM's publication *VSE/Access Control — Logging and Reporting: Program Reference and Operations Guide*.

A CAUTIONARY TALE

It's true that the security features of VSE/ESA Access Control are excellent, but take a moment to read the true story of a little keystroke and the havoc it wreaked, lest you become overconfident . . .

Early one morning, the programmers gathered at the water cooler, all complaining at once. None of their programs would compile. No one could tell them why. The entire application programming staff was unable to work.


The entire technical support staff was hard at work trying to identify and resolve the problem. The technical staff was large, training was plentiful, and the latest releases of VSE and CICS were installed. Nonetheless, they couldn't find the error, no doubt due to the fact that while they were using VSE/ESA Access Control they didn't have the Logging and Reporting optional program.

Hours passed. Tempers flared. After lunch, the part-time intern arrived for his afternoon shift.

Upon hearing the commotion, the intern volunteered that he had reassembled DTSECTAB on the previous day. After an hour of careful examination, the technical staff found that a single comma had been accidentally omitted at a critical spot within this crucial table.

This scenario actually happened at a local VSE shop (which shall remain nameless). The company lost valuable work time and gained an increase in ill will between the programmers and the technical support staff. The questionable judgment that allowed a part-time college student to be working on

security tables can be explored in another article. For now, just keep in mind that the most sophisticated of security software still depends on human implementation. Haven't we all experienced system dysfunction resulting from typing too fast?

We've taken an introductory look at IBM's VSE/ESA Access Control and the optional program VSE/ESA Access Control—Logging and Reporting (ACLR). Together they make a sophisticated security system that you can use to your advantage. So put time and thought into your security configuration, carefully select and supervise the people who implement that security, and watch out for those commas! 



NaSPA member Linda Dockstader is a technical writer and systems programmer. Along with her husband, NaSPA member Bill Dockstader, she runs Technology Service Company, a data processing consulting firm in Seattle, Wash.

©1996 Technical Enterprises, Inc. Reprinted with permission of **Technical Support** magazine. For subscription information, email mbrship@naspa.net or call 414-768-8000, Ext. 116.