

Network Security 6.0 Enhancements

New Activation Process

- Network Security 6.0 includes an updated activation/deactivation process that makes it easier to activate or deactivate exit points by server. You can select the servers to activate/deactivate and run the activation/deactivation process for only those servers.

Object Rules

- Network Security 6.0 allows you to define authority rules to control access at the object level. This includes programs, files, libraries, folders, and IFS directories and files. The rules can be specific to a user, a group, or *PUBLIC, or a location. Object rules let you define access to both the object and the data contained within the object.
- Use object rules to specify the operation that the rule allows. Operations include *ALL, *CREATE, *READ, *UPDATE, or *DELETE. The object rule also specifies the action to take when someone attempts to access the object or its data. Actions include *REJECT (reject the access request), *OS400 (allow the access request), or *SWITCH (allows access to the object data using the authority of a specified switch profile).
- When you define an object rule, you select the servers and functions that will enforce the rule. This creates *MEMOBJ Authority filter rules for the user or location object rule. The *MEMOBJ Authority filter rule tells Network Security to check memorized transactions (MTR) for authority. If no MTR authority is found, it then checks the transaction against the object rules.
- To create object rules, you first define an object list that contains the objects for which you want to control access. An object list can be one of two types: type Q contains objects in a library on your system; type I contains objects from the IFS.
- For each object rule by user or location that you create, you specify the name of the object list to which the rule applies. You then specify the data access and object access rights to the object in the object list.

New Reports Menu

Network Security's new Reports menu added reports for object lists and object rules:

- The Print Object Lists report prints a list of the object lists that have been defined to Network Security. You can print information for a specific object list, or a group of object lists. You also can specify whether to include the object list entries, and the rules on which the object list is used.
- The Print Object Rules report creates a report containing the object rules defined to Network Security. You can limit the report by entering selection criteria for location, user, object list, operation, and whether to include object list entries for object lists in the report.

Command Changes

- Network Security 6.0 eliminated the LPWRPURGE command because it is no longer necessary. The LPWRPURGE command was used previously to clear the captured transaction file. In Network Security 6.0, the Capture Transaction Summarization process now cleans up journal receivers containing captured transactions. You can specify how you want the journal receivers deleted.
- Network Security 6.0 added the following commands:
 - **LSTRCAPSUM** Start Captured Transaction Summarization
 - **LENDCAPSUM** End Captured Transaction Summarization (replaces the LSENCAPSUM command)
 - **CRTOBJRUL** Create Object Rule
 - **CHGOBJRUL** Change Object Rule
 - **DLTOBJRUL** Delete Object Rule
 - **DSPOBJRUL** Display Object Rule
 - **ADDOBJLE** Add Object List Entry
 - **CHGOBJLE** Change Object List Entry
 - **RMVOBJLE** Remove Object List Entry
 - **CHGOBJL** Change Object List
 - **CPYOBJL** Copy Object List
 - **CRTOBJL** Create Object List
 - **DLTOBJL** Delete Object List
 - **PRTOBJL** Print Object List
 - **RNMOBJL** Rename Object List
 - **WRKOBJL** Work with Object Lists
 - **PRTOBJRUL** Print Object Rule
 - **WRKOBJRUL** Work with Object Rules

Upgrading Network Security

- The Merge Previous NS (MRGPRVNS) command allows you to merge information from a previous version of Network Security into Network Security 6.0. You can run the command after you've installed Network Security 6.

In Addition...

- Several menus and screens in Network Security were redesigned for a new look and to bring increased functionality to the process of defining access rules.
- A new installation wizard automates and streamlines the installation process.