NonStop NET/MASTER Tips and Techniques

by John New

Gresham Software Labs

Email: jnew@greshamsoftwarelabs.com.au

This article originally appeared in *The Tandem Connection*, Volume 21, No. 3 - May/June 2000, and is reproduced with permission from the International Tandem Users' Group (ITUG).

Introduction

This is an ongoing column with NonStop NET/MASTER tips and techniques. Each column is also accessible from http://www.greshamsoftwarelabs.com.au/ (Gresham Software Labs). Please send all comments and suggestions to John New at jnew@greshamsoftwarelabs.com.au.

Biography

John New is a technical writer. He has written and updated various Tandem manuals. He currently writes hard-copy, online, and web documents for a variety of software products.

Protecting Your NonStop NET/MASTER Files

This article discusses how to protect your NonStop NET/MASTER files by using proper file security settings. It summarizes the files that are distributed with NonStop NET/MASTER, then discusses security considerations that are appropriate for various file types. Properly securing NonStop NET/MASTER files is very important because knowledgeable users can compromise Tandem system access if inappropriate file security settings are used.

Files Distributed With NonStop NET/MASTER

NonStop NET/MASTER is distributed with a mixture of file types, each type being located by default in a well-known subvolume. These include program object files, data files, and NCL and panel source and object files. After the REPSUBSYS phase of the Tandem Install program, files distributed with NonStop NET/MASTER are located in the following subvolumes:

$SYSTEM.SYSTEM Contains the NNM program, which is used to log on to NonStop NET/MASTER from TACL, or to shut down NonStop NET/MASTER from TACL.

ZNNM Contains program object files, including:

NCP Used to start NonStop NET/MASTER from TACL, and to monitor and manage NonStop NET/MASTER processes.
NMNC0001 NonStop NET/MASTER application program file.
TRACEEXE Trace application program file.

ZNNMDATA Contains various data files, including:

UACAUTH Database with customized Guardian utility authority settings.
UACUTIL Database with customized Guardian utility definitions.
UADAUTH Database with distributed Guardian utility authority settings.
UADUTIL Database with distributed Guardian utility definitions.
UMSFILE User ID Management Services (UMS) database with user ID records for NonStop NET/MASTER users.

ZNNMNDO Contains the distributed NCL object files, NCODE and RMSNCODE, which contain precompiled object code for all distributed NCL source files.

ZNNMNDS Contains distributed NCL source files.

ZNNMPDS Contains the distributed panel object files, PCODE and RMSPCODE, which contain precompiled object code for all distributed panel source files. Contains distributed panel source files.

Securing the NonStop NET/MASTER NNM Program

The purpose of the NNM program is threefold. The NonStop NET/MASTER owner (NNM.MANAGER or similar) uses the program to log on after starting NonStop NET/MASTER for the first time. Other NonStop NET/MASTER users can use the program to log on to NonStop NET/MASTER from TACL. The NonStop NET/MASTER owner or other privileged users can use the program to shut down NonStop NET/MASTER from TACL.

Note that users who can run the NNM program can log on to NonStop NET/MASTER from TACL only if they have a user ID/password and dynamic access. In other words, a user who has execute access to the NNM program may not necessarily be allowed to log on from TACL. NonStop NET/MASTER makes its own security checks before permitting a user to log on from TACL.

Therefore, while write and purge access to the NNM program should be tightly controlled, read and execute access could be unrestricted.

For local access, a reasonable security setting for the NNM program would be "A-A-"; for remote access, "N-N-"

Securing NonStop NET/MASTER Program Files

Properly securing NonStop NET/MASTER program files in the ZNNM subvolume is particularly important. Proper file security is designed to prevent unauthorized users from starting private NonStop NET/MASTER systems and creating a user ID with unrestricted Tandem system access.

An additional reason for properly securing NonStop NET/MASTER program files is that some program files (NMNC0001 and TRACEEXE) contain privileged code and must be licensed.

Therefore, execute access to NonStop NET/MASTER program files should be restricted to the NonStop NET/MASTER owner.

Read access to NonStop NET/MASTER program files should also be restricted. If a user can read the program files, the user can duplicate the files and enable execute access.

Tandem recommends that you secure all program files in the ZNNM subvolume on your local node with "--O-". This gives read, write, and purge access to SUPER.SUPER, and execute access to the owner of the files. This allows only SUPER.SUPER to copy the files and allows only the NonStop NET/MASTER owner to execute the files. It also permits the NonStop NET/MASTER owner to be a user other than SUPER.SUPER.

Use the following FUP command to secure NonStop NET/MASTER program files with "--O-":

```
FUP SECURE file-name, %7727
```

If you intend to start NonStop NET/MASTER from a remote node, specify "--U-" as the file security for the program files:

```
FUP SECURE file-name, %7767
```

An EMS event is logged if you start NonStop NET/MASTER and the file security of any licensed NonStop NET/MASTER object file is neither "--O-" nor "--U-". You can safely ignore this message if you are confident that the file security settings you have chosen are appropriate for your NonStop NET/MASTER system.

Many NonStop NET/MASTER sites use an obey file to run the NCP program object file or specify a CONFIG file when starting NonStop NET/MASTER. If so, the NonStop NET/MASTER owner must have read access to the obey file or CONFIG file; otherwise, a file security error results. For these files, specify "O---".

Securing NonStop NET/MASTER Data Files

NonStop NET/MASTER must have read and write access to the data files in the ZNNMDATA subvolume. This is so that NonStop NET/MASTER end users can read information, and so that authorized NonStop NET/MASTER users can add, copy, modify, and delete data. The files should be owned by the NonStop NET/MASTER owner.

Two reasonable security settings for data files are "OO--" and "OO-O". The former gives read and write access to the NonStop NET/MASTER owner. The latter adds purge authority.

Whether data files have execute access is not relevant because data files are never executed.

When you start NonStop NET/MASTER for the first time, NonStop NET/MASTER automatically creates custom data files from certain distributed model data files (model files include CEXCCF, MAPFILE, UACAUTH, UACUTIL, UMSFILE, and others). The custom files are recreated automatically if the files are purged and NonStop NET/MASTER is restarted. Custom data files are secured with the default file security setting of the NonStop NET/MASTER owner. If this is other than "OO--" or "OO-O", you may want to properly resecure the files.

Securing NonStop NET/MASTER NCL and Panel Files

NCL and panel files are not executed in the Guardian environment; they are executed by NonStop NET/MASTER in an internal NCL processing environment. You cannot execute NCL procedures or display panels from TACL, only from NonStop NET/MASTER. Therefore, whether NCL procedures and panels have Guardian execute access is not relevant to whether NonStop NET/MASTER can execute and display them.

However, because NCL and panel files are executed by NonStop NET/MASTER, the NonStop NET/MASTER owner must have Guardian read access to the files. In fact, to run NCL procedures and display panels, only Guardian read access by the NonStop NET/MASTER owner is necessary. Write and purge access is not relevant to execution (although it is, of course, needed by users who create, modify, and purge the source files).

For NonStop NET/MASTER to read NCL procedures and display panels, it does not matter which NonStop NET/MASTER user created them. If the file security of an NCL or panel source file makes it available for reading, NonStop NET/MASTER can execute the NCL procedure and display the panel. This means that any NonStop NET/MASTER user who has the authority to invoke NCL can run the procedure.

While not relevant to file security, it is worth noting that there are various ways to secure access to NCL and panel files from within NonStop NET/MASTER. For example, it is very easy for the NonStop NET/MASTER security administrator to increase the command authority level for the START and EXEC commands to prevent certain users or groups of users from running NCL procedures. It is also possible to give each user or user group who develops NCL procedures and panels their own private development subvolume.

Securing Distributed NCL and Panel Files

As described in "Files Distributed With NonStop NET/MASTER," the locations of distributed NCL and panel files are ZNNMNDO, ZNNMNDS, and ZNNMPDS. NonStop NET/MASTER is designed so that you need never modify files in these locations. Additionally, it is not advisable to purge distributed files.

The suggested file security setting for distributed NCL and panel source and object files is "O---".

Securing Custom NCL and Panel Files

There are two types of custom NCL and panel files: customized and user-written.

Customized NCL and panel files are distributed NCL and panel files that you or other users have modified. Because NonStop NET/MASTER is designed so that you never need to modify the distributed NCL and panel files, it is also designed so you can copy the distributed source files to another subvolume and customize the copies. NonStop NET/MASTER then uses the NCL search path to execute customized versions instead of distributed versions. The well-known locations for customized NCL and panel source files are:

ZNNMNCS	Contains customized NCL source files
ZNNMPCS	Contains customized panel source files

User-written NCL and panel files are those written and maintained by you or your users. Typically each user or user group has their own development subvolume.

For both types of custom NCL and panel files, the NonStop NET/MASTER owner must have read access to execute the NCL procedures and display the panels. The user who maintains the source files must have read, write, and purge access.

If the NonStop NET/MASTER owner and the source file maintainer is the same user, "OO-O" would be a reasonable file security setting.

If the NonStop NET/MASTER owner and the source file maintainer are in the same group, you may want to use "GO-O" as the file security setting (assuming that the files are owned by the maintainer). This gives read access to the NonStop NET/MASTER owner, and read, write, and purge access to the maintainer. Note that it also gives read access to all other users in the same group.

Finally, if the NonStop NET/MASTER owner and the source file maintainer are in different groups, you may consider that "AO-O" is appropriate (assuming that the files are owned by the maintainer). This gives read access to the NonStop NET/MASTER owner, and read, write, and purge access to all local users regardless of their group.

NCL programmers and other NonStop NET/MASTER users sometimes fall into a trap when using Edit Services. Edit Services is normally used to create and execute NCL procedures, and to create and display panels. But sometimes a user's NCL and panel file security prevents the NonStop NET/MASTER owner from reading the files. The result is that a user can create NCL procedures and panels but NonStop NET/MASTER cannot compile and execute the NCL procedures or display the panels. If this occurs, either change the user's default file security setting or resecure their files to enable read access by the NonStop NET/MASTER owner.

Conclusion

Understanding NonStop NET/MASTER file security is necessary to properly secure program files, data files, and NCL and panel source and object files. For more information on all aspects of NonStop NET/MASTER security, refer to the *NonStop NET/MASTER MS System Management Guide*. This manual describes file security and topics such as User ID Management Services (UMS), command authority levels, and utility command security.