·R·S·I·

Ross Systems International

White Paper

Reporting HP NonStop (Tandem) SAFEGUARD Protected Disk Files Using FINFO

by

Rupert Stanley

© Ross Systems International Limited, 2010

This document is issued by Ross Systems International Limited (hereinafter referred to as RSI) in confidence and is not to be reproduced in whole or in part without written approval.

Ross Systems International Limited.
The Hollies
18 New Road
Mistley
Manningtree
Essex CO11 2AG
Tel. +44-1206-392923
Email. info@rsi-ns.com

Abstract.

SAFEGUARD is a HP NonStop (Tandem) proprietary product which is used to provide an extra layer of security to HP NonStop objects, such as Users, Processes, Devices and Disk Files.

Disk Files are protected the Volume, SubVolume and File Name Level using a combination of:

1. Access Control Lists, which contain information as to if permission to access the objects is to be granted or denied based on user (group, number) and operation (read, write…).
2. File Transaction Auditing Conditions, based on type (Access / Management), Outcome (Success or Failure) and Source (None, Local, Remote or All).
3. File Status Information. i.e. whether the file is Licensed, ProgId'd, to be Cleared on Purge or if it is Persistent

This facility is very important is securing sensitive systems, particularly in the financial service industries, where there is a statutory obligation, and it provides a very competent facility for meeting these obligations.

Although the Auditing facilities are excellent there are several operational challenges in status reporting which extensions to the RSI file information product FINFO address.

This white paper addresses this technical challenge and shows how it is solved by FINFO 3.3.

Introduction.

This white paper is structured so that firstly the commercial imperatives of each aspect of the technology is discussed and then the ways in which the situation can be improved by levering appropriate techniques and suitable improvements is explored.

HP NonStop Systems are used for transferring a large percentage of the funds within the financial services industry. They are used for not only POS and ATM based transactions but also for Interbank funds transfers and for Stock Trading throughout the world.

The systems which performs these transactions need to be integrated into Information Security Management Systems (ISMS) and are in the category Highly Secure. As such they must contain both strict user authorisation and enforced user-operation-object restrictions (Access Control Lists).

This implies a complete implementation of Safeguard or some similar third party software and the Access Control Lists (ACLs) must explicitly allow users to perform the functions requested, with all other requests being denied.

An ISMS requires that there is a high level of control of people, procedures and objects, which include the regular generation of reports, such as:

1. System Configuration, with special emphasis on the security of objects
2. System activity audits

The reports need to be regularly reviewed and acted upon. It is to be noted that the emphasis between strategic and tactical varies depending of the type of breach to be expected. System Configuration tends to be more strategic where as system activity tends to be more tactical, for the obvious reason that if money is disappearing out of the system the problem needs to be addressed: NOW!

At the heart of these financial systems is the data store, i.e. the disks and the structures contained therein: subvolumes and files and the files themselves contain the crown jewels of the system and indeed the corporations running them in the form of the bits and bytes corresponding to millions or billions of pounds.

Operational challenges in managing an ISMS using SAFEGUARD on the data store of NonStop systems which has been brought to my attention and resulted in the upgrade of FINFO to address this technical challenge and to make the generation of the vital system configuration reports, easier, more consistent, legible and accessible to analysis.

Tandem when it implemented SAFEGUARD produced a product which is highly reliable for securing NonStop Systems and provides an excellent audit trail of system activity for use by system managers and hence is the product of choice for this purpose.

However, system configuration is made difficult by challenges presented in configuration reporting which is an essential part of the ISMS loop and to which the rest of this white paper will be addressed.

The Challenge

The HP NonStop Data store is a classical hierarchical system consisting of:

1. Volumes, which contain
2. SubVolumes, which contain files
3. Files which contain the data to be protected

SAFEGUARD recognises this and provides protection at all three levels and each object at a given level can contain access control lists containing user identities and permissions types which can be either to grant or deny access to the object.

SAFEGUARD also provides comprehensive auditing facilities and the File, SubVolume and Volume SAFEGUARD records determine if a transaction is to be written to the Audit Log. This is determined by transaction type (Access / Management), Outcome (Success or Failure) and Source (None, Local, Remote or All).

Since SAFEGUARD Security replaces Guardian Security the file SAFEGUARD records also contain details of File Status Information. i.e. whether the file is Licensed, ProgId'd, to be Cleared on Purge or if it is Persistent

Thus a file will be subject to the provisions of its own SAFEGUARD settings including ACL and also those at the subvolume and volume levels.

The resulting structure is a branching tree with many levels of access protection in many modes, which is something which is not easily represented on a piece of paper of screen.

Thus SafeGuard reports on a file as such:

```
$WORK NATIVE 4> safecom
SAFEGUARD COMMAND INTERPRETER - T9750D45 - (24OCT97)    SYSTEM  \SIRIUS
=info diskfile zstub, detail
                  LAST-MODIFIED     OWNER    STATUS
$WORK.NATIVE
 ZSTUB           29JUL10, 18:34     127,1    THAWED
    127,001      R,W,E,P
    127,004 DENY   W,  P
  AUDIT-ACCESS-PASS = LOCAL       AUDIT-MANAGE-PASS = REMOTE
  AUDIT-ACCESS-FAIL = ALL         AUDIT-MANAGE-FAIL = NONE
  LICENSE = OFF  PROGID = OFF  CLEARONPURGE =  ON  PERSISTENT =  ON
```

Yes, it is a bit messy but it does tell us all about the object, doesn't it? Lets try again:

```
=info diskfile ztest,detail
* WARNING * RECORD FOR DISKFILE $WORK.NATIVE.ZTEST: NOT FOUND
```

Simple, ZTEST is NOT SafeGuard protected, really? How about this:

```
=info subvolume native,detail
                  LAST-MODIFIED     OWNER    STATUS
$WORK.NATIVE
                  8AUG10, 12:55     127,1    THAWED
    127,*       R,W,E,P,C,O
  AUDIT-ACCESS-PASS = NONE        AUDIT-MANAGE-PASS = NONE
  AUDIT-ACCESS-FAIL = NONE        AUDIT-MANAGE-FAIL = NONE
```

This is inconsistent! ZTEST is protected in spite of SAFECOM saying it is not but at the SubVolume level and we will have to use many man hours to extract the results from the reports. The same situation also exists at the Volume and System level and there is no command to view just the SafeGuard protected objects in context. So we have a reporting system which:

1. Has a clunky command line. (Why do we have to tell it is is a diskfile?)
2. Has clunky output, why so many lines per file (This is an export nightmare!)
3. Does not show the linking between files, subvolumes, volumes and the system.

This represents a considerable challenge in systems auditing under an ISMS. Something needs to be done and the rest of this paper will show what was done and the results to be expected.

FINFO Version 3.3 The Solution

FINFO is a Guardian File Information display utility which can be used to select a set of files based on a wide selection of criteria for example, name, size, date, type, user name/number…, sort the selected results by for example name, size, last modified date user…,

The results can be displayed in a number of formats, standard, date field, extents, EXCEL export. Thereby enabling the user to obtain the information required with the least amount of extraneous information, from the user's viewpoint and in the most compact format.

Subvolume and volume totals are also provided as standard.

There are special commands for extracting volume and subvolume summaries together with file exception reports, file reaching full, index level too deep…

However, in Version 3.2 there was no facility to display SafeGuard information a facility which was crying out for attention seeing the challenges detailed above.

The approach was to maintain conformity with the rest of the FINFO functionality, in as far as possible, with the following aims:

1. To select safeguard protected files using a –SG command line parameter

2. To have a special safeguard display using a –G command line parameter

3. To have SafeGuard information in the Excel Export Format report
   –X command line parameter.

I also became aware that the Guardian security for safeguard protected files needed to be changed from the "RWEP" codes to "****" for safeguard protected files.

Selecting SAFEGUARD Protected Files (-SG)

FILE_GETINFOLISTBYNAME_ has a parameter 69 to get the SafeGuard status of a file. However this only shows if a file is protected directly. However it does not show if the Volume or SubVolume are protected. To do this it is necessary to use the SafeGuard SPI interface.

The –SG Command Line Parameter was thus programmed to select all SafeGuard Protected Files either directly or indirectly. i.e.

```
$WORK NATIVE 9> finfo -sg
FINFO V3.3  Native 08/08/2010 13:44
-----
Copyright Ross Systems International Ltd. 2008,2009,2010

Full Version (Release Date 28th July 2010)
------------------------------------------
Files on \SIRIUS.$WORK.NATIVE

Name     Last Modified         Code TP RWEP    Size   User No  PExt  SExt Pages
ZLIST4   14-Nov-2008 12:29:43   101 U  ****  61,936   127,001     4    16    36
ZSTUB    18-Nov-2008 14:25:59   101 U  ****   2,314   127,001     2     2     2

Selected User Totals for SubVolume \SIRIUS.$WORK.NATIVE
User No  User Name          Files            Bytes Used      Pages Used
127,001  RSI.RUPERT             2                64,250              38
Totals:                         2                64,250              38
```

Note, The RWEP Column has **** in it to indicate SafeGuard protection, i.e. The Guardian protection has been superseded by the SafeGuard Security.

Displaying SafeGuard protected Files (-G)

Displaying SafeGuard protected files is complex since files can have the following statuses:

1. Not protected
2. File level protection
3. File and Subvolume protection
4. File and Volume protection
5. File, SubVolume and Volume protection
6. SubVolume protection
7. Volume Protection
8. SubVolume and Volume protection

Thus for reasons of simplicity it was decided to display the file data, i.e. Name, Modification date, Size, Owner and Protection Status for all files.

```
Name     Last Modified         Size Status LPCP PassFail PassFail Owner   RWEPO
ZTEST    07-Aug-2010 17:12   63,331 Subvolume Protection          127,001 NNNN
```

If the file was protected as a DISKFILE object to include the Licensed, ProgId'd, Clear on Purge and Persistent Flags as letters in an LPCP column and have columns for Audit-Access Audit-Manage with sub columns for the Pass and Fail Auditing Actions with ***, LOC, REM ALL for the None, Local, Remote and All Audit Log Actions.

```
Name     Last Modified         Size Status LPCP PassFail PassFail Owner   RWEPO
ZLIST4   14-Nov-2008 12:29   63,331 Thawed NNNN *** ***  *** ***  127,001 ****
```

The DISKFILE ACL was to be put in a separate rows at the end of the Display with an explicit statement as to whether Access was GRANTED or DENIED or even ABSENT. With a reference to the Higher level protection record, if one existed.

```
ZSTUB    18-Nov-2008 14:25   63,331 Thawed NNYY LOC ALL  REM ***  127,001 ****
         (+SubVol, see below)       Access Control List     GRANT 127,001 RWEP
                                                            DENY  127,004  W P


ZLIST4   14-Nov-2008 12:29   63,331 Thawed NNNN *** ***  *** ***  127,001 ****
         (+SubVol, see below)       Access Control List     ABSENT
```

As well at the file line changes it was also decided to include extra lines reporting on the SUBVOLUME and VOLUME protection Status with associated ACLs.

```
SAFEGUARD Data for Subvolume \SIRIUS.$WORK.NATIVE
Status Owner     Audit-Access  Audit-Manage  Access-Control-List
                 Pass   Fail   Pass   Fail   Mode  Owner   RWEPOC
Thawed 127,001   NONE   NONE   NONE   NONE   GRANT 127,*   RWEPOC
```

There was also a change made in the level at which Volume/SubVolume Information was displayed. Previously if only a subvolume was displayed then the Volume information was not also displayed. However, since the Volume Protection is significant, if a volume is SafeGuard protected then its summary information is also added at the end of a display.

Finally, the global diskfile SAFEGUARD settings are very important in determining how the ACLs are evaluated, and so this information was appended to the start of the display, together with the global SAFEGUARD auditing information.

Also to improve readability it was decided that when there was an ACL that there should be a space after it to separate it from the following file data and also, when there was not ACL associated with a DISKFILE object that the word ABSENT should be used to retain clarity of output.

The complete display has the format:

```
$WORK NATIVE 28> finfo33 -g
FINFO V3.3  Native 08/08/2010 14:33
-----
Copyright Ross Systems International Ltd. 2008,2009,2010

Full Version (Release Date 28th July 2010)
------------------------------------------

SAFEGUARD Diskfile System defaults
----------------------------------
Check Volume: OFF, Check SubVolume:  ON, Check File Name:  ON
ACLs not required for File Access, but used if present
DISKFILE ACL must grant the requested access
Super Undeniable: YES

SAFEGUARD Auditing System
-------------------------
Current Audit File: $SYSTEM.SAFE.A0000441
Current Audit Pool: $SYSTEM.SAFE, Next Audit Pool: <not defined>
Max Files: 2, Max Extents: 16, Extent Sizes: (128, 128) pages
Current State: Recycling,  Write Through Cache:  NO,  EOF Refresh:  NO

Files on \SIRIUS.$WORK.NATIVE                         Audit
                                    Safeguard    Access   Manage
Name     Last Modified         Size Status LPCP PassFail PassFail Owner   RWEPO
ZLIST4   14-Nov-2008 12:29   63,331 Thawed NNNN *** ***  *** ***  127,001 ****
         (+SubVol, see below)       Access Control List     ABSENT

ZSTUB    18-Nov-2008 14:25   63,331 Thawed NNYY LOC ALL  REM ***  127,001 ****
         (+SubVol, see below)       Access Control List     GRANT 127,001 RWEP
                                                            DENY  127,004  W P

ZTEST    07-Aug-2010 17:12   63,331 Subvolume Protection          127,001 NNNN

Selected User Totals for SubVolume \SIRIUS.$WORK.NATIVE
User No  User Name           Files           Bytes Used      Pages Used
127,001  RSI.RUPERT             57            4,600,550           2,658
Totals:                         57            4,600,550           2,658

SAFEGUARD Data for Subvolume \SIRIUS.$WORK.NATIVE
Status Owner    Audit-Access  Audit-Manage  Access-Control-List
                Pass   Fail   Pass   Fail   Mode  Owner   RWEPOC
Thawed 127,001  NONE   NONE   NONE   NONE   GRANT 127,*   RWEPOC
```

Note: It is not possible to demonstrate within the scope of a white paper all the possible combinations of Volume, SubVolume and File ACLs together with the corresponding system settings. However, FINFO is sensitive to all these combinations and does explicitly give usage and status information for all ACLs selected and describes the linkage between the various SAFEGUARD records protecting the HP NonStop data store.

EXCEL Export Format (-XG)

This part of the functionality of FINFO led to a departure from the normal procedure of outputting one row per file because of the change of the file permissions structure from Guardian to SafeGuard. Under Guardian the file permissions can be put into an orthogonal array whereas under SafeGuard the permissions is a branching tree structure fanning out from the File itself into the DISKFILE, SUBVOLUME AND VOLUME objects with their associated ACLs. All of which need to be put into an orthogonal array, depending on the ACLs used, which itself is dependent on the global check volume, check subvolume and check diskfile settings.

It was thus decided to have the file information repeated for each individual ACL which applied to it thus the EXCEL table is designed to have the general structure:

File Name	Guardian Details	SafeGuard Type	SafeGuard Data	ACL Data
MyFile	Details	FILE	File Object Data	File ACL 1
MyFile	Details	FILE	File Object Data	File ACL 2
MyFile	Details	FILE	File Object Data	File ACL 3
MyFile	Details	SUBVOLUME	SubVol Object Data	SubVol ACL 1
MyFile	Details	VOLUME	Volume Object Data	Volume ACL 1

This data is then amenable for analysis using the standard spreadsheet/database tools for importing into reports. For instance it is easily possible to determine the level of access for any user in the system, i.e. to what he is granted/denied access and the auditing which will be applied to him. It was also decided that since the safeguard information was not required in all circumstances that the original –X command would be reserved for the classical guardian export format and –XG would be the modified version of the command for SafeGuard information.

The Safeguard Columns contain:

SafeGuard Level	File, Subvolume or Volume
SFG Status	Frozen or Thawed
SFG Owner	Group, User with * for wildcard
SFG Licensed	YES or NO
SFG ProgId	YES or NO
SFG Clear On Purge	YES or NO
SFG Persistent	YES or NO
Audit Access Pass	***, LOC, REM or ALL
Audit Access Fail	***, LOC, REM or ALL
Audit manage Pass	***, LOC, REM or ALL
Audit manage Fail	***, LOC, REM or ALL
ACL Type	GRANT or DENY
ACL Owner	Group, User with * for wildcard
ACL RWEPCO	Letters to represent (Read, Write, Execute, Purge, Create or Owner) Permissions.

The extracted table below shows the relationship between the File Names, SafeGuard Data and ACLs.

Volume	Sub Volume	FileName	Other Guardian Data	SafeGuard Level	SFG Status	SFG Owner	Other SFG Data	ACL Type	ACL Owner	ACL RWEPCO
$WORK	NATIVE	ZLIST4	…	FILE	Thawed	127,001	…	No ACL		
$WORK	NATIVE	ZLIST4	…	SUBVOLUME	Thawed	127,001	…	GRANT	127,*	RWEPOC
$WORK	NATIVE	ZSTUB	…	FILE	Thawed	127,001	…	GRANT	127,001	RWEP
$WORK	NATIVE	ZSTUB	…	FILE	Thawed	127,001	…	DENY	127,004	W P
$WORK	NATIVE	ZSTUB	…	SUBVOLUME	Thawed	127,001	…	GRANT	127,*	RWEPOC
$WORK	NATIVE	ZTEST	…	SUBVOLUME	Thawed	127,001	…	GRANT	127,*	RWEPOC

Conclusions

The growing operational challenge of implementing ISMS with their requirement for effective auditing of both use and configuration of systems has revealed a need for an improved reporting mechanism for HP NonStop SAFEGUARD protected DiskFile, SubVolume and Volume objects.

FINFO version 3.3 onwards meets this need with a well considered SAFEGUARD file selection and reporting facility.

This capability takes full account of the SafeGuard Object Structure for the HP NonStop Data Store (File/SubVolume/Volume) with associated ACL Permission/Denial structures and global SAFEGUARD settings.

It provides functionality for both report generation and the export of SAFEGUARD file protection data into spreadsheets for further analysis and reporting.

This new functionality is in addition to its extensive Guardian system management reporting.

It is designed to save a considerable amount of systems management time and money.
It does this by providing a clear concise and intuitive method of generating and displaying management reports of both the Guardian file system and also the SAFEGUARD File System configuration.

The program has superb technical performance produced by its optimisation to reduce the system load and execution time to a minimum. This is achieved by reducing the number of system calls to the minimum necessary and the object code executing in native mode on the target processor.

FINFO Version 3.3 is reasonably priced and provides a very cost effective and comprehensive integrated file reporting tool for the HP NonStop platform. We also have a policy of providing our customers with free product upgrades and pegging the license fees to a given price line determined by inflation and RPI. This means that early adopters of our products are shielded from the effects of quantum leaps in price associated with major releases.

Feedback from stakeholders in the NonStop platform is very important to us and provides many of the ideas for the future development of our products and so your comments will be very welcome. Hence, we are offering 30 day trial licenses with technical support so that you can fully appraise the product.

FINFO Version 3.4 is already in the planning stage. It will be a major release with the inclusion of a Java based GUI, TCP/IP and SPI interface, contact us and be part of the process.

eMail: info@rsi-ns.com

web: www.rsi-ns.com