GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials (Security 401)"
at http://www.giac.org/registration/gsec

HP NonStop Security – A Practical Guide

Robert Larson

January 13, 2003

Summary

The objective of this paper is to present a new security administrator with an overview of the administrative structure for platform security on an HP NonStop computer system. The three security environments on the HP NonStop are introduced. Basic components of the Safeguard utility are described and examples of its use are provided. An important component, Safecom, allows the administrator to maintain the Safeguard environment while the object type records provide the administrator with control over the security environment. The unique features of the NonStop user ids are shown with an example and the alias concept is explained. Authorization and auditing functions are discussed. The paper concludes with a list of third-party vendors of HP NonStop security enhancement products.

Introduction

The HP NonStop computer system has gone through several name changes. The original fault tolerant systems were developed and marketed by the Tandem Computer Corporation. Several years ago Compaq purchased Tandem and it's fault-tolerant computers. In 2002, HP (Hewlett Packard) purchased Compaq and has renamed the Compaq Himalaya servers the HP NonStop S-series servers. One of the system's features that provides fault-tolerant, continuous availability to stock exchanges, retail, and financial institutions is a multifunction processor unit with two central processing units executing the same instructions. The multifunction processor unit's CPUs are connected by multiple paths to routers that provide access to the other elements of the server. Each server can have 2 to 16 independent processor units. The NonStop Kernel operating system runs in each CPU.[1]

Platform security for the HP Nonstop can be viewed at three levels, the kernel or Guardian level, the Safeguard (operating system security utility) level and third party software level. The emphasis will be on the Safeguard level.

The paper will describe the authentication, authorization and auditing aspects of securing a single node. Securing the Posix environment will be touched on. Finally, third party vendors will be identified.

Security standards are important

Here standards refer to the platform security standards derived from the institution's security policies. The standards must be published and be accepted by management of the involved Information Technology departments and the business units that use the platform for their systems. Early awareness of the security standards by the persons from the departments that do their work on the

1 hp NonStop S-series servers http://nonstop.compaq.com/view.asp?IO=SSERIESPD

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

systems is essential to the ability to implement successful platform security. The standards dealt with in this paper are described in Patrick Jones' "Organizational Information Security from Scratch" at rr.sans.org/standards as follows:

- "User Access Administration - Consistent procedures for controlling user access in all corporate systems help to ensure effective control of proprietary information. This policy defines access administration procedures"
- "Computer Applications - Internal Control / Program Security - To ensure that all mechanized applications are configured for maximum performance and security.."
- "Audit Trails, Security Review Procedures - The consistent collection of data throughout all systems and establishment of sound review procedures ensure that the data needed to analyze unauthorized changes (intentional and inadvertent) to corporate data bases are available."[2]

Without these standards in place and without the awareness and buy-in by the developers and business users, the chances for a satisfactory security implementation will not be good.

Administrative structure

Starting with a new system

Guardian

When a new NonStop system is booted (coldloaded) the security is under the Guardian NSK Operating System control. Only two users exist, a root user, named Super Super and a null user named Null Null. The super ID has unrestricted access to files, devices and processes, including Safecom. The Null Null user should be deleted as it is no longer needed by the current versions of NSK.

A user name and user identification number identify HP NonStop users. Each user name is associated with its unique user id number. The form of the NonStop user name is specific to the NonStop platform. It consists of a group name and a user (member) name separated by a period; i.e. Group name.member name. The group name is unique to the system node and the member name is unique within the group-name. The user identification consists of a group number and a member number separated by a comma; i.e. group number,member number. The Guardian group numbers range from 0 through 255 and are called administrative group numbers to distinguish them from file-group numbers used in the Posix operating environment.

Under Guardian, the Super user can create additional users. Of the sixteen commands related to Guardian security these three are the principal commands for processing user ids.

- ADDUSER - Adds new users to the system
- DELUSER - Deletes users from the system
- PASSWORD - Selects, changes, or deletes a local password

[2] Organizational Information Security from Scratch – A Guarantee for Doing It Right Patrick Jones, July 18, 2001 http://rr.sans.org/standards/scratch.php

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

There are three classes of Guardian users, in addition to the Super user.

- Super group – Performs various system functions such as managing system files, disks, and other devices. This group is for the operations and system administration users. The user ID is 255,n, where *n* is an integer from 0 to 254
- Group managers – Are responsible for members of their specific user group. The manager id can maintain the user ids within its group. The user id is g,255 where g is the group number.
- Application users - Log on to a system to run one or more specific applications. This includes developers on a development system as well as applications on a production system.[3]

HP NonStop security best practice is to start Safeguard and perform the security functions under Safeguard as soon as the system is operational.

Safeguard

Safeguard is a NonStop system-level utility that upgrades the operating system security. It can provide access control lists for volumes, subvolumes, and files, as well as devices, and processors. It can also be set up to write to audit logs.

The most secure (hardened) method of running Safeguard is to start it during the system initialization process. This will cause Safeguard to run continuously from the time the system is initialized until it is shut down. Consequently, it requires the highest level of experience with Safeguard and the operating system. If the security administrator and the Super user become locked out – inadvertently or due to a malicious attack – the system must be shutdown and restarted with a clean operating system image. The trick here is to have a backup system image CIIN file that does not start Safeguard; that is, a CIIN file with no Safeguard command in it. (The CIIN file is a startup file that contains a limited set of commands, one of which will start the Safeguard processes.) The system can then be started from this backup image and the Super id can gain control of the Safeguard processes without restarting from a SUT tape, which is the site update tape from HP used to load the operating system on the system hardware.

The second method of running Safeguard is to start it after the operating system has been initialized. Running the OSMP program out of the system subvolume starts Safeguard. In this case, running the Safecom Stop command can stop it. If Safeguard is stopped the operating system reverts back to Guardian security. This method of running Safeguard is less secure than the first. The level of security depends on how well the Safeguard assets are protected by Safeguard itself. A new security administrator may wish to initially run Safeguard in this manner but the goal should always be to arrive at the first method.

[3] Security Management Guide, HP Systems Software Library, part number 118610

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

OSS (Open System Services)

The Open System Services environment on the HP NonStop computer provides user and programming interfaces that are similar to those of a UNIX operating environment. The HP NonStop OSS is based on the Posix (Portable Operating System Interface)[4] standards and the X/Open Portability Guide, XPG4.

The OSS environment coexists with the Guardian environment. Security functions are run from the two environments. The Guardian Safeguard utility is required to maintain user and group access to OSS resources (authentication). Access to OSS files and directories is controlled by OSS functions, chmod, chgrp, and chown (authorization). A caveat here is that Safeguard volume-level security, if used , must be synchronized with permissions on file set pools that are spread across physical disk volumes.

The OSS environment will come pre-installed on the HP NonStop system or will be installed by the system administration group. Part of the configuration process will be to ensure that Safeguard is running and that users have been created with access to the OSS environment.

Using Safeguard to secure the system

Safecom

Safecom is the command interpreter that lets the security administrator set user authentication, object-access authorization, and auditing on systems that Safeguard controls. Safecom has a standard set of commands that can be used, with few exceptions, to manipulate all Safeguard user and object records. The commands are

- Add
- Alter
- Delete
- Freeze
- Reset
- Set
- Thaw

Administrative commands include:

- Assume – a default object class for ensuing commands
- Display – allows the user to control the information displayed by certain commands
- Exit – to end the Safecom session
- FC – displays previous commands with the ability to edit them
- History -- displays a list of previous commands
- Info – displays attributes for the object
- Log – specifies a log file for capturing Safecom commands
- Obey – accepts an input file of Safecom commands

[4] The IEEE's Portable Application Standards Committee develops the POSIX family of standards, http://www.pasc.org/; see also http://www.wikipedia.org/wiki/POSIX

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

- Show – displays the current default attributes for the object

Objecttype records

Understanding the usage of objecttype records is fundamental to gaining control of the HP NonStop Safeguard security environment. By default, Safeguard allows any user in the Super group, not just the Super user, to create volume, device, and subdevice control records. Any user can create Safeguard control records for processes, subprocesses, subvolumes, and disk files, by default. This provides for a very uncontrolled security situation. The way to gain control this is to create Safeguard objecttype records that will only give the security administration group, and trusted users the ability to create Safeguard control (authentication) records.

The Safeguard Objecttypes are as follows.

- Diskfile
- Subvolume
- Volume
- Device
- Subdevice
- Process
- Subprocess
- Objecttype
- User

Each objecttype record can have two control attributes and four standard audit attributes. The control attributes are

- Access
- Owner

The access attribute defines the access control list of users that can create Safeguard records for the named object. The owner attribute defines the user(s) that controls the specific objecttype record. Only the owner can change the access control lists or the owner and delete the entire record.

First, have a super group user transfer control of the Objecttype Objecttype record to the security administration users by giving them access and owner rights. Then the security administrators can add objecttype records for all the other objecttypes using the access and owner attributes. At that point, the security administrators will (almost) have control of Safeguard security.

Authentication

Creating and maintaining user ids

All user ids are created and maintained by the Safeguard utility as soon as it is activated. Users can access both the Guardian and OSS environments. When Safeguard is activated, any use of the Guardian Adduser and Deluser commands is controlled by Safeguard. To review the structure of the HP NonStop user naming and numbering conventions refer to Guardian, under Administrative Structure.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

During the security planning phase, a security-centric or a decentralized model will be adopted for user id maintenance. Under a decentralized model, the Super Super user can create any user ids and group managers, (group-number,255) can create users within their group. Under a security-centric model, the Safeguard Objecttype User is created. The Objecttype User record will be set up so that the security administration group users can control the maintenance of user ids. The maintenance function may be delegated to an Access Control group with proper documentation and protection in place.

Let us assume that we need an application group called Claims. The following command will provide the minimum information required to add the owner of the Claims application.

```
Add user claims.owner     , 175,200 ,password 8charact
```

The other user attributes will be default attributes.

Let us suppose that the id was created with the following attributes.

```
GROUP.USER    USER-ID   OWNER   LAST-MODIFIED LAST-LOGON   STATUS
claims.owner  175,200   249,2     10jan04,     NONE *    USER-EXP

  UID                          =     45000
  USER-EXPIRES                 =    * NONE *
  PASSWORD-EXPIRES             = 09jan04, 00:00
  PASSWORD-MAY-CHANGE          =    * NONE *
  PASSWORD-MUST-CHANGE EVERY   =     63 DAYS
  PASSWORD-EXPIRY-GRACE        =      8 DAYS
  LAST-LOGON                   =    * NONE *
  LAST-UNSUCCESSFUL-ATTEMPT    =    * NONE *
  LAST-MODIFIED                = 10jan04,  9:41
  FROZEN/THAWED                = THAWED
  STATIC FAILED LOGON COUNT    =      0
  GUARDIAN DEFAULT SECURITY    = NCCC
  GUARDIAN DEFAULT VOLUME      = $DATA01.CLAIMDB

  AUDIT-AUTHENTICATE-PASS = ALL        AUDIT-MANAGE-PASS = ALL
  AUDIT-AUTHENTICATE-FAIL = ALL        AUDIT-MANAGE-FAIL = ALL
  AUDIT-USER-ACTION-PASS  = NONE
  AUDIT-USER-ACTION-FAIL  = NONE

  CI-PROG = $SYSTEM.SYS33.OSH
  CI-LIB  = * NONE *
  CI-NAME = * NONE *
  CI-SWAP = * NONE *
  CI-CPU  = * NONE *
  CI-PRI  = * NONE *
  CI-PARAM-TEXT =

  INITIAL-PROGTYPE = PROGRAM
  INITIAL-PROGRAM  = /bin/ksh
  INITIAL-DIRECTORY = /home/owner

  PRIMARY-GROUP = CLAIMS
  GROUP         = CLAIMS
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
REMOTEPASSWORD = \KLAIM   owner

SUBJECT DEFAULT-PROTECTION SECTION UNDEFINED!
```

The user id's attributes are explained in HP's *Safeguard Reference Manual—520618-001*. The items below point out some interesting aspects of the attributes.

- UID is the user ID number for the OSS environment. The UID is calculated from the user's group number and user number. UID = (group number times 256) plus user number.
- User-expires can be set to a future date for temporary users such as contractors.
- Password-expires can be set to a date in the past so that the user will have to change their password the first time they log on.
- Frozen/Thawed indicates whether a user can log on (Thawed) to the user id or not (Frozen). Processes can still be run for programs owned by a frozen user id.
- Static failed logon count is the number of unsuccessful logon attempts for the user id. There doesn't seem to be any way to reset the attribute.
- Guardian default volume is the user's home subvolume when they log on.
- Audit-authenticate-pass/fail indicates if and when a user's logon attempts will be written to a Safeguard audit log.
- Audit-manage-pass/fail indicates if and when attempts to change the user authentication record will be written to a Safeguard audit log.
- Audit-user-action-pass/fail indicates whether or not to audit the user's attempts to access volumes, subvolumes, files, processes and devices. It also indicates whether or not to audit attempts by the user to manage Safeguard authorization records.
- The three Initial attributes provide the user's initial working directory in OSS and the initial program pathname in OSS. The Initial-progtype attribute is not implemented at this time.
- Group includes all of the groups to which the user id belongs. In addition to the user's administrative group, it can be assigned to as many as 31 file groups for OSS.
- Remotepassword indicates the name of the system for which the user has a remote password as well as the password. Multiple remote passwords are possible to any NonStop nodes on a network. Remote passwords are kept in the clear and are used to let the user remotely access resources on another system.

Using aliases

Aliases, or additional names, may be attached to a Guardian user id. Aliases provide Unix-like names as alternatives to NonStop Guardian names for Unix users in the OSS environment. Aliases also provide granularity for separation of duties and auditing user access to system resources. This is especially useful when developers need access to a production system to troubleshoot problems.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Each developer can be given an alias under the production owner user id. Each alias can be tracked using its audit attributes.

Aliases are added using the Safeguard utility command Add Alias. The basic Add Alias command is the same as the Add User command.

```
ADD ALIAS Claims_Jen, 175,200 , PASSWORD Jen45678
```

The Add Alias command attaches the alias to the user id claims.owner (175,200). An alias has the same attributes as a user id but the attribute values can be completely different from those of the underlying user id. (See user id attributes in Creating and maintaining user ids, above.)

The alias name is free form, up to 32 characters long. It is case sensitive and can contain alphabetic, numeric, and the special characters period, hyphen, and underscore. It can not have the same name, in upper or lower case, as a user id; for example, CLAIMS.OWNER.

An alias's access to files is controlled differently in the Guardian and the OSS environments. In the Guardian environment, access to files, or processes and devices, is based on the alias's underlying user id. Safeguard access control lists for files only specify user ids. The alias inherits the Guardian access rights of its user id. In the OSS environment, an alias can be assigned to up to 32 file-sharing groups that are found in the Group attribute. When an alias user attempts to access an OSS file, the file's group permissions will determine the alias's access rights if the alias belongs to the file group. If not, the file's world permissions are used.

Authorization using access control lists

Safeguard controls access to Guardian disk files at the volume, subvolume, and file levels. OSS file access is controlled by the OSS (Posix) permissions structure.

This section uses a production environment as the example for giving users Safeguard authorization rights to Guardian files. The access control plan will consider the production application (user) owner, data base manager, change control functions, developers, production control, and possibly file transfer users.

Guardian production files will usually be segregated in subvolumes by usage. Typical subvolume categories are databases, flat files, executable files, library files, script files and batch files. The Insurance Claims production group, (Claims), will require access rights for the following user groups, Database manager (DBM), change control (CCM), production control (PCM), and file transfers (XFR).

Subvolume access control lists

Access will be controlled at the subvolume level. Use the Safecom utility to create the subvolume ACLs. Safecom allows the following access authorities for subvolumes.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

- Read - to read disk files within the subvolume
- Write - to write to disk files within the subvolume
- Execute - to execute program files within the subvolume
- Purge - to remove disk files from the subvolume
- Create - to create a disk file on a subvolume
- Owner - to change the authorization record on the subvolume

For the database subvolume, $disk01.claimdb, give the production user read and write access, the local database manager all accesses except owner, the remote database manager read and write access, remote production control read access, deny all but read access to the Super user, and make the security administrator owner of the authorization record. Use the following Safecom commands to do this.

```
Add subvolume $disk01.claimdb, access \*.Claims.owner (r,w);    &
Dbm.mgr (r,w,e,p,c);  \*.Dbm.mgr (r,w);  \*.Prod.cntrl r;       &
Super.super  deny (w,e,p,c); Sec.admin  o
```

The Safecom Info command will show the following results:

```
                    LAST-MODIFIED     OWNER    STATUS
$DISK01.CLAIMDB
                  24DEC02, 11:17  \*.220,220  THAWED

          175,200       R,W,E,P,C
        \*.077,250       R,W
        \*.175,200       R,W
        \*.220,220                 O
        \*.255,005       R
        \*.255,255 DENY    W,E,P,C
```

The application owner is Claims.Owner (077,250). The owner is given remote access so that it can work between the primary and backup production systems. Remote access implies local access as well unless local access is explicitly defined. The database manager (175,200) can only read and write database records from another system while they can also execute programs, purge and create database files from the local system. The 24X7 production control user (255,005) is given remote read access to assist with first level troubleshooting. Because the Super user (255,255) may implicitly have all accesses, everything except read access is denied on production database subvolumes. Note that remote users are specified by *. This means the remote user access will be accepted from any node where the user has a remote password. The developers will have access to the production environment as aliases to the Claims.Owner. Aliases are discussed in the Authentication section.

An existing subvolume acl list can be changed by deleting the entire entry or by altering the contents. The acl lists can be changed with the instructions in the Alter command. The minus sign can be used to remove existing accesses and wild cards, * and ?, can be used to define the subvolumes; for example,

```
Alter subvolume $disk*.claimdb, access \*.Dbm.mgr – e
```

will remove the execute access for Dbm.mgr on the claimdb subvolume on all volumes starting with $disk.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

The same procedure can be used to add access lists to the subvolumes for flat files, executable files, libraries, script files, and batch files.

File-level access control lists

Occasionally, individual files within a subvolume will require nonstandard security.
Let's say the Betting file should only be accessed by the Super user. Assuming a bottom-up direction for the Direction-diskfile configuration attribute, the security can be added as shown below.

```
Add diskfile $disk01.claimdb.betting  access super.super (r,w,e,p,c)
```

The Safecom info command will show the following results.

```
                    LAST-MODIFIED     OWNER    STATUS
$DISK01.CLAIMDB
 BETTING         24DEC02, 13:47  \*.220,220  THAWED

           255,255       R,W,E,P,C
```

Note that the Betting file must exist before Safeguard will add an authorization record for that file. The administrator may have to create a dummy file prior to running the diskfile add command. The file can be deleted and the acl will remain if the diskfile Add command includes the Persistent On attribute.

The following attributes can be defined for disk files.

- License ON or OFF
- Progid ON or OFF
- Clearonpurge ON or OFF
- Persistent ON or OFF

The License attribute allows programs that can only be run by the Super user to be run by other users. The privileged programs normally contain restricted code written by HP to bypass all Safeguard and Guardian security restrictions. Only the Super user can turn the license attribute On but any user with access to the program can turn it off. The attribute should have reserved for object files specified by HP or a trusted vendor.

The Progid attribute allows the user id that owns a program (process accessor id) to be changed. By default, the process accessor id, or Paid, is the id of the user running the program. With Progid set to On the program's Paid becomes that of the user id that owns the program file. This becomes important where access to the files used by the process is restricted to the owner of the process.

If the Clearonpurge file attribute is On Safeguard will overwrite the file space with null characters when it is deleted.

If the Persistent file attribute is On the Safeguard authorization record will not be removed if the file is purged. If a file is purged and then recreated the Safeguard

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

acl will be reinstated for the new file. Conversely, if persistent is Off and the file is purged the Safeguard acl is lost.

Audit attributes

The Safeguard authorization records for volumes, subvolumes, and files provide the capability to audit attempts to access their associated files and to manage the associated authorization records. The following attributes can be activated.

```
AUDIT-ACCESS-PASS
AUDIT-ACCESS-FAIL
AUDIT-MANAGE-PASS
AUDIT-MANAGE-FAIL
```

As the name implies, the Access-pass attribute specifies the condition for writing an audit log record when a file is successfully accessed. The Access-fail attribute establishes the condition when an access attempt fails. By definition, a file is accessed when it is opened, renamed, or purged. A program executable file is also accessed when it is executed.

The Audit attribute for file access may be `ALL, LOCAL, REMOTE,` or `NONE.`
If the attribute is All both local and remote access attempts will be logged. If the attribute is Local only attempts by local users will be logged. If the attribute is Remote only attempts by remote users will be logged. If the attribute is None no attempts will be logged. The default setting is None.

The Manage-pass attribute establishes the condition for writing an audit log record when a Safeguard volume, subvolume, or file authorization record is successfully maintained.
The attribute values are the same as those for the Audit attributes above.

The two principal considerations for turning on file access logging are the criticality and sensitivity of the data in the file and the overhead created by the logging processes. A good policy; especially on production machines is to turn On both Audit-manage-pass and Audit-manage-file. Any audit logging is useless if the information in the logs can not be retrieved in a usable form. Although Safeguard provides the Safeart tool for reading and reporting on data in Safeguard audit logs third party products are often used to do the reporting.

Help from Third Party Software

Because security is an ongoing process there are always opportunities for third party vendors to provide solutions that will improve the overall protection of any platform. The HP NonStop platform has a diverse group of third party companies that provide security add-ons. Some examples are provided here. They should not be considered all encompassing or necessarily the best of breed. Each user organization must do their own analysis to decide what works best for them.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Xypro Technology Corporation[5] has a series of products that work with Safeguard to provide security enhancements and granularity for securing and auditing system assets. They also have encryption products.

GreenHouse Software & Consulting[6], a German company, provides security enhancement and encryption products and, maybe best of all, several freeware products to automate some of the tedious security administration tasks.

Cross-el Software Solutions[7] provides secure access solutions for the HP NonStop platform.

Computer Security Products, Inc.[8] has a complete replacement product for Safecom, the command interpreter that maintains Safeguard records. They also have a wide range of security enhancement products.

Baker Street Software[9] offers a broad choice of security enhancement products.

Conclusion

This paper only touches the surface of a complete package of platform security for the HP NonStop. While the security structure of the HP NonStop platform is unique it has its roots in the Unix-like world. The inclusion of the OSS environment has provided an additional challenge for the Safeguard-oriented security administrator. Opening up the platform to the Internet will continue to provide new security challenges, as it has for other operating systems.

List of References

1. **hp NonStop S-series servers,** http://nonstop.compaq.com/view.asp?IO=SSERIESPD
2. **Organizational Information Security from Scratch – A Guarantee for Doing It Right**, Patrick Jones, http://rr.sans.org/standards/scratch.php
3. Security Management Guide, HP Systems Software Library, part number 118610
4. The IEEE's Portable Application Standards Committee develops the POSIX family of standards, http://www.pasc.org/; see also http://www.wikipedia.org/wiki/POSIX
5. Xypro Technology Corporation, http://www.xypro.com/
6. GreenHouse Software & Consulting, http://www.greenhouse.de
7. Cross-el Software Solutions, http://www.crossel.com
8. Computer Security Products, Inc., http://www.cspsecurity.com
9. Baker Street Software, http://www.bakerstreetsoftware.com

[5] Xypro Technology Corporation, http://www.xypro.com/
[6] GreenHouse Software & Consulting, http://www.greenhouse.de
[7] Cross-el Software Solutions, http://www.crossel.com
[8] Computer Security Products, Inc., http://www.cspsecurity.com
[9] Baker Street Software, http://www.bakerstreetsoftware.com

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.