

G06.29 Release Version Update Compendium

Abstract

This compendium provides a summary for the products that have major changes in the G06.29 release version update (RVU), including the products' new features, migration issues, and fallback considerations. The compendium is written for system managers or anyone who needs to understand how migrating to G06.29 affects installation, configuration, operations, system management, maintenance, applications, networks, and databases.

Product Version

N.A.

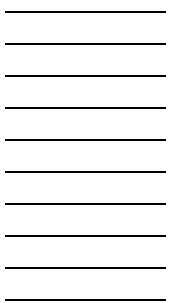
Supported Release Version Updates (RVUs)

This publication supports the G06.29 RVU only.

Part Number	Published
542946-001	July 2006

Document History

Part Number	Product Version	Published
542946-001	N.A.	July 2006



G06.29 Release Version Update Compendium

Tables

- [What's New in This Manual](#) iii
- [Manual Information](#) iii
 - [New and Changed Information](#) iii
- [About This Manual](#) v
- [Who Should Use This Guide?](#) v
 - [Organization](#) v
 - [Related RVU Manuals](#) v

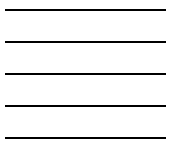
1. G06.29 Overview

- [Major New Features](#) 1-1
- [Products Removed From the Site Update Tape \(SUT\)](#) 1-2

2. Operating System

- [NonStop Operating System](#) 2-1
 - [Migration](#) 2-1
 - [Fallback](#) 2-1
- [OSS ACLs](#) 2-2
 - [Migration](#) 2-3
 - [Fallback](#) 2-3
- [OSS Files Larger Than 2 GB](#) 2-3
 - [Large OSS File Aware and Large OSS File Safe Applications](#) 2-3
 - [Large OSS File Aware and Large OSS File Safe APIs](#) 2-4
 - [Interoperability](#) 2-6
 - [Migration](#) 2-8
 - [Fallback](#) 2-10
- [OSS Standard Posix Threads](#) 2-11
 - [Migration](#) 2-12
- [OSS Standard Security APIs](#) 2-12

3. Application Development Products**4. Database and Transaction Processing Products**[SQL/MP](#) 4-1**5. Installation and Configuration Products**[DSM/SCM](#) 5-1**6. Manageability Products**[Safeguard](#) 6-1[Encryption](#) 6-1[Safeguard Support for OSS ACLs](#) 6-2[Migration in a Safeguard Environment](#) 6-2[Fallback in a Safeguard Environment](#) 6-3[Migration With Standard Security \(Safeguard Not Installed\)](#) 6-4[Fallback With Standard Security \(Safeguard Not Installed\)](#) 6-4[Fallback Considerations for OSS ACLs](#) 6-4[Additional Technical Information](#) 6-4[OSM and TSM](#) 6-5[Installation and Configuration](#) 6-5**7. Hardware Products**[NonStop S-Series Servers](#) 7-1[Tape Drives](#) 7-1**8. Networking Products**[SWAN](#) 8-1[Fallback](#) 8-1**A. Sources for Migration Assistance and Information**[ExpressNotice](#) A-1[Information on the Site Update Tape \(SUT\)](#) A-2[Scout for NonStop Servers](#) A-2[Global Customer Support Center \(GCSC\)](#) A-2[NonStop Technical Library \(NTL\)](#) A-2**Tables**[Table 1-1. Summary of the G06.29 RVU](#) 1-1



What's New in This Manual

Manual Information

Abstract

This compendium provides a summary for the products that have major changes in the G06.29 release version update (RVU), including the products' new features, migration issues, and fallback considerations. The compendium is written for system managers or anyone who needs to understand how migrating to G06.29 affects installation, configuration, operations, system management, maintenance, applications, networks, and databases.

Product Version

N.A.

Supported Release Version Updates (RVUs)

This publication supports the G06.29 RVU only.

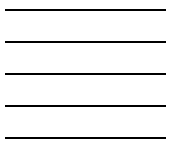
Part Number	Published
542946-001	July 2006

Document History

Part Number	Product Version	Published
542946-001	N.A.	July 2006

New and Changed Information

This is a new manual.



About This Manual

This compendium provides categorized information for new features, migration issues, and fallback considerations for G06.29. It also includes references and sources for migration planning.

Who Should Use This Guide?

This compendium is written for system managers or anyone who needs to understand how migrating to G06.29 affects installation, configuration, operations, system management, maintenance, applications, networks, and databases.

Organization

Section	Description
Section 1, G06.29 Overview	An overview listing the products that have major changes
Section 2, Operating System Section 3, Application Development Products Section 4, Database and Transaction Processing Products Section 5, Installation and Configuration Products Section 6, Manageability Products Section 7, Hardware Products Section 8, Networking Products	Categorized product information that summarizes: <ul style="list-style-type: none">● New features● Migration issues (if available)● Fallback considerations (if available)
Appendix A, Sources for Migration Assistance and Information	References and sources for migration planning

Related RVU Manuals

For a list of RVU and migration manuals, see [NonStop Technical Library \(NTL\)](#) on page A-2.

1 G06.29 Overview

This section lists the major new features for the G06.29 RVU.

Major New Features

For descriptions of new features, see the appropriate sections in [Table 1-1](#).

Table 1-1. Summary of the G06.29 RVU

Sections and Categories	Major New Features	Migration Alerts	Fallback Alerts
Section 2, Operating System	<ul style="list-style-type: none"> ● NonStop Operating System ● OSS ACLs ● OSS Files Larger Than 2 GB ● OSS Standard Posix Threads ● OSS Standard Security APIs 	X X X X	X X X
Section 3, Application Development Products	No new features.		
Section 4, Database and Transaction Processing Products	<ul style="list-style-type: none"> ● SQL/MP 		
Section 5, Installation and Configuration Products	<ul style="list-style-type: none"> ● DSM/SCM 		
Section 6, Manageability Products	<ul style="list-style-type: none"> ● Safeguard ● OSM and TSM 	X X	X
Section 7, Hardware Products	<ul style="list-style-type: none"> ● NonStop S-Series Servers ● Tape Drives 		
Section 8, Networking Products	<ul style="list-style-type: none"> ● SWAN 		X

Products Removed From the Site Update Tape (SUT)

No products are removed from the site update tape (SUT) at G06.29.

For recent product removal information, see the Discontinuation Notices at
<http://h20223.www2.hp.com/NonStopComputing/cache/77208-0-0-225-121.aspx>.

2 Operating System

The G06.29 RVU contains these changes for the HP NonStop operating system:

- [NonStop Operating System](#)
- [OSS ACLs](#)
- [OSS Files Larger Than 2 GB](#)
- [OSS Standard Posix Threads](#)
- [OSS Standard Security APIs](#)

NonStop Operating System

Beginning with 2007, daylight saving time (DST) for the United States changes. The NonStop Operating System (T9050) is enhanced to reflect the DST changes for 2007 and later.

Migration

- If the DST option is TABLE and you want to implement the new U.S. algorithm, follow one of these two steps:
 - Delete the DST transition values for 2007 and later by using the `DST_TRANSITION_DELETE_` Guardian procedure call and add the new DST transition values by using the `DST_TRANSITION_ADD_` Guardian procedure call. You can also use TACL statements to add the DST transition values.
 - Modify the existing values with the new DST transition values for 2007 and later by using the `DST_TRANSITION_MODIFY_` Guardian procedure call.
- If you are outside of the United States and currently are using the USA66 option but your countries are not adopting the new U.S. algorithm, follow these steps:
 - Change the DST option to TABLE.
 - Reset the processors and load the system.
 - Add the new DST transition values for 2007 and later by using the `DST_TRANSITION_ADD_` Guardian procedure call. You can also use TACL statements to load the DST table with the DST transition values.
- If the DST option is USA66, reset the processors and load the system to reflect the new DST transitions.

For details on the Guardian procedure calls, see the *Guardian Procedure Calls Reference Manual*.

Fallback

If the DST transition for 2007 does not display the correct time change, switch to the TABLE option and add the DST transition entries into the DST table for 2007 and later. If you use the TABLE option, you do not need to fall back to a previous SPR, because

the new SPR supports DST transition for 2007 and later for the TABLE option. If you fall back, a system load is required.

OSS ACLs

The G06.29 RVU adds support for access control lists (ACLs) for NonStop Open System Services (OSS) regular files, directories, first-in, first-out (FIFO) special files, and bound AF_UNIX sockets in OSS Version 3 filesets. OSS ACLs:

- Provide finer access control than standard UNIX permissions
- Support up to 150 ACL entries
- Support separate permissions for up to 146 users and groups in addition to the owner and the owning group
- Support default ACL inheritance
- Are based on the POSIX 1003.1e draft standard and the HP-UX implementation

Version 3 filesets are not supported on pre-G06.29 RVUs. To upgrade to a Version 3 fileset or to downgrade to a Version 2 fileset, you must use a G06.29 or later version of the `fsck` utility.

As of the G06.29 RVU, Version 1 filesets are not supported. Version 2 filesets continue to be supported. All new filesets created on systems running G06.29 and later G-series RVUs are Version 3 filesets.

The OSS Network File System (NFS) does not support OSS ACLs.

For more information about OSS ACLs, see the `acl(5)` reference page either online or in the *Open System Services System Calls Reference Manual*.

To restore backup tapes containing files on systems running G06.29 and later G-series RVUs onto systems running the G06.23 through G06.28 RVUs, install these Backup and Restore 2 and file system SPRs:

- Backup and Restore 2 SPRs:
 - T2721G06^AAL, BRCOM
 - T2722G06^AAL, BR2 TAPE SERVICES
 - T2749G06^AAL, BR2 DMA & CSP
 - T2750G06^AAL, B/R 2 DATA SERVICE
- The file system SPR T9055G11^AFI (for G06.23 through G06.26 RVUs) or T9055G12^AFJ (for G06.27)

Note. For G06.28, the required file system SPR is already included in the G06.28 SUT.

These SPRs are required because changes have been made to the information stored with each object.

Migration

As of the G06.29 RVU, Version 1 filesets are not supported. You must upgrade Version 1 filesets to Version 2 or Version 3 filesets.

To use OSS ACLs, you must first migrate to the G06.29 RVU and then you must migrate your existing filesets to Version 3 filesets. To migrate filesets, you must stop the OSS file system and the OSS environment and use the `fsck DIAGNOSE FILESET, UPGRADE` command as described in the *Open System Services Management and Operations Guide*.

Fallback

To fall back, you must install the previous SPRs for the OSS products and for DP2. In addition, in either of these cases, you must run `fsck` on the fileset to downgrade the fileset to Version 2:

- If the `fsck` utility has been run on a fileset to upgrade to Version 3 filesets
- If the fileset was created on a system running the G06.29 or later G-series RVU

When the fileset is downgraded to Version 2, any optional ACLs associated with the files in the fileset are lost.

OSS Files Larger Than 2 GB

As of G06.29, OSS supports files larger than the previous limit of approximately 2 gigabytes (GB) in the OSS file system, DP2, C run-time library, C++ run-time library, COBOL run-time library, and OSS utilities. The OSS file system and utilities can handle OSS files up to a limit of 1 terabyte, although the upper limit of the actual file size depends on the size of the volume containing the file.

OSS files are created with an underlying Guardian file format of Format 2 whenever creation is requested through a 64-bit API. Existing OSS files are converted to an underlying Guardian file format of Format 2 the first time they are accessed by either the new OSS 64-bit APIs or existing Enscribe APIs. Any program that uses the existing 32-bit APIs can open and access any OSS files smaller than approximately 2 GB.

Large OSS File Aware and Large OSS File Safe Applications

An application that is large OSS file aware (LFA) can process OSS files larger than 2 GB with the same functionality as processing OSS files smaller than 2 GB. Such an application is capable of handling large files as input and generating large files as output.

An application that is large OSS file safe (LFS) causes no data loss or corruption when it encounters an OSS file larger than 2 GB. It might not have the capability to process OSS files larger than 2 GB, but it has the appropriate logic to handle errors or warnings detected during file manipulation operations and fail gracefully.

As of G06.29, these SUT-based applications are large OSS file aware:

- Backup and Restore 2
- DSAP/DCOM
- FUP
- iTP Webserver
- FTP
- C/C++ compiler
- COBOL compiler
- OSS utilities and unsupported utilities

All other OSS applications (including utilities, tools, or libraries) are large OSS file safe for G06.29 and later RVUs.

Large OSS File Aware and Large OSS File Safe APIs

To support OSS files larger than 2 GB, new 64-bit file I/O APIs are available. These APIs can handle files larger than 2 GB and files smaller than 2 GB. The large OSS file aware I/O APIs include:

- `creat64()`
- `open64()`
- `ftruncate64()`
- `lseek64()`
- `fcntl()`
- `fstat64()`
- `lstat64()`
- `stat64()`
- `fstatvfs64()`
- `statvfs64()`
- `readdir64()`
- `ftw64()`
- `nftw64()`
- `glob()`

Existing file I/O APIs are modified to fail safely on OSS files larger than 2 GB. These APIs return an error (`E_OVERFLOW` or `EFBIG`) when an action cannot be performed on OSS files larger than 2 GB or an attribute cannot be represented for such a file. The large OSS file safe I/O APIs include:

- `creat()`
- `open()`
- `read()`
- `write()`
- `ftruncate()`
- `lseek()`
- `fcntl()`
- `fstat()`
- `lstat()`

- `stat()`
- `fstatvfs()`
- `statvfs()`
- `readdir()`
- `ftw()`
- `nftw()`

These native C run-time library APIs are large OSS file aware:

- `__ns_backup_fopen64()`
- `__ns_fopen64_special()`
- `fgetpos64()`
- `fopen64()`
- `fopen64_guardian()`
- `fopen64_oss()`
- `fopen64_std_file()`
- `freopen64()`
- `freopen64_guardian()`
- `freopen64_oss()`
- `fseeko64()`
- `fsetpos64()`
- `ftello64()`
- `scandir64()`
- `tmpfile64()`
- `tmpfile64_guardian()`
- `tmpfile64_oss()`

These native C run-time library APIs are large OSS file safe:

- `fclose()`
- `fflush()`
- `fgetc()`
- `fgetpos()`
- `fgets()`
- `fgetwc()`
- `fgetws()`
- `fopen_oss()`
- `fprintf()`
- `fputc()`
- `fputs()`
- `fputwc()`
- `fputws()`
- `fread()`
- `freopen_oss()`
- `fwrite()`
- `fscanf()`
- `fseek()`
- `fsetpos()`
- `ftell()`

- `getc()`
- `getchar()`
- `gets()`
- `getw()`
- `getwc()`
- `getws()`
- `getwchar()`
- `printf()`
- `putc()`
- `putchar()`
- `puts()`
- `putw()`
- `putws()`
- `putwchar()`
- `scanf()`
- `vfprintf()`
- `vprintf()`

The Native C++ run-time libraries do not have new 64-bit specific APIs in the C++ library products. However, the logic implementing `IOStream` classes is enhanced to be large OSS file safe for programs built with the regular compilation environment or large OSS file aware for programs built with the large file compilation environment (that is, macro `_FILE_OFFSET_BITS` is defined to have value 64.)

Interoperability

- Interoperability for file copy operations:

HP NonStop programs that are capable of copying files from one system to another behave appropriately when the target system runs on a pre-G06.29 RVU. The programs successfully copy files smaller than 2 GB, which appear as Guardian Format 1 files on the target system. The programs refuse, in a user-understandable way, to copy files larger than approximately 2 GB.

- Interoperability for opens of OSS files:

Applications running on a pre-G06.29 system can open any OSS file smaller than approximately 2 GB on a G06.29 or later system through either OSS or Enscribe APIs.

HP does not support OSS opens of OSS files larger than approximately 2 GB on systems running pre-G06.29 RVUs. However, because Enscribe has long understood Guardian Format 2 files, a program running on a pre-G06.29 system that uses Enscribe with 64-bit elections can open a large OSS file that resides on a G06.29 or later system. If the file is smaller than 2 GB, the file size limit for that open is 2 GB. If the file is larger than 2 GB, the file size limit for that open is the size of the volume.

- Interoperability for opens of Guardian C files:

As of G06.29, OSS can create Guardian files in the /G name space through `creat64()` and `open64()`. The resulting files, regardless of size, are Guardian Format 2 C files with file code 180. If a program running on any RVU attempts to open this type of file through `FILE_OPEN_` without 64-bit elections, the open succeeds if the file is smaller than approximately 4 GB and fails if it is larger than 4 GB.

If the open call includes 64-bit elections and is issued on a G06.29 or later RVU, the open succeeds regardless of file size.

If an application running on a pre-G06.29 system invokes `FILE_OPEN_` with 64-bit elections, the open succeeds. However, if the file size is smaller than 4 GB, the file size limit for that open is 4 GB. If the file size is larger than 4 GB, the file size limit for that open is the limit defined at file-creation time.

- Compatibility issue with Guardian files created by OSS APIs:

For G06.29, OSS adds support for files greater than 2 GB and adds related 64-bit OSS APIs. Previously, OSS files were always Guardian Format 1, but now may be Format 1 or Format 2. For applications using OSS APIs to access OSS files, the format is not visible and there are no known compatibility issues. For applications using Enscribe APIs to access Guardian files created by OSS APIs there is a known compatibility issue.

Prior to G06.29, Guardian files created by OSS APIs were always format 1 with a 175 MB maximum size. As of G06.29, Guardian files created by the `open()` and `creat()` APIs are Guardian Format 1 with an approximate 2 GB maximum size, and Guardian files created by the `open64()` and `creat64()` APIs are Guardian Format 2 with an approximate 26 GB maximum size.

The standard OSS utilities, such as `cp`, `pax` and `pinstall`, now use `open64()` and `creat64()` and thus create a Guardian Format 2 file when given a /G output file name.

Example:

```
cp myfile /G/disk/subvol/myfile
```

Guardian applications that use file attributes such as file format and maximum size are likely to be affected. These programs may fail when unexpected values are returned (such as Format 2 if only Format 1 is expected).

Guardian applications that use file data and ignore file attributes are unaffected, if running on G06.29 and the Format 2 file is unstructured, code 180 with an EOF less than the Format 1 limit of approximately 4 GB. However, `FILE_OPEN_` fails with error 580, if the RVU is pre-G06.29, or if the file code is not 180, or if the EOF is greater than the Format 1 limit.

Recovery choices include:

- Choice 1 - Change the application to accept Guardian Format 2 files.

- Choice 2 - Protect the application by converting the file to Guardian Format 1 using these steps:

```
FUP CREATE TEMP, FORMAT 1, TYPE U, ODDUNSTR, CODE 180, &
EXT (28,1400), MAXTENTS 749
```

```
FUP COPY MYFILE,TEMP
```

```
FUP PURGE MYFILE
```

```
FUP RENAME TEMP,MYFILE
```

- Choice 3 - Protect the application by pre-creating the file as a Guardian Format 1 file and then appending data to the file.

For example:

Replace the command

```
cp myfile /G/disk/subvol/myfile
```

With the commands

```
gtacl -c 'FUP CREATE $disk.subvol.myfile, FORMAT 1,
TYPE U, ODDUNSTR,
```

```
CODE 180, EXT (28,1400), MAXTENTS 749'
```

```
cat myfile >> /G/disk/subvol/myfile
```

Migration

- HP does not support transferring files larger than 2 GB to a system running a pre-G06.29 RVU.
- If you are currently running a pre-G06.24 RVU, consider migrating to the G06.28 RVU before migrating to G06.29 in order to facilitate fallback if fallback becomes necessary.
- Before migrating to G06.29, HP strongly recommends that users who are migrating from G06.24 through G06.27 install the DP2 fallback SPR T9053G11^AQS in case a fallback becomes necessary. T9053G11^AQS is on the G06.28 SUT. Installing the T9053G11^AQS SPR requires a system load.

If the users choose not to install the DP2 SPR before migrating to G06.29 and they later encounter a need for fallback, they must perform a system load on their prior RVU. In addition, before using any OSS files, they must install and system-load to the DP2 SPR. Falling back to the G06.23 or earlier RVUs is not supported.

For additional information on the SPR, see [Fallback](#) on page 2-10.

- If you have a tape file with a mix of OSS files smaller than and larger than 2 GB that need to be restored to a G06.23 to G06.28 file set that does not support files

larger than 2 GB, install these Backup and Restore 2 SPRs to restore files smaller than 2 GB:

- T2721G06^AAL, BRCOM
- T2722G06^AAL, BR2 TAPE SERVICES
- T2749G06^AAL, BR2 DMA & CSP
- T2750G06^AAL, B/R 2 DATA SERVICE

In addition to the Backup and Restore 2 SPRs, install the file system SPR:

- T9055G11^AFI for G06.23 through G06.26 RVUs
- T9055G12^AFJ for G06.27

Note. For G06.28, the required file system SPR is already included in the G06.28 SUT.

Files larger than 2 GB are skipped. The Backup and Restore 2 and the file system SPRs do not support pre-G06.23 RVUs. You cannot restore OSS files to G06.22 or earlier RVUs.

- The DSAPDDL file in the G06.29 version of DSAP/DCOM (T9543G08^ABJ) is changed, resulting in the change of the work file layout. You must use the DSAPDDL file distributed with T9543G08^ABJ when running ENFORM queries on the work file created with this SPR.

The DSAPDDL file for T9543G08^ABJ contains these changes to the `directory-record` structure:

- The field named `fifth` is changed from type binary unsigned to type binary 32 unsigned, which also has the effect of changing the locations within the layout of subsequent fields.
- These fields are added to the end of the structure:
 - Field `flab2_flags1` of type binary unsigned to identify OSS files larger than 2 GB.
 - Field `ext-0-fsu` of type binary unsigned to contain the extent size of OSS files larger than 2 GB for extent number 0.
 - Field `ext-1-128-fsu` of type binary unsigned to contain the extent size of OSS files larger than 2 GB for extent number 1-128.

Fallback

In summary, if you are falling back to:

Any pre-G06.29 RVU:	Install the DP2 fallback SPR: <ul style="list-style-type: none"> ● T9053G11^AQS
A G06.24 to G06.28 RVU:	Also install the DSAP/DCOM SPR: <ul style="list-style-type: none"> ● T9543G08^ABJ
A G06.23 to G06.28 RVU:	Also install the Backup and Restore 2 SPRs: <ul style="list-style-type: none"> ● T2721G06^AAL ● T2722G06^AAL ● T2749G06^AAL ● T2750G06^AAL
A G06.23 to G06.27 RVU:	Also install the file system SPR: <ul style="list-style-type: none"> ● T9055G11^AFI (G06.23 to G06.26) ● T9055G12^AFJ (G06.27)

DP2

Before migrating to G06.29, HP strongly recommends that you install the DP2 fallback SPR T9053G11^AQS. Installing this fallback SPR enables you to, after fallback, access OSS files smaller than 2 GB that were created by the new software. Installing the T9053G11^AQS SPR requires a system load. T9053G11^AQS is included on the G06.28 SUT.

If the DP2 fallback SPR is not installed, you cannot use either OSS or Enscribe to access any OSS file that has an underlying Guardian file format of Format 2, even if the files are smaller than 2 GB.

If the T9053G11^AQS DP2 fallback SPR is installed:

- OSS files smaller than approximately 2 GB are converted to use an underlying Guardian file format of Format 1 when opened, so that the files remain accessible using 32-bit APIs. The file size cannot exceed the limit of approximately 2 GB.
- OSS files larger than 2 GB are no longer accessible through the OSS file system and utilities, and DP2 returns errors for any operation other than purging them. However, you can use Enscribe with 64-bit elections to access the files from Guardian.
- A file smaller than 2 GB that was converted to Format 2 on G06.29 appears initially to most utilities (except DSAP/DCOM T9543G08^ABJ) as a zero-size Format 2 file after fallback. When the file is accessed for the first time after the fallback, it is converted to Format 1 and shows its actual size.

If you did not install the DP2 fallback SPR before migrating to G06.29, you must install the SPR upon fallback to ensure a successful fallback.

DSAP/DCOM

The SPR of DSAP/DCOM (T9543G08^ABJ) delivered in G06.29 is large OSS file safe, but previous SPRs are not. T9543G08^ABJ supports G06.24 and later RVUs. If you fall back from G06.29 to a system running a G06.24 or later RVU, HP recommends that you install T9543G08^ABJ after the fallback.

The DSAPDDL file in T9543G08^ABJ is changed, resulting in a different work file layout. If you install T9543G08^ABJ, you must use the DSAPDDL file distributed with T9543G08^ABJ when running ENFORM queries on the work file created with this SPR. For additional information on the DSAPDDL file changes, see [Migration](#) on page 2-8.

Backup and Restore 2 and File System

If you are falling back to a system running a G06.23 through G06.28 RVU, install these Backup and Restore 2 SPRs to restore files smaller than 2 GB:

- T2721G06^AAL, BRCOM
- T2722G06^AAL, BR2 TAPE SERVICES
- T2749G06^AAL, BR2 DMA & CSP
- T2750G06^AAL, B/R 2 DATA SERVICE

In addition to the Backup and Restore 2 SPRs, install the file system SPR:

- T9055G11^AFI for G06.23 through G06.26 RVUs
- T9055G12^AFJ for G06.27

Note. For G06.28, the required file system SPR is already included in the G06.28 SUT.

Files larger than 2 GB are skipped. The Backup and Restore 2 and the file system SPRs do not support pre-G06.23 RVUs. You cannot restore OSS files to G06.22 or earlier RVUs.

OSS Standard Posix Threads

The OSS Standard Posix Threads product (T1248) is enhanced to:

- Catch externally generated OSS signals in addition to the synchronous signals that result from events occurring inside the process.
- Deliver caught signals to the correct thread.

As a part of this enhancement, these new APIs are available:

- `spt_alarm()`
- `spt_signal()`

Migration

To enable the signal-handling enhancement, you must set the environment variable `SPT_THREAD_AWARE_SIGNAL` to value 1 within the shell (export `SPT_THREAD_AWARE_SIGNAL=1`).

OSS Standard Security APIs

The OSS environment now supports these functions:

- `getsid()` — Obtain the session ID of a process
- `setpgrp()` — Set the process group

For detailed information about these functions, see the *Open System Services System Calls Reference Manual*.

3

Application Development Products

The G06.29 RVU contains no new features for application development products.

4

Database and Transaction Processing Products

The G06.29 RVU contains new features for this database and transaction processing product:

- [SQL/MP](#)

SQL/MP

- You can use the DEFERRED option in the CREATE CONSTRAINT statement to delay the validation of the constraints against the existing rows in the table. SQL/MP applies the constraints to the table immediately to validate the new inserts or updates. After the constraints are applied, the locks on the table are released, and a browse-mode validation of the existing rows is performed. This enhancement enables concurrent data manipulation language (DML) operations on the table to complete without waiting for the locks to release.

To use the DEFERRED option, you must specify it explicitly in the CREATE CONSTRAINT statement. For more information, see the CREATE CONSTRAINT statement in the *SQL/MP Reference Manual*.

- SQL/MP is enhanced to detect an inconsistency between the rows of the base table and the index. It returns error 1186 when the index has rows that are not present in the tables, resulting in the inconsistency.

To correct the inconsistency, cancel the operation that caused the inconsistency or re-create the index if the table contains the correct data.

For more information, see the SQL 1186 error in the *SQL/MP Messages Manual*.

5

Installation and Configuration Products

The G06.29 RVU contains a new feature for this installation and configuration product:

- [DSM/SCM](#)

DSM/SCM

During the software installation process, DSM/SCM now allows users to specify which Heap Manager (T8431 or T1269) they want to install. Previously, if both Heap Managers were present in the configuration revision, DSM/SCM would ignore T1269 and install T8431 as the default Heap Manager.

6

Manageability Products

The G06.29 RVU contains new features for these manageability products:

- [Safeguard](#)
- [OSM and TSM](#)

Safeguard

The G07 version of Safeguard and the G06 version of Standard Security improve the cryptology of user passwords in the NonStop S-series server environments. The default values of some attributes are changed to increase the "Out of Box" password security.

If you do not want to adopt the new defaults, you can follow the regular migration steps for Safeguard. However, if you use Standard Security alone, you will be impacted by this change.

Attributes specific to Safeguard configuration are:

Attribute	Previous Default Value	New Default Value
PASSWORD-ENCRYPT	OFF	ON
PASSWORD-MINIMUM-LENGTH	0	6

Attributes specific to the PASSWORD utility of Standard Security are:

Attribute	Previous Default Value	New Default Value
ENCRYPTPASSWORD	OFF	ON
MINPASSWORDLEN	0	6
PROMPTPASSWORD	OFF	BLIND

All attributes are applied as each user changes his or her password only.

Encryption

If PASSWORD-ALGORITHM is set to DES or PASSWORD-ENCRYPT is set to OFF, the password (DES-encrypted or in clear text, respectively) is written to both the existing L/USERID and the new L/USERAX files. This approach allows for direct fallback to earlier versions of Safeguard and Standard Security.

If you enable the new HMAC256 encryption option, each subsequently changed password is encrypted using HMAC with the SHA256 algorithm and stored in L/USERAX. Because earlier versions of the security products do not understand HMAC, fallback requires extra steps. For additional information, see [Fallback in a Safeguard Environment](#) on page 6-3 and [Fallback With Standard Security \(Safeguard Not Installed\)](#) on page 6-4.

To assist fallback after PASSWORD-ALGORITHM is set to HMAC256, the DES or clear-text version of each preexisting password is retained in L/USERID. When you change your password, the old password in L/USERID is marked as expired as of that date. For a new user added to the system after the algorithm is changed to HMAC256, the password in L/USERID file is no longer retained.

Safeguard Support for OSS ACLs

The G07 version of Safeguard and the G06 version of Standard Security support the OSS access control lists (ACLs):

- The new Safeguard security group, SECURITY-OSS-ADMINISTRATOR, like the SECURITY-ADMINISTRATOR and the SYSTEM-OPERATOR security groups, is managed through the SAFECOM and SPI commands. Members of the SECURITY-OSS-ADMINISTRATOR security group have additional OSS security management privileges over regular users, including the ability to change the ownership and permissions of OSS files and directories. This group does not exist until it is added to the Safeguard database.
- Use the new Safeguard configuration attribute, AUDIT-CLIENT-OSS, to determine whether OSS audit records are written to the Safeguard audit trail. This new attribute allows you to configure the auditing of OSS related operations independently of the existing AUDIT-CLIENT-SERVICE attribute, which currently controls auditing for OSS and all other subsystem clients. A synonym, AUDIT-CLIENT-GUARDIAN, is also created for the existing AUDIT-CLIENT-SERVICE attribute and is used in all SAFECOM and SAFEART display outputs.

Migration in a Safeguard Environment

Follow these migration steps:

1. Use VPROC to determine the current versions of:
 - OSMP
 - OSMON
 - SAFEART
 - SAFECOM
2. Back up current Safeguard files (\$*.SAFE.* and \$SYSTEM.SYSTEM.USERID).
3. Use SAFECOM to build an OBEY file to save the current policy. To create an OBEY file, perform these steps in SAFECOM:

```
TACL> safecom/out $system.safe.safevalu/  
=display as commands on  
=info safeguard, detail
```

The output from these commands is retained in a file name SAFEVALU located at \$SYSTEM.SAFE.

4. When the new version of Safeguard is installed and you want to retain your original Safeguard values, obey the SAFEVALU file created in Step 3 in SAFECOM.

Note.

- When you migrate to the new password encryption feature, if you do not follow the preceding migration steps or if you do not want to accept the new password configuration default values, use SAFECOM to modify the appropriate attributes after the new version is installed.
 - The Safeguard configuration attribute AUDIT-CLIENT-OSS is set to ON. If you do not want to audit client subsystems other than OSS, you can disable the Safeguard attribute AUDIT-CLIENT-GUARDIAN after migration. Use the SAFECOM NEXTFILE command to switch to next audit file.
-

For more details, see the *Safeguard Administrator's Manual*.

Fallback in a Safeguard Environment

Because of the new password encryption algorithm, fallback requires advance planning.

In all cases, fall back to the previous version of security software.

If PASSWORD-ENCRYPT is set to OFF or PASSWORD-ALGORITHM is set to DES, no extra fallback steps are required.

If PASSWORD-ENCRYPT is HMAC256, extra fallback steps are required. When users first change their password after HMAC256 is enabled, they must remember their immediate previous password. This step is especially important for the system administrator. After installing the previous version of Safeguard and Standard Security:

1. Before starting Safeguard, the system administrator must log in with the old password. The old password is the one used before the algorithm was changed to HMAC256.
2. Start Safeguard.
3. The system administrator must set an appropriate grace period for users to change their expired passwords.
4. Users are prompted to change their password when logging into the system if one of these statements is true:
 - Their user account existed before the installation of the new version of Safeguard.
 - They are new users and their password was encrypted in DES or not encrypted at all before PASSWORD-ALGORITHM was changed to HMAC256.

When prompted, users should enter and re-enter a new password and log into the system as usual.

5. If new users were added to the system after PASSWORD-ALGORITHM was changed to HMAC256, the system administrator must reset their passwords to enable them to log into the system. Otherwise, the users cannot access the system after fallback.

Migration With Standard Security (Safeguard Not Installed)

When the new version is installed, use the new PWCONFIG utility to modify the appropriate attributes if you do not want to accept the new default values.

Fallback With Standard Security (Safeguard Not Installed)

In all cases, install the previous version of Standard Security.

If ENCRYPTPASSWORD is OFF or ALGORITHM is set to DES, no extra fallback steps are required.

If ALGORITHM is set to HMAC256:

- When users first change their password after HMAC256 is enabled, they must remember their immediate previous password.
- After fallback, users must use their old password to log into the system if one of these statements is true:
 - Their user account existed before the installation of the new version of Standard Security.
 - They are new users whose password was encrypted in DES or not encrypted at all before ALGORITHM was changed to HMAC256.
- If new users were added to the system after ALGORITHM was changed to HMAC256, they must use a blank password to log into the system.

Fallback Considerations for OSS ACLs

- The Safeguard configuration attribute AUDIT-CLIENT-GUARDIAN, which is a synonym for AUDIT-CLIENT-SERVICE, is no longer available after fallback.
- To audit OSS related operations after fallback, you must enable the Safeguard configuration attribute AUDIT-CLIENT-SERVICE.
- Switch to next audit file by using the SAFECOM NEXTFILE command.

Additional Technical Information

- The password configuration attributes PROMPTPASSWORD, BLINDPASSWORD, ENCRYPTPASSWORD and PASSWORD MINIMUM LENGTH are duplicated in the \$SYSTEM.SAFE.CONFIGP file so that Safeguard and Standard Security can access them. Any change in these attributes is updated in the \$SYSTEM.SAFE.CONFIGP file only. As a result, Safeguard is enhanced to obtain

the values of the these attributes from the \$SYSTEM.SAFE.CONFIGP file instead of the \$SYSTEM.SAFE.CONFIG file.

- The password history record is maintained and updated in the \$SYSTEM.SYSTEM.USERID and \$SYSTEM.SYSTEM.USERAX files as long as encryption is either DES-based or OFF. However, if HMAC256 is enabled, the password history is kept up to date only in USERAX. Therefore, after fallback, you might not see the same password history as before fallback.
- When you move a copy of the USERID file from one system to another, you must also move its associated USERAX file. In addition, consider also moving \$SYSTEM.SAFE.* when performing this type of operation.

OSM and TSM

The new version of the NonStop Open System Management (OSM) Interface and Compaq TSM module redundant power-scrub test provides independent battery testing and an extended load test for the bulk power supplies. With this new version of the power-scrub test, the redundant power scrub action can take up to 25 minutes to complete.

The ability of the new battery scrub to detect weak or failed batteries is significantly enhanced. For systems with many old batteries (over 5 years old), the battery scrub might call out multiple batteries for replacement.

Installation and Configuration

- To use the power-scrub feature, you must install one of these SPRs delivered with the G06.29 RVU:
 - T0682G07^AAR or later for OSM
 - T7945G06^ABV or later for TSM
- To select the new power-scrub version, add this line in \$SYSTEM.ZSERVICE.OSMCONF:

```
PowerScrubVersion = 2.
```

Select this new version only if all enclosures have been updated with a new PIB-to-PIB crossover cable (FCO 44440).

- The default test interval for the new power-scrub version is 7 days instead of 24 hours. To change the test interval, add this line in \$SYSTEM.ZSERVICE.OSMCONF:

```
DailyScrubTestingInterval = n,
```

where *n* is the number of days between power-scrub tests, up to a maximum value of 30 days.

HP recommends leaving the default as 7 days unless an event requires a reduced time between scrubs.

7 Hardware Products

The G06.29 RVU contains new features for these hardware products:

- [NonStop S-Series Servers](#)
- [Tape Drives](#)

NonStop S-Series Servers

These new HP NonStop S-series servers are introduced at G06.29 and supported by G06.25 and later RVUs:

- The NonStop S78BSE server, which replaces the NonStop S78SE server
- The NonStop S78B server, which replaces the NonStop S78 server
- The NonStop S7800B server, which replaces the NonStop S7800 server

For more information on the NonStop S78BSE server, see the G06.29 version of the *NonStop S-Series Central Office Server Installation and Service Guide*.

For more information on the NonStop S78B and S7800B servers, see the G06.29 version of the *NonStop S-Series Planning and Configuration Guide*.

Tape Drives

New automatic cartridge loader (ACL) versions of the HP Ultrium Linear Tape open (LTO) Gen 2 tape drives, the N1526A and N1527A, replace the N1524A and N1525A tape drives, respectively. For more information, see the *N1526A and N1527A ACL Installation and User's Guide*.

DAT72 5243 drives, the 5243 and 5243-2SE (a telco product), replace the DAT72 5242 and 5242-2SE drives, respectively. For more information, see the *5243 Tape Drive Installation and User's Guide* and the *5243-2SE Tape Drive Installation and User's Guide*.

8 Networking Products

The G06.29 RVU contains new features for this networking product:

- [SWAN](#)

SWAN

The WAN Line Check (WANLNCK) program enables you to check the quality of the communication link between a SWAN or SWAN2 concentrator and a modem.

The T0465AAF and later SPRs of WANLNCK support the external loopback test for the SWAN and SWAN 2 concentrators. The external loopback test checks the WAN port pins of a SWAN or SWAN 2 concentrator and the connection between the SWAN or SWAN 2 concentrator and a local or a remote modem.

You must explicitly invoke the external loopback test by using this command:

```
WANLNCK {HELP | TRACKID trackid ,CLIP clip-number  
,LINENUM line-number [ ,TIMES Number of tests ]  
[ ,DIAG diag-task-filename ] [ ,FILE out-put-filename ]}
```

For more information, see the *SWAN Concentrator and WAN Subsystem Troubleshooting Guide*.

Fallback

If the communication link check fails abruptly or does not reflect the correct status of the link, fall back to the previous SPR. The new feature for WANLNCK is no longer available after the fallback. To verify the fallback, run the WANLNCK command:

```
wanlnck clip <clip number>, Trackid "<trackid>", Linenum  
<portnum>, Diag <diagfilename>
```

WANLNCK should return an error indicating invalid parameters.

A

Sources for Migration Assistance and Information

This appendix describes the assistance HP provides when problems arise during the migration and testing process. HP also provides services that can help you develop a migration plan and implement migration tasks. Most migration and release documentation is available through the HP NonStop Technical Library (NTL).

This appendix includes information about these sources for migration assistance and information:

- [ExpressNotice](#)
- [Information on the Site Update Tape \(SUT\)](#)
- [Scout for NonStop Servers](#)
- [Global Customer Support Center \(GCSC\)](#)
- [NonStop Technical Library \(NTL\)](#)

ExpressNotice

ExpressNotice is an automated information delivery system that proactively sends information pertinent to your installed products and software release whenever there are any issues or changes. (ExpressNotice generates notices only for supported RVUs.) Use ExpressNotice to customize your information notification needs interactively online. You can access ExpressNotice through the HP NonStop eServices Portal at <https://onepoint.nonstop.compaq.com/buildpage.asp>.

ExpressNotice message types include:

- Software Revision Notifications summarize the content and impact of newly released, generally available time-critical fix software product revisions (SPRs).
- Hotstuff messages alert you to product problems that might have particularly serious consequences. The three types of Hotstuff messages are general, Outage Prevention Notifications (OPNs), and Software Recall/Withdrawal.
- Support Notes (SUPNOTES) provide information of a more routine nature than that provided in Hotstuff messages.

ExpressNotice messages are also available through Scout for NonStop Servers (see page [A-2](#)).

You can ask the Global Customer Support Center (GCSC) for the *ExpressNotice User's Guide*. You can also contact the ExpressNotice Help Desk by e-mail at express.notice@hp.com.

Information on the Site Update Tape (SUT)

These documents are available on the Y9230G_{nn} release subvolume located on the SUT for each G-series RVU:

- Content file
Contains a list of the product versions and software product revisions (SPRs) that are included on the site update tape (SUT).
- README
This file contains information that was not yet available when the manuals or softdocs were published.

You can access all other RVU information through NTL.

Scout for NonStop Servers

Scout for NonStop Servers is a Web-based SPR analysis and delivery tool available through Electronic Support Services. You can access Scout through the HP NonStop eServices Portal at <https://onepoint.nonstop.compaq.com/buildpage.asp>. Online help for using Scout is available at the Scout Web site.

By providing access to a data warehouse with SPR information for many different RVUs, Scout makes SPR analysis fast, easy, and accurate. Through the Scout main menu, you can display detailed information about:

- Release version updates (RVUs)
- Product versions (PVs) and software product revisions (SPRs)
- Outage Prevention Notifications, Hotstuff messages, and Support Notes
- Prerequisites for an SPR
- Available SUTs and Independent Products

After researching available SPRs, you can download those you consider appropriate for your systems directly to your workstation, or you can request tape delivery.

Global Customer Support Center (GCSC)

If you have questions or problems while implementing your migration plan or testing a new system, contact the Global Customer Support Center (GCSC) at 1-800-255-5010.

You can also access information on products and services at <http://support.nonstop.compaq.com/>.

NonStop Technical Library (NTL)

In addition to this compendium, RVU and migration information is available in several other documents and manuals that you can access through NTL. Information is provided about planning your site for a new NonStop server, product installation and

configuration, product availability in a particular RVU, and performance information for a specific RVU.

- *G06.29 Software Installation and Upgrade Guide*

Provides procedures for upgrading to the G06.29 RVU. Instructions include installing the G06.29 SUT and other related installation tasks.

- *NonStop S-Series Hardware Installation and FastPath Guide*

Written for anyone qualified to install a NonStop S-series server. Describes how to install and start a NonStop S-series server for the first time. It includes information about installing server hardware, cabling system enclosures, installing and starting system consoles, installing external system devices, starting the server, and configuring the server after startup. This guide also includes a case study of installing a sample system and a quick reference to installing and configuring a two-processor or four-processor NonStop S-series server in the Tetra 8 topology.

- *NonStop S-Series Planning and Configuration Guide*

Describes the ServerNet system area network (ServerNet SAN), the available hardware and software configurations for NonStop S-series servers, site planning and preparation, creating the operational environment, and making hardware and software configuration changes to an existing server. This guide describes how to plan and configure a NonStop S-series server and provides a case study documenting a sample system. This guide is written for those who are responsible for planning the installation, configuration, and maintenance of the server and the software environment at a particular site.

- *Hotstuff Messages*

If you do not enroll to receive ExpressNotice messages, you can view Hotstuff messages, SPR Notes, or other ExpressNotice messages in the NTL Support and Service library. For more information, see [ExpressNotice](#) on page A-1.

Note. SPR Notes are discontinued as of June 2006. Previously published SPR Notes continue to be available in NTL.

- *The Interactive Upgrade Guide and the Interactive Upgrade Guide 2*

Browser-based tools that are accessed through NTL, these guides provide customized migration planning information and highlight new features. The Interactive Upgrade Guide supports D-series through G06.24 RVUs. The Interactive Upgrade Guide 2 supports G06.16 and later RVUs and H-series RVUs.

- *Managing Software Changes*

Serves as an introduction and reference to the TRM2000, the system migration and installation process, SPR analysis, and HP resources for evaluating new RVUs and SPRs.

- *NonStop S-Series Operations Guide*

Written for system operators, this guide describes how to perform routine system hardware operations for NonStop S-series servers. These tasks include starting and stopping the system, monitoring the system, operating disk and tape subsystems, performing routine hardware maintenance, and performing recovery operations.

- *NonStop S-Series Service Provider Supplement*

Written for system support planners responsible for the correct operation of system hardware, this guide describes how to replace system hardware components defined as field-replaceable units (FRUs) on a NonStop S-series server. You can find this document in the Hardware Service and Maintenance Publications category of the NTL Support and Service library.

- *The NonStop System Console Installer Guide*

Provides information about upgrading a system console to the latest versions of the applications delivered on the NonStop System Console Installer CD.