LTS/OnGuard™

Software Release Bulletin: 7.1d

Transaction Design, Inc.

Notice

The information contained in this document is subject to change without notice.

Transaction Design, Inc. makes no warranty of any kind with regard to this material, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Transaction Design, Inc., shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance or use of this material.

Transaction Design, Inc.
542 San Pedro Cove
San Rafael, CA 94901
USA
1-415-256-8369 Voice
1-415-256-1844 Fax
assist@transactiondesign.com
www.transactiondesign.com

Manual number: OG003
Printing date: March 2017 Release 7.1d

Contents

Section 1: Introduction

The purpose of this manual

The LTS/OnGuard Software Release Bulletin describes the changes to the product for this release. Full information on the product is available in the LTS/OnGuard Reference Manual (OG001) which describes the state of the product.

Audience

This manual is intended for users who must audit and control the environment on their system, such as Security Administrators and System Administrators.

The manual assumes that you can use the system. It also assumes that you are familiar with LTS/OnGuard. Refer to the LTS/OnGuard Reference Manual (OG001) and the LTS/OnGuard Installation Manual (OG002) for further information about LTS/OnGuard.

Manual organization

This manual has two sections:

Section 1 highlights the changes in LTS/OnGuard Release.

Section 2 highlights the changes for the Security Administrator.

Highlights

Release 7.1d – Changes to existing commands

All users

- audit_file_integrity has been enhanced to include a level 4 check. Level 4 check calculates and compares crc32c (crc-32/Castagnoli) values. The comparison of checksum, crc, and crc32c values for each index is now supported. Files are no longer considered "CHANGED" when unable to perform requested check level.
- audit_security_parameters updated index "unchanged" message.
- Updated lts_terminate_account.cm and lts_reinstate_account.cm to use set_account_status for 17.2 and greater.
- Turned off command echo in match.com

Administrators

- install_lts.cm and install_lts_sp.cm now have a -log switch to enable/disable logging of the install process.
- add_to_administrator_start_up_cm has example code to restrict the LTS server processes to the LTS and VOS command libraries only.

Release 7.1d - New commands

All users

- lts_report_asr_process.cm is a new command to call execute_as_request with report_asr_process, which provides details of the user's LTS analyze_system process.

Release 7.1c – Changes to existing commands

All users

- audit_security_parameters and audit_password_info have several corrections to messages.
- execute_as_request has a new command: report_asr_process, which provides details of the user's LTS analyze_system process.

Release 7.1b – Changes to existing commands

All users

- audit_password_info has been enhanced per user request to identify and properly handle permanent passwords.
- audit_security_parameters has been changed such that standard tables are case-sensitive. No error message is written if a configuration file (stcp, smb, or ssh) is not found.
- audit_file_integrity has been updated to retrieve and store new file and index status fields.

Release 7.1a – Changes to existing commands

All users

- Added license support for long system name.
- audit_security_parameters has been enhanced with a -detail switch to control report details. It now allows a starname to -sshd_files to specify multiple sshd_config files in a configuration.
- Updated lts_login_admin, lts_set_tuning_paramters, and lts_set_password_security to handle VOS 19 changes.

- audit_security_logs, audit_logs_by_name, and audit_logs_by_terminal now handle an empty database.
- audit_acl_integrity now handles the disk root properly.
- Additional fixes to audit_acl_integrity, audit_file_integrity, update_password_info, audit_security_log, set_stream_files.cm,specify_cpu_configuration.cm, reset_configuration.cm

Release 7.0f – Changes to existing commands

All users

- Fixes to configure_login_admin.cm and configure_password_security.cm.
- All reports now report the CAC Site Id in addition to the system/module name in the standard report header.
- lts_run_reports.cm day option sets audit_admin –format_long.
- 7.0f has been certified for VOS 19 alpha.

Release 7.0 – General Comments

- Release 7.0 now supports command lines passed to the privileged_command_server and as_request_server of up to 4,000 characters in length. This provides sufficient room for multiple path names and longer include/exclude strings when passing parameters.
- Release 7.0 requires new licenses for each module.
- The priv_cmd_commands.tin/dd/table now allows for command names of up to 64 characters.
- -include and –exclude parameters allow up to 20 (versus 5) tokens to be matched against the target string.
- Default database locations are now in (master_disk)>system>lts>db versus >system>lts. Existing databases are moved there during installation.

Release 7.0 - New commands

All users

- lts_verify_license – examines the license file and reports on its status for the module. It will also ask the user if necessary to enter the title to be used in reporting, and to acknowledge the license document.
- add_disk_alias – VOS 18
- delete_disk_alias– VOS 18
- set_deferred_salvage– VOS 18
- set_dir_expand_mode– VOS 18
- set_stream_files– VOS 18
- validate_dir_limits– VOS 18

Release 7.0 – Changes to existing commands

All users

- All front-end commands have been reviewed and updated to handle longer parameter strings.
- audit_lts_logs, audit_logs_by_name, audit_logs_by_type now have additional selection criteria: -user, -from, -to, -include, and –exclude.
- audit_last_login now optionally produces a CSV report.
- priv_cmd_user_info handles long commands.
- create_security_log_db and audit_security_logs now work with long command lines, and the database is now an extent file. VOS 18 log formats are supported.

- audit_security_logs has a –user selection parameter.
- audit_login_activity now selects with –user, -from, and –to parameters.
- audit_password_info now selects with –person. A new –show_settings switch controls whether current password parameters will be reported.
- audit_who_accessed now selects by user and optionally reports using the show_logs switch.
- create_acctg_log_db defaults to (master_disk)>system>lts>db folder. New parameters include –show_logs, -gap, -csv_file, and –append. –append allows adding accounting logs to an existing database. –csv_file creates a CSV file reporting logins. –gap controls wheter gaps in accounting files are allowed in the database.
- create_lts_log_db defaults to (master_disk)>system>lts>db folder. It now creates extent-based files and indexes. It does a much more complete job of categorizing log entries, including OS 18 entries and log format.
- create_security_log_db creates an extent-based file and indexes. The –show_other parameter displays security_log messages that are not recognized or categorized. –csv_path creates a CSV file of log entries.
- execute_as_request handles long command lines up to 4,000 characters.
- execute_privileged_command handles long command lines up to 4,000 characters.
- scan_as_rqst_tables now allows include/exclude by user, privilege class, and command.
- scan_priv_cmd_tables now allows include/exclude by user, privilege class, and command.
- start_priv_cmd_server will also run lts_verify_license and may ask the user to enter the report title and acknowledge the license document.
- set_registration_info now records its action to the ra_history file for auditing.
- lts_verify_license confirms the validity of the module's license.

Software Licenses

This LTS/OnGuard release is a major release that replaces any earlier release. New license files are needed if upgrading from a previous release.

Software compatibility

This LTS/OnGuard Release is a major release that replaces any earlier release. The installation procedure for this release will overwrite any files belonging to an earlier release.

The priv_cmd_commands.table file must be rebuilt for this release. Use install_priv_cmd_tables.cm and priv_cmd_commands.new for this function.

Other `.tin` and `.table` files created by the administrator for the restricted environments in earlier releases will not be overwritten and will continue to work with the servers without any changes.

Command macro files in the LTS command directory (`>system>lts>command_library`) will be renamed to *`macro`*`.lts` but will not be deleted. If these files have been customized (for example, with `set_tape_defaults`), the changes should be applied to the new macros.

A database of information created under a release prior to 5.7 with `create_lts_log_db`, `create_security_log_db`, or `create_acct_log_db` will not be removed and will continue to work with current commands without any changes.

NOTE

The full release includes “front-end” macros and programs to mimic the command line interface for non-privileged users who are in the privileged command and `analyze_system` environments. If you have created site-specific front-ends, they will be overwritten by the installation process if they are contained in the destination directory. Make sure to read the installation instructions carefully.

Controlled directories

The directory tree from `(master_disk)>system>lts` and below will be affected by the installation of this release. All files that are part of the product will be overwritten by the new files. If you have modified any access rights under `(master_disk)>system>lts`, they will be returned to the initial values set by the earlier release installation tool. You should not change access rights under this directory, since the changes may interfere with the use of the product.

These site-created files will **not** be affected:

- Existing audit log files created by the restricted environment servers will not be affected by the installation.
- The `.tin` and `.table` files created for the restricted environments will not be affected. Noe, however, that the priv_cmd_commands.table must be rebuilt.
- An existing database of login activity, security log incidents, or LTS privileged command or `analyze_system` environments will be moved to >system>lts>db but will remain unchanged.
- An existing database of executable programs with owner access set on will not be affected.

Documentation

The following manuals have been revised for this release:

LTS/OnGuard Reference Manual (OG001)
LTS/OnGuard Installation Manual (OG002)

Support

We recommend that users visit the Transaction Design, Inc. site on the World Wide Web at www.transactiondesign.com and follow the links to the support pages and files for LTS/OnGuard. The email address assist@transactiondesign.com is monitored frequently and is an excellent way to ask questions and receive support.

Section 2:
Changes for the Security Administrator

This section describes the changes and additions to commands for the security administrator in this release.

Release 7.0 - New commands

- create_lts_license is obsolete.
- lts_verify_license is the new command which does the following:
  1. At first execution, the SysAdmin user will be asked to enter the string to be used as the report title for LTS/OnGuard reporting. This title resides in >system>lts>admin_tools>report_company_name.txt and may be edited if necessary.
  2. At first execution, the SysAdmin user will be asked to confirm the LTS/OnGuard license document and send it to TDI.
  3. lts_verify_license will then verify the license file against the module name (%sys#m1) and against the RSN site id (available via validate_hub).

Changes to commands

Administrative users

- The install_lts.cm macro has several changes:
  1. The epc_tools and ear_tools directories are obsolete and are no longer created or accessed.
  2. LTS/OnGuard default databases will be moved from >system>lts to >system>lts>db if they don't already exist in that folder. The databases include lldb1, amt, fmt, oal, accounting_db, security_db, lts_pc_db, lts_asr_db, and ra_history.
  3. *.dd files will now be installed, overwriting the old *.dd files. This is a change from the past necessitated by the longer priv_cmd_commands table entries.
- The priv_cmd_commands.[dd,new.tin] files have been updated. Commands may now be up to 64 characters in length.