LTS/ONGUARD™ Service Release Bulletin

Release 7.5a

kurIT Solutions, LLC.

Notice

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

Transaction Design, Inc. and kurIT Solutions, LLC 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. and kurIT Solutions, LLC, 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.

kurIT Solutions, LLC

16276 SW 104th Ave

Portland, OR 97224

USA

1-503-500-1571 Voice

assist@kuritsolutions.com

www.kuritsolutions.com

Manual number: 0G003

Printing date: February 2025 Release 7.5a

Table of Contents

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.

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 kurIT Solutions website (www.kuritsolutions.com) and follow the links to the support pages and files for LTS/OnGuard. The email address, mailto:assist@kuritsolutions.com, is monitored frequently and is an excellent way to ask questions and receive support.Software Licenses

This LTS/OnGuard release is a minor release that replaces any earlier release. New license files are not needed if upgrading from a previous release.

Software compatibility

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

The `sec_messages.table` file must be rebuilt if upgrading to release 7.0 from an earlier release. Use `install_sec_messages.cm` and `sec_messages.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. Note, however, that the `sec_messages.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.

Section 1:

Changes to LTS/OnGuard

Release 7.5a – Changes to existing commands (Feb 2025)

All users

- Create_acct_log and Audit_last_login – When create_acct_log_db is run for an accounting log containing the last login activities for a user that has since been deleted, followed by the user being added back, and create_acct_log_db runs again, the audit_last_login report was showing the incorrect 'added date'. The 'added date' is populated with the 'last login date' rather than the correct added. This has been corrected with release 7.5a.

Release 7.5 – Changes to existing commands (Sept 2023)

All users

- Lts_registration_admin: Addition of "-ext_tin_file" to support processing of external registration_admin.tin file.
- Added support for functionality and reporting unique to Stratus VOS command, password_admin.
    - Audit_registration_information has been updated to report the detailed encryption information and encryption type counts like password_admin.
    - Check_alias detailed output has been updated to include encryption information.
    - New Lts_pwd_admin has been added to support the following global actions:
        - Force users to change their password with the next login
        - Change last password change to the current time.

Release 7.4c - Changes to existing commands (April 2023)

All users

- New front end macro: set_password_info.cm. See *Changes for the Security Administrator* sections regarding updates to priv_cmd_command.table.
- Update front end macros:
    - set_registration_info.cm – for VOS 19.3, updated to call system>set_registration_info.cm as set_registration_info.pm no longer exists.
    - Add_disk_alias.cm and delete_disk_alias.cm – erroneously marked an obsolete in LTS 7.4.

Release 7.4b - Changes to existing commands (March 2023)

All users

- License check: License check uses the rsn_bridge_server.table. If this file is not found initially, license check will wait 30 seconds and check for the rsn_bridge_server.table. If it is found, license is validated. If not, license check fails.
- Execute_privleged_command: When waiting for initial output, execute_privileged_command will fail with "*CMD* failed. The server process id down. (s$seq_read)" if there's no command handler found 30 seconds after startup.

Release 7.4a - Changes to existing commands

All users

- Audit_acl_integrity and Audit_file_integrity
    - Added "-subdirs" includes all subdirectories and their contents that match the object_to_check/file_to_check on actions update,verify, list, and remove
    - "Some directory missing" error is no longer treated a fatal error. It is treated the same as "No object found".
- lts_verify_license display location of license file when -verbose specified.

Release 7.4 - Changes to existing commands

All users

- priv_cmd_server: the execution of an object with a pathname is not allowed by priv_cmd_server. The error message "BAD COMMAND LINE" is displayed in these situation.
- priv_cmd_server, as_request_server, as_request_user_info, and priv_command_user_info: fixed issue so requested programs will properly display commands that an user name can execute.
- Several front-end macros are obsolete as their counterpart VOS commands are obsolete. When run the macro will display "command is obsolete" message and stop. The obsolete front-end macros are: add_bad_blocks.cm, add_disk_alias.cm, add_link_board.cm, configure_boards.cm, convert_pick_partition.cm, delete_disk_alias.cm, delete_link_board.cm, display_calendar_clock.cm, display_link_meters.cm, display_net_trace.cm, display_ring.cm, dump_channel_info.cm, dump_iop_meters.cm, dump_lap_meters.cm, dump_tcbh.cm, memory_control.cm, obsolete_template, reconfigure_memory.cm, setup_disk_pack.cm, set_cpu_config.cm, set_net_trace.cm, set_pick_partition_size.cm, specify_cpu_configuration.cm, start_link_diagnostics.cm, stop_link.cm, stop_link_server.cm, terminal_meters.cm, timer_meters.cm
- Added front_end macro, cancel_broadcast_requests.cm.
- Updated the following front_end macros/programs to match their counterpart VOS commands parameter set: cache_meters.cm, disk_meters.cm, dump_cache_info.cm, format_disk.cm, interrupt_meters.cm, lock_meters.cm, lts_list_boards.pm, sched_meters.cm, sim_int_mters.cm, transaction_meters.cm.
- Updated front-end macro, set_stream_files.cm, to be available for vos 17.2 and above.
- Intall_lts.cm: Runs compare_files again "*.new" and "*.dd" files. If there are differences with "*.dd" files, install_lts.cm does not move the file and puts out a

warning message that the ".dd" has changed and the corresponding table needs to be updated. "*.new" files are default "*.tin" and if there are differences with "*.new", install_lts.cm puts out a warning message to update your site's ".tin" and rebuild the table.

- Standard_posix.dd: corrected EOL character. The wrong EOL was introduced in prior release when comment section was updated. Standard_posix.dd should manually be moved during release upgrade and tables do not need to be updated.

Release 7.3c - Changes to existing commands

All users

- Audit_acl_integrity: When ACL changed for a directory, DACL was not being listed on "verify" action. Now DACL is always displayed.
- Lts_run_reports: Fixed issues with time zone check.

Release 7.3c - Removed an existing command

- Removed front-end macro, validate_hub.cm, and update priv_cmd_commands.new and priv_cmd_commands.tin. Validate_hub is not a privileged command. For existing installs validate_hub needs to be removed manually:
- Delete validate_hub.cm from LTS user library.
- Use install_priv_cmd_tables.cm to remove validate_hub.cm entry from priv_cmd_commands.tin and rebuild table.
- Bounce privileged command server using stop_priv_cmd_server and start_priv_cmd_server.

Release 7.3b - Changes to existing commands

All users

- Create_acct_log_db: Update person name in last login database when it has changed.
- Audit_last_login, audit_lts_logs, audit_password_info, audit_registration_info: -person or -person_name now match is caseless.

Release 7.3a - Changes to existing commands

All users

- audit_security_parameters:
    - Fixed reporting of min_digit_chars and min_punctuation_chars from set_password_security.
    - Changed format of forbidden passwords report. Created "Conforms To Standards", "NOT FOUND in standards", and "Standard passwords MISSING" sections. Each section reports passwords in 2-4 columns based upon the length of the longest password.
    - "-no_details" parameter suppresses the "Conforms To Standards" report section for forbidden passwords.
    - Added passwords in the standard_forbidden_pwds.tin included in the default Stratus VOS forbidden_passwords.tin.

- create_acct_log_db and audit_last_login: Changed last login database and reporting of *Date Added* for deleted users. The *Date Added* for users that are no longer registered is set to zero and reported as "No Record." If user is re-added, *Date Added* is updated the same as a new user.
- create_security_log_db and associated audit reports: Updated sec_messages.tin for LTS/OnGuard 7.3. See changes to create_security_log_db. This may require rebuilding the sec_messages.table file by running install_sec_messages.cm
- Security database format (version 4) enhanced to include ip address and port. create_security_log_db, audit_security_logs, audit_logs_by_terminal, and audit_logs_by_name updated to support enhanced database format.
- create_security_log_db:
    - IPv4/IPv6 addresses and port are extracted from telnet, ftp, sftp, and ssh security messages. IP, port, and terminal mappings are saved and when possible, messages containing only terminal names are mapped to the matching IP and port.
    - Enhanced parsing of the terminal name. If terminal name is not found in the 1st line of the security message or in the "Source:", the "Text:" of [AUTH][INFO] message is searched for terminal name.
    - Enhanced parsing of user. For [AUTH] messages reported by "root.root", the "Text:" is searched for the actual user of the service. Most useful for ssh and sftp sessions.
    - The changes to security database enhance reporting by audit_security_logs, audit_logs_by_terminal, and audit_logs_by_name.
    - Updated processing of sec_messages.table. Catch-all messages are input sequence '97'-'106'. Input sequence '107' or greater supersedes these sequences.
    - Terminal names and IP addresses are standardized.
    - Added "-ipv4_dotted_quad" switch. Switch is used to determine the format of IPv4 addresses. "-ipv4_dotted_quad" means Ipv4 dotted-quad notation (::ffff:98.232.206.58) is used as format. "-no_ipv4_dotted_quad" switch means IPv4 Mapped IPv6 address format (::ffff:62e8:ce3a) is used.
- audit_security_logs: Added "ip" as "-sort_by" type to report by IP address. If no terminal is available, then "Not available" is reported for terminal name. Added "IP Connections Summary" report for "-sort_by" "ip" and "person".
- audit_logs_by_name: Added "IP Connections Summary" report for "-sort_by" "person".
- audit_logs_by_terminal: Reporting of terminal name has been updated to match report output of audit_security_logs and audit_logs_by_name. Terminal name is reported as "Terminal:" followed by the terminal name. If no terminal is available, then "Not available" is reported for terminal name.
- install_sec_messages.cm: Compares sec_messages.new to sec_messages.tin. In interactive mode, gives option to create sec_messages table.
- install_lts.cm: Updated to call install_sec_message.cm using full path.

Release 7.2c - Changes to existing commands

All users

- For audit_registration_info, fixed no details report to list users properly when either group or user is "*". Added gid and uid to no details report. Added a -brief report for listing users. When -no_group_name_detail and -no_person_name_detail is used then no details report is produced if -no_brief passed and brief report is produced if -brief passed.
- LTS_registration_admin.pm now explicitly calls lts_registration_admin.pm internally. Previously if a site had lts_registration_admin.cm the call would fail.

- Added -include and -exclude to audit_file_integrity and audit_acl_integrity.
- For audit_file_backups fixed -exclude for directories to look at entire directory path.

Release 7.2b – Extending license support

All users

• Add license support for license dates beyond 2048. Expiration dates through 2079 are now supported.

Release 7.2a – Supporting Release 7.2 for Continuum

All users

- For audit_file_integrity, level 4 check and integrity check of indexes are not supported for Continuum.

Release 7.2 – Changes to existing commands

All users

- Fixed issue regarding licensing.
- create_security_log_db uses a new sec_messages.tin/new/table to categorize security_log messages reported by audit_security_logs, audit_logs_by_name, and audit_logs_by_terminal. Categories, summarization, and output order can be specified for security_log messages via sec_messages.tin.
- audit_security_logs, audit_logs_by_name, and audit_logs_by_terminal now sort and categorize messages based upon sec_messages.table.
- audit_file_integrity has been updated to check the integrity of item and indexes longer than 64 characters. Index level checking is not done on deleted_record and record indexes.

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.

Section 2:

Changes for the Security Administrator

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

Release 7.5 - New commands

The `priv_cmd_commands.[new.tin]` files have been update to support lts_pwd_admin. New entry for lts_pwd_admin. Update priv_cmd_commands and rebuild table using install_priv_cmd_tables.cm.

Release 7.4c - New commands

The `priv_cmd_commands.[new.tin]` files have been update to support set_password_info. New entry for lts_spi_inr.cm has been added. Update priv_cmd_commands and rebuild table using install_priv_cmd_tables.cm.

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 must run the .pm version of the command. They 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`).

Release 7.0 - 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.