LTS/OnGuard™

Usage Recommendations

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: OG004
Printing date: September 16, 2019

Contents

Section 1: Introduction

The purpose of this manual

The LTS/OnGuard Usage Recommendations provides suggestion for using the LTS/OnGuard product. 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.

Manual organization

This manual has two sections:

Section 1 is this section.

Section 2 provides recommendations for using LTS/OnGuard.

Section 2:
Recommendations for Using LTS/OnGuard

The key to deciding when to report on the system is really dependent on your level of concern. If you are reasonably confident that you don't have external exposure, that internal controls are in place, and that there are no internal events happening that might cause you to be concerned, then you don't need to examine a lot of things very often. If you're not so confident, then you need to watch things more closely.

One of the points to remember is that if you establish a timetable for reporting and create the reports on a regular basis (however often that is), you may be helping yourself in the event of a problem. In general, reports that are generated "in the normal course of doing business" might be allowed as evidence without challenge if you should ever have to prove wrongdoing. Of course, you must check with your own legal department to see how this might apply at your site.

What to watch depends on which VOS features you are using. Some things are universal (such as the security logs and user registrations). Others are very dependent on special features (file auditing, etc.).

The following are only suggestions for when you might want to examine various reports and logs. Adjust these suggestions according to the features you use and your level of concern.

Security Menu

The released software contains a macro set which provides a basic security menu for SysAdmins to manage the LTS/OnGuard environment. This macro is intended to be renamed and customized by the site for its purposes.

lts_security_menu.cm

Sample Batch Macro Set

The released software contains a macro set which is intended for the user to customize. These macros are intended to be renamed and customized by the site for its purposes. The latest version uses a file to list the directories and files to be audited, and optionally creates HTML.

lts_daily_batch.cm

lts_run_reports.cm

lts_check_integrity.cm

Every time a user logs in:

User file and login integrity:

verify_my_login

This command, which should become part of the user's start_up.cm, verifies that the start_up.cm and the abbreviations files have not changed, and shows the user's current registration information.

Check daily:

VOS Security Log

create_security_log_db –yesterday

audit_security_logs –totals_only –sort_by target (or type or person)

This gives you the quickest look at security incidents on the system.

Over time, you will develop a feel for numbers and types of incidents which are "normal". If you see changes from this, you can then look in more detail. If you are very paranoid, remember that a clever, determined user can shift the normal counts over time by increasing the number of incidents at a rate that is slow enough to not attract your attention until they are able to trigger a number of security incidents without your noticing.

If you are concerned about overnight activity, you will also want to create the database -today when you first come in the morning.

LTS/OnGuard Logs

create_lts_log_db –yesterday

audit_lts_logs –no_show_ok

audit_lts_logs as_rqst -no_show_ok

If you are using the privileged command and analyze_system servers to protect the system, this will show you the requests that failed. This could simply be mis-typing the name of the command, but it could be a user trying to exceed their authority.

If you are concerned about overnight activity, you will also want to create the database -today when you first come in the morning.

Passwords

audit_password_info -terminated_only

This is a list of users whose accounts have been frozen by VOS because they have exceeded the number of failed login attempts.

Inactive Logouts

tail_file (master_disk)>system>lts>terminator.out

or

display (master_disk)>system>lts>terminator.out -match stop

These are not reports, but running these commands against the output file from the terminator process will show you the users who were logged out for inactivity.

User Logins

create_acct_log_db

audit_login_activity

If the security logs or other reports indicate a potential problem, you may want to find out when users were on the system. If you are using the accounting system to track user logins, you can create the database and run reports against it if you need details of user activity.

Check Periodically

How often you run these reports depends on how worried you are and how secure you think the system is. Some sites might run some of them daily, others might run them monthly or quarterly. If you have reason to think there is a problem at the site, you should run them immediately.

audit_security_parameters

This reports on the set of security-related system settings. It will report any conflict between the settings and a set of standard definitions for those settings.

audit_password_info -expiration_check_days n

This is a list of users whose passwords will expire within the next n days. For convenience, you might want to check this weekly or so and send a reminder email so that you won't be getting called to reset expired passwords.

audit_file_integrity

Compares current file and directory attributes and contents to a database you have previously created. Check if you are concerned about malicious programs or changes to your executables. You may want to be sure that the command macro that you run has not been modified. Is the version of a program module you run privileged, in batch, the same or has it been modified or replaced by another version? Use this to help verify that what you execute is what you have safely run before and not what has been modified without your knowledge. Do it once a month, more often if you are in a more volatile environment. You may want to create a command macro to call this on certain files. Also in a command macro you can check the command before you execute it. This would only be recommended if you are very concerned that all programs you run in a batch job are "certified" as the correct versions.

audit_registration_info -privileged_only

This is a list of users who can login as privileged users.

audit_registration_info -group_name SysAdmin (or other powerful group)

This is a list of users who can login using this group name.

audit_prelogin_commands

This is a list of commands which can be executed without going through the login challenge.

audit_file_auditing

This is a list of files which VOS is monitoring accesses for.

audit_file_safety_settings

This is a list of files which have the safety switch or expiration date set.

audit_who_can_access

This is a list of users and their level of access to the target. Use this to monitor access to any critical files, directories, devices, or internal commands.

audit_acl_integrity

Compares current ACL settings to a database you have previously created. You may want to create a command macro to call this on certain files and directories or you may want to use it with the walk_dir command. Note that there is an option on this command to create a command macro that will restore changed ACLs to the saved settings.

audit_owner_access

Lists files with the owner access attribute set.

audit_file_usage

Reports files used in a date range. Run to see if critical files are being accessed, modified, or created. You can specify an author name to check for files created or modified.

Check as needed.

These reports are for administrative purposes, so run them on an "as needed" basis:

audit_file_backups

Lists files modified or created since last backup. Run this after doing a backup to verify that the backup coverage was complete.

audit_unused_files

Lists files unused since a given date. Run to find files that can safely be deleted or archived without leaving them exposed on the system.

audit_links_to_object

Lists links anywhere on the module to the specified object. Run this before removing an object to avoid "orphan" links. There is an option on this command to report bad links that it finds while checking for links to an object; you can use this to clean useless links from the system.

audit_password_info

Lists password configuration settings and password aging for all users.

Use while configuring the system.

The full range of reports is intended to help you configure and then document the settings for various parts of the system. Run these reports during and after the configuration process. Don’t forget to run them again when you make changes.

These reports are intended to help find inconsistencies in access rights for the directory structure, so run them when configuring ACLs:

audit_access_lists

Run before configuration so you will have something to work from. Run after configuration to document your desired configuration.

audit_access_consistency acls
audit_access_consistency users
audit_user_access
audit_group_access
audit_group_member_access

Run any of these while you are working on the configuration to make sure that you are not leaving holes in the access structure.

Baseline

Run these reports to help you configure the system, then run a final copy to save as a baseline for comparison over time:

audit_owner_access -all_disks

Run to find files with owner access set. The side effect of the –all_disks option is to create a database of files with owner access. This database is used by audit_who_can_access to verify owner access as well as direct file access.

audit_file_safety_settings
audit_file_auditing
audit_object_acl_files

Run these reports against critical files and directories.

audit_acl_integrity

audit_file_integrity

Both of these commands create a database to be used for future comparison.

audit_who_can_access

audit_security_parameters

audit_prelogin_commands

audit_terminal_settings

audit_registration_info

Run these reports against the system settings and save for future reference.

audit_lts_site_preferences

scan_priv_cmd_tables

scan_as_rqst_tables

Run these reports if you are using the servers to protect privileged commands and analyze_system requests.