LTS/OnGuard™

The VOS security solution…

Concepts and Facilities

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

inform@transactiondesign.com
www.transactiondesign.com

Manual number:	OG004
Revision number:	6.0h
Printing date:	October 2012
LTS/OnGuard release:	6.0h

Contents

What is LTS/OnGuard?

The VOS operating system on Stratus computers gives you the basic capabilities to secure your corporate information. VOS already contains features such as access control, password security, and security logging. However, for many users, VOS all by itself cannot fully meet their security requirements.

LTS/OnGuard does not modify VOS, nor does it interfere with the user environment. You can choose on a user-by-user or object-by-object basis who or what will be controlled and audited and who or what will not.

LTS/OnGuard allows users to perform their jobs within a controlled, audited environment without the need for the `privileged` or `SysAdmin` attributes..

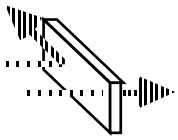
LTS/OnGuard utilities for audit and control

LTS/OnGuard is a set of utility programs which run under VOS to control and audit security functions on Stratus computers. LTS/OnGuard enhances the operating system features by giving you:

- control over powerful privileged commands and other system resources
- the ability to audit and report on system security information

LTS/OnGuard controls powerful privileged commands

LTS/OnGuard allows you to establish a controlled environment for users to execute the powerful (but potentially dangerous) privileged commands.



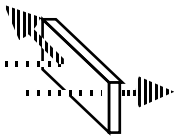
- Allow a specific user to execute specific privileged commands
- Establish privilege classes so that users in a class can execute specific commands
- Require that a user only execute privileged commands from a specific terminal
- Automatically create an audit trail of every privileged command (including its arguments!) that is requested
- Control which users can update communications channel attributes for specific devices

LTS/OnGuard controls user/application commands

LTS/OnGuard allows you to establish a controlled environment for certain application commands, operations commands, macros, or batch jobs, if desired.

LTS/OnGuard controls *analyze_system* requests

LTS/OnGuard also allows you to establish a controlled environment for users to execute requests from the *analyze_system* tool..



- Allow a specific user to execute specific requests
- Establish privilege classes so that users in a class can execute specific requests
- Require that a user only execute *analyze_system* requests from a specific terminal
- Automatically create an audit trail of every command (including its arguments!) that is requested

LTS/OnGuard controls system resources

The LTS/OnGuard user registration interface provides greater flexibility than the standard VOS interface.

- User profiles can be maintained by non-privileged users
- Separation of duties for creating and installing user profiles
- Audit trail of additions, deletions, and modifications of user profiles
- Direct control and audit trail of termination/reactivation of user profiles
- Direct control and audit trail of deletion of user home directories

The LTS/OnGuard terminal monitor watches for inactivity by users and logs them off after a grace time.

- Site-configured table determines which terminals are monitored
- Each terminal or user/group set can be set to a different inactive grace time
- Status facility allows the Administrator to verify which terminals are being monitored, their grace times, and whether they are inactive

LTS/OnGuard creates formatted reports

LTS/OnGuard audit utilities turn system data into easy-to-use, formatted reports.

- Create a comprehensive, easy-to-read report with a single command
- View the information on-line for immediate action
- Create a formatted report file that is ready for printing. Reports can be distributed for management action or archived for audit requirements

LTS/OnGuard is easy to use

LTS/OnGuard commands are implemented with the standard system interface — nothing new to learn. Or, use the simple security menu to access all LTS/OnGuard facilities.

- Issue single commands in the standard format, including display forms and on-line help
- Use a simple, menu-driven approach for an easy-to-use, guided interface to the utilities

LTS/OnGuard is easy to install

The LTS/OnGuard environment install in minutes. An installation tool creates the appropriate directory structure and installs the files. The utilities are ready to use immediately. There is no need to reboot the system when installing LTS/OnGuard.

Implementation of a corporate security policy may be rolled-out in an incremental, staged process under LTS/OnGuard. The site may select on a user-by-user basis which users are to use LTS/OnGuard.

Why use LTS/OnGuard?

Help meet security requirements

Security requirements for information processing are becoming increasingly complex. In addition to basic, sound business practices (such as separation of duties and individual accountability) and your own corporate policy, government and industry regulation are combining with legal liability awareness to demand ever stricter monitoring and control over your information assets. LTS/OnGuard can provide you with the tools to implement your response to these needs.

Help protect against data loss

Your mission-critical dependency on your Stratus means that any loss of data or capability represents an ever-growing business risk. Any unauthorized loss of processing or data, whether deliberate or accidental, means a business loss as well. LTS/OnGuard simplifies the job of making sure that adequate controls are in place.

Provide management support

To control the system resources, management needs coherent information, organized to make interpretation of current status and trends easy. LTS/OnGuard reports can provide easy-to-read, intelligible information on a timely basis.

Provide auditor support

Auditors need to operate independently of administrators and operators. Yet, they often work on many platforms and don't have time to become technical experts on each one. LTS/OnGuard protects the separation of duties by simplifying the task of generating reports for audit purposes. By using the facility to control privileged commands, you can let your auditors run their reports without needing the authorizations of administrators.

Cost-effective

Your technical people play an important role in making your business profitable. When you implement LTS/OnGuard, you free them to concentrate on your business, rather than on supporting administrative and audit requirements. With an easy-to-use interface, on-line help, complete documentation, and support, LTS/OnGuard makes it simple to control and audit your Stratus.

Security Menu

Standard command interface

Each LTS/OnGuard command is implemented using the standard system command interface. That means that you do not have to learn a new way of issuing commands to secure your system.

```
----- audit_access_consistency -----
start_dir:      (current_dir)
check_type:     acls
-report_file:
-display:       yes
-file:          no
```

Each command can accept arguments in the lineal form or in the display form.

Each command provides on-line help for each argument field using the HELP key.

Script your standard checking through macros

Since the commands can be issued individually and use the standard command interface, you can easily create scripts of command macros to report on aspects of system security on a regular basis.

By submitting macros to run from batch, you can have a set of security reports delivered every morning, every week, or on your own convenient schedule. We provide templates for a daily report job which covers database creation and periodic reporting.

Or, a menu-driven interface

For auditors and administrators who do not use the system regularly or who prefer a guided approach, LTS/OnGuard provides a security menu, where all LTS/OnGuard facilities are available through submenu screens.

Once you enter the main menu, you will find a range of submenus, arranged by function. Select a submenu by number and you will see the range of reports available on that topic. Select a command by number, and you enter the display form for that command.

After a command finishes executing, you are returned to the calling menu, ready for the next action.

The main menu

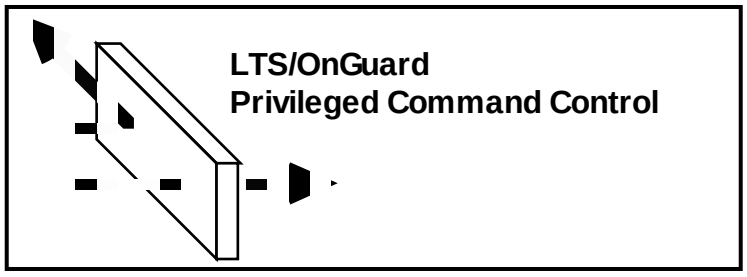
```
LTS/OnGuard(TM) Security Tools                          Main Menu


System Auditing                        Exit Security Functions
---------------                        -----------------------
(1) System Security Parameters        (99) Exit to system
(2) System Security Logs
(3) User Accounts
(4) Terminal Devices
(5) Files and Directories
(6) Commands
(7) Login Activity


Controlling Sensitive Commands
------------------------------
(8) Control of Privileged Commands
(9) Control of analyze_system Requests


Controlling Terminals
---------------------
(10) Control Inactive Logout
```

Controlling System Resources

Privileged commands

The most powerful operating system commands are protected by the *privilege* attribute. To execute one of these commands, the user must be registered as a *privileged user*. However, to execute even **one** privileged command (such as an operator executing spooler_admin to control a printer), the user must be made a privileged user for **all** commands (such as shutdown the computer or format_disk). The *privilege* attribute is all or nothing.

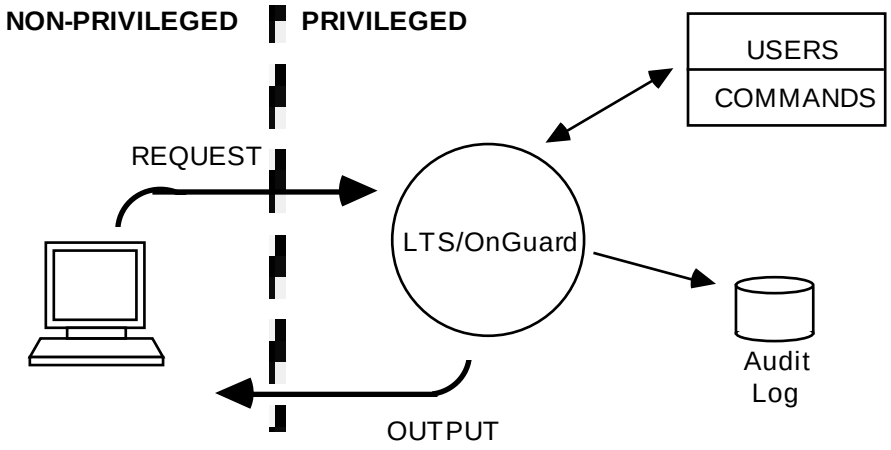
You can try to control the use of privileged commands by registering users as privileged and then controlling their actions through the use of a command menu or shell. The danger to this approach occurs if the user manages to break out of the controlling environment — they are now free in the system as a privileged user.



LTS/OnGuard allows you to create an environment where your users do not need to be registered as privileged to the operating system, but can still execute certain privileged commands.

In this environment, the non-privileged user invokes an LTS/OnGuard command to request execution of a privileged command. This non-privileged command passes the request to the LTS privileged command server program.

The LTS privileged command server (which runs in privileged mode) checks the user's name and request against tables which the site administrator has customized. If the requesting user is authorized for the requested command, the server causes it to be executed in privileged mode. The user's request (whether successful or not) and all the command arguments are logged by the server for later audit. After the command runs, the output is passed back to the user.



Notice that the user never needs to be logged in *privileged*. If users should break out of the command, they are still **not** privileged users. The LTS/OnGuard client/server implementation of privileged command control provides the layer of fail-safe protection lacking in shell designs. At the same time, LTS-supplied front ends give the users the look and feel of VOS privileged commands, while isolating them from privileged status.

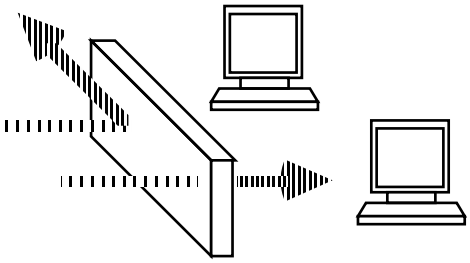
You can control the privileged command environment with individual commands or you can use the security menu.

You can reconfigure the permissions tables without taking the server off-line. A simple command choice allows you to notify the server to begin using updated tables before handling the next user request.

You can consolidate the daily audit logs into a database of privileged command activity during a specified time interval. Using a single command, you can then extract reports showing all privileged command activity sorted by name, time, or terminal.

Application and user commands

Almost any command may be added to the LTS/OnGuard controlled environment. This may include application programs, operations macros, and batch jobs. When a command is registered within LTS/OnGuard and secured away from direct execution by the users, it may be run under LTS/OnGuard's control with full auditing



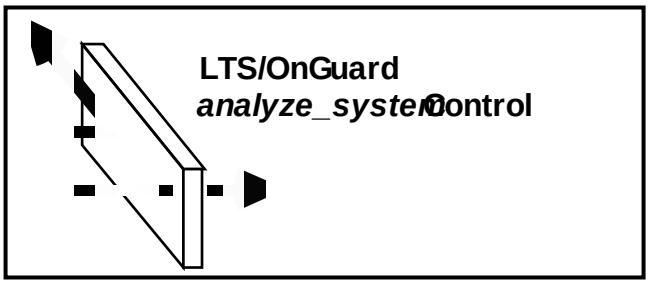
Per-device control of *update_channel_info*

The update_channel_info command is a system command which allows a privileged user to change the channel characteristics for a device.

Using the LTS/OnGuard privileged command environment, you can not only allow only specified, non-privileged users to perform an update_channel_info, but you can further restrict these users to only update specific channels.

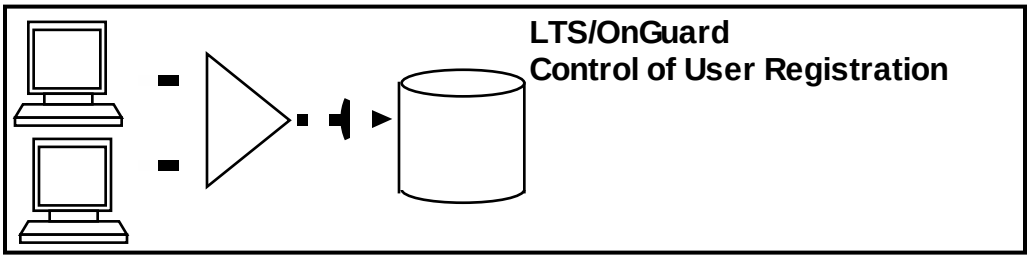
For example, if you have two divisions of the company sharing a processing module, you can authorize an operator to update the channels which belong to one division, but not the other.

Use of the channel restriction is optional and is configured at the site.



The analyze_system tool provides over 300 entry points to examine and modify user processes, the operating system, and disk objects. This powerful tool is itself a privileged command, but again, if a user can execute any one request (such as an operator using analyze_system: list_boards to review the current state of the hardware) they can use any other request (such as analyze_system: call_pcp which stops the computer).

LTS/OnGuard provides a privileged server environment for analyze_system requests, just like that for privileged commands. Now non-privileged users can be authorized for individual analyze_system requests. All requests are logged for later auditing.

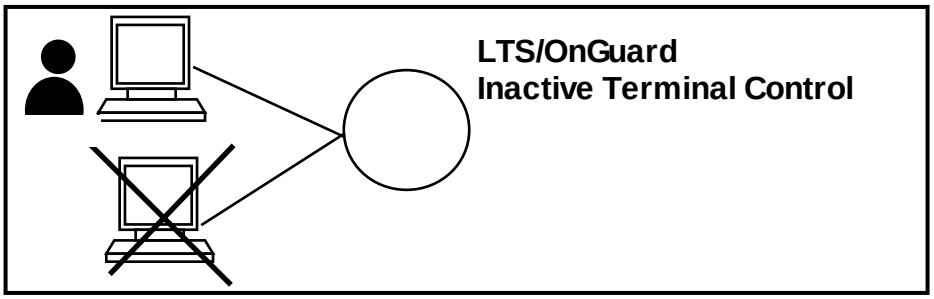


The operating system command registration_admin is used to maintain user profiles and process them into the registration database for use. The command is protected by requiring the user to be privileged and in the SysAdmin group. However, once a user meets these criteria, that user can make any changes they desire to the registration database.

The LTS registration interface uses the privileged command environment to allow a non-privileged user who is not in the SysAdmin group to configure user profiles. You can control whether a user can create and process profiles or just create them. You can configure a second user to use a process-only command to view a file created by the first user and process it into the database. The second user cannot create or modify profile files.

After processing a file into the database, the command then checks the requested users against the database and records users who are added, deleted, or modified (and which fields were changed) into a history file. A tool is provided to produce a formatted report from the history file.

Additional commands are provided which allow an administrator to directly terminate a user account, and to delete the account's home dir.



A user who remains logged in but leaves the terminal area violates good security practice. The operating system command logout_admin can be used to logout users who are logged in on a terminal but who are inactive. However, the command does not distinguish between terminals, users, or groups in applying the grace time and does not allow the exclusion of particular lines.

An LTS/OnGuard facility runs in background to periodically check terminals, users, and groups which you have configured into a table. Each entry has its own individual grace time associated with it. Whenever a terminal has a user logged on who exceeds the grace time for inactivity, the monitor first warns the user, then logs them off.

The configuration table can be updated at any time and does not require stopping the monitor.

A tool is provided to interrogate the monitor to determine which terminals have users on them, their configuration values, and their current status.

Audit and Report Commands

LTS/OnGuard auditing commands allow the System Administrator or Security Officer to monitor the system in an easy, consistent way. The reports generated by these commands allow the DP Auditor to verify the state of the system and archive the information for later use.

LTS/OnGuard reports

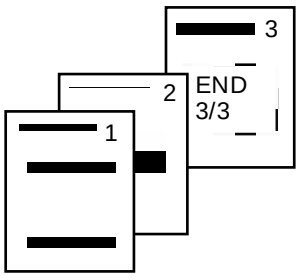
```
************************************************
* SYSTEM SECURITY REPORT               * Page 1*
*----------------------------------------------*
* Requested: Monday, January 3, 1995  3:37 pm  *
*        By: Paul_Chadwick.SysAdmin            *
*    Module: %system#m1                        *
*----------------------------------------------*
*          LTS/OnGuard(TM) -- Release 3.0      *
* (c) 1989-1994 Lakeside Transaction Services  *
************************************************

                      **********************
                      * REPORT DESCRIPTION *
                      **********************


This report contains values showing system  information under the
various directories.

Option settings for this report:

Detailed information will be shown for each directory, as well as
the summary information


                    *************************
                    * SYSTEM SECURITY REPORT *
                    *************************


-------------------------------------------------
%system#d1>system>command_library
-------------------------------------------------

This directory contains the system information which was requested

-------------------------------------------------
%system#d1>system>maint_library
-------------------------------------------------

This directory does not contain the requested information.
```

Standard header on the first page shows a page number, who requested the report, when the report was made, and what module it covers

Description shows what is contained in this report

Option settings explain the effect of command arguments on this report

Standard topic headers categorize the detailed information for you



Each page in the report is numbered consecutively. The final page is marked with an “END” banner and gives the total page count.

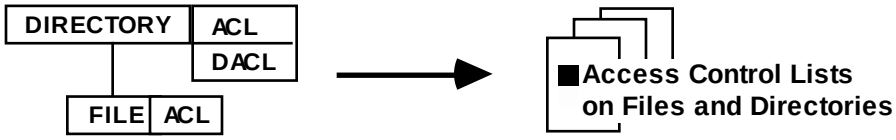
Auditing file and directory security

There are two major security concerns for protecting your data as it is stored on disk — access lists and file attributes. There are LTS/OnGuard commands to report on the current settings of these authorizations and attributes.

All of the commands which check attributes on the directory hierarchy automatically "walk" the directory tree, starting from a given directory. Simply issuing the command allows you to monitor an entire disk or any subtree you specify. You can even specify an "all disks" option to make a report covering all the disks on a module.

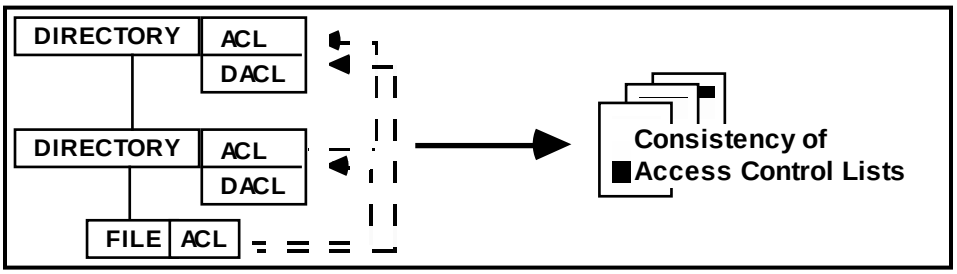
You can generate these reports by invoking individual commands, or you can access them through the security menu.

File and directory reports



Access control lists are used by the operating system to determine which kind of access each user is authorized for on a file or directory. This report shows the contents of access lists and default access lists on directories and access lists on files. Use this report to verify that access rights have been set according to security policy and that they have not been changed.

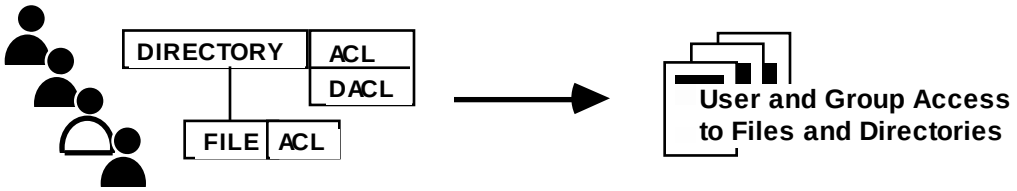
A command option lets you report (for auditing purposes) or suppress files with empty access lists.



An access inconsistency appears when a user has been restricted at some point in the directory tree, but has enough authority at a higher level to change access. This "hole" would allow the user to remove the restriction! This report scans the access lists from the starting point all the way back up to the pack master directory at the top of the tree, pointing out any inconsistencies along the way.

A command option allows you to choose between two types of checking:

- Type 1 checks access lists terms against those at higher directory levels.
- Type 2 uses the actual names in the registration database to verify access for all users against the terms in the access lists.

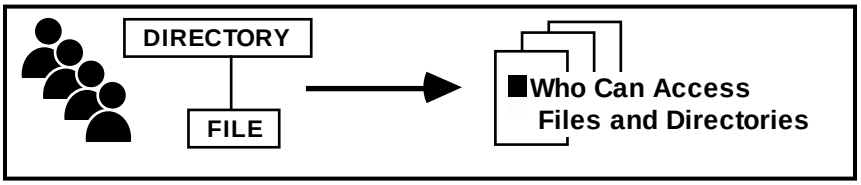


Once a security policy is in place governing what access groups and persons have in various parts of the directory tree, a set of three reports allow the Administrator to verify the implementation of the policy.

One report shows the access that a particular user has to objects in the directory tree.

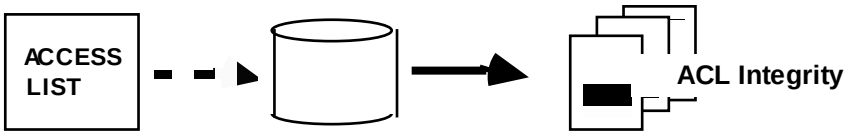
A second report shows the access that a particular group (such as SysAdmin) has to the objects in the directory tree.

The third report shows where the access rights of a selected user differ from those assigned to the user's group, highlighting the exceptions for this user.



The "owner" of a resource on the system, such as a particular data file, or the DP auditors may require a report verifying which users have what kind of access on that resource. However, correlating the entries in the registration database with the access control lists is a very tedious, time-consuming task.

This report shows the access allowed to each possible name in the registration database for the specified file or directory.

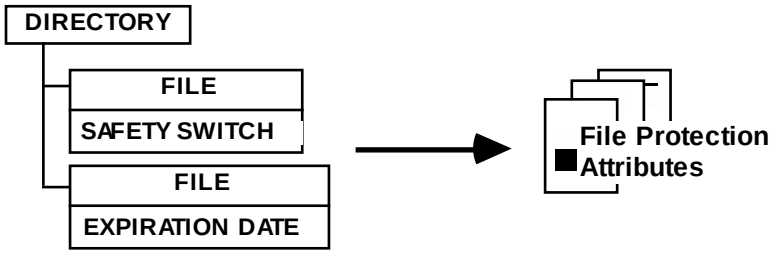


Making sure that no one has altered an access control entry is critical after you have implemented your access control policy.

This command creates a record of the ACL (and DACL) entries for a file or directory and stores it in an encrypted database. At a later time, the command reports whether the access list for the object has been changed since it was stored in the database.

A command option will create for you a command macro file containing the system commands necessary to "undo" access changes which are found and return them to their database settings automatically.

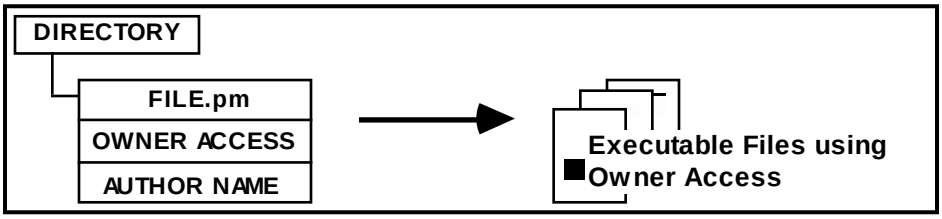
Other command options allow you to add, delete, and list the objects in the database.



A file can have an *expiration date* set on it, which prevents the deletion of the file before that date. A file could also have the *safety switch* set, which not only prevents the file from being deleted, but also moved, renamed, or otherwise altered.

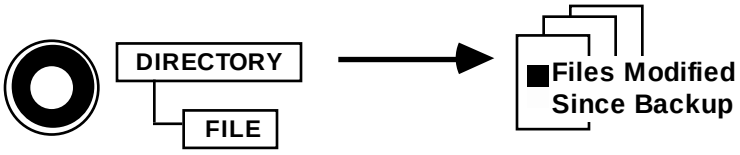
You will need to make sure that files which are supposed to be protected by these attributes have them on (and are not exposed to deletion or changing). You should also make sure that no files have these attributes set if they are not supposed to be there (and may remain on disk with their contents exposed when they should have been removed).

This report shows files which have the expiration date or safety switch set. A command option allows you to report (for auditing purposes) or suppress the names of directories which do not have any files with these attributes set.



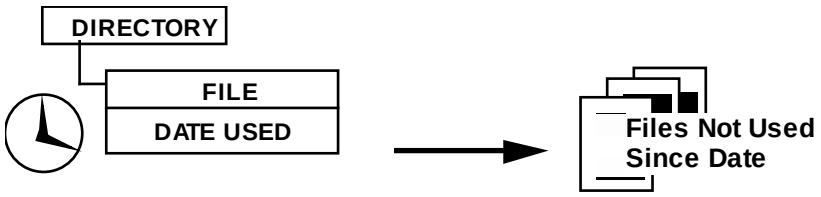
The owner access attribute allows an executable file to run with the access rights of the "author name" on the file, rather than the name of the user who is executing it. Used legitimately, this can secure a file from unauthorized access. When applied in an unauthorized way, it can allow users to bypass their normal restrictions. Use this report to make sure that programs which are supposed to execute with owner access have it on and that no other programs are using it.

This report shows executable files (ending in *.pm*) which have the owner access attribute set on. A command option allows you to report (for auditing purposes) or suppress the names of directories which either do not have any executable files or do not have any executable files with the owner access attribute set.



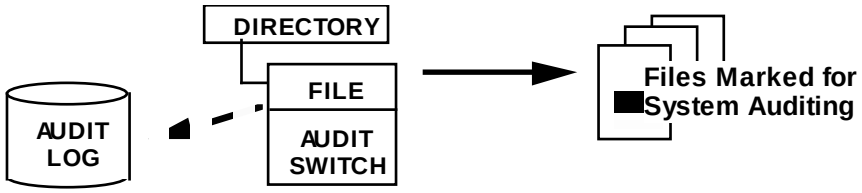
The success of your backup policy depends on scheduling the frequency of backups to match changes to the files.

To measure your exposure for unprotected files, this report shows you any files which have been modified on disk since they were last backed up.



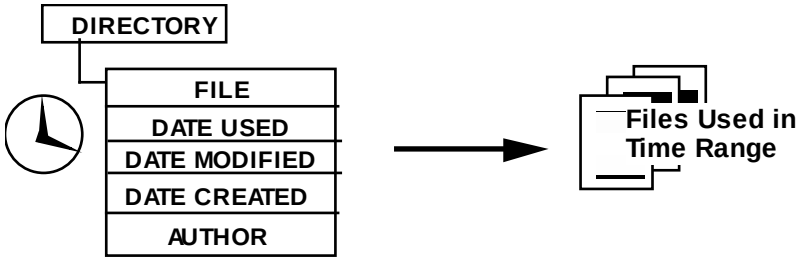
Leaving data on the system after it is no longer needed creates an opportunity for the information to be disclosed. Data files should be removed from the system if they are not required.

To measure your exposure for unused data files, this report shows you any files which have not been used within a given period of time.



You can mark individual files for auditing. If a marked file is touched by a user, a record is written to the system security log by the operating system.

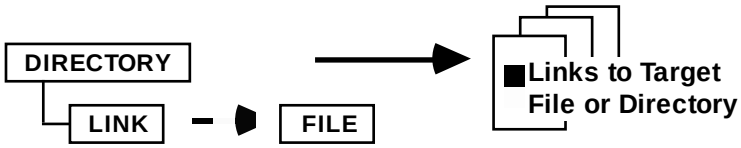
This report walks the directory hierarchy showing you any files which have been marked for auditing.



Knowing when files have been used or changed can be important in implementing your security policy.

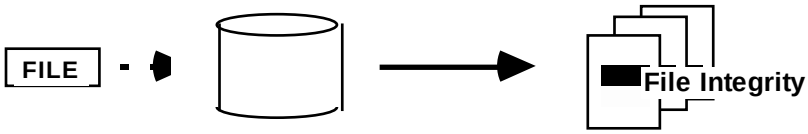
This report shows you any files which have been used (or modified or created) within a given period of time.

An option on this command will filter the report of new or modified files against a user name, only showing you files created or modified by the given user.



Directory links point to files and directories at other places in the directory hierarchy. If you move or delete the target of a link, users who use the link to access the target will be unable to find the new location.

To find links to an object before moving it, this report searches the module to find links to the given file or directory.



Making sure that no one has altered a data or executable file is of utmost importance to maintaining security on the system. The introduction of a "Trojan horse" or other harmful code can be catastrophic to the system.

This command creates a "fingerprint" of the specified file and stores it in an encrypted database. At a later time, the command reports whether the file has been changed since its fingerprint was stored.

A command option allows you to choose the level of fingerprinting to apply to the file

- Level 1 collects external attributes similar to the display_file_status command
- Level 2 performs Level 1 checking and then checksums the contents of the file. This will find many changes, including single and some multiple bit changes.
- Level 3 performs Level 2 checking and then performs a CRC check on the contents of the file. This will find virtually all changes, including most complementary multiple bit changes.

Other command options allow you to add, delete, and list the files in the database.

The report will list files which are new to a directory and not in the database, and files missing from the directory but which are in the database.

A user command is available that executes with the privileged command environment allowing any user to verify the start_up.cm and abbreviations file in their home directory, as well as whether there have been any changes to their account registration. This command can be placed in the user's startup file to be executed on login.

Auditing command security

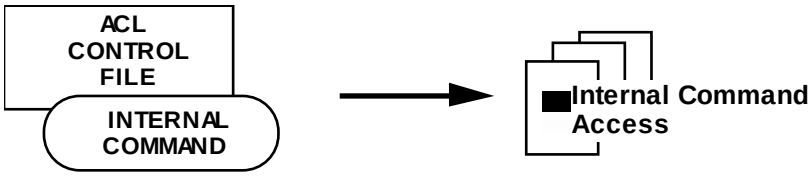
The external commands are executable files in the command search libraries. They are protected from unauthorized use and modification by access control lists, just like any other files. The commands described above to help ensure the authorized use of files and changes to files apply to these files as well. The integrity of the executable file can also be verified like any other file.

Any user or application command may be protected from unauthorized use and modification by access control lists, just like any other files. Their execution may be controlled and audited by LTS/OnGuard through the privileged command facility.

Internal commands can also be controlled for access, just like external commands.

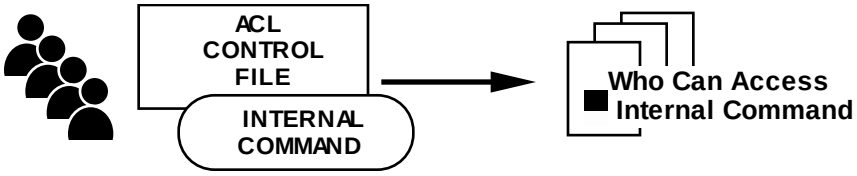
The special case of "prelogin commands", the commands available to a user before passing the screening of logging in, is a particular concern.

Command reports



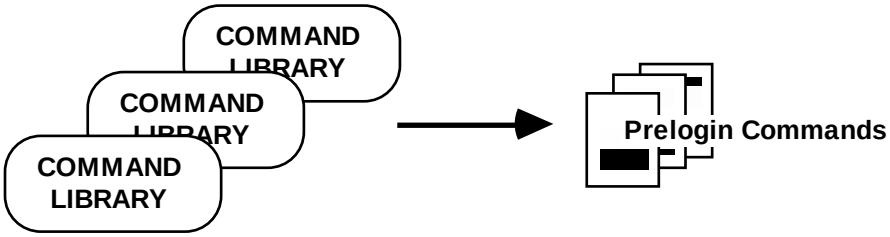
Internal commands can be associated with files in one of the system directories. The user's access to that file determines their access to the internal command.

This report shows the access rights to all of the control files in the system directory and which internal commands are associated with which file.



If you are using control files to establish access rights to internal commands you may wish to know how your access policy is implemented.

This report shows the access rights of all users in the registration database to the internal command which is specified.



"Prelogin commands" are available to the user before passing the login validation. The prelogin user executes as a privileged user with the access group name of "System", which is extremely powerful.

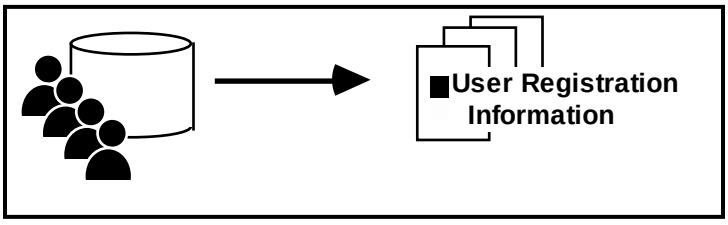
You should monitor the default search paths for commands to verify that no-one has added any prelogin commands without authorization or has substituted a file of their own as a Trojan horse.

This report shows any files in the command libraries which are available as prelogin. If the name is a link, the target of the link is reported.

Auditing user registration information

The user profile which the administrator puts in the registration data base controls what that particular user is allowed to access on the system, what restrictions are placed on them, and how much resource the user can consume.

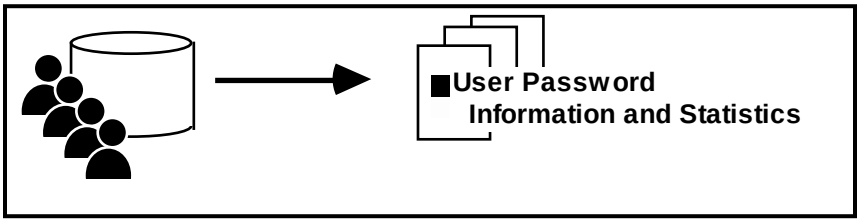
User information reports



Although the registration database is easy to administer with the system interface, there is no way to bring the registration information back out for filing or printing.

This report will show you (in brief or detailed format), the information about how the user is registered.

Using the command options, you can make a report showing registration information for one or more users. You can make a report selecting users who are registered in a specific group (such as SysAdmin) whether it is their primary group or one of their alternative groups. You can even request a report showing the users who are registered as privileged.



User passwords are the way that the operating authenticates a user for a particular account. You can select certain attributes for password formats and can specify how often they must be changed.

If a user attempts to login with a bad password, the operating system keeps track of those attempts until the user is successful. If the user makes several unsuccessful attempts in a row, the account is “terminated” or frozen, waiting for action by the administrator.

This report shows the current settings for password formats and forced expirations. It contains summary statistics showing the average and median password ages, and the percent of users in each category of password age. For individual users, it reports how old each password is and the date is was last changed. It will also report any users who have unsuccessful logins against their accounts since their last login and shows any accounts which have been terminated.

A command option allows you to report only a list of terminated users or externally-authorized users. Another option reports only users who have changed their passwords in the given number of days.

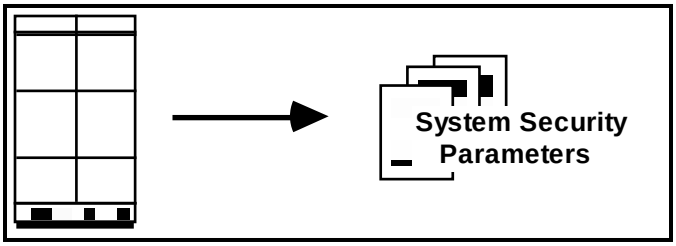
Specific commands allow the termination of a user account, and the removal of the account's home directory.

Auditing system security parameters

To set the various parameters on the system which control security features, you must execute several different commands. To see what the current settings are, you must bring up these commands on a terminal to examine the default values. The LTS/OnGuard reports allow you to return all of the information into a single report, either on the terminal or in a file for printing.

A site may also establish a set of 'standard' security setting, and the report will highlight any current settings which do not conform to the standard.

System parameters report



This report combines the values of security settings from several system commands and tools in a single report.

security_admin

Show security logging is in use and the approximate time of the last security log entry

login_admin

Show a variety of information about password and user attributes

logout_admin

Show how long terminals may remain unattended before being logged out

set_password_security

Show constraints for choosing passwords

audit_admin

Show settings for auditing of system objects to the system logs

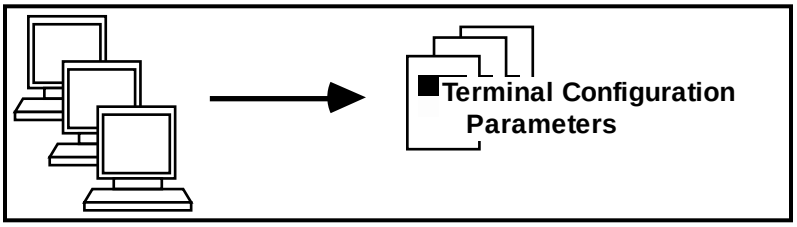
network_access.table

This file controls how much checking is done when users come in remotely over a network

Auditing terminal security

Each terminal line can be configured separately by the Administrator to have the characteristics appropriate for its use and location. These include whether the terminal can be used for logging in, whether privileged commands can be executed at this terminal, and whether it will listen for dialup users on a modem.

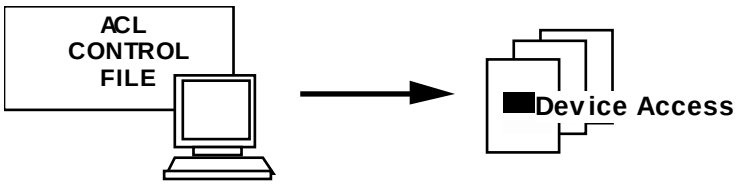
Terminal devices report



This report will show you the configured and current values for several configuration settings for a terminal line, such as whether privileged commands are allowed, whether users are allowed to login, whether dialups are allowed and whether the “force listen” attribute is set on. If these settings have been changed incorrectly, you may either have users who cannot perform their jobs, or you may have users who are capable of unauthorized actions.

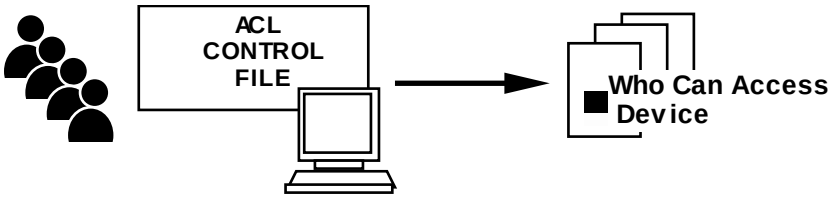
It will also show whether any user is currently on the terminal. If there is more than one user on a line, you may have an application error which will interfere with the use of the line, or you may have a Trojan Horse with a false login message. If more than one user is found, a warning message appears in the report.

For your convenience, you can also request a report that only shows terminals whose current settings are different from their configured settings. You can also request a report showing the differences from configured settings for any reported attributes, not just those which are security related.



Devices can be associated with files in one of the system directories. The user's access to that file determines their access to the device.

This report shows the access rights to all of the control files in the system directory and which devices are associated with which file.



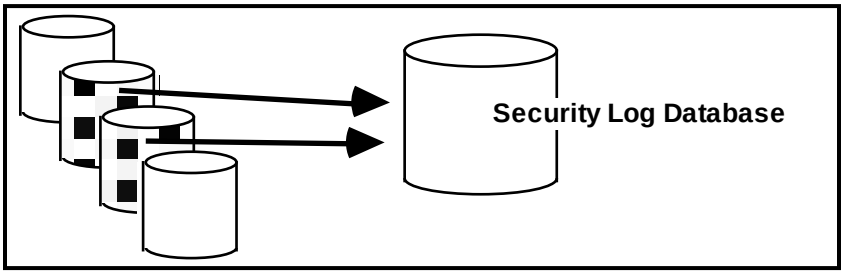
If you are using control files to establish access rights to devices you may wish to know how your access policy is implemented.

This report shows the access rights of all users in the registration database to the device which is specified.

Reporting security incidents

The operating system provides a security logging mechanism where various incidents are logged by the system into a security log for the day. Although the data is available to you in the log, it can be difficult to spot problems, especially on a busy system where lots of entries show up in the log.

The LTS/OnGuard utilities for handling security logs make it easy to spot problem areas and trends.



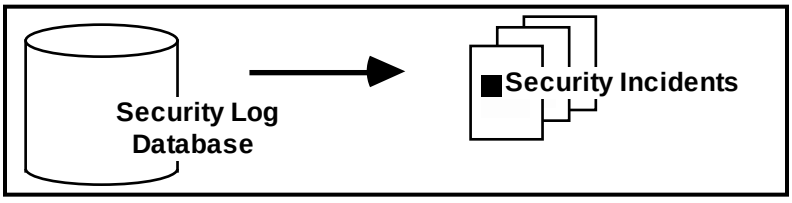
LTS/OnGuard consolidates a range of system security logs into a single database which can then be analyzed by security reporting commands.

You can select logs for the database with command options such as -today, -yesterday, -last_week, or -all. You can also specify start and end dates to get a particular range that you need to examine.

The command verifies the sequence of incident numbers in the logs and reports any missing numbers (which mean the logs have been edited!) and any place the sequence numbers restart at one (which means that the system was booted).

An option on this command exports the incident information to a comma-separated variable file. You can perform any further data analysis you wish by using this file.

Security incident reports



This report shows security incidents from the database with the incidents sorted by person name, group name, terminal name, target of the incident, incident type, event type, or status. You can choose to report

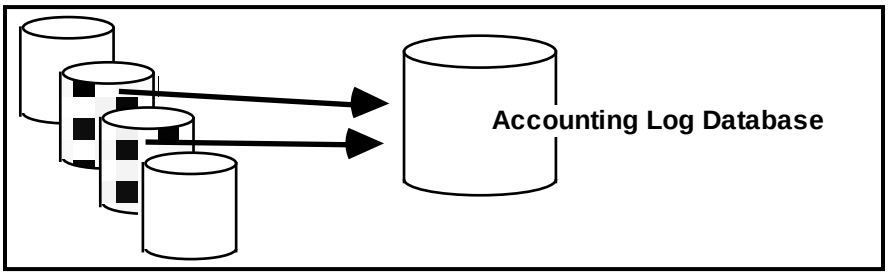
the detail for each incident or just the total counts of incident types. Keeping the counts over consistent time periods will help you to model a "typical" security profile for each module.

You can use this report to spot trends of incidents at unattended terminals, dialup lines, user login attempts, etc.

Reporting login activity

You may wish to keep track of when various users or background jobs logged in and logged out. The operating system provides an accounting mechanism where logins and logouts are logged by the system into an accounting file for the day. Although the data is available to you in the raw file, it does not “matchup” logins with logouts.

The LTS/OnGuard utilities for handling login activity make it easy to see when particular users were on the system.

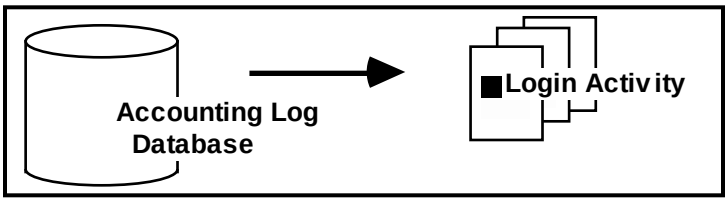


LTS/OnGuard consolidates a range of system accounting logs into a single database which can then be analyzed by a login reporting command.

You can select logs for the database with command options such as -today, -yesterday, -last_week, or -all. You can also specify start and end dates to get a particular range that you need to examine.

An option on this command exports the login information to a comma-separated variable file. You can perform any further data analysis you wish by using this file.

Login activity reports



This report shows login activity from the database with the sessions sorted by user name, process name, or terminal name.

You can use this report to spot trends of jobs which abort at various times and when particular users are on the system.

A command option allows you to report only interactive users, batch users, or all.

Reporting last login activity

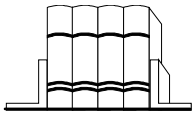
You may wish to report when a person was last logged in, or who has or has not logged in a certain period. LTS/OnGuard creates a compact database from the accounting logs which records last login and last process start activity for each user. The database will contain up to 2 years of history.

LTS/OnGuard will use this information to create a report which shows user activity. The report may be focused by selecting a person, a date, before/after/all based on the date, and sorted by person, alias, external name, or last login.

Reporting command or file access activity

You may wish to report who accessed a particular file or command. The operating system provides an accounting mechanism where command execution and file access is logged by the system into the day's accounting file.

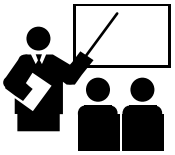
LTS/OnGuard will use this information to create a report which shows command execution and file/path utilization. The report may be focused by selecting a user, process, command, and/or file starname.



Technical Documentation

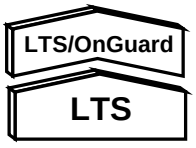
Reference manuals are available to guide the installation, configuration, administration, and use of the LTS/OnGuard utilities:

OG001	LTS/OnGuard Reference Manual
OG002	Installing a Release of LTS/OnGuard
OG003	LTS/OnGuard Software Release Bulletin



Training

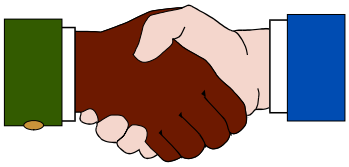
Many users do not require any training to install or use LTS/OnGuard. For those who desire formal training, LTS offers on-site seminars both for Stratus security topics and for using LTS/OnGuard to secure the system.



Software Support and Maintenance

LTS/OnGuard is backed by maintenance service which can be contracted for on an annual basis. Maintenance includes answering questions about the use of LTS/OnGuard, resolving and fixing any problems which may occur, and providing update releases and documentation as they become available.

About Transaction Design, Inc.



Transaction Design, Inc. (TDI) is the leading provider of security audit and control software for the Stratus VOS computer. Founded in 1990, TDI has helped users protect their data for over 20 years.

LTS/OnGuard is installed at Stratus users around the world. Business across the United States as well as in Asia, Australia, South America, and Europe depend on LTS/OnGuard to help them meet the needs of system administrators, security officers, auditors, and management.

Industries which use LTS/OnGuard to protect their assets include:

- Finance (banks, stock exchanges, credit cards)
- Retail (department stores, specialty chains)
- Health care (medical centers, pharmacies)
- Telecommunications
- VARs

Transaction Design, Inc.
542 San Pedro Cove
San Rafael, CA 94901
USA

1.415.256.8369
inform@transactiondesign.com
www.transactiondesign.com