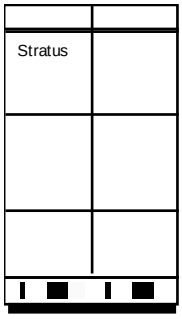
Security and Audit Solution for Stratus VOS Computers

LTS/OnGuard™

LTS/OnGuard audits and reports system security information. It protects system resources by controlling powerful authorizations.



SECURITY CONTROL

- Privileged Commands
- *analyze_system* Requests
- Inactive Timeout
- User Registration

AUDIT REPORTS

- Users
- Access Rights
- Passwords
- Commands
- Terminals
- Backups
- System Settings
- Security Incidents

LTS/OnGuard™ gives the Stratus Security Administrator an easy-to-use and efficient way to audit and document system security under the VOS® operating system. It allows the Administrator to control and monitor the use of the powerful privileged commands on a per-user, per-command basis, as well as control other system resources. LTS/OnGuard™ allows system administrators and operators to do their work without being privileged or in the SysAdmin group.

The LTS/OnGuard audit and reporting utilities consolidate and format system security and control information into easy-to-read, easy-to-understand reports. These give the Security Administrator the information necessary to audit and control the module. The reports are provided both as on-screen displays and as report files formatted for printing. The Security Administrator need not be VOS-knowledgeable to understand the reports.

LTS/OnGuard security control utilities allow the Security Administrator to establish classes for users. This changes the granularity of privilege for each user from its standard on/off state to a more secure per-command state. Execution rights to a privileged command (or an otherwise-secured command) are then granted selectively to a class of users, rather than to all privileged users. The end user can remain non-privileged but now has the ability to execute his or her permitted commands. Other features control the use of *analyze_system* requests, logout of selected processes for inactivity, and separation of duties for registering users.

LTS/OnGuard Audit Reports

The LTS/OnGuard auditing utilities investigate aspects of the system which impact security. They report the results on screen or in a formatted report file. The Administrator only has to execute a single audit command instead of many VOS commands to see important data. A standard report format allows the Administrator to focus on critical information. A security menu and daily batch reporting is included.

USERS

- Complete user profiles for selected or all registered users
- List of all privileged users
- List of all users in a selected group (such as SysAdmin)

PASSWORDS

- Password aging for each user
- Password constraints
- List of terminated accounts
- List of externally-authorized accounts
- List of users who have changed passwords within the specified number of days

FILE AND DIRECTORY ACCESS

- Access control lists for objects below the selected directory
- Analysis of access list consistency *vs.* higher access lists and *vs.* registered user names
- Analysis of specified user access *vs.* group access
- Files with safety switch or expiration date set
- Access of all users to a given file or directory
- Who accessed a file or path

FILE/DIRECTORY INTEGRITY

- Compare file attributes and directory contents to a database to determine if a file has been altered, added, or deleted

SYSTEM SECURITY SETTINGS

- State of security logging, password constraints, timeout periods for inactive users, and remote system access restrictions
- List of restricted users

LOGIN DEVICE SETTINGS

- Current *vs.* configured values for attributes that impact security (such as privilege and force listen)
- List of current users for each device

FILE BACKUPS

- Files which have been created or modified since the last backup

COMMAND ACCESS

- Commands which are available to users before logging in
- Executable files which have the owner access attribute set
- Who executed a command

CONSOLIDATED LOG REPORTS

LTS/OnGuard commands consolidate important system logs for a selected time period into an incident database. From this database, the Administrator can produce sorted reports with one command. A command option allows the exporting of system data into a comma-separated file, suitable for further analysis.

SECURITY INCIDENTS

- Consolidates system security logs into an incident database
- Reports from database with incidents sorted by user, group, or terminal
- Reports counts of incident types, allowing trend monitoring
- Exports comma-separated file

USER ACTIVITY

- Consolidates system accounting logs into history databases
- Reports from database with login sessions sorted by time, user, or device
- Reports from database when a person last logged in or started a process
- Reports from database who accessed a command or path
- Exports comma-separated file

LTS/OnGuard Security Controls

The LTS/OnGuard control utilities give the Administrator tighter control over what users can do on the system than the operating system alone provides. A user may need to execute certain powerful privileged commands and *analyze_system* requests to do their job properly, but authority is granted by VOS as all or none. The LTS/OnGuard environments allow the Administrator to grant authority down to the individual command on an as-needed basis. Similar control and auditing may be done for any command at the Administrator's discretion, whether it be a standard VOS command or application program or macro. Other tools allow separation of duties for registering users and control of timeout for inactivity on a per-terminal, per-user basis.

PRIVILEGED COMMAND ENVIRONMENT

LTS/OnGuard allows you to establish a controlled environment for users to execute the powerful (but potentially dangerous) privileged commands. Other commands may be similarly controlled and audited.

- Allow a specific user to execute specific commands
- Establish classes so that users in a class can execute specific commands
- Require that a user only execute commands from a specific terminal authorized for that user
- Automatically create an audit trail showing every command that is requested, its arguments, and completion code
- Control which users can update specific devices

analyze_system ENVIRONMENT

LTS/OnGuard allows you to establish a controlled environment for users to execute *analyze_system* requests, just like privileged commands. Users are authorized only for necessary *analyze_system* requests according to their class. An audit trail is created for every request, including all of the given arguments.

SEPARATION OF DUTIES FOR USER REGISTRATION

LTS/OnGuard provides a forms-driven interface which looks to the user like the system command *registration_admin* for adding, deleting, and updating user profiles. However the user need not be privileged or in the SysAdmin group to perform these activities. The interface uses the privileged command environment to control whether one user can create and process the profiles or whether it requires a second user to approve and process the changes. After the changes are sent to the registration database, the interface updates a history file. A report utility is available to retrieve the audit trail from the history file, showing users added and deleted and modifications made to each field of user profiles. Commands are also available for terminating user accounts and removing home directories.

PER-USER, PER-TERMINAL LOGOUT CRITERIA FOR INACTIVITY

The VOS operating system provides a mechanism for logging out users who remain logged in but inactive on a terminal. When activated, this mechanism logs out every terminal after the same amount of grace time. LTS/OnGuard provides a background monitor which uses a site-configured table of terminal names, user names, and grace times. When the monitor detects that one of the terminals or users in its table has exceeded the grace time for inactivity, it stops the inactive process.

LTS/OnGuard — the VOS security solution for you

LTS/OnGuard is installed at Stratus users around the world. Businesses 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.
California, USA

1.415.256.8369
inform@transactiondesign.com
www.transactiondesign.com