



LT Auditor+ 9

for SUSE® Linux NSS File Systems

360° View of NSS File Systems on SUSE Linux Servers

Clear, Concise, Actionable Intelligence

Ensuring the privacy, integrity and availability of sensitive and confidential files is key to meeting security and compliance initiatives.

LT Auditor+ 9 for SUSE Linux NSS File Systems is designed to provide detailed auditing and monitoring of NSS file system activity—delivering Clear, Concise, Actionable Intelligence.

LT Auditor+ 9 for SUSE Linux NSS File Systems interacts seamlessly and unobtrusively with the operating system to capture:

- Creations, Modifications and Deletions;
- Successful/Failed File and Folder Operations; and
- Changes to Trustee Assignments on Files and Folders

LT Auditor+ 9 for SUSE Linux NSS File Systems delivers a bullet-proof audit trail, through easy-to-read forensic reports and real-time alerts, to precisely identify **Who** did **What**, from **Where** and **When**.

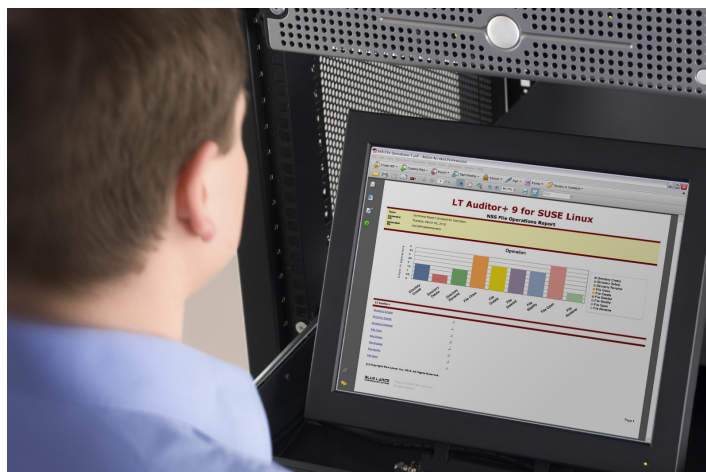
One look and you will see why thousands of organizations have chosen LT Auditor+ for more than 20 years to maximize the return on their security and compliance investment.

Compliance in a Click

LT Auditor+ 9 for SUSE Linux NSS File Systems, part of the LT Auditor+ 9 for SUSE Linux suite, provides the intelligence required to audit user and administrative activity in accordance with organizational policies to demonstrate compliance with regulations and guidelines such as Sarbanes-Oxley (SOX); GLBA; FDIC/OCC; FFIEC; PCI DSS; HIPAA; and FISMA; and IT security frameworks such as COBIT 4.1 and NIST SP800-53.

LT Auditor+ 9 for SUSE Linux NSS File Systems' built-in scalability and fault tolerance prevents audit data loss and ensures the consolidation of audit data from servers within the organization. Without fear of loss, encrypted data collected through all LT Auditor+ agents is deposited into a single, secure repository, which provides accurate compliance reports on-demand.

LT Auditor+ 9 for SUSE Linux NSS File Systems provides executive summary reports, with drill-down capability detailing administrative and user activity about files, folders and users on servers. Reports can be scheduled for automatic distribution to administrative personnel at designated intervals.



Product Benefits

LT Auditor+ 9 allows organizations to immediately reap the benefits of continuous security and compliance.

Prepare for the IT security audit process with comprehensive reports delivering clear, concise, and complete information on unsuccessful login and authentication attempts; access control changes made by privileged users and administrators; and access to sensitive files and resources. LT Auditor+ 9 for SUSE Linux NSS File Systems simplifies the IT security audit process by providing automated report delivery using a robust scheduler and valuable report templates.

Meet compliance control transformation requirements pertaining to accountability, transparency and integrity by monitoring changes to controls and privileges that create material weaknesses. Compliance control transformation requirements are met by monitoring system login activity, application access, and modifications/deletions of sensitive files, including system configuration files. LT Auditor+ 9 for SUSE Linux NSS File Systems ensures the availability and integrity of mission critical servers hosting databases containing sensitive information, such as financial data, health records and other confidential information.

Ensure privacy, confidentiality and integrity of sensitive information by monitoring changes to the trustee assignments that define user and group access permissions to critical servers, files and folders. LT Auditor+ 9 for SUSE Linux NSS File Systems comprehensively audits creations, deletions, modifications and access to sensitive files and folders.

Product Features

- ❖ 24x7 Monitoring with real-time alerts
- ❖ Management Summary reports with drill-down capability
- ❖ Over 100 security and compliance report templates
- ❖ Translation and correlation of user activity into plain English reports and alerts
- ❖ Multiple report formats including Excel, Word, HTML and PDF
- ❖ Automatic report scheduling and delivery
- ❖ Audit access to files, folders
- ❖ Enterprise-wide data consolidation
- ❖ Comprehensive Auditing with Granular filtering
- ❖ Audit the Auditor
- ❖ Robust, fault tolerant and load balanced architecture
- ❖ Multi-Manager-Agent architecture
- ❖ Automatic audit policy deployment

Improve incident response through immediate alerts of monitored authorized and unauthorized access to files and folders. LT Auditor+ 9 for SUSE Linux NSS File Systems accurately tracks the execution, modifications and deletions of critical files and helps determine the scope of damage due to unauthorized user activity or the execution of malware (virus, trojans, and spyware). Comprehensive reports detail the activity leading up to an event, thus; reducing the time required to investigate the magnitude of a security incident.

Save Time and Money with clear, concise, easy-to-read LT Auditor+ reports and alerts in plain English, eliminating the complex task of sifting through large volumes of fragmented, incomplete data provided by system logs, dispersed throughout the organization. LT Auditor's scalable, fault tolerant design, coupled with superior audit data filtering and enterprise-wide data consolidation provides a powerful auditing solution with optimal performance.

Engineered for Flexible, Reliable Auditing

Secure and Scalable

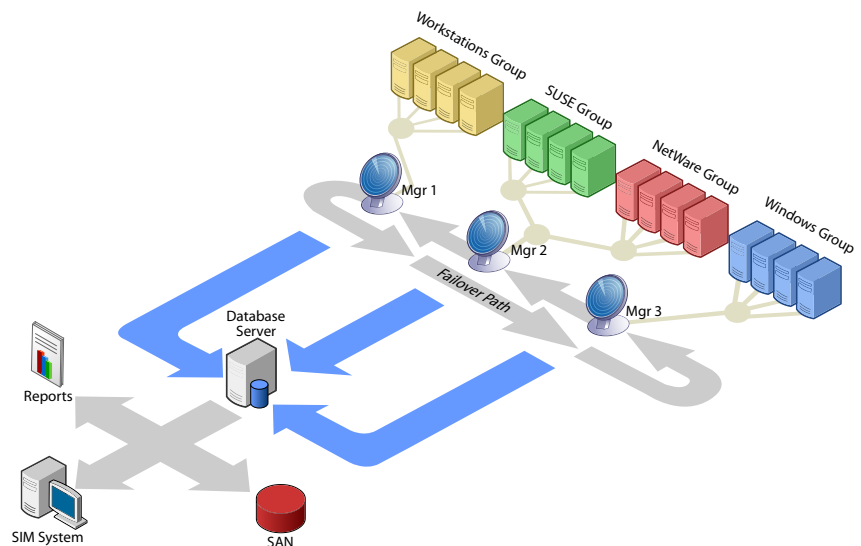
LT Auditor+ 9 employs a secure and scalable architecture which allows consolidation of audit data from thousands of servers within an enterprise into a centralized repository. The flexible manager-agent architecture allows for logical grouping of servers, each of which can be handled by separate managers, to easily oversee the deployment of audit policies and schedule the encrypted transfer and consolidation of audit data.

Built-in Fault Tolerance

With built-in fault tolerance, LT Auditor+ 9 ensures the availability of audit data. If the link between an audited server and its primary manager is severed, the communication is automatically rerouted to the next available manager. The audit agent will continue to monitor the availability of its primary manager, shifting back once communications are restored.

Comprehensive Reporting and Alerting

LT Auditor+ 9 comes with an early warning detection system that alerts security administrators immediately when a breach or violation occurs.





Alerts may be delivered via SMTP/e-mail, SNMP, or Syslog messages.

Reporting with LT Auditor+ 9 has never been faster or easier. Centralized reporting allows users to consolidate data and create forensic analysis reports organization-wide. LT Auditor+ 9 offers over 100 standard reports that target both security and compliance, all while adding drill-down capability to individual events. Consolidation offers reporting across multiple platforms including Windows, NetWare and SUSE Linux; providing true enterprise wide reporting of user activity. Additionally, new reports may be created and customized to display only required details and scheduled for automated delivery.

Management Summary Reports

LT Auditor+ 9 for SUSE Linux NSS File Systems includes several high-level graphical reports that summarize data and information with drill-down capabilities to view specific details. This alleviates the issue of parsing through hundreds of pages of data while looking for information.

Compliance Reports

Audited Operations

Files Auditing Activity

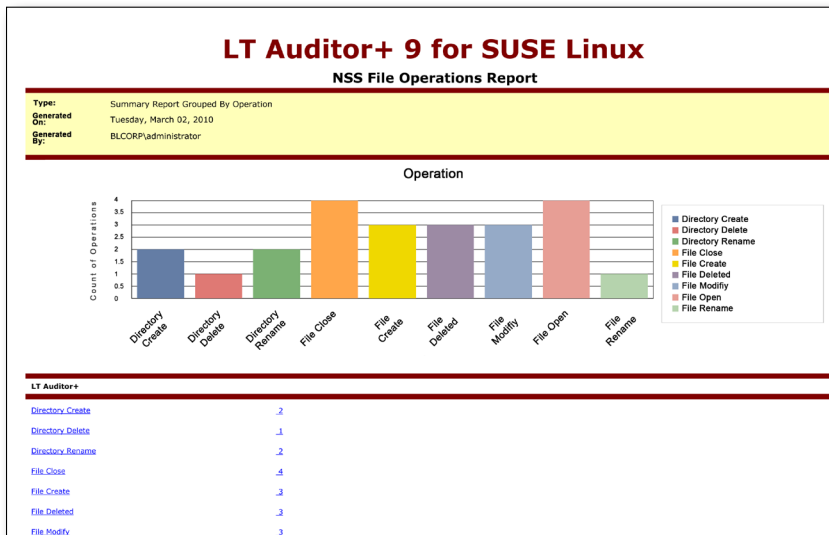
- ❖ File Open
- ❖ File Close
- ❖ Create File
- ❖ Delete File
- ❖ Rename File
- ❖ Modified File
- ❖ Create Link

Directory Auditing Activity

- ❖ Create Directory
- ❖ Remove Directory
- ❖ Rename Directory

Trustee Auditing Activity

- ❖ Add Trustee
- ❖ Remove Trustee
- ❖ Set Inherited Rights



LT Auditor+ 9 for SUSE Linux NSS File Systems includes reports that help organizations stay compliant with regulations such as Sarbanes-Oxley (SOX); GLBA; FDIC/OCC; FFIEC; PCI DSS; HIPAA; and FISMA; and IT security frameworks such as COBIT 4.1 and NIST SP800-53.

Date & Time	User	Node	Operation	File	Server
2/16/2010 12:39:29PM	cbean.acme	10.0.4.5	File Create	AUDIT:/HR/Personnel/Salaries.xlsx	ACMEPROD
2/16/2010 12:39:33PM	cbean.acme	10.0.4.5	Directory Create	AUDIT:/HOME/CBEAN/New Folder	ACMEPROD
2/16/2010 12:39:40PM	cbean.acme	10.0.4.5	Directory Rename	AUDIT:/HOME/CBEAN/New Folder	ACMEPROD
2/16/2010 12:39:42PM	cbean.acme	10.0.4.5	File Open	AUDIT:/HR/Personnel/Salaries.xlsx	ACMEPROD
2/16/2010	cbean.acme	10.0.4.5	File Close	AUDIT:/HR/Personnel/Salaries.xlsx	ACMEPROD

System Requirements

LT Auditor+ Manager

Processor - Intel Pentium 4 Processor or above

- RAM- 1 GB RAM
- Hard Disk - 200+ GB
- Operating System -
- Microsoft Windows Server 2003/2008
- Microsoft Windows 2000 SP4+ / MDAC v. 2.7
- Microsoft Windows XP
- Microsoft Windows Vista
- Microsoft Windows 7
- Software - .NET v1.1
- Database - Microsoft SQL Server 2000/2005, Oracle 9i/10g

LT Auditor+ Agent

- RAM - 512 MB RAM
- Hard Disk - 10+ GB
- Operating System
- SUSE Linux Enterprise Server 10 with Service Pack 3
- Open Enterprise Server (OES2) with Service Pack 2

Get Started Now

LT Auditor+ 9 for SUSE Linux NSS File Systems is configurable to fit seamlessly into any organization—from the largest to the smallest. In addition to LT Auditor+ 9 for SUSE Linux NSS File Systems, Blue Lance also offers comprehensive, flexible and reliable auditing solutions for eDirectory and a full complement of products for Windows servers and workstations.



Blue Lance, Inc.
410 Pierce Street, Ste. 303
Houston, TX 77002

Toll Free: 800.856.2583
713.255.4800
Fax: 713.622.1370
www.bluelance.com

BLUE LANCE
COMPUTER SECURITY SOFTWARE