DATA SHEET

LT AUDITOR+

SUSE LINUX EDIRECTORY

Real Time Auditing for SUSE LINUX eDirectory

BLUE LANCE

THE CHALLENGE

Whether on Netware or Linux, ensuring the privacy, integrity and availability of sensitive and confidential files is the key to meeting compliance and security initiatives. Managing either eDirectory in a dynamic organization can be a complicated task. Due to their architectural design and commonly used security policies, there are some basic security risks that most eDirectory implementations share.

THE SOLUTION

Blue Lance's LT Auditor+ for eDirectory is designed to provide detailed auditing and monitoring system activity delivering Clear, Concise, Actionable intelligence. LT Auditor+ for eDirectory interacts seamlessly and unobtrusively with the operating system to capture all essential activity and changes for SUSE Linux eDirectory.

Transform your cryptic & chaotic logs to clear, actionable reports

BLUE LANCE

eDirectory Activity Report

LT Auditor+ Oversight Report

Generated On: Tuesday, October 16, 2012
Generated By: LTAMGR\Administrator

Date & Time	User	Node	Remarks
10/4/2012 3:31:36AM	Lmcashen.TBD.ACME	10.0.4.200	Failed to login in to server BLPROD4
10/4/2012 9:49:19AM	rscott.HR.Users.Acme	10.0.4.200	Logged in to server BLPROD4
10/4/2012 9:50:00AM	rscott.HR.Users.Acme	10.0.4.200	Deleted inetOrgPerson 'fDario.Acme' on ACMEEDIR
10/4/2012 1:19:01PM	rscott.HR.Users.Acme	10.0.4.200	Failed to login in to server BLPROD4
10/4/2012 1:19:11PM	rscott.HR.Users.Acme	10.0.4.200	Logged in to server BLPROD4
10/4/2012 1:25:01PM	rscott.HR.Users.Acme	10.0.4.200	Created inetOrgPerson 'cbean.Acme' on ACMEEDIR
10/4/2012 1:26:10PM	rscott.HR.Users.Acme	10.0.4.200	Made 'cbean.Acme' security equivalent to 'admin.Acme' on ACMEEDIR
10/4/2012 2:01:51PM	rscott.HR.Users.Acme	10.0.4.200	Logged in to server BLPROD4
10/4/2012 4:42:29PM	rscott.HR.Users.Acme	10.0.4.200	Made 'jJacobs.Acme' security equivalent to 'admin.Acme' on ACMEEDIR
10/4/2012 4:42:29PM	rscott.HR.Users.Acme	10.0.4.200	Added value of attribute 'securityEquals' [cn=admin,o=Acme] for 'jJacobs .Acme' [inetOrgPerson] on ACMEEDIR
10/4/2012 4:44:42PM	rscott.HR.Users.Acme	10.0.4.200	Logged in to server BLPROD4
10/4/2012 5:11:04PM	rscott.HR.Users.Acme	10.0.4.200	Logged in to server BLPROD4
10/4/2012 8:51:05PM	rscott.HR.Users.Acme	10.0.4.200	Added value of attribute 'fullName' [Frank Dario] for 'fDario .Acme' [inetOrgPerson] on ACMEEDIR
10/4/2012 8:51:05PM	rscott.HR.Users.Acme	10.0.4.200	Added value of attribute 'Language' [] for 'fDario .Acme' [inetOrgPerson] on ACMEEDIR
10/4/2012 8:51:05PM	rscott.HR.Users.Acme	10.0.4.200	Added value of attribute 'sn' [Frank Dario] for 'fDario .Acme' [inetOrgPerson] on ACMEEDIR
10/4/2012 8:51:05PM	rscott.HR.Users.Acme	10.0.4.200	Added value of attribute 'uid' [fDario] for 'fDario.Acme' [inetOrgPerson] on ACMEEDIR
10/4/2012 8:51:05PM	rscott.HR.Users.Acme	10.0.4.200	Added value of attribute 'creatorsName' [cn=admin,o=Acme] for 'fDario .Acme' [inetOrgPerson] on ACMEEDIR
10/4/2012 8:55:08PM	rscott.HR.Users.Acme	10.0.4.200	Logged in to server BLPROD4

End of Report

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 raw event log data into plain English reports and alerts

Multiple report formats including Excel, Word, HTML and PDF

Automatic report scheduling and delivery

Audit files, folders, user authentications and USB storage devices

Automatic archiving of Windows native event logs

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

Built-in agent status and health monitoring

THiNK: Ahead.

410 Pierce Street | Houston, Texas 77002 | bluelance.com

DATA SHEET

LT AUDITOR+

SUSE LINUX EDIRECTORY

Real Time Auditing for SUSE LINUX eDirectory

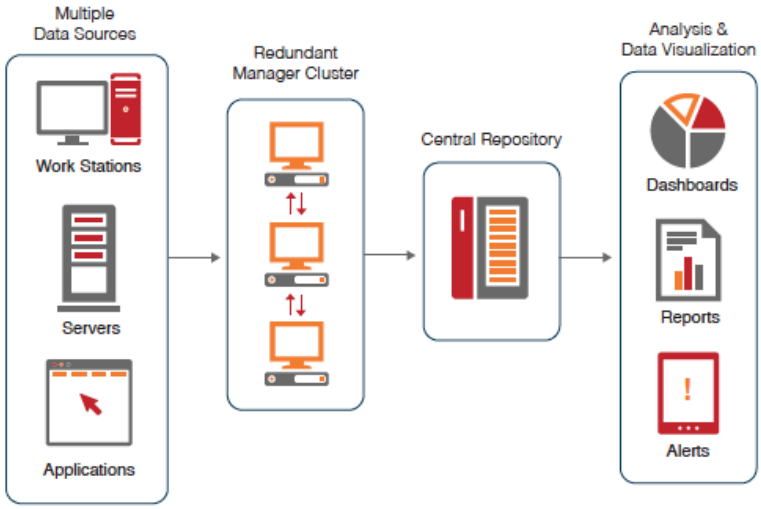
BLUE LANCE

BENEFITS

LT Auditor+ for eDirectory is configurable to fit seamlessly into any organization, large or small. LT Auditor+ allows your organization to immediately reap the benefits of continuous security and compliance monitoring by enabling your organization to improve incident response time, provide comprehensive audit reports, meet compliance control transformation requirements, ensure privacy, confidentiality and integrity, all while saving time and money.

Reporting with LT Auditor+ for eDirectory has never been faster and easier. Through centralized reporting, users can consolidate data or create forensic analysis reports organization-wide. LT Auditor+ for eDirectory offers over 100 standard reports that target both security and compliance, all while adding drill-down capability to individual events. Additionally, new reports may be created and customized to display only required details and scheduled for automated delivery.

Information Flow



ABOUT BLUE LANCE

Blue Lance is a global provider of cybersecurity governance solutions helping organizations protect their digitally managed assets for over 25 years. Blue Lance solutions allow organizations to minimize risk from sophisticated Cyber thieves, complex industry and government regulations. Blue Lance stands with customers as a trusted partner offering cybersecurity governance solutions that enable expanded oversight and validation of audit readiness for internal policies, industry or government regulations; and the safe keeping of confidential information, trade secrets, intellectual property, critical infrastructure, and other digitally managed assets. Blue Lance is headquartered in Houston, Texas.

AUDITED OPERATIONS

EDIRECTORY OBJECT AUDITING

Create Object
Delete Object
Rename Object
Move Object
Modified Object
Add NDS Value
Delete NDS Value
Add Security Equivalence
Remove Security Equivalence

DIRECTORY AUDITING

Schema Class Added
Schema Class Removed
Schema Attribute Added
Schema Attribute Removed

ACCOUNT MODIFICATION AUDITING

Enable Account
Disable Account
Set Password
Change Password
Account Locked Out
Account Unlocked

GROUP MEMBERSHIP AUDITING

Add Member to Group
Remove Member from Group

THINK: Ahead.