[CM::
[metadata:
title
desc
kwds]
[content:
H1
Subtitle
[Intro: 2 para high-level desc of specific things X does to solve problem Y
Bulleted list: benefits/value of doing X]
[Problem block: short list and desc of main problems]
[Solution block: how problem solved with features and functions]
[Features box: sidebar with short bulleted list of features]
]

============================
METADATA

Title: File Activity Monitoring

Description: Likewise's high-performance file activity monitoring system audits access to files, tracks changes, sends alerts, and generates compliance reports.

Keywords: file activity monitoring, unstructured data activity monitoring, file server monitoring, data security, compliance auditing, FAM

============================
H1:
File Activity Monitoring

Subtitle:
Tracking Unstructured Data for Security and Compliance

As unstructured data rapidly accumulates on file servers and NAS systems, a new security requirement is becoming paramount: File activity monitoring. It stems from the pressing need to track and protect sensitive unstructured data.

Likewise Data Analytics and Governance includes a cross-platform, high-performance file monitoring system that associates user identities with file access and content changes in real time. The identity-aware system can audit access to folders and files, track changes to content, send security alerts when exceptions occur, and generate compliance reports.

The benefits of file activity monitoring, or FAM, are far-reaching:

<b>*Demonstrate compliance with regulations and standards.</b>

<b>*Mitigate the risk of security breeches, data loss, fraud, noncompliance, and legal problems.</b>

<b>*Ensure the quality, integrity, and availability of important unstructured data to improve decision making and bolster the bottom line.</b>

<b>*Reduce the costs associated with identity management, records management, storage, and security. </b>

============================

Problems in File Activity Monitoring

Monitoring unstructured data is harder than storing it. Three problems stand in the way:

<b>1. Data silos.</b> Because of different storage access protocols, the data of Windows users and Unix users ends up in separate silos, making it difficult to track the data with a single, standardized monitoring system.

<b>2. User identities.</b> Because of different identity management and access control systems, it is hard to associate file events with user identities on both Unix and Windows computers.

<b>3. Performance.</b> Because of the sheer volume and rapid growth of file events for unstructured data, most monitoring solutions bog down in several areas: Network performance issues caused by an over-reliance on extraneous layers like sniffers, agents, and shims; file server performance issues traditionally associated with collecting millions of file events; and database performance and scalability issues associated with the write speeds and clustering requirements of SQL databases.

The Likewise monitoring system solves all three problems by integrating a multiprotocol storage system with an identity management system and a high-performance NoSQL database. The combination provides centralized, standardized file activity monitoring that can track unstructured data across data silos, associate file events with user identities, and perform at mach speed. When other solutions bog down, Likewise excels.

============================

Solution

Monitoring Across Data Silos

Because Likewise Storage Services supports both the SMB/CIFS and the NFS protocols, the Likewise Data Governance and Analytics application can monitor file activity that originates from both Windows and Unix or Linux clients.

Not using Likewise Storage Services? No problem: The Likewise application can accept a wide range of events and log data through its predefined RESTful API, including events and log data from NetApp and EMC NAS devices.

Associating File Events with User Identities

File activity monitoring is at its most powerful when it is tied to identity management. The integration of the identity management system with the monitoring system is a precondition for effective <a href="exception-monitoring.php">exception monitoring</a>. It is effective because it records exceptions at the intersection of user identity, resource access, and file activity. As such, it provides visibility in a security-aware context.

Tapping NoSQL Technology for High-Performance

The performance of the event monitoring system plays a key role in how efficiently end-user components that rely on events will function. To be expedient and relevant, the dashboard and <a href="/solutions/file_server_reporting_features/index.php">compliance reports</a> depend on how fast events are collected and correlated.

The NoSQL database adds a unique high-performance layer: It digests events with write speeds faster than SQL databases and, more importantly, can easily scale horizontally to handle more events.

File Integrity Monitoring for Compliance
Even in multi-departmental enterprises with millions of file server events, the NoSQL database scales to deliver high-performance monitoring to help meet such compliance regulations as the file integrity monitoring stipulated in PCI DSS requirement 11.5 -- raising an alert for unauthorized changes to content files.

============================
Visualizing Activity in Context for Situational Awareness
The importance of file activity monitoring highlights the shift in IT toward contextualized security -- in this case, viewing content in the context of identity, entitlements, access patterns, sensitivity levels, file events, and other factors related to security.

A file server with an identity service can collect supplemental data, such as the following, which can be combined in different ways to produce real-time situational awareness:

<!-- bulleted list with first word or two and colon set in bold as a lede-in -->
*<b>Identity:</b> Authentication transactions, business roles of users and groups, entitlements, permissions.

*Access: Whether access is granted or denied, type of access (read or write), time of access, IP address and type of client requesting access, etc.

*Content and metadata: Tracked directories or files, files marked sensitive, types of files such as spreadsheets or Word documents, directory name, file name, files marked for a compliance regulation.

*Event: Actions such as read, write, modify, copy, move, or delete a file or directory; changes to security descriptors and permissions.

When identities, access, content, and events are tracked at the file server, monitoring is enriched by contextualized security data -- the correlations that take place at the intersection of users with known roles and entitlements accessing tracked content to perform logged events.

The data lights up a dashboard with context-aware security events and exceptions that can be used for decision making, security-policy adjustments, troubleshooting, forensics, and compliance auditing.

============================
<!-- CAN YOU PLACE THIS AS A SIDE BOX OR SOME SUCH NEAR TOP OF PAGE? -->
Features
*Identity-aware monitoring

*Dashboard with custom views
*Alerts for policy violations and exceptions by email and SNMP
*Custom reports
*User rights monitoring
*Privileged user monitoring
*Exception monitoring
*Event aggregation from various sources, including NetApp and EMC NAS devices
*NoSQL database for super-fast performance and analytics
*Compliance reports for HIPAA, PCI DSS, FISMA, and SOX