

=====

METADATA

TITLE:

Exception Monitoring and Reporting

Desc:

Likewise provides identity-aware exception monitoring and reporting for unstructured data stored on file servers.

Kwds:

exception monitoring, exception reporting, unstructured data, NAS, network attached storage, data monitoring, information security, compliance reporting, file server

=====

H1:

Exception Monitoring and Reporting

Subtitle:

Identity-Aware Exception Monitoring for Security and Compliance

=====

Unmanaged piles of unstructured data can be unnerving. When file servers overflow with documents that might contain sensitive, proprietary, or confidential content, you get that sinking feeling: There might be information in there that violates one or more compliance regulations. And if exposed, whether through an internal or external threat, it could damage the reputation of your company, undermine your competitive advantage, and lead to legal problems and fines.

Identity-aware exception monitoring and reporting is an effective way to get visibility into anomalies around access to unstructured data: You can see when someone who should not access or modify a document attempts to do so. Exception monitoring can help you comply with compliance regulations such as PCI DSS Requirement 11.5, which mandates that alerts are raised for unauthorized changes to content files. The benefits of exception monitoring and reporting prop up information security and IT operations:

- *Identify and rapidly respond to security threats and incidents.
- *Cut costs associated with security policies, breaches, and responses.
- *Comply with regulations like HIPAA, SOX, and PCI DSS.

There are two complementary approaches to exception-based management: exception monitoring and exception reporting. The monitoring takes place in near real-time so you can proactively respond to potential security incidents. Reporting takes place later so you can compile information to show regulatory compliance.

=====

Barriers to Effective Exception Monitoring

Traditionally, there have been two major barriers to effective exception monitoring of

unstructured data in large enterprises: performance and identity awareness.

Performance

The millions of file events generated by hundreds, if not thousands, of users in a large enterprise can easily overwhelm the network and the monitoring system. In an enterprise environment with, for example, 50 million objects stored across a 25-node array, more than 2 million objects can be modified a day, with the number of events for access attempts and file views much higher.

Because of the sheer number of events generated as a multitude of users view and modify files, performance requirements have largely blocked large-scale, effective exception monitoring. Yes, it's been tried, and some vendors have solutions, but all too frequently performance issues emerge: networks slow down, databases overwhelm disk space, dashboards freeze.

The performance of the event monitoring system is the pivot point that determines the viability of exception monitoring. Once the performance issue is solved, it's a relatively easy task to parse out the access-denied events, the write-failure events, and the failed attempts to change security descriptors. Another problem, however, remains: Without tying such exceptions to the identities of users, the effectiveness of exception monitoring is limited.

Identity Awareness

Exception monitoring isn't particularly useful unless it can tie exceptions to people. In heterogeneous networks, most monitoring frameworks fail to do so because different identity management systems for Unix and Windows users impede the association of user identities with events.

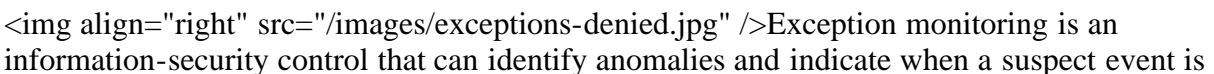
=====
The Likewise Exception Monitoring Solution

The Likewise Storage Services platform includes a [cross-platform access control](/products/likewise_storage_services/cross-platform-storage-access-control.php) system that authenticates and authorizes users from both Linux and Windows clients, making identity-aware exception monitoring a snap.

Meanwhile, the Likewise Data Analytics and Governance application adds a unique high-performance layer that overcomes the performance barriers to event monitoring: a NoSQL database. It digests events with write speeds faster than SQL databases and, more importantly, can cost-effectively scale horizontally to handle more events. When the monitoring system is engineered with performance in mind, it ensures that the system can scale to deliver high-performance exception monitoring in high-traffic environments.

Identity-aware storage coupled with a NoSQL database provides the basis for exception monitoring and reporting.

Exception Monitoring for Storage Security

Exception monitoring is an information-security control that can identify anomalies and indicate when a suspect event is

in progress. When monitoring is integrated with a cross-platform access control system, it has the power to link events with user identities. The Likewise solution provides a highly effective form of exception monitoring that can parse and analyze suspect events at the nexus of user identity, access, and activity.

Exception monitoring helps fulfill both general and specific requirements of compliance regulations. Monitoring can address general requirements, such as the following risk management requirement from HIPAA, by providing a security measure that reduces risks and vulnerabilities:

"Risk management (Required). Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with §164.306(a)."

The Likewise solution also gives you visibility to suspected security incidents so you can begin to mitigate them, which helps fulfill the following requirement from HIPAA:

"Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity; and document security incidents and their outcomes."

Finally, exception monitoring provides audit controls to track and record activity to help comply with the following requirement from HIPAA:

"Standard: Audit controls. Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information."

To meet regulatory requirements such as these, the Likewise solution does the following:

- *Associates suspect security events with identities and organizational roles.
- *Reduces the clutter from millions of file-access events to focus on unusual events -- anomalies that might signal a security incident.
- *Gives you near real-time feedback on your security policies and access events to optimize access, availability, and utilization.
- *Protects sensitive documents by monitoring access and changes to them.
- *Sends you security alerts when specified exceptions occur.
- *Displays exception reports in a browser-based dashboard or on your smart phone.

In addition, the event monitoring system can perform identity-aware [file activity monitoring](/products/likewise_data_analytics_governance_application/file-activity-monitoring.php) to track changes to sensitive content.

The image is a placeholder for a screenshot of the exceptions dashboard, which would show a list of security exceptions and their details.

Exception Reporting for Regulatory Compliance

The second aspect of exception-based management is exception reporting. The Likewise solution provides reports specifically tailored to fulfill the requirements of regulatory

standards. There are predefined templates that generate exception reports for SOX, PCI DSS, FISMA, and HIPAA. You can also create custom exception reports to meet your own requirements.

But the key here is the power of exception [reporting](/solutions/file_server_reporting_features/index.php) to help fulfill some of the most challenging aspects of regulations. Consider this requirement from HIPAA:

"Information system activity review (Required). Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports."

With the Likewise solution, you can create compliance reports to review access to files and to track security incidents.

=====

Conclusion

The return on investment for exception management is immediate: Through monitoring and reports, you can improve security and comply with regulations.

=====

Related

*[Cross-Platform Storage Access Control](/products/likewise_storage_services/cross-platform-storage-access-control.php)

*[Reporting Features for IT Auditing and Compliance](/solutions/file_server_reporting_features/index.php)

*[File Activity Monitoring](/products/likewise_data_analytics_governance_application/file-activity-monitoring.php)

=====

Features

- *Identity-aware exception monitoring of stored files
- *Access reports for HIPAA, PCI DSS, SOX, and FISMA
- *Templates for custom exception reports
- *Historical reports for auditing and forensics
- *Browser-based dashboard works with smart phones