Audit Logging

Audit logging is the process of documenting activity within the software systems used across your organization. Audit logs record the occurrence of an event, the time at which it occurred, the responsible user or service, and the impacted entity. All of the devices in your network, your cloud services, and your applications emit logs that may be used for auditing purposes.

Audit Trail

A series of audit logs is called an audit trail because it shows a sequential record of all the activity on a specific system. By reviewing audit logs and correlated audit trails, systems administrators can track user activity, and security teams can investigate breaches and ensure compliance with regulatory requirements.

What Do Audit Logs and Audit Trails Document?

Audit logs and audit trails document a complete historical record of system actions and activities. They serve as a security measure to monitor and verify system activities, ensure compliance, and aid in troubleshooting and forensic investigations.

Here are some key types of information documented in audit logs and trails:

- User Activity: The actions of individual users, such as the time they logged in or out, the resources they accessed, and the changes they made to data or system settings.
- System Events: Important system-related activities, such as system start-ups or shutdowns, system errors or failures, and security-related events.

- Data Access and Modifications: Any actions related to accessing, creating, viewing, modifying, or deleting data. This helps track how data is being used and by whom.
- Transaction History: Detailed records of all transactions processed by the system, such as financial transactions in a banking system or order placements in an e-commerce platform.
- Security Incidents: Any potential or actual security breaches, failed login attempts, changes to access rights, and activations of virus-detection software.
- Configuration Changes: Any changes made to the system's configuration settings, including software installations, updates, or modifications to network settings.
- Administrative Actions: Actions performed by system administrators, such as user account creation, privilege assignments, system backups, or system restore operations.

What Types of Activity Do Audit Logs Track?

Audit logs can track a variety of system activities. This includes but is not limited to:

- Login and Logout: This includes successful and unsuccessful attempts.
- Access to Sensitive Data: Any attempts to read, modify, copy, or delete sensitive data are tracked.
- Changes in User Permissions: Any changes to system or data access permissions or roles.
- System and Configuration Changes: Any system configurations or settings modifications.
- Network Activities: Information about requests for accessing network resources or alterations in network configuration.
- User Actions: Activities performed by a user in a system such as file editing, system command execution, and data creation.

- Application Activities: Any interactions with software applications like updates/installations, starting/stopping applications, and any modifications made within the application.
- Security Events include any alterations to security policies or control systems, detection of viruses or malware, and firewall function.
- Errors or System Failures: Any application or system errors, crashes, or performance issues.
- Transaction Histories: In systems handling transactions, such as payment gateways or databases, logs of all transactions are maintained.

What to Look For in An Audit Logging Tool(Requirements):

There are several key features and capabilities to look for when choosing an audit logging tool:

- Real-Time Monitoring: A good logging tool should allow for real-time monitoring and the ability to send real-time alerts when certain events of interest occur.
- Easy to Read and Understand: Logs should be easy to read and understand. The tool should organize and present log data in a clear way, perhaps with graphs or charts for easier comprehension.
- Compatibility: The logging tool should be compatible with your current systems. If you use multiple systems, it is important that the tool is able to integrate with all of them.
- Scalability: The tool should be able to handle large volumes of log data and scale accordingly as your business grows.
- Log Management: Log management capabilities, including collecting, storing, and analyzing logs, are important. A suitable tool would retain logs for an appropriate amount of time per an organization's regulation requirement.

- Security Features: Look for tools that provide encryption and secure log access. The tool itself should also be protected from vulnerabilities.
- Compliance: Consider whether the tool helps you comply with relevant industry standards or regulations (e.g., GDPR, HIPAA, PCI DSS).
- Automated Analysis: A good logging tool can automatically analyze log data and generate reports based on the analysis.
- Easy to Use: The logging tool should be easy to use, with a user-friendly interface and straightforward set-up process.
- Customizability: The ability to customize the tool to your specific needs is beneficial. This can include creating custom alerts or reports.
- Cost: Evaluate the pricing structure of the tool, considering your budget and the return on investment it offers.
- Support: Check if the software vendor provides reliable support if you need help with setup, troubleshooting, or queries.