Residência em Software

Módulo Programação JAVA (Avançado)

MÊS 02

INSTITUIÇÃO EXECUTORA

cepedi UESC

COORDENADORA

MCTI FUTURO Softex

APOIO

MINISTÉRIO DA CIÊNCIA, TECNOLOGIA E INOVAÇÃO

GOVERNO FEDERAL BRASIL UNIÃO E RECONSTRUÇÃO

Trilha de Auditoria - **Monitoramento da atividade do usuário (UAM)**

O que é uma Trilha de Auditoria?

Uma série de registros sequenciais de toda a atividade em um sistema específico. Esses registros são chamados de logs de auditoria.

Basicamente, os logs de auditoria, respondem a uma pergunta simples: **quem fez o quê, onde e quando?**

Ao revisar logs e trilhas de auditoria correlacionadas, os administradores de sistemas podem **rastrear a atividade do usuário** e as equipes de segurança podem **investigar violações** e garantir a conformidade com os requisitos normativos.

Trilha de Auditoria - **Monitoramento da atividade do usuário (UAM)**

O que as trilhas de auditoria documentam?

1. **Identificação e Descrição do Evento:**
   Nome do Evento: Conforme identificado no sistema.
   Descrição do Evento: Explicação clara e compreensível da funcionalidade requisitada.
2. **Detalhes Temporais e de Localização:**
   Carimbo de Data/Hora: Data e hora exatas do evento.
   Localização: Inclui dados do protocolo TCP/IP e outras informações geográficas relevantes.
3. **Autor e Objeto Afetado:**
   Ator do Evento: Quem acessou, criou, editou ou excluiu o evento (ID do usuário ou ID da API).
   Objeto Impactado: Aplicativo, dispositivo, sistema ou objeto (endereço IP, ID do dispositivo, etc.).

Trilha de Auditoria - **Monitoramento da atividade do usuário (UAM)**

O que as trilhas de auditoria documentam?

4. **Origem do Acesso e Ações:**
   Origem: País, nome do host, endereço IP, ID do dispositivo, etc.
   Ações Registradas: Tipos de ação, alterações de conta, alterações em todo o sistema e mudanças no estado das informações.
5. **Métricas e Segurança:**
   Métricas Predefinidas: Métricas específicas monitoradas.
   Segurança: Acesso a dados, tentativas de login, falhas e informações de autenticação.
6. **Detalhes Adicionais:**
   Marcas Personalizadas: Tags especificadas pelo usuário, como nível de severidade do evento.
   Detalhes de Erros: Informações sobre quaisquer erros ocorridos.
   Detalhes de Transação: Informações específicas sobre transações realizadas.

Trilha de Auditoria - **Monitoramento da atividade do usuário (UAM)**

Casos de uso para logs de auditoria

O log de auditoria pode ter quatro domínios principais em sua aplicação:

- Segurança
- Conformidade
- Responsabilidade
- Perícia cibernética

Casos de uso para logs de auditoria - Segurança

Objetivo: Identificar comportamentos anômalos e padrões de tráfego de rede.
Métodos: Integração com soluções de monitoramento e observabilidade para extrair insights e detectar alterações de rede não autorizadas mediante políticas de segurança predefinidas.

Casos de uso para logs de auditoria - Legislação e Compliance

Objetivo: Cumprimento de regulamentos externos.
Métodos: Manutenção de logs específicos e estabelecimento de monitoramento em tempo real, visando atender a requisitos de normas como ISO 27001.

Casos de uso para logs de auditoria - Responsabilidade e Autenticação

Objetivo: Garantir a prestação de contas e a verificação de informações factuais.
Aplicações Comuns: Políticas organizacionais, contabilidade e finanças, políticas de RH.
Métodos: Análise do desempenho de usuários em ações financeiras e comparação com orçamentos.

Casos de uso para logs de auditoria - Perícia Cibernética

Objetivo: Reconstituição de eventos e obtenção de insights em processos tecnológicos para provas legais.
Contexto: Necessário principalmente em resposta a intimações judiciais ou grandes incidentes cibernéticos.
Métodos: Análise detalhada de logs para descrever sequências de ação e fornecer insights profundos sobre eventos representados.

Práticas Recomendadas para Gestão de Logs de Auditoria

1. Transparência no Monitoramento:

Importância: Informar claramente os usuários sobre as práticas de monitoramento. Isso pode ser comunicado por meio de políticas, termos e condições, ou acordos contratuais.
Objetivo: Garantir que todos os envolvidos estejam cientes e concordem com as práticas antes de suas atividades serem monitoradas.

Práticas Recomendadas para Gestão de Logs de Auditoria

2. Anonimização de Dados:

Técnicas: Utilize a tokenização ou hashes para desassociar as ações do usuário de suas identidades pessoais sempre que possível.
Vantagem: Protege a privacidade do usuário enquanto permite a análise de comportamento.

Práticas Recomendadas para Gestão de Logs de Auditoria

3. Acesso Restrito aos Dados:

Quem Deve Acessar: Limitar o acesso a dados de monitoramento apenas a posições autorizadas, como analistas de dados e profissionais de segurança cibernética.
Motivo: Minimiza o risco de vazamento ou uso indevido de dados sensíveis.

Práticas Recomendadas para Gestão de Logs de Auditoria

4. Políticas de Proteção de Dados Robustas:

Conteúdo: Desenvolva políticas claras que detalhem as práticas de monitoramento, o uso aceitável de dados e as medidas de segurança adotadas.
Impacto: Assegura que todos na organização entendam suas responsabilidades e os procedimentos para manuseio de dados.

Práticas Recomendadas para Gestão de Logs de Auditoria

5. Cuidados com Provedores Terceirizados:

Obrigações: Verifique se os provedores externos que oferecem ferramentas de monitoramento estão conforme os regulamentos de proteção de dados.
Benefício: Protege a organização contra riscos legais e reputacionais associados a falhas de conformidade dos parceiros.

Trilha de Auditoria - **Monitoramento da atividade do usuário (UAM)**

Recapitulando...

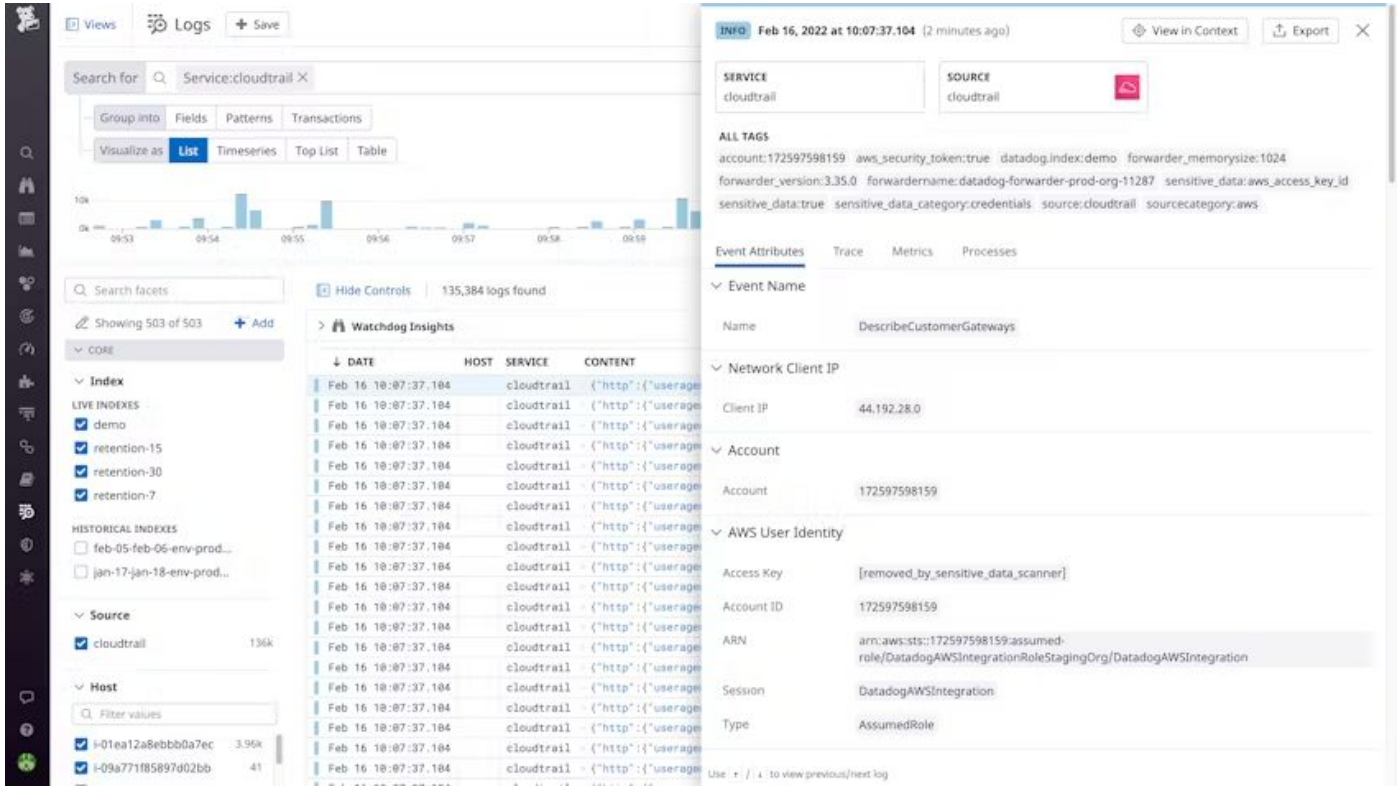
A trilha de auditoria é essencial para a segurança organizacional, fornecendo uma ferramenta robusta para monitorar e registrar atividades suspeitas que possam indicar fraudes ou a ação de clientes de alto risco.

Ela permite distinguir entre ações de usuários reais e comportamentos automatizados, como os de bots, e é fundamental na elaboração de Relatórios de Atividade Suspeita (SAR), que documentam evidências de atividades ilícitas para reguladores ou autoridades policiais.

Além disso, a análise dessas trilhas ajuda a identificar padrões de comportamento malicioso, tanto internos quanto externos, reforçando a segurança e ajudando a prevenir ameaças à integridade da empresa e de seus clientes.

Residência em Software

Trilha de Auditoria - **Monitoramento da atividade do usuário (UAM)**



Exemplo de implementação usando Spring Boot

Implementação em Comum (Componentes que são comuns a ambas as implementações).

1. Dependências do Maven
Adicione as seguintes dependências ao seu arquivo pom.xml
https://gist.github.com/rog3r/9dd57516fcac33a16be1c7e3711dfb04

2. Entity AuditLog
Crie uma entidade AuditLog para armazenar registros de auditoria:
https://gist.github.com/rog3r/03a679585b8f4dbc9cb8cd7e36d73800
https://gist.github.com/rog3r/6beee3e213e181e1abeba40db99378cf //teste

Exemplo de implementação usando Spring Boot

Implementação em Comum (Componentes que são comuns a ambas as implementações).

3. Repositório AuditLogRepository
Crie um repositório para a entidade AuditLog:
https://gist.github.com/rog3r/6ddc13ab987bcc87a56b2c72ec00255a

4. Serviço AuditService
Implemente o serviço para registrar eventos de auditoria:
https://gist.github.com/rog3r/5774e1c6a1972a1751b0702f7e564a41

Exemplo de implementação usando Spring Boot

Implementação Usando AuditInterceptor

1. Definindo o AuditInterceptor

Crie um interceptor que capta informações de cada requisição HTTP:
https://gist.github.com/rog3r/9e3ac8a1736e808278046be494789da4

2. Registrar o Interceptor

Adicione o interceptor ao registro global de interceptores no Spring MVC:
https://gist.github.com/rog3r/604d7f5d717233e5aa139e1abf68e8eb

Exemplo de implementação usando Spring Boot

Implementação Usando LoggingAspect (AOP)

1. Definindo o LoggingAspect

Configure um aspecto para interceptar chamadas de método nos serviços:
https://gist.github.com/rog3r/112289b6c5cae1231af2c1285e2be4e7

2. Configurações Adicionais

WebConfig deve ser adaptado para interceptar a captura do IP da requisição, apenas.
Nenhuma configuração adicional é necessária para o aspecto, uma vez que ele é automaticamente registrado pelo Spring Boot quando o **@Aspect** é usado e o componente é detectado via **@Component**.

Residência em Software

Contato

rogerio.jesus@cepedi.org.br

https://moodle.residenciatic18.cepedi.org.br/