Log de Auditoria

O log de auditoria grava informações de eventos ocorridos em um sistema, gerando um histórico das alterações. Através desse histórico é possível auditar detalhadamente as mudanças ocorridas no sistema, obtendo informações do que foi alterado, quem o fez, quando ocorreu e outros detalhes. O Cronapp fornece essa funcionalidade para eventos que ocorram nas entidades, usando fontes de dados ou blocos de programação servidor, facilitando a análise de problemas como segurança ou erros do sistema.

A auditoria ocorre na camada de dados, então, ao utilizar serviços REST com as entidades através de fonte de dados ou blocos de programação, esses também serão registrados.

Nesta página

Habilitar log

Para gerar log, basta habilitar a caixa de seleção **auditoria em log** nas classes do diagrama de dados, bloco de programação ou fonte de dados.

Entidade

Há duas formas de habilitar os logs para uma entidade no Diagrama de dados. A primeira é pela caixa de checagem **Auditoria em Log** que se encontra na janela de configurações da entidade (destaque 1 da Figura 1). Por padrão, esse campo vem desabilitado.

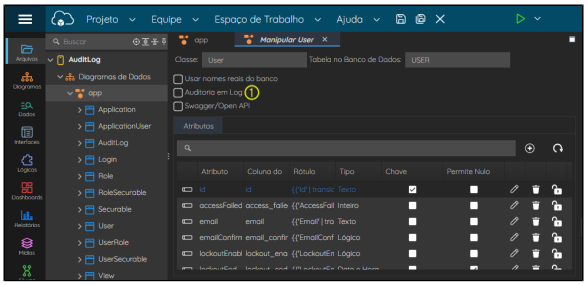

Figura 1 - Habilitar Auditoria em Log para entidade pela janela

O segundo modo é através da caixa de checagem **Audit** na aba **propriedades e eventos** (destaque 1 da Figura 1.1), no menu lateral do diagrama. O campo é mostrado quando a classe é selecionada.

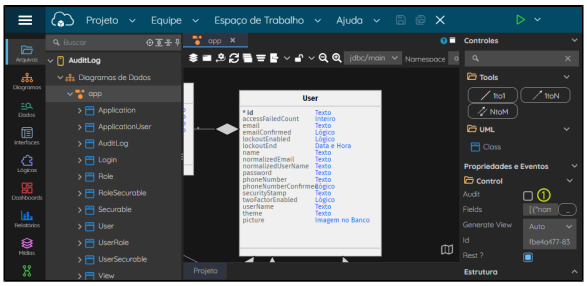

Figura 1.1 - Habilitar Auditoria em Log para entidade pela aba

Fonte de dados

Para gerar log de uma Fonte de dados, marque a caixa de checagem **Auditoria em Log** (destaque 1 da Figura 1.2) nas configurações da Fonte de dados.

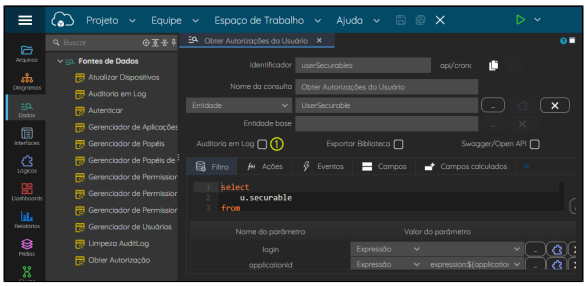

Figura 1.2 - Habilitar Auditoria em Log para fonte de dados

Bloco de programação

Para os blocos de programação servidor, a opção encontra-se na janela de configuração do mesmo (destaque 1 da Figura 1.3).

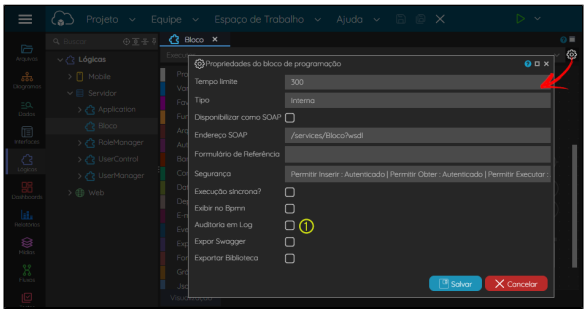

Figura 1.3 - Habilitar auditoria em log para bloco de programação

Duração do log de auditoria

Nas Configurações do projeto é possível definir o tempo no qual será mantido o log de auditoria, como mostrado abaixo (Figura 1.4).

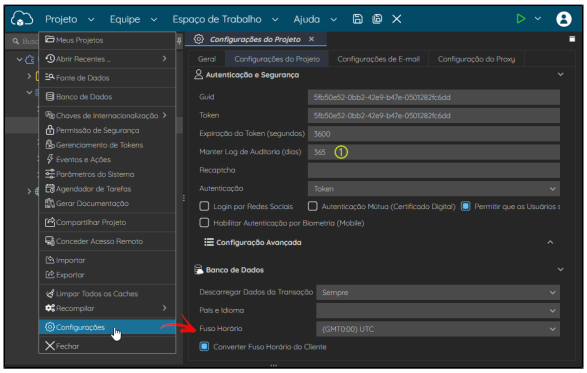

Figura 1.4 - Duração do armazenamento dos logs de auditoria

1. **Manter Log de Auditoria (dias):** define o tempo que os dados da auditoria em log ficarão salvos no banco de dados (tabela `AUDIT_LOG`).

Local de armazenamento

Todas as alterações ocorridas na Entidade, seja por blocos, Fontes de dados ou da própria entidades, são salvas na tabela `AUDIT_LOG` (Classe `AuditLog`) através a Fonte de Dados **Auditoria em Log**. Esse processo ocorre de forma automática quando a opção Auditoria em Log for habilitado em um bloco de programação, Fonte de dados ou entidade.

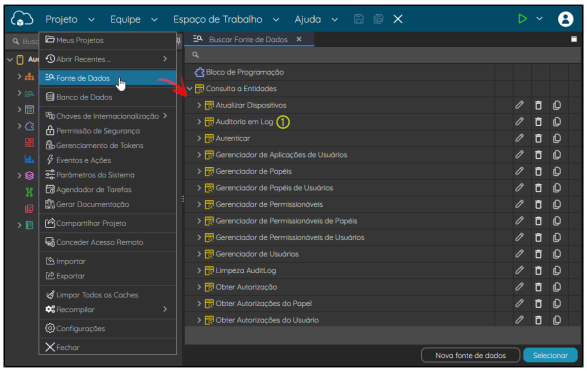

Figura 2 - Classe AuditLog e a fonte de dados responsável pela auditoria

Veja abaixo o significado de cada atributo da classe `AuditLog`.

- **id:** identificador numérico do log.
- **type**: qual recurso foi auditado. Ex: app.entity.Entity, blocky.CalculaFolha.
- **command**: qual comando foi utilizado. Ex: UPDATE, DELETE.
- **date**: a data em que ocorreu o evento.
- **objectData**: qual objeto foi modificado.
- **user**: informação do usuário que realizou a modificação.
- **host**: o endereço IP do usuário que realizou a modificação.
- **agent**: qual navegador utilizado para realizar a modificação.
- **server**: endereço IP privado do servidor que gerou o registro.
- **affectedFields**: quais campos foram modificados.
- **category**: informação de qual categoria do log ocorreu a modificação. Ex: Entity, Blockly ou DataSource.
- **application**: hash do nome da aplicação.
- **error**: indica se ocorreu um erro durante uma operação ou ação específica.

Página de auditoria

As informações do log podem ser visualizadas na página Log de Auditoria do sistema para os usuários que tiverem permissão de administrador (Figura 2.1)

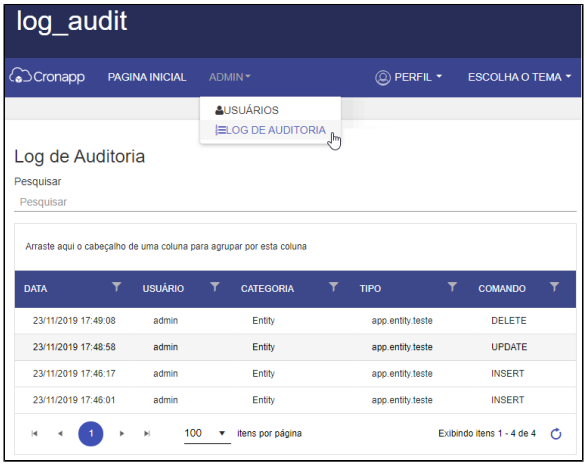

Figura 2.1 - Página de auditoria do sistema

Para visualizar mais informações sobre uma determinada ação, clique na coluna "Detalhe" em uma das linhas da grade para abrir o modal (Figura 2.2),

Figura 2.2 - Selecione uma linha na grade para ver os detalhes da ação