Administrador de Banco de Dados (extra Abril) - Turma 2024A

5.3 Controle de acesso e permissões

O controle de acesso e permissões é um aspecto crítico do gerenciamento de banco de dados, uma vez que garante que apenas usuários autorizados tenham acesso aos dados armazenados. O controle de acesso é a capacidade de restringir o acesso de usuários a determinados recursos, enquanto as permissões definem quais ações os usuários podem executar em relação a esses recursos.

O controle de acesso pode ser implementado em vários níveis, desde a autenticação do usuário até a autorização para executar determinadas tarefas. Por exemplo, para acessar um banco de dados, um usuário precisa primeiro autenticar sua identidade, fornecendo um nome de usuário e uma senha válidos. Se a autenticação for bem-sucedida, o usuário é então autorizado a acessar o banco de dados, mas suas ações dentro do banco de dados são limitadas pelas permissões concedidas pelo administrador de banco de dados (DBA).

As permissões são geralmente definidas em um nível granular, ou seja, para cada recurso ou objeto no banco de dados. Por exemplo, um DBA pode conceder a um usuário a permissão de somente leitura em uma tabela específica, ou a permissão de atualização em outra tabela diferente. As permissões também podem ser aplicadas a procedimentos armazenados, visualizações e outras entidades no banco de dados.

O controle de acesso e permissões também pode ser aplicado em nível de campo, o que significa que o acesso a campos específicos em uma tabela pode ser restringido a usuários específicos. Isso pode ser especialmente importante para dados confidenciais ou sensíveis, como informações pessoais ou financeiras.

A implementação adequada de controles de acesso e permissões é fundamental para garantir a integridade e a segurança dos dados armazenados em um banco de dados. Um DBA competente deve avaliar cuidadosamente as necessidades de acesso de cada usuário e definir as permissões de acordo com as políticas de segurança e regulamentações aplicáveis. O DBA deve também monitorar regularmente o uso do banco de dados, identificando quaisquer atividades suspeitas ou não autorizadas.

PostgreSQL

No PostgreSQL, o controle de acesso e permissões é feito por meio de regras e funções de acesso, que determinam quais usuários têm acesso a determinados objetos (como tabelas, visualizações, funções etc.) e quais tipos de operações podem ser realizadas nesses objetos.

Para conceder permissões a um usuário específico, você pode usar o comando GRANT, seguido da lista de permissões que você deseja conceder e o nome do objeto a ser afetado (como uma tabela ou uma função). Por exemplo, para conceder permissão para SELECT em uma tabela específica para um usuário:

```
GRANT SELECT ON nome_da_tabela TO nome_do_usuario;
```

Para revogar uma permissão de um usuário, use o comando REVOKE, seguido da lista de permissões que você deseja revogar e o nome do objeto afetado. Por exemplo, para revogar a permissão de SELECT em uma tabela específica para um usuário:

```
REVOKE SELECT ON nome_da_tabela FROM nome_do_usuario;
```

Além disso, é possível definir outras opções de configuração de permissões, como o tempo máximo de inatividade, as restrições de conexão e as configurações de criptografia.

Também é possível usar o conceito de "papéis" no PostgreSQL, que são conjuntos de permissões que podem ser atribuídos a usuários ou grupos de usuários. Para criar um papel, use o comando CREATE ROLE, seguido do nome do papel e as permissões que você deseja conceder. Por exemplo:

```
CREATE ROLE nome_do_papel LOGIN PASSWORD 'senha_do_papel';
GRANT SELECT ON nome_da_tabela TO nome_do_papel;
```

Em seguida, você pode atribuir esse papel a um usuário específico usando o comando ALTER USER. Por exemplo:

```
ALTER USER nome_do_usuario SET ROLE nome_do_papel;
```

Dessa forma, todas as permissões concedidas ao papel serão aplicadas ao usuário.

MySQL

No MySQL, o controle de acesso e permissões é feito por meio de concessão de privilégios aos usuários, que determinam quais usuários têm acesso a determinados objetos (como tabelas, visualizações, procedimentos armazenados etc.) e quais tipos de operações podem ser realizadas nesses objetos.

Para conceder privilégios a um usuário específico, você pode usar o comando GRANT, seguido da lista de privilégios que você deseja conceder e o nome do objeto a ser afetado (como uma tabela ou uma função). Por exemplo, para conceder permissão para SELECT em uma tabela específica para um usuário:

```
GRANT SELECT ON nome_da_tabela TO nome_do_usuario@'localhost' IDENTIFIED BY 'senha_do_usuario';
```

Para revogar um privilégio de um usuário, use o comando REVOKE, seguido da lista de privilégios que você deseja revogar e o nome do objeto afetado. Por exemplo, para revogar a permissão de SELECT em uma tabela específica para um usuário:

```
REVOKE SELECT ON nome_da_tabela FROM nome_do_usuario@'localhost';
```

Além disso, é possível definir outras opções de configuração de privilégios, como o tempo máximo de inatividade, as restrições de conexão e as configurações de criptografia.

Também é possível usar o conceito de "papéis" no MySQL, que são conjuntos de privilégios que podem ser atribuídos a usuários ou grupos de usuários. Para criar um papel, use o comando CREATE ROLE, seguido do nome do papel e as permissões que você deseja conceder. Por exemplo:

```
CREATE ROLE nome_do_papel;
GRANT SELECT ON nome_da_tabela TO nome_do_papel;
```

Em seguida, você pode atribuir esse papel a um usuário específico usando o comando GRANT. Por exemplo:

```
GRANT nome_do_papel TO nome_do_usuario@'localhost' IDENTIFIED BY 'senha_do_usuario';
```

Dessa forma, todas as permissões concedidas ao papel serão aplicadas ao usuário.

Última atualização: terça, 21 mar 2023, 13:06

◄ 5.2 Criação e gerenciamento de usuários

Seguir para...

5.4 Autenticação e criptografia ►