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

5.4 Autenticação e criptografia

A autenticação e criptografia são medidas fundamentais de segurança em um banco de dados, que garantem que apenas usuários autorizados possam acessar os dados e que as informações armazenadas estejam protegidas contra acesso não autorizado ou interceptação.

A autenticação é o processo de verificar a identidade de um usuário que está tentando acessar o banco de dados. Isso envolve a solicitação de credenciais de autenticação, como nome de usuário e senha, e a validação dessas credenciais pelo sistema de autenticação. O objetivo da autenticação é garantir que apenas usuários autorizados possam acessar o banco de dados e que a autenticação seja realizada de forma segura e confiável.

A criptografia, por sua vez, é o processo de transformar informações em um formato ilegível para quem não tem acesso à chave de criptografia. A criptografia é usada para proteger informações confidenciais, como senhas de usuário, informações de cartão de crédito e outras informações sensíveis. Ao criptografar as informações, mesmo que alguém intercepte os dados, não será capaz de acessá-los sem a chave de criptografia.

A autenticação e criptografia são frequentemente usadas em conjunto em bancos de dados para proteger as informações armazenadas. A autenticação é usada para verificar a identidade do usuário, enquanto a criptografia é usada para proteger as informações que são transmitidas ou armazenadas no banco de dados.

Um DBA competente deve avaliar cuidadosamente as necessidades de autenticação e criptografia para o banco de dados, garantindo que as medidas de segurança sejam apropriadas para os tipos de dados armazenados. Além disso, é importante que as chaves de criptografia sejam gerenciadas de forma segura e que os usuários sejam orientados a escolher senhas seguras.

A autenticação e criptografia no PostgreSQL e no MySQL podem ser implementadas de maneira semelhante. Ambos os sistemas de gerenciamento de banco de dados suportam vários métodos de autenticação e criptografia, incluindo o uso de SSL/TLS e o uso de senhas criptografadas.

No PostgreSQL, é possível configurar a autenticação e criptografia por meio do arquivo postgresql.conf e do arquivo pg_hba.conf. O arquivo postgresql.conf contém as configurações gerais do PostgreSQL, incluindo a configuração de SSL/TLS. O arquivo pg_hba.conf contém as regras de autenticação de host-based, que definem como os clientes se conectam ao servidor PostgreSQL.

Para configurar a autenticação com senhas criptografadas no PostgreSQL, é necessário definir uma senha criptografada para cada usuário. Isso pode ser feito usando o comando ALTER USER seguido do nome do usuário e da nova senha criptografada. Por exemplo:

```
ALTER USER nome_do_usuario WITH PASSWORD 'senha_criptografada';
```

No MySQL, a autenticação e criptografia também podem ser configuradas por meio do arquivo de configuração do servidor, que geralmente é chamado de my.cnf. Para configurar a autenticação com senhas criptografadas no MySQL, é necessário definir uma senha criptografada para cada usuário. Isso pode ser feito usando o comando SET PASSWORD seguido do nome do usuário e da nova senha criptografada. Por exemplo:

```
SET PASSWORD FOR nome_do_usuario = 'senha_criptografada';
```

Além disso, é possível configurar o uso de SSL/TLS para criptografar as conexões entre o cliente e o servidor no MySQL. Isso pode ser feito definindo as opções de configuração appropriate, tais como "ssl-ca", "ssl-cert" e "ssl-key".

É importante lembrar que é recomendável usar senhas fortes e criptografadas para a autenticação e também implementar o SSL/TLS para garantir a segurança das conexões.

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

◄ 5.3 Controle de acesso e permissões

Seguir para...

5.5 Configuração de segurança e acesso ao banco de dados ►