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

5.5 Configuração de segurança e acesso ao banco de dados

A configuração de segurança e acesso ao banco de dados é um aspecto crítico do gerenciamento de bancos de dados, pois garante a integridade, a confidencialidade e a disponibilidade dos dados armazenados. Essa configuração inclui a definição de permissões, controles de acesso e outras medidas de segurança para garantir que somente usuários autorizados tenham acesso aos dados.

Uma das primeiras medidas de segurança que um administrador de banco de dados (DBA) deve tomar é garantir que o banco de dados esteja instalado e configurado corretamente, com todas as atualizações de segurança e patches aplicados. O DBA deve garantir que as configurações padrão do banco de dados estejam configuradas de maneira segura e que as contas de usuário padrão tenham as permissões adequadas.

O DBA também deve garantir que as permissões de usuário sejam definidas de acordo com as políticas de segurança da organização e que as contas de usuário sejam criadas somente para usuários autorizados. Isso envolve a criação de senhas fortes, a configuração de políticas de senha e a aplicação de restrições de login, como limites de tempo ou endereço IP.

Além disso, o DBA deve monitorar regularmente as atividades do usuário, verificando as tentativas de login e as permissões concedidas aos usuários. Isso pode ajudar a identificar quaisquer tentativas de acesso não autorizadas ou atividades suspeitas.

O DBA também deve garantir que os backups do banco de dados estejam configurados corretamente e que exista um plano de recuperação de desastres em vigor. Isso pode incluir a configuração de backups regulares, armazenando cópias dos backups em um local seguro e testando regularmente o plano de recuperação de desastres para garantir que ele seja eficaz.

Outra medida importante de segurança é a criptografia, que pode ser usada para proteger as informações armazenadas e transmitidas pelo banco de dados. O DBA deve garantir que a criptografia esteja ativada e configurada corretamente para garantir que as informações sejam protegidas.

Algumas medidas de segurança e acesso que podem ser implementadas no PostgreSQL e no MySQL:

1. Usuários e permissões: Configure usuários e permissões de acesso ao banco de dados, limitando o acesso apenas aos usuários autorizados e concedendo apenas as permissões necessárias para realizar suas tarefas. Use senhas fortes e criptografadas para garantir a segurança das contas de usuário.
2. Firewall: Configure o firewall para permitir apenas o tráfego de rede necessário para o funcionamento do banco de dados. Bloqueie todas as outras conexões de entrada e saída que não são necessárias.
3. SSL/TLS: Configure o SSL/TLS para criptografar as conexões entre o cliente e o servidor, garantindo que as informações transmitidas sejam protegidas contra interceptação.
4. Backups: Realize backups regularmente para garantir que, em caso de falhas de hardware ou software, os dados possam ser recuperados com facilidade. Armazene os backups em locais seguros e protegidos contra acesso não autorizado.
5. Monitoramento e registro: Configure o sistema de monitoramento e registro do banco de dados para detectar atividades suspeitas e violações de segurança, permitindo que medidas preventivas sejam tomadas rapidamente.

Última atualização: terça, 21 mar 2023, 13:26

◄ 5.4 Autenticação e criptografia

Seguir para...

5.6 Teste seus conhecimentos ►