DES11 – Administração de Banco de Dados – QUESTÕES PARA FIXAÇÃO

|  |  |  |
| --- | --- | --- |
| Módulo | | 04 |
| Questão | | **01** |
| Finalidade | | **Fixação** |
| **Enunciado** | | **Sobre criação de ROLES qual das afirmações abaixo é FALSA?** |
| Resposta 01 |  | A role com atributo LOGIN pode conectar-se ao PostgreSQL |
| Feedback 01 |  | **Errado.** Esta é uma afirmação verdadeira, é necessário possuir o atributo LOGIN senão a role é tratada como um grupo e não pode conectar. |
| Resposta 02 |  | Um atributo CREATEROLE garante a role privilégio de criar outras |
| Feedback 02 |  | **Errado.** Esta é uma afirmação verdadeira, usuários ou grupos que possuem CREATEROLE podem criar outros usuários e grupos. |
| Resposta 03 |  | A opção VALID UNTIL define uma data de expiração para a role |
| Feedback 03 |  | **Errado.** Esta é uma afirmação verdadeira. |
| Resposta 04 | X | Somente o usuário postgres é um superusuário, não há forma de criar outro |
| Feedback 04 |  | **Correto.** Esta afirmação é falsa, o atributo SUPERUSER quando criando um usuário fornece à role o privilégio de superusuário. Roles com essa opção não  precisam ter nenhum outro privilégio. |

|  |  |  |
| --- | --- | --- |
| Módulo | | 04 |
| Questão | | **02** |
| Finalidade | | **Fixação** |
| **Enunciado** | | **Sobre exclusão de ROLES qual das afirmações abaixo é VERDADEIRA?** |
| Resposta 01 |  | DROP ROLE excluirá a role e todos os objetos que ela possui |
| Feedback 01 |  | **Errado.** Para uma role ser removida, ela não pode ter nenhum privilégio ou ser dona de objetos ou bases. Se houver, ou os objetos deverão ser excluídos previamente ou devemos revogar os privilégios e alterar os donos. |
| Resposta 02 |  | Usa-se DROP OWNED para alterar o dono de objetos |
| Feedback 02 |  | **Errado.** Este comando é usado para remover todos os objetos de uma role. |
| Resposta 03 | X | DROP OWNED BY remove privilégios e objetos que determinada role possui. Com CASCADE pode remover objetos que não pertencem a role. |
| Feedback 03 |  | **Correto.** Comando bastante poderoso e perigoso, remove todos os objetos (tabelas, views, funções,…) de uma role e com o uso de CASCADE pode remover objetos dependentes que pertencem a outros usuários. |
| Resposta 04 |  | REASSIGN OWNED BY remove objetos que pertencem a role. |
| Feedback 04 |  | **Errado.** Este comando é usado para trocar a role dona de objetos |

|  |  |  |
| --- | --- | --- |
| Módulo | | 04 |
| Questão | | **03** |
| Finalidade | | **Fixação** |
| **Enunciado** | | **Qual das opções abaixo NÃO é um privilégio em Bases de Dados?** |
| Resposta 01 | X | USAGE |
| Feedback 01 |  | **Correto.** Este é um privilégio para outros tipos de objetos, mas não para uma base de dados. |
| Resposta 02 |  | CREATE |
| Feedback 02 |  | **Errado.** Este privilégio permite à role criar schemas na base. |
| Resposta 03 |  | CONNECT |
| Feedback 03 |  | **Errado.** Este privilégio permite à role conectar-se à base. |
| Resposta 04 |  | TEMP |
| Feedback 04 |  | **Errado.** Este privilégio permite à role criar tabelas temporárias na base. |

|  |  |  |
| --- | --- | --- |
| Módulo | | 04 |
| Questão | | **04** |
| Finalidade | | **Fixação** |
| **Enunciado** | | **Qual das opções abaixo de configuração no arquivo pg\_hba.conf permitem que todos os usuários do grupo contabilidade, conectem sem senha, a partir de um único servidor na base contábil?** |
| Resposta 01 |  | host contabil +contabilidade 172.22.3.0/24 trust |
| Feedback 01 |  | **Errado.** O endereço indicado é para uma rede IPv4. |
| Resposta 02 |  | host contabil +contabilidade 172.22.3.0/24 md5 |
| Feedback 02 |  | **Errado.** O método MD5 exige autenticação com senha e está permitindo uma rede completa 172.22.3.\* |
| Resposta 03 |  | host contabil contabilidade 172.22.3.45/32 md5 |
| Feedback 03 |  | **Errado.** O método MD5 indicado exige autenticação com senha e não está permitindo um grupo pela ausência do ”+” |
| Resposta 04 | X | host contabil +contabilidade 172.22.3.45/32 trust |
| Feedback 04 |  | **Correto.** O “+” indica que contabilidade é um grupo, o “/32” indica um endereço e não uma rede e o “trust” indica não necessidade de senha |

|  |  |  |
| --- | --- | --- |
| Módulo | | 04 |
| Questão | | **05** |
| Finalidade | | **Fixação** |
| **Enunciado** | | **Sobre o recurso RLS - Row Security Level, ou Permissão por Registros, qual das afirmações abaixo é VERDADEIRA?** |
| Resposta 01 |  | O superusuário também é afetado pelo controle de Permissões por Registros |
| Feedback 01 |  | **Errado.** Superusuários não passam por nenhum controle de permissão |
| Resposta 02 | X | Para evitar problemas durante o dump quando a Permissão por Registros estiver ligada, deve-se usar o superusuario ou um usuário com o atributo BYPASSRLS para executar o backup |
| Feedback 02 |  | **Correto.** Como o RLS pode ocultar registros de forma silenciosa, sem gerar erros ou warnings, quando utilizando-o é necessário cuidado com o backup. |
| Resposta 03 |  | O owner da tabela também é afetado pelo controle de Permissões por Registros |
| Feedback 03 |  | **Errado.** O proprietário da tabela não é afetado por políticas RLS |
| Resposta 04 |  | Quando um usuário não possui permissão a um registro um erro é gerado |
| Feedback 04 |  | **Errado.** A segurança por registro não dispara erros. Os registros são apenas omitidos se as condições da policy não forem atendidas. |

|  |  |  |
| --- | --- | --- |
| Módulo | | 04 |
| Questão | | **06** |
| Finalidade | | **Fixação** |
| **Enunciado** | | **Dada a seguinte instrução:**  **GRANT SELECT, INSERT ON geral.contas TO moliveira WITH GRANT OPTION;**  **Qual dos seguintes comandos a role moliveira pode executar:** |
| Resposta 01 | X | GRANT ALL ON geral.contas TO jsilva; |
| Feedback 01 |  | **Correto.** Ela pode repassar as permissões que possui, SELECT e INSERT, usando ALL estes dois privilégios serão repassados. |
| Resposta 02 |  | GRANT UPDATE ON geral.contas to jsilva; |
| Feedback 02 |  | **Errado.** A role moliveira não possui o privilégio UPDATE, logo não pode repassá-lo |
| Resposta 03 |  | GRANT DELETE ON geral.contas to jsilva; |
| Feedback 03 |  | **Errado.** A role moliveira não possui o privilégio DELETE, logo não pode repassá-lo |
| Resposta 04 |  | GRANT REFERENCES ON geral.contas to jsilva; |
| Feedback 04 |  | **Errado.** A role moliveira não possui o privilégio REFERENCES, logo não pode repassá-lo |

|  |  |  |
| --- | --- | --- |
| Módulo | | 04 |
| Questão | | **07** |
| Finalidade | | **Fixação** |
| **Enunciado** | | **Qual das seguintes cláusulas NÃO está correta sobre privilégios em Tabelas:** |
| Resposta 01 |  | GRANT UPDATE (descricao) ON geral.balanco TO psouza; |
| Feedback 01 |  | **Errado.** A sintaxe está correta, fornece permissão de atualização na coluna descricao da tabela geral.balanco |
| Resposta 02 |  | GRANT SELECT, INSERT, UPDATE, DELETE, TRIGGER, REFERENCES, TRUNCATE ON geral.balanco TO psouza; |
| Feedback 02 |  | **Errado.** O comando está correto, todos estes privilégios são válidos para uma tabela |
| Resposta 03 | X | GRANT TRUNCATE (descricao) ON geral.balanco TO psouza; |
| Feedback 03 |  | **Correto.** Sintaxe inválida para o privilégio TRUNCATE, não é possível truncar apenas uma coluna |
| Resposta 04 |  | GRANT REFERENCES ON geral.balanco TO psouza, jsilva, moliveira; |
| Feedback 04 |  | **Errado.** Cláusula correta, REFERENCES é um privilégio válido e é possível informar várias roles ao mesmo tempo |

|  |  |  |
| --- | --- | --- |
| Módulo | | 04 |
| Questão | | **08** |
| Finalidade | | **Fixação** |
| **Enunciado** | | **Sobre privilégios em objetos em geral, qual seguinte afirmação é verdadeira:** |
| Resposta 01 |  | Visões não podem receber GRANT de INSERT e UPDATE |
| Feedback 01 |  | **Errado.** Afirmação verdadeira, apesar de parecer estranho à primeira vista, é possível uma visão receber insert ou update caso ela seja derivada de apenas uma tabela. Sendo que a operação existe, é possível fornecer o privilégio. |
| Resposta 02 |  | Com GRANT USAGE a role não pode alterar o valor da sequência |
| Feedback 02 |  | **Errado.** O privilégio USAGE possibilita a execução da função nextval, que incrementa e retorna o valor da sequence. |
| Resposta 03 |  | Não é necessário informar a função com a definição de parâmetros durante o GRANT |
| Feedback 03 |  | **Errado.** Quando usando o GRANT com funções, é necessário informar a assinatura completa da função, com parâmetros. Por exemplo: GRANT EXECUTE ON FUNCTION f\_calculo(int, int) TO jsilva |
| Resposta 04 | X | É possível utilizar a sintaxe ALL … IN SCHEMA com tabelas, visões e sequências |
| Feedback 04 |  | **Errado. Correto, para fornecer permissão em todos os objetos de determinado tipo em um schema usa-se ALL VIEWS, ALL FUNCTIONS e ALL [TABLES] IN SCHEMA** |

|  |  |  |
| --- | --- | --- |
| Módulo | | 04 |
| Questão | | **09** |
| Finalidade | | **Fixação** |
| **Enunciado** | | **Sobre privilégios em objetos em geral, qual seguinte afirmação é verdadeira:** |
| Resposta 01 |  | Visões não podem receber GRANT de INSERT e UPDATE |
| Feedback 01 |  | **Errado.** Afirmação verdadeira, apesar de parecer estranho à primeira vista, é possível uma visão receber insert ou update caso ela seja derivada de apenas uma tabela. Sendo que a operação existe, é possível fornecer o privilégio. |
| Resposta 02 |  | Com GRANT USAGE a role não pode alterar o valor da sequência |
| Feedback 02 |  | **Errado.** O privilégio USAGE possibilita a execução da função nextval, que incrementa e retorna o valor da sequence. |
| Resposta 03 |  | Não é necessário informar a função com a definição de parâmetros durante o GRANT |
| Feedback 03 |  | **Errado.** Quando usando o GRANT com funções, é necessário informar a assinatura completa da função, com parâmetros. Por exemplo: GRANT EXECUTE ON FUNCTION f\_calculo(int, int) TO jsilva |
| Resposta 04 | X | É possível utilizar a sintaxe ALL … IN SCHEMA com tabelas, visões e sequências |
| Feedback 04 |  | **Correto.** Para fornecer permissão em todos os objetos de determinado tipo em um schema usa-se ALL VIEWS, ALL FUNCTIONS e ALL [TABLES] IN SCHEMA ... |

|  |  |  |
| --- | --- | --- |
| Módulo | | 04 |
| Questão | | **10** |
| Finalidade | | **Fixação** |
| **Enunciado** | | **Sobre a retirada de permissões, qual seguinte afirmação é verdadeira:** |
| Resposta 01 |  | Para remover o usuário jsilva de um grupo contabilidade, usa-se:  ALTER ROLE jsilva REMOVE contabilidade; |
| Feedback 01 |  | **Errado.** Esta sintaxe é inválida, não existe a cláusula REMOVE. |
| Resposta 02 |  | Para retirar a permissão de inserção de uma tabela usa-se:  REVOKE INSERT FROM tabela TO usuario; |
| Feedback 02 |  | **Errado.** Sintaxe errada, o correto seria revoke insert ON tabela FROM usuario |
| Resposta 03 |  | Não é possível utilizar ALL com REVOKE, é necessário sempre explicitar todas os privilégios que se deseja remover |
| Feedback 03 |  | **Errado.** REVOKE ALL é completamente correta |
| Resposta 04 | X | Para remover o usuário jsilva do grupo contabilidade, usa-se: REVOKE contabilidade FROM jsilva; |
| Feedback 04 |  | **Correto.** Usa-se REVOKE para remover uma role de outra role, fornecendo o aspecto de grupo e membro |