8. Security Management

Este capítulo fornece diretrizes sobre como configurar as políticas de segurança para um banco de dados, e inclui informações sobre segurança, níveis de autoridade e privilégios de tabelas.

8.1 Security Policies

O DBMaker oferece dois tipos de segurança:

- **Autoridade de banco de dados** — determina quem pode acessar o DBMaker e as ações que podem realizar.
- **Privilégios de objeto** — controla os direitos de acesso aos objetos do DBMaker. Os objetos do DBMaker incluem tabelas, colunas, visualizações, domínios e sinônimos.

8.2 Database Authority

A autoridade de banco de dados é usada para determinar o acesso a um banco de dados. O DBMaker controla o acesso ao banco de dados com nomes de usuários e senhas e possui cinco classes de usuários, conforme mostrado na Figura 8-1.

O SYSADM é o nível de autoridade mais poderoso no DBMaker. Pode haver apenas um SYSADM para cada banco de dados. Um usuário com autoridade SYSADM pode conceder autoridade SYSDBA, DBA, RESOURCE ou CONNECT a outros usuários, definir a ACL (Lista de Controle de Acesso) para outros usuários e possui todos os privilégios dos níveis de autoridade SYSDBA e DBA no banco de dados.

Usuários com autoridade SYSDBA podem tanto conceder quanto revogar CONNECT, RESOURCE e DBA de outros usuários, alterar senhas de outros usuários, exceto usuários com autoridade SYSADM ou SYSDBA, e definir a ACL (Lista de Controle de Acesso) para usuários com autoridade inferior. Usuários com autoridade SYSDBA têm todos os privilégios de autoridade DBA e apenas usuários com autoridade SYSADM podem conceder ou revogar a autoridade SYSDBA de usuários. Para usuários com autoridade SYSDBA, se o SYSADM revogar a autoridade SYSDBA, os usuários ainda terão autoridade DBA, mas se o SYSADM revogar a autoridade DBA, os usuários não terão nem a autoridade SYSDBA nem a DBA.

Usuários com nível de autoridade DBA têm todos os privilégios para todos os objetos no banco de dados e podem conceder, alterar ou revogar privilégios de objeto para

qualquer usuário, exceto usuários com autoridade SYSADM, SYSDBA ou DBA. Eles também podem criar novos recursos, como tablespaces e arquivos, e realizar operações administrativas do banco de dados, como iniciar/terminar e fazer backup de bancos de dados.

Usuários com autoridade RESOURCE podem criar novas tabelas ou visualizações e conceder privilégios sobre suas próprias tabelas a outros usuários.

Usuários com apenas autoridade CONNECT podem acessar objetos para os quais receberam privilégios, mas não podem criar novas tabelas ou visualizações. Eles também podem selecionar informações das tabelas do sistema.

Os níveis de autoridade são hierárquicos.

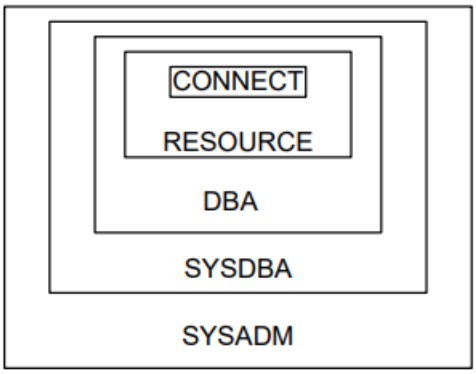


Figure 8-1: DBMaker database authority level hierarchy

LEVEL	PRIVILEGES
SYSADM	Pode conceder e revogar níveis de autoridade de segurança (CONNECT/RESOURCE/DBA/SYSDBA) para todos os usuários, exceto aqueles com autoridade SYSADM. Pode alterar as senhas de todos os usuários. Possui todos os privilégios do nível de autoridade SYSDBA.

RESOURCE	• Pode criar e excluir tabelas, visões (views), domínios e sinônimos. • Pode excluir apenas tabelas, visões, domínios e sinônimos criados pelo próprio usuário. • Pode conceder ou revogar privilégios de tabelas/visões de sua propriedade para outros usuários. • Possui privilégios sobre quaisquer tabelas que tenham sido concedidos ao usuário. • Possui todos os privilégios do nível de autoridade CONNECT.
CONNECT	• Pode fazer login no banco de dados. • Pode selecionar algumas tabelas do sistema (SYSTEM). • Possui alguns privilégios de tabela concedidos ao usuário. • Este nível de autoridade deve ser concedido antes dos outros níveis de autoridade.

Managing Users

O DBMaker oferece vários comandos SQL para gerenciar usuários. Esses comandos permitem adicionar novos usuários, remover usuários existentes de um banco de dados, definir ou alterar senhas de usuários e conceder níveis de autoridade aos usuários.

ADDING A USER

O SYSADM deve atribuir a cada usuário um nome de usuário e uma senha usando o comando GRANT (autoridade de banco de dados) antes que um usuário possa acessar o sistema.

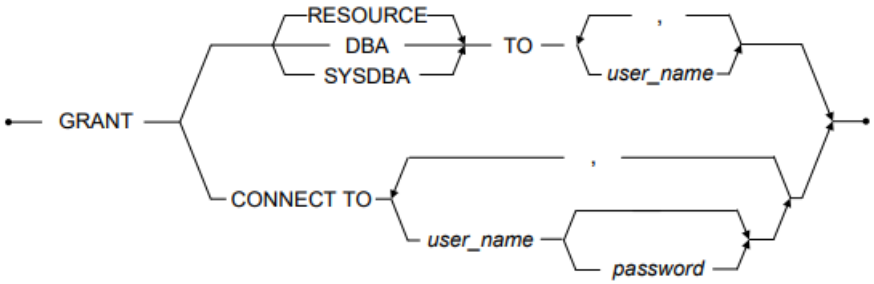


Figure 8-2 Syntax for the GRANT command

O comando GRANT concede níveis de autoridade aos usuários. Somente o SYSADM pode conceder níveis de autoridade a outros usuários. O nível de autoridade SYSADM não pode ser concedido a outros usuários. Como resultado, para cada banco de dados, há apenas um usuário com o nome de usuário SYSADM e o nível de autoridade SYSADM. O SYSADM também é o usuário padrão que cria o banco de dados. Somente a senha pode ser alterada para o nome de usuário SYSADM.

O SYSADM pode conceder as autoridades CONNECT, RESOURCE, DBA, SYSDBA e ACL a outros usuários. Se o comando GRANT for usado para conceder autoridade RESOURCE, DBA ou SYSDBA a um usuário, isso só terá efeito na próxima vez que o usuário se conectar ao banco de dados.

Usuários com autoridade SYSADM ou SYSDBA podem conceder uma senha a usuários com autoridade CONNECT. Se o SYSADM não especificar a senha, isso significa que o usuário não precisa de uma senha para acessar o banco de dados. Uma senha pode ser qualquer identificador SQL válido, que não tenha mais de dezesseis bytes.

Exemplo 1:

Para conceder o nível de autoridade CONNECT e a senha jeff123 ao usuário Jeff:

```
dmSQL> GRANT CONNECT TO Jeff jeff123;
```

Exemplo 2:

Para aumentar o nível de autoridade do usuário Jeff para RESOURCE

```
dmSQL> GRANT RESOURCE TO Jeff;
```

Exemplo 3:

Para aumentar o nível de autoridade do usuário Jeff para DBA:

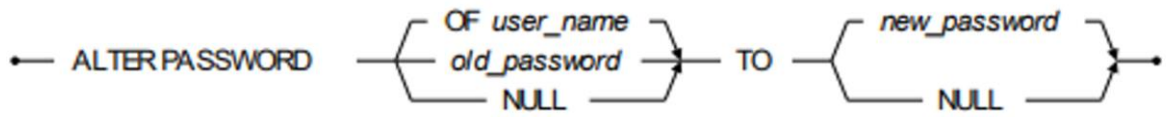
```
dmSQL>  GRANT  DBA  TO  Jeff;
```

Exemplo 4:

Para aumentar o nível de autoridade do usuário Jeff para SYSDBA:

```
dmSQL>  GRANT  SYSDBA  TO  Jeff;
```

CHANGING A PASSWORD O comando ALTER PASSWORD pode ser usado para alterar a senha de um usuário.



Existem duas maneiras de usar o comando: • Um usuário pode alterar sua própria senha com o comando ALTER PASSWORD <old_password> TO <new_password>. A <old_password> deve corresponder à senha original armazenada no banco de dados. • O SYSADM pode alterar a senha de qualquer usuário com o comando ALTER PASSWORD OF <user_name> TO <new_password>. Não é necessário que o SYSADM conheça a senha antiga dos outros usuários.

Exemplo 1:

O usuário Jeff altera sua senha de nenhuma senha para xyz@#:

```
dmSQL>  ALTER  PASSWORD  NULL  TO  "xyz@#";
```

Exemplo 2:

O SYSDBA altera a senha do usuário Jeff para abc@#:

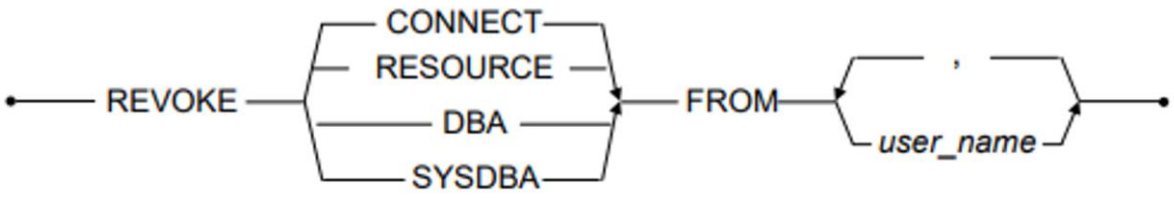
```
dmSQL> ALTER PASSWORD OF Jeff TO "abc@#";
```

Exemplo 3:

O SYSADM altera a senha do usuário Jeff para xyz@#:

```
dmSQL> ALTER PASSWORD OF Jeff TO "xyz@#";
```

REMOVING A USER OR CHANGING A USER'S AUTHORITY LEVEL



Revogar a autoridade RESOURCE, DBA ou SYSDBA de um usuário não terá efeito até a próxima vez que o usuário se conectar ao banco de dados.

Usuários com a autoridade SYSADM podem revogar CONNECT, RESOURCE, DBA, SYSDBA e ACL (Lista de Controle de Acesso) de outros usuários, mas não podem revogar privilégios de usuários com autoridade SYSADM.

Os usuários com autoridade SYSDBA também podem revogar CONNECT, RESOURCE, DBA e ACL (Lista de Controle de Acesso) de usuários com autoridade inferior, mas não podem revogar privilégios de usuários com autoridade SYSDBA.

Exemplo 1:

Para revogar a autoridade SYSDBA do usuário Jeff:

```
dmSQL>  REVOKE  SYSDBA  FROM  Jeff;
```

Após a execução do comando, Jeff não terá mais a autoridade SYSDBA, mas ainda manterá a autoridade DBA.

Exemplo 2:

Para revogar a autoridade DBA do usuário Jeff:

```
dmSQL>  REVOKE  DBA  FROM  Jeff;
```

Após a execução do comando, Jeff não terá mais a autoridade DBA, mas ainda manterá a autoridade CONNECT.

Exemplo 3:

Para remover a autoridade CONNECT de Jeff e retirar sua capacidade de acessar o sistema:

```
dmSQL> REVOKE CONNECT FROM Jeff;
```

REVOKED PRIVILEGE	DESCRIPTION
SYSDBA	Revogar a autoridade SYSDBA de um usuário significa que o usuário não poderá mais conceder ou revogar níveis de autoridade de segurança (CONNECT/RESOURCE/DBA) para outros usuários, nem poderá mais alterar as senhas de outros usuários. • O usuário manterá a autoridade DBA. • Todas as tabelas, visões, domínios e sinônimos criados por esse usuário permanecerão no banco de dados.
DBA	Revogar a autoridade DBA de um usuário significa que o usuário não poderá mais criar ou excluir tabelas, nem conceder ou revogar privilégios de outros usuários. • O usuário manterá apenas a autoridade CONNECT, a menos que lhe seja concedido o privilégio RESOURCE. • Todas as tabelas, visões, domínios e sinônimos criados por esse usuário permanecerão no banco de dados.
RESOURCE	Revogar a autoridade RESOURCE significa que o usuário não poderá mais criar ou excluir tabelas. • O usuário manterá apenas a autoridade CONNECT, a menos que lhe seja concedido o privilégio DBA. • Todas as tabelas, visões, domínios e sinônimos criados por esse usuário permanecerão no banco de dados.
CONNECT	Revoking this authority means the user can no longer log on to the database. • All privileges owned by this user on tables and views will be revoked. • All tables, views, domains, and synonyms created by this user remain in database.

Managing Groups

Para simplificar a gestão dos níveis de autoridade, use um grupo para reunir vários usuários ou outros grupos. Privilégios de banco de dados podem ser concedidos a todos os membros de um grupo ao mesmo tempo com um único comando. Embora um grupo seja diferente de um usuário, ele pode ser tratado como um usuário. Os privilégios de objeto concedidos a um grupo se aplicam a todos os membros do grupo.

Apenas usuários com níveis de autoridade SYSADM, SYSDBA ou DBA podem:

- Criar grupos
- Adicionar membros a grupos
- Remover membros de grupos
- Excluir grupos

CREATING GROUPS

A instrução CREATE GROUP é usada para criar um novo grupo.

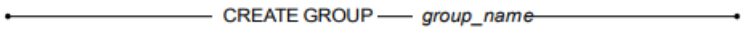


Figure 8-5 Syntax for the CREATE GROUP command

A identificação do grupo (nome do grupo) identifica exclusivamente o nome de um grupo no DBMaker. O nome do grupo não pode ser SYSTEM, PUBLIC, GROUP ou qualquer nome de usuário ou grupo existente.

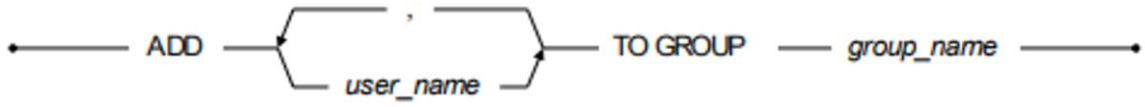
Exemplo:

Para criar um novo grupo chamado COMMITTEE:

```
dmSQL>                CREATE                GROUP                COMMITEE;
```

ADDING MEMBERS TO GROUPS

Após criar um novo grupo, os usuários podem ser adicionados usando o comando ADD <nome do usuário ou nome do grupo> TO GROUP.



Um grupo não pode ser adicionado como um novo membro de si mesmo. Os membros de um grupo podem incluir qualquer nome de usuário ou nome de grupo existente.

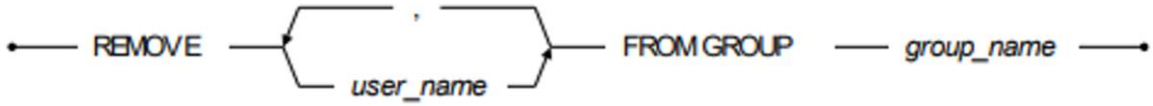
Exemplo:
Para adicionar o usuário Jeff e o grupo RD ao grupo COMMITTEE e conceder o privilégio SELECT à tabela CASEMaker.TB_STAFF

```
dmSQL> ADD Jeff, RD TO GROUP COMMITEE; dmSQL> GRANT SELECT ON CASEMaker.TB_STAFF TO COMMITEE;
```

Após a execução deste comando, o usuário Jeff será removido do grupo COMMITTEE e perderá o privilégio SELECT na tabela CASEMaker.TB_STAFF.

REMOVING MEMBERS FROM GROUPS

O comando `REMOVE <nome_do_usuario_ou_do_grupo> FROM GROUP` pode ser usado para remover usuários de um grupo especificado.



Os membros removidos do grupo perderão todos os privilégios concedidos ao grupo especificado, mas manterão os privilégios concedidos diretamente a eles.

Exemplo:

Para remover o usuário Jeff do grupo COMMITTEE:

```
dmSQL> REMOVE Jeff FROM GROUP COMMITEE;
```

Após a execução deste comando, o usuário Jeff será removido do grupo COMMITTEE e perderá o privilégio SELECT na tabela CASEMaker.TB_STAFF.

DROPPING GROUPS

O comando DROP GROUP excluirá um grupo especificado de um banco de dados; todos os membros do grupo perderão os privilégios concedidos ao grupo.

Figure 8-8 Syntax for the DROP GROUP command

Exemplo:

Para excluir o grupo COMMITTEE do banco de dados:

```
dmSQL>  DROP  GROUP  COMMITEE;
```

Checking IP Addresses

Você pode querer que os clientes se conectem ao seu banco de dados apenas usando endereços IP específicos, por exemplo, 192.72.112.*, ou deseja que certos endereços IP sejam proibidos de se conectar ao banco de dados, por exemplo, 192.168.0.*. Ativar a verificação de IP permite que você controle os endereços IP que os clientes podem usar para acessar seu banco de dados e os endereços IP proibidos. Todas as configurações dos usuários são armazenadas no catálogo do sistema SYSACL.

O catálogo contém três colunas: USER_NAME, ADDRESS e PRIVILEGE.

- **USER_NAME**: O nome e as configurações do usuário que está tentando se conectar.
- **ADDRESS**: O endereço IP permitido para se conectar ao banco de dados.
- **PRIVILEGE**: O endereço IP especificado é permitido ou bloqueado (privilégio ALLOW ou BLOCK) para se conectar ao banco de dados.

O nome de usuário PUBLIC é reservado. Se você usar o nome de usuário PUBLIC, todos os usuários devem satisfazer as configurações especificadas para se conectar ao banco de dados.

Quando um banco de dados é criado, a visualização SYSORDERACL é automaticamente criada e exibe informações sobre os endereços IP de todos os usuários. Portanto, os usuários podem consultar essas informações para verificar se um endereço IP é permitido para se conectar ao banco de dados.

ENABLE IP CHECKING

Você pode usar a palavra-chave DB_StACL no arquivo dmconfig.ini para habilitar a verificação de IP. É necessário configurar a verificação de IP antes de iniciar o banco de dados.

- **DB_StACL = 1**: Habilita a verificação de IP
- **DB_StACL = 0**: Desabilita a verificação de IP (padrão)

CREATE A RULE

Existem dois tipos de regras de verificação de IP: baseadas em lista de permissões (whitelist) e baseadas em lista de bloqueio (blacklist). Para o mesmo endereço IP, o resultado das restrições sob as duas regras segue a tabela abaixo:

Match	Whitelist-based	Blacklist-based
Corresponder apenas à lista de endereços IP permitidos	Permitido	Permitido
Corresponder apenas à lista de endereços IP bloqueados	Bloqueado	Bloqueado
Não corresponder a nenhum dos dois	Bloqueado	Permitido
Corresponder a ambos	Bloqueado	Permitido

Conjunto baseado em lista branca, a coluna ACLORDER de SYSAUTHUSER está marcada com 0;

conjunto baseado em lista negra, a coluna ACLORDER de SYSAUTHUSER está marcada com 1.

Para permitir a maioria dos endereços IP e, ao mesmo tempo, proibir alguns endereços IP específicos, o método baseado em lista branca é mais apropriado; para proibir a maioria dos endereços IP e, ao mesmo tempo, permitir alguns endereços IP específicos, o método baseado em lista negra é mais apropriado. A regra padrão é baseada em lista branca.

Exemplo 1a:

Glow seleciona o método baseado em lista negra como sua regra de verificação de IP e proíbe clientes de se conectar ao banco de dados usando todos os endereços IP do segmento 127.0.0.* exceto 127.0.0.1.

```
dmSQL> GRANT BLOCK TO Glow '127.0.0.*';
dmSQL> GRANT ALLOW TO Glow '127.0.0.1';
```

Exemplo 1b:

Jeff seleciona o método baseado em lista branca como sua regra de verificação de IP e permite que os clientes se conectem ao banco de dados usando todos os endereços IP do segmento 192.168.0.*, exceto 192.168.0.3.

```
dmSQL>    GRANT    ALLOW    TO    Jeff    '192.168.0.*';
dmSQL>    GRANT    BLOCK    TO    Jeff    '192.168.0.3';
```

Um usuário pode selecionar apenas um tipo de regra de verificação de IP. Para alterar a regra de verificação de IP para um usuário, use a instrução ALTER ACL ORDER. Observe que, antes de alterar a regra, é recomendável que os usuários revoguem todas as restrições concedidas. Para detalhes sobre restrições, consulte as seções: Criar uma restrição e Remover uma restrição.

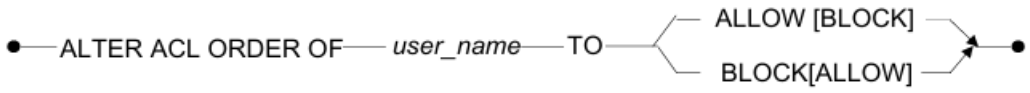


Figure 8-9 ALTER ACL ORDER

Exemplo 2:

```
dmSQL> REVOKE BLOCK FROM Vivian ALL;
dmSQL> REVOKE ALLOW FROM Vivian ALL;
dmSQL> ALTER ACL ORDER OF Vivian TO ALLOW BLOCK;
```

CREATE A CONSTRAINT

Após configurar as regras de verificação de IP, os usuários podem criar uma restrição para a regra de verificação de IP especificada com as instruções GRANT ALLOW e GRANT BLOCK.

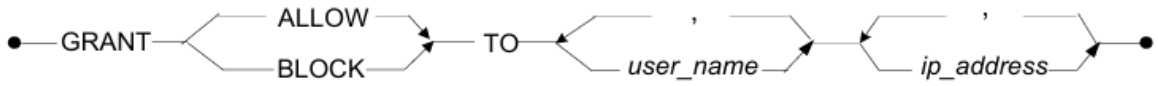


Figure 8-10 GRANT ALLOW/BLOCK TO USERLIST IPLIST

The GRANT ALLOW statement is same as the GRANT ACCESS statement.

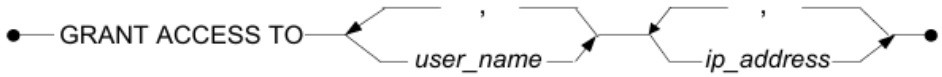


Figure 8-11 GRANT ACCESS TO USERLIST IPLIST

Exemplo:

```
dmSQL>  GRANT   ACCESS   TO   vivian,joe    '192.72.5.23','140.21.55.*';
dmSQL>  GRANT   ALLOW    TO   jane,jetty    '192.72.12.20','140.15.45.*';
dmSQL>  GRANT   BLOCK    TO   pine,jim      '192.70.16.20','139.15.45.*';
```

Observe que apenas o privilégio ALLOW em endereços IP pode ser concedido ao grupo PUBLIC. Se os usuários concederem o privilégio BLOCK em endereços IP ao grupo PUBLIC, será retornado o ERRO (6890). Além disso, com base no fato de que o privilégio ALLOW em vários endereços IP foi concedido ao grupo PUBLIC, um usuário pertencente ao grupo PUBLIC também pode adicionar regras baseadas em lista branca ou lista negra para si mesmo.

REMOVE A CONSTRAINT

Para revogar uma restrição para a regra de verificação de IP especificada, use as instruções REVOKE ALLOW e REVOKE BLOCK.

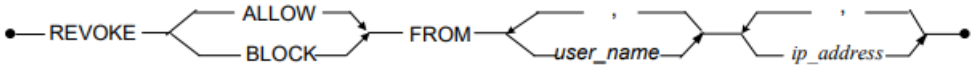


Figure 8-12 REVOKE ALLOW/BLOCK FROM USERLIST IPLIST

A instrução REVOKE ALLOW é equivalente à instrução REVOKE ACCESS.

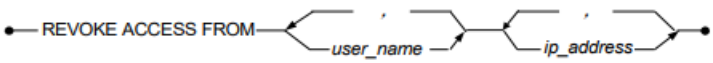


Figure 8-13 REVOKE ACCESS FROM USERLIST IPLIST

Para revogar todas as restrições de um usuário para a regra de verificação de IP especificada de uma só vez, use a instrução "REVOKE ALLOW/BLOCK FROM user_name ALL". O termo ALL indica todos os endereços IP.

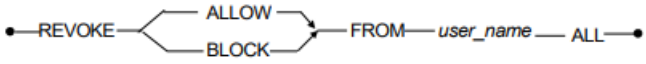


Figure 8-14 REVOKE ALLOW/BLOCK FROM user_name ALL

Exemplo:

```
dmSQL> REVOKE ACCESS FROM vivian,joe '192.72.77.*','140.44.88.23';
dmSQL> REVOKE ALLOW FROM jane,jetty '192.72.12.20','140.15.45.*';
dmSQL> REVOKE BLOCK FROM pine,jim '192.70.16.20','139.15.45.*';
dmSQL> REVOKE BLOCK FROM glow ALL;
```

8.3 Object Privileges

Um objeto em um banco de dados inclui os seguintes itens: tabelas, visualizações e colunas em tabelas/visualizações, domínios ou sinônimos. O DBMaker fornece gerenciamento de segurança para objetos, permitindo que os usuários CONCEDAM ou REVOGUEM privilégios de objeto para outros usuários.

Todos os usuários podem referenciar um domínio por padrão, mas apenas o criador pode excluir o domínio. Os privilégios para um sinônimo são baseados em uma tabela base. Consulte o Capítulo 6, Gerenciamento de Esquema e Objetos de Esquema, para definições detalhadas de visualizações, domínios e sinônimos.

Granting Object Privileges

O usuário que cria um objeto se torna o proprietário do objeto e possui todos os privilégios sobre ele. O proprietário também pode conceder privilégios sobre o objeto a outros usuários usando o comando SQL GRANT <object privilege>.

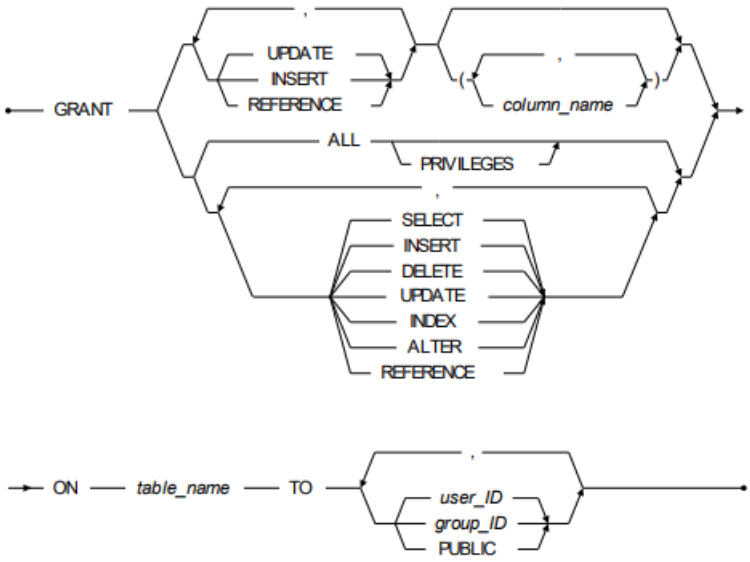


Figure 8-15 Syntax for the GRANT command

Um usuário com autoridade DBA pode conceder privilégios para qualquer tabela ou visualização em um banco de dados. Um usuário com autoridade RESOURCE pode conceder privilégios apenas em tabelas ou visualizações que ele criou. Todos os privilégios suportados pelo DBMaker estão descritos na Tabela 12-3.

Os privilégios INSERT, UPDATE e DELETE devem ser controlados para evitar a corrupção de informações no banco de dados. Os privilégios ALTER e INDEX devem ser restritos a desenvolvedores.

Os privilégios UPDATE, INSERT e REFERENCE podem ser restritos a algumas colunas específicas. Cada nome de coluna deve ser qualificado e estar em cada tabela identificada na cláusula ON.

PRIVILEGE	DESCRIPTION
SELECT	Permite que os usuários selecionem dados de uma tabela ou visão.
INSERT	Permite que os usuários insiram linhas em uma tabela ou visão e, opcionalmente, insiram em colunas específicas.
DELETE	Permite que os usuários excluam linhas de uma tabela ou visão.
UPDATE	Permite que os usuários atualizem uma tabela ou visão e, opcionalmente, atualizem colunas específicas.
INDEX	Permite que os usuários criem ou excluam índices para uma tabela.
ALTER	Permite que os usuários alterem a definição de uma tabela.

REFERENCE	Permite que os usuários criem uma chave estrangeira em uma tabela de origem que faça referência a uma chave primária em uma tabela ou visão de destino.
ALL [PIVILEGES]	Permite que os usuários exerçam todos os privilégios acima para uma tabela ou visão. O termo PRIVILEGES é opcional.

O usuário em um comando GRANT deve ter pelo menos autoridade CONNECT. O nome do grupo é criado usando o comando CREATE GROUP. A palavra-chave PUBLIC inclui todos os usuários atuais e futuros.

Exemplo 1:

Jeff executa o comando GRANT para conceder a Cathy o privilégio de leitura dos dados na tabela TB_INFO, criada por ele:

```
dmSQL> GRANT SELECT ON TB_INFO TO Cathy;
```

Exemplo 2:

Um DBA executa o comando GRANT para conceder a Cathy o privilégio de leitura dos dados na tabela TB_INFO, criada por Jeff:

```
dmSQL> GRANT SELECT ON Jeff.TB_INFO TO Cathy;
```

Exemplo 3:

Um DBA concede os privilégios INSERT e UPDATE para a coluna PHONENO da tabela TB_INFO a Cathy:

```
dmSQL> GRANT INSERT (PHONENO) ON Jeff.TB_INFO TO Cathy;
dmSQL> GRANT UPDATE (PHONENO) ON Jeff.TB_INFO TO Cathy;
```

Cathy não terá privilégios para excluir informações da coluna.

Exemplo 4:

Uso da palavra-chave PUBLIC para permitir que todos os usuários leiam dados na tabela Jeff.TB_INFO:

```
dmSQL> GRANT SELECT ON Jeff.TB_INFO TO PUBLIC;
```

Revoking Object Privileges

O comando REVOKE <object privileges> revoga os privilégios concedidos a um usuário. A sintaxe para esse comando é mostrada na Figura 8-16.

Os privilégios no comando REVOKE (object privileges) são os mesmos do comando GRANT (object privileges). No diagrama, o nome de usuário representa um usuário autorizado no banco de dados, o nome do grupo representa um grupo de usuários e a palavra-chave PUBLIC representa todos os usuários no banco de dados.

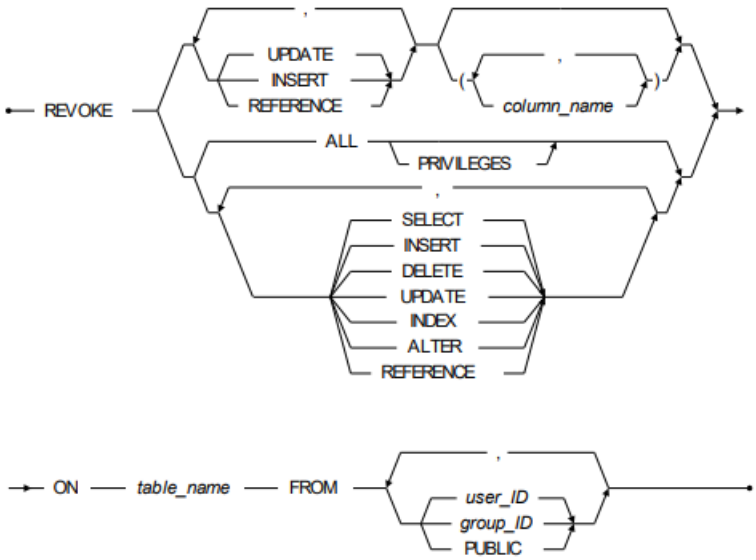


Figure 8-16 The REVOKE (object privileges) command

Exemplo 1:

O seguinte comando revoga o privilégio SELECT para a tabela TB_INFO de Cathy:

```
dmSQL> REVOKE SELECT ON TB_INFO FROM Cathy;
```

Exemplo 2:

O seguinte comando revoga o privilégio SELECT para a tabela Jeff.TB_INFO de Cathy:

```
dmSQL> REVOKE SELECT on Jeff.TB_INFO FROM Cathy;
```

Exemplo 3:

O seguinte comando revoga os privilégios UPDATE na coluna PHONENO na tabela Jeff.TB_INFO do grupo1:

```
dmSQL> REVOKE UPDATE (PHONENO) on Jeff.TB_INFO FROM group1;
```

Exemplo 4:

O seguinte comando revoga todos os privilégios concedidos ao PUBLIC na tabela TB_INFO:

```
dmSQL> REVOKE ALL ON TB_INFO FROM PUBLIC;
```

Exemplo 5:

O seguinte comando revoga os privilégios INSERT, UPDATE e SELECT para a tabela TB_INFO do usuário Cathy e de todos os usuários no grupo2:

```
dmSQL> REVOKE INSERT, UPDATE, SELECT ON TB_INFO FROM Cathy, group2;
```

8.4 Security System Catalog

Todas as informações sobre níveis de autoridade, privilégios e grupos são registradas nos seguintes catálogos do sistema:

- **SYSAUTHUSER** — nível de autoridade de cada usuário
- **SYSAUTHTABLE** — privilégios sobre tabelas
- **SYSAUTHCOL** — colunas de uma tabela para as quais um usuário foi restrito quanto aos privilégios INSERT, UPDATE e REFERENCE
- **SYSAUTH** — nome do grupo, criador do grupo e número de membros do grupo
- **SYSACL** — regras de verificação de IP dos usuários

Os catálogos de segurança do sistema são propriedade do SYSTEM. Nenhum usuário, incluindo SYSADM, pode modificar os catálogos do sistema. Consulte o *System Catalog Reference* para mais detalhes sobre os catálogos do sistema DBMaker.