





Aula 24 – Autenticação e Autorização





O que iremos aprender?



- Segurança no SQL Server;
- Usuário de conexão do SQL Server
- Autorizações
- Autorizações a nível de servidor e banco
- Autorizações através do Management Studio





Segurança no SQL Server

Abordaremos os seguintes tópicos:

- Contas de serviço do SQL Server;
- Autenticação e autorização;



Segurança – Contas de serviço

- NT SERVICE\MSSQLSERVER para os serviços do DB;
- NT SERVICE\SQLSERVERAGENT para os serviços de agente do SQL;

Se usarmos instâncias nomeadas, este nome estará no nome da conta de serviço. Podermos associar esta conta de serviço a:

- Contas de serviço gerenciadas;
- Contas do sistema internas;
- Contas de serviço gerenciadas do grupo;
- Contas de usuário do domínio;
- Contas do Windows locais.





Autorização de acesso

O SQL Server possui duas autorizações de acesso:

SQL Server autenticação

- Windows autenticação
 - Local windows account;
 - Local windows group;
 - Domain account;
 - Domain group.





Autorização de acesso

 Podemos adicionar o login de um grupo do Windows ou usuário com o comando CREATE LOGIN

CREATE LOGIN [SQLSERVER\GRUPO] FROM WINDOWS

CREATE LOGIN [SQLSERVER\Pedro] FROM WINDOWS



Autorização de acesso

No caso do usuário SQL SERVER nós mesmos especificamos o login e senha

```
CREATE LOGIN [nome do usuario] WITH PASSWORD = '123'
```

 Podemos associar a senha do usuário SQL com as diretivas de segurança do Windows.

```
CREATE LOGIN [nome do usuario] WITH PASSWORD = '123',
CHECK_EXPIRATION=ON, CHECK_POLICY=ON
```

Gerenciamento de propriedades do login

Podemos verificar as propriedades dos LOGINs do SQL SERVER

master.sys.sql_logins



Autorizações

Existem nove funções de servidor fixas predefinidas em cada servidor que você pode usar como ponto de partida para proteger o ambiente do SQL Server.

- sysadmin Membros dessa função podem executar qualquer atividade no servidor;
- bulkadmin Membros podem executar BULK INSERT e usar a ferramenta bcp.exe;
- diskadmin Os membros podem gerenciar arquivos de disco;
- processadmin Membros podem MATAR processos em execução no SQL Server.
- public Cada login é um membro da função pública. Se um objeto não recebe uma configuração específica ele será público;
- securityadmin Os membros podem gerenciar logins e suas propriedades;
- serveradmin Podem alterar as configurações no nível do servidor e encerrar o SQL Server.



Autorizações

- setupadmin Os membros podem criar servidores vinculadados com comando TSQL;
- dbcreator Podem gerenciar banco de dados.





Autorizações

Comando ALTER SERVER ROLE pode adicionar usuários a regras pré-definidas.

• dbcreator – Podem gerenciar banco de dados.

ALTER SERVER ROLE [SYSADMIN] ADD MEMBER [NOME DO USUARIO]

ALTER SERVER ROLE [SYSADMIN] ADD MEMBER [DOMINIO\NOME DO USUARIO]

ALTER SERVER ROLE [SYSADMIN] DROP MEMBER [NOME DO USUARIO]





Autorizações Servidor

Se executarmos o comando abaixo veremos as seguranças a nível servidor.

```
SELECT * FROM SYS.FN_BUILTIN_PERMISSIONS('')
WHERE CLASS_DESC = 'SERVER'
```





É uma lista extensa. Podemos mencionar alguns caso:

CREATE ANY DATABASE— Permite ao usuário criar novos bancos de dados e armazenar bancos de dados.

ALTER ANY LOGIN – Permite ao usuário modificar logins na instancia, redefinir senhas e criar novos logins.

ALTER ANY DATABASE – Permite que o usuário altere as opções do banco de dados e crie novos bancos de dados.



Existem algumas autorizações de acessos a banco de dados que podem ser associados aos usuários:

db_owner – Os membros da função de banco de dados fixa db_owner podem executar todas as atividades de configuração e manutenção no banco de dados, bem como remover o banco de dados no SQL Server.

db_securityadmin – Os membros da função de banco de dados fixa db_security podem modificar a associação de funções e gerenciar permissões.

db_acessadmin – Os membros dessa função podem adicionar ou remover o acesso ao banco de dados para logons do Windows, grupos do Windows e logons do SQL Server.



db_backupoperator – Os membros com essa função de banco de dados podem fazer backup do banco de dados.

db_ddladmin – Os membros dessa função de banco de dados podem executar qualquer comando DDL (Data Definition Language) em um banco de dados.

db_datawrite – Os membros dessa função podem adicionar, excluir ou alterar dados em todas as tabelas de usuário.

db_datareader— Os membros dessa função de banco de dados ler todos os dados de todas as tabelas de usuário.





db_denydatawritter – Os membros dessa função de banco de dados não podem adicionar, modificar ou excluir nenhum dado nas tabelas de usuário de um banco de dados.

db_denydatareader – Os membros dessa função de banco de dados não podem ler nenhum dado nas tabelas de usuário de um banco de dados.

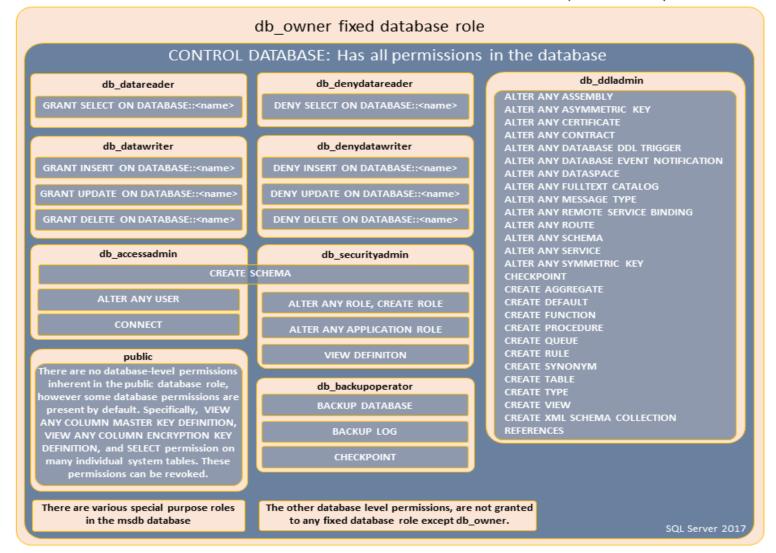


SERVIÇO NACIONAL DE APRENDIZAGEM INDUSTRIAL



Autorizações Banco de Dados

DATABASE LEVEL ROLES AND PERMISSIONS: 11 fixed database roles, 77 database permissions





SERVIÇO NACIONAL DE APRENDIZAGEM INDUSTRIAL



Autorizações Banco de Dados

```
USE <NOME DA BASE DA DADOS>
```

```
SP_ADDROLEMEMBER '<NOME DA REGRA>','<USUARIO>'
```



SERVIÇO NACIONAL DE APRENDIZAGEM INDUSTRIAL



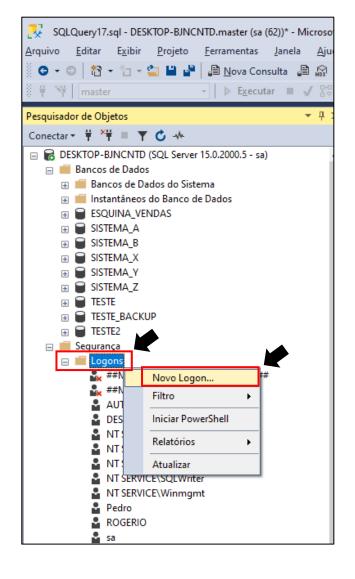
Autorizações Banco de Dados

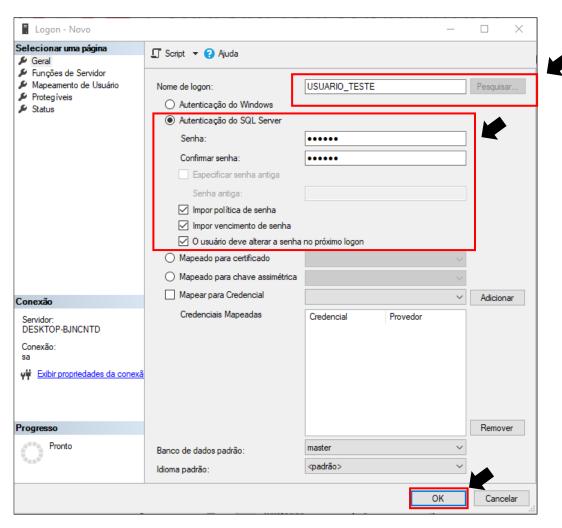
ALTER ROLE [NOME DA REGRA] ADD MEMBER [USUARIO]

ALTER ROLE [NOME DA REGRA] DROP MEMBER [USUARIO]



Autorizações através do Management Studio



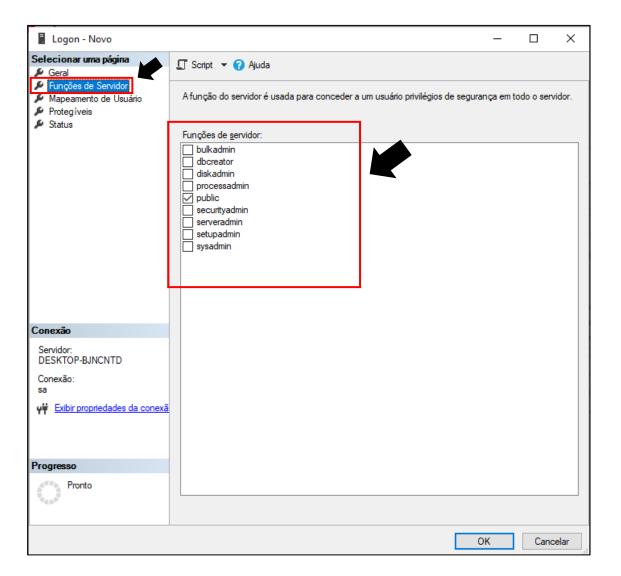


Microsoft®



Autorizações através do Management Studiò

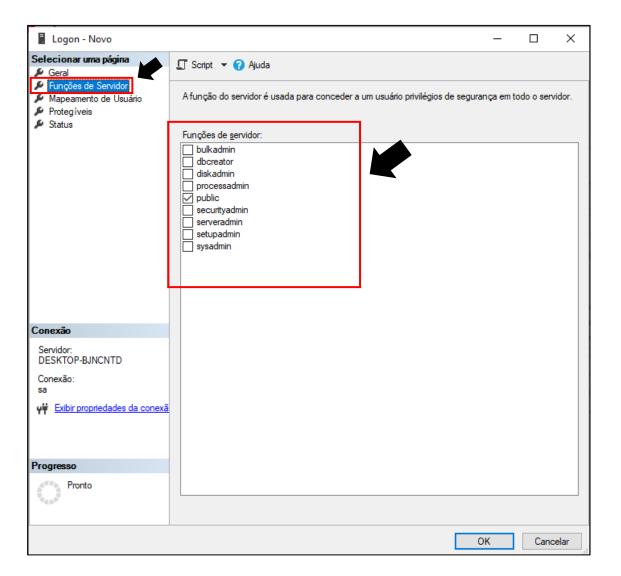
Microsoft®





Autorizações através do Management Studiò

Microsoft®







Autorizações através do Management Studiò

Funções de Servidor Mapeamento de Usuário	napeados para este logon: Banco de Dados Usuário Esquema Padrão ESQUINA_VENDAS master model msdb SISTEMA_A SISTEMA_B SISTEMA_B SISTEMA_Y SISTEMA_Y SISTEMA_Z tempdb TESTE TESTE TESTE_BACKUP TESTE2 Convidado habilitada para: ESQUINA_VENDAS cessadmin ckupoperator tareader tawriter ladmin nydatareader nydatawriter oner curityadmin	elecionar uma página								
Usuários mapeados para este logon: Mapa Banco de Dados Usuário Esquema Padrão Sistaus ESQUINA_VENDAS master model model model model	Banco de Dados Usuário Esquema Padrão ESQUINA_VENDAS master model msdb SISTEMA_A SISTEMA_B SISTEMA_Y SISTEMA_Y SISTEMA_Z tempdb TESTE TESTE_BACKUP TESTE2 Convidado habilitada para: ESQUINA_VENDAS cessadmin ckupoperator tareader tawriter ladmin nydatareader nydatawriter vner curityadmin	Geral								
Mapa Banco de Dados Usuário Esquema Padrão	Banco de Dados Usuário Esquema Padrão ESQUINA_VENDAS master model msdb SISTEMA_A SISTEMA_B SISTEMA_Y SISTEMA_Z tempdb TESTE TESTE_BACKUP TESTE2 Convidado habilitada para: ESQUINA_VENDAS cessadmin ckupoperator tareader tawriter ladmin nydatareader nydatawriter vner curityadmin	Mapeamento de Usuário	Usuários mapeados para este logo	n:						
master model msdb SISTEMA_A SISTEMA_B SISTEMA_Y SISTEMA_Z tempdb TESTE TESTE TESTE TESTE TESTE TESTE TESTE TESTE SEKTOP-BJNCNTD viewăo: view zion db de	master model msdb SISTEMA_A SISTEMA_B SISTEMA_X SISTEMA_Y SISTEMA_Z tempdb TESTE TESTE_BACKUP TESTE2 Convidado habilitada para: ESQUINA_VENDAS to à função de banco de dados para: ESQUINA_VENDAS cessadmin ckupoperator tareader tareader tareader tareader inydatareader nydatawriter ner curityadmin	Protegíveis	-		Esquema Padrão					
model msdb SISTEMA_A SISTEMA_B SISTEMA_Y SISTEMA_Z tempdb TESTE TESTE_BACKUP TESTE2 Conta Convidado habilitada para: ESQUINA_VENDAS Exibir propriedades da conexão Exibir propriedades da conexão Exibir propriedades da conexão Degresso Degresso Degresso Degresso Degresso Descriptor Descrip	model msdb SISTEMA_A SISTEMA_B SISTEMA_X SISTEMA_Y SISTEMA_Z tempdb TESTE TESTE_BACKUP TESTE2 Convidado habilitada para: ESQUINA_VENDAS io à função de banco de dados para: ESQUINA_VENDAS cessadmin ckupoperator tareader tawriter ladmin nydatareader nydatawriter viner curityadmin	Status	☐ ESQUINA_VENDAS							
msdb SISTEMA_A SISTEMA_B SISTEMA_X SISTEMA_Y SISTEMA_Z tempdb TESTE TESTE TESTE TESTE TESTE SEKTOP-BJNCNTD TESTE SISTEMA_Z TESTE TES	msdb SISTEMA_A SISTEMA_B SISTEMA_X SISTEMA_Y SISTEMA_Z tempdb TESTE TESTE_BACKUP TESTE2 Convidado habilitada para: ESQUINA_VENDAS to à função de banco de dados para: ESQUINA_VENDAS cessadmin ckupoperator tareader tawriter ladmin nydatareader nydatawriter viner curityadmin		master							
SISTEMA_A SISTEMA_B SISTEMA_X SISTEMA_Y SISTEMA_Z tempdb TESTE TESTE TESTE TESTE SISTEMA_C TESTE Associação à função de banco de dados para: ESQUINA_VENDAS TESTE Exibir propriedades da conexã Exibir propriedades da conexã Dogresso Dogresso Dogresso Dogresso Dogresso SISTEMA_X SISTEMA_X SISTEMA_Y SISTEMA_Z TESTE Departa Departa SISTEMA_Y SISTEM	SISTEMA_A SISTEMA_X SISTEMA_Y SISTEMA_Z tempdb TESTE TESTE_BACKUP TESTE2 Convidado habilitada para: ESQUINA_VENDAS to à função de banco de dados para: ESQUINA_VENDAS cessadmin ckupoperator tareader tawriter ladmin nydatareader nydatawriter vner curityadmin		model							
SISTEMA_B SISTEMA_X SISTEMA_Y SISTEMA_Z tempdb TESTE TESTE TESTE TESTE SESKTOP-BJNCNTD Associação à função de banco de dados para: ESQUINA_VENDAS Conexão: Describe dades da conexã La backupoperator Describe dadas de conexã Describe dadas de conexão: Describe dadas da conexão: Describe dadas de conexão: Describe dadas de conexão: Describe dadas da conexão: Describe da conexão:	SISTEMA_X SISTEMA_Y SISTEMA_Z tempdb TESTE TESTE_BACKUP TESTE2 Convidado habilitada para: ESQUINA_VENDAS io à função de banco de dados para: ESQUINA_VENDAS cessadmin ckupoperator tareader tawriter ladmin nydatareader nydatawriter vner curityadmin		msdb							
SISTEMA_X SISTEMA_Y SISTEMA_Z tempdb TESTE TESTE TESTE TESTESTE TESTESTE TESTES Conta Convidado habilitada para: ESQUINA_VENDAS SESKTOP-BJNCNTD TESTES Associação à função de banco de dados para: ESQUINA_VENDAS SONEXÃO: Associação à função de banco de dados para: ESQUINA_VENDAS De propriedades da conexã De propriedades da conexão De propriedades da conexão De propriedades da conexão De propriedades da conexão De p	SISTEMA_X SISTEMA_Z tempdb TESTE TESTE_BACKUP TESTE2 Convidado habilitada para: ESQUINA_VENDAS to à função de banco de dados para: ESQUINA_VENDAS cessadmin ckupoperator tareader tawriter ladmin nydatareader nydatawriter vner curityadmin		SISTEMA_A							
SISTEMA_Y SISTEMA_Z tempdb TESTE TESTE_BACKUP TESTE2 Conta Convidado habilitada para: ESQUINA_VENDAS SESKTOP-BJNCNTD	SISTEMA_Z tempdb TESTE TESTE_BACKUP TESTE2 Convidado habilitada para: ESQUINA_VENDAS to à função de banco de dados para: ESQUINA_VENDAS cessadmin ckupoperator tareader tawriter lladmin nydatareader nydatawriter viner curityadmin		SISTEMA_B							
SISTEMA_Z tempdb TESTE TESTE TESTE_BACKUP TESTE2 TESTE TESTE2 Teste2 Teste2 Conta Convidado habilitada para: ESQUINA_VENDAS Associação à função de banco de dados para: ESQUINA_VENDAS Description Descrip	SISTEMA_Z tempdb TESTE TESTE_BACKUP TESTE2 Convidado habilitada para: ESQUINA_VENDAS to à função de banco de dados para: ESQUINA_VENDAS to cessadmin ckupoperator ttareader ttareader ttawriter ladmin nydatareader nydatawriter viner curityadmin		☐ SISTEMA_X							
tempdb TESTE TESTE_BACKUP TESTE2 Conta Convidado habilitada para: ESQUINA_VENDAS Conexão: DeskTOP-BJNCNTD Conexão: Desk	tempdb TESTE TESTE_BACKUP TESTE2 Convidado habilitada para: ESQUINA_VENDAS to à função de banco de dados para: ESQUINA_VENDAS cessadmin ckupoperator tareader tawriter lladmin mydatareader mydatawriter viner curityadmin		☐ SISTEMA_Y							
tempdb TESTE TESTE_BACKUP TESTE2 Conta Convidado habilitada para: ESQUINA_VENDAS Conexão: DeskTOP-BJNCNTD Conexão: Desk	tempdb TESTE TESTE_BACKUP TESTE2 Convidado habilitada para: ESQUINA_VENDAS to à função de banco de dados para: ESQUINA_VENDAS cessadmin ckupoperator tareader tawriter lladmin mydatareader mydatawriter viner curityadmin		☐ SISTEMA_Z							
TESTE_BACKUP TESTE2 Conta Convidado habilitada para: ESQUINA_VENDAS Conexão: Conexã	TESTE_BACKUP TESTE2 Convidado habilitada para: ESQUINA_VENDAS io à função de banco de dados para: ESQUINA_VENDAS cessadmin ckupoperator tareader tawriter lladmin nydatareader nydatawriter vner curityadmin		_							
TESTE2 Conta Convidado habilitada para: ESQUINA_VENDAS Conexão: a	TESTE2 Convidado habilitada para: ESQUINA_VENDAS so à função de banco de dados para: ESQUINA_VENDAS coessadmin ckupoperator tareader tawriter lladmin nydatareader nydatawriter vner curityadmin		☐ TESTE							
Conta Convidado habilitada para: ESQUINA_VENDAS ESEKTOP-BJNCNTD Associação à função de banco de dados para: ESQUINA_VENDAS db_accessadmin db_backupoperator db_datareader db_datawriter db_ddladmin db_denydatareader db_denydatawriter db_denydatawriter db_denydatawriter db_denydatawriter db_denydatawriter db_denydatawriter db_denydatawriter db_denydatawriter db_denydatawriter db_securityadmin	Convidado habilitada para: ESQUINA_VENDAS io à função de banco de dados para: ESQUINA_VENDAS cessadmin ckupoperator tareader tawriter ladmin nydatareader nydatawriter vner curityadmin		☐ TESTE_BACKUP							
Conta Convidado habilitada para: ESQUINA_VENDAS Servidor: DESKTOP-BJNCNTD Associação à função de banco de dados para: ESQUINA_VENDAS db_accessadmin db_backupoperator db_datareader db_datareader db_ddladmin db_denydatareader	io à função de banco de dados para: ESQUINA_VENDAS cessadmin ckupoperator tareader tawriter lladmin rnydatareader rnydatawriter viner curityadmin									
Conta Convidado habilitada para: ESQUINA_VENDAS Servidor: DESKTOP-BJNCNTD Associação à função de banco de dados para: ESQUINA_VENDAS db_accessadmin db_backupoperator db_datareader db_datareader db_ddladmin db_denydatareader	io à função de banco de dados para: ESQUINA_VENDAS cessadmin ckupoperator tareader tawriter lladmin nydatareader nydatawriter vner curityadmin	onexão								
Associação à função de banco de dados para: ESQUINA_VENDAS db_accessadmin db_backupoperator db_datareader db_datawriter db_ddladmin db_denydatareader db_denydatawriter db_securityadmin	cessadmin ckupoperator tareader tawriter ladmin nydatareader nydatawriter ner curityadmin		Conta Convidado habilitada par	a: ESQUINA_VENDAS						
db_accessadmin db_backupoperator db_datareader db_datawriter db_daladmin db_denydatareader db_denydatawriter db_securityadmin db_securityadmin	cessadmin ckupoperator tareader tawriter ladmin nydatareader nydatawriter uner curityadmin	Servidor: DESKTOP-BJNCNTD	Accesiones à función de bonce de	dadaa para: ESOLIINA	VENDAC					
Libert Points Libert Point	ckupoperator tareader tawriter lladmin nydatareader nydatawriter vner curityadmin	Conevão:		dados para. E3QUINA_	VENDAS					
Exibir propriedades da conexã db_datareader db_datawriter db_ddladmin db_denydatareader db_denydatawriter db_denydatawriter db_owner db_securityadmin	tareader tawriter ladmin nydatareader nydatawriter vner curityadmin	3a								
db_datawriter db_ddladmin db_denydatareader db_denydatawriter db_owner db_owner db_securityadmin	tawriter Iladmin nydatareader nydatawriter vner curityadmin	# Evibir propriedades da consul								
db_ddladmin	ladmin nydatareader nydatawriter vner curityadmin	EXIDII propriedades da coriexa								
db_denydatareader db_denydatawriter db_owner db_securityadmin	nydatareader nydatawriter vner curityadmin									
db_denydatawriter db_owner db_securityadmin	nydatawriter vner curityadmin									
ogresso db_owner db_securityadmin	vner curityadmin									
Books db_securityadmin	curityadmin	ogresso								
and the second s	OK Cancelar	Pronto								
da age	OK Cancel	Nagara Pagara	[4] beauti							



Autorizações através do Management Studio

Logon - Novo				_		×
Selecionar uma página Geral		▼ 😯 Ajuda				
Funções de Servidor Mapeamento de Usuário	Usuários	mapeados para este logon:				
▶ Protegíveis▶ Status	Мара	Banco de Dados	Usuário	Esquema Padrão)	
Status	\square	ESQUINA_VENDAS	USUARIO_TESTE			
		master				
		model				
		msdb				
		SISTEMA_A				
		SISTEMA_B				
		SISTEMA_X				
		SISTEMA_Y				
		SISTEMA_Z				
		tempdb				
		TESTE				
		TESTE_BACKUP				
		TESTE2				
Conexão						
Servidor: DESKTOP-BJNCNTD Conexão: sa vi Exibir propriedades da conexã Progresso Pronto	Associação db_ac db_dc db_dc db_dc dc db_dc dc db_dc dc db_dc dc db_dc dc db_dc dc db_dc dc d	ecurityadmin		DAS		
				OK	Can	celar .::



GRANT - CONCEDER

Concede permissões em um protegível.

GRANT <NOME DE PERMISSAO> ON <OBJETO> TO <NOME DO USUARIO>

GRANT OPTION – O usuário pode conceder o acesso para outro acesso

GRANT <NOME DE PERMISSAO> ON <OBJETO> TO <NOME DO USUARIO> WITH GRANT OPTION





REVOKE - REVOGAR

Revoga permissões em um protegível

REVOKE <NOME DE PERMISSAO> ON <OBJETO> TO <NOME DO USUARIO>





DENY - NEGAR

Nega uma permissão a uma entidade de segurança.

DENY <NOME DE PERMISSAO> ON <OBJETO> TO <NOME DO USUARIO>