SENAI SERVIÇO NACIONAL DE APRENDIZAGEM INDUSTRIAL

Microsoft SQL Server

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

SENAI | SERVIÇO NACIONAL DE APRENDIZAGEM INDUSTRIAL

Microsoft SQL Server

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'
```

Autorizações Banco de Dados

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.

Autorizações Banco 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.

Autorizações Banco de Dados

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.

Autorizações Banco de Dados

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.

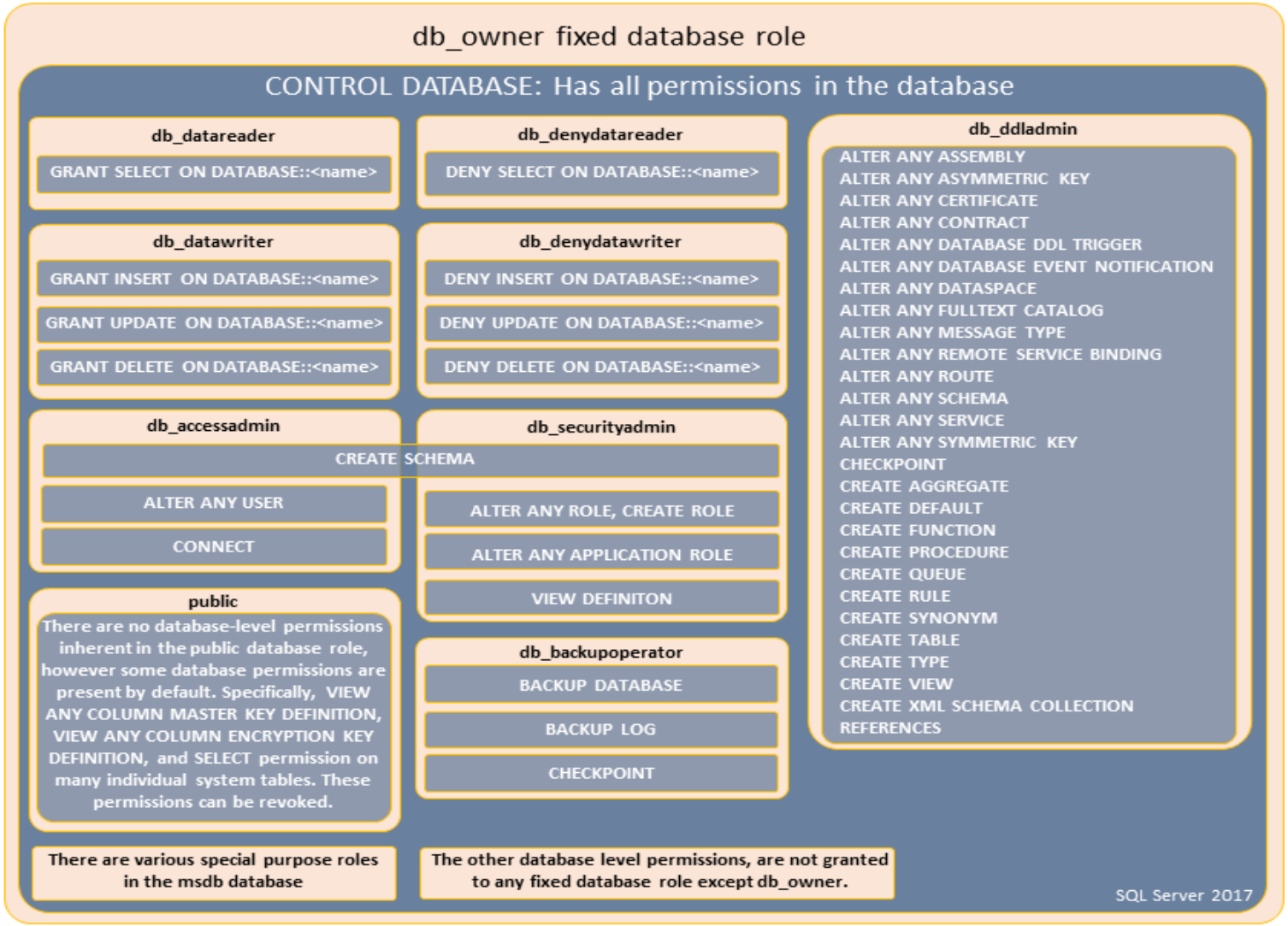
db_denydatareader – Os membros dessa função de banco de dados não podem ler nenhum dado nas tabelas de usuário de um banco de dados.

SENAI SERVIÇO NACIONAL DE APRENDIZAGEM INDUSTRIAL

Microsoft SQL Server

Autorizações Banco de Dados

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



SERVIÇO NACIONAL DE APRENDIZAGEM INDUSTRIAL

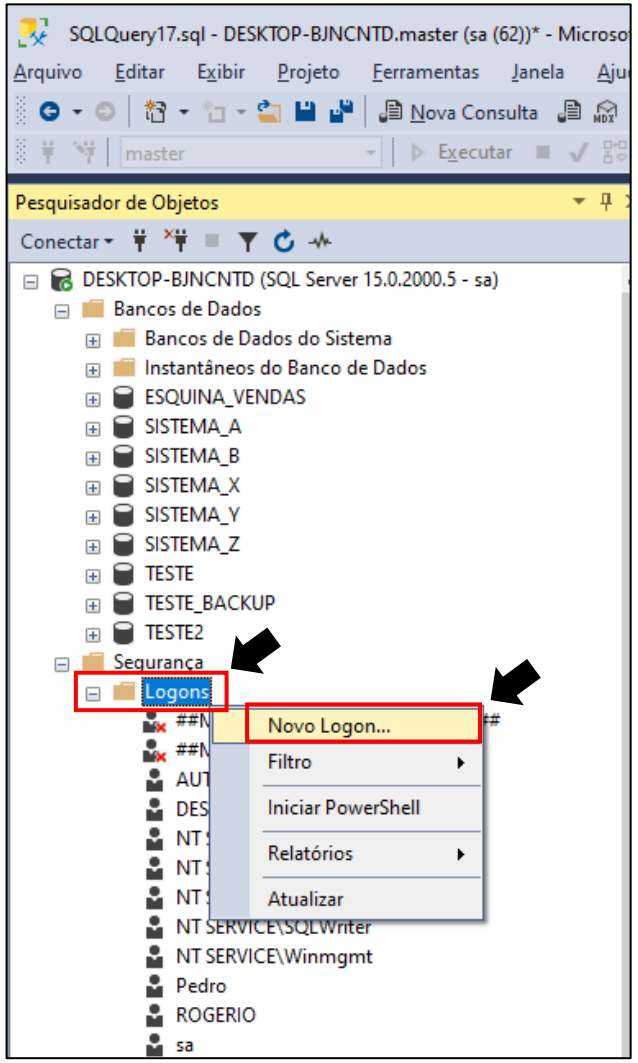
Autorizações Banco de Dados

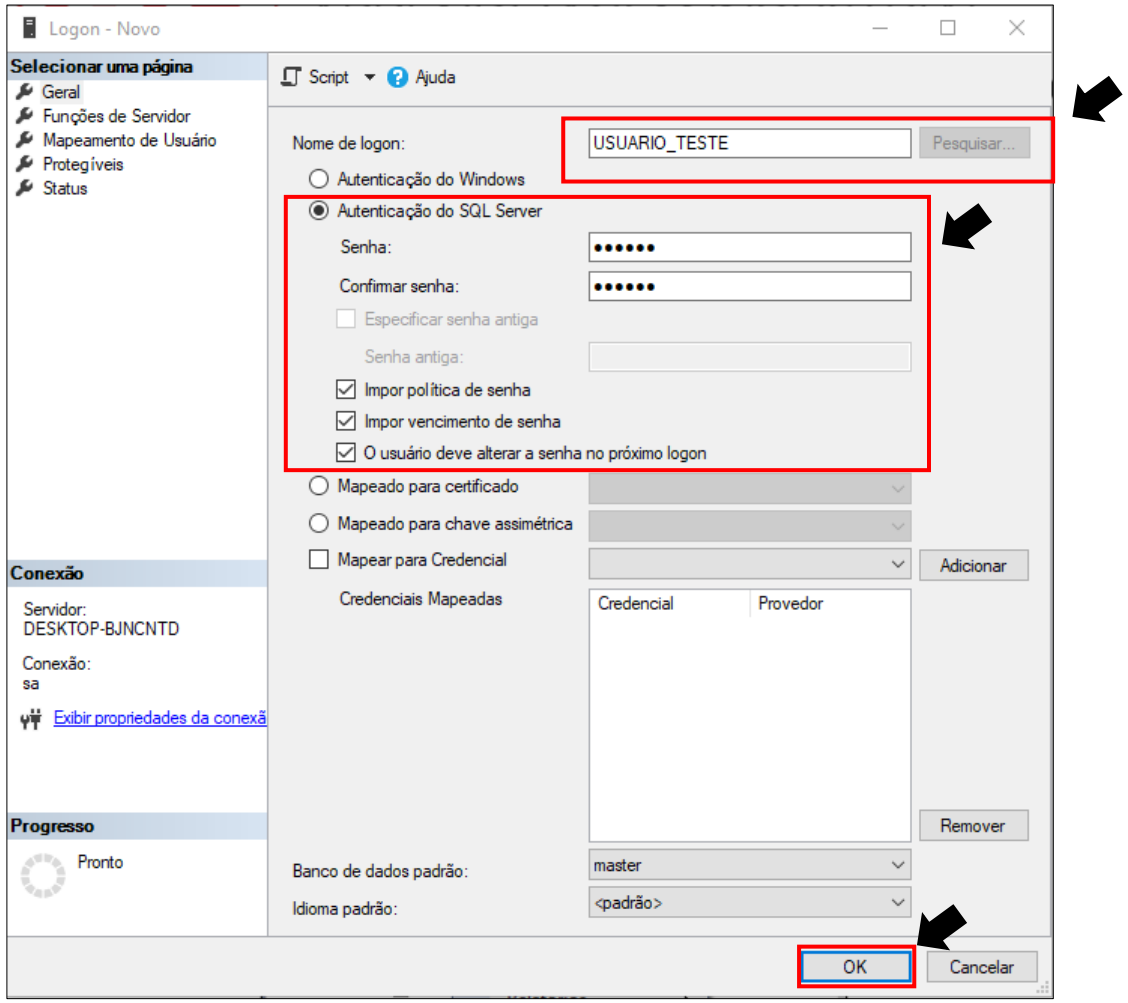
```
USE <NOME DA BASE DA DADOS>

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

Autorizações Banco de Dados

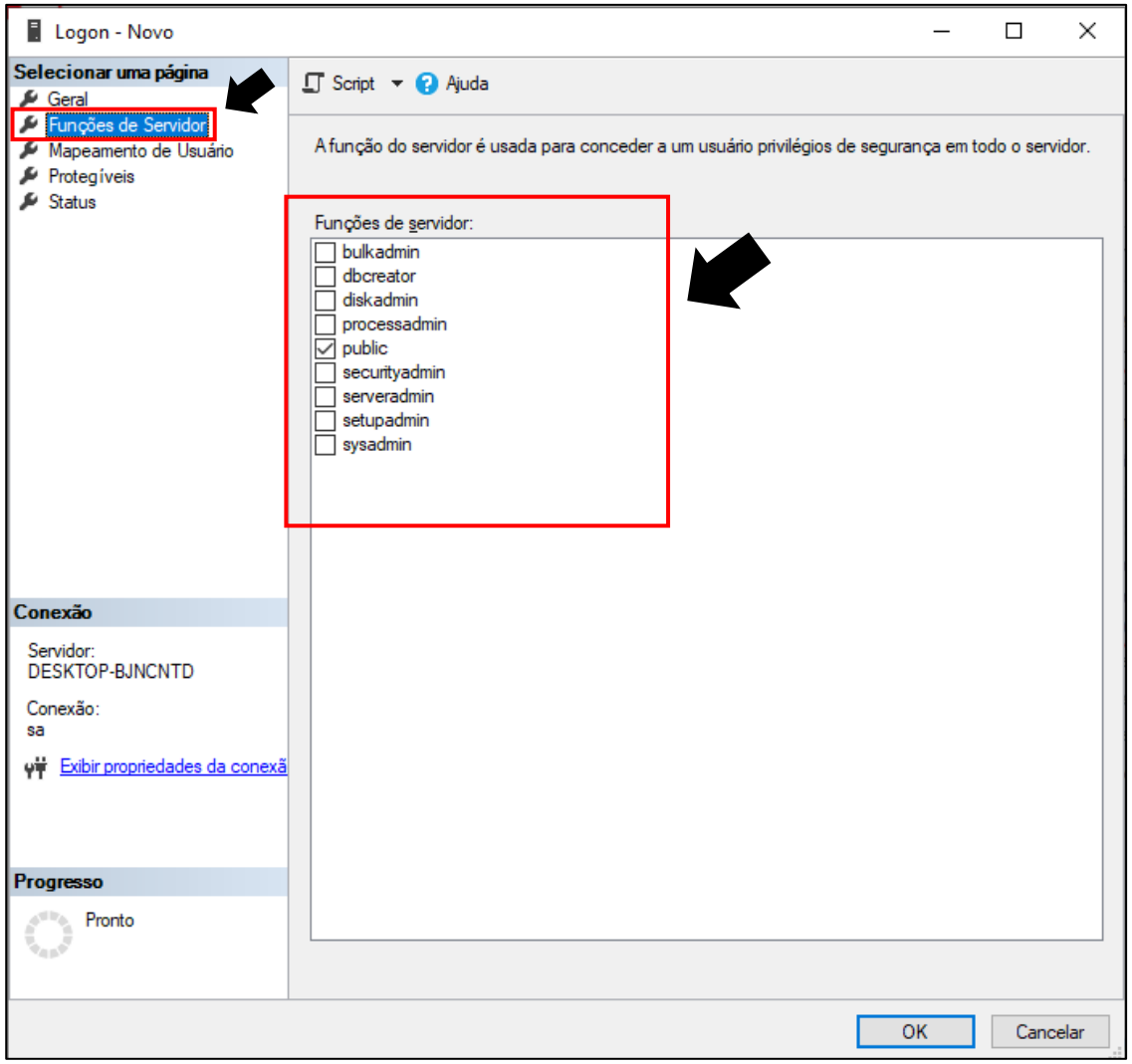
```
ALTER  ROLE [NOME DA REGRA] ADD MEMBER [USUARIO]

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

Autorizações através do Management Studio

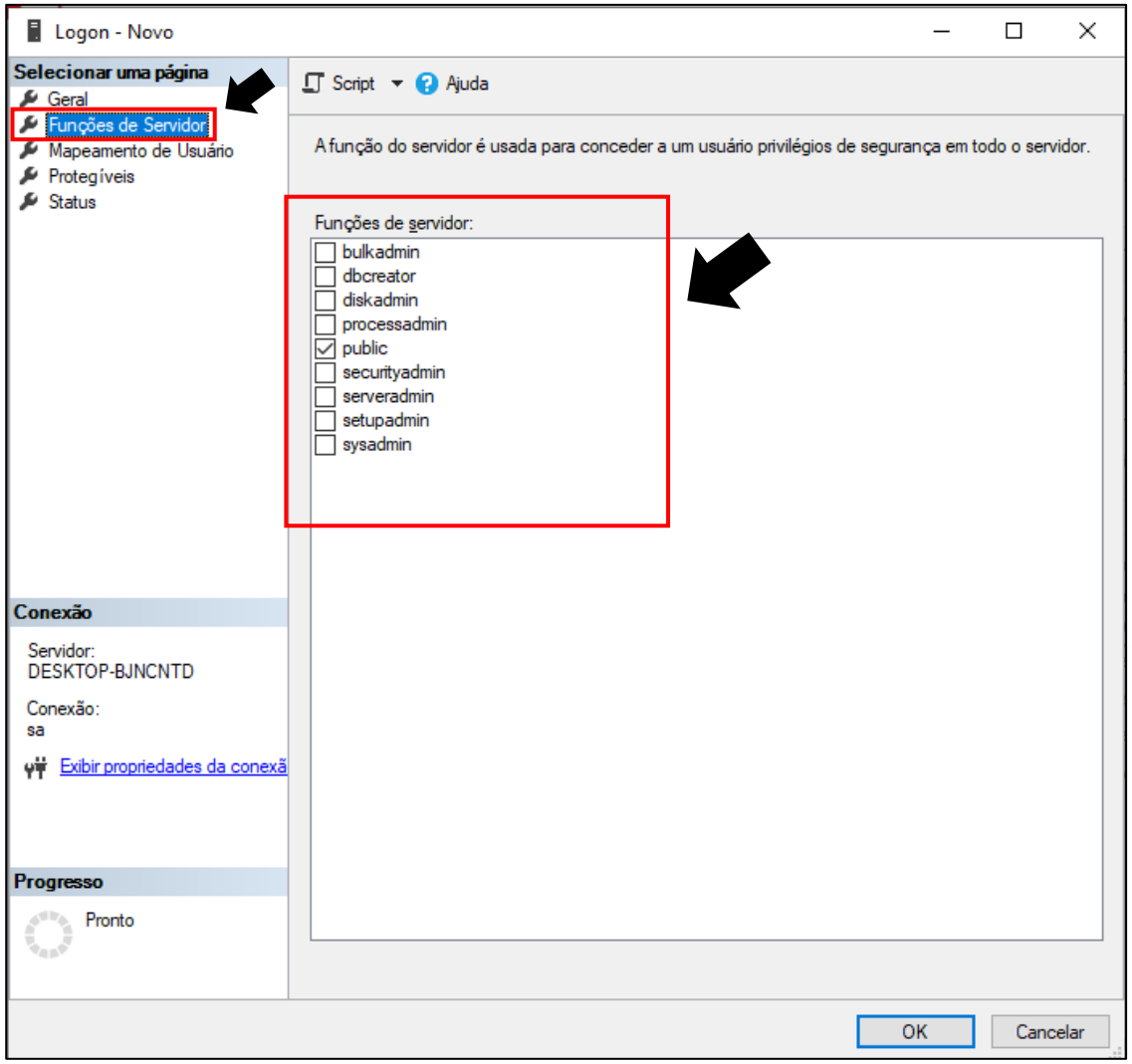




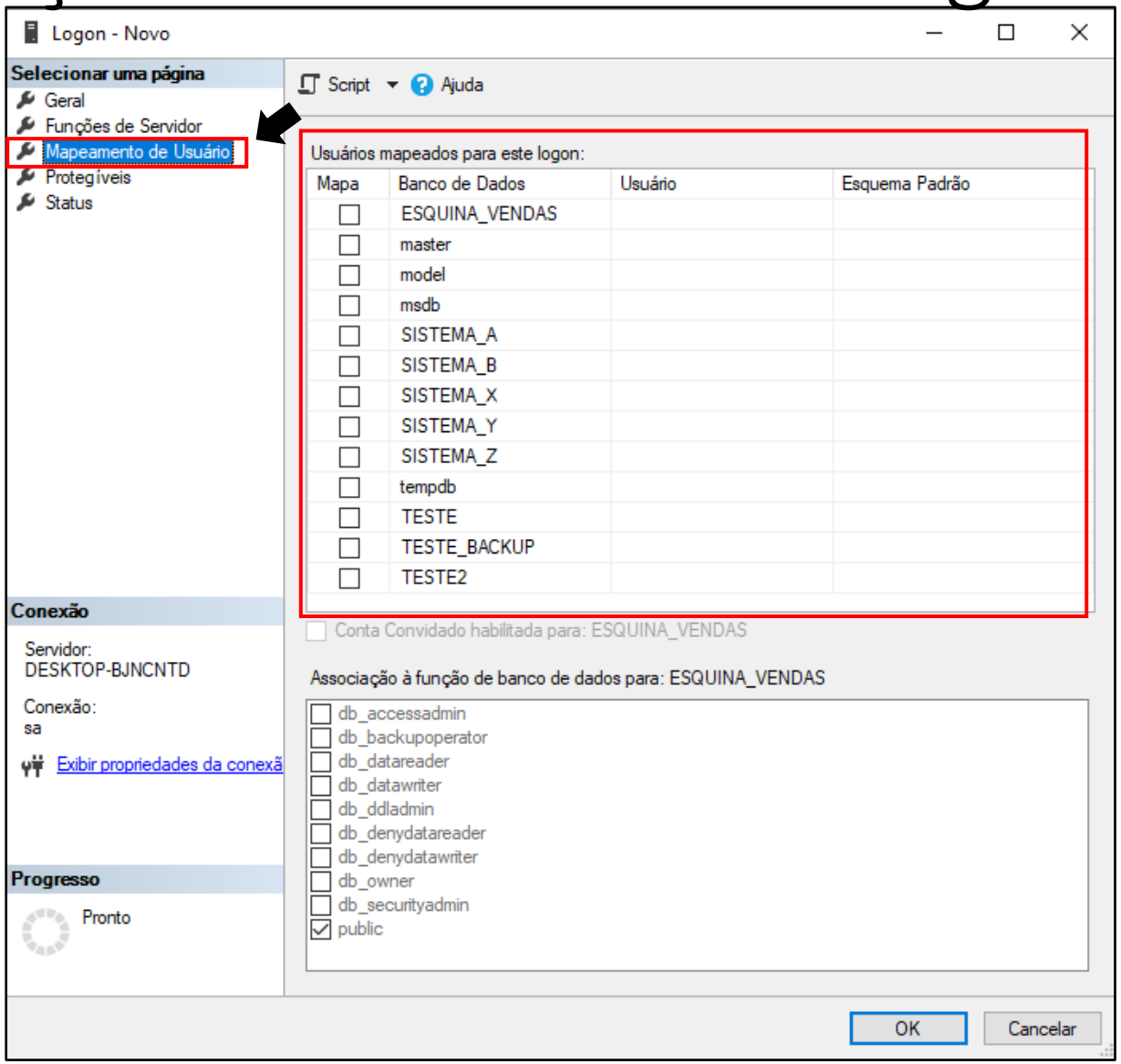
Autorizações através do Management Studio



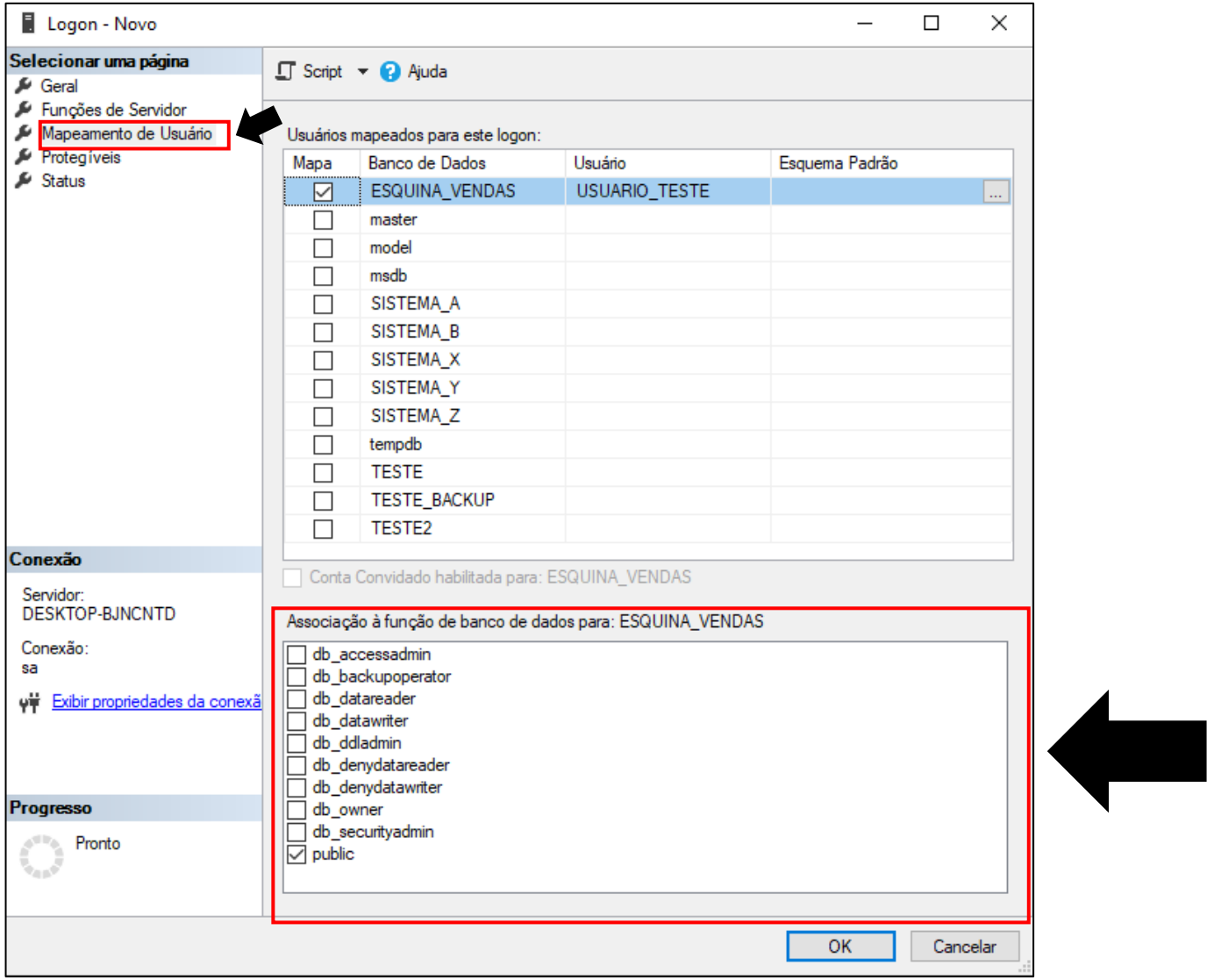
Autorizações através do Management Studio



Autorizações através do Management Studio



Autorizações através do Management Studio



SENAI SERVIÇO NACIONAL DE APRENDIZAGEM INDUSTRIAL

Microsoft SQL Server

Autorizações Banco de Dados

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
```

SENAI SERVIÇO NACIONAL DE APRENDIZAGEM INDUSTRIAL

Microsoft SQL Server

Autorizações Banco de Dados

REVOKE - REVOGAR

Revoga permissões em um protegível

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

SERVIÇO NACIONAL DE APRENDIZAGEM INDUSTRIAL

Autorizações Banco de Dados

DENY - NEGAR

Nega uma permissão a uma entidade de segurança.

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