BANCO DE DADOS

SEGURANÇA

RICARDO SONAGLIO ALBANO

Banco de Dados

Introdução

- De modo simplificado, a segurança no acesso às informações significa que o usuário deve ser capaz de acessar os dados necessários com nível de acesso suficiente (e não mais do que suficiente), para que o usuário realize seu trabalho.
- Através do mecanismo de segurança também evitamos que pessoas não-autorizadas tenham acesso aos dados.

Banco de Dados

Temas

- Uma visão geral da segurança.
- Tipos de segurança disponíveis.
- O papel, criação e administração de Schemas e User Logins.
- Como atribuir permissões aos objetos de um Banco de Dados.
- O que são Roles, como criá-las e administrá-las.
- O planejamento e o gerenciamento da segurança.

Banco de Dados

Modos de controle de segurança

- Logins
- Usuários (User Accounts)
- Papéis (Roles)
- Permissões (Permissions)

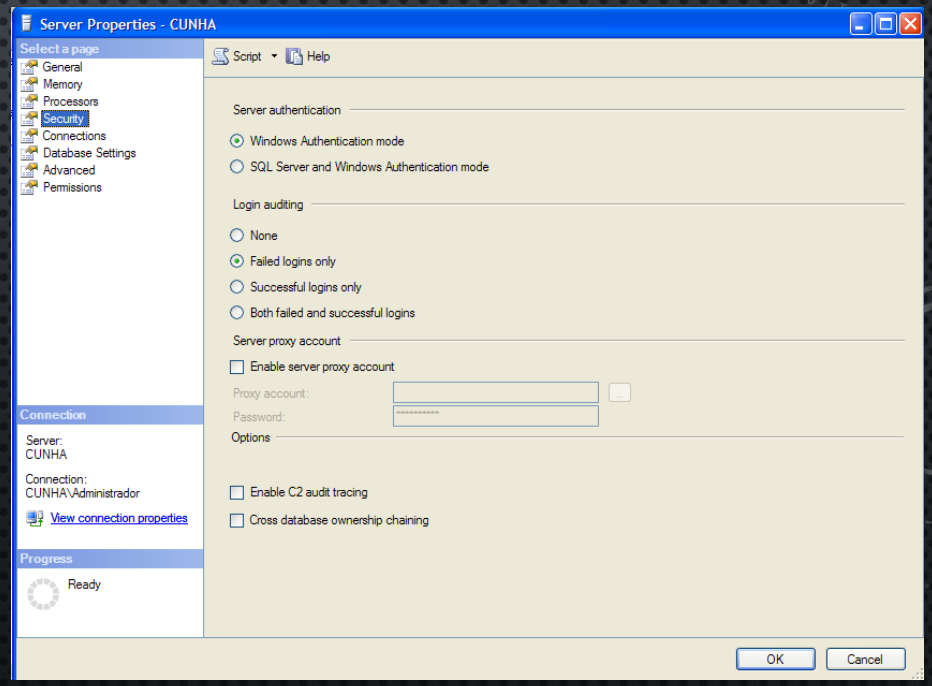
Obs:

- Com esses elementos podemos controlar o acesso aos bancos de dados da instancia e aos seus objetos.

Banco de Dados

Controle de Acesso

- O primeiro passo para que o usuário possa acessar o servidor SQL Server é estabelecer uma conexão com uma instância do servidor SQL Server.
- Esse processo de autenticação pode ser pelo:
  - Windows Authentication;
  - Modo mixed / SQL Server Authentication.



Banco de Dados

Processo de autenticação

- WINDOWS AUTHENTICATION:
  - A autenticação do sistema operacional para acessar a instância do SQL Server;
  - O usuário cadastrado para fazer LOGIN no sistema operacional do Windows poderá fazer conexão com o banco de dados;

- MODO MIXED / SQL SERVER AUTHENTICATION:
  - O administrador de sistema do SQL Server define uma conta de LOGIN e uma senha para o SQL Server.

Banco de Dados

Autenticação de usuário

- Fazer o Logon no SQL Server não garante acesso a um ou mais Banco de Dados.
- O usuário precisa ter permissão de acesso a(os) Banco(s) de Dados e, além do mais, precisa ter permissão de acesso aos objetos do Banco de Dados.
- O fato de definir permissões para cada objeto dá uma grande flexibilidade.
- Alguns usuários devem ter permissão de leitura aos dados; outros de leitura e alteração; outros leitura, alteração e exclusão e assim por diante.

Banco de Dados

Autenticação de usuário

- LOGIN: Dá acesso a instância do SQL Server;
- USUÁRIO: Dá acesso ao banco de dados;

- Observações:
  - LOGIN e o Usuário podem ou não serem vinculados;
  - Usuário sempre vai ter vinculo com um LOGIN;

Banco de Dados

Autenticação de usuário

- Criar Login:

```
create LOGIN nome_do_login with password= ‘senha‘ default_database = nomeBD;
```

- Croar Usuário:

```
create USER nome_do_usuário From nome_do_login with default_schema = [dbo];
```

Banco de Dados

Autenticação de usuário

- Excluir ou Alterar um LOGIN e USUÁRIO:
  - Excluir:
    - login: drop login nome_do_login;
    - usuário: drop user nome_do_usuário;
  - Alterar:
    - login: alter login nome_do_login with password = ‘nova senha‘;
    - usuário: alter user nome_do_usuário with name = joao;

Banco de Dados

Roles – Função / Papel:

- Pode-se utilizar Roles para simplificar a atribuição de permissões de acesso aos objetos do SQL Server.
- São semelhantes ao conceito de grupos de usuários do Windows.
- As Roles podem ser:
  - De servidor: Privilégios administrativos no nível do servidor. São independentes do BD.
  - Banco de dados: Privilégios administrativos no nível do banco de dados.
  - Própria: Pode-se criar Roles próprias para melhor gerenciar os usuários

Banco de Dados

Roles de servidor

Cargo	Permissão
Dbcreator	Criam e alteram os bancos de dados
Diskadmin	Gerenciam os arquivos do disco
Processadmin	Gerenciam os processos do SQL Server
Securityadmin	Gerenciam e auditam os logins do servidor
Serveradmin	Configuram as definições do servidor
Setupadmin	Instalam a duplicação
Sysadmin	Executam qualquer atividade
(bulkadmin)	Executam a instrução BULK INSERT

Banco de Dados

Roles de Banco de dados

Cargo	Permissão
public	Mantém todas as permissões padrão;
db_owner	Executa qualquer atividade de cargo de BD
db_accessadmin	Adiciona ou remove usuários, grupos e cargos do DB
db_ddladmin	Adiciona, modifica ou elimina objetos do BD
db_securityadmin	Atríbuí permissões de objetos e instruções
db_backupoperator	Backup de banco de dados
db_datareader	Lê os dados de qualquer tabela
db_datawriter	Adiciona, altera ou exclui dados de todas as tabelas
db_denydatareader	Não pode ler dados de nenhuma tabela
db_denydatawriter	Não pode alterar dados em nenhuma tabela

Banco de Dados

Roles próprias

- Por exemplo:
  - FinancaConsulta (permissões somente de leitura)
  - FinancaAlteraca (permissões de leitura/Escrita e exclusão)
- Depois, incluímos os usuários que precisam de acesso somente leitura na role FinançaConsulta, e os que precisam de acesso de manutenção no banco, incluímos na role FinançaAlteração.

Banco de Dados

Roles - Procedures:

Procedure	Finalidade
sp_addrole	Adiciona uma nova ROLE
sp_droprole	Exclui uma ROLE
sp_helprole	Fornece informações sobre todas as roles do BD
sp_grantdbaccess	Adicionar um logins à lista de usuários autorizados a acessar um BD
sp_revokedbaccess	retirar a permissão de acesso do usuário a um Banco de Dados
sp_addsvrrolemember	adicionar um usuário a uma role de servidor
sp_dropsvrrolemember	excluir um usuário de uma role do servidor
sp_addrolemember	adicionar um usuário a uma role de Banco de Dados
sp_droprolemember	Para excluir um usuário de uma role de Banco de Dados

Banco de Dados

Roles - Procedures:

- Exemplos:
  - Use Northwind;
  - Exec sp_grantdbaccess ‘Exemplo\user1’;
  - Exec sp_revokedbaccess ‘Exemplo\user1’;
  - Exec sp_addsvrrolemember ‘Exemplo\user1’, ‘sysadmin’;
  - Exec sp_dropsvrrolemember ‘Exemplo\user1’, ‘sysadmin’;
  - Exec sp_addrolemember ‘Consulta’, ‘Exemplo\user1’;
  - Exec sp_droprolemember ‘Consulta’, ‘Exemplo\user1’;

Banco de Dados

Gerenciamento de usuários

- Permissões - DCL – Linguagem de controle de dados:
  - Controlar o acesso dos usuários aos objetos de um banco de dados ou servidor;
  - Previlégios: Connect, create, select, insert, update, delete, execute
  - Podem ser: por usuário ou por objeto;
  - Comandos:
    - GRANT: Concede permissão para executar a tarefa relacionada;
    - DENY: Nega permissão para executar tarefas;
    - REVOKE: remove a permissão.

Banco de Dados

Gerenciamento de usuários

- Exemplo por usuário:
  - Grant select to nome_do_usuário;
  - Deny insert to nome_do_usuário;
  - Revoke create table to nome_do_usuário;
- Exemplo por objeto:
  - Grant select ON ESTADO to nome_do_usuário;
  - Deny insert ON ESTADO to nome_do_usuário;
  - Revoke select ON ESTADO to nome_do_usuário;

Banco de Dados

Gerenciamento de usuários

- Usando procedures do SQL Server:

Comando	Utilizado
Sp_grantlogin	Logins do Windows. Pode-se adicionar usuários ou grupos. Utilizar o formato DOMINIO\nome ou SERVIDOR\nome.
Sp_addlogin	Para adicionar logins do SQL Server.
sp_revokelogin	Remove logins do SQL Server.
sp_denylogin	Nega a permissão ao usuário.
sp_droplogin	Remove o usuário

Obrigado por sua atenção!

Ricardo Sonaglio Albano