Sécurité SQL Server

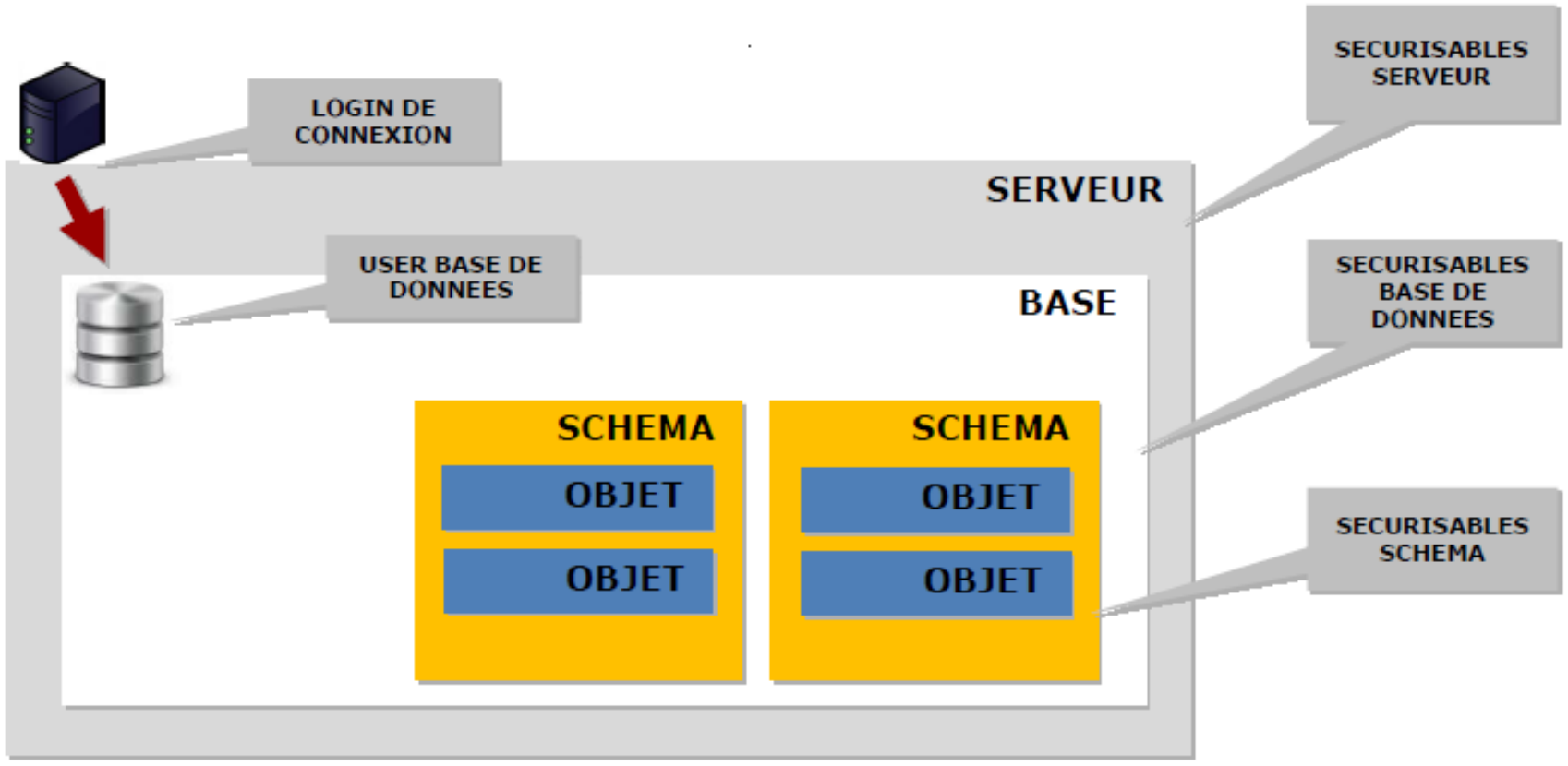
Authentification SQL Server

- Les entités de sécurité : compte de sécurité qui dispose d'un accès au serveur de données SQL.

- Les sécurisables : objets gérés par le serveur (serveur, base, schema)

- Les autorisations : sont accordées aux entités de sécurité afin de pouvoir travailler avec les sécurisables.

Architecture de la sécurité d'accès



Les modes d’authentfication

- Mode d’authentification Windows
  - Utilisateurs authentifiés par Windows
  - L’accès des utilisateurs se fait via une connexion mappée à leur compte Windows
  - Mode d’authentification par défaut
- Mode d’authentification mixte (SQL Server et Windows)
  - Les utilisateurs connectés via une connexion Windows déclarés sous SQL Server sont validés
  - Les utilisateurs connectés via un compte non Windows déclarés sous SQL Server sont validés

Les entités de sécurités

- Configuration des identifiants SQL Server
  - Identifiant = accès des utilisateurs à SQL Server

- Création d'un identifiant (authentification Windows)
  - Syntaxe

CREATE LOGIN [<domaine>\<nom_connexion>] FROM WINDOWS
[WITH DEFAULT_DATABASE=<base_de_données> | DEFAULT_LANGUAGE=<langue>

- Création d'un identifiant (authentification SQL Server)
  - Syntaxe

CREATE LOGIN <nom_connexion> WITH PASSWORD=<mot_de_passe>
[MUST_CHANGED] |, DEFAULT_DATABASE=<base_de_donnes> |,
DEFAULT_LANGUAGE=<langue> | , CHECK_EXPIRATION={ ON | OFF} |
CHECK_POLICY={ ON| OFF} | , [CREDENTIAL=<nom_credit>

Les entités de sécurités

Les vues systèmes :

- sys.server_principals : Entités de sécurité définis au niveau serveur.

- sys.sql_logins : Liste des connexions au niveau serveur.

Les entités de sécurités

- Modification
  - Syntaxe

    ALTER LOGIN <nom_utilisateur> WITH <option>

- Désactivation
  - Syntaxe

    ALTER LOGIN <nom_utilisateur> DISABLE

- Suppression
  - Syntaxe

    DROP LOGIN <nom_utilisateur>

    DROP LOGIN [domaine\nom_utilisateur]

Les utilisateurs de base données

- Création d'un utilisateur de base de données
  - Syntaxe

    CREATE USER <utilisateur> FOR LOGIN <login> WITH DEFAULT_SCHEMA=<schema>
- Modification d'un utilisateur de base de données
  - Syntaxe

    ALTER USER <utilisateur> WITH NAME=<new_nom>, DEFAULT_SCHEMA=<schema>
- Suppression d'un utilisateur de base de données
  - Syntaxe

    DROP USER <utilisateur>

Les utilisateurs de base données

- Les vues systèmes
  - sys.database_principals
- Savoir qui est connecté
  - Procédure sp_who

Gestion des droits sous SQL Server

- Plusieurs niveau d'attribution des privilèges
  - Au niveau serveur
  - Au niveau base
  - Au niveau schéma
  - Au niveau des objets
- Deux types de droits au niveau base
  - Droits d'utilisation d'instructions
  - Droits sur les objets

Gestion des privilèges

- GRANT pour l'attribution des privilèges
- REVOKE pour retirer des privilèges
- DENY pour interdire l'utilisation d'un privilège

Les privilèges d'utilisation des instructions

- CREATE DATABASE pour créer une base de données
- CREATE PROCEDURE pour créer une procédure stockée
- CREATE TABLE pour créer une table
- BACKUP DATABASE pour réaliser une sauvegarde
- CREATE DEFAULT
- CREATE RULE pour créer un rôle
- CREATE VIEW pour créer une vue
- BACKUP LOG pour réaliser une sauvegarde du journal des transactions

Gestion des privilèges

- La commande GRANT

GRANT <nom_privilege> [, ...] TO <utilisateur> > [, ...] [WITH GRANT OPTION]

- La commande REVOKE

REVOKE [GRANT OPTION FOR] <nom_privilege> [, ...] FROM <utilisateur> [, ...] [CASCADE]

- La commande DENY

DENY<nom_privilege> [, ...] TO <utilisateur> [, ...] [CASCADE]

Les privilèges sur les objets

- Tables
  - SELECT, INSERT, UPDATE, DELETE
- Procédures
  - EXECUTE

Les privilèges sur les objets

- La commande GRANT

GRANT { ALL | <nom_privilege>[(colonne [, ...]] [, ...]) } ON <nom_objet> TO <utilisateur> [, ...] [WITH GRANT OPTION]

- La commande REVOKE

REVOKE [GRANT OPTION FOR] { ALL | <nom_privilege>[(colonne [, ...]] [, ...]) } ON <nom_objet> [(colonne [, ...]] [, ...]) FROM <utilisateur> [, ...] [CASCADE]

- La commande DENY

DENY { ALL | <nom_privilege>[(colonne [, ...]] [, ...]) } ON <nom_objet> [(colonne [, ...]] [, ...]) TO <utilisateur> [, ...] [CASCADE]

Droits au niveau base de données

- La commande GRANT

GRANT <nom_privilege_base> [, ...] TO <utilisateur> [, ...] [WITH GRANT OPTION] [AS [<groupe> | <role>]

- La commande REVOKE

REVOKE [GRANT OPTION FOR] <nom_privilege_base> [, ...] FROM <utilisateur> [, ...] [CASCADE]

- La commande DENY

DENY <nom_privilege_base> [, ...] TO <utilisateur> [, ...] [CASCADE]

Gestion des rôles

- Ensemble de privilèges (regroupement de privilèges)
- Existe à trois niveaux dans l'architecture SQL Server
  - Au niveau serveur
  - Au niveau base
  - Au niveau application

- Deux types de rôles
  - Rôles utilisateur (au niveau base et application)
  - Rôles fixes (au niveau base et serveur)

Les rôles au niveau serveur (prédéfinis)

- sysadmin super administrateur de l'instance
- serveradmin configuration des paramètres au niveau serveur
- setupadmin ajout/suppression des serveurs liés et éxecution de certaines procstocks
- securityadmin gestion des connexions d'accès au serveur
- processadmin gestion des traitements sous SQL Server
- dbcreator création et modification des bases de données
- diskadmin gestion des fichiers sur disque
- bulkadmin exécution de l'instruction BULK INSER

Gestion des rôles au niveau base de données

- Les rôles prédéfinis
  - db_owner propriétiaire de la base de données
  - db_accessadmin ajoute ou supprime des utilisateurs à la base de données
  - db_datareader SELECT sur toutes les tables de la base de données
  - db_datawriter INSERT, UPDATE, DELETE sur toutes les tables de la base de données
  - db_ddladmin ordre DDL (CREATE, ALTER)
  - db_securityadmin gestion des rôles, des autorisations sur les instructions et les objets
  - db_backupoperator réalisation de sauvegarde de la base de données
  - db_denydatareader pour interdire le SELECT/INSET sur toute la base
  - db_denydatawriter pour interdire le INSERT, UPDATE, DELETE sur toute la base

Gestion des rôles au niveau base de données

- Les rôles utilisateurs
  - Gestion des rolês utilisateurs
    - CREATE ROLE <nom_role> AUTHORIZATION <nom_propriétaire>
    - sp_addrolemember ajouter un membre au rôle
    - sp_droprolemember retire un membre au rôle
    - DROP ROLE <nom_role>