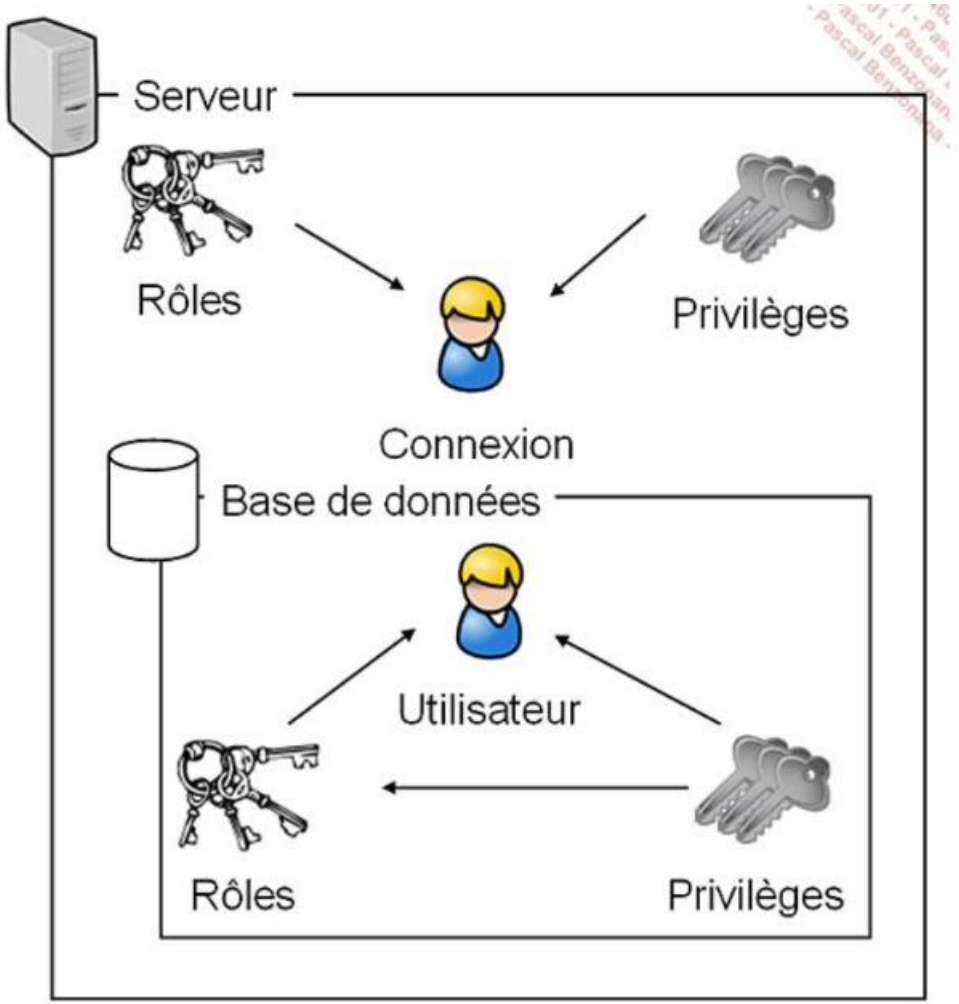
GESTION DES DROITS DANS SQL SERVER

Quelques définitions

- Principal de sécurité : personnes ou groupes de personnes en général qui utilisent SQL Server et autorisés à prendre des mesures
- Exemple :
  - « server principal » (ou login),
  - « database principal » (ou user)

- Utilisateur sa : administrateur

Droits dans SQL Server

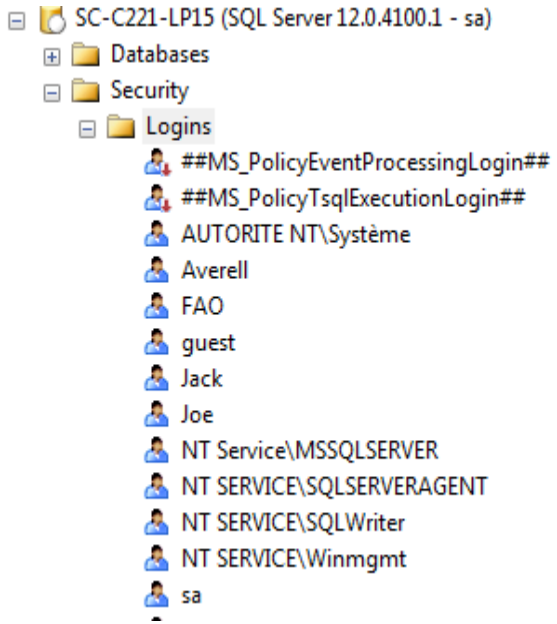


Création d'un utilisateur (1)

1) Créer un login (une connexion)
2) Créer un user

Comment créer un login?

- Avec l'interface graphique dans MS SQL Server Management Studio



- Ou par script :

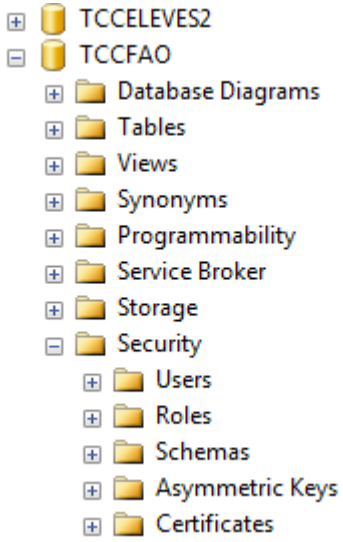
```
CREATE LOGIN <login_name>
WITH PASSWORD = '<password>' MUST_CHANGE,
CHECK_EXPIRATION = ON, CHECK_POLICY = ON, DEFAULT_DATABASE
=TCCFAO
```

Plus de paramètres sur
https://msdn.microsoft.com/en-us/library/ms189751.aspx

Création d'un utilisateur (2)

- Comment créer un user basé sur un login ?

- Avec l'interface graphique dans MS SQL Server Management Studio



- Par script :

```
CREATE USER user_name
FROM  LOGIN login_name
```

Plus de paramètres et d'informations sur https://msdn.microsoft.com/en-us/library/ms173463.aspx

Exemple

- CREATE LOGIN test WITH PASSWORD = 'Tst_12@45' MUST_CHANGE, CHECK_EXPIRATION = ON, CHECK_POLICY = ON, DEFAULT_DATABASE = TCCFAO

- CREATE USER TCCtest FOR LOGIN test

Droits d’accès aux données

- Propriétaire de tables et vues créées par l’utilisateur
- Possibilité de donner aux autres utilisateurs de la base le droits de manipuler nos données
- Possibilité de passer le droit cité précédemment à d’autres utilisateurs
- Possibilité de supprimer les droits transmis

- GRANT : accorde une autorisation
- REVOKE : révoque une autorisation
- DENY : refuse une autorisation. A priorité sur l’autorisation.

GRANT – REVOKE

GRANT <permission> [,...n] ON object_name [(column [,...n])] TO <database_principal> [,...n] [WITH GRANT OPTION]

Exemples :

GRANT SELECT, INSERT, ALTER ON booking TO TCCtest

GRANT SELECT on [user] to TCCtest with grant option -- TCCtest peut passer les droits

use TCCFAO

grant SELECT on DATABASE::TCCFAO to TCCtest

https://msdn.microsoft.com/fr-ch/library/ms188371.aspx

GRANT – REVOKE

REVOKE <permission> [,...n] ON object_name [(column [,...n])] TO <database_principal> [,...n]

Exemple : REVOKE ALTER on booking to TCCtest

https://msdn.microsoft.com/fr-ch/library/ms187719.aspx

DENY

DENY <permission> [,...n] ON object_name [(column [,...n])] TO <database_principal> [,...n] [CASCADE]

Exemples :

DENY SELECT ON [user] to TCCTest CASCADE

DENY SELECT ON booking to TCCTest

ROLE DE BASE DE DONNEES

Similaires aux ***groupes*** du système d'exploitation Microsoft Windows

Pour créer un rôle de base de données :
CREATE ROLE role_name

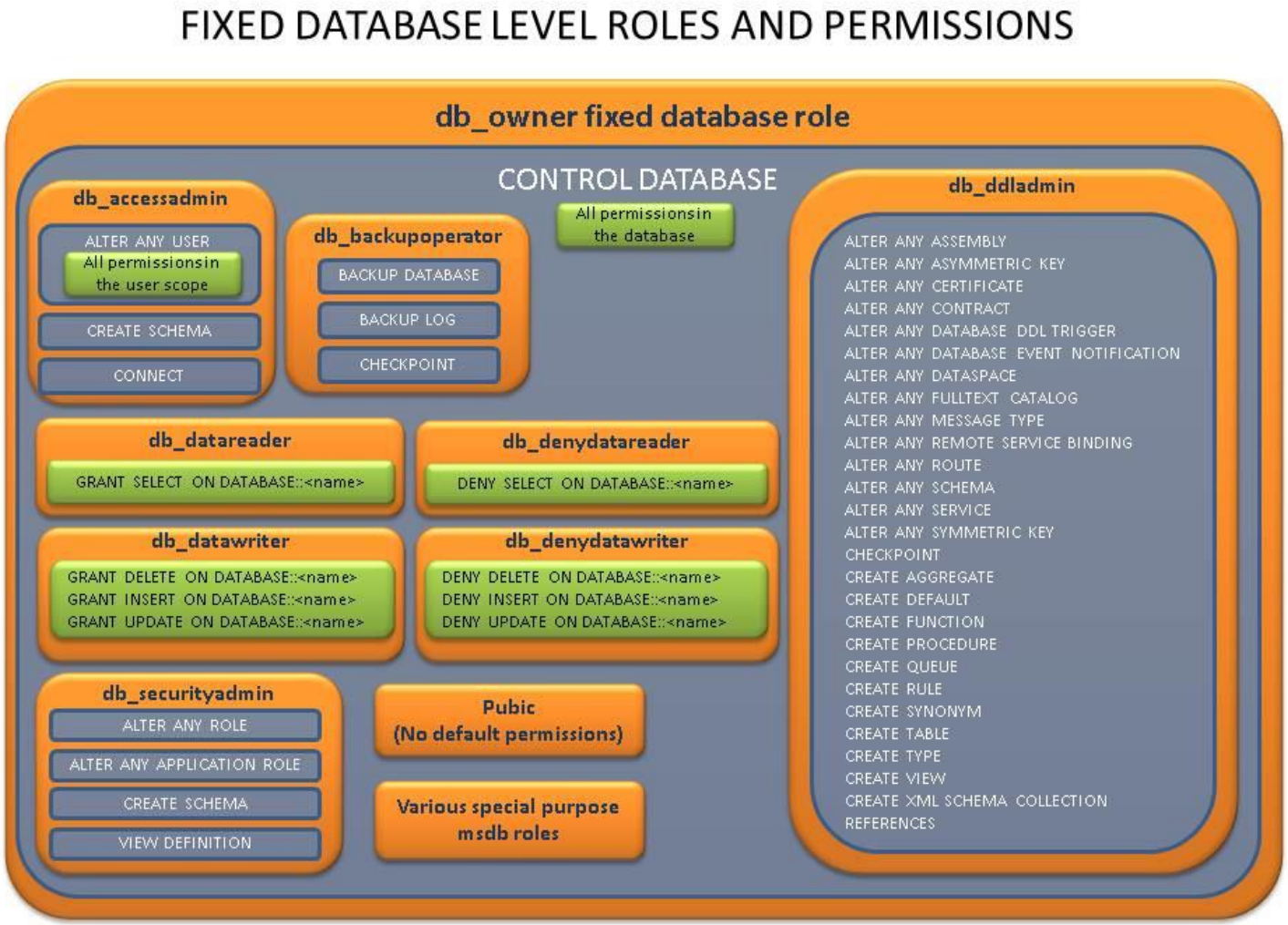
Pour ajouter / supprimer un membre, utilisez les options ADD MEMBER et DROP MEMBER de l'instruction ALTER ROLE.

ALTER ROLE role_name { ADD MEMBER database_principal | DROP MEMBER database_principal | WITH NAME = new_name }

Exemples :
CREATE ROLE Sales;
ALTER ROLE Sales ADD MEMBER Barry;
ALTER ROLE Sales DROP MEMBER Barry;

https://msdn.microsoft.com/fr-ch/library/ms189121.aspx

Rôles existants



Autorisations minimums

- Suivre toujours le principe d’accorder le minimum de droits nécessaires

- Accorder le minimum de permissions necessaire à un utilisateur pour accorder une tâche donnnée

Permissions basées sur les rôles

Role-Based Permissions
Granting permissions to roles rather than to users simplifies security administration. Permission sets that are assigned to roles are inherited by all members of the role. It is easier to add or remove users from a role than it is to recreate separate permission sets for individual users. Roles can be nested; however, too many levels of nesting can degrade performance. You can also add users to fixed database roles to simplify assigning permissions.
You can grant permissions at the schema level. Users automatically inherit permissions on all new objects created in the schema; you do not need to grant permissions as new objects are created.