Synthèse Labo Sécurité des données

Créer une base de données et l'utiliser :

CREATE< DATABASE pokemon_db

GO

use pokemon_db

Créer une table :

CREATE TABLE <nom de la table> (

<nom colonne> <type colonne> <contrainte>,

…… …….. ……

) ;

<type colonne> → int,float ,varchar(<number>),date,datetime(date et heure),time…

<contrainte> → PRIMARY KEY, FOREIGN KEY REFERENCES <table voisine>(<colonne>), NOT NULL, UNIQUE, IDENTITY(<nb>,<nb>)(génère automatiquement des numéros séquentiels pour l'insertion dans une table – ex : IDENTITY(1,1)→valeur qui va commencer par 1 et qui aura un pas de 1),…

Modifier la structure d'une table :

- ALTER TABLE <table> ADD (<nom colonne> <type> <contrainte>); → ajouter une colonne
- ALTER TABLE<table> ALTER COLUMN <nom colonne> <type>); → change le type d'une colonne
- ALTER TABLE <table> DROP COLUMN <nom colonne>; → supprime une table

Renommer une table : EXEC sp_rename '<nom table>', '<nouveau nom table>';

Renommer une colonne : EXEC sp_rename '<nom table<nom colonne>.', '<nouveau nom colonne>', 'COLUMN';

Vider une table : TRUNCATE TABLE <nom table>

Supprimer une table : DROP TABLE <nom table>

Afficher les éléments d'une table :

```
SELECT  * | [ DISTINCT ] <expressions> [ <alias> ] , ...
FROM    <table(s)>
[ WHERE  <condition(s)> ]
[ GROUP BY  <colonne>, …  ] ;
[ HAVING  <condition(s) de groupe> ] ;
[ ORDER BY {<colonne> | <expr> | <alias> [ ASC | DESC ] , … } ] ;
```

Expressions :

- → affiche toutes les colonnes
- DISTINCT <nom colonne> → Affiche une seule fois chaque valeur contenue dans la colonne
- AVG(<nom colonne>) ALIAS avg FROM <table> → affiche la moyenne des valeurs de la table et renomme la colonne à l'affichage
- COUNT(<nom colonne1>) FROM <table> GROUP BY <colonne2> HAVING <nb_association> > 10 : affiche par colonne 2 le nombre de colonne 1 associés si la colonne 2 a plus de 10 associations avec colonne 1

Conditions :

Opérateur	Description
=	Égale
<>	Pas égale
!=	Pas égale
>	Supérieur à
<	Inférieur à
>=	Supérieur ou égale à
<=	Inférieur ou égale à
IN	Liste de plusieurs valeurs possibles
BETWEEN	Valeur comprise dans un intervalle donnée (utile pour les nombres ou dates)
LIKE	Recherche en spécifiant le début, milieu ou fin d'un mot.
IS NULL	Valeur est nulle
IS NOT NULL	Valeur n'est pas nulle

WHERE LOWER(<colonne>)='<texte en minuscule>'

ORDER BY <colonne>,… [ASC/DESC]

Jointures exemple :

```
SELECT DISTINCT POKEMON.* FROM POKEMON
INNER JOIN CAPTURED
ON POKEMON.POKEDEX_NUMBER =
CAPTURED.POKEMON_NUMBER
WHERE CAPTURED.CAPTURATION_DATE > '01-01-2021';
```

Insérer une valeur dans une colonne d'une table :

Exemple : INSERT INTO [dbo].[Person] ([name],[age],[job]) VALUES ('bastien','26','Student') ;

```
INSERT
INTO        <table>   [ ( <colonnes> ) ]
VALUES      ( <valeurs> );
```

Modifier une valeur dans une colonne d'une table :

```
UPDATE      <table>
SET         <colonne> = <valeur>, ...
[ WHERE     <condition> ] ;
```

Supprimer une valeur dans une colonne d'une table :

```
DELETE
[ FROM ]    <table>
[ WHERE     <condition> ] ;
```

Créer une vue :

```
CREATE VIEW <schema>.<view_name>
AS
SELECT ...
```

Supprimer toutes les données d'une table :

```
TRUNCATE TABLE dbo.Nums;
```

Faire un backup d'une base de données → 2 Solutions

Clic droit sur Base de données → Taches → Sauvegarder → Choisir le type de sauvegarde → Choisir le chemin du fichier contenant la sauvegarde en supprimant le précédant

Exécuter la requête ci-dessous :

```
USE master;
GO
BACKUP DATABASE AdventureWorks2014 TO DISK='c:\Backup\Manip8.bak';
```

Restaurer une BD → 2 solutions :

- Clic droit sur base de données → Restaurer → Cocher support et choisir le fichier contenant la BD → Nommer la BD comme on le souhaite → ok
- Exécuter la requête ci-dessous :

```
USE master;

GO

RESTORE DATABASE LambotL FROM DISK = 'D:\Backup\LL.bak'
```

Générer un script de restauration → Clic droit sur la base de données que le script doit restaurer → Taches → Générer des scripts → Enregistrer comme fichier de script

Pour l'utiliser on doit simplement le déplacer de la fenêtre de l'explorateur de fichier sur une nouvelle requête vide.

Créer une sauvegarde chiffrée :

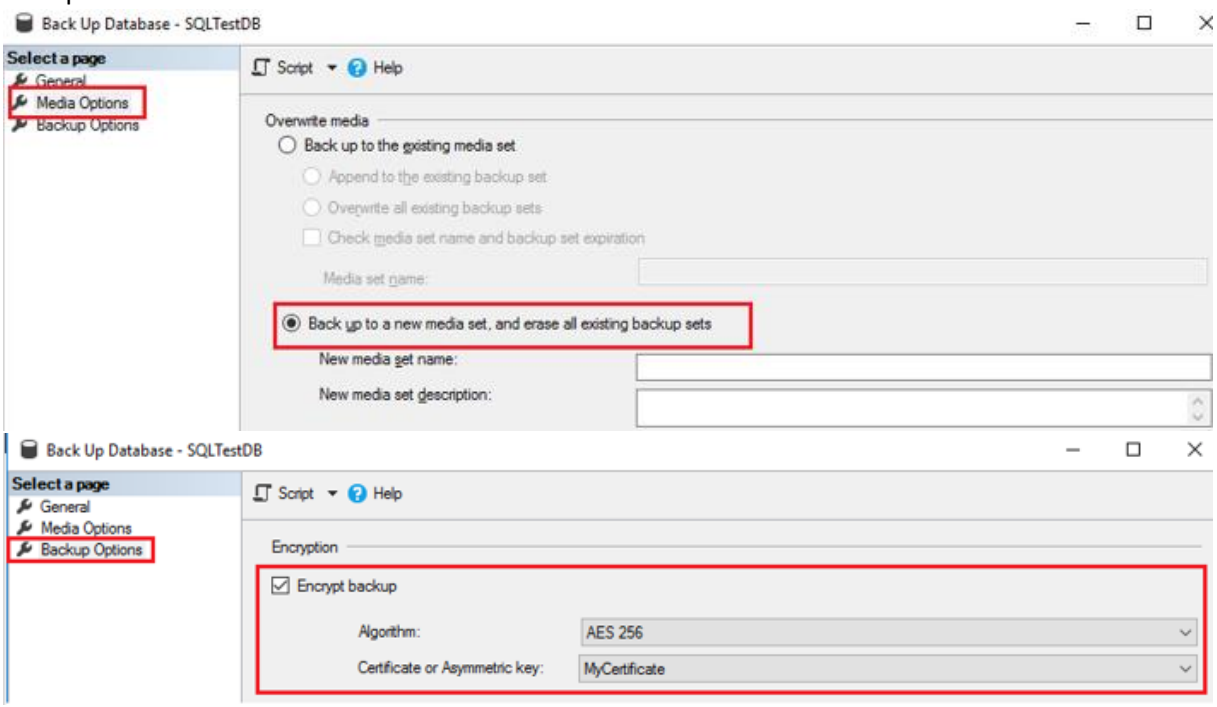
- Exécuter la requête suivant pour créer une clé principale de BD et un certificat

```
-- Create the master key
CREATE MASTER KEY ENCRYPTION BY PASSWORD = '23987hxJ#KL95234nl0zBe';

-- If the master key already exists, open it in the same session that you create the certificate (see next step)
OPEN MASTER KEY DECRYPTION BY PASSWORD = '23987hxJ#KL95234nl0zBe'

-- Create the certificate encrypted by the master key
CREATE CERTIFICATE MyCertificate
WITH SUBJECT = 'Backup Cert', EXPIRY_DATE = '20201031';
```

- Puis clic-droit sur la BD → Sauvegarder → Dans général, nous faisons comme d'habitude mais pour le reste nous faisons ceci :



Restaurer la sauvegarde chiffrée se fait exactement de la même manière qu'une sauvegarde basique.

Réaliser une sauvegarde différentielle → Il faut simplement cocher différentielle dans le type de sauvegarde

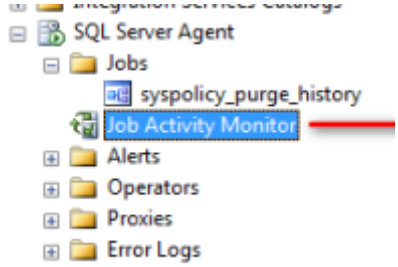
Restaurer une sauvegarde différentielle → il faut sélectionner la sauvegarde différentielle et la sauvegarde complète

Il ne faut pas oublier de démarrer SQL Server Agent avant de créer un job.

Automatisation avantages :

- Moins de tâches administratives
- Plus grandes fiabilité des tâches courantes (- de risque d'oubli)
- Pas de copies des mauvaises données
- Pas d'erreur dans le nom de fichier de sauvegarde

Le job activity monitor permet de voir les travaux :



Créer un job (qui insert une valeur dans une table toutes les 10 secondes dans cet exemple)→ SQL server Agent →Travail → nouveau → Dans général, on met le nom et l'owner (par défaut c'est notre utilisateur mais si on a des problèmes de droits, il faut aller mettre sa) → Dans Etapes, on va ajouter la requête qui va insérer la valeur dans la table(exemple) → Dans planifications, on va ajouter une nouvelle planification qui est 'Toutes les 10 secondes' → puis on peut cliquer sur OK

Après avoir créé le job, il faut le démarrer.

Exemple étape de job qui supprime un enregistrement de la table Person chaque minute :

```
DELETE FROM Person WHERE idPerson =(SELECT MAX(idPerson) FROM Person);
```

Démarrer SQL Profiler → Outils(en haut) → SQL Server Profiler

Dans SQL Profiler → RPC = Job

Pour afficher le plan d'exécution d'une requête (Query Analyzer) → sélectionner la requêtre → clic-droit → afficher le plan d'exécution estimé

Afficher les roles serveurs → EXEC sp_helpsrvrole

Voici les roles serveurs :

- **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

Il y a 3 niveaux de rôles ou d'autorisations : Niveau serveur, niveau base de données et niveau application. Il y a 2 types : utilisateurs et fixes.

Les autorisations données à un user au niveau serveur ont un impact sur l'ensemble des bases de données alors que les autorisations au niveau de base de données ont un impact uniquement sur cette BD.

Voici les roles de base de données :

- **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

Les connexions ou login permettent d'arriver jusqu'au serveur et le serveur mappe ce login à un user.

Changer le mode d'authentification : clic-droit sur le serveur → propriétés → sécurité

Créer un utilisateur de type SQL SERVER avec T-SQL :

- CREATE LOGIN <nom user> WITH PASSWORD = '<mdp>';

Créer un login Windows sur base d'un utilisateur local :

- Server → sécurité → connexion → nouvelle connexion → authentification Windows → rechercher → Trouver le nom de l'utilisateur local

Ajouter un utilisateur local dans un role en T-SQL :

- EXEC master.. sp_addsrvrolemember '<nom ordinateur>\<nom user>','<nom du rôle>';

Ajouter un utilisateur SQL dans un role en T-SQL :

- sp_addsrvrolemember '<nom user>', '<rôle>';

Ajouter un user dans rôle avec l'interface graphique :

- Serveur → connexion →clic droit sur l'user →Propriété →roles du serveur →cocher

Créer un rôle :

- Serveur → Sécurité → rôles serveur → nouveau rôle
- CREATE SERVER ROLE <nom du rôle>;

Permettre à ce rôle d'accorder une permission :

- général → cocher le serveur dans serveurs → trouver et cocher la permission
- grant <permission>(ex :create any database) to <nom rôle> with grant option;

Ajouter un user dans un rôle serveur:

- Serveur → rôles serveur → clic droit sur le rôle→propriétés →membres→ajouter→rechercher → parcourir→sélectionner l'utilisateur

Ajouter un user dans un rôle de BD :

- Serveur → Sécurité → connexion →clic droit sur l'user → mappage user → sélectionner la DB → sélectionner le rôle
- Le mappage va permettre au login d'être dans les utilisateurs de la BD

Créer un rôle de BD :

- CREATE ROLE <nom rôle> ;(en étant dans la BD)
- Base de données → rôles→ rôles de base de données →nouveau

Donner une permission à un rôle de BD :

- Base de données → sécurité → rôles →clic droit sur rôle → élément sécurisable (cocher la DB) → sélectionner les autorisations → éléments sécurisables → définir permissions

Créer un schéma : BD → schéma → nouveau schéma → créer

Octroyer à un rôle des privilèges sur un schéma :

- Base de données → sécu → schema → clic droit sur le schema → propriétés → autorisations →rechercher le rôle → cocher les permissions
- GRANT <permission> ON SCHEMA :: <nom schema> TO <nom role>

Update → modifie les lignes

Alter → Modifie la structure

Créer un index :

- CREATE INDEX <nom index> ON <table> (<colonne>);
- Base de données → table → index → clic droit → nouveau index (on peut cocher unique si l'index est unique)
- CREATE UNIQUE INDEX <nom index> ON <table>(<colonne>); (si l'index est unique)

Désactiver un index : Bd → table → table en question → index → clic droit sur l'index en question → désactiver. Lorsque les index sont désactivé ils ne prennent plus de place.

L'index cluster est unique et créé automatiquement pour la clé primaire. L'index non-cluster peut être créé par le user.

Index unique → clé unique (Id, registre national, email, ect)

Index non unique → clé non unique (nom, prénom,ect)

Pourquoi ne pas mettre des index partout ?

- Ils accélèrent la recherche, mais ils ralentissent les autres opérations !
- Ils prennent de la place.

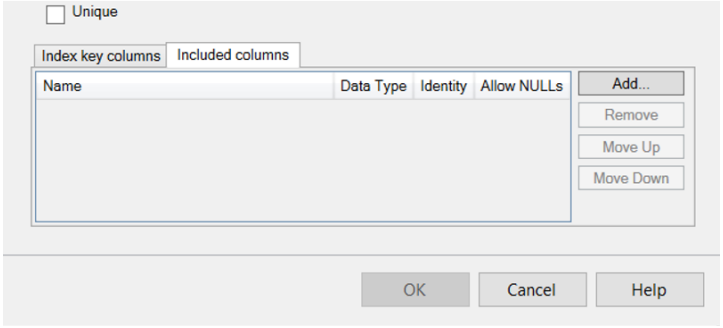
Pourquoi les index ralentissent les autres opérations ?

- Les index sont des B-Trees, les données sont donc organisées
- Les opérations INSERT/UPDATE/DELETE peuvent provoquer une réorganisation du B-Tree

Créer un index avec des colonnes inclues :

- CREATE INDEX index ON table(col1) INCLUDE (col2, col3, …)

- En interface graphique :

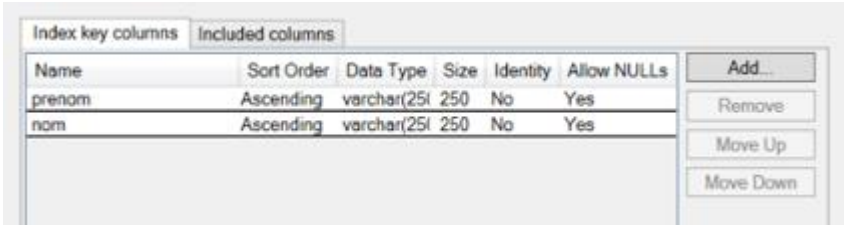


On peut également mettre des conditions pour sélectionner précisément les données que l'on veut indexer :

- CREATE INDEX <nom index> ON <table> (<colonne>) WHERE <condition>;
- En interface graphique :

Il est également possible de créer un index sur plusieurs colonnes :

- CREATE INDEX <nom index> ON <table> (<colonne1>,<colonne2>) ;
- En interface graphique :



Différence avec les index avec colonnes inclues ?

- Quand l'index est sur plusieurs colonnes, il faut trier les données pour chaque colonne.
- Quand l'index contient des colonnes(inclues), aucun tri n'est effectué sur ces colonnes.

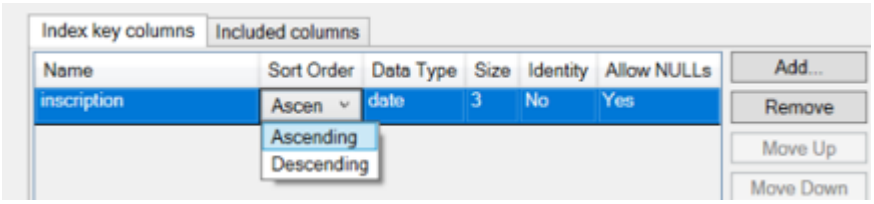
Attention, s'il on souhaite créer un index multicolonnes, il faut que l'ordre des colonnes dans l'index soit le même que l'ordre dans la requête. Exemple :

- CREATE INDEX i1 ON users(prenom,nom)
  SELECT prenom,nom FROM users →fonctionne
- CREATE INDEX i1 ON users(nom,prenom)
  SELECT prenom,nom FROM users → ne fonctionne pas

Il est possible d'indexer les données dans un ordre précis (« ASC » ou « DESC ») :

- Par défaut, il est toujours « ASC »
- CREATE INDEX <nom index> ON <tabel> (<colonne> DESC);

- EN interface graphique:



Les différents type d'index peuvent s'utiliser ensemble. Exemple : CREATE UNIQUE INDEX i1 ON t1 (col1 DESC, col2 ASC, col3 DESC);

Il est préférable de créer des index lorsqu'on possède une table qui :

- Possède beaucoup de données.
- N'est pas souvent modifiée.
- Qui nécessite des **requêtes complexes** dont il faut accélérer la recherche.

Supprimer le cache de SQL Server :

- CHECKPOINT;
  GO
  DBCC DROPCLEANBUFFERS;
  GO

Active une mesure précise du temps d'exécution des requêtes : SET STATISTICS TIME ON (OFF pour désactiver)

Regarder la taille que prennent les index sur le disque dur : Clic droit sur la db → reports → reports standard → disk usage by top tables

Générer une évaluation des vulnérabilités d'une BD : BD → clic-droit → Tâches → Evaluation des vulnérabilités → Rechercher les vulnérabilités

Bonnes pratiques en matières de sécurité des données :

- Toujours donner le strict minimum pour les droits des utilisateurs.
- Principe du Need To Know. L'utilisateur a-t-il besoin de voir telle table, a-t-il besoin de modifier une table ?
- Si un employé n'a plus besoin d'accéder à la base de données : on supprime le compte.
- Un mot de passe : ne doit pas contenir le nom de l'utilisateur, doit être de minimum 8 caractères, doit contenir des majuscules, des minuscules, des chiffres et des caractères spéciaux, peut être au maximum de 128 caractères
- Stratégie de sauvegarde : si la base de données subit une perte totale ou partielle, il suffirait de restaurer la base, mais il faut renouveler la sauvegarder avec une fréquence stricte et respectée.
- Chiffrement des données(des backup) : les données sont alors inutiles en l'absence du mot de passe ou de la clé de déchiffrement correspondante
- Journalisation

Créer un audit et l'activer : Serveur → Sécurité → Audit → Nouvel audit → Clic droit sur le nouvel audit → activer l'audit puis BD → Sécurité → Spécification de l'audit de la base de données → activer la spécification de l'audit de la base de données

On peut préciser ce qu'on veut journaliser : DB → sécurité → spécification de l'audit → propriétés

Consulter les journaux d'audit : Sécurité → Audits → Clic droit sur l'audit → Afficher les journaux d'audit

Installer SNMP sur Windows 10 : Paramètres -> applications -> fonctionnalités facultatives -> ajouter une fonctionnalité -> SNMP.Dans services.msc -> sécurité -> ajouter « public » en lecture seule et cocher « accepter les paquets SNMP provenant de n'importe quel hôte ».

Installer SNMP sur Debian(chronologique) :

- Installer SHH : apt update && apt install ssh
- Modifier le fichier sshd_config : nano /etc/ssh/sshd_config
  - Permitrootlogin yes
- Modifier le fichier sources.list : nano /etc/apt/sources.list ->
  - ajouter « contrib » et « non-free » à la première ligne.
- Installer SNMP : apt install snmp snmpd snmp-mibs-downloader
- Permettre l'utilisation des MIB : nano /etc/snmp/snmp.conf
  - Ajouter : mibs +ALL
- Modifier snmpd : nano /etc/snmp/snmpd.conf
  - Modifier ou ajouter : agentAddress upd:161, udp6:[::1]:161
  - Modifier ou ajouter : view systemonly included .1.3.6.1.2.1.25.1
  - Modifier ou ajouter : view systemonly included .1.3.6.1.2.1.1
  - Modifier ou ajouter : rocommunity public default
  - Relancer le service : systemctl restart snmpd

MIB : ensemble de données à propos de la machine organisées sous forme d'un arbre.

OID : objet (nœud) de l'arbre.

Parcourir tout le MIB : snmpwalk -v 2c -c public <adresse IP>

Parcourir un OID du MIB : snmpwalk -v 2c -c public <adresse IP> <OID>

Récupérer un objet précis : snmpget -v 1 -c public <adresse IP> <OID>

Obtenir l'adresse MAC : OID = .1.3.6.1.2.1.4.22.1.2

Obtenir statut de l'interface : OID = .1.3.6.1.2.1.2.2.1.8

Obtenir le nom de la machine : OID = .1.3.6.1.2.1.1.5

MTU des interfaces : OID = .1.3.6.1.2.1.2.2.1.4

Obtenir l'uptime de la machine : OID = .1.3.6.1.2.1.1.3

Système description : OID = .1.3.6.1.2.1.1.1