

ADMINISTRATION ET SÉCURITÉ DES BASES DE DONNÉES

ABD3502

TRAVAIL – PRATIQUE 5 - NOTÉ

SÉCURITÉ des Bases de Données

20 Points

License 3 – ASSRI

Temps (2.5h à 3.5h max)

Année Scolaire 2022-2023

Par

Professeur: **Robert Yavo**

Email: ryavo@hotmail.com WhatsApp: +225-07-88-63-26-58

Table des matières

Ex 01 – Sécuriser le serveur « SQL Server 2019 » (4 points).....	3
Ex 02 – Gérer les accès et authentifications (6 points).....	3
Ex 03 – Chiffrer une colonne sensible (10 points)	3

NB : Toutes vos réponses doit se trouver dans le dossier C:\TP5_Note

Ex 01 – Sécuriser le serveur « SQL Server 2019 » (4 points)

- Créez un Dossier nommé **TP5_Note** sur votre disque dur C: Assurez-vous que les 2 Services **SQL Server (MSSQLSERVER)** et **SQL Server Agent (MSSQLSERVER)** sont démarrés et en mode **Automatique**.
Créez un fichier ListeEtudiants.txt dans TP5_Note qui porte vos Noms et Prénoms, Email et Téléphone WhatsApp. (Pour la correction par le Prof)
- Utilisez SSMS pour configurer la Propriété **NetworkPacketSize** du Facet **Server Performance** à **8192 bytes**. Et **exportez** la configuration dans votre dossier TP5_Note.
- Évaluez les vulnérabilités de la base de données AdventureWorks2016.
Commentez le résultat en quelques mots et Identifiez 2 des vulnérabilités qui présentent des Risques Moyens et/ou Élevés. Choisissez au moins un des Risques identifiés et décrivez la solution proposée. Faites un Imprime-Écran du résultat du scannage et le mettre dans un document word ou une image et le sauver dans le dossier TP5_Note.

Ex 02 – Gérer les accès et authentications (6 points)

- Déterminer le Nom du Rôle Serveur fixe définit pour la connexion du service **NT SERVICE\SQLWriter** de la base de données **AdventureWorks2016**.
- Quel est le **nom de la permission accordée** aux objets **dbo.spt_values** et **dbo.spt_monitor** de la base de données MASTER.
- A l'aide de T-SQL créez les 2 comptes de connexions suivantes :
 - Authentification Windows de l'utilisateur MARC et le serveur MySERVER-01
 - Authentification SQL Server de l'utilisateur JAMES dont le mot de passe est Jimmy123 et que James **doit changer** son mot de passe qui expirera à la prochaine connexion.
- Créez un **Usager SQL Server** nommé **SMITH** et mot de passe **John123** qui doit se connecter à l'aide de SQL Server et non Windows. (Créez le LOGIN et l'USAGER)

Ex 03 – Chiffrer une colonne sensible (10 points)

Créez une BD nommée **TP5Note** et utilisez-la pour répondre aux questions suivantes :

- Créez une table nommée **payment** avec les colonnes suivantes :
payment_ID **int Primary Key**,
userId **int**,
orderId **int**,
cartecredit **varchar(20)**
- Créez un Master Key dont le mot de passe est: **Robert123_** et Créez le certificat nommé **Certif_CC01** avec la description: 'Certificat de Protection de carte de crédit'
- Créer la clé Symétrique nommée **SymKeyCC01** du certificat Certif_CC01 avec un algorithme de chiffrement **AES_256**

- d) Ajoutez une Colonne nommée `cartecredit_encrypted` de type `varbinary(200)` dans la table `payment` puis ouvrez la clé Symétrique créée
- e) Chiffrez la valeur de la colonne `cartecredit` en utilisant la clé symétrique `SymKeyCC01` et sauvez le résultat dans la colonne **`cartecredit_encrypted`** de la même table `payment` avec hash **SHA2_256** comme nous l'avons vu en classe. (Il s'agit ici, de faire une mise à jour (`update`) de la colonne `cartecredit_encrypted`.)
- f) Insérez cette ligne dans la table `payment` (1, 10, 152, '45095788805107324')
Et faites la mise à jour comme à l'étape e) pour vérifier si la colonne `cartecredit_encrypted` est vraiment chiffrée comme le montre l'écran suivant :

Results		Messages			
	payment_ID	userId	orderId	cartecredit	cartecredit_encrypted
1	1	10	152	45095788805107324	0x0095C61F2467B046BD8A19BB376258B1020000007910498...
2	2	12	300	95095788805107320	0x0095C61F2467B046BD8A19BB376258B102000000072251...

N'oubliez pas d'ouvrir la clé symétrique créée avant de faire le « **update** ».
Ce qui nous conduit à la question bonus g)

g) Question Bonus (1 point)

Créez un TRIGGER qui va se déclencher et mettre à jour automatiquement la colonne `cartecredit_encrypted` à chaque fois qu'on insère un nouveau `payment` avec une nouvelle carte de crédit bien sûr.

Remarque importante:

Toutes vos réponses doivent être sauvegardées dans le dossier TP5Note.