

ADMINISTRATION ET SÉCURITÉ DES BASES DE DONNÉES

ABD3502

TRAVAIL – PRATIQUE 4

SÉCURITÉ des Bases de Données

(TP4)

License 3 – ASSRI

Année Scolaire 2022-2023

Par

Professeur: **Robert Yavo**

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

Table des matières

Exercice 01 - Requêtes Avec Windows Batch	3
Exercice 02 – Requête avec PowerShell.....	3
Exercice 03 – Automatisation Complète.....	3

Exercice 01 – Sécuriser le serveur « SQL Server 2019 »

- A l'aide de **SQL Server Configuration Manager**, assurez-vous que les 2 Services **SQL Server (MSSQLSERVER)** et **SQL Server Agent (MSSQLSERVER)** sont démarrés et en mode **Automatic**.
- Utilisez SSMS pour Activer la Propriété **DatabaseMailEnabled** du **Facet Surface Area Configuration**. Et exportez la configuration dans un fichier XML.
- Évaluez les vulnérabilités d'une base de données comme TPRobert et commentez le Résultat. Identifiez les vulnérabilités qui présentent des Hauts Risques ou des Risques moyens. Et choisissez au moins un des Risques identifiés et décrire la solution proposée (Remediation).

Exercice 02 – Gérer les accès et les authentifications

- Déterminer le Nom du Rôle Serveur fixe définit pour les services MSSQLSERVER et SQLSERVERAGENT dans votre base de données SQL Server.
- Quel est la liste des autorisations qui ont été accordées ou refusées au niveau du Serveur Master de votre base de données?
- Quel est la liste des autorisations qui ont été accordées ou refusées au niveau de chaque base de données.
- A l'aide de T-SQL créez les 2 comptes de connexions suivantes :
 - Authentification Windows avec le nom d'utilisateur JOHN et le serveur DESKTOP20A
 - Authentification SQL Server de l'utilisateur MARIAM dont le mot de passe est Mariam123 et que Mariam **doit changer** son mot de passe qui expirera à la prochaine connexion.
- Créez un Usager SQL Server nommé **BOB** et mot de passe **Orange123** qui doit se connecter à l'aide de SQL Server et non Windows. (Il s'agit de créer le LOGIN d'abord et ensuite l'USAGER et son mot de passe)

Exercice 03 – Chiffrer les colonnes de données sensibles

Utilisez la base de données du TP1 Noté pour répondre aux questions suivantes :

- Ajouter la colonne CarteCredit de type varchar(25) dans la table **usager** ou **client**
- Chiffrer avec le Chiffrement Symétrique et l'authentificateur en créant le certificat, la clé, la colonne qui stock les données chiffrées de type varbinary (160), Ouvrir la clé avec laquelle les données ont été chiffrées et chiffrez la valeur de la colonne CarteCredit en utilisant la clé symétrique créée. Sauvez le résultat dans la colonne créée pour stocker les données chiffrées (Page 18/25)
- Quelle requête pour vérifier que le chiffrement en a) et b) a marché.

Exercice 04 – Créer des Audits

Audit avec T-SQL

Créez un audit de votre Serveur qui va auditer les connexions qui on échouées

Activez l'audit que vous avez créé (voir Page 20/25)