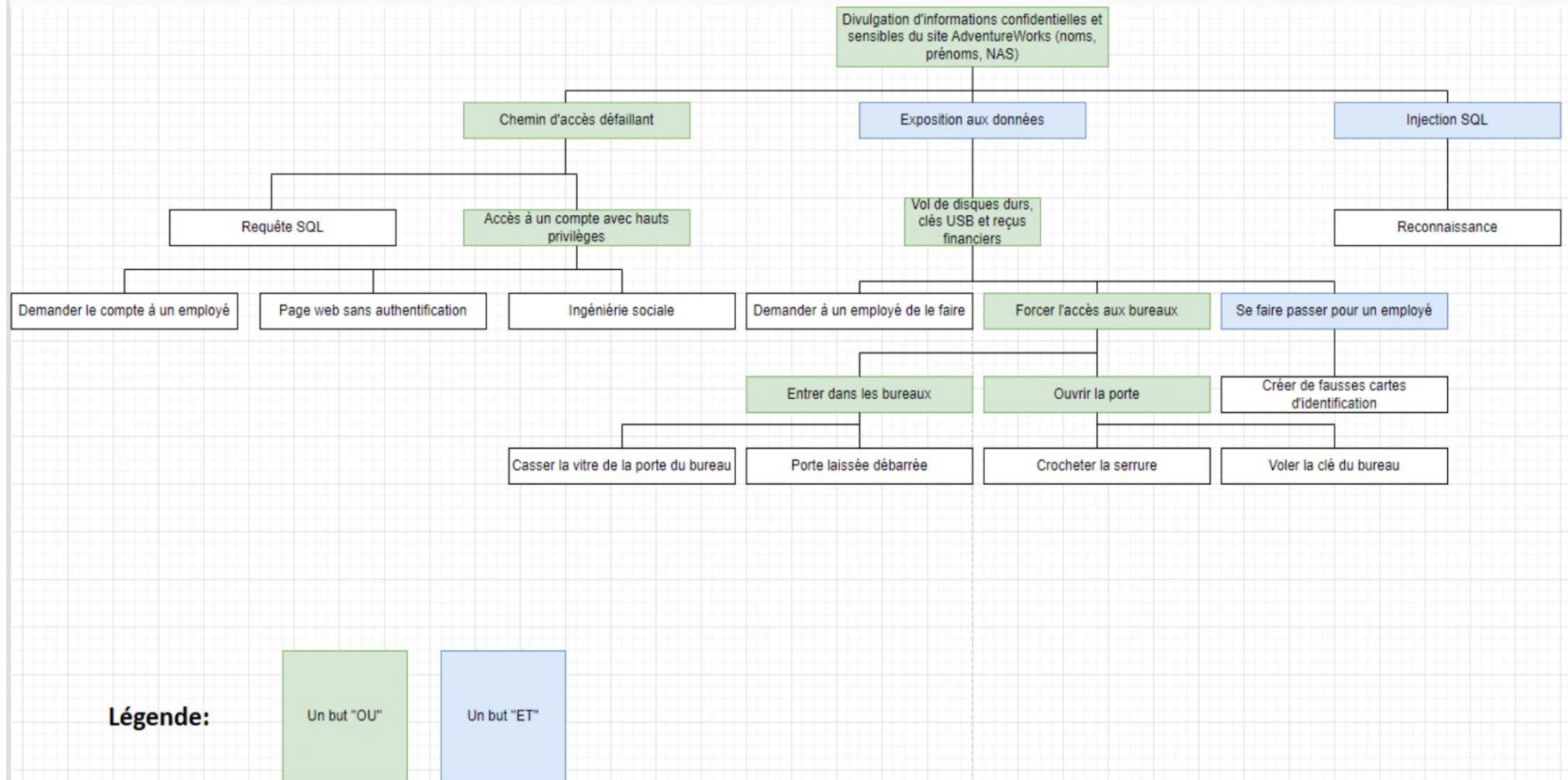


Q1 – Arbre d'attaque

Faites un arbre d'attaque de « Aller chercher le nom, prénom et numéro d'assurance social des employés » dans la BD. Sachant que la BD est liée à un site web de type ERP (relation client). (Inspirez-vous des informations données lorsqu'on a vu la vulnérabilité de divulgation d'information)

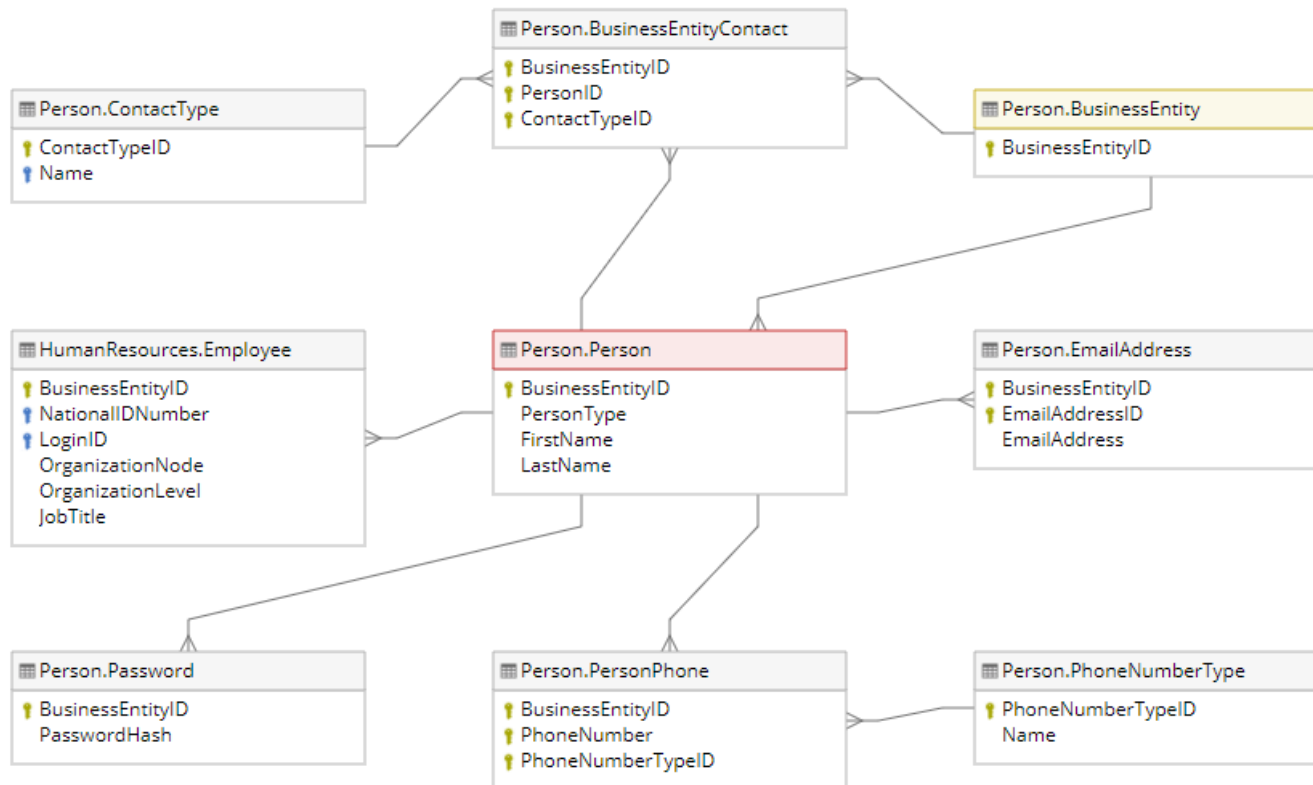
Réponse Q1 :



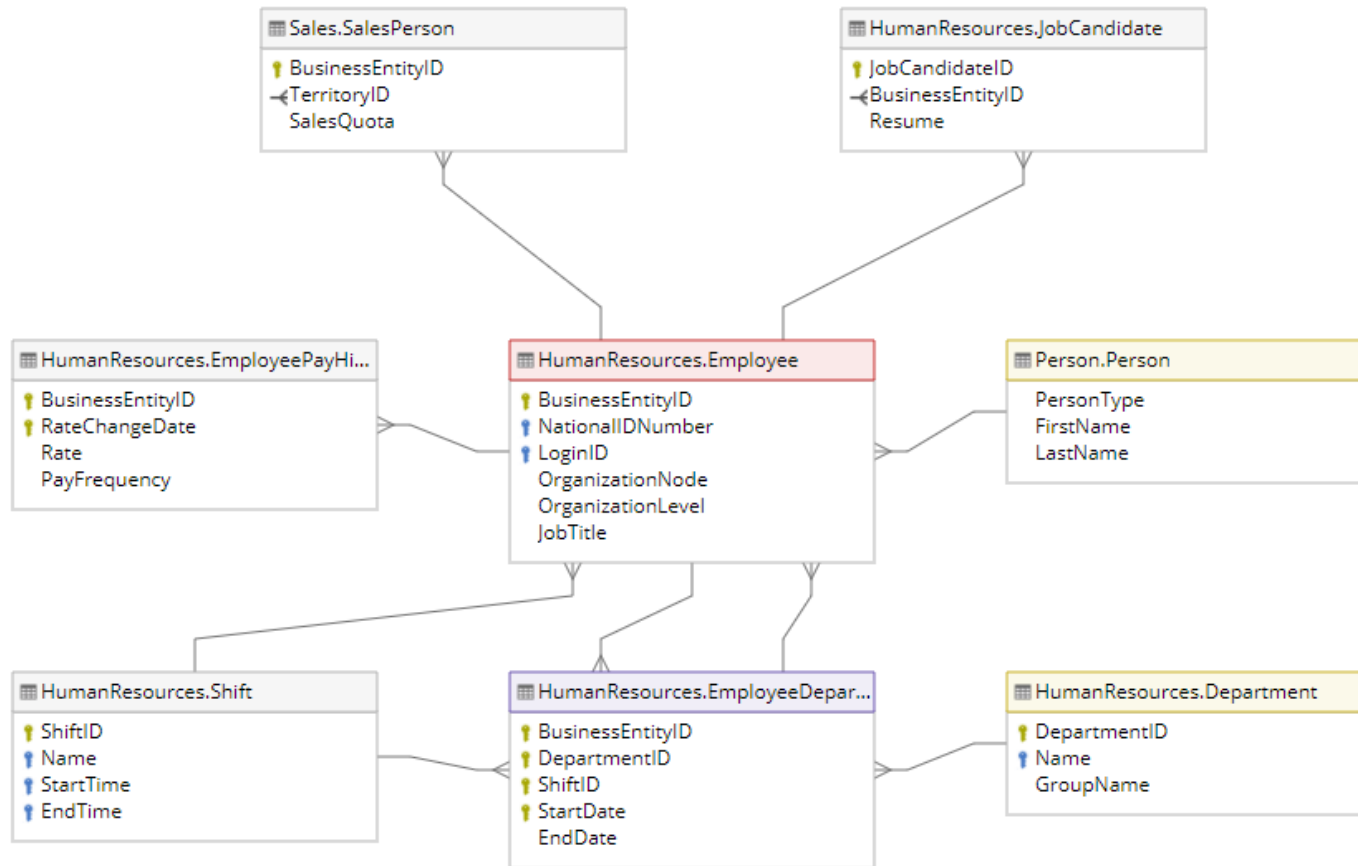
Q2 – Classification des données

Exportez votre SQL Data Classification Report mis à jour selon votre analyse. Ajoutez le avec ce gabarit de réponses. Vous devez classifiez **seulement** les données qui sont sous les diagrammes suivants :

People



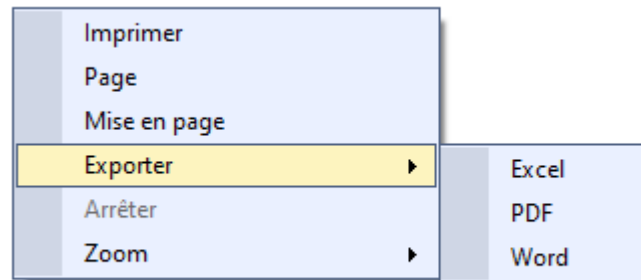
Human Resources



Production.ProductReview	
ProductReviewID	int
ProductID	int
ReviewerName	nvarchar(50)
ReviewDate	datetime
EmailAddress	nvarchar(50)
Rating	int
Comments	nvarchar(3850)

Réponse Q2 :

À mettre dans un fichier à part. Faites Exporter > Word. À remettre avec ce gabarit de réponse.



Nom du fichier : Data Classification – 2022-11-29 224 AM - FREDMAINPC

Q3 – Rôles

Créez des rôles pertinents au contexte. Donnez un exemple de comment vous avez ajouté 1 rôle. (<https://docs.microsoft.com/en-us/sql/relational-databases/security/permissions-database-engine?view=sql-server-ver15>).

Réponse Q3 :

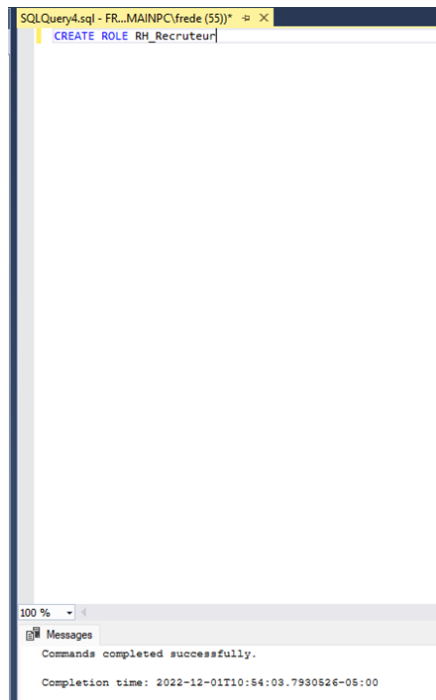
Seulement pour les tables qui seront utilisées par les Ressources Humaines faites un tableau des rôles que vous mettriez.

Pistes de réflexion : sachez que le département des ressources humaines a un service de recrutement, un service de paie, un service administratif et un service fiscal et que ce dernier n'envoie que les comptes de taxe à la fermeture de l'année civile lors de la mise à jour des taxes.

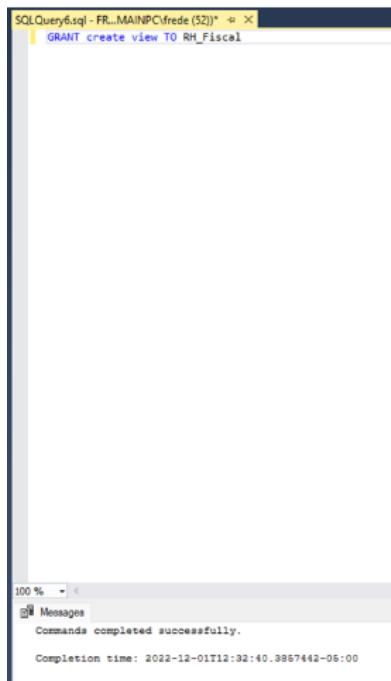
Rôle	Table	Description des permissions	Détails
RH_Recruteur	JobCandidate	Créer, Edit, Insert	Le recruteur ne peut qu'éditer et créer dans la BD les infos relatives aux candidats
RH_Fiscal	EmployeePayHistory	Lire	A seulement accès à la lecture aux données fiscales que pour envoyer ces dernières à la fermeture de l'année civile
RH_AdminManager	Toutes les tables de HumanResources	Créer, Supprimer, Edit, Lire, Insert, Alter, etc.	Permission administrative à l'instance au complet. Ce rôle devrait être attribué à la personne à la tête des Ressources Humaines
RH_PayrollManager	EmployeePayHistory	Lire, Edit, Insert, Supprimer	Le payroll manager s'occupe de tout ce qui a trait aux paies (erreurs, changements de pay rate, etc.) Il peut lire, éditer, insérer et supprimer dans la table EmployeePayHistory

Exemple du script ou procédure (montrez que vous l'avez essayé) :

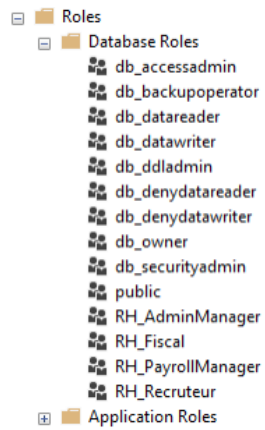
1- Nous avons ajouté un rôle de recruteur pour les RH. Voir image ci-dessous :



2- Voici une capture d'écran qui démontre également la permission de lire ou "view" pour le rôle RH_Fiscal :
la même chose a été effectué pour chaque rôle et leur permission donnée au tableau ci-dessus



3- Et finalement voici une capture d'écran qui démontre bel et bien nos 4 rôles ajoutés à la BD :



Q4 – Masques

Choisissez 3 colonnes auxquels se prêtent l'utilisation des masques. Utilisez prioritairement les données confidentielles.

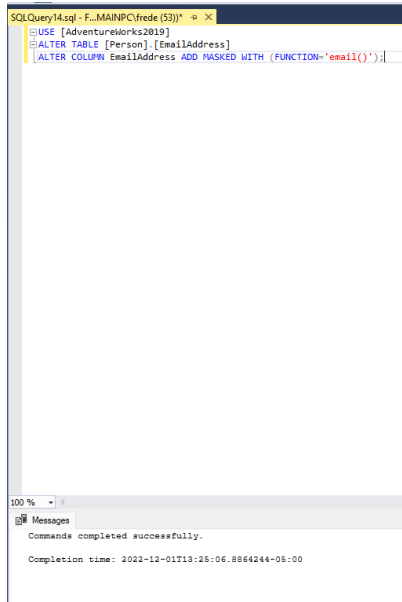
Vous ne pouvez pas utiliser NationalIdNumber ou CreditCardNumber.

Faites un select de chacun des masques que vous avez mis en place avec un rôle qui a accès et un autre qui n'a pas accès, collez les impression écran pour chacun (requête + résultats) et mettez-les ici :

Les adresses e-mail ont été masquées simplement avec la fonction default ainsi que le LoginID des employés et leur taux de paie. Voir images des commandes utilisées ci-dessous :

Réponse Q4 :

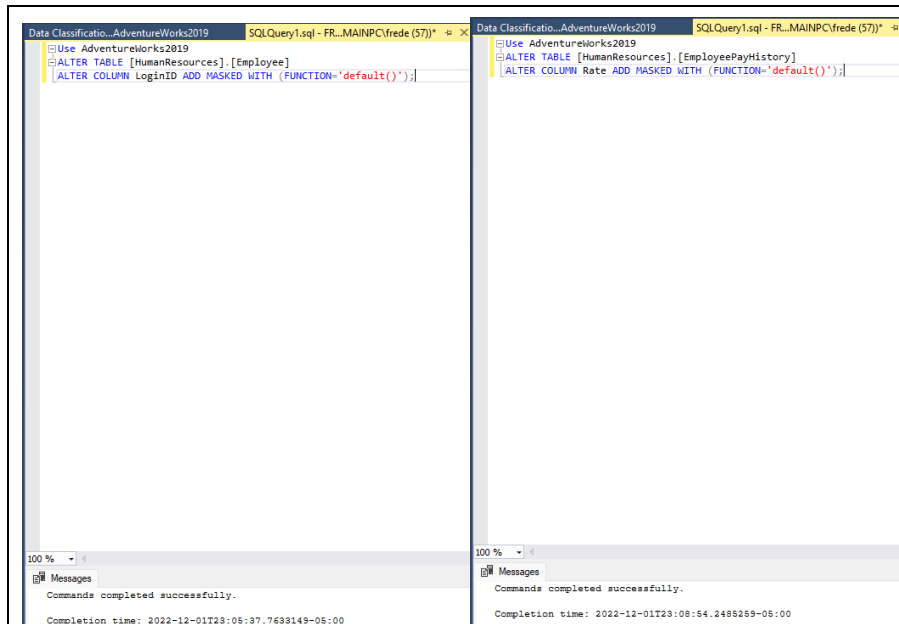
1- Nous avons utilisé la commande suivant pour masker les adresses email avec la fonction d'email



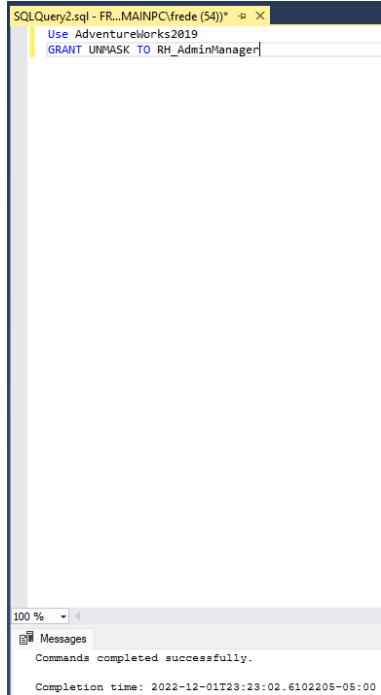
```
SQLQuery14.sql - F:\MAINPC\Frede (53) - X
USE [Adventureworks2019]
ALTER TABLE [Person].[EmailAddress]
ALTER COLUMN EmailAddress ADD MASKED WITH (FUNCTION='email()');
```

100 %
Messages
Commands completed successfully.
Completion time: 2022-12-01T13:26:06.8864244+05:00

2- Voici les captures d'écran qui démontrent aussi les masques des LoginID et des taux de paie des employés :



3- Voici maintenant le rôle HR_AdminManager avec sa permission de voir les masques :



The screenshot shows a SQL Server Enterprise Manager window titled "SQLQuery2.sql - FR...MAINPC\Frede (54)". The query editor contains the following T-SQL commands:

```
Use AdventureWorks2019
GRANT UNMASK TO RH_AdminManager
```

At the bottom, the "Messages" pane shows the execution results:

```
Commands completed successfully.
Completion time: 2022-12-01T23:23:02.6102205-05:00
```

Les autres rôles par défaut n'ont pas accès aux données masquées.

Q5 – Certificat et encryption

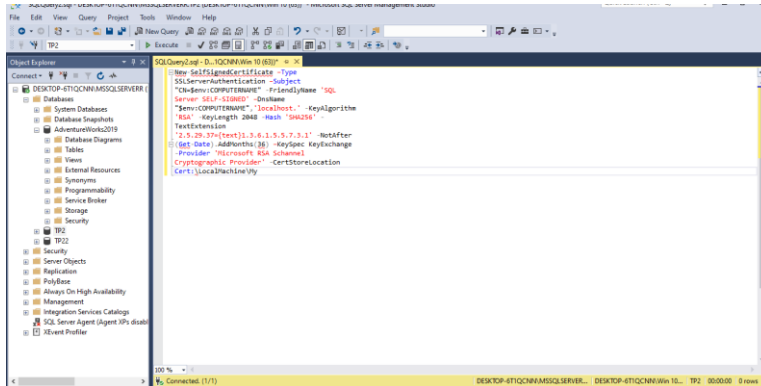
Faites des captures écrans des commandes et des résultats de vos commandes et/ou de la fenêtre SSMS

- Encrypter la base de données et les backups en expliquant ce que vous faites.
- Utilisez Always Encrypted pour HumanResources.Employee.NationalIDNumber en expliquant ce que vous faites.
- Encryptez manuellement (donc sans utiliser Always Encrypted) la colonne Sales.CreditCard.CreditCardNumber en expliquant ce que vous faites.
- Activez TLS pour les requêtes.

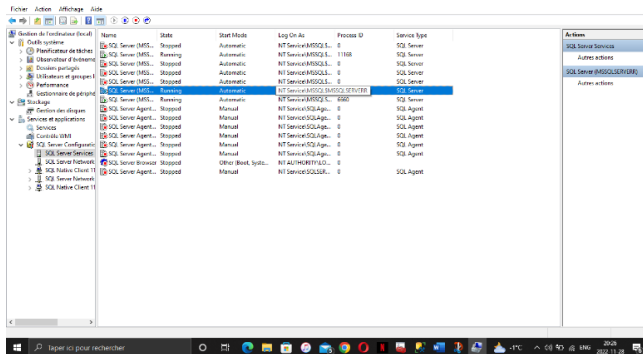
Réponse Q5 :

Pour **encrypter la BD** nous avons dû :

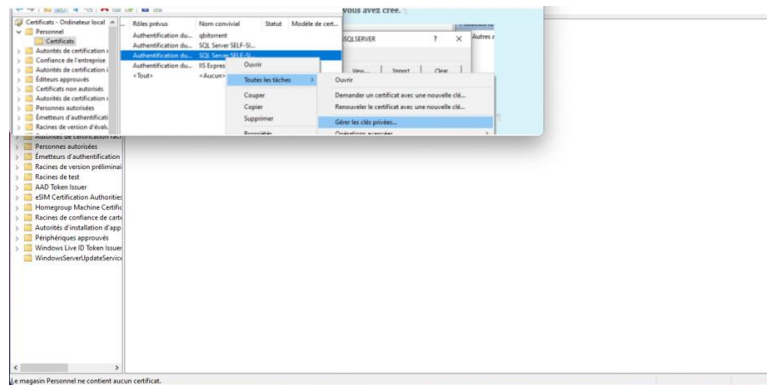
1- Créer notre propre certificat **TLS**.



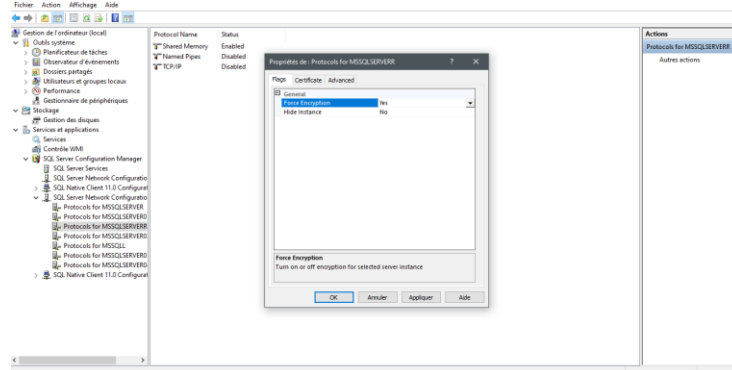
2- Aller dans : gestion de l'ordinateur le nom du sql serveur qu'on a installé.



3- Nous sommes allées dans : gestion des certificats pour activer le certificat qu'on a installé afin de l'appliquer à sql



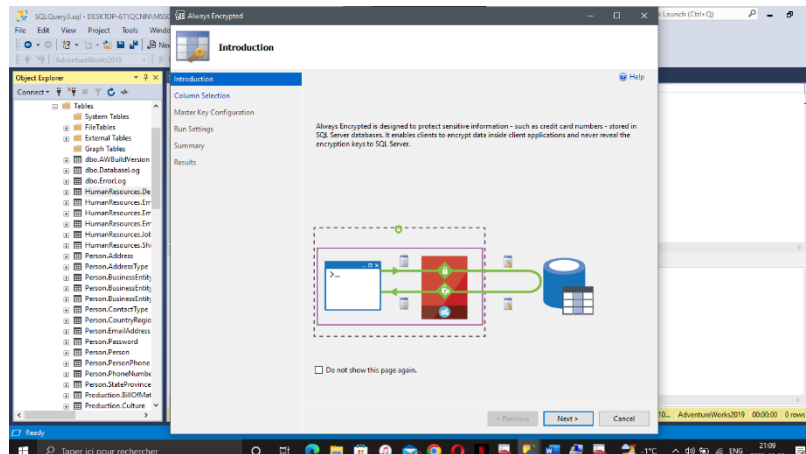
4- On a forcé l'encryptions sur SQL serveur en choisissant le certificat qu'on a créé



Pour **Always Encrypted** la colone HumanResources.Employee.NationalIDNumber on a :

1- Cliquer sur graphe Tables

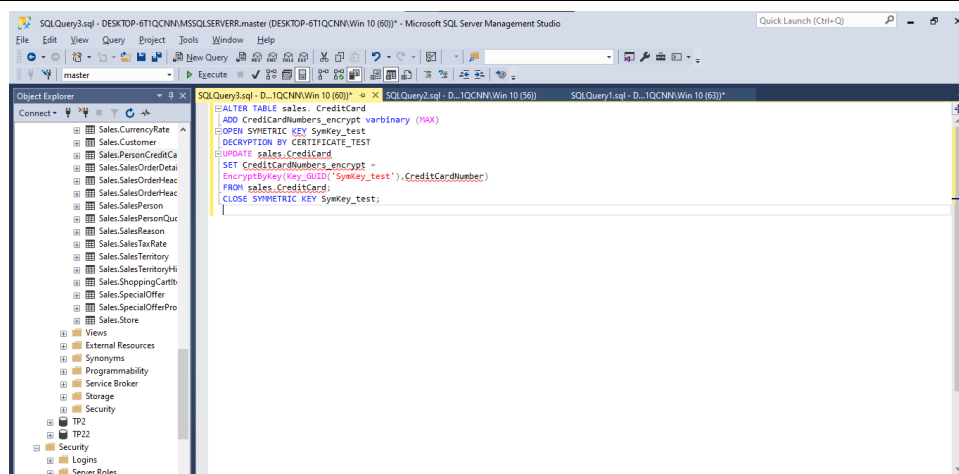
2- Clic droit sur la colonne concerné – Encrypt Columns, ensuite nous avons suivi les étapes de configuration



Pour encrypter manuellement **Sales.CreditCard.CreditCardNumber** nous avons :

- 1- Grace au certificat que nous avons créé on a pu encrypter la colonne sales.CreditCard.CreditCardNumbers en rentrant les commandes suivantes sur SQL :

```
ALTER TABLE sales. CreditCard
ADD CrediCardNumbers_encrypt varbinary (MAX)
OPEN SYMETRIC KEY SymKey_test
DECRYPTION BY CERTIFICATE_TEST
UPDATE sales.CrediCard
SET CreditCardNumbers_encrypt =
EncryptByKey(Key_GUID('SymKey_test'),CreditCardNumber)
FROM sales.CreditCard;
CLOSE SYMMETRIC KEY SymKey_test;
```

2- Supprimer l'ancienne colonne et on renomme celle qu'on vient d'ajouter.

Q6 – Script de backup

Faire des backups encryptés journaliers.

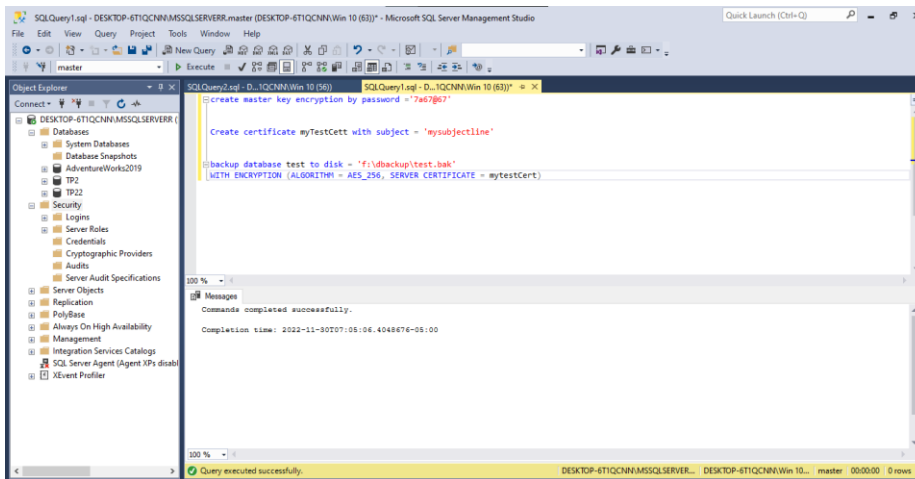
Mettre une capture d'écran de cette configuration

Réponse Q6 :

Étape 1 : On a fait un backup du certificat qu'on a créée avec la commande

Backup certificate myTestCert to file = 'f:\dbbackup\test.bakcup\Test_db_certificate.cert'

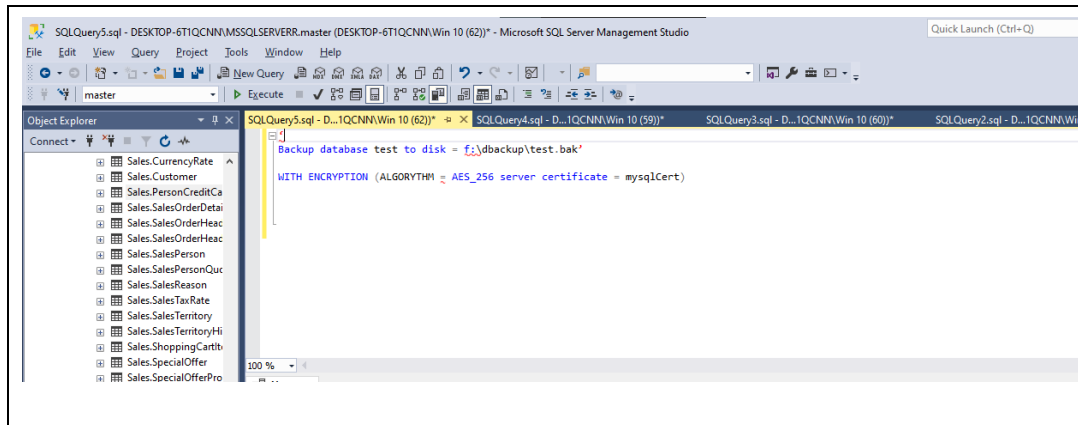
With private key (file = 'f:\dbbackup\test.bakcup\Test_dbkey.key', encryption by password : 12345sql)



Étape 2 : En suite on a renter les commandes suivantes pour faire le backup de la BD.

Backup database test to disk = 'f:\dbbackup\test.bak'

WITH ENCRYPTION (ALGORITHM = AES_256 server certificate = mysqlCert)

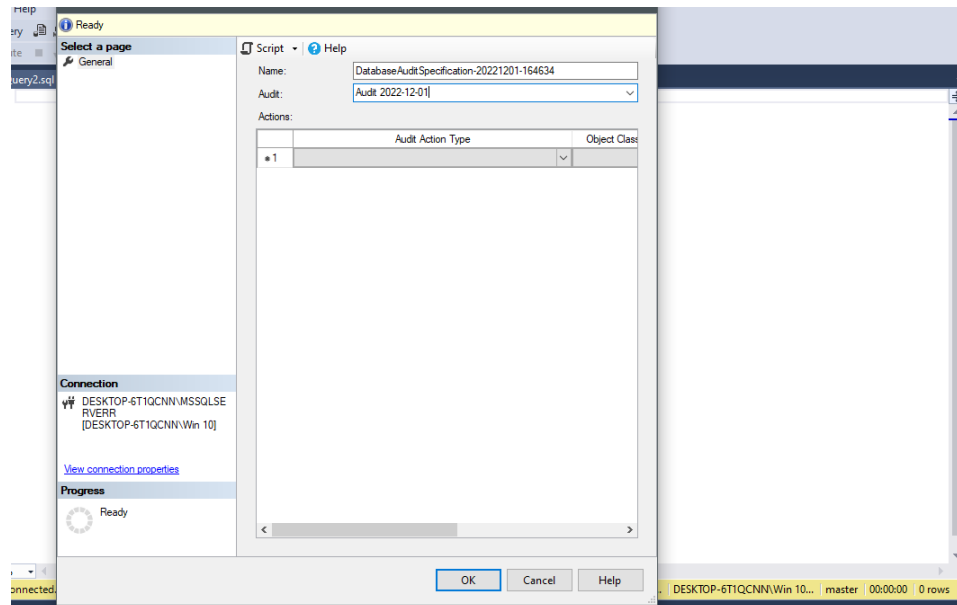


Q7 – Activez l’audit sur l’insertion ou la modification des ProductReview.

Copiez-collez votre script ci-dessous :

Réponse Q7 :

1. Cliquer droit sur Audit - New Audit – New Audit Database Specification



2. Afficher l’audit :

```
SELECT * FROM sys.fn_get_audit_file ('C:\tmp\AuditMotDePasse_C51805EE-DFEB-4F48- AA11-50206988DDC9_0_132812358377770000.sqlaudit',de fault,default);
```

Q8 – Recommandations pour le client

Donnez vos recommandations à votre client qui met en place cette BD en opération.

Est-ce qu'il y aurait des suggestions en matière de sécurité que vous pourriez mettre en place pour sécuriser l'application ? Sachant que le client ne connaît pas grand-chose à l'informatique et encore moins à la sécurité.

Réponse Q8 :

Recommandations

- Encrypter toutes les colonnes sensibles pour empêcher que l'information sensible ne soit accédée par une personne non autorisée. Utiliser always encrypted pour les données au repos et sur le réseau (Microsoft SQL Server).
- Sécurité au niveau des lignes SNL afin que les utilisateurs de la BD n'aient accès qu'aux données qui concernent leur fonction. (Microsoft SQL Server).
- Activez l'audit au niveau du serveur et autorisez l'audit au niveau de la base de données à hériter de la propriété au niveau du serveur pour toutes les bases de données.
- S'assurer d'avoir une bonne authentification pour les utilisateurs et selon leur rôle et s'assurer d'avoir un journal des logs d'utilisateurs (Microsoft SQL).
- Pratique de sécurité basée sur le moindre privilège.
- Choisir Active Directory au lieu de l'authentification SQL.
- Exiger des mots de passe robustes et implanter l'authentification multi facteur.
- Réduire les droits qui sont accordés au compte Admin, s'assurer de supprimer les comptes administrateur système après leur utilisation.
- Il est recommandé d'activer uniquement les fonctionnalités requises par votre environnement afin de réduire le nombre de fonctionnalités susceptibles d'être attaquées.
- Faire une évaluation courante des vulnérabilités.
- Sauvegarder la master key et la mettre en route.
- Faire un Backup des données et les localiser dans un autre système que celui de la BD afin de pouvoir la restaurer en cas de perte de données et s'assurer d'encrypter ses backups.
- Stocker uniquement l'information nécessaire.
- Faire usage des fonctions de hachage.

- Faire attention aux attaques par injection de code qui sont courante avec les BD en faisant une supervision de la saisie automatique des applications, s'assurer de la protection complète du serveur, renforcer la BD en utilisant des codes solides (Inos.fr).

Q (bonus) – Ajouter un utilisateur et un rôle pour ce nouveau site. Ajustez leurs permissions.

Copiez-collez votre script ci-dessous :

Réponse Q10.2 : Pour ajouter un nouvel utilisateur

On va dans Sécurité → User → New User → On rentre le User Name et mot de passe → Rentrer le serveur sql auquel il a accès

Références :

<https://www.ionos.fr/digitalguide/serveur/securite/injection-sql-bases-et-mesures-pour-se-proteger/>

[How to Encrypt a Database Backup in SQL server || Backup Encryption || Ms SQL](#)

<https://learn.microsoft.com/fr-fr/sql/relational-databases/security/sql-server-security-best-practices?view=sql-server-ver16>