Microsoft
experiences'16
Palais des Congrès de Paris

*Mardi 4 octobre • Journée **Business***

*Mercredi 5 octobre • Journée **Technique***

#experiences

experiences.microsoft.fr

Microsoft

Microsoft experiences'16

Mercredi 5 octobre • Palais des Congrès de Paris

Pascale DOZ Consulting

pascale@pascale-doz.com

Daniel PASQUIER - Microsoft

danielp@microsoft.com

#experiences

Microsoft


La Sécurité dans SQL Server 2016 & Azure SQL Database
Microsoft

Sécurité & Conformité

Sécurité

Protection des Données

Données en transit — ***Transport Layer Security*** (TLS)
Données au repos et en cours d'utilisation (client) — ***Transparent Data Encryption*** (TDE), ***Always Encrypted*** (AE)

Contrôle d'Accès

Accès Base de Données — ***Azure Active Directory Authentication*** (AAD)
Accès Applications — ***Row-Level Security*** (RLS), ***Dynamic Data Masking*** (DDM)

Surveillance Proactive

Suivi & Détection — ***Auditing & Threat Detection***

Conformité

FedRAMP, ISO, HIPPA, PCI 3.1, EU Model Clauses, UK G-Cloud

(gouvernement) (médical) (paiement) (personnel) (secteur public)

Protection des Données

Données en transit => ***Transport Layer Security (TLS)***
Données au repos => ***Transparent Data Encryption*** (TDE)
et en cours d'utilisation (client) => ***Always Encrypted*** (AE)

Chiffrement SSL/TLS

Protection des données: en transit

- **Assurez-vous que la communication SQL est chiffrée**
- **N'impacte pas directement le moteur SQL**
  Charge générée par le chiffrement allers et retours au niveau de l'OS
- **Peut être imposé au niveau du client ou du serveur**
  La connexion client peut échouer si le pilote ne supporte pas le chiffrement
- **Certificat d'Autorité digne de confiance (Auto-Signé possible)**

Transparent Data Encryption

Protection des données: au repos

- **Pas de changement au niveau applicatif – transparent ☺**
- **Pas de chiffrement des données en mémoire ou en transit**
  Les pages sont déchiffrées à la volé (monté dans la mémoire SQL)
  Les données déchiffrées peuvent être écrites sur le disque (paged out)
- **Nécessite un certificat pour le chiffrement/déchiffrement de la base de données**
  Le certificat et la clé privée doivent être présent pour restaurer la base sur une instance différente
- **Fonctionnalité disponible en version Enterprise**
- **Les fichiers de la database et les sauvegardes seront chiffrés ainsi que Tempdb**

Always Encrypted

Protection des données: en cours d'utilisation (client)

- **Généralement le DBA a accès à TOUTES les données sensibles même si elles sont chiffrées**

  Il n'existe pas de moyen pour éviter cela dans les versions précédentes, hormis la mise en oeuvre d'un développement personnalisé

- **Un administrateur sécurité peut générer/positioner les clés tandis que le DBA configure le chiffrement**

  Cela empêche le DBA de voir les données de la base car le Serveur SQL ne détient jamais le certificat et la clé privée

  Des cmdlets Powershell existent pour séparer ces tâches

Always Encrypted

Protection de données: en cours d'utilisation (client)

Protège les données sensibles en cours d'utilisation de privilèges élevés SQL

Chiffrement coté client

Chiffrement des données sensibles coté client à l'aide de clés qui ne sont jamais données au système de base de données.

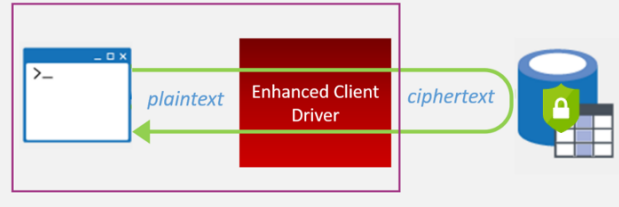
Requêtes sur des données chiffrées

Support de la comparaison d'égalité, jointure incl., Group by et opérateurs distincts.

Transparent pour l'application

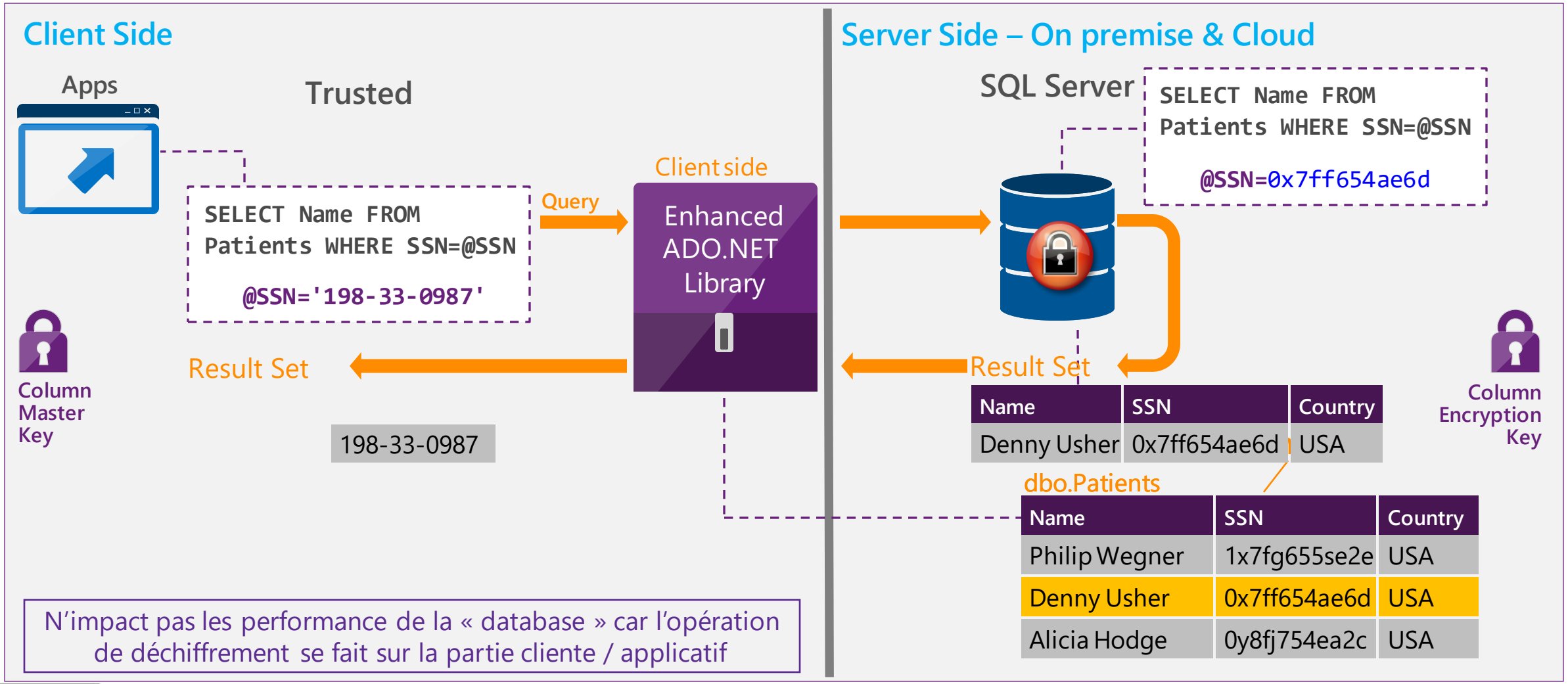
Changements mineurs au niveau application serveur et améliorations de la librairie cliente.

Outillage disponible avec SSMS, SSDT (new), PowerShell (new)



Always Encrypted

Aide à protéger les données au repos et en mouvement, local & Cloud



Always Encrypted

Column Master Key

- **Une entrée de métadonnées qui pointe vers un certificat**

  Le certificat est stocké dans un magasin de clés externe tel que Azure Key Vault

- **Utilisé pour chiffrer une "Column Encryption Key"**

```
CREATE COLUMN MASTER KEY [AKV_CMK]
WITH
(
    KEY_STORE_PROVIDER_NAME = N'AZURE_KEY_VAULT',
    KEY_PATH = N'https://AKVChapman.vault.azure.net/keys/AEFirstKey'
)
GO
```

```
CREATE COLUMN MASTER KEY CMK1
WITH
(
     KEY_STORE_PROVIDER_NAME = N'MSSQL_CERTIFICATE_STORE',
     KEY_PATH = N'CurrentUser/My/86CCACD078D047DB2423BD94EE1CF79B6B87C5D5'
)
GO
```

Always Encrypted

Column Encryption Key

- Clé utilisée pour chiffrer les valeurs de colonne de la table
- Chiffrée / Protégée par la Column Master Key (CMK)
- Peut avoir jusqu'à 2 valeurs chiffrées (pour la rotation CMK)

```
CREATE COLUMN ENCRYPTION KEY [AKV_CEK]
WITH VALUES
(
    COLUMN_MASTER_KEY = [AKV_CMK],
    ALGORITHM = 'RSA_OAEP',
    ENCRYPTED_VALUE = 0x016400000168007400740070007300 3A002F002F0061006B00760063006800
)
GO
```

Always Encrypted

Mise en oeuvre de Always Encrypted

1. Créer /Sécuriser un Certificat & clé privée (externe à SQL)
   - Magasin Windows Certificate
   - Azure Key Vault
   - Hardware Security Module (HSM)
2. Créer une Column Master Key (dans SQL)
3. Créer une Column Encryption Key (dans SQL)
4. Chiffrer les données
5. Donner à l'application l'accès aux données

Always Encrypted

Création des objets Always Encrypted

- Spécifier la Column Encryption Key
- Spécifier l'algorithme et le type de cryptage
- Cryptage déterministe nécessite un classement BIN2

```
CREATE TABLE dbo.People
(
IDCol INT IDENTITY(1,1) NOT NULL,
SSN CHAR(9) COLLATE Latin1_General_BIN2
    ENCRYPTED WITH (ENCRYPTION_TYPE = DETERMINISTIC,
    ALGORITHM = 'AEAD_AES_256_CBC_HMAC_SHA_256',
    COLUMN_ENCRYPTION_KEY = AKV_CEK) NOT NULL,
FirstName VARCHAR(255) NOT NULL,
LastName VARCHAR(255)
    ENCRYPTED WITH (ENCRYPTION_TYPE = RANDOMIZED,
    ALGORITHM = 'AEAD_AES_256_CBC_HMAC_SHA_256',
    COLUMN_ENCRYPTION_KEY = AKV_CEK) NOT NULL,
BirthDate DATE NULL
)
```

Aléatoires

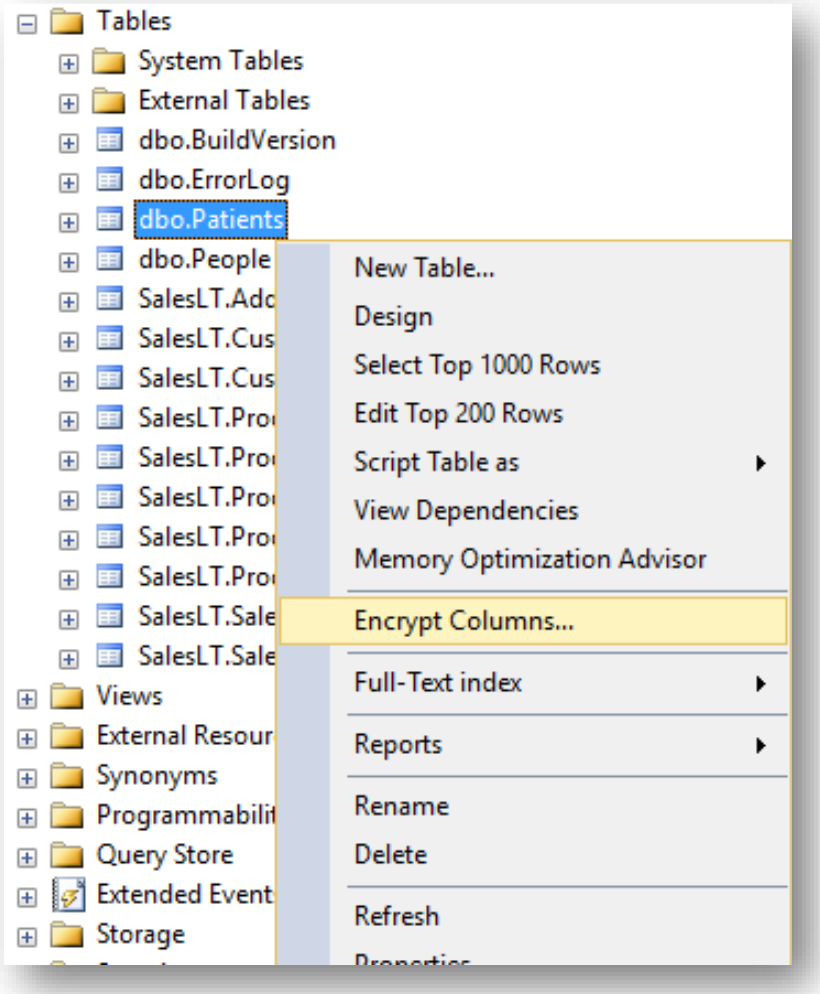
- Crypte les données d'une manière moins prévisible
- Plus sûr
- Ne permet pas les opérations de recherche

Always Encrypted

Convertir une Table existante pour utiliser AE

- Peut être effectué via SSMS UI
- Créer une nouvelle table et déplacer les données
- Doit avoir accès au certificate pour la CMK
- SSMS vous permet de générer un script Powershell à exécuter ultérieurement

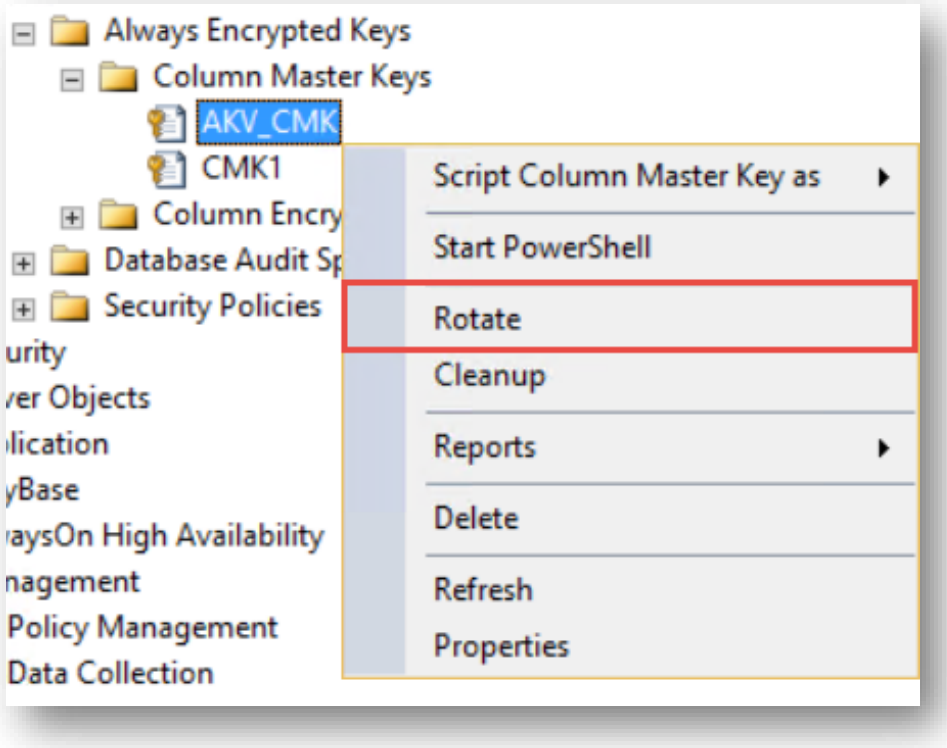
Déplacer une base SQL Always Encrypted comme n'importe quelle autre base



Always Encrypted

Rotation de la Column Master Key

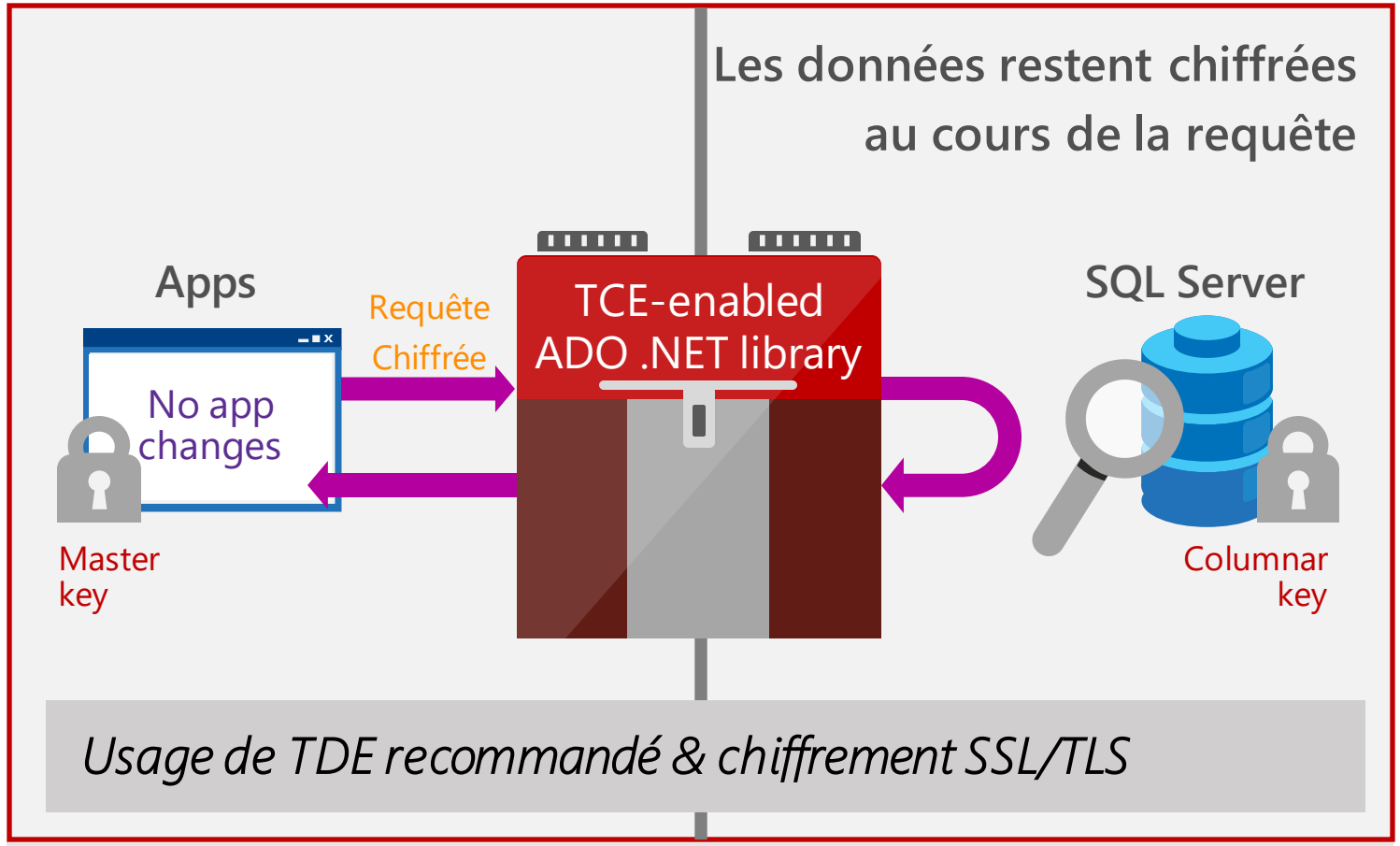
- Rotation des clés est parfois requise à des fins réglementaires
- La rotation de la Column Master Key ajoute une clé sous forme chiffrée à la Column Encryption Key
- Ne provoque pas le « rechiffrement » des données de la table



DEMO
SQL Always Encrypted

Always Encrypted

Résumé: Always Encrypted



Fonctionnalité

- ADO.Net client fournit le chiffrement transparent côté client, tandis que SQL Server exécute des requêtes T-SQL sur des données chiffrées

Avantages

- Les données sensibles restent cryptées et requêtables en tout temps on-premises & cloud (Pas d'accès aux DBA / Admin Azure)
- Des utilisateurs non autorisés n'ont jamais accès aux données ou aux clés
- Aucun changement sur l'application, nécessite juste un paramétrage de la base de données

Always Encrypted

Limitations actuelles sur Always Encrypted

- XML/Image/text/variant data types
- Filestream
- ROWGUID
- Partition columns
- Sparse columns
- Check/default constraints
- Referenced columns in FKeys
- Dynamic Data Masking
- StetchDB columns
- Transactional/Merge repl
- Linked Server queries
- Temporal
- Efficient inequality searches

Contrôle d'Accès

Accès Base de Données => ***Azure Active Directory Authentication*** (AAD)
Accès Application => ***Row-Level Security*** (RLS)
=> ***Dynamic Data Masking***

Azure AD Authentication

Contrôle d'Accès: Accès Base de Données

Centraliser la gestion des autorisations des utilisateurs

Gestion centrale des identités

Aide à stopper la prolifération des identités d'utilisateurs sur des serveurs de base de données.

Gestion de l'autorisation simplifiée

Les clients peuvent gérer les autorisations de base de données à l'aide des groupes Azure AD.

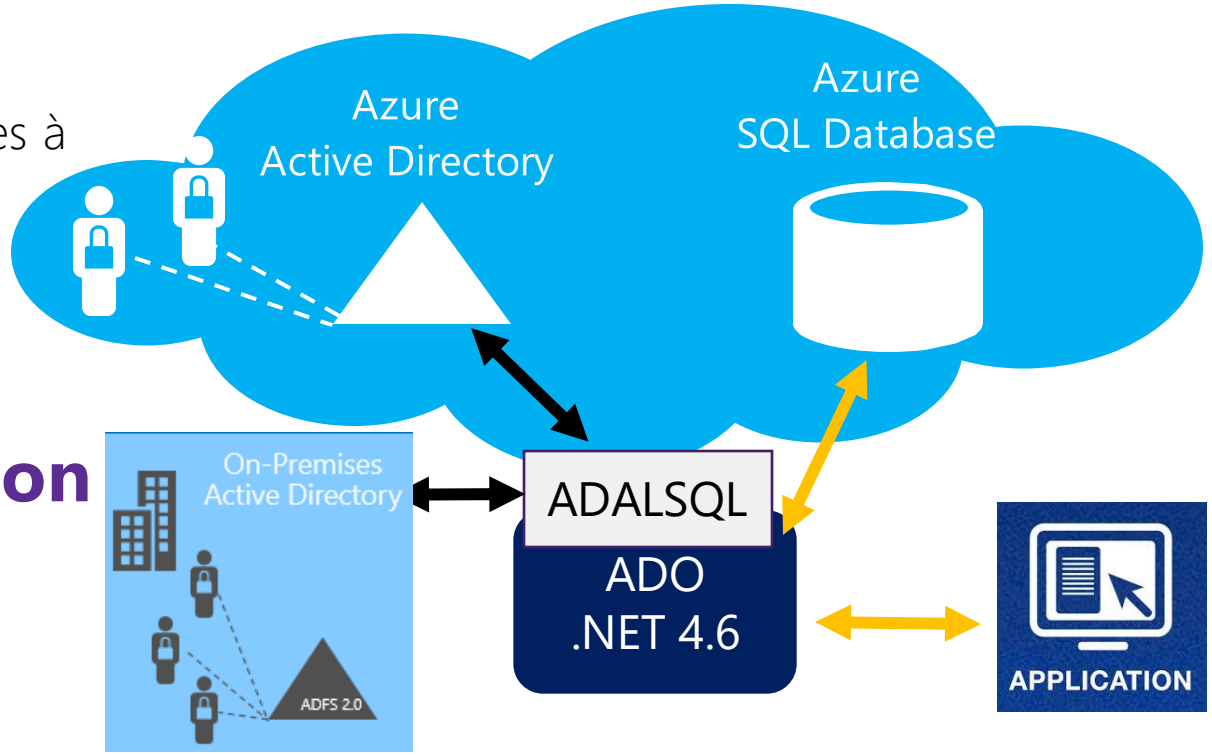
"Single Sign-On"

Une fois connecté à un ordinateur joint au domaine, les utilisateurs se connectent à leurs bases de données SQL, le portail Azure et les outils (par exemple, l'éditeur de requête) sans avoir à fournir des informations d'identification.

Azure AD Authentication

Un point central pour gérer les utilisateurs sur l'ensemble des services

- ✓ Alternative à l'authentification SQL Server
- ✓ Simplifie la gestion des autorisations à la base de données à l'aide des groupes externes d'Azure Active Directory
- ✓ Permet le changement de mot de passe à partir d'un point central



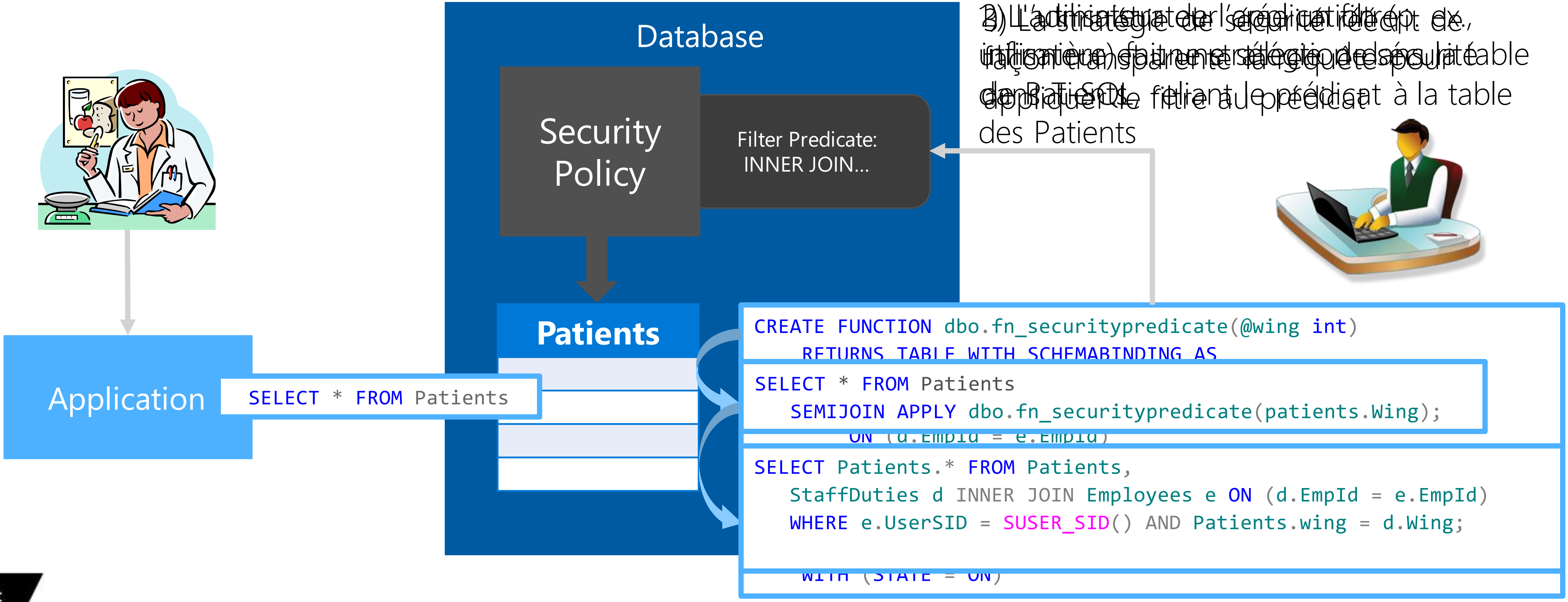
Plusieurs méthodes d'authentification

- ✓ **Username/password** pour les comptes Azure AD
- ✓ **Integrated Windows authentication**, pour les domaines fédérés qui sont authentifiés via Azure AD
- ✓ **Certificate-based authentication**, dans le cas où le certificat est enregistré dans Azure AD

Row-Level Security (RLS)

Contrôle d'Acces: Accès Application

RLS permet aux clients de contrôler l'accès aux lignes d'une table de base de données basée sur les caractéristiques de l'utilisateur qui exécute une requête



Dynamic Data Masking

Contrôle d'Accès: Accès Application

3) La stratégie de masquage dynamique des données sensibles de la table Employee


```
ALTER TABLE [Employee] ALTER COLUMN [SocialSecurityNumber]
ADD MASKED WITH (FUNCTION = 'partial(0,"***-**-",4)') NULL
ALTER TABLE [Employee] ALTER COLUMN [Email]
ADD MASKED WITH (FUNCTION = 'EMAIL()')

ALTER TABLE [Employee] ALTER COLUMN [Salary]
ADD MASKED WITH (FUNCTION = 'RANDOM(1,20000)')

GRANT UNMASK to admin1
```

Security Officer

```
SELECT [Name],
       [SocialSecurityNumber],
       [Email],
       [Salary]
FROM [Employee]
```

other login

	First Name	Social Security Number	Email	Salary
1	LILA	XXX-XX-XX37	lXX@XXXX.net	8940
2	JAMIE	XXX-XX-XX14	jXX@XXXX.com	19582
3	SHELLEY	XXX-XX-XX28	sXX@XXXX.net	3713
4	MARCELLA	XXX-XX-XX65	mXX@XXXX.net	11572
5	GILBERT	XXX-XX-XX87	gXX@XXXX.net	4487

admin1 login

	First Name	Social Security Num...	Email	Salary
1	LILA	758-10-9637	lila.barnett@comcast.net	1012794
2	JAMIE	113-29-4314	jamie.brown@ntlworld.com	1025713
3	SHELLEY	550-72-2028	shelley.lynn@charter.net	1040131
4	MARCELLA	903-94-5665	marcella.estrada@comcast.net	1040753
5	GILBERT	376-79-4787	gilbert.juarez@verizon.net	1041308

DEMO
Dynamic Data Masking
Row Level Security

Surveillance Proactive

Suivi & Détection = > ***Auditing & Threat Detection***

Auditing & Threat Detection

Surveillance et Proactive: Suivi & Detection

Surveiller et détecter des activités suspectes sur vos bases de données et rationaliser les tâches relatives à la conformité.

Respect de la réglementation

Auditing aide les clients de les entreprises à répondre aux normes de sécurité et aux exigences réglementaires (ex: PCI-DSS, HIPAA).

L'intelligence du Cloud

Des algorithmes propriétaires travaillent 24h/24 pour construire un profil comportemental de votre base de données et identifier les activités anormales et les menaces potentielles.

Enquêter et atténuer

Réagir et répondre aux menaces en temps réel, via des alertes courriel et le portail Azure. La Sécurité de l'entreprise est plus facile que jamais.

Statut: Auditing disponible, Threat Detection en Preview

Auditing & Threat Detection

Auditing

- ✓ Configuré via le portail Azure & les APIs standards
- ✓ Les journaux d'audit se trouvent dans votre compte Azure Storage
- ✓ Le portail Azure et les modèles Excel vous aident à analyser vos journaux d'audit

Threat Detection

- ✓ Configuré via le portail Azure & les APIs standards
- ✓ Plusieurs ensembles d'algorithmes:
  - Possibles vulnérabilités d'injection SQL
  - Éventuels exploits d'injection SQL
  - Accès à partir d'adresses IP anormales
  - …plus à venir!
- ✓ Notification immédiate lors de la détection des activités suspectes
- ✓ UX simplifiée vous aide à investiguer et atténuer en utilisant le portail Azure
- ✓ Intégration avec Azure Security Center

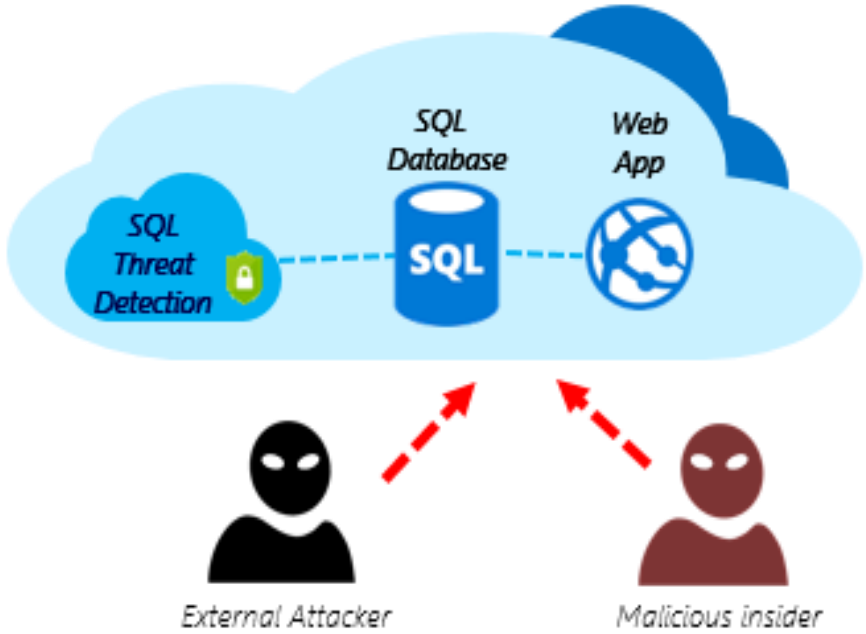
DEMO
Threat Detection en action

Auditing & Threat Detection

Azure SQL Database Threat Detection assure la sécurité en détectant les activités qui peuvent indiquer une menace telle que les attaques par injection SQL.

Les avantages de Azure SQL Database Threat Detection inclus:

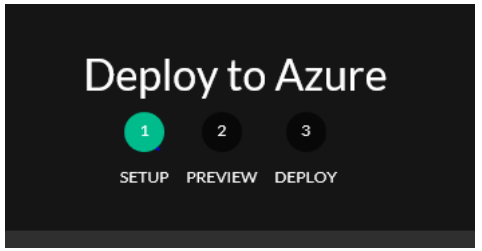
- Configuration simple de SQL threat detection
- Alertes email en cas de détection de requêtes suspectes indiquant d'éventuels événements d'injection SQL
- Capacité à explorer le journal d'audit au moment des événements suspects
- Pas besoin de mofidier la base de données ou le code de l'application
- Intégration avec Azure Portal et Microsoft Excel

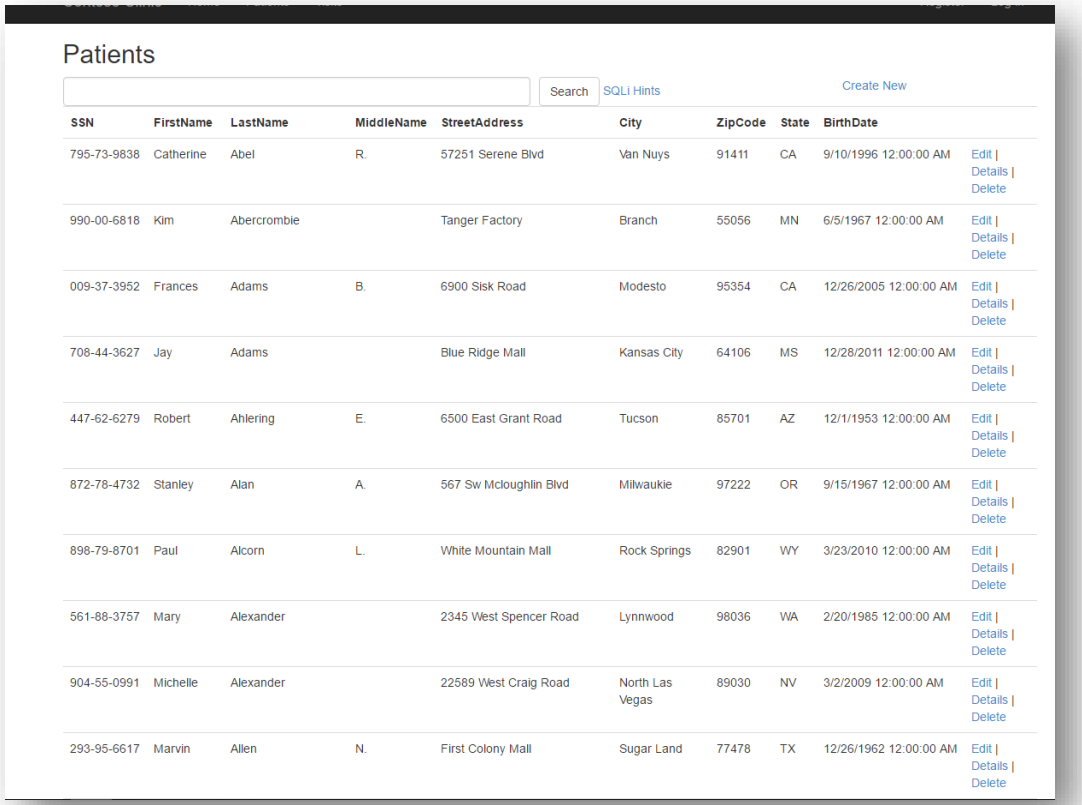


SQL Security Public Demo

Fonctionnalités incluses:

- Auditing & Threat Detection
- Always Encrypted
- Row Level Security (RLS)
- Dynamic Data Masking





Patients

Search SQLi Hints Create New

SSN	FirstName	LastName	MiddleName	StreetAddress	City	ZipCode	State	BirthDate	
795-73-9838	Catherine	Abel	R.	57251 Serene Blvd	Van Nuys	91411	CA	9/10/1996 12:00:00 AM	Edit | Details | Delete
990-00-6818	Kim	Abercrombie		Tanger Factory	Branch	55056	MN	6/5/1967 12:00:00 AM	Edit | Details | Delete
009-37-3952	Frances	Adams	B.	6900 Sisk Road	Modesto	95354	CA	12/26/2005 12:00:00 AM	Edit | Details | Delete
708-44-3627	Jay	Adams		Blue Ridge Mall	Kansas City	64106	MS	12/28/2011 12:00:00 AM	Edit | Details | Delete
447-62-6279	Robert	Ahlering	E.	6500 East Grant Road	Tucson	85701	AZ	12/1/1953 12:00:00 AM	Edit | Details | Delete
872-78-4732	Stanley	Alan	A.	567 Sw Mcloughlin Blvd	Milwaukie	97222	OR	9/15/1967 12:00:00 AM	Edit | Details | Delete
898-79-8701	Paul	Alcorn	L.	White Mountain Mall	Rock Springs	82901	WY	3/23/2010 12:00:00 AM	Edit | Details | Delete
561-88-3757	Mary	Alexander		2345 West Spencer Road	Lynnwood	98036	WA	2/20/1985 12:00:00 AM	Edit | Details | Delete
904-55-0991	Michelle	Alexander		22589 West Craig Road	North Las Vegas	89030	NV	3/2/2009 12:00:00 AM	Edit | Details | Delete
293-95-6617	Marvin	Allen	N.	First Colony Mall	Sugar Land	77478	TX	12/26/1962 12:00:00 AM	Edit | Details | Delete

Faites un essai sur GitHub:

https://github.com/Microsoft/azure-sql-security-sample

Microsoft
experiences'16
Palais des Congrès de Paris

MERCI !

#experiences

experiences.microsoft.fr

Microsoft


Microsoft
experiences'16
Mercredi 5 octobre • Palais des Congrès de Paris
Poursuivons la discussion avec
#experiences
@microsoftfrance @Technet_France @msdev_fr
experiences.microsoft.fr
Microsoft

Microsoft
experiences'16
Mercredi 5 octobre • Palais des Congrès de Paris

Notez cette session

Et tentez de gagner un SURFACE BOOK

Doublez votre chance en répondant aussi au questionnaire de satisfaction globale

** Le règlement est disponible sur demande au commissariat général de l'exposition. Image non-contractuelle*