UNIVERSITÉ DU QUÉBEC

CESI
CENTRE D'EXPERTISE EN SÉCURITÉ DE L'INFORMATION

TLP : VERT (DIFFUSION PERMISE)

Microsoft SQL Server 2016 : Recommandation de configuration sécurisée

CIS v3.0.0 du 22-02-2024

Juillet 2024

UNIVERSITÉ DU QUÉBEC

CESI
CENTRE D'EXPERTISE EN SÉCURITÉ DE L'INFORMATION

TLP : VERT (DIFFUSION PERMISE)

TABLE DES MATIERES

UNIVERSITÉ DU QUÉBEC

CESI
CENTRE D'EXPERTISE EN SÉCURITÉ DE L'INFORMATION

TLP : VERT (DIFFUSION PERMISE)

1 INTRODUCTION

La sécurité des bases de données est une priorité pour toute organisation cherchant à protéger ses informations sensibles et ses ressources critiques. Dans le réseau universitaire, les bases de données contiennent des informations précieuses, telles que les données des étudiants, les recherches académiques et les informations administratives. Microsoft SQL Server 2016 est une solution de gestion de base de données largement utilisée, mais elle doit être correctement configurée pour améliorer sa sécurité. Le Centre pour la sécurité de l'Internet (CIS) fournit des « benchmarks », qui sont des normes de configuration reconnues pour sécuriser les systèmes d'information. Ce guide détaille les recommandations du CIS Benchmark 3.0.0 pour Microsoft SQL Server 2016.

Dans un monde où les cybermenaces sont de plus en plus sophistiquées, il est crucial de suivre des pratiques de sécurité rigoureuses pour protéger les bases de données. Les attaques contre les bases de données peuvent entraîner des pertes de données, des violations de la confidentialité et des interruptions de service. En appliquant les recommandations du CIS, les administrateurs de bases de données dans un environnement universitaire peuvent réduire considérablement les risques et renforcer la sécurité de leur environnement SQL Server. La complexité et la diversité des utilisateurs et des dispositifs connectés dans les universités nécessitent une attention particulière pour sécuriser efficacement ces ressources critiques.

Ce guide s'adresse principalement aux administrateurs de bases de données, aux administrateurs système et aux professionnels de la sécurité opérant dans le réseau universitaire. Il vise à fournir des instructions claires et détaillées pour sécuriser les instances de Microsoft SQL Server 2016, en mettant l'accent sur les configurations de sécurité essentielles et les meilleures pratiques. En suivant ce guide, les universités peuvent s'assurer que leurs bases de données sont protégées contre les menaces courantes et conformes aux normes de sécurité reconnues, garantissant ainsi la confidentialité, l'intégrité et la disponibilité des données académiques et administratives.

Le *Benchmark CIS* a été créé à l'aide d'un processus d'examen consensuel composé d'une communauté mondiale d'experts en la matière.

Ce processus combine l'expérience du monde réel avec des informations basées sur des données pour créer des conseils spécifiques à la technologie afin d'aider les utilisateurs à sécuriser leurs environnements. Les participants au consensus apportent leur point de vue à partir d'un ensemble diversifié d'expériences, notamment le conseil, le développement de

logiciels, l'audit et la conformité, la recherche en matière de sécurité, les opérations, le gouvernement, et le domaine juridique.

Chaque critère de référence du CIS fait l'objet de deux phases d'examen par consensus :

La première phase
Elle a lieu lors de l'élaboration initiale du critère de référence. Au cours de cette phase, les experts en la matière se réunissent pour discuter, créer et tester des projets de travail du critère de référence. Cette discussion se poursuit jusqu'à ce qu'un consensus soit atteint sur les recommandations du critère de référence.

La deuxième phase
Elle commence après la publication du critère de référence. Au cours de cette phase, tous les commentaires fournis par la communauté Internet sont examinés par l'équipe de consensus en vue de leur intégration dans le critère de référence.

1.1 CONTEXTE

Dans un environnement universitaire, la sécurité des bases de données est cruciale pour protéger les informations sensibles des étudiants, du personnel et des recherches. Les universités disposent souvent de réseaux étendus avec de nombreux points d'accès, ce qui les rend vulnérables aux attaques. Il est essentiel de sécuriser les bases de données pour prévenir les accès non autorisés et les fuites de données. La diversité des utilisateurs, allant des étudiants aux chercheurs, crée une surface d'attaque variée et complexe nécessitant des mesures de sécurité robustes et adaptées.

Les universités gèrent un volume considérable de données personnelles, académiques et financières. Les informations concernant les étudiants, les résultats de recherches et les données administratives doivent être protégées pour respecter les réglementations en vigueur et préserver la confidentialité. Une configuration sécurisée de SQL Server 2016 contribue à garantir l'intégrité et la disponibilité de ces données critiques. Les données académiques, en particulier, peuvent être sensibles et stratégiques, nécessitant une protection renforcée contre les cyberattaques et surtout les accès non autorisés.

En raison de la nature ouverte des environnements universitaires avec de nombreux utilisateurs et appareils connectés, les bases de données peuvent être exposées à divers types de menaces. Les cyberattaques, telles que les injections SQL, les attaques par déni de service et les violations de données, peuvent entraîner des conséquences graves. Par conséquent, il est impératif d'adopter des mesures de sécurité robustes pour protéger les actifs informationnels

des universités. Ce guide fournit des recommandations spécifiques permettant de renforcer la sécurité des bases de données SQL Server 2016. Notre guide se base sur les critères de référence du CIS.

Ces critères se concentrent sur les paramètres de configuration technique utilisés pour maintenir ou renforcer la sécurité de la technologie concernée. Ils doivent être utilisés en conjonction avec d'autres tâches essentielles de cyberhygiène telles que :

- La recherche de vulnérabilités dans le système d'exploitation de base et la mise à jour rapide avec les derniers correctifs de sécurité.
- La surveillance des applications et des bibliothèques pour détecter les vulnérabilités et les mettre rapidement à jour avec les derniers correctifs de sécurité.

En fin de compte, les critères CIS sont conçus comme un élément clé d'un programme de cybersécurité complet.

1.2 OBJECTIF

L'objectif de ce guide est de fournir des instructions détaillées pour configurer SQL Server de manière sécurisée en suivant les recommandations des critères de référence du CIS. En appliquant ces configurations, vous réduirez les risques de sécurité liés à l'utilisation et protégerez vos données contre les menaces.

L'objectif de ce guide est de fournir des instructions détaillées pour sécuriser une installation de Microsoft SQL Server 2016 en suivant les recommandations du CIS Benchmark 3.0.0. En adoptant ces recommandations, les administrateurs peuvent renforcer la sécurité de leurs instances SQL Server et protéger les données contre les menaces. Ce guide est conçu pour également répondre aux besoins du réseau universitaire, où la protection des données académiques et administratives est primordiale.

De plus, ce guide fournit des informations pratiques et concrètes pour mettre en œuvre les recommandations du CIS Benchmark. Chaque section offre des étapes spécifiques et des conseils détaillés pour configurer correctement les paramètres de sécurité de SQL Server 2016. En suivant ce guide, les administrateurs peuvent minimiser les risques de sécurité et garantir la conformité avec les standards de sécurité reconnus. L'objectif ultime est de créer un environnement sécurisé pour les données universitaires, garantissant ainsi la confidentialité, l'intégrité et la disponibilité des informations critiques.

1.3 PORTEE

Ce guide couvre la configuration de sécurité de base, la configuration sécurisée de l'instance SQL Server, l'authentification, les permissions, l'audit, la surveillance, et la configuration des politiques de sécurité pour Microsoft SQL Server 2016. Il s'agit d'une approche complète pour sécuriser toutes les facettes de votre installation SQL Server, en tenant compte des exigences spécifiques des environnements universitaires.

La portée de ce guide inclut également des recommandations pour la configuration initiale du système, y compris les étapes pour accéder aux paramètres de configuration de SQL Server. En plus des configurations de base, ce guide traite des paramètres de sécurité avancés et des pratiques recommandées pour protéger les données au repos et en transit. Chaque section est conçue pour fournir des instructions claires et précises, facilitant ainsi la mise en œuvre des recommandations de sécurité dans un contexte universitaire, où les menaces peuvent être variées et complexes.

1.4 DEFINITIONS

Statut de l'évaluation
Un statut d'évaluation est inclus pour chaque recommandation. L'état d'évaluation indique si la recommandation donnée peut être automatisée ou si sa mise en œuvre nécessite des étapes manuelles.

Automatisée
Représente les recommandations pour lesquelles l'évaluation d'un contrôle technique peut être entièrement automatisée et validée par un état succès/échec. Les recommandations comprennent les informations nécessaires à la mise en œuvre de l'automatisation.

Manuel
Représente les recommandations pour lesquelles l'évaluation d'un contrôle technique ne peut pas être entièrement automatisée et nécessite tout ou en partie des étapes manuelles pour confirmer que l'état configuré est défini comme prévu. L'état attendu peut varier en fonction de l'environnement.

Description
Elle comprend les informations détaillées relatives à l'environnement concerné par la recommandation. Dans certains cas, la description comprendra la valeur recommandée.

Justification
Elle représente la motivation détaillée de la recommandation afin de fournir à l'utilisateur une compréhension claire et concise de l'importance de la recommandation.

Analyse d'impact
Toutes les conséquences en matière de sécurité, de fonctionnalité ou d'exploitation qui peuvent résulter de l'application de la recommandation.

Procédure d'audit
Instructions systématiques permettant de déterminer si le système cible est conforme à la recommandation.

Procédure de remédiation
Instructions systématiques pour appliquer les recommandations au système cible afin de le mettre en conformité avec la recommandation.

Valeur par défaut
Valeur par défaut pour le paramètre donné dans cette recommandation, si elle est connue. Si elle n'est pas connue, c'est la valeur « non configurée » ou « non définie » qui sera appliquée.

Profil
Ensemble de recommandations visant à sécuriser une technologie ou une plate-forme de support. La plupart des référentiels incluent au moins un profil de niveau 1 et de niveau 2.

Définitions des profils
Les profils de configuration suivants sont définis par cette évaluation comparative :

a) **Niveau 1 (L1) - Environnement d'entreprise (utilisation générale)**
Les éléments de ce profil sont destinés à :
- ❖ Être la base de départ pour la plupart des organisations;
- ❖ Être pratiques et prudents;
- ❖ Offrir un avantage clair en matière de sécurité;
- ❖ Ne pas entraver l'utilité de la technologie au-delà des moyens acceptables.

b) **Niveau 1 (L1) + BitLocker (BL)**
Ce profil étend le profil « Niveau 1 (L1) » et inclut des recommandations relatives à BitLocker.

c) **Niveau 2 (L2) - Environnement de haute sécurité/données sensibles (fonctionnalité limitée)**
Ce profil prolonge le profil de « niveau 1 (L1) ». Les éléments de ce profil présentent une ou plusieurs des caractéristiques suivantes :
- ❖ Ils sont destinés à des environnements ou à des cas d'utilisation où la sécurité est plus importante que la facilité de gestion et d'utilisation;
- ❖ Ils peuvent nuire à l'utilité ou aux performances de la technologie;
- ❖ Limiter la capacité de gestion/accès à distance.

Remarque : la mise en œuvre du niveau 2 exige que les paramètres des niveaux 1 et 2 soient appliqués.

d) **Niveau 2 (L2) + BitLocker (BL)**
Ce profil étend le profil « Niveau 2 (L2) » et inclut des recommandations relatives à BitLocker.

2 SECURITE DE BASE

Les paramètres de base de SQL Serveur 2016 permettent d'avoir une configuration saine et fonctionnelle de la base de données. Elle jette également les bases adéquates permettant de suivre les recommandations de configurations sécuritaires.

2.1 PARAMETRES DE BASE

Configuration de l'Instance SQL Server :

- ✓ Changer le port par défaut : Changez le port par défaut pour rendre l'instance SQL Server moins visible.

- ✓ Désactiver les protocoles inutilisés : Désactivez les protocoles non nécessaires pour réduire la surface d'attaque.

Configuration de l'authentification :

Comme mentionné précédemment, changez le port par défaut pour rendre l'instance SQL Server moins visible.

- ✓ Activer l'Authentification Windows uniquement : L'Authentification Windows utilise les mécanismes de sécurité de Windows, ce qui offre une meilleure sécurité que l'authentification SQL Server.

Pour activer l'Authentification Windows uniquement :

Ouvrez SQL Server Management Studio.

Connectez-vous à l'instance SQL Server.

Faites un clic droit sur le serveur, sélectionnez Propriétés, puis allez dans l'onglet Sécurité et choisissez Authentification Windows.

- ✓ Désactiver le Compte « sa » : Le compte « sa » est un compte administrateur par défaut souvent ciblé par les attaquants. Désactivez-le ou renommez-le pour réduire les risques.

Configuration des permissions :

- ✓ Utiliser des comptes de services minimaux : Assurez-vous que les comptes de service ont uniquement les permissions nécessaires pour fonctionner.

- ✓ Revues régulières des permissions : Effectuez des revues régulières des permissions pour vous assurer qu'elles sont appropriées et qu'aucun accès non autorisé n'est accordé.

Audit et Surveillance :

- ✓ Activer l'audit SQL Server : Configurez l'audit pour suivre les actions critiques sur le serveur et les bases de données.

Pour activer l'audit :

Ouvrez SQL Server Management Studio.

Allez dans Sécurité > Audits et configurez les audits nécessaires.

- ✓ Configurer des alertes pour les activités suspectes : Configurez des alertes pour surveiller les activités suspectes ou non autorisées et réagir rapidement en cas d'incident.

Configuration des Politiques de Sécurité :

- ✓ Activer Transparent Data Encryption (TDE) : Activez TDE pour protéger les données au repos en chiffrant les fichiers de la base de données.

Pour activer TDE :

Créez une clé maître dans la base de données master.

Créez un certificat sécurisé par cette clé maître.

Créez une clé de chiffrement de base de données (DEK) protégée par le certificat.

Activez TDE sur la base de données.

- ✓ Configurer les sauvegardes chiffrées : Assurez-vous que toutes les sauvegardes de bases de données sont chiffrées pour protéger les données en cas de vol ou de perte.

3 RECOMMANDATION RELATIVE AUX CRITERES DE CIS POUR MICROSOFT SQL SERVER 2016

Cette section contient tous les contrôles recommandés par le CIS. Certains contrôles sont configurés par défaut lors de l'installation de MS SQL Server 2016. La mise en œuvre de ces contrôles permettra d'améliorer la sécurité de votre base de données.

- **Mettre en œuvre et gérer un pare-feu sur les serveurs**

  Implémenter et gérer un pare-feu sur les serveurs, le cas échéant. Les exemples d'implémentation incluent un pare-feu virtuel, un pare-feu de système d'exploitation ou un agent de pare-feu tiers.

- **Mise en œuvre et gestion d'un pare-feu sur les appareils des utilisateurs finaux**

  Mettre en œuvre et gérer un pare-feu basé sur l'hôte ou un outil de filtrage des ports sur les appareils des utilisateurs finaux, avec une règle de refus par défaut qui bloque tout le trafic à l'exception des services et des ports explicitement autorisés.

- **Veiller à ce que seuls les ports, protocoles et services approuvés fonctionnent**

  Veiller à ce que seuls les ports, protocoles et services en écoute sur un système dont les besoins professionnels ont été validés soient exécutés sur chaque système.

Recommandation de référence CIS		Contrôle en place	
		Oui	Non
1	**Installation, mises à jour et correctifs**		
1.1	S'assurer que les derniers Service Pack et Hotfixe de SQL Server sont installés (Manuel).	☐	☐
1.2	S'assurer que des serveurs membres à fonction unique (*Single-Function Member Servers*) sont utilisés (manuel).	☐	☐
2	**Réduction de la surface**		
2.1	S'assurer que l'option de configuration du serveur « Ad Hoc Distributed Queries » est réglée sur « 0 » (automatique).	☐	☐
2.2	Assurez-vous que l'option de configuration du serveur « CLR activé » est réglée sur « 0 » (automatisé).	☐	☐

Recommandation de référence CIS		Contrôle en place	
		Oui	Non
2.3	Assurez-vous que l'option de configuration du serveur « Cross DB Ownership Chaining » est réglée sur « 0 » (automatique).	☐	☐
2.4	Assurez-vous que l'option de configuration du serveur « Database Mail XPs » est réglée sur « 0 » (automatisée).	☐	☐
2.5	S'assurer que l'option de configuration du serveur « Ole Automation Procedures » est réglée sur « 0 » (automatisé).	☐	☐
2.6	Assurez-vous que l'option de configuration du serveur « Accès à distance » est réglée sur « 0 » (automatisé).	☐	☐
2.7	Assurez-vous que l'option de configuration du serveur « Connexions d'administration à distance » est réglée sur « 0 » (automatisée).	☐	☐
2.8	Assurez-vous que l'option de configuration du serveur « Scan for Startup Procs » est réglée sur « 0 » (automatisé).	☐	☐
2.9	S'assurer que la propriété « *Trustworthy* » de la base de données est réglée sur « Off » (automatisée).	☐	☐
2.10	Assurez-vous que les protocoles inutiles du serveur SQL sont désactivés (manuel).	☐	☐
2.11	S'assurer que SQL Server est configuré pour utiliser des ports non standard (automatisé).	☐	☐
2.12	S'assurer que l'option « Hide Instance » est réglée sur « Yes » pour les instances de production du serveur SQL (automatisé).	☐	☐

Recommandation de référence CIS		Contrôle en place	
		Oui	Non
2.13	Assurez-vous que le compte de connexion « sa » est réglé sur « désactivé » (automatisé).	☐	☐
2.14	S'assurer que le compte de connexion « sa » a été renommé (automatique).	☐	☐
2.15	Assurez-vous que l'option de configuration du serveur « xp_cmdshell » est réglée sur « 0 » (automatique).	☐	☐
2.16	Assurez-vous que le paramètre « AUTO_CLOSE » est réglé sur « OFF » pour les bases de données contenues (automatisées).	☐	☐
2.17	S'assurer qu'il n'existe pas de connexion avec le nom « sa » (automatisé).	☐	☐
3	**Authentification et autorisation**		
3.1	Assurez-vous que la propriété « Authentification du serveur » est définie sur « Mode d'authentification Windows » (automatisé).	☐	☐
3.2	S'assurer que les permissions CONNECT de l'utilisateur « guest » sont révoquées dans toutes les bases de données du serveur SQL (automatisé).	☐	☐
3.3	S'assurer que les « utilisateurs orphelins » sont supprimés des bases de données SQL Server (automatisé).	☐	☐
3.4	S'assurer que l'authentification SQL n'est pas utilisée dans les bases de données contenues (automatisé).	☐	☐
3.5	S'assurer que le compte de service MSSQL du serveur SQL n'est pas un administrateur (manuel).	☐	☐

Recommandation de référence CIS		Contrôle en place	
		Oui	Non
3.6	S'assurer que le compte de service SQLAgent du serveur SQL n'est pas un administrateur (manuel).	☐	☐
3.7	S'assurer que le compte du service Full-Text du serveur SQL n'est pas un administrateur (manuel).	☐	☐
3.8	Assurez-vous que seules les autorisations par défaut spécifiées par Microsoft sont accordées au rôle de serveur public (automatisé).	☐	☐
3.9	S'assurer que les groupes Windows BUILTIN ne sont pas des connexions SQL (automatisé).	☐	☐
3.10	S'assurer que les groupes locaux Windows ne sont pas des connexions SQL (automatisé).	☐	☐
3.11	S'assurer que le rôle public de la base de données msdb n'a pas accès aux proxys de l'agent SQL (automatisé).	☐	☐
4	**Politiques en matière de mots de passe**		
4.1	S'assurer que l'option « MUST_CHANGE » est activée pour toutes les connexions authentifiées par SQL (manuel).	☐	☐
4.2	S'assurer que l'option « CHECK_EXPIRATION » est activée pour toutes les connexions SQL authentifiées dans le rôle d'administrateur système (automatisé).	☐	☐
4.3	S'assurer que l'option « CHECK_POLICY » est activée pour toutes les connexions SQL authentifiées (automatisées).	☐	☐

Recommandation de référence CIS		Contrôle en place	
		Oui	Non
5	**Audit et journalisation**		
5.1	Assurez-vous que le « Nombre maximal de fichiers journaux d'erreurs » est supérieur ou égal à « 12 » (automatisé).	☐	☐
5.2	Assurez-vous que l'option de configuration du serveur « Trace par défaut activée » est réglée sur « 1 » (automatique).	☐	☐
5.3	Assurez-vous que l'option « Audit des connexions » est réglée sur « connexions échouées » (automatisé).	☐	☐
5.4	Assurez-vous que l'audit du serveur SQL est configuré pour capturer à la fois les connexions échouées et les connexions réussies (automatisé).	☐	☐
6	**Développement d'applications**		
6.1	Veillez à ce que les données saisies par les utilisateurs des bases de données et des applications soient assainies (manuel).	☐	☐
6.2	S'assurer que l'ensemble des permissions de l'assemblage CLR est défini sur « SAFE_ACCESS » pour tous les assemblages CLR (automatisé).	☐	☐
7	**Cryptage**		
7.1	Assurez-vous que l'algorithme de cryptage des clés symétriques est défini sur « AES_128 » ou sur une valeur supérieure dans les bases de données hors système (automatisé).	☐	☐

Recommandation de référence CIS		Contrôle en place	
		Oui	Non
7.2	Assurez-vous que la taille de la clé asymétrique est définie sur « supérieure ou égale à 2048 » dans les bases de données hors système (automatisé).	☐	☐
7.3	Veiller à ce que les sauvegardes de la base de données soient cryptées (automatisées).	☐	☐
7.4	S'assurer que le chiffrement du réseau est configuré et activé (automatisé).	☐	☐
7.5	S'assurer que les bases de données sont cryptées avec TDE (automatisé).	☐	☐
8	**Annexe : Considérations supplémentaires**		
8.1	Assurez-vous que le service de navigation du serveur SQL est configuré correctement (manuel).	☐	☐

4 ANNEXE : QUELQUES DEFINITIONS

Terme/Sigle	Signification
Service Pack	Ensemble cumulé de mises à jour, de corrections, d'améliorations et de nouvelles fonctionnalités pour un logiciel spécifique, publié par Microsoft.
Hotfix	Mise à jour rapide conçue pour corriger un problème spécifique rencontré par un utilisateur, souvent pour des problèmes critiques de sécurité ou des bogues importants.

Terme/Sigle	Signification
Single-Function Member Servers	Serveurs membres configurés pour exécuter une seule fonction ou un rôle spécifique, réduisant les risques en limitant les services et applications sur le même serveur.
Ad Hoc Distributed Queries	Fonctionnalité permettant d'exécuter des requêtes distribuées ponctuelles, souvent pour accéder à des données provenant de sources externes ou hétérogènes.
CLR (Common Language Runtime)	Environnement d'exécution permettant l'exécution de code managé dans SQL Server, écrit en C# ou VB.NET, pour créer des fonctions, procédures stockées et déclencheurs.
SAFE_ACCESS	Niveau de permission pour les assemblages CLR indiquant que le code managé est limité à l'accès aux ressources sécurisées et aux opérations non dangereuses.
Cross DB Ownership Chaining	Chaîne de possession entre bases de données différentes, permettant l'accès à des objets dans plusieurs bases de données avec les permissions appropriées.
Database Mail XPs	Extension permettant à SQL Server d'envoyer des courriels via le service Database Mail, nécessitant une configuration et une sécurisation appropriées.
Ole Automation Procedures	Procédures stockées permettant à SQL Server d'interagir avec les composants COM (Component Object Model), pouvant représenter un risque de sécurité si mal gérées.

Terme/Sigle	Signification
Accès à distance	Configuration permettant aux connexions distantes d'accéder à SQL Server, pouvant poser des risques de sécurité s'il n'est pas contrôlé.
Scan for Startup Procs	Option de configuration permettant à SQL Server de scanner et exécuter des procédures stockées spécifiées au démarrage du serveur.
Trustworthy	Propriété d'une base de données indiquant si elle peut être considérée comme *digne de confiance*, permettant certaines actions potentiellement dangereuses si activée.
Protocoles inutiles	Protocoles de communication non nécessaires pour le fonctionnement de SQL Server, pouvant être désactivés pour réduire la surface d'attaque.
Ports non standard	Ports différents des valeurs par défaut utilisés par SQL Server pour améliorer la sécurité en réduisant les risques de détection par les attaquants.
Hide Instance	Configuration permettant de masquer une instance de SQL Server pour qu'elle ne soit pas visible lors des requêtes réseau, renforçant la sécurité.
Compte de connexion « sa »	Compte administrateur par défaut de SQL Server, souvent ciblé par les attaquants, pouvant être désactivé ou renommé pour améliorer la sécurité.

Terme/Sigle	Signification
xp_cmdshell	Procédure étendue permettant l'exécution de commandes de l'interpréteur de commandes Windows (cmd.exe) depuis SQL Server, représentant un risque de sécurité significatif et nécessitant une gestion stricte.
AUTO_CLOSE	Option de base de données fermant automatiquement la base de données lorsqu'il n'y a aucune connexion active, pouvant impacter les performances et non recommandée pour les bases de données à usage fréquent.
Mode d'authentification Windows	Mode d'authentification de SQL Server utilisant les identifiants de Windows pour valider l'accès des utilisateurs.
Permissions CONNECT de l'utilisateur « guest »	Autorisations accordées à l'utilisateur par défaut « guest » dans SQL Server, souvent révoquées pour des raisons de sécurité.
Utilisateurs orphelins	Comptes d'utilisateurs dans une base de données SQL Server sans connexion associée au niveau du serveur, résultant souvent de restaurations ou de migrations de bases de données.
Compte de service MSSQL	Compte sous lequel le service principal de SQL Server (MSSQL) s'exécute, devant être limité en permissions pour des raisons de sécurité.
Compte de service SQLAgent	Compte sous lequel le service SQL Server Agent s'exécute, devant être limité en permissions pour des raisons de sécurité.

Terme/Sigle	Signification
Compte de service Full-Text	Compte sous lequel le service Full-Text de SQL Server s'exécute, devant être limité en permissions pour des raisons de sécurité.
Rôle de serveur public	Rôle par défaut attribué à tous les utilisateurs de SQL Server, fournissant des autorisations minimales de base.
Groupes Windows BUILTIN	Groupes de sécurité intégrés à Windows utilisés pour attribuer des permissions et des rôles aux utilisateurs et groupes Windows dans SQL Server.
Groupes locaux Windows	Groupes locaux de sécurité sur le serveur Windows, pouvant avoir des permissions SQL, souvent limitées pour des raisons de sécurité.
Proxys de l'agent SQL	Comptes permettant à SQL Server Agent d'exécuter des travaux avec des autorisations spécifiques, souvent restreints pour des raisons de sécurité.
Permissions de l'assemblage CLR « SAFE_ACCESS »	Niveau de permission pour les assemblages CLR indiquant que le code managé est limité à l'accès aux ressources sécurisées et aux opérations non dangereuses.
AES_128	Algorithme de cryptage symétrique utilisé pour protéger les données, recommandé pour sa sécurité et ses performances.
Clé asymétrique	Type de clé cryptographique utilisant une paire de clés (publique et privée) pour le chiffrement et le déchiffrement des données, avec des tailles souvent égales ou supérieures à 2048 bits pour la sécurité.

Terme/Sigle	Signification
Cryptage des sauvegardes	Processus de chiffrement des sauvegardes de bases de données pour protéger les données en cas de vol ou de perte.
Bases de données cryptées avec TDE	Utilisation de Transparent Data Encryption (TDE) pour chiffrer les bases de données au repos et protéger les fichiers de données et de journaux.
Pare-feu	Système de sécurité réseau qui surveille et contrôle le trafic réseau entrant et sortant en fonction de règles de sécurité prédéfinies.
Instance SQL Server	Une installation distincte de SQL Server pouvant coexister sur le même serveur physique avec d'autres instances, chacune fonctionnant de manière indépendante avec ses propres bases de données, connexions, et configurations.
Multi-Instance	Capacité d'un serveur physique à héberger plusieurs instances de SQL Server, permettant une isolation et une gestion indépendante des différentes applications et bases de données.
Instance Name	Nom unique attribué à une instance de SQL Server pour la différencier des autres instances sur le même serveur physique.
Default Instance	Instance principale de SQL Server sur un serveur, accessible sans spécifier de nom d'instance. Généralement référencée par le nom du serveur.
Collation	Ensemble de règles qui déterminent comment les données de caractères sont triées et comparées dans une base de données.

Terme/Sigle	Signification
SQL Server Browser	Service qui fournit des informations sur les instances de SQL Server sur le réseau, permettant aux clients de se connecter aux instances nommées.
TempDB	Base de données système utilisée par SQL Server pour stocker les objets temporaires comme les tables temporaires, les curseurs et les objets intermédiaires des transactions.
Master Database	Base de données système contenant toutes les informations sur l'instance de SQL Server, y compris les connexions, les configurations système et les informations sur les autres bases de données.
Model Database	Modèle de base de données utilisé comme modèle pour toutes les nouvelles bases de données créées dans l'instance de SQL Server.
msdb	Base de données système utilisée par SQL Server Agent pour stocker les informations sur les travaux, les alertes, les opérateurs, et les historiques des sauvegardes.
Resource Database	Base de données système cachée contenant les objets système lus uniquement qui sont utilisés par SQL Server.
SSIS (SQL Server Integration Services)	Composant de SQL Server utilisé pour les tâches d'extraction, de transformation et de chargement (ETL) de données.
SSRS (SQL Server Reporting Services)	Composant de SQL Server utilisé pour créer, déployer et gérer des rapports interactifs et imprimables.

Terme/Sigle	Signification
SSAS (SQL Server Analysis Services)	Composant de SQL Server utilisé pour les analyses de données en ligne (OLAP) et les modèles de données multidimensionnels.
Data Masking	Technique utilisée pour protéger les données sensibles en les remplaçant par des valeurs fictives ou anonymes.
Always Encrypted	Fonctionnalité de SQL Server permettant de chiffrer les données sensibles de manière à ce qu'elles restent chiffrées en transit et au repos, tout en permettant aux applications de les traiter sous forme chiffrée.
Row-Level Security (RLS)	Fonctionnalité permettant de restreindre l'accès aux données au niveau de la ligne, en fonction des droits de l'utilisateur qui exécute la requête.
Dynamic Data Masking (DDM)	Fonctionnalité permettant de masquer les données sensibles en temps réel pour empêcher les utilisateurs non autorisés de les voir, tout en permettant aux utilisateurs autorisés d'accéder aux données originales.
SQL Injection	Type d'attaque où un attaquant injecte du code SQL malveillant dans une requête pour manipuler la base de données.
TLS (Transport Layer Security)	Protocole de sécurité qui chiffre les données échangées entre le client et le serveur pour protéger la confidentialité et l'intégrité des informations.
Encryption	Processus de transformation des données en une forme codée pour empêcher l'accès non autorisé.

Terme/Sigle	Signification
Authentication	Processus de vérification de l'identité d'un utilisateur ou d'un système avant de lui permettre d'accéder aux ressources.
Authorization	Processus de détermination des droits et des permissions d'un utilisateur ou d'un système, une fois l'authentification réussie.
Auditing	Processus de suivi et d'enregistrement des actions effectuées dans le système pour des raisons de sécurité et de conformité.
Backup	Processus de copie des données pour les protéger contre la perte ou les dommages et pour permettre leur restauration en cas de sinistre.
Restore	Processus de récupération des données à partir d'une sauvegarde pour les remettre à leur état original après une perte ou un dommage.
RAID (Redundant Array of Independent Disks)	Technologie de stockage qui combine plusieurs disques durs pour améliorer les performances ou la redondance des données.
Failover Cluster	Configuration de haute disponibilité qui permet à plusieurs serveurs de fonctionner ensemble pour assurer une disponibilité continue des services en cas de défaillance d'un serveur.
Replication	Processus de copie et de distribution des données et des objets de base de données d'une base de données à une autre pour assurer la cohérence et la disponibilité des données.

Terme/Sigle	Signification
Mirroring	Technique de haute disponibilité qui maintient une copie en temps réel des données d'une base de données principale sur une base de données miroir pour assurer la continuité des services en cas de défaillance.
Log Shipping	Méthode de sauvegarde et de restauration des journaux de transaction d'une base de données primaire à une base de données secondaire pour assurer la continuité des services et la récupération des données en cas de sinistre.
Transparent Data Encryption (TDE)	Méthode de chiffrement des données en repos pour protéger les bases de données contre l'accès non autorisé aux fichiers de données et de journal.
Public Role	Rôle par défaut attribué à tous les utilisateurs de SQL Server, fournissant des autorisations minimales de base.
Extended Events	Système de surveillance léger pour collecter des informations sur les performances, les problèmes de sécurité et d'autres événements dans SQL Server.
SQL Server Management Studio (SSMS)	Outil intégré pour gérer les instances de SQL Server, configurer la sécurité, surveiller les performances et effectuer des tâches administratives.
Data Loss Prevention (DLP)	Stratégies et technologies utilisées pour prévenir la fuite de données sensibles en dehors de l'organisation.

Terme/Sigle	Signification
Policy-Based Management	Fonctionnalité permettant de créer et d'appliquer des règles de gestion pour les instances SQL Server afin de maintenir la conformité et les bonnes pratiques.
Resource Governor	Fonctionnalité permettant de gérer la distribution des ressources (CPU et mémoire) entre différentes charges de travail pour assurer des performances optimales et éviter la contention des ressources.
SQL Server Audit	Fonctionnalité intégrée pour surveiller et enregistrer les événements de sécurité et d'accès aux données dans SQL Server pour des raisons de conformité et d'audit.
Server Principal	Identité au niveau du serveur, comme une connexion SQL Server ou un groupe Windows, utilisée pour authentifier et autoriser les utilisateurs dans SQL Server.
Database Principal	Identité au niveau de la base de données, comme un utilisateur, un rôle ou un groupe d'applications, utilisée pour gérer l'accès aux objets de la base de données.
Contained Database	Type de base de données où toutes les métadonnées nécessaires pour définir l'application sont stockées dans la base de données elle-même, permettant une portabilité plus facile entre les instances de SQL Server.
Temporal Tables	Fonctionnalité permettant de suivre et d'enregistrer l'historique complet des changements de données sur une table de base de données.

Terme/Sigle	Signification
Database Encryption Key (DEK)	Clé utilisée pour chiffrer une base de données protégée par Transparent Data Encryption (TDE).
Endpoint	Objet de serveur définissant la manière dont SQL Server communique sur le réseau, utilisé pour configurer et gérer les communications réseau, comme l'activation de mirroring ou de services Web.
SQL Server Agent	Composant de SQL Server utilisé pour planifier et exécuter des tâches automatisées telles que les sauvegardes, les indexations, et l'envoi d'alertes.
Linked Server	Configuration permettant à SQL Server de traiter des commandes SQL sur des bases de données externes situées sur des serveurs distincts.

5 RECOMMANDATION POUR LA MISE EN ŒUVRE DES CONTROLES CIS

Microsoft SQL Server 2016 - Recommandation pour la mise en oeuvre des controles CIS.pdf

6 ANALYSE DE CONFORMITE

Ci-dessous, un exemple de processus pouvant être utilisé (dans notre cas) pour avoir un état des lieux ainsi qu'une analyse de conformité des contrôles CIS avec un outil comme Tenable.sc.

Processus de durcissement du système d'exploitation v1.0.pdf

7 REVISIONS

Date de révision : 2024-07-08