SQL Audit Platform

RAPPORT D'AUDIT SQL SERVER

PRÉPARÉ POUR

SRV-APP-01

PRODUCTION · Microsoft SQL Server 2016 (SP3) · Standard Edition (64-bit)

· srv-app-01.atlantique.local

Score global de santé

Moyen C

sur 100

Premier audit — pas encore de tendance

AUDIT RÉALISÉ LE	DOCUMENT GÉNÉRÉ LE	COLLECTEUR
09 septembre 2026	23 septembre 2026	4.2.0

Synthèse pour la direction

70

Score global de santé

Moyen C

Premier audit — pas encore de tendance

Sécurité	Performance	Résilience	Opérations
65/100	96/100	75/100	84/100

285	29	1	9	10
CONFORMES	ÉCARTS	AVERTISSEMENTS	CRITIQUES	ÉLEVÉS

90

Posture de sécurité technique — CIS SQL Server L1 (échantillon)

56 contrôle(s) conforme(s) sur 62 évalué(s)

Ces contrôles contribuent aussi aux mesures techniques RGPD (Art. 32) et NIS2 (Art. 21).

Taux de conformité sur l'échantillon de contrôles CIS testés par la plateforme — pas une couverture du référentiel CIS complet.

Risques métier prioritaires

Traduits en langage métier, classés par enjeu. Le risque est exprimé en niveau (Élevé / Moyen / Faible) et en effort, sans chiffrage financier.

1 Vos sauvegardes ne protègent pas d'une panne ou d'une attaque

CRITIQUE

En cas de panne disque, de corruption ou de ransomware, vous risquez de perdre des données sans pouvoir les restaurer.

NIVEAU DE RISQUE **Critique** EFFORT **Élevé**

Piste recommandée Planifiez des sauvegardes Full hebdomadaires minimum

2 Votre base de données est exposée à un accès non autorisé

CRITIQUE

Une faille de sécurité peut permettre le vol ou la fuite de vos données clients et métier.

NIVEAU DE RISQUE **Critique** EFFORT **Faible**

Piste recommandée Désactivez le compte SA et créez des comptes nommés dédiés pour les administrateurs — le compte SA est une cible privilégiée des attaques par force brute. Intervention rapide, faible risque (vérifiez au préalable qu'aucune application ne s'y connecte).

3 Votre base risque de s'arrêter sans reprise garantie

CRITIQUE

Si votre continuité de service n'est pas garantie, une panne peut interrompre votre activité plusieurs heures ou jours.

NIVEAU DE RISQUE **Critique** EFFORT **Élevé**

Piste recommandée Lancez une vérification d'intégrité complète de la base, identifiez l'étendue de la corruption, puis restaurez les pages ou la base à partir d'une sauvegarde saine — une corruption non traitée entraîne une perte de données. Intervention urgente, risque élevé (faites-vous accompagner avant toute réparation).

4

La configuration du serveur s'écarte des bonnes pratiques

CRITIQUE

Des réglages inadaptés peuvent fragiliser la stabilité, la sécurité ou les performances de votre base.

NIVEAU DE RISQUE **Critique** EFFORT **Faible**

Piste recommandée Plafonnez la mémoire maximale du serveur en réservant de la RAM à l'OS (règle de départ : RAM totale - 4 Go, ou - 10 % au-delà de 16 Go) — sans plafond, SQL Server peut affamer le système et provoquer du swap. Intervention rapide, faible risque.

5

Vos données sensibles ne sont pas chiffrées

CRITIQUE

En cas de vol de fichiers ou de support, les données restent lisibles et la conformité RGPD n'est pas assurée.

NIVEAU DE RISQUE **Critique** EFFORT **Élevé**

Piste recommandée Sauvegardez chaque certificat TDE avec sa clé privée et conservez-les hors du serveur, dans un coffre sécurisé — sans cette sauvegarde, une base chiffrée devient irrécupérable en cas de sinistre. Intervention rapide, faible risque (protégez impérativement le mot de passe de la clé).

6

L'entretien régulier de la base n'est pas en place

CRITIQUE

Sans maintenance, les problèmes de données passent inaperçus et s'aggravent avec le temps.

NIVEAU DE RISQUE **Critique** EFFORT **Modéré**

Piste recommandée Planifiez une vérification d'intégrité hebdomadaire (CHECKDB) sur chaque base — c'est le seul moyen de détecter tôt une corruption silencieuse avant qu'elle ne se propage aux sauvegardes. Effort modéré, faible risque.

Annexe technique — résultats détaillés

Détail des écarts et avertissements par domaine, avec la piste de remédiation recommandée.

S Sécurité des accès

Qui peut entrer dans la base et ce qu'il peut y faire.

5 Écarts · 1 Avertissements · 97 Conformes

SEC001 Compte SA activé — CRITIQUE

Écart détecté — voir remédiation.

Constaté: KO

Piste recommandée: Désactivez le compte SA et créez des comptes nommés dédiés pour les administrateurs — le compte SA est une cible privilégiée des attaques par force brute. Intervention rapide, faible risque (vérifiez au préalable qu'aucune application ne s'y connecte).

SEC002 Politique de mot de passe — ÉLEVÉ

Écart détecté — voir remédiation.

Constaté: KO

Piste recommandée: Appliquez la politique de mot de passe Windows (CHECK_POLICY) à chaque login SQL — sans elle, des mots de passe faibles ou jamais expirés affaiblissent l'authentification. Intervention rapide, faible risque.

SEC004 Membres sysadmin — ÉLEVÉ

Écart détecté — voir remédiation.

Constaté: KO

Piste recommandée: Retirez les accès sysadmin non nécessaires, utilisez des rôles moins privilégiés

SEC005 Compte Guest actif — MOYEN

Écart détecté — voir remédiation.

Constaté: KO

Piste recommandée: Révoquez l'accès du compte Guest dans chaque base utilisateur — un Guest actif ouvre la base à tout login serveur, même non autorisé. Intervention rapide, faible risque (ne touchez pas master/tempdb).

SEC003 Utilisateurs orphelins — MOYEN

Écart détecté — voir remédiation.

Constaté: KO

Piste recommandée: Remappez chaque utilisateur orphelin vers son login serveur, ou supprimez-le s'il n'est plus utilisé — un orphelin peut masquer un accès résiduel après une migration. Effort modéré, faible risque.

SEC006 Permissions du rôle Public — INFO

Écart détecté — voir remédiation.

Constaté: KO

Piste recommandée: Auditez et révoquez les permissions accordées au rôle public

C Réglages du serveur

Paramètres qui conditionnent stabilité et performance.

4 Écarts · 29 Conformes

CFG001 Max Server Memory — CRITIQUE

Écart détecté — voir remédiation.

Constaté: KO

Piste recommandée: Plafonnez la mémoire maximale du serveur en réservant de la RAM à l'OS (règle de départ : RAM totale - 4 Go, ou - 10 % au-delà de 16 Go) — sans plafond, SQL Server peut affamer le système et provoquer du swap. Intervention rapide, faible risque.

CFG004 MAXDOP — ÉLEVÉ

Écart détecté — voir remédiation.

Constaté: KO

Piste recommandée: NUMA: min(8, cores/node). Sans NUMA: min(8, total cores)

CFG003 Cost Threshold for Parallelism — MOYEN

Écart détecté — voir remédiation.

Constaté: KO

Piste recommandée: Relevez le seuil de coût pour le parallélisme (point de départ recommandé : 50) — la valeur par défaut de 5 parallélise trop de petites requêtes et gaspille du CPU sur les charges OLTP. Intervention rapide, faible risque.

CFG002 Min Server Memory — FAIBLE

Écart détecté — voir remédiation.

Constaté: KO

Piste recommandée: Généralement 0 ou 25% de max server memory

F Organisation des fichiers

Comment la base est stockée sur les disques — marge de croissance.

2 Écarts · 8 Conformes

FILE002 TempDB sur disque système — CRITIQUE

Écart détecté — voir remédiation.

Constaté: KO

Piste recommandée: Déplacez TempDB sur un disque dédié rapide (SSD)

FILE001 Data et Log sur même disque — ÉLEVÉ

Écart détecté — voir remédiation.

Constaté: KO

Piste recommandée: Déplacez les fichiers log sur un disque dédié

B Sauvegardes

Votre filet de sécurité en cas d'incident ou de perte de données.

3 Écarts · 8 Conformes

BACK001 Sauvegarde Full récente — CRITIQUE

Écart détecté — voir remédiation.

Constaté: KO

Piste recommandée: Planifiez des sauvegardes Full hebdomadaires minimum

BACK003 Sauvegarde Log récente — CRITIQUE

Écart détecté — voir remédiation.

Constaté: KO

Piste recommandée: Planifiez des backups log toutes les 15-60 minutes selon RPO

BACK002 **Sauvegarde Diff configurée** MOYEN

Écart détecté — voir remédiation.

Constaté: KO

Piste recommandée: Planifiez des sauvegardes Diff quotidiennes

M Entretien régulier

Tâches d'hygiène qui gardent la base rapide et fiable.

3 Écarts · 30 Conformes

MAINT001 **DBCC CHECKDB récent** CRITIQUE

Écart détecté — voir remédiation.

Constaté: KO

Piste recommandée: Planifiez une vérification d'intégrité hebdomadaire (CHECKDB) sur chaque base — c'est le seul moyen de détecter tôt une corruption silencieuse avant qu'elle ne se propage aux sauvegardes. Effort modéré, faible risque.

MAINT002 **Fragmentation index** MOYEN

Écart détecté — voir remédiation.

Constaté: KO

Piste recommandée: Reorganize (10-30%) ou Rebuild (>30%) les index

MAINT003 **Statistiques obsolètes** MOYEN

Écart détecté — voir remédiation.

Constaté: KO

Piste recommandée: Mettez à jour les statistiques régulièrement (job de maintenance) et assurez-vous que la mise à jour automatique des statistiques est activée — des statistiques périmées dégradent les plans d'exécution. Effort modéré, faible risque.

P Rapidité

La réactivité ressentie par vos utilisateurs au quotidien.

2 Écarts · 27 Conformes

PERF001 **Page Life Expectancy** MOYEN

Écart détecté — voir remédiation.

Constaté: KO

Piste recommandée: Corroborer avec les wait stats (PAGEIOLATCH) avant de conclure à une pression mémoire ; vérifier Max Server Memory

PERF002 **Buffer Cache Hit Ratio** INFO

Écart détecté — voir remédiation.

Constaté: KO

Piste recommandée: Ne pas se fier au BCHR ; utiliser les wait stats et la tendance du PLE

R Continuité de service

Capacité à rester disponible et à repartir après un incident.

3 Écarts · 61 Conformes

REL001 **Corruption détectée** CRITIQUE

Écart détecté — voir remédiation.

Constaté: KO

Piste recommandée: Lancez une vérification d'intégrité complète de la base, identifiez l'étendue de la corruption, puis restaurez les pages ou la base à partir d'une sauvegarde saine — une corruption non traitée entraîne une perte de données. Intervention urgente, risque élevé (faites-vous accompagner avant toute réparation).

REL003 **Mirroring status** ÉLEVÉ

Écart détecté — voir remédiation.

Constaté: KO

Piste recommandée: Résolvez les problèmes de synchronisation

REL002 **Memory dumps** ÉLEVÉ

Écart détecté — voir remédiation.

Constaté: KO

Piste recommandée: Analysez les dumps et contactez le support Microsoft si récurrent

I Accès aux disques

La vitesse de lecture/écriture sur le stockage.

2 Écarts · 3 Conformes

IO002 **Fichiers les plus lents** ÉLEVÉ

Écart détecté — voir remédiation.

Constaté: KO

Piste recommandée: Déplacez les fichiers chauds vers un stockage plus rapide et répartissez la charge I/O.

IO001 **Latence par disque** ÉLEVÉ

Écart détecté — voir remédiation.

Constaté: KO

Piste recommandée: Au-delà de ~20 ms, investiguez le stockage (file d'attente, cache, contention, dimensionnement).

DS Options des bases

Réglages de chaque base affectant sécurité et performance.

3 Écarts · 10 Conformes

DBSET003 **Page Verify pas CHECKSUM** CRITIQUE

Écart détecté — voir remédiation.

Constaté: KO

Piste recommandée: Réglez l'option de vérification des pages sur CHECKSUM pour chaque base — c'est ce qui permet de détecter une corruption disque silencieuse. Intervention rapide, faible risque (la protection ne couvre que les pages réécrites ensuite).

DBSET001 **AutoClose activé** ÉLEVÉ

Écart détecté — voir remédiation.

Constaté: KO

Piste recommandée: Désactivez AutoClose sur chaque base concernée — il ferme la base à chaque déconnexion et impose une coûteuse réouverture à la connexion suivante. Intervention rapide, faible risque.

DBSET002 **AutoShrink activé** ÉLEVÉ

Écart détecté — voir remédiation.

Constaté: KO

Piste recommandée: Désactivez AutoShrink sur chaque base concernée — les réductions automatiques répétées provoquent une fragmentation massive des index et une charge I/O inutile. Intervention rapide, faible risque.

En Chiffrement des données

Vos données sont-elles illisibles si un disque est volé.

2 Écarts · 12 Conformes

ENC002 **Sauvegarde certificats TDE** CRITIQUE

Écart détecté — voir remédiation.

Constaté: KO

Piste recommandée: Sauvegardez chaque certificat TDE avec sa clé privée et conservez-les hors du serveur, dans un coffre sécurisé — sans cette sauvegarde, une base chiffrée devient irrécupérable en cas de sinistre. Intervention rapide, faible risque (protégez impérativement le mot de passe de la clé).

ENC001 **État TDE détaillé** INFO

Écart détecté — voir remédiation.

Constaté: KO

Piste recommandée: Informationnel: état actuel du chiffrement TDE