

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

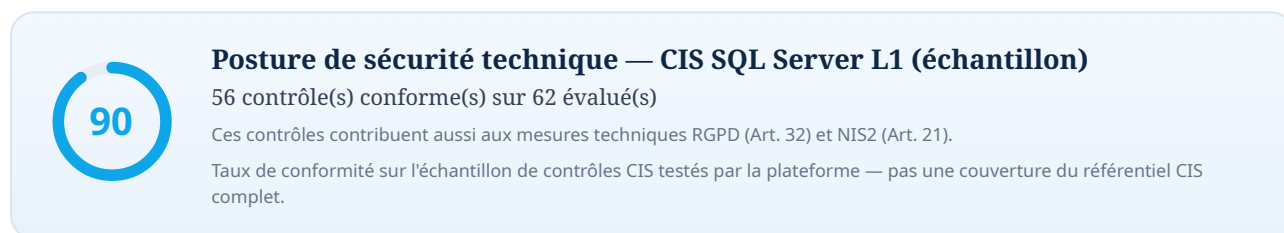
Synthèse de direction — Remédiation



À corriger : 30 écart(s) ouvert(s), dont 19 prioritaire(s) (critiques + élevés)



Premier audit — pas encore d'historique pour mesurer la progression.



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).