

PREPARED FOR

SRV-APP-01

PRODUCTION

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

· srv-app-01.atlantique.local



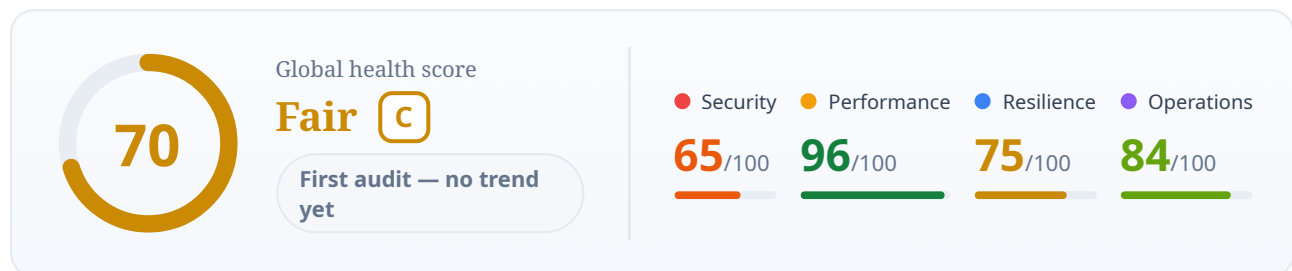
Global health score

Fair C

out of 100

First audit — no trend yet

Executive summary



Top business risks

Translated into business language, ranked by stakes. Risk is expressed as a level (High / Medium / Low) and an effort, with no financial figure.

- 1 Your backups won't protect you from a failure or an attack** CRITICAL

In case of disk failure, corruption or ransomware, you risk losing data with no way to restore it.

RISK LEVEL **Critical** EFFORT **High**

Recommended action Planifiez des sauvegardes Full hebdomadaires minimum
- 2 Your database is exposed to unauthorized access** CRITICAL

A security gap can allow theft or leakage of your customer and business data.

RISK LEVEL **Critical** EFFORT **Low**

Recommended action 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 Your database could go down without guaranteed recovery** CRITICAL

If your service continuity isn't guaranteed, an outage can halt your operations for hours or days.

RISK LEVEL **Critical** EFFORT **High**

Recommended action 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

The server configuration deviates from best practices

! CRITICAL

Unsuitable settings can undermine the stability, security or performance of your database.

RISK LEVEL **Critical** EFFORT **Low**

Recommended action 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

Your sensitive data is not encrypted

! CRITICAL

If files or media are stolen, the data stays readable and GDPR compliance is not ensured.

RISK LEVEL **Critical** EFFORT **High**

Recommended action Back up each TDE certificate together with its private key and keep them off-server in a secure vault — without this backup, an encrypted database becomes unrecoverable after a disaster. Quick to do, low risk (be sure to protect the key password).

6

Regular database upkeep is not in place

! CRITICAL

Without maintenance, data issues go unnoticed and worsen over time.

RISK LEVEL **Critical** EFFORT **Medium**

Recommended action 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.

Technical annex — detailed results

Detailed gaps and warnings by domain, with the recommended remediation guidance.

S Access security Who can reach the database and what they may do there.		5 Gaps · 1 Warnings · 97 Compliant
! SEC001 Compte SA activé	Écart détecté — voir remédiation. Observed: KO Recommended action: 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).	CRITICAL
⚠ SEC002 Politique de mot de passe	Écart détecté — voir remédiation. Observed: KO Recommended action: 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.	HIGH
⚠ SEC004 Membres sysadmin	Écart détecté — voir remédiation. Observed: KO Recommended action: Retirez les accès sysadmin non nécessaires, utilisez des rôles moins privilégiés	HIGH
! SEC005 Compte Guest actif	Écart détecté — voir remédiation. Observed: KO Recommended action: 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).	MEDIUM
! SEC003 Utilisateurs orphelins	Écart détecté — voir remédiation. Observed: KO Recommended action: 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.	MEDIUM
i SEC006 Permissions du rôle Public	Écart détecté — voir remédiation. Observed: KO Recommended action: Auditez et révoquez les permissions accordées au rôle public	INFO



Server settings

Settings that drive stability and performance.

4 Gaps · 29 Compliant



CFG001

Max Server Memory

CRITICAL

Écart détecté — voir remédiation.

Observed: KO

Recommended action: 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

HIGH

Écart détecté — voir remédiation.

Observed: KO

Recommended action: NUMA: min(8, cores/node). Sans NUMA: min(8, total cores)



CFG003

Cost Threshold for Parallelism

MEDIUM

Écart détecté — voir remédiation.

Observed: KO

Recommended action: 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

LOW

Écart détecté — voir remédiation.

Observed: KO

Recommended action: Généralement 0 ou 25% de max server memory



File layout

How the database is stored on disk — room to grow.

2 Gaps · 8 Compliant



FILE002

TempDB sur disque système

CRITICAL

Écart détecté — voir remédiation.

Observed: KO

Recommended action: Déplacez TempDB sur un disque dédié rapide (SSD)



FILE001

Data et Log sur même disque

HIGH

Écart détecté — voir remédiation.

Observed: KO

Recommended action: Déplacez les fichiers log sur un disque dédié

B

Backups

Your safety net if data is lost or corrupted.

3 Gaps · 8 Compliant



BACK001

Sauvegarde Full récente

CRITICAL

Écart détecté — voir remédiation.

Observed: KO

Recommended action: Planifiez des sauvegardes Full hebdomadaires minimum

BACK003

Sauvegarde Log récente

CRITICAL

Écart détecté — voir remédiation.

Observed: KO

Recommended action: Planifiez des backups log toutes les 15-60 minutes selon RPO

BACK002

Sauvegarde Diff configurée

MEDIUM

Écart détecté — voir remédiation.

Observed: KO

Recommended action: Planifiez des sauvegardes Diff quotidiennes

M

Routine upkeep

Housekeeping that keeps the database fast and reliable.

3 Gaps · 30 Compliant



MAINT001

DBCC CHECKDB récent

CRITICAL

Écart détecté — voir remédiation.

Observed: KO

Recommended action: 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

MEDIUM

Écart détecté — voir remédiation.

Observed: KO

Recommended action: Reorganize (10-30%) ou Rebuild (>30%) les index

MAINT003

Statistiques obsolètes

MEDIUM

Écart détecté — voir remédiation.

Observed: KO

Recommended action: 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

Speed

The responsiveness your users feel day to day.

2 Gaps · 27 Compliant



PERF001

Page Life Expectancy

MEDIUM

Écart détecté — voir remédiation.

Observed: KO

Recommended action: 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.

Observed: KO

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

R

Service continuity

Staying available and recovering after an incident.

3 Gaps · 61 Compliant



REL001

Corruption détectée

CRITICAL

Écart détecté — voir remédiation.

Observed: KO

Recommended action: 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

HIGH

Écart détecté — voir remédiation.

Observed: KO

Recommended action: Résolvez les problèmes de synchronisation



REL002

Memory dumps

HIGH

Écart détecté — voir remédiation.

Observed: KO

Recommended action: Analysez les dumps et contactez le support Microsoft si récurrent



Disk access

Read/write speed on the underlying storage.

2 Gaps · 3 Compliant



IO002

Fichiers les plus lents

HIGH

Écart détecté — voir remédiation.

Observed: KO

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



IO001

Latence par disque

HIGH

Écart détecté — voir remédiation.

Observed: KO

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



Database options

Per-database settings affecting security and speed.

3 Gaps · 10 Compliant



DBSET003

Page Verify not CHECKSUM

CRITICAL

Écart détecté — voir remédiation.

Observed: KO

Recommended action: Set the page verification option to CHECKSUM on each database — this is what allows silent disk corruption to be detected. Quick to do, low risk (protection only covers pages written after the change).



DBSET001

AutoClose enabled

HIGH

Écart détecté — voir remédiation.

Observed: KO

Recommended action: Turn off AutoClose on each affected database — it closes the database on every disconnect and forces a costly reopen on the next connection. Quick to do, low risk.



DBSET002

AutoShrink enabled

HIGH

Écart détecté — voir remédiation.

Observed: KO

Recommended action: Turn off AutoShrink on each affected database — repeated automatic shrinks cause massive index fragmentation and needless I/O load. Quick to do, low risk.



ENC002

TDE certificates backup**CRITICAL**

Écart détecté — voir remédiation.

Observed: KO

Recommended action: Back up each TDE certificate together with its private key and keep them off-server in a secure vault — without this backup, an encrypted database becomes unrecoverable after a disaster. Quick to do, low risk (be sure to protect the key password).



ENC001

TDE status details**INFO**

Écart détecté — voir remédiation.

Observed: KO

Recommended action: Informational: current TDE encryption state