

Cas pratique : mini-PC serveur client (simulation chez moi)

Oct 17, 2026 · @Jacques

Objectif et matériel

Vous installez chez vous, sur un mini-PC Windows, exactement ce que vous installerez plus tard chez un client : votre application KEEN (Next.js + Prisma + MariaDB), le HTTPS, les sauvegardes chiffrées et l'accès de maintenance. Votre PC habituel joue le rôle de « votre poste de consultant », et vos autres appareils (téléphone, portable) jouent les postes des managers du client.

À la fin, vous saurez faire l'installation en une demi-journée, et vous aurez éprouvé les pannes typiques : coupure de courant, redémarrage Windows, restauration d'une sauvegarde.

Matériel à réunir

Élément	Ce qu'il faut	Remarque
Mini-PC	4 cœurs, 8 Go de RAM minimum, SSD 256 Go	Intel N100 ou mieux
Windows	Windows 11 Pro	Pro est nécessaire pour BitLocker et le Bureau à distance
Clavier, souris, écran	Pour l'installation seulement	Ensuite le mini-PC tourne sans écran
Câble Ethernet	Du mini-PC vers votre box	Pas de Wi-Fi pour un serveur
Disque USB externe	64 Go suffisent pour l'exercice	Sert de disque de sauvegarde
Onduleur	Facultatif pour l'exercice, avec câble USB	Indispensable chez un vrai client
Clé USB	8 Go	Pour transférer l'application depuis votre PC

Fiche d'identité du client simulé (à recopier au stylo, elle servira tout au long du guide)

Information	Valeur pour l'exercice	Votre valeur
Nom du client fictif	Société Test CI	
Nom du mini-PC	SRV-KEEN	
Adresse IP fixe	192.168.1.50	
Plage du réseau local	192.168.1.0/24	
Compte administrateur client	admin-client	
Compte de maintenance (vous)	maintenance-keen	
Adresse de l'application	https://keen.local	

Vérifiez d'abord la plage de votre box : dans une invite de commandes de votre PC, tapez `ipconfig` et lisez la ligne « Passerelle par défaut ». Si elle indique 192.168.0.1, remplacez partout 192.168.1 par 192.168.0.

Raccordement réseau : câble ou mini-routeur

Le mini-PC est toujours branché en Ethernet : soit directement à la box (option 1), soit à un mini-routeur qui capte le Wi-Fi de la box (option 2). Dans les deux cas, il doit se retrouver **sur le même réseau que les postes du client**, en 192.168.1.x, sinon les utilisateurs ne le verront pas.

	Option 1 : câble direct	Option 2 : mini-routeur Wi-Fi → Ethernet
Quand	Le mini-PC peut être placé à côté de la box, ou un câble peut être tiré	Aucun câble possible jusqu'à la box
Matériel	Câble Ethernet cat. 6 de la bonne longueur	Mini-routeur de voyage + câble Ethernet court (0,5 à 1 m)
Fiabilité	Excellente	Bonne si le signal Wi-Fi est bon à l'endroit choisi
Adresse IP fixe	Réservation dans la box (étape 1, point 8)	Adresse fixée dans Windows (voir ci-dessous)
Prix indicatif	2 000 à 5 000 FCFA	20 000 à 35 000 FCFA (à vérifier sur le marché local)

Option 1 : câble direct. Branchez le mini-PC sur un port LAN de la box (ou d'un switch relié à la box) et suivez l'étape 1 telle quelle.

Option 2 : le mini-routeur, ce qu'il faut acheter

- Un **mini-routeur de voyage qui a un mode « Client »** (aussi appelé « pont » ou « bridge »). Exemples courants : TP-Link TL-WR902AC (double bande 2,4 et 5 GHz, recommandé) ou TP-Link TL-WR802N (2,4 GHz seulement, moins cher). Un répéteur Wi-Fi qui possède un port Ethernet (TP-Link RE200, RE305...) fait le même travail.
- Un câble Ethernet court.
- Son alimentation USB, branchée sur l'onduleur avec le mini-PC.

Le piège à éviter : le mode « **WISP** » ou « Routeur » crée un second réseau (par exemple 192.168.0.x) derrière le mini-routeur. Le mini-PC aurait Internet, mais les postes du client ne pourraient plus l'atteindre. Il faut le mode **Client** (ou « Extender », « Bridge »), qui prolonge le réseau de la box sans en créer un autre.

Configuration (exemple TL-WR902AC, comptez 20 minutes)

1. Branchez le mini-routeur sur le secteur et reliez-le par câble à votre PC portable.
2. Ouvrez <http://tplinkwifi.net> (ou l'adresse indiquée sous l'appareil) et créez le mot de passe d'administration. Notez-le sur la fiche.
3. Choisissez le mode **Client** (Mode de fonctionnement > Client ; certains modèles ont aussi un sélecteur physique, voir la notice).
4. Lancez la recherche des réseaux, choisissez le Wi-Fi du client, tapez sa clé Wi-Fi, laissez l'adresse IP du mini-routeur en automatique. Le mini-routeur redémarre.
5. Placez-le **à l'endroit où le Wi-Fi est bon**, au plus près de la box, sans mur porteur ni armoire métallique entre les deux. Le câble court le relie au mini-PC.
6. **Adresse IP fixe dans Windows.** En mode Client, la box voit souvent l'adresse du mini-routeur à la place de celle du mini-PC : la réservation dans la box ne marche pas toujours. Fixez donc l'adresse sur le mini-PC : Paramètres > Réseau et Internet > Ethernet > Attribution d'adresse IP > Modifier > Manuelle > IPv4. Adresse 192.168.1.50, masque 255.255.255.0, passerelle et DNS 192.168.1.1. Choisissez une adresse que la box ne distribue pas elle-même (regardez la plage DHCP dans les réglages de la box, souvent .100 à .200).

Contrôle : sur le mini-PC, `ipconfig` affiche l'adresse 192.168.1.50 et la passerelle 192.168.1.1, la même que sur les autres postes. Depuis un poste du client, `ping 192.168.1.50 -t` pendant une heure ne montre aucun « Délai d'attente dépassé ». Coupez puis rallumez l'onduleur : le mini-routeur et le mini-PC doivent revenir seuls sur le réseau.

Dans le dossier de remise, notez que si le client change la clé Wi-Fi de sa box, le serveur se déconnecte : il faudra la ressaisir dans le mini-routeur (étape 4 ci-dessus).

Étape 1 : préparer Windows sur le mini-PC

Cette étape rend le mini-PC autonome : il redémarre seul après une coupure, ne se met jamais en veille et ne redémarre pas pour une mise à jour en pleine journée. Comptez une heure.

1. **BIOS.** Au démarrage, appuyez sur Suppr ou F2 (selon la marque). Cherchez « Restore on AC Power Loss » (ou « After Power Failure ») et choisissez **Power On**. Enregistrez avec F10.
2. **Installation de Windows 11 Pro.** Suivez l'assistant. Créez le compte local **admin-client** avec un mot de passe long, écrit sur la fiche.
3. **Nom du PC.** Paramètres > Système > Informations système > Renommer ce PC : **SRV-KEEN**. Redémarrez.
4. **Mises à jour.** Paramètres > Windows Update : installez tout et redémarrez autant de fois que nécessaire.
5. **Compte de maintenance.** Paramètres > Comptes > Autres utilisateurs > Ajouter un compte > « Je ne dispose pas des informations de connexion » > « Ajouter un utilisateur sans compte Microsoft » : **maintenance-keen**. Donnez-lui le type Administrateur.
6. **Pas de mise en veille.** Ouvrez PowerShell en administrateur (clic droit sur Démarrer > Terminal (administrateur)) et tapez :

```
powercfg /change standby-timeout-ac 0
powercfg /change hibernate-timeout-ac 0
powercfg /change disk-timeout-ac 0
```

7. **Pas de redémarrage surprise.** Tapez `gpedit.msc` dans Démarrer. Allez dans Configuration ordinateur > Modèles d'administration > Composants Windows > Windows Update > Gérer l'expérience utilisateur final. Activez « Pas de redémarrage automatique avec des utilisateurs connectés pour les installations planifiées ». Puis dans Paramètres > Windows Update > Options avancées > Heures d'activité, réglez de 7 h à 22 h.
8. **Adresse IP fixe.** Branchez le câble Ethernet (avec le mini-routeur, suivez plutôt le point 6 de la section Raccordement réseau). Dans l'interface de votre box (souvent `http://192.168.1.1`, identifiants sous la box), cherchez « Bail DHCP statique » ou « Réservation d'adresse » et attribuez **192.168.1.50** à SRV-KEEN. Redémarrez le mini-PC, puis vérifiez avec `ipconfig`.

9. **BitLocker**. Panneau de configuration > Chiffrement de lecteur BitLocker > Activer BitLocker sur C:. Choisissez « Imprimer la clé de récupération » et rangez la feuille avec ce guide.

Contrôle : débranchez la prise du mini-PC, attendez 10 secondes, rebranchez. Il doit redémarrer seul jusqu'à l'écran de connexion, sans demander la clé BitLocker.

Étape 2 : installer les logiciels

Cinq logiciels gratuits suffisent. Téléchargez-les depuis leur site officiel uniquement, connecté avec le compte admin-client. Comptez 45 minutes.

Logiciel	Site	Rôle
MariaDB 11.4 LTS (installeur MSI)	mariadb.org	La base de données
Node.js LTS (installeur MSI)	nodejs.org	Fait tourner l'application
NSSM	nssm.cc	Transforme un programme en service Windows
Caddy	caddyserver.com	Le HTTPS
7-Zip	7-zip.org	Chiffre les sauvegardes

1. Créez les dossiers de travail dans PowerShell (administrateur) :

```
New-Item -ItemType Directory C:\Keen\app, C:\Keen\caddy, C:\Keen\logs,
C:\Keen\tmp, C:\Keen\outils
```

2. **MariaDB**. Lancez le MSI. Cochez « Install as service » (nom du service : MariaDB), port 3306, et choisissez un mot de passe root long, noté sur la fiche. **Décochez** « Enable access from remote machines for root user ».
3. Pour que la base ne soit jamais visible sur le réseau, ouvrez `C:\Program Files\MariaDB 11.4\data\my.ini` avec le Bloc-notes (en administrateur) et ajoutez sous `[mysqld]` la ligne `bind-address=127.0.0.1`. Redémarrez le service : `Restart-Service MariaDB`.
4. **Node.js**. Lancez le MSI avec les options par défaut. Vérifiez dans un nouveau PowerShell : `node -v` doit afficher un numéro de version.
5. **NSSM et Caddy**. Dézippez NSSM et copiez `nssm.exe` (dossier win64) dans `C:\Keen\outils`. Copiez `caddy.exe` dans `C:\Keen\caddy`.
6. **7-Zip**. Lancez l'installeur avec les options par défaut.

7. **Créer la base de l'application.** Ouvrez « MySQL Client (MariaDB 11.4) » depuis le menu Démarrer, tapez le mot de passe root, puis :

```
CREATE DATABASE keen CHARACTER SET utf8mb4 COLLATE utf8mb4_unicode_ci;  
CREATE USER 'keen'@'localhost' IDENTIFIED BY 'MotDePasseAppliTresLong2026';  
GRANT ALL PRIVILEGES ON keen.* TO 'keen'@'localhost';  
FLUSH PRIVILEGES;  
EXIT;
```

Remplacez le mot de passe d'exemple par le vôtre et notez-le.

Contrôle : dans `services.msc`, le service **MariaDB** est « En cours d'exécution », type de démarrage « Automatique ».

Étape 3 : déployer l'application comme service Windows

L'application est construite sur votre PC de consultant, puis copiée sur le mini-PC par clé USB, comme vous le ferez chez un client. Comptez une heure.

Sur votre PC (dossier KEEN_SERVICES)

1. Dans `next.config.ts`, ajoutez `output: "standalone"`, dans l'objet de configuration. Claude Code peut le faire pour vous.
2. Construisez : `npm run build`.
3. Préparez un dossier `livraison-1.0.0` sur la clé USB contenant :
 - tout le contenu de `.next\standalone` ;
 - le dossier `.next\static`, copié dans `livraison-1.0.0\.next\static` ;
 - le dossier `public` ;
 - le dossier `prisma` et le fichier `prisma.config.ts`.

Sur le mini-PC

4. Copiez le contenu de `livraison-1.0.0` dans `C:\Keen\app`.
5. Créez les tables. Dans PowerShell, depuis `C:\Keen\app` :

```
cd C:\Keen\app  
$env:DATABASE_URL = "mysql://keen:MotDePasseAppli@localhost:3306/keen"  
npx prisma migrate deploy
```

La dernière ligne doit finir par « All migrations have been successfully applied ». En cas d'erreur, photographiez le message et envoyez-le moi.

6. Créez le service **KeenApp**. Les réglages secrets sont donnés au service lui-même, pas dans un fichier :

```
$nssm = "C:\Keen\outils\nssm.exe"
& $nssm install KeenApp "C:\Program Files\nodejs\node.exe"
"C:\Keen\app\server.js"
& $nssm set KeenApp AppDirectory C:\Keen\app
& $nssm set KeenApp AppEnvironmentExtra "PORT=3000" "HOSTNAME=127.0.0.1"
"DATABASE_URL=mysql://keen:MotDePasseAppli@localhost:3306/keen"
"BETTER_AUTH_SECRET=UneChaineAleatoireDe32Caracteres"
"BETTER_AUTH_URL=https://keen.local"
& $nssm set KeenApp AppStdout C:\Keen\logs\app.log
& $nssm set KeenApp AppStderr C:\Keen\logs\app-erreurs.log
& $nssm set KeenApp DependOnService MariaDB
& $nssm set KeenApp Start SERVICE_AUTO_START
& $nssm start KeenApp
```

Pour obtenir une chaîne aléatoire : `[Convert]::ToBase64String((1..32 | ForEach-Object { Get-Random -Max 256 })))`.

Contrôle : sur le mini-PC, ouvrez le navigateur à l'adresse `http://127.0.0.1:3000`. Le site KEEN doit s'afficher. Sinon, lisez `C:\Keen\logs\app-erreurs.log`.

À savoir avant un vrai client : aujourd'hui, dans KEEN_SERVICES, tout utilisateur connecté a les droits d'administrateur. Pour l'exercice ce n'est pas grave, mais il faudra ajouter des rôles avant la première installation réelle.

Étape 4 : HTTPS et accès depuis les autres appareils

Caddy reçoit les connexions en HTTPS sur le port 443 et les passe à l'application. C'est la seule porte ouverte du mini-PC. Comptez 45 minutes.

1. Créez le fichier `C:\Keen\caddy\Caddyfile` (sans extension) avec le Bloc-notes :

```
keen.local, admin.keen.local, 192.168.1.50 {
    tls internal
    reverse_proxy 127.0.0.1:3000
}
```

2. Créez le service **Caddy** :

```
$nssm = "C:\Keen\outils\nssm.exe"
& $nssm install Caddy "C:\Keen\caddy\caddy.exe" "run --config
C:\Keen\caddy\Caddyfile"
& $nssm set Caddy AppDirectory C:\Keen\caddy
& $nssm set Caddy AppStderr C:\Keen\logs\caddy.log
& $nssm set Caddy DependOnService KeenApp
& $nssm start Caddy
```

3. Ouvrez le port 443 au réseau local seulement :

```
New-NetFirewallRule -DisplayName "Keen HTTPS" -Direction Inbound -Protocol TCP -LocalPort 443 -RemoteAddress 192.168.1.0/24 -Action Allow
```

4. Sur votre PC de consultant, faites connaître le nom keen.local. Ouvrez le Bloc-notes en administrateur, puis le fichier `C:\Windows\System32\drivers\etc\hosts`, et ajoutez :

```
192.168.1.50 keen.local
192.168.1.50 admin.keen.local
```

5. Supprimer l'alerte de sécurité du navigateur. Sur le mini-PC, copiez sur la clé USB le certificat racine de Caddy :

`C:\Windows\System32\config\systemprofile\AppData\Roaming\Caddy\pki\authorities\local\root.crt`. Sur votre PC, double-cliquez dessus > Installer le certificat > Ordinateur local > « Placer tous les certificats dans le magasin suivant » > Autorités de certification racines de confiance.

6. Sur votre téléphone (connecté au Wi-Fi de la maison), ouvrez `https://192.168.1.50` et acceptez l'avertissement. Chez un client, on installera le certificat sur chaque poste, ou on déclarera `keen.local` dans sa box.

Contrôle : depuis votre PC, `https://keen.local` affiche le site avec un cadenas, et `https://admin.keen.local` affiche la console. Depuis le téléphone, `https://192.168.1.50` fonctionne. En revanche, `http://192.168.1.50:3000` ne doit **pas** répondre : l'application n'est joignable qu'à travers Caddy.

Étape 5 : sauvegardes et test de restauration

Chaque nuit à 2 h, une tâche copie la base dans une archive chiffrée sur le disque USB. Le test de restauration est la partie la plus importante de tout l'exercice. Comptez une heure.

1. Branchez le disque USB et notez sa lettre (ici **E:**). Créez le dossier `E:\Sauvegardes`.
2. Créez le fichier `C:\Keen\outils\sauvegarde.cnf` avec le mot de passe root :

```
[client]
user=root
password=VotreMotDePasseRoot
```

3. Créez le fichier `C:\Keen\outils\cle-sauvegarde.txt` contenant une seule ligne : le mot de passe des archives (long, noté sur la fiche). Chez un client, ce mot de passe lui appartient.
4. Protégez ces deux fichiers : clic droit > Propriétés > Sécurité > Avancé > Désactiver l'héritage, puis ne laissez que SYSTEM et Administrateurs.

5. Créez le script `C:\Keen\sauvegarde.ps1` :

```
$date = Get-Date -Format "yyyy-MM-dd_HH:mm"
$dump = "C:\Keen\tmp\keen-$date.sql"
$cle = Get-Content C:\Keen\outils\cle-sauvegarde.txt
& "C:\Program Files\MariaDB 11.4\bin\mariadb-dump.exe" --defaults-extra-
file=C:\Keen\outils\sauvegarde.cnf --single-transaction --result-file=$dump
keen
& "C:\Program Files\7-Zip\7z.exe" a -t7z -mhe=on "-p$cle"
"E:\Sauvegardes\keen-$date.7z" $dump
Remove-Item $dump
Get-ChildItem E:\Sauvegardes\keen-*.7z | Where-Object LastWriteTime -lt (Get-
Date).AddDays(-30) | Remove-Item
```

6. Planifiez-le : ouvrez le Planificateur de tâches > Créer une tâche. Nom : **Sauvegarde KEEN**. Cochez « Exécuter même si l'utilisateur n'est pas connecté » et « Exécuter avec les autorisations maximales ». Déclencheur : tous les jours à 2:00. Action : programme `powershell.exe`, arguments `-ExecutionPolicy Bypass -File C:\Keen\sauvegarde.ps1`.

7. Lancez-la une première fois à la main (clic droit > Exécuter) et vérifiez qu'une archive `.7z` apparaît dans `E:\Sauvegardes`.

Test de restauration (à faire maintenant, puis une fois par mois chez un client)

8. Dans l'application, créez une donnée reconnaissable (par exemple un prospect nommé « TEST RESTAURATION »), puis lancez une sauvegarde.

9. Supprimez ce prospect dans l'application.

10. Restaurez la sauvegarde dans une base de test, pour ne pas toucher à la vraie :

```
& "C:\Program Files\7-Zip\7z.exe" x E:\Sauvegardes\keen-AAAA-MM-JJ_HHMM.7z -
oC:\Keen\tmp
cmd /c '"C:\Program Files\MariaDB 11.4\bin\mariadb.exe" --defaults-extra-
file=C:\Keen\outils\sauvegarde.cnf -e "CREATE DATABASE keen_test"'
cmd /c '"C:\Program Files\MariaDB 11.4\bin\mariadb.exe" --defaults-extra-
file=C:\Keen\outils\sauvegarde.cnf keen_test < C:\Keen\tmp\keen-AAAA-MM-
JJ_HHMM.sql'
```

7-Zip demande le mot de passe des archives. Remplacez AAAA-MM-JJ_HHMM par le nom réel du fichier.

Contrôle : dans le client MariaDB, `USE keen_test`; puis cherchez le prospect dans la table des prospects. Il doit y être. Supprimez ensuite la base de test (`DROP DATABASE keen_test`;) et le fichier `.sql` du dossier `C:\Keen\tmp`.

Étape 6 : maintenance à distance avec Tailscale

Tailscale relie vos appareils par un réseau privé chiffré, sans ouvrir aucun port sur la box. Le « client » ouvre et ferme lui-même la porte. Comptez 30 minutes.

1. Créez un compte gratuit sur tailscale.com. Chez un vrai client, le compte sera à son nom.
2. Installez Tailscale sur le mini-PC (session admin-client) et connectez-le au compte. Notez son adresse Tailscale, qui commence par 100. (exemple : 100.101.102.103).
3. Installez Tailscale sur votre PC de consultant et sur votre téléphone, avec le même compte.
4. Sur le mini-PC, activez le Bureau à distance : Paramètres > Système > Bureau à distance > Activé.
5. Limitez le Bureau à distance au réseau Tailscale :

```
Get-NetFirewallRule -DisplayGroup "Bureau à distance" | Set-NetFirewallRule -RemoteAddress 100.64.0.0/10
```

6. **Simuler une intervention depuis l'extérieur.** Coupez le Wi-Fi de votre téléphone pour passer en données mobiles. Ouvrez Tailscale, puis l'application « Windows App » (Bureau à distance de Microsoft) et connectez-vous à l'adresse 100.x du mini-PC avec le compte maintenance-keen.
7. **Le client ferme la porte.** Sur le mini-PC, clic droit sur l'icône Tailscale > Disconnect. Votre connexion doit tomber et ne plus être possible. Reconnectez ensuite.

Contrôle : connexion possible en 4G quand Tailscale est actif sur le mini-PC, impossible quand il est déconnecté. Depuis le Wi-Fi de la maison sans Tailscale, le Bureau à distance sur 192.168.1.50 doit être refusé.

Étape 7 : simuler la vie chez un client

Ces tests reproduisent les incidents que vous rencontrerez vraiment. Faites-les dans l'ordre et cochez la dernière colonne au stylo.

#	Incident	Comment le provoquer	Résultat attendu	OK
1	Coupure de courant	Débrancher la prise pendant que l'appli est ouverte sur le téléphone	Redémarrage seul, site de nouveau en ligne en moins de 3 minutes, sans ouvrir de session	

#	Incident	Comment le provoquer	Résultat attendu	OK
2	Redémarrage Windows	Démarrer > Redémarrer	Les services MariaDB, KeenApp et Caddy repartent seuls	
3	L'application plante	Gestionnaire des tâches > terminer le processus node.exe	NSSM relance l'appli en quelques secondes	
4	Internet coupé	Débrancher le câble Internet (fibre ou ADSL) de la box	Le site marche toujours depuis le PC et le téléphone en Wi-Fi	
5	Disque USB absent	Débrancher le disque, lancer la tâche Sauvegarde KEEN	La tâche échoue ; vous savez le voir dans l'historique du Planificateur	
6	Mise à jour de l'appli	Procédure ci-dessous, version 1.0.1	Nouvelle version en ligne, données intactes	
7	Mise à jour ratée	Remettre l'ancien dossier (fin de la procédure)	Retour à la version 1.0.0 en moins de 10 minutes	

Procédure de mise à jour (test 6)

1. Sur votre PC, changez un petit texte visible du site, reconstruisez (`npm run build`) et préparez `livraison-1.0.1` comme à l'étape 3.
2. Sur le mini-PC, lancez d'abord une sauvegarde (Planificateur > Sauvegarde KEEN > Exécuter).
3. Arrêtez l'appli : `C:\Keen\outils\nssm.exe stop KeenApp`.
4. Renommez `C:\Keen\app` en `C:\Keen\app-1.0.0`, puis copiez `livraison-1.0.1` dans un nouveau dossier `C:\Keen\app`.
5. Appliquez les éventuelles nouvelles migrations : `npx prisma migrate deploy` (avec `$env:DATABASE_URL` comme à l'étape 3).
6. Redémarrez : `C:\Keen\outils\nssm.exe start KeenApp`, et vérifiez le nouveau texte.

Retour arrière (test 7) : arrêtez KeenApp, renommez `C:\Keen\app` en `C:\Keen\app-1.0.1-rate`, renommez `C:\Keen\app-1.0.0` en `C:\Keen\app`, redémarrez KeenApp. Si la mise à jour avait modifié la base, restaurez aussi la sauvegarde faite au point 2.

Étape 8 : héberger plusieurs applications sur le même mini-PC

Un seul mini-PC peut faire tourner plusieurs applications, par exemple KEEN, le dashboard et le SIRH. La règle : **un seul MariaDB et un seul Caddy pour tout le monde, mais pour chaque application sa propre base, son propre dossier, son propre port et son propre service**. Une panne ou une mise à jour d'une application ne touche pas les autres. Comptez 30 minutes par application.

Plan d'adressage (à compléter au stylo pour chaque nouvelle application)

Application	Dossier	Base / utilisateur	Port	Service	Adresse
KEEN (site + console)	C:\Keen\app	keen / keen	3000	KeenApp	keen.local, admin.keen.local
Dashboard	C:\Keen\apps\dashboard	dashboard / dashboard	3001	KeenDashboard	dashboard.keen.local
SIRH	C:\Keen\apps\sirh	sirh / sirh	3002	KeenSirh	sirh.keen.local

Pour chaque nouvelle application (exemple : le dashboard)

1. **Sa base.** Dans le client MariaDB (en root) :

```
CREATE DATABASE dashboard CHARACTER SET utf8mb4 COLLATE utf8mb4_unicode_ci;
CREATE USER 'dashboard'@'localhost' IDENTIFIED BY 'AutreMotDePasseLong2026';
GRANT ALL PRIVILEGES ON dashboard.* TO 'dashboard'@'localhost';
FLUSH PRIVILEGES;
```

Un utilisateur différent par application : si l'une est compromise, elle ne peut pas lire les données des autres.

2. **Son dossier.** Construisez l'application sur votre PC comme à l'étape 3 et copiez la livraison dans `C:\Keen\apps\dashboard`. Lancez `npx prisma migrate deploy` depuis ce dossier, avec son propre `DATABASE_URL`.

3. **Son service**, sur un port libre :

```

$nssm = "C:\Keen\outils\nssm.exe"
& $nssm install KeenDashboard "C:\Program Files\nodejs\node.exe"
"C:\Keen\apps\dashboard\server.js"
& $nssm set KeenDashboard AppDirectory C:\Keen\apps\dashboard
& $nssm set KeenDashboard AppEnvironmentExtra "PORT=3001"
"HOSTNAME=127.0.0.1"
"DATABASE_URL=mysql://dashboard:AutreMotDePasse@localhost:3306/dashboard"
"BETTER_AUTH_SECRET=UneAutreChaineAleatoire"
"BETTER_AUTH_URL=https://dashboard.keen.local"
& $nssm set KeenDashboard AppStdout C:\Keen\logs\dashboard.log
& $nssm set KeenDashboard AppStderr C:\Keen\logs\dashboard-erreurs.log
& $nssm set KeenDashboard DependOnService MariaDB
& $nssm set KeenDashboard Start SERVICE_AUTO_START
& $nssm start KeenDashboard

```

Chaque application a son propre `BETTER_AUTH_SECRET`.

4. **Son adresse.** Ajoutez un bloc dans `C:\Keen\caddy\Caddyfile` :

```

keen.local, admin.keen.local, 192.168.1.50 {
    tls internal
    reverse_proxy 127.0.0.1:3000
}

dashboard.keen.local {
    tls internal
    reverse_proxy 127.0.0.1:3001
}

sirh.keen.local {
    tls internal
    reverse_proxy 127.0.0.1:3002
}

```

Puis redémarrez Caddy : `C:\Keen\outils\nssm.exe restart Caddy`. Le pare-feu ne change pas : tout passe toujours par le seul port 443.

5. **Sur les postes**, ajoutez la ligne `192.168.1.50 dashboard.keen.local` dans le fichier `hosts` (étape 4).

6. **Sauvegarde** : ajoutez l'application à la liste du script de l'étape 9.

Contrôle : `https://keen.local` et `https://dashboard.keen.local` s'ouvrent toutes les deux. Arrêtez KeenDashboard dans `services.msc` : le dashboard ne répond plus, mais KEEN continue de fonctionner.

Limite à connaître : comptez environ 300 à 500 Mo de mémoire par application Next.js. Avec 8 Go de RAM, trois ou quatre applications tiennent à l'aise ; au-delà, passez à 16 Go.

Étape 9 : applications qui importent des fichiers

Quand une application reçoit des fichiers (Excel importés par les managers, pièces jointes du SIRH, photos), ses données sont en deux morceaux : **la base MariaDB et le dossier des fichiers**. Les deux doivent être rangés hors du dossier de l'application et sauvegardés ensemble, sinon une sauvegarde restaurée pointe vers des fichiers absents. Comptez 45 minutes.

Organisation des dossiers

C:\Keen\	
app\	programme KEEN (remplacé à chaque mise à jour)
apps\dashboard\	programme du dashboard (remplacé à chaque mise à jour)
donnees\	
keen\	fichiers reçus par KEEN (jamais remplacés)
dashboard\	fichiers reçus par le dashboard (jamais remplacés)

Si les fichiers étaient dans `C:\Keen\apps\dashboard`, la procédure de mise à jour (étape 7) les ferait disparaître avec l'ancien dossier.

1. Créer le dossier de données : `New-Item -ItemType Directory`

`C:\Keen\donnees\dashboard`.

2. Dire à l'application où ranger les fichiers. Dans votre code, lisez le chemin depuis une variable `UPLOAD_DIR` au lieu d'un chemin écrit en dur (Claude Code peut faire cette modification). Puis donnez-la au service, en reprenant toute la liste des variables de l'étape 8 :

```
$nssm = "C:\Keen\outils\nssm.exe"
& $nssm set KeenDashboard AppEnvironmentExtra "PORT=3001"
"HOSTNAME=127.0.0.1"
"DATABASE_URL=mysql://dashboard:AutreMotDePasse@localhost:3306/dashboard"
"BETTER_AUTH_SECRET=UneAutreChaineAleatoire"
"BETTER_AUTH_URL=https://dashboard.keen.local"
"UPLOAD_DIR=C:\Keen\donnees\dashboard"
& $nssm restart KeenDashboard
```

3. Taille maximale des fichiers. Next.js refuse par défaut les envois de plus de 1 Mo par les « server actions ». Si vos imports passent par là, ajoutez dans `next.config.ts` : `experimental: { serverActions: { bodySizeLimit: "20mb" } }`. Les envois par une route API ne sont pas concernés. Caddy, lui, n'impose aucune limite.

4. **Sauvegarde commune base + fichiers.** Remplacez le script `C:\Keen\sauvegarde.ps1` de l'étape 5 par celui-ci, qui traite toutes les applications de la liste. Chaque archive contient la base **et** le dossier de fichiers d'une application, au même instant :

```
$date = Get-Date -Format "yyyy-MM-dd_HH:mm"
$cle = Get-Content C:\Keen\outils\cle-sauvegarde.txt
$app = @(
    @{ nom = "keen"; base = "keen"; dossier = "C:\Keen\donnees\keen"
},
    @{ nom = "dashboard"; base = "dashboard"; dossier =
"C:\Keen\donnees\dashboard" }
)
foreach ($a in $apps) {
    $dump = "C:\Keen\tmp\$($a.base)-$date.sql"
    & "C:\Program Files\MariaDB 11.4\bin\mariadb-dump.exe" --defaults-extra-
file=C:\Keen\outils\sauvegarde.cnf --single-transaction --result-file=$dump
$a.base
    & "C:\Program Files\7-Zip\7z.exe" a -t7z -mhe=on "-p$cle"
"E:\Sauvegardes\$($a.nom)-$date.7z" $dump $a.dossier
    Remove-Item $dump
}
Get-ChildItem E:\Sauvegardes\*.7z | Where-Object LastWriteTime -lt (Get-
Date).AddDays(-30) | Remove-Item
```

Pour une nouvelle application, il suffit d'ajouter une ligne dans la liste `$apps`.

5. **Surveiller la place.** Les fichiers s'accumulent. Une fois par mois, regardez l'espace libre du disque C: et du disque de sauvegarde (clic droit > Propriétés). Au-dessous de 20 % libre, faites le ménage ou changez de disque.

Test de restauration base + fichiers

6. Dans le dashboard, importez un fichier Excel reconnaissable, lancez la sauvegarde, puis supprimez l'import dans l'application.
7. Extrayez l'archive : `& "C:\Program Files\7-Zip\7z.exe" x`
`E:\Sauvegardes\dashboard-AAAA-MM-JJ_HHMM.7z -oC:\Keen\tmp\restau`. Vous obtenez le fichier `.sql` et le dossier `dashboard` avec les fichiers.
8. Pour une vraie restauration : arrêtez le service (`nssm stop KeenDashboard`), restaurez la base comme à l'étape 5 (dans la base `dashboard` cette fois), remplacez le contenu de `C:\Keen\donnees\dashboard` par le dossier extrait, puis redémarrez le service.

Contrôle : après restauration, l'import supprimé réapparaît dans le dashboard **et** son fichier s'ouvre. Faites aussi une mise à jour de l'application (étape 7) : les fichiers importés doivent toujours être là après.

Étape 10 : versions PWA (téléphone) et Electron (bureau)

La PWA et l'application Electron ne sont que deux façons d'ouvrir la même application.

Les données et la base restent sur le mini-PC ; le téléphone et le poste de bureau affichent et envoient, mais ne stockent rien d'important. Rien ne change donc aux étapes 1 à 9. Comptez une heure.

	PWA	Electron
Servie par	Le mini-PC, comme le site (même adresse)	Un installateur .exe posé sur chaque poste
Données	Sur le mini-PC	Sur le mini-PC, via l'adresse https de l'application
Mise à jour	Automatique avec celle du serveur (étape 7)	Fichier de mise à jour déposé sur le mini-PC
Condition	Certificat HTTPS reconnu par le téléphone	Certificat reconnu par Windows

A. PWA sur téléphone

Une PWA ne s'installe que si le téléphone fait confiance au certificat HTTPS. Avec l'avertissement accepté à l'étape 4, le site s'affiche mais le bouton « Installer l'application » n'apparaît pas.

1. Installer le certificat de Caddy sur le téléphone. Envoyez-vous le fichier `root.crt` (étape 4).

- Android : Paramètres > Sécurité > Chiffrement et identifiants > Installer un certificat > Certificat CA.
- iPhone : ouvrez le fichier, puis Réglages > Profil téléchargé > Installer, puis Réglages > Général > Informations > Réglages des certificats > activer la confiance totale.

2. Utiliser une adresse par nom. Un téléphone ne lit pas le fichier hosts. Déclarez `dashboard.keen.local` vers 192.168.1.50 dans la box si elle le permet (« DNS local »). Sinon, utilisez la solution recommandée ci-dessous.

3. Ouvrez l'adresse dans Chrome (Android) ou Safari (iPhone) > menu > « Installer l'application » ou « Sur l'écran d'accueil ».

Solution recommandée chez un vrai client : un vrai nom de domaine, par exemple `dashboard.client1.keenexpertises.com`, qui pointe vers 192.168.1.50 dans Cloudflare, et un vrai certificat Let's Encrypt obtenu par Caddy avec le module Cloudflare (validation DNS, aucun port ouvert). Les téléphones et les postes font alors confiance au certificat

sans rien installer. Cette variante demande une version de Caddy avec le module Cloudflare, et une connexion Internet au moins tous les 60 jours pour renouveler le certificat.

Prudence avec le mode hors ligne : ne mettez pas en cache sur le téléphone des données nominatives (SIRH). Un téléphone perdu ne doit rien révéler.

B. Application Electron sur les postes

4. **Modèle à suivre : un « client léger ».** La fenêtre Electron ouvre l'adresse https de l'application sur le mini-PC. Ne mettez **jamais** de base de données dans Electron, et ne connectez jamais Electron directement à MariaDB : le port 3306 reste fermé, tout passe par l'application.
5. **Adresse du serveur dans un fichier, pas dans le code.** Faites lire par Electron un fichier `config.json` placé à côté du programme, par exemple `{ "serveur": "https://dashboard.keen.local" }`. Le même installateur sert alors pour tous vos clients.
6. **Certificat.** Electron utilise le magasin de certificats de Windows : le `root.crt` installé à l'étape 4 suffit. Avec la solution du vrai domaine, rien à faire.
7. **Distribuer l'installateur depuis le mini-PC.** Créez `C:\Keen\telechargements`, déposez-y l'installateur (fabriqué avec electron-builder sur votre PC), et ajoutez ce bloc au Caddyfile :

```
telechargements.keen.local {
    tls internal
    root * C:\Keen\telechargements
    file_server browse
}
```

Redémarrez Caddy, ajoutez le nom au fichier hosts des postes, et les utilisateurs téléchargent l'installateur à l'adresse `https://telechargements.keen.local`.

8. **Mises à jour automatiques.** Avec electron-updater en mode « generic », l'application vérifie ce même dossier au démarrage. Pour publier une version, vous déposez le nouvel installateur et le fichier `latest.yml` produit par electron-builder dans `C:\Keen\telechargements`.
9. **Avertissement Windows.** Sans certificat de signature de code (payant, environ 200 à 400 € par an), Windows SmartScreen affiche « Windows a protégé votre ordinateur » à l'installation. Chez un client, prévenez les utilisateurs ou faites l'installation vous-même (Informations complémentaires > Exécuter quand même).

Contrôle : la PWA est installée sur votre téléphone et affiche les mêmes données que le navigateur. L'application Electron, installée sur votre PC depuis `https://telechargements.keen.local`, s'ouvre sur le mini-PC. Arrêtez le service de

l'application : la PWA et Electron affichent toutes deux une erreur de connexion, ce qui prouve que les données ne sont bien que sur le serveur.

Fiche de suivi et carnet de bord

Cochez chaque étape une fois son contrôle réussi. Une étape non contrôlée n'est pas finie.

- ☐ Raccordement : même passerelle que les autres postes, ping sans perte pendant une heure
- ☐ Étape 1 : le mini-PC redémarre seul après une coupure, IP fixe 192.168.1.50, BitLocker actif
- ☐ Étape 2 : service MariaDB automatique, base keen créée
- ☐ Étape 3 : le site répond sur <http://127.0.0.1:3000> depuis le mini-PC
- ☐ Étape 4 : <https://keen.local> avec cadenas depuis le PC, le port 3000 fermé depuis l'extérieur
- ☐ Étape 5 : archive chiffrée sur le disque USB et restauration réussie dans keen_test
- ☐ Étape 6 : Bureau à distance en 4G via Tailscale, refusé après déconnexion
- ☐ Étape 7 : les 7 incidents testés et cochés
- ☐ Étape 8 : deux applications en ligne, l'arrêt de l'une ne gêne pas l'autre
- ☐ Étape 9 : fichiers rangés dans C:\Keen\donnees, restaurés avec la base, intacts après une mise à jour
- ☐ Étape 10 : PWA installée sur le téléphone, Electron installé depuis le mini-PC, les deux sans données locales

Carnet de bord : notez ici chaque problème rencontré et sa solution. Ce carnet deviendra la base de votre procédure d'installation chez les clients.

Date	Étape	Problème rencontré	Solution trouvée	Temps passé

Pour imprimer : cliquez sur le nom du document en haut > Exporter > PDF. Les mots de passe écrits sur la fiche d'identité restent sur papier, jamais dans ce document en ligne.