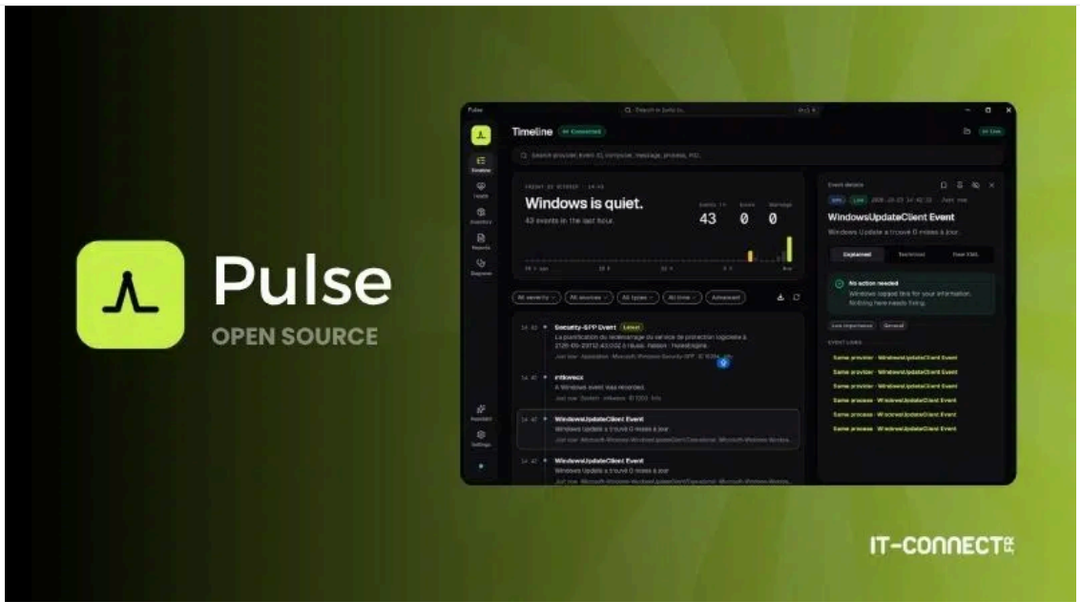


ASTUCES & LOGICIELS SELF-HOSTING & OPEN SOURCE

Pulse : les journaux d'événements de Windows facilement lisibles, avec de l'IA locale

24/10/2026 Florian BURNEL 0 commentaire Open Source, Windows

Écran bleu, redémarrage inattendu, service qui plante : Windows a presque toujours noté la cause quelque part, encore faut-il réussir à la lire dans l'Observateur d'événements.

Que vous dépanniez le PC d'un proche, un poste utilisateur ou votre propre machine, le réflexe est souvent le même : ouvrir l'Observateur d'événements et faire défiler des milliers de lignes à la recherche de la bonne information à propos de l'erreur. C'est là qu'intervient **Pulse**, un outil gratuit et open source pour Windows 10 et Windows 11, qui vous aide à y voir plus clair dans les journaux d'événements de Windows.

Sommaire [-]

- Qu'est-ce que Pulse ?
- Installer Pulse sur Windows
- Découvrir l'interface de Pulse
  - La Timeline : les journaux Windows en clair
  - Expliqué, technique ou XML brut
  - Filtrer et rechercher dans les événements
  - Santé du système et inventaire
- Utiliser l'assistant IA local de Pulse avec Ollama ou LM Studio
  - Préparer le modèle d'IA local
  - Interroger l'assistant de Pulse
- Analyser les journaux d'un autre PC avec un fichier EVTX
  - Exporter le journal sur le PC à analyser
  - Ouvrir le fichier EVTX dans Pulse
- Générer des rapports avec Pulse
- Conclusion

Qu'est-ce que Pulse ?

Pulse est une application de diagnostic pour Windows 10 et Windows 11, gratuite et open source (licence MIT), qui lit les journaux d'événements de Windows et les reformule en phrases compréhensibles. Elle fonctionne en lecture seule, entièrement en local, et peut s'appuyer sur un assistant IA exécuté sur le PC (Ollama ou LM Studio) pour répondre à des questions posées en langage naturel.

Là où l'Observateur d'événements affiche un fournisseur, un ID d'événement et un bloc XML, Pulse affiche une phrase. Le dépôt du projet donne quelques exemples parlants :

CE QU'AFFICHE L'OBSERVATEUR D'ÉVÉNEMENTS	CE QUE DIT PULSE (TRADUIT)
Application Error, ID 1000	L'Explorateur s'est fermé de façon inattendue. Windows a redémarré l'Explorateur.
Kernel-Power, ID 41, BugcheckCode 159	Windows a redémarré après un écran bleu. Code d'arrêt : DRIVER_POWER_STATE_FAILURE.
Kernel-Power, ID 41, toutes les valeurs à 0	Le PC a perdu son alimentation ou s'est arrêté brutalement. Vérifiez l'alimentation, les températures et l'overclocking.

Cette application relativement jeune s'appuie sur un service Windows natif écrit en C++20 (`PulseService`) qui collecte et interprète les événements, et une application de bureau développée avec Flutter (Dart) pour l'interface. Il n'y a pas de télémétrie, ni de compte ou de dépendance avec un service Cloud.

Les ressources officielles du projet :

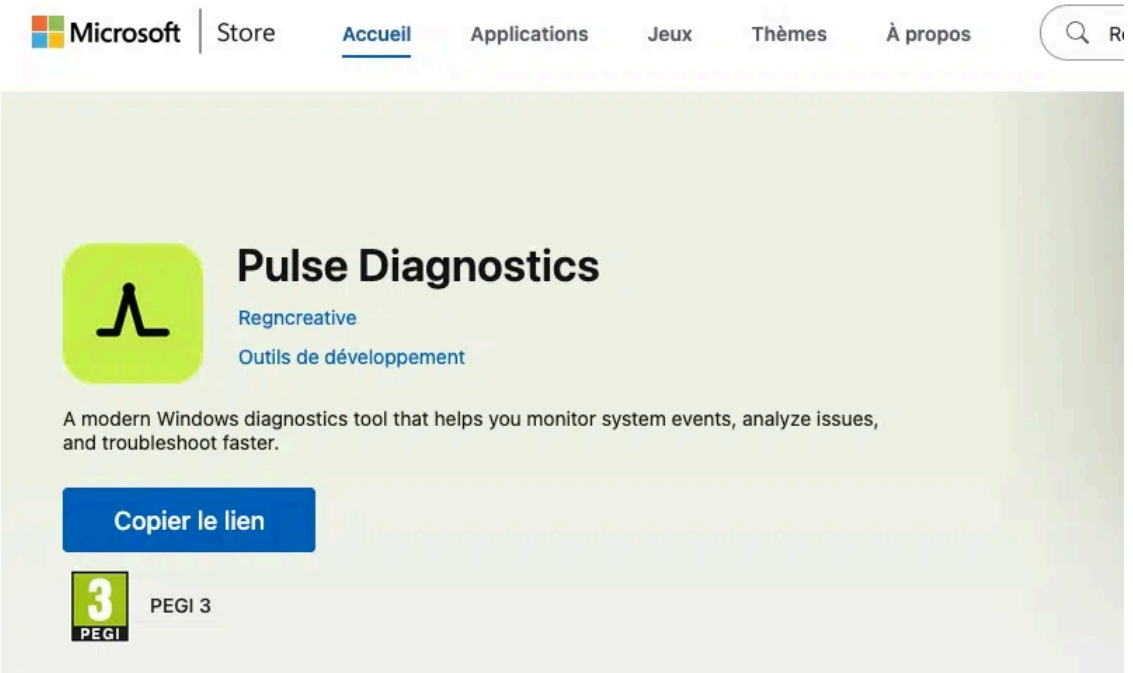
- Site officiel de Pulse
- Dépôt GitHub de Pulse (Regncreative/Pulse)
- Pulse Diagnostics sur le Microsoft Store

Installer Pulse sur Windows

Deux méthodes d'installation sont proposées : l'installeur publié sur GitHub et le Microsoft Store. Il n'y a rien de spécial à effectuer pour l'installer, quelques clics suffisent... Vous pouvez récupérer la dernière version dans la section Releases du dépôt GitHub. Par exemple, téléchargez le fichier `Pulse-Setup-1.5.0-windows-x64.exe` .

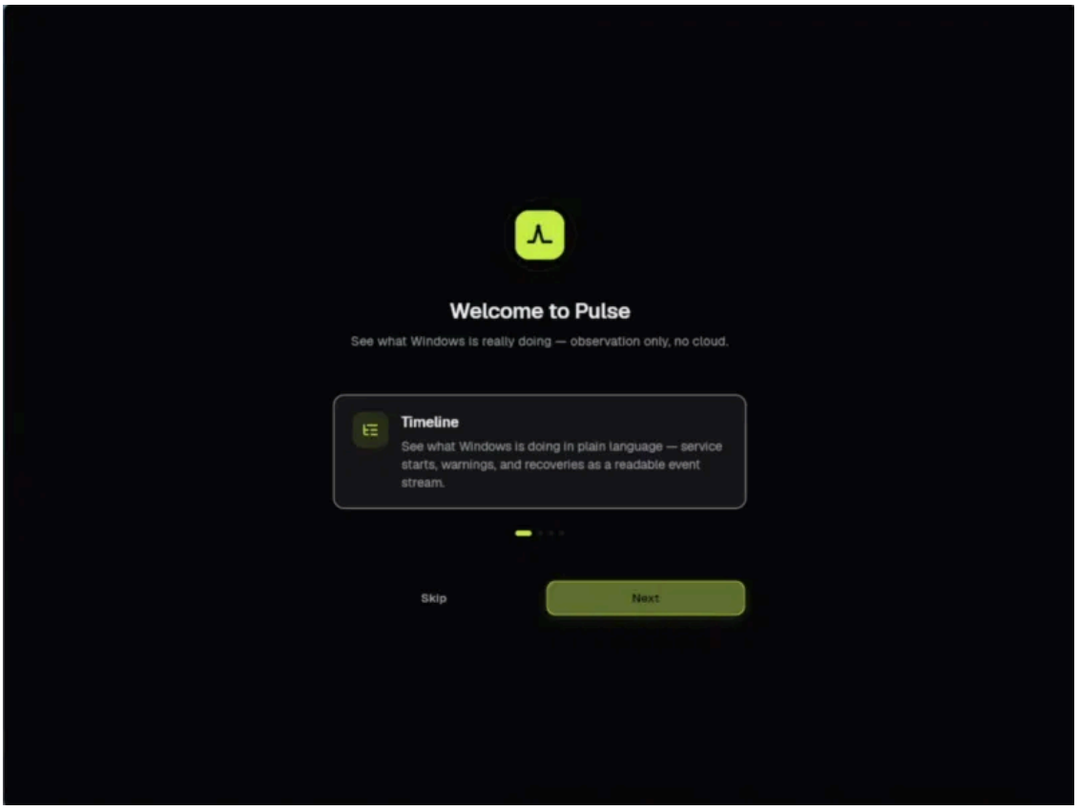
> **Attention** : en l'absence de signature, Windows SmartScreen ou votre antivirus peuvent afficher un avertissement au lancement de l'installeur. Le développeur a déposé une demande auprès du programme gratuit de la SignPath Foundation pour signer les prochaines versions (demande en cours d'examen au moment où j'écris ces lignes).

Pulse est également disponible sur le Microsoft Store sous le nom Pulse Diagnostics. Dans ce cas, le service est intégré au paquet de l'application, les mises à jour passent par le Store.



Découvrir l'interface de Pulse

Au premier lancement, Pulse présente ses différentes sections : Timeline, System Health, Diagnostics et le rôle du service `PulseService` . Le slogan donne le ton : « See what Windows is really doing », avec la mention « observation only, no cloud ».

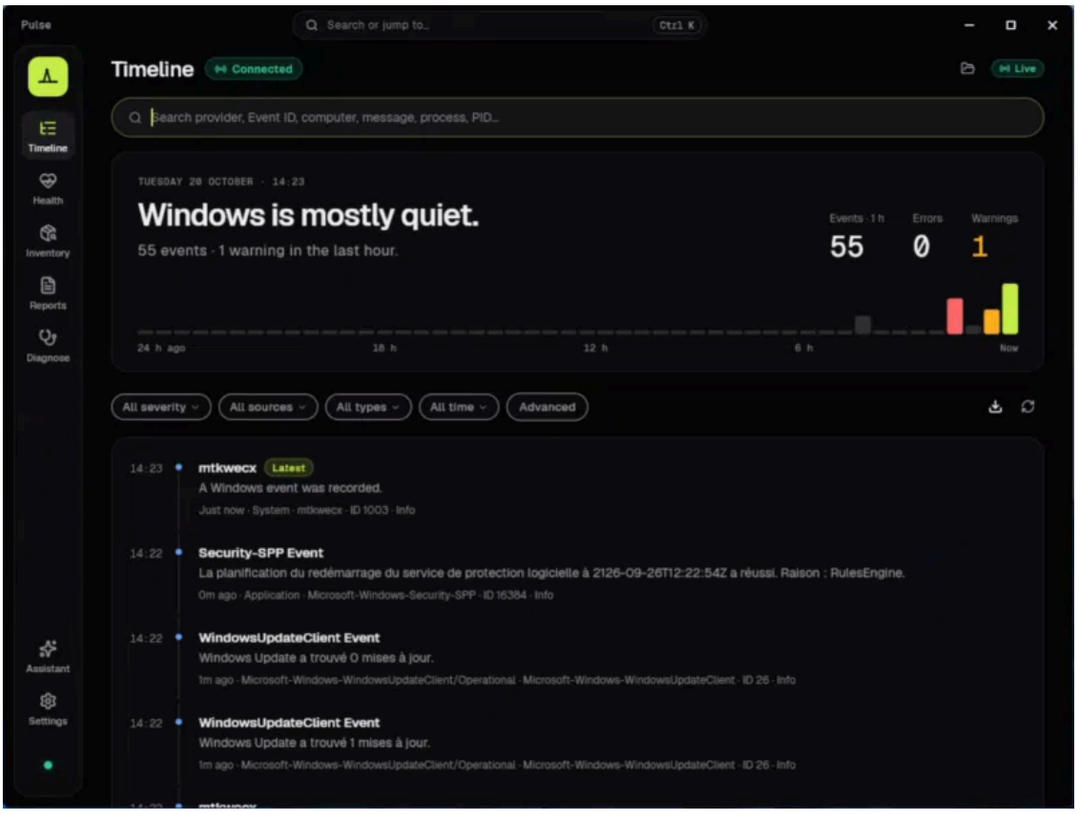


Précision : l'interface de Pulse est uniquement en anglais, et le dépôt ne contient pas de fichiers de traduction à ce jour. En revanche, les messages des événements remontés par Windows restent dans la langue du système, donc en français sur un Windows français.

La Timeline : les journaux Windows en clair

La Timeline est la vue principale de Pulse. En haut, une phrase résume la dernière heure (« *Windows is mostly quiet* », ou au contraire « *Windows reported a problem in the last hour* »), accompagnée de trois compteurs : le nombre d'événements, d'erreurs et d'avertissements sur une heure. Une bande d'activité sur 24 heures permet de repérer d'un coup d'œil les pics d'erreurs.

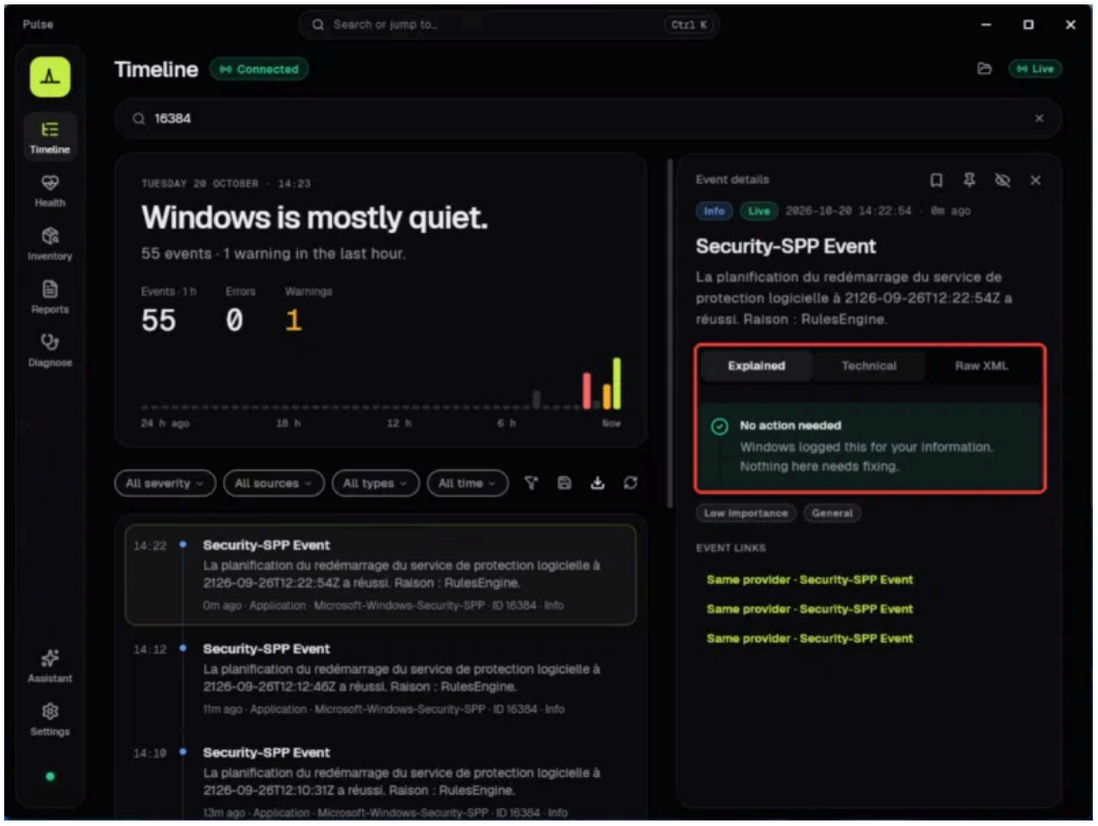
En dessous, les événements défilent en direct, du plus récent au plus ancien. Le badge « Live » indique que le flux est actualisé en temps réel.



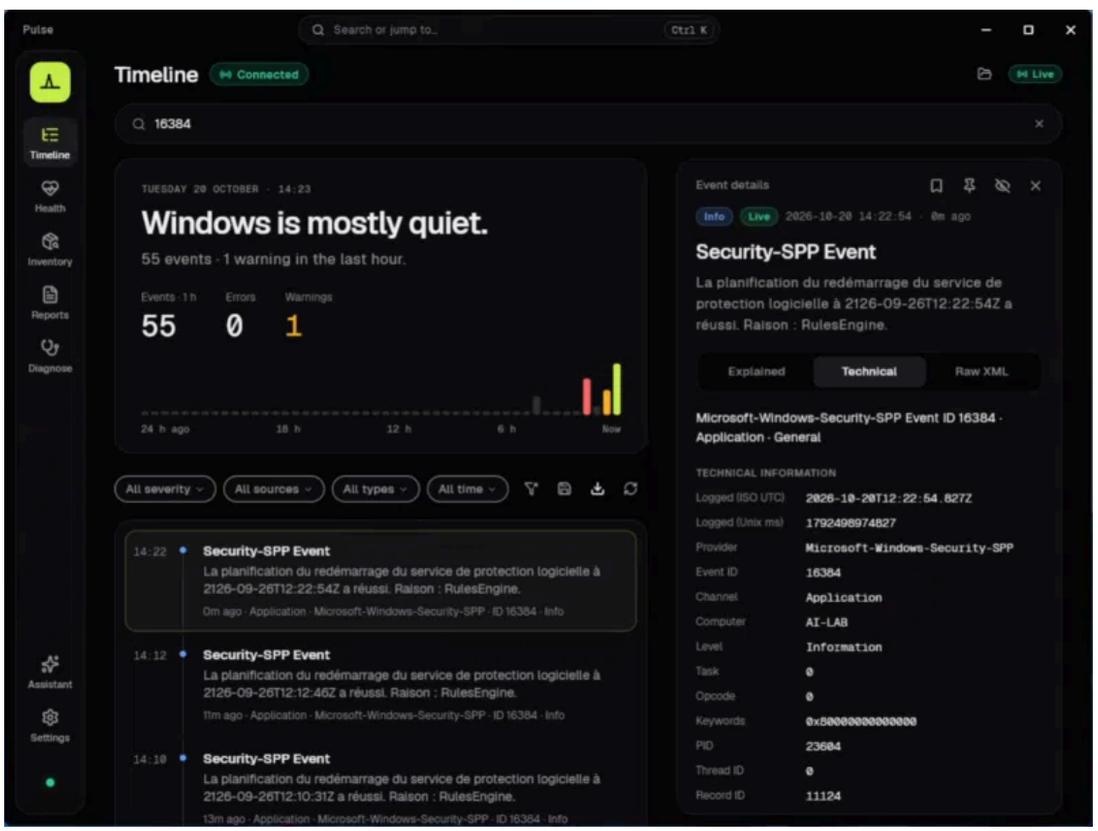
Expliqué, technique ou XML brut

Un clic sur un événement ouvre le panneau « Event details », qui propose trois niveaux de lecture :

- **Explained** : l'explication en langage clair, avec une indication sur l'action à mener. Ici, « **No action needed** » : Windows a simplement consigné une information.
- **Technical** : les champs habituels de l'événement (fournisseur, ID d'événement, journal, ordinateur, niveau, mots-clés, ID de processus, etc.).
- **Raw XML** : le XML brut de l'événement, identique à celui de l'onglet « **Détails** » de l'Observateur d'événements.



L'onglet « **Technical** » reste précieux pour un administrateur, notamment pour retrouver l'ID d'événement et le fournisseur à reporter dans une recherche plus poussée.

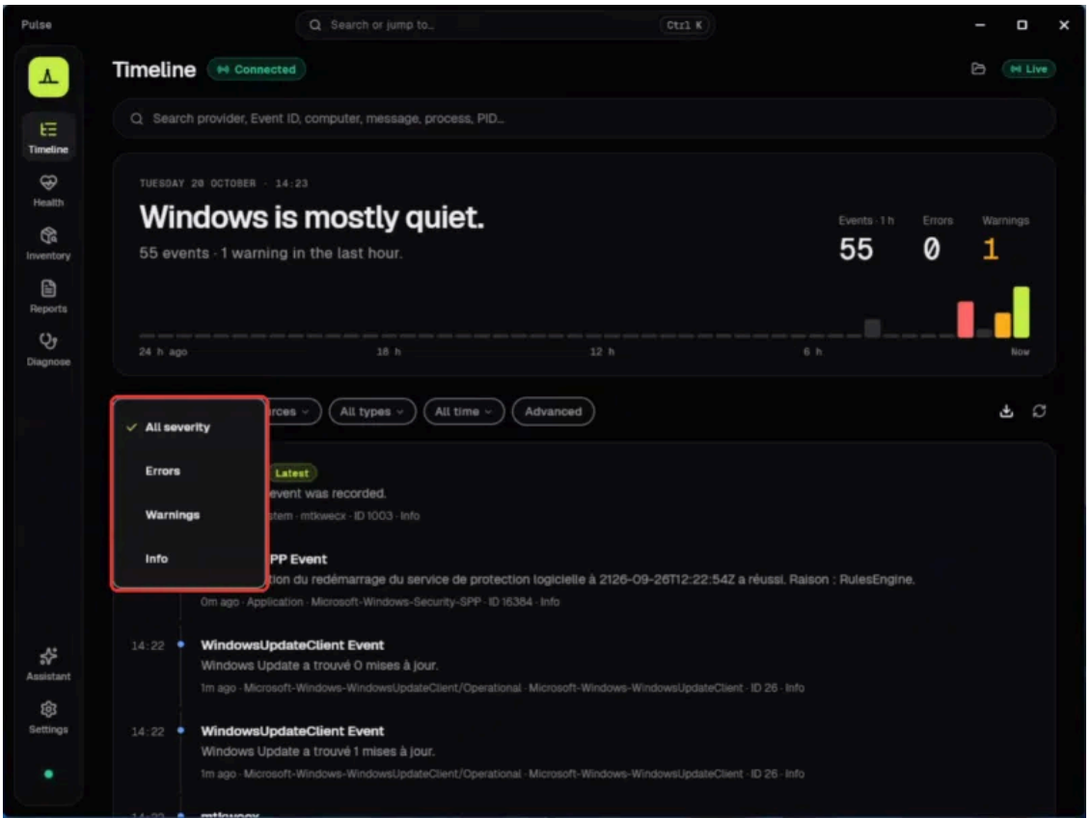


Le panneau affiche aussi des liens vers les événements proches (« Same provider », « Same process »), ce qui permet de remonter le fil d'un incident. Pulse cherche d'ailleurs à regrouper des événements liés en un seul incident : le plantage d'une application avec son rapport d'erreur, un écran bleu avec le redémarrage qui suit, ou encore le plantage d'un service avec l'action de récupération déclenchée par Windows.

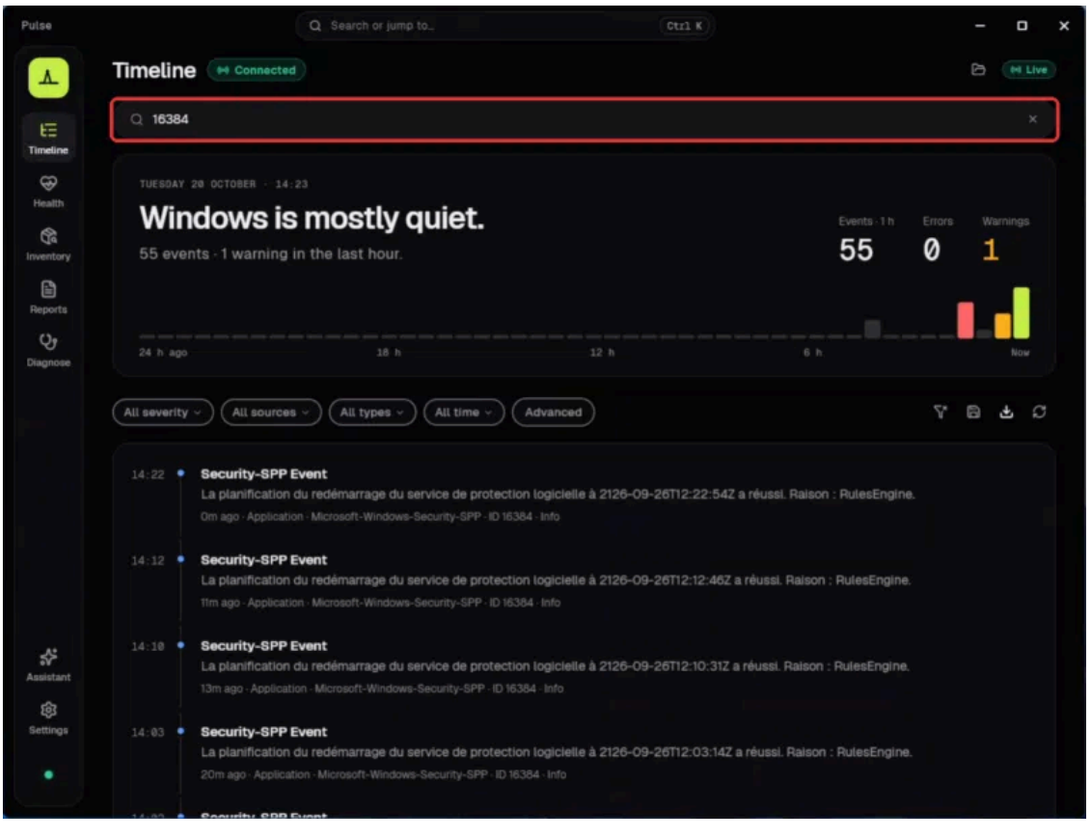
Filtrer et rechercher dans les événements

La barre de filtres permet de trier les événements par :

- **Gravité** : erreurs, avertissements ou informations.
- **Source** : le fournisseur de l'événement.
- **Type** : plantage, service, alimentation, mise à jour, périphérique, démarrage, sécurité, stockage.
- **Période** : 15 minutes, 1 heure, 24 heures, 7 jours ou une plage personnalisée.



Le champ de recherche accepte un fournisseur, un ID d'événement, un nom d'ordinateur, un extrait de message, un nom de processus ou un PID. Dans l'exemple ci-dessous, la recherche porte sur l'ID d'événement `16384`.



Les recherches peuvent être enregistrées, et les événements marqués d'un signet ou épinglés. Il y a aussi une option nommée « Hide events like this » pour masquer tous les événements de même fournisseur et de même ID dans la Timeline et dans les compteurs. C'est pratique pour faire taire un événement récurrent et sans vraiment d'importance.

Pulse lit aussi les métadonnées des événements de façon à tenter d'expliquer l'origine d'un écran bleu : le nom du code d'arrêt, ce qui le provoque habituellement et les points à vérifier ensuite. Il distingue donc un arrêt forcé, d'une coupure d'alimentation ou d'une erreur matérielle.

> **Note** : Pulse s'appuie sur les journaux d'événements, pas sur les fichiers de vidage mémoire. L'analyse des minidumps figure dans la feuille de route du projet, mais elle n'est pas encore disponible.

Santé du système et inventaire

La section « Health » (System Health) affiche un score de santé et l'activité en direct du processeur, de la mémoire, du GPU, du disque et du réseau, avec un historique de 60

secondes. La charge GPU est calculée de la même manière que dans le Gestionnaire des tâches, et un PC équipé de deux GPU (intégré et dédié) les affiche tous les deux.

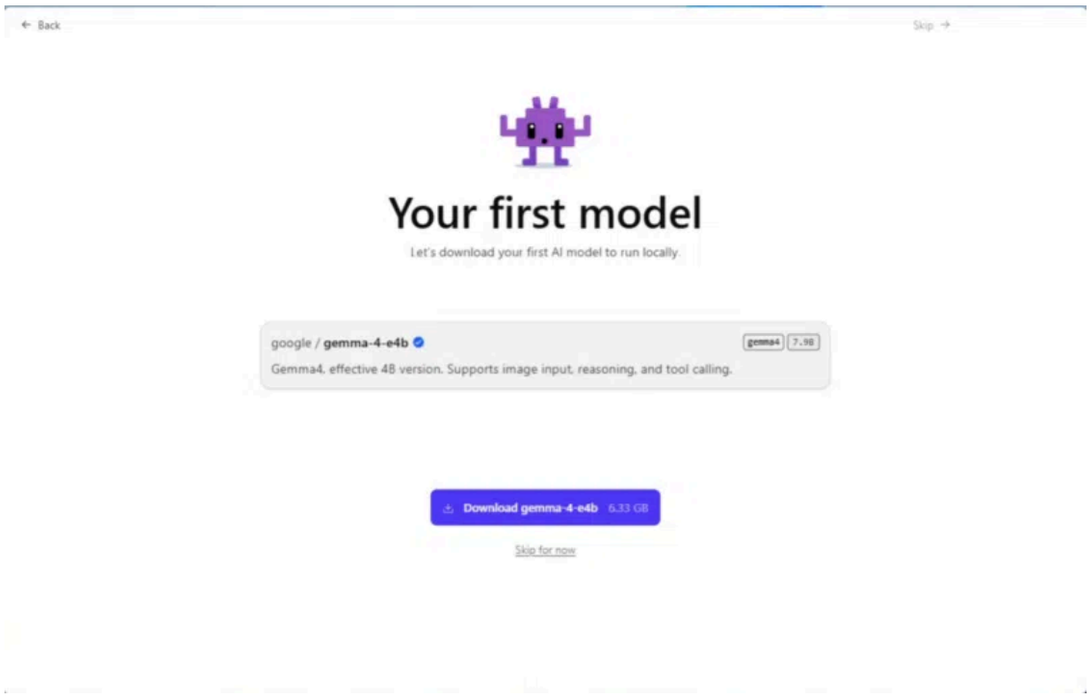
La consommation est également détaillée par processus. En complément, des alertes peuvent être activées en arrière-plan, depuis la zone de notification, en cas de charge CPU ou mémoire élevée et prolongée. La section « **Inventory** » liste quant à elle le matériel (carte mère, BIOS, processeur, barrettes mémoire, stockage, cartes réseau), les périphériques ainsi que les logiciels, pilotes et services installés.

Utiliser l'assistant IA local de Pulse avec Ollama ou LM Studio

Pulse intègre un assistant facultatif auquel vous pouvez poser des questions en langage naturel sur l'état du PC : « *Why is my PC slow?* », « *What's using the most memory?* », etc. Cet assistant ne s'appuie sur aucun service cloud : il interroge un modèle de langage exécuté localement, via **Ollama** ou **LM Studio**.

Préparer le modèle d'IA local

Pulse n'installe ni Ollama ni LM Studio : c'est à vous de le faire, puis de télécharger un modèle. Pour mes tests, j'ai utilisé LM Studio avec le modèle `google/gemma-4-e4b`, proposé dès le premier lancement de LM Studio.

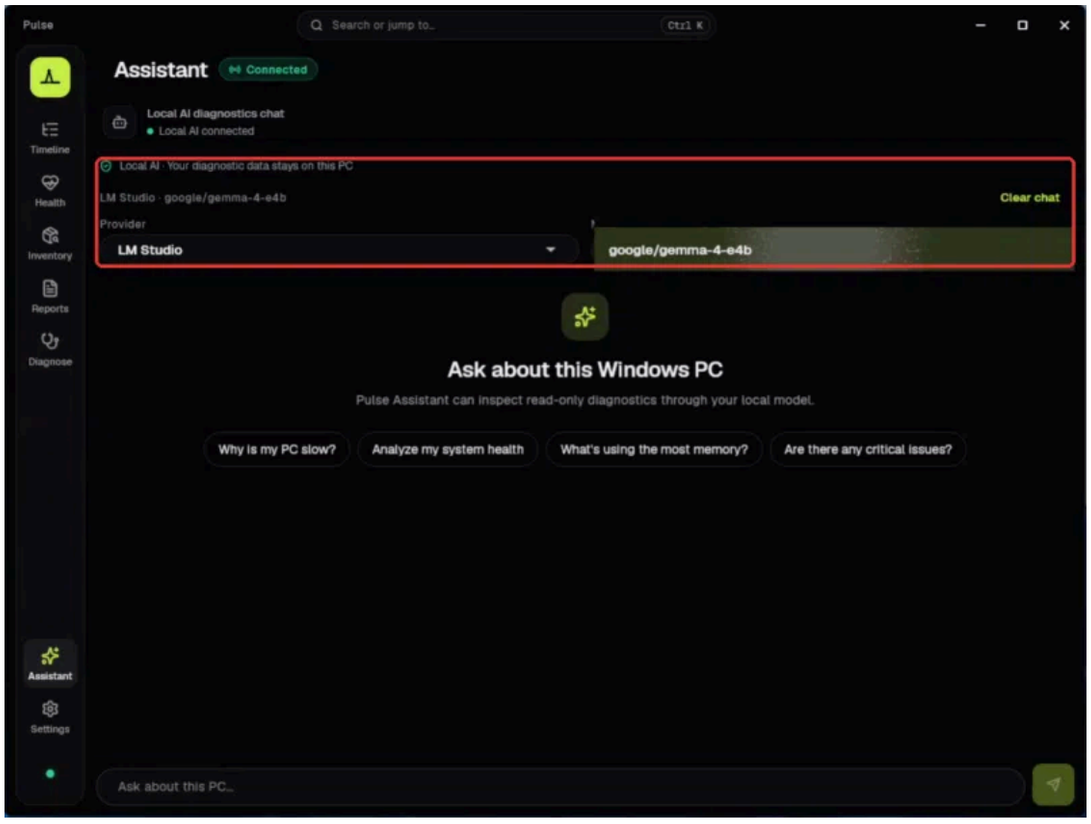


Si vous préférez Ollama, notre tutoriel pour installer Ollama et Open WebUI sur Windows 11 vous guidera. Pour choisir un modèle adapté à votre matériel, l'article CanIRun.ai et LLMfit : trouvez le modèle d'IA adapté pour votre PC pourra vous aider.

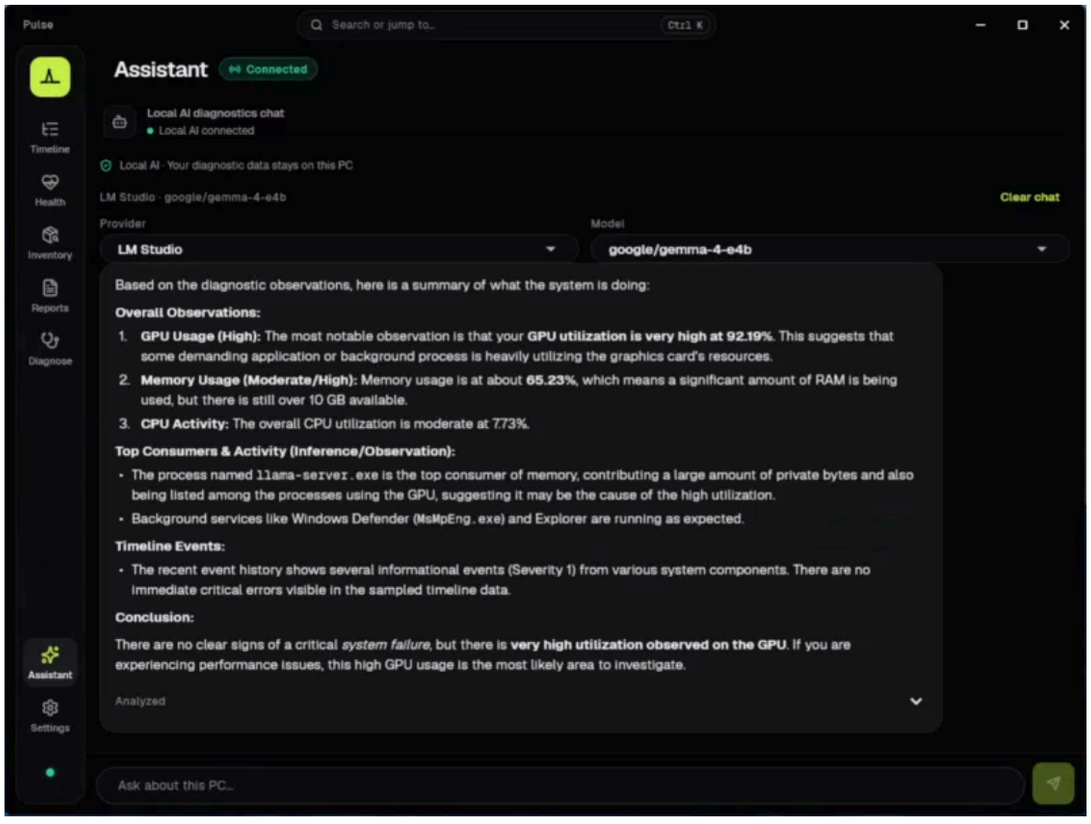
Par défaut, Pulse contacte Ollama sur le port `11434` et LM Studio sur le port `1234`. Vous devez donc configurer LM Studio (ou Ollama) de façon à être en écoute sur ce port, et de toute façon, LM Studio n'est pas en écoute du tout par défaut.

Interroger l'assistant de Pulse

Dans la section « **Assistant** », choisissez le fournisseur et le modèle. La mention « *Local AI · Your diagnostic data stays on this PC* » rappelle que les données ne quittent pas la machine. Des suggestions de questions sont proposées pour démarrer.



Au hasard et à titre d'exemple pour cet article, j'ai posé la question « *Are there any critical issues?* » proposée par Pulse. L'assistant interroge alors Pulse au travers d'outils en lecture seule (événements récents, métriques, processus, services) et rédige une synthèse : observations générales, processus les plus gourmands, événements de la Timeline et conclusion.



La réponse est pertinente, avec une petite ironie : le processus le plus gourmand signalé par l'assistant, `llama-server.exe`, n'est autre que le moteur qui exécute le modèle d'IA lui-même. Gardez aussi en tête que la génération locale prend du temps, surtout si vous n'avez pas de GPU dédié ou si vous utilisez un LLM trop gourmand.

Analyser les journaux d'un autre PC avec un fichier EVTX

Pulse ne se limite pas au PC sur lequel il est installé : il sait ouvrir un fichier `.evtx` exporté depuis une autre machine. C'est très pratique pour analyser les journaux d'un poste à distance sans y installer Pulse : certains vont préférer collecter les journaux dans un SIEM, mais là nous sommes dans un contexte différente (voir à une échelle différente).

Exporter le journal sur le PC à analyser

Sur la machine source, vous pouvez exporter un journal depuis l'Observateur d'événements, avec l'action **Enregistrer tous les événements sous...**, ou en ligne de commande avec `wevtutil`, depuis une console lancée en tant qu'administrateur :

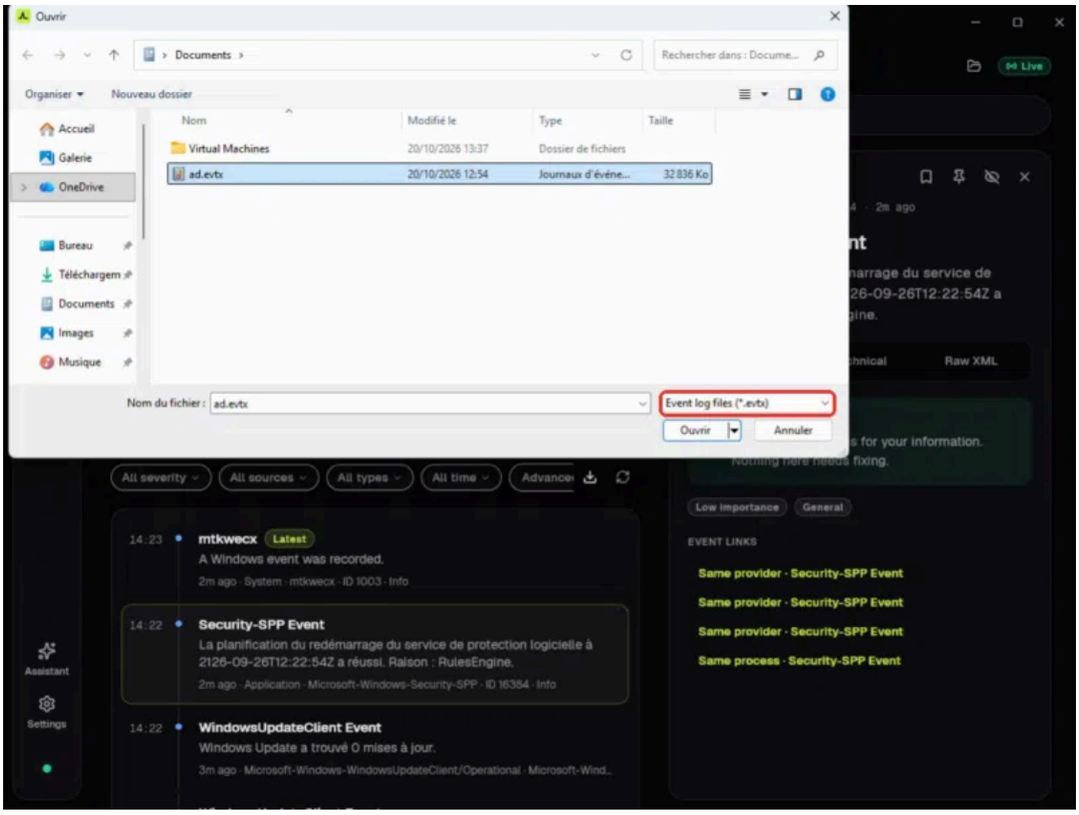
```
wevtutil epl System C:\Temp\System.evtx
```

Quelques précisions sur cette commande :

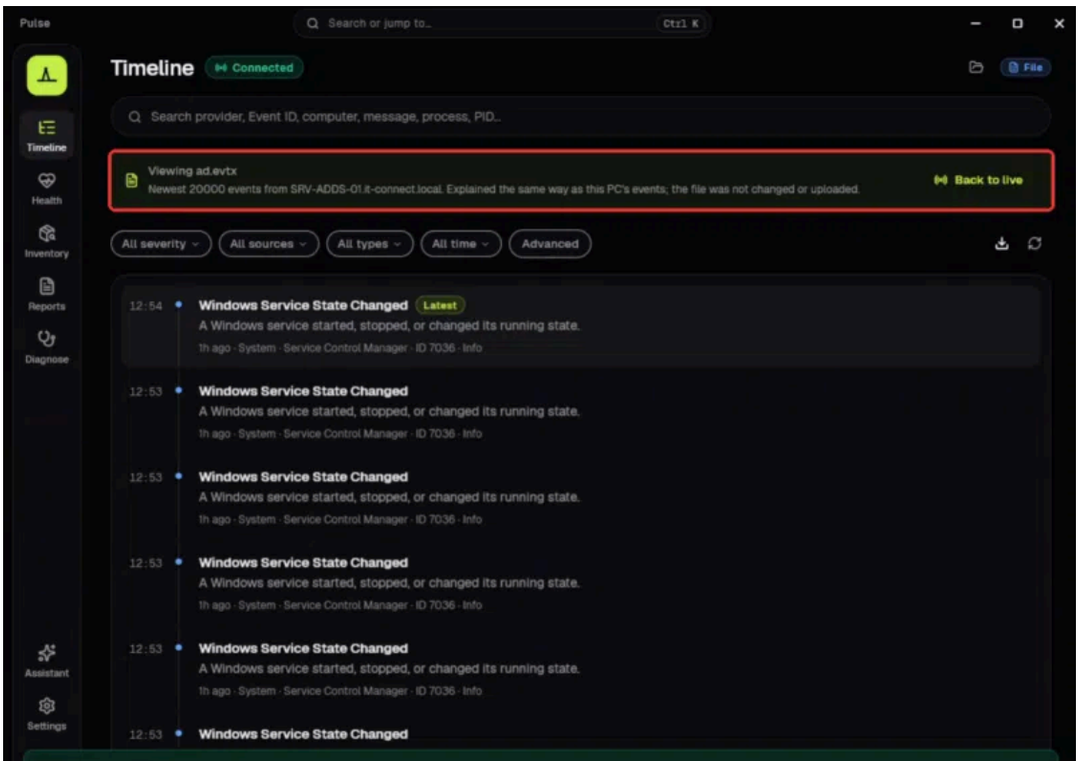
- `epl` : abréviation de `export-log`, la sous-commande qui exporte un journal vers un fichier.
- `System` : le nom du journal à exporter. Vous pouvez aussi indiquer `Application`, `Security`, ou le nom complet d'un journal d'applications et de services.
- `C:\Temp\System.evtx` : le chemin du fichier de destination. Le dossier doit exister au préalable.

Ouvrir le fichier EVTX dans Pulse

Dans la Timeline, cliquez sur l'icône en forme de dossier, en haut à droite, puis sélectionnez le fichier. La boîte de dialogue filtre directement les fichiers de type EVTX.



Pour cet exemple, j'ai ouvert le fichier `ad.evtx`, exporté depuis le contrôleur de domaine `SRV-ADDS-01.it-connect.local`. Un bandeau confirme la source (« Viewing ad.evtx ») et indique que les 20 000 événements les plus récents du fichier sont expliqués de la même façon que ceux du PC local.



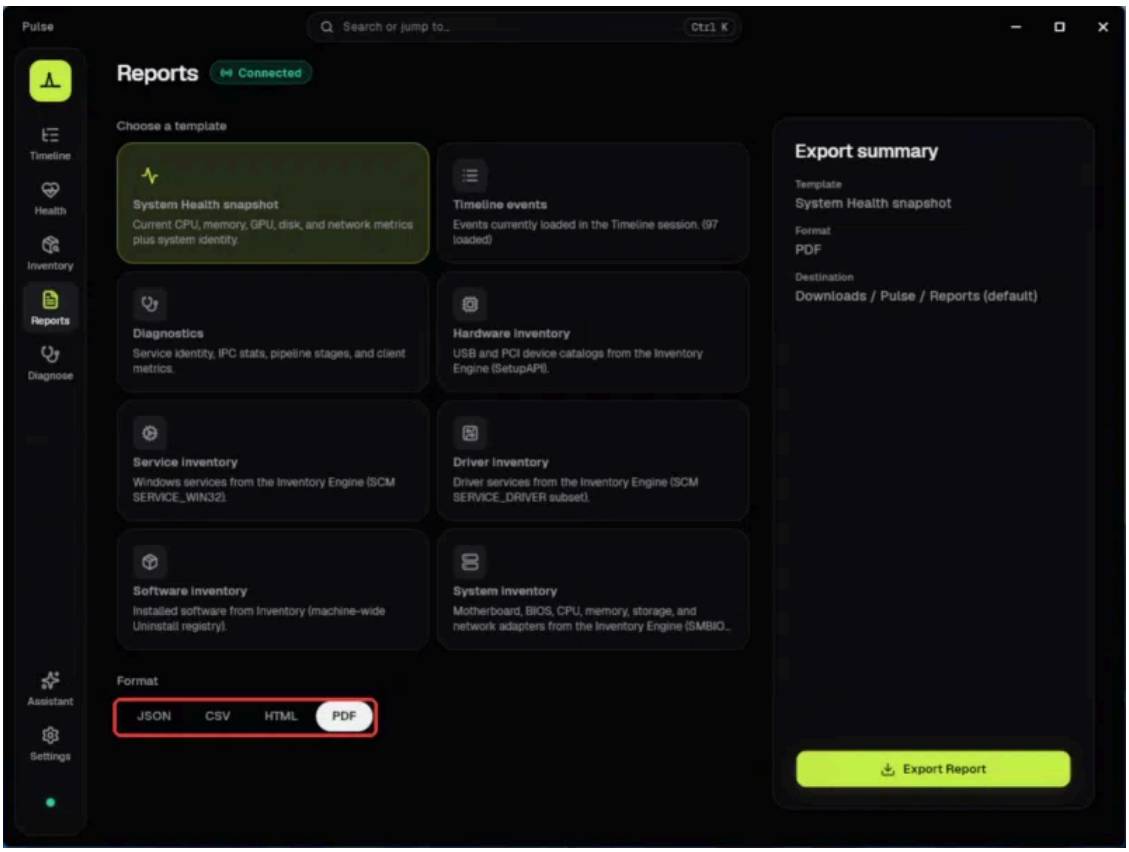
Note : Pulse n'est pas un outil d'investigation numérique. Pour analyser des journaux de sécurité à la recherche de traces d'attaque, tournez-vous vers des outils dédiés comme Zircolite : consultez notre article Comment effectuer une investigation numérique sur les journaux d'événements Windows avec Zircolite ?.

Générer des rapports avec Pulse

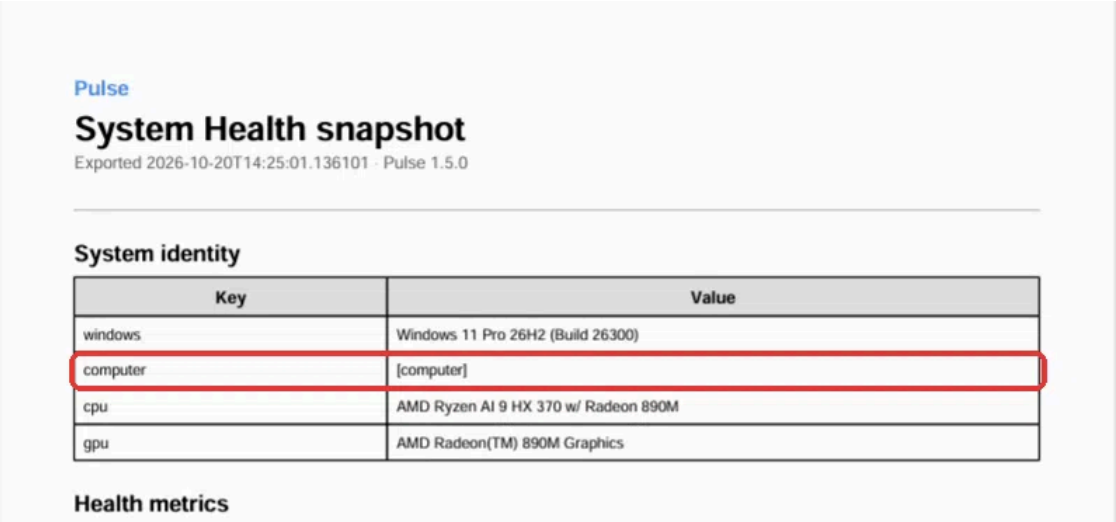
La section « **Reports** » permet d'exporter un rapport à partir de plusieurs modèles :

- **System Health snapshot** : métriques CPU, mémoire, GPU, disque et réseau, avec l'identité du système.
- **Timeline events** : les événements chargés dans la Timeline.
- **Diagnostics** : l'état du service et du canal de communication avec l'application.
- **Hardware inventory**, **Service inventory**, **Driver inventory**, **Software inventory** et **System inventory** : les différents volets de l'inventaire.

Quatre formats sont disponibles : JSON, CSV, HTML et PDF. Voici un aperçu des rapports proposés :



Côté confidentialité, Pulse peut masquer les informations personnelles dans les rapports et les exports. Les noms d'utilisateur et d'ordinateur, les chemins de profil, les SID, les adresses e-mail, IP et MAC ainsi que les numéros de série sont remplacés par des jetons (comme `[computer]` dans l'exemple ci-dessous). C'est une option configurable dans les paramètres de Pulse.



Pulse

System Health snapshot

Exported 2026-10-20T14:25:01.136101 · Pulse 1.5.0

System identity

Key	Value
windows	Windows 11 Pro 26H2 (Build 26300)
computer	[computer]
cpu	AMD Ryzen AI 9 HX 370 w/ Radeon 890M
gpu	AMD Radeon(TM) 890M Graphics

Health metrics

Key	Value
windows_edition	Windows 11 Pro
windows_version	26H2 (Build 26300)
cpu_model	AMD Ryzen AI 9 HX 370 w/ Radeon 890M
gpu_model	AMD Radeon(TM) 890M Graphics
installed_ram_bytes	34359738368
primary_storage_bytes	1998858481664
active_network_adapter	Realtek Gaming 2.5GbE Family Controller #2
sample_unix_ms	1792499101084
cpu_percent	21.7
memory_used_bytes	11352018944
memory_total_bytes	29654626304
gpu_percent	1.8

Conclusion

Pulse répond à un vrai besoin : y voir plus clair dans les journaux de Windows, sans devoir déchiffrer des ID d'événements et du XML. La Timeline en direct, les explications en langage clair, la lecture des fichiers EVTX et les rapports anonymisés en font un outil prometteur pour le dépannage. L'assistant IA local est un vrai plus, et j'apprécie l'approche tout en local. Néanmoins, je pense que rien ne vous empêche de solliciter un LM Studio ou un Ollama distant.

Le projet est encore jeune, mais j'avais envie de le mettre en avant car je trouve l'idée vraiment bonne. Je vous invite donc à le tester d'abord sur une machine virtuelle afin de vous faire un premier avis dessus. Pour un usage en entreprise, Pulse ne remplace pas une solution de collecte centralisée des journaux : c'est un outil de diagnostic à l'échelle d'un poste.

Ajouter IT-Connect à mes sources préférées

Florian BURNEL | Co-founder of IT-Connect

Cofondateur d'IT-Connect et Microsoft MVP "Cloud and Datacenter Management". Mon obsession depuis près de 15 ans ? Rendre l'administration système et la cybersécurité accessibles, que vous soyez junior ou confirmé. Plus qu'un métier, l'IT est pour moi une véritable passion. J'accompagne au quotidien les sysadmins et les professionnels de l'IT dans leur montée en compétences et leur veille technique.
Voir la bio complète ›

Open Source Windows Server PowerShell

Partagez cet article

PHP SIGNALE UNE NOUVELLE FAILLE RCE (CVE-2026-115560) : APPLIQUEZ LE MÊME RÉGLAGE QUE PHP2SHELL

Vous pourrez aussi aimer

Comment améliorer la recherche du menu Démarrer de Windows 10 ?
24/07/2019 0

ChangeDetection.io : un outil de veille pour surveiller les changements sur les pages web
22/12/2025 2

Laisser un commentaire

Votre adresse e-mail ne sera pas publiée. Les champs obligatoires sont indiqués avec *

Commentaire *

Nom *

E-mail *

Site web

☐ Enregistrer mon nom, mon e-mail et mon site dans le navigateur pour mon prochain commentaire.

Laisser un commentaire

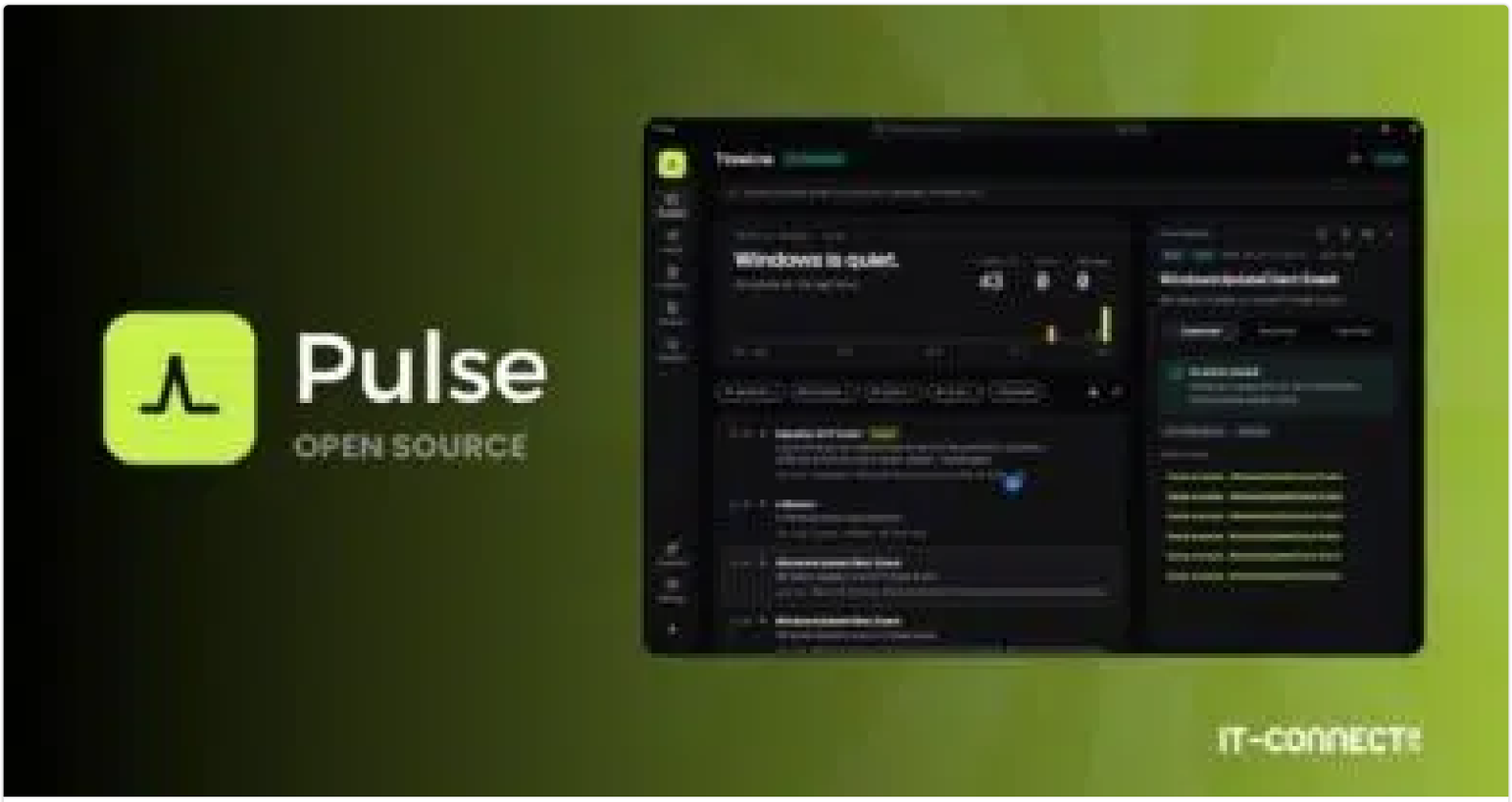
Ce site utilise Akismet pour réduire les indésirables. Découvrez comment les données de vos commentaires sont traitées.

✉ Newsletter : 1 e-mail par semaine !

Votre adresse e-mail*

S'abonner

📄 Guides & Tutos



ASTUCES & LOGICIELS SELF-HOSTING & OPEN SOURCE

Pulse : les journaux d'événements de Windows facilement lisibles, avec de l'IA locale

24/10/2026 Florian BURNEL 0 commentaire

Pulse est un outil gratuit et open source qui traduit les journaux d'événements de Windows 10 et 11 en langage clair, avec une IA locale (Ollama, LM Studio).

Exchange Online : vos applications EWS ne fonctionnent plus ? Voici comment les débloquer

23/10/2026 0 commentaire

Tiny11 Builder : créez un Windows 11 allégé facilement, sans toucher à PowerShell

22/10/2026 2 commentaires

⭐ Veille IT & Bons Plans

ACTU CYBERSÉCURITÉ

PHP signale une nouvelle faille RCE (CVE-2026-115560) : appliquez le même réglage que PHP2Shell

23/10/2026 Florian BURNEL 0 commentaire

CVE-2026-115560 : PHP signale une nouvelle faille RCE. Désactiver Session Upload Progress, déjà conseillé pour PHP2Shell, suffit en attendant le correctif.

Windows 11 : avec Project Pantheon, Microsoft teste une mémoire IA qui ne retient que ce que vous choisissez

23/10/2026 0 commentaire

Node2Shell : la faille Brotli qui expose Node.js à une exécution de code à distance

23/10/2026 0 commentaire

Réseau Tor : 333 relais de sortie compromis interceptaient les connexions SSH pour diffuser Ebury

23/10/2026 0 commentaire

Capcom piraté : 11,7 millions de comptes exposés et des mots de passe changés par l'attaquant

23/10/2026 0 commentaire

PHP2Shell : les attaquants avaient quatre jours d'avance sur le correctif

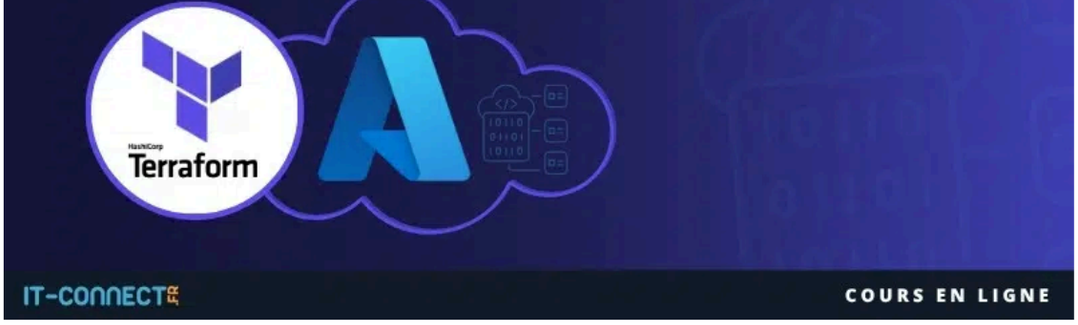
23/10/2026 0 commentaire

📚 Nos derniers cours gratuits

16 chapitres ★★★★★

Docker et Kubernetes : de l'initiation à la mise en production

Jérémy GAK



18 chapitres ★★★★★

L'Infrastructure as Code avec Terraform pour Microsoft Azure

Luc BRETON

Vous cherchez quelque chose ?

Recherche

Découvrir IT-Connect

A propos

Comment contribuer sur IT-Connect ?

Contact

Espace annonceurs

L'Équipe

Offres d'emploi

Politique de confidentialité

Puis-je réutiliser le contenu publié sur IT-Connect ?

Soutenir IT-Connect

Espace personnel

Se connecter

Créer un compte

Flux des publications

Changer de langue

Recommandations

Blogmotion

Tech2tech

Générateur de mots de passe

IT-Connect - Copyright © 2026 | Creative Commons License BY-NC 4.0