Automatisation du diagnostic Windows

ULTRADIAGPRO.PS1

Script PowerShell de diagnostic intelligent — Analyse automatique des événements système pour les techniciens N1/N2.

Le problème du diagnostic manuel

L'Observateur d'événements Windows

Lent

Navigation fastidieuse dans des milliers d'entrées

Complexe

Interface peu lisible, logs techniques difficiles à interpréter

Bruyant

Rempli de faux positifs qui noient les vraies alertes

Les conséquences terrain

Perte de temps

10 à 20 minutes perdues par ticket à fouiller les journaux manuellement

Risque d'erreur

Difficulté à identifier la vraie cause racine sous la masse d'événements

Manque de standardisation

Chaque technicien analyse à sa façon, sans méthode commune

La solution : UltraDiagPro.ps1

Un script PowerShell qui remplace entièrement l'analyse manuelle des journaux Windows — plus rapide, plus fiable, plus reproductible.

Automatisé

Exécution en une commande, sans intervention manuelle

Intelligent

Analyse basée sur une base de règles métier enrichie

Lisible

Génère un rapport .txt clair et directement exploitable

Fonctionnement global en 4 étapes

Analyse et corrélation

Application d'une base de règles.

Filtrage du bruit

Élimination des faux positifs.

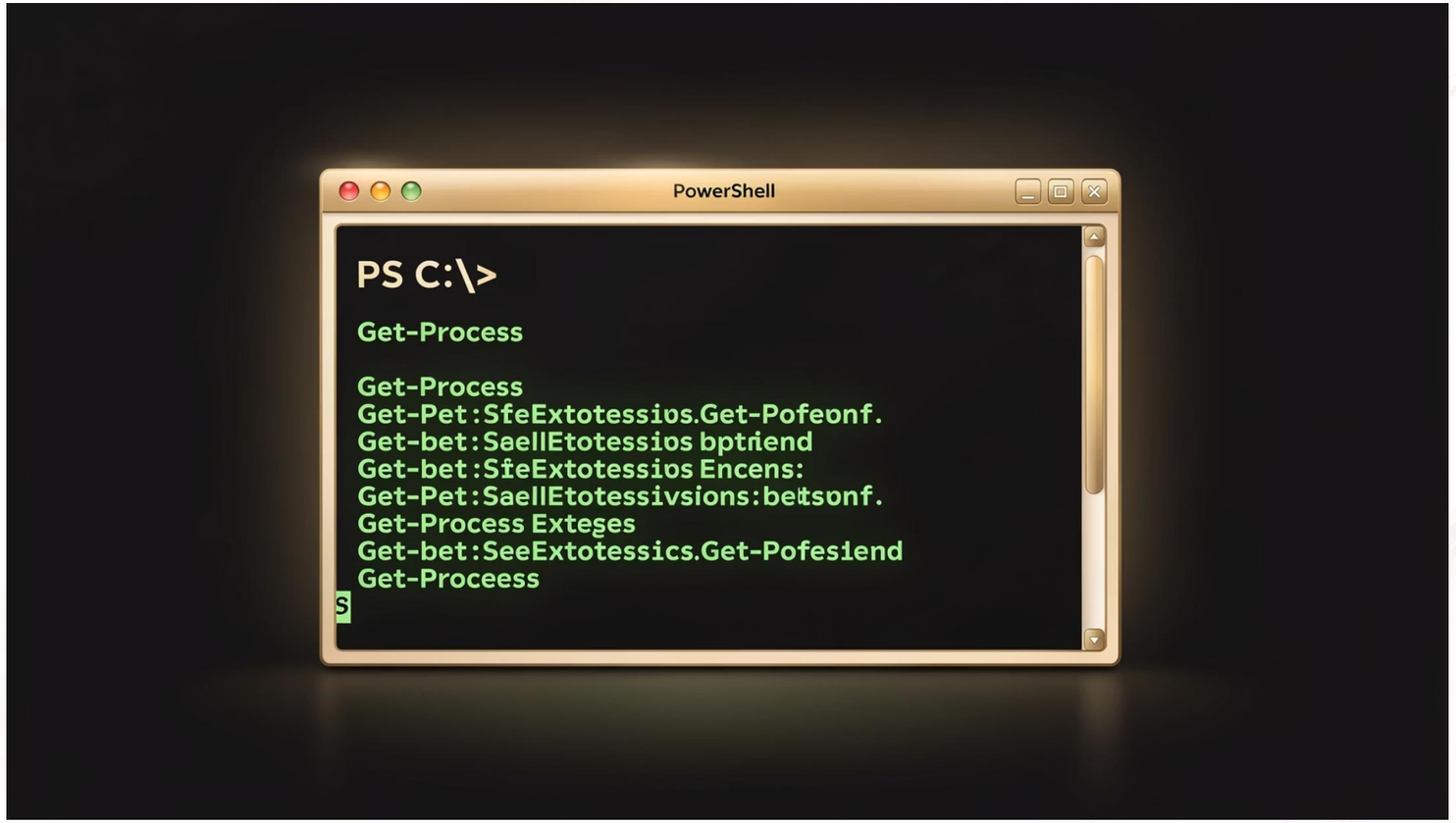
Collecte des données

Récupération via Get-WinEvent.

Génération du rapport

Exportation finale au format .txt.

Chaque étape est orchestrée automatiquement — de la collecte brute des événements jusqu'à la production d'un rapport structuré avec actions correctives.



ÉTAPE 1

Collecte des données

Le script exploite la cmdlet native `Get-WinEvent` pour interroger les journaux **System** et **Application** de Windows.

Fenêtre temporelle

Analyse configurable sur les dernières 24h ou 48h

Filtrage à la source

Seuls les événements de niveau **Erreur** et **Critique** sont extraits

Analyse et corrélation intelligente

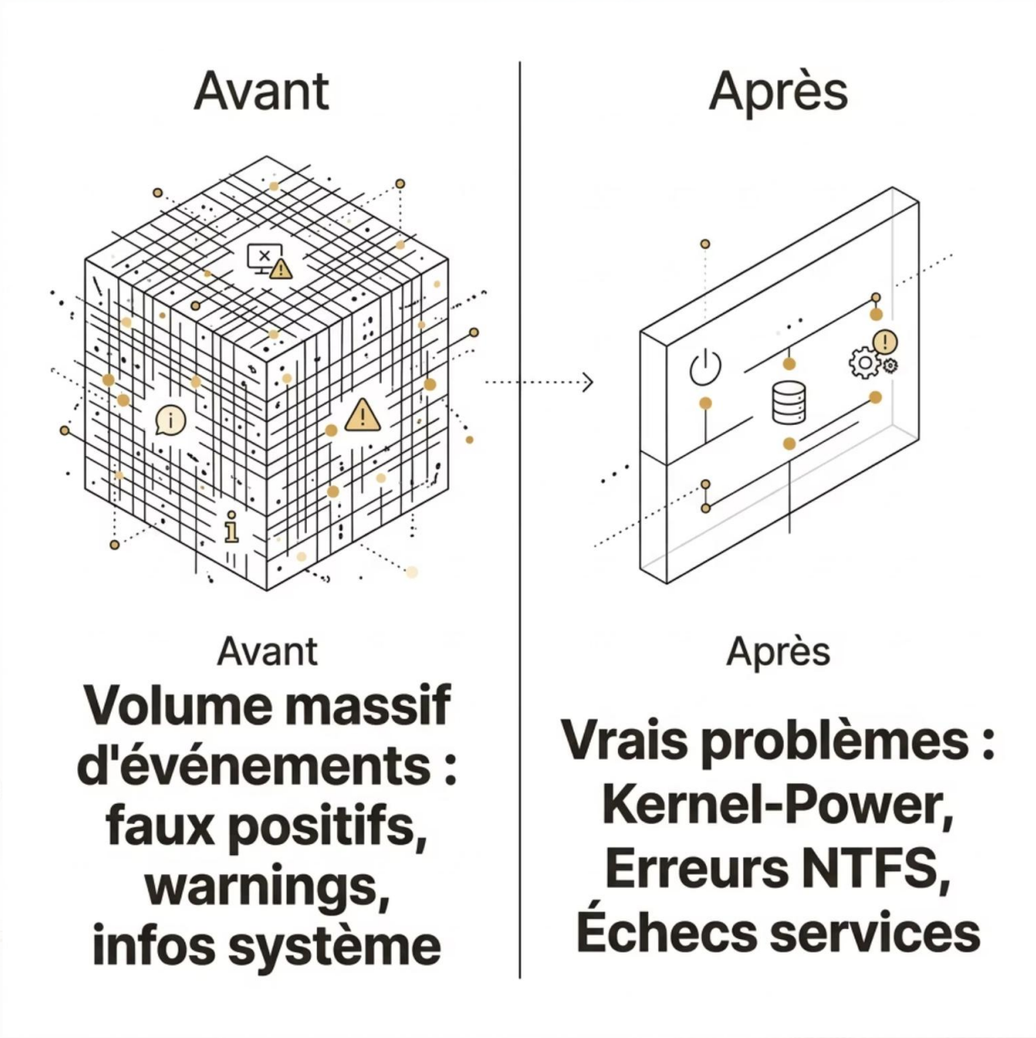
Le cœur du script repose sur une variable `$Rules` — une base de règles qui associe chaque événement à une catégorie métier.

Catégorie	Exemple d'événement	Impact
Crash système	Kernel-Power ID 41	Arrêt inopiné, BSOD
Erreurs disque	Erreurs NTFS / Disk	Corruption, perte de données
Services instables	Applications bloquées	Indisponibilité métier
Réseau défaillant	DNS / DHCP en échec	Perte de connectivité

Chaque règle transforme un événement brut en information exploitable par un technicien N1/N2, sans expertise approfondie requise.

Filtre anti-bruit

Windows génère naturellement de nombreux événements sans impact réel. Le script identifie et supprime ces faux positifs connus pour ne conserver que les alertes véritablement critiques.



Exemple typique

L'erreur `DCOM 10016` apparaît des centaines de fois dans les journaux — elle est bénigne et systématiquement filtrée.

Résultat

Le technicien ne voit que les événements qui méritent une intervention, réduisant le volume à analyser de 80 à 95 %.

Rapport final généré automatiquement

Structure du fichier .txt

01

Statut global

Synthèse immédiate : ✅ OK ou 🔴 ALERTE

ĆČ

Problèmes détectés

Liste ordonnée par criticité avec identifiants d'événements

03

Actions recommandées

Préconisations concrètes associées à chaque problème identifié

Caractéristiques du rapport

Lisible par tous

Format texte simple, sans outil spécifique nécessaire

Archivable

Horodaté automatiquement pour traçabilité et historisation

Transmissible

Peut être joint à un ticket ITSM ou partagé par email

Exemples d'actions recommandées

Selon les problèmes détectés, le script propose des actions correctives directement actionnables par le technicien.

Vérification disque

Lancer `chkdsk /f` et vérifier l'état S.M.A.R.T. du disque dur

Mise à jour drivers

Identifier et mettre à jour les pilotes obsolètes ou corrompus

Correction réseau

Diagnostiquer DNS, renouveler le bail DHCP ou réinitialiser la pile TCP/IP

Démarrage rapide

Désactiver le démarrage rapide Windows pour résoudre les problèmes de réveil

Avant / Après : l'impact concret

❌ Avant UltraDiagPro

Analyse manuelle fastidieuse

10 000+ lignes de logs à parcourir à la main

Temps de diagnostic élevé

15 à 20 minutes minimum par machine analysée

Risque d'erreur humaine

Événements critiques facilement manqués dans la masse

Non reproductible

Méthode variable selon le technicien, résultats inconsistants

✅ Après UltraDiagPro

Diagnostic automatisé

Exécution en une commande, résultats en moins de 2 minutes

Lecture immédiate

Rapport synthétique avec statut global et actions prêtes

Fiabilité renforcée

Aucune erreur d'omission, règles appliquées de façon systématique

Méthode unifiée

Même niveau d'analyse pour tous les techniciens de l'équipe

Apport métier pour les équipes support

~15 min

Économisées

Par diagnostic, en moyenne, libérées pour d'autres tickets

100%

Standardisé

Même procédure appliquée par tous, N1 comme N2

-95%

Bruit réduit

Des faux positifs filtrés avant présentation au technicien

La standardisation du diagnostic améliore non seulement la vitesse de résolution, mais aussi la qualité perçue du support par les utilisateurs finaux.

Conclusion et perspectives

Bénéfices immédiats

Automatisation intelligente

Fini l'analyse manuelle — le script pense à votre place

Fiabilité accrue

Règles systématiques, zéro oubli, résultats reproductibles

Gain de productivité

Jusqu'à 15 minutes récupérées par intervention

Évolutions envisagées

Export HTML / Dashboard

Rapport visuel interactif consultable dans un navigateur

Intégration ITSM (GLPI)

Création automatique de tickets enrichis depuis le rapport

Déploiement à grande échelle

Exécution distante via GPO ou outil de gestion de parc

En résumé

> « Face au temps perdu à analyser manuellement les journaux Windows, j'ai développé un script PowerShell qui automatise la collecte, filtre les faux positifs et corrèle les erreurs via une base de règles. Le résultat : un rapport clair avec des actions concrètes — pour diagnostiquer plus vite, mieux, et de façon identique à chaque intervention. »

ULTRADIAGPRO.PS1 POWERSHELL DIAGNOSTIC WINDOWS SUPPORT N1/N2