

TIP 1.9

Diagnostiquer un problème Windows ou applicatif

Fiche de révision - Support utilisateur

1. Méthode générale

Un incident Windows ou applicatif doit être traité méthodiquement : préciser le symptôme, déterminer l'étendue, rechercher les changements récents, formuler des hypothèses, tester, corriger, valider puis documenter.

À retenir :

Symptôme → Étendue → Contexte → Hypothèses → Tests → Correction → Validation → Documentation

2. Déterminer l'étendue

Observation	Piste principale
Une seule application	Application, version, dépendance, service ou configuration.
Plusieurs applications	Windows, ressources système, stockage ou services.
Un seul utilisateur	Profil, paramètres ou droits.
Plusieurs utilisateurs	Application commune, serveur ou infrastructure.

3. Rechercher les changements récents

Une mise à jour Windows ou applicative, une installation, une désinstallation, un changement de mot de passe, une modification de droits ou une nouvelle GPO peuvent fournir une piste. Un changement récent n'est cependant pas une preuve.

4. Outils de diagnostic Windows

Outil / commande	Utilité
Ctrl + Maj + Échap	Ouvrir le Gestionnaire des tâches.
Get-Process	Afficher les processus en cours.
services.msc / Get-Service	Contrôler les services Windows.
eventvwr.msc	Consulter les journaux système et applicatifs.
Get-Volume	Vérifier les volumes et l'espace disponible.
winver	Afficher l'édition et la version de Windows.

5. Profil utilisateur et droits

Si le problème n'existe que pour un utilisateur, tester un autre compte sur le même poste peut aider à isoler un profil endommagé, un paramètre personnel ou un problème de droits. Ne jamais attribuer des droits administrateur simplement pour contourner une erreur d'accès.

6. Réparer sans sur-réagir

La réparation ou la réinstallation d'une application peut être utile, mais seulement après diagnostic. Avant toute réinstallation, vérifier les données, paramètres, licences, dépendances et version à réinstaller.

7. SFC et DISM

Ces outils sont utiles lorsque l'intégrité des composants Windows est réellement suspectée. Ils ne doivent pas être lancés automatiquement pour tout incident.

Commande	Rôle
sfc /scannow	Vérifie certains fichiers système protégés et tente de réparer ceux qui sont endommagés.
DISM /Online /Cleanup-Image /RestoreHealth	Peut réparer l'image Windows utilisée notamment par SFC.

8. Redémarrer : utile mais insuffisant

Un redémarrage peut débloquent un processus, un service ou une mise à jour en attente. Si l'incident revient, il faut poursuivre le diagnostic au lieu de considérer le redémarrage comme la résolution définitive.

9. Exemple de diagnostic

Étape	GestionClients se ferme au lancement
Étendue	Autres utilisateurs fonctionnels : incident probablement local.
Contexte	Mise à jour de l'application la veille.
Tests	Gestionnaire des tâches, journaux, services, autre utilisateur sur le poste.
Hypothèse	Profil, paramètres locaux ou installation sur ce poste.
Validation	Relancer l'application et reproduire l'opération initialement en échec.

10. Quand escalader ?

Escalader si l'incident concerne une application ou un serveur géré par une autre équipe, une modification de GPO, des droits hors périmètre, un problème de sécurité, plusieurs utilisateurs ou un diagnostic devenu trop complexe.

11. Erreurs à éviter

Erreur	Bonne pratique
Réinstaller immédiatement	Diagnostiquer avant de corriger.
Ignorer les journaux	Rechercher les événements à l'heure de l'incident.
Donner les droits admin	Identifier et corriger le problème de permissions.
Lancer SFC/DISM systématiquement	Utiliser les outils selon une hypothèse.
Clôturer après un redémarrage	Reproduire et valider le fonctionnement réel.

12. À retenir

Un bon diagnostic Windows/applicatif distingue le symptôme de la cause. Vérifier l'étendue, les changements récents, les ressources, les services, les journaux, les profils et les droits avant d'appliquer une correction. Toujours valider avec l'utilisateur et documenter l'intervention.