

SITUATION PROFESSIONNELLE N°3

GESTION DES INCIDENTS
D'AUTHENTIFICATION UTILISATEUR :

COMPTE UTILISATEUR VERROUILLÉ /
MOT DE PASSE EXPIRÉ

SOMMAIRE



1

Contexte professionnel et enjeux d'authentification

2

Signalement de l'incident aux techniciens

3

Prise en charge et qualification de la demande

4

Diagnostic de l'incident d'authentification

4.1

Test et validation avec l'utilisateur

4.2

Compétences BTS SIO mobilisées

5

Intervention technique et résolution

5.1

Déverrouillage du compte utilisateur

5.2

Réinitialisation du mot de passe

6

Validation de l'intervention avec l'utilisateur

7

Clôture de l'incident et traçabilité

8

Compétences professionnelles mobilisées

1. Contexte professionnel et enjeux d'authentification

Dans le cadre de mon activité au sein du service informatique du Puy du Fou, je suis régulièrement sollicité pour des problèmes liés à l'authentification des utilisateurs.

Dans cette situation, l'utilisateur me contacte par téléphone afin de m'indiquer que son compte est verrouillé et qu'il ne peut plus accéder à sa session de travail.

Étant dans l'impossibilité de se connecter à son poste, l'utilisateur ne peut pas créer de ticket par ses propres moyens.

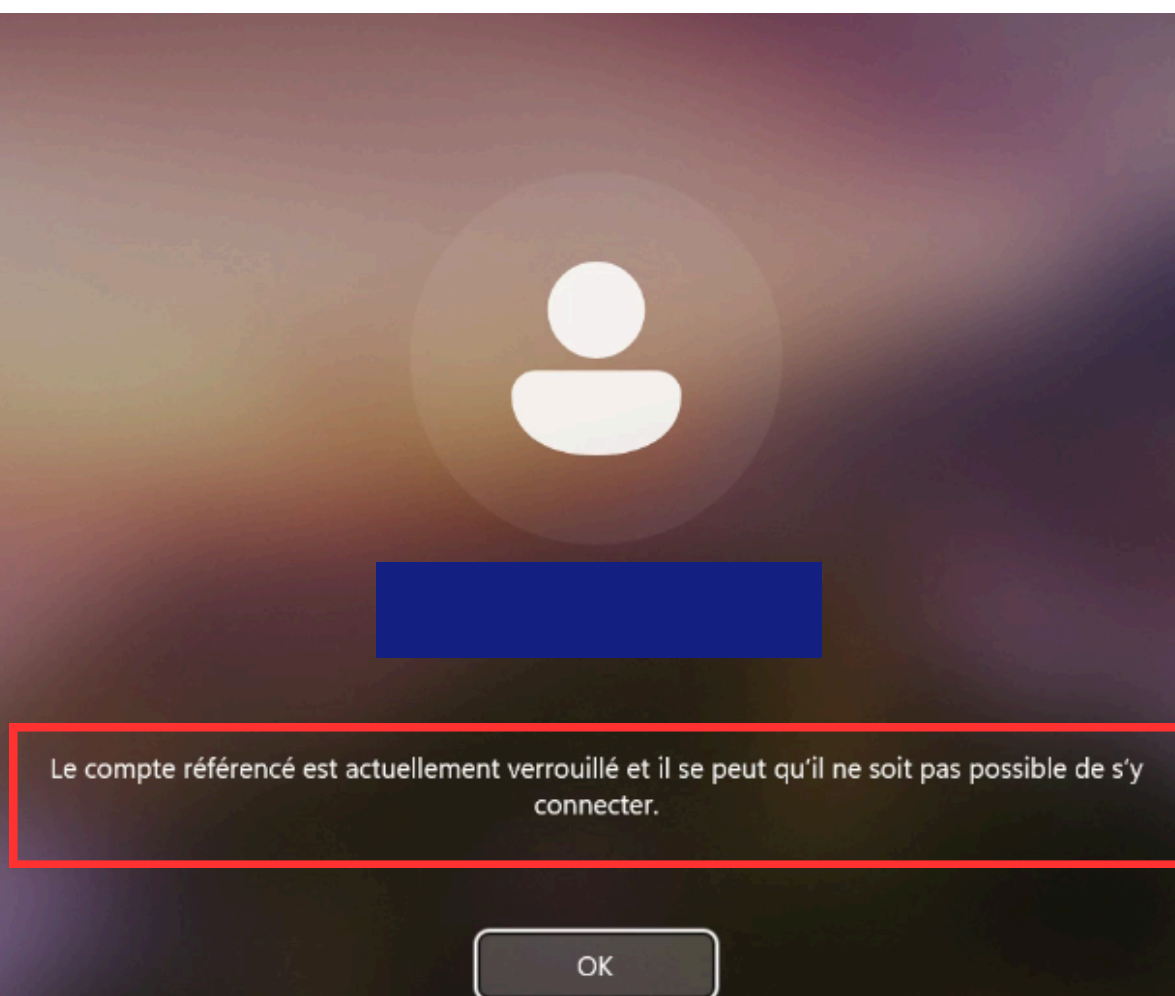
Je lui demande alors de se déplacer directement au bureau du service informatique afin que je puisse intervenir rapidement.

2. Signalement de l'incident aux techniciens

L'utilisateur se présente au bureau du service informatique et m'explique la situation rencontrée lors de la tentative de connexion à sa session.

Le message affiché indique que le compte utilisateur est verrouillé, suite à plusieurs tentatives de connexion infructueuses.

Cet incident empêche totalement l'utilisateur de travailler, ce qui nécessite une prise en charge immédiate.

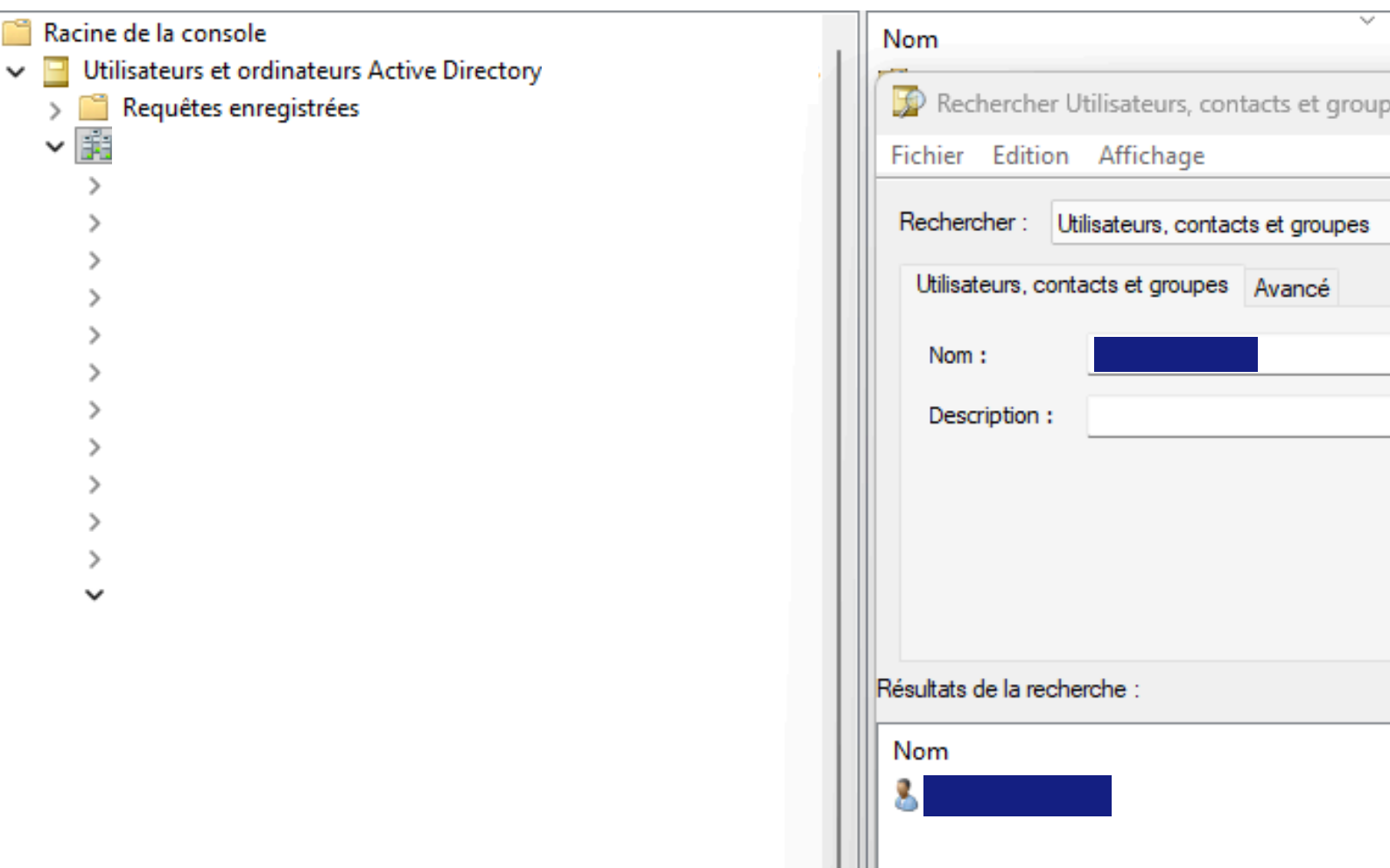


3. Prise en charge et qualification de la demande

Après avoir recueilli les informations nécessaires (nom de l'utilisateur, poste concerné), je qualifie l'incident comme un problème d'authentification lié au compte Active Directory.

L'incident étant clairement identifié, je procède à la vérification de l'état du compte utilisateur dans Active Directory afin de confirmer le diagnostic.

Je me dirige donc dans l'AD et entre son nom d'utilisateur dans le domaine

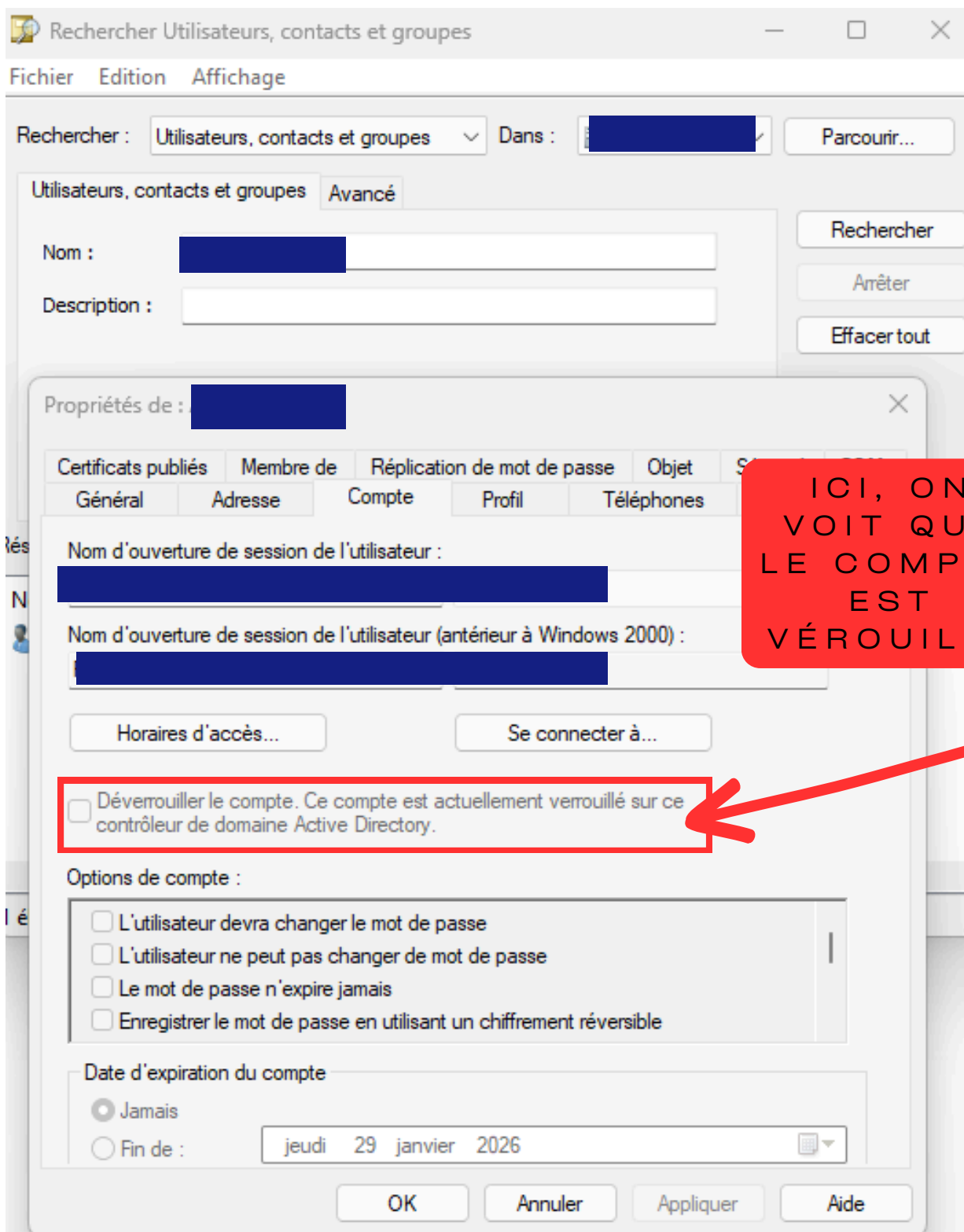


4. Diagnostic de l'incident d'authentification

4.1 Compte utilisateur verrouillé

À l'aide de l'outil Utilisateurs et ordinateurs Active Directory, je constate que le compte utilisateur est effectivement verrouillé, conformément à la politique de sécurité du domaine. On se rends alors sur :

Propriété → Compte



4. Diagnostic de l'incident d'authentification

Mais ce que l'on peut également regarder dans ce cas là , c'est la date d'expiration du compte, ici elle est en "Jamais", et on sait que l'utilisateur s'est plusieurs fois trompé de mot de passe

Propriétés de : [redacted]

Certificats publiés | Membre de | Réplication de mot de passe | Objet | Sécurité | COM+
Général | Adresse | **Compte** | Profil | Téléphones | Organisation

Nom d'ouverture de session de l'utilisateur :
[redacted]

Nom d'ouverture de session de l'utilisateur (antérieur à Windows 2000) :
[redacted]

[Horaires d'accès...](#) [Se connecter à...](#)

☐ Déverrouiller le compte. Ce compte est actuellement verrouillé sur ce contrôleur de domaine Active Directory.

Options de compte :

- ☐ L'utilisateur devra changer le mot de passe
- ☐ L'utilisateur ne peut pas changer de mot de passe
- ☐ Le mot de passe n'expire jamais
- ☐ Enregistrer le mot de passe en utilisant un chiffrement réversible

Date d'expiration du compte

☒ Jamais

☐ Fin de : jeudi 29 janvier 2026

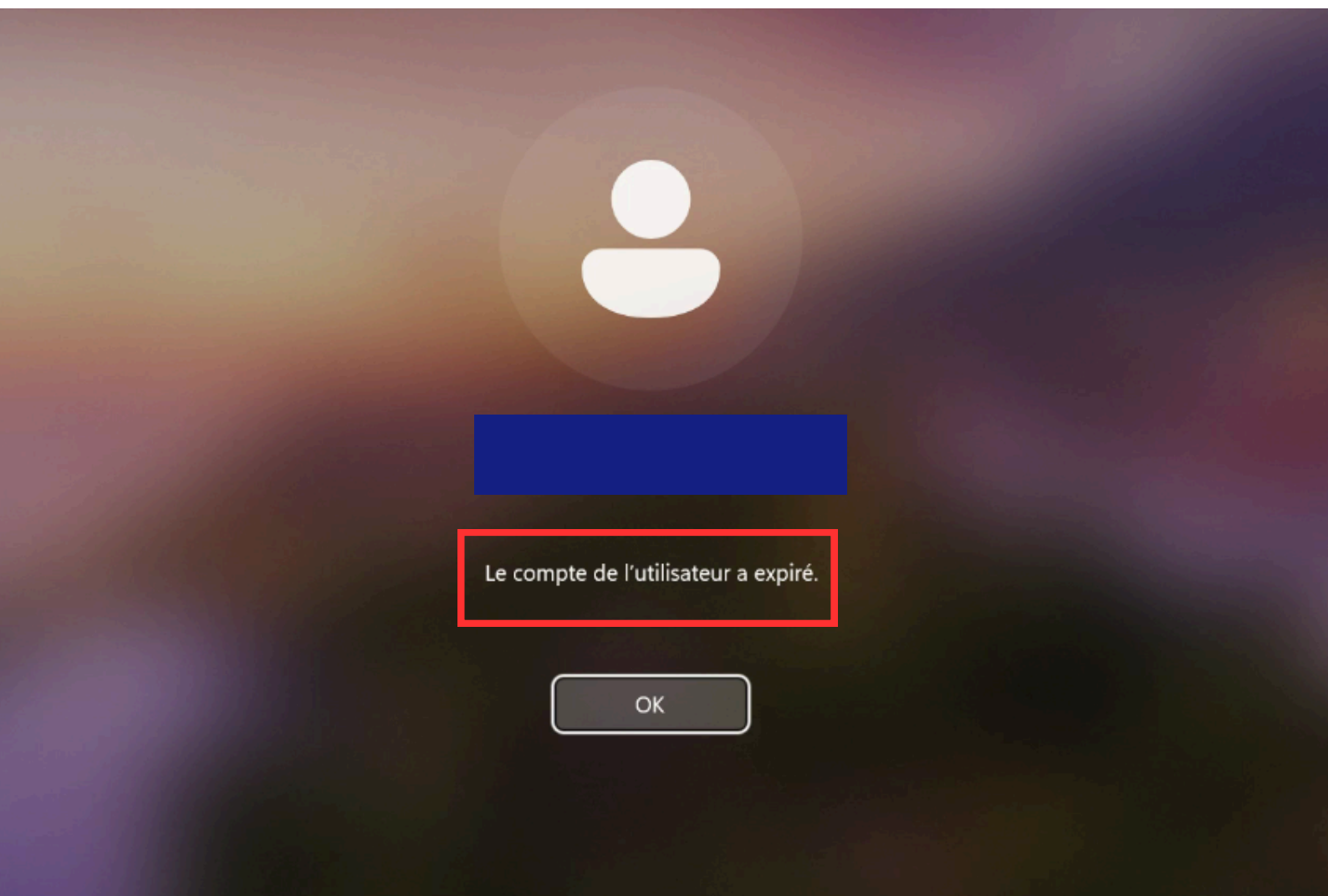
[OK](#) [Annuler](#) [Appliquer](#) [Aide](#)

4. Diagnostic de l'incident d'authentification

4.2 Mot de passe utilisateur expiré (cas similaire)

Dans une situation similaire, le message affiché lors de la connexion peut indiquer que le mot de passe de l'utilisateur a expiré.

Dans ce cas, l'utilisateur ne peut pas non plus accéder à sa session et se présente directement au service informatique afin de signaler le problème.



5. Intervention technique et résolution

5.1 Déverrouillage du compte utilisateur

Après confirmation du verrouillage, je procède au déverrouillage du compte utilisateur via Active Directory.

Une fois l'action effectuée, l'utilisateur est invité à se reconnecter afin de vérifier le rétablissement de l'accès.

Propriétés de : [redacted] ✕

Certificats publiés	Membre de	Réplication de mot de passe	Objet	Sécurité	COM+
Général	Adresse	Compte	Profil	Téléphones	Organisation

Nom d'ouverture de session de l'utilisateur :

[redacted]

[redacted] ▾

Nom d'ouverture de session de l'utilisateur (antérieur à Windows 2000) :

[redacted]

[redacted]

Horaires d'accès...

Se connecter à...

☒ Déverrouiller le compte. Ce compte est actuellement verrouillé sur ce contrôleur de domaine Active Directory.

Options de compte :

☐ L'utilisateur devra changer le mot de passe

☐ L'utilisateur ne peut pas changer de mot de passe

☐ Le mot de passe n'expire jamais

☐ Enregistrer le mot de passe en utilisant un chiffrement réversible

Date d'expiration du compte

☒ Jamais

☐ Fin de :

jeudi 29 janvier 2026 📅 ▾

OK

Annuler

Appliquer

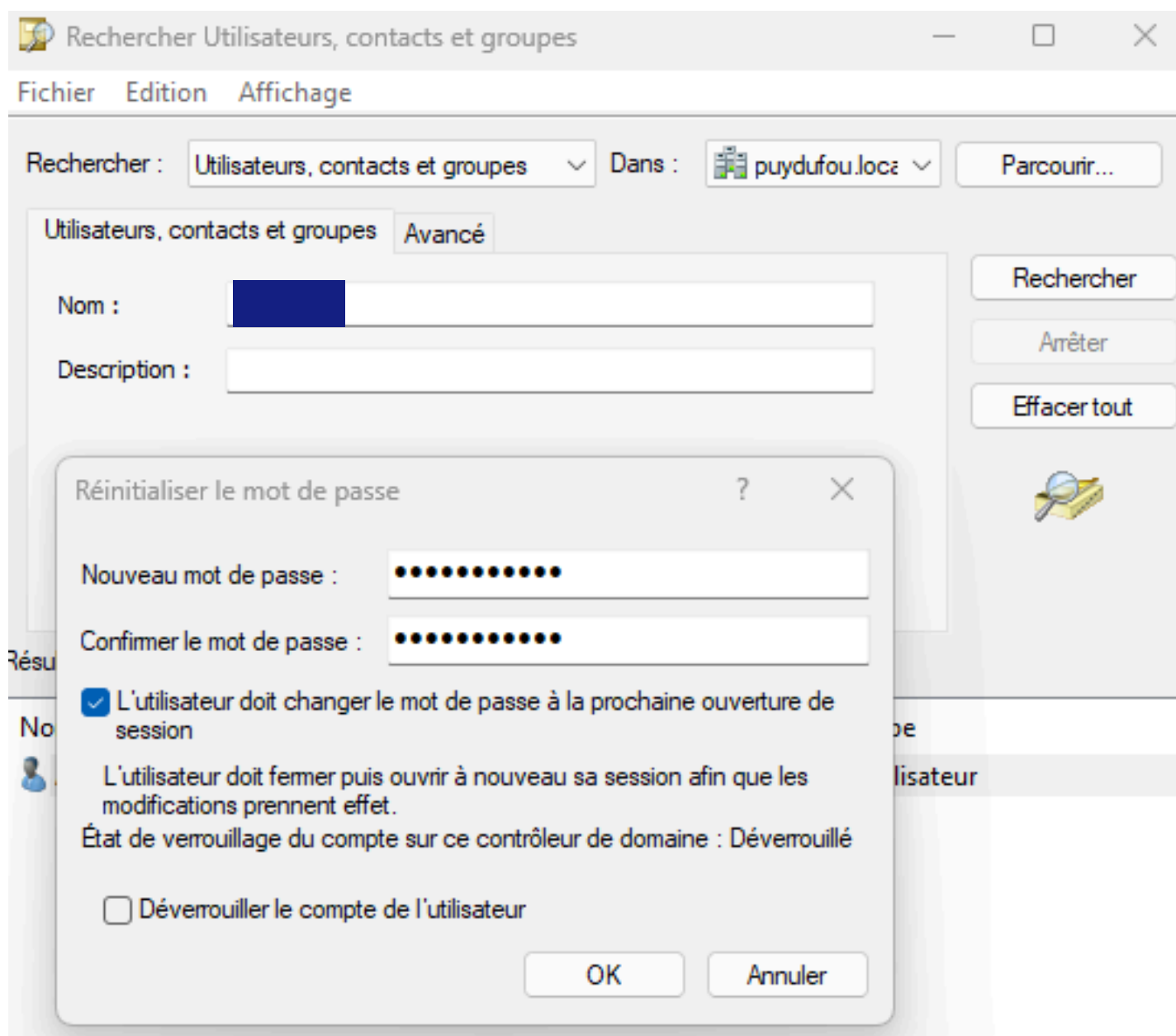
Aide

5. Intervention technique et résolution

5.2 Réinitialisation du mot de passe

Dans le cas d'un mot de passe expiré, je procède à la réinitialisation du mot de passe utilisateur via Active Directory.

Je fournis ensuite un mot de passe temporaire à l'utilisateur et lui demande de le modifier lors de la prochaine ouverture de session, conformément aux règles de sécurité.

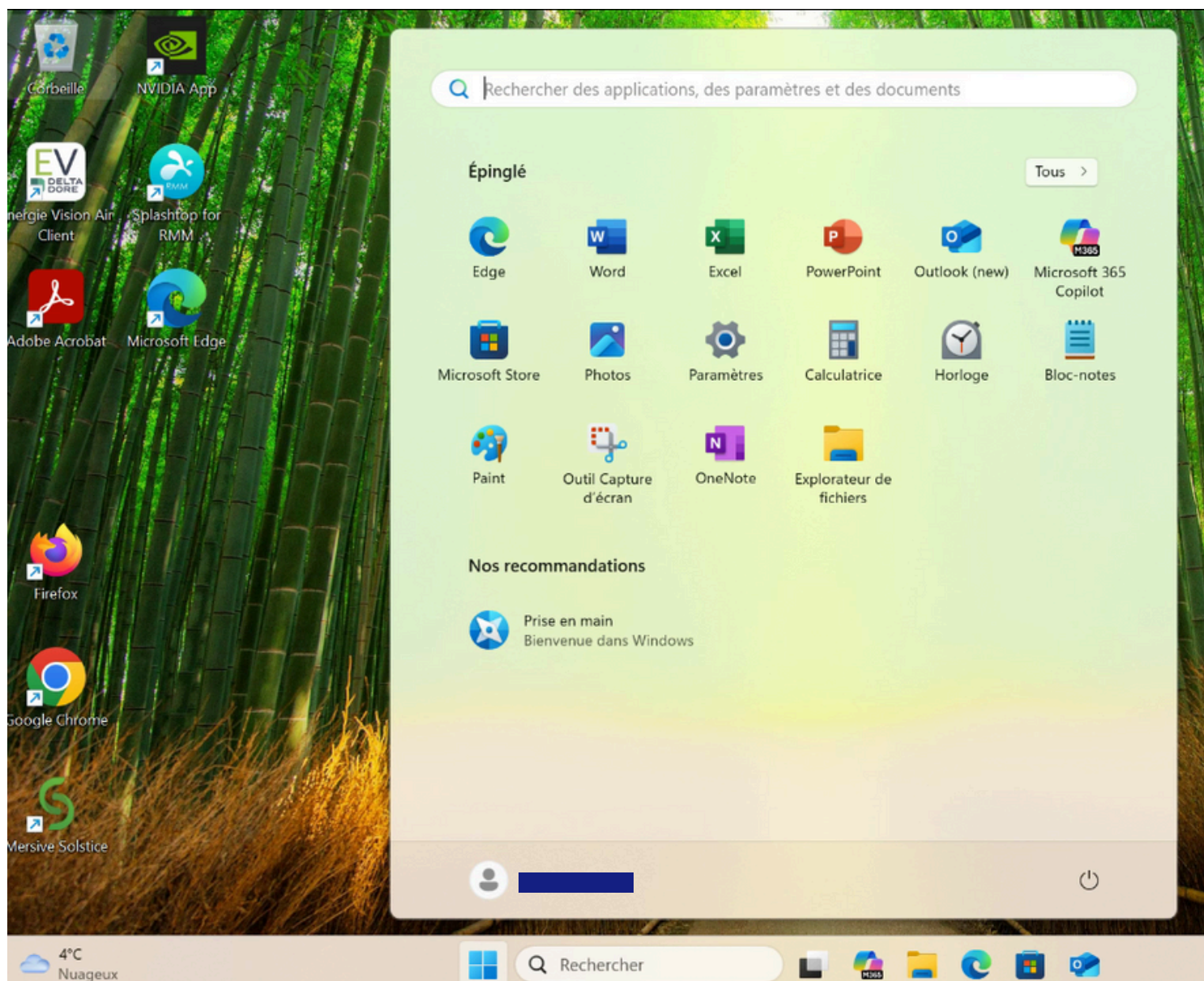


6. Validation de l'intervention avec l'utilisateur

Une fois l'intervention réalisée, je demande à l'utilisateur de tester l'ouverture de sa session directement depuis son poste.

- Dans le cas du compte verrouillé, l'utilisateur parvient à se connecter normalement après le déverrouillage.
- Dans le cas du mot de passe expiré, l'utilisateur se connecte avec le mot de passe temporaire et est invité à définir un nouveau mot de passe personnel.

L'utilisateur confirme que l'accès à sa session est rétabli et qu'il peut reprendre son activité normalement.



7. Clôture de l'incident et traçabilité

Une fois le problème résolu et validé avec l'utilisateur, l'incident est considéré comme clôturé.

Pour assurer la traçabilité de l'intervention, un ticket est créé ou complété dans l'outil Atera par le service informatique, indiquant :

- la nature de l'incident (compte verrouillé ou mot de passe expiré),
- la cause identifiée,
- l'action réalisée (déverrouillage ou réinitialisation),
- la validation par l'utilisateur.

Cette traçabilité permet de :

- conserver un historique des interventions,
- faciliter le suivi en cas de problème récurrent,
- assurer une organisation efficace du support informatique.

← #5414 | [REGUL] Compte verrouillé

Créé il y a un mois • Modifié il y a un mois

Statut

Assigner un technicien

Groupe assigné

Statut d'activité

SLA suspendu...

Résolu ▾

EG ▾

DSI - Support ▾

● Lu ▾

PL

Réponse publique

Note interne

✦ Générer une réponse

 ou saisissez votre message ici

📎 Joindre des fichiers

Sélectionner un modèle de réponse rapide ▾

Conversation (2)

Activité du ticket (14)

Résolution (1)

☰ Trier par : Le plus récent ▾

✦ Générer l'article

EG Nov 25, 2025, 9:25 AM

Compte déverrouillé OK

EG Nov 25, 2025, 9:24 AM ▾

Appel le 25/11 09:18 de : compte verrouillé

8. Compétences professionnelles mobilisées

Cette situation professionnelle mobilise les compétences suivantes :

- Gestion des identités et des accès
- Intervention sur des comptes utilisateurs Active Directory.
- Sécurité des systèmes d'information
- Application des politiques de verrouillage et d'expiration des mots de passe.
- Support et assistance aux utilisateurs
- Prise en charge directe de l'utilisateur et rétablissement rapide de l'accès.
- Organisation et suivi des incidents
- Traçabilité des interventions via un outil de ticketing.
- Communication professionnelle
- Échange clair avec l'utilisateur pour expliquer la cause du problème et la solution apportée.

