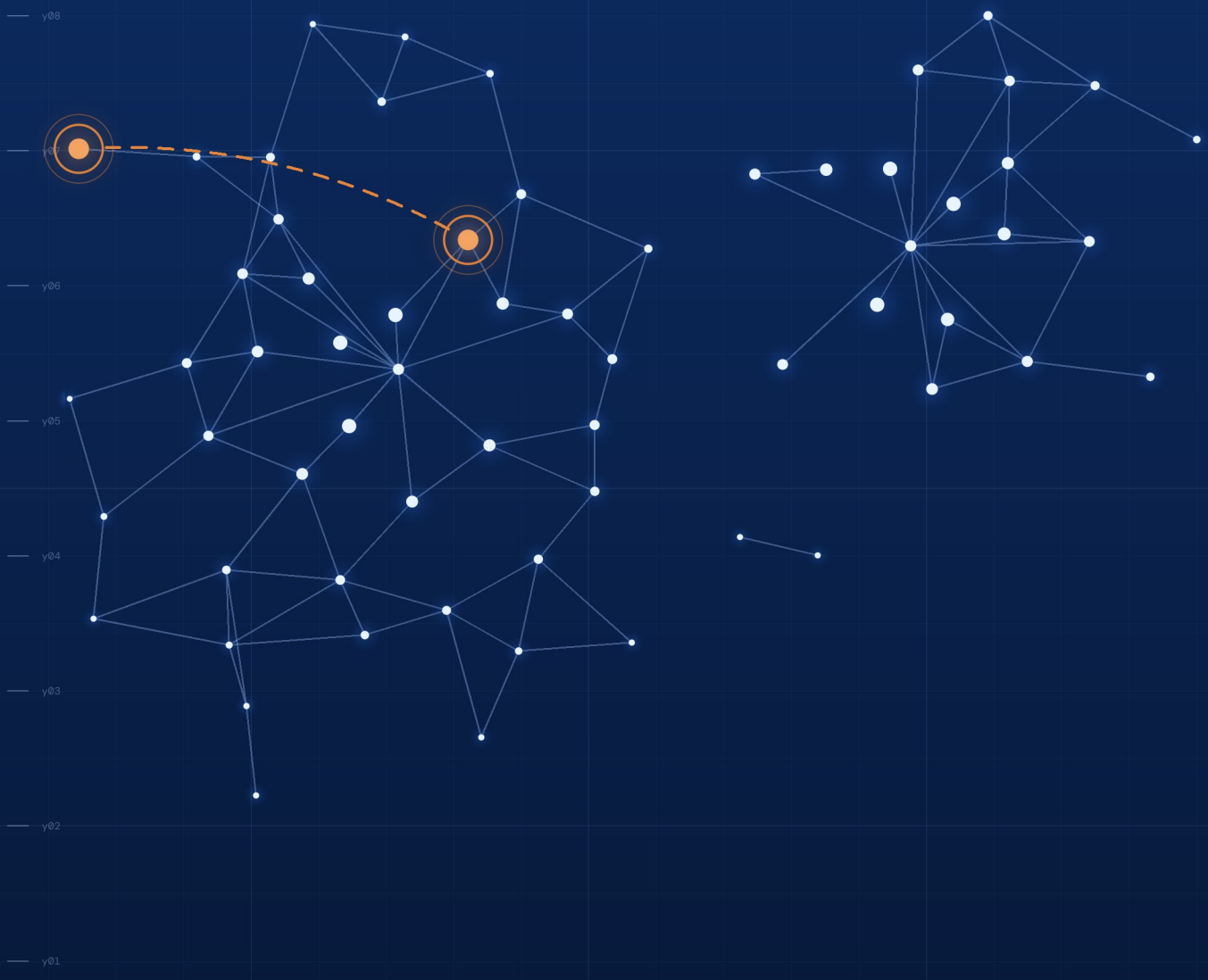


CATÉGORIE GLPI · JP CONSULTING

Playbook Comptes et accès

Les runbooks de la catégorie GLPI Comptes et accès

Jean-Philippe Rebischung

Sommaire

Ce playbook regroupe les runbooks de la catégorie GLPI **Comptes et accès**. Un runbook par sous-catégorie ; chaque runbook décrit, cas par cas, la conduite à tenir pour un incident ou une demande.

Arrivée et départ **3**

Demande · Préparer le compte d'un nouvel arrivant 4

Demande · Fermer le compte d'un salarié qui quitte l'entreprise 7

Droits d'accès **11**

Demande · Un utilisateur ne peut pas enregistrer dans le partage Commun 12

Incident · Un dossier du partage a disparu pour un utilisateur 15

Mot de passe et verrouillage **19**

Incident · Un utilisateur ne peut plus se connecter, son compte est bloqué 20

Incident · Le mot de passe ne fonctionne plus, il a expiré 24

Incident · Le compte se verrouille de nouveau après avoir été débloqué 27

Index par symptôme

Ce que je reçois	Runbook	Page
Un responsable : « un nouveau collègue arrive lundi, il lui faut un compte »	Arrivée et départ	4
Un responsable : « tel salarié part vendredi, merci de fermer son compte »	Arrivée et départ	7
Un utilisateur : « accès refusé quand j'enregistre dans le dossier Commun »	Droits d'accès	12
Un utilisateur : « un dossier a disparu de P:, ma collègue le voit encore »	Droits d'accès	15
Un utilisateur : « je n'arrive plus à me connecter, mon compte est bloqué »	Mot de passe et verrouillage	20
Un utilisateur : « mon mot de passe ne marche plus depuis ce matin »	Mot de passe et verrouillage	24
Un utilisateur : « vous m'avez débloqué, et je suis de nouveau bloqué »	Mot de passe et verrouillage	27

Les champs à remplacer

Dans les commandes et les messages, un texte entre chevrons, comme `<N°_TICKET>` ou `<NOM_DU_DOSSIER>`, est **à remplacer par la valeur de ton cas, chevrons compris**. Exemple : `E:\Restauration-<N°_TICKET>` devient `E:\Restauration-21`.

Avant de valider une commande, relis-la : s'il reste un chevron, elle n'est pas prête.

RUNBOOK · PLAYBOOK COMPTES ET ACCÈS

Arrivée et départ

La création et la fermeture des comptes : nouvel arrivant, départ d'un salarié.

Cas traités dans ce runbook

DEMANDE Préparer le compte d'un nouvel arrivant.....4

DEMANDE Fermer le compte d'un salarié qui quitte l'entreprise.....7

Statut : non validé

Préparer le compte d'un nouvel arrivant

Niveau	N2. Règle de nommage ou droits particuliers : décision du N3 et du responsable des données.
Où	**`SRV-DC01`** (le contrôleur de domaine), compte **`JPCONSULTING\admin.domaine`**, PowerShell ouvert **en administrateur**. Sur ce lab, le technicien N2 ne peut pas se connecter au contrôleur de domaine : on utilise un compte administrateur.
GLPI	type Demande · catégorie : Comptes et accès › Arrivée et départ. *Statut : non validé*

Ce que tu reçois et ce qu'on attend de toi

Un nouveau salarié arrive : il lui faut un **compte** dans l'annuaire, placé dans l'**UO*** de son service et membre du **groupe global** de ce service. Tout le reste en découle : lecteurs réseau, imprimante, accès à GLPI.

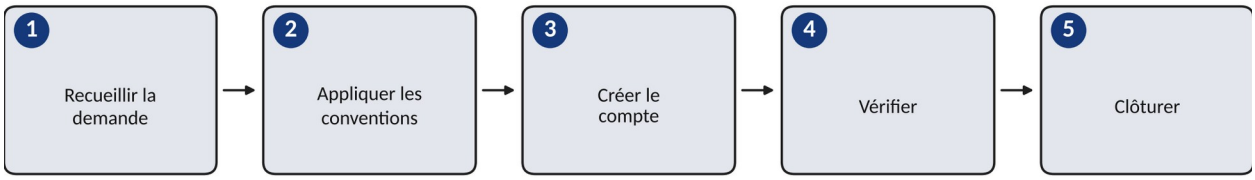
Ton travail : recueillir les bonnes informations, créer le compte selon les conventions du lab, vérifier qu'il fonctionne, et remettre le premier mot de passe de façon sûre.

Ce que tu reçois, par exemple, de la part d'un responsable : « Un nouveau commercial arrive lundi, pouvez-vous lui préparer un compte ? »

Regle d'or

Un compte se crée sur **demande d'un responsable**, jamais sur la seule demande de l'intéressé.

Les droits se donnent par les **groupes** (modèle AGDLP*), jamais en ajoutant un utilisateur directement sur un dossier.



Les étapes de ce cas.

1 Recueillir la demande

- Prénom et nom, service, date d'arrivée.
- Poste de travail prévu (existant ou à préparer : voir le playbook Poste de travail, runbook Nouveau poste).
- Accès particuliers au-delà de ceux du service (un dossier, une application) : à faire valider par le responsable des données concernées.
- Qui remet le premier mot de passe à l'arrivant, et quand ?

Ticket : type **Demande**, catégorie **Comptes et accès › Arrivée et départ**, demandeur = le responsable qui a fait la demande.

2 Appliquer les conventions

Convention du lab	Valeur
Nom de connexion	la forme prenom.nom (ex. alex.terieur). Si ce nom existe déjà : ne pas improviser, faire décider la règle (N3)
UO du compte	celle du service, sous **`JP Consulting`** : **`ADMINISTRATION`**, **`COMMERCIAL`**, **`DIRECTION`**, **`INFORMATIQUE`**, **`PRODUCTION`**
Groupe métier	le **`GG_`** du service : **`GG_Administration`**, **`GG_Commercial`**, **`GG_Direction`**, **`GG_Informatique`**, **`GG_Production`**
Premier mot de passe	provisoire, avec **changement obligatoire** à la première ouverture de session

Vérifie que le nom n'est pas déjà pris :

Machine : SRV-DC01 | **Compte :** JPCONSULTING\admin.domaine | **Outil :** PowerShell (administrateur)

```
Get-ADUser -Filter "SamAccountName -eq '<PRÉNOM>'"
```

Je dois voir

Aucune ligne : le nom est libre. Une ligne : le nom existe déjà ; stop, fais décider la règle de nommage.

3 Créer le compte

Console **Utilisateurs et ordinateurs Active Directory** : développe **`JP Consulting`**, clic droit sur l'UO du service → **Nouveau** → **Utilisateur**. Prénom, nom, nom d'ouverture de session (prenom.nom). Page suivante : mot de passe provisoire, case **L'utilisateur doit changer le mot de passe à la prochaine ouverture de session** cochée. Terminer.

Puis double-clic sur le nouveau compte, onglet **Membre de** → **Ajouter...** → le **`GG_`** du service → **OK**.

Pourquoi

Le compte reçoit tout le reste **automatiquement** : la GPO *Utilisateurs - Mappage lecteurs* lui donne **`P:`** (Commun) parce qu'il est dans **`JP Consulting`** ; la GPO *Utilisateurs - Imprimantes* lui donne l'imprimante **`IMP-Commun`**. Dans GLPI, le compte est créé **à sa première connexion**, parce qu'il est dans la branche lue par GLPI (**`OU=JP Consulting`**).

4 Vérifier

Machine : SRV-DC01 | **Compte :** JPCONSULTING\admin.domaine | **Outil :** PowerShell (administrateur)

```
Get-ADUser <PRÉNOM> -Properties Enabled, DistinguishedName, MemberOf | Select-Object
Name, Enabled, DistinguishedName, MemberOf
```

Je dois voir

`Enabled : True`, **`DistinguishedName`** dans l'UO du service (**`OU=<SERVICE>,OU=JP Consulting,…`**), **`MemberOf`** contient le **`GG_`** du service.

Le compte est dans **`CN=Users`** : il a été créé au mauvais endroit ; il ne recevra ni les GPO ni l'accès à GLPI. Déplace-le dans l'UO du service.

À la première connexion de l'arrivant sur son poste : il choisit son mot de passe, puis tu vérifies avec lui :

Machine : Le poste de l'arrivant | **Compte :** l'arrivant | **Outil :** Invite de commandes

```
net use
```

Je dois voir

Le lecteur **`P:`** (Commun) est connecté. L'arrivant ouvre GLPI avec son compte et voit l'interface simplifiée.

5 Clôturer

Attention

Le mot de passe provisoire ne figure **ni dans le ticket, ni dans un message GLPI**. Il se remet en main propre, à l'arrivant ou au responsable.

Texte de la tâche (GLPI)

Demande de <RESPONSABLE> du <DATE>. Compte **`<PRÉNOM>`** créé dans **`OU=<SERVICE>,OU=JP Consulting`**, membre de **`<GG_SERVICE>`**, changement de mot de passe obligatoire à la première ouverture. Vérifications : **`Get-ADUser`** (UO, groupe, activé), première session le <DATE> : **`P:`** connecté, GLPI ouvert.

Texte de la solution (GLPI), lisible par le demandeur

Bonjour <RESPONSABLE>,

Le compte de <PRÉNOM> <NOM> est prêt pour le <DATE>. Son identifiant est « <PRÉNOM> » ; le mot de passe provisoire vous est remis <COMMENT>, et il choisira le sien à la première connexion. Il aura accès au partage Commun et à l'imprimante du service.

Cordialement,

Fermer le compte d'un salarié qui quitte l'entreprise

Niveau	N2. Suppression définitive, UO des comptes désactivés : décision N3.
Où	**`SRV-DC01`** (le contrôleur de domaine), compte **`JPCONSULTING\admin.domaine`**, PowerShell ouvert **en administrateur**. Sur ce lab, le technicien N2 ne peut pas se connecter au contrôleur de domaine : on utilise un compte administrateur.
GLPI	type Demande · catégorie : Comptes et accès › Arrivée et départ. *Statut : non validé*

Ce que tu reçois et ce qu'on attend de toi

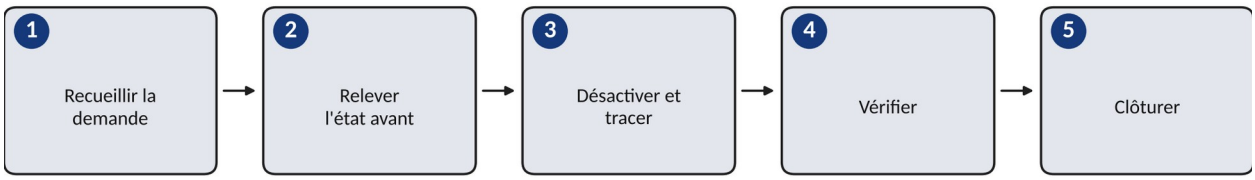
Un salarié quitte l'entreprise. Son compte doit cesser de fonctionner **à la date prévue**, sans perdre ce qui appartient à l'entreprise (fichiers, historique des tickets).

Ton travail : appliquer la demande du responsable, **désactiver** (et non supprimer) le compte, fermer ses accès, le tracer, et prouver que la connexion est refusée.

Ce que tu reçois, par exemple, de la part d'un responsable : « Otto Matique quitte la société vendredi soir, merci de fermer son compte. »

Regle d'or

On **désactive**, on ne supprime pas : un compte supprimé ne se récupère qu'avec la Corbeille AD, et son historique (tickets, droits) devient illisible. La suppression éventuelle vient plus tard, sur décision.



Les étapes de ce cas.

1 Recueillir la demande

- Qui demande ? (un responsable, jamais un collègue) Quel compte, quelle date et quelle heure de fin ?
- Que deviennent ses fichiers et son travail en cours ? À qui les transmettre ?
- A-t-il des accès particuliers (groupes, applications, matériel) à reprendre ?

Ticket : type **Demande**, catégorie **Comptes et accès › Arrivée et départ**, demandeur = le responsable. Si la date est à venir, planifie l'action : rien ne se fait avant.

2 Relever l'état avant

Machine : SRV-DC01 | **Compte :** JPCONSULTING\admin.domaine | **Outil :** PowerShell (administrateur)

```
Get-ADUser <PRÉNOM> -Properties Enabled, MemberOf, LastLogonDate, Description |
Select-Object Name, Enabled, MemberOf, LastLogonDate, Description
```

Je dois voir

Note dans le ticket l'état **avant** : activé, groupes (`MemberOf`), dernière connexion. C'est ce qui permettra de revenir en arrière en cas d'erreur.

3 Désactiver et tracer

Console **Utilisateurs et ordinateurs Active Directory** : clic droit sur le compte → **Désactiver le compte**. Puis double-clic → onglet **Général**, champ **Description** : « Désactivé le <DATE> — départ — ticket n° <N> ».

Attention

Dans le lab : il n'existe pas d'UO pour les comptes désactivés. Le compte reste dans l'UO de son service ; la création d'une telle UO est une décision du N3.

Sur ce lab, GLPI s'authentifie par l'annuaire : le compte désactivé ne peut plus s'y connecter, mais **ses tickets restent** dans GLPI. Ne supprime pas l'utilisateur dans GLPI.

Les retraits de groupes et le transfert des fichiers se font **seulement** si la demande le précise (décision du responsable).

4 Vérifier

Machine : SRV-DC01 | **Compte :** JPCONSULTING\admin.domaine | **Outil :** PowerShell (administrateur)

```
Get-ADUser <PRÉNOM> -Properties Enabled, Description | Select-Object Name, Enabled,
Description
```

Je dois voir

`Enabled : False` et la description renseignée. Puis la preuve par l'usage : une ouverture de session avec ce compte sur un poste est **refusée** (« Votre compte a été désactivé »).

Pourquoi

Une session déjà ouverte au moment de la désactivation peut continuer jusqu'à sa fermeture : si le départ est sensible, fais fermer les sessions (`quser`, `logoff`) au moment de la désactivation.

5 Clôturer

Texte de la tâche (GLPI)

Demande de <RESPONSABLE> du <DATE> : départ de <PRÉNOM> le <DATE> à <HEURE>. État avant : activé, groupes <LISTE>, dernière connexion <DATE>. Compte désactivé le <DATE> à <HEURE>, description renseignée. <RETRAITS / TRANSFERTS DEMANDÉS>. Vérification : Enabled False, ouverture de session refusée.

Texte de la solution (GLPI), lisible par le demandeur

Bonjour <RESPONSABLE>,

Le compte de <PRÉNOM> est désactivé depuis le <DATE> à <HEURE> : il ne permet plus de se connecter. Ses fichiers sont conservés <OÙ / TRANSMIS À QUI>. Le compte pourra être supprimé définitivement sur votre demande.

Cordialement,

Lexique

Les mots marqués d'un astérisque (*) dans ce runbook.

UO (unité d'organisation)

Dossier de l'annuaire qui range comptes et ordinateurs. Les GPO s'appliquent par UO : un compte mal rangé ne reçoit pas les bons réglages.

AGDLP

Méthode de gestion des droits : les comptes (**A**) vont dans des groupes globaux (**G**, `GG_`), qui vont dans des groupes de domaine local (**DL**, `DL_`), qui reçoivent les permissions (**P**).

Désactiver / supprimer

Un compte désactivé existe toujours mais refuse toute connexion ; il se réactive en un clic. Un compte supprimé disparaît (Corbeille AD seulement).

Corbeille Active Directory

Fonction qui permet de restaurer un objet supprimé de l'annuaire pendant un délai ; activée sur ce lab.

RUNBOOK · PLAYBOOK COMPTES ET ACCÈS

Droits d'accès

L'accès des utilisateurs aux dossiers partagés et aux ressources, donné par les groupes (AGDLP).

Cas traités dans ce runbook

DEMANDE Un utilisateur ne peut pas enregistrer dans le partage Commun…12

INCIDENT Un dossier du partage a disparu pour un utilisateur……15

Statut : non validé

Un utilisateur ne peut pas enregistrer dans le partage Commun

Niveau	N1 (constater, expliquer). Modification d'un groupe : N2, après décision du responsable des données.
Où	`SRV-DC01` (le contrôleur de domaine), compte `JPCONSULTING\admin.domaine`, PowerShell ouvert **en administrateur**. Sur ce lab, le technicien N2 ne peut pas se connecter au contrôleur de domaine : on utilise un compte administrateur.
GLPI	type Demande (ou Incident si le droit existait) · catégorie : Comptes et accès › Droits d'accès. *Statut : non validé*

Ce que tu reçois et ce qu'on attend de toi

Un utilisateur ne peut pas enregistrer dans un dossier partagé. Avant de parler de panne, il faut savoir **ce que ses droits prévoient**. Sur ce lab, tout le monde **lit** `Commun`, mais seules l'Administration et la Direction peuvent y **écrire** : un commercial refusé n'a pas de panne.

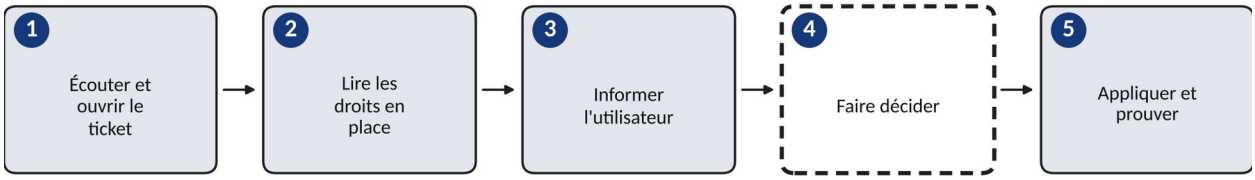
Ton travail : prouver le droit réellement en place, puis, si l'utilisateur a besoin d'autre chose, faire **décider** le responsable des données avant tout changement.

Ce que tu reçois, par exemple : « Je n'arrive pas à enregistrer mon devis dans le dossier Commun, j'ai un message d'accès refusé. »

Regle d'or

Un droit se donne sur **décision écrite** du responsable des données, jamais parce que l'utilisateur le demande.

On ajoute un **groupe** à un groupe, jamais un utilisateur directement sur un dossier.



Les étapes de ce cas. À l'étape 4, c'est le responsable des données qui décide.

1 Écouter et ouvrir le ticket

- Le message exact (« accès refusé », « espace insuffisant », autre) : chaque message désigne une barrière différente.
- Le chemin complet (lecteur `P:` ou chemin réseau) et le fichier.
- Pouvez-vous **ouvrir** les fichiers du dossier ? Lire et écrire sont deux droits distincts.
- Un collègue du même service est-il dans le même cas ?

Ticket : type **Demande** si l'utilisateur n'a jamais eu ce droit ; **Incident** s'il l'avait et l'a perdu. Catégorie **Comptes et accès › Droits d'accès**.

2 Lire les droits en place

Machine : SRV-DC01 | **Compte :** JPCONSULTING\admin.domaine | **Outil :** PowerShell (administrateur)

```
Get-ADPrincipalGroupMembership <PRÉNOM> | Select-Object Name
```

Lire la commande

Liste les groupes **directs** du compte (ici, son **GG_** de service). Les groupes **DL_** sont atteints par l'intermédiaire du **GG_**.

Machine : SRV-DC01 | **Compte :** JPCONSULTING\admin.domaine | **Outil :** PowerShell (administrateur)

```
Get-ADGroupMember DL_Commun_M | Select-Object Name
```

Groupe	Membres (lab)	Droit sur `Commun`
DL_Commun_L	les cinq **GG_** de service	lecture (**RX**) : tout le monde lit
DL_Commun_M	**GG_Administration**, **GG_Direction**	modification (**M**) : seuls ces deux services écrivent

Je dois voir

Le **GG_** de l'utilisateur figure dans **DL_Commun_M** : il devrait pouvoir écrire ; cherche ailleurs (droits NTFS du sous-dossier, quota, fichier ouvert).

Il n'y figure pas : le refus est **normal**, c'est le droit prévu. Ce n'est pas une panne, c'est une demande de droit.

Pour voir le droit réellement obtenu sur le dossier : clic droit sur **E:\Commun** → **Propriétés** → onglet **Sécurité** → **Avancé** → onglet **Accès effectif**, **Sélectionner un utilisateur**, puis **Afficher l'accès effectif**.

3 Informer l'utilisateur

Réponds à l'utilisateur avec les faits, sans promettre de changement :

Message à l'utilisateur (suivi GLPI)

Bonjour <PRÉNOM>,

Le dossier Commun est en lecture pour tous les services ; l'enregistrement y est réservé à l'Administration et à la Direction. Le refus que vous voyez correspond donc au réglage prévu.

Si vous avez besoin d'y enregistrer, nous transmettons votre demande à la responsable du dossier, qui décidera. Pouvez-vous nous préciser ce que vous devez y déposer, et pour qui ?

Cordialement,

4 Faire décider

Le responsable des données de **Commun** est **Sam Plante**. Dans le ticket : **Demander une validation** à Sam Plante, avec le besoin exprimé et l'effet du changement possible.

Pourquoi

Ajouter **`GG_Commercial`** à **`DL_Commun_M`** donnerait l'écriture à **tout** le service Commercial, pas seulement à l'utilisateur. Le responsable doit le savoir pour décider ; il peut aussi préférer une autre solution (un dossier propre au service, un dépôt par une personne autorisée).

5 Appliquer et prouver

Si la décision est positive : console **Utilisateurs et ordinateurs Active Directory**, groupe **`DL_Commun_M`**, onglet **Membres** → **Ajouter…** → le **`GG_`** décidé → **OK**.

Machine : SRV-DC01 | **Compte :** JPCONSULTING\admin.domaine | **Outil :** PowerShell (administrateur)

```
Get-ADGroupMember DL_Commun_M | Select-Object Name
```

Attention

L'utilisateur doit **fermer sa session et la rouvrir** : ses groupes sont lus à l'ouverture de session (jeton*). Sans cela, le refus continue alors que le droit est en place.

Je dois voir

Le **`GG_`** apparaît dans la liste. Après reconnexion, l'utilisateur enregistre un fichier dans **`P:\`** : c'est la preuve.

Texte de la tâche (GLPI)

Demande de <PRÉNOM> (<SERVICE>) le <DATE> : écriture dans Commun. Constat : **`<GG_SERVICE>`** absent de **`DL_Commun_M`** (droit prévu = lecture). Validation demandée à Sam Plante le <DATE> ; décision : <ACCORD / REFUS / AUTRE SOLUTION> le <DATE>. <SI ACCORD : **`<GG_SERVICE>`** ajouté à **`DL_Commun_M`** à <HEURE> ; reconnexion de l'utilisateur ; enregistrement réussi.>

Texte de la solution (GLPI), lisible par l'utilisateur

Bonjour <PRÉNOM>,

<SI ACCORD : Sam Plante a validé votre demande. Après vous être déconnecté puis reconnecté, vous pouvez enregistrer dans le dossier Commun.> <SI REFUS : Sam Plante n'a pas retenu cette demande ; <SOLUTION_PROPOSÉE>.>

Cordialement,

Un dossier du partage a disparu pour un utilisateur

Niveau	N2 (droits NTFS), décision du responsable des données.
Où	**`SRV-DC01`** (le contrôleur de domaine), compte **`JPCONSULTING\admin.domaine`**, PowerShell ouvert **en administrateur**. Sur ce lab, le technicien N2 ne peut pas se connecter au contrôleur de domaine : on utilise un compte administrateur.
GLPI	type Incident · catégorie : Comptes et accès › Droits d'accès. *Statut : non validé*

Ce que tu reçois et ce qu'on attend de toi

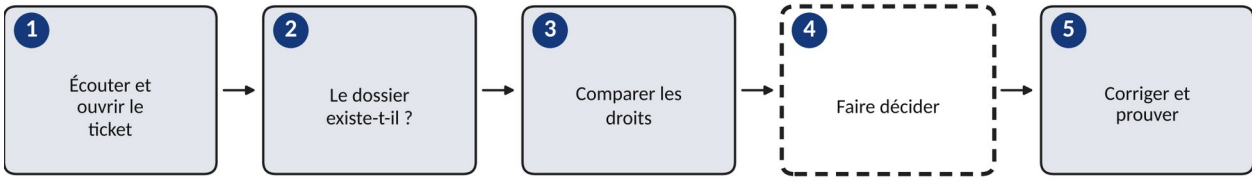
Sur ce lab, les partages utilisent l'**ABE*** (énumération basée sur l'accès) : un dossier sur lequel on n'a **aucun droit de lecture n'apparaît pas**. L'utilisateur ne voit pas « accès refusé » : il voit un dossier qui a disparu.

Ton travail : comparer avec un collègue qui le voit, trouver **quel droit manque et pourquoi** (groupe, héritage coupé), puis faire décider avant de corriger.

Ce que tu reçois, par exemple : « Le dossier Planning a disparu du lecteur P:, ma collègue le voit encore. »

Regle d'or

Un dossier « disparu » est d'abord un dossier **invisible** : on vérifie les droits avant de parler de suppression ou de restauration.



Les étapes de ce cas. À l'étape 4, c'est le responsable des données qui décide.

1 Écouter et ouvrir le ticket

- Le chemin exact du dossier et le nom d'un collègue qui le voit encore.
- Le voyiez-vous avant ? Depuis quand a-t-il disparu ?
- Quelqu'un a-t-il réorganisé ce dossier récemment ?

Ticket : **Incident**, catégorie **Comptes et accès › Droits d'accès**.

2 Le dossier existe-t-il ?

Machine : SRV-DC01 | **Compte :** JPCONSULTING\admin.domaine | **Outil :** PowerShell (administrateur)

```
Test-Path -LiteralPath 'E:\Commun\<NOM_DU_DOSSIER>'
```

Je dois voir

`True` : le dossier existe ; il est seulement invisible pour l'utilisateur. `False` : il n'existe plus à cet endroit, voir le playbook Exploitation, runbook Sauvegarde et restauration.

Machine : SRV-DC01 | **Compte :** JPCONSULTING\admin.domaine | **Outil :** PowerShell (administrateur)

```
Get-SmbShare | Select-Object Name, Path, FolderEnumerationMode
```

Lire la commande

`FolderEnumerationMode : AccessBased` : l'ABE est actif sur ce partage. Un dossier sans droit de lecture y est masqué.

3 Comparer les droits

Machine : SRV-DC01 | **Compte :** JPCONSULTING\admin.domaine | **Outil :** PowerShell (administrateur)

```
icacls 'E:\Commun'
```

Machine : SRV-DC01 | **Compte :** JPCONSULTING\admin.domaine | **Outil :** PowerShell (administrateur)

```
icacls 'E:\Commun\<NOM_DU_DOSSIER>'
```

Je dois voir

Sur un dossier normal : les mêmes entrées que le parent, précédées de `(I)` (héritées), dont `DL_Commun_L` en **RX**.

Des entrées **sans** `(I)` et pas de `DL_Commun_L` : l'**héritage* a été coupé** et les droits remplacés. Le service de l'utilisateur a perdu la lecture : d'où l'invisibilité.

Contrôle par l'onglet **Accès effectif** (Propriétés du dossier → Sécurité → Avancé → Accès effectif), pour l'utilisateur puis pour le collègue qui le voit.

4 Faire décider

Celui qui a coupé l'héritage l'a peut-être fait **exprès** (dossier réservé à un service). Ne rétablis rien de toi-même : **Demander une validation** au responsable des données de `Commun` (**Sam Plante**), avec le constat et les deux options : rétablir l'héritage, ou ajouter le groupe du service.

5 Corriger et prouver

Si la décision est de rétablir l'héritage : Propriétés du dossier → **Sécurité** → **Avancé** → **Activer l'héritage** → **OK**. Puis :

Machine : SRV-DC01 | **Compte :** JPCONSULTING\admin.domaine | **Outil :** PowerShell (administrateur)

```
icacls 'E:\Commun\<NOM_DU_DOSSIER>'
```

Je dois voir

Les entrées du parent réapparaissent avec `(I)`. L'utilisateur actualise `P:` (touche F5) : le dossier est visible et s'ouvre.

Texte de la tâche (GLPI)

Dossier **`E:\Commun\<NOM_DU_DOSSIER>`** invisible pour <PRÉNOM> (<SERVICE>), visible pour <COLLÈGUE>. ABE actif. **`icacls`** : héritage coupé, **`DL_Commun_L`** absent. Validation de Sam Plante le <DATE> : <DÉCISION>. Action : <ACTION> à <HEURE>. Preuve : **`icacls`** après, dossier visible et ouvert par l'utilisateur.

Texte de la solution (GLPI), lisible par l'utilisateur

Bonjour <PRÉNOM>,

Le dossier <NOM_DU_DOSSIER> n'avait pas disparu : un changement de droits le rendait invisible pour votre service. Après accord de la responsable du dossier, vous le voyez de nouveau.

Cordialement,

Lexique

Les mots marqués d'un astérisque (*) dans ce runbook.

AGDLP

Comptes → groupes globaux **`GG_`** → groupes de domaine local **`DL_`** → permissions sur le dossier. On change un droit en changeant l'appartenance d'un groupe.

Jeton (d'accès)

Liste des groupes d'un utilisateur, calculée à l'ouverture de session. Un groupe ajouté ensuite n'est pris en compte qu'à la session suivante.

Accès effectif

Onglet des paramètres de sécurité avancés qui calcule le droit réel d'un compte sur un dossier, groupes compris.

ABE (énumération basée sur l'accès)

Réglage d'un partage qui masque les dossiers sur lesquels l'utilisateur n'a pas le droit de lecture.

Héritage (droits NTFS)

Un dossier reprend les droits de son parent ; marqués **`(I)`** dans **`icacls`**. Couper l'héritage remplace ces droits par des droits propres au dossier.

RUNBOOK · PLAYBOOK COMPTES ET ACCÈS

Mot de passe et verrouillage

Les refus de connexion : compte verrouillé, mot de passe expiré ou oublié.

Cas traités dans ce runbook

INCIDENT Un utilisateur ne peut plus se connecter, son compte est bloqué 20

INCIDENT Le mot de passe ne fonctionne plus, il a expiré..... 24

INCIDENT Le compte se verrouille de nouveau après avoir été débloqué.... 27

Statut : non validé

Un utilisateur ne peut plus se connecter, son compte est bloqué

Niveau	N1 (constater, déverrouiller, réinitialiser). Source du verrouillage inconnue ou répétée : N2.
Où	**`SRV-DC01`** (le contrôleur de domaine), compte **`JPCONSULTING\admin.domaine`**, PowerShell ouvert **en administrateur**. Sur ce lab, le technicien N2 ne peut pas se connecter au contrôleur de domaine : on utilise un compte administrateur.
GLPI	type Incident · catégorie : Comptes et accès › Mot de passe et verrouillage. *Statut : non validé*

Ce que tu reçois et ce qu'on attend de toi

Un compte se **verrouille*** après plusieurs mauvais mots de passe : c'est une protection contre ceux qui essaient de deviner. L'utilisateur, lui, dit seulement « je n'arrive plus à me connecter ».

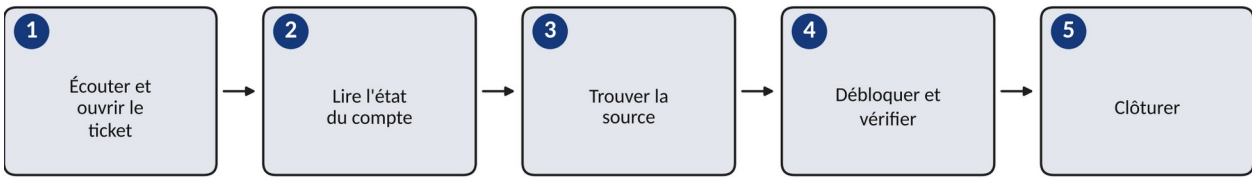
Ton travail : vérifier **qui** appelle, **prouver** ce qui bloque (verrouillage, mot de passe expiré, simple faute de frappe), débloquer si c'est justifié, et expliquer simplement ce qui s'est passé.

Ce que tu reçois, par exemple : « Bonjour, je n'arrive plus à me connecter, mon compte est bloqué. »
L'utilisateur peut se tromper sur la cause : il appelle « bloqué » tout refus de connexion.

Regle d'or

On ne touche jamais à un compte sans avoir vérifié l'identité de la personne qui le demande.

On ne pose pas la cause avant la preuve : « compte verrouillé » est une hypothèse tant que l'annuaire ne l'a pas confirmé.



Les étapes de ce cas.

1 Écouter et ouvrir le ticket

Sur ce lab, l'authentification de GLPI passe par l'annuaire : **un utilisateur bloqué ne peut pas se connecter à GLPI**. C'est donc toi qui ouvres le ticket pour lui. Mets-le bien en **demandeur** (le champ reprend facilement ton propre compte).

- Qui êtes-vous, dans quel service, sur quel poste ?
- Quel message exact voyez-vous ? (le recopier mot pour mot)
- Depuis quand ? Ça fonctionnait avant ? Avez-vous changé votre mot de passe récemment ?
- Le pavé numérique est-il allumé ? Le clavier est-il en majuscules ?
- Êtes-vous connecté ailleurs (autre poste, téléphone) avec ce compte ?

Attention

Vérifie l'identité **avant** d'agir : le compte appartient-il bien à la personne qui appelle ? Dans le lab, la personne qui appelle n'est pas toujours celle dont le compte est verrouillé (constaté lors d'un exercice).

Ticket : type **Incident**, catégorie **Comptes et accès › Mot de passe et verrouillage**, titre « Connexion refusée pour <PRÉNOM> ». **Urgence*** selon le travail bloqué ; **impact*** : une personne.

2 Lire l'état du compte

Interface graphique : console **Utilisateurs et ordinateurs Active Directory**, double-clic sur le compte, onglet **Compte**. Si le compte est verrouillé, la case **Déverrouiller le compte** est proposée. Puis la même lecture en PowerShell, qui se garde dans le ticket :

Machine : SRV-DC01 | **Compte :** JPCONSULTING\admin.domaine | **Outil :** PowerShell (administrateur)

```
Get-ADUser <PRÉNOM> -Properties LockedOut, BadLogonCount, LastBadPasswordAttempt,
PasswordExpired, PasswordLastSet, Enabled | Select-Object Name, Enabled, LockedOut,
BadLogonCount, LastBadPasswordAttempt, PasswordExpired, PasswordLastSet
```

Lire la commande

`Get-ADUser <NOM_DE_CONNEXION>` : lit le compte dans l'annuaire (nom de connexion de la forme prenom.nom).

`-Properties …` : demande des informations qui ne sont pas affichées par défaut. **`Select-Object`** : choisit les colonnes à afficher.

Ce que tu lis	Ce que ça veut dire	Suite
`LockedOut : True`	Compte **verrouillé** : trop de mauvais mots de passe	Étape 3 (d'où viennent les essais)
`PasswordExpired : True`	Mot de passe **expiré** (42 jours sur ce lab)	Cas « Mot de passe expiré »
`Enabled : False`	Compte **désactivé** (départ, décision d'un responsable)	Escalade : on ne réactive pas sans décision
Tout est normal	L'annuaire n'est pas en cause	Le poste ou la saisie : clavier, pavé numérique, mauvais compte

Je dois voir

`LastBadPasswordAttempt` donne l'heure du dernier mauvais essai : compare-la avec ce que dit l'utilisateur.

Sur ce lab : **5 essais** ratés verrouillent le compte pendant **15 minutes** ; le compteur repart à zéro après 15 minutes sans erreur.

3 Trouver la source

Le contrôleur de domaine note chaque verrouillage (**événement 4740***), avec le **nom de l'ordinateur** d'où viennent les essais :

Machine : SRV-DC01 | **Compte :** JPCONSULTING\admin.domaine | **Outil :** PowerShell (administrateur)

```
Get-WinEvent -FilterHashtable @{LogName='Security'; Id=4740} -MaxEvents 10 | Format-
List TimeCreated, Message
```

Je dois voir

Une entrée par verrouillage : l'heure, le compte verrouillé et, plus bas, **le nom de l'ordinateur appelant**.

Si l'ordinateur appelant n'est pas le poste de l'utilisateur : une autre machine essaie avec un ancien mot de passe (session restée ouverte, lecteur réseau, téléphone). Tant qu'elle n'est pas corrigée, le compte se reverrouillera.

Attention

Sur ce lab, l'audit des échecs d'ouverture de session (**événement 4625**) n'est **pas prouvé** : lors d'un exercice, des essais ratés n'y sont pas apparus. L'absence de 4625 ne prouve donc rien. Note-le dans le ticket au lieu de conclure.

4 Débloquer et vérifier

Si le verrouillage est prouvé et la source comprise : dans la console, onglet **Compte**, coche **Déverrouiller le compte**, puis **OK**. Si l'utilisateur a oublié son mot de passe : clic droit sur le compte → **Réinitialiser le mot de passe...**, coche **L'utilisateur doit changer le mot de passe à la prochaine ouverture de session**, et **Déverrouiller le compte de l'utilisateur**.

Attention

Le mot de passe provisoire ne s'écrit **jamais** dans le ticket ni dans un message GLPI. Il se donne de vive voix, après vérification de l'identité.

Sans action de ta part, le compte se déverrouille seul au bout de 15 minutes : c'est une solution acceptable si l'utilisateur peut attendre.

Vérifie dans l'annuaire :

Machine : SRV-DC01 | **Compte :** JPCONSULTING\admin.domaine | **Outil :** PowerShell (administrateur)

```
Get-ADUser <PRÉNOM> -Properties LockedOut, BadLogonCount | Select-Object Name,
LockedOut, BadLogonCount
```

Je dois voir

`LockedOut : False` et `BadLogonCount : 0`. Ensuite, la vraie preuve : l'utilisateur **ouvre sa session** sur son poste.

5 Clôturer

Dans GLPI, dans cet ordre : une **tâche** (le détail technique), puis la **solution**, lisible par l'utilisateur. Le demandeur approuve la solution ; dans ce lab, le N3 ne peut que clore.

Texte de la tâche (GLPI)

Demande reçue le <DATE> à <HEURE> de <PRÉNOM>, identité vérifiée (<COMMENT>). `Get-ADUser` : LockedOut <True/False>, BadLogonCount <N>, dernier mauvais essai <HEURE>. Événement 4740 : verrouillé à <HEURE>, ordinateur appelant <NOM_DU_POSTE>. Action : <DÉVERROUILLAGE / RÉINITIALISATION AVEC CHANGEMENT À LA PROCHAINE OUVERTURE>. Vérification : LockedOut False, session ouverte par l'utilisateur à <HEURE>.

Texte de la solution (GLPI), lisible par l'utilisateur

Bonjour <PRÉNOM>,

Votre compte s'était bloqué après plusieurs mots de passe erronés saisis depuis <NOM_DU_POSTE>. Il est débloqué et vous avez pu vous reconnecter.

<SI_RÉINITIALISÉ : Windows vous demandera de choisir un nouveau mot de passe à la prochaine connexion.> Si le blocage se reproduit, signalez-le : un autre appareil utilise peut-être encore votre ancien mot de passe.

Cordialement,

Le mot de passe ne fonctionne plus, il a expiré

Niveau	N1.
Où	**`SRV-DC01`** (le contrôleur de domaine), compte **`JPCONSULTING\admin.domaine`**, PowerShell ouvert **en administrateur**. Sur ce lab, le technicien N2 ne peut pas se connecter au contrôleur de domaine : on utilise un compte administrateur.
GLPI	type Incident · catégorie : Comptes et accès › Mot de passe et verrouillage. *Statut : non validé*

Ce que tu reçois et ce qu'on attend de toi

Sur ce lab, un mot de passe **expire*** au bout de **42 jours**. Windows prévient quelques jours avant, puis refuse l'ancien mot de passe. L'utilisateur dit « mon mot de passe ne marche plus » : il pense souvent à une panne.

Ton travail : prouver l'expiration, faire changer le mot de passe **par l'utilisateur lui-même**, et vérifier qu'il peut travailler (session, GLPI, lecteurs).

Ce que tu reçois, par exemple : « Mon mot de passe ne fonctionne plus depuis ce matin, pourtant je ne l'ai pas changé. »

Regle d'or

Le mot de passe appartient à l'utilisateur : c'est lui qui le choisit. Le technicien ne le connaît pas et ne l'écrit nulle part.



Les étapes de ce cas.

1 Écouter et ouvrir le ticket

- Qui êtes-vous, sur quel poste ? (identité vérifiée avant toute action)
- Quel message exact ? « Le mot de passe de l'utilisateur doit être modifié » n'est pas « mot de passe incorrect ».
- Depuis quand ? Avez-vous ignoré un avertissement de changement les jours précédents ?

Ticket ouvert par toi pour l'utilisateur (il ne peut pas se connecter à GLPI tant que son mot de passe est expiré). Catégorie **Comptes et accès › Mot de passe et verrouillage**.

2 Prouver l'expiration

Machine : SRV-DC01 | **Compte :** JPCONSULTING\admin.domaine | **Outil :** PowerShell (administrateur)

```
Get-ADUser <PRÉNOM> -Properties PasswordExpired, PasswordLastSet,
PasswordNeverExpires, "msDS-UserPasswordExpiryTimeComputed" | Select-Object Name,
PasswordExpired, PasswordLastSet, PasswordNeverExpires,
@{n='Expire';e={[datetime]::FromFileTime($_.'msDS-UserPasswordExpiryTimeComputed')}}
```

Lire la commande

`PasswordLastSet` : date du dernier changement. **`PasswordExpired : True`** : le mot de passe a expiré.

`msDS-UserPasswordExpiryTimeComputed` : la date d'expiration calculée par l'annuaire, en format brut ; **`[datetime]::FromFileTime(…)`** la rend lisible (colonne **`Expire`**).

Je dois voir

`PasswordExpired : True` et une date **`Expire`** passée : l'expiration est prouvée.

`PasswordExpired : False` : ce n'est pas l'expiration ; reprends le cas « compte bloqué » (verrouillage, saisie).

3 Faire changer le mot de passe

Solution préférée : **l'utilisateur change lui-même** son mot de passe sur l'écran de connexion de son poste. Windows le propose dès qu'il saisit l'ancien mot de passe (le poste doit joindre le contrôleur de domaine). Il saisit l'ancien, puis deux fois le nouveau.

Si l'utilisateur ne se souvient plus de l'ancien : console **Utilisateurs et ordinateurs Active Directory**, clic droit sur le compte → **Réinitialiser le mot de passe…**, mot de passe provisoire, case **L'utilisateur doit changer le mot de passe à la prochaine ouverture de session** cochée.

Attention

Le nouveau mot de passe doit respecter la stratégie du domaine : **7 caractères minimum**, complexité (trois types de caractères parmi majuscules, minuscules, chiffres, symboles), différent des **24 derniers**. Un refus de Windows vient souvent de là.

Ne coche jamais **Le mot de passe n'expire jamais** pour « dépanner » un compte d'utilisateur : c'est une décision de sécurité, pas un geste de support.

4 Vérifier

Machine : SRV-DC01 | **Compte :** JPCONSULTING\admin.domaine | **Outil :** PowerShell (administrateur)

```
Get-ADUser <PRÉNOM> -Properties PasswordExpired, PasswordLastSet | Select-Object Name,
PasswordExpired, PasswordLastSet
```

Je dois voir

`PasswordExpired : False` et **`PasswordLastSet`** à la date et l'heure du changement.

Puis l'utilisateur ouvre sa session, retrouve ses lecteurs réseau et se connecte à GLPI avec le nouveau mot de passe (GLPI lit l'annuaire).

5 Clôturer

Texte de la tâche (GLPI)

Demande de <PRÉNOM> le <DATE> à <HEURE>, identité vérifiée. `Get-ADUser` : PasswordExpired True, dernier changement le <DATE> (expiration à 42 jours). Changement fait par l'utilisateur sur l'écran de connexion <OU : RÉINITIALISATION AVEC CHANGEMENT OBLIGATOIRE>. Vérification : PasswordExpired False, PasswordLastSet <DATE_HEURE>, session et GLPI ouverts.

Texte de la solution (GLPI), lisible par l'utilisateur

Bonjour <PRÉNOM>,

Votre mot de passe était arrivé à expiration (il doit être changé tous les 42 jours). Vous l'avez remplacé et vous avez pu vous reconnecter.

Windows vous prévient quelques jours avant la prochaine échéance : pensez à le changer à ce moment-là.

Cordialement,

Le compte se verrouille de nouveau après avoir été débloqué

Niveau	N2 (recherche de la source sur une autre machine).
Où	**`SRV-DC01`** (journal Sécurité), puis la machine désignée par le 4740 (console ou session), compte **`JPCONSULTING\admin.domaine`**.
GLPI	type Incident · catégorie : Comptes et accès › Mot de passe et verrouillage. *Statut : non validé*

Ce que tu reçois et ce qu'on attend de toi

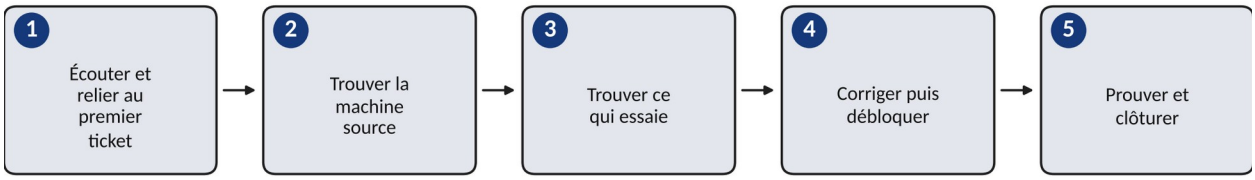
Le compte a été débloqué, et il se bloque **de nouveau** peu après. Ce n'est plus une erreur de frappe : quelque chose essaie **tout seul**, avec un **ancien mot de passe** (session restée ouverte sur un autre poste, lecteur réseau ou identifiant mémorisé, tâche planifiée, service).

Ton travail : trouver la **machine** d'où viennent les essais, puis **ce qui**, sur cette machine, utilise l'ancien mot de passe. Débloquer sans cela ne sert à rien.

Ce que tu reçois, par exemple : « Vous m'avez débloqué ce matin, et je suis de nouveau bloqué ! »

Regle d'or

On ne débloque pas une troisième fois sans avoir trouvé la source : le compte se rebloquera, et l'utilisateur perdra confiance.



Les étapes de ce cas.

1 Écouter et relier au premier ticket

- Avez-vous changé votre mot de passe récemment ? (la cause la plus fréquente)
- Sur quels autres postes vous êtes-vous connecté ces derniers jours ? Une session y est-elle restée ouverte ?
- Avez-vous enregistré votre mot de passe quelque part (lecteur réseau, application, accès à un partage) ?

Rouvre le ticket existant s'il est récent, ou crée-en un nouveau qui cite le précédent. Catégorie **Comptes et accès › Mot de passe et verrouillage**.

2 Trouver la machine source

Machine : SRV-DC01 | **Compte :** JPCONSULTING\admin.domaine | **Outil :** PowerShell (administrateur)

```
Get-WinEvent -FilterHashtable @{LogName='Security'; Id=4740} -MaxEvents 20 | Where-Object Message -like '*<PRÉNOM>*' | Format-List TimeCreated, Message
```

Lire la commande

Ne garde que les verrouillages qui citent ce compte. Pour chacun : l'heure et le **nom de l'ordinateur appelant**.

Je dois voir

Le même nom d'ordinateur à chaque verrouillage, et ce n'est pas le poste de l'utilisateur : c'est la source. Note-le.

Les heures sont régulières (toutes les heures, chaque matin à la même heure) : pense à une **tâche planifiée** ou un **service**.

L'ordinateur appelant est vide ou est le contrôleur lui-même : la tentative vient d'un accès réseau ; note-le et escalade au N2.

3 Trouver ce qui essaie

Sur la machine trouvée (console de la VM si besoin), avec un compte d'administration :

Machine : La machine source (ordinateur appelant) | **Compte :** JPCONSULTING\admin.domaine | **Outil :** Invite de commandes (administrateur)

```
quser
```

Je dois voir

Une session de l'utilisateur, ouverte ou déconnectée : elle garde l'ancien mot de passe en mémoire. C'est la cause la plus courante.

Machine : La machine source | **Compte :** l'utilisateur, dans sa session (ou administrateur) | **Outil :** Invite de commandes

```
cmdkey /list
```

Je dois voir

Des identifiants mémorisés vers **`jpconsulting.lan`**, le DC ou un partage, au nom de l'utilisateur : Windows les réessaie avec l'ancien mot de passe.

Machine : La machine source | **Compte :** JPCONSULTING\admin.domaine | **Outil :** PowerShell (administrateur)

```
Get-ScheduledTask | Where-Object { $_.Principal.UserId -like '*<PRÉNOM>*' } | Select-Object TaskName, TaskPath, State
```

Machine : La machine source | **Compte :** JPCONSULTING\admin.domaine | **Outil :** PowerShell (administrateur)

```
Get-CimInstance Win32_Service | Where-Object StartName -like '*<PRÉNOM>*' | Select-Object Name, StartName, State
```

Je dois voir

Une tâche ou un service qui s'exécute avec le compte de l'utilisateur : chaque exécution essaie l'ancien mot de passe. Un compte de personne ne devrait pas faire tourner un service : signale-le au N2.

4 Corriger puis débloquer

Source trouvée	Correction
Session restée ouverte	Fermer la session (avec l'accord de l'utilisateur) : `logoff <ID>` (numéro donné par `quser`)
Identifiant mémorisé	Le supprimer : **Panneau de configuration → Gestionnaire d'identification → Informations d'identification Windows**, ou `cmdkey /delete:<CIBLE>` dans la session de l'utilisateur
Tâche planifiée ou service	Escalade N2 : changer le compte d'exécution, sur décision du propriétaire de la tâche

Puis débloque le compte (cas « compte bloqué », étape 4).

5 Prouver et clôturer

Machine : SRV-DC01 | **Compte :** JPCONSULTING\admin.domaine | **Outil :** PowerShell (administrateur)

```
Get-ADUser <PRÉNOM> -Properties LockedOut, BadLogonCount, LastBadPasswordAttempt |
Select-Object Name, LockedOut, BadLogonCount, LastBadPasswordAttempt
```

Je dois voir

`LockedOut : False`, `BadLogonCount : 0`, et **aucun nouveau 4740** pour ce compte après la correction (relis l'étape 2 un peu plus tard : c'est la vraie preuve).

Texte de la tâche (GLPI)

Reverrouillage de <PRÉNOM> le <DATE> à <HEURE> (déjà débloqué le <DATE>, ticket n° <N>). 4740 : <N> verrouillages, ordinateur appelant <NOM>. Sur <NOM> : <SESSION / IDENTIFIANT / TÂCHE / SERVICE> utilisant l'ancien mot de passe. Correction : <ACTION>. Compte débloqué à <HEURE> ; aucun nouveau 4740 à <HEURE>.

Texte de la solution (GLPI), lisible par l'utilisateur

Bonjour <PRÉNOM>,

Votre compte se bloquait parce que <CAUSE_EN_MOTS_SIMPLES> essayait encore votre ancien mot de passe. C'est corrigé et votre compte est débloqué.

Après un changement de mot de passe, pensez à fermer vos sessions sur les autres postes.

Cordialement,

Lexique

Les mots marqués d'un astérisque (*) dans ce runbook.

Verrouillage

Blocage automatique d'un compte après un nombre de mauvais mots de passe (ici 5 en 15 minutes, pendant 15 minutes). Il protège contre la devinette des mots de passe.

Événement 4740 / 4625

Numéros du journal Sécurité du contrôleur de domaine : 4740 = un compte a été verrouillé ; 4625 = une ouverture de session a échoué.

Urgence / impact

L'urgence dit **dans quel délai** il faut agir ; l'impact dit **combien de personnes** sont touchées. Les deux donnent la priorité.

Expiration du mot de passe

Durée de vie maximale d'un mot de passe (ici 42 jours, fixée par la stratégie du domaine). Après, Windows impose d'en choisir un nouveau.

Stratégie de mot de passe

Règles du domaine : longueur minimale (7), complexité, historique (24 derniers interdits), durée de vie (42 jours).

Ordinateur appelant

Dans l'événement 4740, la machine d'où viennent les mauvais mots de passe. Ce n'est pas forcément le poste de l'utilisateur.

Identifiants mémorisés

Mots de passe que Windows garde pour se reconnecter seul (partages, lecteurs). Après un changement de mot de passe, ils deviennent faux et provoquent des échecs.