

COMPTE RENDU D'INTERVENTION

Integration d'un poste dans l'Active Directory

Jonction au domaine mlk.local et vérification

PETIT Gabin
BTS SIO SISR
INSTA
Mai 2026

Sommaire

1. Contexte de l'intervention3
1.1 Infrastructure concernée3
2. Description de la tâche3
2.1 État initial du poste3
3. Démarche de réalisation4
3.1 Étape 1 – Vérification des prérequis réseau4
3.2 Étape 2 – Ouverture des propriétés système4
3.3 Étape 3 – Saisie du domaine cible5
3.4 Étape 4 – Authentification avec un compte du domaine5
3.5 Étape 5 – Confirmation de la jonction et redémarrage6
4. Vérification de la jonction6
4.1 Vérification côté client – Écran de connexion 7
4.2 Vérification côté serveur – Console Active Directory7
4.3 Vérification des propriétés système après jonction7
5. Bilan de l'intervention7
5.1 Résultat7
5.2 Compétences mobilisées7
5.3 Préconisations8
6. Conclusion 8

1. Contexte de l'intervention

Dans le cadre de mon stage au sein du service informatique du lycée Martin Luther King, j'ai été chargé d'intégrer un nouveau poste dans l'infrastructure Active Directory de l'établissement. Cette opération consiste à joindre une machine Windows 11 au domaine mlk.local afin que les utilisateurs puissent s'y connecter avec leurs identifiants du domaine et bénéficier des stratégies de groupe appliquées par le serveur.

1.1 Infrastructure concernée

Élément	Détail
Poste client	Windows 11 (23H2) – carte mère ASRock A620AM-X
Nom de la machine	004-GAMER06
Domaine cible	mlk.local
Serveur AD	Contrôleur de domaine du lycée (domaine mlk.local)
Réseau	Réseau local du lycée Martin Luther King

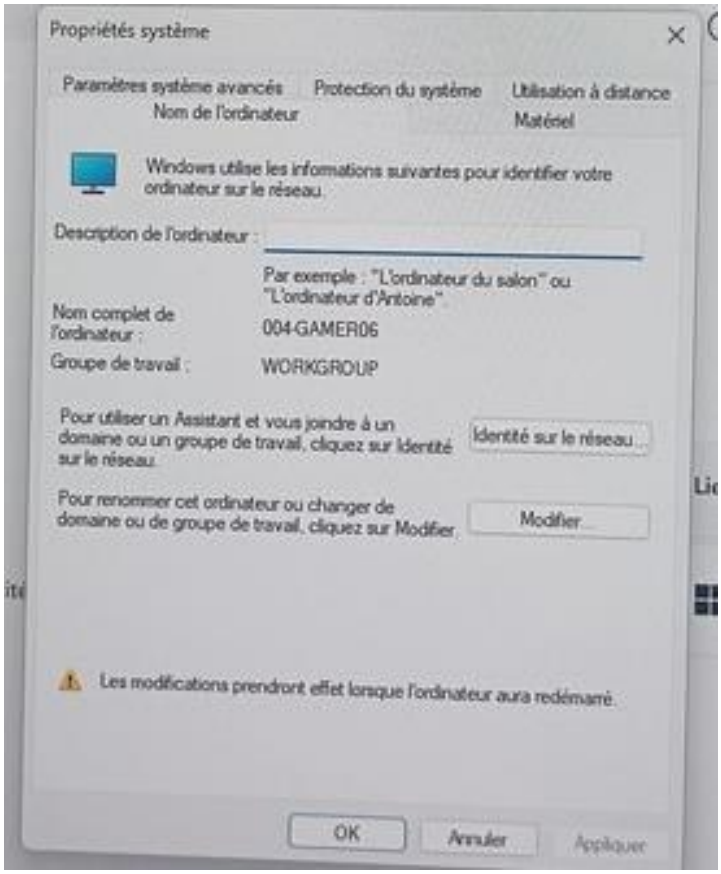
2. Description de la tâche

Le poste était initialement dans un groupe de travail (WORKGROUP) sans lien avec le domaine. L'objectif est de le joindre au domaine mlk.local pour qu'il soit géré centralement par l'Active Directory du lycée.

2.1 État initial du poste

Avant toute manipulation, le poste présentait la configuration suivante :

Paramètre	Valeur
Nom de l'ordinateur	004-GAMER06
Appartenance	WORKGROUP (groupe de travail, hors domaine)
Utilisateur local	mlk (compte local)
Système d'exploitation	Windows 11 23H2 – Build 22631.6199
Carte mère	ASRock A620AM-X



État initial – poste en WORKGROUP avant jonction au domaine

3. Démarche de réalisation

3.1 Étape 1 – Vérification des prérequis réseau

Avant de procéder à la jonction, il est indispensable de s'assurer que le poste peut joindre le contrôleur de domaine sur le réseau. Un test de ping vers le serveur AD a été réalisé depuis le poste.

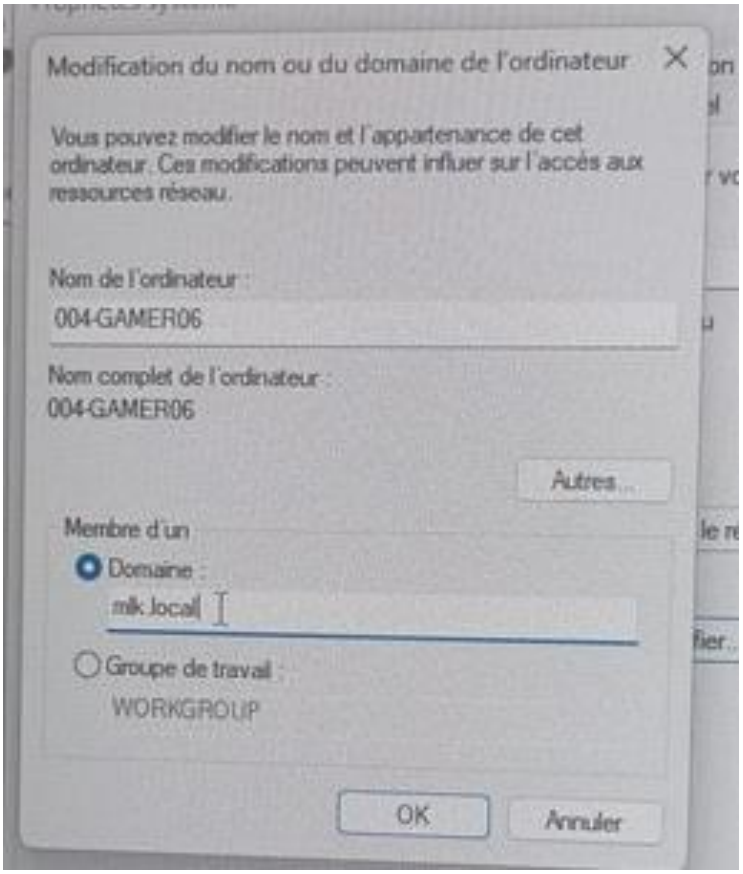
Terminal Windows : ping [IP du serveur AD] → réponses reçues, connectivité confirmée.

3.2 Étape 2 – Ouverture des propriétés système

L'accès aux propriétés système se fait via : Paramètres > Système > Informations système, puis « Renommer ce PC (avancé) ». Depuis l'onglet « Nom de l'ordinateur », on clique sur « Modifier » pour accéder à la fenêtre de jonction au domaine.

3.3 Étape 3 – Saisie du domaine cible

Dans la fenêtre de modification, on sélectionne « Domaine » puis on saisit le nom du domaine : mlk.local. Windows demande ensuite les identifiants d'un compte autorisé à joindre des machines au domaine.



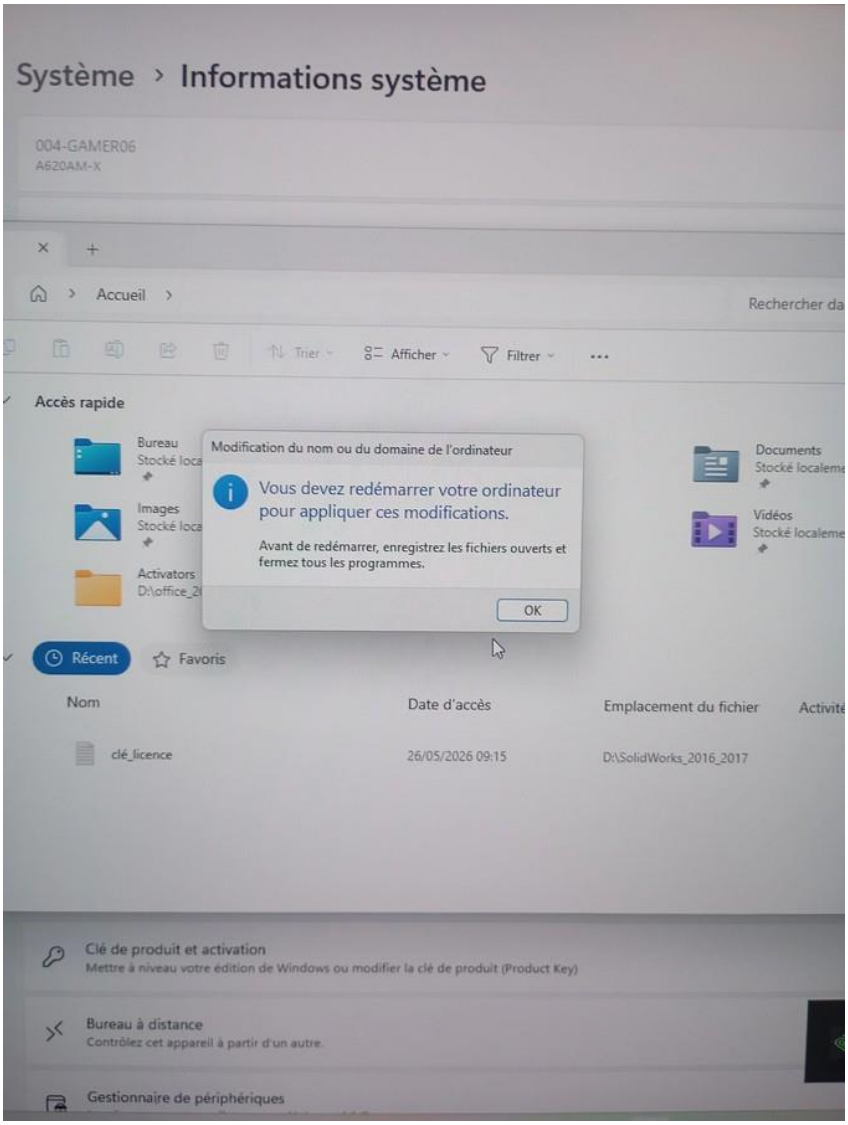
Fenêtre de jonction – saisie du domaine mlk.local

3.4 Étape 4 – Authentification avec un compte du domaine

Windows demande les identifiants d'un administrateur du domaine pour autoriser la jonction. Ces credentials sont vérifiés par le contrôleur de domaine.

3.5 Étape 5 – Confirmation de la jonction et redémarrage

Si les identifiants sont corrects et que le serveur AD est joignable, Windows affiche un message de bienvenue dans le domaine mlk.local. Un redémarrage est obligatoire pour appliquer les modifications.

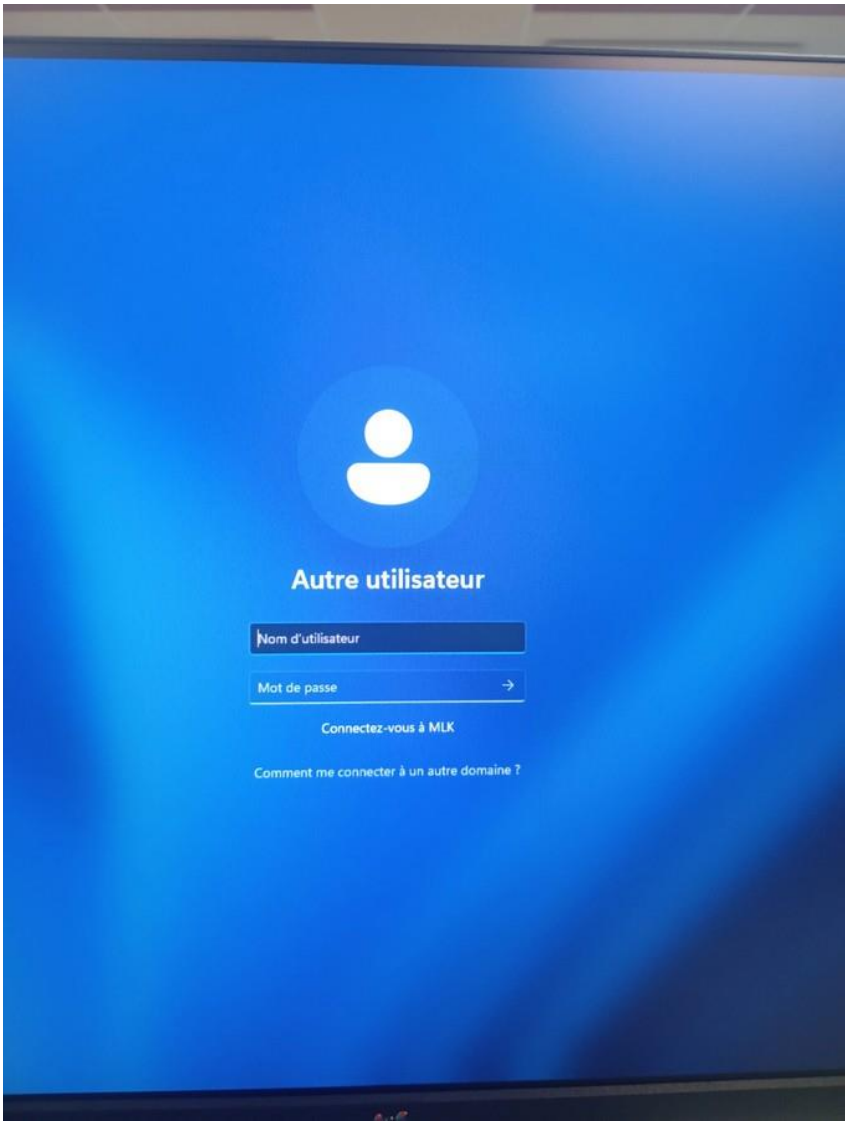


Message de confirmation – redémarrage requis après jonction réussie

4. Vérification de la jonction

4.1 Vérification côté client – Écran de connexion

Au redémarrage, l'écran de connexion Windows affiche désormais « Connectez-vous à MLK », confirmant que le poste reconnaît le domaine et propose de s'y authentifier.



Écran de connexion – « Connectez-vous à MLK »

4.2 Vérification côté serveur – Console Active Directory

La vérification côté serveur est effectuée depuis la console « Utilisateurs et ordinateurs Active Directory » (dsa.msc) sur le contrôleur de domaine. Le poste 004-GAMER06 doit apparaître dans le conteneur Computers du domaine mlk.local.

4.3 Vérification des propriétés système après jonction

Après redémarrage, les propriétés système confirment que le poste appartient désormais au domaine mlk.local et non plus à WORKGROUP.

5. Bilan de l'intervention

5.1 Résultat

La jonction au domaine mlk.local a été réalisée avec succès. Le poste 004-GAMER06 est désormais géré par l'Active Directory du lycée Martin Luther King. Les utilisateurs du domaine peuvent s'y connecter avec leurs identifiants habituels et bénéficier des stratégies de groupe (GPO) appliquées par le contrôleur de domaine.

5.2 Compétences mobilisées

- Connaissance de l'architecture Active Directory (domaine, contrôleur de domaine, objets Computers)
- Configuration réseau : vérification de la connectivité entre le poste et le serveur AD
- Manipulation des propriétés système Windows (sysdm.cpl)
- Utilisation des comptes d'administration du domaine pour autoriser la jonction
- Vérification de la jonction côté client (écran de connexion) et côté serveur (console dsa.msc)

5.3 Préconisations

- Attribuer une IP fixe ou une réservation DHCP au poste pour garantir sa joignabilité permanente dans le domaine
- Renommer la machine selon la convention de nommage du lycée avant la jonction (déjà respecté : 004-GAMER06)
- Déplacer le compte ordinateur dans une OU dédiée (ex. : Salles > Salle004) pour l'application des GPO appropriées
- Documenter la jonction dans l'inventaire du parc informatique (nom, IP, date de jonction, VLAN)

6. Conclusion

Cette intervention illustre une tâche courante dans la gestion d'un parc informatique en entreprise : l'intégration d'un nouveau poste dans l'infrastructure Active Directory. La procédure, bien que simple en apparence, nécessite une vérification rigoureuse à chaque étape — prérequis réseau, authentification, confirmation côté client et côté serveur — afin de garantir que le poste est correctement pris en charge par le domaine. Elle met en œuvre des compétences clés du référentiel BTS SIO SISR : administration Windows, gestion des identités et des accès, et maintenance du parc.