Mise en place d'un RODC (Read-Only Domain Controller)

Sommaire :

I. Présentation de la mécanique RODC :

Le **RODC (Read-Only Domain Controller)** est un contrôleur de domaine en lecture seule introduit avec Windows Server 2008. Il s'intègre dans une infrastructure Active Directory et permet d'ajouter un serveur contrôleur de domaine dans des environnements où la sécurité ne peut pas être totalement garantie, comme dans des sites distants ou des succursales.

Contrairement à un contrôleur de domaine classique (RWDC – Read-Write Domain Controller), le RODC contient une **copie en lecture seule de la base Active Directory**. Cela signifie qu'aucune modification ne peut être effectuée localement sur le RODC. Toutes les écritures (ajouts, modifications d'objets, etc.) doivent être faites sur un RWDC. Le RODC se contente de répliquer les données autorisées depuis le contrôleur principal.

L'avantage principal de cette mécanique réside dans la **sécurité** : si le serveur RODC est compromis, l'impact est limité car :

- Il ne contient pas tous les mots de passe des utilisateurs (seuls ceux explicitement autorisés à être stockés le sont),
- Il ne peut pas altérer les objets dans l'annuaire,
- Il peut être administré localement par un compte non-administrateur du domaine (administration déléguée).

Le RODC est donc particulièrement utile pour les organisations disposant de **sites distants**, avec peu ou pas de personnel informatique sur place, tout en garantissant un accès rapide et sécurisé à l'Active Directory pour les utilisateurs du site.

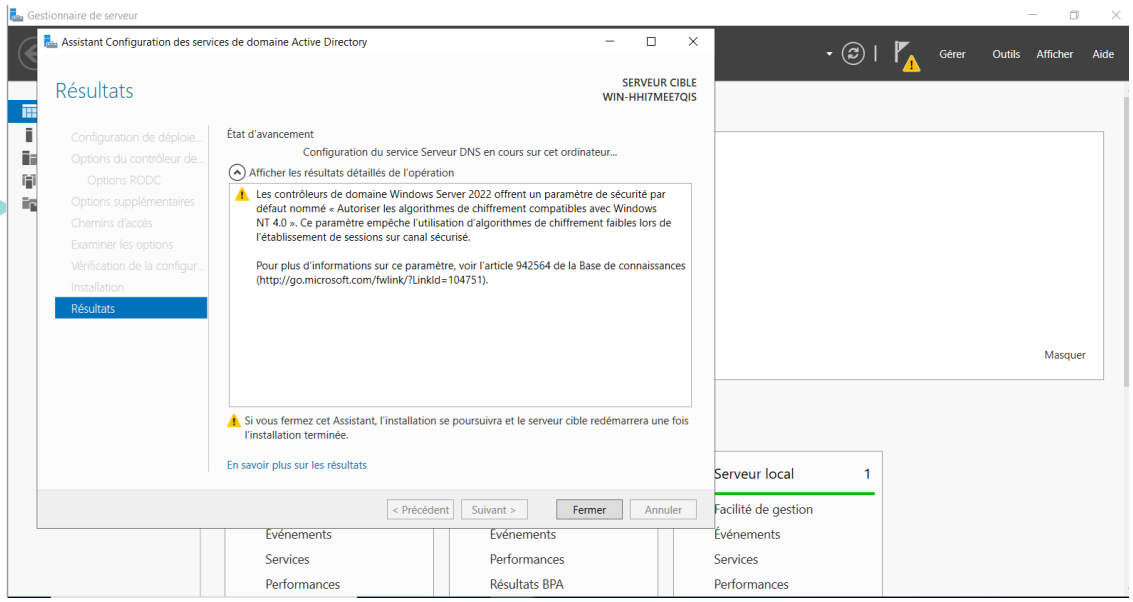
II. Procédure de mise en place d'un RODC :

Prérequis :

- Le niveau fonctionnel de la forêt et du domaine doit être au minimum Windows Server 2003.
- Exécuter la commande adprep /rodcprep sur le contrôleur de domaine détenant le rôle de "maître d'infrastructure".
- Assurez-vous que le RODC peut transférer les requêtes d'authentification vers les contrôleurs de domaine standards (Windows Server 2008 minimum).

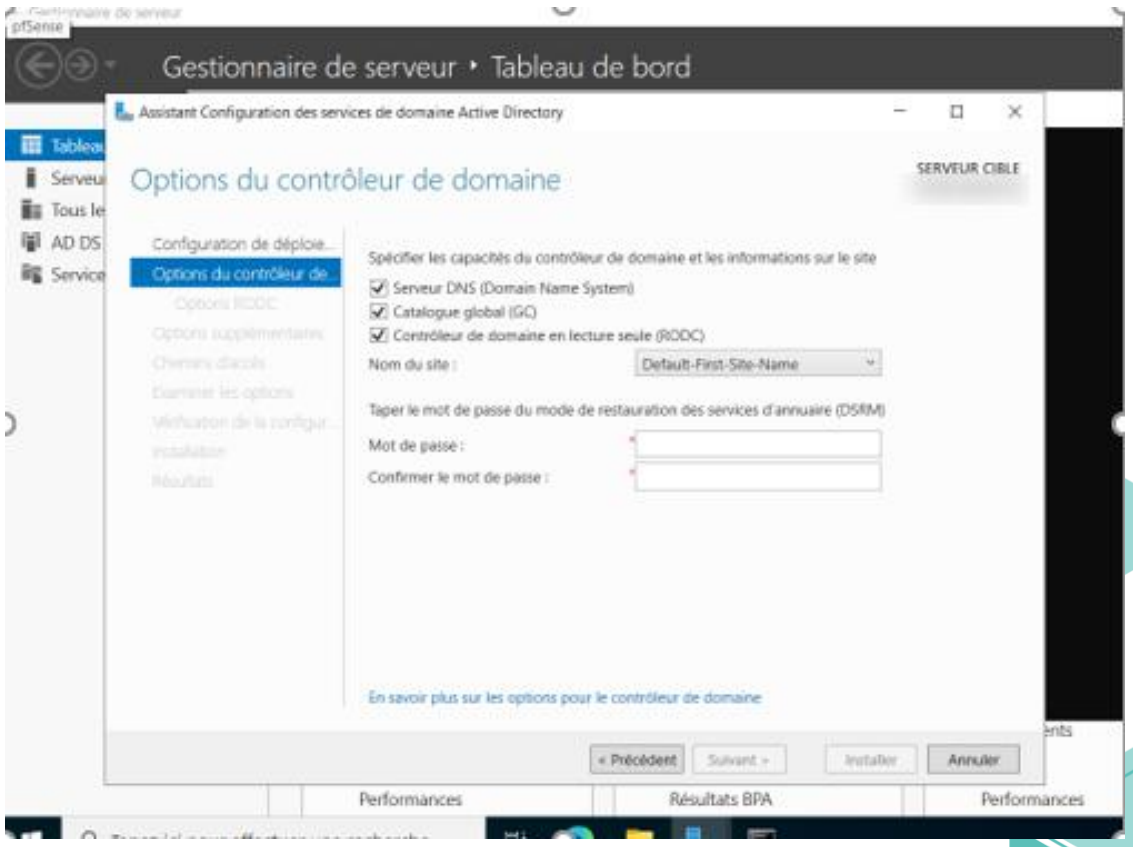
Installation du rôle AD DS sur le serveur distant (futur RODC) :

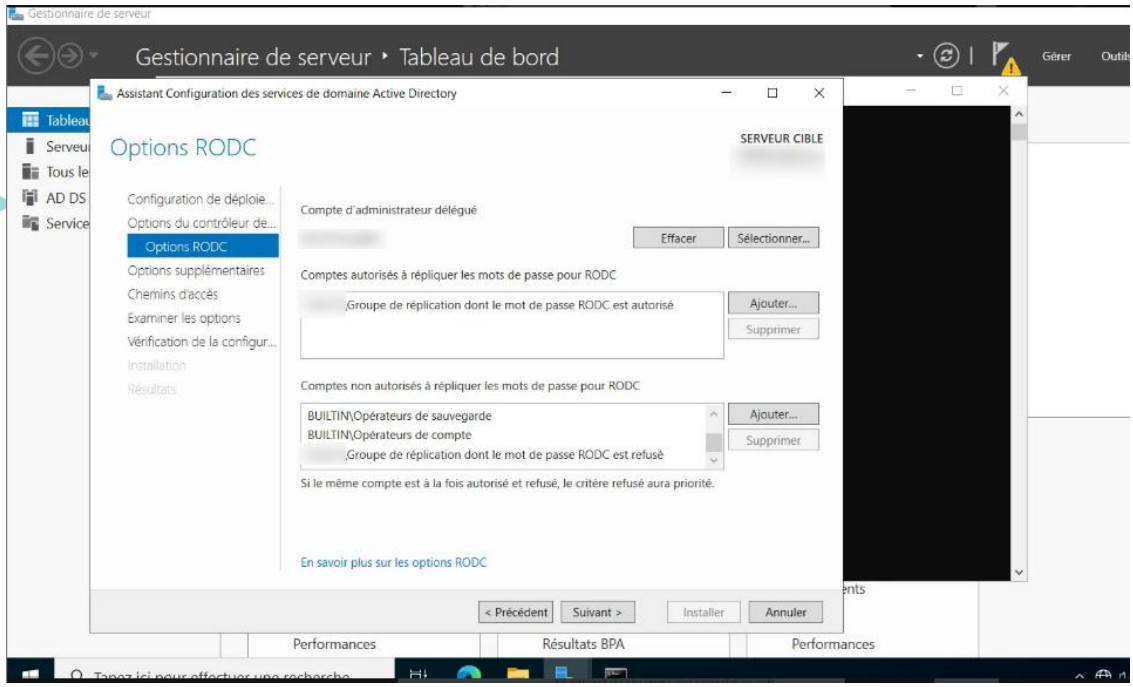
- Ouvrez le gestionnaire de serveur, cliquez sur « Gérer » puis « Ajouter des rôles et fonctionnalités ».
- Sélectionnez le type d'installation et le serveur cible.
- Dans la liste des rôles, choisissez "Services AD DS".
- Confirmez l'ajout des fonctionnalités requises.
- Confirmez l'installation. Si problème de réplication : essayer la commande repadmin /showrepl sur un powershell de l'AD pour vérifier la réplication Active Directory.



Une fois la configuration terminée, retournez dans le gestionnaire de serveur, Cliquez sur la notification, puis "Promouvoir ce serveur en contrôleur de domaine".

Dans les prochaines parties, choisir Contrôleur de domaine en lecteure seule et saisir le compte permettant la réplication.





Configuration du RODC :

Compte d'administrateur délégué : Spécifiez un compte d'administrateur local pour le serveur RODC.

Groupes de réplication des mots de passe :

- Définissez les utilisateurs ou groupes dont les mots de passe sont autorisés à être répliqués sur le RODC en les ajoutant au "Groupe de réplication dont le mot de passe RODC est autorisé".
- Définissez les utilisateurs ou groupes dont les mots de passe ne sont pas autorisés à être répliqués sur le RODC en les ajoutant au "Groupe de réplication dont le mot de passe RODC est refusé". Les comptes sensibles, comme les administrateurs, sont généralement ajoutés à ce groupe.

Serveur source de réplication :

Indiquez un contrôleur de domaine standard depuis lequel le RODC répliquera les informations.

Emplacement des fichiers :

Indiquez l'emplacement de la base de données, des fichiers journaux et de SYSVOL.

Finalisation de l'installation :

Vérifiez les options et cliquez sur « Installer ».

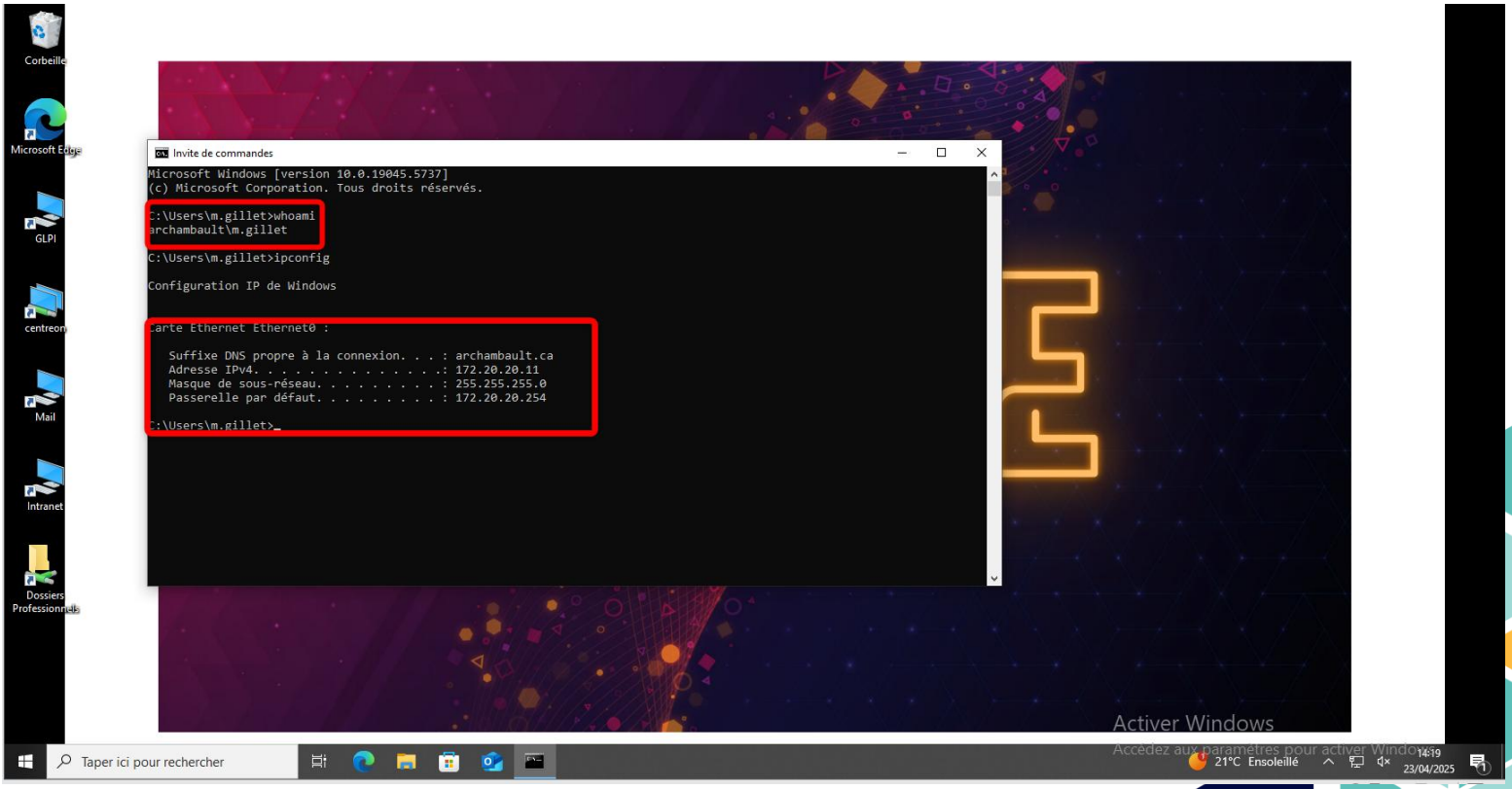
Le serveur redémarre automatiquement à la fin de l'installation.

III. Test et vérifications :

Pour vérifier si la réplication est fonctionnelle nous pouvons vérifier deux choses :

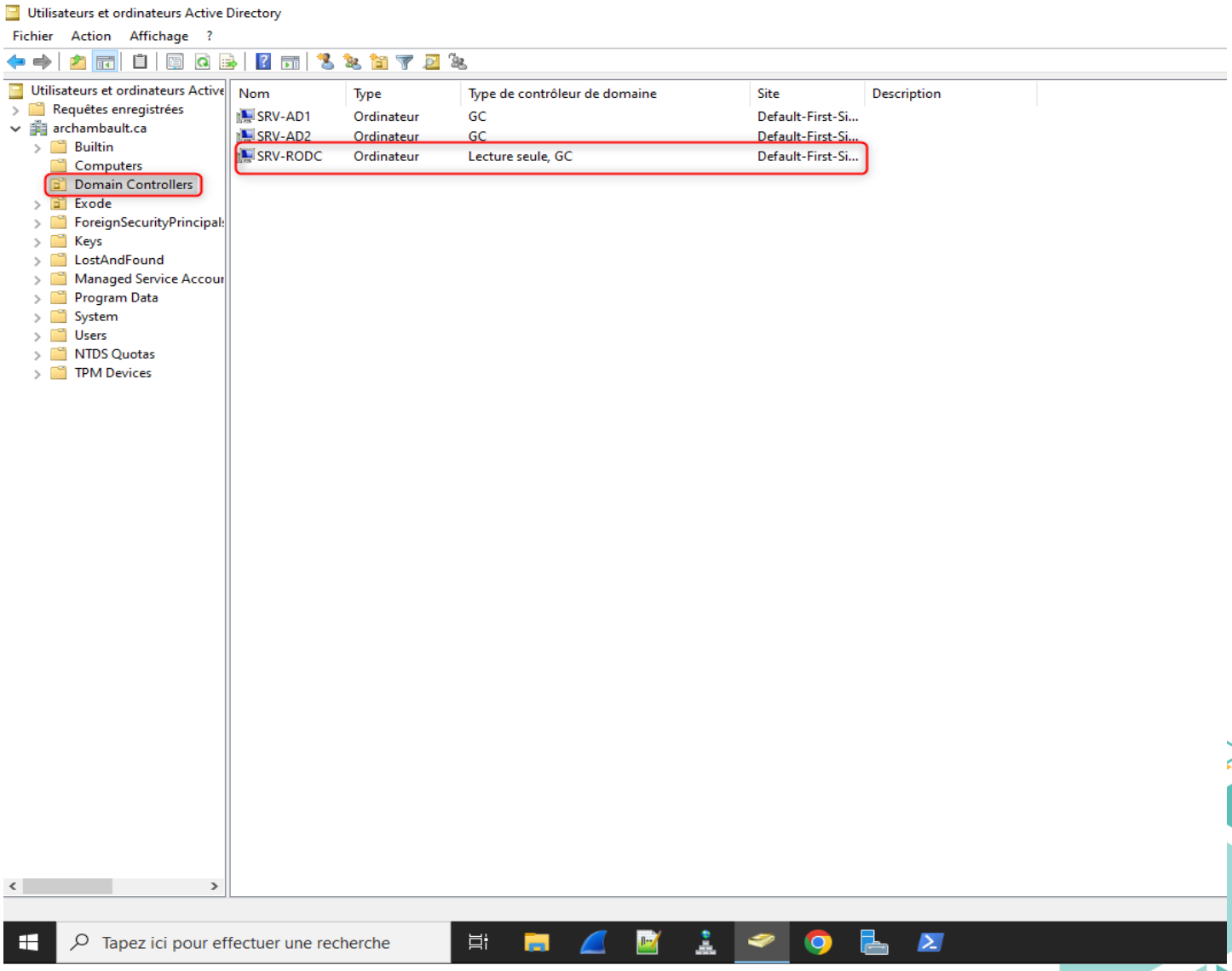
- La connexion avec un compte utilisateur du domaine sur un PC distant.
- La présence dans les Domain Controller du SRV-RODC en lecture seule.

Pour ce qui est de la connexion avec un compte utilisateur :



La connexion utilisateur du VLAN Direction avec un compte de la direction est bien fonctionnelle.

Maintenant nous pouvons vérifier la présence du RODC dans l'AD :



Le serveur RODC est bien présent et uniquement en lecture seule.

IV. Accès et utilité d'un RODC :

Une fois le RODC installé et configuré dans un site distant, il devient un point d'accès local à l'Active Directory pour les utilisateurs présents sur ce site. Cela améliore la **réactivité des connexions** et réduit la **dépendance vis-à-vis du lien réseau avec le siège**, où se trouvent généralement les contrôleurs de domaine principaux (RWDC).

Accès :

Les utilisateurs accèdent au RODC de manière **transparente**, comme s'ils se connectaient à un contrôleur de domaine classique. Lorsqu'ils s'authentifient, le RODC traite la demande en local si les informations nécessaires (notamment les mots de passe) ont été préalablement répliquées. Sinon, il interroge un RWDC via le lien réseau.

Le RODC peut également héberger un **serveur DNS en lecture seule**, ce qui permet aux postes du site distant de **résoudre les noms de domaine localement** sans surcharger la liaison WAN. Cette fonctionnalité est essentielle pour garantir des performances optimales et une continuité de service dans les environnements distants.

Utilité :

- **Performance** : en ayant un accès local à l'annuaire et au DNS, les utilisateurs bénéficient de temps de réponse plus courts.
- **Continuité de service** : en cas de coupure réseau entre le site distant et le site principal, le RODC permet aux utilisateurs de continuer à s'authentifier si leurs identifiants sont en cache, et de continuer à résoudre les noms DNS localement.

- **Sécurité renforcée** : en ne stockant que les informations nécessaires, le RODC limite les risques en cas de vol ou de compromission du serveur.
- **Administration déléguée** : un technicien sur site peut avoir les droits pour administrer le RODC (matériel, redémarrage, services de base) sans être administrateur du domaine.

Le RODC constitue donc un élément clé pour **étendre un domaine Active Directory de manière sécurisée et optimisée**, tout en tenant compte des contraintes de sécurité et de connectivité des sites distants.

V. Compétences mises en œuvre :

Compétence du référentiel	Mise en œuvre dans le projet
Répondre aux incidents et aux demandes d'assistance et d'évolutions	Amélioration des performances d'accès au domaine, ainsi qu'une sécurisation des données d'annuaire. Déchargement du réseau WAN, puisque les utilisateurs sont directement authentifiés grâce au RODC.
Mettre à disposition des utilisateurs un service informatique	Mise en place de l'authentification locale sécurisée et la résolution DNS. Mise en place transparente pour les utilisateurs, sans qu'ils aient conscience de la complexité sous-jacente.
Gérer le patrimoine informatique	Déploiement d'un RODC permettant d'optimiser l'infrastructure existante en ajoutant un composant sécurisé. Préparation de l'infrastructure et intégration au domaine.

VI. Problèmes rencontrés et solutions :

Dans le cadre du déploiement d'un contrôleur de domaine en lecture seule (RODC) sur un site distant, certaines difficultés techniques ont été rencontrées lors de la phase de configuration. Voici un exemple concret de problématique et la solution apportée.

Problème :

Lors de la mise en place du RODC dans un site distant, les utilisateurs du site ne parvenaient pas à s'authentifier localement. À chaque tentative, l'authentification était redirigée vers le contrôleur de domaine principal (RWDC), ce qui provoquait des lenteurs, surtout en cas de coupure de la liaison réseau entre les sites.

Ce problème venait du fait **que** les mots de passe des comptes utilisateurs du site distant n'étaient pas mis en cache sur le RODC, empêchant toute authentification locale en cas d'indisponibilité du lien WAN.

Solution :

Pour résoudre ce problème, une stratégie de mot de passe en cache (Password Replication Policy - PRP) a été configurée. Les comptes des utilisateurs du site distant ont été ajoutés au groupe autorisé à répliquer leurs mots de passe sur le RODC. Une fois cette configuration appliquée et les utilisateurs authentifiés une première fois, leurs informations ont été mises en cache.

Ainsi, en cas de perte de connexion avec le DC principal, les utilisateurs peuvent désormais s'authentifier localement grâce aux informations stockées dans le RODC, assurant une meilleure autonomie et disponibilité du service.