SPRINT 1 — Infrastructure AD DS

Sprint 1.1 : Installer le premier contrôleur de domaine sur Windows Server, configurer le DNS, créer la forêt sio.local et sécuriser le compte admin du domaine

- Besoin :
  - Adressage réseau fixe : Fixer l'IP du serveur pour que l'AD et le DNS restent stables. ○ Identité du domaine : Mettre en place le domaine Active Directory sio.local pour centraliser l'authentification.
  - Résolution DNS locale : Activer le rôle DNS sur le contrôleur de domaine pour gérer la zone racine. ○ Sécurisation du compte d'administration : Mettre un mot de passe fort sur le compte Administrateur du domaine.
  - Accès Internet des clients : Permettre aux PC clients d'aller sur Internet □ Analyse/Etude :
  - Système d'exploitation et rôle : Utilisation de Windows Server avec le rôle Active Directory Domain Services (AD DS). ○ Adressage IP et DNS : Utilisation de l'adresse 172.16.20.100. Le serveur pointe sur lui-même (127.0.0.1)
  - Fonctionnement des redirigeurs : Les PC clients doivent interroger uniquement le serveur SRV-AD (172.16.20.100). Si un élève cherche un site externe, SRV-AD ne connaît pas la réponse et doit transmettre la requête à la passerelle du réseau (172.16.10.254) □ Paramétrage :
  - Configuration du serveur :
  - 

Figure 1: Configuration de l'adresse IP fixe et du serveur DNS local sur le serveur SRV-AD.

  - Déploiement AD DS et DNS :

- Installation des rôles Services de domaine Active Directory et Serveur DNS dans le Gestionnaire de serveur.

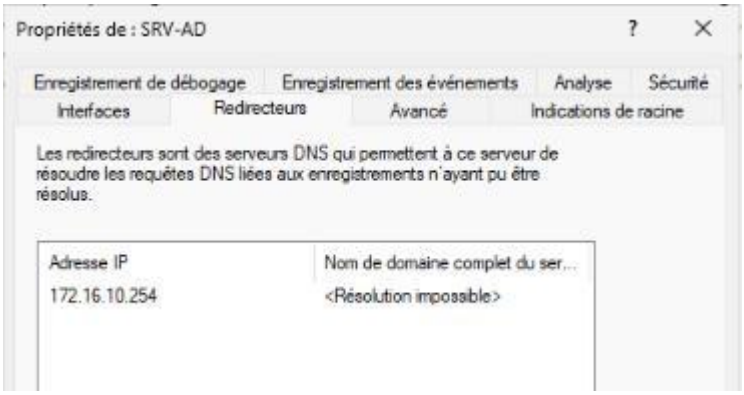


Figure 2: Configuration des redirecteurs DNS vers la passerelle réseau pour permettre la résolution Internet aux postes clients.

- Promotion du serveur en contrôleur de domaine avec création de la nouvelle forêt sio.local. ○ Sécurisation du compte Administrateur :
- Définition d'un mot de passe fort respectant la politique de complexité 16 caractères (stocké de manière sécurisée dans le gestionnaire de mots de passe de l'équipe).

- Test :

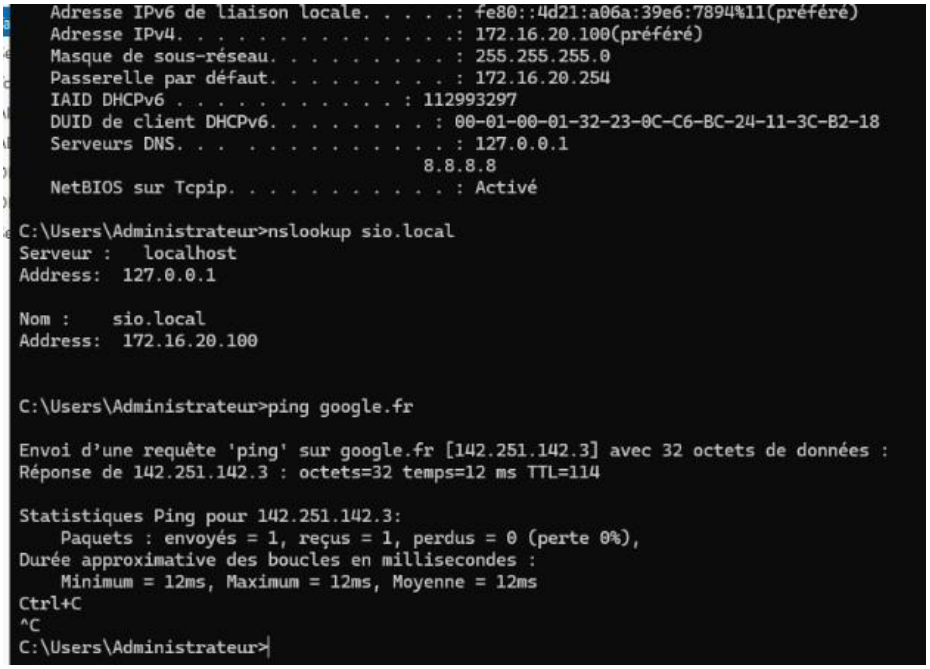


Figure 3: Vérification

Sprint 1.2 : Organiser l'Active Directory avec des Unités d'Organisation (OU), créer les groupes de sécurité et ajouter les comptes utilisateurs.

- Besoin :
    - Segmentation de l'annuaire : Organiser (utilisateurs, machines, comptes de service) avec des Unités d'Organisation (OU). ○ Gestion des droits ciblée : Créer des « groupes de sécurité globaux » pour attribuer les accès aux partages. ○ Comptes de service : comptes dédiés aux liaisons (connecteur GLPI).



- Analyse/Etude :
    - Arborescence des OU :
        - OU=Utilisateurs (divisée en SIO1, SIO2 et License).
        - OU=Postes (pour les ordinateurs Windows 11 du parc).
        - OU=Connecteur (isole le compte de service dédié à la synchronisation LDAP). ○ Groupes des groupes de sécurité : Groupes globaux G_SIO1, G_SIO2 et G_License (rangés dans leur UO respectives) utilisés pour le ciblage des GPO et l'accès au serveur de fichiers.
    - Création des comptes :
    - Création des comptes élèves Paramétrage :

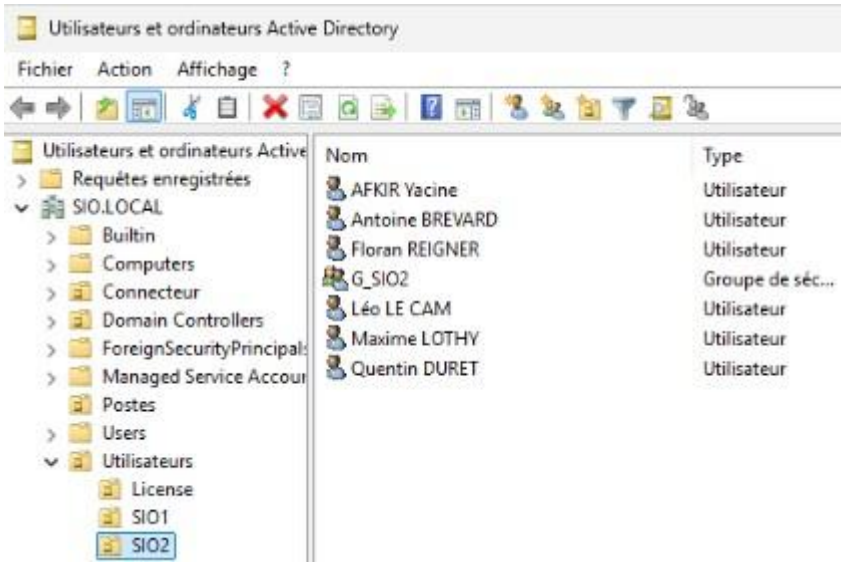


Figure 4: Structuration de l'AD en UO

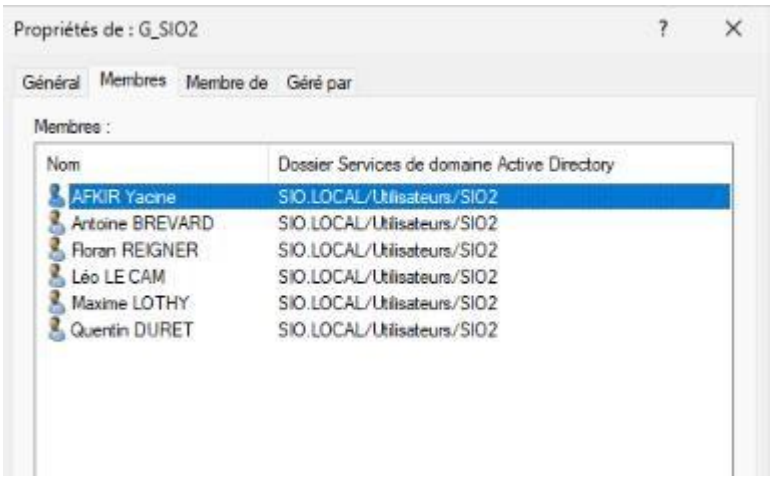


Figure 5: association aux groupes de sécurité ciblés (G_SIO1, G_SIO2).

- Test :

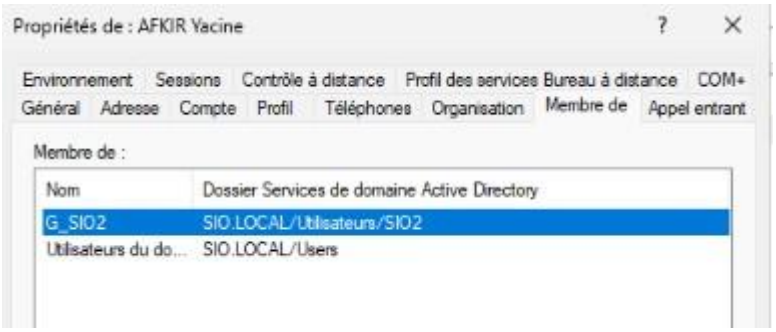


Figure 6: Contrôle de l'affectation de l'utilisateur dans son groupe de sécurité (G_SIO2).

Sprint 1.3 : Adapter la politique de sécurité des mots de passe du domaine (Default Domain Policy)

- Besoin :
  - Autoriser le changement immédiat : Supprimer le délai d'attente de 24h imposé par défaut avant de pouvoir modifier un mot de passe créer récemment
  - Éviter le blocage d'expiration : Désactiver l'expiration automatique des mots de passe à 42 jours pour la gestion de la classe.
- Fluidifier la première ouverture de session : Éviter que Windows refuse le nouveau mot de passe quand l'utilisateur doit le changer.
- Analyse/Etude :
  - Durée de vie minimale : La fixer à 0 jour pour que la case "L'utilisateur doit changer le mot de passe à la prochaine ouverture de session" fonctionne immédiatement.
  - Durée de vie maximale : La fixer à 0 (jamais d'expiration) dans le cadre de la maquette de classe.
- Exigences de complexité : Désactiver la complexité obligatoire, tout en gardant la règle de base de l'AD qui bloque si le mot de passe contient le nom ou le prénom.

- Paramétrage :

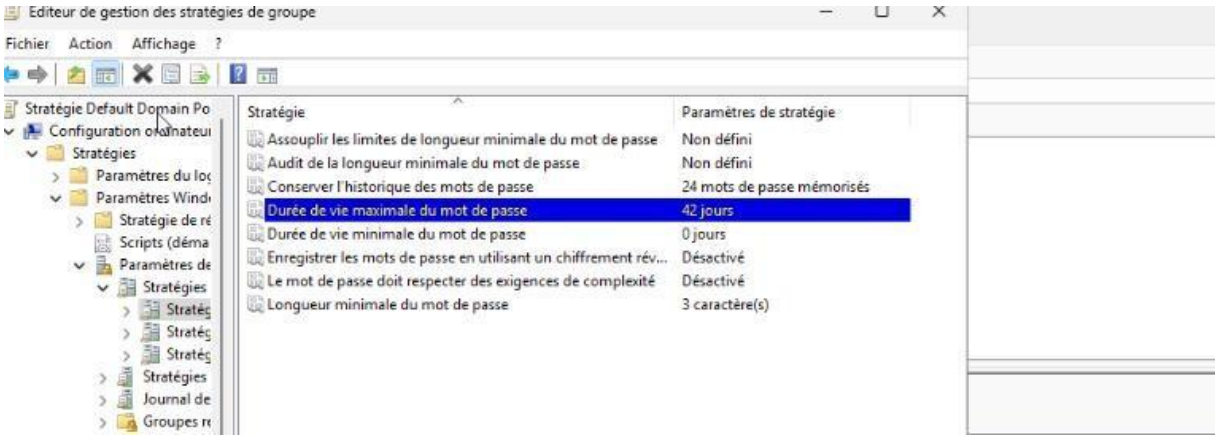


Figure 7: Adaptation de la Default Domain Policy fixant la durée de vie minimale du mot de passe à 0 jour pour autoriser le changement immédiat à la première connexion.

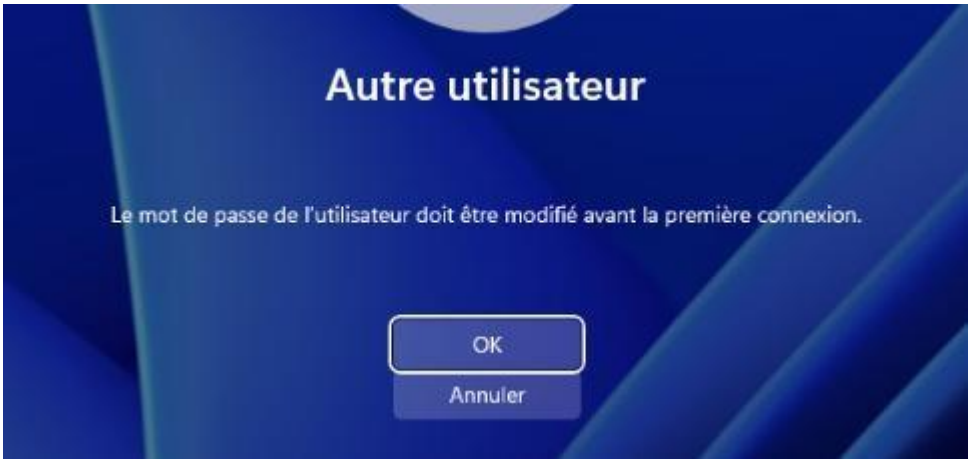
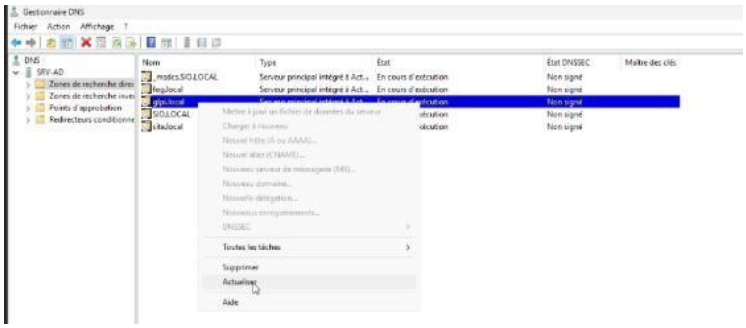
- Test :
  - Faire la commande gpupdate /force sur le contrôleur de domaine SRV-AD.
  - 

Figure 8: Validation de l'application de la stratégie de mot de passe lors de la première ouverture de session d'un élève.

SPRINT 3 — Configuration des services DNS, déploiement des GPO et Environnement Postes Clients

Demande 3.1 : Configurer les zones de recherche directe DNS pour la résolution d'adresse des services web de la salle.

- Besoin :
    - Résolution FQDN interne : Permettre aux postes d'atteindre les applications web (GLPI, FOG, Site SIO) avec des noms de domaine clairs sans devoir taper les IP. ○ Indirection des services : Associer les noms des services aux vraies adresses IP des serveurs qui tournent sur Proxmox.
- Analyse/Etude :
    - Zones DNS indépendantes : Création de zones de recherche directe intégrées à l'Active Directory.
    - Enregistrements A (Hôtes) :
        - glpi.sio.local -> 172.16.20.101
        - fog.sio.local -> 172.16.20.102
        - site.sio.local -> 172.16.20.105 ○ () : Pour dégriser la création d'un enregistrement Nouvel hôte (A), la zone doit être sélectionnée dans l'arborescence du volet gauche de la console DNS.



- Paramétrage :

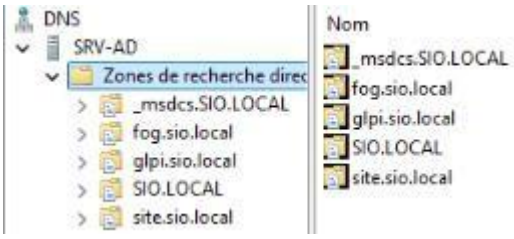


Figure 9: Création des zones de recherche directe intégrées AD pour les applications de la salle.



Figure 10: Déclaration de l'enregistrement associant le nom glpi.sio.local à l'adresse IP de l'application.

- Test :

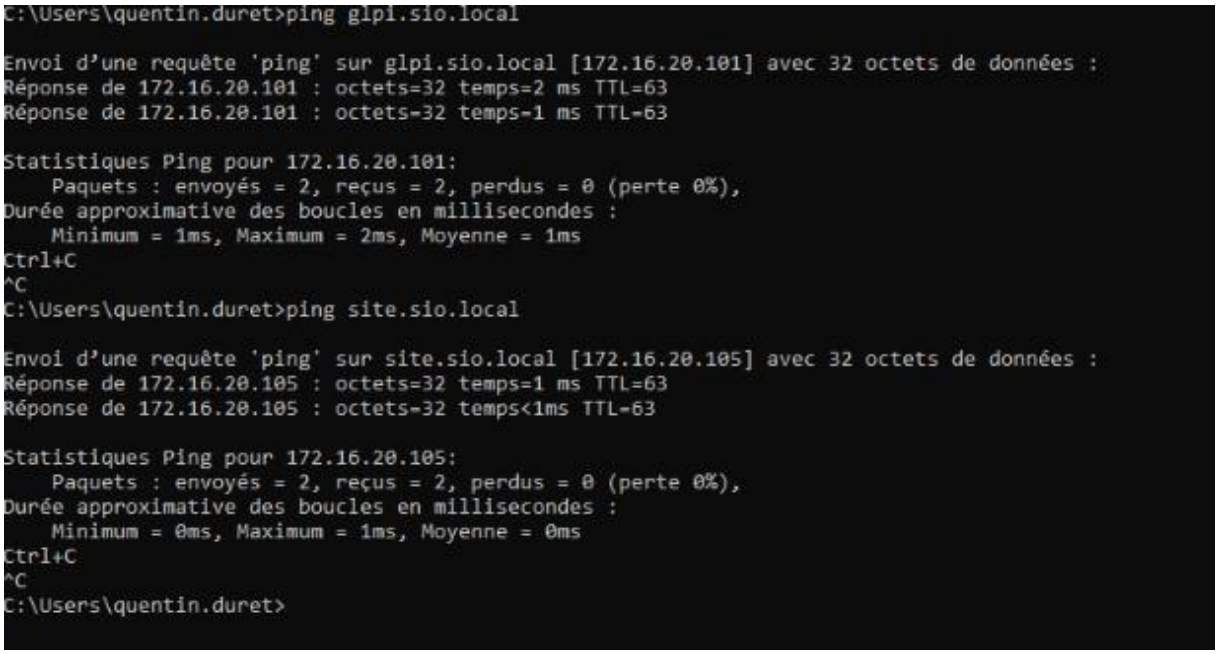


Figure 11: bon fonctionnement des zones DNS ciblées depuis un poste client

Demande 3.2 : Déployer par stratégie de groupe (GPO) les raccourcis web et le mappage automatique des lecteurs réseau ciblés par groupe.

- Besoin :
  - Accès web automatique : Déposer sur le bureau des utilisateurs les raccourcis d'accès aux services (GLPI, Site)
  - Lecteurs réseau dynamiques : Monter automatiquement la lettre réseau S/T: pointant vers le dossier de la classe de l'utilisateur connecté (SIO1 ou SIO2).
- Analyse/Etude :
  - GPO : Utilisation de la branche Configuration utilisateur > Préférences > Paramètres Windows.
- Ciblage par élément : Filtrer le mappage des lecteurs réseau pour monter le partage \\172.16.20.103\SIO1 chez le groupe G_SIO1 et \\172.16.20.103\SIO2 chez G_SIO2.

- Paramétrage :
  - GPO Raccourcis Web (GPO_Raccourcis_Web) :



Figure 12: Configuration de la GPO

- GPO Lecteurs Mappes (GPO_Lecteurs_Mappes) :



Figure 13: Configuration de la GPO

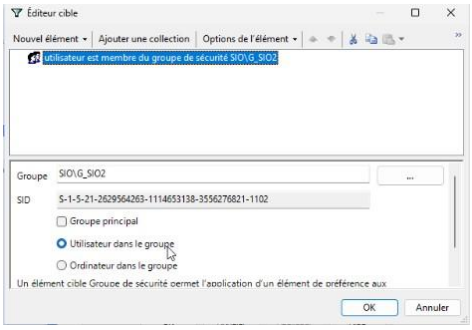


Figure 14: ciblage par groupe de sécurité

- Test :

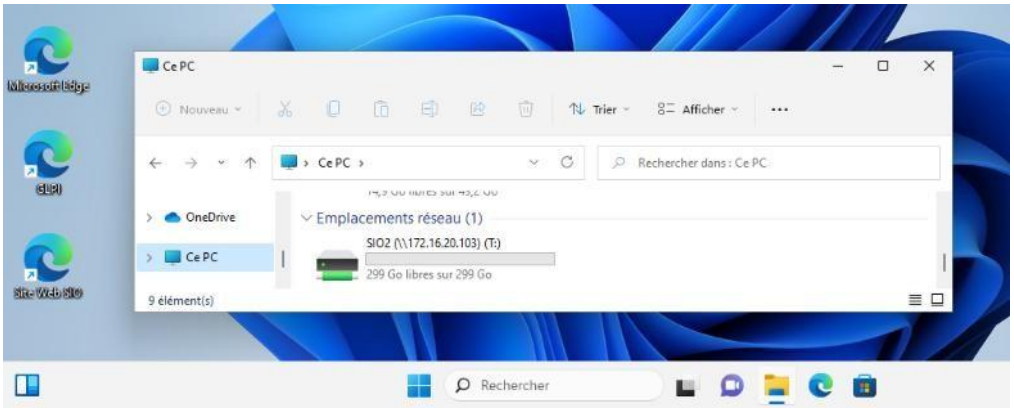


Figure 15: Validation de l'application des GPO : présence des raccourcis Web sur le bureau et montage automatique du lecteur réseau de classe

Demande 3.3 : Déploiement automatisé d'applications par GPO (Configuration Ordinateur)

- Besoin :
  - Installation transparente : Déployer automatiquement les logiciels métiers (fichiers .msi) sur l'ensemble des machines du parc sans intervention des utilisateurs.
  - Exécution au démarrage : Effectuer l'installation sous le privilège système avant l'ouverture de session.
- Analyse/Etude :
  - Emplacement du paquet : Utilisation du partage réseau \\172.16.20.103\Logiciels\
  - Niveau d'application : Branche Configuration ordinateur > Stratégies > Paramètres du logiciel > Installation de logiciel.
  - Ciblage : GPO liée à l'Unité d'Organisation OU=Postes (contenant les comptes ordinateurs).

- Paramétrage :
  - (SCREEN)Création et liaison de la GPO
  - (SCREEN)Ajout d'un nouveau package dans Installation de logiciel en spécifiant impérativement le chemin UNC réseau \\172.16.20.103\Logiciels\MonApplication.msi.
  - (SCREEN)Activation de la stratégie système : Configuration ordinateur > Modèles d'administration > Système > Ouverture de session > Toujours attendre le réseau au démarrage de l'ordinateur.

- Test :
  - (SCREEN)Exécution de gpupdate /force /boot sur le poste client Windows 11.
  - (SCREEN)Redémarrage du poste client et vérification de la présence des logiciels