Compte Rendu Détaillé du Projet : Installation et Configuration d’un Poste Client Windows 10 et Jonction de Domaine

Date de rendu : 04/042025

Durée du projet : 3 jours (temps total passé pendant les heures d’école)

**1. Contexte et Objectifs**

Objectif principal : Intégrer un poste client Windows 10 dans un domaine Active Directory existant, en assurant la gestion des profils utilisateurs et des paramètres de sécurité conformément aux politiques de l’entreprise.

Livrables attendus :

- Poste client Windows 10 installé, configuré et joint au domaine.

- Profils utilisateurs centralisés (roaming ou via GPO).

- Sécurité renforcée (pare-feu, stratégies locales, chiffrement).

- Documentation technique et procédures.

Contraintes :

- Respect des normes de sécurité de l’entreprise.

- Compatibilité avec l’infrastructure existante (serveurs, réseaux).

**2. Méthodologie et Organisation**

2.1. Rôles de l’Équipe

- Chef de Projet : Axel (moi-même)

- Technicien Système : Axel (moi-même)

- Administrateur Active Directory : Axel (moi-même)

- Responsable Sécurité : Axel (moi-même)

- Documentaliste : Axel (moi-même)

2.2. Outils Utilisés

- Microsoft Deployment Toolkit (MDT) : Déploiement automatisé de Windows 10.

- Active Directory Users and Computers (ADUC) : Création des comptes utilisateurs.

- Group Policy Management Console (GPMC) : Déploiement des stratégies de groupe.

- PowerShell : Scripts pour automatiser les configurations.

**3. Phases du Projet**

3.1. Phase 1 : Préparation (1h)

Objectif : Définir les besoins et préparer l’environnement.

Tâches réalisées :

- Vérification des spécifications matérielles : Compatibilité Windows 10 (CPU 1 GHz, RAM 4 Go, espace disque 64 Go).

- Préparation de l’image Windows 10 avec MDT : Intégration des drivers, mises à jour.

- Création d’un compte de service dans Active Directory pour la jonction au domaine.

- Rédaction d’un plan de test : Vérification de la connectivité réseau, des GPO.

3.2. Phase 2: Installation de Windows 10 (2h)

Objectif : Installer et configurer le système d’exploitation.

Tâches réalisées :

- Déploiement via MDT :

- Partitionnement du disque (système, données).

- Installation des pilotes manquants via DISM.

- Configuration initiale :

- Nom du poste : BTS-SIO2-PC01.

3.3. Phase 3 : Jonction au Domaine (1h)

Objectif : Intégrer le poste dans l’environnement Active Directory.

Tâches réalisées :

- Connexion au réseau d’entreprise : Configuration DNS (adresse du contrôleur de domaine).

- Jonction au domaine :

powershell

Add-Computer -DomainName "domaine.local" -Credential "domaine\admin" -Restart

- Vérification dans ADUC : Apparition du poste dans l’OU PostesClients.

3.4. Phase 4 : Gestion des Profils Utilisateurs (2h)

Objectif : Centraliser les profils et appliquer les restrictions.

Tâches réalisées :

- Stratégies de groupe (GPO) :

- Redirection des dossiers Documents/Desktop vers un serveur NAS.

- Activation des profils itinérants (roaming profiles).

- Restrictions : Désactivation du Panneau de configuration pour les utilisateurs standard.

- Script de connexion : Synchronisation des imprimantes réseau via PowerShell.

3.5. Phase 5 : Sécurité (2h)

Objectif : Renforcer la sécurité du poste client.

Tâches réalisées :

- Stratégies locales :

- Pare-feu Windows : Blocage des ports non essentiels (ex: 135-139, 445).

- Configuration de l’UAC (User Account Control) au niveau maximal.

- Antivirus : Déploiement de Microsoft Defender avec mise à jour hebdomadaire.

3.6. Phase 6 : Tests et Documentation (1h)

Objectif : Valider le fonctionnement et rédiger les guides.

Tâches réalisées :

- Tests fonctionnels :

- Connexion d’un utilisateur du domaine : Vérification du profil itinérant.

- Application des GPO : Test via `gpresult /r`.

- Documentation :

- Guide utilisateur : Accès au NAS, utilisation des imprimantes.

- Guide technique : Procédure de réinitialisation de mot de passe AD.

**4. Résultats et Livrables**

4.1. Poste Client Configuré

- Statut domaine : Vérifié via `systeminfo | findstr /B "Domain"`.

- Sécurité :

- BitLocker activé (TPM 2.0 requis).

- Rapport de sécurité : Aucune vulnérabilité critique (outil Microsoft Baseline Security Analyzer).

4.2. Documentation

- Fiche technique du poste : Spécifications matérielles, adresse IP, nom de domaine.

- Procédures de dépannage : Résolution des erreurs courantes (ex: DNS, GPO).

**5. Défis Rencontrés et Solutions**

- Problème : Échec de jonction au domaine (erreur "DNS name does not exist").

- Solution : Vérification des paramètres DNS (adresse du contrôleur de domaine).

- Problème : Lenteur des profils itinérants.

- Solution : Optimisation de la taille des profils (exclusion des fichiers temporaires).

**6. Bilan et Améliorations Futures**

- Points forts : Automatisation via MDT/PowerShell, conformité aux politiques de sécurité.

- Axes d’amélioration :

- Migration vers Windows 11 et déploiement via Autopilot.

- Mise en place d’une solution de sauvegarde locale (Veeam Agent).

**Annexes**

Annexe 1 : Capture d’écran Trello

Tableau Trello :

Légende : Suivi des tâches "Installation des pilotes", "Jonction au domaine".

Annexe 2 : Exemple de Stratégie de Groupe

GPO :

Légende : Stratégie de restriction d’accès au Panneau de configuration.

Annexe 3 : Script PowerShell pour la jonction au domaine

```powershell

# Joindre le domaine et redémarrer

Add-Computer -DomainName "domaine.local" -Credential (Get-Credential) -Restart

```

Équipe Projet

Membres : Axel