MIGRATION WINDOWS : DÉPLOIEMENT AUTOMATISÉ DES POSTES AVEC IVANTI

Identification

Titre de la mission : Migration Windows – Déploiement automatisé de postes via Ivanti
Période : du 07/05/2025 au 10/05/2025
Lieu de réalisation : Service Informatique – Eau de Paris

Encadrant : Administrateur systèmes et postes de travail

Nature de l'activité

Contexte

Dans le cadre d'un projet global de migration vers **Windows 11**, le service informatique a constaté que plusieurs postes, notamment les **modèles HP G6**, ne répondaient pas aux exigences matérielles de compatibilité (absence de **puce TPM 2.0**).
Afin d'assurer la continuité du service et la conformité du parc, il a été décidé de **remplacer et provisionner automatiquement** les postes non compatibles à l'aide de l'outil de gestion de parc **Ivanti Management Suite**.

Notion :

- **TPM (Trusted Platform Module)** : puce matérielle qui stocke de manière sécurisée les clés de chiffrement et garantit l'intégrité du système. Sans TPM 2.0, le système n'atteint pas le niveau de sécurité minimum exigé par Windows 11 et l'installation est refusée

- **Ivanti Management Suite** : suite logicielle de gestion de parc informatique permettant le provisioning, l'inventaire et la maintenance centralisée des postes.

Objectifs

- Identifier les postes incompatibles à la migration.
- Préparer et déployer de nouveaux postes via un **provisioning automatisé**.
- Intégrer ces postes dans le **domaine Active Directory (edp.net)** selon la politique AGDLP.
- Garantir la **traçabilité** et la **sécurisation** du matériel mis en production.

Notions :

- **Active Directory (AD)** est un service de gestion d'identités et d'accès développé par Microsoft, essentiel pour les administrateurs de réseaux dans les entreprises. Il permet de centraliser la gestion des utilisateurs, des ordinateurs, et d'autres objets au sein d'un réseau d'entreprise.

L'Active Directory sert avant tout à centraliser les données d'authentification et d'autorisation pour les utilisateurs et les machines dans un environnement Windows.

- **AGDLP** : La méthode AGDLP (**A**ccount, **G**lobal, **D**omain **L**ocal, **P**ermission) est une bonne pratique pour définir et gérer les accès aux ressources partagées dans un Active Directory.

Le principe est que chaque utilisateur soit relié à un ou des groupes globaux qui symbolisent les fonctions de chaque utilisateur. Chaque groupe global est ensuite relié à un ou plusieurs groupes locaux qui symbolisent le type d'accès aux ressources.
Et enfin chaque ressource (dossier, fichier, imprimante) se voit assigner des permissions vers les groupes locaux.

Lieu

Mission réalisée en entreprise, au sein du **pôle postes de travail** du service informatique.

Solutions envisageables

Solution 1 : Installation manuelle poste par poste

- **Avantages :** contrôle total de chaque poste, adaptation aux besoins utilisateurs.
- **Inconvénients :** temps de déploiement long, risque d'erreurs humaines, absence d'homogénéité logicielle.

Solution 2 : Déploiement automatisé via Ivanti

- **Avantages :** rapidité, standardisation des configurations, intégration automatique au domaine, traçabilité.
- **Inconvénients :** dépendance au réseau et au serveur Ivanti, nécessité de modèles de provisioning à jour.

Choix retenu :

La **solution automatisée via Ivanti** a été retenue pour garantir un **gain de temps significatif**, une **cohérence logicielle** et une **intégration automatisée** dans le système d'information.

Solution retenue

Conditions initiales

- Présence de postes HP G6 sous Windows 10 non compatibles avec Windows 11.
- Absence de puce TPM 2.0 empêchant l'installation.
- Nécessité de remplacer ces postes tout en conservant les paramètres réseau et la structure Active Directory.

Conditions finales

- Nouveaux postes HP G9 configurés via **PXE Boot (UEFI IPv4 Network)** et provisionnés automatiquement.
- Intégration dans l'Active Directory, renommage automatique (ex. : *BL12345*).
- Postes vérifiés, sécurisés (compte *adm_local* géré par LAPS), et mis à disposition des utilisateurs finaux.

Notions :

- Un **Environnement d'Exécution de Pré-Démarrage (PXE)** est une interface client-serveur qui permet aux ordinateurs d'un réseau d'être démarrés à partir d'un serveur.

Grâce au démarrage PXE, le système d'exploitation peut être directement chargé dans les ordinateurs à partir d'un serveur au lieu d'un CD ou d'un disque dur.

En outre, un environnement d'exécution de pré-démarrage peut garantir une installation plus rapide et plus transparente des systèmes d'exploitation sur les ordinateurs, facilitant ainsi le déploiement du système d'exploitation sur de nombreux ordinateurs.

- **IPv4 Network** : (Le protocole ipv4, ou Internet Protocol version 4, désigne une méthode standardisée pour organiser, adresser et acheminer les paquets d'information sur un réseau)

- **Firmware** : (appelé micrologiciel en français, est un programme informatique qui est intégré à un matériel électronique)

- **UEFI IPv4 Network** : option de démarrage réseau (PXE) utilisant le firmware UEFI et le protocole IPv4 pour installer un système d'exploitation à distance.

Outils utilisés

- **Ivanti Management Suite** : détection, provisioning, suivi des tâches.
- **Active Directory (Windows Server)** : intégration des postes et gestion des OU.
- **LAPS (Local Administrator Password Solution)** : rotation automatique du mot de passe administrateur local.
- **Matériels :** HP G9, réseau Ethernet dédié au provisioning.

Notions :

- **Unité d'Organisation (OU)** : est un conteneur spécial dans Active Directory qui peut contenir différents objets AD, tels que des utilisateurs, des groupes et des ordinateurs. Les OU sont utilisées pour organiser ces objets en conteneurs administratifs logiques, facilitant ainsi la gestion et l'application de stratégies spécifiques.

- Windows LAPS **(Local Administrator Password Solution)** : est une solution intégrée à Windows qui permet de gérer les mots de passe des comptes administrateurs locaux sur des machines jointes à un domaine Active Directory. Elle génère des mots de passe uniques, robustes et les stocke de manière sécurisée dans Active Directory, tout en assurant une rotation automatique pour renforcer la sécurité.

Conditions de réalisation

- **Matériels :** Postes HP (G6 → G9), serveurs Windows, switchs et prises réseaux configurés pour le provisioning.
- **Logiciels :** Ivanti Management Suite, Windows 11, outils bureautiques (Suite Office, Teams, GlobalProtect).
- **Durée totale :** 3 jours (dont 1 pour le déploiement effectif, sur une base de 10 postes à remplacer).
- **Contraintes :** disponibilité des utilisateurs, homogénéité des configurations, gestion sécurisée des comptes locaux, respect du calendrier de migration.

Réalisations effectuées

Dans le cadre du projet de migration vers Windows 11, j'ai pris en charge, de manière autonome, le **remplacement des postes non compatibles** avec les nouvelles exigences matérielles de Microsoft.
Grâce à **Ivanti Management Suite**, j'ai commencé par **identifier et lister les postes incompatibles**, en ciblant notamment les modèles **HP G6** dépourvus de **puce TPM 2.0**, indispensable à l'installation de Windows 11.
Cette incompatibilité étant confirmée par Ivanti lors de l'analyse du parc, j'ai ensuite **contacté individuellement les utilisateurs concernés** afin de planifier un rendez-vous pour le remplacement de leur poste.

Préparation et déploiement du poste

Une fois un poste compatible sélectionné (souvent un **HP G9**), j'ai procédé à son **provisioning automatique via le réseau**, à l'aide d'un **port Ethernet dédié** configuré pour le **PXE Boot (UEFI IPv4 Network)**.
Pour ce faire :

1. J'ai démarré le poste en appuyant sur la touche **F12**, puis choisi le **démarrage réseau UEFI N/W - IPv4 Network**.
2. Une authentification m'a été demandée sur le serveur Ivanti, avec les identifiants du **domaine edp.net** :
    - Domaine : edp
    - Nom d'utilisateur : adm_egu
    - Mot de passe : **********
3. J'ai ensuite sélectionné le modèle de déploiement :
   Public > 01-Bureautique > BUR - PRD - 00 - WW POSTES INDIVIDUELS.
4. Le **nom du poste** a été défini selon la convention interne :
    - Format : **BLXXXXX** (Bureautique Laptop)
    - Les chiffres correspondent à l'**identifiant matériel EDP** présent sur l'**étiquette QR code** apposée sur chaque équipement.

Cette étiquette, associée à la base d'inventaire du parc, permet de **tracer l'ensemble du matériel** depuis sa réception jusqu'à sa mise en production. Les numéros et QR codes sont **rattachés dans Ivanti** à la fiche du poste correspondant, ce qui facilite la gestion du patrimoine informatique et répond à la compétence **D1.1 – Recenser les ressources**.

Étapes du provisioning

Le **template Ivanti** utilisé pour le déploiement est structuré en **quatre grandes phases** :

1. **Pré-installation de l'OS** : effacement des partitions, préparation du disque.
2. **Installation de l'OS** : déploiement de Windows 11 depuis le serveur Ivanti.
3. **Post-installation** : ajout des pilotes, des logiciels bureautiques, intégration au domaine AD, renommage automatique, activation de LAPS

La durée moyenne du processus est de **30 à 40 minutes** par poste.

Intégration dans l'Active Directory

Une fois le déploiement terminé, le poste est automatiquement **ajouté dans l'OU "00-Préparation"** de l'**Active Directory** du domaine edp.net.
L'architecture AD repose sur la méthode **AGDLP** et comporte plusieurs **OU principales** :

- **00-Préparation** : postes nouvellement provisionnés.
- **01-Intégration** : comptes et machines de la DSI.
- **02-Recettes** : utilisateurs en contrat temporaire (CDD).
- **03-Production** : utilisateurs permanents (CDI).

Après validation du provisioning, le poste est déplacé dans l'OU appropriée selon le profil de l'utilisateur final.

Vérification et sécurisation

La validation du provisioning se fait de deux manières :

1. **Depuis Ivanti**, en consultant le rapport d'exécution de la tâche (succès ou échec d'actions).
2. **En local sur le poste**, via le compte administrateur local adm_local, pour vérifier la présence des logiciels essentiels (Office, Outlook, Teams, GlobalProtect…).

Concernant la sécurité du compte adm_local, celui-ci est **géré par la solution Windows LAPS (Local Administrator Password Solution)**.
Lorsqu'un poste est dans l'OU "00-Préparation", le mot de passe est commun et connu des techniciens.
Une fois déplacé dans une autre OU, **LAPS génère automatiquement un mot de passe unique et complexe**, stocké de manière sécurisée dans l'Active Directory. Ce mot de passe est **régulièrement régénéré (plusieurs fois par jour)**, garantissant ainsi la confidentialité et empêchant tout usage abusif du compte.

Mise en stock et attribution

Après validation complète, le poste est **rangé dans le stock informatique**, classé par **modèle (G7, G8, G9, etc.)**, puis **attribué à l'utilisateur** prévu.

En cas d’échec partiel du provisioning (par exemple, installation manquée d’un logiciel comptable), j’ai su :

- soit **relancer un déploiement**,
- soit effectuer une **installation manuelle temporaire**,
  avant de signaler le problème à un **administrateur poste de travail** pour correction du modèle Ivanti.

⚙ Compétences mobilisées

Bloc D1 – Gestion du patrimoine informatique

- **D1.1 – Recenser les ressources** : Identification des postes incompatibles à la migration via Ivanti, inventaire matériel et étiquetage QR code.
- **D1.2 – Gérer les habilitations** : Intégration des postes dans l’Active Directory, respect de la méthode AGDLP.
- **D1.4 – Assurer la continuité du service** : Déploiement automatisé et supervision du provisioning pour éviter les interruptions.

Bloc D5 – Mise à disposition de services

- **D5.1 – Réaliser les tests** : Contrôle de la réussite du provisioning via Ivanti et en local sur le poste.
- **D5.2 – Déployer un service** : Provisioning complet via PXE, intégration automatique au domaine.

Bloc D6 – Développement professionnel

- **D6.1 – S’approprier l’environnement d’apprentissage** : Découverte et utilisation professionnelle d’Ivanti et de LAPS.
- **D6.3 – Construire son identité professionnelle** : Travail en autonomie, respect des procédures et communication avec la DSI.

Conclusion

Cette mission m’a permis d’acquérir une vision complète du **cycle de vie d’un poste de travail**, de sa détection à sa mise en production.
J’ai développé mes compétences en **gestion de parc**, en **déploiement automatisé** et en **sécurisation des systèmes**, tout en comprenant l’importance de la traçabilité et de la standardisation.
Les principales difficultés rencontrées concernaient les **échecs ponctuels de**

provisioning et la **coordination avec les utilisateurs**. Ces obstacles ont été surmontés par des vérifications manuelles et un dialogue constant avec l'équipe de support.

Évolutions possibles

- Automatiser davantage la détection et la planification du remplacement des postes via des **rapports Ivanti dynamiques**.
- Documenter et diffuser une **procédure de provisioning simplifiée** à destination des nouveaux techniciens.