**Introduction**

Contexte du projet

Ce projet a été réalisé dans le cadre de l’épreuve E6 du BTS SIO (option SISR). Il vise à démontrer la capacité à concevoir, déployer et administrer une infrastructure réseau complète sous Windows Server. Le projet porte principalement sur la mise en place d’un contrôleur de domaine Active Directory (AD DS), d’un serveur WSUS pour la gestion centralisée des mises à jour, et d’un serveur DHCP pour l’attribution automatique des adresses IP.

Objectif du projet

* Mettre en place un contrôleur de domaine (AD DS) sous Windows Server 2016.
* Intégrer un poste client Windows 10 au domaine.
* Appliquer des stratégies de groupe (GPO) pour la gestion des utilisateurs et des permissions.
* Déployer un serveur WSUS pour administrer les mises à jour Windows.
* Installer et configurer un serveur DHCP pour automatiser la gestion des adresses IP.
* Assurer la communication réseau entre les machines et sécuriser l’environnement

**Fiche de réalisation n°1 : Mise en place d’Active Directory**

Objectif

L’objectif de cette réalisation est d’installer et configurer un contrôleur de domaine permettant de gérer centralement les utilisateurs et les ressources d’un réseau d’entreprise.

Étapes réalisées

1. **Installation de Windows Server 2016**
   * Téléchargement et installation de Windows Server sur VirtualBox.
   * Configuration initiale du serveur (Nom, IP statique, Workgroupe).
2. Ajout du rôle Active Directory Domain Services (AD DS)
   * Installation du rôle AD DS via le gestionnaire de serveur.
   * Promotion du serveur en tant que contrôleur de domaine.
   * Création du domaine ayant pour nom DomainFictif.local
3. Création et gestion des utilisateurs
   * Ajout d’un administrateur de domaine et de plusieurs utilisateurs.
   * Création de groupes de sécurité et affectation des utilisateurs.
4. Application des stratégies de groupe (GPO)
   * Configuration des stratégies de mot de passe et de sécurité.
   * Restriction de l’accès à certaines fonctionnalités via les GPO.
   * Application des stratégies sur les OU correspondantes.
5. Test et validation
   * Vérification de l’authentification des utilisateurs sur le domaine.
   * Test des restrictions et paramètres définis dans les GPO

Résultats obtenus

Un contrôleur de domaine fonctionnel avec une gestion centralisée des utilisateurs.

Une configuration réseau permettant la communication entre le serveur et les clients.

Des stratégies de groupe appliquées avec succès pour la sécurisation des accès.

Fiche de réalisation n°2 : Déploiement et configuration de WSUS

Objectif

Mettre en place un serveur WSUS (Windows Server Update Services) afin de gérer et contrôler la distribution des mises à jour Windows sur le réseau.

Étapes réalisées

1. **Installation de WSUS**
   * Ajout du rôle WSUS via le Gestionnaire de serveur.
   * Choix d’une base de données interne pour le stockage des mises à jour.
   * Configuration initiale du service et premier démarrage.
2. **Configuration du service WSUS**
   * Définition des produits et classifications des mises à jour (Windows 10, Windows Server 2016, mises à jour critiques et de sécurité).
   * Planification de la synchronisation automatique avec les serveurs Microsoft Update.
3. **Approbation et distribution des mise à jour**
   * Mise en place d’une politique d’approbation automatique des mises à jour critiques et de sécurité.
   * Création de groupes d’ordinateurs pour mieux gérer la distribution des mises à jour.
4. **Configuration des postes clients via GPO**
   * Mise en place d’une stratégie de groupe pour forcer les clients à passer par le service WSUS.
   * Configuration de l’URL du serveur WSUS (<https://serveur-wsus:8530>).
5. **Test et validation**
   * Vérification de la communication des clients avec le serveur WSUS.
   * Test du téléchargement des mises à jour.

Résultats obtenus

Un serveur WSUS opérationnel avec une gestion optimisée du stockage des mises à jour.

Une stratégie de mise à jour centralisée appliquée aux postes clients.

Une réduction de la consommation de la bande passante sur le réseau

Fiche de réalisation n°3 : Installation et configuration du serveur DHCP

Objectif

Mettre en place un serveur DHCP pour attribuer dynamiquement des adresses IP aux machines clientes et éviter la configuration manuelle des IP.

Étapes réalisées

1. **Installation du rôle DHCP**
   * Ajout du rôle DHCP via le Gestionnaire de serveur.
   * Configuration de l’autorisation DHCP sur le domaine.
2. **Création de la plage d’adresses DHCP**
   * Définition d’une plage d’adresse IP (10.0.2.100 à 10.0.2.200).
   * Attribution de la passerelle et des serveurs DNS aux clients DHCP.
3. **Test et validation**
   * Vérification que les machines clientes reçoivent bien une adresse IP dynamique.
   * Tests de connectivité avec le serveur AD et WSUS.

Résultats obtenus

Un serveur DHCP opérationnel permettant la distribution automatique des adresses IP.

Une réduction des erreurs de configuration manuelle.

Une infrastructure plus facile à gérer.

Conclusion et perspectives

Bilan du projet

Ce projet m’a permis de mettre en pratique plusieurs compétences essentielles en administration système et réseau. La mise en place d’un contrôleur de domaine Active Directory a facilité la gestion centralisée des utilisateurs et des ressources du réseau. Ensuite, la configuration des stratégies de groupe (GPO) a permis de sécuriser et d’optimiser la gestion des postes clients.

L’implémentation d’un serveur WSUS a contribué à la centralisation et à l’optimisation de la gestion des mises à jour Windows. Enfin, l’installation et la configuration d’un serveur DHCP ont permis d’automatiser l’attribution des adresses IP aux machines clientes, simplifiant ainsi l’administration du réseau.

Grâce à ces différentes étapes, une infrastructure réseau fonctionnelle et évolutive a été mise en place, garantissant à la fois la stabilité, la sécurité et la facilité d’administration.

Améliorations possibles

Pour aller plus loin et améliorer encore l’infrastructure, plusieurs pistes d’optimisation pourraient être envisagées :

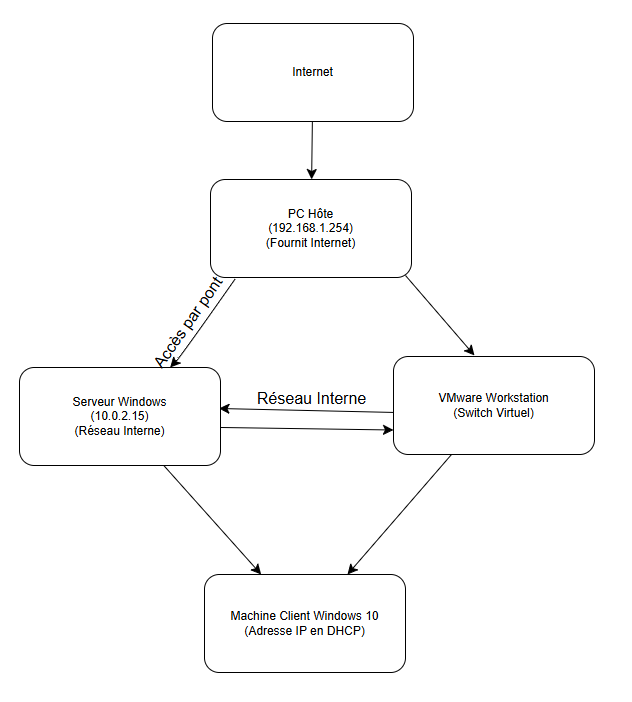
* Mise en place d’un VPN : Cette solution permettrait d’autoriser des connexions sécurisées à distance pour les utilisateurs externes ou en télétravail.
* Ajout d’une solution de supervision et d’analyse réseau : L’intégration d’un outil comme PRTG Network Monitor permettrait de surveiller les performances du réseau, tandis que Wireshark offrirait une analyse détaillée du trafic pour détecter d’éventuels problèmes de communication ou de sécurité.
* Optimisation de la gestion des utilisateurs : Une automatisation plus poussée des stratégies de groupe pourrait être mis en place afin de renforcer la gestion des accès et la sécurisation des ressources.

En conclusion, ce projet constitue une base solide pour la gestion d’un réseau d’entreprise et pourrait être évolutif en fonction des besoins futurs de l’infrastructure.

Annexes

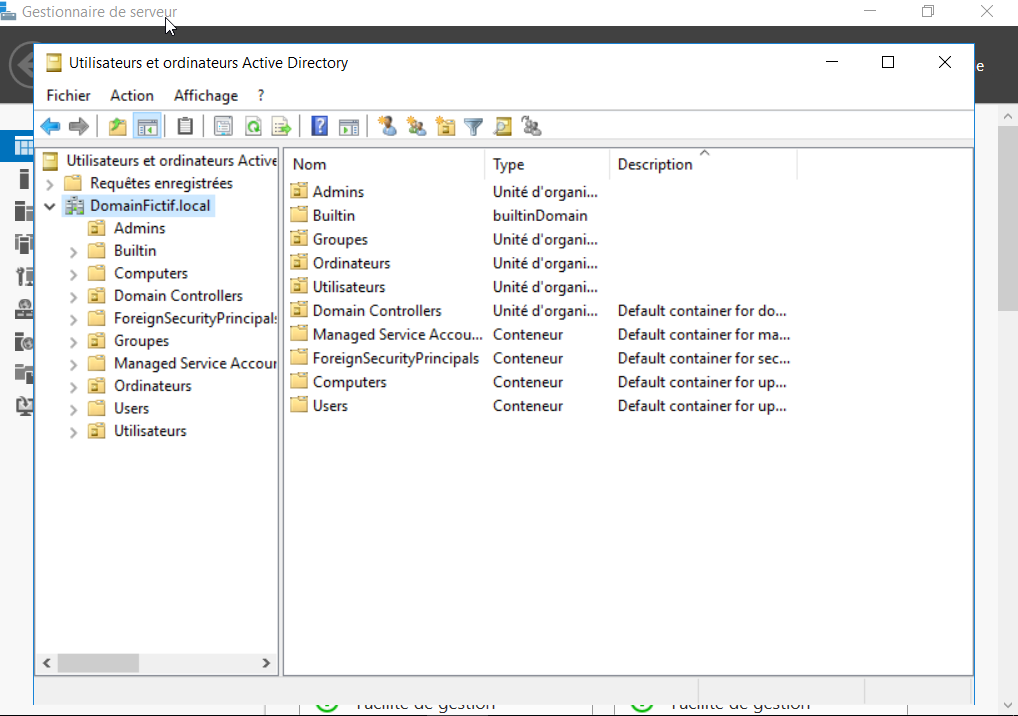
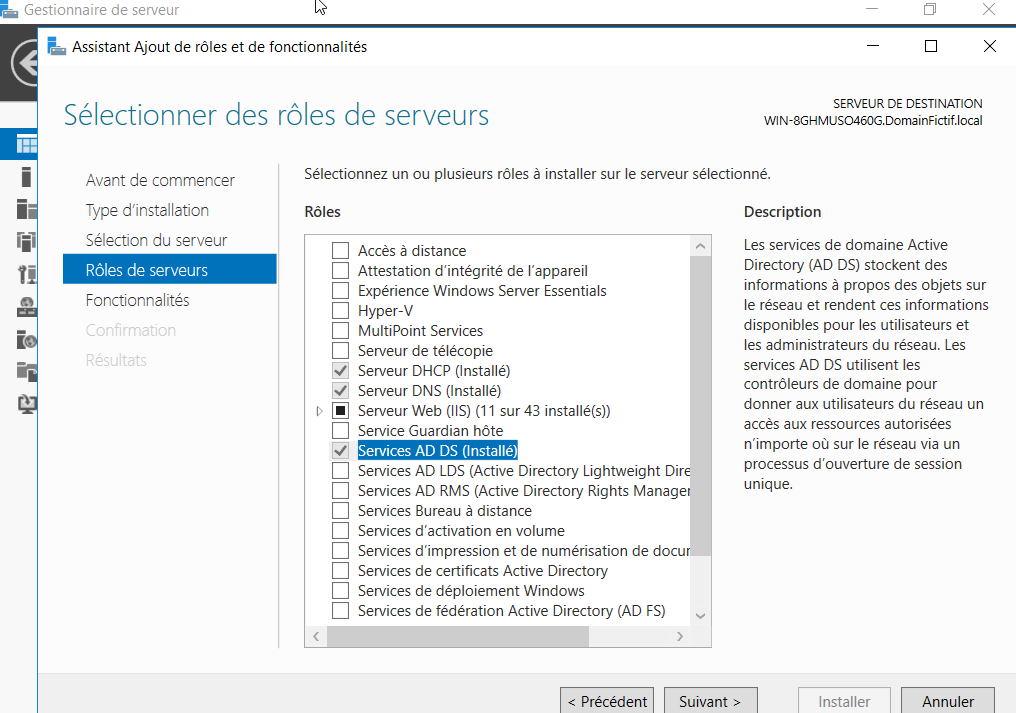
Annexe 1 : Schéma réseau

Le schéma ci-dessous illustre l’architecture réseau mis en place, incluant le serveur Windows, le poste client Windows 10 et la gestion via le logiciel de virtualisation VirtualBox.



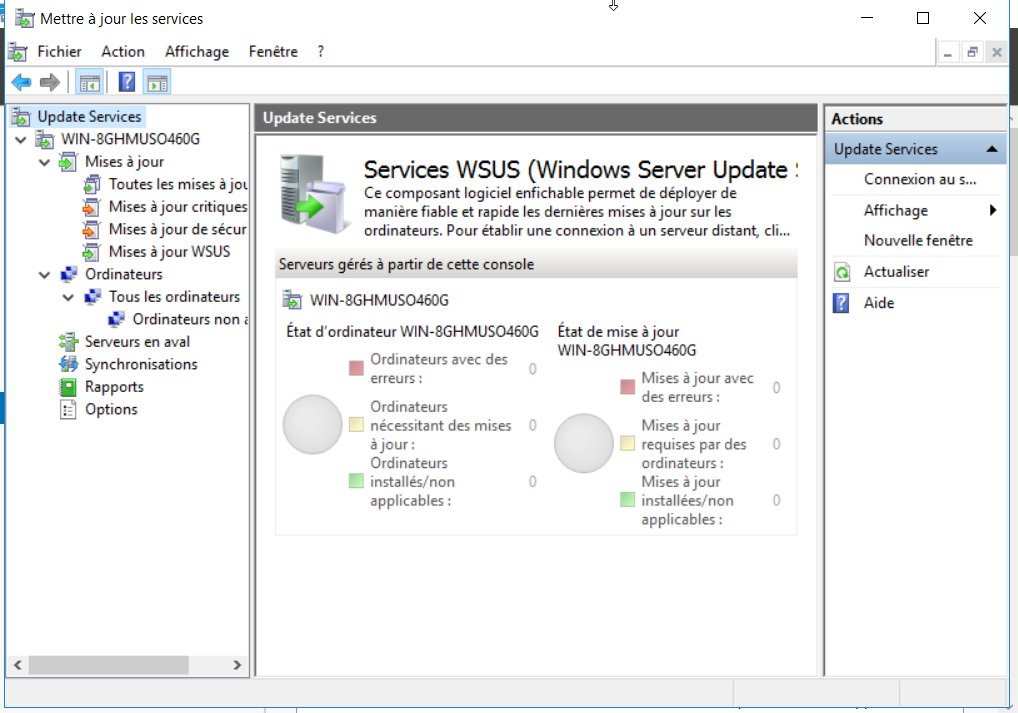
Annexe 2: Configuration Active Directory (AD DS)

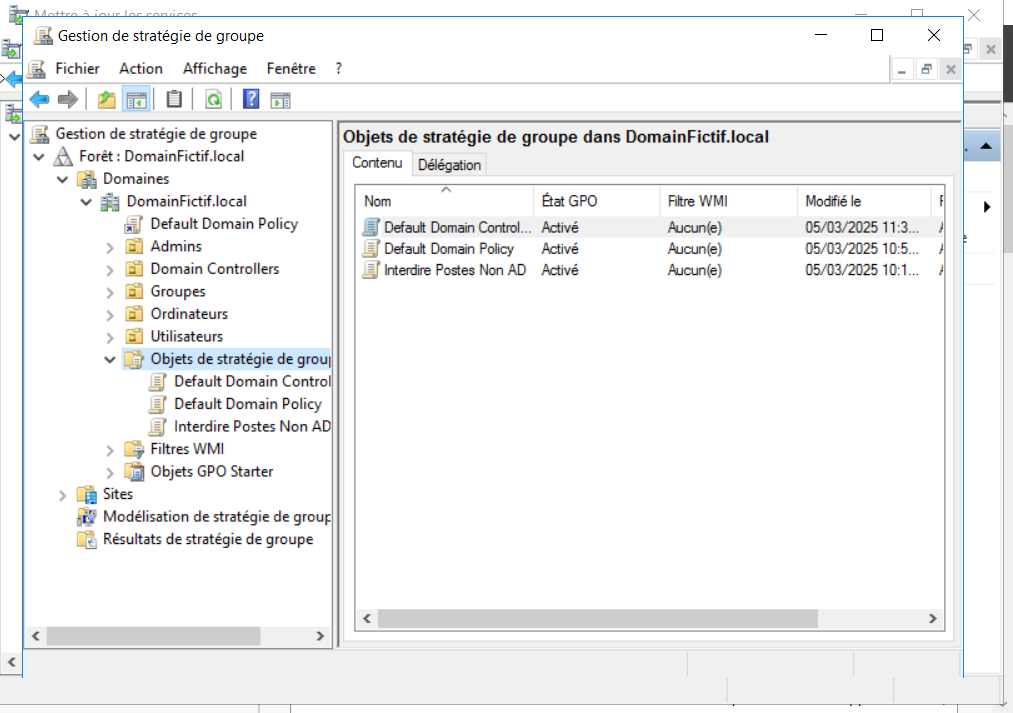
Cette annexe présente les étapes clés de l’installation et de la configuration d’Active Directory sur le serveur Windows Serveur 2016.



Annexe 3: Configuration WSUS

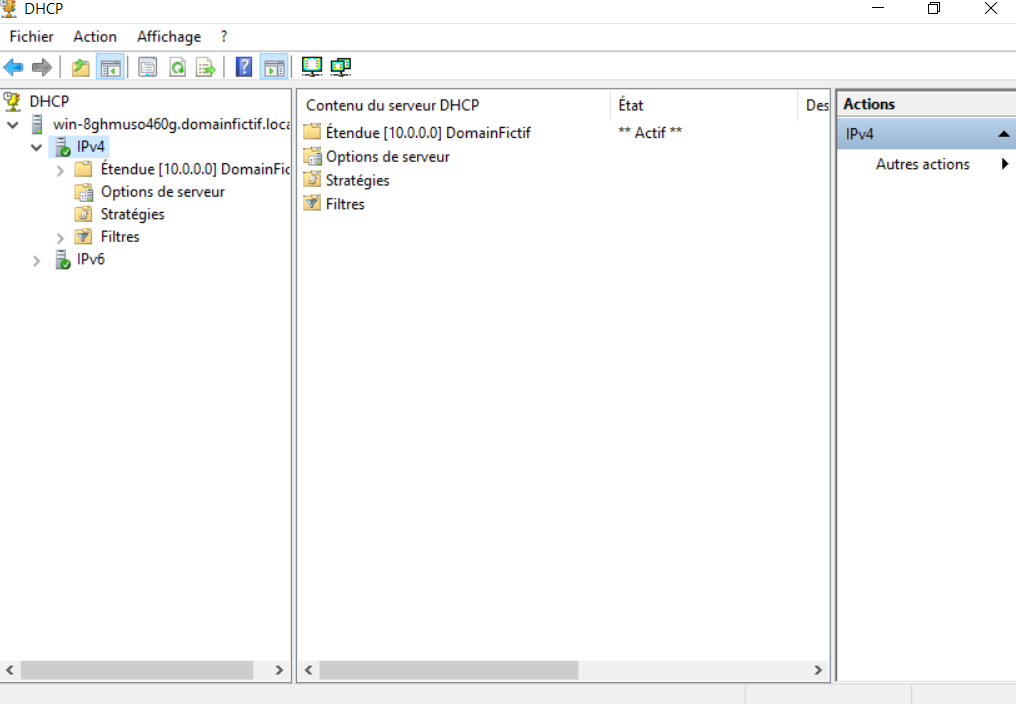
Cette annexe décrit la mise en place du serveur WSUS et la gestion des mises à jour des postes clients via Group Policy Object (GPO).





Annexe 4: Configuration DHCP

Détails de la mise en place du serveur DHCP et de la distribution automatique des adresses IP.



Annexe 5 : Paramètrage des strategies de groupes (GPO)

Tableau des stratégies de groupe appliquées pour sécuriser et gérer le réseau.

|  |  |
| --- | --- |
| Stratégie | Objectif |
| Restriction des accès à certains panneaux | Sécuriser les postes clients |
| Configuration WSUS via GPO | Automatiser les mises à jour des machines clients |
| Application d’une politique de renouvellement des mots de passe | Forcer les utilisateurs à changer régulièrement leur mot de passe pour renforcer la sécurité |

Annexe 6 : Commandes réseaux utilisées

Liste des principales commandes utilisées pour vérifier le bon fonctionnement du réseau.

|  |  |
| --- | --- |
| Commande | Description |
| Ipconfig /all | Affiche la configuration IP |
| Ping [adresse IP] | Teste la connexion vers un hôte |
| Netstat -an | Affiche les ports ouverts |
| Gpupdate /force | Applique immédiatement les stratégies de groupe |
| Nslookup [nom du domaine] | Vérifie la résolution DNS |

Annexe 7 : Mots de passe

Mot de passe admin du Windows Server 2016 :

MadatedenaissanceC2001.

Mot de passe du compte Admin IT :

@Azerty246810

Mot de passe de tous les utilisateurs :

Matija92.

Mot de passe local Windows 10 Pro :

Matija92.