Projet d'infrastructure pour MedSearch

Conception, mise en œuvre et justification technique

Évaluation pratique 4MCSA

Client	MedSearch
Livrable	Rapport Projet d'infrastructure pour MedSearch

Participants :

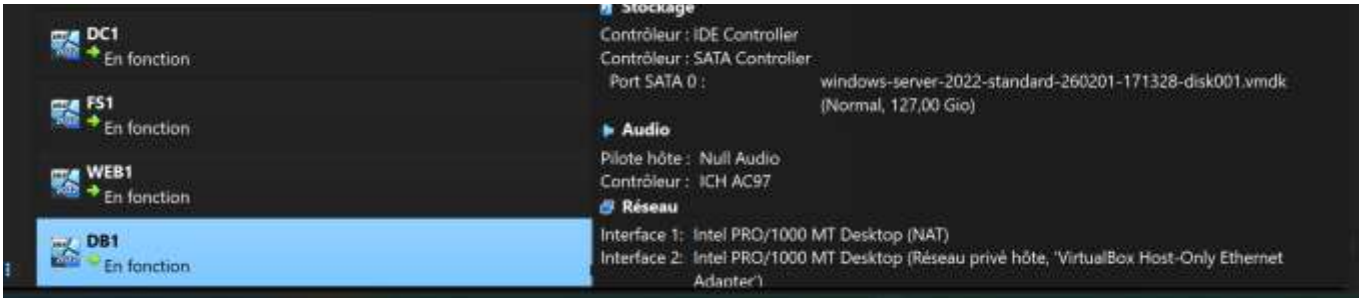
Participant
- MEVENGUE FRANCK
- Lilia Halfaoui
- Aweni Idmanth Karimou

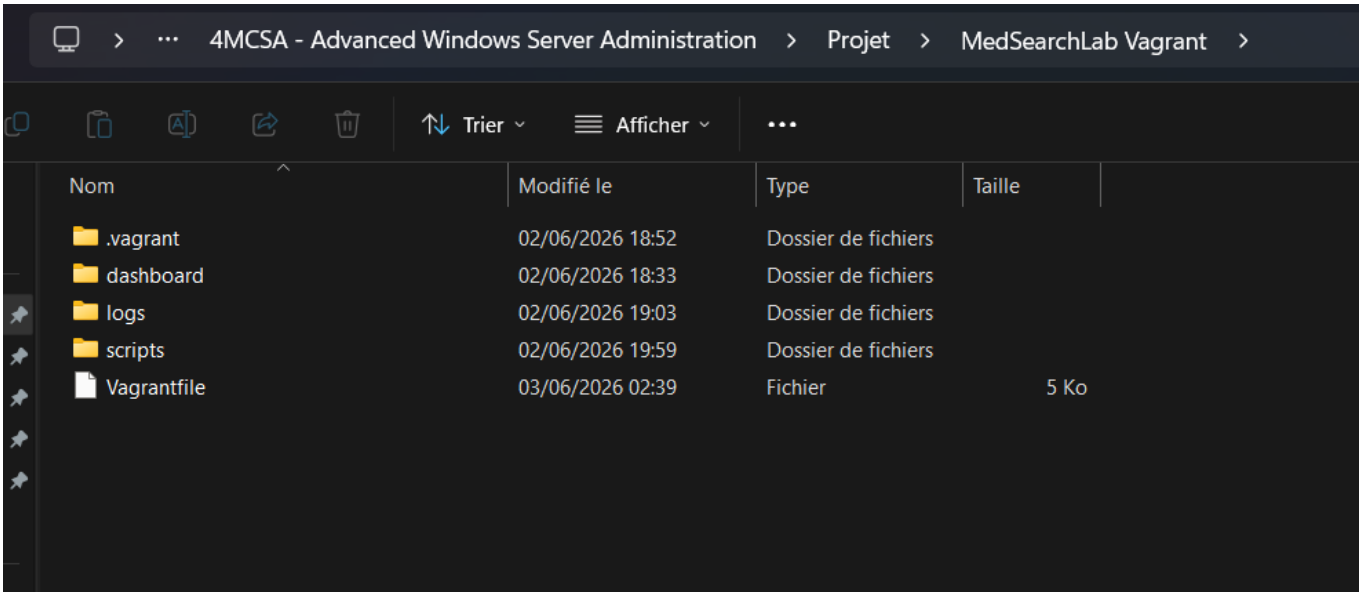
Sommaire :

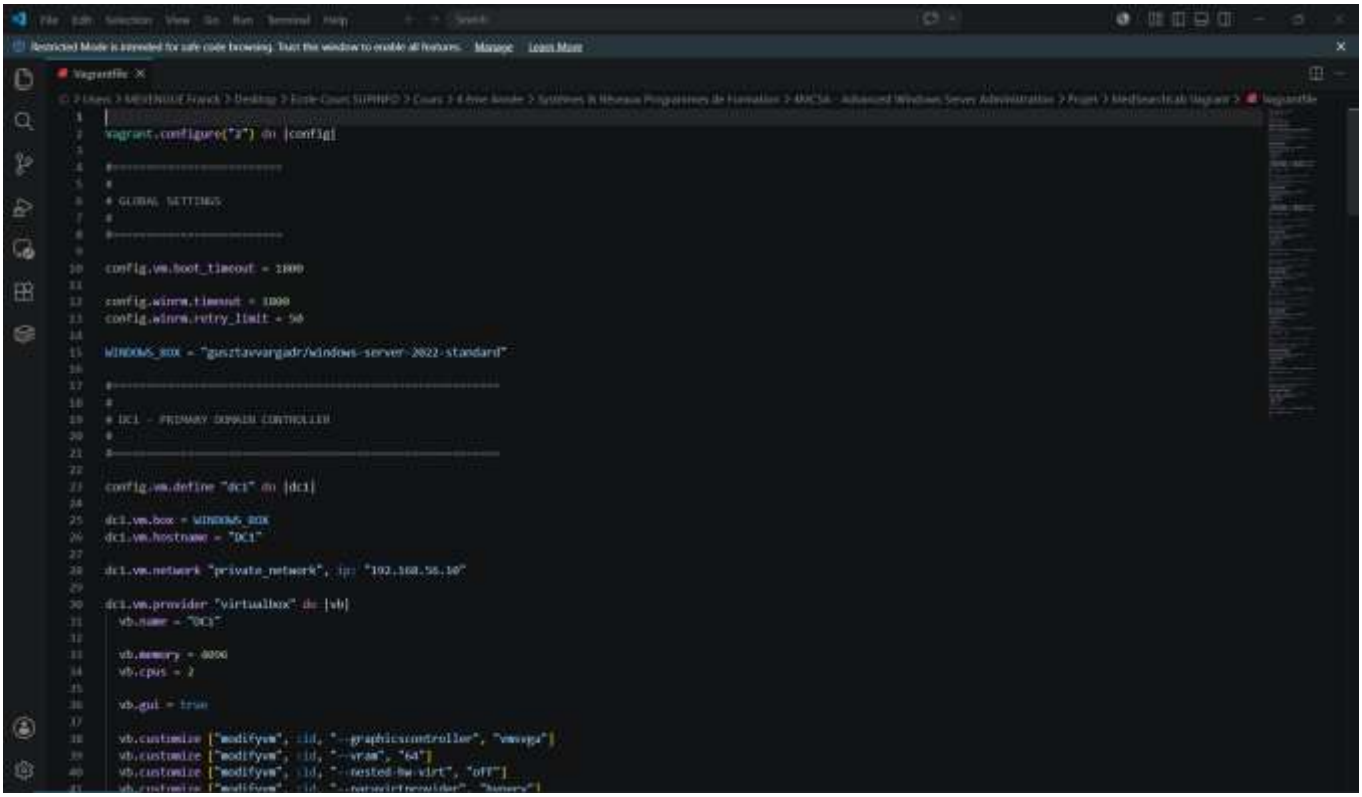
INTRODUCTION :

Le projet MedSearch consiste à concevoir et mettre en œuvre une infrastructure Microsoft centralisée capable de répondre aux besoins d'une entreprise manipulant des données sensibles et nécessitant une administration simplifiée, sécurisée et évolutive.

L'infrastructure a été déployée dans un environnement virtualisé reposant sur Oracle VirtualBox et automatisé grâce à Vagrant et PowerShell. Cette approche permet de reproduire rapidement l'environnement, standardiser les configurations et réduire les opérations manuelles d'administration.







L’objectif principal du projet est de fournir un socle d’infrastructure cohérent autour des technologies Microsoft suivantes :

- Active Directory Domain Services
- DNS
- Stratégies de groupe (GPO)
- Partage de fichiers SMB
- Administration centralisée
- Gestion des utilisateurs et groupes
- Supervision
- Portail web IIS
- Services d’entreprise (WSUS, SQL, DFS)

L’architecture repose sur plusieurs machines virtuelles spécialisées :

- DC1 : contrôleur de domaine principal
- FS1 : serveur de fichiers

- WEB1 : serveur IIS et portail MedSearch
- DB1 : serveur SQL
- WSUS1 : gestion centralisée des mises à jour
- MONITOR1 : supervision et monitoring
- CLIENT1 / CLIENT2 : postes utilisateurs

Le projet met particulièrement l'accent sur :

- L'automatisation de l'infrastructure
- La centralisation de l'administration
- La sécurité via les GPO
- La gestion des accès
- La reproductibilité de l'environnement

Contrairement à une infrastructure configurée manuellement, l'utilisation de Vagrant permet de déployer rapidement les machines virtuelles avec leurs paramètres réseau, leurs ressources matérielles et leurs scripts de configuration PowerShell.

Le document ne se limite pas à une présentation théorique : il décrit les choix techniques réalisés, les configurations réellement mises en place, les démonstrations effectuées ainsi que les bénéfices apportés à une entreprise de type MedSearch.

1. Contexte et besoins :

MedSearch possède plusieurs postes utilisateurs et doit centraliser ses ressources informatiques afin d'améliorer :

- La sécurité des données
- La gestion des utilisateurs
- Le partage des fichiers
- L'administration système
- La supervision de l'infrastructure

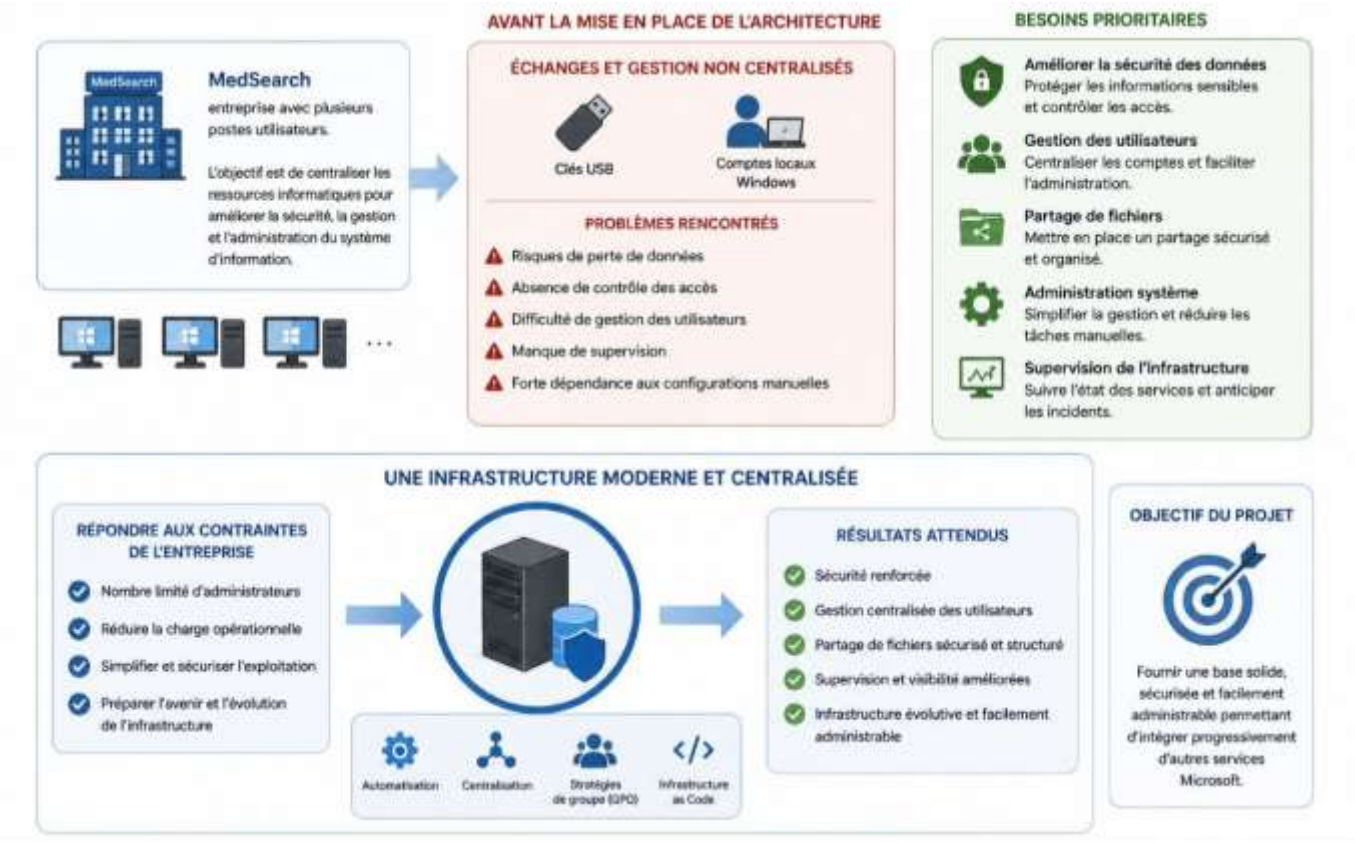
Avant la mise en place de cette architecture, les échanges de données reposaient principalement sur des méthodes non centralisées comme les clés USB ou les comptes locaux Windows, ce qui entraînait plusieurs problèmes :

- Risques de perte de données
- Absence de contrôle des accès
- Difficulté de gestion des utilisateurs
- Manque de supervision
- Forte dépendance aux configurations manuelles

L'entreprise ayant un nombre limité d'administrateurs, l'infrastructure devait également réduire la charge opérationnelle quotidienne grâce à :

- L'automatisation
- La centralisation
- Les stratégies de groupe
- L'Infrastructure as Code

Le projet devait donc fournir une base solide, sécurisée et facilement administrable permettant d'intégrer progressivement d'autres services Microsoft.



2. Architecture cible :

L’architecture retenue repose sur un environnement virtualisé utilisant VirtualBox comme hyperviseur et Vagrant comme outil d’automatisation du déploiement.

Chaque rôle d’infrastructure est isolé dans une machine virtuelle dédiée afin de respecter les bonnes pratiques d’administration Microsoft et simplifier :

- La maintenance
- La supervision
- Les mises à jour
- Les tests
- L’évolution future de l’infrastructure

L’ensemble des machines communique via un réseau privé VirtualBox utilisant le plan d’adressage :

192.168.56.0/24

Cette segmentation permet d’isoler l’environnement MedSearch du réseau physique de l’hôte tout en conservant une communication complète entre les serveurs et les postes clients.

Les principales machines virtuelles prévues dans l’architecture sont :

VM	**Rôle**	**Adresse IP**
DC1	Contrôleur de domaine Active Directory	192.168.56.10
FS1	Serveur de fichiers SMB	192.168.56.20
WEB1	Serveur IIS / portail web	192.168.56.30
DB1	Serveur SQL Server	192.168.56.40
WSUS1	Gestion des mises à jour	192.168.56.50
MONITOR1	Supervision infrastructure	192.168.56.60
CLIENT1	Poste utilisateur domaine	192.168.56.101
CLIENT2	Poste utilisateur domaine	192.168.56.102

L’architecture mise en place repose sur plusieurs principes importants :

- Centralisation des identités avec Active Directory
- Contrôle des accès via groupes AD
- Automatisation avec Vagrant et PowerShell
- Partage sécurisé via SMB et permissions NTFS
- Application automatique des politiques de sécurité via GPO
- Supervision centralisée
- Préparation à l’intégration de services IIS, WSUS, DFS et SQL

L’ensemble de l’infrastructure a été pensé afin de reproduire une architecture réaliste de niveau entreprise tout en restant compatible avec les contraintes matérielles d’un environnement de laboratoire académique.

Afin de séparer proprement les rôles et de simplifier les mises à jour ou les remplacements.

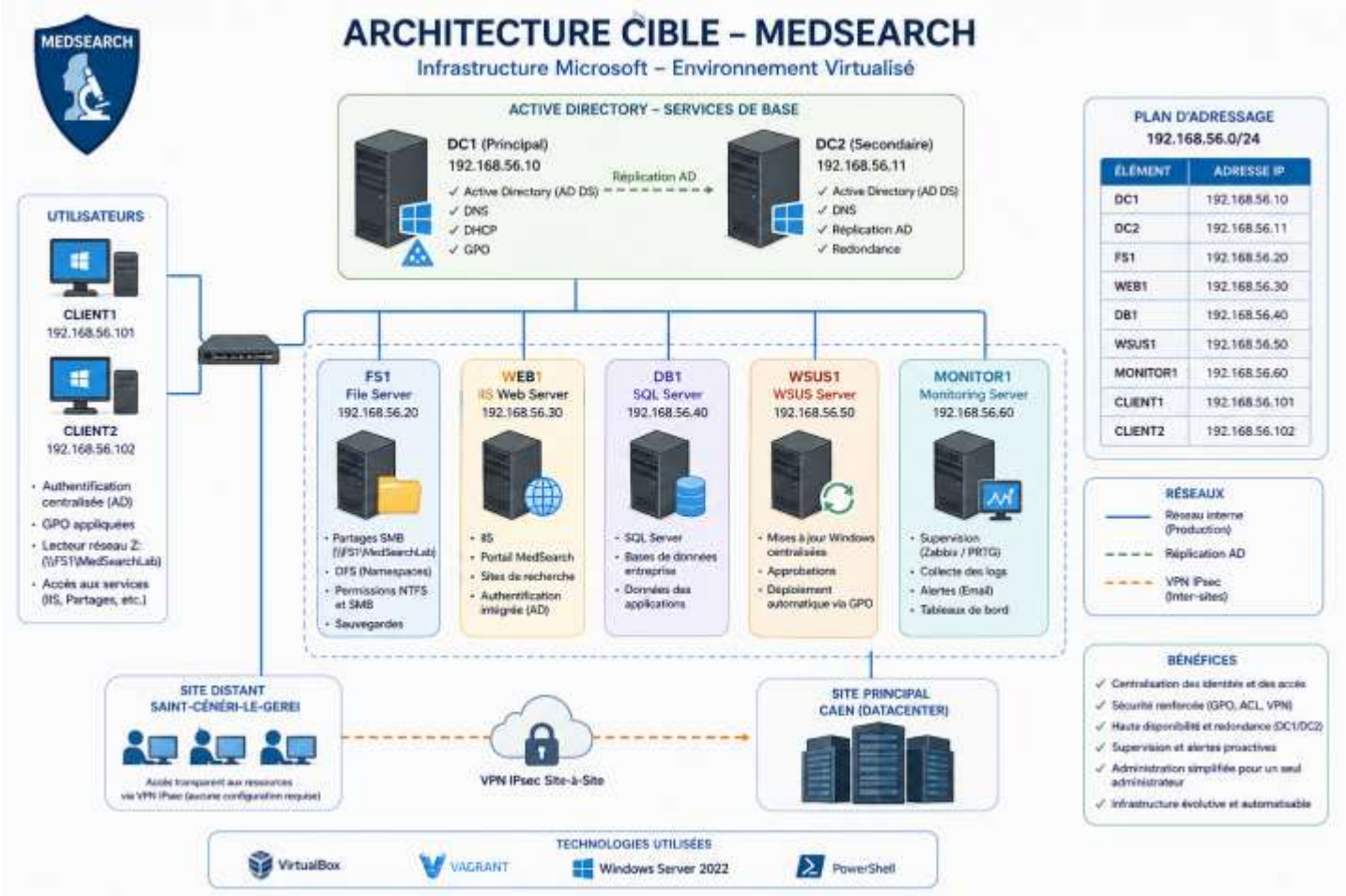


Figure 1 — Schéma global de l'architecture MedSearch

2.1 Segmentation réseau :

L'infrastructure MedSearch repose sur une segmentation logique du réseau afin d'améliorer :

- la sécurité
- l'isolation des services
- les performances
- la supervision des flux
- la facilité d'administration

Même dans un environnement virtualisé sous VirtualBox, cette approche reproduit les bonnes pratiques utilisées dans les infrastructures d'entreprise.

La séparation des flux permet notamment d'éviter qu'un problème sur un service impacte l'ensemble du système d'information.

Réseau / Segment	Fonction	Contrôle / Sécurité	Commentaires
Management	Administration des serveurs et accès administrateur	Comptes administrateurs dédiés, accès restreints, PowerShell distant	Utilisé pour la maintenance, Vagrant, WinRM et l'administration centralisée
Production	Hébergement des services métiers et machines virtuelles	Contrôle des accès via Active Directory et GPO	Contient les serveurs DC1, FS1, WEB1, DB1, WSUS1 et MONITOR1
File Services	Partages SMB et accès fichiers	Permissions NTFS + SMB, groupes AD	Sécurisation des accès utilisateurs aux ressources partagées
Clients	Postes utilisateurs du domaine	Authentification centralisée, GPO de sécurité	CLIENT1 et CLIENT2 utilisent les services du domaine MedSearchLab.local
Inter-services	Communications entre serveurs	Filtrage logique et résolution DNS interne	Flux entre AD, DNS, IIS, SQL, WSUS et supervision
Inter-sites (prévu)	Communication entre sites distants	VPN IPsec avec chiffrement et authentification forte	Permettrait la connexion sécurisée entre Caen et Saint-Cénéri

Réseau privé VirtualBox

L'ensemble des machines virtuelles communique via un réseau privé VirtualBox :

192.168.56.0/24

Ce réseau interne permet :

- l'isolation complète du laboratoire MedSearch
- la communication entre les serveurs
- les tests d'infrastructure
- la simulation d'un environnement entreprise

Adressage IP principal :

Machine	Adresse IP	Rôle
DC1	192.168.56.10	Contrôleur de domaine Active Directory
FS1	192.168.56.20	Serveur de fichiers SMB
WEB1	192.168.56.30	Serveur IIS
DB1	192.168.56.40	SQL Server
WSUS1	192.168.56.50	Gestion des mises à jour
MONITOR1	192.168.56.60	Supervision infrastructure
CLIENT1	192.168.56.101	Poste utilisateur
CLIENT2	192.168.56.102	Poste utilisateur

Intérêt de la segmentation

Cette organisation réseau apporte plusieurs avantages :

Sécurité

Les services critiques sont isolés logiquement afin de limiter les risques de propagation d'incidents.

Performance

Les flux d'administration, de fichiers et de production sont séparés afin d'éviter les congestions réseau.

Administration simplifiée

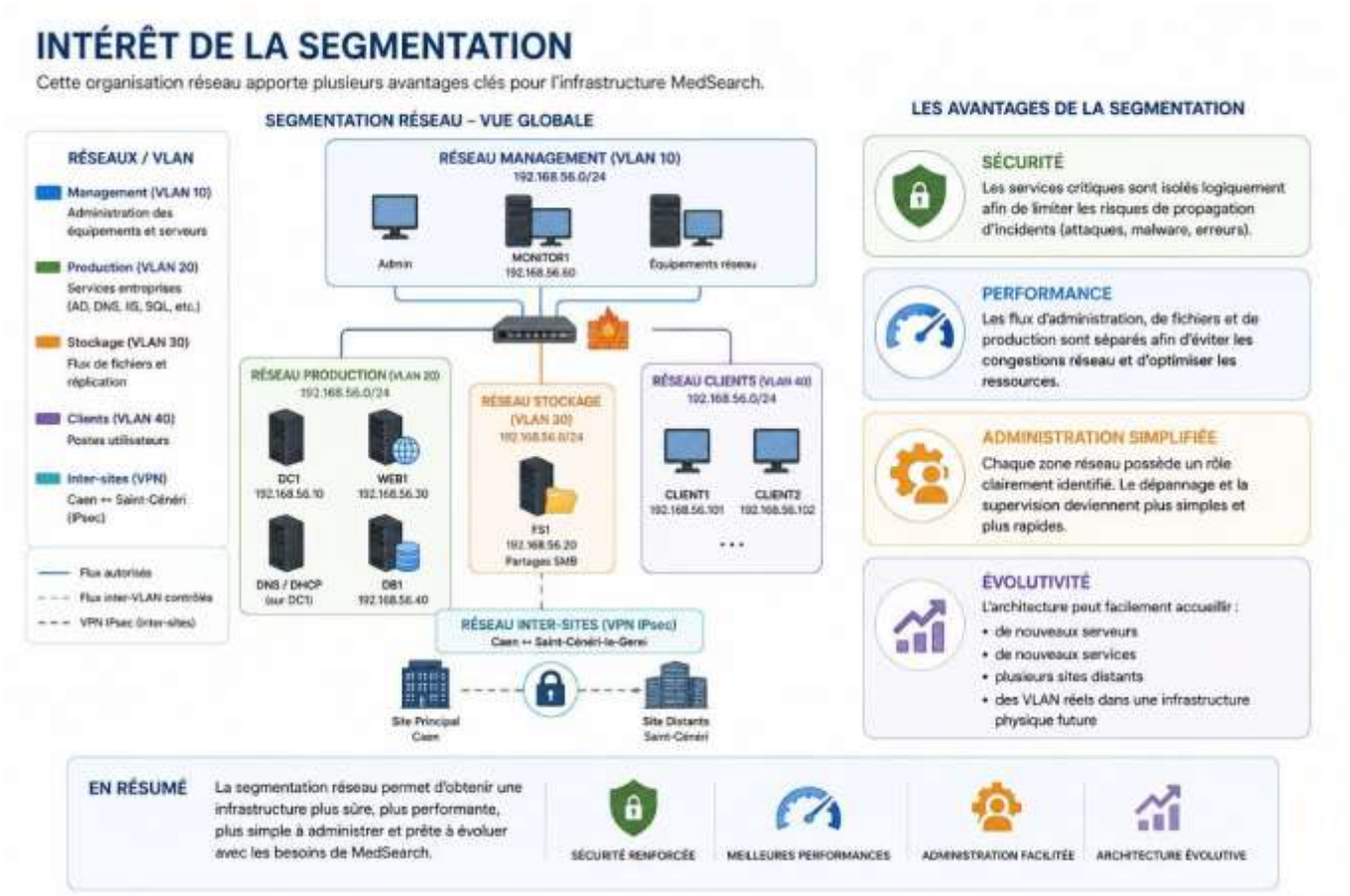
Chaque zone réseau possède un rôle clairement identifié, ce qui facilite le dépannage et la supervision.

Évolutivité

L'architecture peut facilement accueillir :

- de nouveaux serveurs
- de nouveaux services

- plusieurs sites distants
- Des VLAN réels dans une infrastructure physique future



3. Rôles et composants principaux :

L'infrastructure MedSearch repose sur une architecture virtualisée composée de plusieurs machines virtuelles Windows Server spécialisées.

L'environnement a été déployé avec :

- Oracle VirtualBox comme hyperviseur
- Vagrant pour l'automatisation du déploiement
- PowerShell pour le provisioning et l'administration

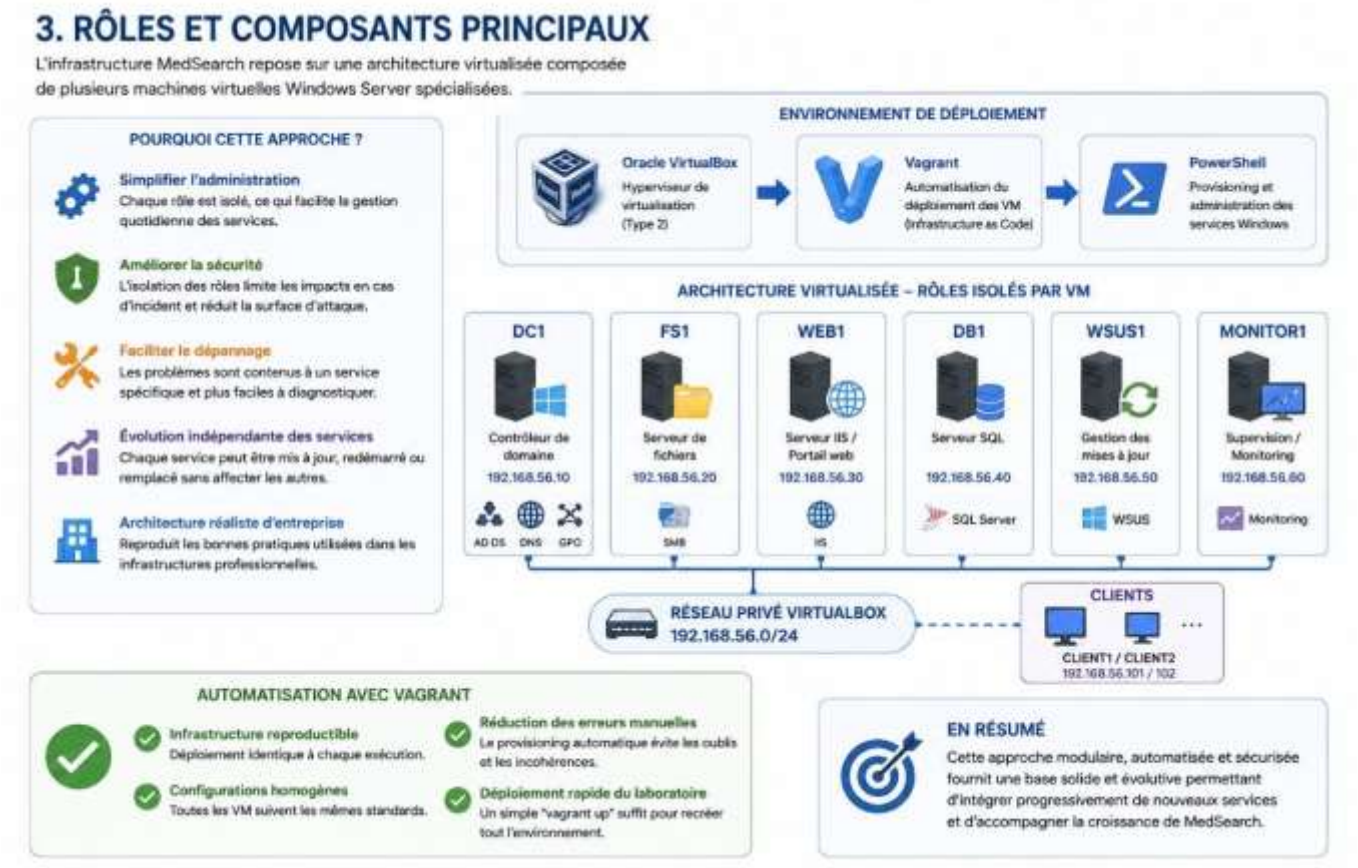
Cette approche permet d'éviter une architecture monolithique où tous les services seraient installés sur une seule machine.

Chaque rôle est isolé dans une VM dédiée afin de :

- Simplifier l'administration
- Améliorer la sécurité
- Faciliter le dépannage
- Permettre une évolution indépendante des services
- Reproduire une architecture réaliste de niveau entreprise

Les machines virtuelles sont automatiquement configurées grâce à Vagrant, ce qui garantit :

- Une infrastructure reproductible
- Des configurations homogènes
- Une réduction des erreurs manuelles
- Un déploiement rapide du laboratoire



3.1 Socle d'infrastructure :

Le socle principal de l'infrastructure repose sur plusieurs serveurs spécialisés communiquant via le réseau privé VirtualBox 192.168.56.0/24.

Les contrôleurs de domaine, le serveur de fichiers et les services d'administration centralisée constituent le cœur du système d'information MedSearch.

L'environnement a été pensé afin de pouvoir intégrer progressivement d'autres services Microsoft comme IIS, WSUS, SQL Server, DFS ou encore la supervision centralisée.

Composant	Rôle	Administration / disponibilité	Point clé
DC1 — Active Directory / DNS	Authentification centralisée, gestion des utilisateurs, résolution DNS	Administration centralisée via PowerShell et GPO	Socle principal du domaine MedSearchLab.local
FS1 — File Server	Partage SMB et stockage centralisé	Gestion des permissions NTFS et SMB	Accès sécurisé aux ressources partagées
GPO	Application automatique des politiques de sécurité	Déploiement centralisé via Active Directory	Sécurisation homogène des postes et serveurs
Vagrant	Déploiement automatisé des VM	Infrastructure as Code	Réduction des opérations manuelles
PowerShell	Administration et automatisation	Scripts de provisioning et gestion AD	Industrialisation des tâches d'administration
IIS (prévu)	Hébergement du portail MedSearch	VM dédiée WEB1	Centralisation des services web
WSUS (prévu)	Gestion centralisée des mises à jour	Déploiement automatique via GPO	Sécurisation et conformité Windows
SQL Server (prévu)	Hébergement des bases applicatives	VM DB1 dédiée	Centralisation des données métiers
Monitoring (prévu)	Supervision infrastructure	Collecte d'événements et alertes	Visibilité globale du SI

Active Directory et services de domaine

Le contrôleur de domaine DC1 constitue le cœur de l'infrastructure.

Les services déjà mis en place incluent :

- Active Directory Domain Services
- DNS
- gestion des utilisateurs
- gestion des groupes
- organisation via OU
- stratégies de groupe (GPO)

Le domaine :

medsearchlab.local

Permet de centraliser :

- l'authentification
- les permissions
- les politiques de sécurité
- l'administration des postes et serveurs

Les utilisateurs et groupes ont été créés directement via PowerShell afin d'automatiser l'administration du domaine.

Capture 1 — Vérification du domaine AD

Capture 2 - Utilisateur Franck créé

```
PS C:\Users\vagrant> Get-ADUser

cmdlet Get-ADUser at command pipeline position 1
Supply values for the following parameters:
(Type !? for Help.)
Filter: *


DistinguishedName : CN=Administrator,CN=Users,DC=medsearchlab,DC=local
Enabled           : True
GivenName         :
Name              : Administrator
ObjectClass       : user
ObjectGUID        : 46279fb3-2c9d-44a7-a4c3-51af81a8ba8f
SamAccountName    : Administrator
SID               : S-1-5-21-589369152-2961588623-2958806467-500
Surname           :
UserPrincipalName :

DistinguishedName : CN=Guest,CN=Users,DC=medsearchlab,DC=local
Enabled           : False
GivenName         :
Name              : Guest
ObjectClass       : user
ObjectGUID        : 9887faca-381e-4ee0-b693-836f8154e96f
SamAccountName    : Guest
SID               : S-1-5-21-589369152-2961588623-2958806467-501
Surname           :
UserPrincipalName :

DistinguishedName : CN=vagrant,CN=Users,DC=medsearchlab,DC=local
Enabled           : True
GivenName         :
Name              : vagrant
ObjectClass       : user
ObjectGUID        : a082c4e1-33b5-4eb1-9fdf-c1bf1c809281
SamAccountName    : vagrant
SID               : S-1-5-21-589369152-2961588623-2958806467-1000
Surname           :
UserPrincipalName :

DistinguishedName : CN=krbtgt,CN=Users,DC=medsearchlab,DC=local
Enabled           : False
GivenName         :
Name              : krbtgt
ObjectClass       : user
```

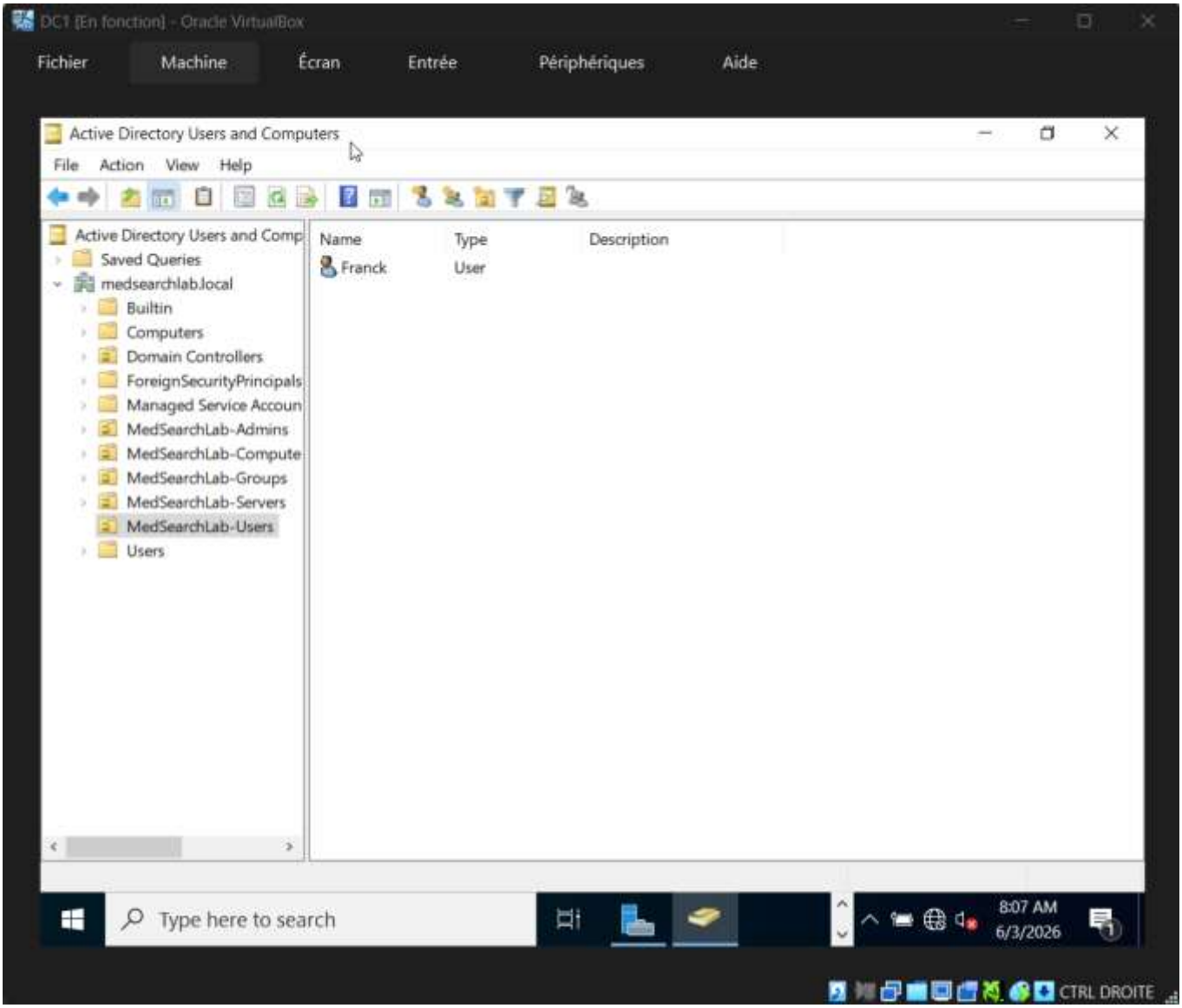
```
DistinguishedName : CN=Franck,OU=MedSearchLab-Users,DC=medsearchlab,DC=local
Enabled           : True
GivenName         : Franck
Name              : Franck
ObjectClass       : user
ObjectGUID        : 7bd29b1d-0a35-4593-ad08-5b281ac561bf
SamAccountName    : franck
SID               : S-1-5-21-589369152-2961588623-2958806467-1105
Surname           : Mevengue
UserPrincipalName : franck@medsearchlab.local
```

Capture 3 - Groupe FileServer-Users

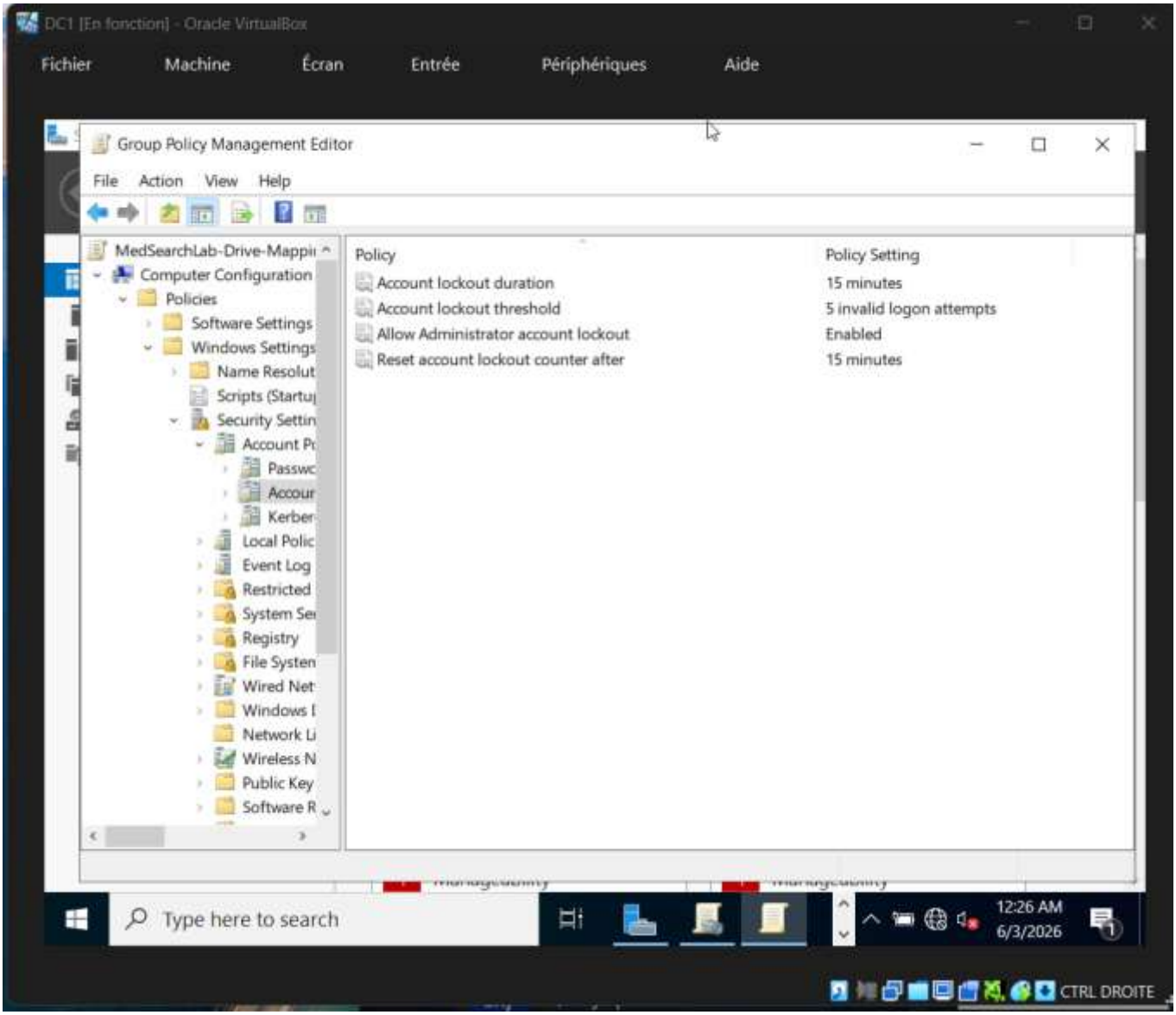
```
PS C:\Users\vagrant> Get-ADGroupMember "FileServer-Users"


distinguishedName : CN=vagrant,CN=Users,DC=medsearchlab,DC=local
name              : vagrant
objectClass       : user
objectGUID        : a082c4e1-33b5-4eb1-9fdf-c1bf1c809281
SamAccountName    : vagrant
SID               : S-1-5-21-589369152-2961588623-2958806467-1000

distinguishedName : CN=Franck,OU=MedSearchLab-Users,DC=medsearchlab,DC=local
name              : Franck
objectClass       : user
objectGUID        : 7bd29b1d-0a35-4593-ad08-5b281ac561bf
SamAccountName    : franck
SID               : S-1-5-21-589369152-2961588623-2958806467-1105
```

Capture 4 - Groupe FileServer-Users

```
PS C:\Users\vagrant> Get-ADGroupMember "FileServer-Users"


distinguishedName : CN=vagrant,CN=Users,DC=medsearchlab,DC=local
name              : vagrant
objectClass       : user
objectGUID        : a082c4e1-33b5-4eb1-9fdf-c1bf1c809281
SamAccountName    : vagrant
SID               : S-1-5-21-589369152-2961588623-2958806467-1000

distinguishedName : CN=Franck,OU=MedSearchLab-Users,DC=medsearchlab,DC=lo
name              : Franck
objectClass       : user
objectGUID        : 7bd29b1d-0a35-4593-ad08-5b281ac561bf
SamAccountName    : franck
SID               : S-1-5-21-589369152-2961588623-2958806467-1105
```



Capture 5 - Group Policy Management




```
PS C:\Users\vagrant> net accounts
Force user logoff how long after time expires?:       Never
Minimum password age (days):                          1
Maximum password age (days):                          42
Minimum password length:                              7
Length of password history maintained:                24
Lockout threshold:                                    Never
Lockout duration (minutes):                           10
Lockout observation window (minutes):                 10
Computer role:                                        PRIMARY
The command completed successfully.

PS C:\Users\vagrant>
```

Serveur de fichiers FS1

Le serveur FS1 fournit un espace de stockage partagé accessible via SMB.

Le partage :

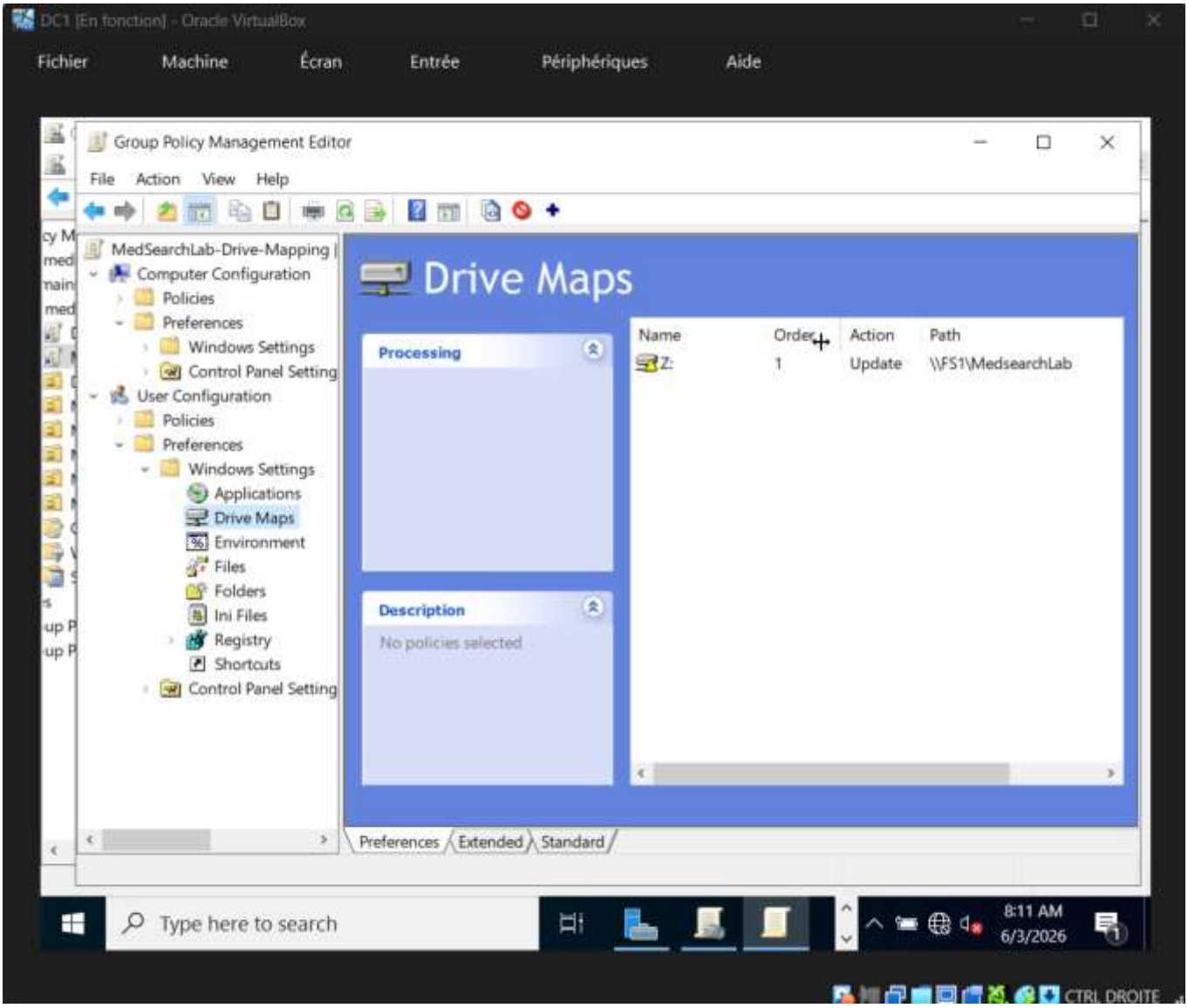
\FS1\MedSearchLab

A été sécurisé grâce :

- aux permissions SMB
- aux permissions NTFS
- aux groupes Active Directory

Le lecteur réseau Z: est automatiquement monté via GPO afin de simplifier l’accès utilisateur.

Cette approche reproduit le fonctionnement d’un serveur de fichiers d’entreprise centralisé.



Capture 6 – SMB Share

```
PS C:\Users\vagrant> Get-SmbShare

Name     ScopeName Path                                        Description
----     --------- ----                                        -----------
ADMIN$   *         C:\Windows                                  Remote Admin
C$       *         C:\                                         Default share
IPC$     *                                                     Remote IPC
NETLOGON *         C:\Windows\SYSVOL\sysvol\medsearchlab.local\SCRIPTS Logon server share
SYSVOL   *         C:\Windows\SYSVOL\sysvol                    Logon server share
```

Capture 7 – Drive Mapping

```
PS C:\Users\vagrant> net use
New connections will be remembered.


Status       Local     Remote                    Network

-------------------------------------------------------------------------------
Disconnected Z:        \\FS1\MedSearchLab        Microsoft Windows Network
The command completed successfully.
```

Automatisation de l'infrastructure

L'un des objectifs majeurs du projet était de réduire les opérations manuelles d'administration.

L'infrastructure est donc automatisée grâce à :

Vagrant

Vagrant permet :

- le déploiement automatique des VM
- la configuration réseau
- le paramétrage des ressources VirtualBox
- l'exécution des scripts de provisioning

PowerShell

PowerShell a été utilisé pour :

- joindre les machines au domaine
- créer les utilisateurs Active Directory
- créer les groupes
- configurer les partages SMB
- appliquer les permissions NTFS
- automatiser l'administration système

Cette approche correspond aux pratiques modernes d'Infrastructure as Code utilisées dans les environnements professionnels.

3.2 Déploiement rapide des sites IIS :

L'infrastructure MedSearch a été conçue afin de permettre le déploiement rapide et standardisé de services web internes.

L’objectif est de simplifier la création de nouveaux sites IIS tout en limitant les opérations manuelles de configuration.

Dans le projet, cette approche repose principalement sur :

- VirtualBox pour la virtualisation
- Vagrant pour le déploiement automatisé
- PowerShell pour l’installation et la configuration des rôles Windows
- IIS pour l’hébergement des applications et portails internes

Standardisation des serveurs web

Le serveur WEB1 est prévu comme plateforme d’hébergement centralisée pour :

- Le portail MedSearch
- Les interfaces d’administration
- Les tableaux de supervision
- Les services ASP.NET internes

Grâce à l’automatisation mise en place avec Vagrant, une nouvelle VM IIS peut être créée rapidement avec :

- Une configuration réseau prédéfinie
- Une adresse IP fixe
- Un nom d’hôte standardisé
- L’intégration automatique au domaine
- L’installation automatique des rôles Windows nécessaires

Cette approche réduit fortement les risques d’erreur humaine et améliore la reproductibilité de l’infrastructure.

Déploiement automatisé

Le provisioning PowerShell permet d’automatiser :

- L’installation du rôle IIS
- L’ouverture des règles firewall

- La création des sites web
- La configuration DNS
- Les paramètres de sécurité IIS

L'administrateur peut ainsi déployer rapidement un nouveau service web avec un minimum d'interventions manuelles.

Avantages pour l'entreprise

Gain de temps

Les nouveaux services peuvent être mis en ligne rapidement sans reconfigurer manuellement chaque serveur.

Standardisation

Toutes les VM IIS utilisent la même configuration de base, ce qui simplifie :

- La maintenance
- Les mises à jour
- La supervision
- Le dépannage

Évolutivité

L'infrastructure peut facilement accueillir :

- De nouveaux portails web
- Des applications internes
- Des tableaux de bord de supervision
- Des API métiers

3.3 Supervision et journalisation :

La supervision constitue un élément essentiel de l'infrastructure MedSearch.

L'objectif n'est pas de mettre en place une plateforme complexe difficile à maintenir, mais une supervision claire, centralisée et immédiatement exploitable par l'administrateur.

L'architecture prévoit donc :

- La collecte centralisée des événements Windows
- La supervision des performances
- La détection des incidents
- L'affichage synthétique de l'état des serveurs

Objectifs de la supervision :

Le système de monitoring doit permettre :

- D’identifier rapidement les pannes
- De surveiller les performances des serveurs
- De centraliser les événements critiques
- D’améliorer la réactivité de l’administration
- De fournir une visibilité globale de l’infrastructure

Cette approche est particulièrement importante dans le contexte MedSearch où un nombre limité d’administrateurs supervise l’ensemble du système d’information.

Infrastructure de supervision prévue :

Le serveur MONITOR1 est destiné à centraliser :

- Les alertes
- Les journaux Windows
- Les indicateurs système
- Les données de disponibilité

Les outils envisagés incluent :

- Windows Event Forwarding (WEF)
- Zabbix

Données surveillées :

Donnée surveillée	Source	Seuil / événement	Action
CPU / RAM serveurs	Zabbix	Dépassement prolongé	Génération d'alerte
Journaux Windows	Event Viewer / WEF	Warning / Critical	Historisation et affichage
Disponibilité services	Ping / tests applicatifs	Service inaccessible	Signalement dans le portail
IIS / SMB / AD	Vérification applicative	Échec de réponse	Alerte supervision
Incidents multiples	Corrélation événements	Plusieurs anomalies simultanées	Escalade prioritaire

Journalisation centralisée :

La centralisation des événements permet :

- D'éviter la consultation manuelle de chaque serveur
- D'améliorer le diagnostic des incidents
- De conserver un historique des événements critiques
- D'identifier rapidement les problèmes récurrents

Les logs critiques peuvent ensuite être exploités par le portail de supervision MedSearch.

Figure 2 — Flux de supervision et d'escalade du portail de santé

3.4 Portail web de santé des serveurs :

Le projet MedSearch prévoit la mise en place d'un portail web centralisé permettant à l'administrateur de visualiser rapidement l'état global de l'infrastructure.

Ce portail répond directement au besoin de supervision demandé dans le cahier des charges.

Objectifs du portail

Le portail doit fournir :

- une vue synthétique de l'état des serveurs
- les derniers événements critiques

- l'état des services importants
- les indicateurs de disponibilité
- un accès rapide aux informations techniques

Le portail est prévu pour être hébergé sur IIS via le serveur WEB1.

Fonctionnement prévu

Le portail consomme les informations collectées par :

- les outils de monitoring
- les journaux Windows
- les tests de disponibilité
- les indicateurs système

L'ensemble des données est ensuite affiché dans une interface web centralisée accessible depuis le réseau interne.

Tableau de bord principal

Bloc du portail	Contenu affiché	Utilité
Vue globale	État des serveurs (vert / orange / rouge)	Lecture immédiate de l'infrastructure
Historique événements	Derniers événements Warning / Critical	Diagnostic rapide
Supervision services	État IIS, AD, SMB, DNS	Vérification des services critiques
Indicateurs système	CPU, RAM, disponibilité	Analyse des performances
Escalade	Génération d'alertes ou tickets	Réaction rapide aux incidents

Intérêt pour l'administration

Cette centralisation permet :

- de gagner du temps
- de réduire les diagnostics manuels
- d'améliorer la visibilité du SI

- de simplifier le suivi des incidents

3.5 Administration distante et accès sécurisés :

L'administration distante constitue un élément fondamental de l'architecture MedSearch.

L'objectif est de permettre une gestion centralisée des serveurs tout en limitant l'exposition des services sensibles.

Administration centralisée

Les serveurs sont principalement administrés via :

- PowerShell
- WinRM
- Vagrant
- Outils Microsoft RSAT
- Active Directory

Cette approche réduit la dépendance aux interfaces graphiques et facilite l'automatisation.

Sécurisation des accès

L'infrastructure prévoit plusieurs mécanismes de sécurité :

- Authentification Active Directory
- Comptes administrateurs dédiés
- Contrôle des accès via groupes AD
- GPO de sécurité
- Segmentation réseau logique

L'objectif est d'éviter l'exposition directe des services d'administration.

Évolutions prévues

L'architecture pourra intégrer ultérieurement :

- RRAS
- VPN IPsec
- RDS Gateway
- Bastion d’administration

Afin de sécuriser davantage les accès distants entre plusieurs sites.

3.6 Communication inter-sites :

L’architecture MedSearch a été pensée pour pouvoir évoluer vers plusieurs sites géographiques.

Le scénario étudié prévoit notamment une communication sécurisée entre :

- Caen
- Saint-Cénéri-le-Gerei

VPN site-à-site IPsec

La communication inter-sites doit reposer sur un tunnel VPN IPsec permettant :

- Le chiffrement des flux
- L’authentification sécurisée
- La protection des données
- L’accès transparent aux ressources internes

Les utilisateurs accèdent ainsi aux services comme s’ils étaient présents sur le réseau local principal.

Services concernés

Le VPN doit permettre l’accès sécurisé à :

- Active Directory
- DNS
- Partages SMB
- IIS

- Supervision
- Bases SQL

DFS et accès unifiés

L'utilisation de DFS Namespace permettra de présenter :

- Un chemin unique
- Une arborescence centralisée
- Une simplification de l'accès utilisateur

Exemple :

\medsearchlab.local\Documents

Cette approche masque la complexité réelle de l'infrastructure aux utilisateurs.

Évolutivité de l'architecture

Même si le VPN inter-sites n'a pas été entièrement déployé dans le laboratoire VirtualBox actuel, l'architecture réseau et les services Active Directory ont été pensés pour permettre cette extension future.

4. Automatisation de l'infrastructure :

Le déploiement de l'infrastructure MedSearch a été pensé de manière progressive afin de stabiliser le socle système avant d'ajouter les services applicatifs.

L'objectif est de garantir :

- La cohérence de l'infrastructure
- La stabilité des services
- La simplicité d'administration
- la reproductibilité des déploiements

Dans le cadre du laboratoire, l'ensemble de l'environnement repose principalement sur :

- VirtualBox pour la virtualisation

- Vagrant pour l'automatisation du déploiement
- PowerShell pour la configuration des rôles Windows
- Windows Server 2022 pour les services d'infrastructure

Cette approche permet de reproduire rapidement l'environnement complet à partir d'un simple Vagrantfile.

Séquence de déploiement :

Étape	Action	Résultat attendu
1	Déploiement automatisé des VM avec Vagrant	Infrastructure VirtualBox opérationnelle
2	Configuration réseau privée 192.168.56.0/24	Communication inter-VM fonctionnelle
3	Installation et promotion du contrôleur de domaine DC1	Domaine Active Directory opérationnel
4	Mise en place DNS et Active Directory	Résolution de noms et authentification centralisée
5	Déploiement et intégration du serveur FS1	Serveur de fichiers joint au domaine
6	Création des utilisateurs, groupes et OU	Organisation logique de l'infrastructure
7	Configuration des partages SMB et permissions NTFS	Gestion sécurisée des accès fichiers
8	Déploiement des GPO de sécurité	Application automatique des politiques
9	Mise en place du Drive Mapping	Montage automatique du lecteur réseau Z:
10	Préparation des serveurs WEB1, DB1, WSUS1 et MONITOR1	Extension future de l'infrastructure
11	Déploiement du portail IIS MedSearch	Centralisation des services web
12	Intégration monitoring et supervision	Supervision globale des serveurs

Déploiement automatisé avec Vagrant :

L'un des éléments les plus importants du projet est l'automatisation complète de l'infrastructure.

Le Vagrantfile permet :

- De créer automatiquement les VM
- D'attribuer les ressources matérielles
- De configurer les cartes réseau
- De lancer les scripts PowerShell
- De standardiser les configurations

Cette approche correspond aux pratiques modernes d'Infrastructure as Code (IaC).

Infrastructure actuellement opérationnelle

Malgré les contraintes matérielles du poste de travail, plusieurs éléments critiques ont été entièrement mis en place et validés :

DC1 — Contrôleur de domaine

Fonctions déployées :

- Active Directory
- DNS
- GPO
- Gestion centralisée des utilisateurs
- Gestion des groupes de sécurité

FS1 — Serveur de fichiers

Fonctions déployées :

- Partage SMB sécurisé
- Permissions NTFS
- Groupes de sécurité Active Directory
- Intégration au domaine
- Lecteur réseau Z:

Évolutions prévues

L'architecture a été pensée pour accueillir facilement :

- WEB1 → IIS / portail MedSearch
- DB1 → SQL Server
- WSUS1 → gestion centralisée des mises à jour
- MONITOR1 → supervision et monitoring
- CLIENT1 / CLIENT2 → postes utilisateurs

Même si ces VM n'ont pas toutes été déployées dans le laboratoire final à cause des limitations matérielles, leur intégration reste prévue et documentée.

5. Choix techniques et valeur ajoutée :

Les choix techniques réalisés dans le projet MedSearch ont été faits dans une logique :

- De simplicité
- De cohérence
- D'automatisation
- De sécurité
- D'évolutivité

L'objectif était de construire une infrastructure réaliste tout en restant compatible avec les contraintes matérielles du laboratoire VirtualBox.

Principaux choix techniques

Choix	Avantage principal	Justification
VirtualBox	Virtualisation accessible	Compatible environnement étudiant
Vagrant	Automatisation complète	Déploiement rapide et reproductible
PowerShell	Administration centralisée	Standard Microsoft moderne

Windows Server 2022	Intégration native Microsoft	Cohérence avec Active Directory
Active Directory	Centralisation des identités	Gestion simplifiée des utilisateurs
GPO	Sécurité automatisée	Standardisation des politiques
SMB + NTFS	Contrôle précis des accès	Sécurisation des fichiers
IIS	Hébergement portail interne	Intégration Windows native
DNS interne	Résolution centralisée	Dépendance Active Directory
Monitoring centralisé	Visibilité infrastructure	Réduction du temps de diagnostic

Valeur ajoutée du projet

Le projet ne se limite pas à une simple démonstration technique.

Il met en œuvre plusieurs concepts utilisés en entreprise :

- Infrastructure as Code
- Active Directory
- Automatisation
- Administration centralisée
- Sécurité réseau
- Gestion des accès
- Supervision
- Standardisation des configurations

Gestion des contraintes matérielles

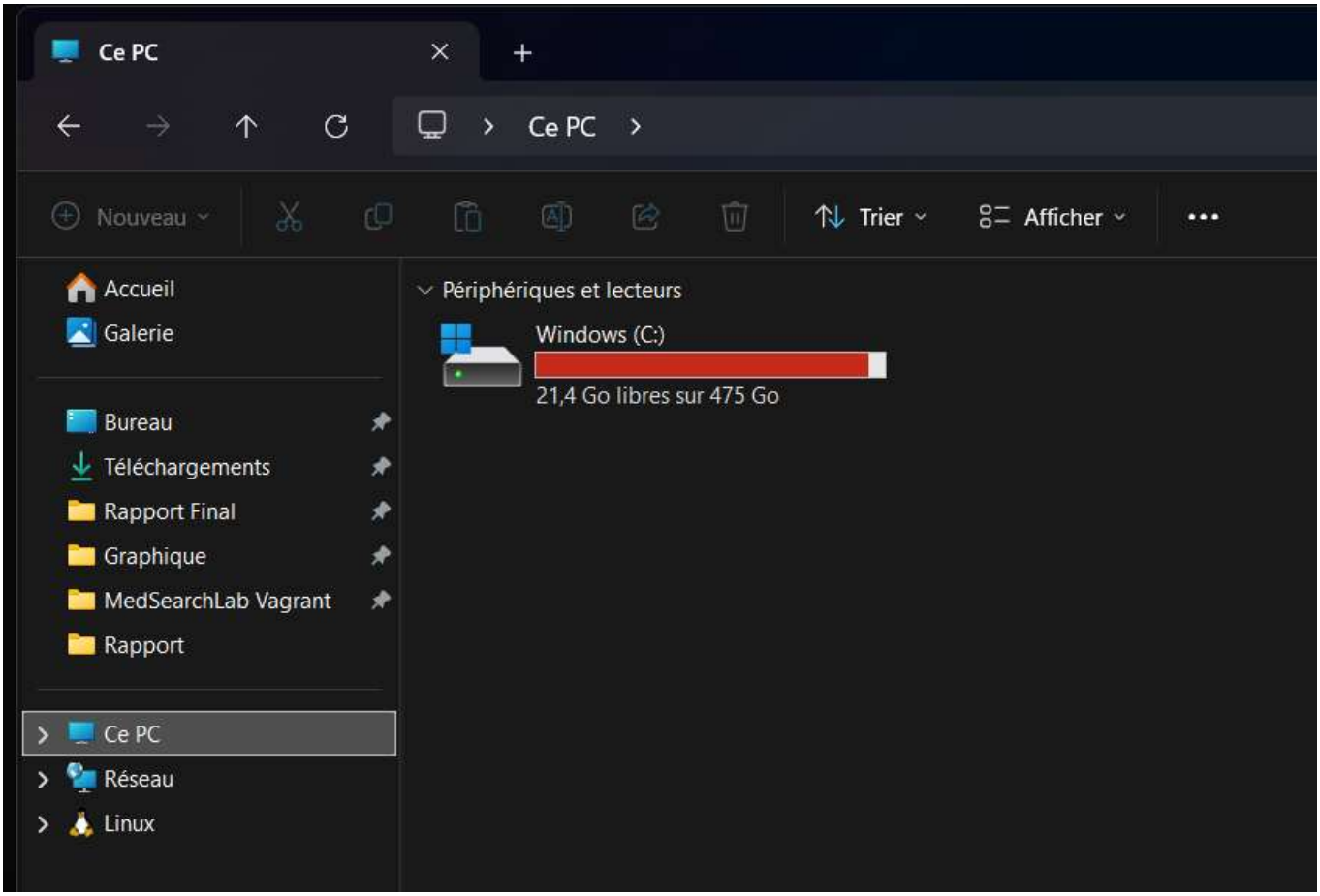
Le laboratoire a été conçu dans un environnement limité en ressources matérielles.

Pour cette raison :

- Seules les VM critiques ont été complètement déployées
- L’architecture globale reste néanmoins entièrement documentée
- Les VM futures sont prévues dans le Vagrantfile

- L’infrastructure reste extensible

Cette approche démontre également une capacité d’adaptation et de priorisation des services critiques.



6. Résultats obtenus :

Les services critiques ont été déployés avec succès :

- contrôleur de domaine DC1
- serveur de fichiers FS1
- gestion centralisée des utilisateurs
- groupes Active Directory
- politiques GPO
- permissions NTFS et SMB
- lecteur réseau automatique

L'ensemble de ces éléments constitue déjà une infrastructure d'entreprise cohérente et fonctionnelle.

Automatisation et industrialisation :

L'un des points forts majeurs du projet est l'automatisation complète de l'infrastructure grâce à :

- Vagrant
- PowerShell
- Provisioning automatique

Cette approche permet :

- De reproduire rapidement l'environnement
- De standardiser les configurations
- De réduire les erreurs humaines
- De simplifier l'administration

Évolutivité de l'architecture :

Même si certaines VM supplémentaires n'ont pas pu être complètement déployées à cause des limitations matérielles du poste de travail, l'architecture reste prévue pour intégrer :

- IIS
- SQL Server
- WSUS
- Monitoring
- Portail web MedSearch

L'environnement reste donc totalement évolutif.

Vision globale du projet :

Le projet démontre :

- La centralisation des services

- La gestion sécurisée des accès
- L'automatisation de l'infrastructure
- L'utilisation des bonnes pratiques Microsoft
- Une architecture pensée pour l'entreprise

7. Conclusion générale :

Cette architecture répond aux principaux besoins de MedSearch en combinant centralisation des services, sécurité, simplicité d'administration et automatisation. L'infrastructure repose sur un environnement virtualisé sous VirtualBox et déployé automatiquement grâce à Vagrant et PowerShell, ce qui permet de reproduire rapidement les machines virtuelles et standardiser l'ensemble des configurations. Les services critiques mis en place, notamment Active Directory, DNS, les GPO et le serveur de fichiers sécurisé, fournissent une base cohérente et évolutive pour l'entreprise. L'architecture a également été pensée pour intégrer progressivement d'autres services comme IIS, WSUS, SQL Server ou la supervision centralisée. La force du projet repose autant sur les services fonctionnels démontrés que sur la cohérence globale de l'architecture, l'automatisation de l'infrastructure, les preuves de validation et la qualité de la documentation technique.