B\*\*

*15/03/2024*

*2008 R2*

1. Table des matières

[I. Introduction 3](#_Toc161430579)

[II. Installation des rôles essentiels 3](#_Toc161430580)

[1. Configuration d’une IP statique : 3](#_Toc161430581)

[2. Installation de l'Active Directory. 4](#_Toc161430582)

[3. Configuration de l’Active Directory : 4](#_Toc161430583)

[4. Configuration DHCP : 6](#_Toc161430584)

[III. Création du réseau de test 6](#_Toc161430585)

[5. Adhésion de la machine Windows7 au serveur 2008R2 6](#_Toc161430586)

[6. Test de la connectivité et de l’appartenance au domaine 7](#_Toc161430587)

[IV. Fonctions assurées par l’active Directory 8](#_Toc161430588)

[7. Création d’UO et de groupes 8](#_Toc161430589)

[8. Attribution d’UO pour la machine test W7 10](#_Toc161430590)

[V. Fonctions assurées par le serveur de fichier 11](#_Toc161430591)

[9. Installation du serveur de fichiers et mise en place des autorisations de partage 11](#_Toc161430592)

[10. Mise en place des autorisations de sécurité 12](#_Toc161430593)

[VI. Test des autorisations mises en place avec la STA W7 14](#_Toc161430594)

[11. Test des autorisations avec le compte administrateur 14](#_Toc161430595)

[12. Test des autorisations avec un compte professeur 15](#_Toc161430596)

[13. Test des autorisations avec un compte étudiant 16](#_Toc161430597)

[VII. Conclusion 17](#_Toc161430598)

# Introduction

Nous examinons la configuration d'un serveur 2008 dans le cadre du module B1 - Support des services et des serveurs. Étant donné que l'Active Directory, le DHCP et le DNS font partie des services les plus importants et indispensables pour un réseau complet, la configuration sur un système emblématique comme 2008 nous fournit des bases solides pour un technicien chargé de la configuration des services et des serveurs.

# Installation des rôles essentiels

Sur un serveur, il y a le serveur Active Directory qui gère l'authentification et l'autorisation des utilisateurs, le DHCP qui attribue les adresses IP aux périphériques sur le réseau, et le DNS qui traduit les noms de domaine en adresses IP. Nous allons configurer ces trois services, mais avant cela, il est important de passer le serveur en IP statique pour que les autres postes puissent le trouver sur le réseau et éviter les attaques de type "man-in-the-middle" trop évidentes

## Configuration d’une IP statique :

En accédant aux propriétés du réseau local, il est possible de modifier et configurer une adresse IP statique.

|  |  |
| --- | --- |
| Une image contenant texte, Appareils électroniques, capture d’écran, logiciel  Description générée automatiquement |  |

## Installation de l'Active Directory.

Le premier service à installer est l'Active Directory, car les autres services s'appuient sur lui, tels que le DNS. Nous allons donc commencer par aller dans "Ajout des rôles" puis Active Directory

|  |  |
| --- | --- |
| Une image contenant texte, capture d’écran, logiciel, affichage  Description générée automatiquement | Une image contenant texte, capture d’écran, logiciel, affichage  Description générée automatiquement |

## Configuration de l’Active Directory :

Une fois le service activé, il va falloir le configurer pour qu'il soit totalement opérationnel.

|  |  |
| --- | --- |
| Une image contenant texte, capture d’écran, logiciel, affichage  Description générée automatiquement | Une image contenant texte, Appareils électroniques, capture d’écran, affichage  Description générée automatiquement  On configure le nom de domaine en fonction de nos initial |

Une image contenant texte, Appareils électroniques, capture d’écran, affichage

Description générée automatiquementWindows, étant convivial pour l'utilisateur, nous avertit qu'il n'y a pas de zone parente et qu'elle est introuvable. C'est normal car elle n'existe pas. Ce message est présent pour les utilisateurs novices, mais n'est pas vraiment pertinent pour nous. Nous allons simplement le valider.

Windows nous propose de stocker les fichiers à un emplacement de notre choix. Nous n'allons pas y toucher car nous n'avons pas de consignes de sécurité particulières. Cependant, il pourrait être intéressant de configurer des dossiers différents plutôt que d'utiliser les paramètres par défaut :

|  |  |
| --- | --- |
| Une image contenant texte, Appareils électroniques, capture d’écran, logiciel  Description générée automatiquement | Une image contenant texte, Appareils électroniques, capture d’écran, logiciel  Description générée automatiquement |

L’active directory que nous venons de créer nous permettra de regrouper des postes au sein du même réseau, ainsi nous pourrons par exemple utiliser un système d’authentification centralisée, cela permet de se connecter sur n’importe quel poste du réseau avec un compte lui aussi présent sur l’active directory si l’ordinateur est bien membre du réseau lui aussi.

L’active Directory permet aussi d’affecter des services tel que DNS et DHCP que nous allons voir par la suite ainsi que leur mise en place :

## Configuration DHCP :

|  |  |
| --- | --- |
| Une image contenant texte, capture d’écran, affichage, logiciel  Description générée automatiquement | La configuration du DHCP passe par les mêmes étapes que pour les autres services. Il faut donc configurer le pool de DHCP qui sera diffusé. |

Le serveur DNS permet de résoudre des noms de domaines en adresses IP pour pouvoir communiquer avec le nom de domaine, le serveur DNS est créé automatiquement avec la création de l’Active Directory, cela est une option supplémentaire à ajouter sur le contrôleur de domaine.

Le serveur DHCP permet d’attribuer des adresses IP de manière dynamique à des postes présents sur le réseau, ainsi les postes se verront attribuer une adresse IP automatiquement.

Les rôles étant installés nous pourrons à présent commencer la configuration de ces derniers ainsi que la création d’autres fonctionnalités.

# Création du réseau de test

Mais avant de continuer nous allons réaliser une snapshot qui nous permettra de potentiellement revenir en arrière en cas de problème de configuration ou d’erreur, la snapshot est une copie instantanée de l’état actuel du système et nous permettra de revenir à cet état dans le futur.

## Adhésion de la machine Windows7 au serveur 2008R2

Pour continuer nous allons utiliser une autre STA qui est une STA windows7, nous ferons adhérer cette dernière au domaine que nous venons de créer, pour cela il faut que nous vérifiions que cette dernière est bien présente sur le même réseau que notre serveur sinon nous ne pourrons pas connecter la STA au domaine que nous venons de créer.

Pour cela il est nécessaire que la STA W7 et le serveur WIN2008R2 soient tous les deux sur le même LAN dans notre cas le LAN associé à notre UTI.

Pour VirtualBox, la manipulation est assez simple : il suffit d'aller dans les paramètres de notre machine virtuelle et de les configurer tous les deux dans le même réseau interne LAN. La connexion se fera automatiquement si la configuration a été effectuée correctement.Une image contenant capture d’écran, texte, logiciel, Logiciel multimédia

Description générée automatiquement

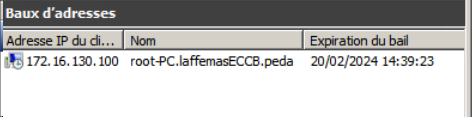
L’objectif étant de faire communiquer la STA W7 et le serveur 2008R2. Le lancement des machines virtuelles doit se faire dans le bon ordre : d’abord le serveur 2008R2, puis la machine W7.

|  |  |
| --- | --- |
| Après avoir vérifié que les machines sont sur le même réseau nous allons faire adhérer la machine Windows7 au domaine pour cela nous accédons aux propriétés du système sur la machine W7 puis nous modifions dans la catégorie “Membre d’un” de “Groupe de travail” à “Domaine”.  Ainsi nous rejoignons le domaine que nous avons créé avec l’Active Directory. |  |

## Test de la connectivité et de l’appartenance au domaine

Pour tester la connectivité dans le domaine entre le serveur et la STA que nous avons créé nous pouvons effectuer une requête de ping vers l’adresse IP du serveur.

Ainsi nous obtiendront un résultat selon le lien entre la STA et le Serveur2008R2 mais cela ne testera pas l’appartenance au domaine car une autre STA n’appartenant pas au domaine pourra elle aussi effectuer ce test de connectivité et le mener à bien.

Or ce que nous voulons est tester l’appartenance de la STA au domaine, pour cela nous accédons directement au domaine puis nous allons voir les différents baux en cours d’utilisation et nous cherchons un bail possédant comme adresse IP celle de notre STA que nous venons de connecter, cela devrait être simple car une seule STA fait partie du domaine à l’heure actuelle, voici à quoi le bail ressemble sur le serveur 2008R2 :

# Fonctions assurées par l’active Directory

Les fonctions d'authentification, de partage de ressources, de protection des données et de filtrage des accès sont gérées par le biais de l'Active Directory, ainsi que par l'administration des comptes et des ressources. De plus, le serveur de fichiers et les dossiers partagés jouent également un rôle important dans ces tâches.

L’installation de l’Active Directory a aussi mis en place le rôle de contrôleur de domaine, nous allons maintenant structurer l’Active Directory ainsi qu’appliquer des autorisations à propos des utilisateurs et des STA ainsi que tester leur fonctionnement, pour cela nous allons avoir recours à des UO (Unités d’Organisation), les Unités d'Organisation (OU) sont un élément clé de l'Active Directory. Elles permettent d'organiser et de structurer les objets du domaine, tels que les utilisateurs, les groupes et les ordinateurs, en fonction de l'organisation interne.

## Création d’UO et de groupes

Pour créer des UO nous accédons au serveur 2008R2 puis nous accédons à la gestion du serveur dans laquelle nous allons sélectionner comment gérer notre serveur, sur cette dernière nous pourrons alors choisir de créer différentes UO .

Une image contenant texte, capture d’écran, logiciel, Icône d’ordinateur

Description générée automatiquementNous créons alors un dossier dans lequel nous stockerons les différentes UO et les différents utilisateurs et groupes, ce dossier s’appellera « Lycee » dans notre exemple, dans ce dossier nous créerons aussi deux UO différentes tel qu’ « Etudiants » et « Profs », voici un aperçu :

Parmi ces UO nous créerons différents groupes que nous attribuerons à des utilisateurs.

Nous allons créer deux groupes différents qui seront chacun dans un dossier différent, les deux groupes seront « profSIO » et « etudiantSIO », respectivement les professeurs seront dans le groupe prof et les étudiants dans le groupe étudiant.

Chaque groupe possédera une étendue Globale ainsi que le type groupe de sécurité, d’autres possibilités sont disponibles mais nous ne les explorerons pas :

* Étendue locale (Local Scope) : Les groupes de cette étendue sont utilisés au sein d'un seul ordinateur ou d'un serveur local. Ils ne peuvent pas être utilisés pour accorder des autorisations sur des ressources partagées dans le domaine.
* Étendue globale (Global Scope) : Les groupes de cette étendue sont utilisés pour regrouper des utilisateurs et des ordinateurs provenant de plusieurs domaines au sein d'une même forêt. Ces groupes peuvent être utilisés pour accorder des autorisations sur des ressources partagées dans le domaine, ainsi que pour appliquer des stratégies de groupe.
* Étendue universelle (Universal Scope) : Les groupes de cette étendue sont utilisés pour regrouper des utilisateurs et des ordinateurs provenant de plusieurs domaines au sein d'une même forêt. Ils offrent une flexibilité accrue en matière de gestion des autorisations et de stratégies de groupe, car ils peuvent être utilisés dans différents domaines.

Types de groupe :

* Groupe de sécurité (Security Group) : Les groupes de sécurité sont utilisés pour gérer les autorisations sur les ressources. Ils permettent de définir des listes de contrôle d'accès (ACL) pour les fichiers, dossiers, partages réseau, imprimantes, etc. Les utilisateurs et les ordinateurs peuvent être membres de ces groupes, ce qui facilite la gestion des autorisations.
* Groupe de distribution (Distribution Group) : Les groupes de distribution sont utilisés pour envoyer des messages électroniques à un ensemble de destinataires. Ils ne sont pas utilisés pour gérer les autorisations sur les ressources, mais plutôt pour simplifier l'envoi de courriers électroniques à un groupe de personnes.

Une image contenant texte, logiciel, Icône d’ordinateur, Logiciel multimédia

Description générée automatiquementIl est important de choisir l'étendue et le type de groupe appropriés en fonction des besoins de l’infrastructure. Dans notre cas, nous avons choisi une étendue globale pour les groupes "profSIO" et "etudiantSIO", ce qui permet de regrouper des utilisateurs et des ordinateurs provenant de plusieurs domaines au sein de notre forêt Active Directory.

Voici ce que nous obtenons dans l’active directory après avoir crée le groupe dans le dossier :

Une image contenant texte, capture d’écran, logiciel, affichage

Description générée automatiquementDans chaque groupe que nous venons de créer, respectivement profSIO et etudiantSIO nous ajouterons trois utilisateurs tel que prof1,2,3 et etudiant1,2,3.

Le formulaire de création est plutôt simple et nous permet de créer les utilisateurs directement à l’aide d’une interface graphique.

**Une image contenant texte, logiciel, Icône d’ordinateur, Logiciel multimédia

Description générée automatiquement**Nous allons alors ajouter trois utilisateurs dans chaque catégorie comme présenté précédemment, nous obtenons alors le résultat suivant :

**Une image contenant texte, Police, conception, capture d’écran

Description générée automatiquement**Nous appliquons le même raisonnement pour la gestion des ordinateurs, pour cela nous allons créer deux UO dans lesquels nous organiserons les ordinateurs présents sur notre réseau, pour cela nous faisons clic droit et nous ajoutons une nouvelle UO, dans cette dernière nous allons déplacer la machine W7 étant déjà adhérente au réseau, cette dernière sera déplacée dans l’UO « salle181 » tandis que l’UO « salle184 » restera sans ordinateur pour l’instant.

## Une image contenant texte, capture d’écran, logiciel, Icône d’ordinateur Description générée automatiquementAttribution d’UO pour la machine test W7

Nous créons comme UO deux salles respectivement 181 et 184. Puis nous sélectionnons notre machine windows7 et nous faisons alors clic droit puis déplacer vers l’UO salle181.

Les UO permettent de structurer le réseau en créant une hiérarchie logique pour les ordinateurs. Par exemple, nous pouvons créer des OUs pour les différentes salles de classe, les départements ou les services spécifiques du lycée, tels que l'administration, la bibliothèque etc…

Les UO permettent aussi de définir des stratégies de groupe (Group Policies) spécifiques pour chaque unité d'organisation. Par exemple, nous pouvons configurer des politiques de groupe différentes pour les ordinateurs des salles de classe et ceux de l'administration.

# Fonctions assurées par le serveur de fichier

Le serveur de fichiers joue un rôle essentiel dans le partage et la sécurisation des fichiers au sein d'une infrastructure informatique, par exemple il permet de centraliser et de consolider les fichiers d'une organisation en un emplacement unique. Cela facilite la gestion et l'accès aux fichiers pour les utilisateurs autorisés. Le serveur de fichiers permet aussi aux utilisateurs de partager des fichiers avec d'autres utilisateurs du réseau. Il offre des mécanismes de contrôle d'accès pour définir qui peut accéder aux fichiers partagés et les permissions qui leur sont accordées (lecture, écriture, suppression, etc.).

## Installation du serveur de fichiers et mise en place des autorisations de partage

**Une image contenant texte, Appareils électroniques, capture d’écran, logiciel

Description générée automatiquement**Pour installer le serveur de fichier nous allons choisir d’ajouter un rôle comme précédemment pour le DHCP précédemment :

**Une image contenant texte, capture d’écran, logiciel, Icône d’ordinateur

Description générée automatiquement**Nous obtenons par la suite un choix des différents services de rôle à installer pour les Services de fichiers, nous n’ajouterons aucun service supplémentaire car dans le cas actuel nous n’en avons pas le besoin mais plusieurs services de rôle sont installables et peuvent permettre diverses options tel qu’un système de service d’indexation.

Nous allons aussi créer des dossiers auxquels nous attribuerons des autorisations de partage, uniquement sur ces dossiers et non pas sur le répertoire général.

Les autorisations de partages quant à elles seront sur les trois dossiers identiques car les restrictions seront appliquées sur les autorisations de sécurité. Les trois dossiers possèderont en autorisation de partage Contrôle total un seul groupe qui sera « Tout le monde »

**Une image contenant texte, capture d’écran, logiciel, Icône d’ordinateur

Description générée automatiquement**Voici les différentes étapes de la création et du partage des dossier, dans un premier temps nous créons les différents dossiers puis nous partagerons ce dernier au groupe « Tout le monde »

**Une image contenant texte, capture d’écran, logiciel, Icône d’ordinateur

Description générée automatiquement**

## Mise en place des autorisations de sécurité

Par défaut les autorisations sont héritées du dossier parent, nous allons donc casser l’héritage pour mettre par la suite en place des autorisations spécifiques aux différents dossiers.

Il est donc décidé d’attribuer sur les trois dossiers *individus*, *applications* et *ressources* des autorisations aux trois groupes d’utilisateurs, profSIO, etudiantSIO et administrateurs.

**12°) Quel message d’erreur apparait quand vous essayez de supprimer par exemple *Utilisateurs* de la liste des noms dans les autorisations de sécurité d’un des trois dossiers ? Expliquez le sens de ce message.**

Si l'on tente de supprimer un utilisateur que l'on a créé, aucun message d'erreur n'apparaît, seulement un message d'avertissement pour confirmer notre action. Cependant, si l'on essaie de supprimer un utilisateur créé par les différents services, un message d'erreur apparaît. Cela est normal car ces comptes sont utilisés par l'Active Directory et les différents services pour assurer leur bon fonctionnement.

|  |  |
| --- | --- |
| Avertissement : | Message d'erreur : |
| **Une image contenant texte, capture d’écran, Police, logiciel  Description générée automatiquement** | **Une image contenant texte, capture d’écran, logiciel, Police  Description générée automatiquement** |

Pour bloquer l’héritage des permissions, nous allons afficher les propriétés du dossier, dans l’onglet *Sécurité*, nous cliquons sur le bouton *Avancé*, puis sur *modifier les autorisations*, désactiver la case à cocher *Inclure les autorisations pouvant être héritées du parent de cet objet*.

Dans la nouvelle fenêtre, nous cliquons sur *Supprimer* afin de supprimer les autorisations héritées et ne conserver que les autorisations explicitement spécifiées.

Pour ajouter des lignes dans la liste de noms d’utilisateurs ou de groupes, il faut cliquer sur *ajouter* puis sélectionnez les noms voulus.

Voici les autorisations souhaitées :

|  |  |  |  |
| --- | --- | --- | --- |
| Dossiers | Individus | Applications | Ressources |
| Autorisation NTFS (sécurité) | Seuls autorisés les **administrateurs** ont un contrôle total | - Les **administrateurs** ont un contrôle total  - Les **utilisateurs** ne peuvent que lire et exécuter | - Les **administrateurs** ont un contrôle total  - Les **professeurs** **de SIO** peuvent effectuer des modifications  - Les **étudiants de SIO** ne peuvent que lire et exécuter |

Voici alors les différentes autorisations NTFS mises sur les dossiers :

Une image contenant texte, capture d’écran, logiciel, affichage

Description générée automatiquement**Individus :**

Une image contenant texte, capture d’écran, logiciel, Icône d’ordinateur

Description générée automatiquement**Applications :**

Une image contenant texte, capture d’écran, logiciel, Icône d’ordinateur

Description générée automatiquement**Une image contenant texte, capture d’écran, logiciel, affichage

Description générée automatiquement**

**Une image contenant texte, capture d’écran, logiciel, affichage

Description générée automatiquementRessources :**

**Une image contenant texte, capture d’écran, logiciel, affichage

Description générée automatiquement**

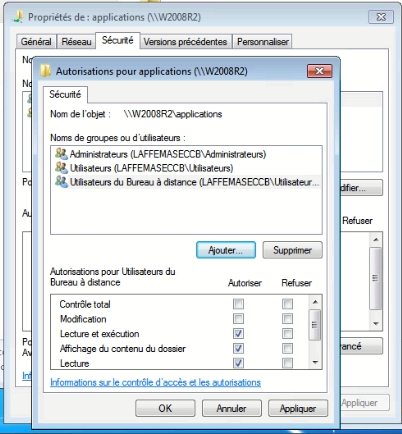
# Test des autorisations mises en place avec la STA W7

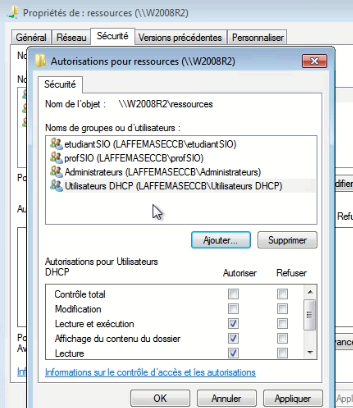
Pour tester les autorisations que nous venons de mettre en place sur les différents dossiers nous allons tester les différentes possibilités selon le type d’utilisateur, nous allons ainsi tester le niveau d’autorisation le plus élevé pour le fichier qui est censé échouer ainsi que le niveau le plus élevé étant accompli.

## Test des autorisations avec le compte administrateur

Pour L’administrateur nous allons essayer le contrôle total qui est censé être possible sur chaque dossier, ainsi nous pouvons normalement selon les autorisations que nous avons défini au préalable assigner des autorisations sur tous les fichiers partagés.

Administrateur :

Une image contenant texte, capture d’écran, logiciel, affichage

Description générée automatiquementEn étant connecté comme administrateur nous pouvons ajouter des permissions comme prévu avec les autorisations que nous avons accordées. Il n’est pas nécessaire de tester les autres autorisations car les autorisations sont en cascade (attribuées de manière hiérarchique, ce qui signifie que si un utilisateur a une autorisation parente, il héritera également des autorisations enfants associées.).

## Test des autorisations avec un compte professeur

***Une image contenant texte, logiciel, Icône d’ordinateur, Page web

Description générée automatiquement***En tant que professeur nous allons tester comme précédemment l’autorisation la plus haute et l’autorisation la plus haute pouvant être accomplie.

Nous ne pouvons pas accéder au répertoire individus car ce dernier ne possède aucune autorisation pour le groupe professeur

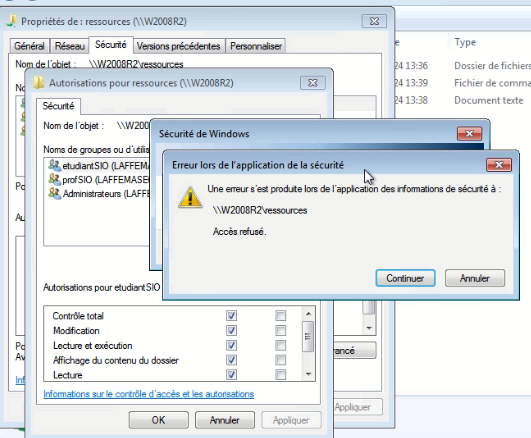
***Une image contenant texte, capture d’écran, logiciel, ordinateur

Description générée automatiquementUne image contenant texte, capture d’écran, logiciel, Page web

Description générée automatiquement***Pour le répertoire applications nous ne pouvons pas renommer car nous n’avons pas l’autorisation de modification mais nous pouvons lire et exécuter un programme :

***Une image contenant texte, capture d’écran, logiciel, Icône d’ordinateur

Description générée automatiquement***Pour le répertoire ressources nous pouvons renommer un fichier, ce qui signifie que nous possédons l’autorisation de modification :

Nous ne pouvons pas donner des permissions aux autres utilisateurs car nous n’avons pas le contrôle total sur le dossier :

## Test des autorisations avec un compte étudiant

**Une image contenant texte, logiciel, Icône d’ordinateur, Page web

Description générée automatiquement**En tant qu’étudiant nous allons tester comme précédemment l’autorisation la plus haute et l’autorisation la plus haute pouvant être accomplie.

Nous ne pouvons pas accéder au répertoire individus car ce dernier ne possède aucune autorisation pour le groupe étudiant.

**Une image contenant texte, logiciel, ordinateur, Logiciel multimédia

Description générée automatiquementUne image contenant texte, logiciel, Icône d’ordinateur, Page web

Description générée automatiquement**Dans le dossier ressources nous ne pouvons pas renommer car nous n’avons pas l’autorisation de modification mais nous pouvons lire et exécuter un programme :

**Une image contenant texte, capture d’écran, logiciel, Icône d’ordinateur

Description générée automatiquement**

**Une image contenant texte, capture d’écran, logiciel, Icône d’ordinateur

Description générée automatiquement**Dans le dossier applications nous ne pouvons pas renommer car nous n’avons pas l’autorisation de modification mais nous pouvons lire et exécuter un programme :

# Conclusion

En conclusion, ce projet de configuration d'un serveur 2008 dans le cadre du module B1 - Support des services et des serveurs nous a permis d'acquérir des compétences essentielles pour la configuration et la gestion des services réseau. En mettant en place des services comme l'Active Directory, le DHCP et le DNS, ainsi qu'en organisant efficacement les ressources avec des unités d'organisation (OU) et des autorisations de partage et de sécurité, nous avons démontré notre capacité à administrer un réseau de manière professionnelle et sécurisée.