République Algérienne Démocratique et Populaire

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université Saad Dahleb Blida 1

Faculté des sciences

Département d'informatique

Mémoire

Présenté en vue de l'obtention du diplôme

Master

Option : informatique

Spécialité : sécurité des systèmes d'information

Par : ZOUAOUI Rofila

Thème

Configuration d'un contrôleur de domaine (Active Directory) pour une gestion centralisée des utilisateurs et ordinateurs au sein de la CNAS Blida

---

Encadré par : Mr. BOUDERBALA Mohamed

Promoteur : Mr. BENYAHIA

Devant le jury composé de : - Mr. BENAISSI

- M. CHERFA

Promotion : 2021/2022

Remerciement :

Merci à dieux le tout puissant de m'avoir donné la force et la santé et la volonté d'entamer et de terminer ce mémoire.

Tous d'abord, ce travail ne serait pas aussi riche et n'aurait pas pu avoir le jour sans l'aide et l'encadrement de monsieur ***BOUDERBALA Mohamed****, je le remercie pour la qualité de son encadrement, sa patience, sa rigueur, et sa disponibilité durant toute la période de mon stage.*

Mes remerciements s'adressent aussi à madame ***MOUSSAOUI Ourida*** *pour sa confiance, son aide pratique, et soutien morale.*

Je tiens à remercier mon promoteur monsieur ***BENYAHIA Mohamed*** *de m'avoir suivi tout au long de la réalisation de ce mémoire.*

Je remercie également mes gratitudes aux membres de jurys qui m'ont honoré en acceptant de juger ce travail.

Enfin, je tiens à exprimer vivement mes remerciements avec une profonde gratitude à toutes les personnes qui ont contribués de près ou de loin à sa réalisation, car un projet ne peut pas être le fruit d'une seule personne.

Dédicaces :

Je dédiée ce travail à mon cher père, l'homme qui doit ma vie, ma réussite et tout mon respect, qui m'a toujours soutenu et vers qui je retourne toujours.

A la femme qui a souffert sans me laisser souffrir, qui n'a jamais dit non âmes exigences et qui n'a épargnés aucun effort pour me rendre heureuse, Mon adorable mère❤

A mon cher mari qui ma soutenue et encourage pour finir ce travail

A mes frères, merci pour m'avoir toujours supporté que dieu vous paye pour tous vos bienfaits.

A ma cousine Wissem que dieu la donne une longue et joyeuse vie.

A mes grands-mères, grands-pères, mes tantes et mes oncles, mes cousins et cousines.

A ma belle-famille pour leur encouragement et leurs soutiens.

A toute la famille ***ZOUAOUI*** *et* ***BOUKARA****.*

A toutes la promotion SSI 2021/2022.

Table de matières :

Chapitre III : Découverte de CNAS Blida

Chapitre IV : installation et configuration d'Active Directory

Liste des figures :

Introduction générale

Chaque organisation a son propre cadre organisationnel dans lequel les rôles et les responsabilités des différents départements tels que les ventes, l'informatique, la fabrication et l'assurance qualité sont définis pour atteindre l'objectif commun souhaité.

Les employeurs utilisent les ressources de l'entreprise pour exécuter les opérations commerciales, ainsi que les compétences et l'expertise.

Pour utiliser efficacement ces ressources, il est essentiel de mettre en place un outil de contrôle d'accès.

Active Directory est l'un de ces outils qui gère les utilisateurs, les applications et les ressources et permet de gérer l'autorisation et l'authentification des utilisateurs pour ces ressources. l'Active Directory est un **must-have** pour toute entreprise qui souhaite centraliser la gestion de ses ressources informatique et mettre en place une politique de sécurité robuste. L'entreprise CNAS de Blida ne dispose pas à ce jour un réseau opérationnel, où toutes les machines sont isolées et l'échange de l'informations se fait de main à main

La problématique générale de notre travail est :
Comment gérer tous les comptes des utilisateurs et les ordinateurs de l'entreprise, et comment garantir la sécurité des accès et des utilisations des informations enregistrées dans les équipements informatiques en utilisant un contrôleur de domaine Active Directory sous Windows server 2012 R2 ?

Le but de ce travail est de mettre en place un contrôleur de domaine qui sera en mesure de rependre aux critères habituellement utilisés par l'administrateur de réseau de la CNAS Blida tels que :

- L'authentification des utilisateurs sur les postes de travail
- La gestion des droits d'accès

Chapitre I

Les réseaux informatiques

Chapitre I : les réseaux informatiques

1. Introduction :

Un contrôleur de domaine est un serveur qui répond aux demandes d'authentification et contrôle les utilisateurs des réseaux informatiques.

Dans ce chapitre on va voire c'est quoi un réseau informatique, les types des réseaux informatiques, l'architecture d'un réseau informatique,

2. Vision générale sur les réseaux :

Un réseau est un moyen de communication qui permet à des individus ou à des groupes de partager des informations et des services.

La technologie des réseaux informatiques constitue l'ensemble des outils qui permettent à des ordinateurs de partager des informations et des ressources.

Un réseau est constitué d'équipement appelés nœuds. En fonction de leur étendue et de leur domaine d'application, ces réseaux sont catégorisés.

Pour communiquer entre eux, les nœuds utilisent des protocoles, ou langage compréhensible par tous.

3. Types des réseaux informatiques :

3.1. Le réseau personnel :

La plus petite étendue du réseau est nommée en anglais *Personnel Area Network* (PAN). Centré sur l'utilisateur, elle désigne un interconnexion d'équipement informatique dans un espace d'une dizaine de mètres autour de celui-ci, deux autres appellations de ce type de réseau sont : réseau individuel et réseau domestique.

3.2. Le réseau local :

Le *Local Area Network* (LAN) en français réseau local d'entreprise (RLE), relie entre eux des ordinateurs, des serveurs… il est couramment utilisé pour le partage de ressources communes, comme les périphériques, des données, ou des applications.

3.3. Le réseau métropolitain :

Le réseau métropolitain ou *Metropolitan Area Network* (MAN), est également nommé réseau fédérateur. Il assure des communications sur de plus longues distances, interconnectant souvent plusieurs réseaux LAN. Il peut servir à interconnecter, par une liaison privée ou non, différents bâtiments, distants de quelques dizaines de kilomètres.

3.4. Le réseau étendu :

Les étendues de réseaux les plus conséquentes sont classés en WAN, acronyme de *Wide Area Network*. Constitués de réseaux de type LAN, voire MAN, les réseaux étendus sont capables de transmettre les informations sur des milliers de kilomètres à travers le monde entier. Le WAN le plus célèbre est le réseau publique internet.

4. Architecture d'un réseau informatique :

4.1. Le modèle OSI :

Un système ouvert est un ordinateur, un terminal, un réseau, n'importe quel équipement respectant cette norme est donc apte à échanger des informations avec d'autres équipements hétérogènes et issus de constructeurs différents.

Le premier objectif de la norme OSI a été de définir un modèle de toute architecture de réseau base sur découpage en sept couche chacun de ces couches correspond à une fonctionnalité particulière d'un réseau.

La couche application : La couche application du modèle OSI fournit essentiellement des options de mise en réseau aux programmes exécutés sur un ordinateur. Il fonctionne presque exclusivement avec des applications, leur fournissant une interface à utiliser pour transmettre des données. Lorsque les données sont transmises à la couche application, elles sont transmises à la couche présentation.

La couche présentation : La couche présentation reçoit les données de la couche application. Ces données ont tendance à être dans un format que l'application comprend, mais elles ne sont pas nécessairement dans un format standardisé qui pourrait être compris par la couche application de l'ordinateur récepteur. La couche de présentation traduit les données dans un format normalisé, ainsi que la gestion de tout chiffrement, compression ou autres transformations des données. Une fois cette opération terminée, les données sont transmises à la couche de session.

La couche session : Lorsque la couche session reçoit les données correctement formatées de la couche présentation, elle regarde si elle peut établir une connexion avec l'autre ordinateur sur le réseau. S'il ne le peut pas, il renvoie une erreur et le processus ne va pas plus loin. Si une séance peut être établi, c'est le travail de la couche session de le maintenir, ainsi que de coopérer avec la couche session de l'ordinateur distant afin de synchroniser les communications. La couche session est particulièrement importante car la session qu'elle crée est unique à la communication en question. C'est ce qui vous permet de faire plusieurs requêtes à différents points de terminaison simultanément sans que toutes les données ne se mélangent (pensez à ouvrir deux onglets dans un navigateur Web en même temps) ! Lorsque la couche de session a enregistré avec succès une connexion entre l'hôte et l'ordinateur distant, les données sont transmises à la couche 4 : la couche de transport.

La couche transport : La couche de transport est une couche très intéressante qui remplit de nombreuses fonctions importantes. Son premier objectif est de choisir le protocole sur lequel les données doivent être transmises. Les deux protocoles les plus courants dans la couche transport sont TCP (Transmission Control Protocol) et UDP (User Datagram Protocol) ; avec TCP, la transmission est basée sur la connexion, ce qui signifie qu'une connexion entre les ordinateurs est établie et maintenue pendant la durée de la demande. Cela permet une transmission fiable, car la connexion peut être utilisée pour s'assurer que tous les paquets arriver au bon endroit. Une connexion TCP permet aux deux ordinateurs de rester en communication constante pour s'assurer que les données sont envoyées à une vitesse acceptable et que toute donnée perdue est renvoyée. Avec UDP, c'est le contraire qui est vrai ; des paquets de données sont essentiellement jetés sur l'ordinateur récepteur - s'il ne peut pas suivre, c'est son problème (c'est pourquoi une transmission vidéo sur quelque chose comme Skype peut être pixélisée si la connexion est mauvaise). Cela signifie que TCP serait généralement choisi pour les situations où la précision est privilégiée par rapport à la vitesse (par exemple, le transfert de fichiers ou le chargement d'une page Web), et UDP serait utilisé dans les situations où la vitesse est plus importante (par exemple, le streaming vidéo).

Avec un protocole sélectionné, la couche de transport divise ensuite la transmission en petits morceaux (sur TCP, on les appelle segments, sur UDP, on les appelle datagrammes), ce qui facilite la transmission réussie du message.

La couche réseau : La couche réseau est chargée de localiser la destination de votre requête. Par exemple, Internet est un immense réseau ; lorsque vous souhaitez demander des informations à partir d'une page Web, c'est la couche réseau qui prend l'adresse IP de la page et détermine le meilleur itinéraire à suivre. À ce stade, nous travaillons avec ce que l'on appelle

l'adressage logique (c'est-à-dire les adresses IP) qui sont toujours contrôlées par logiciel. Les adresses logiques sont utilisées pour ordonner les réseaux, les catégoriser et nous permettre de les trier correctement. Actuellement, la forme d'adressage logique la plus courante est le format IPV4, que vous connaissez probablement déjà (par exemple, 192.168.1.1 est une adresse courante pour un routeur domestique).

La couche liaison : La couche liaison de données se concentre sur l'adressage physique de la transmission. Il reçoit un paquet de la couche réseau et ajoute l'adresse physique (MAC) du point de terminaison récepteur. À l'intérieur de chaque ordinateur compatible réseau se trouve une carte d'interface réseau (NIC) qui est fournie avec une adresse MAC (Media Access Control) unique pour l'identifier.

Les adresses MAC sont définies par le fabricant et littéralement gravées dans la carte ; ils ne peuvent pas être modifiés, bien qu'ils puissent être usurpés. Lorsque des informations sont envoyées sur un réseau, c'est en fait l'adresse physique qui est utilisée pour identifier exactement où envoyer les informations.

De plus, c'est aussi le travail de la couche liaison de données de présenter les données dans un format adapté à la transmission.

La couche liaison de données remplit également une fonction importante lorsqu'elle reçoit des données, car elle vérifie les informations reçues pour s'assurer qu'elles n'ont pas été corrompues lors de la transmission, ce qui pourrait bien arriver lorsque les données sont transmises par la couche 1 : la couche physique.

La couche physique : La couche physique va jusqu'au matériel de l'ordinateur. C'est là que les impulsions électriques qui composent le transfert de

données sur un réseau sont envoyées et reçues. C'est le travail de la couche physique de convertir les données binaires de la transmission en signaux et de les transmettre sur le réseau, ainsi que de recevoir les signaux entrants et de les reconvertir en données binaires.

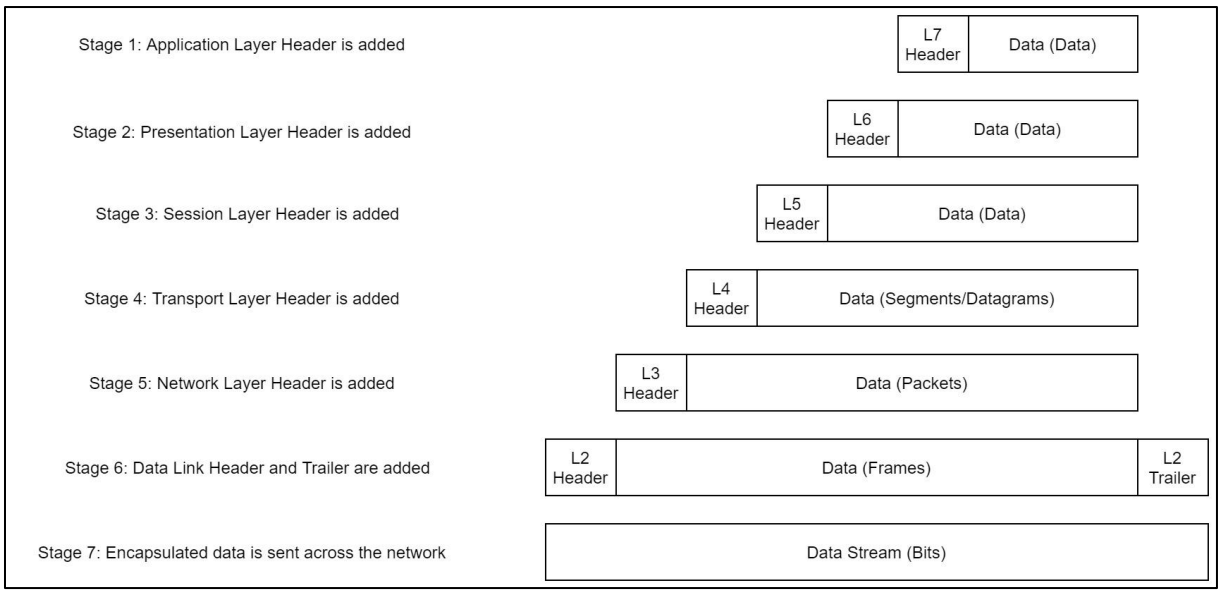

Figure 1 : les couches du modèle OSI

4.2. Le modèle TCP/IP :

Le modèle TCP/IP peut en effet être décrit comme une architecture réseau à 4 couches :

La couche hôte réseau : Elle est en fait composée de deux couches : Physique et Liaison

La couche internet : Son rôle est l'injection de paquets dans n'importe quel réseau. Lorsque deux terminaux communiquent entre eux via ce protocole, aucun chemin pour le transfert des données n'est établi à l'avance : il est dit que le protocole est « non orienté connexion ». Ainsi les paquets envoyés peuvent arriver dans le désordre car ils n'auront pas suivi la même route. C'est le protocole transport qui se chargera de remettre les paquets dans le bon ordre.

La couche transport : Son rôle est similaire à celui de la couche transport du modèle OSI. Les protocoles utilisés à ce niveau sont TCP et UDP. TCP est fiable, acheminant sans erreur les paquets à destination, utilisant des services d'acquittement, de gestion du temps d'attente… UDP est non fiable mais plus rapide. Il est utilisé dans les liaisons voix IP, où l'on préfère perdre quelques données qu'attendre. Utilisé aussi pour le streaming ou la vidéo conférence.

La couche application : Le Modèle TCP/IP est fondé sur le constat que les logiciels réseaux n'utilisent que très peu, ou pas, les couches session et présentation. Cette couche regroupe toute les protocoles de haut niveau (FTP, SMTP, HTTP, DNS…). Cette couche devra choisir un protocole de transport adapté au service demandé.

4.3. La différence entre le modèle OSI et le modèle TCP/IP :

Le modèle TCP/IP est plus simple qu'OSI, avec seulement quatre couches : liaison, Internet, transport et application. La différence avec OSI est simplement que certaines couches ont été fusionnées. La couche liaison de TCP/IP regroupe notamment les couches physiques et liaison d'OSI. De même, la couche application de TCP/IP regroupe les couches session, application et présentation d'OSI.

<table>
<tr><th>OSI</th><th>TCP/IP</th></tr>
<tr><td>Application</td><td rowspan="3">Application</td></tr>
<tr><td>Presentation</td></tr>
<tr><td>Session</td></tr>
<tr><td>Transport</td><td>Transport</td></tr>
<tr><td>Network</td><td>Internet</td></tr>
<tr><td>Data Link</td><td rowspan="2">Network Interface</td></tr>
<tr><td>Physical</td></tr>
</table>

Figure 2 : La différence entre le modèle OSI et le modèle TCP/IP

5. Sécurité des systèmes d'information :

5.1. Introduction :

La Sécurité des systèmes d'information (SSI) est un domaine extrêmement vaste puisqu'elle fait appel à de nombreux concepts juridiques, sociaux, et économiques, à la gestion de personnel, et à des connaissances techniques extrêmement pointues.

5.2. Les principes de la sécurité informatique :

La sécurité informatique vise généralement des principaux objectifs :

La confidentialité : rendre l'information inintelligible à d'autres personnes que les seuls acteurs d'une transaction.

L'intégrité : c'est-à-dire garantir que les données sont bien celles que l'on croit être.

La disponibilité : permettant de maintenir le bon fonctionnement du système d'information.

L'authentification : consistant à assurer que seules les personnes autorisées aient accès aux ressources.

- **La non répudiation :** garantir qu'une transaction ne peut être niée.

6. Les menaces informatiques :

Une menace est une entité ou un évènement qui perturbe le système d'information.

Elle inclut les erreurs volontaires ou involontaires, les fraudes, les actions possibles des employés mécontents, les incendies et autres causes naturelles, les hackers, les programmes néfastes ou virus.

- **Les failles de sécurité**

Les failles de sécurité ne sont pas des menaces directes. Ce sont des portes d'entrée utilisées par les pirates pour pénétrer les systèmes informatiques. Ces vulnérabilités peuvent être externes, logicielles ou matérielles, provenant de l'éditeur ou du fabricant. Il peut s'agir par exemple de failles de sécurité sur les processeurs ou sur les systèmes d'exploitation. Il y a également les vulnérabilités internes liées à une mauvaise ou insuffisante configuration du système informatique, ou de l'un de ses composants.

- **Les malwares**

C'est une terminologie utilisée pour désigner tous les types de logiciels malveillants. Elle englobe donc les adware (publicités intempestives), les virus, spyware et autres chevaux de Troie. Ces derniers sont plus dangereux car ils ont pour but de provoquer des dégâts directement, de prendre le contrôle de vos appareils ou de voler des informations.

- **L'hameçonnage (ou phishing)**

Le phishing est l'escroquerie la plus courante. Elle consiste à envoyer un email ou un sms frauduleux en **se faisant passer pour un tiers de confiance** (une entreprise ou une administration). Les mails notamment sont trompeurs car ils imitent le logo et l'identité visuelle de ces tiers. L'objectif est de récupérer des informations de la victime (souvent ses identifiants) ou de lui faire exécuter une action visant à installer un logiciel malveillant.

- **Les rançongiciels (ou ransomeware)**

C’est un malware qui bloque l’accès au système informatique ou à des fichiers de l’entreprise. Le rétablissement de l’accès fait l’objet d’un chantage et d’une demande de rançon.

7. Conclusion :

Dans ce chapitre on a parlé d’une façon générale sur les réseaux informatiques, ces types et l’architecture d’un réseau informatique. Ainsi que la sécurité des systèmes d’information et les menaces informatique.

Chapitre II

Etude de service d’annuaire active directory

Chapitre II : étude de service d'annuaire active directory

1. Introduction :

Toute entreprise, quelle que soit sa taille, qui enregistre des données client sur son réseau a besoin d'un contrôleur de domaine pour en améliorer la sécurité.

Dans ce chapitre on va présenter pourquoi on a besoin d'un annuaire ? c'est quoi un service d'annuaire « Active Directory », son rôle, ces objets, ces fonctionnalités,

2. Pourquoi un annuaire ?

Active Directory est avant toute chose un annuaire, Avant d'aller plus loin dans l'étude d'Active Directory, il faut définir ce qu'est exactement un annuaire.

Avec le développement des réseaux, les services offerts se sont multipliés. On trouve ainsi couramment sur un même réseau un service de messagerie, un serveur de fichiers, un agenda partagé, etc.
Avant d'accéder à un quelconque service, il est souvent demandé aux utilisateurs de s'authentifier, afin de se faire reconnaitre du service en question. De même, chaque utilisateur d'un service disposera de ses propres données, de ses propres paramètres, pour l'utilisation du service.

3. Contraintes d'un annuaire :

3.1. L'aspect dynamique :

Un annuaire électronique doit avant tout être dynamique. Il doit pouvoir être mis à jour rapidement, et ces modifications doivent être accessibles immédiatement, ce dans le but de diminuer le délai de diffusion de l'information sur le réseau. L'aspect dynamique d'un annuaire permet également de faciliter la délégation des responsabilités. C'est le propriétaire d'une information qui met celle-ci à

jour ; l'information se trouve ainsi rapprochée de sa source afin de la rendre toujours plus pertinente.

3.2. La flexibilité :

Un annuaire électronique doit également répondre à une deuxième contrainte, celle de la flexibilité. Pour qu'il soit efficace, la structure d'un annuaire doit pouvoir être modifiée pour s'adapter aux nouvelles entrées qui doivent y être enregistrées. L'ajout d'un attribut, d'une structure de données complète ou d'une entrée dans un annuaire électronique doit pouvoir se faire sans altérer les informations existantes pour le reste de l'annuaire.

De même, il doit être possible de modifier l'organisation des données au sein de l'annuaire. La fonction principale d'un annuaire est d'organiser les données de telle façon qu'elles puissent être retrouvées le plus rapidement possible. Pour ce faire, un annuaire met en place un classement qui lui est propre, susceptible d'évoluer en fonction des informations qui sont ajoutées à l'annuaire.

3.3. La sécurité :

Un annuaire électronique doit être en mesure de contrôler les données qu'il fournit, et ce en fonction de différents critères, qui peuvent aller de la localisation géographique de l'utilisateur demandant une information à son identité complète. Des mécanismes d'authentification doivent être présent afin de permettre, par exemple, d'interdire l'accès à un sous-ensemble de l'annuaire, ou à certains attributs.

Il doit également être possible de restreindre l'accès à certaines informations en fonction de relations établies ou non dans les données existant dans l'annuaire. Par exemple, un administrateur local devra pouvoir accéder aux profils des utilisateurs locaux, mais pas à ceux des utilisateurs du domaine. De même, un

utilisateur local ne pourra pas accéder aux informations concernant l'administrateur.

Il est également envisageable de filtrer les informations en fonction de l'endroit d'où une personne accède à l'annuaire. Par exemple, un annuaire peut avoir une interface privée et une interface publique. Les informations dites publiques étant accessibles depuis Internet, et les informations privées seulement depuis un intranet.

Enfin, recoupant la contrainte de flexibilité, il doit être possible de contrôler précisément la délégation des responsabilités.

4. C'est quoi Active Directory :

Active Directory est un annuaire introduit par Windows 2000 Server et destiné à être installé sur les Windows Server. En stockant dans une base de données les renseignements relatifs aux ressources réseau d'un domaine, Son implémentation permet de centraliser des informations relatives aux utilisateurs et aux ressources d'une entreprise en fournissant des mécanismes d'identification et d'authentification tout en sécurisant l'accès aux données. Ces fonctions additionnelles permettent aux administrateurs de gérer efficacement une stratégie de groupe, ainsi que l'installation des logiciels et des mises à jour sur les stations du réseau.

5. Etude d'Active Directory :

5.1. Rôle d'Active Directory :

Active Directory est le service d'annuaire de la famille Windows Server 2012 R2. Il étend la fonctionnalité de base d'un service d'annuaire et fournit les avantages suivants :

- **Intégration DNS :** Active Directory utilise les conventions d'attribution de noms DNS pour créer une structure hiérarchique qui fournit une vue familière, ordonnée et évolutive des connexions réseau. DNS sert également à faire correspondre les noms d'hôtes, tels que google.com, à des adresses numériques TCP/IP, telles que 192.168.1.120.
- **Évolution :** Active Directory est organisé en sections qui permettent de stocker un très grand nombre d'objets. Active Directory peut de ce fait évoluer en fonction des besoins de l'entreprise. Une organisation qui dispose d'un seul serveur avec quelques centaines d'objets peut évoluer vers des milliers de serveurs et des millions d'objets.
- **Administration centralisée :** Active Directory permet aux administrateurs d'administrer les ordinateurs distribués, les services réseau et les applications à partir d'un emplacement central tout en utilisant une interface d'administration cohérente. Active Directory fournit également un contrôle centralisé de l'accès aux ressources réseau en permettant aux utilisateurs d'ouvrir une fois une session et d'obtenir un accès complet aux ressources d'Active Directory.
- **Administration déléguée :** La structure hiérarchique d'Active Directory permet de déléguer le contrôle d'administration sur des parties spécifiques de la hiérarchie. Un utilisateur autorisé par une autorité administrative plus élevée peut effectuer des tâches d'administration dans la partie de la structure qui lui a été affectée.

5.2. Objets d'Active Directory :

Active Directory est un service d'annuaire utilisé pour stocker des informations relatives aux ressources réseau sur un domaine.

Une structure Active Directory (AD) est une organisation hiérarchisée d'objets. Les objets sont classés en trois grandes catégories : les ressources (par exemple

les imprimantes), les services (par exemple le courrier électronique) et les utilisateurs (comptes utilisateurs et groupes). L'AD fournit des informations sur les objets, il les organise et contrôle les accès et la sécurité.

Le nombre de types d'objets disponibles dans un Active Directory n'est pas limité, en voici quelques exemples :

- Ordinateur
- Utilisateur
- Imprimante
- L'Unité d'Organisation : Dans l'arborescence, ce sont des conteneurs qui permettent de créer une hiérarchie d'objets au sein d'un domaine. Ces OU sont principalement utilisées pour permettre la délégation de droits et pour l'application de GPO. Les OU sont parfois confondues avec les groupes, qui sont des objets et non des conteneurs.

- Groupe : il est principalement destiné à établir des listes d'utilisateurs pour leur attribuer des droits ou des services. On distingue trois types de groupes :

    - Le groupe local : il ne peut comprendre que des utilisateurs de son propre domaine.
    - Le groupe global : au sein d'un domaine, il est principalement utilisé pour affecter des droits à des ressources dans un domaine. Il peut comprendre des utilisateurs, des groupes globaux ou universels, issus d'autres domaines.
    - Le groupe universel : disponible depuis la version 2000, permet d'inclure des groupes et utilisateurs d'autres domaines.

Figure 3: objets d'active directory

5.3. Base de données d'active directory :

Active Directory est un annuaire, il lui faut donc enregistrer les informations qu'il contient dans une base de donnée. Cette base de données est modélisée sous la forme d'un seul fichier, appelé ntds.dit, et localisé dans %systemroot%\NTDS\ntds.dit.

L'extension de ce fichier, DIT, signifie Directory Information Tree, ou arborescence d'informations de l'annuaire. Cette base de données est basée sur la base ESE (Extensible Storage Engine), créée à l'origine pour Microsoft Exchange Server. Elle peut stocker plusieurs millions d'objets, et atteindre une taille maximale théorique de 70To.

Dans le répertoire accueillant la base de données d'Active Directory, se trouvent également les journaux des transactions (ebd*.log). Ces journaux sont circulaires, ce qui peut être assez déroutant pour un administrateur venant du monde Unix. Afin d'éviter une perte des journaux dans le cas où le système viendrait à manquer d'espace disque, Windows 2000 créée deux fichiers de journaux réservés, res1.log et res2.log.

5.4. Structure d'Active Directory :

5.4.1. Structure logique d'Active Directory :

Active Directory fournit un stockage sécurisé des informations sur les objets dans sa structure logique hiérarchique.

Les objets Active Directory représentent des utilisateurs et des objets tels que des ordinateurs et des imprimantes. Certains objets contiennent d'autres objets.

Une fois que vous avez compris les rôles et les fonctions de ces objets, vous pouvez effectuer diverses tâches, telles que la configuration, la gestion et le dépannage d'Active Directory.

La structure logique d'Active Directory inclut les composants suivants :

- **Les objets :** Il s'agit des composants les plus élémentaires de la structure logique. Les classes d'objets sont des modèles pour les types d'objets que vous pouvez créer dans Active Directory. Chaque classe d'objet est définie par une liste d'attributs, qui définit les valeurs possibles que vous pouvez associer à un objet. Chaque objet possède une combinaison unique de valeurs d'attributs.
- **Les unités d'organisations (OU) :** Vous utilisez ces objets conteneurs pour organiser d'autres objets de telle manière qu'ils prennent en compte vos objectifs administratifs. La disposition de ces objets par unité d'organisation simplifie la recherche et la gestion des objets. Vous pouvez également déléguer l'autorité de gestion d'une unité d'organisation. Les unités d'organisation peuvent être imbriquées les unes dans les autres, ce qui simplifie d'autant la gestion d'objets.
- **Les domaines :** Unités fonctionnelles centrales dans la structure logique d'Active Directory, les domaines sont un ensemble d'objets définis

administrativement qui partagent une base de données d'annuaire commune, des stratégies de sécurité et des relations d'approbation avec d'autres domaines. Les domaines disposent des trois fonctions suivantes :

• Une limite d'administration pour objets

• Une méthode de gestion de la sécurité pour les ressources partagées

• Une unité de réplication pour les objets

- **Les arborescences de domaines :** Les domaines regroupés en structures hiérarchiques sont appelés arborescences de domaines. Lorsque vous ajoutez un second domaine à une arborescence, il devient enfant du domaine racine de l'arborescence. Le domaine auquel un domaine enfant est attaché et appelé domaine parent. Un domaine enfant peut à son tour avoir son propre domaine enfant. Le nom d'un domaine enfant est associé à celui de son domaine parent pour former son nom DNS (Domain Name System) unique, par exemple sdsi.cnas.blida. De cette manière, une arborescence a un espace de noms contigu.
- **Les forêts :** Une forêt est une instance complète d'Active Directory. Elle consiste en une ou plusieurs arborescences. Dans une arborescence unique à deux niveaux, qui est recommandée pour la plupart des organisations, tous les domaines enfants sont des enfants du domaine racine de la forêt afin de former une arborescence contiguë. Le premier domaine de la forêt est appelé le domaine racine de la forêt. Le nom de ce domaine fait référence à la forêt, par exemple nwtraders.msft. Par défaut, les informations dans Active Directory ne sont partagées qu'à l'intérieur de la forêt. Ainsi, la forêt est une limite de sécurité pour les informations contenues dans l'instance d'Active Directory.

5.4.2. Structure physique d'Active Directory :

Contrairement à la structure logique, qui modélise des exigences administratives, la structure physique d'Active Directory optimise le trafic réseau en déterminant où et quand se produit un trafic de connexions et de réplications. Pour optimiser l'utilisation par Active Directory de la bande passante du réseau, vous devez en comprendre la structure physique. Les éléments de la structure physique d'Active Directory sont :

- **Les contrôleurs de domaine :** Ces ordinateurs exécutent Microsoft Windows Server. 2003 ou Windows® 2000 Server et Active Directory. Chaque contrôleur de domaine exécute des fonctions de stockage et de réplication. Un contrôleur de domaine ne peut gérer qu'un seul domaine. Pour assurer une disponibilité permanente d'Active Directory, chaque domaine doit disposer de plusieurs contrôleurs de domaine.
- **Les sites Active Directory :** Ces sites sont des groupes d'ordinateurs connectés par des liaisons rapides. Lorsque vous créez des sites, les contrôleurs de domaine au sein d'un même site communiquent fréquemment. Ces communications réduisent le délai de latence de réplication à l'intérieur du site ; autrement dit, le temps requis pour qu'une modification effectuée sur un contrôleur de domaine soit répliquée sur d'autres contrôleurs de domaine. Vous pouvez donc créer des sites pour optimiser l'utilisation de la bande passante entre des contrôleurs de domaines situés à des emplacements différents.
- **Partitions Active Directory :** Chaque contrôleur de domaine contient les partitions Active Directory suivantes :

    - **La partition de domaine :** contient les réplicas de tous les objets de ce domaine. La partition de domaine n'est répliquée que dans d'autres contrôleurs appartenant au même domaine.

- **La partition de configuration :** contient la topologie de la forêt. La topologie est un enregistrement de tous les contrôleurs de domaine et des connexions entre eux dans une forêt.
- **La partition de schéma :** contient le schéma étendu au niveau de la forêt. Chaque forêt comporte un schéma de sorte que la définition de chaque classe d'objet est cohérente. Les partitions de configuration et de schéma sont répliquées dans chaque contrôleur de domaine dans la forêt.
- **Les partitions d'applications facultatives :** contiennent des objets non liés à la sécurité et utilisés par une ou plusieurs applications. Les partitions d'applications sont répliquées dans des contrôleurs de domaine spécifiés dans la forêt.

5.5. Les composants d'Active Directory :

Il existe différents composants dans Active Directory. A partir de Windows 2008, des termes sont apparus pour les désigner.

- **ADDS : Active Directory Domain Services**. Il s'agit du composant principal qui va gérer les utilisateurs, ordinateurs, stratégies de groupe, etc.
- **ADCS : Active Directory Certificate Services**. Il s'agit du composant d'autorité de certification. Il va nous permettre de générer des certificats de sécurité pour nos utilisateurs et notre réseau.
- **ADFS : Active Directory Federation Services**. Il s'agit du composant permettant la fédération de services entre différents environnements Active Directory. Cela permet à une entreprise d'établir des relations de confiance avec des partenaires externes (fournisseurs, fabricants, etc.) afin de leur donner un accès à certains de nos services internes de manière contrôlée et sécurisée.

- **ADLDS : Active Directory Lightweight Directory Services** (anciennement ADAM). C'est ADDS mais allégé : seul l'annuaire est disponible. Cela est utile dans les cas où nous avons besoin d'un accès à des données de l'Active Directory sans avoir une autorisation de lecture totale dessus. C'est utilisé notamment dans la passerelle d'hygiène d'Exchange (Edge). ADLDS contiendra une copie partielle de notre Active Directory.
- **ADRMS : Active Directory Rights Management Services**. Ce composant permet de gérer les droits de manière pointue dans notre entreprise. Il ne s'agit pas des droits sur le fichier mais sur le contenu du fichier.

5.6. Fonctionnalité d'active directory :

Active Directory dispose des fonctionnalités suivantes :

- Accès pour les utilisateurs et les applications aux informations concernant des objets. Ces informations sont stockées sous forme de valeurs d'attributs. Vous pouvez rechercher des objets selon leur classe d'objet, leurs attributs, leurs valeurs d'attributs et leur emplacement au sein de la structure Active Directory ou selon toute combinaison de ces valeurs.

- Transparence des protocoles et de la topologie physique du réseau. Un utilisateur sur un réseau peut accéder à toute ressource, une imprimante par exemple, sans savoir où celle-ci se trouve ou comment elle est connectée physiquement au réseau.

- Possibilité de stockage d'un très grand nombre d'objets. Comme il est organisé en partitions, Active Directory peut répondre aux besoins issus de la croissance d'une organisation. Par exemple, un annuaire peut ainsi passer

d’un serveur unique contenant quelques centaines d’objets à des milliers de serveurs contenant des millions d’objets.

- Possibilité d’exécution en tant que service indépendant du système d’exploitation. AD/AM (Active Directory in Application Mode) est une nouvelle fonctionnalité de Microsoft Active Directory permettant de résoudre certains scénarios de déploiement liés à des applications utilisant un annuaire. AD/AM s’exécute comme un service indépendant du système d’exploitation qui, en tant que tel, ne nécessite pas de déploiement sur un contrôleur de domaine. L’exécution en tant que service indépendant du système d’exploitation signifie que plusieurs instances AD/AM peuvent s’exécuter simultanément sur un serveur unique, chaque instance étant configurable de manière indépendante.

Chapitre III

Présentation de l'entreprise

« CNAS »

Chapitre III : Présentation de l'entreprise « CNAS »

1. Introduction :

Caisse nationale des assurances sociales (CNAS), La CNAS est un établissement public national à caractère administratif jouissant d'une personnalité juridique et d'une autonomie financière, en application de l'article 49 de la loi no 88-01 du 12 janvier 1988. La CNAS est administrée par un Conseil d'Administration, elle est placée sous la tutelle du Ministre du travail, de l'Emploi et de la Sécurité sociale.

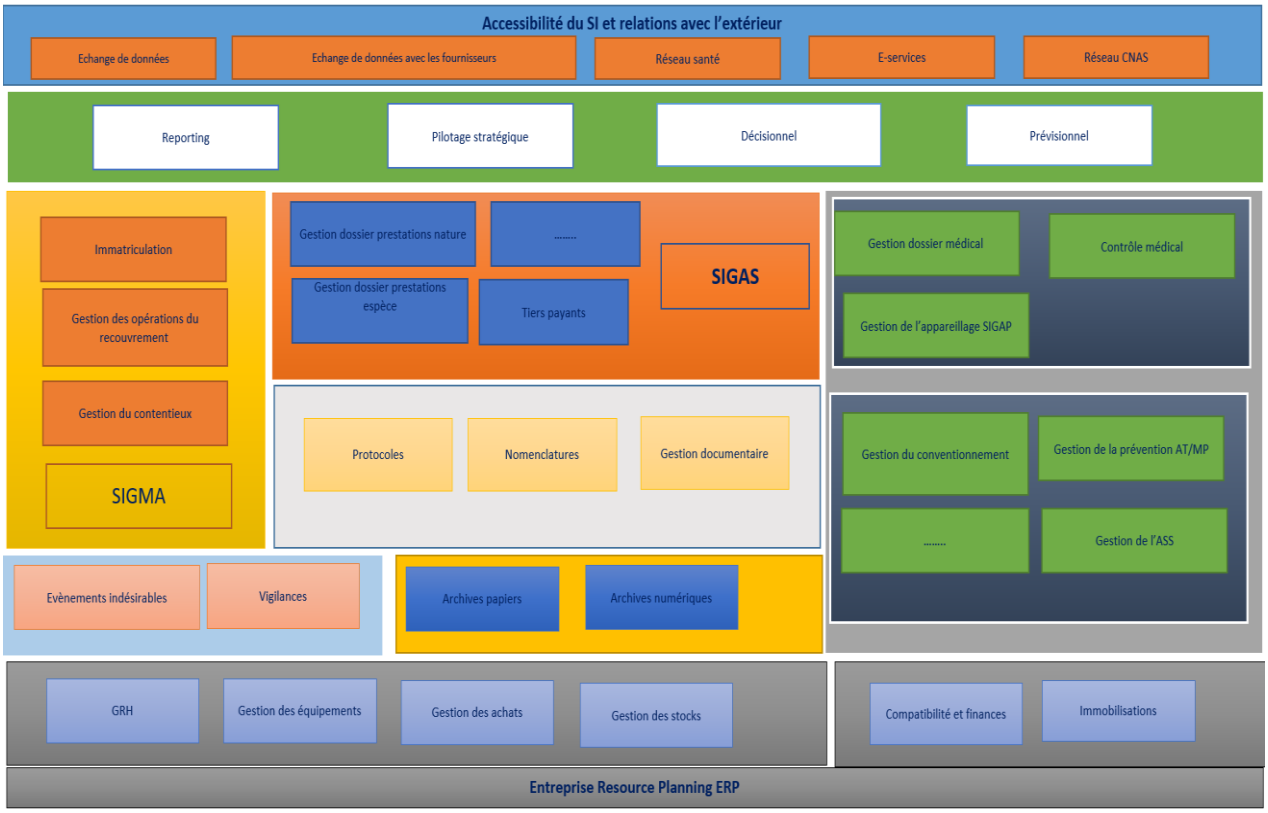

Figure 4: Schéma de la CNAS

Ce projet a été réalisé au sein de la sous-direction des systèmes d'information (SDSI) de la CNAS Blida,

2. La sous-direction des systèmes d’information :

Le suivi informatique de la Caisse Nationale de Prévoyance Sociale des Salariés est l'axe d'activité le plus important, dans lequel l'amélioration du service public a occupé une place dans son agenda, dans le cadre d'un format complet et intégré et d'une série de procédures clés pour simplifier les démarches administratives et réduire du fardeau des documents exigés des citoyens pour obtenir la sortie.

3. Le système d’information de la CNAS :

Il traite des données relatives à diverses activités et branches afin de collecter, organiser et stocker des informations.

Le système assure un service public à part entière, puisqu'il contient l'ensemble des applications et plateformes numériques d'où émanent les e-services, destinés aux bénéficiaires et contractants du CNAS, y compris les professionnels de santé et diverses institutions, et met à la disposition des décideurs les données et informations nécessaires pour les processus de planification et de prise de décision.

4. Les réalisations :

- **Dans le domaine de l'organisation :**

Restructuration de la Direction de la Modernisation et des Systèmes d'Information, et l'installation de la Sous-Direction de la Sécurité de l'Information, en application du Décret Présidentiel 20-05 du 20 janvier 2020.

- **Dans le domaine de la formation :**

Les ressources humaines reçoivent une formation spécialisée dans le domaine des technologies modernes de numérisation.

- **Renforcer la confiance dans la numérisation :**

Renforcement de la communication interne sur la transformation numérique et les nouveaux projets de l'entreprise.

Diffuser l'esprit d'appartenance, de participation et de créativité.

5. Les services numériques :

5.1. La plateforme numérique « El-Hanna » :

- Imprimer les relevés de compte pour les performances soumises.
- Connaître l'usage des médicaments.
- Le pourcentage de couverture sociale et la date de fin d'éligibilité aux paiements.
- Dépôt de maladie à distance.
- Délivrance d'une attestation d'affiliation à la Sécurité Sociale.
- Recevez diverses notifications.
- Demande de carte Chifaa à distance.
- Demande de capital décès à distance.

5.2. Notifications par SMS :

- Recevoir des convocations médicales.
- Recevoir le montant du remboursement de l'ordonnance.
- Recevoir une indemnité journalière.

- Prise de rendez-vous au niveau des centres régionaux d'imagerie médicale.
- Une invitation à recevoir la carte Chifa.

5.3. La plateforme numérique « télé-déclaration » :

- Paiement des abonnements par paiement électronique
- Consultation et extraction des attestations d'affiliation des travailleurs.
- Vérifier les déclarations annuelles.
- Demander la numérotation et l'affiliation des employés.
- Demander une carte de reprise au profit des salariés.
- Déclaration des réceptacles de souscription à la sécurité sociale
- Visualisation, extraction et appariement du certificat d'exécution des créances.
- Numériser les dossiers des employeurs pour examen au niveau national.

5.4. Plateforme mutuel social :

Il s'agit d'un espace électronique orienté vers la gestion électronique de la relation contractuelle avec les partenaires sociaux contractants et la mise à jour automatique des droits en matière de parrainage de 20%, afin que l'assuré bénéficie de 100% des versements dans le cadre du système de tiers payant.

5.5. Plateforme contractuel numérique :

Il est orienté vers la gestion électronique des relations contractuelles avec divers praticiens de santé conventionnés (cliniques cardiaques - cliniques obstétriques, centres d'hémodialyse et concessionnaires de transport sanitaire).

6. Mesures prises pour protéger et sécuriser les systèmes d'information de la CNAS :

- Adoption d'un nouveau système interne,
- Adoption d'un réseau d'information avec une ingénierie plus moderne,
- En utilisant du matériel et des logiciels très avancés pour assurer la protection,
- Mise en service du centre de réserve des systèmes d'information,
- Création d'une direction subsidiaire pour la sécurité de l'information.

7. Les perspectives que la CNAS aspire à atteindre :

- Adoption d'une infrastructure très avancée et hautement disponible (SDWAN),
- Adoption de dispositifs modernes d'assurance contre les risques cyber,
- Augmenter la vitesse de circulation à travers les agences régional,
- Achever le processus de généralisation du système de gestion des processus de collecte,
- Achever le processus de généralisation du système de gestion des ressources de planification l'ERP,
- Dédier le travail avec la technologie de conférence à distance,
- Mise à jour et développement du système CHIFA.

8. Conclusion :

L'objectif fondamental de la CNAS pour les services numériques est d'améliorer et de moderniser le service public, de lutter contre la bureaucratie et d'abandonner progressivement l'émission de documents papier pour permettre aux citoyens d'obtenir des paiements basés sur les technologies de l'information.

Chapitre IV

Implémentation d'Active Directory

Chapitre IV : implémentation d'Active Directory

1. Introduction :

Une fois le plan d'implémentation d'Active Directory en place, on peut commencer à implémenter Active Directory conformément à notre plan de conception.

Dans ce chapitre on va montrer les tâches qu'on doit exécuter Pour implémenter Active Directory.

2. Installation de Windows server 2012 R2 :

On commence l'installation de **Windows server 2012** après la création d'une machine virtuelle en utilisant le logiciel **VMware.**

Tout d'abord on a besoin d'un CD Windows server 2012 r2 ou bien une image ISO de ce dernier

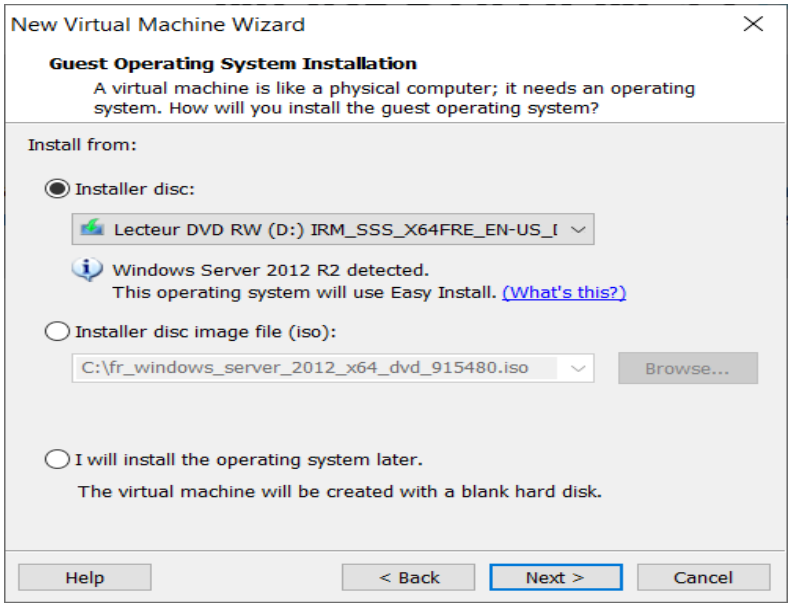

Figure 5: création d'une machine virtuelle

Ensuite on définit les caractéristiques de notre machine virtuelle.

Dans ce cas on a une machine dont les caractéristiques sont les suivants :

- Disque dur : 60GB
- RAM : 4GB
- Système d'exploitation : Windows server 2012 R2

- Emplacement : C:\Users\Lenovo\OneDrive\Documents\Virtual Machines\Windows Server 2012

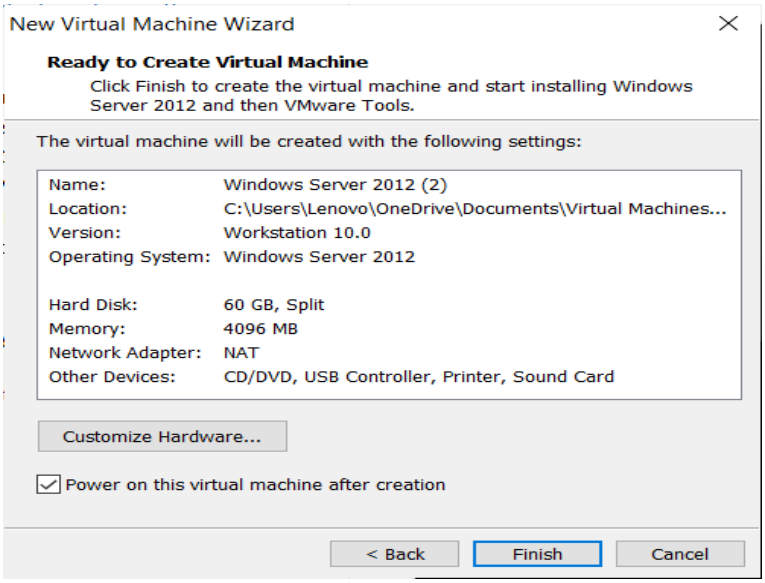

Figure 6 : les caractéristiques de la machine virtuelle

Une fois on clique sur **finish** l'installation de Windows server 2012 R2 commence.

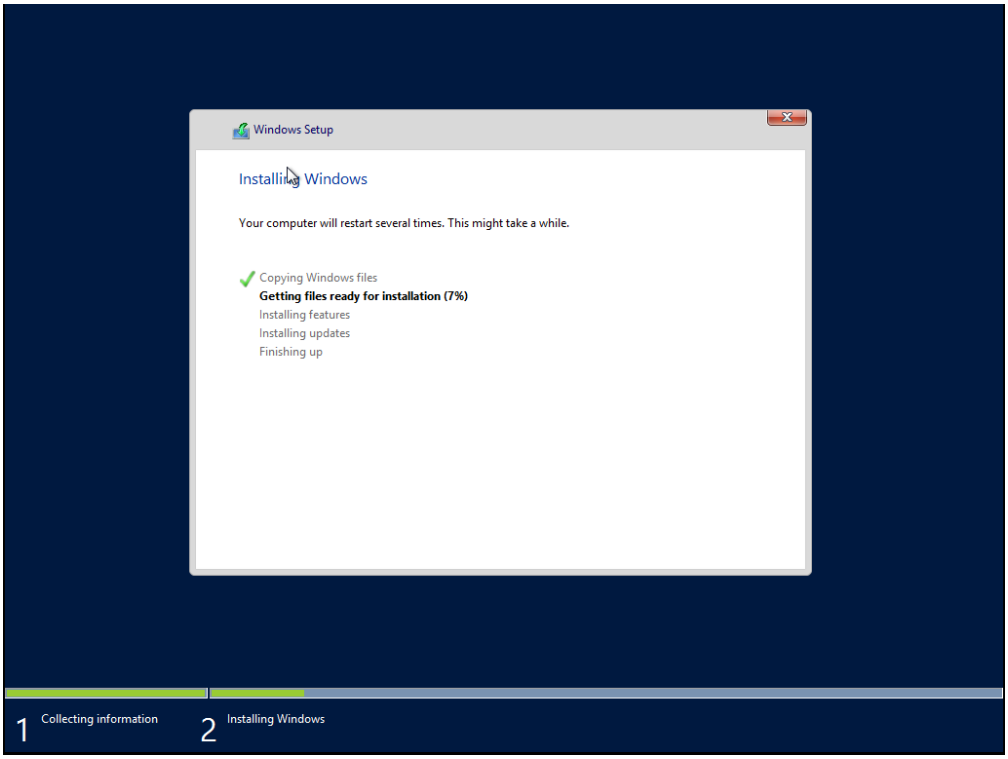

Figure 7 : installation de Windows server 2012 R2

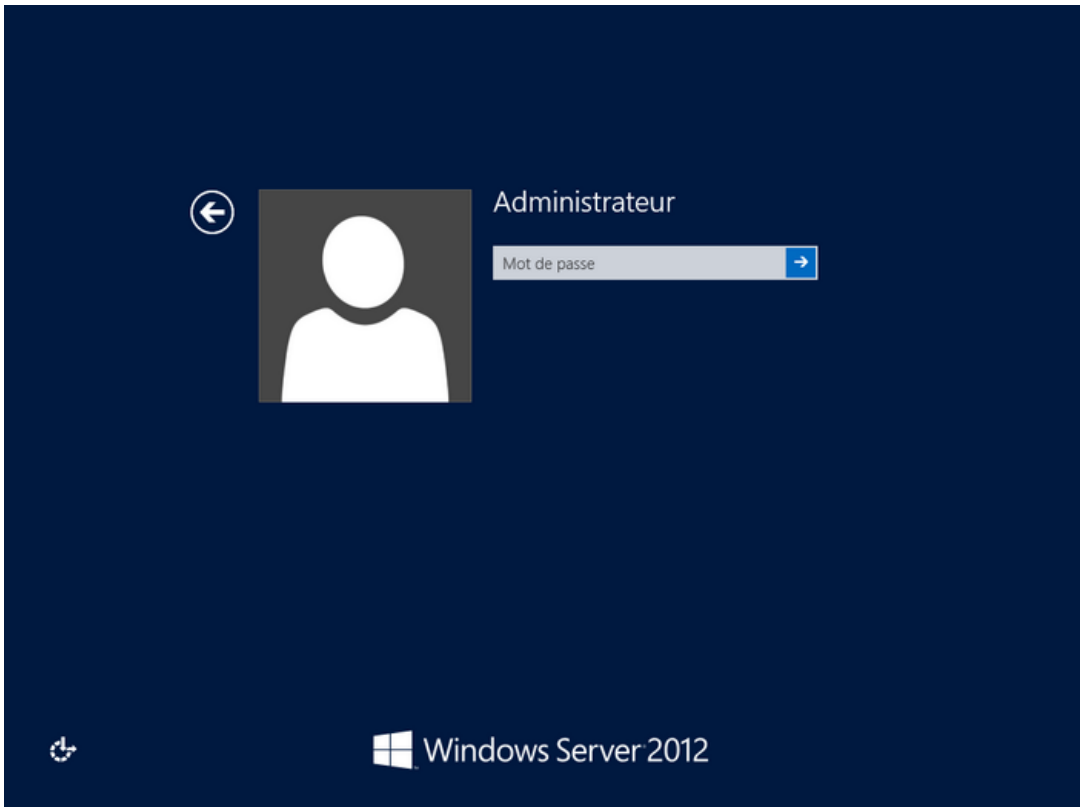

Figure 8 : session Administrateur

3. Installation d'Active Directory :

Pour installer le rôle Active Directory il faut suivre les étapes suivantes :

- Ouvrir **le gestionnaire de server** (server manager)

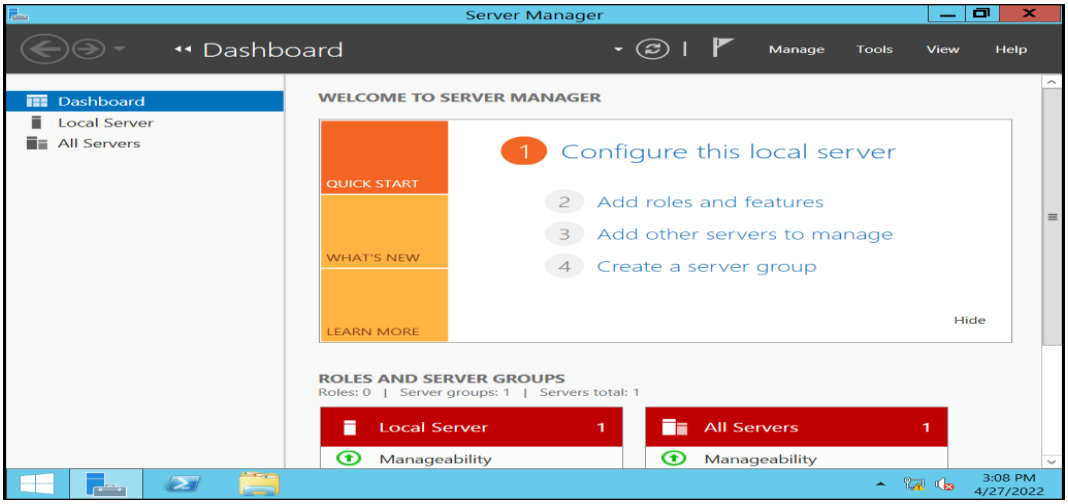

Figure 9 : gestionnaire de serveur

- Cliquer sur **Manage → add roles and features** (ajouter des rôles et des fonctionnalités)

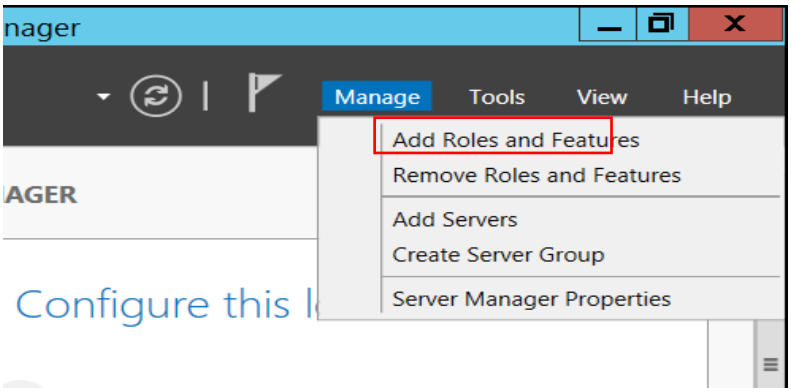

Figure 10 : ajouter des rôles et des fonctionnalités

- Jusqu'à la deuxième étape on laisse le choix par défaut
- Le type d'installation doit être basé sur un seul rôle. On installe l'ADDS uniquement sur ce serveur

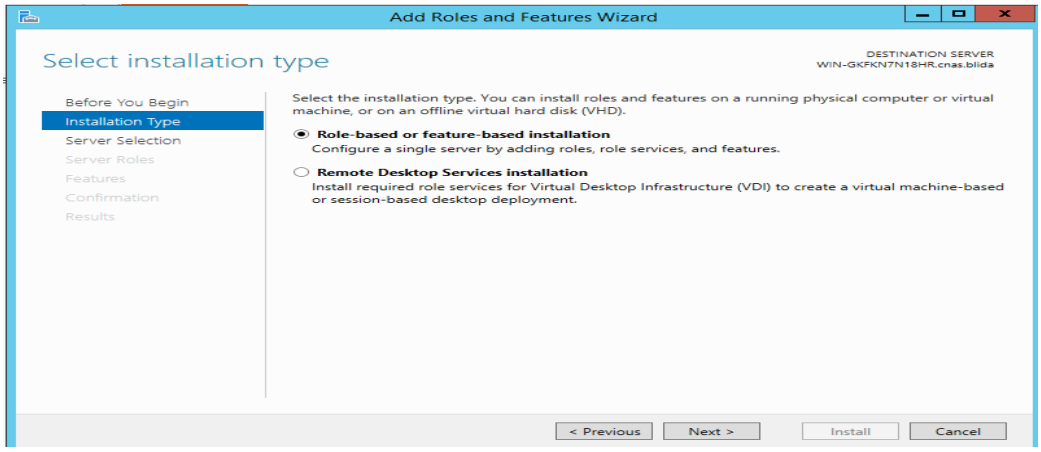

Figure 11 : Type d'installation du Active Directory

- La prochaine étape est de sélectionner le serveur, dans notre cas on a un seul server on le sélectionne et on clique sur **Next**

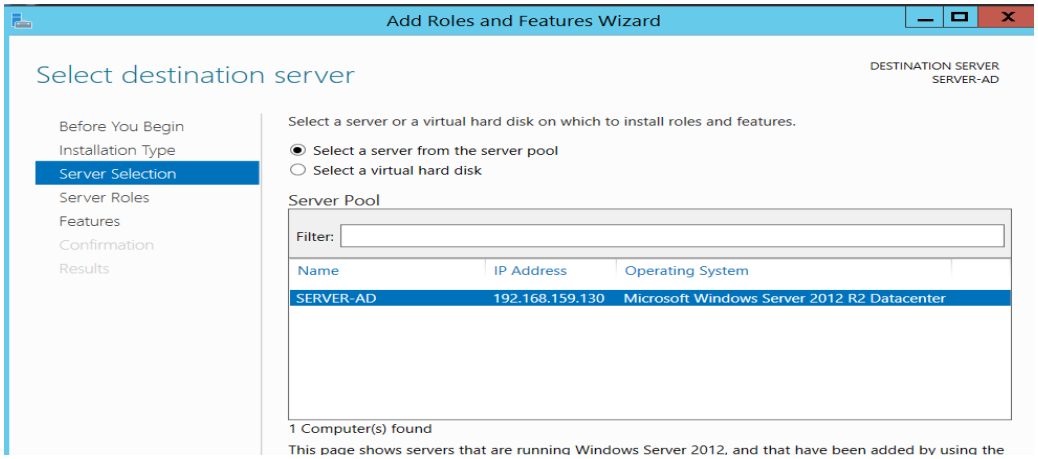

Figure 12 : Sélectionner un serveur

- La quatrième étape est de cochet les rôles qu'on souhaite installer. On sélectionne **« Active Directory domaine services »** et on clique sur **Next**

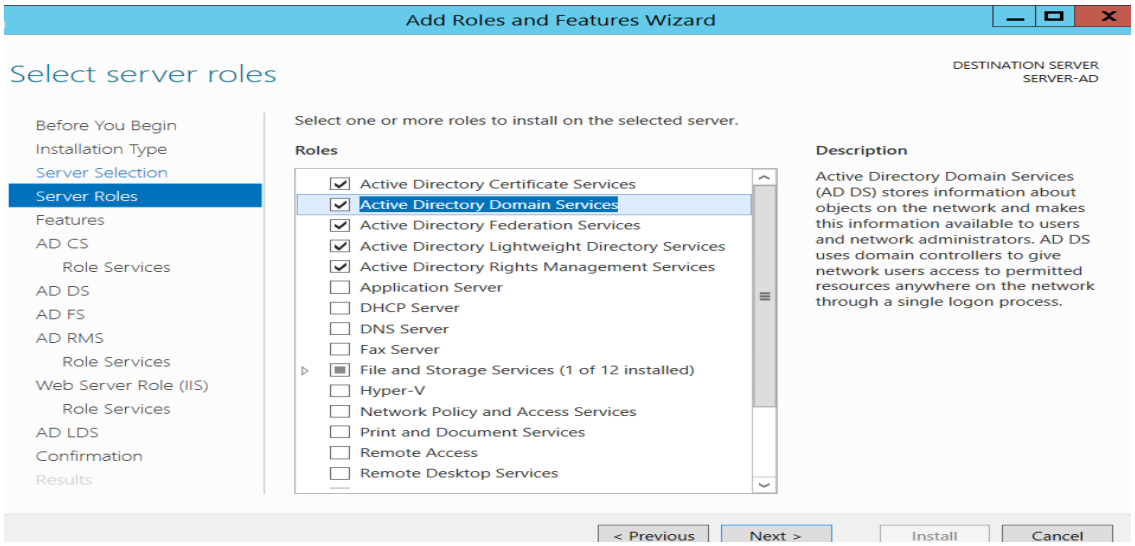

Figure 13 : Les rôles qu'on souhaite installer

- On passe à l'étape de confirmation, on vérifie si tous les données sont juste et on clique sur installe

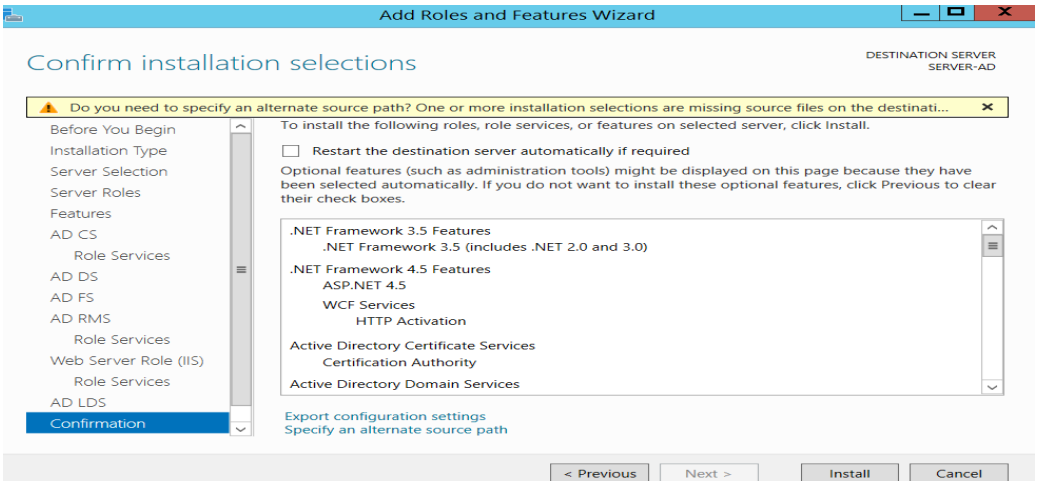

Figure 14 : vérification des données et installation

- On attend la fin de l'installation et on clique sur close.

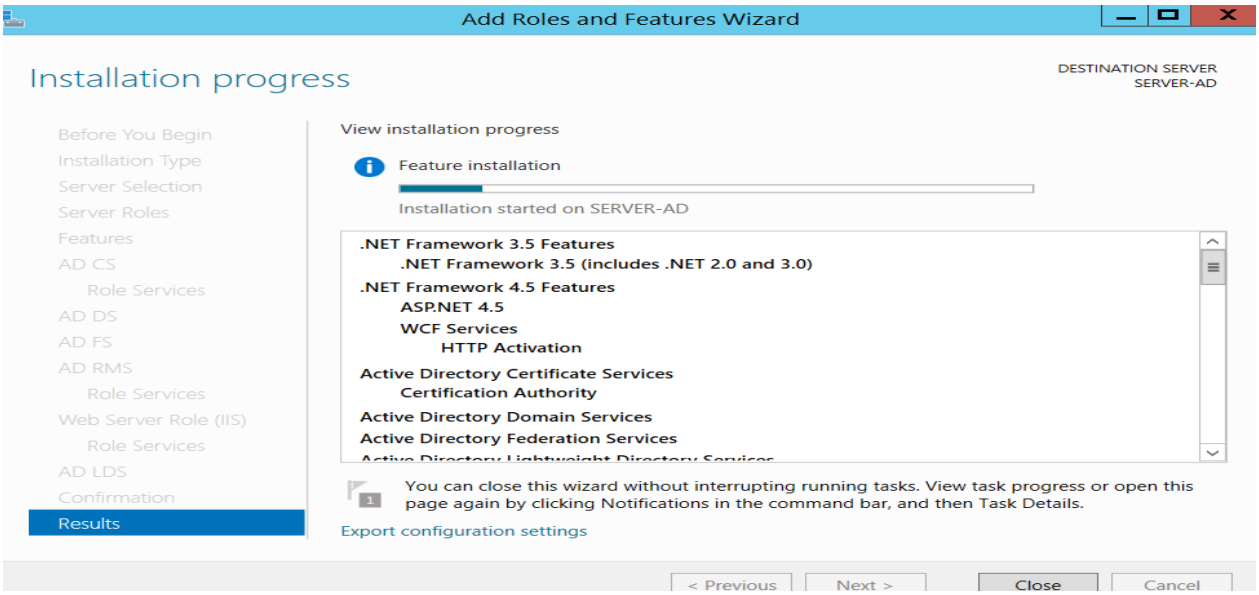

Figure 15 : progrès d'installation

4. Configuration du rôle AD DS :

Dès que l'installation d'Active directory est terminée, on revient au gestionnaire de serveur et on clique sur le **drapeau de notifications** en haut de la fenêtre pour commencer la configuration.

Nous allons créer un **nouveau domaine** « cnas.blida » dans une **nouvelle forêt.**

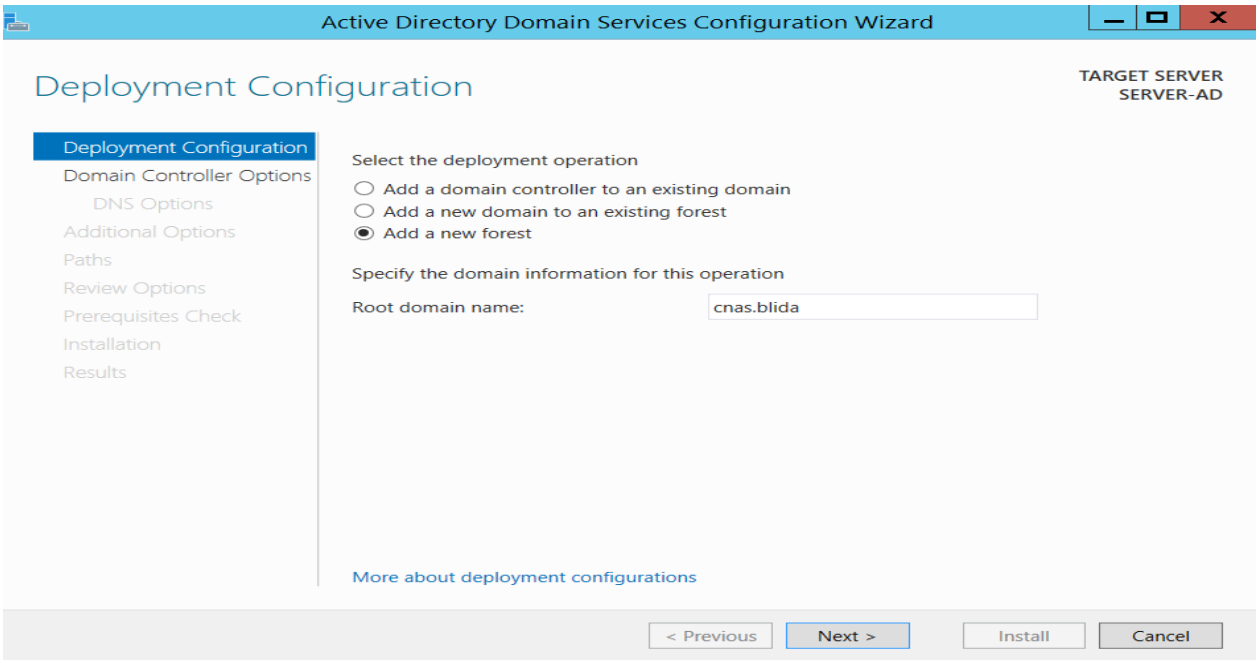

Figure 16 : Création d'un nouveau domaine

Ensuite, il faut choisir si vous voulez être compatible avec les anciennes versions de Windows.
Si on sélectionne une ancienne version, certaines fonctionnalités de "Windows Server 2012" seront désactivées donc on va pas choisir une version ancienne tant qu'on a pas de pc avec d'anciennes versions de Windows.
S'il vous demande de choisir, c'est simplement parce que les droits ne fonctionnent pas de la même manière sur les anciennes et les nouvelles versions de "Windows"

- On doit aussi choisir un mot de passe pour la restauration des services d'annuaire. Le mot de passe pour le mode de restauration des services d'annuaire (DSRM) doit être différent de celui du compte Administrateur.

On clique sur **suivant** pour continuer.

- Le nom **NetBIOS** est automatiquement défini suivant le nom de domaine que nous avons indiqué précédemment. On peut bien sûr le modifier manuellement si nécessaire.
- L'étape suivante est de définir l'emplacement des dossiers contenants la base de données, les fichiers journaux et le SYSVOL, on va les laisser par défaut et on clique sur suivant

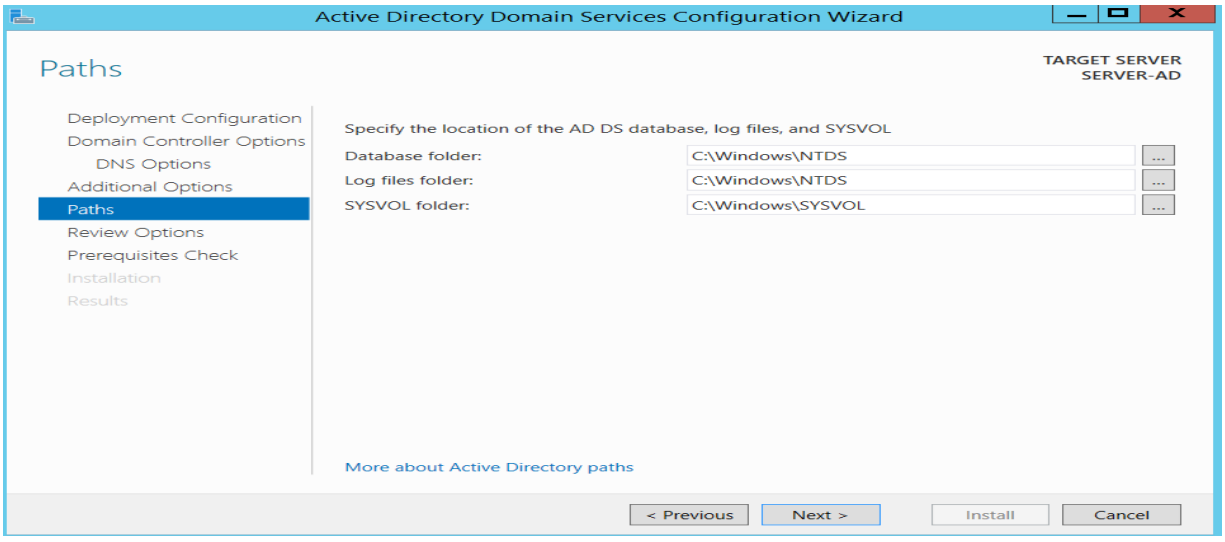

Figure 17 : l'emplacement de la base de données, fichiers journaux et SYSVOL

Et enfin, l'assistant nous affiche un résumé de la configuration de notre Active Directory.

Lors de la vérification de la configuration de notre serveur, on obtient plusieurs avertissements. Le seul qui est intéressant dans notre cas est celui concernant les adresses IP de nos cartes réseau.
Un serveur doit toujours avoir une adresse IP statique pour ne pas que celle-ci ne change à un moment donné.

Pour définir l'adresse IP du serveur on suit les étapes suivantes :

- Ouvrir le centre de réseau et partage.
- Cliquer sur **modifier les paramètres de la carte.**
- On fait un clic droit sur notre carte réseau et cliquer sur **propriétés.**
- Cliquez sur **"Protocole Internet version 4 (TCP/IPv4)" → Propriétés.**
- Sélectionnez **"Utiliser l'adresse IP suivante"** et définissez une adresse IP statique ainsi qu'un Serveur DNS préféré.

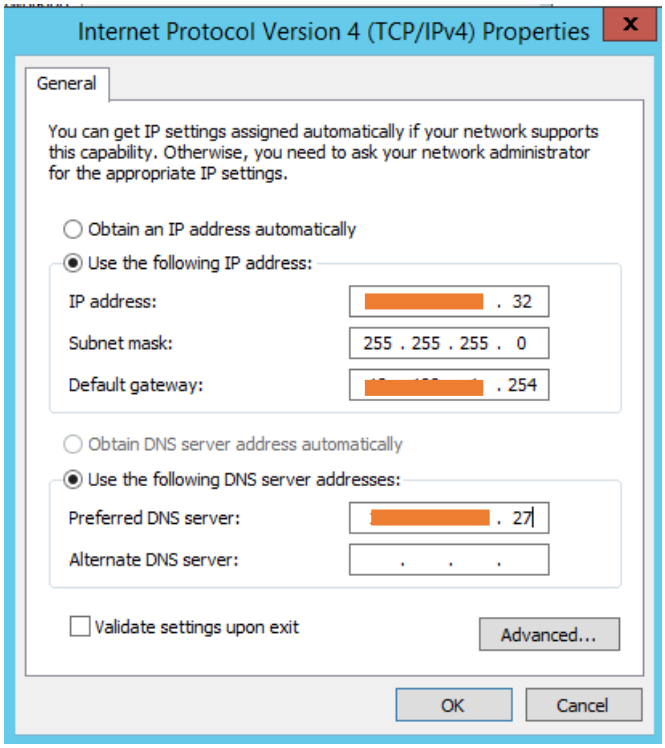

Figure 18 : Ajouter une adresse IP et adresse dns

Maintenant on peut installer la configuration qu'on a venez de faire.

5. Gestion des comptes :

5.1. Création d'une unité d'organisation :

Avant de créer un compte utilisateur on doit tout d'abord créer une unité d'organisation pour deux raisons :

1. Pour mieux organiser notre travail
2. Pour donner des droits d'accès à ces derniers (on ne peut pas donner certain pouvoir pour un conteneur comme User)

On commence à créer une unité d'organisation :

- Cliquer sur **« tools »**
- Cliquer sur **« Active Directory users and computers »**

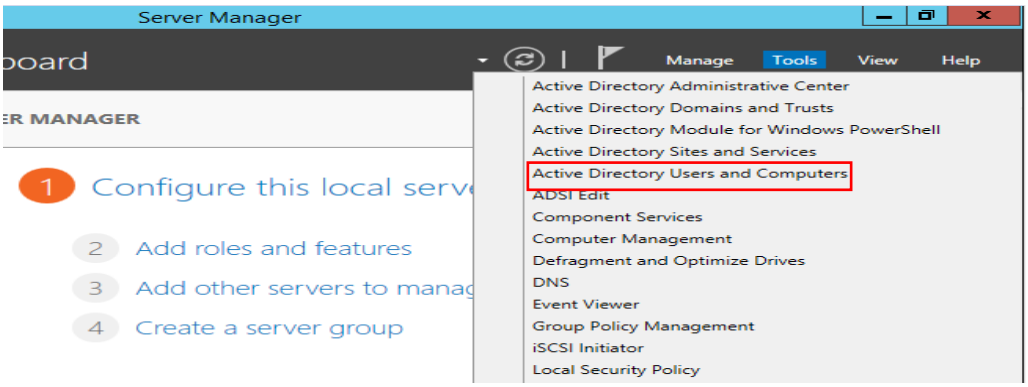

Figure 19 : chemin vers les utilisateurs et ordinateurs du domaine

Par une clique à droite sur le nom du domaine dans la fenêtre **« Active Directory users and computers »** on choisit **New → organizational unit**

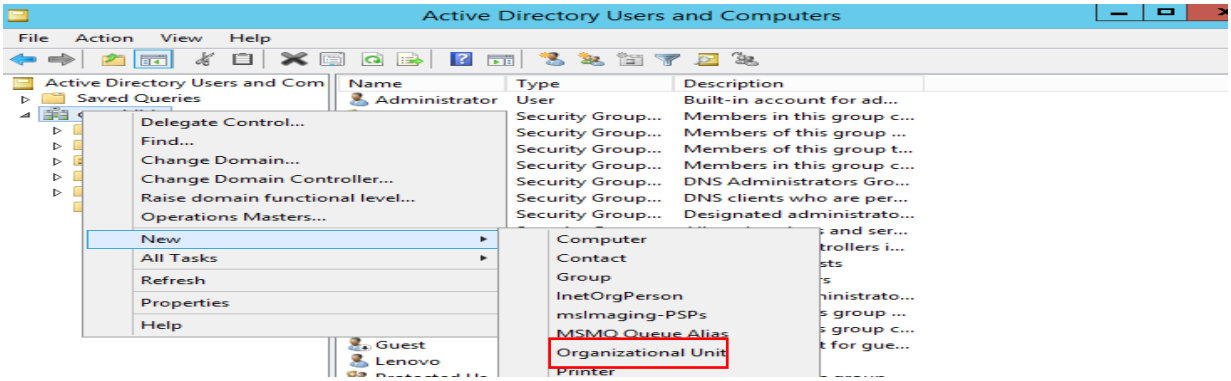

Figure 20 : le chemin pour ajouter un OU

- Une fenêtre **« Organizational Unit »** apparaitre

- On entre le nom de la nouvel unité d'organisation et on clique sur **OK**

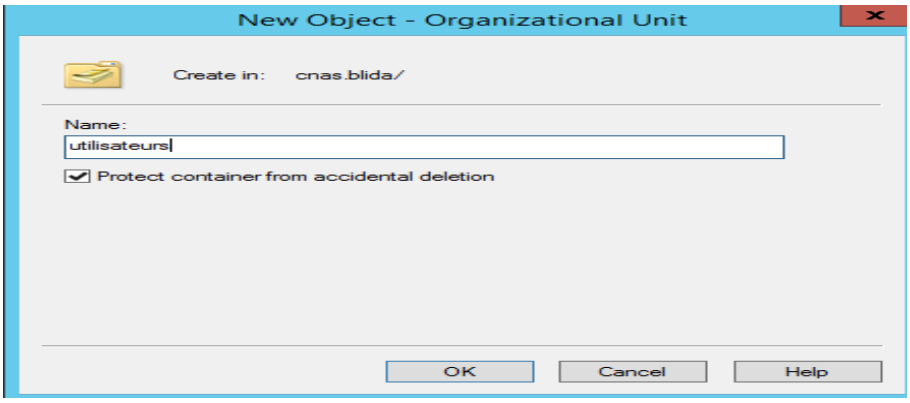

Figure 21 : nomination d'une unité d'organisation

5.2. Création d'un compte utilisateur :

Dans la nouvel OU on va créer une autre OU en suivant les mêmes étapes et on la donne le nom SDSI **« sous-direction des systèmes d'information »**

Et dans cette OU on va créer l'utilisateur :

- On clique à droite sur **« SDSI »** et on choisit **New → User**

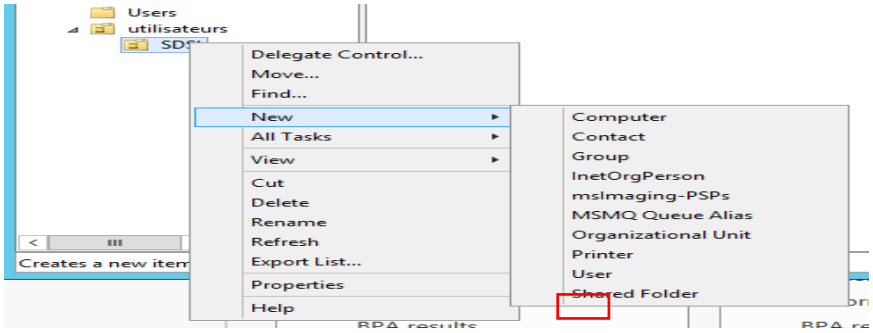

Figure 22 : ajouter un utilisateur

Une fenetre **« New object – User »** apparaitre

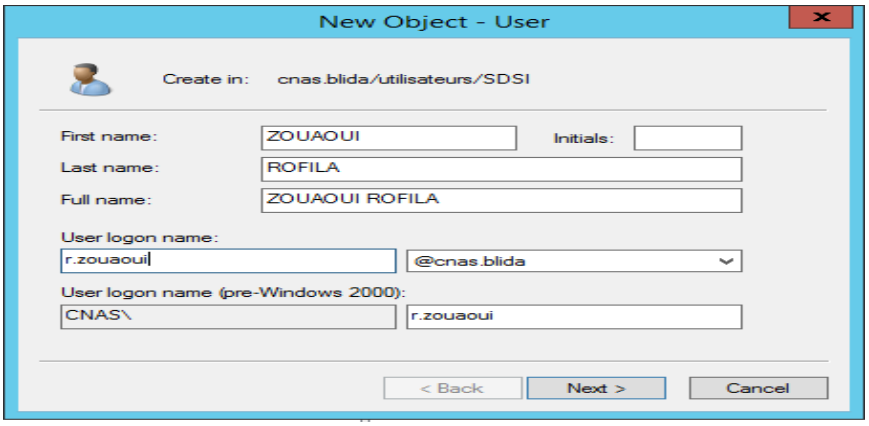

Figure 23 : insertion des informations de l'utilisateur

On entre les informations requises et on clique sur **Next**

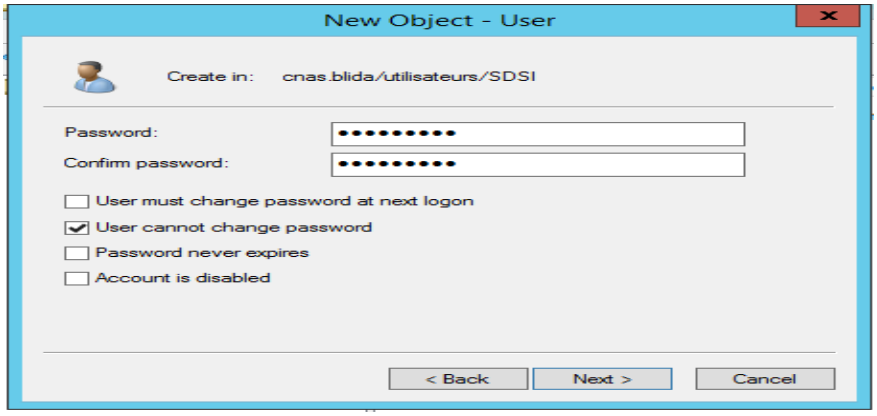

Figure 24 : ajouter un mot de passe à l'utilisateur

On entre le mot de passe et on clique sur **Next**

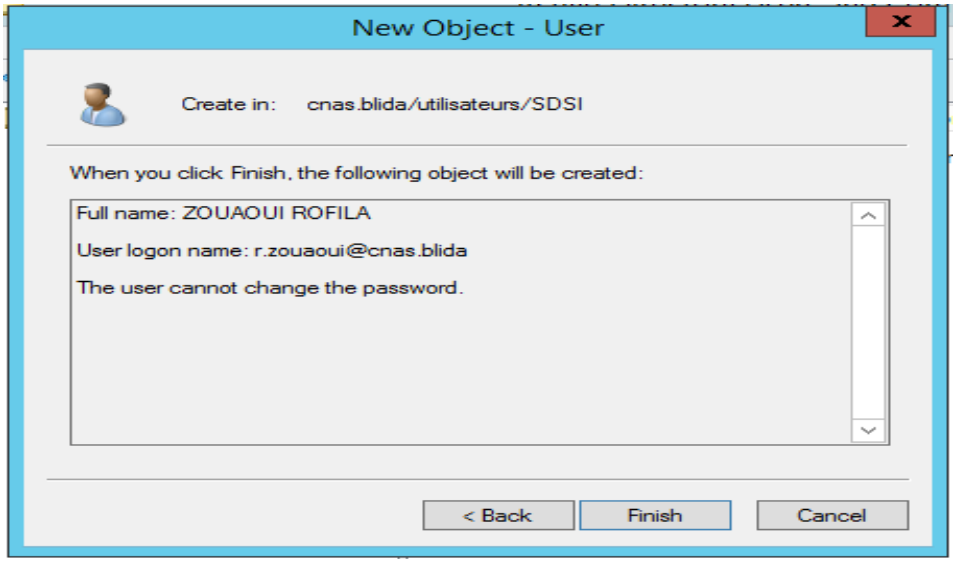

Figure 25 : création de l'utilisateur réussite

L’utilisateur ZOUAOUI ROFILA est dans le domaine et peut accéder à son compte par n’importe quel PC qui est encore dans le domaine en entrent son **« nom d’utilisateur »** et **« mot de passe »**

Dans ce cas on peut accéder à ce compte par deux méthode

1. Par le **nom d’utilisateur** r.zouaoui@cnas.blida et le **mot de passe**
2. Par le **nom d’utilisateur** CNAS\r.zouaoui et le **mot de passe**

5.3. Ajouter un ordinateur dans le domaine :

Pour connecter un ordinateur à un domaine on suit les étapes suivantes :

Dans les propriétés système on clique sur modifier

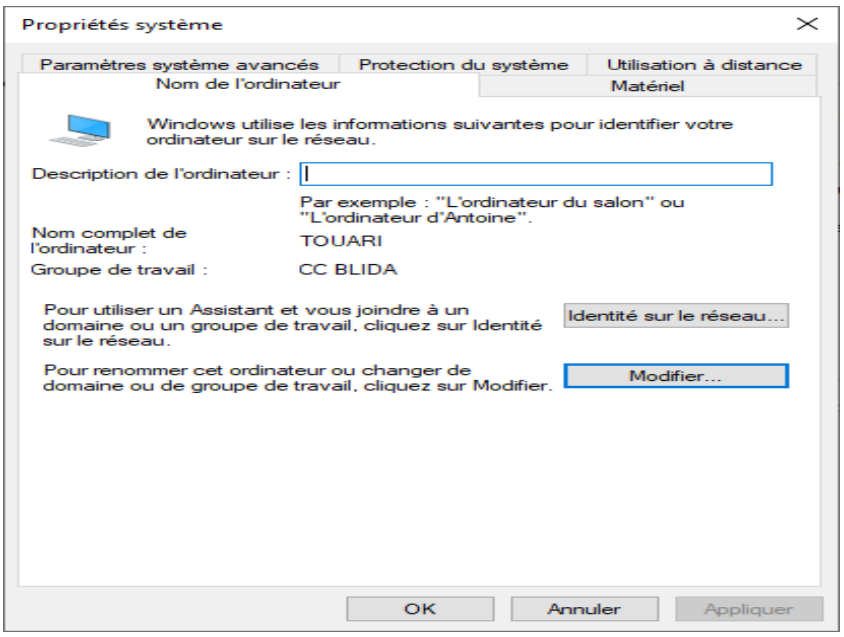

Figure 26 : propriétés du système

Une nouvelle fenêtre apparaitre « modification du nom ou du domaine de l’ordinateur » on introduit le nom du domaine et on clique sur OK

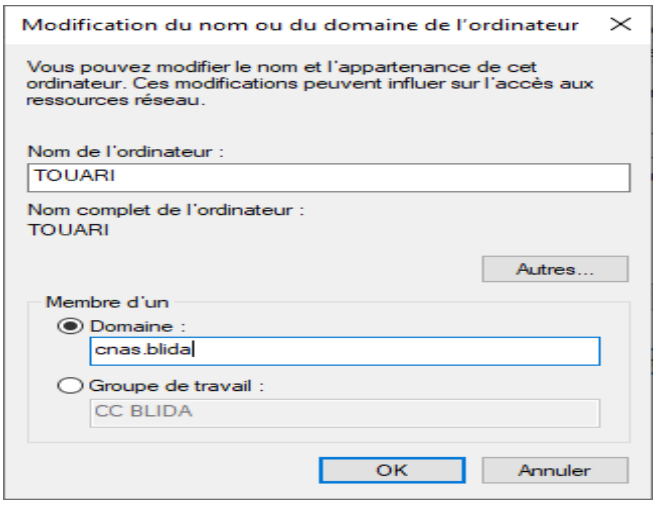

Figure 27 : changer le domaine de l'ordinateur

Si le nom du domaine est juste, le system demande une authentification avec le nom de l'utilisateur et le mot de passe de domaine.

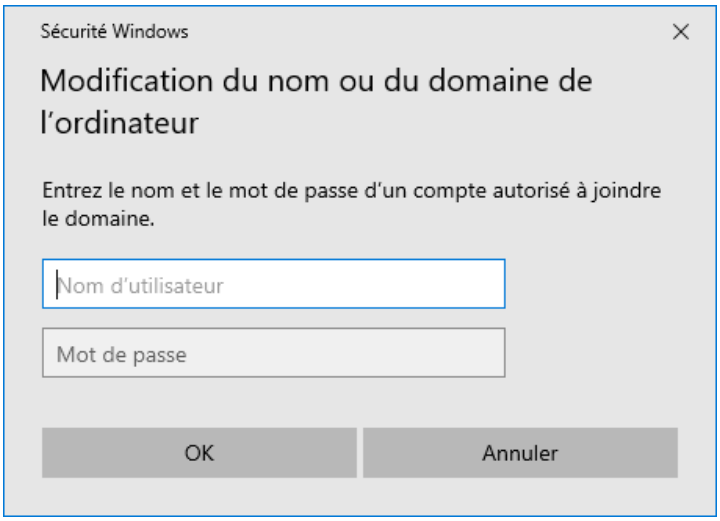

Figure 28 : entrer le nom et mot de passe du domaine

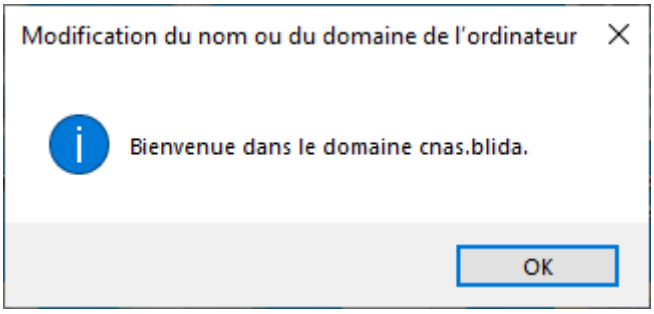

Figure 29 : message de bienvenue en domaine

Si le nom d'utilisateur et le mot de passe sont juste, un message « bienvenue dans le domaine cnas.blida » apparaitra.

6. Les stratégies de groupe « GPO » :

Une stratégie de groupe est un ensemble d'outils intégrés à Windows Server qui permet au service informatique de centraliser la gestion de l'environnement utilisateur et la configuration des machines grâce à l'application de politiques.

Chaque stratégie dispose de ses propres paramètres, définis par l'administrateur système, et qui seront appliqués ensuite à des postes de travail, des serveurs ou des utilisateurs.
Les GPO abritent de nombreuses options de configuration qui permettent de centraliser la gestion d'un parc informatique. Cela peut se faire tant au niveau utilisateur qu'un niveau ordinateur. Au final, bien maitrisés, les GPO vous garantissent une maîtrise de la configuration au sein de votre réseau.

6.1. Créer un groupe de comptes :

On souhaite appliquer une stratégie de groupe sur différents utilisateurs de différents OU, alors on droit tous d'abord créer un groupe dont les membres sont les utilisateurs précédents.

Pour créer un groupe il faut suivre les étapes suivantes :

- Cliquer sur tools du « server manager », sélectionner « active directory users and computers »
- Une clique droite sur le nom du domaine cnas.blida → New → Group

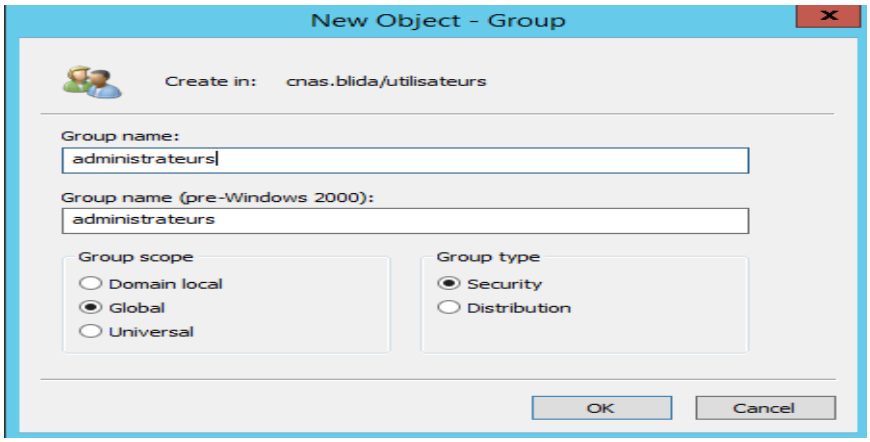

Figure 30 : création d'un groupe

- On remplit les champs vides et on clique sur OK.

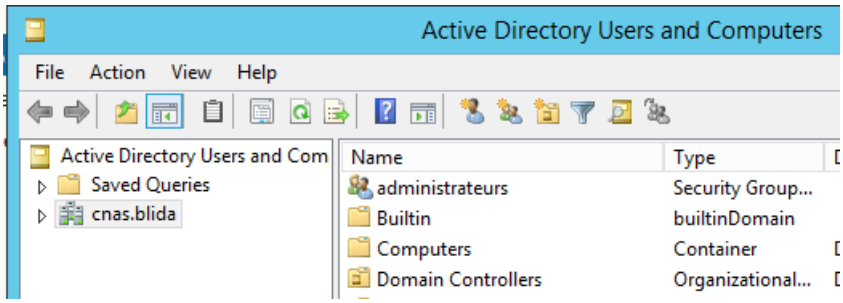

Figure 31 : l'emplacement du groupe dans le domaine

Une fois le groupe est créé on doit ajouter des membres dans le groupe.

Pour ajouter un membre on suit les étapes suivantes :

- Une clique droite sur le nom du groupe → properties
- L'interface suivante apparaîtra, on clique sur « membres » ensuite « Add »

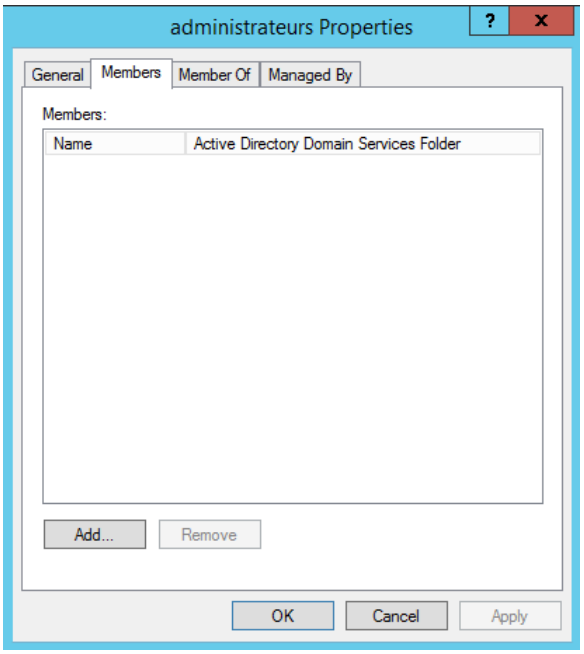

Figure 32 : ajouter un membre dans un groupe

- On entre le nom de l'utilisateur qu'on veut ajouter au groupe (juste les premiers caractères de son nom et on clique sur **« check names »**) et on clique sur **OK**

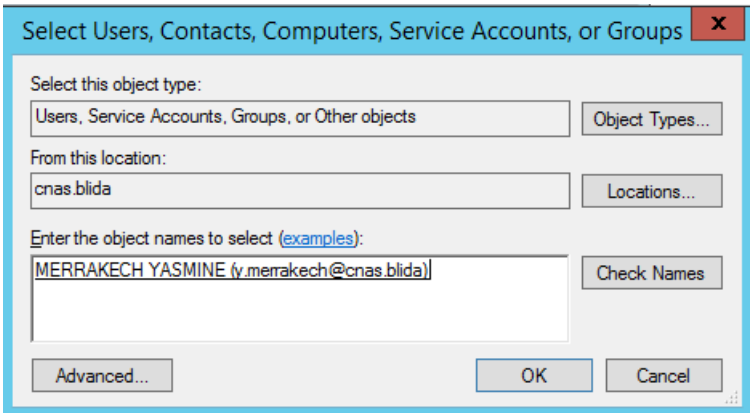

Figure 33 : chercher des membres à ajouter

6.2. Une GPO permet d'afficher un message avant la connexion :

On souhaite afficher un message d'avertissement sur les postes du domaine pour avertir les utilisateurs d'un changement ou d'une nouvelle mise à jour, ce message apparaitra avant que l'utilisateur ouvre sa session.

La mise en place de ce message d'avertissement avant la connexion de l'utilisateur implique la modification de deux paramètres, l'un pour définir le titre de message, et l'autre pour définir le contenu du message. Pour cela, on va créer une nouvelle GPO qui doit s'appliquer sur des objets "ordinateurs".

Le titre de la GPO sera « message d'information » et elle sera liée à l'OU « ordinateurs » de l'annuaire. Après on suit le chemin : computer settings/ Windows settings/ Security settings/ local policies/ Security options

Là il Ya deux paramètres intéressantes par rapport à l'objectif :

- Ouverture de session interactive : titre du message pour les utilisateurs essayant de se connecter.
- Ouverture de session interactive : contenu du message pour les utilisateurs essayant de se connecter.

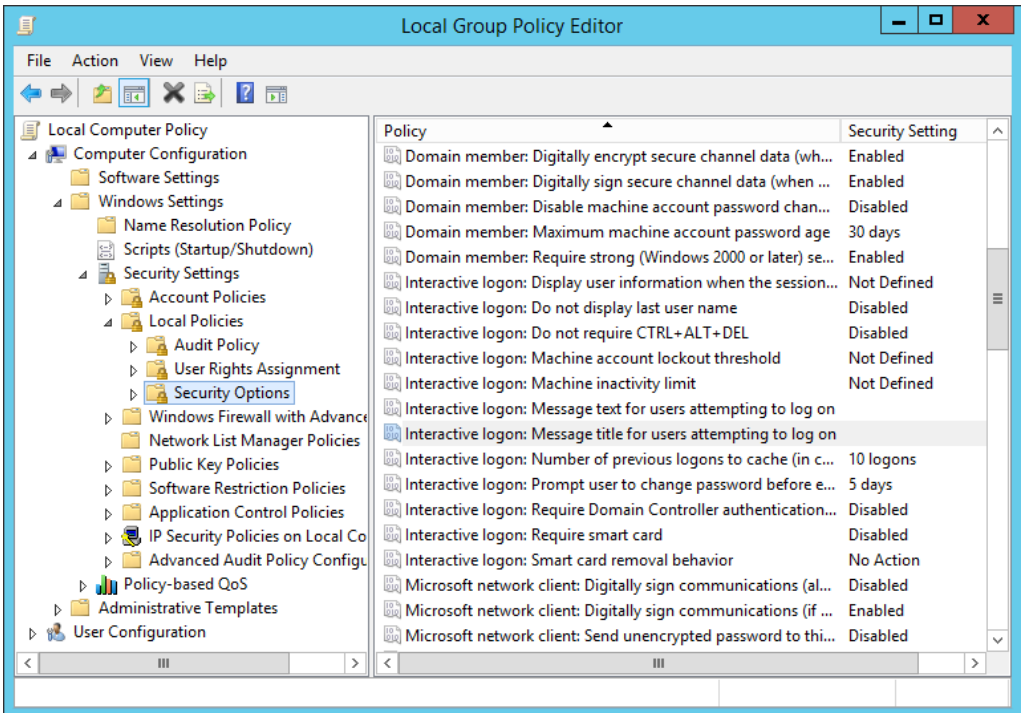

Figure 34 : les paramètres qui permettre d'afficher un message au utilisateurs

Commençons par le paramètre permettant de définir le titre, on clique sur le paramètre, une boite de dialogue apparaitre, on indique le titre dans la zone de saisie « message d'avertissement ».

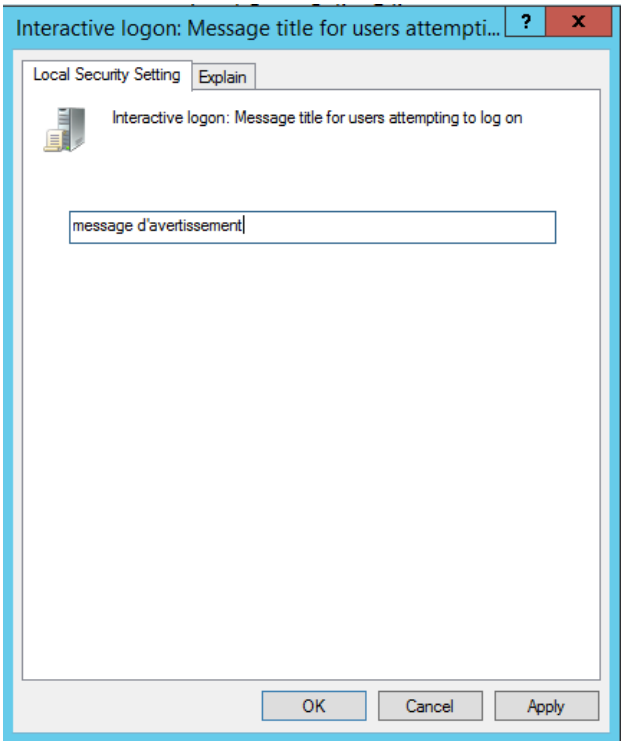

Figure 35 : titre du message

Sur exactement le même principe, le second paramètre va permettre de définir le contenu du message.

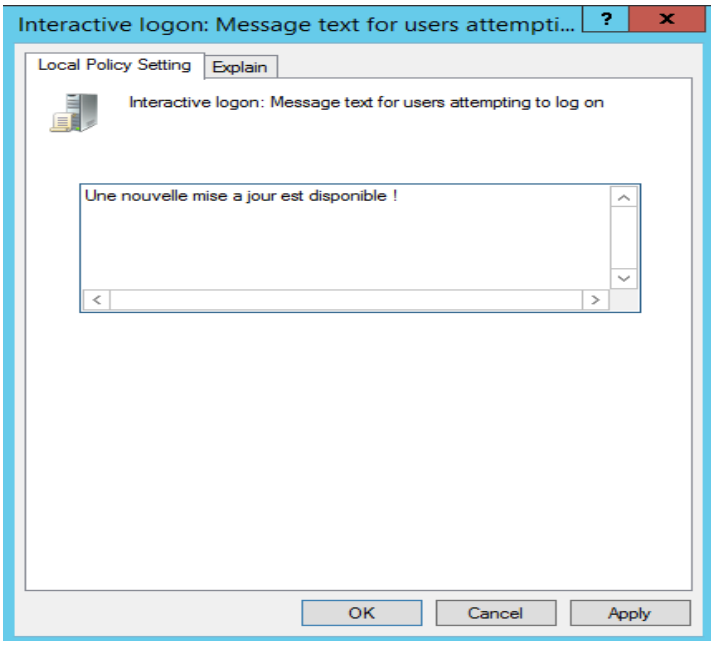

Figure 36 : contenue du message

La GPO est prête ! il ne reste qu'à faire un « gpupdate/force » sur une machine ciblée par la GPO et à redémarrer

6.3. Créer une GPO pour la configuration du pare-feu :

Il est possible via les GPO de forcer l'activation/désactivation du pare-feu :

Pour commencer la procédure, on va créer tout d'abord une nouvelle stratégie qui va être appliquée sur les ordinateurs, puis on va modifier cette GPO en suivant le chemin **computer configuration/policies/Windows settings/security settings/Windows Firewall with advanced security**

Sur la même fenêtre à droite on clique sur **Windows firewall properties.**

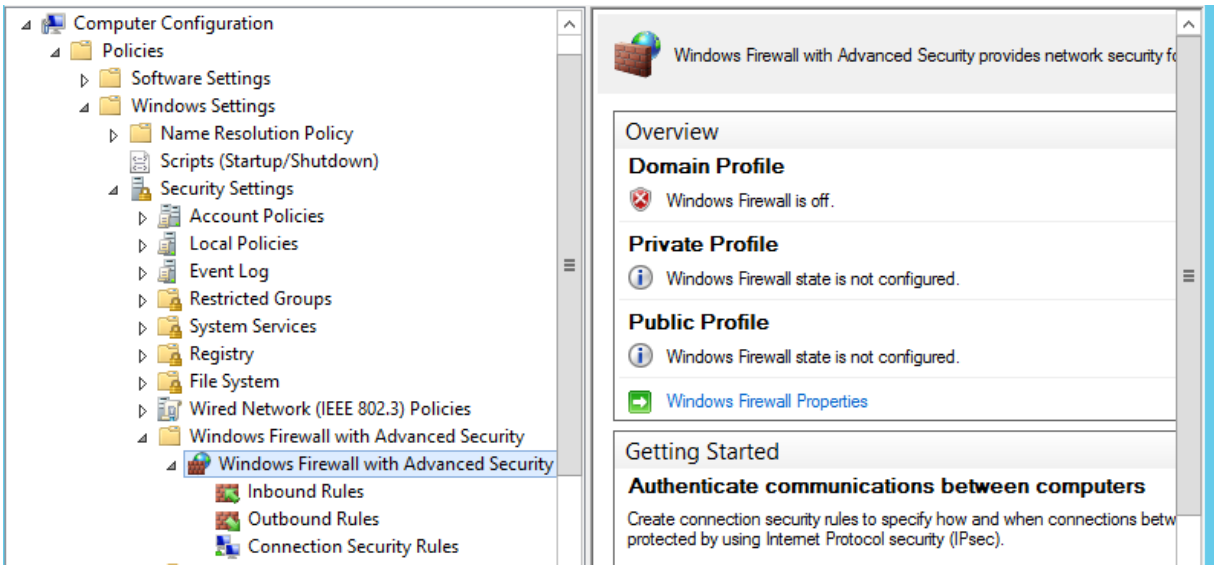

Figure 37 : le chemin pour configurer le pare-feu

Une nouvelle fenêtre apparaitre : on va configurer les paramètres selon nos besoins.

Dans ce cas on a :

- Activer le pare-feu.
- Bloquer la connexion entrante.
- Autoriser la connexion sortante.

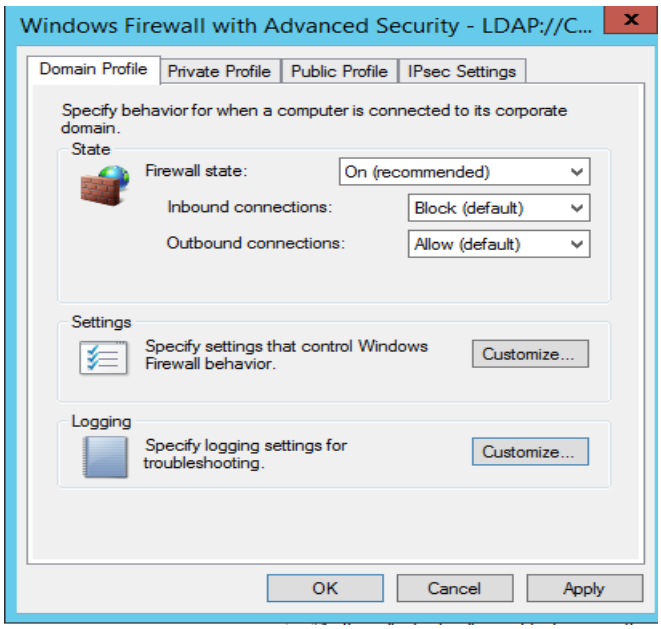

Figure 38 : configuration des paramètres de pare-feu

- En cas d'une connexion entrante bloquer on doit notifier l'utilisateur :
- Sur le champ settings on clique sur customize, une fenêtre apparaitre, on change le paramètre **Display a notification** à **Yes** puis on clique sur **OK.**

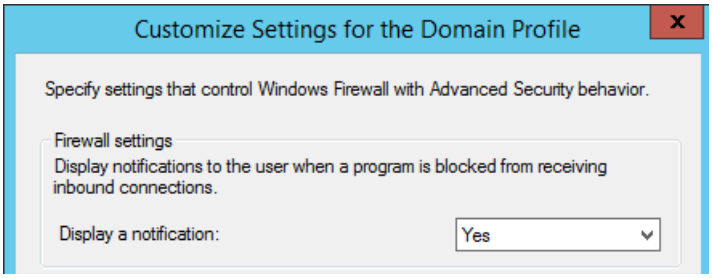

Figure 39 : activer les notifications

6.4. Une GPO qui permet l'installation à distance d'un package .MSI :

Dans cet partie, nous allons voir comment déployer des applications au format MSI à l'aide de stratégie de groupe (GPO) dans un environnement Active Directory.

Il existe deux modes de déploiement :

- Attribué : s'applique principalement aux ordinateurs, l'installation du programme est forcée.
- Publié : s'applique uniquement aux utilisateurs, ce mode permet l'installation du logiciel à la demande de l'utilisateur, celui-ci est publié à l'aide panneau de configuration.

Avant de commencer la mise en place de la GPO, il faut mettre en place un partage accessible aux ordinateurs, et copier l'installable dans ce dossier.
Informations sur le partage :

- **Nom du partage** : partage
- **Droits sur le partage :** "Tout le monde" en contrôle total
- **Droits NTFS sur le dossier du partage** : "Ordinateurs du domaine" en lecture et exécution.

- **Partage accessible via ce chemin :** \\SERVER-DC\partage

Une fois avoir créé le partage correctement, on peut tenter un accès et déposer le fichier MSI à déployer.

Dans cette partie on va déployer le logiciel Kaspersky anti-virus en format msi à tous les ordinateurs du domaine.

Tous d'abord, ouvrir la console **« gestion de stratégies de groupe »**. On va créer une nouvelle stratégie **« déploiement Kaspersky »** qui vas être appliquer sur l'unité d'organisation **« ordinateurs »**.

On va modifier la stratégie et suivre ce chemin : **Computer/ configuration/ policies/ software settings/ software installation**

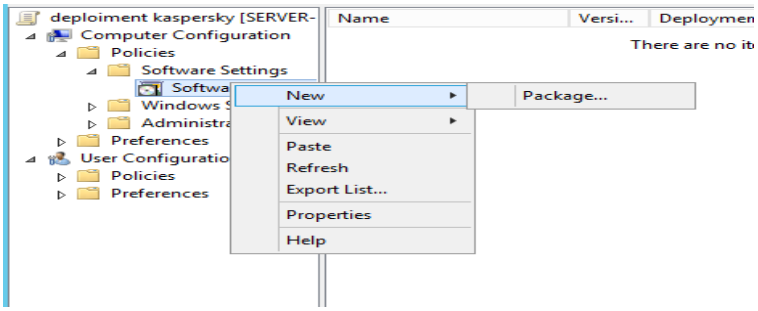

Figure 40 : ajouter un package .msi

On va indiquer le chemin vers le fichier MSI. **On va utiliser pas le chemin local, mais le chemin réseau vers le partage pour rechercher le fichier MSI.**

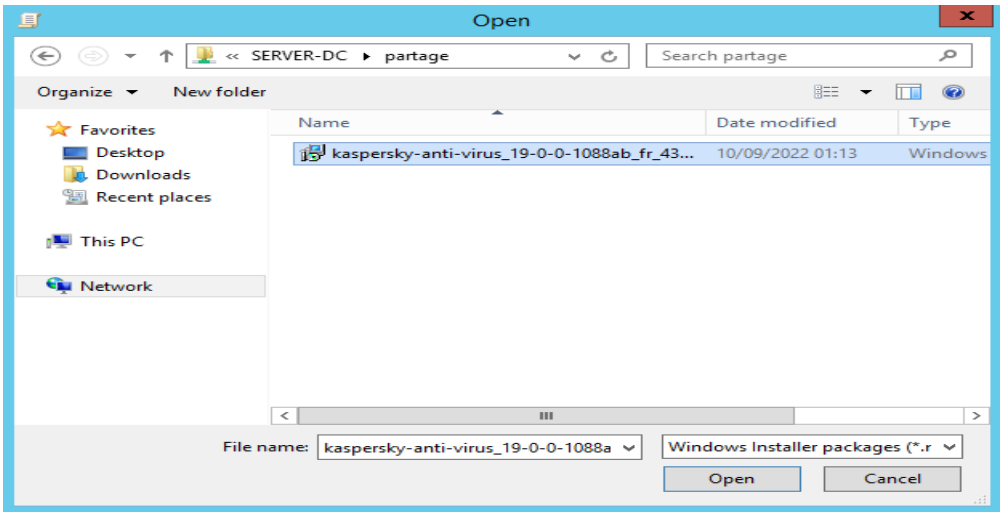

Figure 41 : sélectionner le package .msi à déployer

On clique sur open, et une fenêtre apparaitre pour choisir la méthode de déploiement, Cochez "**Assigned (Attribué)**" et cliquez sur "**OK**".

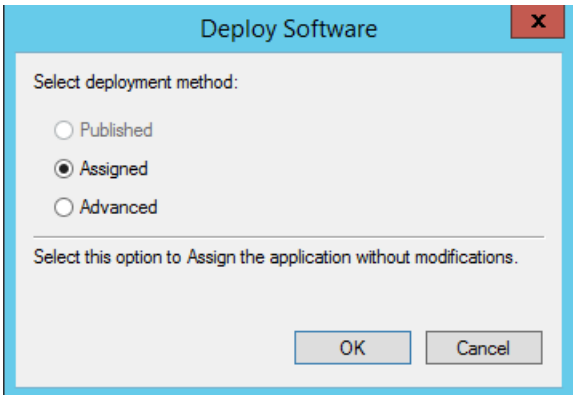

Figure 42 : mode de déploiement

Le programme d'installation apparaît comme ceci :

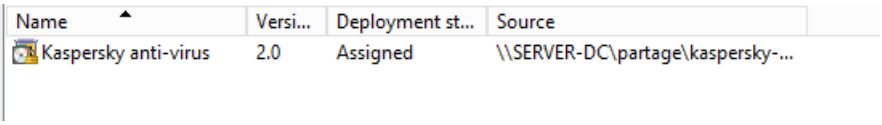

Figure 43 : résultat de déploiement

Sans rien faire de plus, notre GPO est prête à l'emploi.

6.5. Une GPO qui permet l'installation à distance d'un logiciel .exe :

Dans cette partie on souhaite installer à distance **Google Chrome** sur tous les ordinateurs du domaine.

On va utiliser le même dossier partager **« partage »** pour copier l'exécutable de Google Chrome.

L'installation cette fois est différente de l'installation d'un package .msi.

Pour installer un fichier .exe on a besoin d'un script .cmd/ .bat qui contient le chemin vers l'exécutable de l'application

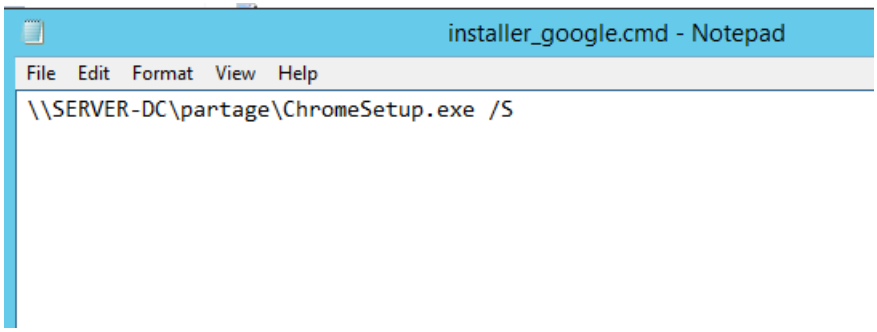

Figure 44 : contenue du script

/S : pour que l'installation soit silencieuse.

Ensuite, on passe à la création d'une nouvelle GPO appeler **« installation Google »** et la modifier et suivre le chemin : **computer policies/ Windows settings/ Scripts(Startup/Shutdown).**

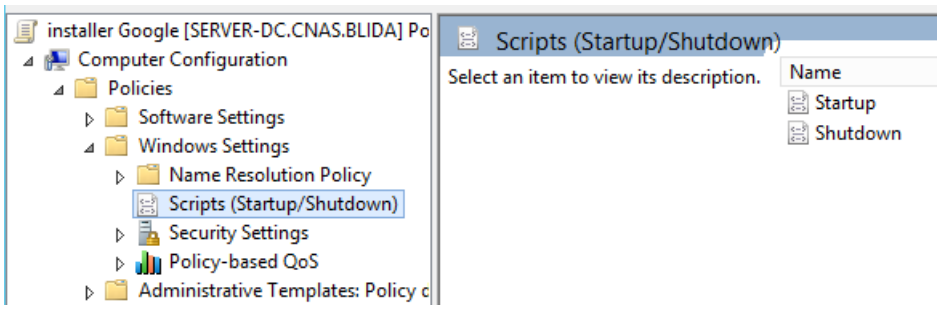

Figure 45 : le chemin à suivre pour ajouter un script d'installation

Sur la même fenêtre à droite on clique sur **startup (démarrage de session)**

Une nouvelle fenêtre apparaitre qui permet d'ajouter un Script, on clique sur **Add**

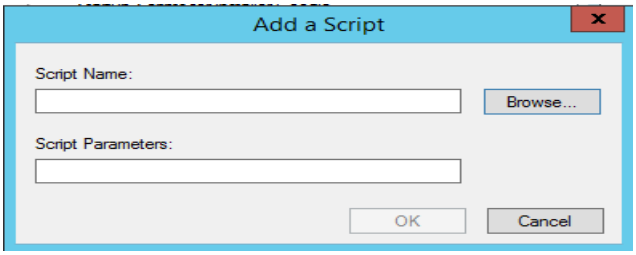

Figure 46 : fenêtre qui permet d'ajouter un script

On écrit directement le chemin vers le script d'installation dans le champ **« script name »** ou bien on clique sur **browse** et chercher le script d'installation puis cliquer sur **Open**.

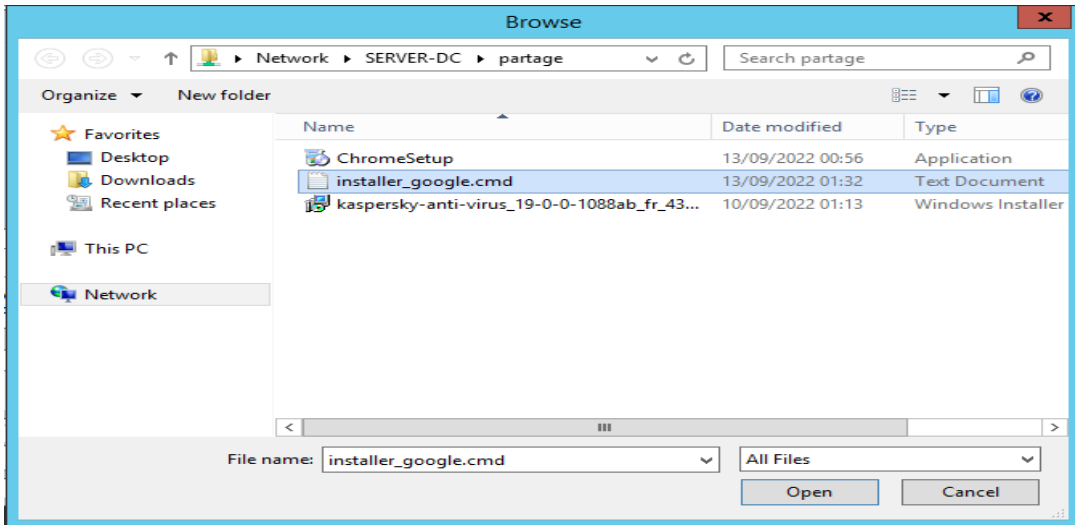

Figure 47 : chercher le script d'installation

On clique sur **open** puis sur **Apply** et **OK.**

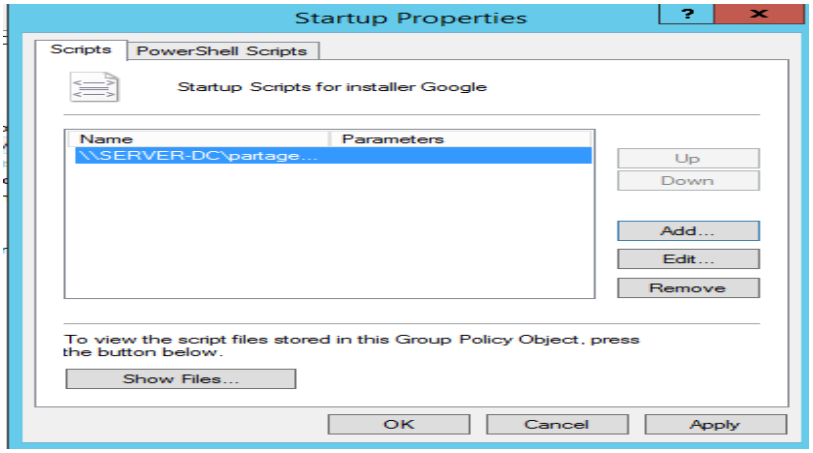

Figure 48 : le script est bien ajouté

Conclusion :

Dans ce chapitre nous avons montré les étapes d'installation et configuration de Windows server 2012 R2. Ainsi que le rôle AD DS.

On a créé des comptes pour les utilisateurs du domaine et ajouter les ordinateurs de l'entreprise au domaine. Ensuite on a appliqué des GPO sur ces derniers.

Conclusion générale :

Dans le cadre de réaliser mon mémoire de fin d'étude, ce projet est le fruit d'une recherche très approfondi afin de répondre aux besoins de l'entreprise CNAS, celle de mettre en place un service d'annuaire Active Directory.

Active Directory (AD) est un composant des environnements logiciels Microsoft Windows, spécifiquement destiné aux réseaux qui nécessitent des services de gestion de domaine. De plus il facilite la sécurité dans l'ensemble d'une entreprise. Grâce à la délégation, les autorités de gestion de niveau supérieur peuvent définir des autorisations pour les ressources et les applications à d'autres administrateurs ou utilisateurs.

C'est pour ça qu'on a parlé un premier temps sur les généralités des réseaux et de la sécurité informatique.

Ensuite, on a fait une étude sur Active directory avant de commencé l'implémentation de ce dernier.

Enfin, pour répondre à la problématique initiale on a installé Windows server 2012 R2 et Active directory qui est l'outil qui gère les utilisateurs, les ressources et les applications de l'entreprise et autoriser l'authentification des utilisateurs au ressources de l'entreprise.

La réalisation de ce projet nous a permet d'expérimenter la vie professionnelle et d'approfondir les connaissances acquises durant les années d'études à l'université.

Résumé :

La sécurité des réseaux englobe toutes les activités visant à protéger la fonctionnalité et l'intégrité d'un réseau et de données. Ce projet nous a permet de mettre en œuvre une configuration sécurisée d'un contrôleur de domaine pour une gestion centralisée des utilisateurs et ordinateurs au sein de l'entreprise « CNAS » sous Windows Server 2012 R2. Ce dernier représente une plateforme qui offre plusieurs services, parmi ces services utilisés dans notre projet, un service qui s'occupe de gérer les comptes utilisateurs et ordinateurs « AD DS », Tous les utilisateurs ne doivent pas avoir accès à notre réseau. Pour tenir les éventuelles attaques à l'écart, on a besoin de reconnaître chaque utilisateur et chaque appareil. Ensuite, on peut mettre en application nos politiques de sécurité, ces derniers sont les « GPO ». On peut bloquer des dispositifs de points d'extrémité non conformes ou leur accorder un accès limité seulement. Afin de sécurisé les postes de travail, les sessions des utilisateurs et pour protéger le réseau de l'entreprise contre les attaques extérieures.

Pour réaliser ce projet on a utilisé différents logiciels informatiques tels que : VMware Workstation 10, Windows Server 2012 R2.

Mots clés : réseau informatique, sécurité, Active Directory, CNAS, ADDS, DNS, GPO.

Abstract:

Network security encompasses all activities aimed at protecting the functionality and integrity of a network and data. This project allowed us to implement a secure configuration of a domain controller for centralized management of users and computers within the “CNAS” company under Windows Server 2012 R2. The latter represents a platform that offers several services, among these services used in our project, a service that takes care of managing “AD DS” user and computer accounts. Not all users must have access to our network. To keep possible attacks away, we need to recognize each user and each device. Then, we can implement our security policies, these are the “GPOs”. Non-compliant endpoint devices can be blocked or granted limited access only. In order to secure workstations, user sessions and to protect the company network against external attacks.

To carry out this project we used different computer software such as: VMware Workstation 10, Windows Server 2012 R2.

Keywords : computer network, security, Active Directory, CNAS, ADDS, DNS, GPO.

ملخص

يشمل أمن الشبكات جميع الأنشطة التي تهدف إلى حماية وظائف وسلامة الشبكة والبيانات. سمح لنا هذا المشروع بتنفيذ تكوين آمن لوحدة تحكم المجال للإدارة المركزية للمستخدمين وأجهزة الكمبيوتر داخل Windows Server 2012 R2. ضمن "CNAS" شركة وتمثل الأخيرة منصة تقدم عدة خدمات، من AD" بين هذه الخدمات المستخدمة في مشروعنا، خدمة تعتني بإدارة حسابات المستخدمين والكمبيوتر ، ولا يجب أن يكون لدى جميع المستخدمين حق الوصول إلى شبكتنا. لإبعاد الهجمات المحتملة، "DS نحتاج إلى التعرف على كل مستخدم وكل جهاز. وبعد ذلك، يمكننا تنفيذ سياساتنا الأمنية، وهي "كائنات يمكن حظر أجهزة نقطة النهاية غير المتوافقة أو منحها وصولاً محدودًا ."(GPOs) سياسة المجموعة .فقط. من أجل تأمين محطات العمل وجلسات المستخدم وحماية شبكة الشركة من الهجمات الخارجية

لتنفيذ هذا المشروع استخدمنا برامج كمبيوتر مختلفة مثل

VMware Workstation 10, Windows Server 2012 R2.

الكلمات المفتاحية:

.GPO، DNS، ADDS، CNAS شبكة الكمبيوتر، الأمان، الدليل النشط،

Références Web :

[1]« Service d'annuaire Active Directory », [En ligne] www.ofppt.info

[2] https://apcpedagogie.com/les-principes-de-securite-informatique/

[3] https://www.varonis.com/fr/blog/controleur-de-domaine/

[4] https://sibus.fr/les-menaces-informatiques-qui-ciblent-les-entreprises/

[5] https://www.techniques-ingenieur.fr/base-documentaire/technologies-de-l-information-th9/securite-des-si-organisation-dans-l-entreprise-et-legislation-42458210/introduction-a-la-securite-des-systemes-d-information-ssi-h5000/

[6] Emmanuel le Chevoir, Etude d'active directory

[7] www.microsoft.com

[8] www.it-connect.fr

[9]www.rdr-it.com

[10] www.wikipedia.com

[11] Melle. SADAOUI Kamilia, Migration d'une infrastructure réseau de Windows server 2003 ver Windows server 2008 R2, UNIVERSITE MOULOUD MAMMERI de TIZI-OUZOU,2013

[12] SDSI document de la CNAS

[13] https://kidan.co/fr/blog/importance-dactive-directory-pour-les-entreprises-encroissance/#:~:text=Active%20Directory%20facilite%20la%20s%C3%A9curit%C3%A9,Active%20Directory%20sont%20reli%C3%A9s%20hi%C3%A9rarchiquement.