

Mission 2

| | |
|---|----|
| Mission 2..... | 1 |
| I)Contexte..... | 2 |
| a) Présentation de l'entreprise :..... | 2 |
| b) Présentation du prestataire informatique | 2 |
| c)Information sur le système informatique | 3 |
| Téléphones et PC de StadiumCompany: | 3 |
| Schéma de l'état des lieux : | 4 |
| Serveur et service : | 5 |
| Organisation de l'équipe A..... | 5 |
| Organisation de l'équipe B | 6 |
| Accueil de l'équipe « visiteuse »..... | 6 |
| Fournisseur de concessions..... | 6 |
| Organisation du restaurant de luxe | 6 |
| Prise en charge des loges de luxe | 7 |
| Prise en charge de la zone de presse | 7 |
| Prise en charge de site distant..... | 7 |
| II) Cahier des charges..... | 8 |
| Mission 1 : | 8 |
| Mission 2 : | 9 |
| III) Solutions | 10 |
| Test des solutions : | 10 |
| Choix de la solution : | 11 |
| IV)PROJET | 12 |
| a) Objectif et but du projet | 12 |
| b) Phase du projet | 12 |
| Prérequis : | 12 |
| Configuration AD | 14 |
| Configuration DHCP | 21 |
| Configuration GPO | 30 |
| Installation DNS SECONDAIRE | 38 |
| Présentation du service DNS | 38 |
| Avantage d'un serveur DNS secondaire : | 39 |

| | |
|---|----|
| Prérequis | 39 |
| Vérifier la configuration des zones configurer :..... | 42 |
| V)Conclusion | 43 |
| VI)Compétence acquise | 43 |

I)Contexte

a) Présentation de l'entreprise :

Lors de la construction de ce stade, le réseau qui prenait en charge ses bureaux commerciaux et ses services de sécurité proposait des fonctionnalités de communication de pointe. Au fil des ans, la société a ajouté de nouveaux équipements et augmenté le nombre de connexions sans tenir compte des objectifs commerciaux généraux ni de la conception de l'infrastructure à long terme. Certains projets ont été menés sans souci des conditions de bande passante, de définition de priorités de trafic et autres, requises pour prendre en charge ce réseau critique de pointe. StadiumCompany fournit l'infrastructure réseau et les installations sur le stade.

StadiumCompany emploie 170 personnes à temps plein :

- 35 dirigeants et responsables
- 135 employés

De plus, environ 80 intérimaires sont embauchés en fonction des besoins, pour des événements spéciaux dans les services installations et sécurité.

À présent, la direction de StadiumCompany veut améliorer la satisfaction des clients en ajoutant des fonctions haute technologie et en permettant l'organisation de concerts, mais le réseau existant ne le permet pas.

La direction de StadiumCompany sait qu'elle ne dispose pas du savoir-faire voulu en matière de réseau pour prendre en charge cette mise à niveau. StadiumCompany décide de faire appel à des consultants réseau pour prendre en charge la conception, la gestion du projet et sa mise en œuvre. Ce projet sera mis en œuvre suivant trois phases.

La première phase consiste à planifier le projet et préparer la conception réseau de haut niveau.

La deuxième phase consiste à développer la conception réseau détaillée.

La troisième phase consiste à mettre en œuvre la conception

b) Présentation du prestataire informatique

NetworkingCompany, une société locale spécialisée dans la conception de réseaux et le conseil, de la phase 1, la conception de haut niveau. NetworkingCompany est une société partenaire Cisco Premier Partner. Elle emploie 20 ingénieurs réseau qui disposent de diverses certifications et d'une grande expérience dans ce secteur. Pour créer la conception de haut niveau, NetworkingCompany a tout d'abord interrogé le personnel du stade et décrit un profil de l'organisation et des installations.

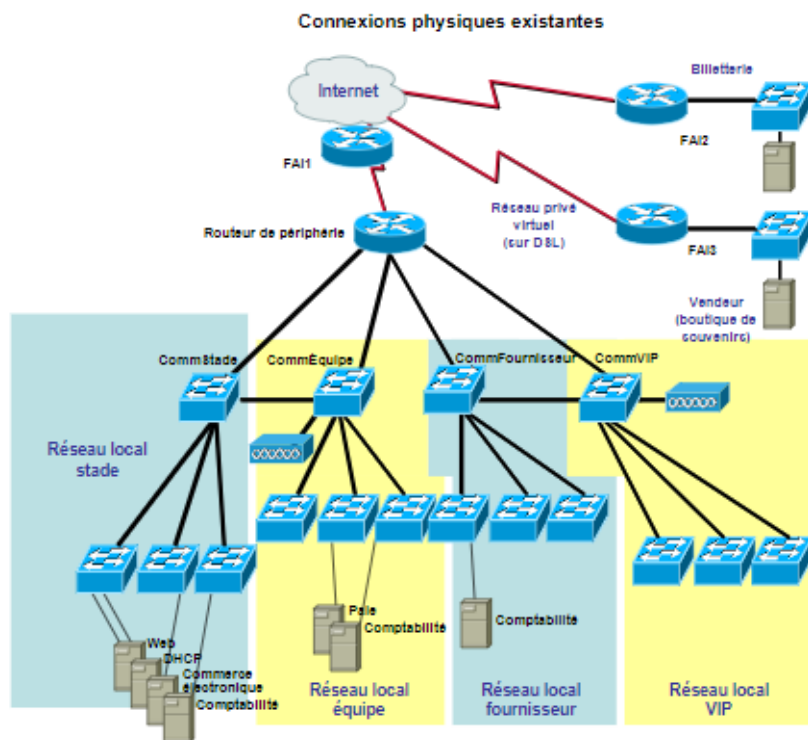
c) Information sur le système informatique

Téléphones et PC de StadiumCompany:

Tous les dirigeants et responsables de StadiumCompany utilisent des PC et téléphones connectés à un PABX vocal numérique. À l'exception des préposés au terrain à temps plein et des gardiens, tous les salariés utilisent également des PC et des téléphones.

Cinquante téléphones partagés sont répartis dans le stade pour le personnel de sécurité. On compte également 12 téléphones analogiques, certains prenant également en charge les télécopies et d'autres offrant un accès direct aux services de police et des pompiers. Le groupe sécurité dispose également de 30 caméras de sécurité raccordées à un réseau distinct.

Schéma de l'état des lieux :



Serveur et service :

StadiumCompany propose des installations et une prise en charge de réseau pour deux équipes de sports (Équipe A et Équipe B), une équipe « visiteurs », un restaurant et un fournisseur de concessions.

Le stade mesure environ 220 mètres sur 375. Il est construit sur deux niveaux.

En raison de la taille des installations, plusieurs locaux techniques connectés par des câbles à fibre optique sont répartis sur l'ensemble du stade.

Les vestiaires des équipes A et B et les salons des joueurs sont situés au premier niveau de la partie sud du stade. Les bureaux des équipes occupent une surface d'environ 15 mètres par 60 au deuxième niveau.

Le bureau et le vestiaire de l'équipe « visiteuse

» sont également situés au premier niveau.

Les bureaux de StadiumCompany se trouvent dans la partie nord du stade, répartis sur les deux niveaux.

L'espace des bureaux occupe environ 60 mètres par 18 au premier niveau et 60 mètres par 15 au deuxième niveau.

Les équipes A et B sont engagées dans des compétitions sportives différentes, organisées à des dates différentes. Elles sont toutes les deux sous contrat avec

StadiumCompany pour leurs bureaux et services au sein du stade.

Organisation de l'équipe A

L'équipe A compte 90 personnes :

- 4 dirigeants
- 12 entraîneurs
- 14 employés (y compris des médecins, kinés, secrétaires, assistants, comptables et assistants financiers)
- 60 joueurs L'équipe A dispose de 15 bureaux dans le stade pour ses employés non joueurs.

Cinq de ces bureaux sont partagés. 24 PC et 28 téléphones sont installés dans les bureaux.

L'équipe A dispose également d'un vestiaire des joueurs, d'un grand salon pour les joueurs et d'une salle d'entraînement.

Les employés non joueurs utilisent les locaux toute l'année. Les joueurs ont accès au vestiaire et aux équipements d'entraînement pendant et en dehors de la saison. Le vestiaire est équipé de 5 téléphones et le salon des joueurs de 15 téléphones.

Des rumeurs indiquent que l'équipe A aurait récemment installé un concentrateur sans fil dans le salon des joueurs.

Organisation de l'équipe B

L'équipe B compte 64 personnes :

- 4 dirigeants
- 8 entraîneurs
- 12 employés (y compris des médecins, kinés, secrétaires, assistants, comptables et assistants financiers)
- 40 joueurs L'équipe B dispose de 12 bureaux dans le stade pour ses employés autres que les joueurs.

Trois de ces bureaux sont partagés. 19 PC et 22 téléphones sont installés dans les bureaux. L'équipe B dispose également d'un vestiaire des joueurs et d'un grand salon pour les joueurs. Les employés non joueurs utilisent les locaux toute l'année.

Les joueurs ont accès au vestiaire et aux équipements d'entraînement pendant et en dehors de la saison. Le vestiaire est équipé de 5 téléphones et le salon des joueurs de 15 téléphones.

Accueil de l'équipe « visiteuse »

L'équipe « visiteuse » dispose d'un vestiaire et d'un salon équipés de 10 téléphones. Chaque équipe « visiteuse » demande des services provisoires le jour du match et quelques jours auparavant.

Les équipes « visiteuses » passent également un contrat avec StadiumCompany pour les bureaux et services au sein du stade.

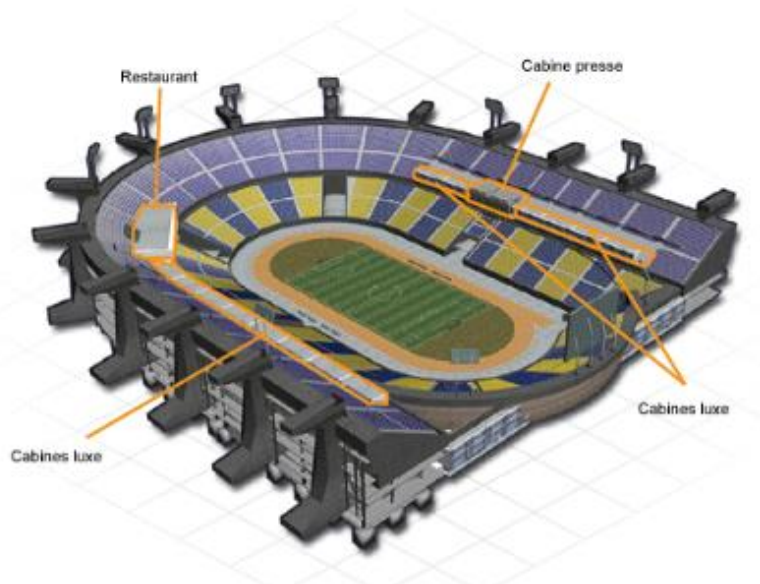
Fournisseur de concessions

Un fournisseur de concessions gère les services proposés lors des matchs et événements. Il compte 5 employés à temps plein. Ils occupent deux bureaux privés et deux bureaux partagés équipés de cinq PC et sept téléphones. Ces bureaux se trouvent dans la partie sud du stade, entre les bureaux des équipes A et B. Deux employés à temps partiel prennent les commandes auprès des loges au cours des événements. Le concessionnaire de services emploie des intérimaires saisonniers pour gérer 32 stands permanents et autres services répartis sur l'ensemble du stade. Il n'y a actuellement aucun téléphone ni PC dans les zones de vente.

Organisation du restaurant de luxe

Le stade propose un restaurant de luxe ouvert toute l'année. En plus des salles et des cuisines, le restaurant loue des bureaux auprès de StadiumCompany. Les quatre dirigeants ont chacun un bureau privé. Les deux employés en charge des questions financières et comptables partagent un bureau. Six

PC et téléphones sont pris en charge. Deux téléphones supplémentaires sont utilisés en salle pour les réservations.



Prise en charge des loges de luxe

Le stade compte 20 loges de luxe. StadiumCompany équipe chaque loge d'un téléphone permettant de passer des appels locaux et d'appeler le restaurant et le concessionnaire de services.

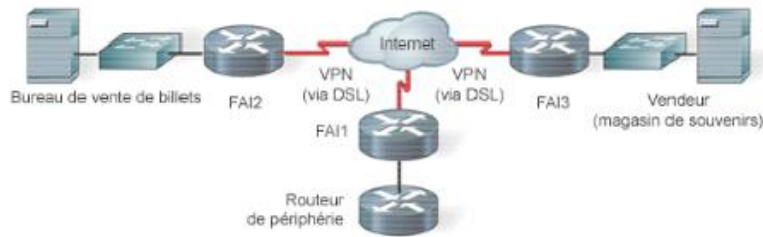
Prise en charge de la zone de presse

StadiumCompany propose un espace presse avec trois zones partagées :

- La zone presse écrite accueille généralement 40 à 50 journalistes au cours d'un match. Cette zone partagée est équipée de 10 téléphones analogiques et de deux ports de données partagés. On sait qu'un journaliste stagiaire apporte un petit point d'accès sans fil lorsqu'il couvre un match.
- La zone de presse pour les radios peut accueillir 15 à 20 stations de radio. Elle est équipée de 10 lignes téléphoniques analogiques.
- La zone de presse télévisée accueille généralement 10 personnes. Elle est équipée de 5 téléphones.

Prise en charge de site distant

StadiumCompany compte actuellement deux sites distants : une billetterie en centre-ville et une boutique de souvenirs dans une galerie marchande locale. Les sites distants sont connectés via un service DSL à un FAI local.



Le stade est connecté au FAI local à l'aide de FAI1, un routeur de services gérés qui appartient au FAI. Les deux sites distants sont connectés au même FAI par les routeurs FAI2 et FAI3, fournis et gérés par le FAI. Cette connexion permet aux sites distants d'accéder aux bases de données situées sur les serveurs dans les bureaux de StadiumCompany.

StadiumCompany dispose également d'un routeur de périmètre, nommé Routeur de périphérie, connecté au routeur FAI1 du stade.

II) Cahier des charges

Mission 1 :

Vous intégrez le service informatique du centre administratif de stade. Sur ce site sont effectuées toutes les opérations concernant la gestion du personnel, et l'administration du stade. On y trouve 7 grands services :

- Service Administration (170 personnes)
- Service Equipes (164 personnes)
- Service Wifi (100 personnes)
- Service Caméra IP (80 caméras)
- Service VIP-Press (80 personnes)
- Service Fournisseurs (44 personnes)
- Service Restaurant (14 personnes)

Le réseau de StadiumCompany doit comporter plusieurs périmètres de sécurité

- Adressage réseau et attribution de noms faciles à mettre à niveau : 172.20.0.0/22

- Un système de cloisonnement du réseau devra être testé. Les commutateurs devront être facilement administrables afin de propager les configurations rapidement et aisément
- Solution permettant l'interconnexion des différents sites (stade, billetterie et magasin). Les différents commutateurs ainsi que le routeur doivent disposer de réglages de base homogènes. La solution doit se faire avec les équipements réseau CISCO !

Mission 2 :

StadiumCompagny possède le nom de domaine StadiumCompagny.com

Les principaux serveurs sont hébergés au stade au centre d'hébergement informatique.

Selon les cas, certains services sont répliqués sur les sites eux-mêmes. Par exemple, les services d'annuaire Active Directory sont généralement répliqués sur le site de stade. Le réseau de magasin et le réseau de billetterie sont tous composés de la même manière :

- X Postes pour les employés

- Le site du stade dispose d'un service Active Directory, d'un service DHCP, et d'un DNS primaire sur une machine sous Windows 2012 Server.

Celle-ci permet aussi le stockage des fichiers utilisateurs. Un serveur RSync et DNS secondaire sous Linux Debian.

Annuaire du site de stade :

Les utilisateurs sont authentifiés via le serveur Active Directory du domaine Stadiumcompagny.local. Il est configuré en regroupant les utilisateurs par service. Les UO suivantes sont présentes sur le serveur : Admin, Wifi,

Chaque UO contient les utilisateurs du service concerné, un groupe d'utilisateurs dont le nom est au format G_xxxx où xxxx=le nom du service, un groupe regroupant les utilisateurs avec pouvoir du service GP_Admin (directeurs et responsables notamment) et une GPO permettant d'imposer des contraintes d'utilisation et d'habilitations sur les machines du réseau.

Extrait d'une GPO : service equipes → gpo_equipes

- Accès au panneau de configuration, l'accès aux paramètres réseau est interdit
- Un script de démarrage Equipesstart.bat permet la connexion des lecteurs réseaux accédant aux dossiers partagés.
- Les utilisateurs démarrent avec un bureau imposé (barre de menu, fond d'écran...)
- Les utilisateurs ont des logins construits sur la base suivante - pnom – p=première lettre du prénom et nom=nom de famille. S'il y a homonymie un chiffre de 1 à 10 sera ajouté. Chaque utilisateur possède un dossier personnel et un profil centralisé.

Une stratégie de complexité des mots de passe est définie au niveau domaine.

DNS :

Les serveurs DNS sont configurés pour résoudre la zone directe stadiumcompagny.local et la zone inverse du 172.20.0.x/24. Le serveur primaire est hébergé sur une machine Windows Server et le DNS secondaire sur une Linux Debian.

DHCP :

Une plage est définie sur le 172.20.0.x/24 avec des options de routeur renvoyant vers la passerelle/pare-feu. Les serveurs DNS sont aussi transmis via les options DHCP.

III) Solutions

Test des solutions :

Active Directory (AD) est un **service d'annuaire**. Sa fonction principale consiste à permettre aux administrateurs de gérer les permissions et de contrôler l'accès aux ressources du réseau. Dans Active Directory, les données sont stockées sous forme d'objets. Ceux-ci comprennent les utilisateurs, les groupes, les applications et les périphériques. En outre, ils sont **classés en fonction de leur nom et de leurs attributs**.

| AD SUR WINDOWS | AD SUR LINUX (OPENLDAP) |
|---|--|
| <ul style="list-style-type: none">- Windows possède une interface graphique riche et peut être facilement utilisé par des personnes techniques ou non techniques. C'est très simple et convivial.- Facile à installer. Nécessite beaucoup moins d'entrées utilisateur lors de l'installation. Cependant, l'installation de Windows prend plus de temps que l'installation de Linux.- Windows est moins fiable que Linux. Au cours des dernières années, la fiabilité de Windows s'est beaucoup améliorée. Cependant, il présente encore des instabilités système et des faiblesses en matière de sécurité en raison de sa conception trop simplifiée. | <ul style="list-style-type: none">- Il est principalement utilisé par les techniciens expérimentés car vous devez connaître diverses commandes Linux pour pouvoir travailler avec le système d'exploitation Linux. Pour un utilisateur moyen, il faudra beaucoup de temps pour apprendre Linux. De plus, le processus de dépannage sous Linux est plus compliqué que sous Windows.- Compliqué à mettre en place. Nécessite beaucoup d'entrées utilisateur pour l'installation.- Très fiable et sécurisé. Il met l'accent sur la gestion des processus, la sécurité du système et la disponibilité. |

Le serveur DNS (Domain Name System, ou Système de noms de domaine en français) est un service dont la principale fonction est de traduire un nom de domaine en adresse IP. Pour simplifier, le serveur DNS agit comme un annuaire que consulte un ordinateur au moment d'accéder à un autre ordinateur via un réseau. Autrement dit, le serveur DNS est ce service qui permet d'associer à site web (ou un ordinateur connecté ou un serveur) une adresse IP.

| DNS SUR WINDOWS | DNS SUR LINUX (BIND) |
|--|---|
| <ul style="list-style-type: none">- Facile à prendre en main, utilisation intuitive via l'interface graphique- Les pilotes pour les derniers matériels sont facilement disponibles- Compatible avec un grand nombre d'applications tierces | <ul style="list-style-type: none">- Utilisation gratuite- Les administrateurs profitent des libertés de gestion du système- Permet le travail coopératif sans que des utilisateurs puissent endommager le cœur du programme |

| | |
|---|--|
| <ul style="list-style-type: none"> - Actualisation optionnelle et simple du système - Possibilité de résoudre des problèmes techniques via la récupération du système - Assistance long-terme - Possibilité d'utiliser des programmes exclusifs tels que SharePoint ou Exchange | <ul style="list-style-type: none"> - Rarement visé par les cybercriminels - De rares erreurs de sécurité, qui sont généralement prises en charge rapidement - Faibles exigences matérielles - Fonction de gestion à distance |
|---|--|

Dynamic Host Configuration Protocol (DHCP, protocole de configuration dynamique des hôtes) est un protocole réseau dont le rôle est d'assurer la configuration automatique des paramètres IP d'une station ou d'une machine, notamment en lui attribuant automatiquement une adresse IP et un masque de sous-réseau. DHCP peut aussi configurer l'adresse de la passerelle par défaut, des serveurs de noms DNS

| DHCP SUR WINDOWS | DHCP SUR LINUX (UNBUTU) |
|---|---|
| <ul style="list-style-type: none"> - Configuration d'adresse IP fiable. DHCP réduit les erreurs de configuration provoquée par la configuration d'adresse IP manuelle, telles que des erreurs typographiques, ou résoudre des conflits causés par l'affectation d'une adresse IP à plusieurs ordinateurs en même temps. - La possibilité de définir des configurations TCP/IP à partir d'un emplacement central. - Le transfert des messages DHCP initiales à l'aide d'un agent de relais DHCP, qui élimine la nécessité d'un serveur DHCP sur chaque sous-réseau. | <ul style="list-style-type: none"> - Le protocole DHCP offre une configuration de réseau TCP/IP fiable et simple, empêche les conflits d'adresses et permet de contrôler l'utilisation des adresses IP de façon centralisée - Economie d'adresse. - L'administrateur de réseau contrôle le mode d'attribution des adresses IP en spécifiant une durée de bail - L'adresse IP est libérée automatiquement, à l'expiration du bail - Lorsqu'un client redémarre, il tente d'obtenir un bail pour la même adresse avec le serveur DHCP d'origine, en émettant un DHCPREQUEST. Si la tentative se solde par un échec, le client continue à utiliser la même adresse IP s'il lui reste du temps sur son bail. |

Choix de la solution :

Pour la mise en place d'un annuaire permettant la gestion des utilisateurs et ressources nous avons opté pour l'Active directory sur Windows pour sa facilité d'utilisation, de gestion et de mise en place. En effet l'AD sur Windows permettra aux techniciens moins expérimentés de s'intégrer plus facilement, l'administration sera donc plus simple et plus claire.

Le DNS primaire sera sur le serveur AD, pour sa facilité de mise en place et pour une harmonisation avec notre AD sur Windows serveur. En effet, l'installation se fait en quelques clics, la détection du domaine est automatique.

Ensuite nous mettrons en place un DNS secondaire pour assurer une redondance. Ainsi, si le DNS primaire tombe en panne, le DNS secondaire prendra le relais. Nous évitons donc une interruption de service pour les utilisateurs. Le DNS secondaire sera installé sur une machine linux pour optimisation des ressources. De plus nous utiliserons le DNS Bind9 pour sa stabilité, sa flexibilité dans la configuration, en effet Bind9 nous permet de faire des serveurs DNS, primaire, secondaire, hybride, furtif, récursif ou non. Son adaptabilité le rend donc très intéressant pour une architecture informatique susceptible d'évoluer dans le temps.

IV)PROJET

a) Objectif et but du projet

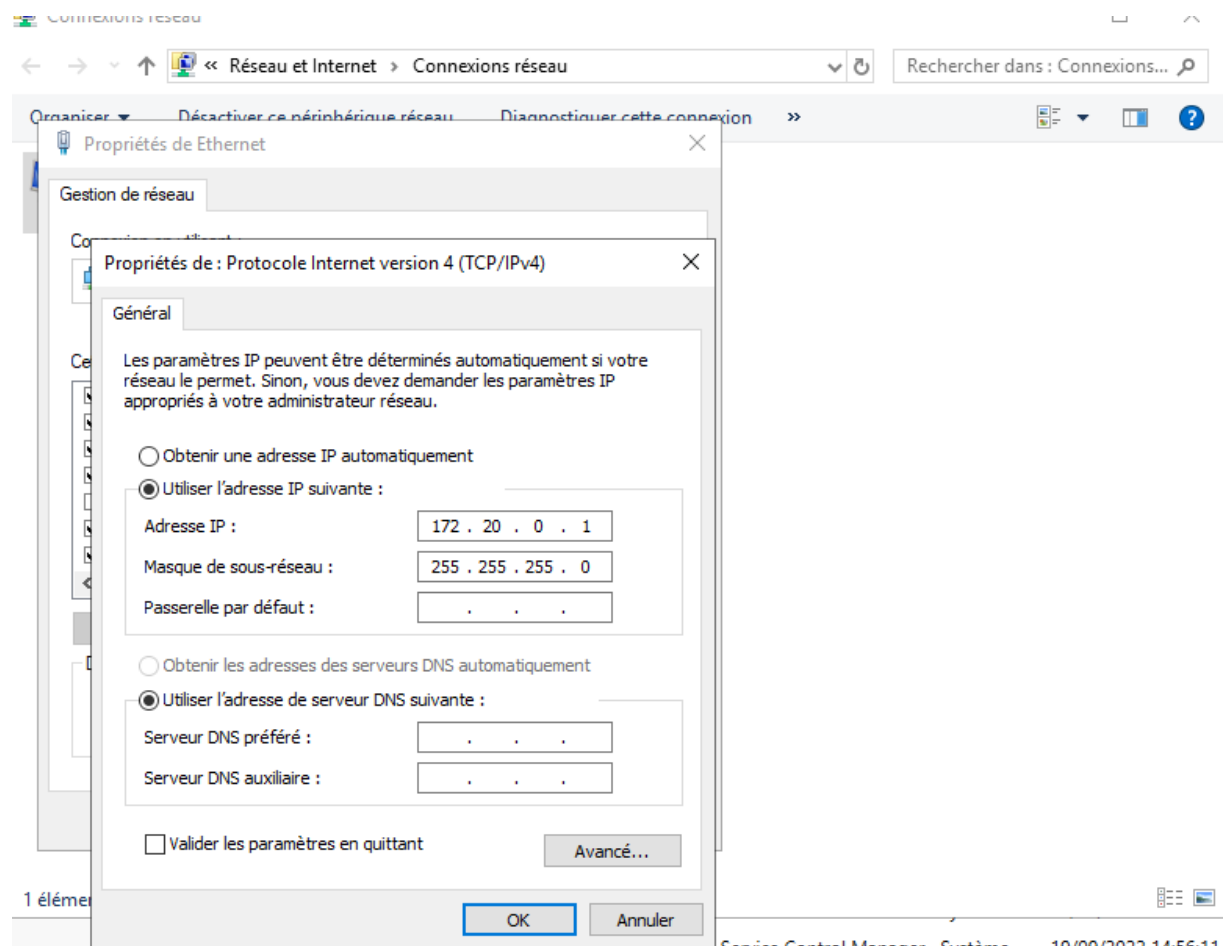
L'objectif du projet est de mettre en place une infrastructure réseau composé d'un serveur AD/DNS/DHCP sur Windows et aussi d'un DNS auxiliaire sous linux,

L'intérêt est de centralisé les services

b) Phases du projet

Prérequis :

Attribution d'un IP Fixe au Serveur.



Après un redémarrage, ajouter des rôles et des fonctionnalités au serveur. Sélectionner le serveur et puis cocher

Assistant Ajout de rôles et de fonctionnalités

Avant de commencer

Type d'installation

Sélection du serveur

Rôles de serveurs

Fonctionnalités

Confirmation

Résultats

Sélectionner le serveur de destination

SERVEUR DE DESTINATION
WIN-V4LCRA0GF80

Sélectionnez le serveur ou le disque dur virtuel sur lequel installer des rôles et des fonctionnalités.

☒ Sélectionner un serveur du pool de serveurs
☐ Sélectionner un disque dur virtuel

Pool de serveurs

Filtre :

| Nom | Adresse IP | Système d'exploitation |
|-----------------|------------|---|
| WIN-V4LCRA0GF80 | 172.20.0.1 | Microsoft Windows Server 2019 Standard Evaluation |

1 ordinateur(s) trouvé(s)

Cette page présente les serveurs qui exécutent Windows Server 2012 ou une version ultérieure et qui ont été ajoutés à l'aide de la commande Ajouter des serveurs dans le Gestionnaire de serveur. Les serveurs hors connexion et les serveurs nouvellement ajoutés dont la collecte de données est toujours incomplète ne sont pas répertoriés.

< Précédent

Suivant >

Installer

Annuler

Assistant Ajout de rôles et de fonctionnalités

Avant de commencer

Type d'installation

Sélection du serveur

Rôles de serveurs

Fonctionnalités

Confirmation

Résultats

Sélectionner des rôles de serveurs

SERVEUR DE DESTINATION
WIN-V4LCRA0GF80

Sélectionnez un ou plusieurs rôles à installer sur le serveur sélectionné.

Rôles

☐ Accès à distance
☐ Attestation d'intégrité de l'appareil
☐ Hyper-V
☐ Serveur de télécopie
☒ Serveur DHCP (Installé)
☒ Serveur DNS (Installé)
☐ Serveur Web (IIS)
☐ Service Guardian hôte
☒ Services AD DS (Installé)
☐ Services AD LDS (Active Directory Lightweight Directory Services)
☐ Services AD RMS (Active Directory Rights Management Services)
☐ Services Bureau à distance
☐ Services d'activation en volume
☐ Services d'impression et de numérisation de documents
☐ Services de certificats Active Directory
☐ Services de déploiement Windows
☐ Services de fédération Active Directory (AD FS)
☒ Services de fichiers et de stockage (1 sur 12 installés)
☐ Services de stratégie et d'accès réseau

Description

L'accès à distance fournit une connectivité transparente via DirectAccess, les réseaux VPN et le proxy d'application Web. DirectAccess fournit une expérience de connectivité permanente et gérée en continu. Le service d'accès à distance (RAS) fournit des services VPN classiques, notamment une connectivité de site à site (filiale ou nuage). Le proxy d'application Web permet la publication de certaines applications HTTP et HTTPS spécifiques de votre réseau d'entreprise à destination d'appareils clients situés hors du réseau d'entreprise. Le routage fournit des fonctionnalités de routage classiques, notamment la traduction d'adresses réseau.

< Précédent

Suivant >

Installer

Annuler

Configuration AD

Puis dans le gestionnaire de serveur, cliquer sur le drapeau puis « Promouvoir ce serveur en contrôleur de domaine ».

Gestionnaire de serveur

Gestionnaire de serveur ▶ Tableau de bord

Gérer Outils Afficher Aide

Tableau de bord

- Serveur local
- Tous les serveurs
- AD DS
- DHCP
- DNS
- Services de fichiers et d...

BIENVENUE DANS GESTIONNAIRE DE SERVEUR

1 DÉMARRAGE RAPIDE

2

3

4

5 Connecter ce serveur aux services cloud

Masquer

Configuration post-déploiement

Configuration requise pour : Services AD DS à SRV-AD

Promouvoir ce serveur en contrôleur de domaine

Configuration post-déploiement

Configuration requise pour : Serveur DHCP à SRV-AD

Terminer la configuration DHCP

Détails de la tâche

Rôles et groupes de serveurs

Rôles : 4 | Groupes de serveurs : 1 | Nombre total de serveurs : 1

| Rôle | Nombre |
|-------|--------|
| AD DS | 1 |
| DHCP | 1 |

Facilité de gestion

- Événements
- Services
- Performances
- Résultats BPA

Assistant Configuration des services de domaine Active Directory

— □ ×

Configuration de déploiement

SERVEUR CIBLE
SRV-AD

- Configuration de déploie...
- Options du contrôleur de...
- Options DNS
- Options supplémentaires
- Chemins d'accès
- Examiner les options
- Vérification de la configur...
- Installation
- Résultats

Sélectionner l'opération de déploiement

- ☐ Ajouter un contrôleur de domaine à un domaine existant
- ☐ Ajouter un nouveau domaine à une forêt existante
- ☒ Ajouter une nouvelle forêt

Spécifiez les informations de domaine pour cette opération

Nom de domaine racine :

[En savoir plus sur les configurations de déploiement](#)

< Précédent Suivant > Installer Annuler

Ajouter une nouvelle forêt, et mettre stadiumcompany.local en nom de domaine puis cliquer sur suivant.

Options du contrôleur de domaine

SERVEUR CIBLE
SRV-AD

Configuration de déploiement...

Options du contrôleur de...

Options DNS

Options supplémentaires

Chemins d'accès

Examiner les options

Vérification de la configur...

Installation

Résultats

Sélectionner le niveau fonctionnel de la nouvelle forêt et du domaine racine

Niveau fonctionnel de la forêt : Windows Server 2016

Niveau fonctionnel du domaine : Windows Server 2016

Spécifier les fonctionnalités de contrôleur de domaine

☒ Serveur DNS (Domain Name System)

☒ Catalogue global (GC)

☐ Contrôleur de domaine en lecture seule (RODC)

Taper le mot de passe du mode de restauration des services d'annuaire (DSRM)

Mot de passe :

Confirmer le mot de passe :

[En savoir plus sur les options pour le contrôleur de domaine](#)

< Précédent

Suivant >

Installer

Annuler

Définir un mot de passe puis cliquer sur suivant.

Options DNS

SERVEUR CIBLE
SRV-AD

⚠ Il est impossible de créer une délégation pour ce serveur DNS car la zone parente faisant autorité est intro... [Afficher plus](#) ×

Configuration de déploiement...

Options du contrôleur de...

Options DNS

Options supplémentaires

Chemins d'accès

Examiner les options

Vérification de la configur...

Installation

Résultats

Spécifier les options de délégation DNS

☐ Créer une délégation DNS

[En savoir plus sur la délégation DNS](#)

< Précédent

Suivant >

Installer

Annuler

Cliquer encore sur suivant.

Options supplémentaires

SERVEUR CIBLE
SRV-AD

Configuration de déploie...

Options du contrôleur de...

Options DNS

Options supplémentaires

Chemins d'accès

Examiner les options

Vérification de la configur...

Installation

Résultats

Vérifiez le nom NetBIOS attribué au domaine et modifiez-le si nécessaire.

Le nom de domaine NetBIOS :

[En savoir plus sur d'autres options](#)

< Précédent

Suivant >

Installer

Annuler

Cliquer à nouveau sur suivant.

Sur les chemins d'accès cliquer également sur suivant.

Assistant Configuration des services de domaine Active Directory

SERVEUR CIBLE
SRV-AD

Chemins d'accès

- Configuration de déploiement...
- Options du contrôleur de domaine...
- Options DNS
- Options supplémentaires
- Chemins d'accès**
- Examiner les options
- Vérification de la configuration...
- Installation
- Résultats

Spécifier l'emplacement de la base de données AD DS, des fichiers journaux et de SYSVOL

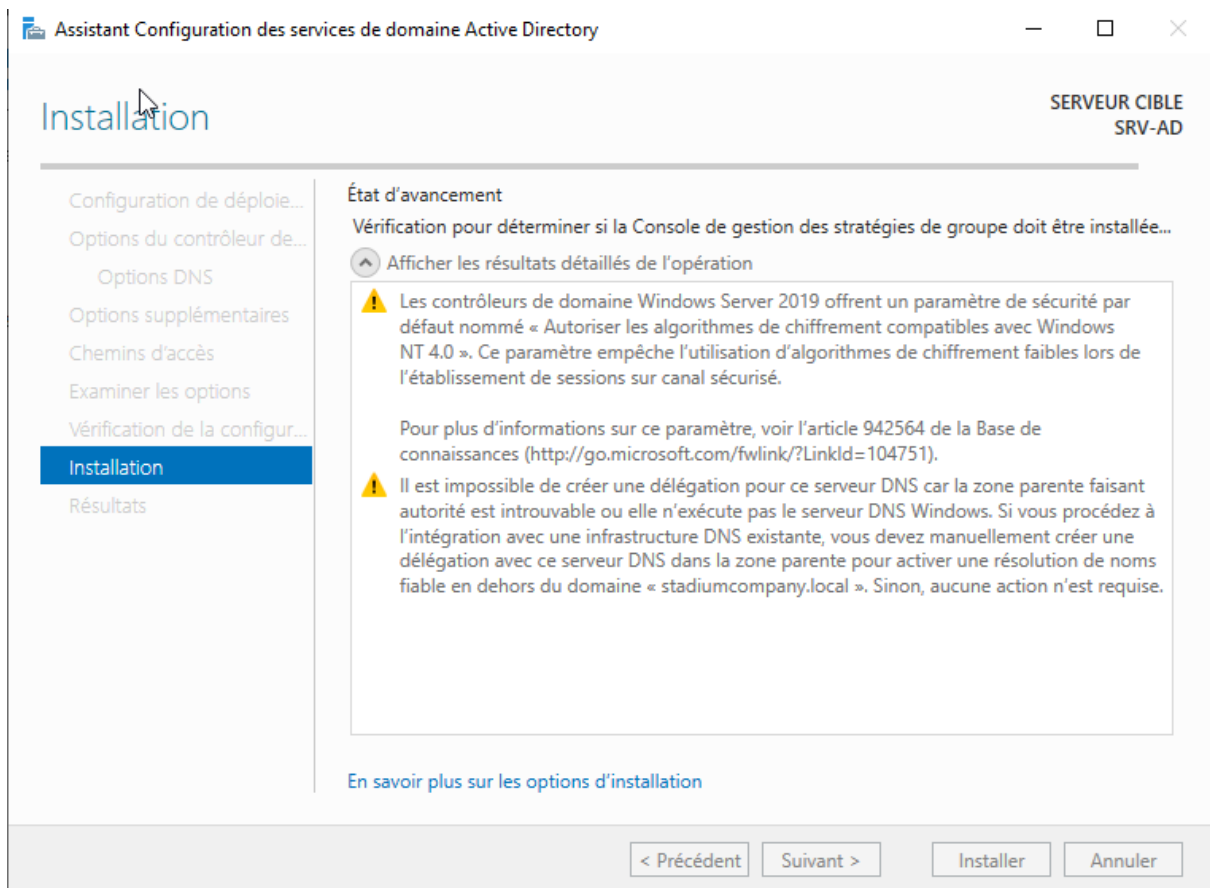
| | | |
|---------------------------------|-------------------|-----|
| Dossier de la base de données : | C:\Windows\NTDS | ... |
| Dossier des fichiers journaux : | C:\Windows\NTDS | ... |
| Dossier SYSVOL : | C:\Windows\SYSVOL | ... |

[En savoir plus sur les chemins d'accès Active Directory](#)

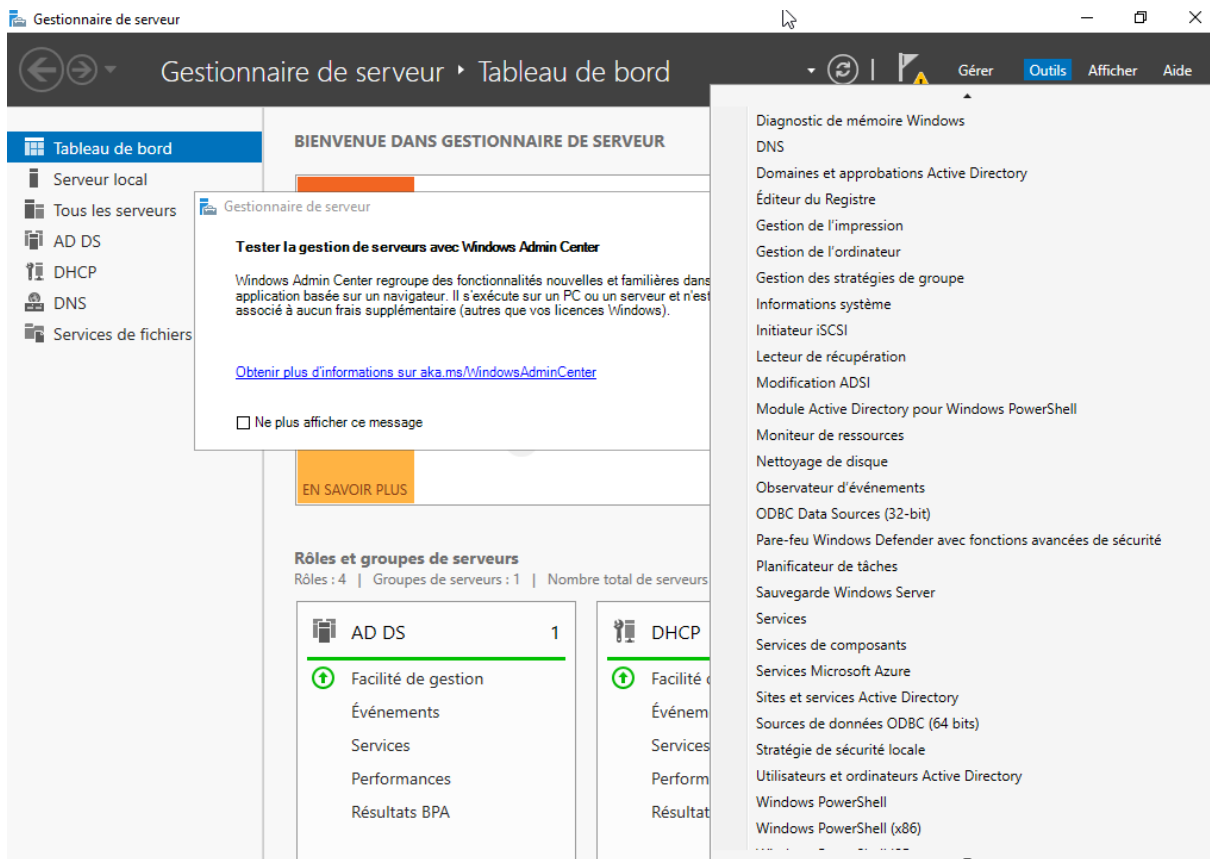
< Précédent Suivant > Installer Annuler

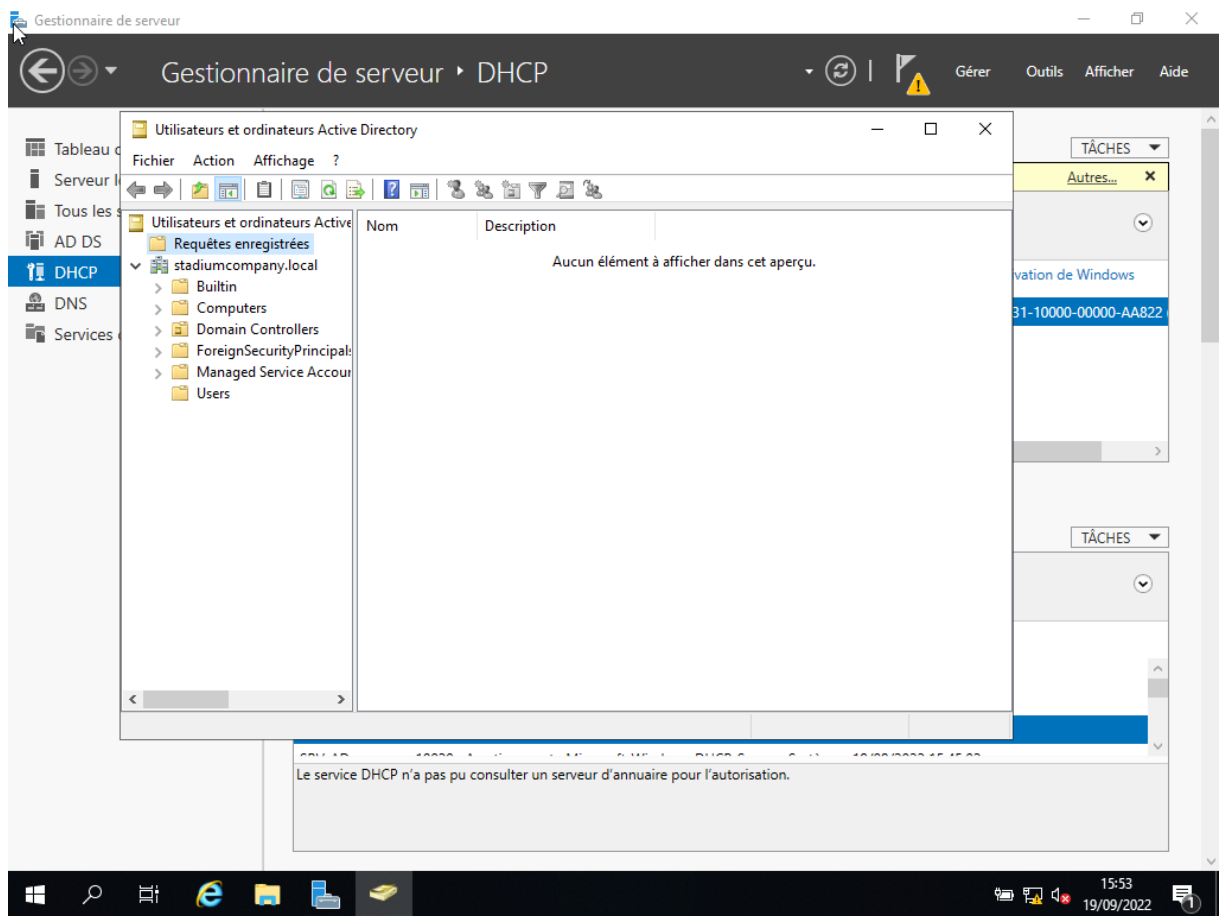
Puis cliquer sur suivant, vous allez avoir la possibilité d'afficher le script si vous le souhaitez.

Cliquer sur installer.



Après un redémarrage, aller dans gestionnaire de serveur puis outils puis « Utilisateurs et ordinateurs active directory »





Configuration DHCP

Gestionnaire de serveur ▸ DHCP

SERVEURS
Tous les serveurs | 1 au total

Configuration requise pour : Serveur DHCP à SRV-AD

Filtrer

| Nom du serveur | Adresse IPv4 | Facilité de gestion |
|----------------|--------------|---------------------------------|
| SRV-AD | 172.20.0.1 | En ligne - Compteurs de perform |

ÉVÉNEMENTS
Tous les événements | 9 au total

Filtrer

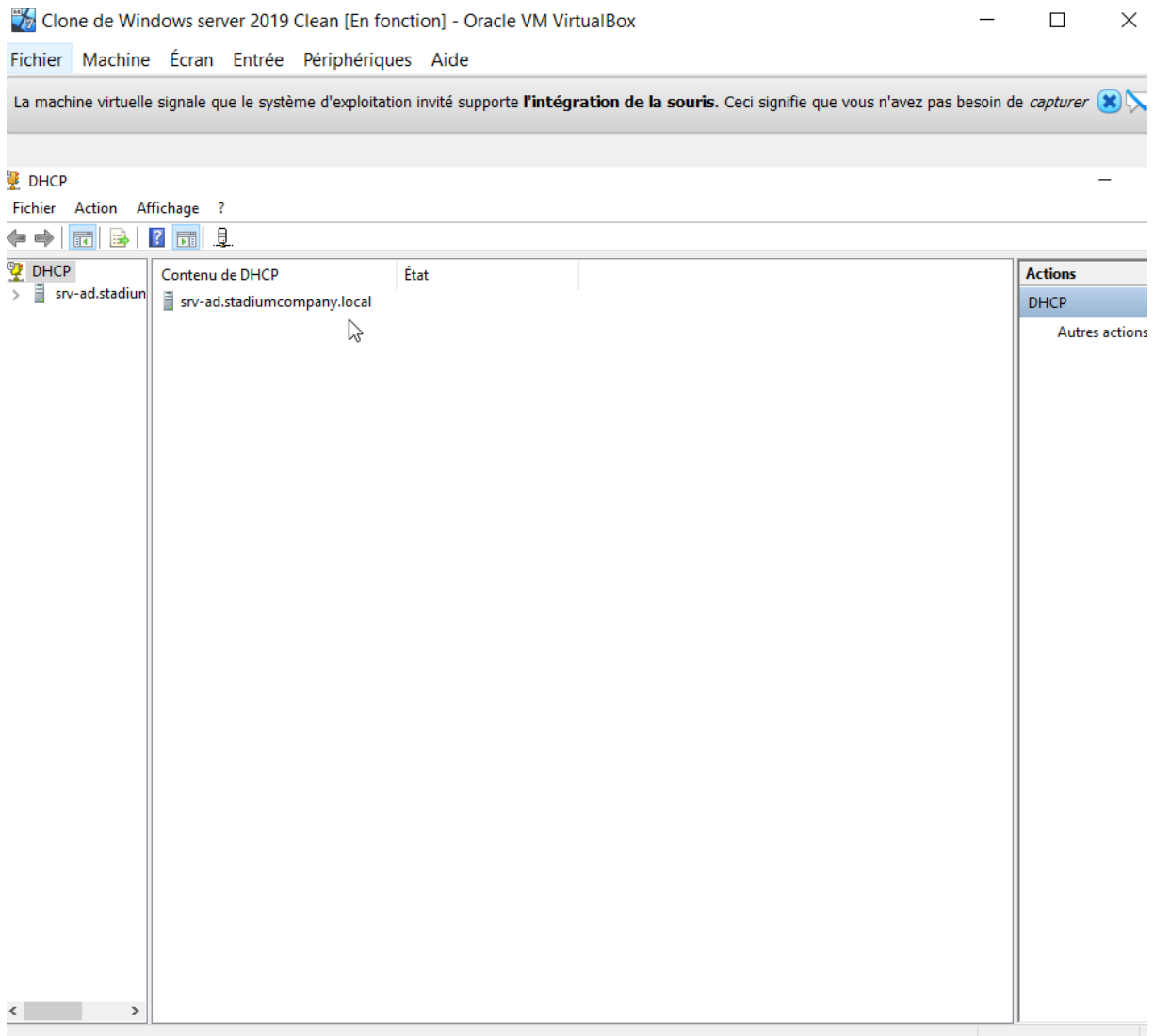
| Nom du serveur | ID | Gravité | Source |
|----------------|------|---------|---------------------|
| SRV-AD | 1059 | Erreur | Microsoft-Windows-D |
| SRV-AD | 1046 | Erreur | Microsoft-Windows-D |
| SRV-AD | 1059 | Erreur | Microsoft-Windows-D |

Le service DHCP n'a pas pu consulter un serveur d'annuaire pour l

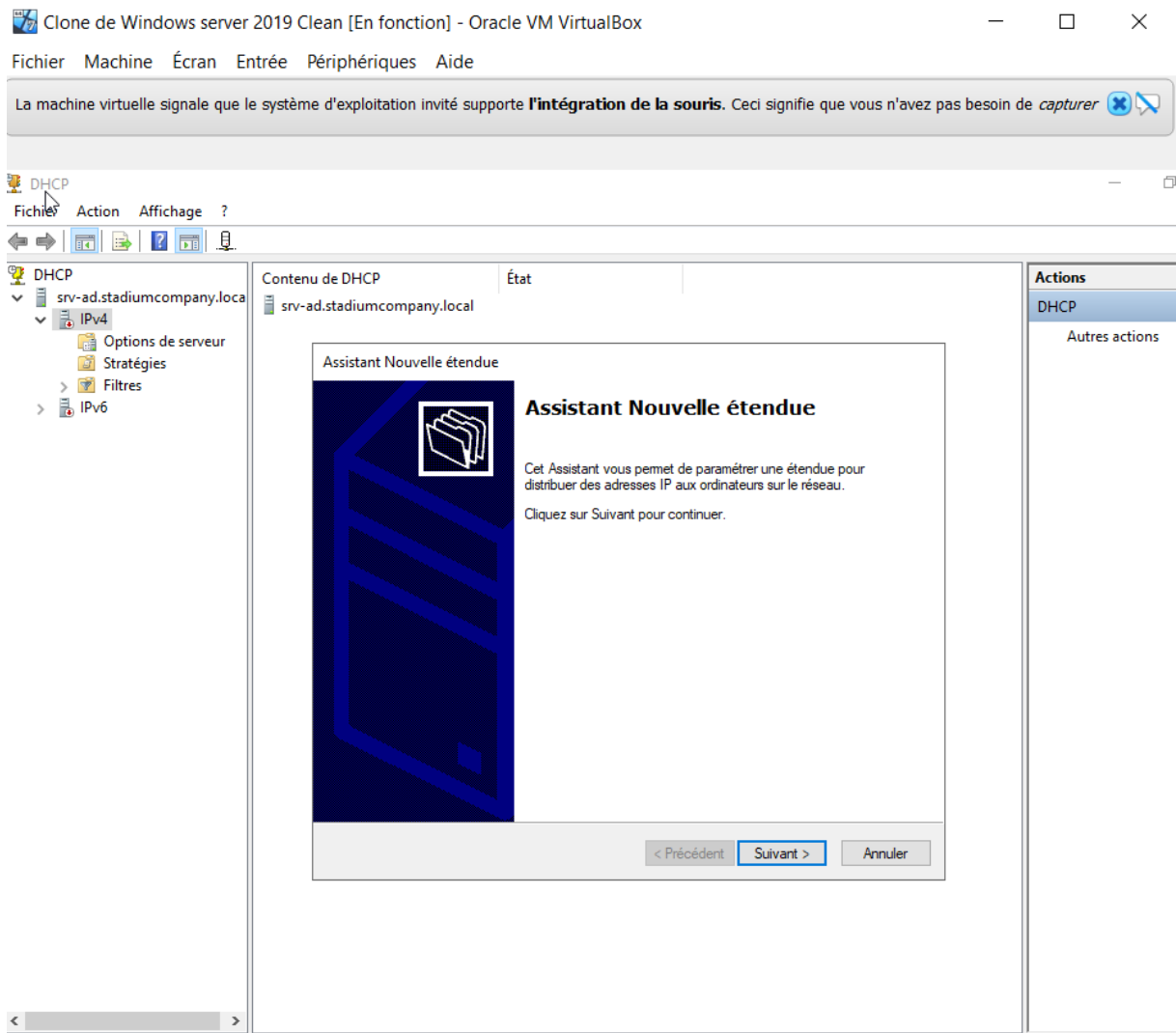
Gérer Outils Afficher

- Configuration du système
- Défragmenter et optimiser les lecteurs
- DHCP
- Diagnostic de mémoire Windows
- DNS
- Domaines et approbations Active Directory
- Éditeur du Registre
- Gestion de l'impression
- Gestion de l'ordinateur
- Gestion des stratégies de groupe
- Informations système
- Initiateur iSCSI
- Lecteur de récupération
- Modification ADSI
- Module Active Directory pour Windows PowerShell
- Moniteur de ressources
- Nettoyage de disque
- Observateur d'événements
- ODBC Data Sources (32-bit)
- Pare-feu Windows Defender avec fonctions avancées de sécur
- Planificateur de tâches
- Sauvegarde Windows Server
- Services
- Services de composants
- Services Microsoft Azure
- Sites et services Active Directory
- Sources de données ODBC (64 bits)
- Stratégie de sécurité locale

Cette fenêtre s'ouvre alors



Dérouler l'arborescence à gauche puis clic droit sur IPV4 et créer une nouvelle étendue.



Il faut définir une plage d'adresses. Puis cliquer sur suivant.

DHCP

Fichier Action Affichage ?

← → ↻ ↺ ↻ ↺ ↻ ↺

DHCP

- srv-ad.stadiumcompany.local
 - IPv4
 - Options de serveur
 - Stratégies
 - Filtres
 - IPv6

Contenu de DHCP

srv-ad.stadiumcompany.local

État

Actions

DHCP

Autres actions

Assistant Nouvelle étendue

Plage d'adresses IP

Vous définissez la plage d'adresses en identifiant un jeu d'adresses IP consécutives.

Paramètres de configuration pour serveur DHCP

Entrez la plage d'adresses que l'étendue peut distribuer.

Adresse IP de début : 172 . 20 . 0 . 1

Adresse IP de fin : 172 . 20 . 0 . 254

Paramètres de configuration qui se propagent au client DHCP.

Longueur : 24

Masque de sous-réseau : 255 . 255 . 255 . 0

< Précédent Suivant > Annuler

Exclure l'adresse du serveur

Assistant Nouvelle étendue

Ajout d'exclusions et de retard

Les exclusions sont des adresses ou une plage d'adresses qui ne sont pas distribuées par le serveur. Un retard est la durée pendant laquelle le serveur retardera la transmission d'un message DHCP OFFER.



Entrez la plage d'adresses IP que vous voulez exclure. Si vous voulez exclure une adresse unique, entrez uniquement une adresse IP de début.

Adresse IP de début :

Adresse IP de fin :

Ajouter

Plage d'adresses exclue :

Adresse 172.20.0.1

Supprimer

Retard du sous-réseau en
millisecondes :

< Précédent

Suivant >

Annuler

Pour les baux, laisser 8 jours

Puis configurer maintenant les options DHCP

Configuration des paramètres DHCP

Vous devez configurer les options DHCP les plus courantes pour que les clients puissent utiliser l'étendue.



Lorsque les clients obtiennent une adresse, ils se voient attribuer des options DHCP, telles que les adresses IP des routeurs (passerelles par défaut), des serveurs DNS, et les paramètres WINS pour cette étendue.

Les paramètres que vous sélectionnez maintenant sont pour cette étendue et ils remplaceront les paramètres configurés dans le dossier Options de serveur pour ce serveur.

Voulez-vous configurer les options DHCP pour cette étendue maintenant ?

- ☒ Oui, je veux configurer ces options maintenant.
- ☐ Non, je configurerai ces options ultérieurement

< Précédent

Suivant >

Annuler

Routeur (passerelle par défaut)

Vous pouvez spécifier les routeurs, ou les passerelles par défaut, qui doivent être distribués par cette étendue.



Pour ajouter une adresse IP pour qu'un routeur soit utilisé par les clients, entrez l'adresse ci-dessous.

Adresse IP :

| . . .

Ajouter

172.20.0.254

Supprimer

Monter

Descendre

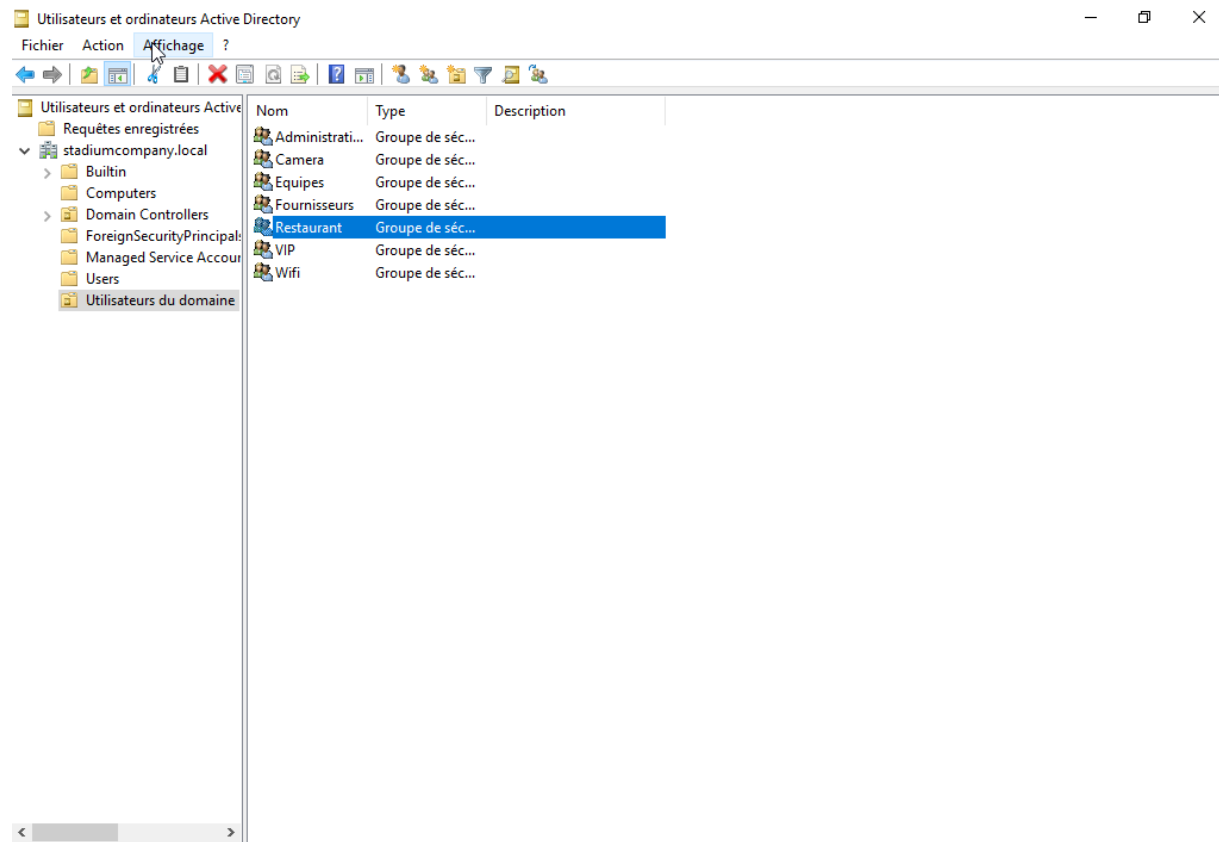
< Précédent

Suivant >

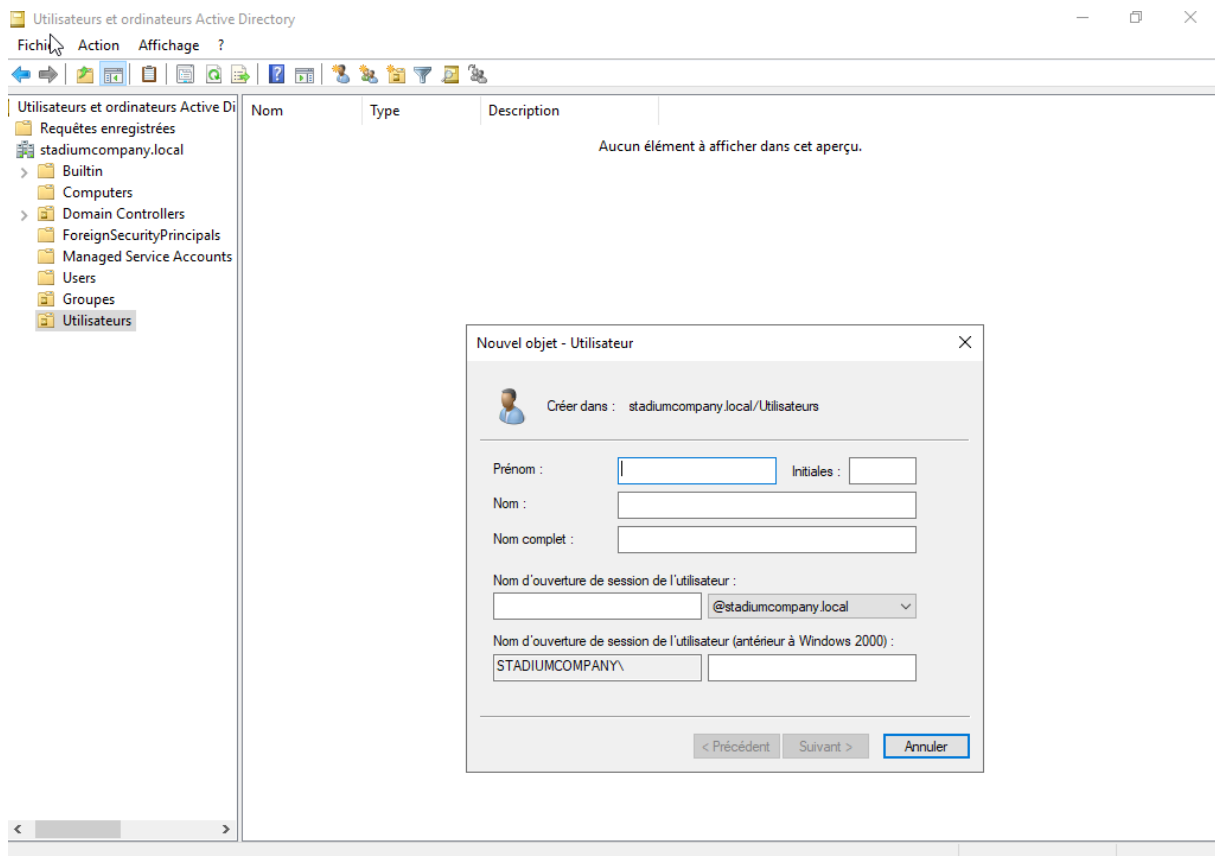
Annuler

Puis après cliquer sur suivant et activer cette étendue maintenant.

Création de l'ensemble des groupes dans l'AD.

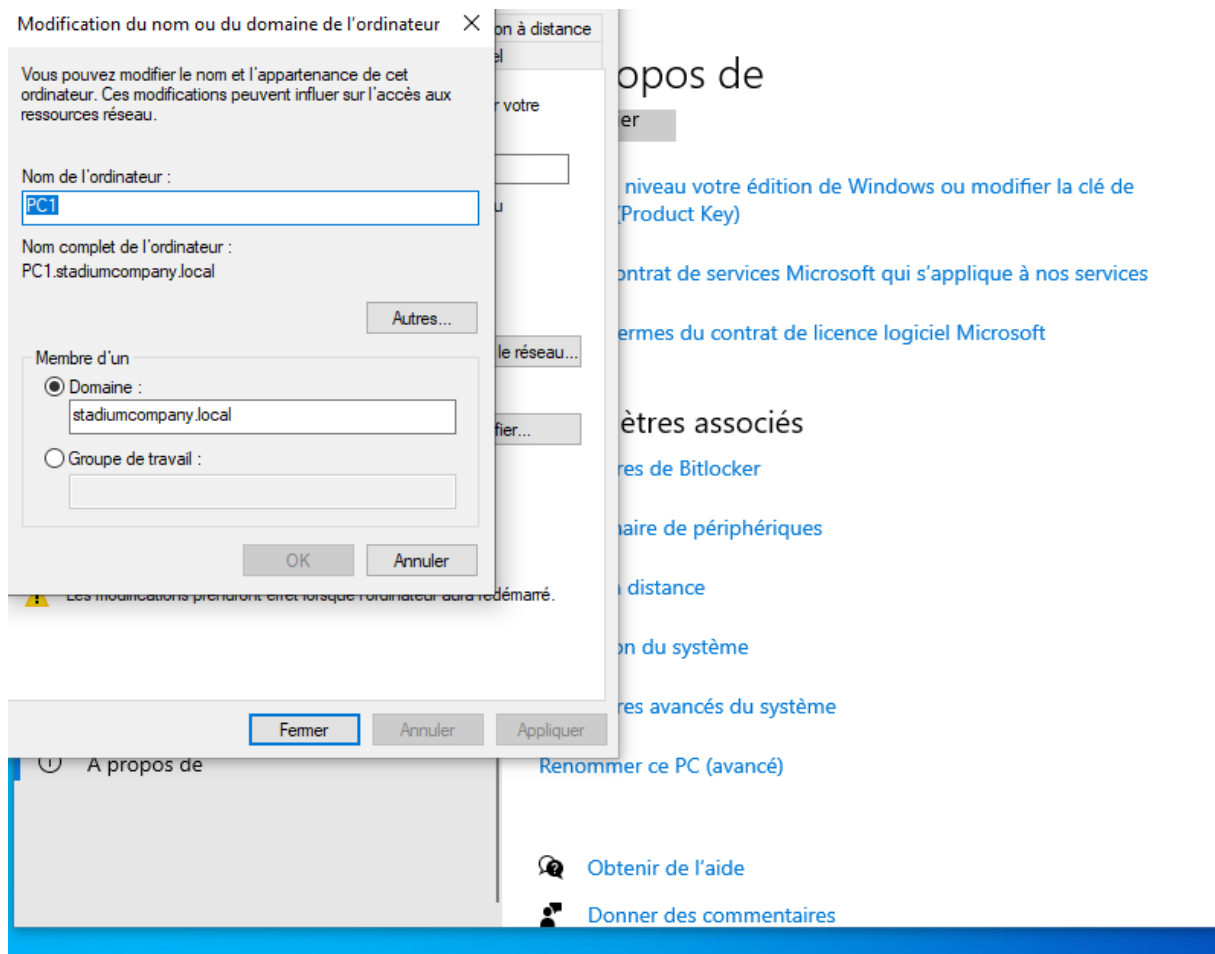


Il faut après créer un utilisateur et le mettre dans le groupe de sécurité administration.



Après démarrer un client Windows 10, joindre le domaine et se connecter avec le compte utilisateur créé. Démarrer un cmd faire un ipconfig /all et vérifier que l'adresse attribuée est bien dans la plage d'adresses configurée pour le service administration.

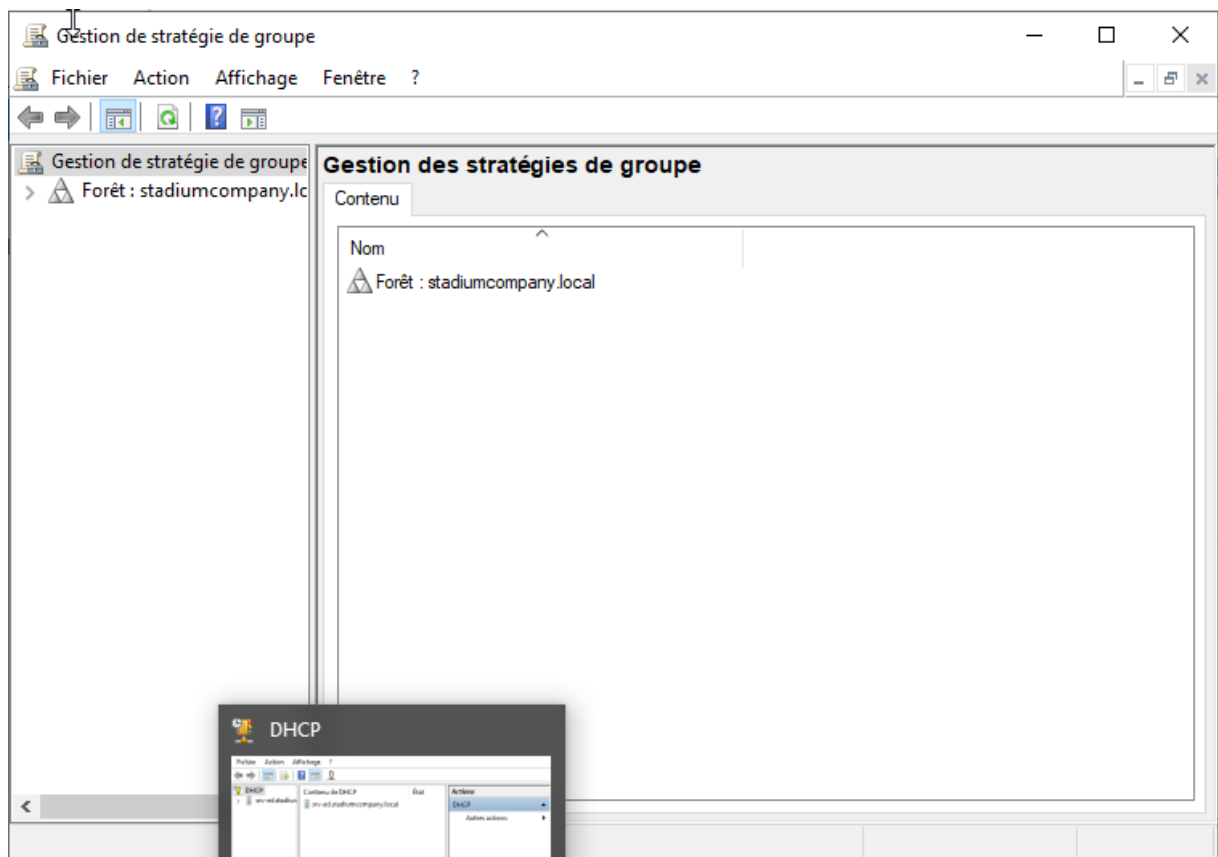
Il faut donc sur le client Windows 10 renommer le PC et joindre le domaine. Puis effectuer un redémarrage.



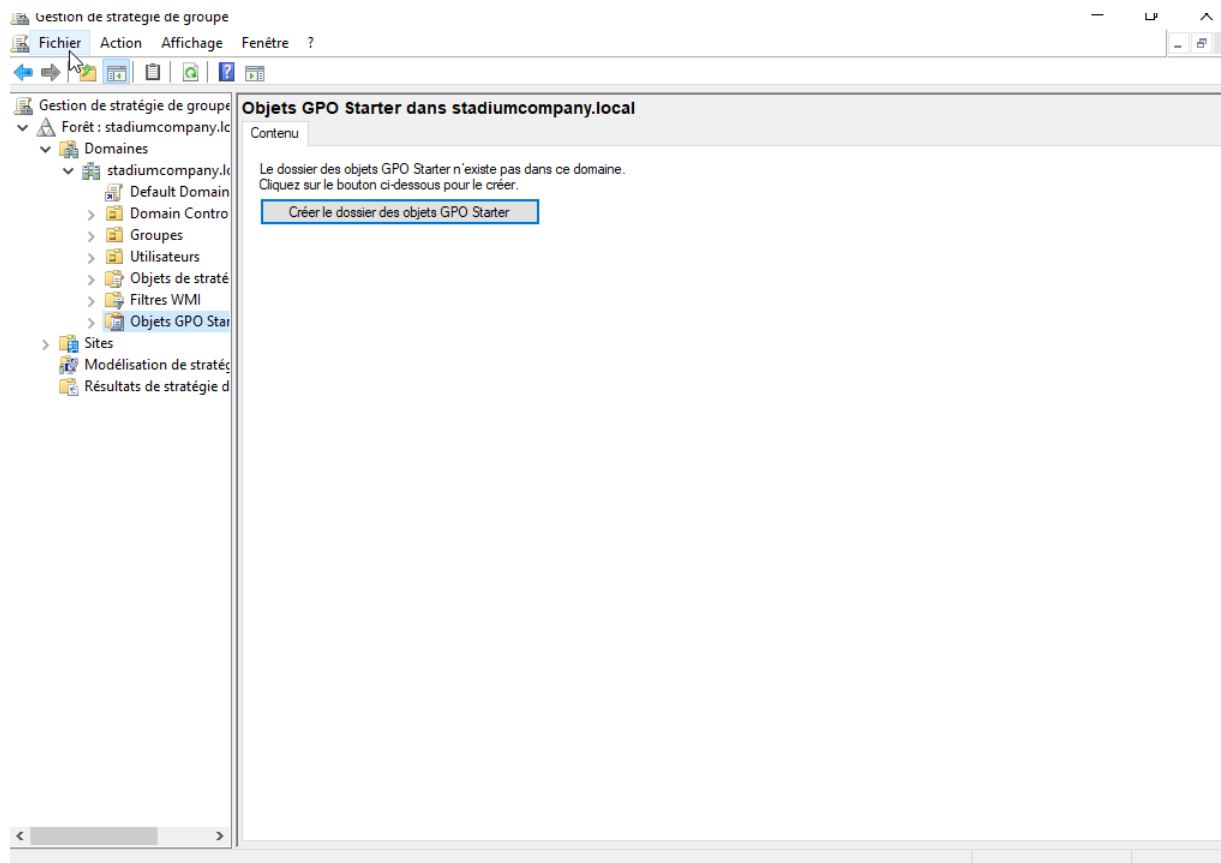
On voit que le client a bien récupéré l'adresse IP.

Configuration GPO

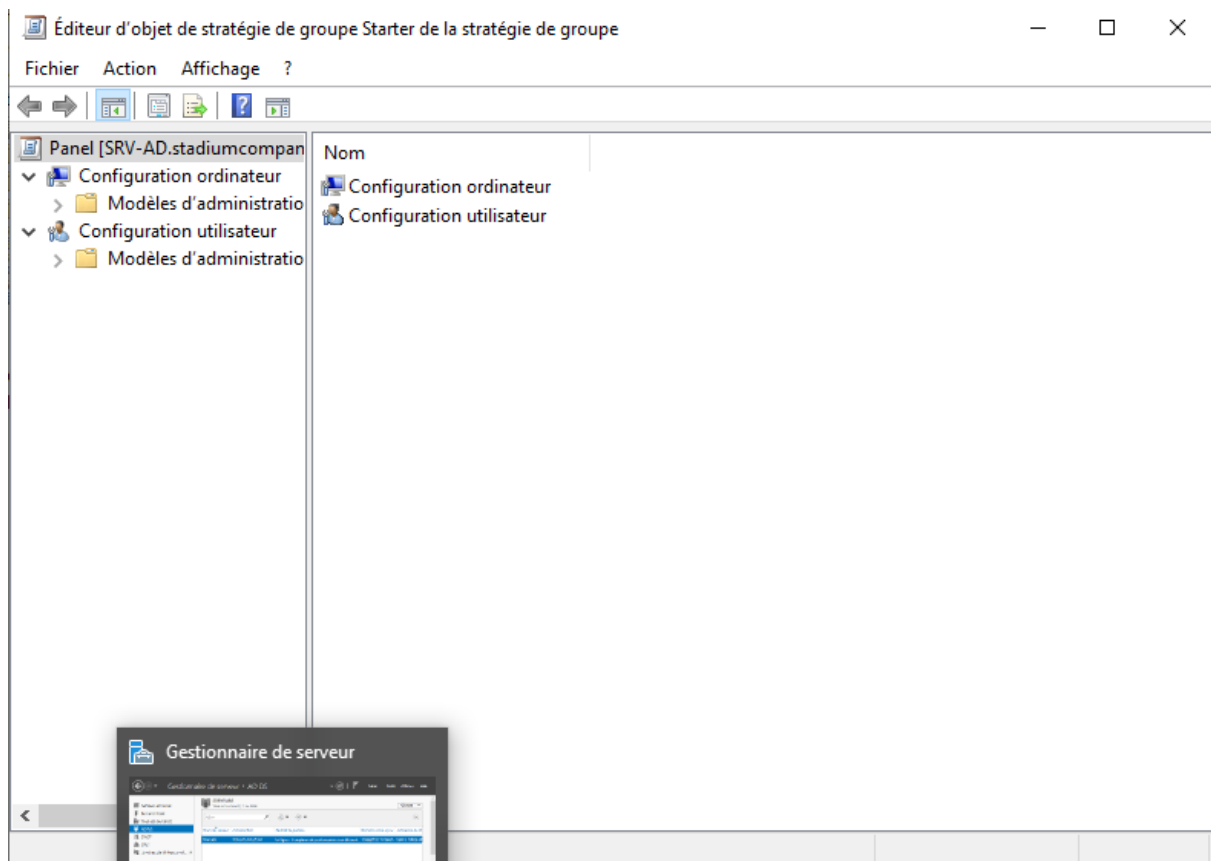
Retourner sur le serveur, ouvrir gestion de stratégie de groupe



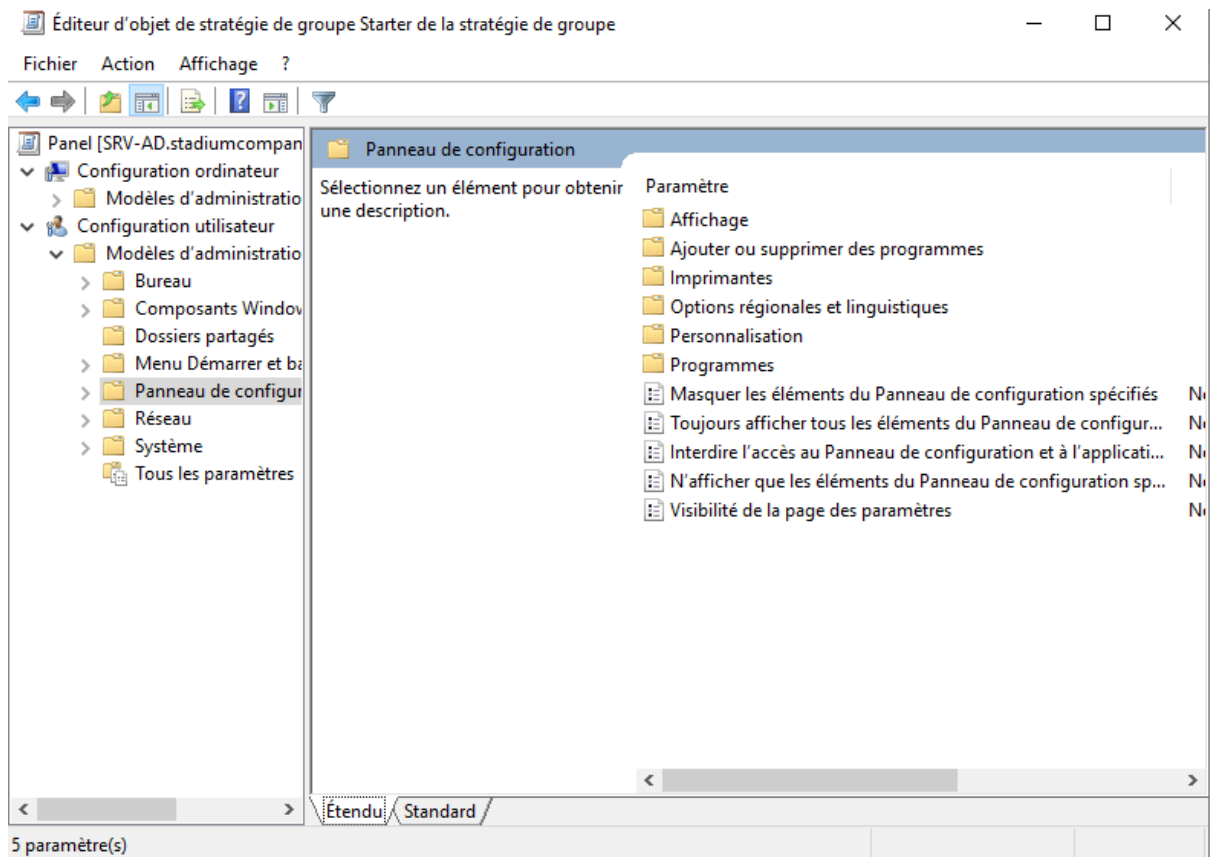
Aller dans domaine, puis stadium puis objet de stratégie.



Cliquer sur créer puis nommer sa GPO puis clique droit « modifier »



Aller dans configuration utilisateur puis modèles d'administration puis Panneau de configuration.



Cliquer sur interdire l'accès au panneau de configuration et puis activer.

Interdire l'accès au Panneau de configuration et à l'application Paramètres du PC

Paramètre précédent Paramètre suivant

☐ Non configuré Commentaire :

☒ Activé

☐ Désactivé

Pris en charge sur :

Options : Aide :

Désactive tous les programmes du Panneau de configuration et l'application Paramètres du PC.

Ce paramètre empêche le démarrage de Control.exe, de SystemSettings.exe, des fichiers programme du Panneau de configuration et de l'application Paramètres du PC. Ainsi, les utilisateurs ne peuvent pas démarrer le Panneau de configuration, l'application Paramètres du PC, ni aucun de leurs éléments.

Ce paramètre permet de supprimer le Panneau de configuration des éléments suivants :

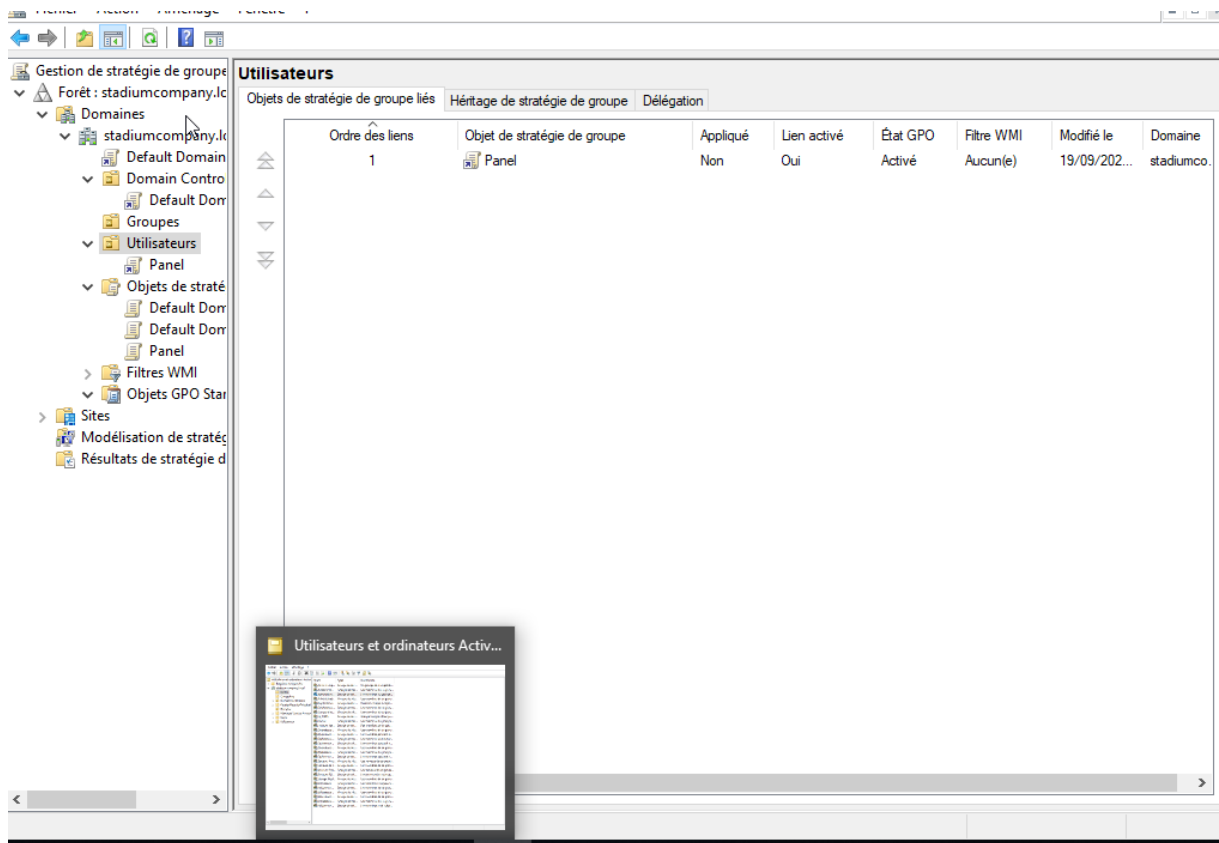
- Écran de démarrage
- Explorateur de fichiers

Ce paramètre permet de supprimer l'application Paramètres du PC des éléments suivants :

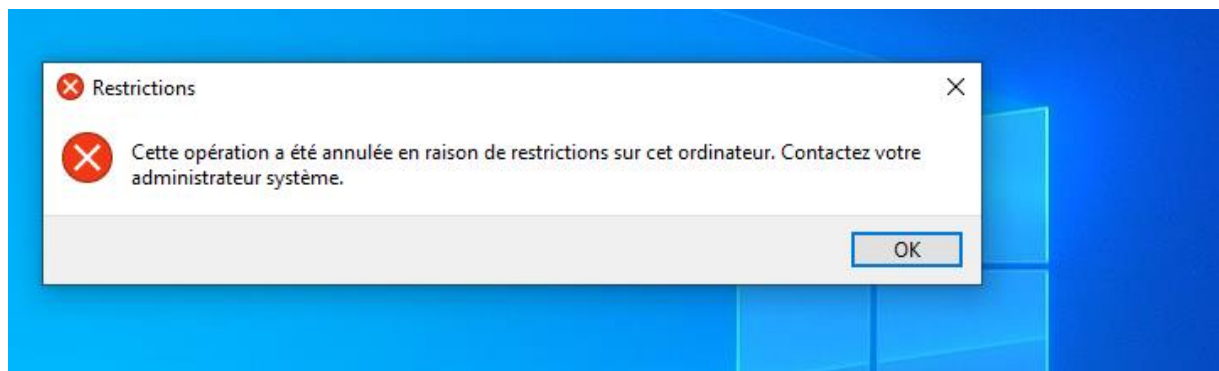
- Écran de démarrage
- Icône Paramètres
- Avatar du compte

OK Annuler Appliquer

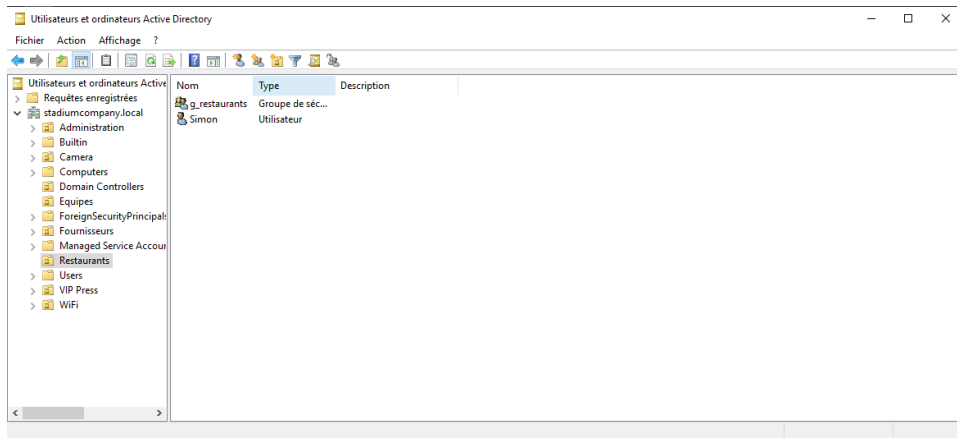
Cliquer sur utilisateur puis lier la GPO, choisir la GPO« panel » et la GPO doit s'appliquer.



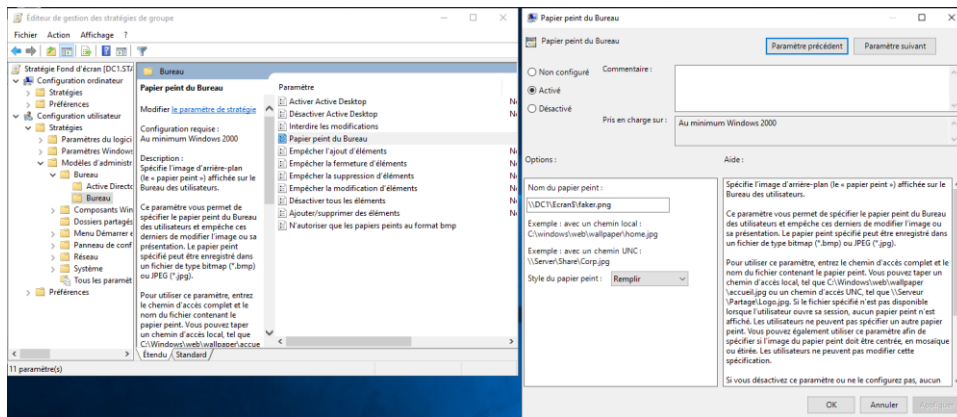
Voilà ce qui doit apparaitre sur le poste utilisateur.



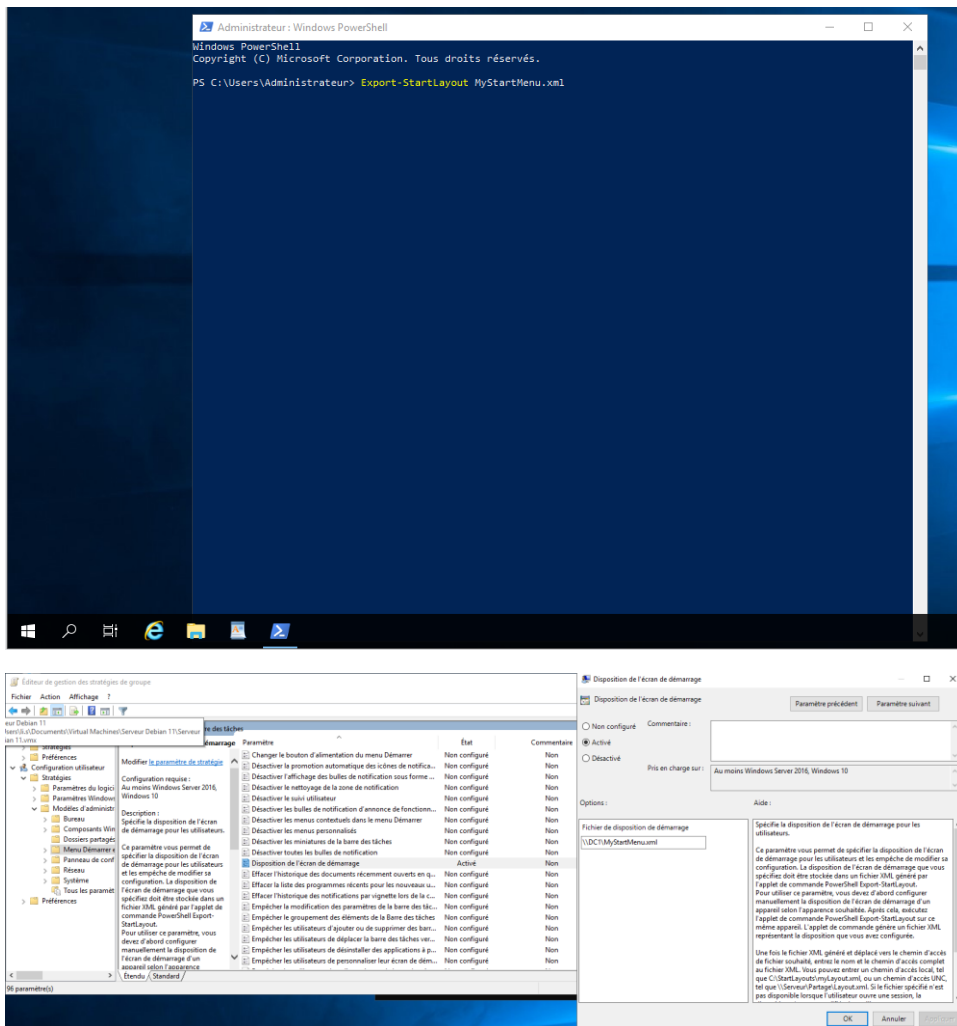
Les unités organisationnelles et leurs groupes respectifs g_nomdel'UO.



GPO fond d'écran



GPO Barre des tâches



Installation DNS SECONDAIRE

Présentation du service DNS

1) Introduction Le Domain Name System (ou DNS, système de noms de domaine) est un service permettant de traduire un nom de domaine en informations de plusieurs types qui y sont associées, notamment en adresses IP de la machine portant ce nom.

2) DNS Primaire Le DNS primaire est le premier serveur que le poste informatique va interroger pour connaître l'adresse IP associé à un nom. Si le poste n'arrive pas à contacter le DNS primaire, il essaiera alors de joindre le secondaire.

3) DNS Secondaire Au moyen d'un serveur DNS votre domaine est connu sur internet. Un serveur DNS secondaire est une sauvegarde (backup) de ce serveur DNS primaire. Les données qui se trouvent sur le serveur secondaire sont les mêmes que celles sur le serveur DNS primaire.

Avantage d'un serveur DNS secondaire :

- Fiable : Grâce au serveur DNS secondaire qui sert de sauvegarde, vos noms de domaine resteront disponibles en dehors de votre réseau, même s'il y a un problème avec le serveur primaire.

Prérequis

- Installation d'une machine virtuelle Debian

Configuration de base du serveur Debian Dans notre architecture le serveur DNS primaire lié à l'AD d'une machine virtuelle sous Windows 2019 serveur d'adresse IP fixe 172.20.0.10/24 Le serveur Debian qui sert de DNS secondaire est à l'adresse IP fixe 172.20.0.3/24

```
auto lo
iface lo net loopback
auto ens33
iface ens33 inet static
address 172.20.0.3
netmask 255.255.255.0
network 172.20.0.0
```

Configuration du fichier « resolv.conf »

```
domain stadiumcompany.local
search stadiumcompany.local
nameserver 172.20.0.10 ---> IP DC1
nameserver 172.20.0.3 --> IP ns-2
```

Fixer le fichier /etc/resolv.conf
chattr +i /etc/resolv.conf

Configuration du fichier « hosts », ce fichier permet de nommer notre serveur

```
127.0.0.1.          localhost
172.20.0.10         ns2      ns-2.stadiumcompany.local
```

Installer bind9

```
apt install bind9 bind9-utils
```

Configuration du Bind9

Arrêter le service Bind9 :
systemctl stop bind9

Les fichiers à configurer sont :

- named.conf.local (répertoire : /etc/bind).
- Les fichiers de zones (à créer).

Configuration du fichier « named.conf.local »

```
zone "stadiumcompany.local"
{
type slave ;
masters {172.20.0.10;};
file "/etc/bind/zones/stadiumcompany.local.db" ;
};
```

Pour rappel le DNS utilise deux structures d'arbres :
 La résolution directe dont la racine est un point.
 La résolution inversée la racine est le in-addr.arpa.
 Ajouter encore les lignes suivantes au dernier fichier :

```
Zone "20.172.in-addr.arpa"
{
type slave;
masters {172.20.0.10;};
file "/etc/bind/zones/stadiumcompany.local.rev"
};
```

Dans ce fichier nous indiquons que notre serveur Debian est esclave « type slave » et que le serveur maître se trouve à l'adresse 172.20.0.1 (serveur AD/DNS windows). Nous notons les fichiers de zone créés précédemment :

- stadiumcompany.com.db, pour la zone directe
- stadiumcompany.com.rev, pour la zone inverse

Le répertoire n'est pas spécifié mais, par défaut, il l'est dans le fichier named.conf.option.

Création et configuration des fichiers de zones.

Les fichiers de zone sont créés dans /etc/bind/ :

- Le fichier de zone directe : touch /etc/bind/zone/stadiumcompany.com.db,
- nano /etc/bind/zone/stadiumcompany.local.rev

Ajouter les lignes suivantes dans le fichier :

```
$TTL 604800
@ IN SOA DC1.stadiumcompany.local DC1.stadiumcompany.local. (
2 ; Serial
604800 ; Refresh
86400 ; Retry
2419200 ; Expire
604800 ) ; Negative Cache TTL
;
@ IN NS DC1.stadiumcompany.local.
@ IN NS ns-2.stadiumcompany.local.
```



```

@      IN      A      172.20.0.10
DC1    IN      A      172.20.0.10
ns-2   IN      A      172.20.0.3

```

```

GNU nano 5.4 /etc/bind/zones/stadiumcompany.local.rev
;
; BIND data file for local loopback interface
;
$TTL 604800
@ IN SOA LON-DC1.stadiumcompany.local LON-DC1.stadiumcompany.local (
2 ; Serial
604800 ; Refresh
86400 ; Retry
2419200 ; Expire
604800 ) ; Negative Cache TTL
;

@ IN NS LON-DC1.stadiumcompany.local.
@ IN NS ns-2.stadiumcompany.local.
@ IN NS 172.20.0.1
@ IN NS 172.20.0.1
LON-DC1 IN A 172.20.0.1
ns-2 IN A 172.20.0.3
10 IN PTR LON-DC1.stadiumcompany.local.
3 IN PTR ns-2.stadiumcompany.local.

```

Le fichier de zone inverse : **touch /etc/bind/zones/stadiumcompany.com.rev, nano /etc/bind/zones/stadiumcompany.com.rev**

```

;
; BIND data file for local loopback interface
;
$TTL 604800
@      IN      SOA      DC1.stadiumcompany.local DC1.stadiumcompany.local. (
                2      ; Serial
                604800  ; Refresh
                86400   ; Retry
                2419200 ; Expire
                604800 ) ; Negative Cache TTL
;
@      IN      NS       DC1.stadiumcompany.local.
@      IN      NS       ns-2.stadiumcompany.local.
DC1    IN      A        172.20.0.10
ns-2   IN      A        172.20.0.3
10     IN      PTR      DC1.stadiumcompany.local.
3      IN      PTR      ns-2.stadiumcompany.local.

```

Il nous reste à relier les fichiers de zone à leur emplacement par défaut comme spécifié dans « `named.conf.option` » : `/var/cache/bind`. Les commandes utilisées : Pour le fichier `stadiumcompany.com.db`,

`ln -s /etc/bind/zone/stadiumcompany.com.db /var/cache/bind/stadiumcompany.com.db`

Pour le fichier `stadiumcompany.com.rev`,

`ln -s /etc/bind/zone/stadiumcompany.com.rev /var/cache/bind/stadiumcompany.com.rev`

Une fois ces commandes effectuées, ce sera le DNS primaire qui mettra à jour ces fichiers.

Redémarrer Bind9 : **`systemctl restart bind9`**

Tests de configuration

Faire un test sur les 3 fichiers configurés : `named.conf.local` avec la commande :

`named-checkconf -p /etc/bind/named.conf.local`

Vérifier la configuration des zones configurées :

`named-checkzone stadiumcompany.local /etc/bind/zone/stadiumcompany.local.db`

`named-checkzone stadiumcompany.local /etc/bind/zone/stadiumcompany.local.rev`

vérifier le fichier `syslog` pour vérifier d'éventuelles erreurs, avec la commande : **`tail -50 /var/log/syslog`**

Autoriser le DNS primaire au transfert de zones

1) Zones de recherche directe

Clic droit sur les `_msdcs.stadiumcompany.local`, propriétés, onglet serveur de nom, ajouter, on renseigne le nom et l'IP de notre DNS secondaire.

Dans l'onglet transferts de zone, on sélectionne uniquement « les serveurs suivants » et on clique sur notifier.

On peut alors ajouter l'IP de notre serveur.

Cette démarche est faite également, pour la zone directe `stadiumcompany.local`.

2) Zone de recherche inversée La procédure reste la même pour la zone inversée : **`0.20.172.in-addr.arpa`**.

On vérifie que les fichiers de zones se mettent à jour, avec la commande :

`cat /var/cache/bind/stadiumcompany.com.db`

`dig SRV1.stadiumcompany.local`

Vérifier les informations dans la section ANSWER SECTION

`SRV1.stadiumcompany.local. 1200 IN A 172.20.0.2`

`;; Query time: 0 msec`

`;; SERVER: 172.20.0.10#53(172.20.0.10)`

:: WHEN: Sat Oct 22 18:36:08 CEST 2022
:: MSG SIZE rcvd: 70

Ensuite refaite la même commande en indiquant cette fois ci le serveur ns-2

```
dig stadiumcompany.local @172.20.0.3

; <<>> DiG 9.16.33-Debian <<>> stadiumcompany.local @172.20.0.3
...
;stadiumcompany.local.      IN      A

;; ANSWER SECTION:
stadiumcompany.local. 600    IN      A      172.20.0.10

;; Query time: 0 msec
;; SERVER: 172.20.0.3#53(172.20.0.3)
;; WHEN: Mon Oct 24 22:11:49 CEST 2022
;; MSG SIZE rcvd: 93
```

V)Conclusion

Nous avons mis en place un serveur DHCP/AD/DNS sur Windows server et un DNS auxiliaires sur Debian, Windows qui répond au cahier des charges grâce à sa facilité d'utilisation, sa facilité de gestion et son interface intuitive. Il permettra d'assurer le service de gestion d'utilisateur, gestion d'une partie du parc informatique. Puis nous avons configuré un DNS secondaire afin qu'elle respecte les conditions et remplissent les besoins définis par StadiumCompany.

VI)Compétences acquises

| Activité | Résultat attendu /production | Vécu/simulé /observe |
|---|---|----------------------|
| "Participation à un Projet" | Projet de refonte du réseau de StadiumCompany | Vécu/simulé/observé |
| "Maquettage et prototypage d'une solution d'infrastructure" | Réalisation de schémas d'infrastructures | Simulé |
| "Rédaction d'une Documentation technique" | Rédaction d'un dossier de projet | Vécu/simulé/observé |

| | | |
|---|--|---------------------|
| "Administration sur site ou à distance des éléments d'un réseau, de serveurs, etc." | Configuration des éléments d'interconnexion et implantation des serveurs | Vécu/simulé/observé |
|---|--|---------------------|