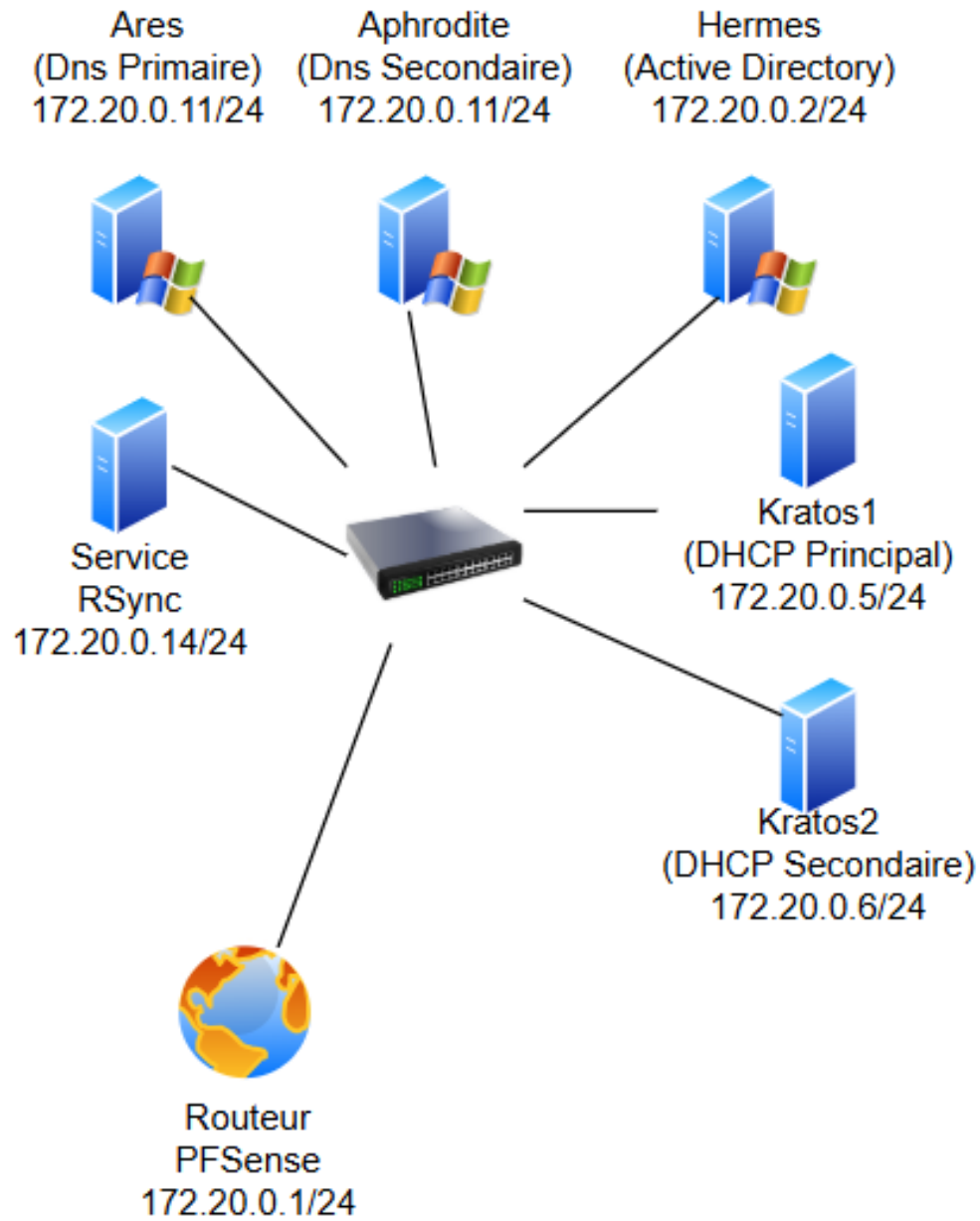


**Mission 2 : Infrastructure, Configuration et Administration des Services Informatiques de StadiumCompany**

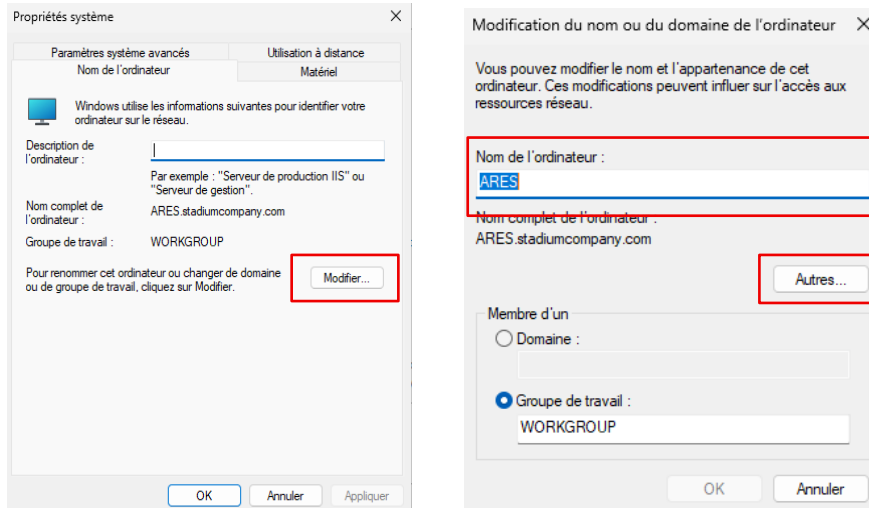


# PARTIE 1 DNS

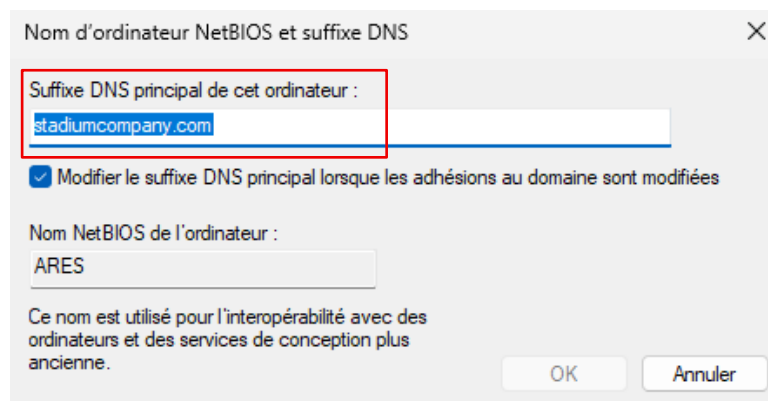
## Configuration DNS PRINCIPAL (ARES) :

### Premier préparatif (PREREQUIS) :

1. Il faut commencer par nommer notre machine ARES dans les propriétés système en cliquant sur modifier. Puis on clique sur Autres... pour ajouter le domaine qu'on va utiliser dans le Suffixe DNS principal de l'ordinateur.

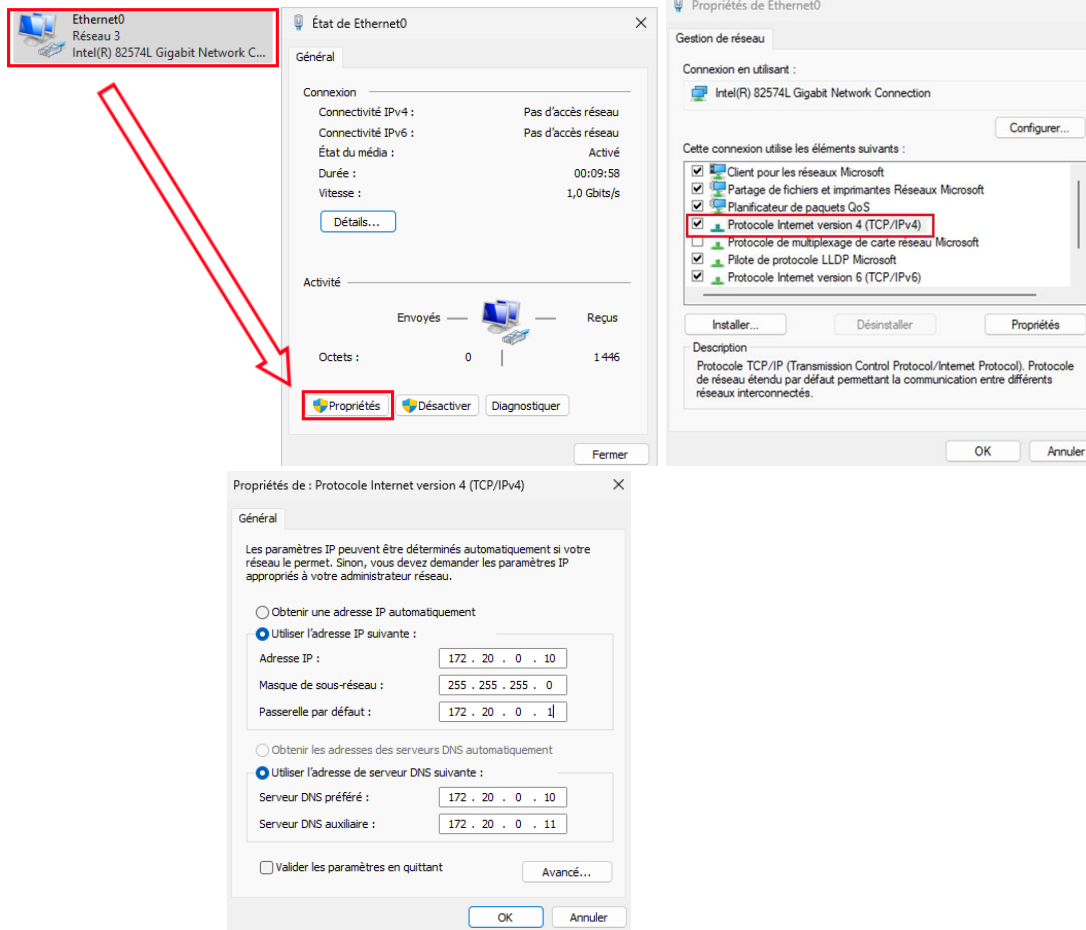


2. Ainsi, on indique le suffixe DNS principal qui est « stadiumcompany.com ». Cela permettra de faire apparaître l'enregistrement de type A correspondant au serveur ARES.



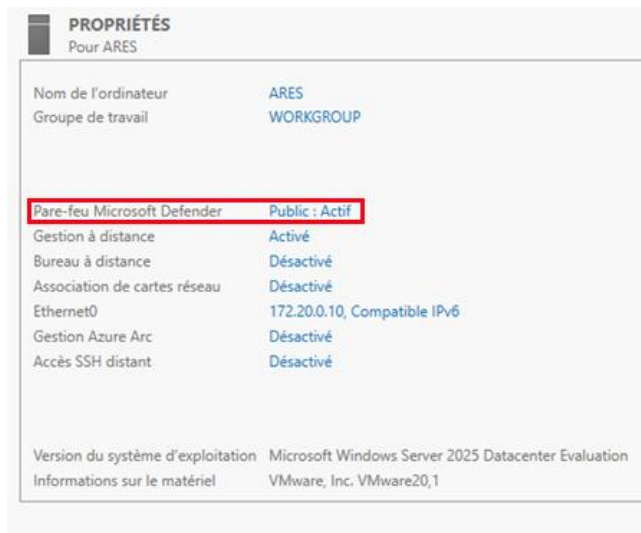
3. De plus, il faut rajouter une adresse IP statique sur notre machine accompagnée d'une passerelle par défaut et d'un serveur DNS préféré qui est celui du DNS Primaire (ARES). On a aussi déjà renseigné l'adresse du DNS Secondaire (APHRODITE) en DNS Auxiliaire.

Pour se faire, il faut se rendre dans les propriétés de l'Ethernet0 et cliquer sur le protocole Internet Version 4 (IPv4).



# Désactivation du Pare-feu

1. On clique sur Pare-feu dans les propriétés d'ARES.



## ⚙️ Pare-feu et protection du réseau

Qui et ce qui peut accéder à vos réseaux.

### 🌐 Réseau avec domaine

Le pare-feu est activé.

### 🏠 Réseau privé

Le pare-feu est activé.

### 🌐 Réseau public (actif)

Le pare-feu est activé.

[Autoriser une application via le pare-feu](#)

[Utilitaire de résolution des problèmes réseau et Internet](#)

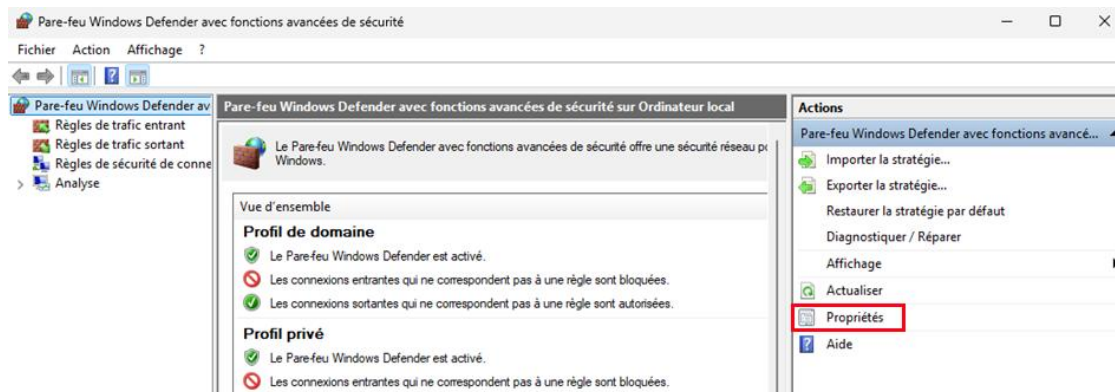
[Paramètres de notification du pare-feu](#)

**Paramètres avancés**

[Restaurer les paramètres par défaut des pare-feux](#)

2. Puis, on va dans les paramètres avancés.

3. Après cela, cliquer sur Pare-feu pour ensuite se rendre dans les propriétés.



4. Enfin, il faut désactiver tous les pare-feux de Windows. Cela nous permettra de faire interagir nos deux machines DNS, Primaire et Secondaire.

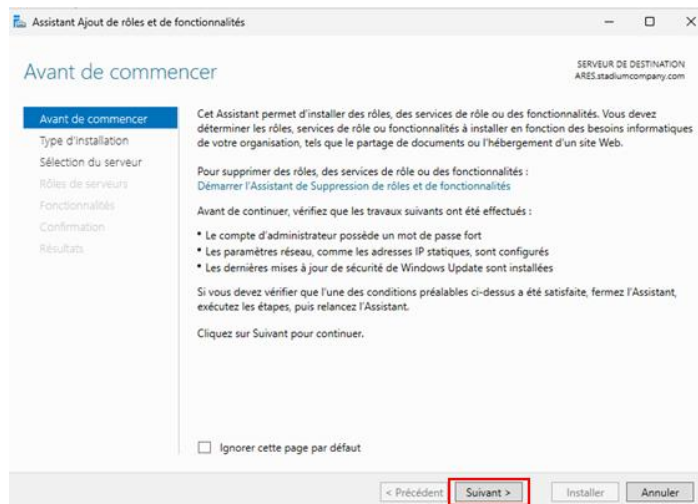


# Installation du DNS

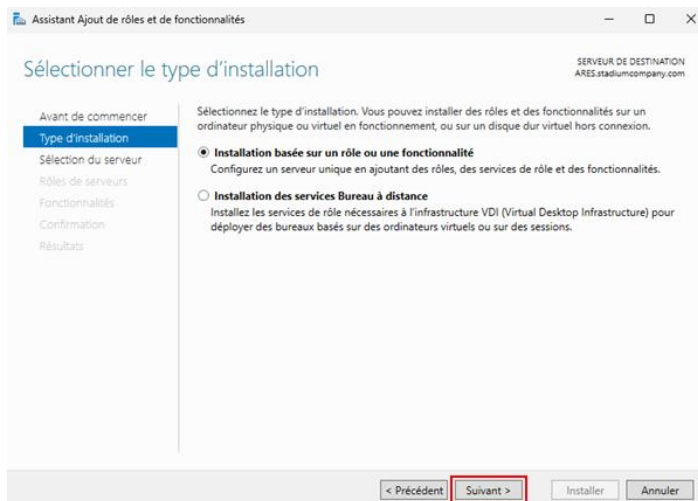
1. Dans le gestionnaire de serveur, cliquer sur Gérer puis Ajouter des rôles et fonctionnalités.



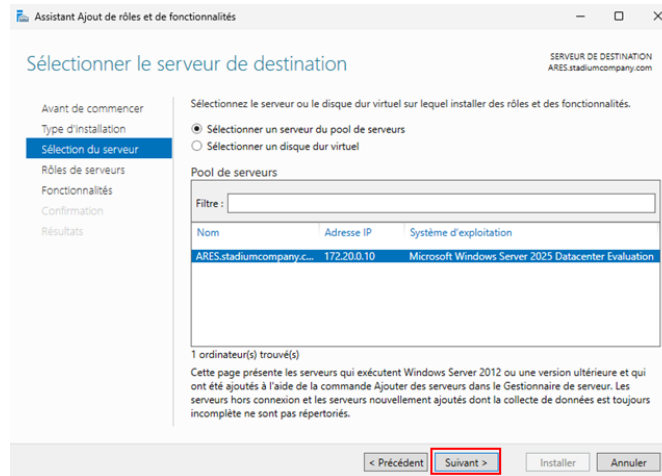
2. Sur l'assistant, il faut passer l'introduction avec « suivant ».



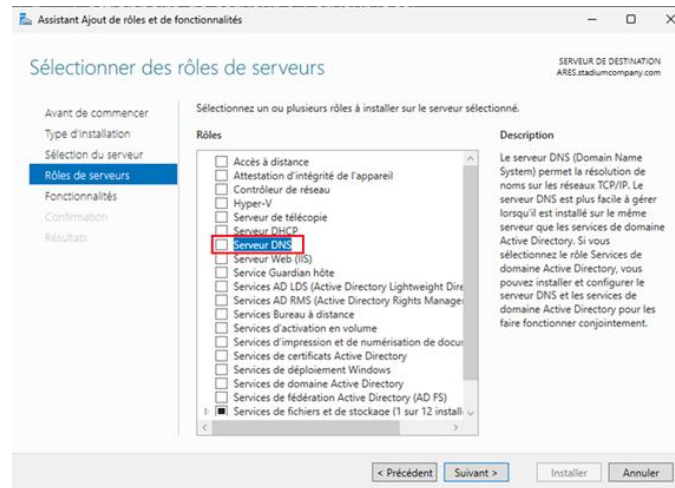
3. Ensuite, sélectionner « installation basée sur un rôle ou une fonctionnalité ».



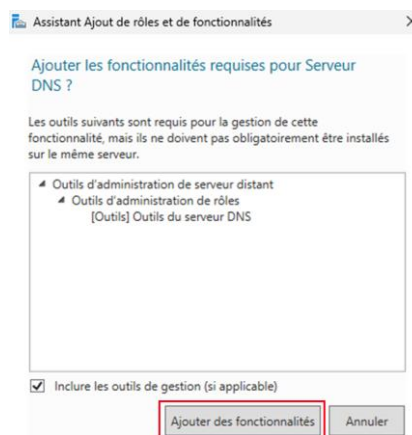
4. Puis sélectionner notre Serveur pool pour installer les rôles et cliquer sur suivant :



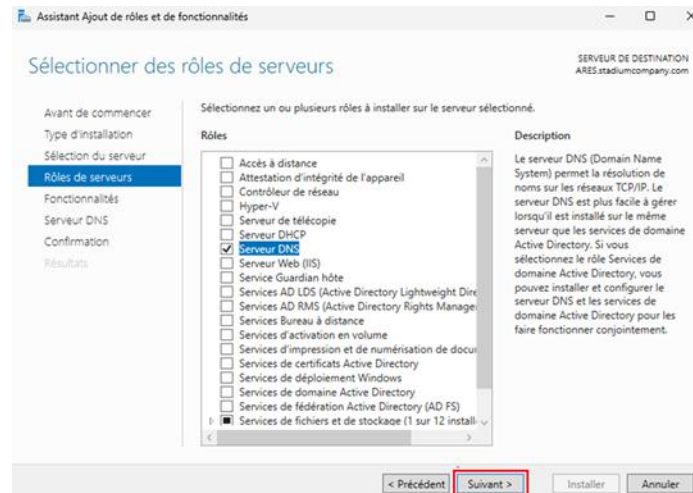
5. Ce qui nous intéresse est le DNS, donc on coche le Serveur DNS.



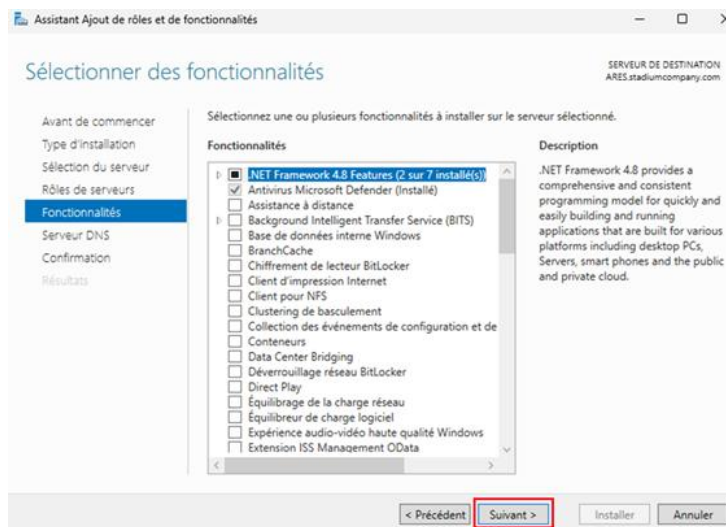
6. Il faut ajouter les fonctionnalités requises pour le Serveur DNS ainsi qu'inclure les outils de gestion.



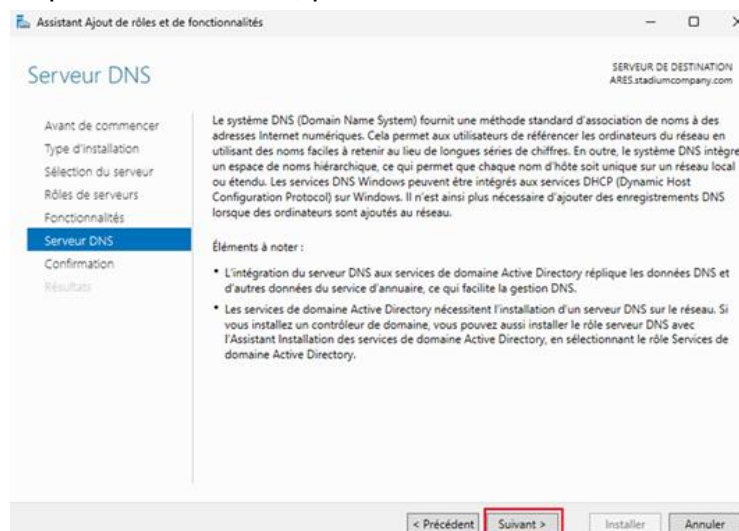
7. A la suite de cela, cliquer sur Suivant.



8. Cependant, il ne faut sélectionner aucune fonctionnalité à part le NET framework qui est déjà coché par défaut avec l'Antivirus. Puis cliquer sur Suivant.

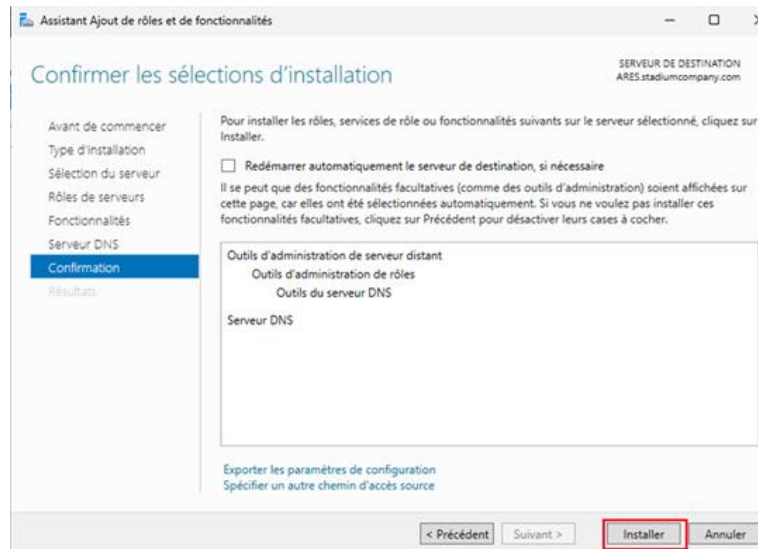


9. Passer les explications du DNS, puis faire Suivant.

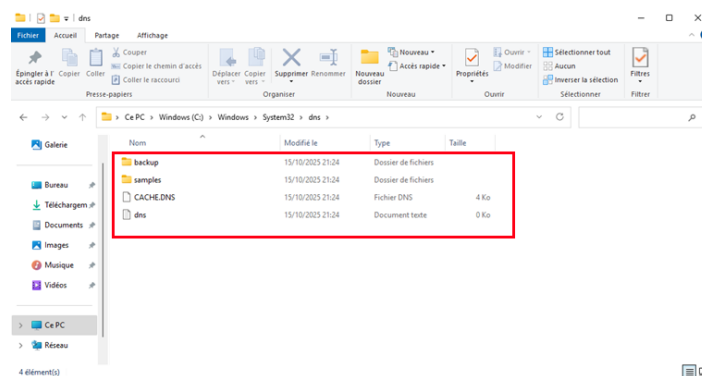


10. Enfin, confirmer l'installation en cliquant sur Installer.

Une fois l'installation terminée, fermer la fenêtre en cliquant sur Fermer qui apparaîtra à la place d'Installer.

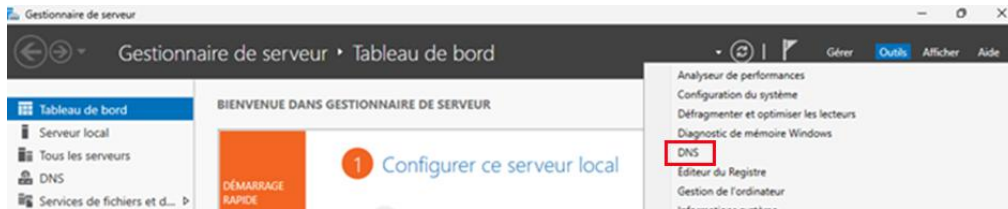


11. Après l'installation du service DNS, on peut constater qu'un répertoire DNS a été créé dans c:\windows\system32. Cela permet de vérifier que l'installation s'est bien déroulée, et ce répertoire va stocker les bases DNS tout comme le fichier cache qui répertorie les 13 serveurs root.

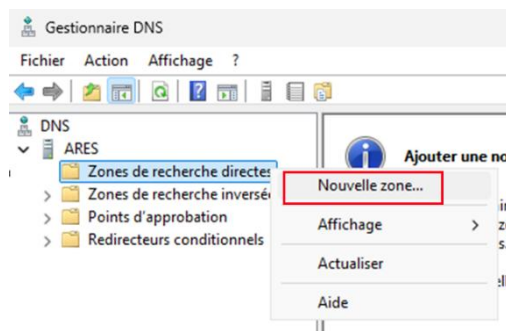


# Configuration

1. Pour configurer les zones de recherche du DNS, il faut se rendre dans Outils, et cliquer sur DNS.



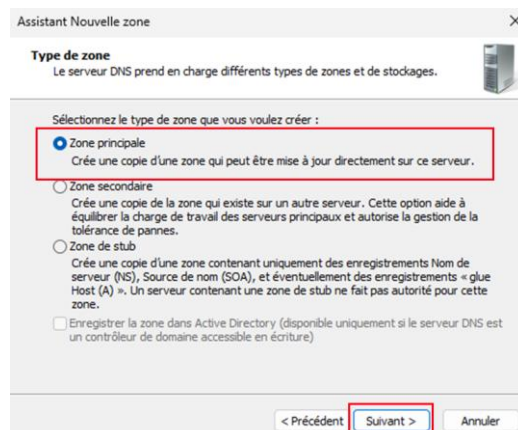
2. Faire un clic droit sur Zones de recherche directes, puis sur Nouvelle zones...



3. Une petite introduction sur le DNS apparaît, faire suivant.



4. Choisir en cochant Zone principale puis Suivant.



5. Mettre le nom « stadiumcompany.com » comme nom de la zone car c'est le domaine qu'on utilise.

Assistant Nouvelle zone

**Nom de la zone**  
Quel est le nom de la nouvelle zone ?

Le nom de la zone spécifie la partie de l'espace de noms DNS pour laquelle ce serveur fait autorité. Il peut s'agir du nom de domaine de votre société (par exemple, microsoft.com) ou d'une partie du nom de domaine (par exemple, nouvelle\_zone.microsoft.com). Le nom de zone n'est pas le nom du serveur DNS.

Nom de la zone :  
stadiumcompany.com

< Précédent Suivant > Annuler

6. « Créer un nouveau fichier nommé » sera rempli automatiquement avec comme ajout à la fin .dns, le cocher et cliquer sur Suivant.

Assistant Nouvelle zone

**Fichier zone**  
Vous pouvez créer un nouveau fichier de zone ou utiliser un fichier copié à partir d'un autre serveur DNS.

Voulez-vous créer un nouveau fichier de zone ou utiliser un fichier existant que vous avez copié à partir d'un autre serveur DNS ?

Créer un nouveau fichier nommé :  
stadiumcompany.com.dns

Utiliser un fichier existant :

Pour utiliser ce fichier existant, vérifiez qu'il a été copié dans le dossier %SystemRoot%\system32\dns sur ce serveur, puis cliquez sur Suivant.

< Précédent Suivant > Annuler

7. Il faut autoriser les mises à jour dynamique, puis faire Suivant.

Assistant Nouvelle zone

**Mise à niveau dynamique**  
Vous pouvez spécifier que cette zone DNS accepte les mises à jour sécurisées, non sécurisées ou non dynamiques.

Les mises à jour dynamiques permettent au client DNS d'enregistrer et de mettre à jour de manière dynamique leurs enregistrements de ressources avec un serveur DNS dès qu'une modification a lieu.  
Sélectionnez le type de mises à jour dynamiques que vous souhaitez autoriser :

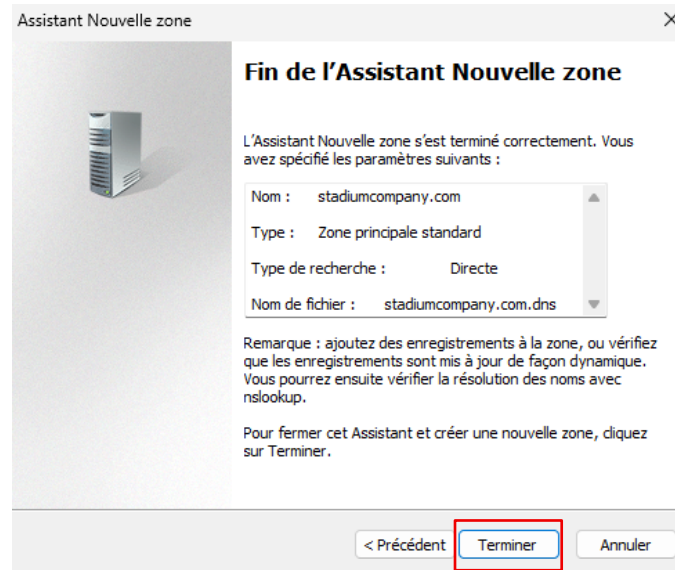
N'autoriser que les mises à jour dynamiques sécurisées (recommandé pour Active Directory)  
Cette option n'est disponible que pour les zones intégrées à Active Directory.

Autoriser à la fois les mises à jours dynamiques sécurisées et non sécurisées  
Les mises à jour dynamiques d'enregistrement de ressources sont acceptées à partir de n'importe quel client.  
**⚠ Cette option peut mettre en danger la sécurité de vos données car les mises à jour risquent d'être acceptées à partir d'une source non approuvée.**

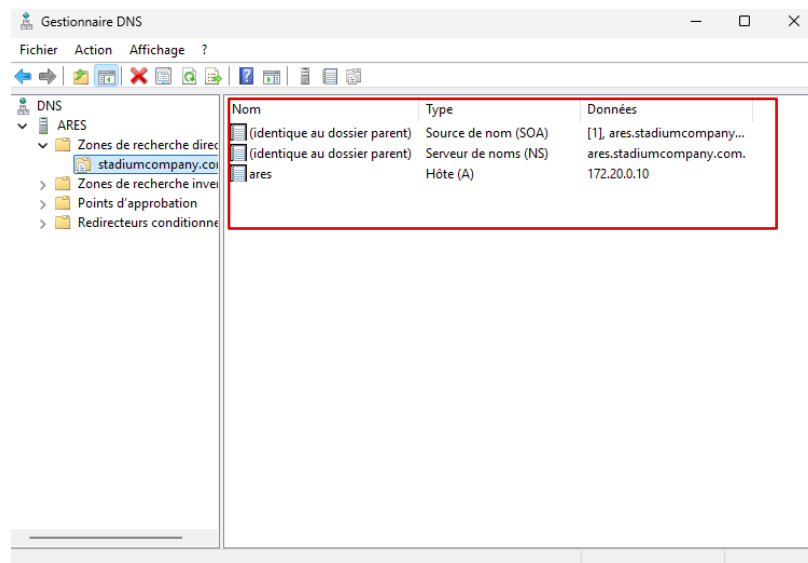
Ne pas autoriser les mises à jour dynamiques  
Les mises à jour dynamiques des enregistrements de ressources ne sont pas acceptées par cette zone. Vous devez mettre à jour ces enregistrements manuellement.

< Précédent Suivant > Annuler

8. Enfin, cliquer sur Terminer, la création de la nouvelle zone est réussie.

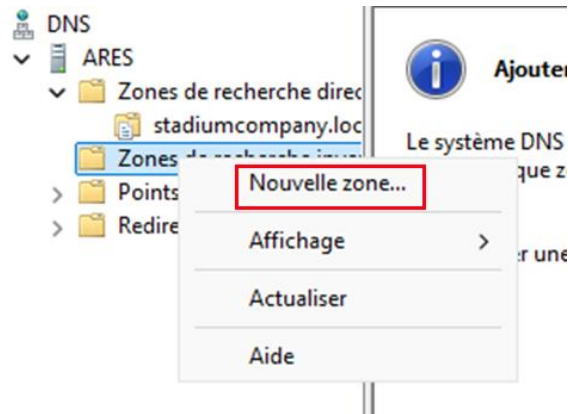


9. Cela développe une zone directe du nom de stadiumcompany.com avec 3 types d'enregistrements, SOA, NS et de type A.

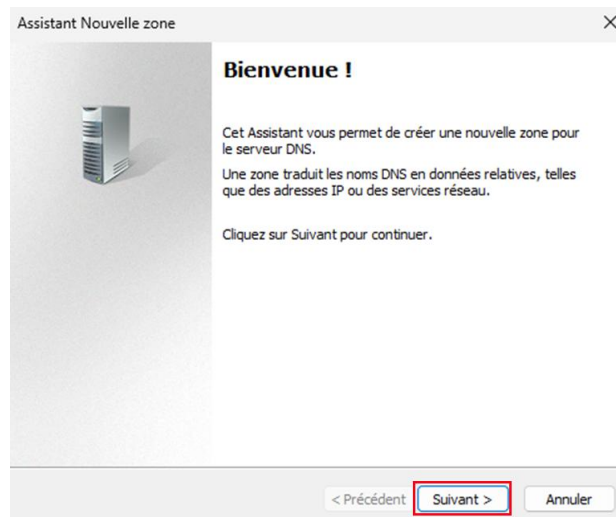


## Création de la zone de recherche inversé

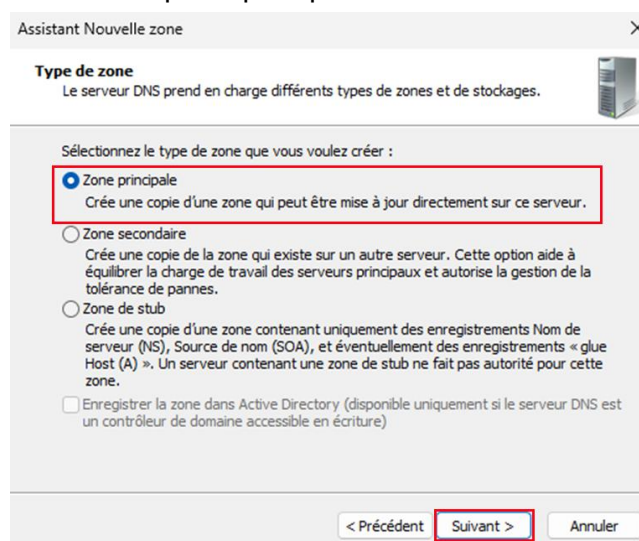
1. Faire un clic droit sur le dossier Zone de recherche inversé cette fois-ci, puis cliquer sur Nouvelle zone...



2. Une petite introduction sur le DNS apparaît, faire suivant.



3. Choisir en cochant Zone principale puis Suivant.



- Sélectionner la Zone de recherche inversée IPv4 puis faire Suivant.

Assistant Nouvelle zone

**Nom de la zone de recherche inversée**  
Une zone de recherche inversée traduit les adresses IP en noms DNS.

Choisissez si vous souhaitez créer une zone de recherche inversée pour les adresses IPv4 ou les adresses IPv6.

Zone de recherche inversée IPv4

Zone de recherche inversée IPv6

< Précédent **Suivant >** Annuler

- Puis choisir « L'ID Réseau » et rentrer notre ID réseau « 172.20.0. ». Cliquer sur Suivant une fois le champ rempli.

Assistant Nouvelle zone

**Nom de la zone de recherche inversée**  
Une zone de recherche inversée traduit les adresses IP en noms DNS.

Pour identifier la zone de recherche inversée, entrez l'ID réseau ou le nom de la zone.

ID réseau :

172.20.0.

L'ID réseau est la partie des adresses IP qui appartient à cette zone. Entrez l'ID réseau dans son ordre normal (non inversé).

Si vous utilisez un zéro dans l'ID réseau, il va apparaître dans le nom de la zone. Par exemple, l'ID réseau 10 crée la zone 10.in-addr.arpa, l'ID réseau 10.0 crée la zone 0.10.in-addr.arpa.

Nom de la zone de recherche inversée :

0.20.172.in-addr.arpa

< Précédent **Suivant >** Annuler

- Ici, c'est rempli automatiquement, on fait suivant

Assistant Nouvelle zone

**Fichier zone**  
Vous pouvez créer un nouveau fichier de zone ou utiliser un fichier copié à partir d'un autre serveur DNS.

Voulez-vous créer un nouveau fichier de zone ou utiliser un fichier existant que vous avez copié à partir d'un autre serveur DNS ?

Créer un nouveau fichier nommé :

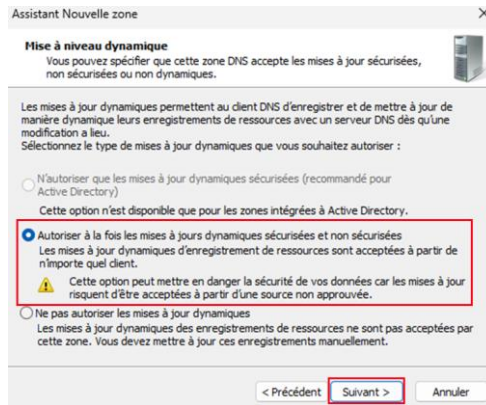
0.20.172.in-addr.arpa.dns

Utiliser un fichier existant :

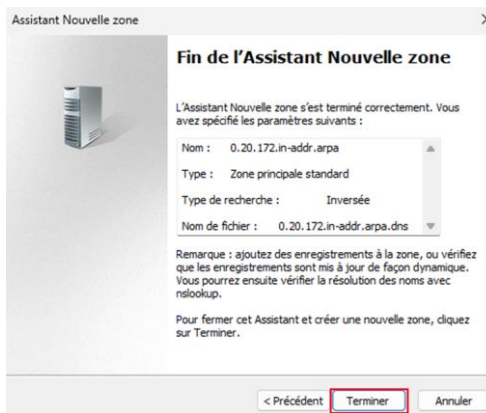
Pour utiliser ce fichier existant, vérifiez qu'il a été copié dans le dossier %SystemRoot%\system32\dns sur ce serveur, puis cliquez sur Suivant.

< Précédent **Suivant >** Annuler

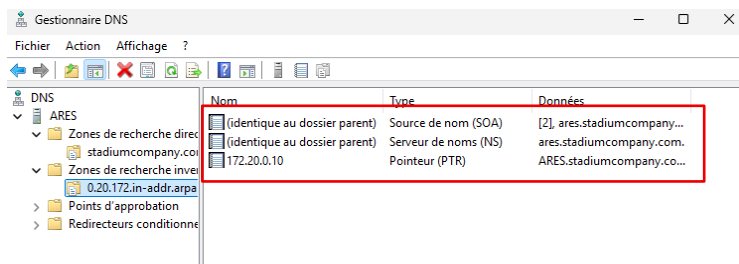
7. Il faut autoriser les mises à jour dynamique, puis faire Suivant.



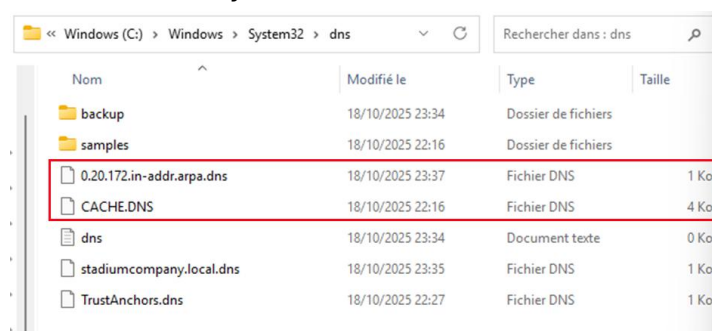
8. Enfin, cliquer sur Terminer, la création de la nouvelle zone est réussie.



9. Cela développe une zone inversée du nom de stadiumcompany.com avec 3 types d'enregistrements, SOA, NS et de type PTR.



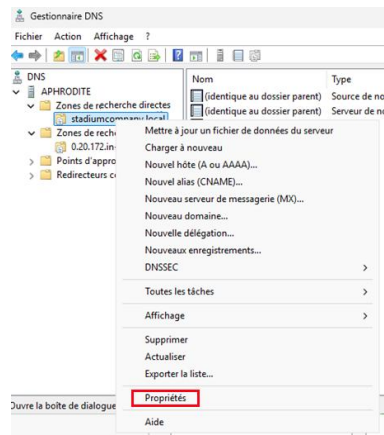
10. Il est possible de vérifier que les bases de données DNS ont bien été créées en se rendant dans c:\windows\system32.



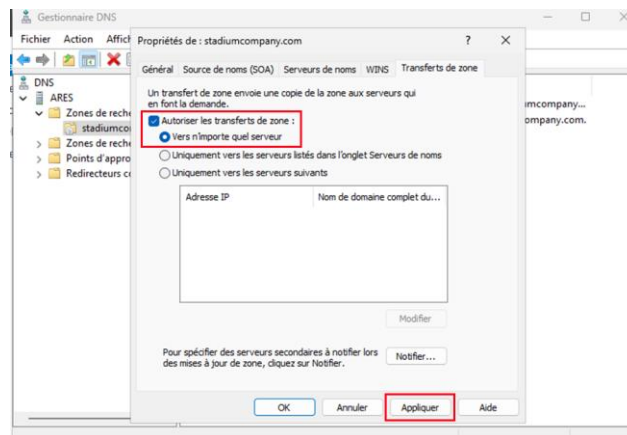
## Autorisation des transferts de zones

Dernière étape importante, l'autorisation des transferts de zones pour les zones directe et inversée sur le serveur maitre :

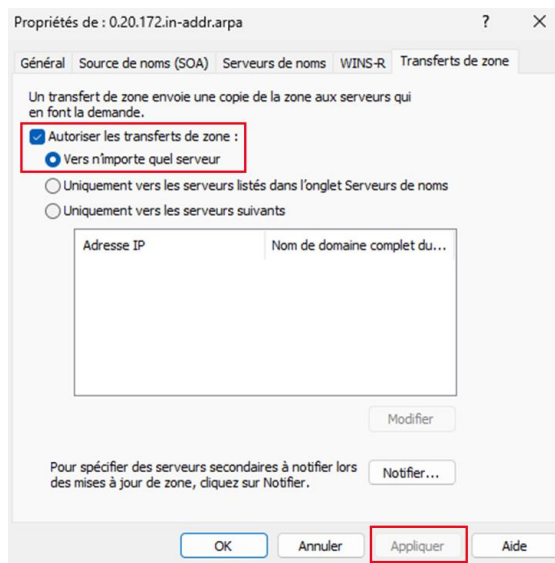
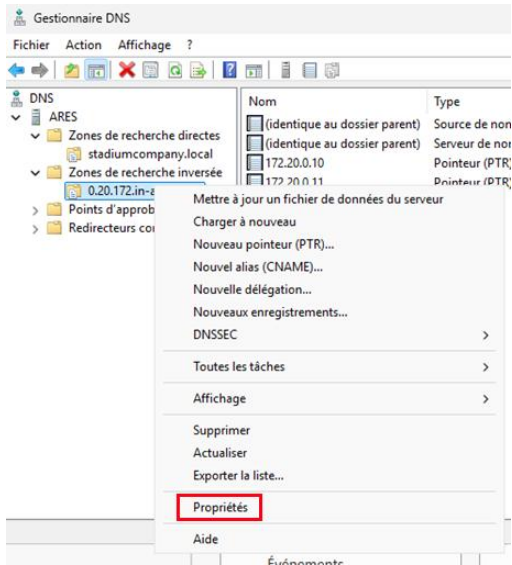
1. Depuis ARES, faire un clique droit sur notre dossier stadiumcompany.com, puis sur Propriétés.



2. Autoriser les Transfert de zone vers n'importe quel serveur, puis cliquer sur Appliquer.



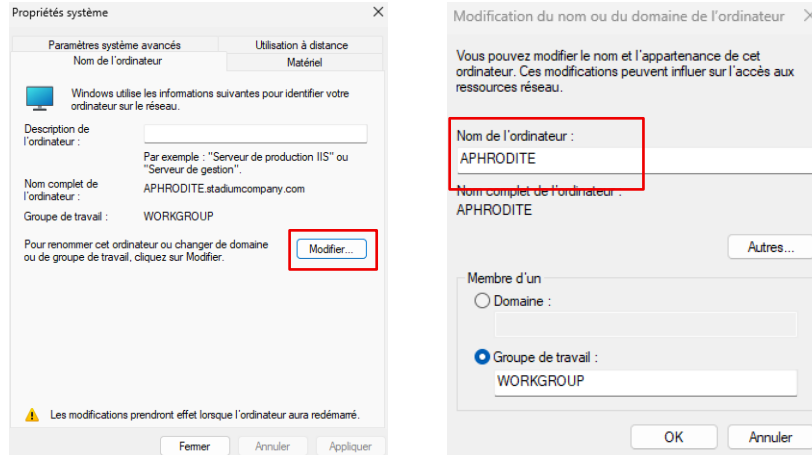
### 3. Répliquer la même chose avec le dossier 0.20.172.in-addr.arpa.



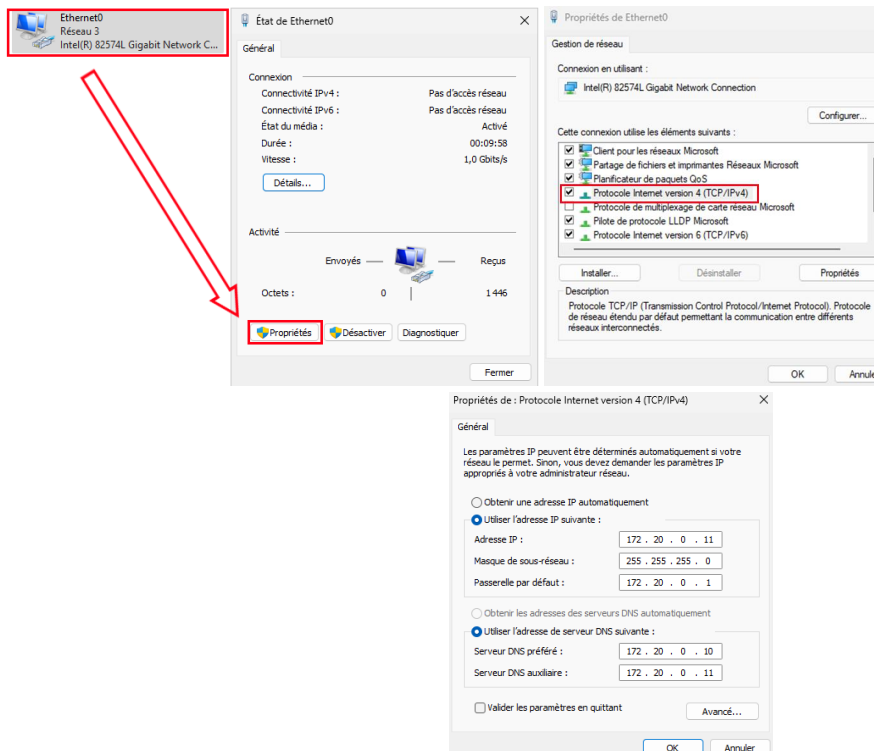
## Configuration DNS SECONDAIRE (APHRODITE) :

Premier préparatif (PREREQUIS) :

1. Il faut commencer par nommer notre machine APHRODITE dans les propriétés système en cliquant sur Modifier.

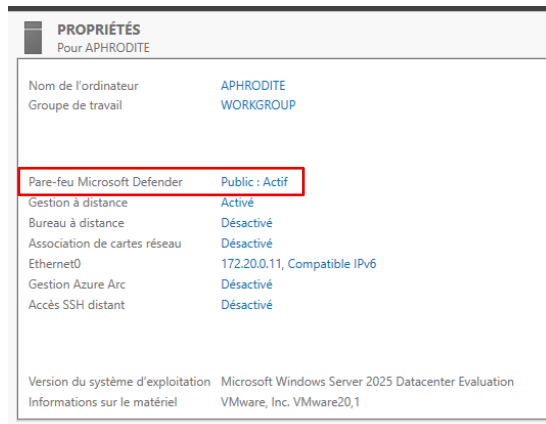


4. De plus, il faut rajouter une adresse IP statique sur notre machine accompagnée d'une passerelle par défaut et d'un serveur DNS préféré qui est celui du DNS Primaire (ARES). On a aussi déjà renseigné l'adresse du DNS Secondaire (APHRODITE) en DNS Auxiliaire. Pour se faire, il faut se rendre dans les propriétés de l'Ethernet0 et cliquer sur le protocole Internet Version 4 (IPv4).



# Désactivation du Pare-feu

1. On clique sur « Pare-feu » dans les propriétés d'APHRODITE.



## Pare-feu et protection du réseau

Qui et ce qui peut accéder à vos réseaux.

**Réseau avec domaine**  
Le pare-feu est activé.

**Réseau privé**  
Le pare-feu est activé.

**Réseau public (actif)**  
Le pare-feu est activé.

Autoriser une application via le pare-feu

Utilitaire de résolution des problèmes réseau et Internet

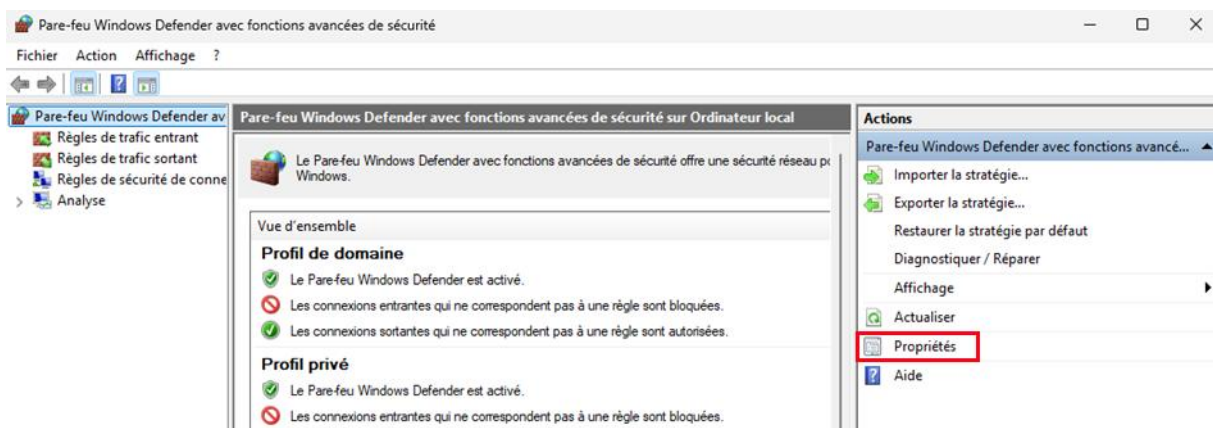
Paramètres de notification du pare-feu

**Paramètres avancés**

Restaurer les paramètres par défaut des pare-feux

2. Puis, on va dans les paramètres avancés.

3. Après cela, cliquer sur Pare-feu pour ensuite se rendre dans les propriétés.



- Enfin, il faut désactiver tous les pare-feux de Windows. Ayant fait cela sur les deux machines DNS, elles pourront alors interagir entre elles.

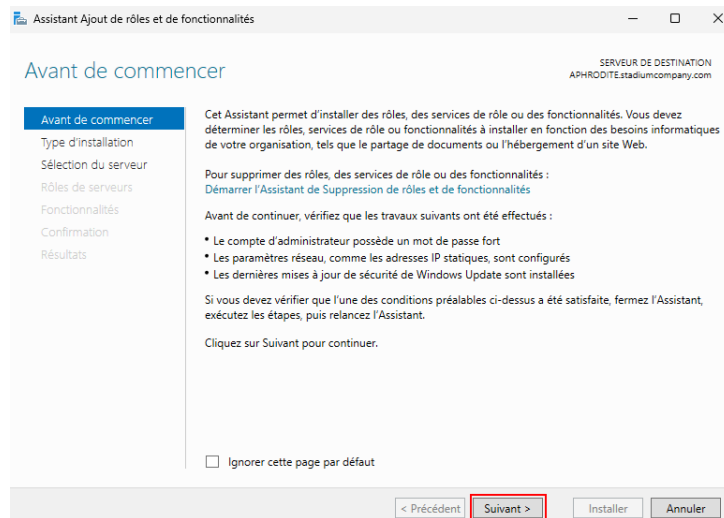


## Installation DNS Secondaire :

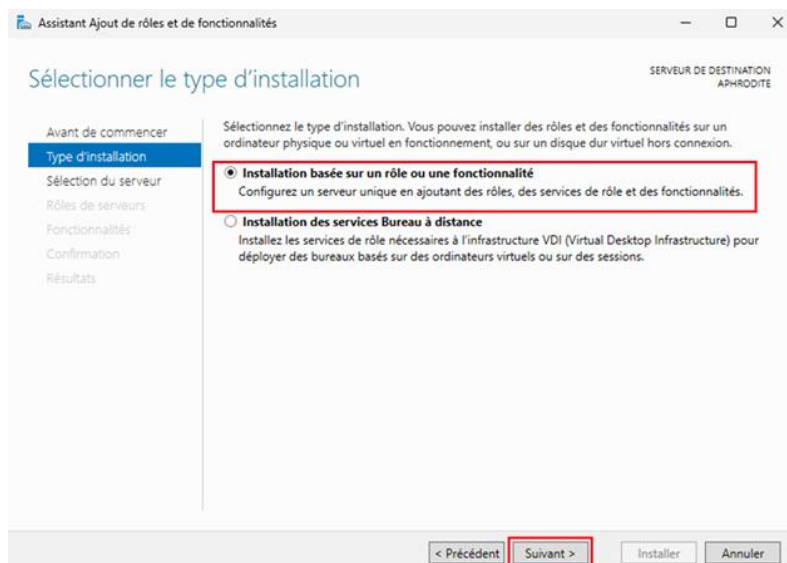
1. Dans le gestionnaire de serveur, cliquer sur Gérer puis Ajouter des rôles et fonctionnalités.



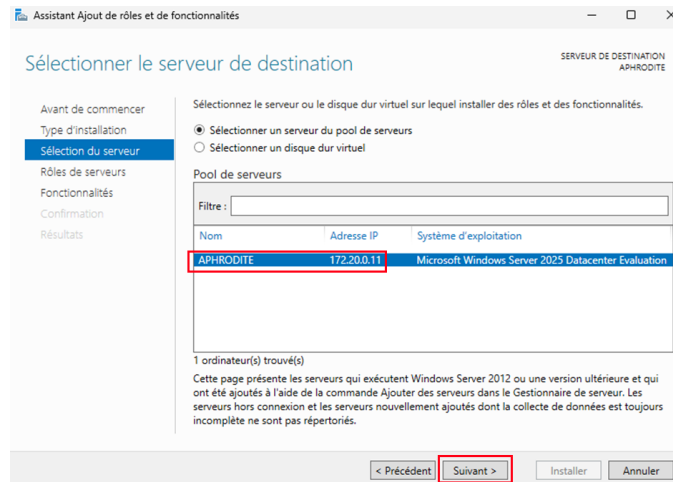
2. Sur l'assistant, il faut passer l'introduction avec « suivant ».



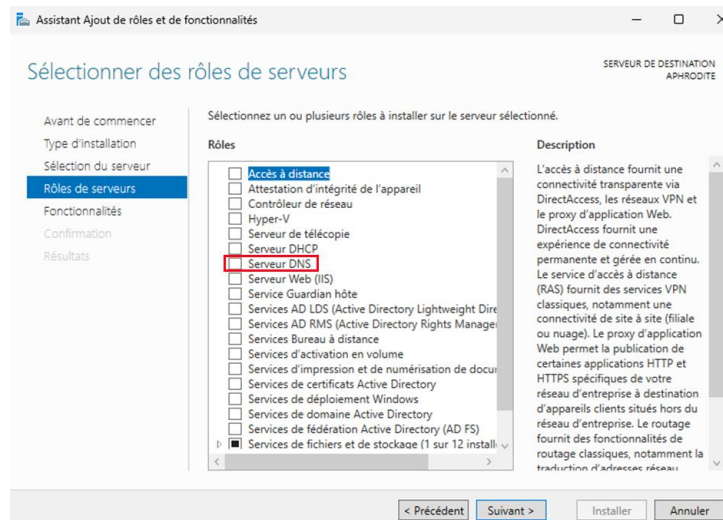
3. Ensuite, sélectionner « installation basée sur un rôle ou une fonctionnalité ».



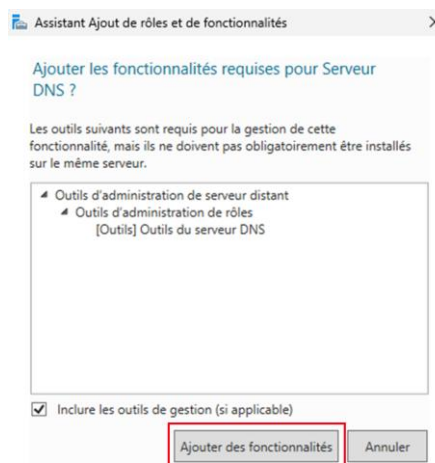
4. Puis sélectionner notre Serveur pool pour installer les rôles et cliquer sur suivant :



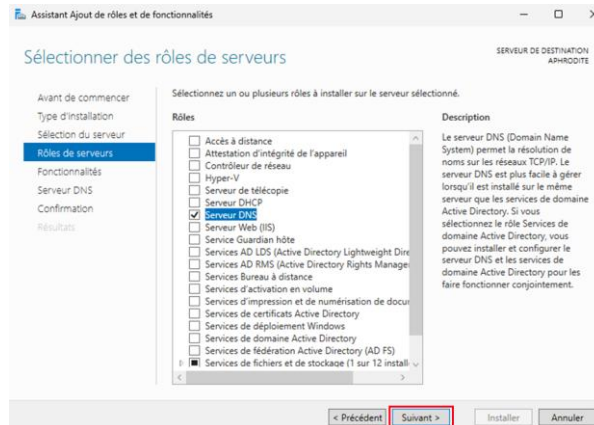
5. Ce qui nous intéresse est le DNS, donc on coche le Serveur DNS



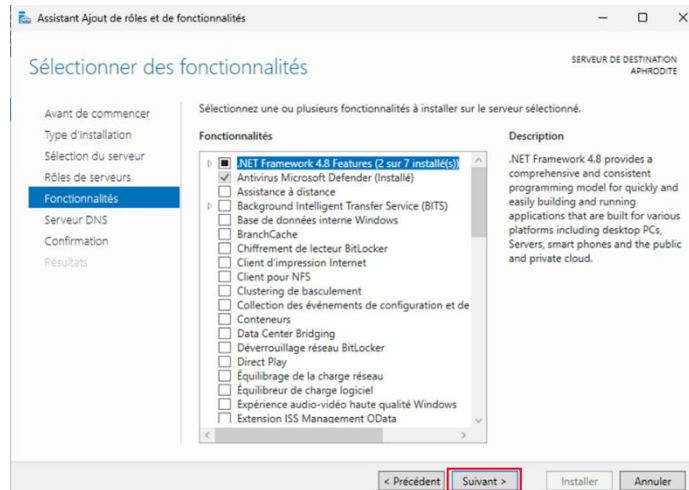
6. Il faut ajouter les fonctionnalités requises pour le Serveur DNS ainsi qu'inclure les outils de gestion.



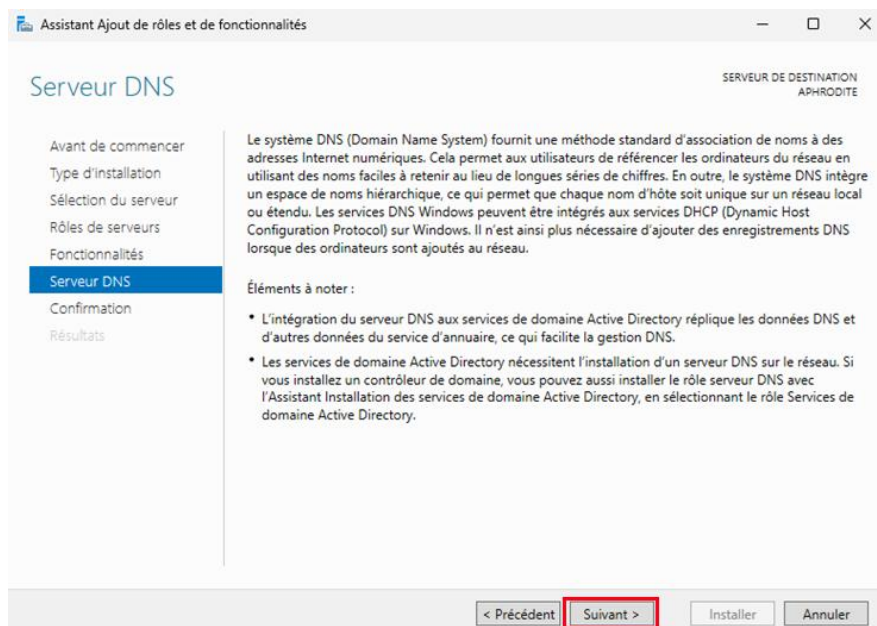
7. A la suite de cela, cliquer sur Suivant.



8. Cependant, il ne faut sélectionner aucune fonctionnalité à part le NET framework qui est déjà coché par défaut avec l'Antivirus. Puis cliquer sur Suivant.

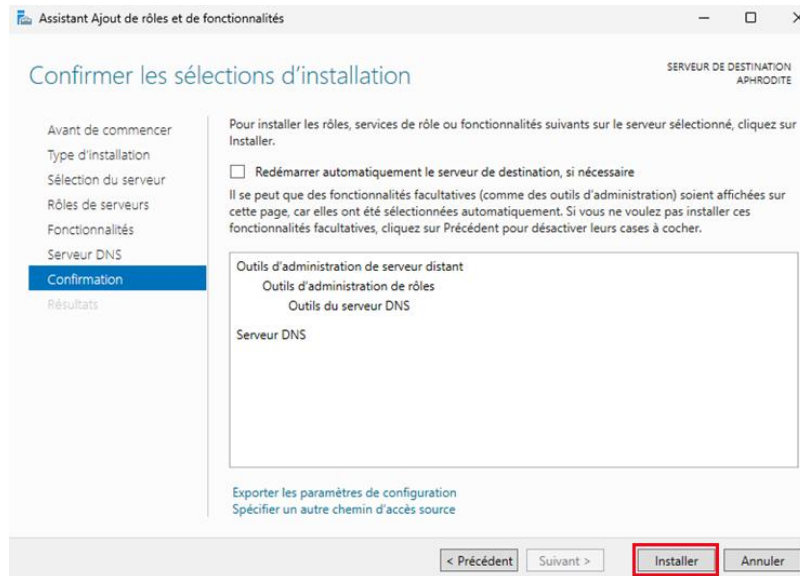


9. Passer les explications du DNS, puis faire Suivant.

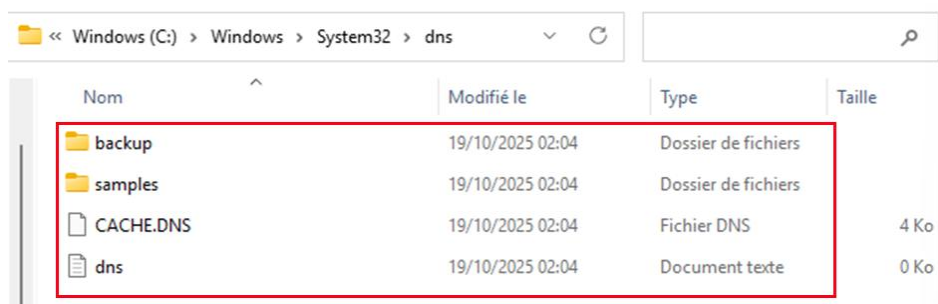


10. Enfin, confirmer l'installation en cliquant sur Installer.

Une fois l'installation terminée, fermer la fenêtre en cliquant sur Fermer qui apparaîtra à la place d'Installer.

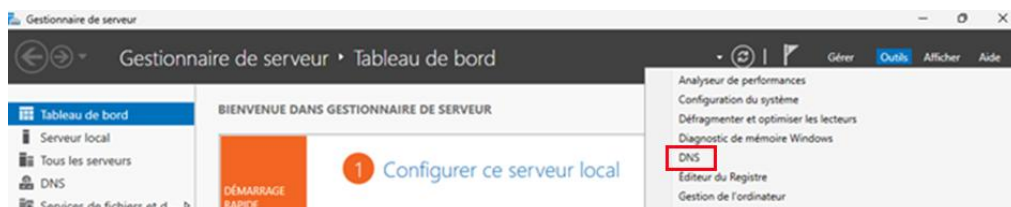


11. Après l'installation du service DNS, on peut constater qu'un répertoire DNS a été créé dans c:\windows\system32. Cela permet de vérifier que l'installation s'est bien déroulée, et ce répertoire va stocker les bases DNS tout comme le fichier cache qui répertorie les 13 serveurs root.

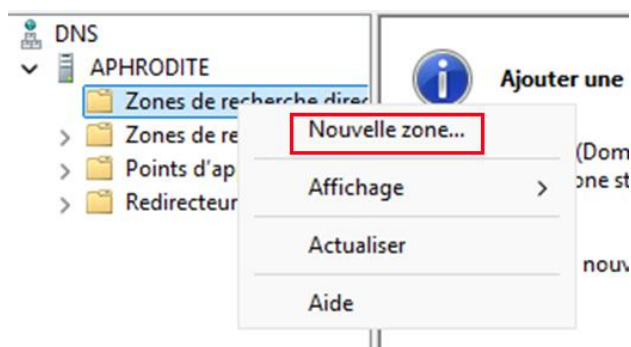


## Configuration :

1. Pour configurer les zones de recherche du DNS, il faut se rendre dans Outils, et cliquer sur DNS.



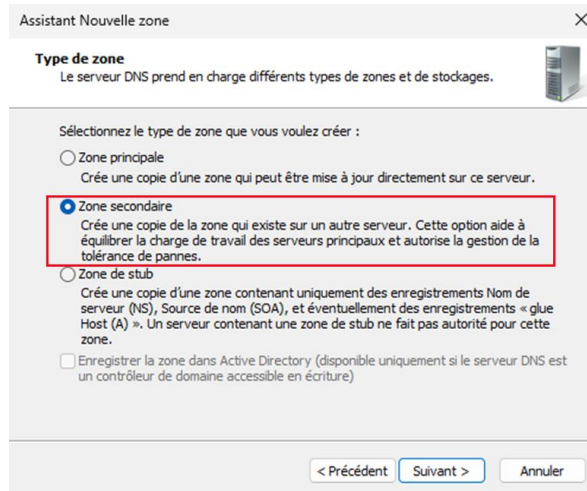
2. Faire un clic droit sur Zones de recherche directes, puis sur Nouvelle zones...



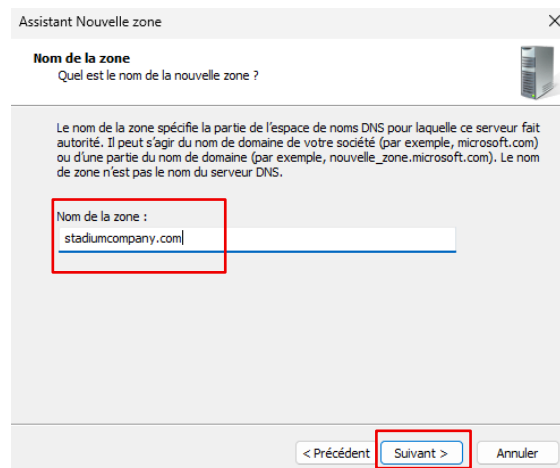
3. Une petite introduction sur le DNS apparaît, faire suivant.



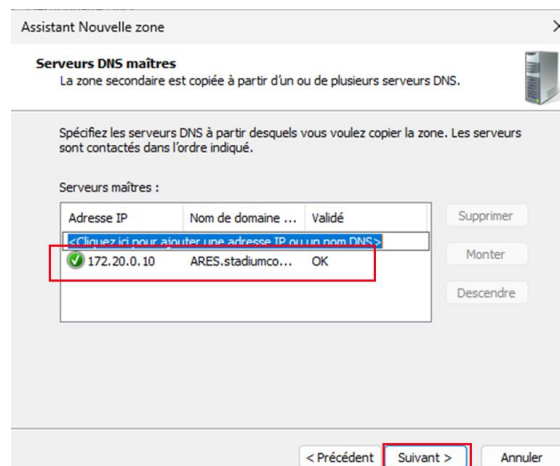
4. Choisir en cochant Zone secondaire puis Suivant. Etant donné que c'est notre DNS secondaire, on ne peut créer des zones principales.



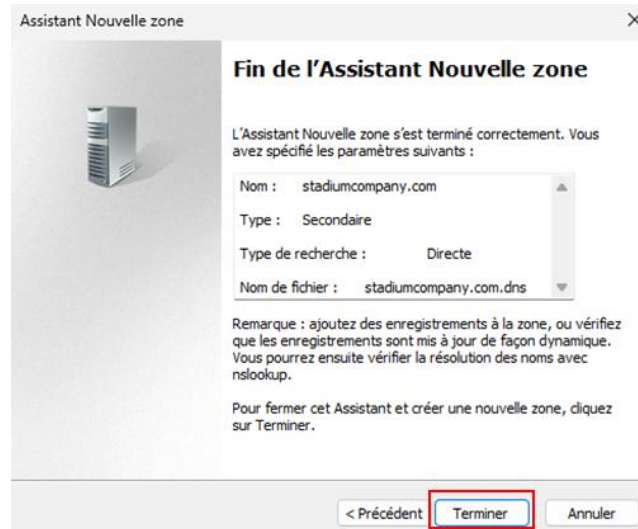
5. Mettre le nom « stadiumcompany.com » comme nom de la zone car c'est le domaine qu'on utilise.



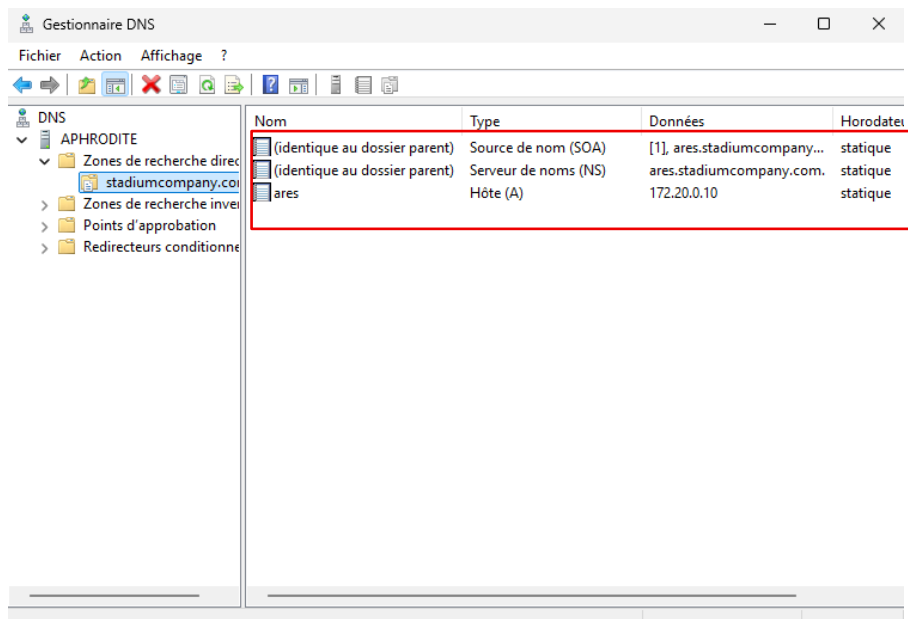
6. Pour trouver notre serveur maître qui est ARES, il faut mettre l'IP de notre DNS principal qui est « 172.20.0.10 » et une fois validé, il recherchera notre DNS principal pour s'y connecter. On peut aussi renseigner le nom de domaine.



7. Enfin, cliquer sur Terminer, la création de la nouvelle zone est réussie.

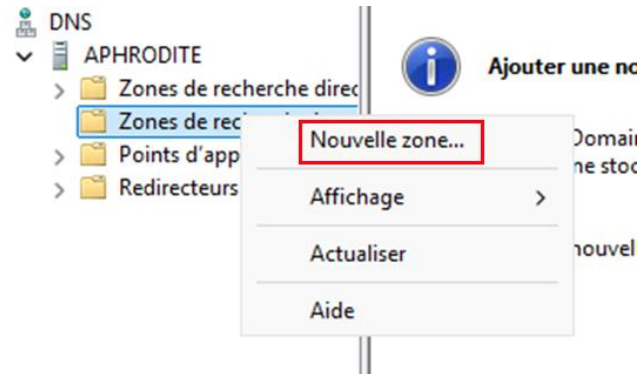


8. Cela développe une zone directe du nom de stadiumcompany.com avec 3 types d'enregistrements, SOA, NS et de type A provenant d'ARES.



## Création de la zone de recherche inversé

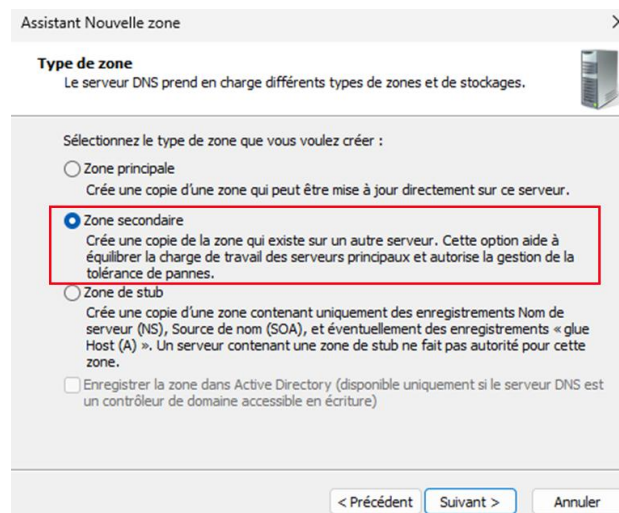
1. Faire un clique droit sur Zones de recherche inversées, puis sur Nouvelle zones...



2. Petite introduction de la création de zone, on fait suivant.



3. Choisir en cochant Zone secondaire puis Suivant.



- Sélectionner la Zone de recherche inversée IPv4 puis faire Suivant.

Assistant Nouvelle zone

**Nom de la zone de recherche inversée**  
Une zone de recherche inversée traduit les adresses IP en noms DNS.

Choisissez si vous souhaitez créer une zone de recherche inversée pour les adresses IPv4 ou les adresses IPv6.

Zone de recherche inversée IPv4  
 Zone de recherche inversée IPv6

< Précédent **Suivant >** Annuler

- Puis choisir « L'ID Réseau » et rentrer notre ID réseau « 172.20.0. ». Cliquer sur Suivant une fois le champ rempli.

Assistant Nouvelle zone

**Nom de la zone de recherche inversée**  
Une zone de recherche inversée traduit les adresses IP en noms DNS.

Pour identifier la zone de recherche inversée, entrez l'ID réseau ou le nom de la zone.

ID réseau :  
172 .20 .0 .

L'ID réseau est la partie des adresses IP qui appartient à cette zone. Entrez l'ID réseau dans son ordre normal (non inversé).

Si vous utilisez un zéro dans l'ID réseau, il va apparaître dans le nom de la zone. Par exemple, l'ID réseau 10 crée la zone 10.in-addr.arpa, l'ID réseau 10.0 crée la zone 0.10.in-addr.arpa.

Nom de la zone de recherche inversée :  
0.20.172.in-addr.arpa

< Précédent **Suivant >** Annuler

- Pour trouver notre serveur maître qui est ARES, il faut mettre l'IP de notre DNS principal qui est « 172.20.0.10 » et une fois validé, il recherchera notre DNS principal pour s'y connecter. On peut aussi renseigner le nom de domaine.

Assistant Nouvelle zone

**Serveurs DNS maîtres**  
La zone secondaire est copiée à partir d'un ou de plusieurs serveurs DNS.

Spécifiez les serveurs DNS à partir desquels vous voulez copier la zone. Les serveurs sont contactés dans l'ordre indiqué.

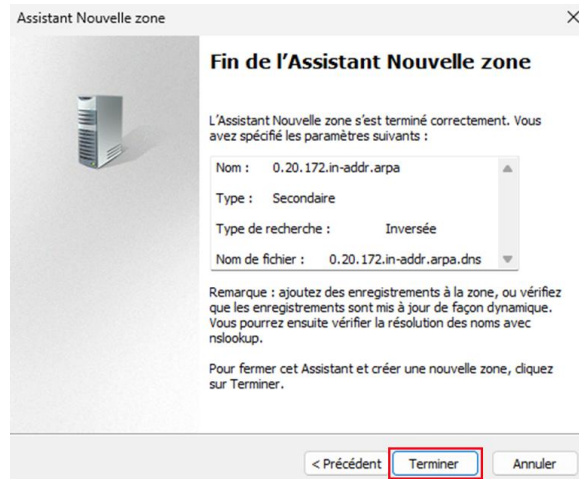
Serveurs maîtres :

Adresse IP	Nom de domaine ...	Validé
<a href="#">&lt; Cliquez ici pour ajouter une adresse IP ou un nom DNS &gt;</a>		
172.20.0.10	ARES.stadiumco...	OK

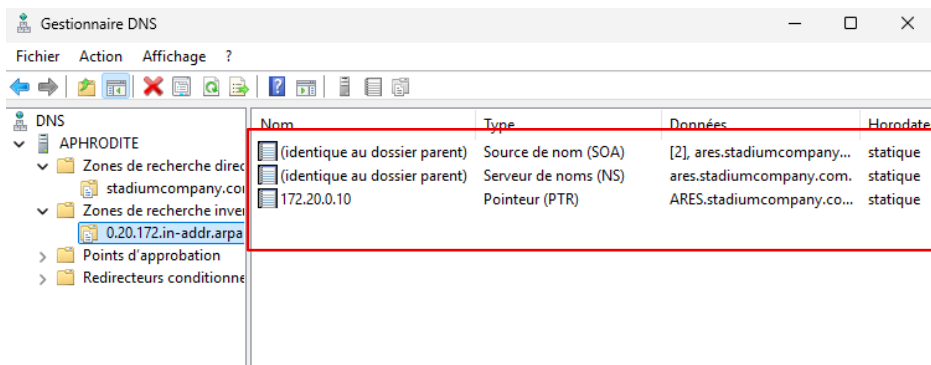
Supprimer  
Monter  
Descendre

< Précédent **Suivant >** Annuler

7. Enfin, cliquer sur Terminer, la création de la nouvelle zone est réussie.



8. Cela développe une zone directe du nom de stadiumcompany.com avec 3 types d'enregistrements, SOA, NS et de type PTR provenant d'ARES. Ainsi, le transfert de zone du DNS primaire vers le DNS secondaire est bien fonctionnel.



# PARTIES 2 DHCP

## Installation du service DHCP

1. Pour commencer sur la machine, il faut mettre à jour et installer le service DHCP.  
Pour cela, il faut taper les 2 commandes suivantes concernant les mises à jour :

Apt update / Apt upgrade à la suite. La première commande permet de rechercher et de télécharger les mises à jour. La deuxième commande permet quant à elle de les installer une fois téléchargées.

Une fois cela fait, il faut taper la commande : Apt install isc-dhcp-server qui va installer le service DHCP.

```
Generating /etc/default/isc-dhcp-server...
Job for isc-dhcp-server.service failed because the control process exited with error code.
See "systemctl status isc-dhcp-server.service" and "journalctl -xeu isc-dhcp-server.service" for details.
invoke-rc.d: initscript isc-dhcp-server, action "start" failed.
* isc-dhcp-server.service - LSB: DHCP server
   Loaded: loaded (/etc/init.d/isc-dhcp-server; generated)
   Active: failed (Result: exit-code) since Wed 2025-10-15 08:44:44 CEST; 22ms ago
 Invocation: b085cf9e3a3c4ada8b632ddf5bbb79dd
   Docs: man:systemd-sysv-generator(8)
  Process: 1483 ExecStart=/etc/init.d/isc-dhcp-server start (code=exited, status=1/FAILURE)
 Mem peak: 2.4M
   CPU: 49ms

oct. 15 08:44:42 Kratos dhcpd[1495]: bugs on either our web page at www.isc.org or in the README file
oct. 15 08:44:42 Kratos dhcpd[1495]: before submitting a bug. These pages explain the proper
oct. 15 08:44:42 Kratos dhcpd[1495]: process and the information we find helpful for debugging.
oct. 15 08:44:42 Kratos dhcpd[1495]:
oct. 15 08:44:42 Kratos dhcpd[1495]: exiting.
oct. 15 08:44:44 Kratos isc-dhcp-server[1483]: Starting ISC DHCPv4 server: dhcpdcheck syslog for diagnostics. ... failed!
oct. 15 08:44:44 Kratos isc-dhcp-server[1483]: failed!
oct. 15 08:44:44 Kratos systemd[1]: isc-dhcp-server.service: Control process exited, code=exited, status=1/FAILURE
oct. 15 08:44:44 Kratos systemd[1]: isc-dhcp-server.service: Failed with result 'exit-code'.
oct. 15 08:44:44 Kratos systemd[1]: Failed to start isc-dhcp-server.service - LSB: DHCP server.
Paramétrage de isc-dhcp-common (4.4.3-P1-8) ...
```

Un message d'erreur apparaîtra une fois l'installation terminée, ceci est normal étant donné que le service DHCP n'est pas encore configuré.

## Configuration de l'IP du DHCP Primaire

1. Pour configurer l'adresse IP statique du Serveur DHCP Primaire, il faut taper la commande suivante : `nano /etc/network/interfaces`.

Ainsi, il faut mettre la seconde carte réseau ajouté ultérieurement sur la machine en 172.20.0.5/24.

```
GNU nano 8.4
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
allow-hotplug ens33
iface ens33 inet dhcp

# The secondary network interface
allow-hotplug ens37
iface ens37 inet static
address 172.20.0.5/24
```

2. Ensuite, pour que la carte réseau prenne la nouvelle configuration en compte, il faut la désactiver puis la réactiver à l'aide de ces commandes :

`Ifdown ens37` qui force la désactivation de la carte réseau.

`Ifup ens37` qui va forcer l'activation de la carte réseau.

Enfin, pour vérifier que cela ait fonctionné, on peut taper `ip a` qui permet de voir les interfaces réseaux de notre machine et là en occurrence, ce qui nous intéresse de vérifier les adressages IP respectives d'ens33 et ens37.

```
root@Kratos:~# ifdown ens37
ifdown: interface ens37 not configured
root@Kratos:~# ifup ens37
root@Kratos:~# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:5f:41:dc brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    altname enx00c295f41dc
    inet 192.168.44.145/24 brd 192.168.44.255 scope global dynamic noprefixroute ens33
        valid_lft 955sec preferred_lft 730sec
    inet6 fe80::1907:6a24:bc40:a30/64 scope link
        valid_lft forever preferred_lft forever
3: ens37: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:5f:41:e6 brd ff:ff:ff:ff:ff:ff
    altname enp2s5
    altname enx00c295f41e6
    inet 172.20.0.5/24 brd 172.20.0.255 scope global ens37
        valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fe5f:41e6/64 scope link proto kernel_ll
        valid_lft forever preferred_lft forever
root@Kratos:~# _
```

Ainsi, notre carte ens37 est bien avec l'IP statique 172.20.0.5/24. C'est par cette interface qu'on véhiculera le DHCP de notre réseau.

## Configuration du service DHCP

1. Une fois le service installé, avant chaque modification, il faut impérativement faire une copie de la configuration actuelle pour revenir en arrière en cas de besoin.

Pour se faire, on se rend dans le dossier qui comprend les fichiers de configuration du DHCP à l'aide de la commande : `cd /etc/dhcp`.

Puis on crée une copie du fichier de configuration avec cette commande : `cp dhcpd.conf dhcpd.conf.old`.

```
root@Kratos:~# cd /etc/dhcp
root@Kratos:/etc/dhcp# cp dhcpd.conf dhcpd.conf.old
root@Kratos:/etc/dhcp# ls -l
total 12
-rw-r--r-- 1 root root 3331  3 mai  19:16 dhcpd6.conf
-rw-r--r-- 1 root root 3496  3 mai  19:16 dhcpd.conf
-rw-r--r-- 1 root root 3496 15 oct.  13:06 dhcpd.conf.old
root@Kratos:/etc/dhcp#
```

Désormais, en tapant `ls -l`, on peut vérifier et on a bien le fichier en `.conf` et le fichier en `.conf.old`.

2. Maintenant, il faut configurer l'interface de sortie du service DHCP avec la commande : `nano /etc/default/isc-dhcp-server`.

Puis décommenter la ligne `DHCPDv4_CONF`, c'est-à-dire supprimer le `#`.

Enfin, indiquer la carte réseau `ens37` sur `INTERFACESv4=ens37`.

```
# Defaults for isc-dhcp-server (sourced by /etc/init.d/isc-dhcp-server)

# Path to dhcpd's config file (default: /etc/dhcp/dhcpd.conf).
DHCPDv4_CONF=/etc/dhcp/dhcpd.conf
#DHCPDv6_CONF=/etc/dhcp/dhcpd6.conf

# Path to dhcpd's PID file (default: /var/run/dhcpd.pid).
#DHCPDv4_PID=/var/run/dhcpd.pid
#DHCPDv6_PID=/var/run/dhcpd6.pid

# Additional options to start dhcpd with.
# Don't use options -cf or -pf here; use DHCPD_CONF/ DHCPD_PID instead
#OPTIONS=""

# On what interfaces should the DHCP server (dhcpd) serve DHCP requests?
# Separate multiple interfaces with spaces, e.g. "eth0 eth1".
INTERFACESv4="ens37"
INTERFACESv6=""
```

3. On configure notre DHCP en se basant sur ce schéma qui met en place la configuration du failover sur le DHCP Principal.

```
Authoritative;
failover peer "failover-partner" {      #Nom du dhcp failover
primary;                                #On dit qu'il est principal (Master)
address 172.20.0.5;                      #Adresse du serveur Master
port 519;                                # Port d'écoute du serveur Master
peer address 172.20.0.6;                 # Adresse du serveur Slave
peer port 520;                           # Port d'écoute du serveur Slave

max-response-delay 60;                  # Temps en seconde, s'il ne répond pas, on le considère down
max-unacked-updates 10;                 #Autorisez jusqu'à 10 mises à jour de liaison non reconnues
mclt 3600;                               #Durée de bail maximale en secondes autorisée sans contact avec le partenaire
split 128;                               #Un équilibrage de charge à 50 %/50 %
load balance max seconds 3; #Servir les demandes des clients d'autres serveurs si la valeur de l'en-tête
DHCP "SECS" est supérieure à 3
}

# Paramétrage de la configuration à distribuer aux postes clients
subnet 172.20.0.0 netmask 255.255.255.0 {
pool{
failover peer "failover-partner";       # Indique la configuration du failover
option routers 172.20.0.1;              # Passerelle par défaut
option domain-name-servers 8.8.8.8 ;   # Serveur DNS
range 172.20.0.100 172.20.0.200;       # Plage d'adresses IP
default-lease-time 21600 ;              # Bail de 6 heures par défaut
max-lease-time 36000 ;                  # Bail pouvant aller jusqu'à 10 heures
}
}
```

```
#dhcpd.conf kratos1
authoritative;

#Configuration du fail over
failover peer "failover-partner" {
primary;
address 172.20.0.5;
port 519;
peer address 172.20.0.6;
peer port 520;

max-response-delay 60;
max-unacked-updates 10;
mclt 3600;
split 128;
load balance max seconds 3;
}

#Configuration de la plage ip
subnet 172.20.0.0 netmask 255.255.255.0 {
pool{
failover peer "failover-partner";
option routers 172.20.0.1;
range 172.20.0.100 172.20.0.200;
option domain-name-servers 172.20.0.10, 172.20.0.11;
option subnet-mask 255.255.255.0;
default-lease-time 21600;
max-lease-time 36000;
}
}
```

4. A la suite de cela, il faut tester la validité du dhcpd.conf avec la commande :  
dhcpd -t.

```
root@Kratos1:~# dhcpd -t
Internet Systems Consortium DHCP Server 4.4.3-P1
Copyright 2004-2022 Internet Systems Consortium.
All rights reserved.
For info, please visit https://www.isc.org/software/dhcp/
Config file: /etc/dhcp/dhcpd.conf
Database file: /var/lib/dhcp/dhcpd.leases
PID file: /var/run/dhcpd.pid
root@Kratos1:~# _
```

Tout semble correct.

5. Désormais, il faut redémarrer le service DHCP à l'aide de la commande :  
systemctl restart isc-dhcp-server.

Puis systemctl status isc-dhcp-server : **Active: active (running)**

On peut observer que le service est bien actif.

## Clonage + Configuration Kratos 2

1. Maintenant, il est possible de cloner la machine Kratos 1 pour créer Kratos 2. Tout d'abord, il faut modifier le hostname pour s'organiser, avec la commande :  
Nano /etc/hostname.

2. A la suite de cela, il faut modifier l'adresse IP de la carte réseau ens37 en mettant : 172.20.0.6/24.

```
GNU nano 8.4
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
allow-hotplug ens33
iface ens33 inet dhcp

# The secondary network interface
allow-hotplug ens37
iface ens37 inet static
address 172.20.0.6/24

gateway 172.20.0.1
```

6. Ensuite, comme sur Kratos 1, il faut la désactiver puis la réactiver à l'aide de ces commandes :

ifdown ens37 qui force la désactivation de la carte réseau.

ifup ens37 qui va forcer l'activation de la carte réseau.

Enfin, pour vérifier que cela ait fonctionné, on peut taper ip a.

```
3: ens37: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_code
link/ether 00:0c:29:58:5e:f1 brd ff:ff:ff:ff:ff:ff
altname enp2s5
altname enx000c29585ef1
inet 172.20.0.6/24 brd 172.20.0.255 scope global ens37
    valid_lft forever preferred_lft forever
inet6 fe80::20c:29ff:fe58:5ef1/64 scope link proto kernel_ll
    valid_lft forever preferred_lft forever
root@Kratos2:~# ping 172.20.0.5
PING 172.20.0.5 (172.20.0.5) 56(84) bytes of data.
64 bytes from 172.20.0.5: icmp_seq=1 ttl=64 time=0.883 ms
64 bytes from 172.20.0.5: icmp_seq=2 ttl=64 time=1.29 ms
64 bytes from 172.20.0.5: icmp_seq=3 ttl=64 time=0.524 ms
^C
--- 172.20.0.5 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2027ms
rtt min/avg/max/mdev = 0.524/0.897/1.286/0.311 ms
root@Kratos2:~# _
```

Dans le même temps, il faut vérifier que Kratos2 ping bien l'IP de Kratos1.

7. On configure notre DHCP en se basant sur ce schéma qui met en place la configuration du failover secondaire.

```
Authoritative;
failover peer "failover-partner" {          #Nom du dhcp failover
secondary;                                #On dit qu'il est secondaire (Slave)
address 172.20.0.6;                        #Adresse du serveur Slave
port 520;                                  # Port d'écoute du serveur Slave
peer address 172.20.0.5;                   # Adresse du serveur Master
peer port 519;                             # Port d'écoute du serveur Master
max-response-delay 60; # Temps en seconde, s'il ne répond pas, on le considère down
max-unacked-updates 10;    #Autorisez jusqu'à 10 mises à jour de liaison non reconnues
load balance max seconds 3; #Servir les demandes des clients d'autres serveurs si la valeur de l'en-tête
DHCP "SECS" est supérieure à 3
}

# Paramétrage de la configuration à distribuer aux postes clients
subnet 172.20.0.0 netmask 255.255.255.0 {
pool{
failover peer "failover-partner";          # Indique la configuration du failover
option routers 172.20.0.1;                # Passerelle par défaut
option domain-name-servers 8.8.8.8;      # Serveur DNS
range 172.20.0.100 172.20.0.199;         # Plage d'adresses IP
default-lease-time 21600;                 # Bail de 6 heures par défaut
max-lease-time 36000;                     # Bail pouvant aller jusqu'à 10 heures
}
}
}
```

```
# dhcpd.conf kratos2
authoritative;

#configuration du fail over
failover peer "failover-partner" {
secondary;
address 172.20.0.6;
port 520;
peer address 172.20.0.5;
peer port 519;

max-response-delay 60;
max-unacked-updates 10;
mclt 3600;
load balance max seconds 3;
}

#Configuration de la plage ip
subnet 172.20.0.0 netmask 255.255.255.0 {
pool{
failover peer "failover-partner";
range 172.20.0.100 172.20.0.200;
option domain-name-servers 172.20.0.10, 172.20.0.11;
option subnet-mask 255.255.255.0;
option routers 172.20.0.1;
default-lease-time 21600;
max-lease-time 36000;
}
}
}
```

8. Là aussi, il faut redémarrer le service DHCP à l'aide de la commande :  
systemctl restart isc-dhcp-server.  
Puis systemctl status isc-dhcp-server.

```
root@Kratos2:~# systemctl status isc-dhcp-server
● isc-dhcp-server.service - LSB: DHCP server
   Loaded: loaded (/etc/init.d/isc-dhcp-server; generated)
   Active: active (running) since Sat 2025-10-18 21:05:46 CEST; 1min 7s ago
  Invocation: 294650668c9c4493a07fe38cc019f917
     Docs: man:systemd-sysv-generator(8)
  Process: 1299 ExecStart=/etc/init.d/isc-dhcp-server start (code=exited, status=0/SUCCESS)
     Tasks: 1 (limit: 4595)
    Memory: 5.1M (peak: 6.6M)
       CPU: 70ms
    CGroup: /system.slice/isc-dhcp-server.service
           └─1311 /usr/sbin/dhcpd -4 -q -cf /etc/dhcp/dhcpd.conf ens37

oct. 18 21:05:44 Kratos2 dhcpd[1311]: failover peer failover-partner: I move from recover to recover-done
oct. 18 21:05:44 Kratos2 dhcpd[1311]: failover peer failover-partner: peer moves from recover-done to normal
oct. 18 21:05:44 Kratos2 dhcpd[1311]: failover peer failover-partner: I move from recover-done to normal
oct. 18 21:05:44 Kratos2 dhcpd[1311]: failover peer failover-partner: Both servers normal
oct. 18 21:05:44 Kratos2 dhcpd[1311]: balancing pool 55db60df06b0 172.20.0.0/24 total 101 free 99 backup 0 lts -49 max-own (+/-)10
oct. 18 21:05:44 Kratos2 dhcpd[1311]: balanced pool 55db60df06b0 172.20.0.0/24 total 101 free 99 backup 0 lts -49 max-misbal 15
oct. 18 21:05:46 Kratos2 isc-dhcp-server[1299]: Starting ISC DHCPv4 server: dhcpd.
oct. 18 21:05:46 Kratos2 systemd[1]: Started isc-dhcp-server.service - LSB: DHCP server.
oct. 18 21:06:47 Kratos2 dhcpd[1311]: balancing pool 55db60df06b0 172.20.0.0/24 total 101 free 50 backup 49 lts 0 max-own (+/-)10
oct. 18 21:06:47 Kratos2 dhcpd[1311]: balanced pool 55db60df06b0 172.20.0.0/24 total 101 free 50 backup 49 lts 0 max-misbal 15
root@Kratos2:~#
```

On peut observer que le service est bien actif.

## Vérification

1. Pour vérifier que toute la configuration a bien été faite, on commence avec le fait qu'il n'y ait aucun DHCP allumé :

Après cela, sur une machine Windows Client, taper `ipconfig /release` pour ne plus avoir d'IP.

Puis `ipconfig /renew` pour redemander une IP à mon service DHCP.

```
C:\Users\home>ipconfig

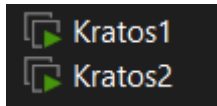
Configuration IP de Windows

Carte Ethernet Ethernet0 :

    Suffixe DNS propre à la connexion. . . . :
    Adresse IPv6 de liaison locale. . . . . : fe80::f827:7369:3727:841a%7
    Adresse d'autoconfiguration IPv4 . . . . : 169.254.136.250
    Masque de sous-réseau. . . . . : 255.255.0.0
    Passerelle par défaut. . . . . :
```

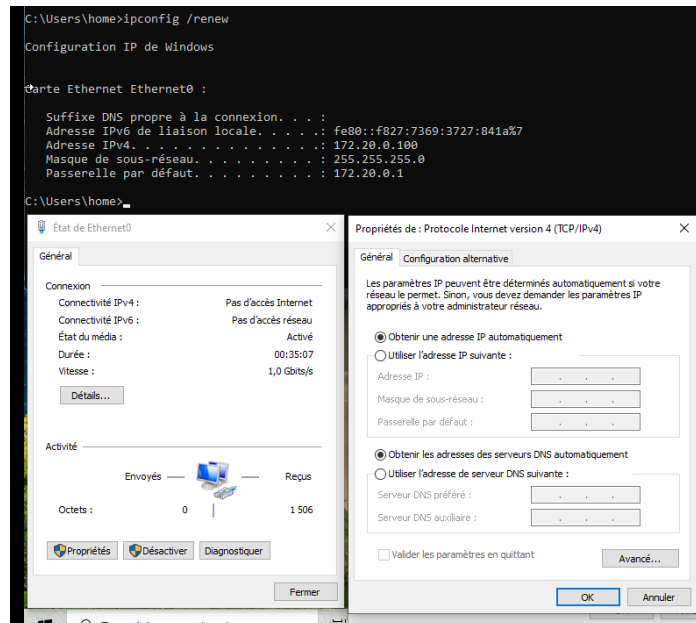
Une IP en 169.254 apparaît, ce qui est normal puisque le DHCP est hors ligne.

2. Maintenant, avec les deux DHCP allumés :



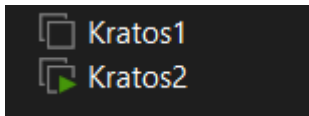
3. On fait la même chose qu'au-dessus, en se rendant sur une machine Windows Client, taper `ipconfig /release` pour ne plus avoir d'IP.

Puis `ipconfig /renew` pour redemander une IP à mon service DHCP.



Une IP en 172.20.0.100 apparaît, correspond à l'IP que le DHCP primaire a donné.

4. Eteindre le DHCP primaire et laisser le DHCP secondaire actif :



On fait la même chose qu'au-dessus, en se rendant sur une machine Windows Client, taper ipconfig /release pour ne plus avoir d'IP.

Puis ipconfig /renew pour redemander une IP à mon service DHCP.

```
C:\Users\home>ipconfig /renew

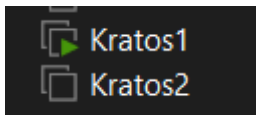
Configuration IP de Windows

Carte Ethernet Ethernet0 :

    Suffixe DNS propre à la connexion. . . . :
    Adresse IPv6 de liaison locale. . . . . : fe80::f827:7369:3727:841a%7
    Adresse IPv4. . . . . : 172.20.0.100
    Masque de sous-réseau. . . . . : 255.255.255.0
    Passerelle par défaut. . . . . : 172.20.0.1
```

Une IP en 172.20.0.100 apparaît, on constate que c'est la même que celle qu'a octroyé le DHCP primaire malgré qu'il soit éteint.

5. Eteindre le DHCP secondaire et laisser le DHCP primaire actif :



On fait la même chose qu'au-dessus, en se rendant sur une machine Windows Client, taper ipconfig /release pour ne plus avoir d'IP.

Puis ipconfig /renew pour redemander une IP à mon service DHCP.

```
C:\Users\home>ipconfig /renew

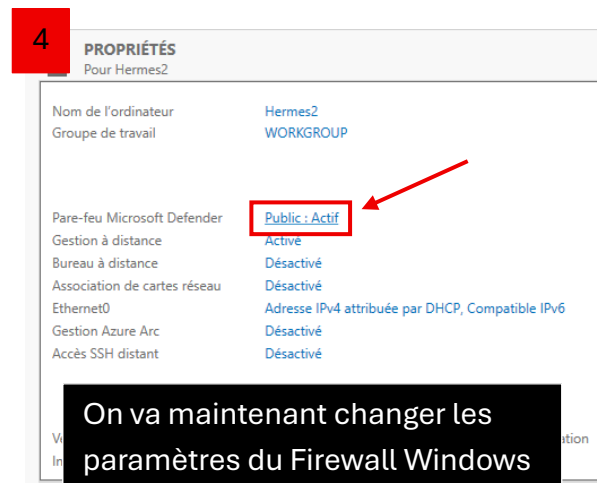
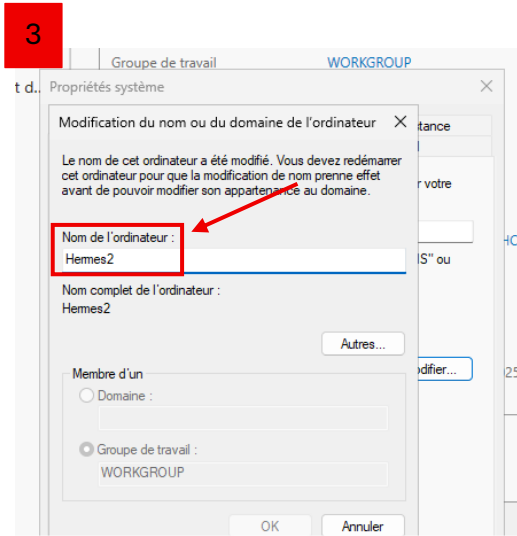
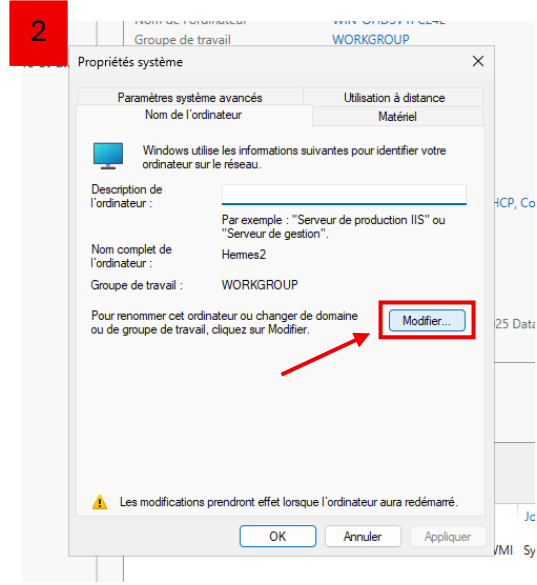
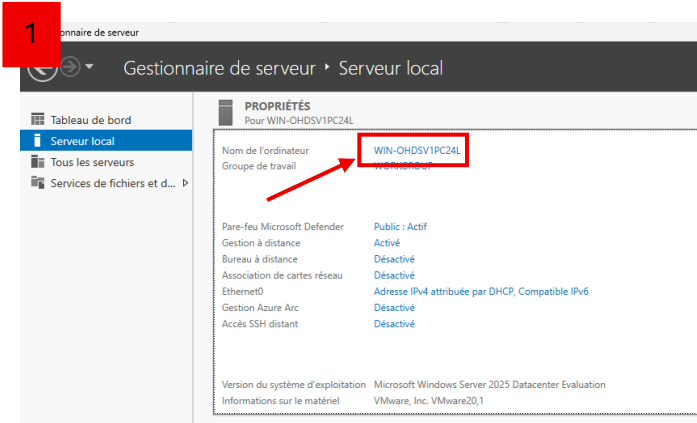
Configuration IP de Windows

Carte Ethernet Ethernet0 :

    Suffixe DNS propre à la connexion. . . . :
    Adresse IPv6 de liaison locale. . . . . : fe80::f827:7369:3727:841a%7
    Adresse IPv4. . . . . : 172.20.0.100
    Masque de sous-réseau. . . . . : 255.255.255.0
    Passerelle par défaut. . . . . : 172.20.0.1
```

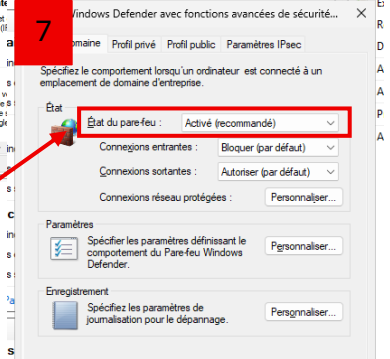
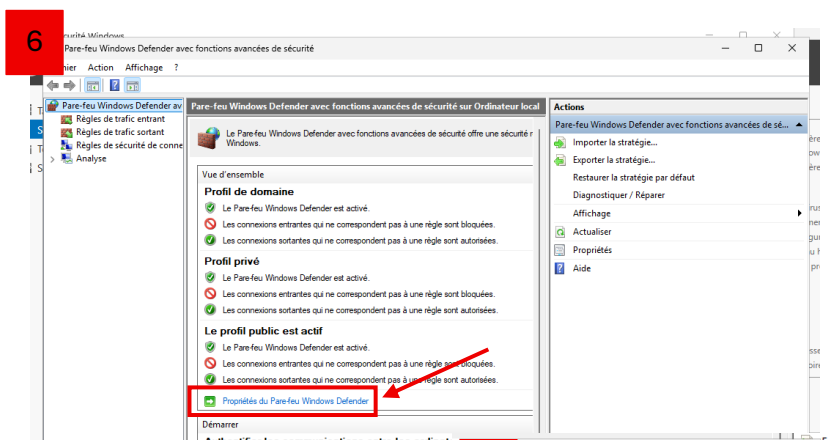
Une IP en 172.20.0.100 apparaît, on constate que le DHCP primaire ou que le DHCP secondaire récupère la même IP.

# PARTIES 3 AD



Dans notre cas, nous appellerons la machine « Hermes2 ». Faites ok, appliquer les changements et redémarrer votre machine.

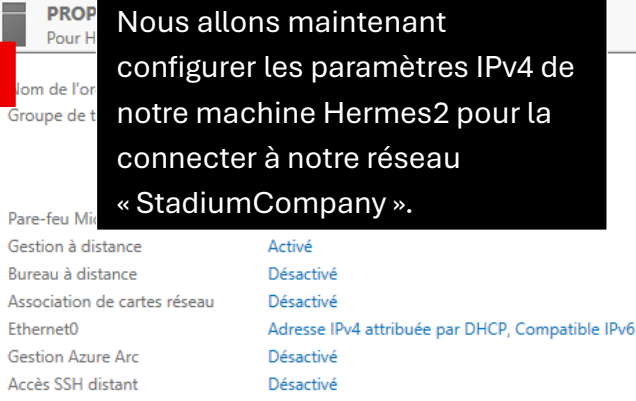
On va maintenant changer les paramètres du Firewall Windows pour nous éviter tout problème.



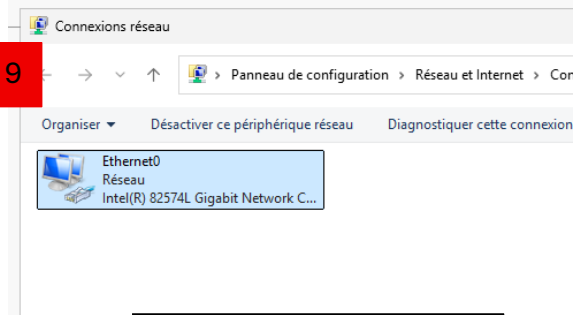
Nous allons mettre l'état du pare-feu sur « Désactiver » et le faire sur chaque profil. Quand cela est fait vous pouvez appliquer les changements et faire ok.

8

Nous allons maintenant configurer les paramètres IPv4 de notre machine Hermes2 pour la connecter à notre réseau « StadiumCompany ».

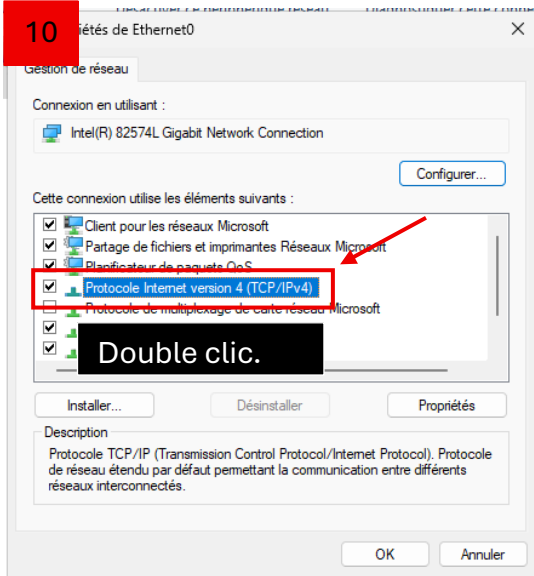


9



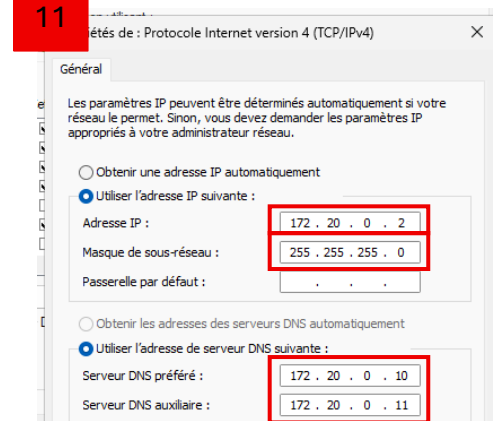
Clique droit sur la carte réseau puis Propriétés.

10



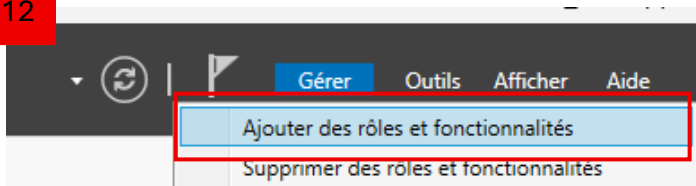
Double clic.

11



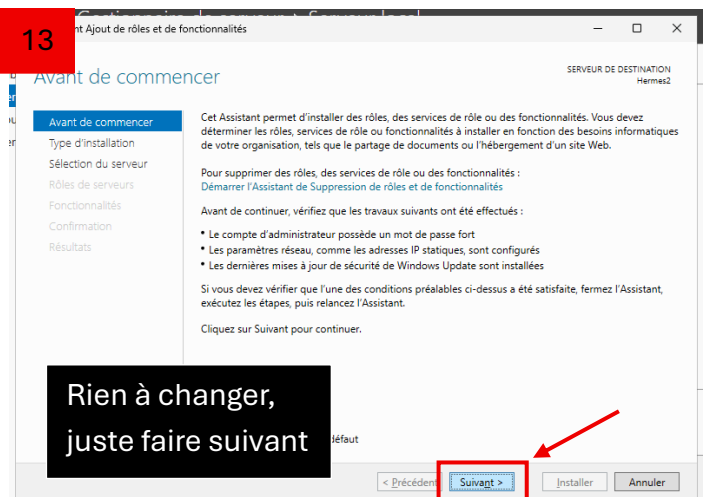
Toutes ces informations sont notées par simple logique, ce n'est pas aléatoire. Vous référer à vos paramétrages et votre tableau.

12

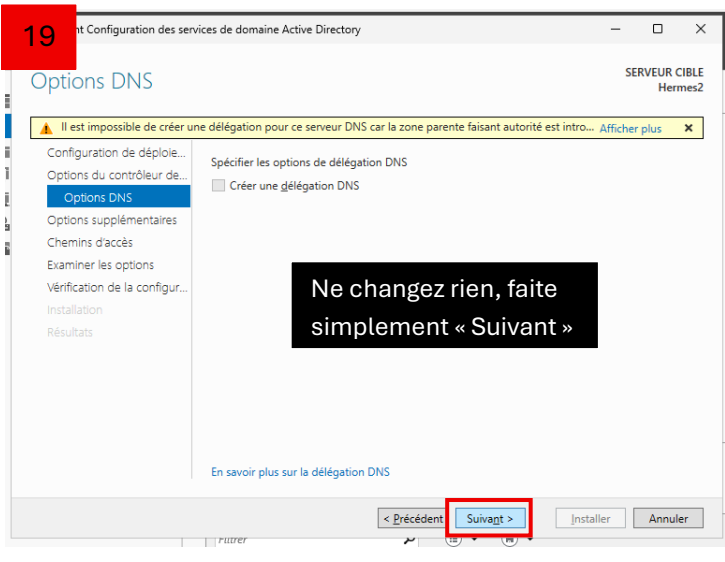
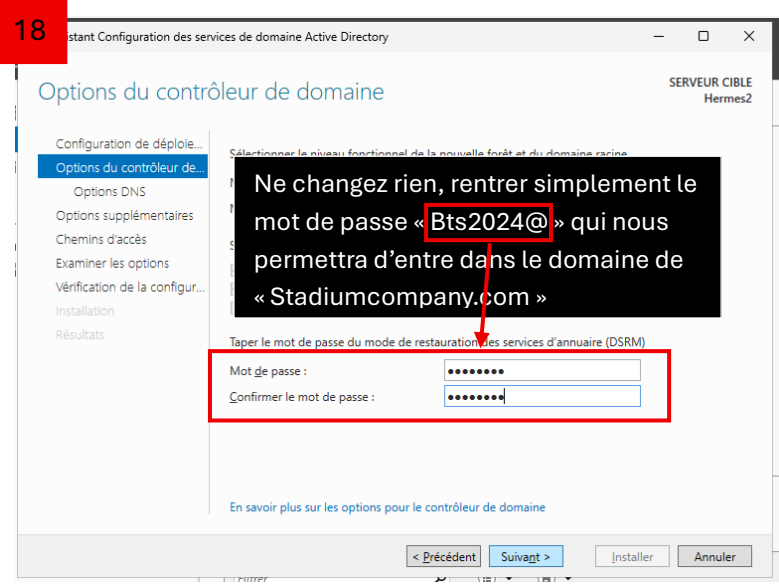
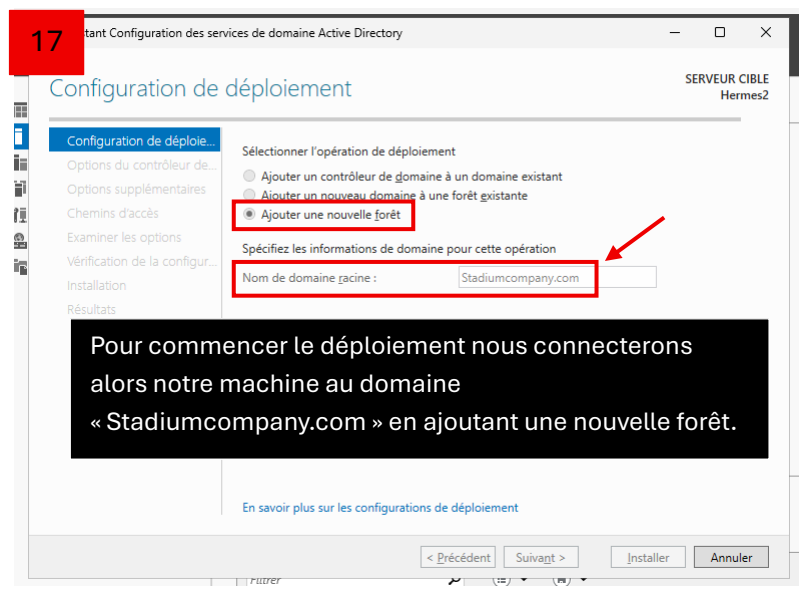
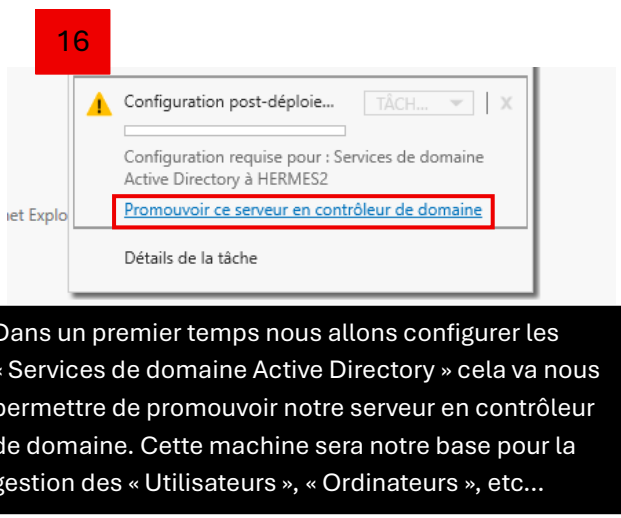
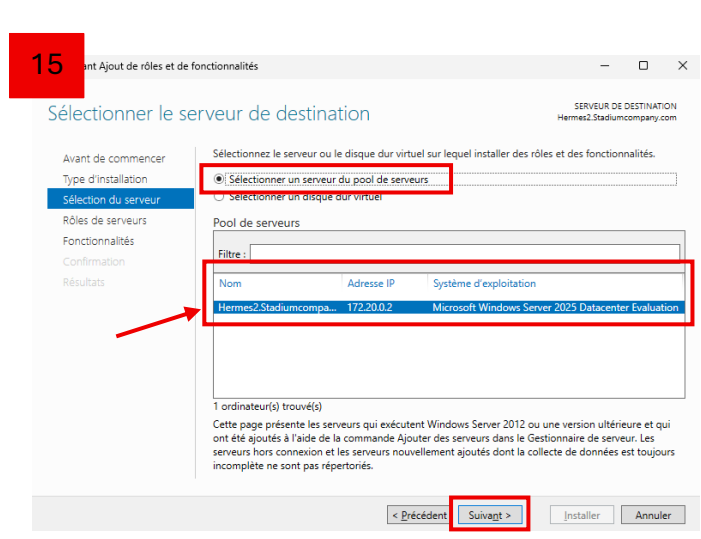
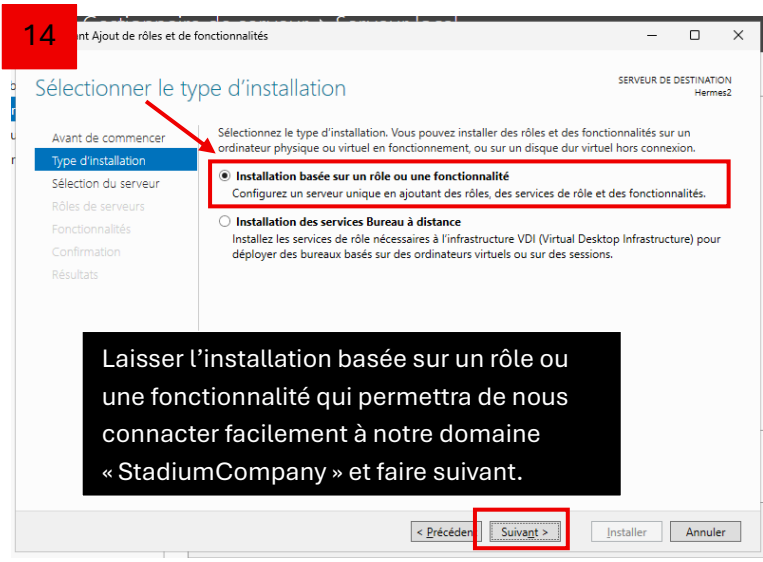


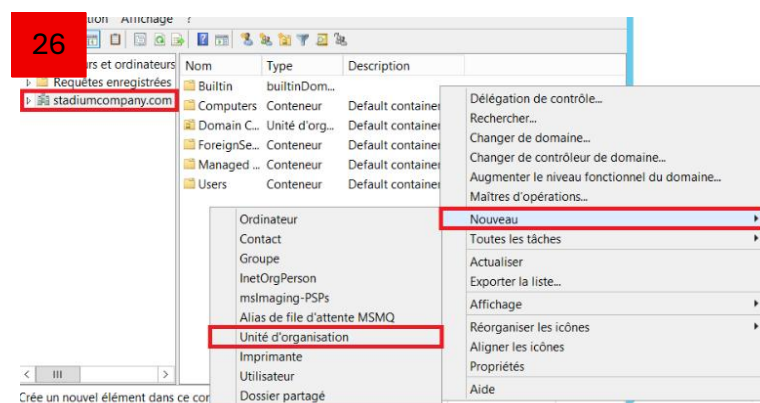
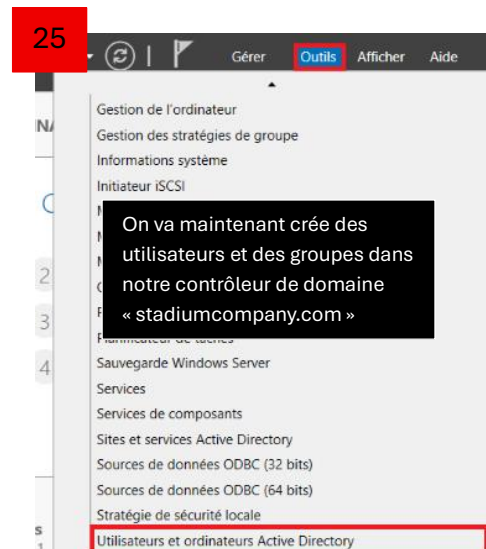
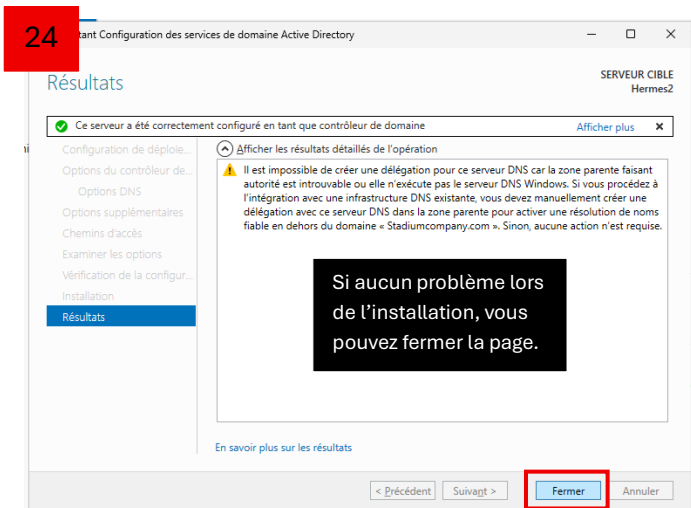
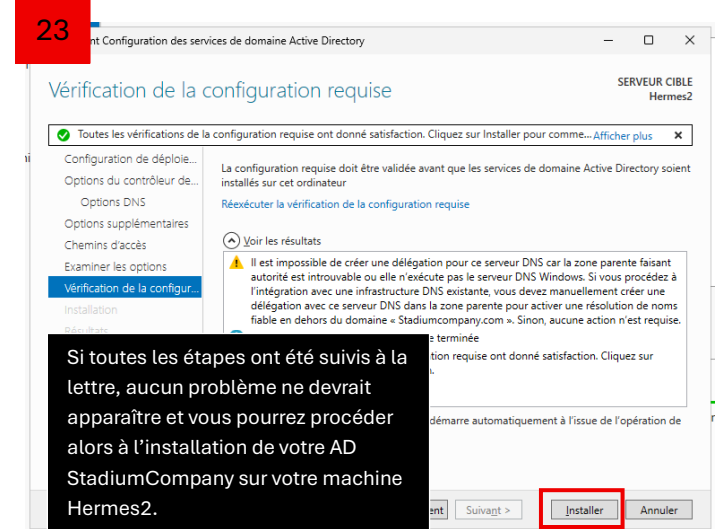
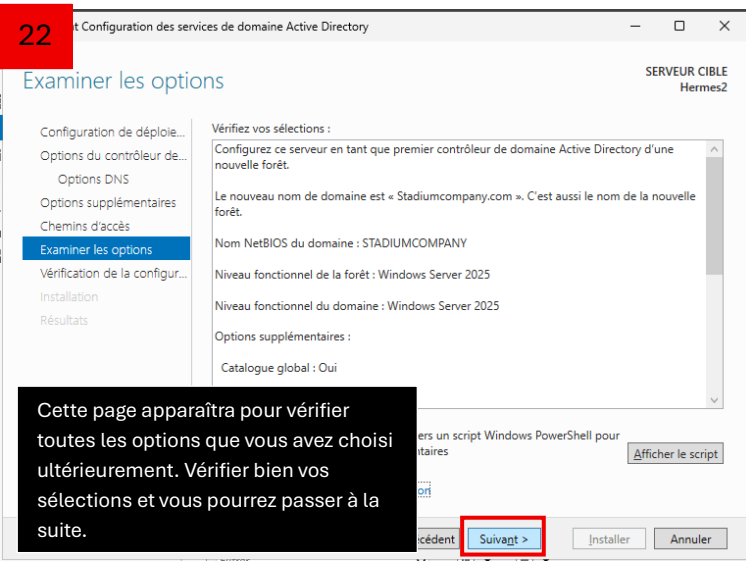
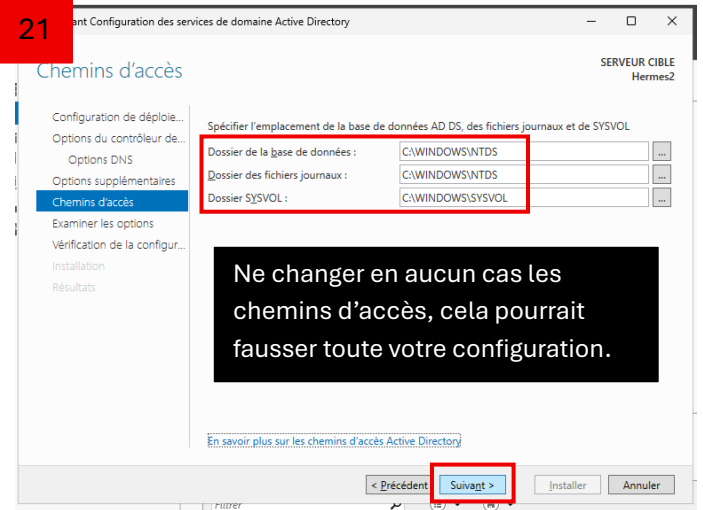
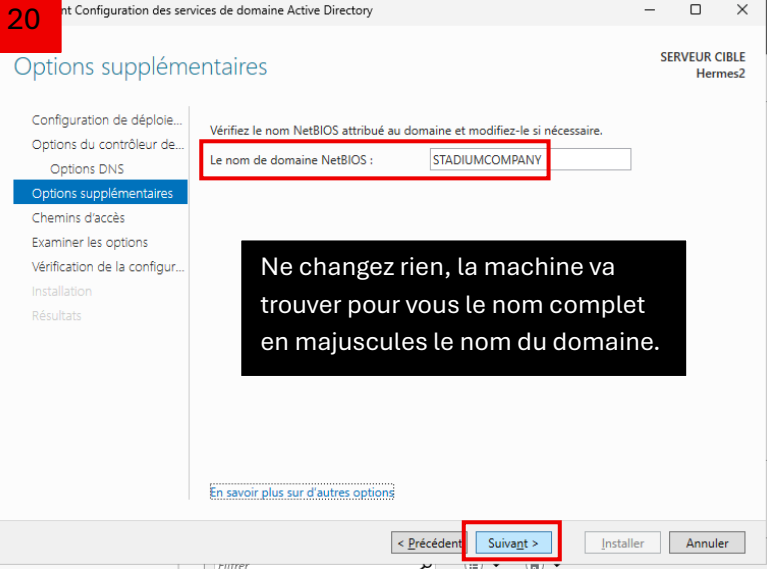
On va maintenant ajouter des rôles et des fonctionnalités.

13



Rien à changer, juste faire suivant





27

Créer dans : stadiumcompany.com/

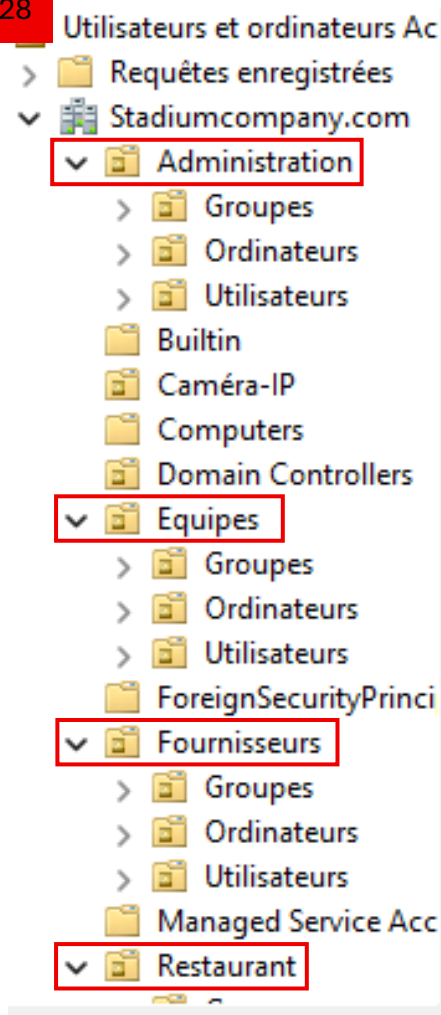
Nom :  
Administration

Protéger le conteneur contre une suppression accidentelle

OK Annuler Aide

Pour la première création nous allons l'appeler Administration. Laissez cocher la case « Protéger le conteneur contre une suppression accidentelle » et appuyer sur « OK ».

28



Vous allez ensuite refaire les mêmes étapes pour créer les autres « Unités d'organisation » comme ci-contre avec donc « Administration » puis « Equipes » puis « Wifi » puis « Caméra-IP » puis « VIP-Pressé » puis « Fournisseurs » puis « Restaurant ».

Dans chaque « Unités d'organisation » citez ici, vous devrez créer trois « Sous Unité d'Organisation » nommée donc « Groupes », « Ordinateurs » et « Utilisateurs ».

Félicitations vous avez maintenant terminé en totalité la configuration de votre machine Hermes2 qui nous servira d'Active Directory pour notre réseau déployé partout dans le stade.

## PARTIES 4 RSync

Le RSync est un outil de synchronisation et de transfert de fichiers utilisé en Linux, mais aussi disponible sur Windows. Il permet de copier, sauvegarder ou synchroniser des fichiers et répertoires entre deux emplacements, soit sur la même machine ou soit entre deux machines différentes.

RSync sert à :

- Copier des fichiers dans le local ou distant
- Synchroniser des répertoires
- Faire des sauvegardes automatiques et incrémentale
- Conserver les permissions, dates, liens symboliques

1. Pour installer le service RSync, il faut aller sur une machine Debian Linux et taper la commande ci-dessous :

Sudo apt install rsync

```
root@RSync:~# sudo apt install rsync
```

2. Puis il faut créer un répertoire de synchronisation, à l'aide de la commande :

Sudo nano /etc/rsyncd.conf.

```
root@RSync:~# sudo nano /etc/rsyncd.conf_
```

Dans ce fichier, il faut renseigner les champs suivants :

```
uid = root
gid = root
use chroot = no
max connections = 5
log file = /var/log/rsync.log
pid file = /var/run/rsyncd.pid

[backup]
path = /srv/backup
comment = Sauvegarde des fichiers utilisateurs
read only = no
auth users = adminrsync
secrets file = /etc/rsyncd.secrets
```

Voici les caractéristiques de chaque champs :

uid = root → Elle va s'exécuter avec l'utilisateur root.

gid = root → C'est la même chose mais pour le groupe.

use chroot = no → le "chroot" permet d'isoler avec le serveur dans un répertoire et le « no » résume que c'est désactivé, donc pas d'isolation.

max connections = 5 → Maximum 5 connexions simultanées dans le serveur RSync

log file = /var/log/rsync.log → C'est là que le RSync va écrire les logs c'est-à-dire les erreurs, son activité, les transferts etc...

pid file = /var/run/rsyncd.pid → C'est là que le fichier où Rsync va stocker son PID, qui est utile pour savoir si le service est en cours ou pour le stopper.

[backup] → C'est le nom du module. C'est comme un nom de partage que le client RSync qui utilisera pour se connecter

path = /srv/backup → C'est un répertoire réel sur le serveur qui sera synchronisé ou sauvegardé

comment = Sauvegarde des fichiers utilisateurs

read only = no → Elle autorise l'écriture. Si vous mettez « yes », le module serait en lecture seule

auth users = adminrsync → L'utilisateur est autorisé à se connecter. Le nom doit correspondre à un utilisateur défini dans le fichier secrets file

secrets file = /etc/rsyncd.secrets → C'est le chemin du fichier contenant les identifiants pour se connecter au module « [backup] »

3. Ensuite, il faut créer le fichier de mot de passe pour RSync, en utilisant la commande tel que :

Echo « adminrsync :motdepassefort » | sudo tee /etc/rsyncd.secrets

```
root@RSync:~# echo "adminrsync:motdepassefort" | sudo tee /etc/rsyncd.secrets_
```

Elle permet de vérifier l'authentification à RSync. Seuls les utilisateurs listés ici avec le mot de passe correct pourront accéder aux partages RSync définis dans le fichier /etc/rsyncd.conf.

4. Après, sécuriser le fichier, grâce à cette commande :

Sudo chmod 600 /etc/rsyncd.secrets

```
root@RSync:~# sudo chmod 600 /etc/rsyncd.secrets
root@RSync:~#
```

Cela empêche n'importe quel utilisateur du système de lire votre mot de passe.

5. Maintenant, il faut démarrer et activer le service RSync, en faisant ceux-ci :

Sudo systemctl enable rsync

```
root@RSync:~# sudo systemctl enable rsync
Synchronizing state of rsync service with
```

Elle configure RSync pour qu'il démarre automatiquement au démarrage de la machine.

```
root@RSync:~# sudo systemctl start rsync
root@RSync:~# sudo systemctl status rsync
● rsync.service - fast remote file copy program daemon
   Loaded: loaded (/lib/systemd/system/rsync.service; enabled; preset: enabled)
   Active: active (running) since Sat 2025-10-18 22:40:19 CEST; 1h 14min ago
     Docs: man:rsync(1)
           man:rsyncd.conf(5)
  Main PID: 1631 (rsync)
    Tasks: 1 (limit: 2257)
   Memory: 844.0K
      CPU: 18ms
   CGroup: /system.slice/rsync.service
           └─1631 /usr/bin/rsync --daemon --no-detach

oct. 18 22:40:19 RSync systemd[1]: Started rsync.service - fast remote file copy program daemon.
root@RSync:~#
```

Donc on peut constater que RSync est bien en fonctionnement et prêt à faire des sauvegardes ou des transferts.