

DHCP Failover

Ce document couvre l'implémentation et la gestion du **DHCP Failover**, une technique essentielle pour garantir la continuité du service DHCP sur les réseaux. La première partie est dédiée à l'installation et la mise en place du **DHCP Failover sous Linux**, avec des étapes détaillées allant de l'installation de DHCP à la configuration du Failover et l'analyse des trames réseau. La deuxième partie explore la mise en œuvre du **DHCP Failover sous Windows**, incluant l'installation du routeur, l'ajout du protocole RIP, ainsi que la configuration du service DHCP et du Failover.

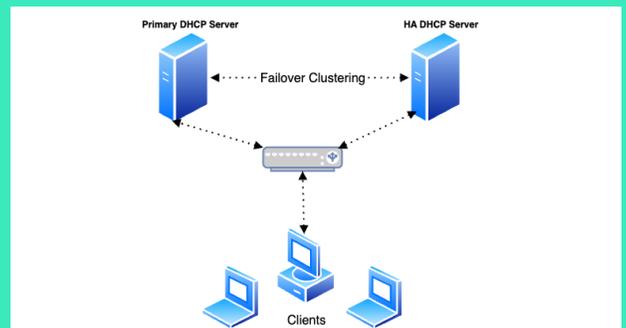


Table des matières

DHCP Failover	1
Table des matières	2
DHCP Failover Linux.....	3
Intro	3
Installation DHCP	3
Mise en place de failOver	6
Analyse des trames.....	8
DHCP Failover Windows	10
Intro	10
Installation du Routeur.....	11
Ajout du Rip.....	14
Mise en place du DHCP	15
Mise en place du FailOver	26



DHCP Failover Linux

03 / 02 / 2024

Version : 1

OBJECTIF : Cette section de la procédure vise à détailler la mise en place de Ubuntu.

MODE OPÉRATOIRE :

Intro

Le **DHCP Failover** est une solution qui permet d'assurer la continuité du service DHCP en cas de défaillance d'un serveur. En utilisant cette méthode, deux serveurs DHCP partagent la charge et se synchronisent pour garantir que les clients obtiennent toujours une adresse IP, même si l'un des serveurs devient indisponible. Ce système est essentiel pour améliorer la disponibilité et la résilience des réseaux.

Installation DHCP

Pour configurer votre machine, suivez les étapes suivantes :

1. Commencez par modifier le nom de votre machine en utilisant la commande :

```
nano /etc/hostname
```

```
nano /etc/hosts
```

2. Mettez à jour votre système en exécutant les commandes : `apt update` et `apt upgrade` .

3. Enfin, installez le paquet ntp en utilisant la commande `apt install ntpsec`, puis vérifiez la date avec la commande : `date` .

Une fois votre configuration de base faite taper la commande :

```
apt install isc-dhcp-server
```

Après avoir installé le serveur DHCP, des erreurs peuvent survenir lors de son exécution. Il est nécessaire de configurer l'interface sur laquelle le serveur DHCP doit écouter en utilisant la commande `nano /etc/default/isc-dhcp-server` :



```
# On what interfaces should the DHCP server (dhcpd) serve DHCP requests?
#       Separate multiple interfaces with spaces, e.g. "eth0 eth1".
INTERFACESv4="enp0s3"
INTERFACESv6=""
```

De plus, il est nécessaire d'éditer le fichier de configuration principal du serveur DHCP en utilisant la commande `nano /etc/dhcp/dhcpd.conf` afin de spécifier les plages d'adresses IP et d'autres configurations requises :



```
# dhcpd.conf
#
# Sample configuration file for ISC dhcpd
#
# option definitions common to all supported networks...
option domain-name "example.org";
option domain-name-servers ns1.example.org, ns2.example.org;

default-lease-time 240;
max-lease-time 240;

# The ddns-updates-style parameter controls whether or not the server will
# attempt to do a DNS update when a lease is confirmed. We default to the
# behavior of the version 2 packages ('none', since DHCP v2 didn't
# have support for DDNS.)
# have support for DDNS.)
ddns-update-style none;

# If this DHCP server is the official DHCP server for the local
# network, the authoritative directive should be uncommented.
authoritative;

# Use this to send dhcp log messages to a different log file (you also
# have to hack syslog.conf to complete the redirection).
#log-facility local7;

# No service will be given on this subnet, but declaring it helps the
# DHCP server to understand the network topology.

#subnet 10.152.187.0 netmask 255.255.255.0 {
#}

# This is a very basic subnet declaration.
```

```
# This is a very basic subnet declaration.

subnet 192.168.2.16 netmask 255.255.255.248 {
    range 192.168.2.17 192.168.2.19;
    option routers 192.168.2.22;
}

subnet 192.168.1.16 netmask 255.255.255.248 {
    range 192.168.1.17 192.168.1.19;
    option routers 192.168.1.22;
}

# This declaration allows BOOTP clients to get dynamic addresses,
# which we don't really recommend.

#subnet 10.254.239.32 netmask 255.255.255.224 {
#    range dynamic-bootp 10.254.239.40 10.254.239.60;
#    option broadcast-address 10.254.239.31;
#    option routers rtr-239-32-1.example.org;
#}

# A slightly different configuration for an internal subnet.
#subnet 10.5.5.0 netmask 255.255.255.224 {
#    range 10.5.5.26 10.5.5.30;
#    option domain-name-servers ns1.internal.example.org;
#    option domain-name "internal.example.org";
#    option routers 10.5.5.1;
#    option broadcast-address 10.5.5.31;
#    default-lease-time 600;
#    max-lease-time 7200;
#}

-
```

Après modification du fichier « `dhcpd.conf` », relancez le serveur DHCP avec la commande `systemctl restart isc-dhcp-server`

Mise en place de failOver

Une fois le DHCP installé sur le réseau, dupliquez-le pour en avoir deux instances. Sur le premier serveur DHCP, retournez dans le fichier **dhcpcd.conf** et insérez les lignes de code suivantes :

Sur le serveur DHCP 1 :



```
# This is a very basic subnet declaration.
failover peer "failover-partner" {
    primary;
    address 172.20.69.1;
    peer address 172.20.69.2;
    max-response-delay 60;
    max-unacked-updates 10;
    mclt 3600;
    split 128;
    load balance max seconds 3;
}

subnet 172.20.0.0 netmask 255.255.0.0 {
    pool {
        failover peer "failover-partner";
        range 172.20.69.3 172.20.69.69;
    }
}

# insert this (with your own key text substituted) into dh

omapi-port 7911;
omapi-key omapi_key;

key omapi_key {
    algorithm hmac-md5;
    secret 0fakekeyfakekeyfakekey==;
}
```

Sur le serveur DHCP 2 :



```
# This is a very basic subnet declaration.

failover peer "failover-partner" {
    secondary;
    address 172.20.69.2;
    peer address 172.20.69.1;
    max-response-delay 60;
    max-unacked-updates 10;
    load balance max seconds 3;
}

subnet 172.20.0.0 netmask 255.255.0.0 {
    pool {
        failover peer "failover-partner";
        range 172.20.69.3 172.20.69.69;
    }
}

omapi-port 7911;
omapi-key omapi_key;

key omapi_key {
    algorithm hmac-md5;
    secret 0fakekeyfakekeyfakekey==;
}
```

Vous pouvez également trouver une documentation plus détaillée sur le site :

→ <https://kb.isc.org/docs/aa-00502>

Analyse des trames

No.	Time	Source	Destination	Protocol	Length	Info
33	12.788963	172.20.69.29	172.20.69.1	DHCP	342	DHCP Release - Transaction ID 0x...
58	20.455042	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x...
62	21.457341	172.20.69.1	172.20.69.29	DHCP	342	DHCP Offer - Transaction ID 0x...
63	21.458031	0.0.0.0	255.255.255.255	DHCP	344	DHCP Request - Transaction ID 0x...
64	21.463651	172.20.69.1	172.20.69.29	DHCP	342	DHCP ACK - Transaction ID 0x...

No.	Time	Source	Destination	Protocol	Length	Info
25	10.215951	172.20.69.1	172.20.69.2	DHCPFO	78	Contact xid: 47
31	12.216742	172.20.69.2	172.20.69.1	DHCPFO	78	Contact xid: 39
34	12.793501	172.20.69.1	172.20.69.2	DHCPFO	145	Binding update xid: 48
41	14.796043	172.20.69.2	172.20.69.1	DHCPFO	86	Binding acknowledge xid: 48
65	21.463651	172.20.69.1	172.20.69.2	DHCPFO	145	Binding update xid: 49
92	23.469472	172.20.69.2	172.20.69.1	DHCPFO	86	Binding acknowledge xid: 49
138	41.464369	172.20.69.1	172.20.69.2	DHCPFO	78	Contact xid: 4a
144	43.470029	172.20.69.2	172.20.69.1	DHCPFO	78	Contact xid: 3a
181	61.468382	172.20.69.1	172.20.69.2	DHCPFO	78	Contact xid: 4b
187	63.470925	172.20.69.2	172.20.69.1	DHCPFO	78	Contact xid: 3b
236	81.470261	172.20.69.1	172.20.69.2	DHCPFO	78	Contact xid: 4c
244	83.471994	172.20.69.2	172.20.69.1	DHCPFO	78	Contact xid: 3c

823	331.352628	PCSSystemtec_0e:a4:...	Broadcast	ARP	60	Who has 172.20.2.254? Tell 172.20.69.2
824	333.102196	PCSSystemtec_0e:a4:...	Broadcast	ARP	60	Who has 172.20.2.254? Tell 172.20.69.2
825	334.105294	PCSSystemtec_0e:a4:...	Broadcast	ARP	60	Who has 172.20.2.254? Tell 172.20.69.2
826	334.123959	172.20.69.2	172.20.69.1	DHCPFO	78	Contact xid: 49
827	334.336680	172.20.69.2	172.20.69.1	TCP	78	[TCP Retransmission] 56305 + 647 [PSH, ACK] Seq=340 Ack=567 Wi...
828	334.553379	172.20.69.2	172.20.69.1	TCP	78	[TCP Retransmission] 56305 + 647 [PSH, ACK] Seq=340 Ack=567 Wi...
829	335.001126	172.20.69.2	172.20.69.1	TCP	78	[TCP Retransmission] 56305 + 647 [PSH, ACK] Seq=340 Ack=567 Wi...
830	335.128958	PCSSystemtec_0e:a4:...	Broadcast	ARP	60	Who has 172.20.2.254? Tell 172.20.69.2
831	335.864875	172.20.69.2	172.20.69.1	TCP	78	[TCP Retransmission] 56305 + 647 [PSH, ACK] Seq=340 Ack=567 Wi...
832	336.152998	PCSSystemtec_0e:a4:...	Broadcast	ARP	60	Who has 172.20.2.254? Tell 172.20.69.2
833	337.177149	PCSSystemtec_0e:a4:...	Broadcast	ARP	60	Who has 172.20.2.254? Tell 172.20.69.2
834	337.592938	172.20.69.2	172.20.69.1	TCP	78	[TCP Retransmission] 56305 + 647 [PSH, ACK] Seq=340 Ack=567 Wi...
835	338.201027	PCSSystemtec_0e:a4:...	Broadcast	ARP	60	Who has 172.20.2.254? Tell 172.20.69.2
836	339.224952	PCSSystemtec_0e:a4:...	Broadcast	ARP	60	Who has 172.20.2.254? Tell 172.20.69.2
837	340.248550	PCSSystemtec_0e:a4:...	Broadcast	ARP	60	Who has 172.20.2.254? Tell 172.20.69.2
838	341.241202	172.20.69.2	172.20.69.1	TCP	78	[TCP Retransmission] 56305 + 647 [PSH, ACK] Seq=340 Ack=567 Wi...
839	341.272541	PCSSystemtec_0e:a4:...	Broadcast	ARP	60	Who has 172.20.2.254? Tell 172.20.69.2
840	342.297428	PCSSystemtec_0e:a4:...	Broadcast	ARP	60	Who has 172.20.2.254? Tell 172.20.69.2

Carte Ethernet Ethernet :

```

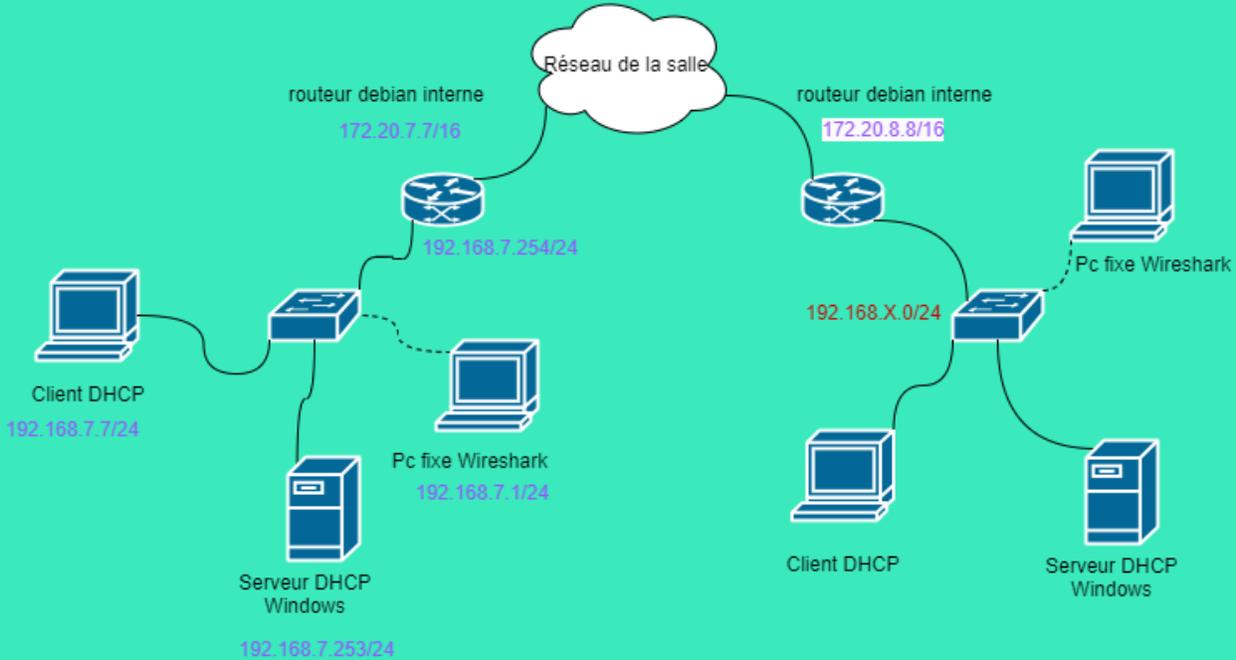
Suffixe DNS propre à la connexion. . . : serveurDHCP.org
Description. . . . . : Intel(R) PRO/1000 MT Desktop Adapter
Adresse physique . . . . . : 08-00-27-0E-76-69
DHCP activé. . . . . : Oui
Configuration automatique activée. . . : Oui
Adresse IPv4. . . . . : 172.20.69.29(préfééré)
Masque de sous-réseau. . . . . : 255.255.0.0
Bail obtenu. . . . . : jeudi 12 septembre 2024 11:14:28
Bail expirant. . . . . : jeudi 12 septembre 2024 11:18:28
Passerelle par défaut. . . . . :
Serveur DHCP . . . . . : 172.20.69.1
NetBIOS sur Tcpiip. . . . . : Activé
  
```

Carte Ethernet Ethernet :

```
Suffixe DNS propre à la connexion. . . : serveurDHCP2.org
Description. . . . . : Intel(R) PRO/1000 MT Desktop Adapter
Adresse physique . . . . . : 08-00-27-0E-76-69
DHCP activé. . . . . : Oui
Configuration automatique activée. . . : Oui
Adresse IPv4. . . . . : 172.20.69.29(préfééré)
Masque de sous-réseau. . . . . : 255.255.0.0
Bail obtenu. . . . . : jeudi 12 septembre 2024 11:14:28
Bail expirant. . . . . : jeudi 12 septembre 2024 11:24:15
Passerelle par défaut. . . . . :
Serveur DHCP . . . . . : 172.20.69.2
NetBIOS sur Tcip. . . . . : Activé
```

Intro

Schéma :



Installation du Routeur

Pour configurer votre machine, suivez les étapes suivantes :

1. Commencez par modifier le nom de votre machine en utilisant la commande :

```
nano /etc/hostname
```

```
nano /etc/hosts
```

2. Mettez à jour votre système en exécutant les commandes : `apt update` et `apt upgrade` .

3. Enfin, installez le paquet ntp en utilisant la commande `apt install ntpsec`, puis vérifiez la date avec la commande : `date` .

Une fois les prérequis terminés, vous pouvez modifier le dossier de configuration avec la commande : `nano /etc/network/interfaces` :

→

```
GNU nano 7.2
# 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 enp0s3
# iface enp0s3 inet dhcp
#
auto enp0s3
#
iface enp0s3 inet static
address 172.20.7.7/16
gateway 172.20.2.254

auto enp0s8
iface enp0s8 inet static
address 192.168.7.254/16
```

Une fois les interfaces configurées, vous devrez démarrer le service des interfaces réseau. Ensuite, vérifiez si les interfaces sont activées à l'aide de la commande `ip -c a` :



```
root@RouteurDebianFO:~# ip -c 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: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:26:59:dc brd ff:ff:ff:ff:ff:ff
    inet 172.20.7.7/16 brd 172.20.255.255 scope global enp0s3
        valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fe26:59dc/64 scope link
        valid_lft forever preferred_lft forever
3: enp0s8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:1b:2c:b4 brd ff:ff:ff:ff:ff:ff
    inet 192.168.7.254/16 brd 192.168.255.255 scope global enp0s8
        valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fe1b:2cb4/64 scope link
```

Une fois les interfaces configurées, activez le routage dans « nano /etc/systemctl.conf » :



```
root@RouteurDebianFO:~# nano /etc/sysctl.conf
root@RouteurDebianFO:~#
```

Recherchez la ligne contenant « net.ipv4.ip.forward » et décommentez-la en retirant le symbole « # » au début de la ligne :



```
# Turn on source address verification in all interfaces to
# prevent some spoofing attacks
#net.ipv4.conf.default.rp_filter=1
#net.ipv4.conf.all.rp_filter=1

# Uncomment the next line to enable TCP/IP SYN cookies
# See http://lwn.net/Articles/277146/
# Note: This may impact IPv6 TCP sessions too
#net.ipv4.tcp_syncookies=1

# Uncomment the next line to enable packet forwarding for IPv4
net.ipv4.ip_forward=1 ←
# Uncomment the next line to enable packet forwarding for IPv6
# Enabling this option disables Stateless Address Autoconfiguration
# based on Router Advertisements for this host
#net.ipv6.conf.all.forwarding=1
```

Il faut également mettre en place le dhcp relay. Pour installer le service de relais, exécutez la commande : `apt install isc-dhcp-relay`. Une fois le service de relais activé, saisissez la commande : `nano /etc/default/isc-dhcp-relay` :



```
# Defaults for isc-dhcp-relay initscript
# sourced by /etc/init.d/isc-dhcp-relay
# installed at /etc/default/isc-dhcp-relay by the maintainer scripts

#
# This is a POSIX shell fragment
#

# What servers should the DHCP relay forward requests to?
SERVERS="192.168.8.253"

# On what interfaces should the DHCP relay (dhrelay) serve DHCP requests?
INTERFACES="enp0s3 enp0s8"

# Additional options that are passed to the DHCP relay daemon?
OPTIONS=""
```

Ajout du Rip

Pour mettre en place le RIP (Routing Information Protocol) sur un système Linux :

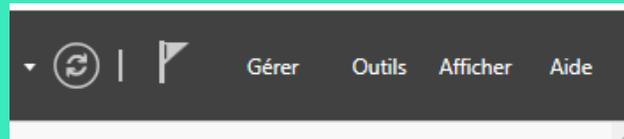
→ Apt install frr

```
root@serverDHCP:~# apt install frr
Lecture des listes de paquets... Fait
```

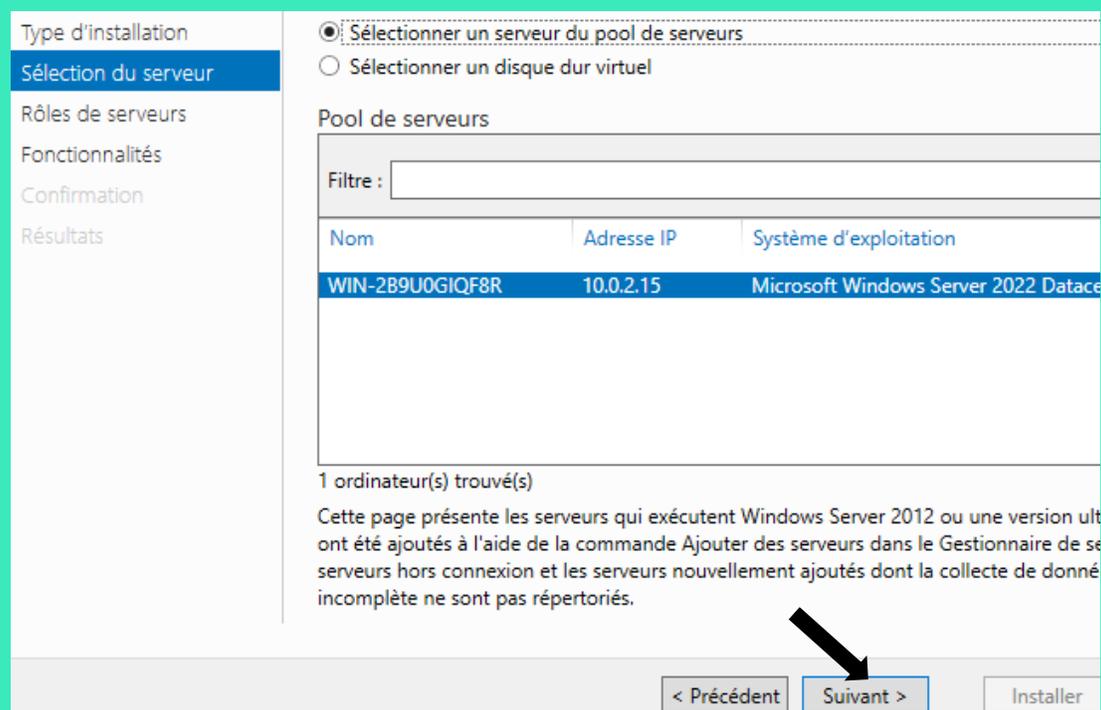
Mise en place du DHCP

Une fois le Rip réaliser lancer votre serveur Windows, et changer lui son ip. Et chnager le nom du PC.

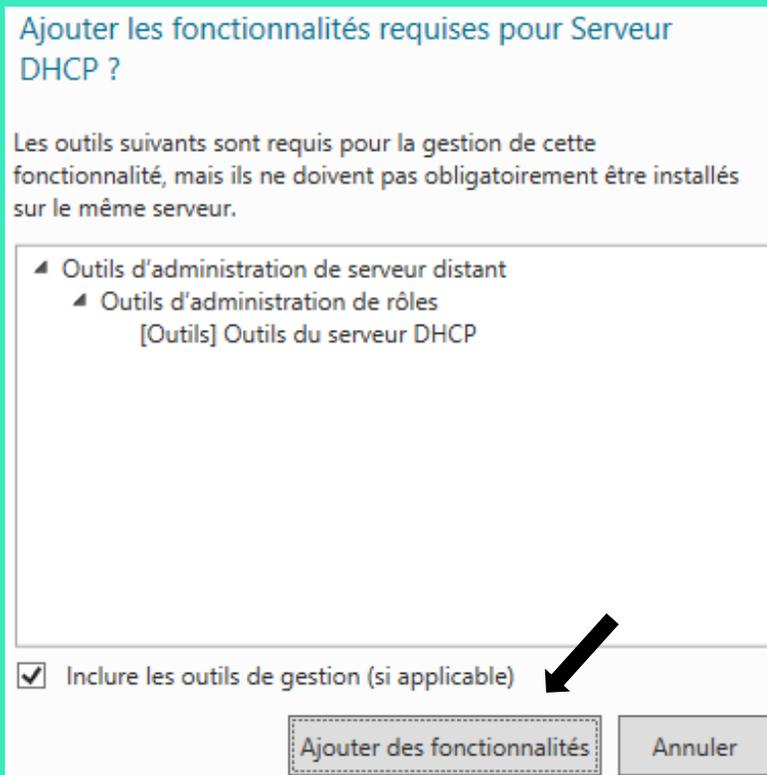
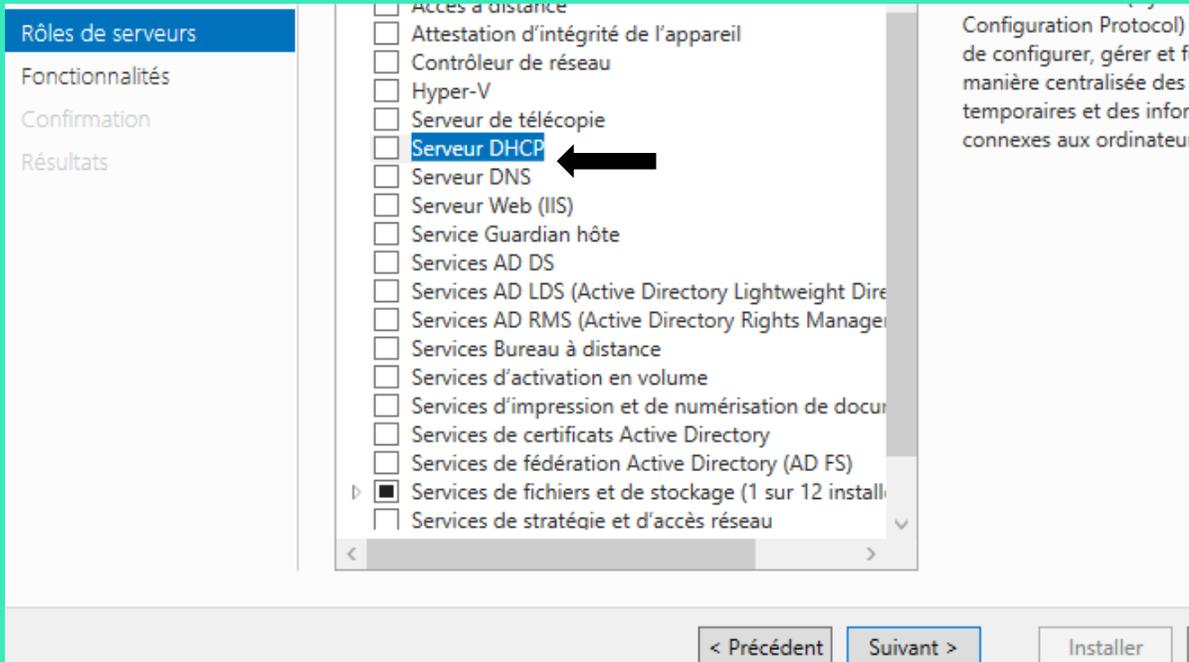
Pour pouvoir le service DHCP, cliquez sur "Gérer" et "Ajouter des rôles et fonctionnalités" :

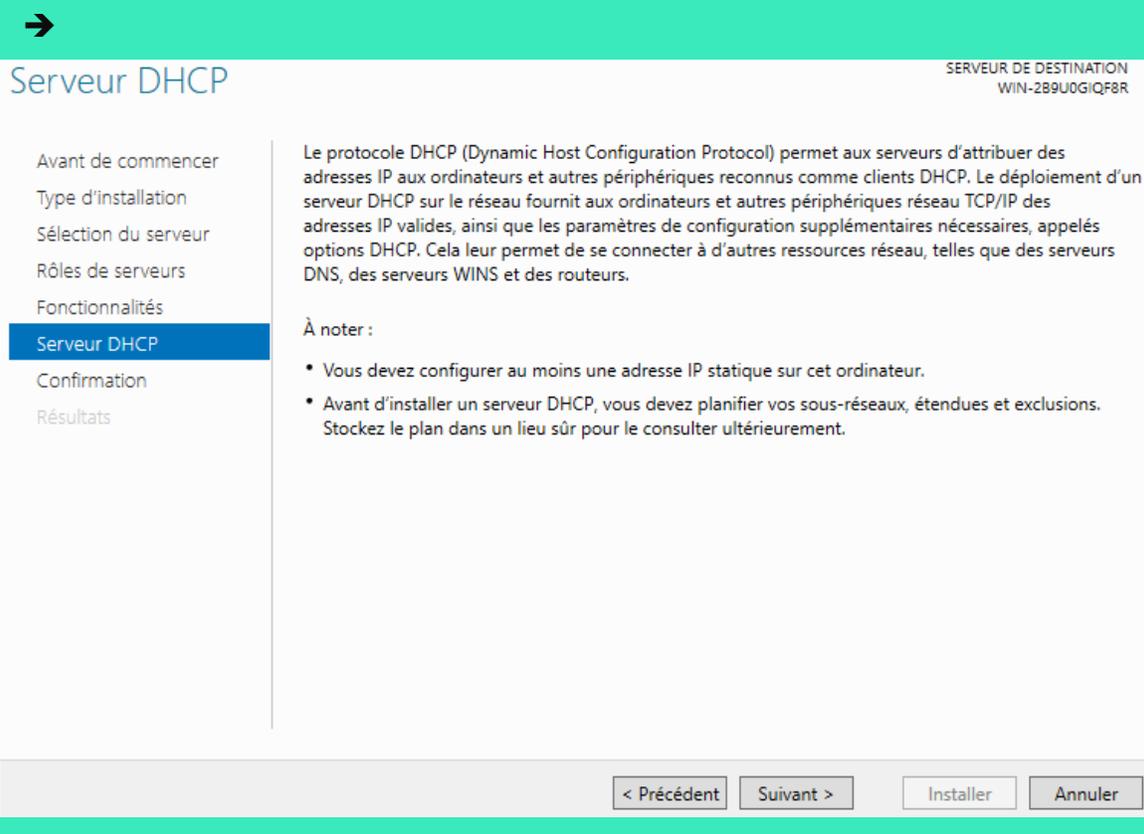
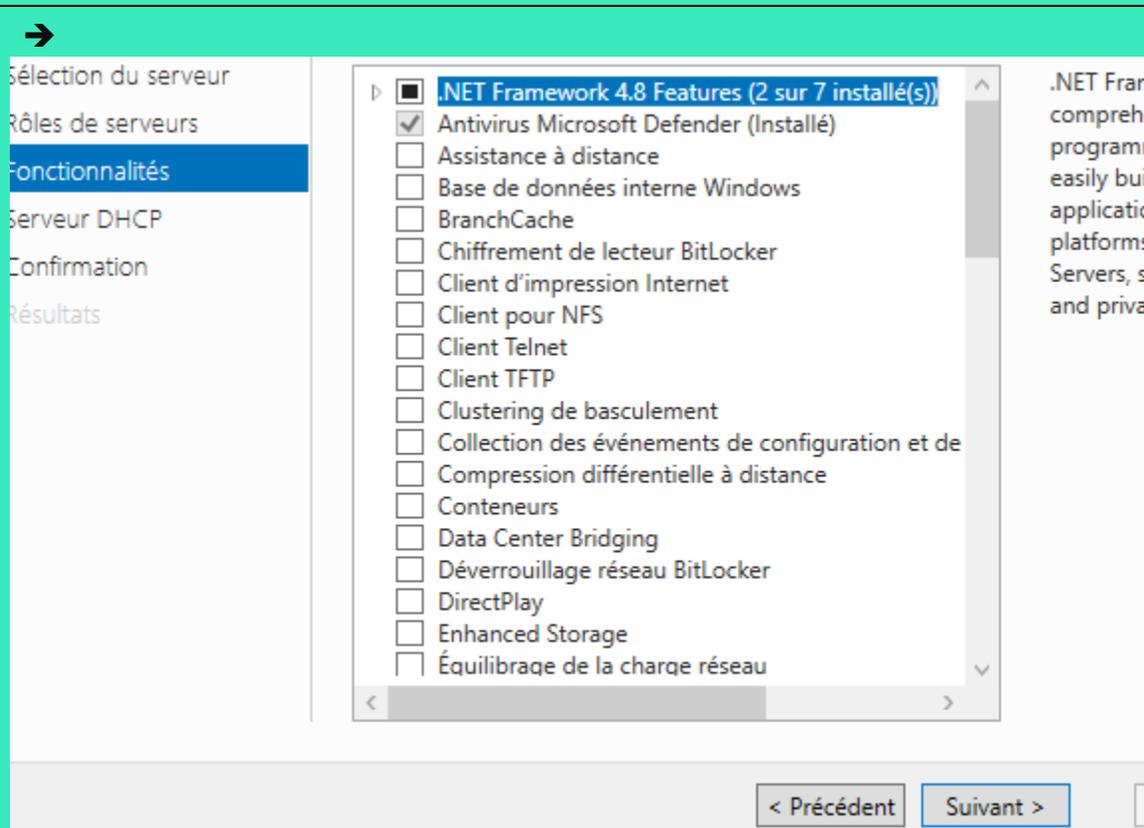


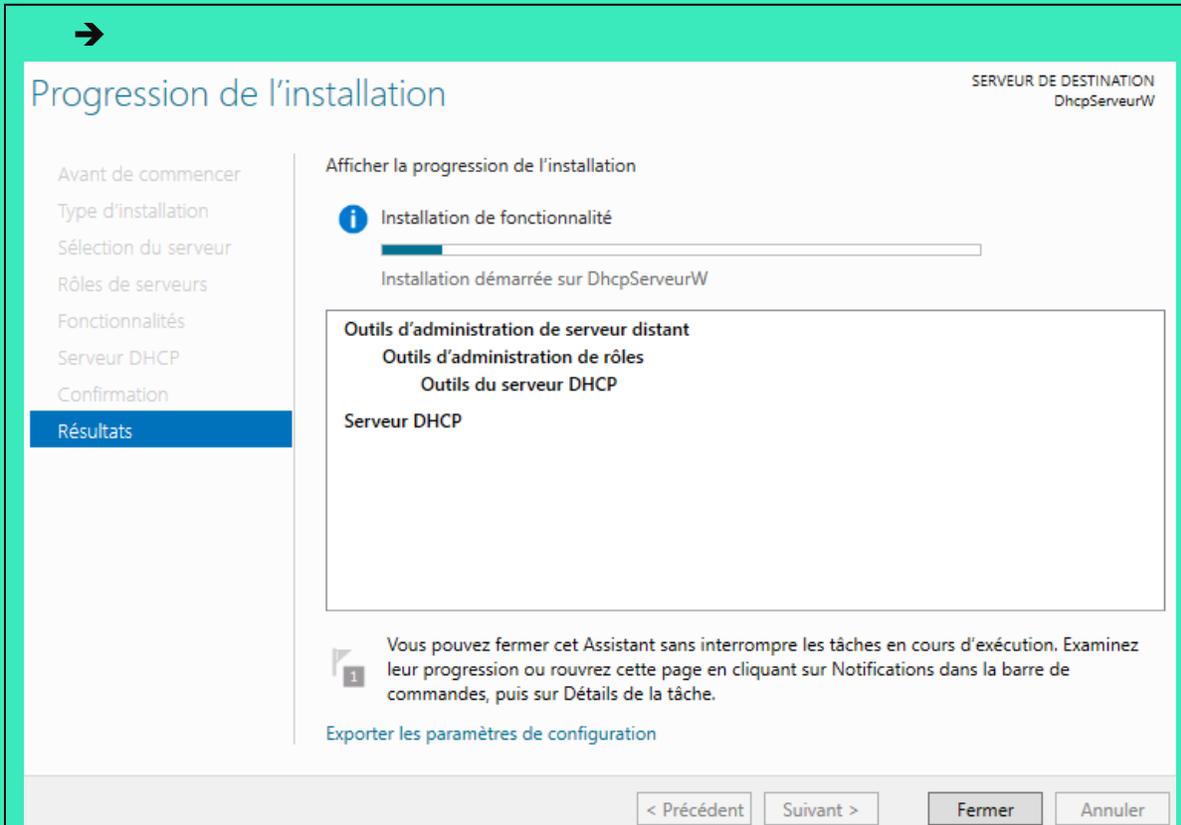
Choisissez l'option "Installation basée sur un rôle ou une fonctionnalité" et poursuivez :



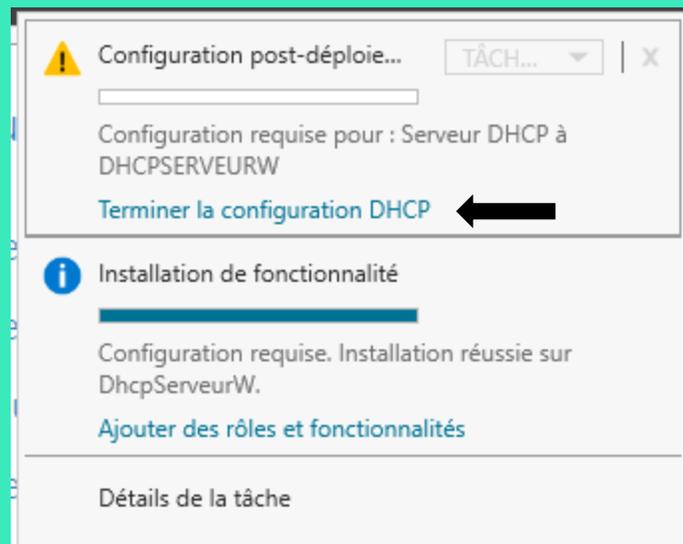
Dans la liste des rôles, cochez "Serveur DHCP" et au sein de la fenêtre qui s'affiche vérifiez que l'option "Inclure les outils de gestion" soit cochée. Elle permet d'ajouter la console de gestion DHCP sur le serveur. Cliquez sur "Ajouter des fonctionnalités" :







Dans le Gestionnaire de serveur, il y a un avertissement en haut à droite. Cliquez sur l'icône puis sur "Terminer la configuration DHCP" :



Si vous êtes déjà connecté en tant qu'administrateur ou avec un compte qui est administrateur de l'entreprise, vous pouvez continuer avec l'option "Utiliser les informations d'identification de l'utilisateur suivant". Sinon, il faudra renseigner un compte en activant l'option "Utiliser d'autres informations d'identification" :



Description

Description

Résumé

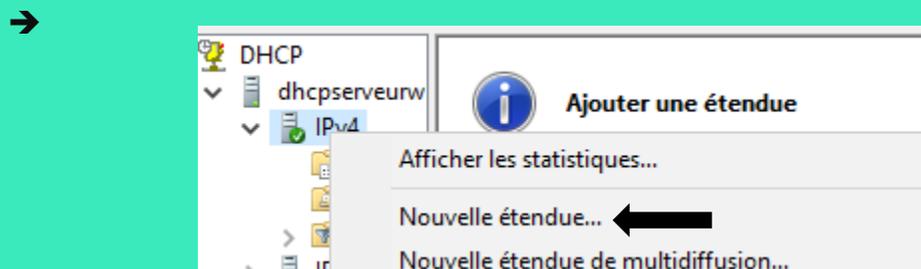
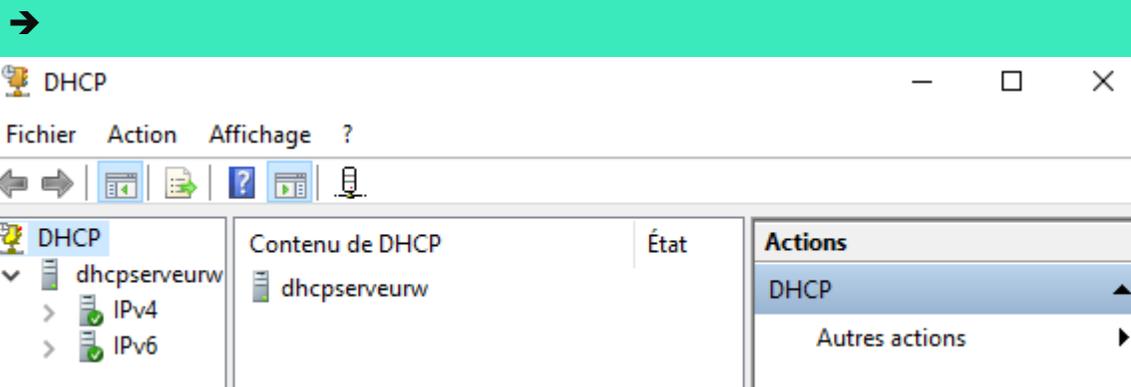
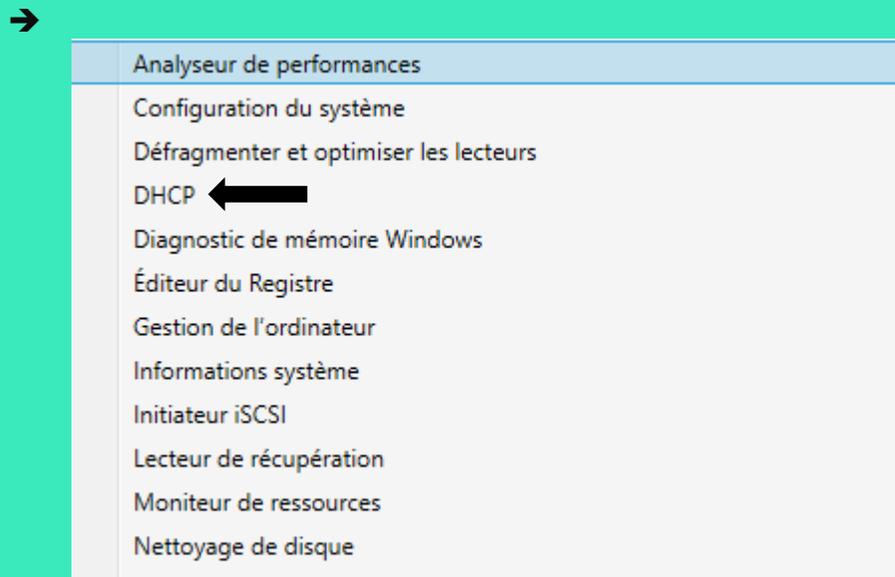
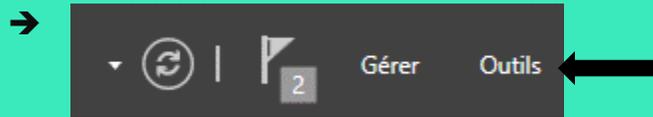
Les étapes suivantes seront effectuées pour configurer le serveur DHCP sur l'ordinateur cible :

Créez les groupes de sécurité suivants pour la délégation de l'administration du serveur DHCP.

- Administrateurs DHCP
- Utilisateurs DHCP

< Précédent Suivant > Valider Annuler

Dans la console DHCP, effectuez un clic droit sur "IPv4" puis sur "Nouvelle étendue" :



Assistant Nouvelle étendue



Assistant Nouvelle étendue

Cet Assistant vous permet de paramétrer une étendue pour distribuer des adresses IP aux ordinateurs sur le réseau.

Cliquez sur Suivant pour continuer.



< Précédent

Suivant >

Annuler



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 :

Adresse IP de fin :

Paramètres de configuration qui se propagent au client DHCP.

Longueur :

Masque de sous-réseau :

< Précédent

Suivant >

Annuler



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 :

Supprimer

Retard du sous-réseau en millisecondes :

< Précédent

Suivant >

Annuler



Durée du bail



La durée du bail spécifie la durée pendant laquelle un client peut utiliser une adresse IP de cette étendue.

La durée du bail doit théoriquement être égale au temps moyen durant lequel l'ordinateur est connecté au même réseau physique. Pour les réseaux mobiles constitués essentiellement par des ordinateurs portables ou des clients d'accès à distance, des durées de bail plus courtes peuvent être utiles.

De la même manière, pour les réseaux stables qui sont constitués principalement d'ordinateurs de bureau ayant des emplacements fixes, des durées de bail plus longues sont plus appropriées.

Définissez la durée des baux d'étendue lorsqu'ils sont distribués par ce serveur.

Limitée à :

Jours :

Heures :

Minutes :

< Précédent

Suivant >

Annuler

A l'étape suivante, sélectionnez "Oui, je veux configurer ces options maintenant" et poursuivez. Cela va permettre de définir des paramètres supplémentaires comme l'attribution d'une passerelle et d'un DNS :

→ Assistant Nouvelle étendue

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

Commençons par le routeur à attribuer aux clients DHCP de cette étendue, autrement dit la passerelle par défaut de votre réseau. Indiquez l'adresse IP et cliquez sur "Ajouter" :

→

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

 Supprimer

 Monter

 Descendre

< Précédent Suivant > Annuler

Nous n'avons pas de DNS, donc pas besoin de le renseigner :

→ **Nom de domaine et serveurs DNS**

DNS (Domain Name System) mappe et traduit les noms de domaines utilisés par les clients sur le réseau.

Vous pouvez spécifier le domaine parent à utiliser par les ordinateurs clients sur le réseau pour la résolution de noms DNS.

Domaine parent :

Pour configurer les clients d'étendue pour qu'ils utilisent les serveurs DNS sur le réseau, entrez les adresses IP pour ces serveurs.

Nom du serveur :	Adresse IP :	
<input type="text"/>	<input type="text" value="8.8.8.8"/>	Ajouter
<input type="button" value="Résoudre"/>		Supprimer
		Monter
		Descendre

< Précédent Suivant > Annuler

La résolution WINS étant obsolète, il n'est pas nécessaire de renseigner un serveur. Laissez vide et poursuivez :

→ **Assistant Nouvelle étendue**

Serveurs WINS

Les ordinateurs fonctionnant avec Windows peuvent utiliser les serveurs WINS pour convertir les noms NetBIOS d'ordinateurs en adresses IP.

Entrer les adresses IP ici permet aux clients Windows d'interroger WINS avant d'utiliser la diffusion pour s'enregistrer et résoudre les noms NetBIOS.

Nom du serveur :	Adresse IP :	
<input type="text"/>	<input type="text"/>	Ajouter
<input type="button" value="Résoudre"/>		Supprimer
		Monter
		Descendre

Pour modifier ce comportement pour les clients DHCP Windows, modifiez l'option 046, type de nœud WINS/NBT, dans les options de l'étendue.

< Précédent Suivant > Annuler



Activer l'étendue

Les clients ne peuvent obtenir des baux d'adresses que si une étendue est activée.



Voulez-vous activer cette étendue maintenant ?

- Oui, je veux activer cette étendue maintenant
- Non, j'activerai cette étendue ultérieurement

< Précédent

Suivant >

Annuler



Fin de l'Assistant Nouvelle étendue

L'Assistant Nouvelle étendue s'est terminé correctement.

Pour offrir une haute disponibilité pour cette étendue, configurez le basculement pour l'étendue nouvellement ajoutée en cliquant avec le bouton droit sur l'étendue, puis en cliquant sur Configurer un basculement.

Pour fermer cet Assistant, cliquez sur Terminer.

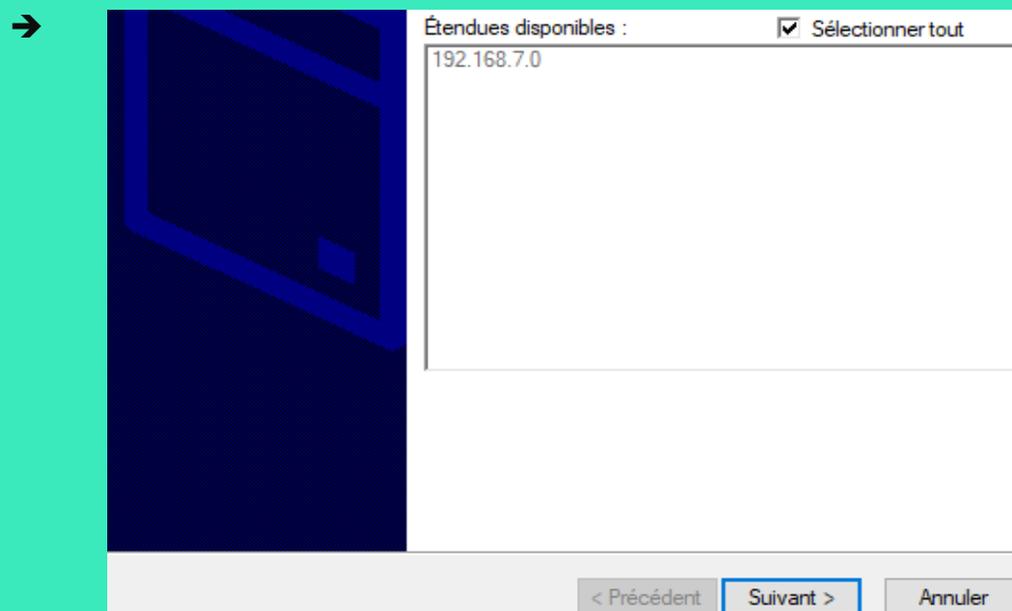
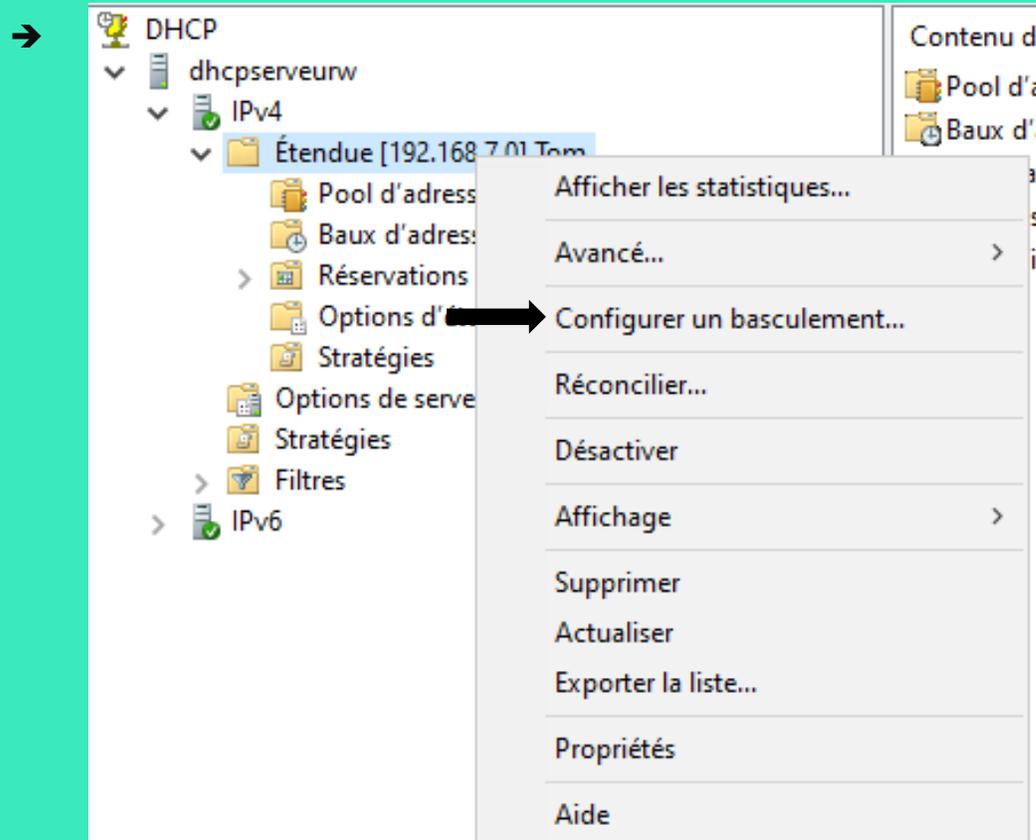
< Précédent

Terminer

Annuler

Mise en place du FailOver

Pour mettre en place un failOver, ouvrez la console DHCP et effectuez un clic droit sur l'étendue, puis cliquez sur "Configurer un basculement" :





Spécifier le serveur partenaire à utiliser pour le basculement



Indiquez le nom d'hôte ou l'adresse IP du serveur DHCP partenaire à utiliser pour la configuration du basculement.

Vous pouvez effectuer votre sélection parmi la liste des serveurs avec une configuration de basculement existant, ou vous pouvez rechercher et sélectionner le serveur approprié dans la liste des serveurs DHCP autorisés.

Vous pouvez également taper le nom d'hôte ou l'adresse IP du serveur partenaire.

Serveur partenaire :

Réutiliser les relations de basculement existantes configurées avec ce serveur (le cas échéant).

< Précédent

Suivant >

Annuler

Ne pas cocher la case pour ne pas avoir le basculement direct avec le serveur.

Saisissez un "Secret partagé" complexe qui sera utilisé pour chiffrer les échanges entre les deux serveurs DHCP du cluster. De cette façon, la synchronisation de la configuration entre les serveurs DHCP ne transitera pas en clair sur le réseau :

→ **Créer une relation de basculement** 

Créer une relation de basculement avec le partenaire 192.168.8.253

Nom de la relation :

Délai de transition maximal du client (MCLT) : heures minutes

Mode :

Configuration du serveur de secours

Rôle du serveur partenaire :

Adresses réservées pour le serveur de secours : %

Intervalle de basculement d'état : minutes

Activer l'authentification du message

Secret partagé :

< Précédent **Suivant >** Annuler

→

Mode :

Configuration du serveur de secours

Rôle du serveur partenaire :

Il faut choisir un mode, dans notre cas le choix "Équilibrage de charge" (load balancing), les deux serveurs seront actifs. Il faut définir le pourcentage de cet équilibrage de charge : 50/50, ou 70/30, par exemple. Cette valeur correspond au pourcentage d'adresses IP de la plage de l'étendue que devra gérer chaque serveur. Par exemple, si dans l'étendue la plage DHCP est de 10 adresses IP et que la répartition est de 50/50, chaque serveur va gérer 5 adresses IP. Le mode "Serveur de secours" (Failover) sert à mettre en place une configuration actif/passif. Ensuite, on choisit le mode "Veille" : le serveur passif distribuera des adresses IP uniquement quand le partenaire sera HS. Il faut en complément préciser le pourcentage d'adresses IP réservées au sein de la plage pour ce serveur de secours. Ainsi, en cas de basculement si le serveur principal est hors service, le serveur de secours est assuré d'avoir X% d'adresses IP disponibles et attribuables (5% garder pour les nouveau client DHCP):



Configuration du serveur de secours
Rôle du serveur partenaire : Veille
Adresses réservées pour le serveur de secours : 5 %

Un basculement va être configuré entre dhcpserveurw et 192.168.8.253 avec les paramètres suivants.

Étendues :
192.168.7.0

n : dhcpserveurw-192.168.8.253
n maximal du client (MCLT) : 1 h 0 min
Serveur de secours
culement d'état : Désactivé

Configuration du serveur de secours
Rôle du serveur partenaire : Veille
Adresses réservées pour le serveur 5 %

< Précédent Terminer Annuler

On peut faire un premier ipconfig/all, on peut remarquer que le serveur DNS est le DHCP en 192.168.7.253 :



```
Carte Ethernet Ethernet :
    Suffixe DNS propre à la connexion. . . : beg-ft-04.prive
    Description. . . . . : Intel(R) PRO/1000 MT Desktop Adapter
    Adresse physique . . . . . : 08-00-27-AD-DA-91
    DHCP activé. . . . . : Oui
    Configuration automatique activée. . . : Oui
    Adresse IPv4. . . . . : 192.168.7.1(préfééré)
    Masque de sous-réseau. . . . . : 255.255.255.0
    Bail obtenu. . . . . : jeudi 12 septembre 2024 15:47:35
    Bail expirant. . . . . : jeudi 12 septembre 2024 16:32:00
    Passerelle par défaut. . . . . : 172.20.2.254
    Serveur DHCP . . . . . : 192.168.7.253
    Serveurs DNS. . . . . : 8.8.8.8
    NetBIOS sur Tcip. . . . . : Activé
```

Puis une fois que nous avons éteint mon serveur DHCP vous pouvez remarquer que le serveur DHCP est passé sur le 192.168.8.253 :



```
Carte Ethernet Ethernet :
    Suffixe DNS propre à la connexion. . . : beg-ft-04.prive
    Description. . . . . : Intel(R) PRO/1000 MT Desktop Adapter
    Adresse physique . . . . . : 08-00-27-AD-DA-91
    DHCP activé. . . . . : Oui
    Configuration automatique activée. . . : Oui
    Adresse IPv4. . . . . : 192.168.7.1(préfééré)
    Masque de sous-réseau. . . . . : 255.255.255.0
    Bail obtenu. . . . . : jeudi 12 septembre 2024 15:47:35
    Bail expirant. . . . . : jeudi 12 septembre 2024 16:33:48
    Passerelle par défaut. . . . . : 172.20.2.254
    Serveur DHCP . . . . . : 192.168.8.253
    Serveurs DNS. . . . . : 8.8.8.8
    NetBIOS sur Tcip. . . . . : Activé
```



Capture en cours de Ethernet

Fichier Editer Vue Aller Capture Analyser Statistiques Telephonie Wireless Outils Aide

dhcp

No.	Time	Source	Destination	Protocol	Length	Info
5623...	1798.983260	0.0.0.0	255.255.255.255	DHCP	324	DHCP Discover - Transaction ID 0x913e6627
5623...	1798.983988	192.168.8.253	255.255.255.255	DHCP	342	DHCP Offer - Transaction ID 0x913e6627
5623...	1798.998383	0.0.0.0	255.255.255.255	DHCP	336	DHCP Request - Transaction ID 0x913e6627
5623...	1798.999409	192.168.8.253	255.255.255.255	DHCP	342	DHCP ACK - Transaction ID 0x913e6627
5900...	2002.385571	192.168.8.253	255.255.255.255	DHCP	290	DHCP Inform - Transaction ID 0x17a10068
5900...	2002.385765	192.168.8.253	255.255.255.255	DHCP	342	DHCP ACK - Transaction ID 0x17a10068
5900...	2002.385765	192.168.8.253	255.255.255.255	DHCP	290	DHCP Inform - Transaction ID 0x17a10068
5900...	2002.386087	192.168.8.253	255.255.255.255	DHCP	342	DHCP ACK - Transaction ID 0x17a10068
5910...	2004.389096	192.168.8.253	255.255.255.255	DHCP	290	DHCP Inform - Transaction ID 0x17a10068
5910...	2004.389250	192.168.8.253	255.255.255.255	DHCP	342	DHCP ACK - Transaction ID 0x17a10068
5910...	2004.391652	192.168.8.253	255.255.255.255	DHCP	290	DHCP Inform - Transaction ID 0x17a10068
5910...	2004.391842	192.168.8.253	255.255.255.255	DHCP	342	DHCP ACK - Transaction ID 0x17a10068

No.	Time	Source	Destination	Protocol	Length	Info
1	14:31:47,680494	192.168.7.2	224.0.0.251	MDNS	75	Standard query response 0x0000 A 192.168.7.2
2	14:33:01,109951	192.168.7.2	192.168.7.2	ICMP	101	Destination unreachable (Host unreachable)
3	14:33:05,118141	192.168.7.2	192.168.7.2	ICMP	101	Destination unreachable (Host unreachable)
4	14:33:09,110588	192.168.7.2	192.168.7.2	ICMP	145	Destination unreachable (Host unreachable)

Éditée par	Tom COELHO	
Révisée par :	Tom COELHO	
Suivie par :	Tom COELHO	
Validée par :	Tom COELHO	
Date : 3 / 01 / 2023		Version : 1