PortailSIO

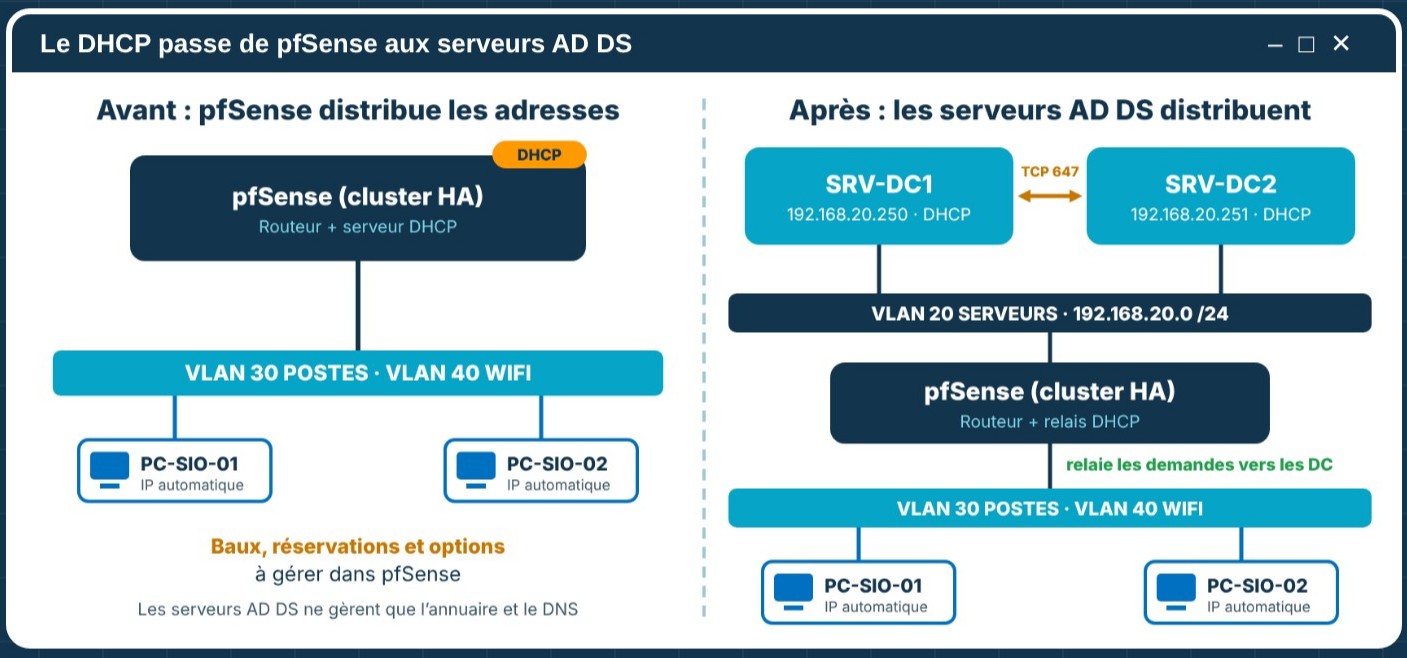
NOUVELLE FORMULE

TUTORIEL

PFSENSE · WINDOWS SERVER 2025

Migrer le DHCP de pfSense vers AD/DS





1. Préparer la migration
2. Créer les étendues sur les serveurs Windows
3. Préparer le pare-feu pfSense
4. Basculer : relais DHCP et haute disponibilité
5. Tester et prévoir le retour arrière

CC BY-NC
Utilisation commerciale interdite
© PortailSIO – 11/2026

Ce tutoriel en ligne

Scannez le QR code. Tous les tutoriels :

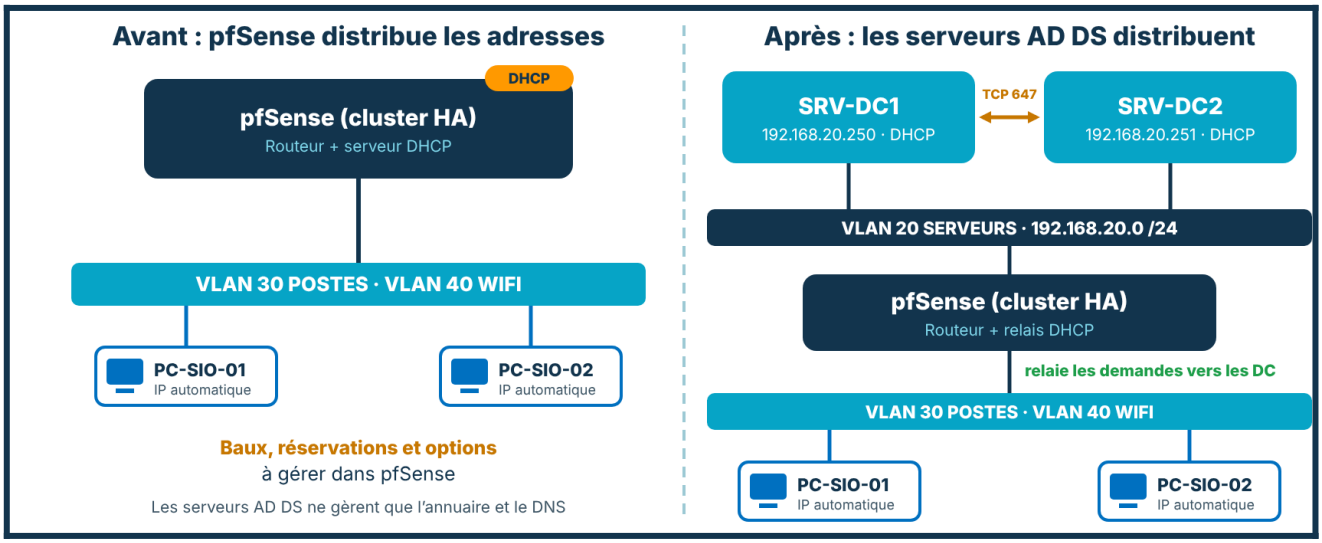
portail.sio-ndlp.fr/tutoriels.php

Ce tutoriel a été réalisé avec l'hyperviseur © Proxmox VE. Il peut être réalisé dans un environnement de virtualisation personnel à l'aide des logiciels © VirtualBox ou © VMware Player et **suppose que vous avez réalisé les tutoriels précédents** : réplication AD DS (**SRV-DC1** et **SRV-DC2**), mise en place du serveur DHCP et **réplication DHCP** (relation de basculement SRV-DC1-SRV-DC2). Il suppose aussi que vous disposez d'un **cluster pfSense en haute disponibilité** (CARP) qui route les VLAN 20 (SERVEURS), 30 (POSTES) et 40 (WIFI).

Jusqu'ici, c'est le pare-feu **pfSense** qui distribue les adresses IP aux postes (VLAN 30) et au Wi-Fi (VLAN 40). Cela fonctionne, mais la gestion des adresses est alors **séparée de l'annuaire** : baux, réservations et options se gèrent dans l'interface de pfSense, alors que les deux serveurs AD DS, pourtant redondants, ne servent pas à distribuer les adresses.

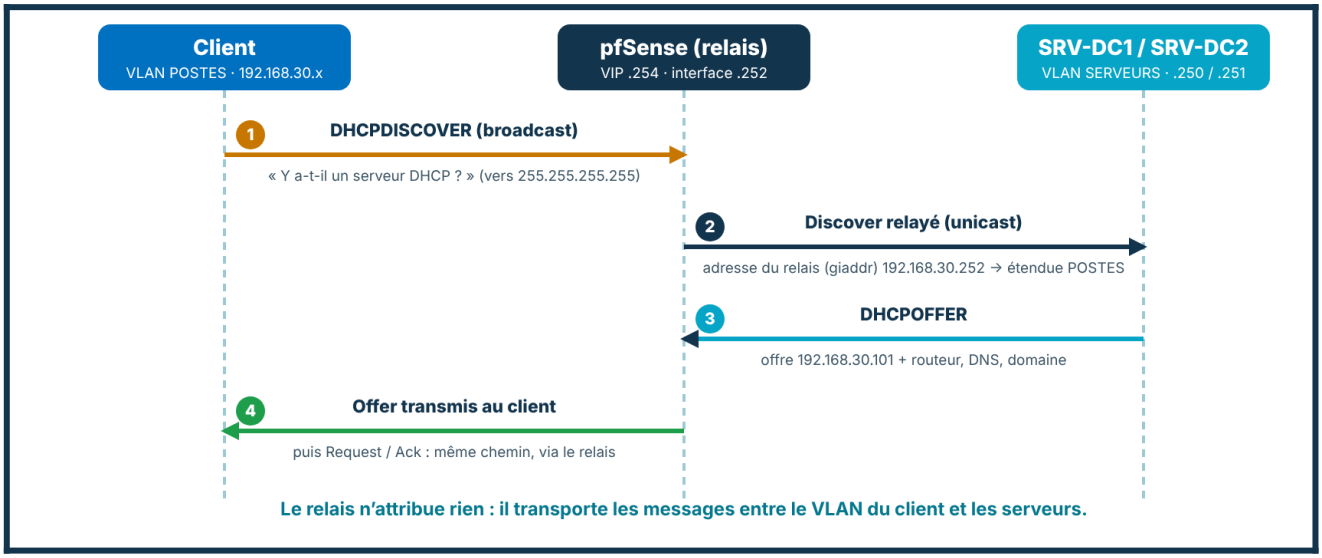
Dans un domaine Active Directory, on confie généralement le DHCP aux **serveurs Windows** : ils sont déjà en basculement, autorisés dans l'annuaire, et les étendues, réservations et options se gèrent au même endroit que le DNS. Il reste un obstacle : les clients des VLAN 30 et 40 ne sont pas dans le même réseau que les serveurs, et **une demande DHCP est un message de diffusion (broadcast) qui ne traverse pas le routeur**. C'est le rôle du **relais DHCP** de pfSense.

Voici la situation avant et après la migration :



Le principe du relais DHCP

- Le client émet un **DHCPDISCOVER en broadcast** : il reste dans son VLAN
- Le **relais DHCP** de pfSense (service `dhcrelay`) écoute dans ce VLAN et **retransmet la demande en unicast** aux serveurs Windows, en y ajoutant sa propre adresse dans le VLAN du client (champ **giaddr**)
- Le serveur Windows utilise cette adresse pour **choisir l'étendue** correspondante (192.168.30.0 pour le VLAN 30), puis répond au relais, qui transmet la réponse au client
- Le relais **n'attribue aucune adresse** : tout est géré par les serveurs DHCP



REMARQUE IMPORTANTE

pfSense ne peut pas être serveur DHCP et relais DHCP en même temps : il faut d'abord désactiver le serveur DHCP sur **toutes** les interfaces, puis activer le relais. Les clients ne peuvent donc plus obtenir d'adresse pendant quelques minutes : réalisez la bascule (étape 4) pendant une plage sans cours et conservez une sauvegarde de la configuration de pfSense.

Dans le cadre de ce tutoriel, nous utilisons le plan d'adressage suivant (adresses des nœuds pfSense : PFS-1 en .252, PFS-2 en .253) :

VLAN	Réseau	Nœuds pfSense	Passerelle (VIP CARP)	DHCP avant	DHCP après
20 SERVEURS	192.168.20.0 /24	.252 / .253	.254	SRV-DC1 / SRV-DC2 (étendue LAN-SIO)	Inchangé
30 POSTES	192.168.30.0 /24	.252 / .253	.254	pfSense	SRV-DC1 / SRV-DC2 via le relais
40 WIFI	192.168.40.0 /24	.252 / .253	.254	pfSense	SRV-DC1 / SRV-DC2 via le relais

Ces valeurs sont données à titre d'exemple : adaptez-les à votre plan d'adressage. L'interface de pfSense est en anglais : les noms des menus et des champs sont donnés tels qu'ils s'affichent.

01

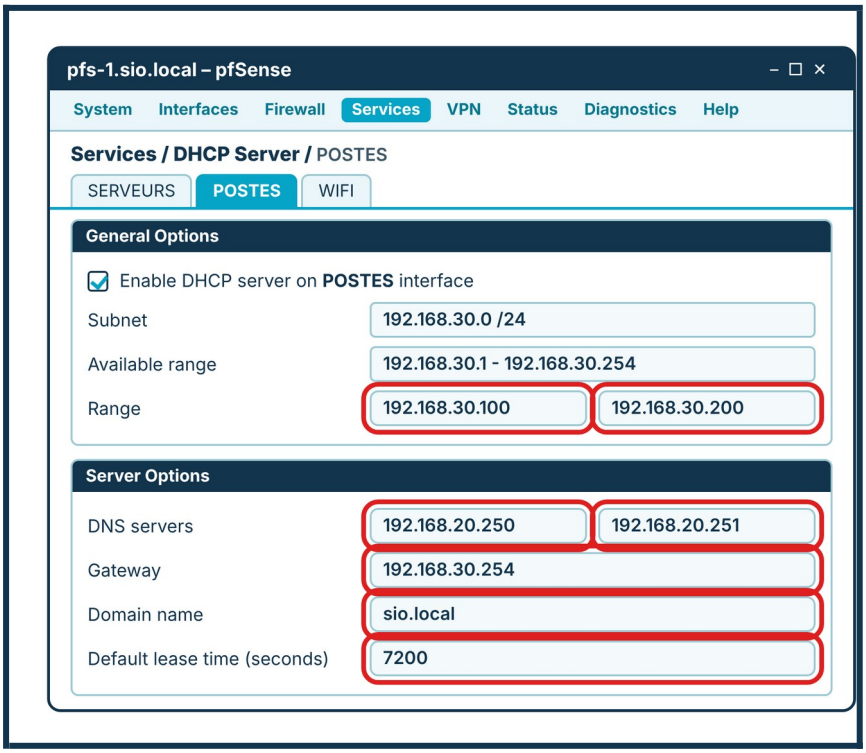
ÉTAPE 1 SUR 5

Préparer la migration

Avant de modifier quoi que ce soit, **sauvegardez** la configuration de pfSense et **relevez** les paramètres DHCP actuels : ils serviront à recréer les étendues sur les serveurs Windows. Connectez-vous à l'interface web du nœud maître **PFS-1** puis effectuez les manipulations suivantes :

1. Cliquez le menu « **Diagnostics** » puis « **Backup & Restore** », laissez « **Backup area** » sur « **All** » et cliquez « **Download configuration as XML** » : conservez le fichier téléchargé en lieu sûr
2. Cliquez le menu « **Services** » puis « **DHCP Server** » et choisissez l'onglet de l'interface **POSTES**

3 Notez, dans « **General Options** », la plage (« **Range** ») et, dans « **Server Options** », les serveurs DNS, la passerelle (« **Gateway** »), le nom de domaine et la durée du bail (« **Default lease time** ») :

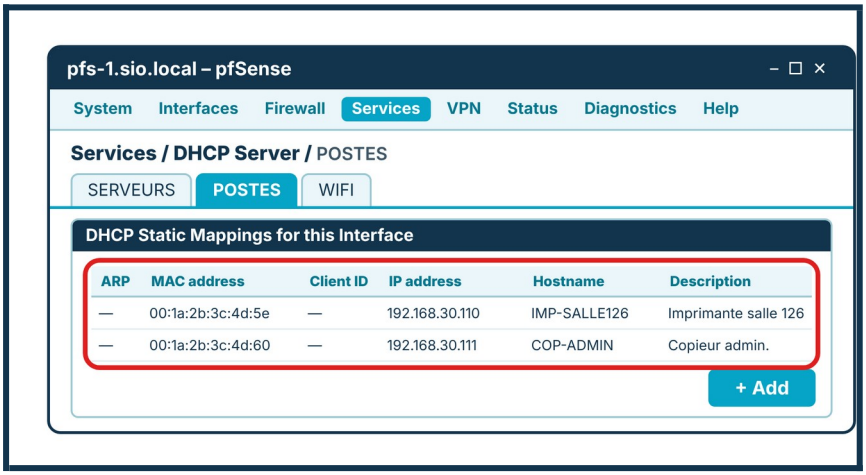


À SAVOIR

Si le champ « Gateway » est vide, pfSense distribue sa propre adresse comme passerelle. Sur un cluster, relevez l'adresse virtuelle CARP (ici .254) : c'est celle que les clients doivent utiliser.

Figure 1 – Services > DHCP Server > POSTES : paramètres à relever

4 Descendez jusqu'à « **DHCP Static Mappings for this Interface** » et notez chaque **réservation** (adresse MAC, adresse IP, nom d'hôte) :



À SAVOIR

Ces réservations seront recréées sur les serveurs Windows (nœud « Réservations » de l'étendue). Si elles sont nombreuses, recopiez-les depuis la sauvegarde XML dans un tableur.

Figure 2 – Réservations statiques de l'interface POSTES

5 Répétez ces relevés pour l'interface **WIFI** (et pour toute autre interface où pfSense distribue des adresses)

Les paramètres de pfSense correspondent à ceux du serveur DHCP Windows de la façon suivante :

pfSense (Services > DHCP Server)	Serveur DHCP Windows	Remarque
Range	Pool d'adresses de l'étendue (début et fin)	Gardez la même plage
Gateway	Option 003 « Routeur »	Adresse virtuelle CARP du VLAN (.254)
DNS servers	Option 006 « Serveurs DNS »	Les deux contrôleurs de domaine
Domain name	Option 015 « Nom de domaine DNS »	sio.local
Default lease time	Durée du bail	Valeur par défaut de Windows : 8 jours
DHCP Static Mappings	Réservations	Une réservation par adresse MAC

À SAVOIR

Dans un réseau en production, **réduisez la durée du bail la veille** de la migration (par exemple 1 heure dans pfSense) : après la bascule, tous les clients renouvelleront rapidement leur bail auprès des serveurs Windows.

Sur **SRV-DC1**, vérifiez que la relation de basculement créée dans le tutoriel précédent est à l'état « Normal » :

POWERSHELL

```
Get-DhcpServerv4Failover | Select-Object Name, Mode, State, ScopeId
```

✔ **POINT DE CONTRÔLE**

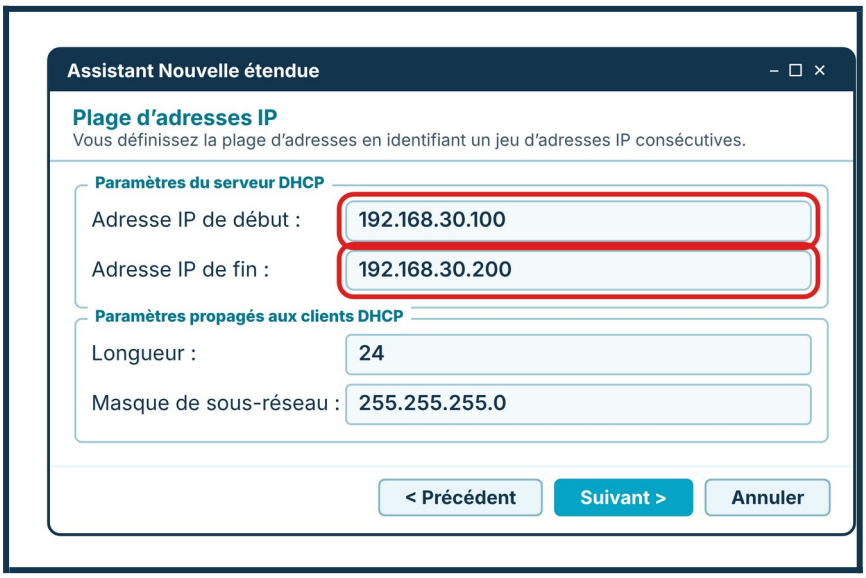
- La configuration de pfSense est **sauvegardée** (fichier XML téléchargé)
- Les plages, options et réservations des interfaces **POSTES** et **WIFI** sont relevées
- La relation **SRV-DC1-SRV-DC2** est à l'état « **Normal** »

02 ÉTAPE 2 SUR 5 — Créer les étendues sur les serveurs Windows

Les étendues se créent **uniquement sur SRV-DC1** ; elles seront ensuite ajoutées à la relation de basculement existante, qui les copiera automatiquement sur SRV-DC2. Ouvrez une session sur **SRV-DC1** avec le compte `SIO\Administrateur` :

1. Dans le « **Gestionnaire de serveur** », cliquez le menu « **Outils** » puis « **DHCP** »
2. Développez « **srv-dc1.sio.local** », faites un clic droit sur « **IPv4** » puis cliquez « **Nouvelle étendue...** » ; cliquez « **Suivant** » sur la page de bienvenue
3. Page « **Nom de l'étendue** » : saisissez `POSTES` (description : `VLAN 30 - postes du labo`) puis cliquez « **Suivant** »

4 Page « **Plage d'adresses IP** » : saisissez l'adresse de début `192.168.30.100`, l'adresse de fin `192.168.30.200` et la longueur `24` :



À SAVOIR

Utilisez exactement la plage relevée dans pfSense. La longueur 24 donne automatiquement le masque 255.255.255.0.

Figure 3 – Assistant « Nouvelle étendue » : plage d'adresses de l'étendue POSTES

5 Page « **Ajout d'exclusions et de retard** » : ne saisissez rien puis cliquez « **Suivant** » ; page « **Durée du bail** » : conservez **8 jours** puis cliquez « **Suivant** »

6 Page « **Configuration des paramètres DHCP** » : choisissez « **Oui, je veux configurer ces options maintenant** » puis cliquez « **Suivant** »

7 Page « **Routeur (passerelle par défaut)** » : saisissez `192.168.30.254` (l'**adresse virtuelle CARP** de pfSense) puis cliquez « **Ajouter** » et « **Suivant** »

8 Page « **Nom de domaine et serveurs DNS** » : domaine parent `sio.local` ; ajoutez les serveurs `192.168.20.250` et `192.168.20.251` puis cliquez « **Suivant** »

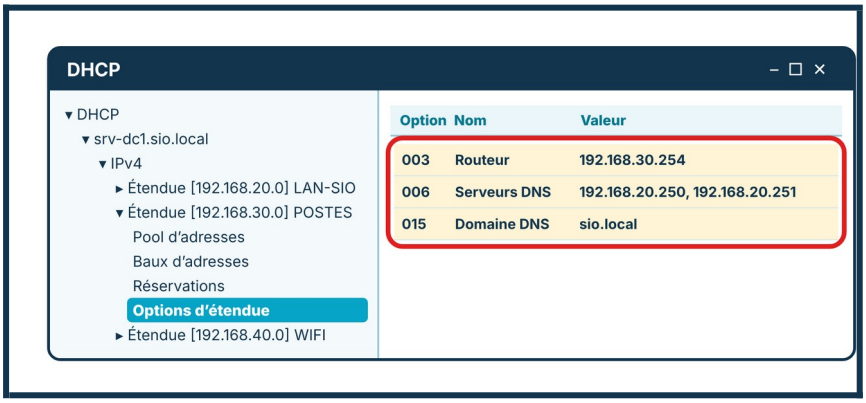
9 Page « **Serveurs WINS** » : cliquez « **Suivant** » sans rien saisir ; page « **Activer l'étendue** » : choisissez « **Oui, je veux activer cette étendue maintenant** » puis cliquez « **Suivant** » et « **Terminer** »

REMARQUE IMPORTANTE

Les clients doivent utiliser l'**adresse virtuelle CARP** (.254) comme passerelle : elle passe d'un pare-feu à l'autre sans que les clients s'en aperçoivent. Ne saisissez jamais l'adresse d'un nœud (.252 ou .253) : elle deviendrait inutilisable en cas de panne de ce nœud.

10 Répétez la création pour le VLAN WIFI : nom `WIFI`, plage `192.168.40.100` à `192.168.40.200`, routeur `192.168.40.254`, mêmes serveurs DNS et même domaine, durée du bail de **1 heure** (clients mobiles)

11 Déroulez chaque nouvelle étendue et cliquez « **Options d'étendue** » pour vérifier les options 003, 006 et 015 :



À SAVOIR

L'option 006 doit contenir les deux contrôleurs de domaine. Si elle est vide, les clients n'ont pas de DNS et ne peuvent pas joindre le domaine.

Figure 4 – Console DHCP de SRV-DC1 : options de l'étendue POSTES

12 Pour chaque réservation relevée à l'étape 1 : clic droit sur « **Réservations** » puis « **Nouvelle réservation…** » ; saisissez le nom, l'adresse IP et l'adresse MAC (sans tirets) puis cliquez « **Ajouter** »

Les mêmes opérations en PowerShell, à exécuter sur SRV-DC1 :

POWERSHELL

```
# Étendue POSTES (VLAN 30)
Add-DhcpServerv4Scope -Name "POSTES" -State Active `
    -StartRange 192.168.30.100 -EndRange 192.168.30.200 `
    -SubnetMask 255.255.255.0 -LeaseDuration 8.00:00:00
Set-DhcpServerv4OptionValue -ScopeId 192.168.30.0 -Router 192.168.30.254 `
    -DnsServer 192.168.20.250,192.168.20.251 -DnsDomain sio.local
Add-DhcpServerv4Reservation -ScopeId 192.168.30.0 -IPAddress 192.168.30.110 `
    -ClientId "00-1A-2B-3C-4D-5E" -Name "IMP-SALLE126" `
    -Description "Imprimante salle 126"

# Étendue WIFI (VLAN 40)
Add-DhcpServerv4Scope -Name "WIFI" -State Active `
    -StartRange 192.168.40.100 -EndRange 192.168.40.200 `
    -SubnetMask 255.255.255.0 -LeaseDuration 01:00:00
Set-DhcpServerv4OptionValue -ScopeId 192.168.40.0 -Router 192.168.40.254 `
    -DnsServer 192.168.20.250,192.168.20.251 -DnsDomain sio.local
```

Ajouter les étendues à la relation de basculement

Les étendues POSTES et WIFI ne sont pas encore protégées : si SRV-DC1 tombe, elles ne répondent plus. Ajoutons-les à la relation **SRV-DC1-SRV-DC2** créée dans le tutoriel précédent :

1 Faites un clic droit sur « **IPv4** » puis cliquez « **Configurer un basculement…** »

2 Page « **Présentation du basculement DHCP** » : cochez les étendues **192.168.30.0** et **192.168.40.0** puis cliquez « **Suivant** » :



Figure 5 – Assistant « Configurer un basculement » : sélection des nouvelles étendues

À SAVOIR

Seules les nouvelles étendues sont à cocher : l'étendue LAN-SIO (192.168.20.0) est déjà protégée par la relation.

3 Page « **Spécifier le serveur partenaire** » : saisissez `srv-dc2.sio.local` et cochez « **Réutiliser les relations de basculement existantes avec ce serveur partenaire** » puis cliquez « **Suivant** » :

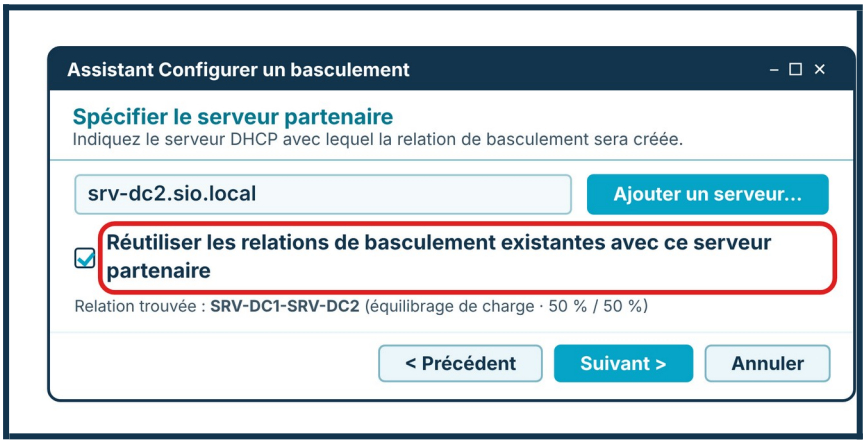


Figure 6 – Assistant « Configurer un basculement » : réutilisation de la relation existante

À SAVOIR

Sans cette case, l'assistant créerait une seconde relation (nouveau nom, mode et secret partagé). Avec elle, les nouvelles étendues rejoignent la relation existante et reprennent son mode.

4 Cliquez « **Suivant** » puis « **Terminer** » ; patientez et cliquez « **Fermer** » quand toutes les étapes sont « **Réussi** »

La même opération en PowerShell :

POWERSHELL

```
Add-DhcpServerv4FailoverScope -Name "SRV-DC1-SRV-DC2" -ScopeId 192.168.30.0,192.168.40.0
Get-DhcpServerv4Failover -Name "SRV-DC1-SRV-DC2" | Select-Object Name, Mode, State,
ScopeId
```

REMARQUE IMPORTANTE

Ne créez pas les étendues à la main sur SRV-DC2 : elles y sont copiées automatiquement, avec leurs options et leurs réservations, par la relation de basculement.

✔ POINT DE CONTRÔLE

- `Get-DhcpServerv4Failover` affiche les trois étendues **192.168.20.0**, **192.168.30.0** et **192.168.40.0**
- Dans la console DHCP de **SRV-DC2**, les étendues POSTES et WIFI sont apparues, avec leurs options et leurs réservations
- Rien n'a changé pour les clients : sans relais, aucune demande des VLAN 30 et 40 n'arrive encore aux serveurs Windows

03 ÉTAPE 3 SUR 5 Préparer le pare-feu pfSense

Les règles de pare-feu se créent **avant** la bascule : elles n'ont aucun effet tant que le relais n'est pas actif. Elles seront copiées automatiquement sur PFS-2 par la synchronisation HA (étape suivante). On commence par un **alias** regroupant les deux serveurs DHCP. Sur **PFS-1** :

1. Cliquez le menu « **Firewall** » puis « **Aliases** », onglet « **IP** » puis bouton « **Add** »
2. Saisissez le nom `DHCP_SERVERS` et une description, laissez le type « **Host(s)** » et ajoutez les adresses `192.168.20.250` et `192.168.20.251` (bouton « **Add Host** ») :

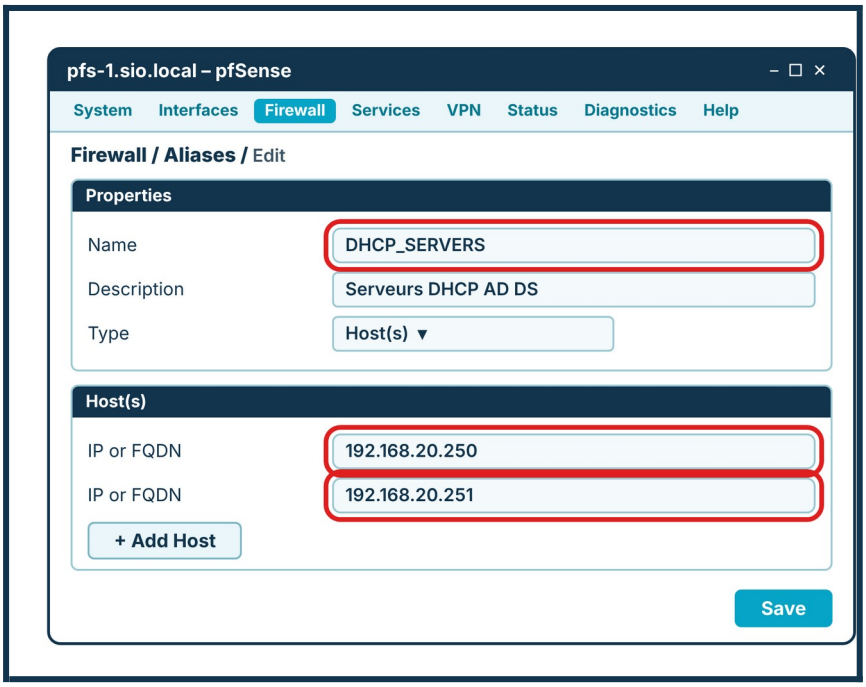


Figure 7 – Firewall > Aliases : alias DHCP_SERVERS

À SAVOIR

Un alias évite de répéter les deux adresses dans chaque règle : si un serveur DHCP change d'adresse, on ne modifie qu'un seul endroit.

3. Cliquez « **Save** » puis « **Apply Changes** »
4. Cliquez le menu « **Firewall** » puis « **Rules** », onglet **POSTES**, et le bouton « **Add** » avec la flèche vers le haut (la règle est placée en tête de liste)

5 Renseignez « **Action** » `Pass`, « **Protocol** » `UDP`, « **Source** » `Any` avec « **Source port range** » de `BOOTPC (68)` à `BOOTPC (68)`, « **Destination** » `DHCP_SERVERS` avec « **Destination port range** » de `BOOTPS (67)` à `BOOTPS (67)`, et une description :

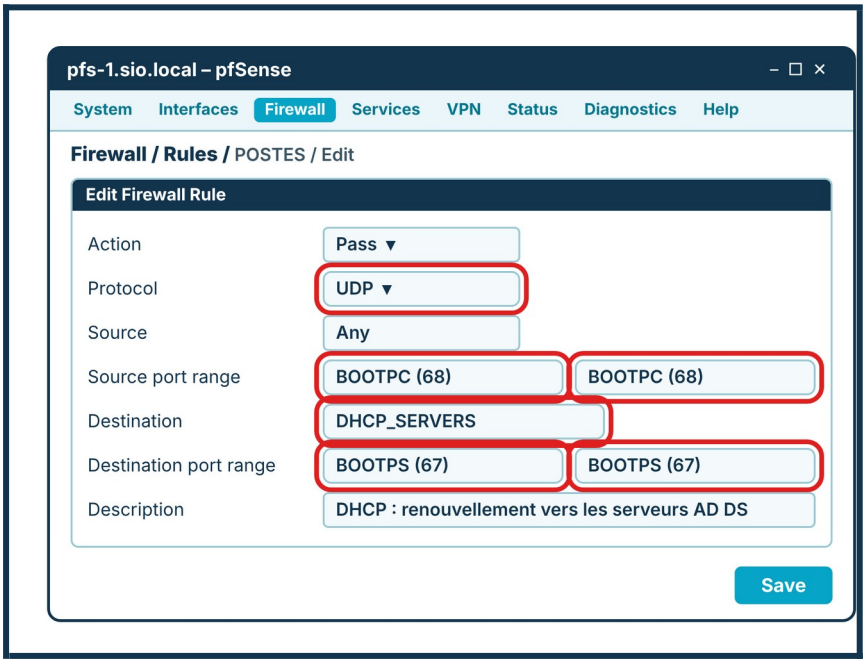


Figure 8 – Firewall > Rules > POSTES : règle UDP 68 vers les serveurs DHCP

À SAVOIR

À mi-bail, un client renouvelle son adresse en unicast, directement auprès du serveur DHCP et sans passer par le relais. Sans cette règle, le renouvellement est bloqué : le client doit attendre 87,5 % du bail pour redemander en broadcast.

6 Cliquez « **Save** », vérifiez que la règle est **au-dessus** d'éventuelles règles de blocage puis cliquez « **Apply Changes** »

7 Copiez la règle pour l'interface **WIFI** (icône « **Copy** » puis choix de l'interface) ou recréez-la à l'identique

À SAVOIR

Les demandes relayées sont émises par pfSense lui-même, et pfSense autorise automatiquement les broadcasts DHCP des clients (UDP 68 vers 67) sur une interface qui utilise le relais : seule la règle ci-dessus est à ajouter.

✔ **POINT DE CONTRÔLE**

- L'alias `DHCP_SERVERS` existe et contient les deux serveurs
- Une règle **UDP 68 vers 67** est présente sur **POSTES** et **WIFI**
- Les modifications ont été appliquées (« Apply Changes »)

04 ÉTAPE 4 SUR 5 Basculer : relais DHCP et haute disponibilité

REMARQUE IMPORTANTE

Les clients ne peuvent plus obtenir d'adresse entre la désactivation du serveur DHCP et l'activation du relais : préparez les deux écrans, enchaînez les manipulations (quelques minutes) et vérifiez que la sauvegarde de l'étape 1 est faite.

A – Désactiver le serveur DHCP de pfSense

1. Cliquez le menu « **Services** » puis « **DHCP Server** », onglet **POSTES** : décochez « **Enable DHCP server on POSTES interface** » puis cliquez « **Save** » :

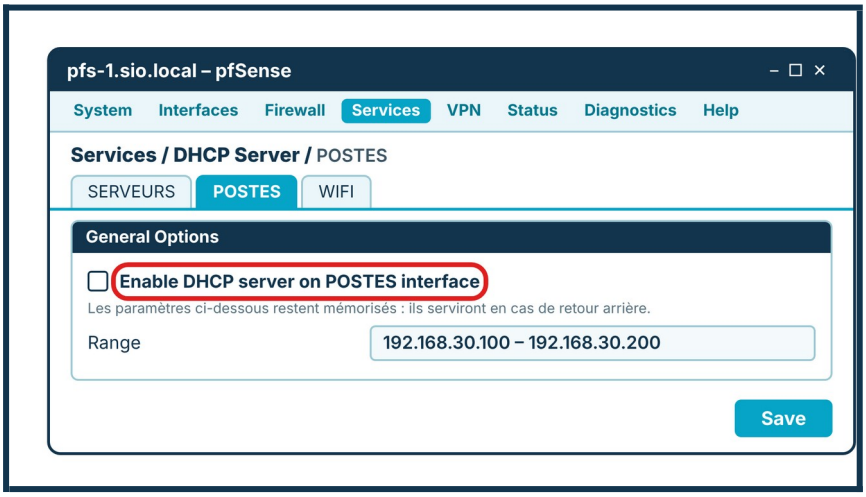


Figure 9 – Services > DHCP Server > POSTES : serveur DHCP désactivé

À SAVOIR

Ne supprimez rien : les paramètres restent enregistrés dans pfSense. En cas de problème, il suffit de recocher la case pour revenir en arrière.

2. Faites de même dans l'onglet **WIFI**, puis dans **tous les autres onglets** où la case est cochée

B – Activer le relais DHCP

1. Cliquez le menu « **Services** » puis « **DHCP Relay** » et cochez « **Enable** DHCP Relay on interface »
2. Dans « **Downstream Interfaces** », sélectionnez **POSTES** et **WIFI** (touche **Ctrl** maintenue pour sélectionner les deux) : ce sont les interfaces où se trouvent les clients
3. Dans « **CARP Status VIP** », choisissez l'adresse virtuelle de POSTES (`192.168.30.254`) : le relais ne fonctionnera que sur le nœud qui est « **MASTER** »
4. Laissez « **Append circuit ID and agent ID to requests** » décoché (inutile avec Windows Server)
5. Dans « **Upstream Servers** », saisissez `192.168.20.250`, cliquez « **Add Upstream Server** » puis saisissez `192.168.20.251`

6 Cliquez « **Save** » :

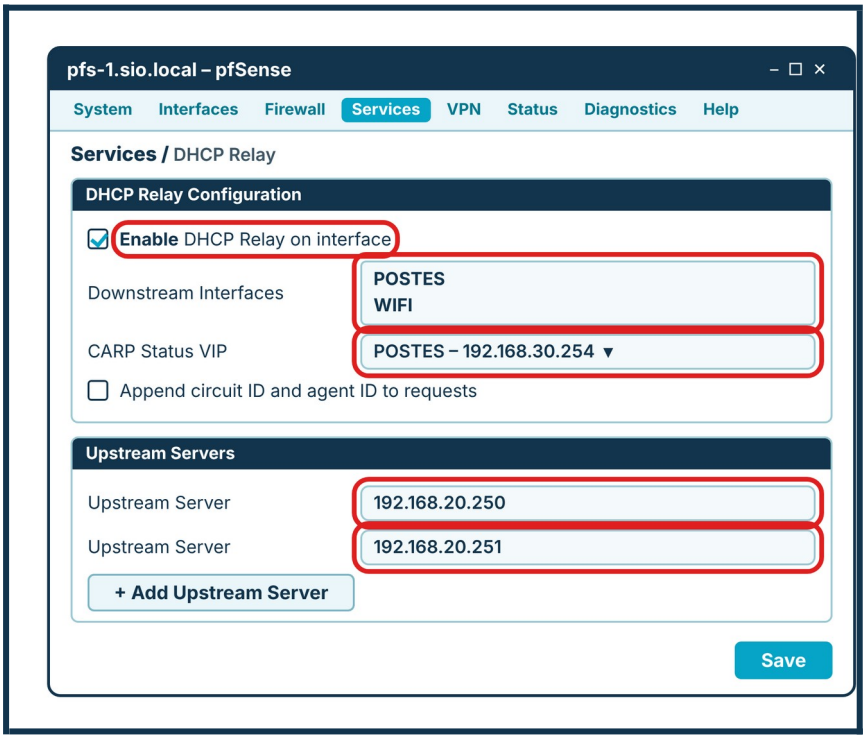


Figure 10 – Services > DHCP Relay : relais vers SRV-DC1 et SRV-DC2

À SAVOIR

Les demandes sont envoyées aux deux serveurs. En équilibrage de charge, un seul répond à chaque client (selon son adresse MAC) ; si l'un est arrêté, l'autre répond.

REMARQUE IMPORTANTE

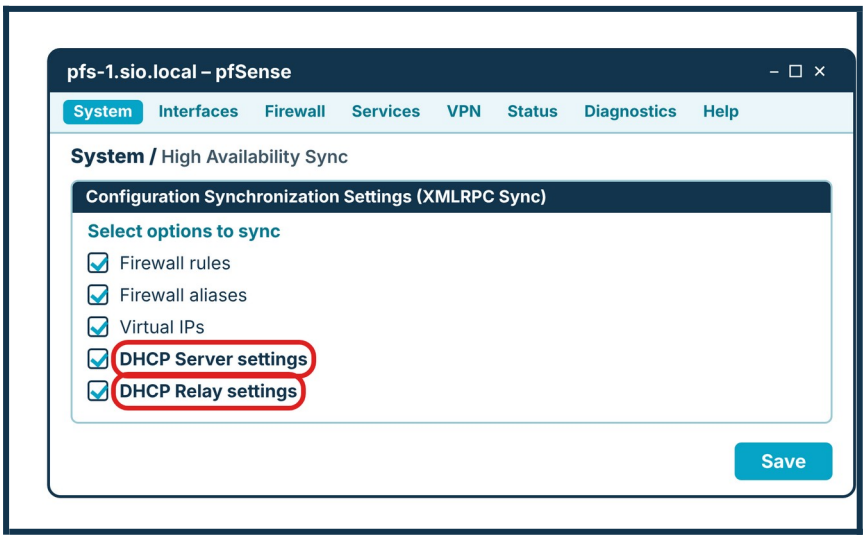
Si pfSense refuse d'activer le relais en signalant que le serveur DHCP est activé, il reste un serveur DHCP actif sur une interface (même inutilisée) : repérez-la dans « Services > DHCP Server » et décochez-la.

C – Synchroniser le cluster

Le relais doit être configuré à l'identique sur les deux nœuds, sinon la bascule CARP laisserait les clients sans DHCP :

1 Sur PFS-1, cliquez le menu « **System** » puis « **High Availability Sync** »

2 Dans « **Select options to sync** », vérifiez que « **DHCP Server settings** » et « **DHCP Relay settings** » sont cochés (ainsi que « **Firewall rules** », « **Firewall aliases** » et « **Virtual IPs** ») puis cliquez « **Save** » :



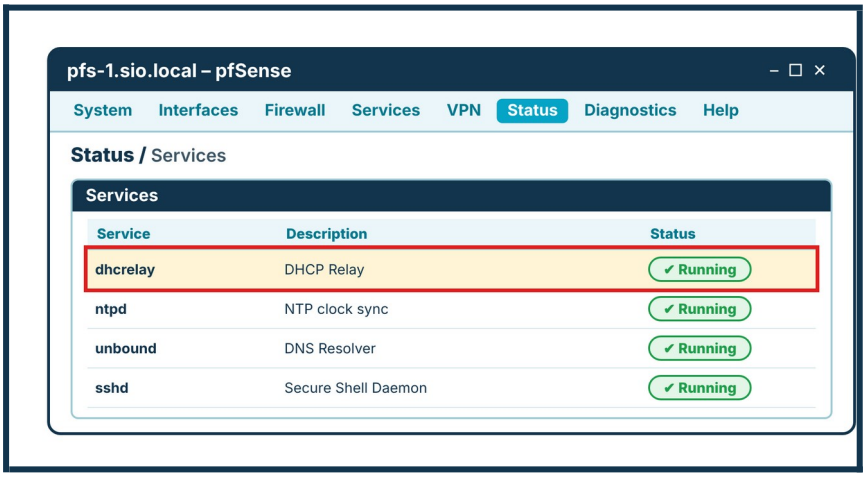
À SAVOIR

« DHCP Server settings » est indispensable : il transmet à PFS-2 la désactivation du serveur DHCP. Sans lui, PFS-2 garderait un serveur DHCP actif, incompatible avec le relais.

Figure 11 – System > High Availability Sync : options de synchronisation

3 Les paramètres sont envoyés à PFS-2 à l'enregistrement. Connectez-vous à **PFS-2** et vérifiez, dans « **Services > DHCP Relay** », que la configuration est identique

4 Sur PFS-1, cliquez « **Status** » puis « **Services** » : le service « **dhcrelay** » doit être « **Running** » :

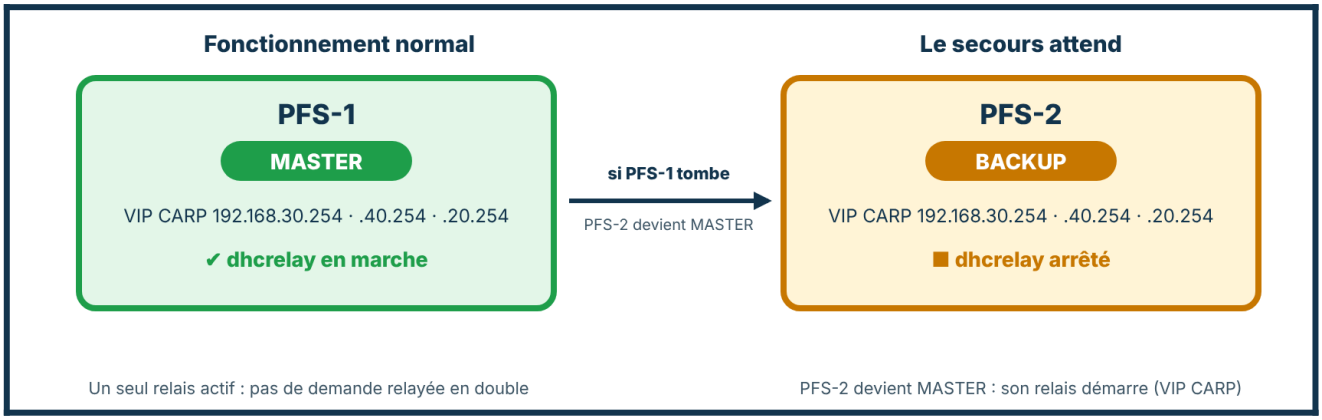


À SAVOIR

Sur PFS-2 (état BACKUP), le service dhcrelay est arrêté : c'est normal, il ne démarre que sur le nœud MASTER.

Figure 12 – Status > Services : service dhcrelay en marche sur PFS-1

Le relais ne fonctionne que sur le nœud « MASTER » du cluster, ce qui évite de relayer chaque demande en double :



✔ POINT DE CONTRÔLE

- Le serveur DHCP de pfSense est **désactivé sur toutes les interfaces**
- Le service `dhcrelay` est « **Running** » sur PFS-1 et la configuration du relais est identique sur PFS-2
- Les deux serveurs Windows sont déclarés comme « **Upstream Servers** »

05 ÉTAPE 5 SUR 5 — Tester et prévoir le retour arrière

A – Test sur un client du VLAN POSTES

Sur un poste Windows 11 du VLAN 30 (adressage automatique), ouvrez une invite de commandes :

1. Saisissez `ipconfig /release`, puis `ipconfig /renew`, puis `ipconfig /all`
2. Contrôlez l'adresse (plage .100 à .200), la passerelle (VIP CARP), les serveurs DNS (les deux contrôleurs de domaine) et surtout « **Serveur DHCP** » : ce doit être l'adresse d'un serveur **Windows** (192.168.20.250 ou .251) et non plus celle de pfSense :

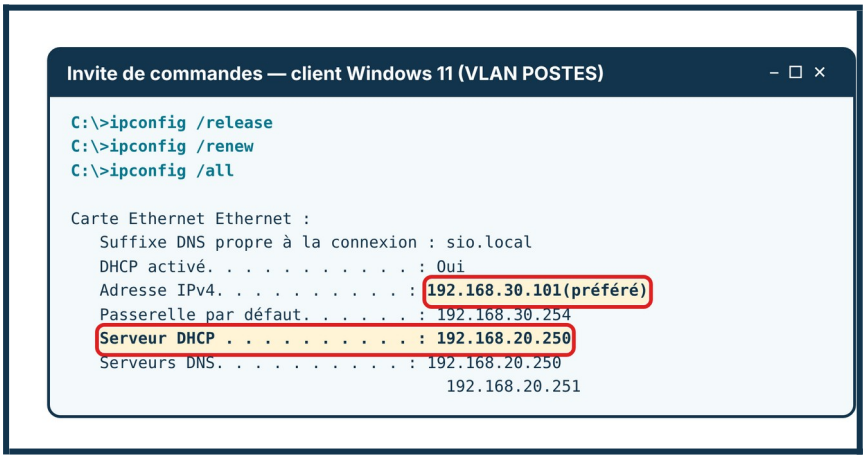


Figure 13 – Invite de commandes du client : bail obtenu auprès d'un serveur Windows

À SAVOIR

Si le client reste en 169.254.x.x, la demande n'aboutit pas : consultez le tableau de dépannage en fin de tutoriel.

B – Contrôle sur les serveurs Windows

1. Dans la console DHCP de **SRV-DC2**, développez l'étendue « **POSTES** » puis cliquez « **Baux d'adresses** » : le bail du client apparaît, même s'il a été accordé par SRV-DC1 (réplication du basculement) :

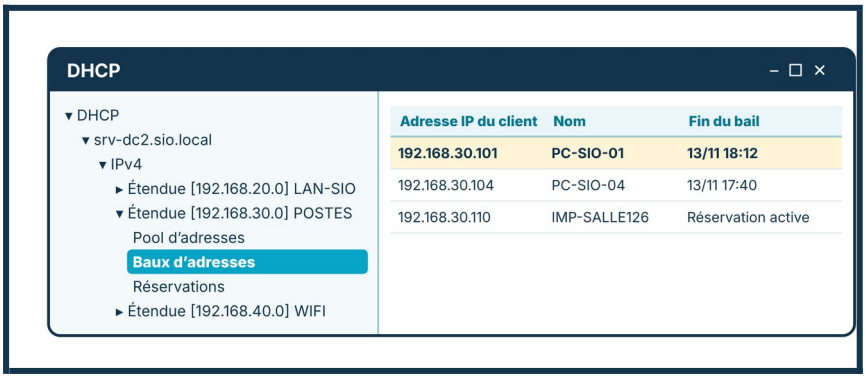


Figure 14 – Console DHCP de SRV-DC2 : baux de l'étendue POSTES

À SAVOIR

La présence du bail sur les deux serveurs prouve que la relation de basculement protège bien les nouvelles étendues.

En PowerShell :

```powershell
Get-DhcpServerv4Lease -ComputerName "srv-dc2.sio.local" -ScopeId 192.168.30.0
```

C – Test de la bascule CARP du pare-feu

1. Sur PFS-1, cliquez « **Status** » puis « **CARP (failover)** » et cliquez « **Enter Persistent CARP Maintenance Mode** » : PFS-2 devient « **MASTER** » :

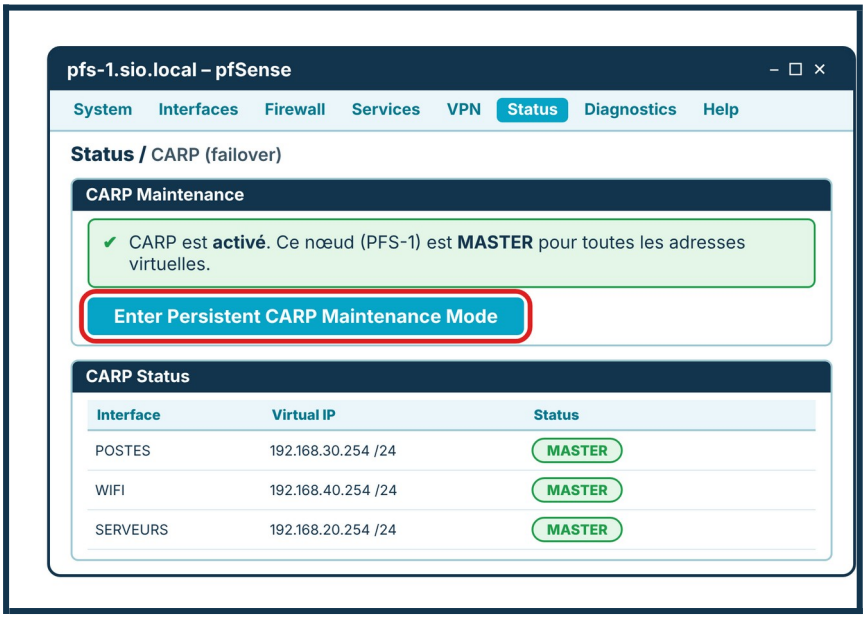


Figure 15 – Status > CARP (failover) : mode maintenance sur PFS-1

À SAVOIR

Le mode maintenance simule la panne de PFS-1 sans l'éteindre : les adresses virtuelles passent sur PFS-2, où le service dhcrelay démarre.

2. Sur PFS-2, vérifiez dans « **Status > Services** » que « **dhcrelay** » est « **Running** »
3. Sur le client, refaites `ipconfig /release` puis `ipconfig /renew` : l'adresse est obtenue normalement
4. Sur PFS-1, cliquez « **Leave Persistent CARP Maintenance Mode** » pour revenir à la situation normale

D – Test de la panne d'un serveur DHCP

1. Sur **SRV-DC1**, arrêtez le service DHCP : `Stop-Service dhcpserver`
2. Sur le client, refaites `ipconfig /release` puis `ipconfig /renew` : SRV-DC2 répond (« Serveur DHCP » = 192.168.20.251)
3. Sur SRV-DC1, redémarrez le service : `Start-Service dhcpserver`

✔ POINT DE CONTRÔLE

- Les clients des VLAN **POSTES** et **WIFI** obtiennent une adresse d'un serveur **Windows**
- Le bail est visible sur **les deux** serveurs DHCP
- Le client obtient une adresse **pendant la bascule CARP** de pfSense
- Le client obtient une adresse alors qu'**un seul serveur DHCP** est en marche

E – Retour arrière

En cas de problème, revenez au fonctionnement précédent :

1. Sur PFS-1, ouvrez « **Services > DHCP Relay** », décochez « **Enable** » puis cliquez « **Save** » : le relais doit être arrêté **avant** de réactiver le serveur DHCP
2. Dans « **Services > DHCP Server** », recochez « **Enable DHCP server** » sur chaque interface (POSTES, WIFI…) puis cliquez « **Save** » : les paramètres d'origine ont été conservés
3. Vérifiez que la synchronisation HA a transmis ces changements à PFS-2, puis faites `ipconfig /renew` sur les clients
4. Pour éviter toute confusion, désactivez les étendues Windows tant que la migration n'est pas reprise : `Set-DhcpServerv4Scope -ScopeId 192.168.30.0 -State InActive`

En dernier recours, restaurez le fichier XML sauvegardé à l'étape 1 (« **Diagnostics > Backup & Restore** », rubrique « **Restore Backup** ») : pfSense redémarre avec la configuration d'origine.

Notre réseau est maintenant **centralisé sur les serveurs AD DS** : pfSense route et relaie les demandes, les deux serveurs Windows distribuent les adresses en basculement, et la panne d'un pare-feu ou d'un serveur DHCP n'interrompt plus la distribution des adresses.

Dépannage : les symptômes les plus fréquents

Symptôme	Cause probable	Solution
Impossible d'activer le relais : le serveur DHCP est signalé comme actif	Le serveur DHCP est encore activé sur une interface	Décocher « Enable DHCP server » sur toutes les interfaces (Services > DHCP Server)
Les clients restent en 169.254.x.x après la bascule	Le relais ne tourne pas (nœud non MASTER, service arrêté) ou les serveurs sont injoignables	Status > Services : « dhcrelay » doit être « Running » sur le MASTER ; vérifier les « Upstream Servers » et le ping vers SRV-DC1 et SRV-DC2 (Diagnostics > Ping)
Le client a une adresse mais ni passerelle ni DNS	Options 003 / 006 absentes de l'étendue Windows	Console DHCP > Options d'étendue : renseigner 003 (VIP CARP), 006 et 015, puis `ipconfig /renew`
Les serveurs reçoivent la demande mais ne répondent pas	Aucune étendue active ne correspond au sous-réseau du relais	Créer et activer l'étendue du sous-réseau (ex. 192.168.30.0) ; consulter le journal « DHCP-Server » de l'Observateur d'événements
Après une bascule CARP, plus d'adresses	Les paramètres du relais ne sont pas synchronisés vers PFS-2, ou la VIP CARP choisie est incorrecte	System > High Availability Sync : cocher « DHCP Relay settings » et « DHCP Server settings » ; contrôler « CARP Status VIP »
Les serveurs répondent mais le client n'obtient rien	Une règle du VLAN SERVEURS bloque UDP 67 vers pfSense	Autoriser UDP 67 depuis l'alias DHCP_SERVERS vers « This Firewall » ; confirmer avec Diagnostics > Packet Capture (port 67)
Le renouvellement à mi-bail échoue	Règle UDP 68 vers 67 absente sur le VLAN du client	Ajouter la règle de l'étape 3 sur POSTES et WIFI

Pense-bête : où regarder

Où / commande	Utilité
Services > DHCP Relay (pfSense)	Active le relais, choisit les interfaces des clients et les serveurs DHCP
Status > Services (pfSense)	Vérifie que « dhcrelay » est « Running » (sur le nœud MASTER uniquement)
Status > CARP (failover) (pfSense)	État MASTER / BACKUP des adresses virtuelles et mode maintenance
Status > System Logs > DHCP (pfSense)	Journal du relais DHCP
Diagnostics > Packet Capture (pfSense)	Capture des trames UDP 67 / 68 sur l'interface des clients ou des serveurs
Get-DhcpServerv4Scope	Liste les étendues et leur état (Active / InActive)
Get-DhcpServerv4Failover	Relations de basculement, mode, état et étendues protégées
Add-DhcpServerv4FailoverScope	Ajoute des étendues à une relation de basculement existante
Get-DhcpServerv4Lease -ScopeId 192.168.30.0	Liste les baux en cours (à comparer sur les deux serveurs)
Export-DhcpServer -Leases	Sauvegarde la configuration DHCP et les baux