Serveur DHCP sous Windows Server 2025

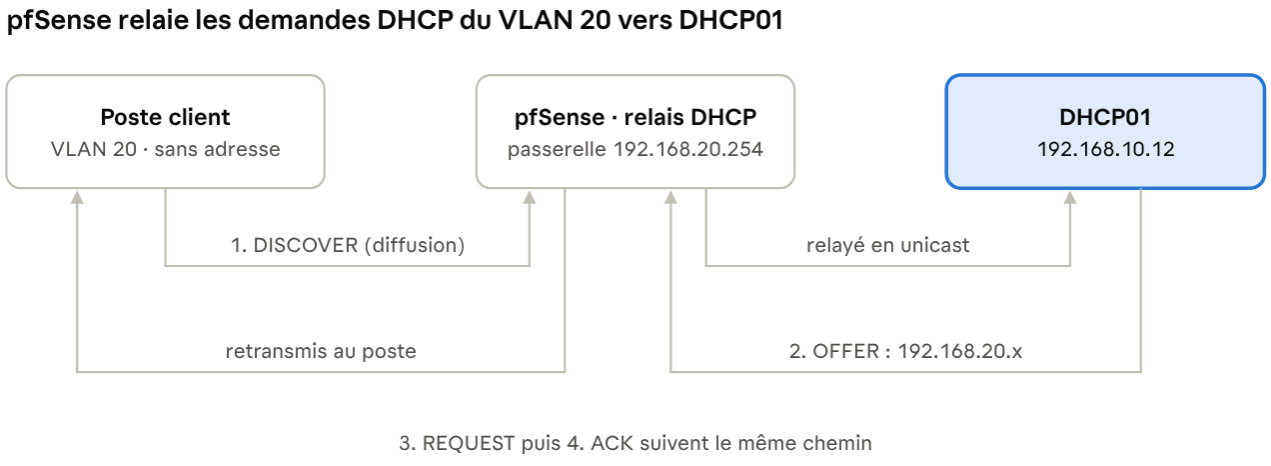
Nov 27, 2026 · @Serge Martins

Objectif et architecture

Ce guide installe un serveur DHCP **DHCP01** sous Windows Server 2025, membre du domaine `martinscie.lan`. Il distribue les adresses du VLAN 20 Clients. Comme il est dans le VLAN 10 Serveurs, pfSense relaie les demandes DHCP d'un VLAN à l'autre.

Élément	Valeur (à adapter)
Serveur DHCP	`DHCP01` – `192.168.10.12/24`, membre de `martinscie.lan`
Contrôleur de domaine / DNS	`DC01` – `192.168.10.10`
Réseau distribué	VLAN 20 Clients – `192.168.20.0/24`
Plage	`192.168.20.100` à `192.168.20.200`
Passerelle (option 003)	`192.168.20.254` (pfSense)
DNS (option 006) / domaine (015)	`192.168.10.10` / `martinscie.lan`
Durée du bail	8 jours

Un DHCP peut aussi s'installer directement sur DC01 ; un serveur séparé évite de mélanger les rôles sur le contrôleur de domaine.



Échange DHCP (DORA) à travers le relais pfSense

Le relais indique à DHCP01 de quel réseau vient la demande, ce qui lui permet de choisir la bonne étendue.

1. Prérequis et installation du rôle

1.1 Préparer DHCP01 (PowerShell en administrateur) :

```
New-NetIPAddress -InterfaceAlias "Ethernet" -IPAddress 192.168.10.12 -
PrefixLength 24 -DefaultGateway 192.168.10.254
Set-DnsClientServerAddress -InterfaceAlias "Ethernet" -ServerAddresses
192.168.10.10
Rename-Computer -NewName DHCP01 -Restart

# Après redémarrage : jonction au domaine
Add-Computer -DomainName martinscie.lan -Credential MARTINSCIE\Administrateur
-Restart
```

Un serveur DHCP doit toujours avoir une **IP fixe**. Installer les mises à jour cumulatives avant de continuer.

1.2 Installer le rôle

- *Interface* : Gestionnaire de serveur > Gérer > Ajouter des rôles et fonctionnalités > **Serveur DHCP** > Installer. Cliquer ensuite sur le drapeau jaune > **Terminer la configuration DHCP** (crée les groupes de sécurité et autorise le serveur).
- *PowerShell* :

```
Install-WindowsFeature DHCP -IncludeManagementTools
# Groupes locaux « Administrateurs DHCP » et « Utilisateurs DHCP »
netsh dhcp add securitygroups
Restart-Service DHCPServer
# Indiquer au Gestionnaire de serveur que la configuration est terminée
Set-ItemProperty -Path HKLM:\SOFTWARE\Microsoft\ServerManager\Roles\12 -Name
ConfigurationState -Value 2
```

2. Autorisation et étendue

2.1 Autoriser le serveur dans l'Active Directory : dans un domaine, un serveur DHCP Windows non autorisé ne distribue aucune adresse (protection contre les serveurs pirates).

```
Add-DhcpServerInDC -DnsName dhcp01.martinscie.lan -IPAddress 192.168.10.12
Get-DhcpServerInDC
```

2.2 Créer l'étendue du VLAN 20

- *Interface* : console DHCP > IPv4 > clic droit > **Nouvelle étendue** : nom, plage, masque, exclusions, durée du bail, puis options (routeur, domaine et DNS) et activation.

- *PowerShell* :

```
Add-DhcpServerv4Scope -Name "VLAN20-Clients" -StartRange 192.168.20.100 -
EndRange 192.168.20.200 `
  -SubnetMask 255.255.255.0 -LeaseDuration 8.00:00:00 -State Active

# Options de l'étendue : passerelle, DNS, nom de domaine
Set-DhcpServerv4OptionValue -ScopeId 192.168.20.0 -Router 192.168.20.254 `
  -DnsServer 192.168.10.10 -DnsDomain martinscie.lan

# Exclusion (imprimantes, équipements fixes)
Add-DhcpServerv4ExclusionRange -ScopeId 192.168.20.0 -StartRange
192.168.20.100 -EndRange 192.168.20.109

# Réservation : toujours la même adresse pour un appareil
Add-DhcpServerv4Reservation -ScopeId 192.168.20.0 -IPAddress 192.168.20.150 `
  -ClientId "00-15-5D-0A-14-01" -Name "IMP-ACCUEIL" -Description "Imprimante
accueil"
```

2.3 Mise à jour du DNS : par défaut, le serveur DHCP enregistre les clients dans le DNS. Pour qu'il le fasse aussi pour les appareils non Windows :

```
Set-DhcpServerv4DnsSetting -ScopeId 192.168.20.0 -DynamicUpdates Always -
DeleteDnsRROnLeaseExpiry $true
```

3. Relais DHCP sur pfSense

Les demandes DHCP sont des diffusions (broadcast) qui ne traversent pas les routeurs. pfSense doit donc les relayer du VLAN 20 vers DHCP01.

1. Services > **DHCP Server** > onglet VLAN 20 : décocher « Enable » (le serveur DHCP de pfSense et le relais ne peuvent pas fonctionner ensemble).
2. Services > **DHCP Relay** : cocher « Enable », interface **VLAN 20**, serveur de destination `192.168.10.12`. Enregistrer.
3. Firewall > Rules > VLAN 10 : autoriser les réponses UDP 67/68 entre pfSense et DHCP01 si une règle les bloque.

Le relais ajoute l'adresse de la passerelle (`192.168.20.254`) dans la demande : c'est ainsi que DHCP01 sait qu'il doit répondre avec l'étendue `192.168.20.0`.

4. Basculement, vérifications et sécurisation

4.1 Basculement (optionnel) : avec un second serveur DHCP (par exemple DC01), le basculement partage l'étendue et ses baux.

```
Add-DhcpServerv4Failover -Name "DHCP01-DC01" -PartnerServer
dc01.martinscie.lan `
  -ScopeId 192.168.20.0 -LoadBalancePercent 50 -SharedSecret "SecretPartagé!"
-AutoStateTransition $true
```

4.2 Vérifications

Sur un poste du VLAN 20 :

```
ipconfig /release
ipconfig /renew
ipconfig /all     # serveur DHCP = 192.168.10.12, DNS = 192.168.10.10
```

Sur DHCP01 :

```
Get-DhcpServerv4Lease -ScopeId 192.168.20.0
Get-DhcpServerv4ScopeStatistics
Get-WinEvent -LogName "Microsoft-Windows-Dhcp-Server/Operational" -MaxEvents
20
```

Symptôme	Cause probable	Correction
Les postes prennent une adresse 169.254.x.x	Relais absent ou mal configuré	Vérifier le relais pfSense et le pare-feu (UDP 67/68)
Le service ne distribue rien	Serveur non autorisé dans l'AD	`Add-DhcpServerInDC`
Les postes ne trouvent pas le domaine	Option 006 incorrecte	DNS = `192.168.10.10`
Le service DHCP s'arrête par intermittence	Mise à jour de juin 2025 (KB5060842)	Installer les mises à jour cumulatives à partir de juillet 2025
Étendue pleine	Trop peu d'adresses ou baux trop longs	Élargir la plage ou réduire la durée du bail

4.3 Sécurisation

- [ ] Activer la **surveillance DHCP** (DHCP snooping) sur les commutateurs pour bloquer les serveurs DHCP pirates.

- [ ] Sauvegarder la configuration : `Export-DhcpServer -File C:\Sauvegarde\dhcp.xml -Leases`.
- [ ] Superviser le service DHCP et le taux d'occupation de l'étendue dans Zabbix.
- [ ] Limiter le groupe « Administrateurs DHCP » aux seuls administrateurs réseau.