# DHCP Sécurisé sur Windows Server 2025 : Guide de Durcissement 2026

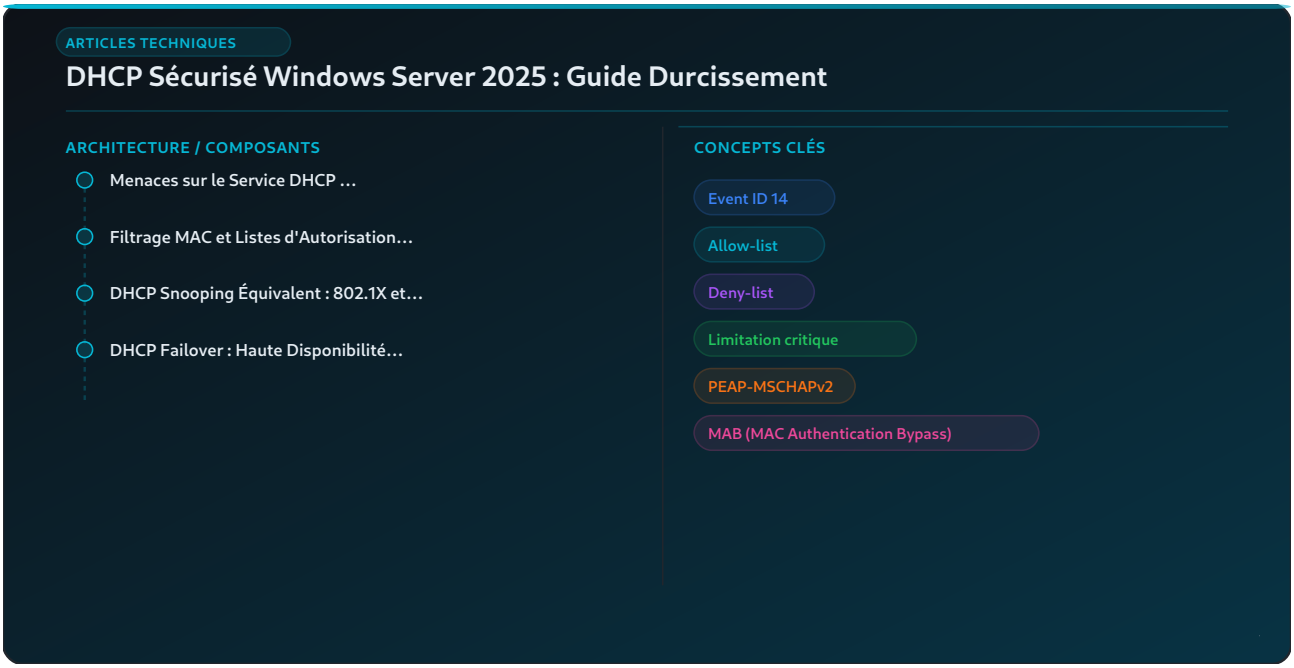
Sécurisez le DHCP sur Windows Server 2025 : protection starvation, rogue DHCP, failover, audit logging et conformité NIS 2 pour administrateurs réseau.

📋 EN BREF

- Le service DHCP est une infrastructure réseau critique : son compromission via un rogue DHCP ou une attaque de starvation peut permettre des attaques man-in-the-middle sur l'ensemble du réseau.
- Windows Server 2025 offre des mécanismes natifs de durcissement : filtres MAC, failover avec shared secret, et audit logging détaillé exploitable par un SIEM.
- Le DHCP snooping sur les switchs (Cisco, HP, Juniper) est la protection la plus efficace contre les rogue DHCP servers en complément des filtres Windows.
- La haute disponibilité DHCP (Add-DhcpServerv4Failover) doit être configurée avec un shared secret pour sécuriser la réplication entre partenaires.
- NIS 2 (Art. 21§2.f) impose la sécurité réseau comme mesure obligatoire : le DHCP doit être documenté, supervisé et ses logs archivés 12 mois minimum.

Dans une entreprise française, le service DHCP est souvent considéré comme une infrastructure de plomberie réseau — fonctionnel, invisible, et rarement audité. Pourtant, c'est l'un des vecteurs d'attaque les plus directs pour compromettre un réseau local entier. Un attaquant capable de déployer un rogue DHCP server peut rediriger tout le trafic réseau via une fausse passerelle, empoisonner les résolutions DNS, et intercepter les communications de centaines de postes de travail sans déclencher la moindre alerte. Pour les RSSI soumis à NIS 2 en France, cette réalité impose une approche proactive : auditer la configuration DHCP, mettre en place des mécanismes de détection des serveurs non autorisés, sécuriser la haute disponibilité, et intégrer les logs DHCP

dans le SIEM d'entreprise. Windows Server 2025 apporte des améliorations notables sur ces aspects, mais sa sécurisation nécessite une configuration explicite que ce guide technique couvre en détail, depuis les filtres MAC jusqu'aux règles Wazuh pour la détection d'anomalies, en passant par le DHCP failover sécurisé et l'intégration DNS dynamique.




## Menaces sur le Service DHCP : Starvation, Rogue DHCP, MITM

Avant de configurer les protections, il est essentiel de comprendre le modèle de menace DHCP. Les trois attaques principales que les équipes sécurité françaises doivent connaître sont le starvation, le rogue DHCP et le MITM par empoisonnement DHCP.

### DHCP Starvation (Gobbler) : épuisement du pool d'adresses

L'attaque de DHCP starvation consiste à envoyer des milliers de requêtes DHCPDISCOVER avec des adresses MAC aléatoires (générées par des outils comme Gobbler ou Yersinia), épuisant le pool d'adresses disponibles. Résultat : les équipements légitimes ne peuvent plus obtenir d'adresse IP.

Impact opérationnel : tous les nouveaux appareils rejoignant le réseau (collaborateurs, visiteurs, IoT) sont déniés de service. Dans un environnement de production, l'impact peut être catastrophique en quelques minutes.

Indicateurs de détection :

**Event ID 14** : "The scope is full. No more addresses are available to give out." — ce log signale l'épuisement du pool.

Nombre anormal de leases DHCP en état "Active" pour des adresses MAC inconnues.

Taux de requêtes DHCP anormalement élevé sur un port de switch spécifique.

### Rogue DHCP server : serveur non autorisé

Un rogue DHCP server est un serveur DHCP non autorisé répondant aux requêtes des clients avant le serveur légitime. Il peut distribuer :

Une fausse passerelle par défaut pointant vers la machine de l'attaquant.

De faux serveurs DNS permettant l'empoisonnement DNS et le phishing.

Des configurations réseau incorrectes pour désorganiser le réseau.

Sur Windows Server 2025, Active Directory refuse d'activer un serveur DHCP non autorisé dans le domaine. Mais un serveur Linux (dnsmasq, ISC DHCP) ou un équipement réseau compromis peut répondre sans restriction.

### DHCP et MITM : DNS poisoning via fausse gateway

Le scénario d'attaque complet combine rogue DHCP et MITM :

L'attaquant déploie un rogue DHCP qui distribue son propre serveur DNS et sa propre passerelle.

Les clients obtiennent des adresses IP "valides" mais avec une gateway et un DNS malveillants.

Tout le trafic HTTP/HTTPS transite par l'attaquant (avec interception SSL si le certificat racine est injecté).

Les résolutions DNS sont falsifiées pour rediriger vers des sites de phishing.

## Filtrage MAC et Listes d'Autorisation DHCP

Windows Server 2025 intègre un système de filtres MAC natif qui permet de définir des listes d'autorisation (allow-list) ou de blocage (deny-list) basées sur les adresses MAC des clients.

> ⚡ **Retour terrain**
>
> Dans les projets techniques complexes, j'ai appris à toujours commencer par auditer la documentation existante plutôt que l'infrastructure elle-même. Dans 80 % des cas, le delta entre la documentation et la réalité est la source première de risques. Une infrastructure bien documentée qui ne correspond pas à la réalité est plus dangereuse qu'une infrastructure sans documentation — parce qu'elle induit une fausse confiance.

### `Set-DhcpServerv4FilterList -Enable $true` : activation des filtres

```
 # Activer le système de filtres MAC
Set-DhcpServerv4FilterList -Enable $true -List Allow

# Vérifier l'état des filtres
Get-DhcpServerv4FilterList

# Ajouter une adresse MAC en liste blanche
Add-DhcpServerv4Filter -MacAddress "AA-BB-CC-DD-EE-FF" -Description "Laptop-RH-001" -List Allow

# Supprimer un filtre
Remove-DhcpServerv4Filter -MacAddress "AA-BB-CC-DD-EE-FF"
```

## Allow-list vs Deny-list, limitations (MAC spoofing)

**Allow-list** (liste blanche) : seules les adresses MAC enregistrées peuvent obtenir un bail DHCP. Avantage : protection maximale. Inconvénient : charge administrative élevée dans les grands environnements (BYOD, invités).

**Deny-list** (liste noire) : les adresses MAC listées sont bloquées. Utile pour isoler rapidement un équipement compromis.

**Limitation critique** : les filtres MAC sont contournables par MAC spoofing. Un attaquant observant une adresse MAC légitime sur le réseau peut la reproduire en quelques secondes. Les filtres MAC ne constituent donc qu'une première couche de défense, jamais la seule.

### Script PowerShell : export/import des filtres MAC

```
function Export-DhcpMacFilters {
    param([string]$OutputPath = "C:\Audit\dhcp-mac-filters-$(Get-Date -Format 'yyyyMMdd').csv")

    $allowList = Get-DhcpServerv4Filter -List Allow -ErrorAction SilentlyContinue
    $denyList = Get-DhcpServerv4Filter -List Deny -ErrorAction SilentlyContinue

    $export = @()
    foreach ($mac in $allowList) {
        $export += [PSCustomObject]@{ MacAddress=$mac.MacAddress; Description=$mac.Description; L
    }
    foreach ($mac in $denyList) {
        $export += [PSCustomObject]@{ MacAddress=$mac.MacAddress; Description=$mac.Description; L
    }
    $export | Export-Csv $OutputPath -NoTypeInformation -Encoding UTF8
    Write-Host "[$($export.Count) filtres exportes vers $OutputPath]"
}

function Import-DhcpMacFilters {
    param([string]$InputPath)
    $filters = Import-Csv $InputPath
    foreach ($f in $filters) {
        Add-DhcpServerv4Filter -MacAddress $f.MacAddress -Description $f.Description -List $f.Lis
    }
    Write-Host "[$($filters.Count) filtres importes]"
}

Export-DhcpMacFilters
```

## DHCP Snooping Équivalent : 802.1X et NAC

Le DHCP snooping est une fonctionnalité des switchs managés qui inspecte le trafic DHCP et bloque les réponses DHCP provenant de ports non autorisés. C'est la protection la plus efficace contre les rogue DHCP servers.

### DHCP Snooping sur switchs (Cisco/HP) : configuration

```
 # Configuration DHCP Snooping sur un switch Cisco IOS
ip dhcp snooping
ip dhcp snooping vlan 10,20,30

# Définir les ports de confiance (uplinks vers les serveurs DHCP autorisés)
interface GigabitEthernet0/1
 ip dhcp snooping trust
 description "Uplink vers serveur DHCP autorise"

# Sur les ports d'accès : limiter le débit des requêtes DHCP
interface GigabitEthernet0/2
 ip dhcp snooping limit rate 15
 description "Port utilisateur - 15 req/s max"

# HP ProCurve
dhcp-snooping
dhcp-snooping vlan 10 20 30
interface 1
   dhcp-snooping trust
```

### 802.1X : authentification avant attribution IP

802.1X authentifie les équipements au niveau du port réseau avant de leur accorder l'accès au VLAN DHCP. Couplé à DHCP snooping, il constitue une protection robuste :

**EAP-TLS** : authentification par certificat client — la plus sécurisée, recommandée pour les postes gérés.

**PEAP-MSCHAPv2** : authentification par credentials AD — acceptable pour les environnements sans PKI interne.

**MAB (MAC Authentication Bypass)** : pour les équipements ne supportant pas 802.1X (imprimantes, IoT).

```
 # Sur Windows Server 2025 : vérifier le rôle NPS (RADIUS) pour 802.1X
Get-WindowsFeature NPAS | Select-Object Name, InstallState
# Vérifier les politiques réseau configurées
netsh nps show np
```

### Network Access Control (NAC) : complément DHCP sécurisé

Un NAC (Cisco ISE, Aruba ClearPass, ForeScout, ou solutions open-source comme PacketFence) permet de :

Contrôler l'accès réseau basé sur la conformité du poste (patch level, antivirus, chiffrement disque).

Isoler automatiquement les équipements non conformes dans un VLAN de quarantaine.

Fournir un audit complet de tous les équipements connectés, enrichissant les données DHCP.

---

## DHCP Failover : Haute Disponibilité Sécurisée

Le failover DHCP natif de Windows Server 2025 permet de synchroniser les baux entre deux serveurs DHCP. Sa configuration sécurisée est essentielle.

### `Add-DhcpServerv4Failover` : configuration Load Balance vs Hot Standby

```
 # Configuration du failover DHCP en mode Load Balance (50/50)
Add-DhcpServerv4Failover `
    -Name "Failover-LAN-Principal" `
    -PartnerServer "dhcp02.domaine.fr" `
    -ScopeId "192.168.1.0" `
    -Mode LoadBalance `
    -LoadBalancePercent 50 `
    -MaxClientLeadTime (New-TimeSpan -Hours 1) `
    -AutoStateTransition $true `
    -StateTransitionInterval (New-TimeSpan -Minutes 15) `
    -SharedSecret "SecretFailoverDHCP2025!"

# Configuration en mode Hot Standby (serveur secondaire en réserve)
Add-DhcpServerv4Failover `
    -Name "Failover-Site-Distant" `
    -PartnerServer "dhcp-backup.site2.fr" `
    -ScopeId "10.10.0.0" `
    -Mode HotStandby `
    -ServerRole Standby `
    -ReservePercent 10 `
    -SharedSecret "SecretFailoverSite2025!"
```

### Shared secret entre partenaires DHCP

Le shared secret est utilisé pour authentifier les messages de synchronisation entre les deux serveurs DHCP failover. Sans shared secret :

Un attaquant peut injecter de fausses données de synchronisation si il accède au port TCP 647.

Les mises à jour de baux entre partenaires ne sont pas authentifiées.

Bonnes pratiques pour le shared secret :

Minimum 16 caractères, complexe (majuscules, minuscules, chiffres, caractères spéciaux).

Stocké dans un gestionnaire de secrets (HashiCorp Vault, Azure Key Vault) et non en clair dans les scripts.

Rotation annuelle avec procédure documentée.

Firewall : restreindre TCP 647 aux seules adresses IP des serveurs DHCP partenaires.

### Monitoring état du failover

```
 # Vérifier l'état du failover DHCP
Get-DhcpServerv4Failover | Select-Object Name, PartnerServer, Mode, State, AutoStateTransition

# Etat détaillé par scope
Get-DhcpServerv4Failover -Name "Failover-LAN-Principal" |
    Select-Object Name, PartnerServer, State, PotentialRole, ServerType, SharedSecret
```

---

## DHCP Audit Logging et Monitoring

Les logs DHCP sont une source précieuse pour la traçabilité réseau, la détection d'anomalies, et la conformité NIS 2. Windows Server 2025 journalise nativement toutes les activités DHCP.

### Fichiers de log DHCP : `%SystemRoot%\System32\DHCP\`

Par défaut, les logs DHCP sont stockés dans `C:\Windows\System32\DHCP\` sous forme de fichiers texte rotatifs quotidiens (DhcpSrvLog-Mon.log, DhcpSrvLog-Tue.log, etc.). Chaque ligne contient : ID d'événement, date, heure, description, adresse IP, nom d'hôte, adresse MAC.

```
 # Configurer la taille et le chemin des logs DHCP
Set-DhcpServerv4AuditLog -Enable $true `
    -Path "D:\Logs\DHCP" `
    -MaxMBFileSize 100 `
    -MinMBDiskSpace 500
```

## Event IDs DHCP : 10, 11, 12, 13, 14, 30, 31, 32

| Event ID | Signification | Sécurité |
|---|---|---|
| 10 | Nouveau bail accordé | Baseline normale |
| 11 | Renouvellement de bail | Baseline normale |
| 12 | Bail libéré | Normal |
| 13 | IP déjà utilisée (ARP check failed) | Possible conflit ou spoofing |
| 14 | Scope épuisé (pool plein) | ALERTE : possible starvation |
| 30 | Démarrage serveur DHCP | A monitorer (redémarrages inattendus) |
| 31 | Arrêt serveur DHCP | ALERTE si non planifié |
| 32 | Pause du service DHCP | ALERTE si non planifié |

Script PowerShell : analyse des logs DHCP pour détection starvation

```
function Analyze-DhcpLogs {
    param(
        [string]$LogPath = "C:\Windows\System32\DHCP",
        [int]$DaysBack = 7
    )

    $logFiles = Get-ChildItem $LogPath -Filter "DhcpSrvLog-*.log" |
        Where-Object {$_.LastWriteTime -gt (Get-Date).AddDays(-$DaysBack)}

    $events = @()
    foreach ($file in $logFiles) {
        $lines = Get-Content $file.FullName | Where-Object {$_ -match "^\d+,"}
        foreach ($line in $lines) {
            $parts = $line -split ","
            if ($parts.Count -ge 5) {
                $events += [PSCustomObject]@{
                    EventID = $parts[0]
                    Date = $parts[1]
                    Time = $parts[2]
                    Description = $parts[3]
                    IPAddress = $parts[4]
                    HostName = if ($parts.Count -gt 5) { $parts[5] } else { "" }
                    MACAddress = if ($parts.Count -gt 6) { $parts[6] } else { "" }
                }
            }
        }
    }

    Write-Host "=== ANALYSE LOGS DHCP ===" -ForegroundColor Cyan
    Write-Host "Total evenements: $($events.Count)"

    # Détection starvation (Event ID 14)
    $starvation = $events | Where-Object {$_.EventID -eq "14"}
    if ($starvation.Count -gt 0) {
        Write-Host "[ALERTE] $($starvation.Count) evenements d'epuisement de scope (ID 14)!" -For
    }

    # MAC addresses les plus actives (suspicion starvation)
    $topMAC = $events | Where-Object {$_.MACAddress -ne "" -and $_.EventID -eq "10"} |
        Group-Object MACAddress | Sort-Object Count -Descending | Select-Object -First 10
    Write-Host "`n=== TOP 10 MAC par nombre de baux ===" -ForegroundColor Yellow
    $topMAC | Format-Table Name, Count
```

```
    return $events
}

Analyze-DhcpLogs
```

### Règles Wazuh pour DHCP

```
 <!-- Règles Wazuh pour alertes DHCP Windows -->
<group name="windows,dhcp">
  <rule id="91001" level="12">
    <if_sid>18145</if_sid>
    <field name="win.system.eventID">14</field>
    <description>DHCP: Pool d'adresses epuise - possible attaque starvation</description>
    <mitre><id>T1498</id></mitre>
  </rule>

  <rule id="91002" level="10">
    <if_sid>18145</if_sid>
    <field name="win.system.eventID">31</field>
    <description>DHCP: Service arrete de facon inattendue</description>
  </rule>
</group>
```

---

## Intégration DHCP/DNS Sécurisée (DDNS)

Le DNS dynamique (DDNS) permet au serveur DHCP de mettre à jour automatiquement les enregistrements DNS lors de l'attribution de baux. Sans sécurisation, ce mécanisme peut être exploité pour empoisonner les zones DNS.

### Dynamic DNS update : sécuriser les mises à jour DNS automatiques

```
 # Configurer les mises à jour DDNS sécurisées pour un scope
Set-DhcpServerv4DnsSetting -ScopeId "192.168.1.0" `
    -DynamicUpdates Always `
    -DeleteDnsRROnLeaseExpiry $true `
    -UpdateDnsRRForOlderClients $false `
    -DisableDnsPtrRRUpdate $false

# Vérifier la configuration DDNS globale
Get-DhcpServerv4DnsSetting
```

`Set-DhcpServerv4DnsSetting -UpdateDnsRRForOlderClients`

Le paramètre `-UpdateDnsRRForOlderClients` détermine si le serveur DHCP met à jour le DNS au nom des clients qui ne le font pas eux-mêmes (Windows XP, anciens Linux sans DDNS client). Désactivez-le dans les environnements modernes pour réduire la surface d'attaque : seuls les clients modernes (qui s'auto-enregistrent avec des credentials kerberos) peuvent modifier leurs enregistrements DNS.

### Comptes de service DHCP pour les mises à jour DNS

Créez un compte de service dédié pour les mises à jour DDNS, membre uniquement du groupe **DnsUpdateProxy** :

```
 # Créer le compte de service DDNS
New-ADUser -Name "svc-dhcpddns" -SamAccountName "svc-dhcpddns" `
    -AccountPassword (ConvertTo-SecureString "P@ssw0rdDDNS2025!" -AsPlainText -Force) `
    -PasswordNeverExpires $true -Enabled $true

# Ne PAS ajouter au groupe DnsUpdateProxy (risque de sécurité documenté par Microsoft)
# Utiliser plutôt les credentials directement dans la configuration DHCP
Set-DhcpServerDnsCredential -DomainName "domaine.fr" `
    -UserName "svc-dhcpddns" `
    -Password (ConvertTo-SecureString "P@ssw0rdDDNS2025!" -AsPlainText -Force)
```

## DHCP Guard et Protection Rogue DHCP

Au-delà du DHCP snooping sur les switchs physiques, plusieurs mécanismes Windows-natifs permettent de protéger l'infrastructure contre les rogue DHCP servers, notamment dans les environnements virtualisés.

### Hyper-V DHCP Guard : bloquer les VM qui répondent DHCP

Hyper-V DHCP Guard permet de bloquer les paquets DHCPOFFER et DHCPACK émis par une VM, empêchant qu'une VM compromise devienne un rogue DHCP server sur le réseau virtuel :

```
 # Activer DHCP Guard sur une VM spécifique (bloque les réponses DHCP de cette VM)
Set-VMNetworkAdapterDhcpGuard -VMName "VM-Finance-01" -SwitchName "vSwitch-LAN" -DhcpGuard On

# Activer sur toutes les VM d'un hôte Hyper-V (sauf le serveur DHCP autorisé)
Get-VM | Where-Object {$_.Name -notlike "DHCP-SRV*"} |
    Get-VMNetworkAdapter |
    Set-VMNetworkAdapterDhcpGuard -DhcpGuard On

# Vérifier les VMs avec DHCP Guard activé
Get-VM | Get-VMNetworkAdapter | Select-Object VMName, DhcpGuard
```

### VLAN isolation des serveurs DHCP

La segmentation VLAN pour les serveurs DHCP est une pratique de sécurité fondamentale :

Placer les serveurs DHCP dans un VLAN d'infrastructure dédié (ex: VLAN 999 - Infrastructure).

Utiliser des IP helpers (relay DHCP) sur les interfaces de routage entre VLANs pour permettre le service sans exposer directement le serveur.

Restreindre les ACL sur le VLAN infrastructure : seul le trafic DHCP (UDP 67/68) vers les serveurs autorisés est permis.

### Dynamic ARP Inspection (DAI) complémentaire

DAI est une fonctionnalité complémentaire au DHCP snooping qui protège contre les attaques ARP poisoning (souvent couplées aux attaques rogue DHCP) :

```
 # Configuration DAI sur Cisco IOS (nécessite DHCP snooping actif)
ip arp inspection vlan 10,20,30

# Ports de confiance (uplinks)
interface GigabitEthernet0/1
 ip arp inspection trust

# Limiter le débit ARP sur les ports utilisateur
interface GigabitEthernet0/2
 ip arp inspection limit rate 100
```

## Script PowerShell Complet d'Audit DHCP

Ce script complet génère un rapport HTML d'audit DHCP pour les RSSI et les équipes d'audit interne, couvrant les scopes, les leases, les filtres, et l'état du failover.

```
function Invoke-DhcpFullAudit {
    param([string]$OutputPath = "C:\Audit\dhcp-audit-$(Get-Date -Format 'yyyyMMdd-HHmm').html")

    $html = @"
<!DOCTYPE html>
<html><head><meta charset='utf-8'>
<title>Rapport Audit DHCP - $(Get-Date -Format 'dd/MM/yyyy')</title>
<style>body{font-family:Arial;} table{border-collapse:collapse;width:100%;}
th,td{border:1px solid #ddd;padding:8px;} th{background:#0078d4;color:white;}
.alert{background:#ffd7d7;} .ok{background:#d7ffd7;}</style>
</head><body>
<h1>Rapport Audit DHCP - $(Get-Date -Format 'dd/MM/yyyy HH:mm')</h1>
<h2>Scopes DHCP</h2>
<table><tr><th>ScopeID</th><th>Nom</th><th>Start</th><th>End</th><th>Actifs</th><th>Libres</th></
"@

    $scopes = Get-DhcpServerv4Scope
    foreach ($scope in $scopes) {
        $stats = Get-DhcpServerv4ScopeStatistics -ScopeId $scope.ScopeId
        $pctUsed = [math]::Round(($stats.InUse / ($stats.InUse + $stats.Free + 1)) * 100, 1)
        $rowClass = if ($pctUsed -gt 90) { "alert" } else { "ok" }
        $html += "<tr class='$rowClass'><td>$($scope.ScopeId)</td><td>$($scope.Name)</td>"
        $html += "<td>$($scope.StartRange)</td><td>$($scope.EndRange)</td>"
        $html += "<td>$($stats.InUse) ($pctUsed%)</td><td>$($stats.Free)</td></tr>"
    }

    $html += "</table><h2>Failover DHCP</h2><table><tr><th>Nom</th><th>Partenaire</th><th>Mode</t
    $failovers = Get-DhcpServerv4Failover -ErrorAction SilentlyContinue
    foreach ($fo in $failovers) {
        $html += "<tr><td>$($fo.Name)</td><td>$($fo.PartnerServer)</td>"
        $html += "<td>$($fo.Mode)</td><td>$($fo.State)</td></tr>"
    }

    $html += "</table><p>Rapport genere le $(Get-Date)</p></body></html>"
    $html | Out-File $OutputPath -Encoding UTF8
    Write-Host "Rapport genere : $OutputPath"
    return $OutputPath
}

Invoke-DhcpFullAudit
```

## Conformité NIS 2 : DHCP comme Infrastructure Réseau Critique

La directive NIS 2, transposée en France par la loi du 17 octobre 2024, positionne le DHCP parmi les infrastructures réseau critiques dont la sécurisation est une obligation légale pour les entités essentielles et importantes.

### NIS 2 Art. 21§2.f (sécurité réseau)

L'article 21§2.f impose des mesures de sécurité réseau comprenant :

**Segmentation réseau** : le DHCP snooping et la séparation VLAN des serveurs DHCP répondent à cette exigence.

**Contrôle des accès réseau** : les filtres MAC et le 802.1X constituent les mesures de contrôle d'accès au niveau DHCP.

**Détection des anomalies** : la surveillance des Event IDs DHCP et les règles SIEM/Wazuh répondent à l'obligation de détection.

### Documentation et traçabilité des assignations IP

Pour les audits NIS 2, les organisations françaises doivent :

Archiver les logs DHCP pendant 12 mois minimum (configurer la rotation et l'archivage des fichiers `DhcpSrvLog-*.log`).

Documenter toutes les plages d'adresses (scopes) avec leur usage, les VLANs associés, et les équipements attendus.

Maintenir un inventaire des baux statiques (reservations) avec justification métier.

Tester régulièrement la procédure de failover DHCP (continuité d'activité, Art. 21§2.e).

### Contexte entreprises françaises

Selon les retours d'expérience des audits NIS 2 en cours en France, le DHCP est l'une des infrastructures réseau les plus fréquemment mal configurées dans les ETI et les collectivités

territoriales. Les principales lacunes constatées : absence de failover DHCP, pas de DHCP snooping sur les switchs, logs DHCP non intégrés au SIEM, et aucune procédure de réponse en cas de rogue DHCP détecté. Ce guide technique couvre l'ensemble de ces points.

Pour approfondir la sécurisation de votre infrastructure réseau Windows, consultez nos guides sur DNSSEC sur Windows Server 2025 et l'audit des permissions DNS dans Active Directory. La surveillance des contrôleurs de domaine est couverte dans notre article sur les événements Windows à surveiller sur un DC, et la sécurisation des communications LDAP dans notre guide LDAP signing et channel binding.

## Questions fréquentes sur le DHCP sécurisé

### Qu'est-ce que le DHCP starvation et comment s'en protéger ?

Le DHCP starvation consiste à épuiser le pool d'adresses IP d'un serveur DHCP en envoyant des milliers de requêtes DHCPDISCOVER avec des adresses MAC falsifiées. La protection passe par l'activation des filtres MAC (allow-list), la limitation du débit DHCP sur les ports de switch (port security, DHCP snooping) et la surveillance de l'Event ID 14 qui signale l'épuisement du pool.

### Comment détecter un serveur DHCP non autorisé (rogue DHCP) sur mon réseau ?

Sur Windows Server 2025, un serveur DHCP doit être autorisé dans Active Directory pour fonctionner — les serveurs non joints au domaine peuvent cependant répondre librement. Utilisez des outils comme Wireshark ou des scripts PowerShell surveillant les DHCPOFFER suspects. Le DHCP snooping sur les switchs est la protection la plus efficace au niveau réseau.

### Quelle est la différence entre le mode Load Balance et Hot Standby pour le failover DHCP ?

En mode Load Balance, les deux serveurs partagent la charge (50/50 par défaut) et se remplacent mutuellement en cas de panne. En mode Hot Standby, un serveur est actif et l'autre est en veille,

n'intervenant qu'en cas de défaillance du principal. Load Balance offre de meilleures performances, Hot Standby est plus simple à superviser. Pour les sites distants, Hot Standby est recommandé.

### Les filtres MAC DHCP sont-ils suffisants pour sécuriser le service DHCP ?

Non, les filtres MAC seuls sont insuffisants car les adresses MAC peuvent être facilement usurpées (MAC spoofing). Ils constituent une couche de défense parmi d'autres. La sécurité DHCP complète nécessite : filtres MAC + DHCP snooping sur les switchs + 802.1X pour l'authentification réseau + surveillance des logs DHCP. En environnement critique, le NAC est la solution la plus robuste.

### Comment le DHCP sécurisé contribue-t-il à la conformité NIS 2 ?

NIS 2 (Article 21§2.f) impose la sécurité des réseaux comme mesure technique obligatoire. Le DHCP est une infrastructure réseau critique : son compromission peut permettre des attaques MITM via une fausse passerelle ou un serveur DNS malveillant. La conformité NIS 2 exige la documentation des plages d'adresses, la traçabilité des assignations IP (logs DHCP sur 12 mois), et des mécanismes de détection des rogue DHCP.

**À RETENIR**

Le DHCP starvation (Event ID 14) et les rogue DHCP servers sont les deux menaces principales : protégez-vous avec les filtres MAC Windows combinés au DHCP snooping sur vos switchs managés pour une défense en profondeur efficace.

Configurez systématiquement le failover DHCP (Add-DhcpServerv4Failover) avec un shared secret robuste — un service DHCP sans haute disponibilité est un risque de continuité d'activité inacceptable pour une entité NIS 2.

Activez le DHCP Guard Hyper-V sur toutes vos VM (sauf le serveur DHCP autorisé) pour empêcher qu'une VM compromise ne devienne un rogue DHCP server sur votre réseau virtuel.

Intégrez les logs DHCP dans votre SIEM : l'Event ID 14 (pool épuisé) doit déclencher une alerte critique immédiate, les Event ID 31/32 (arrêt/pause du service) doivent être corrélés avec les changements planifiés.

NIS 2 Art. 21§2.f impose l'archivage des logs DHCP sur 12 mois minimum : configurez la rotation des fichiers DhcpSrvLog vers un stockage centralisé dès maintenant pour être en conformité.

## Références et documentation


Microsoft Learn — Sécurité Windows Server

ANSSI — Guide de sécurisation Active Directory

MITRE ATT&CK — Techniques Active Directory