

Haute disponibilite avec OPNsense et CARP

Paire actif/passif sans interruption

Mars 2026 | Serie Stack OPNsense — Billet 10

Sommaire

1. Qu'est-ce que CARP ?
2. Prerequis : 2 VMs OPNsense sur Proxmox
3. Configurer les VIPs CARP
4. pfsync : synchronisation des etats
5. XMLRPC Config Sync
6. Tester le basculement (failover)
7. Cas d'usage production
8. Monitoring CARP avec Grafana
9. Prochaines etapes — SIEM Wazuh

1. Qu'est-ce que CARP ?

CARP (Common Address Redundancy Protocol) est un protocole reseau qui permet a plusieurs machines de partager une adresse IP virtuelle (VIP). Developpe initialement pour OpenBSD et integre dans OPNsense/pfSense, CARP garantit la haute disponibilite d'un firewall : si le noeud maitre tombe, le noeud de secours prend le relai en quelques secondes, de maniere totalement transparente pour les connexions en cours.

Dans mon infra BOTUM, j'utilise CARP pour deux cas critiques :

- Mises a jour OPNsense sans interruption : basculer sur le backup, mettre a jour le master, rebasculer
- Pannes materielles ou VM Proxmox : basculement automatique en moins de 3 secondes
- Maintenance planifiee : arret propre du master, le backup prend le relai

2. Prerequis : 2 VMs OPNsense sur Proxmox

Pour mettre en place la haute disponibilite CARP, il vous faut :

- 2 VMs OPNsense identiques sur Proxmox (meme version, meme configuration de base)
- 3 interfaces reseau par VM : WAN, LAN, et SYNC (pfsync)
- Un switch ou VLAN dedie pour le lien de synchronisation
- Acces SSH aux deux noeuds
- Meme version OPNsense sur les deux noeuds (imperatif)

Architecture reseau recommandee

```
# OPNsense-1 (MASTER)
# - vtnet0 : WAN -> IP: 203.0.113.2/28 (reelle)
# - vtnet1 : LAN -> IP: 192.168.1.1/24 (reelle)
# - vtnet2 : SYNC -> IP: 192.168.254.1/30

# OPNsense-2 (BACKUP)
# - vtnet0 : WAN -> IP: 203.0.113.3/28 (reelle)
# - vtnet1 : LAN -> IP: 192.168.1.2/24 (reelle)
# - vtnet2 : SYNC -> IP: 192.168.254.2/30

# VIPs CARP partagees (les clients utilisent ces IPs)
# - WAN VIP : 203.0.113.4/28 (VHID 1)
# - LAN VIP : 192.168.1.254/24 (VHID 2)
```

3. Configurer les VIPs CARP

Creer la VIP WAN sur le MASTER

Dans OPNsense MASTER : Interfaces > Virtual IPs > Add

```
# Interfaces > Virtual IPs > Settings > Add
Type      : CARP
Interface : WAN
IP Address : 203.0.113.4 / 28
Virtual VHID : 1
VHID Password: MonMotDePasseCarp2026
Advertising frequency - Base: 1
Advertising frequency - Skew: 0    <- 0 = MASTER (priorite haute)
Description : WAN-VIP-CARP
```

Créer la VIP LAN sur le MASTER

```
# Repeter pour l'interface LAN
Type      : CARP
Interface : LAN
IP Address : 192.168.1.254 / 24
Virtual VHID : 2
VHID Password: MonMotDePasseCarp2026
Advertising frequency - Base: 1
Advertising frequency - Skew: 0
Description : LAN-VIP-CARP
```

Configurer le BACKUP (Skew 100)

Sur OPNsense BACKUP, créer les mêmes VIPs avec Skew = 100 :

```
# Sur OPNsense-2 (BACKUP) – meme config, seul le skew change :
# WAN VIP : VHID 1, Skew 100    <- 100 = BACKUP (priorite basse)
# LAN VIP : VHID 2, Skew 100

# Regles CARP :
# - Skew 0    = priorite haute -> MASTER actif
# - Skew 100 = priorite basse -> BACKUP en attente
# - Plus le skew est bas, plus le noeud est prioritaire
```

4. pfsync : Synchronisation des états de connexion

pfsync synchronise les tables d'états du firewall entre les deux nœuds en temps réel. Ainsi, lors d'un basculement, les connexions TCP actives (SSH, HTTPS, VPN) ne sont pas interrompues — le backup connaît déjà tous les états.

Activer pfsync sur le MASTER

System > High Availability > Settings

```
# System > High Availability > Settings

[High Availability Sync]
Synchronize States (pfsync)      : checked
Synchronize Interface            : SYNC (vtnet2)
pfsync Synchronize Peer IP       : 192.168.254.2  <- IP SYNC du BACKUP

[Firewall]
Synchronize firewall rules       : checked
Synchronize NAT                  : checked
Synchronize static routes        : checked
```

Activer pfsync sur le BACKUP

```
# System > High Availability > Settings (sur BACKUP)

[High Availability Sync]
Synchronize States (pfsync)      : checked
Synchronize Interface            : SYNC (vtnet2)
pfsync Synchronize Peer IP       : 192.168.254.1  <- IP SYNC du MASTER
```

Le lien SYNC doit être isolé sur un VLAN ou réseau dédié. Ne jamais faire transiter du trafic utilisateur sur cette interface.

5. XMLRPC Config Sync

XMLRPC Config Sync permet de propager automatiquement la configuration OPNsense du MASTER vers le BACKUP. Chaque modification sur le MASTER (nouvelle règle firewall, NAT, alias) est synchronisée sans intervention manuelle.

Configurer XMLRPC sur le MASTER

```
# System > High Availability > Settings

[Configuration Synchronization]
Synchronize Config to IP        : 192.168.254.2  <- IP SYNC du BACKUP
Remote System Username          : root (ou admin)
Remote System Password          : MotDePasseBackup2026

# Sections à synchroniser (cocher toutes) :
Aliases                         Certificates      DHCP Server
DNS Resolver                    Firewall Rules  Gateways
Interfaces                      NAT             OpenVPN / WireGuard
Routes                         Users and Groups
```

Après chaque modification sur le MASTER, cliquer Save & Sync pour propager immédiatement.

6. Tester le basculement (Failover)

Le test de basculement est OBLIGATOIRE avant de passer en production.

```
# System > High Availability > Status

# 1. Verifier l'etat initial :
#   MASTER : CARP State = MASTER (VIPs actives)
#   BACKUP : CARP State = BACKUP (VIPs en attente)

# 2. Sur le MASTER : passer en mode BACKUP manuellement
pfctl -d # Desactiver le firewall (force le basculement)
# OU : System > High Availability > Forcefully become BACKUP

# 3. Observer le BACKUP prendre le relai (~2-3 secondes)
```

Test 2 : Simulation panne (arret brutal)

```
# Dans Proxmox, eteindre la VM OPNsense-1 (MASTER) :
# qm stop 100 (ou via l'interface Proxmox)

# Sur un client reseau, lancer un ping continu vers la VIP :
ping 203.0.113.4
# -> Vous devriez voir 1-2 pertes max pendant le basculement
# -> Le backup reprend en 1-3 secondes

# Verifier sur le BACKUP :
# System > High Availability > Status
# VIP WAN : MASTER | VIP LAN : MASTER OK
```

Test 3 : Connexions actives survivent au failover

```
# Sur un poste client, ouvrir une session SSH via la VIP LAN :
ssh admin@192.168.1.254

# Pendant que la session SSH est ouverte, forcer le basculement
# La session SSH doit SURVIVRE grace a pfsync
# (les etats TCP sont synchronises en temps reel)

# Si la session SSH survit -> pfsync fonctionne correctement
# Si la session SSH se coupe -> verifier la config pfsync
```

7. Cas d'usage : Production sans interruption

La principale valeur ajoutée de CARP dans mon infra BOTUM est la possibilité de faire des maintenances sans fenêtre d'indisponibilité.

Mise à jour OPNsense sans downtime

```
# Etape 1 : Verifier que le backup est sain
#   System > High Availability > Status
#   BACKUP : CARP BACKUP, pfsync OK, config synced

# Etape 2 : Basculer le trafic vers le BACKUP
#   MASTER : System > HA > Forcefully become BACKUP
#   -> BACKUP devient MASTER, prend toutes les VIPs

# Etape 3 : Mettre a jour l'ancien MASTER (maintenant BACKUP)
#   System > Firmware > Updates > Upgrade
#   -> Redemarrage normal, aucun impact sur le trafic

# Etape 4 : Verifier le retour de l'ancien MASTER
#   -> Il revient en mode BACKUP automatiquement
#   -> Verifier sync states + config sync OK

# Etape 5 : Repeter pour l'autre noeud
#   Resultat : 2 noeuds mis a jour, 0 seconde de downtime
```

8. Monitoring CARP avec Grafana

Integration avec la stack Grafana + InfluxDB du Billet 9 pour monitorer l'etat CARP en temps reel.

Collecte des metriques CARP via Telegraf

```
# Dans telegraf.conf (sur le serveur de monitoring) :
[[inputs.http]]
  urls = ["http://OPNSENSE-VIP/api/diagnostics/interface/getVipStatus"]
  method = "GET"
  username = "telegraf_user"
  password = "VOTRE-TOKEN-API"
  data_format = "json"
  name_suffix = "_carp"

# Requete Flux Grafana – etat CARP :
from(bucket: "opnsense")
  |> range(start: -1h)
  |> filter(fn: (r) => r._measurement == "http_carp")
  |> filter(fn: (r) => r._field == "status")
```

Panneaux recommandes (Dashboard Grafana CARP)

- Etat CARP actuel (MASTER/BACKUP) pour chaque VIP — Gauge
- Historique des basculements — Timeline/Log panel
- Compteur pfsync : etats synchronises/seconde — Time series
- Latence lien SYNC — Gauge (alert si > 10ms)
- Nombre d'etats firewall synchronises — Stat panel

9. Prochaines etapes — SIEM Wazuh

Vous avez maintenant une infrastructure OPNsense en haute disponibilité, résiliente aux pannes et aux maintenances. La prochaine étape de la série est le Billet 11 : intégration d'un SIEM avec Wazuh pour centraliser les logs sécurité et détecter les intrusions.

Article complet : blog.botum.ca/opnsense-carp-haute-disponibilite

Site : www.botum.ca |

— Canada