



Procédure Mise en place DHCP et DNS redondés

Table des matières

Procédure Mise en place DHCP et DNS redondés	1
1- Prérequis.....	1
2- Configuration de base.....	1
3- Configuration de la redondance DHCP.....	2
4- Configuration du DNS	5
5- Conclusion.....	8

1- Prérequis

Tout d'abord, nous avons besoin de deux machines (physiques ou virtuelles) différentes.

Une hébergera les services DHCP principal ainsi que le DNS secondaire.

La seconde hébergera le DNS principal et le DHCP secondaire.

Ensuite, nous allons utiliser un client Debian afin de faire nos tests en direct.

Ces deux serveurs devront avoir des adresses IP de configurées, ainsi que les packages

isc-dhcp-server ainsi que **bind9** de préinstallés

2- Configuration de base

Premièrement nous configurons le fichiers **/etc/hosts** de nos deux serveurs :

```
127.0.0.1    localhost
192.168.100.50  srv-deb1.vetele.mv    srv-deb1

# The following lines are desirable for IPv6 capable hosts
::1        localhost ip6-localhost ip6-loopback
ff02::1    ip6-allnodes
ff02::2    ip6-allrouters
```

```
127.0.0.1    localhost
192.168.100.51  srv-deb2.vetele.mv    srv-deb2

# The following lines are desirable for IPv6 capable hosts
::1        localhost ip6-localhost ip6-loopback
ff02::1    ip6-allnodes
ff02::2    ip6-allrouters
```



Et ensuite, le fichier */etc/resolv.conf* sur notre client Debian

```
# Generated by NetworkManager
domain vetele.mv
search vetele.mv
nameserver 192.168.100.50
nameserver 192.168.100.51
```

3- Configuration de la redondance DHCP

Voici la configuration DHCP du serveur principal « maitre » du fichier */etc/dhcp/dhcpd.conf*

Il faut renseigner le serveur principal ainsi que le secondaire. Enfin, nous renseignons la plage d'adresse IP à distribuer. Des informations aussi telles que le port, ou des délais de réponses sont importants pour le fonctionnement de notre service DHCP.

```
GNU nano 7.2 /etc/dhcp/dhcpd.conf
# dhcpd.conf
option domain-name "vetele.mv";
option domain-name-servers 192.168.100.50, 192.168.100.51;

default-lease-time 21966;
max-lease-time 42000;

ddns-update-style none;

authoritative;

log-facility local7;

subnet 192.168.100.0 netmask 255.255.255.0 {
}

failover peer "lanclient-failover" {
    primary;
    address 192.168.100.50;
    port 647;

    peer address 192.168.100.51;
    port 647;

    max-response-delay 60;
    max-unacked-updates 10;
    load balance max seconds 3;
    mclt 3600;
    split 128;
}

subnet 192.168.10.0 netmask 255.255.255.0 {
    option routers 192.168.100.254;

    pool {
        failover peer "lanclient-failover";
        range 192.168.10.1 192.168.10.200;
    }
}
```



Voici le fichier de configuration du serveur secondaire */etc/dhcp/dhcpd.conf* :

```
GNU nano 7.2 /etc/dhcp/dhcpd.conf
# dhcpd.conf
#
# Author:
#   Copyright 1995 by Internet Software Consortium.
#
# Permission to use, copy, modify and distribute this software and its
# documentation for any purpose and on any medium is hereby granted,
# provided that the copyright notice appear in all copies and be
# preserved in its entirety.
#
# This software is distributed in the hope that it will be useful,
# but WITHOUT ANY WARRANTY; without even the implied warranty of
# MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.
#
# The following configures a DHCP server on the local network.
#
# The server can be queried by any DHCP client; the initial broadcast
# is sent to all addresses on the local interface, and to other
# subnets which are advertised in the routers.
#
# The DHCP server has to bind to the interface eth0.
#
# If your interface is named eth0 you will need to set it here in the
#DHCPDv4_CONF=/etc/dhcp/dhcpd.conf
#DHCPDv6_CONF=/etc/dhcp/dhcpd6.conf

# Path to dhcpd's config file (default: /etc/dhcp/dhcpd.conf).
#DHCPDv4_CONF=/etc/dhcp/dhcpd.conf
#DHCPDv6_CONF=/etc/dhcp/dhcpd6.conf

# Path to dhcpd's PID file (default: /var/run/dhcpd.pid).
#DHCPDv4_PID=/var/run/dhcpd.pid
#DHCPDv6_PID=/var/run/dhcpd6.pid

# Additional options to start dhcpd with.
# Don't use options -cf or -pf here; use DHCPD_CONF/ DHCPD_PID instead
#OPTIONS=""

# On what interfaces should the DHCP server (dhcpd) serve DHCP requests?
# Separate multiple interfaces with spaces, e.g. "eth0 eth1".
INTERFACESv4="ens33"
INTERFACESv6=""

#
# A DHCP server can serve static addresses in a number of ways.
# The preselected addresses below represent the minimal configuration
# for a server where users expect to have the same address all the
# time.
#
# If you have multiple subnets, you may want to restrict the
# subnets on which this can happen.
#
# Subnet 192.168.100.0 netmask 255.255.255.0 {
#
#   failoverpeer "lanclient-failover"
#       secondary;
#       address 192.168.100.51
#       port 647;
#
#       peer address 192.168.100.50
#       peer port 647;
#
#       max-response-delay 60;
#       max-unacked-updates 10;
#       load balance max seconds 3;
#   }
#
# Subnet 192.168.10.0 netmask 255.255.255.0
# option routers 192.168.100.254
# pool{
#   failover peer "lanclient-failover";
#   range 192.168.10.1 192.168.10.200;
# }
```

Une fois, les fichiers de configuration de nos deux serveurs complétés, nous devons configurer l'interface sur laquelle le service DHCP va être à l'écoute. Nous devons atteindre ce fichier :

/etc/default/isc-dhcp-server , et faire la configuration ci-dessous, sur les deux serveurs.

```
GNU nano 7.2 /etc/default/isc-dhcp-server
# Defaults for isc-dhcp-server (sourced by /etc/init.d/isc-dhcp-server)
#
# Path to dhcpd's config file (default: /etc/dhcp/dhcpd.conf).
#DHCPDv4_CONF=/etc/dhcp/dhcpd.conf
#DHCPDv6_CONF=/etc/dhcp/dhcpd6.conf
#
# Path to dhcpd's PID file (default: /var/run/dhcpd.pid).
#DHCPDv4_PID=/var/run/dhcpd.pid
#DHCPDv6_PID=/var/run/dhcpd6.pid
#
# Additional options to start dhcpd with.
# Don't use options -cf or -pf here; use DHCPD_CONF/ DHCPD_PID instead
#OPTIONS=""
#
# On what interfaces should the DHCP server (dhcpd) serve DHCP requests?
# Separate multiple interfaces with spaces, e.g. "eth0 eth1".
INTERFACESv4="ens33"
INTERFACESv6=""
```



Enfin, nous allons devoir activer le relai DHCP sur notre routeur PfSense :

Services / Relais DHCP

Configuration de relais DHCP

Activer ☒ Enable DHCP Relay

Downstream Interfaces

WAN
LANCLT
LANSRV

Interfaces without an IPv4 address will not be shown.

CARP Status VIP aucun

DHCP Relay will be stopped when the chosen VIP is in BACKUP status, and started in MASTER status.

☒ Ajouter l'ID du circuit et l'ID de l'agent aux requêtes
Append the circuit ID (interface number) and the agent ID to the DHCP request.

Upstream Servers

192.168.100.50	Supprimer
192.168.100.51	Supprimer

[+ Add Upstream Server](#)

The IPv4 addresses of the servers to which DHCP requests are relayed.

Nous pouvons ensuite vérifier sur nos clients, afin de voir si ils récupèrent bien un adresse IP.

Linux : ***dhclient -r*** puis ***dhclient*** et enfin ***ip a***

Windows: ***ipconfig /release*** puis ***ipconfig /renew*** et enfin ***ipconfig***



4- Configuration du DNS

Nous allons maintenant configurer le service DNS.

Notre srv-deb2 sera le serveur DNS principal, et srv-deb1 sera notre secondaire.

Nous allons commencer par créer une redirection « non-conditionnelle » via ce fichier :
/etc/bind/named.conf.options

```
GNU nano 7.2 /etc/bind/named.conf.options
options {
    directory "/var/cache/bind";

    // If there is a firewall between you and nameservers you want
    // to talk to, you may need to fix the firewall to allow multiple
    // ports to talk. See http://www.kb.cert.org/vuls/id/800113

    // If your ISP provided one or more IP addresses for stable
    // nameservers, you probably want to use them as forwarders.
    // Uncomment the following block, and insert the addresses replacing
    // the all-0's placeholder.

    forwarders {
        1.1.1.1;
    };

    //=====  

    // If BIND logs error messages about the root key being expired,  

    // you will need to update your keys. See https://www.isc.org/bind-keys  

    //=====  

    dnssec-validation auto;  

    allow-query { any; };  

    listen-on-v6 { any; };
};
```

Voici la configuration du fichier ***/etc/bind/named.conf.local*** du serveur principal. Ce fichier est le fichier où nous renseignons les zones, à la fois directes et inverses. Nous y autorisons aussi le transfert de zone, du serveur principal vers le secondaire.

```
GNU nano 7.2 /etc/bind/named.conf.local
//  

// Do any local configuration here  

//  

// Consider adding the 1918 zones here, if they are not used in your  

// organization  

//include "/etc/bind/zones.rfc1918";  

  

zone "vetele.mv" {  
    type master;  
    file "db.vetele.mv";  
    allow-transfer {192.168.100.50; };  
    allow-query { any; };  
    notify yes;  
};  

  

zone "100.168.192.in-addr.arpa" {  
    type master;  
    file "db.inv.100.168.192";  
    allow-transfer {192.168.100.50; };  
    allow-query { any; };  
    notify yes;  
};  

  

zone "10.168.192.in-addr.arpa" {  
    type master;  
    file "db.inv.10.168.192";  
    allow-transfer {192.168.100.50; };  
    allow-query { any; };  
    notify yes;  
};
```



Nous allons devoir créer les fichiers de configurations de nos différentes zones.

Pour faire ceci proprement, il existe des fichiers « templates » (/etc/bind/), à copier ici :
/var/cache/bind/ :

```
root@srv-deb2:/var/cache/bind# ls
db.inv.100.168.192  db.inv.10.168.192  db.vetele.mv
```

```
GNU nano 7.2 db.vetele.mv
;
; BIND data file for local loopback interface
;
$TTL      604800
@         IN      SOA      srv-deb1.vetele.mv. root.srv-deb2.vetele.mv. (
                        2      ; Serial
                        604800 ; Refresh
                        86400  ; Retry
                        2419200 ; Expire
                        604800 ) ; Negative Cache TTL
;
@         IN      NS       srv-deb2.vetele.mv.
@         IN      A        192.168.100.51
@         IN      NS       srv-deb1.vetele.mv.
@         IN      A        192.168.100.50
srv-deb1  IN      A        192.168.100.50
srv-deb2  IN      A        192.168.100.51
LANSRV    IN      A        192.168.100.254
LANCLT    IN      A        192.168.10.254
```

Faites de même pour toutes vos zones (dont les zones inverses).

```
GNU nano 7.2 db.inv.100.168.192
;
; BIND reverse data file for local loopback interface
;
$TTL      604800
@         IN      SOA      srv-deb1.vetele.mv. root.srv-deb2.vetele.mv. (
                        1      ; Serial
                        604800 ; Refresh
                        86400  ; Retry
                        2419200 ; Expire
                        604800 ) ; Negative Cache TTL
;
@         IN      NS       srv-deb1.vetele.mv.
@         IN      NS       srv-deb2.vetele.mv.
srv-deb1  IN      A        192.168.100.50
srv-deb2  IN      A        192.168.100.51
50        IN      PTR      srv-deb1.vetele.mv.
51        IN      PTR      srv-deb2.vetele.mv.
254       IN      PTR      LANSRV.vetele.mv.
```



```
GNU nano 7.2 db.inv.10.168.192
;
; BIND reverse data file for local loopback interface
;
$TTL      604800
@         IN      SOA      srv-deb1.vetele.mv. root.srv-deb2.vetele.mv. (
                        1      ; Serial
                        604800  ; Refresh
                        86400   ; Retry
                        2419200 ; Expire
                        604800 ) ; Negative Cache TTL
;
@         IN      NS       srv-deb1.vetele.mv.
@         IN      NS       srv-deb2.vetele.mv.
srv-deb1  IN      A        192.168.100.50
srv-deb2  IN      A        192.168.100.51
LANCLT    IN      A        192.168.10.254
254       IN      PTR      LANCLT.vetele.mv.
```

Rechargeons le service DNS afin qu'il puisse prendre en compte les modifications récentes, avec la commande ***rndc reload***.

Nous pouvons ensuite tester s'il y a des erreurs dans nos fichiers de configurations avec les commandes : ***named-checkconf -z*** et ***named-checkzone vetele.mv /var/cache/bind/db.vetele.mv***

Configurons ensuite notre serveur secondaire (srv-deb1) via ce fichier ***/etc/bind/named.conf.local*** :

```
GNU nano 7.2 /etc/bind/named.conf.local
//
// Do any local configuration here
//
// Consider adding the 1918 zones here, if they are not used in your
// organization
//include "/etc/bind/zones.rfc1918";

zone "vetele.mv" {
    type master;
    file "db.vetele.mv";
    allow-transfer {192.168.100.50; };
    allow-query { any; };
    notify yes;
};

zone "100.168.192.in-addr.arpa" {
    type master;
    file "db.inv.100.168.192";
    allow-transfer {192.168.100.50; };
    allow-query { any; };
    notify yes;
};

zone "10.168.192.in-addr.arpa" {
    type master;
    file "db.inv.10.168.192";
    allow-transfer {192.168.100.50; };
    allow-query { any; };
    notify yes;
};
```



Bien sûr, il ne faut pas oublier de renseigner nos deux serveurs DNS sur notre PfSense via les paramètres généraux du routeur.

Paramètres du serveur DNS	
Serveurs DNS	<div><div>192.168.100.50</div><div>DNS Hostname</div><div>Supprimer</div></div> <div><div>192.168.100.51</div><div>DNS Hostname</div><div>Supprimer</div></div> <div><div>Adresse</div><div>Saisir les adresses IP des serveurs DNS utilisés par le système. Ceux-ci sont également utilisés pour le service DHCP, le DNS Forwarder et le serveur de résolution DNS lorsqu'il est activé.</div></div> <div><div>Nom d'hôte</div><div>Enter the DNS Server Hostname for TLS Verification in the DNS Resolver (optional).</div></div>
Ajouter un serveur DNS	<div>+ Ajouter un serveur DNS</div>
Remplacer le serveur DNS	<div><input type="checkbox"/> Allow DNS server list to be overridden by DHCP/PPP on WAN or remote OpenVPN server</div> <div>If this option is set, pfSense will use DNS servers assigned by a DHCP/PPP server on WAN or a remote OpenVPN server (if Pull DNS option is enabled) for its own purposes (including the DNS Forwarder/DNS Resolver). However, they will not be assigned to DHCP clients.</div>
DNS Resolution Behavior	<div>Use remote DNS Servers, ignore local DNS</div> <div>By default the firewall will use local DNS service (127.0.0.1, DNS Resolver or Forwarder) as the first DNS server when possible, and it will fall back to remote DNS servers otherwise. Use this option to choose alternate behaviors.</div>

Nous pouvons enfin tester sur nos clients avec des *nslookup*

5- Conclusion

Nous avons maintenant configuré correctement les services DHCP et DNS redondés, afin d'assurer la haute disponibilité des services.