

# Mission 2 - Haute disponibilité

## Sommaire :

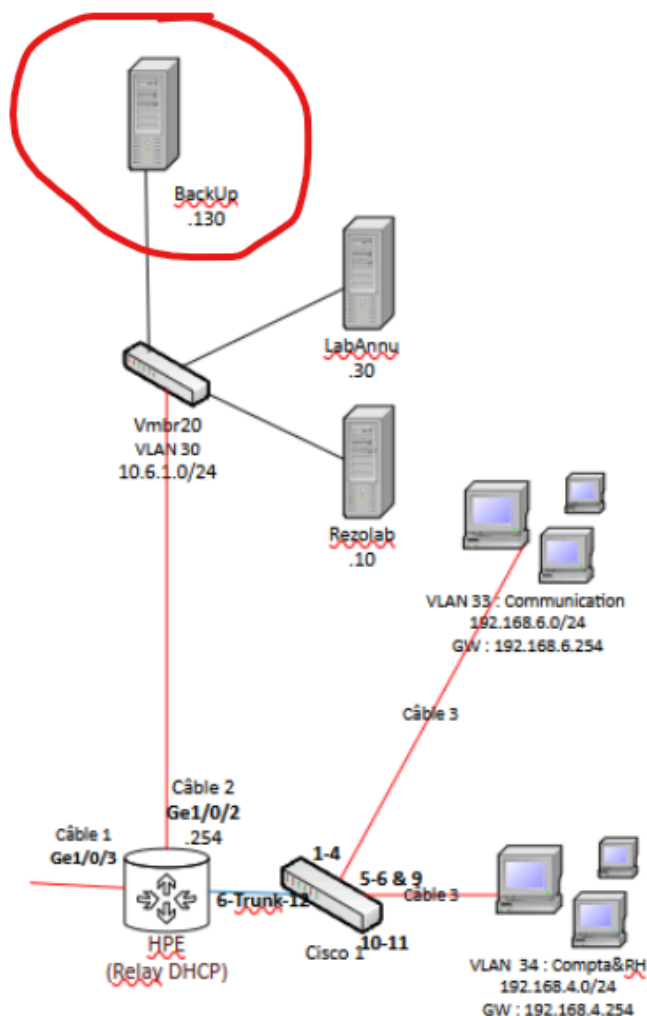
<b>Objectifs :</b> .....	<b>1</b>
<b>1. Création d'un serveur secondaire DNS.....</b>	<b>2</b>
→ Connecter BACKUP au domaine locale gsbx.....	2
- Pour créer le second serveur DNS :.....	3
<b>2. Création d'un second contrôleur de domaine Active Directory.....</b>	<b>6</b>
<b>3. Création d'un second serveur DHCP avec load-balancing.....</b>	<b>8</b>
1ère Partie sur Putty.....	8
2ème Partie sur nos serveurs.....	10
→ Ajout du serveur BACKUP sur Rezolab.....	10
→ Basculement vers le serveur Backup.....	11
• Sélectionner les étendues que vous souhaitez basculer.....	12
• Donner l'adresse IP du serveur sur lequel le basculement doit être effectué...	13
• Mettre un secret partagé (secret).....	13
• Puis le valider.....	14
Configuration des Switchs.....	16
<b>1. Redondance de routeurs avec protocole VRRP.....</b>	<b>17</b>
CISCO 2.....	17
HPE PRINCIPAL.....	18
HPE DE SECOURS.....	20
Configuration VRRP REZOLAB.....	22
Sécurisation DHCP.....	25

# Objectifs :

L'objectif de cette nouvelle mission sera de mettre en place un nouveau serveur " BACKUP " afin :

- d'améliorer la haute disponibilité, c'est-à-dire que notre réseau soit accessible et fiable 100 % du temps grâce à notre nouveau serveur
- de créer un second contrôleur de domaine
- d'améliorer la répartition des charges avec un second serveur DHCP
- d'améliorer la sécurité des switches

## Schéma de L'objectif :



# 1. Création d'un serveur secondaire DNS

Nous allons tout d'abord créer le serveur " BACKUP " et le connecter au vmbr 4 pour qu'il fasse partie du réseau 10.x.1.0/24

Il aura pour adresse IP 10.5.1.130/24 et pour passerelle 10.5.1.254

```
arte Ethernet Ethernet :  
Suffixe DNS propre à la connexion. . . :  
Adresse IPv6 de liaison locale. . . . : fe80::3e16:cdc0:29c6:7a2b%4  
Adresse IPv4. . . . . : 10.6.1.130  
Masque de sous-réseau. . . . . : 255.255.255.0  
Passerelle par défaut. . . . . : 10.6.1.254
```

On vérifie que BACKUP arrive à ping Labannu et Rezolab


```
C:\Users\Administrateur>ping 10.6.1.30  
  
Envoi d'une requête 'Ping' 10.6.1.30 avec 32 octets de données :  
Réponse de 10.6.1.30 : octets=32 temps<1ms TTL=128  
Réponse de 10.6.1.30 : octets=32 temps<1ms TTL=128  
Réponse de 10.6.1.30 : octets=32 temps<1ms TTL=128
```

```
C:\Users\Administrateur>ping 10.6.1.10  
  
Envoi d'une requête 'Ping' 10.6.1.10 avec 32 octets de données :  
Réponse de 10.6.1.10 : octets=32 temps<1ms TTL=128  
Réponse de 10.6.1.10 : octets=32 temps<1ms TTL=128  
Réponse de 10.6.1.10 : octets=32 temps<1ms TTL=128
```

## → Connecter BACKUP au domaine locale gsbx

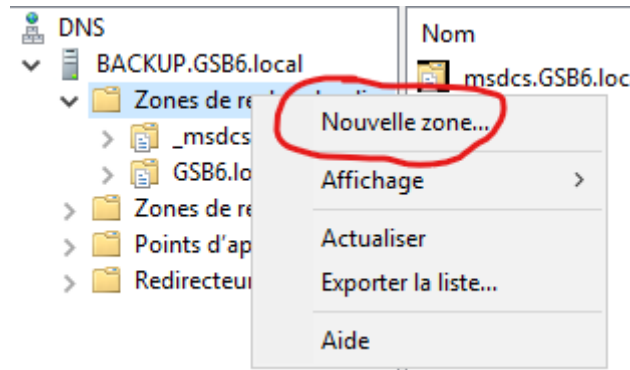
Ce pc, clique droit, propriété, modifier les paramètre et se connecter au domaine GSB5.local en administrateur

Paramètres de nom d'ordinateur, de domaine et de groupe de travail

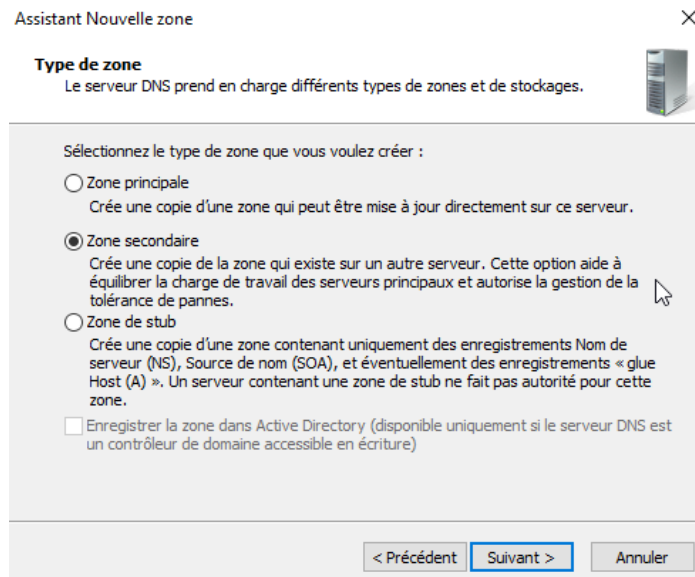
Nom de l'ordinateur :	BACKUP	
Nom complet :	BACKUP.GSB5.local	
Description de l'ordinateur :		
Domaine :	GSB5.local	

- Pour créer le second serveur DNS :

- clique droit sur “Zone de recherche directe”, puis “Nouvelle zone”



- Cocher la case “Zone secondaire”



- Donner le nom de la zone

Assistant Nouvelle zone

**Nom de la zone**  
Quel est le nom de la nouvelle zone ?

Le nom de la zone spécifie la partie de l'espace de noms DNS pour laquelle ce serveur fait autorité. Il peut s'agir du nom de domaine de votre société (par exemple, microsoft.com) ou d'une partie du nom de domaine (par exemple, nouvelle\_zone.microsoft.com). Le nom de zone n'est pas le nom du serveur DNS.

Nom de la zone :

BACKUP.local

< Précédent Suivant > Annuler

- Donner l'IP du serveur maître (ici Labannu)

Assistant Nouvelle zone

**Serveurs DNS maîtres**  
La zone secondaire est copiée à partir d'un ou de plusieurs serveurs DNS.

Spécifiez les serveurs DNS à partir desquels vous voulez copier la zone. Les serveurs sont contactés dans l'ordre indiqué.

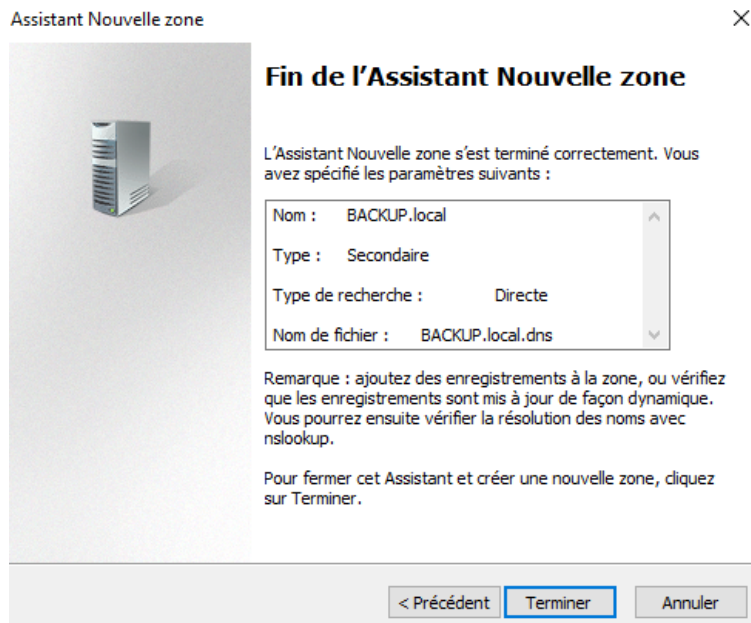
Serveurs maîtres :

Adresse IP	Nom de domaine ...	Validé
<Cliquez ici po...		
10.6.1.30		

Supprimer Monter Descendre

< Précédent Suivant > Annuler

- Puis appuyer sur “Terminer”



Après la création de la zone secondaire DNS sur BACKUP on arrive bien à récupérer la zone principale de Labannu

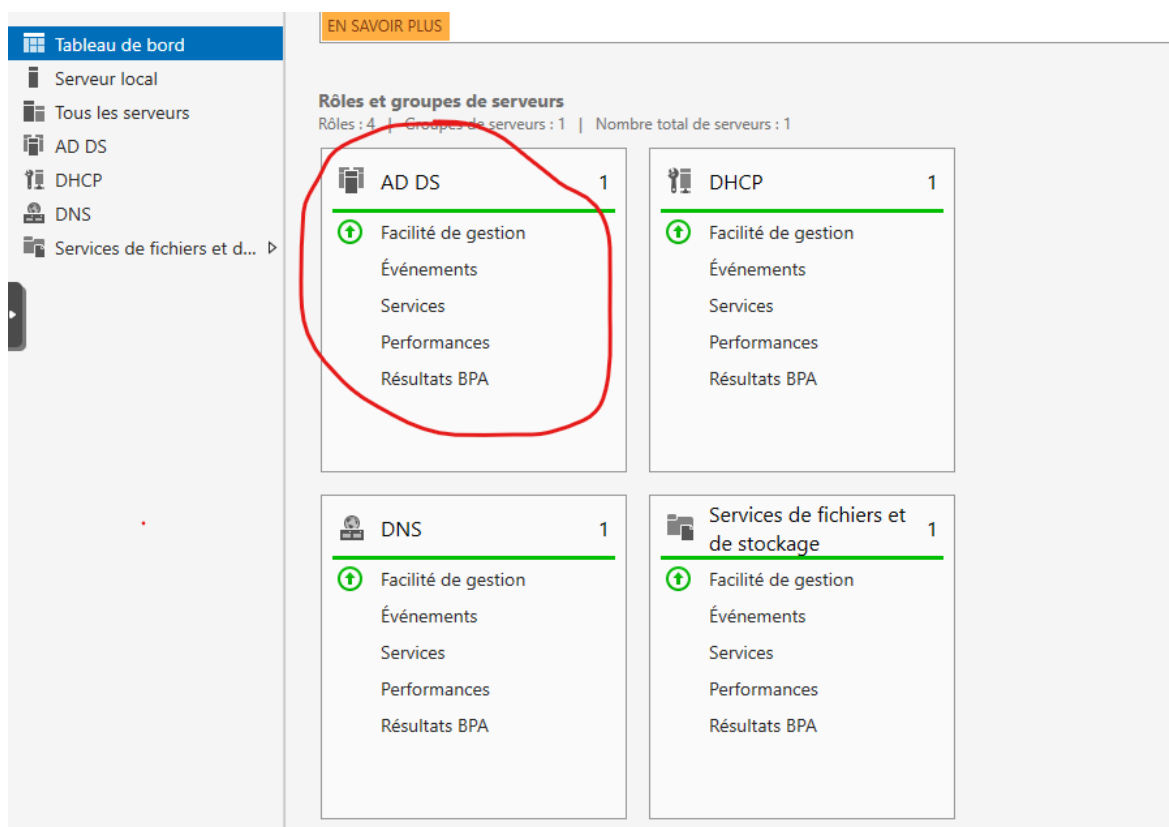
	Nom	Type	Données	Horodate
DNS				
BACKUP				
BACKUP.GSB5.local				
Zones de recherche direc				
gsb5.local				
_msdcs	_msdcs			
_sites	_sites			
_tcp	_tcp			
_udp	_udp			
DomainDnsZones	DomainDnsZones			
ForestDnsZones	ForestDnsZones			
(identique au dossier parent)	(identique au dossier parent)	Source de nom (SOA)	[154], labannu.gsb5.local,...	statique
(identique au dossier parent)	(identique au dossier parent)	Serveur de noms (NS)	BACKUP.	statique
(identique au dossier parent)	(identique au dossier parent)	Serveur de noms (NS)	labannu.gsb5.local.	statique
(identique au dossier parent)	(identique au dossier parent)	Hôte (A)	10.5.1.30	statique
BACKUP	BACKUP	Hôte (A)	10.5.1.130	statique
labannu	labannu	Hôte (A)	10.5.1.30	statique
Zones de recherche inver				
Points d'approbation				
Redirecteurs conditionne				

## 2. Création d'un second contrôleur de domaine Active Directory

Nous allons maintenant créer un second contrôleur de domaine Active Directory

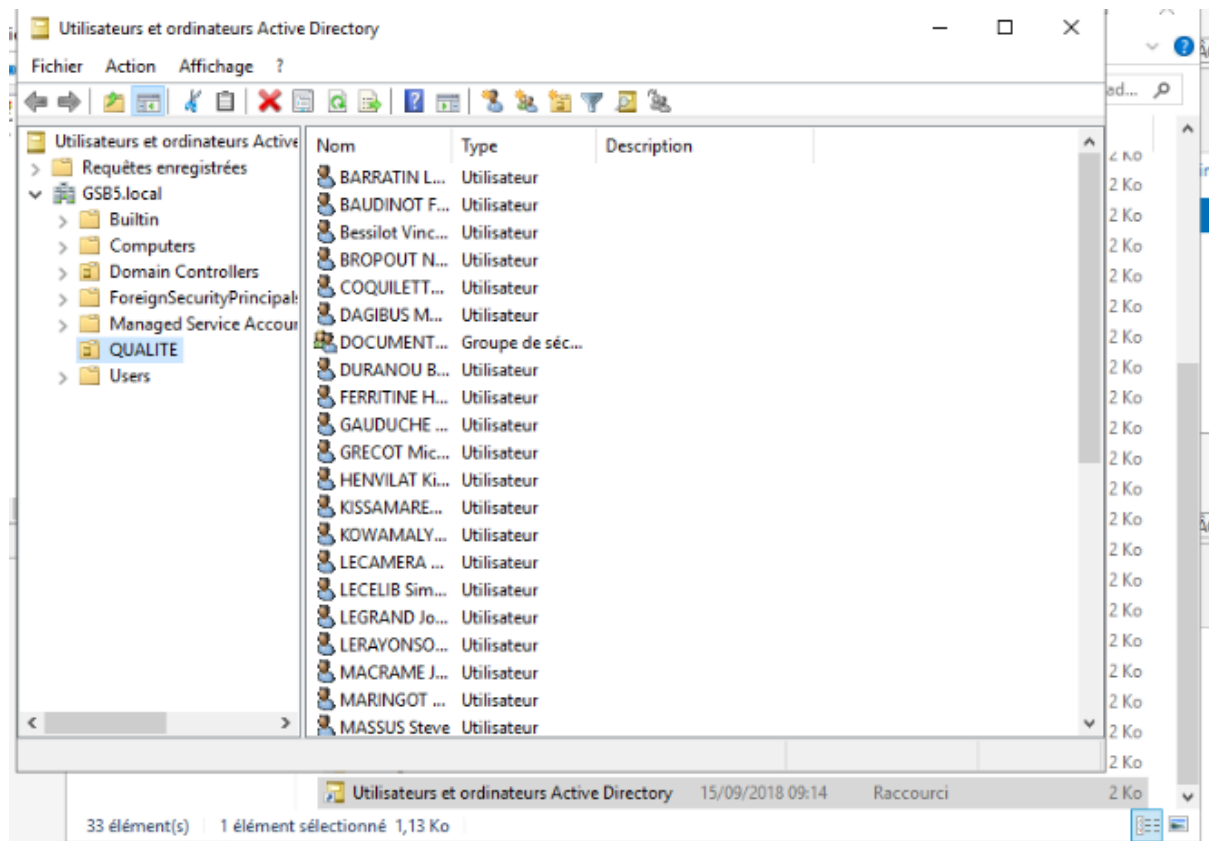
Pour ce faire, nous allons Ajouter des Rôles et Fonctionnalité et installer le serveur AD DS sur le gestionnaire de serveur de BACKUP

Allez dans Gérer > Ajouter des rôles et fonctionnalités > Rôles de serveurs > Service AD DS, Puis faire l'installation



Pour vérifier si notre second contrôleur de domaine fonctionne, il faut éteindre le serveur principal (Labannu) et regarder si on trouve bien nos clients sur l'Active Directory. Le second contrôleur de domaine sur BACKUP devrait prendre le relai et les clients devraient apparaître

- On retrouve bien nos clients sur BACKUP lorsque Labannu est éteint





### 3. Création d'un second serveur DHCP avec load-balancing

Nous allons ici créer un basculement DHCP sur le second serveur afin de retrouver nos étendues

#### 1ère Partie sur Putty

##### A. HPE

Ajout du nouveau relai DHCP sur les vlans 53, 54 et 58

```
interface Vlan-interface53
ip binding vpn-instance lafrej
ip address 192.168.3.254 255.255.255.0
dhcp select relay
dhcp relay server-address 10.5.1.10
dhcp relay server-address 10.5.1.130
#
interface Vlan-interface54
ip binding vpn-instance lafrej
ip address 192.168.4.254 255.255.255.0
dhcp select relay
dhcp relay server-address 10.5.1.10
dhcp relay server-address 10.5.1.130
#
interface Vlan-interface58
ip binding vpn-instance lafrej
ip address 192.168.8.254 255.255.255.0
dhcp select relay
dhcp relay server-address 10.5.1.10
dhcp relay server-address 10.5.1.130
#
```

Ajout du vlan 58 sur l'interface Gig1/0/1 en mode trunk

```
interface GigabitEthernet1/0/1
port link-mode bridge
port link-type trunk
port trunk permit vlan 1 53 to 54 58
```

## B. CISCO

Ajout du vlan sur les vlan 58 sur fa0/11

```
interface FastEthernet0/11
switchport access vlan 58
```

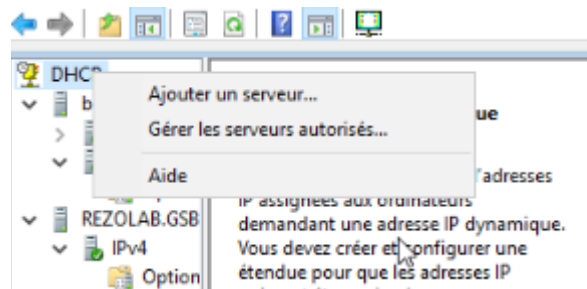
Ajout du vlan 53 54 58 en mode trunk fa0/12

```
interface FastEthernet0/12
switchport trunk allowed vlan 53,54,58
switchport mode trunk
```

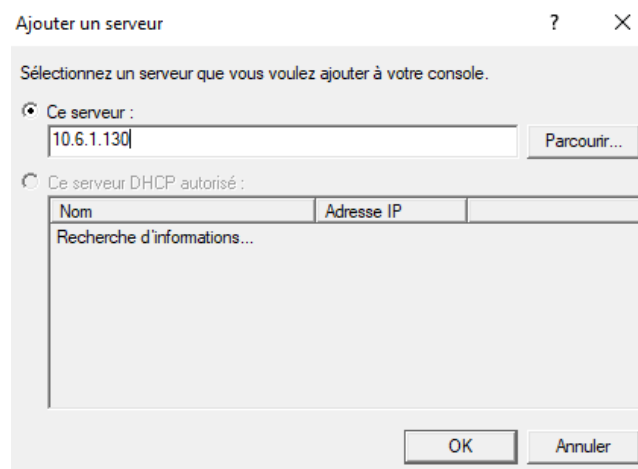
## 2ème Partie sur nos serveurs

### → Ajout du serveur BACKUP sur Rezolab

- Cliquez droit sur DHCP, Ajouter un serveur

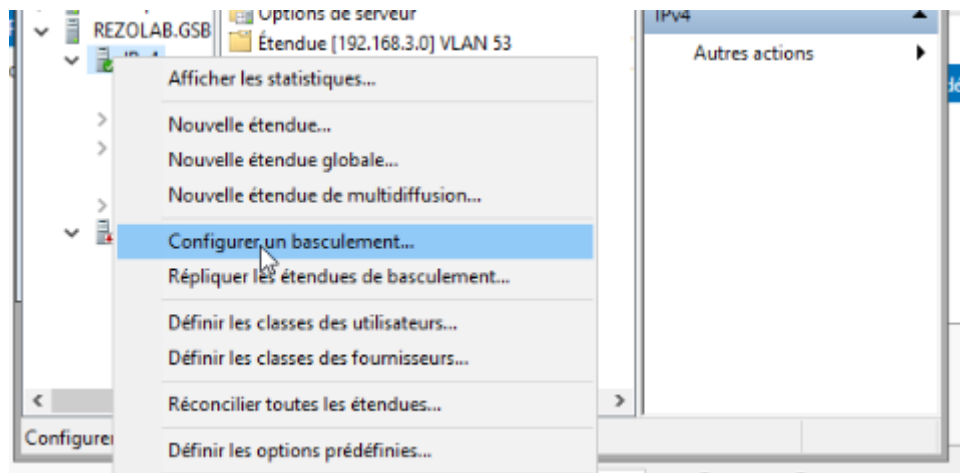


- Donner l'IP du serveur BACKUP 10.5.6.130, puis " OK "



## → Basculement vers le serveur Backup

- Cliquez droit IPv4 sur Rezolab, puis “ Configurer un basculement “



- Nous retrouvons ici les étendues 192.168.4.0 qui correspond au VLAN 54, 192.168.3.0 qui correspond au VLAN 53 et le 192.168.8.0 qui correspond au VLAN 58
- Sélectionner les étendues que vous souhaitez basculer

Configurer un basculement



Introduction au basculement DHCP

Le basculement DHCP permet la haute disponibilité des services DHCP en synchronisant les informations des baux d'adresses IP entre deux serveurs DHCP. Le basculement DHCP fournit également un équilibrage de charge en matière de requêtes DHCP.

Cet Assistant vous guide tout au long de la configuration du basculement DHCP. Sélectionnez dans la liste suivante les étendues disponibles pouvant être configurées pour une haute disponibilité. Les étendues déjà configurées pour une haute disponibilité ne figurent pas dans la liste ci-dessous.

Étendues disponibles : ☒ Sélectionner tout

192.168.8.0
192.168.4.0
192.168.3.0

< Précédent Suivant > Annuler

- Donner l'adresse IP du serveur sur lequel le basculement doit être effectué

Configurer un basculement

**Spécifier le serveur partenaire à utiliser pour le basculement**

Indiquez le nom d'hôte ou l'adresse IP du serveur DHCP partenaire à utiliser pour la configuration du basculement.

Vous pouvez effectuer votre sélection parmi la liste des serveurs avec une configuration de basculement existant, ou vous pouvez rechercher et sélectionner le serveur approprié dans la liste des serveurs DHCP autorisés.

Vous pouvez également taper le nom d'hôte ou l'adresse IP du serveur partenaire.

Serveur partenaire :

☐ Réutiliser les relations de basculement existantes configurées avec ce serveur (le cas échéant).

< Précédent **Suivant >** Annuler

- Mettre un secret partagé (secret)
- Mettre en mode équilibrage de charge (load balancing)

Configurer un basculement

**Créer une relation de basculement**

Créer une relation de basculement avec le partenaire 10.6.1.130

Nom de la relation :

Délai de transition maximal du client (MCLT) :  heures  minutes

Mode :

Pourcentage d'équilibrage de charge

Serveur local :  %

Serveur partenaire :  %

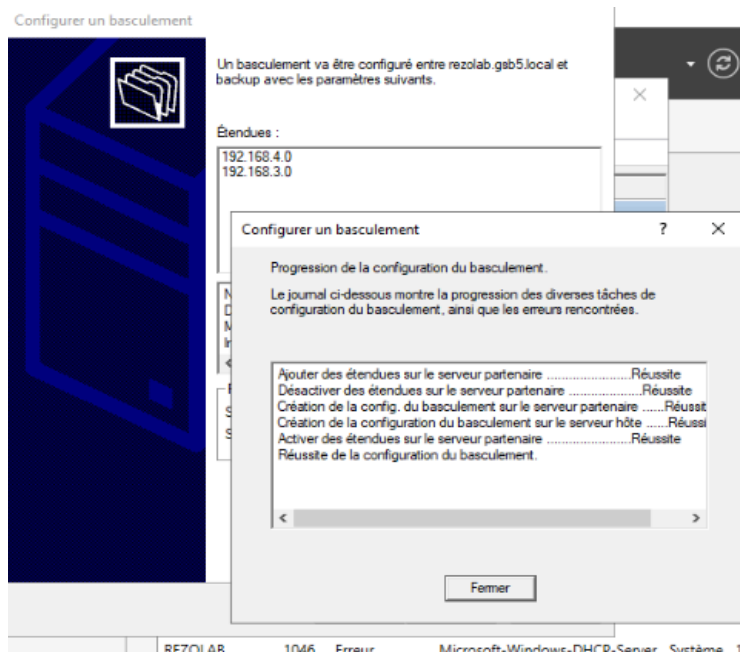
☐ Intervalle de basculement d'état :  minutes

☒ Activer l'authentification du message

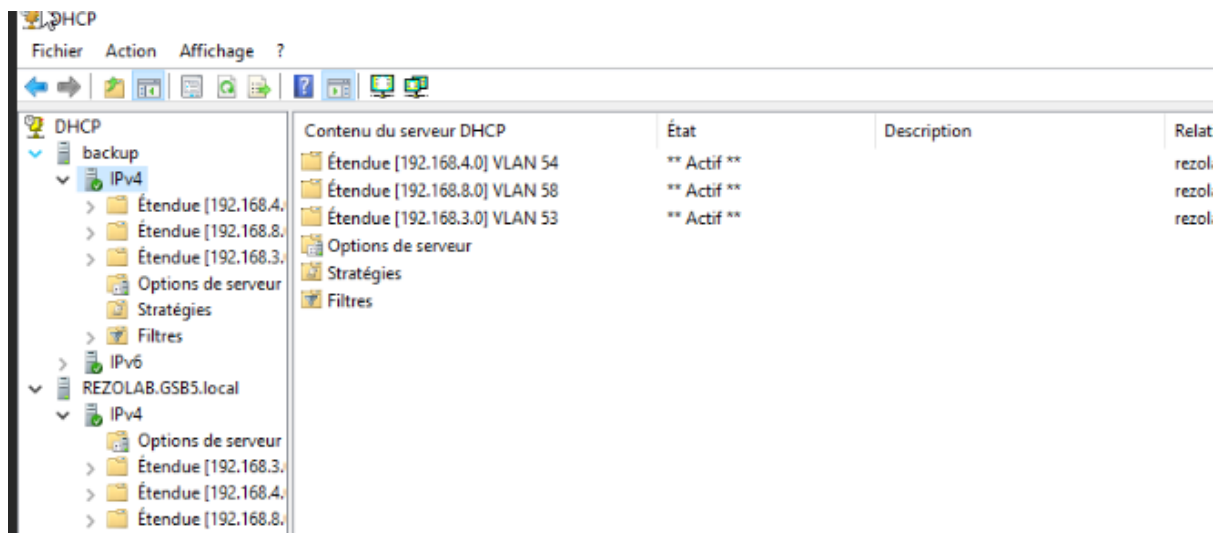
Secret partagé :

< Précédent **Suivant >** Annuler

- Puis le valider



Nous retrouvons sur Rezolab le serveur Backup



Puis sur Backup, nous retrouvons bien le basculement DHCP avec les étendues correspondantes

DHCP	Contenu du serveur DHCP	État	Description	Relation de basculi
▼ backup.gsb5.l	Options de serveur			
▼ IPv4	Étendue [192.168.3.0] VLAN 53	** Actif **		rezolab.gsb5.local-
> Option	Étendue [192.168.4.0] VLAN 54	** Actif **		rezolab.gsb5.local-
> Étendu	Étendue [192.168.8.0] VLAN 58	** Actif **		rezolab.gsb5.local-
> Étendu	Stratégies			
> Étendu	Filtres			
> Stratég				
> Filtres				
> IPv6				



## **Configuration des Switchs**

**Vous trouverez la configuration de mes switchs dans un dossier excel à part.**

# 1. Redondance de routeurs avec protocole VRRP

Le but de la redondance de routeurs avec le protocole VRRP est d'assurer la disponibilité continue du réseau en permettant à un routeur HPE de secours de prendre automatiquement le relais en cas de défaillance de notre routeur HPE, garantissant ainsi une connectivité ininterrompue pour les périphériques du réseau.

## CISCO 2

Sur notre nouveau switch cisco, nous avons ajouté les vlan 50 et 59 sur les ports 1 à 6 qui sont reliés au HPE principale et au HPE de secours, on a aussi brancher nos câbles proxmox 1 et 2 dessus.

```
interface FastEthernet0/1
  switchport access vlan 50
  switchport mode access
!
interface FastEthernet0/2
  switchport access vlan 50
  switchport mode access
!
interface FastEthernet0/3
  switchport access vlan 50
  switchport mode access
!
interface FastEthernet0/4
  switchport access vlan 59
  switchport mode access
!
interface FastEthernet0/5
  switchport access vlan 59
  switchport mode access
!
interface FastEthernet0/6
  switchport access vlan 59
```

## HPE PRINCIPAL

Sur mon HPE pas besoin de recréer les vlan 53, 54, 58 et 59 car ils sont déjà présent, par conséquent il faudra les recréer sur le routeur de secours. Pareil pour les vpn instance

Sur chaque interface de vlan je vais mettre en place un vrrp avec une adresse ip commune et mettre une priorité de 120 sur le routeur principal.

Exemple sur l'interface du vlan 53

vrrp vrid 5 virtual-ip 192.168.3.250

vrrp vrid 5 priority 120

Exemple sur l'interface du vlan 54

vrrp vrid 5 virtual-ip 192.168.4.250

vrrp vrid 5 priority 120

```

interface Vlan-interface50
 ip binding vpn-instance lafrej
 ip address 10.5.1.254 255.255.255.0
 vrrp vrid 5 virtual-ip 10.5.1.250
 vrrp vrid 5 priority 120
#
interface Vlan-interface53
 ip binding vpn-instance lafrej
 ip address 192.168.3.254 255.255.255.0
 vrrp vrid 5 virtual-ip 192.168.3.250
 vrrp vrid 5 priority 120
 dhcp select relay
 dhcp relay server-address 10.5.1.10
 dhcp relay server-address 10.5.1.130
#
interface Vlan-interface54
 ip binding vpn-instance lafrej
 ip address 192.168.4.254 255.255.255.0
 vrrp vrid 5 virtual-ip 192.168.4.250
 vrrp vrid 5 priority 120
 dhcp select relay

```

```

interface Vlan-interface58
 ip binding vpn-instance lafrej
 ip address 192.168.8.254 255.255.255.0
 vrrp vrid 5 virtual-ip 192.168.8.250
 vrrp vrid 5 priority 120
 dhcp select relay
 dhcp relay server-address 10.5.1.10
 dhcp relay server-address 10.5.1.130
#
interface Vlan-interface59
 ip binding vpn-instance lafrej
 ip address 10.5.2.1 255.255.255.0
 vrrp vrid 5 virtual-ip 10.5.2.250
 vrrp vrid 5 priority 120

```

## HPE DE SECOURS

Maintenant on va mettre en place un routeur HPE de secours qui va prendre automatiquement le relais en cas de défaillance de notre routeur principal. Pour commencer nous allons créer mes vlan 50 et 59 qu'on mettra sur un port chacun et les vlan 53,54,58 qu'on mettra en trunk sur un port.

```
The VLANs include:  
1(default), 50, 53-54, 58-59,  
...
```

```
#  
interface GigabitEthernet1/0/13  
port link-mode bridge  
port access vlan 50  
#  
interface GigabitEthernet1/0/14  
port link-mode bridge  
port link-type trunk  
port trunk permit vlan 1 53 to 54 58  
#  
interface GigabitEthernet1/0/15  
port link-mode bridge  
port access vlan 59  
#
```

Ensuite nous allons créer un vpn instance sur chaque interfaces de nos vlan au nom de lafrej, leurs donner une adresse ip avec une passerelle de 253 puisque 254 est utiliser sur notre routeur principal, mais encore un vrrp avec des adresses ip virtuelles communes à nos 2 routeurs qui finissent en 250 et pour finir sur nos vlan 53,54 et 58 qui sont nos postes

clients, mettre en place un agent de relais dhcp qui va permettre d'attribuer des adresses automatiquement sur nos clients. Pour résumer on a refait la configuration de notre HPE principal

```
#
interface Vlan-interface50
 ip binding vpn-instance lafrej
 ip address 10.5.1.253 255.255.255.0
 vrrp vrid 5 virtual-ip 10.5.1.250
#
interface Vlan-interface53
 ip binding vpn-instance lafrej
 ip address 192.168.3.253 255.255.255.0
 vrrp vrid 5 virtual-ip 192.168.3.250
 dhcp select relay
 dhcp relay server-address 10.5.1.10
 dhcp relay server-address 10.5.1.130
#
interface Vlan-interface54
---- More ----%Jan 10 00:47:54:530 2013
 ip binding vpn-instance lafrej
 ip address 192.168.4.253 255.255.255.0
 vrrp vrid 5 virtual-ip 192.168.4.250
 dhcp select relay
 dhcp relay server-address 10.5.1.10
 dhcp relay server-address 10.5.1.130
#
interface Vlan-interface58
 ip binding vpn-instance lafrej
 ip address 192.168.8.253 255.255.255.0
 vrrp vrid 5 virtual-ip 192.168.8.250
 dhcp select relay
 dhcp relay server-address 10.5.1.10
 dhcp relay server-address 10.5.1.130
#
interface Vlan-interface59
 ip binding vpn-instance lafrej
 ip address 10.5.2.1 255.255.255.0
 vrrp vrid 5 virtual-ip 10.5.2.250
#
```

## Configuration VRRP REZOLAB

Maintenant sur REZOLAB nous allons changer la passerelles sur nos étendues dhcp des vlan 53,54,58 qui sera désormais en 250 qui est en lien avec le vrrp. Pour pouvoir faire cela il faut aller dans un vlan sur le gestionnaire de serveur, options d'étendues et double cliquer sur le routeur.

Nom d'option	Fournisseur	Valeur	Nom de la stratégie
003 Routeur	Standard	192.168.4.254	Aucun
006 Serveurs DNS	Standard	10.5.1.30	Aucun
015 Nom de domaine DNS	Standard	rezolab	Aucun

192.168.4.254  
192.168.4.250

Ajouter  
Supprimer  
Monter  
Descendre

192.168.8.254

Ajouter  
Supprimer  
Monter  
Descendre

Adresse IP :  
  

192.168.3.254

Ajouter  
Supprimer  
Monter  
Descendre

On peut voir que si on fait un ipconfig sur l'invite de commande sur le poste client communication qui est le vlan 53 la passerelle qu'on a mis en place a bien été reconnue.

```
C:\Users\pergaud>ipconfig

Configuration IP de Windows

Carte Ethernet Ethernet :

    Suffixe DNS propre à la connexion. . . : gsb5.local
    Adresse IPv6 de liaison locale. . . . : fe80::cd1:8af0:9af:8c55%7
    Adresse IPv4. . . . . : 192.168.3.1
    Masque de sous-réseau. . . . . : 255.255.255.0
    Passerelle par défaut. . . . . : 192.168.3.250
```



Maintenant si on éteint notre routeur hpe principal et qu'on ping la passerelle commune depuis un poste client c'est le routeur hpe de secours qui devrait prendre le relai pour pouvoir communiquer.

Routeur HPE principal éteint :

```
C:\Users\pergaud>ping 192.168.4.250

Envoi d'une requête 'Ping' 192.168.4.250 avec 32 octets de données :
Réponse de 192.168.4.250 : octets=32 temps=1 ms TTL=255
Réponse de 192.168.4.250 : octets=32 temps<1ms TTL=255
Réponse de 192.168.4.250 : octets=32 temps<1ms TTL=255
Réponse de 192.168.4.250 : octets=32 temps<1ms TTL=255

Statistiques Ping pour 192.168.4.250:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 0ms, Maximum = 1ms, Moyenne = 0ms

C:\Users\pergaud>ping 192.168.3.250

Envoi d'une requête 'Ping' 192.168.3.250 avec 32 octets de données :
Réponse de 192.168.3.250 : octets=32 temps=1 ms TTL=255
Réponse de 192.168.3.250 : octets=32 temps<1ms TTL=255
Réponse de 192.168.3.250 : octets=32 temps<1ms TTL=255
Réponse de 192.168.3.250 : octets=32 temps=43 ms TTL=255

Statistiques Ping pour 192.168.3.250:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 0ms, Maximum = 43ms, Moyenne = 11ms

C:\Users\pergaud>ping 192.168.8.250

Envoi d'une requête 'Ping' 192.168.8.250 avec 32 octets de données :
Réponse de 192.168.8.250 : octets=32 temps=56 ms TTL=255
Réponse de 192.168.8.250 : octets=32 temps<1ms TTL=255
Réponse de 192.168.8.250 : octets=32 temps<1ms TTL=255
Réponse de 192.168.8.250 : octets=32 temps<1ms TTL=255

Statistiques Ping pour 192.168.8.250:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 0ms, Maximum = 56ms, Moyenne = 14ms
```

On peut voir que le ping passe, c'est-à-dire que la mise en place du routeur de secours a bien fonctionné et que si une panne intervient sur notre réseau, la communication entre les clients et les serveurs pourra continuer grâce à notre second routeur.

## Sécurisation DHCP

Nous allons mettre en place une sécurisation de notre DHCP avec un outil qui s'appelle le DHCP Snooping, combiné avec l'IP Source Guard, cela va nous permettre de surveiller et de filtrer le trafic DHCP dans notre réseau afin de prévenir les attaques ou les tentatives de détournement du trafic DHCP. Cela se fait en vérifiant et en validant les requêtes DHCP pour s'assurer qu'elles proviennent de sources légitimes.

Le DHCP Snooping implique la déclaration de ports de confiance par lesquels seules les demandes DHCP autorisées peuvent être reçues.

Ici, sur le routeur HPE principales, les Vlan 50, 53, 54, 58 et 59 sont sur les ports 1 à 3.

- Nous avons donc défini les interfaces par lesquelles le commutateur dialogue avec le serveur ou relai DHCP de confiance
- Puis nous avons activé l'IP Source Guard sur les interfaces connectées aux clients

```
interface GigabitEthernet1/0/1
port link-mode bridge
port link-type trunk
port trunk permit vlan 1 53 to 54 58
ip verify source ip-address mac-address
dhcp snooping trust
#
interface GigabitEthernet1/0/2
port link-mode bridge
port access vlan 50
ip verify source ip-address mac-address
dhcp snooping trust
#
interface GigabitEthernet1/0/3
port link-mode bridge
port access vlan 59
ip verify source ip-address mac-address
dhcp snooping trust
```