

Rapport de Mission : Assurer la continuité d'un serveur ou service



Préambule :

GSB veut s'assurer de la continuité de ses services. Pour cela j'ai choisi de partir sur la solution de la redondance sur le matériel : Firewall(externe), Routeur et serveur.

Pour ce faire je vais utiliser le protocole CARP pour le firewall, le protocole HSRP pour le routeur interne et la solution de redondance des services de Windows serveur pour le serveur LABANU (ADDS) et REZOLAB (DHCP)

SOMMAIRE

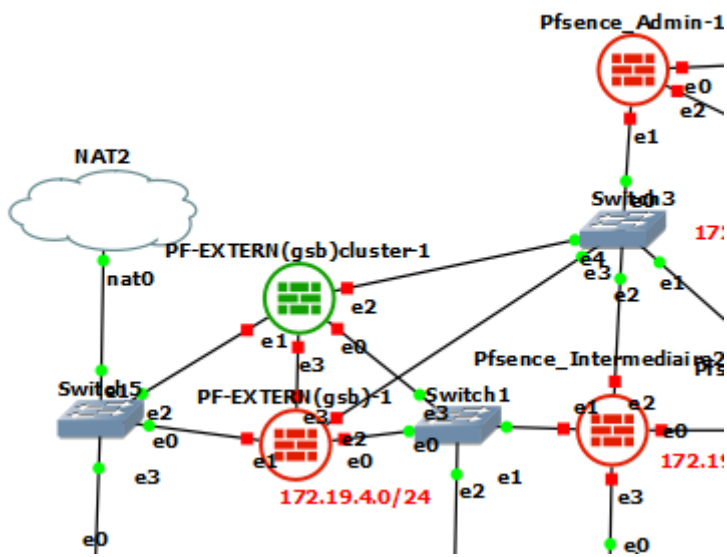
1. Redondance du firewall via CARP
 - a. Etape réaliser
 - b. Test de fonctionnement
2. Redondance Serveur
 - a. Serveur LABANU (ADDS)
 - b. Serveur REZOLAB (DHCP)

Redondance du firewall via CARP

Pour commencer que ce que CARP ?

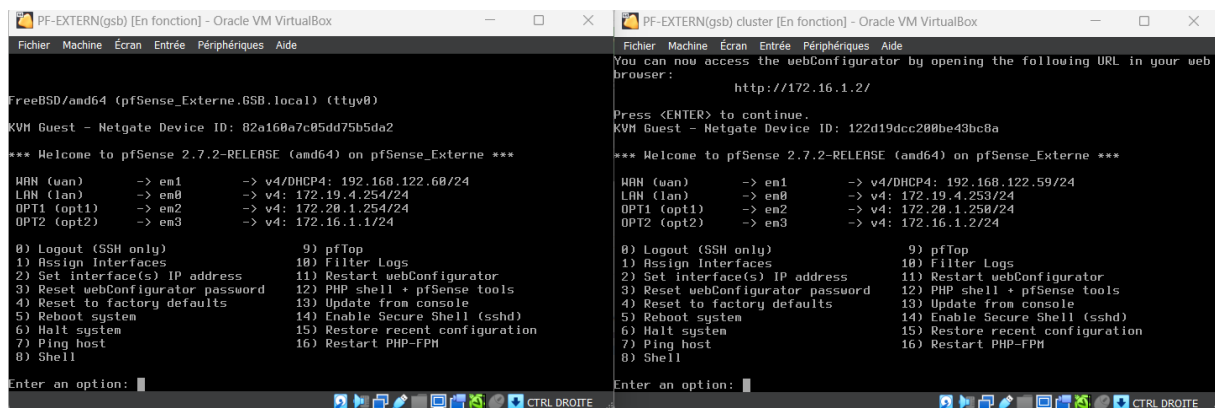
CARP (Common Address Redundancy Protocol) est un protocole de haute disponibilité utilisé dans les pare-feu comme pfSense. Il permet à plusieurs pare-feu de fonctionner ensemble de manière à assurer une redondance des adresses IP et une bascule automatique en cas de défaillance d'un appareil. Avec CARP, un ensemble de pare-feu peut partager une adresse IP virtuelle, assurant ainsi une continuité de service même en cas de panne matérielle ou logicielle sur l'un des appareils. Cela garantit une haute disponibilité et une résilience accrue pour les applications et les services critiques.

Présentation du schéma réaliser :

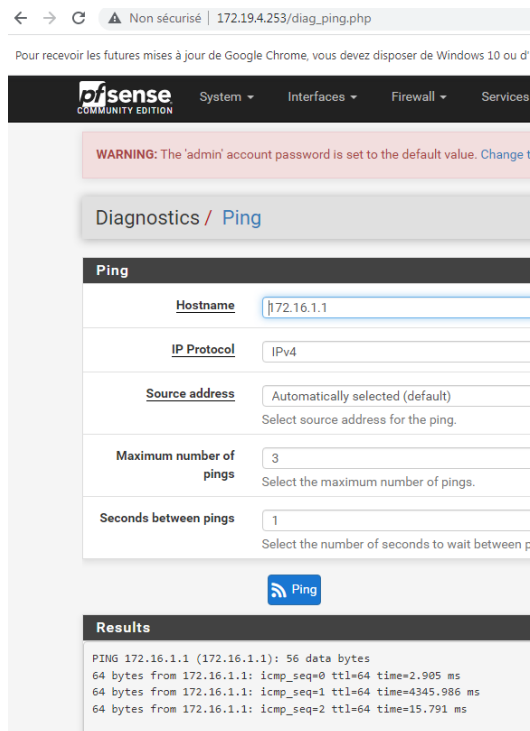


La Pfsense vert est celle redonder

Pour commencer j'ai configuré les deux interfaces des pfsense en leurs créant une nouvelle interface (OPT2) pour qu'il puisse communiquer entre eux :

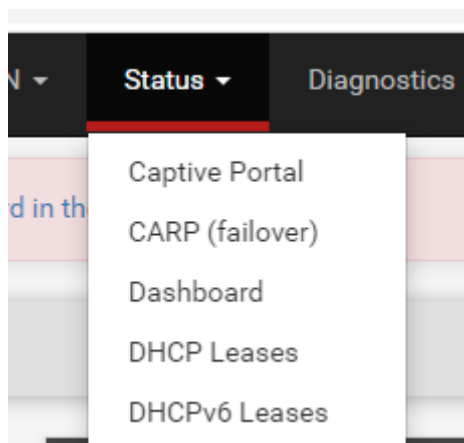


Pour tester la communication entre les deux pfsense j'effectue un ping vers la premier pfsense

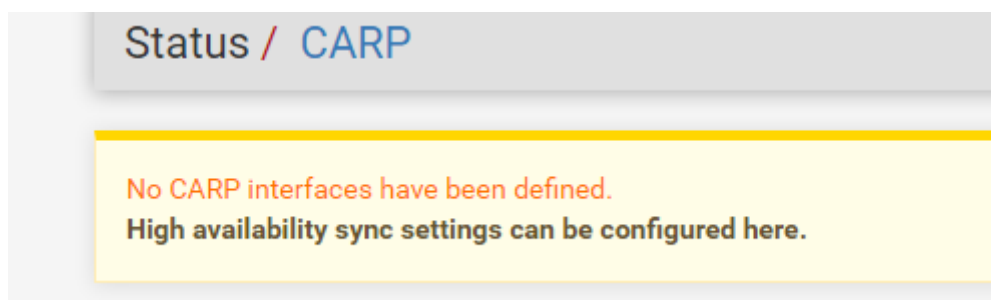


Activation de la synchronisation Pfsync

Maintenant que nos interfaces dédiées Pfsync sont prêtes on se rend dans statu > carp(failover)



Puis on clique la configuration de la synchronisation



System / High Availability Sync

State Synchronization Settings (pfsync)

Synchronize states pfsync transfers state insertion, update, and deletion messages between firewalls.
Each firewall sends these messages out via multicast on a specified interface, using the PFSYNC protocol (IP Protocol 240) interface for similar messages from other firewalls, and imports them into the local state table.
This setting should be enabled on all members of a failover group.
Clicking "Save" will force a configuration sync if it is enabled! (see Configuration Synchronization Settings below)

Synchronize Interface
If Synchronize States is enabled this interface will be used for communication.
It is recommended to set this to an interface other than LAN! A dedicated interface works the best.
An IP must be defined on each machine participating in this failover group.
An IP must be assigned to the interface on any participating sync nodes.

pfsync Synchronize Peer IP
Setting this option will force pfsync to synchronize its state table to this IP address. The default is directed multicast.

Configuration Synchronization Settings (XMLRPC Sync)

Maintenant on va cocher la synchronisation, mettre l'interface qui est utiliser comment synchronisation et l'ip de la pfsense a synchroniser

State Synchronization Settings (pfsync)

Synchronize states pfsync transfers state insertion, update, and deletion messages between firewalls.
Each firewall sends these messages out via multicast on a specified interface, using the PFSYNC protocol (IP Protocol 240). It also listens on that interface for similar messages from other firewalls, and imports them into the local state table.
This setting should be enabled on all members of a failover group.
Clicking "Save" will force a configuration sync if it is enabled! (see Configuration Synchronization Settings below)

Synchronize Interface
If Synchronize States is enabled this interface will be used for communication.
It is recommended to set this to an interface other than LAN! A dedicated interface works the best.
An IP must be defined on each machine participating in this failover group.
An IP must be assigned to the interface on any participating sync nodes.

Filter Host ID
Custom pf host identifier carried in state data to uniquely identify which host created a firewall state.
Must be a non-zero hexadecimal string 8 characters or less (e.g. 1, 2, ff01, abcdef01).
Each node participating in state synchronization must have a different ID.

pfsync Synchronize Peer IP
Setting this option will force pfsync to synchronize its state table to this IP address. The default is directed multicast.

Puis activer les modules de synchronisation à faire sur les deux pfsense

Configuration Synchronization Settings (XMLRPC Sync)

Synchronize Config to IP
Enter the IP address of the firewall to which the selected configuration sections should be synchronized.
XMLRPC sync is currently only supported over connections using the same protocol and port as this system - make sure the remote system's port and protocol are set accordingly!
Do not use the Synchronize Config to IP and password option on backup cluster members!

Remote System Username
Enter the webConfigurator username of the system entered above for synchronizing the configuration.
Do not use the Synchronize Config to IP and username option on backup cluster members!

Remote System Password
Enter the webConfigurator password of the system entered above for synchronizing the configuration.
Do not use the Synchronize Config to IP and password option on backup cluster members!

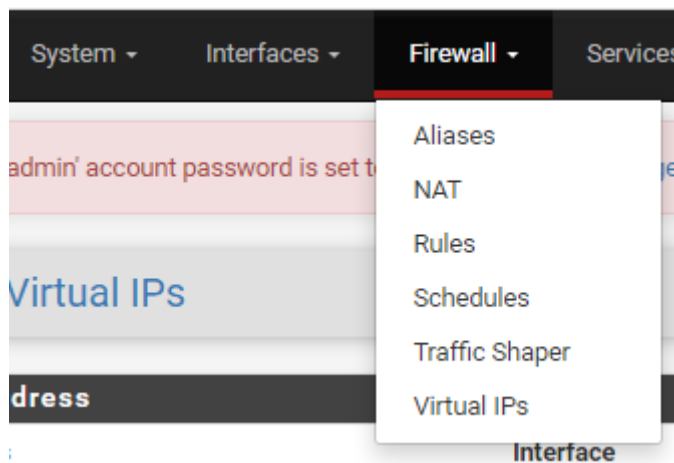
Synchronize admin synchronize admin accounts and autoupdate sync password.
By default, the admin account does not synchronize, and each node may have a different admin password.
This option automatically updates XMLRPC Remote System Password when the password is changed on the Remote System Username account.

Select options to sync

- User manager users and groups
- Authentication servers (e.g. LDAP, RADIUS)
- Certificate Authorities, Certificates, and Certificate Revocation Lists
- Firewall rules
- Firewall schedules
- Firewall aliases
- NAT configuration
- IPsec configuration
- OpenVPN configuration (Implies CA/Cert/CRL Sync)
- DHCP Server settings
- DHCP Relay settings
- DHCPv6 Relay settings
- WoL Server settings

Maintenant on va devoir créer une interface virtuelle que va utiliser les appareils

On se rend dans firewall > virtual Ips



On ajoute une interface, on coche la case CARP et on indique l'ip que nous voulons

Firewall / Virtual IPs / Edit ?

Edit Virtual IP

Type IP Alias CARP Proxy ARP Other

Interface LAN

Address type Single address

Address(es) 172.19.4.254 / 24
The mask must be the network's subnet mask. It does not specify a CIDR range.

Virtual IP Password
Enter the VHID group password. Confirm

VHID Group 1
Enter the VHID group that the machines will share.

Advertising frequency 1 0
Base Skew
 The frequency that this machine will advertise. 0 means usually master. Otherwise the lowest combination of both values in the cluster determines the master.

Description
A description may be entered here for administrative reference (not parsed).

[Save](#)

Après avoir fait tout cela là nous pouvons aller voir dans statuts, CARP et nous pouvons voir que carp est activé

La pfSense Master :

Status / CARP ☰ 📄 ?

CARP Maintenance

[Temporarily Disable CARP](#) [Enter Persistent CARP Maintenance Mode](#)

CARP Status

Interface and VHID	Virtual IP Address	Description	Status
LAN@1	172.19.4.254/24		▶ MASTER

State Synchronization Status

State Creator Host IDs:

La pfSense backup :

Status / CARP ☰ 📄 ?

CARP Maintenance

[Temporarily Disable CARP](#) [Enter Persistent CARP Maintenance Mode](#)

CARP Status

Interface and VHID	Virtual IP Address	Description	Status
LAN@1	172.19.4.254/24		🟡 BACKUP

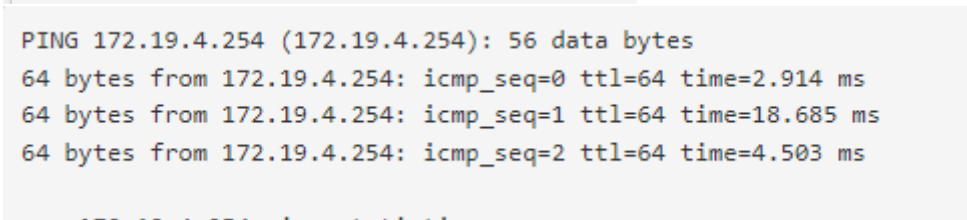
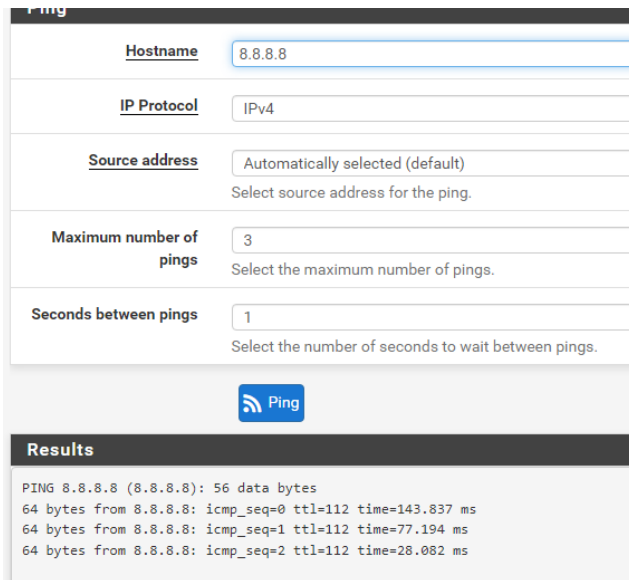
State Synchronization Status

State Creator Host IDs:

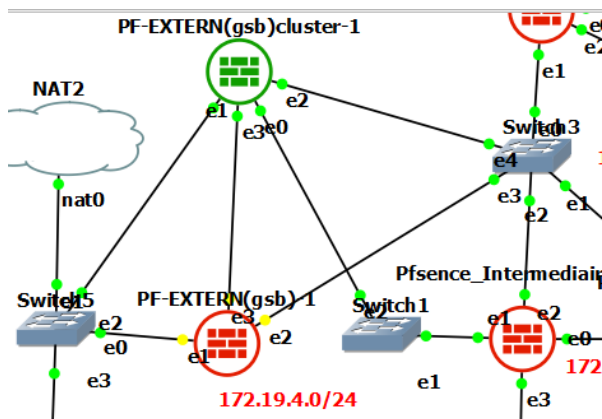
Teste de vérification :

Pour faire les teste je vais utiliser la pfsense intermédiaire et faire un ping vers l'extérieur

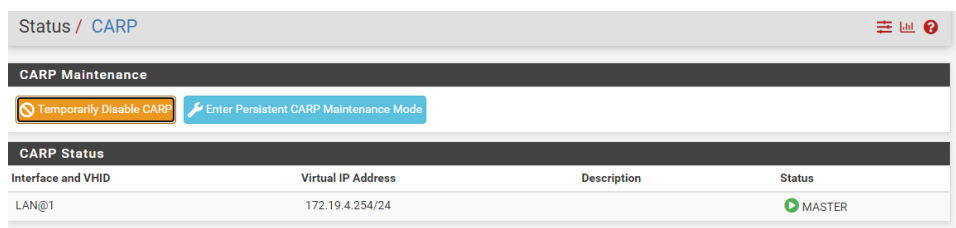
Le teste avec les deux pfsense d'allumer :



Je debranche la pfsene master :



Le statut de la pfsense de backup a changer :



Le ping de l'extérieurs fonction toujours

```
Results  
PING 8.8.8.8 (8.8.8.8): 56 data bytes  
64 bytes from 8.8.8.8: icmp_seq=0 ttl=112 time=91.687 ms  
64 bytes from 8.8.8.8: icmp_seq=1 ttl=112 time=54.472 ms  
64 bytes from 8.8.8.8: icmp_seq=2 ttl=112 time=33.069 ms  
--- 8.8.8.8 ping statistics ---
```

Quand on rebranche la premiers pfsense elle repasse en master

Redondance Serveur ADDS et DHCP

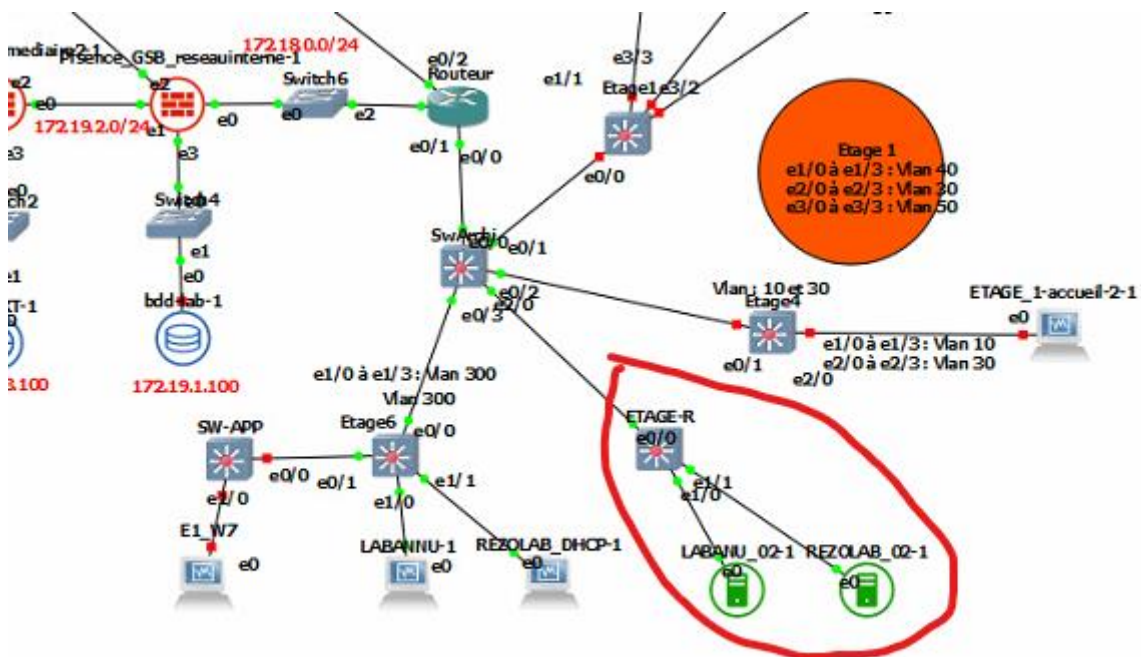
Configuration de l'infrastructure

Avant de commencer il faut préparer l'infrastructure ou va être placé les serveurs.

Pour cela j'ai choisi de les placer dans un autre endroit que les serveurs existents pour plus de sécurité.

Pour ce faire j'ai installé un switch et configuré le nécessaire.

Voilà la structure du réseau.



Configuration du switch étage redondance :

Mettre le Vlan :

VLAN	Name	Status	Ports
1	default	active	Et0/1, Et0/2, Et0/3, Et2/0 Et2/1, Et2/2, Et2/3, Et3/0 Et3/1, Et3/2, Et3/3
300	VLAN0300	active	Et1/0, Et1/1, Et1/2, Et1/3
1002	fddi-default	act/unsup	
1003	token-ring-default	act/unsup	
1004	fddinet-default	act/unsup	
1005	trnet-default	act/unsup	

Configuration du truck :

```
ETAGE-R#sh interfaces trunk
Port      Mode           Encapsulation  Status        Native vlan
Et0/0     on             802.1q         trunking     1

Port      Vlans allowed on trunk
Et0/0     300

Port      Vlans allowed and active in management domain
Et0/0     300

Port      Vlans in spanning tree forwarding state and not pruned
Et0/0     300
ETAGE-R#
```

Configuration du switch archi, mise en p

```
Et0/0     10,20,30,40,50,300,400,500
Et0/1     30,40,50,500
Et0/2     10,30,500
Et0/3     300,500
Et1/0     10,30
Et2/0     300

Port      Vlans allowed and active in management domain
Et0/0     10,20,30,40,50,300,400,500
Et0/1     30,40,50,500
Et0/2     10,30,500
Et0/3     300,500
Et1/0     10,30
Et2/0     300

Port      Vlans in spanning tree forwarding state and not pruned
Et0/0     10,20,30,40,50,300,400,500
Et0/1     30,40,50,500
Et0/2     10,30,500
Et0/3     300,500
Et1/0     10,30
Et2/0     300
SwArchi#
```

Après la configuration des switches fini il nous reste à tester si cela fonctionne bien

Ping depuis le serveur redonder

```
C:\Users\Administrateur>ping 172.17.0.254

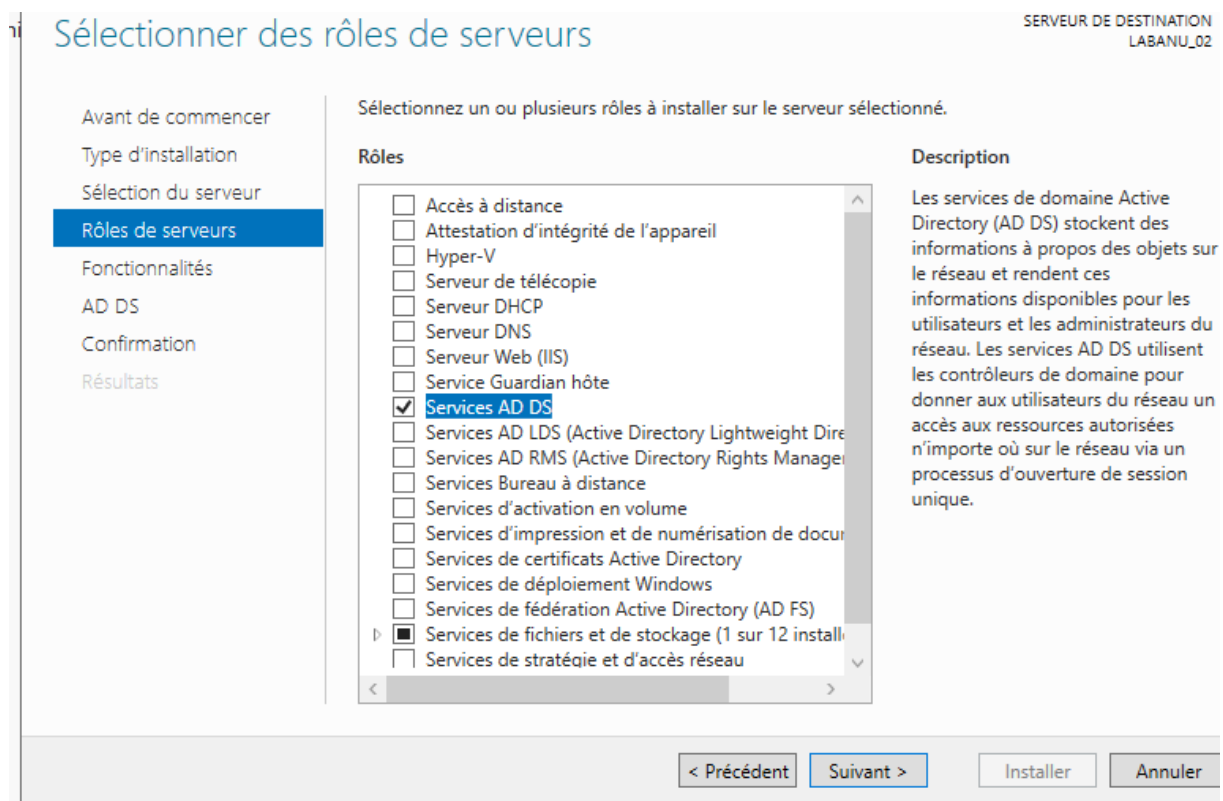
Envoi d'une requête 'Ping' 172.17.0.254 avec 32 octets de données :
Réponse de 172.17.0.254 : octets=32 temps=3 ms TTL=255
Réponse de 172.17.0.254 : octets=32 temps=6 ms TTL=255
Réponse de 172.17.0.254 : octets=32 temps=5 ms TTL=255
Réponse de 172.17.0.254 : octets=32 temps=5 ms TTL=255

Statistiques Ping pour 172.17.0.254:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 3ms, Maximum = 6ms, Moyenne = 4ms

C:\Users\Administrateur>
```

Configuration de la redondance ADDS

Pour configurer une redondance ADDS il faut commencer à installer le service ADDS



Ensuite nous devons promouvoir ce serveur en contrôleur de domaine et l'ajouter à un domaine existant

Sélectionner l'opération de déploiement

Ajouter un contrôleur de domaine à un domaine existant
 Ajouter un nouveau domaine à une forêt existante
 Ajouter une nouvelle forêt

Spécifiez les informations de domaine pour cette opération

Domaine :

Fournir les informations d'identification pour effectuer cette opération

<Aucune information d'identification fournie>

Bien choisir la répllication du domaine

Spécifier les options d'installation à partir du support (IFM)

Installation à partir du support

Spécifier des options de répllication supplémentaires

Répliquer depuis :

Enfin on peut voir les deux serveurs en contrôleur de domaine

	Nom	Type
Utilisateurs et ordinateurs Active Directory		
Requêtes enregistrées		
GSB.local		
> Builtin		
> Computers		
> Domain Controllers	LABANNU	Ordinat
> ForeignSecurityPrincipal:	LABANU_02	Ordinat
> Managed Service Accour		
> Users		

Teste de fonctionnalité :

En laissant par default

```

C:\Users\clement>nltest /dsgetdc:GSB.local
    Contrôleur de domaine : \\LABANNU.GSB.local
    Adresse : \\172.17.0.30
    GUID dom : 9c7c57e1-3995-400a-9a53-d4acf1cd5747
    Nom dom : GSB.local
    Nom de la forêt : GSB.local
    Nom de site du contrôleur de domaine : Default-First-Site-Name
    Nom de notre site : Default-First-Site-Name
    Indicateurs : PDC GC DS LDAP KDC TIMESERU GTIMESERU WRITABLE
    DOMAIN DNS_FOREST CLOSE_SITE FULL_SECRET WS 0x3C000
    La commande a été correctement exécutée

C:\Users\clement>_

```

Sur le serveur 02

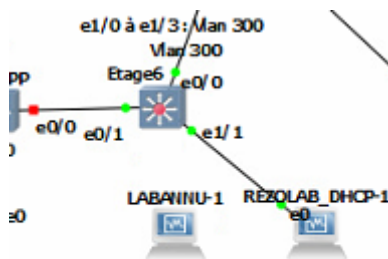
```

C:\Users\Administrateur.GSB>netdom query fsmo
Contrôleur de schéma          LABANNU.GSB.local
Maître des noms de domaine   LABANNU.GSB.local
Contrôleur domaine princip.  LABANNU.GSB.local
Gestionnaire du pool RID      LABANNU.GSB.local
Maître d'infrastructure     LABANNU.GSB.local
L'opération s'est bien déroulée.

C:\Users\Administrateur.GSB>_

```

Je deconnecte le serveur principale



```

C:\Users\clement>nltest /dsgetdc:GSB.local
    Contrôleur de domaine : \\LABANU_02.GSB.local
    Adresse : \\172.17.0.31
    GUID dom : 9c7c57e1-3995-400a-9a53-d4acf1cd5747
    Nom dom : GSB.local
    Nom de la forêt : GSB.local
    Nom de site du contrôleur de domaine : Default-First-Site-Name
    Nom de notre site : Default-First-Site-Name
    Indicateurs : GC DS LDAP KDC TIMESERU WRITABLE DNS_DC DN
    ESTI CLOSE_SITE FULL_SECRET WS 0x3C000
    La commande a été correctement exécutée

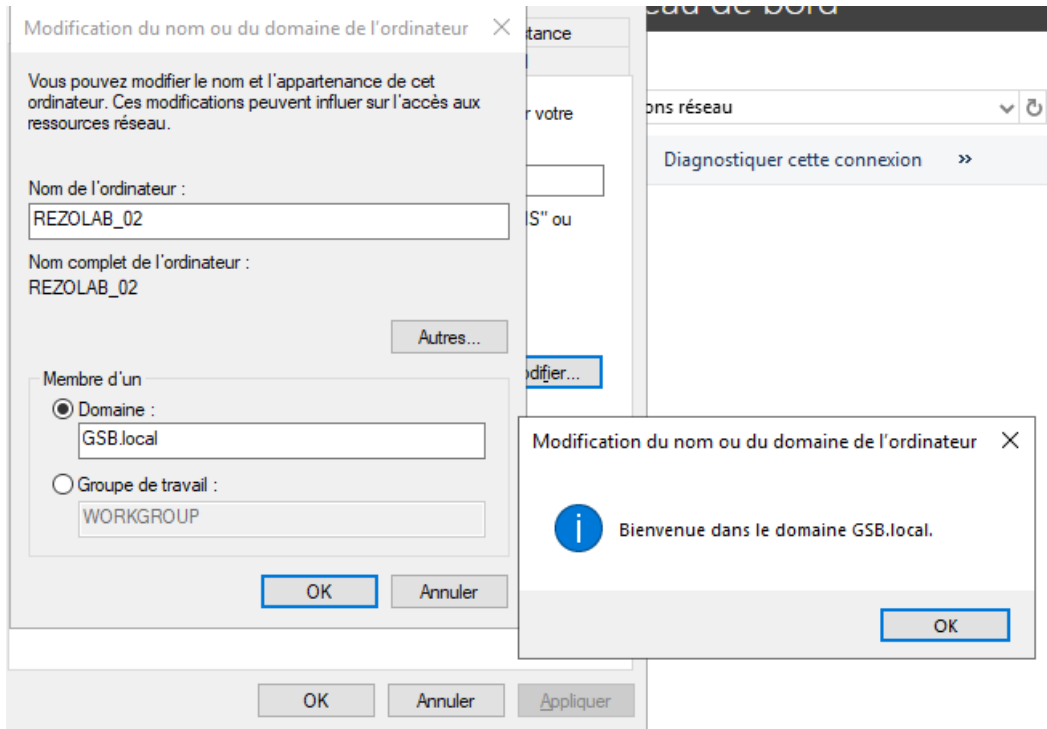
C:\Users\clement>

```

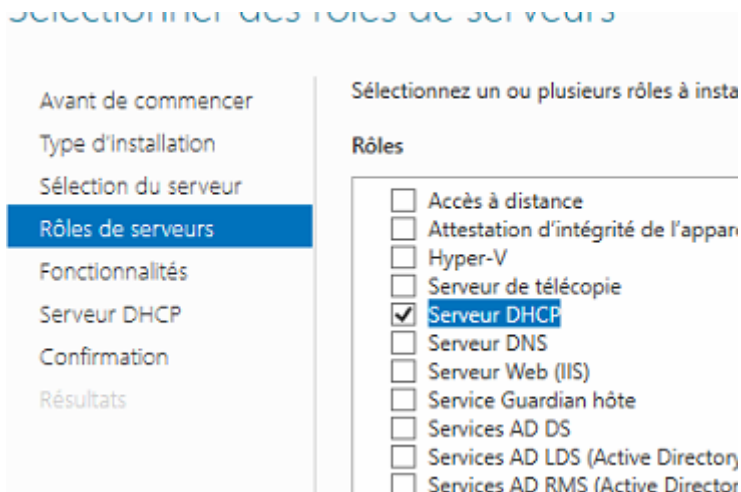
La bascule c'est bien réaliser

Redondance DHCP

Pour comment il faut d'abor interger le serveur REZOLAB_02 dans le domaine



Ensuit nous allons ajouter le rôle DHCP



Enfin il faut retourner sur le premier serveur et ajouter le dexieme serveur sur la configuration dhcp

The screenshot shows the DHCP console interface. On the left, a tree view shows the hierarchy: DHCP > rezolab.gsb.lo > IPv4 > Étendu. The main pane shows 'Contenu de DHCP' with 'rezolab.gsb.local' listed. A dialog box titled 'Gérer les serveurs autorisés' is open, displaying a table of authorized DHCP servers.

Nom	Adresse IP
rezolab.gsb.local	172.17.0.10

Buttons in the dialog: Autoriser..., Interdire, Actualiser, OK, Fermer.

Text in dialog: Pour ajouter un ordinateur à la console DHCP, sélectionnez l'ordinateur, puis cliquez sur OK.

This screenshot shows a close-up of the table from the previous dialog, now integrated into the DHCP console interface. It lists two authorized servers.

Nom	Adresse IP
rezolab.gsb.local	172.17.0.10
rezolab_02.gsb.local	172.17.0.11

Text below the table: Pour ajouter un ordinateur à la console DHCP, sélectionnez l'ordinateur sur OK.

Button: OK

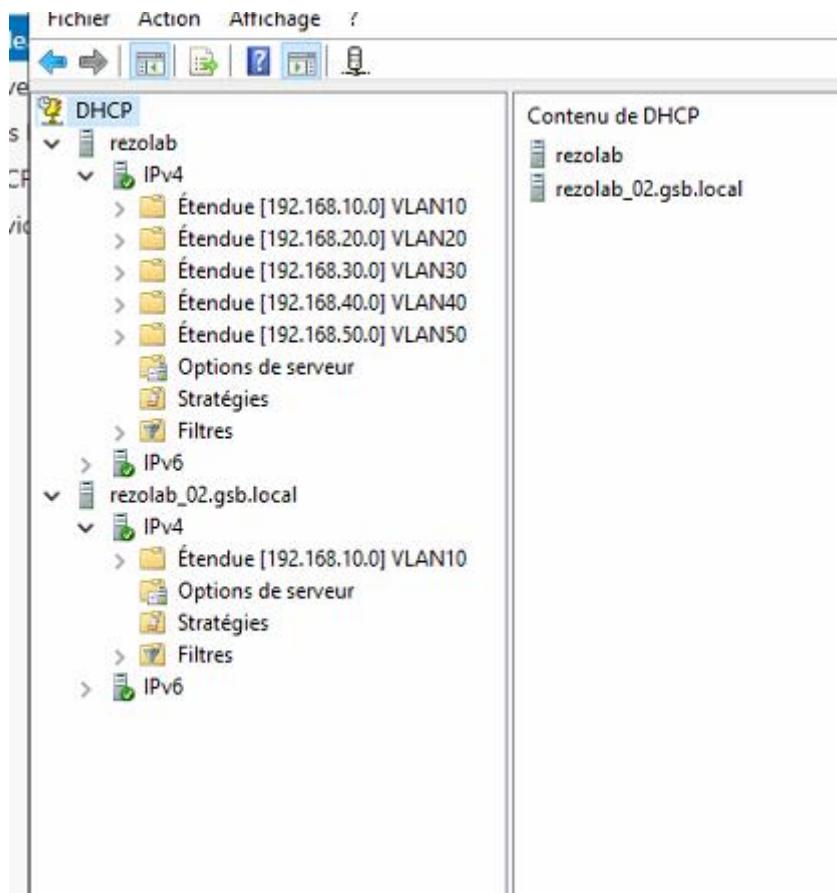
Ensuite on configure le basculement des étendues

The screenshot shows the 'Créer une relation de basculement avec le partenaire rezolab_02' dialog box. It contains the following configuration fields:

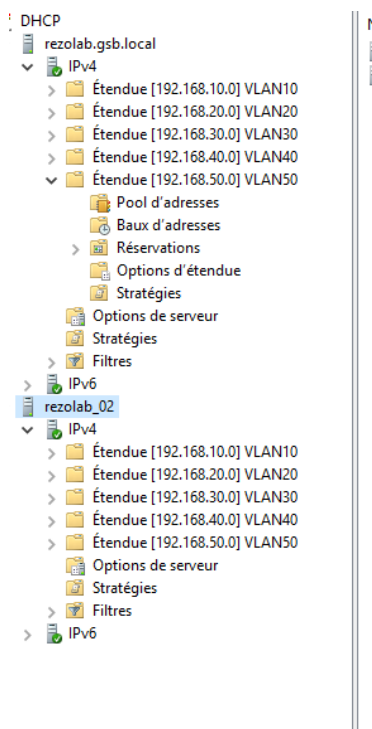
- Nom de la relation : rezolab.gsb.local-rezolab_02
- Délai de transition maximal du client (MCLT) : 1 heures, 0 minutes
- Mode : Serveur de secours
- Configuration du serveur de secours:
 - Rôle du serveur partenaire : Veille
 - Adresses réservées pour le serveur de secours : 5 %
- Intervalle de basculement d'état : 5 minutes
- Activer l'authentification du message
- Secret partagé : (empty field)

Buttons at the bottom: < Précédent, Suivant >, Annuler.

Sur le deuxième serveur on ajoute le serveur principale



Il reste à mettre tous les Vlan dans le basculement



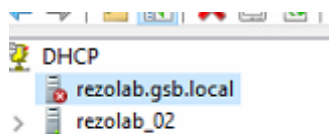
La seule chose qui reste à faire c'est de configurer l'IP helper sur le pour le deuxième serveur

```
Routeur(config)#int e0/0.10
Routeur(config-subif)#ip he
Routeur(config-subif)#ip help
Routeur(config-subif)#ip helper-address 172
% Incomplete command.

Routeur(config-subif)#ip helper-address 172.17.0.11
Routeur(config-subif)#
```

Teste de fonctionnalité :

J'étais le serveur principal



```
Carte Ethernet Connexion au réseau local :
  Suffixe DNS propre à la connexion. . . : GSB.local
  Description. . . . . : Carte Intel(R) PRO/1000 MT pour stat
ion de travail
  Adresse physique . . . . . : 08-00-27-75-CB-10
  DHCP activé. . . . . : Oui
  Configuration automatique activée. . . : Oui
  Adresse IPv6 de liaison locale. . . . . : fe80::c8da:9500:faa0:24a2%11<préféré>
>
  Adresse IPv4. . . . . : 192.168.10.100<préféré>
  Masque de sous-réseau. . . . . : 255.255.255.0
  Bail obtenu. . . . . : jeudi 16 mai 2024 15:21:19
  Bail expirant. . . . . : vendredi 24 mai 2024 15:21:19
  Passerelle par défaut. . . . . : 172.17.0.254
  Serveur DHCP . . . . . : 172.17.0.11
  IAID DHCPv6 . . . . . : 235405351
  DUID de client DHCPv6. . . . . : 00-01-00-01-1D-97-28-8D-08-00-27-57-A8
-67
  Serveurs DNS. . . . . : 172.17.0.30
                          172.17.0.31
  NetBIOS sur Tcpip. . . . . : Activé

Carte Tunnel isatap.GSB.local :
```