



Epreuve E4 Mission

Redondance et haute disponibilité

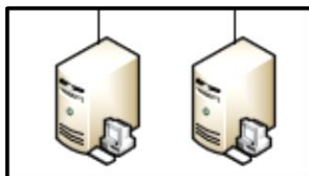
MARTIN Jean-François
BTS SIO

Table des matières

1) Redondance Serveurs AD/DNS/DHCP	2
I. Service DHCP.....	2
II. Service AD/DNS.....	4
2) Redondance routeurs.....	6
I. Routeur Master.....	6
II. Routeur de redondance.....	7
3) Redondance Firewalls	11
I. Firewalls EXT	11
II. Firewalls INT.....	14
4) Redondance Serveur WEB	19
I. Serveur Web INT	19
II. Serveur Web EXT.....	22
5) Redondance site WEB	25
I. Site Web internet.gsb.fr	25
II. Site Web externe.gsb.fr.....	31
6) Redondance BDD	34
7) Redondance Internet	44

JEMMARTIN

1) Redondance Serveurs AD/DNS/DHCP



Propriétés de : Protocole Internet version 4 (TCP/IPv4)

Général

Les paramètres IP peuvent être déterminés automatiquement si votre réseau le permet. Sinon, vous devez demander les paramètres IP appropriés à votre administrateur réseau.

Obtenir une adresse IP automatiquement

Utiliser l'adresse IP suivante :

Adresse IP :

Masque de sous-réseau :

Passerelle par défaut :

Obtenir les adresses des serveurs DNS automatiquement

Utiliser l'adresse de serveur DNS suivante :

Serveur DNS préféré :

Serveur DNS auxiliaire :

Valider les paramètres en quittant

Avancé...

OK Annuler

I. Service DHCP

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 : Ajouter un serveur

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

Configurer un basculement

Sélectionner les relations de basculement déjà configurées sur ce serveur

Il existe des relations de basculement configurées sur ce serveur avec redondance.galaxy-swiss.local.

Sélectionnez l'une des relations existantes à utiliser :

Nom de la relation :

Délai de transition maximal du client (MCLT) : 1 h 0 min

Mode : Serveur de secours

Intervalle de basculement d'état : 5 min

Configuration du serveur de secours

Rôle de ce serveur : Actif

Adresses réservées (serveur de secours) : 5 %

Configurer un basculement

Un basculement va être configuré entre addnsdhcp.galaxy-swiss.lo... et redondance.galaxy-swiss.l... avec les paramètres suivants.

Étendues :
192.168.40.0

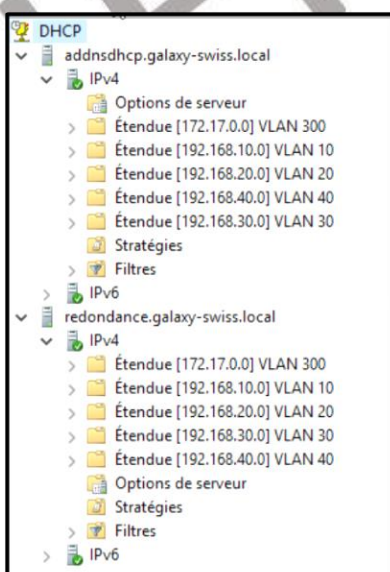
Nom de la relation : addnsdhcp.gal...
Délai de transition maximal du client (MCLT) : 1 h 0 min
Mode : Serveur de sec
Intervalle de basculement d'état : 5 min

Configuration du serveur de secours

Rôle du serveur partenaire : Veille

Adresses réservées pour le serveur 5 %

Rajout du serveur de redondance dans l'affichage DHCP



Rajout de l'IP helper sur le routeur pour chaque VLAN

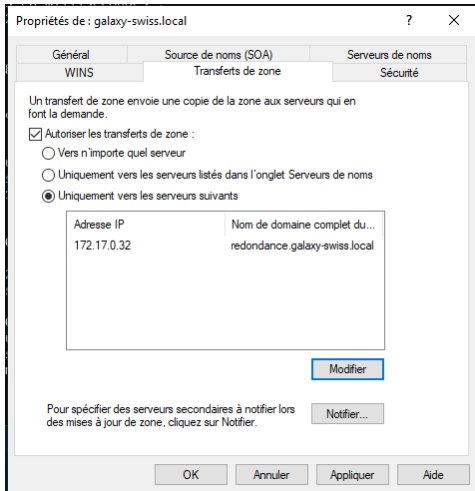
```
interface Ethernet0/1.10
encapsulation dot1Q 10
ip address 192.168.10.254 255.255.255.0
ip helper-address 172.17.0.30
ip helper-address 172.17.0.32
!
interface Ethernet0/1.20
encapsulation dot1Q 20
ip address 192.168.20.254 255.255.255.0
ip helper-address 172.17.0.30
ip helper-address 172.17.0.32
!
interface Ethernet0/1.26
encapsulation dot1Q 26
ip address 172.26.1.254 255.255.255.0
!
interface Ethernet0/1.30
encapsulation dot1Q 30
ip address 192.168.30.254 255.255.255.0
ip helper-address 172.17.0.30
ip helper-address 172.17.0.32
!
interface Ethernet0/1.40
encapsulation dot1Q 40
ip address 192.168.40.254 255.255.255.0
ip helper-address 172.17.0.30
ip helper-address 172.17.0.32
```

Test de fonctionnement en désactivant le DHCP sur 172.17.0.30

```
Suffixe DNS propre à la connexion. . . . : galaxy-swiss.local
Description. . . . . : Intel(R) PRO/1000 MT Desktop Adapter
Adresse physique . . . . . : 08-00-27-4F-70-2A
DHCP activé. . . . . : Oui
Configuration automatique activée. . . . : Oui
Adresse IPv6 de liaison locale. . . . . : fe80::124:7d53:12ad:8803%13(préfééré)
Adresse IPv4. . . . . : 192.168.40.10(préfééré)
Masque de sous-réseau. . . . . : 255.255.255.0
Bail obtenu. . . . . : mercredi 3 février 2021 12:19:07
Bail expirant. . . . . : samedi 12 mars 2157 18:47:45
Passerelle par défaut. . . . . : 192.168.40.254
Serveur DHCP . . . . . : 172.17.0.32
IAID DHCPv6 . . . . . : 101187623
DUID de client DHCPv6. . . . . : 00-01-00-01-27-AB-64-32-08-00-27-4F-70-2A
Serveurs DNS. . . . . : 172.17.0.30
NetBIOS sur Tcpiip. . . . . : Activé
```

II. Service AD/DNS

	Nom	Type	Données
DNS REDONDANCE Zones de recherche directes _msdcs.galaxy-swiss.local galaxy-swiss.local Zones de recherche inversée Points d'approbation Redirecteurs conditionnels	_msdcs		
	_sites		
	_tcp		
	_udp		
	DomainDnsZones		
	ForestDnsZones		
	(identique au dossier parent)	Source de nom (SOA)	[176], redondance.galaxy-...
	(identique au dossier parent)	Serveur de noms (NS)	redondance.galaxy-swiss.l...
	(identique au dossier parent)	Serveur de noms (NS)	addnsdhcp.galaxy-swiss.l...
	(identique au dossier parent)	Hôte (A)	172.17.0.30
	(identique au dossier parent)	Hôte (A)	172.17.0.32
	addnsdhcp	Hôte (A)	172.17.0.30
	PC-VLAN-10	Hôte (A)	192.168.10.10
	PC-VLAN-20	Hôte (A)	192.168.20.10
PC-VLAN-30	Hôte (A)	192.168.30.10	
PC-VLAN-40	Hôte (A)	192.168.40.10	
redondance	Hôte (A)	172.17.0.32	



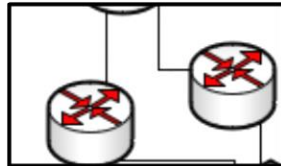
003	Routeur	Standard	172.17.0.250	Aucun
006	Serveurs DNS	Standard	172.17.0.30, 172.17.0.32	Aucun
015	Nom de domaine DNS	Standard	galaxy-swiss.local	Aucun

JEMMARTIN

2) Redondance routeurs

(Suite à des problèmes avec le protocole CARP cette configuration évoluera plus bas)

Pour la redondance je vais utiliser le protocole VRRP



I. Routeur Master

Je mets en place le protocole VRRP sur chaque interface du routeur

J'ajoute les tracks pour chaque interface

```
track 1 interface Ethernet0/0 line-protocol
!
track 10 interface Ethernet0/1.10 line-protocol
!
track 20 interface Ethernet0/1.20 line-protocol
!
track 26 interface Ethernet0/1.26 line-protocol
!
track 30 interface Ethernet0/1.30 line-protocol
!
track 40 interface Ethernet0/1.40 line-protocol
!
track 255 interface Ethernet0/1.300 line-protocol
!
```

Puis je mets les tracks sur l'interface du routeur

```
interface Ethernet0/0
 ip address 172.18.0.1 255.255.255.0
 vrrp 1 description vrrp1
 vrrp 1 ip 172.18.0.250
 vrrp 1 timers advertise 2
 vrrp 1 timers learn
 vrrp 1 preempt delay minimum 5
 vrrp 1 priority 110
 vrrp 1 track 10 decrement 11
 vrrp 1 track 20 decrement 11
 vrrp 1 track 30 decrement 11
 vrrp 1 track 40 decrement 11
 vrrp 1 track 300 decrement 11
,
```

Exemple pour une interface de VLAN

```
interface Ethernet0/1.10
 encapsulation dot1Q 10
 ip address 192.168.10.254 255.255.255.0
 ip helper-address 172.17.0.30
 ip helper-address 172.17.0.32
 vrrp 10 description vrrp10
 vrrp 10 ip 192.168.10.250
 vrrp 10 timers advertise 2
 vrrp 10 timers learn
 vrrp 10 preempt delay minimum 5
 vrrp 10 priority 110
 vrrp 10 track 1 decrement 11
```

II. Routeur de redondance

Puis je configure le routeur de redondance

J'ajoute une interface sur le switch Archi

```
interface Ethernet1/1
 switchport trunk allowed vlan 10,20,26,30,40,300
 switchport trunk encapsulation dot1q
 switchport mode trunk
 spanning-tree bpdufilter enable
```

Puis je déclare chaque groupe VRRP en changeant l'IP de l'interface

```
interface Ethernet0/1.20
 encapsulation dot1Q 20
 ip address 192.168.20.253 255.255.255.0
 ip helper-address 172.17.0.30
 ip helper-address 172.17.0.32
 vrrp 20 description vrrp20
 vrrp 20 ip 192.168.20.250
 vrrp 20 timers advertise 2
 vrrp 20 timers learn
 vrrp 20 preempt delay minimum 5
```

Conf des deux routeurs

Routeur :

Interface	Grp	Pri	Time	Own	Pre	State	Master addr	Group addr
Et0/0	1	110	6570		Y	Master	172.18.0.1	172.18.0.250
Et0/1.10	10	110	6570		Y	Master	192.168.10.254	192.168.10.250
Et0/1.20	20	110	6570		Y	Master	192.168.20.254	192.168.20.250
Et0/1.26	26	110	6570		Y	Master	172.26.1.254	172.26.1.250
Et0/1.30	30	110	6570		Y	Master	192.168.30.254	192.168.30.250
Et0/1.40	40	110	6570		Y	Master	192.168.40.254	192.168.40.250
Et0/1.300	255	110	6570		Y	Master	172.17.0.254	172.17.0.250

Redondance :

Interface	Grp	Pri	Time	Own	Pre	State	Master addr	Group addr
Et0/0	1	100	6609		Y	Backup	172.18.0.1	172.18.0.250
Et0/1.10	10	100	6609		Y	Backup	192.168.10.254	192.168.10.250
Et0/1.20	20	100	6609		Y	Backup	192.168.20.254	192.168.20.250
Et0/1.26	26	100	6609		Y	Backup	172.26.1.254	172.26.1.250
Et0/1.30	30	100	6609		Y	Backup	192.168.30.254	192.168.30.250
Et0/1.40	40	100	6609		Y	Backup	192.168.40.254	192.168.40.250
Et0/1.300	255	100	6609		Y	Backup	172.17.0.254	172.17.0.250

Puis modification de la stratégie DHCP sur le serveur

Nom d'option	Fournisseur	Valeur
003 Routeur	Standard	192.168.10.250
006 Serveurs DNS	Standard	172.17.0.30
015 Nom de domaine DNS	Standard	galaxy-swiss.local

Je désactive l'interface 0/0 pour tester le fonctionnement

Routeur :

```
Routeur(config-if)#sh
Routeur(config-if)#
*Mar 26 00:30:05.877: %VRRP-6-STATECHANGE: Et0/0 Grp 1 state Master -> Init
*Mar 26 00:30:05.878: %TRACK-6-STATE: 1 interface Et0/0 line-protocol Up -> Down
Routeur(config-if)#
*Mar 26 00:30:07.878: %LINK-5-CHANGED: Interface Ethernet0/0, changed state to a
dministratively down
*Mar 26 00:30:08.887: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/
0, changed state to down
Routeur(config-if)#
*Mar 26 00:30:11.168: %VRRP-6-STATECHANGE: Et0/1.300 Grp 255 state Master -> Backu
*Mar 26 00:30:11.458: %VRRP-6-STATECHANGE: Et0/1.40 Grp 40 state Master -> Backup
*Mar 26 00:30:11.627: %VRRP-6-STATECHANGE: Et0/1.20 Grp 20 state Master -> Backup
*Mar 26 00:30:11.958: %VRRP-6-STATECHANGE: Et0/1.26 Grp 26 state Master -> Backup
Routeur(config-if)#
*Mar 26 00:30:12.278: %VRRP-6-STATECHANGE: Et0/1.10 Grp 10 state Master -> Backup
*Mar 26 00:30:12.578: %VRRP-6-STATECHANGE: Et0/1.30 Grp 30 state Master -> Backup
```

Routeur Redondance :

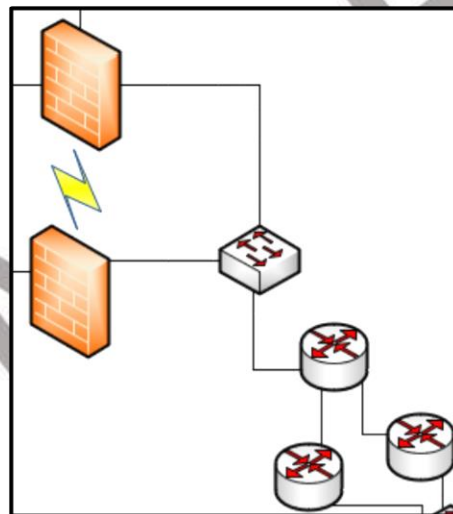
```
*Mar 26 00:30:06.494: %VRRP-6-STATECHANGE: Et0/0 Grp 1 state Backup -> Master
Routeur#
*Mar 26 00:30:11.166: %VRRP-6-STATECHANGE: Et0/1.300 Grp 255 state Backup -> Mas
ter
*Mar 26 00:30:11.457: %VRRP-6-STATECHANGE: Et0/1.40 Grp 40 state Backup -> Maste
r
*Mar 26 00:30:11.626: %VRRP-6-STATECHANGE: Et0/1.20 Grp 20 state Backup -> Maste
r
*Mar 26 00:30:11.951: %VRRP-6-STATECHANGE: Et0/1.26 Grp 26 state Backup -> Maste
r
Routeur#
*Mar 26 00:30:12.277: %VRRP-6-STATECHANGE: Et0/1.10 Grp 10 state Backup -> Maste
r
*Mar 26 00:30:12.577: %VRRP-6-STATECHANGE: Et0/1.30 Grp 30 state Backup -> Maste
r
```

Puis l'état du VRRP

```
Routeur#show vrrp brief
Interface      Grp Pri Time  Own Pre State  Master addr  Group addr
Et0/0          1  110 6570   Y  Init 0.0.0.0  172.18.0.250
Et0/1.10       10  99  6570   Y  Backup 192.168.10.253 192.168.10.250
Et0/1.20       20  99  6570   Y  Backup 192.168.20.253 192.168.20.250
Et0/1.26       26  99  6570   Y  Backup 172.26.1.253  172.26.1.250
Et0/1.30       30  99  6570   Y  Backup 192.168.30.253 192.168.30.250
Et0/1.40       40  99  6570   Y  Backup 192.168.40.253 192.168.40.250
Et0/1.300      255 99  6570   Y  Backup 172.17.0.253  172.17.0.250
```

```
Routeur#show vrrp brief
Interface      Grp Pri Time  Own Pre State  Master addr  Group addr
Et0/0          1  100 6609   Y  Master 172.18.0.3  172.18.0.250
Et0/1.10       10  100 6609   Y  Master 192.168.10.253 192.168.10.250
Et0/1.20       20  100 6609   Y  Master 192.168.20.253 192.168.20.250
Et0/1.26       26  100 6609   Y  Master 172.26.1.253  172.26.1.250
Et0/1.30       30  100 6609   Y  Master 192.168.30.253 192.168.30.250
Et0/1.40       40  100 6609   Y  Master 192.168.40.253 192.168.40.250
Et0/1.300      255 100 6609   Y  Master 172.17.0.253  172.17.0.250
Routeur#
```

Comme le firewall ne fonctionne pas avec la VIP des routeurs qui est sur l'interface 0/0, je rajoute donc un routeur « de sortie » pour que les firewalls tape sur une IP fixe et non une VIP



Je crée donc les routes sur le routeur de sortie

```
routeurdesortie(config)#ip route 0.0.0.0 0.0.0.0 172.18.0.252
routeurdesortie(config)#ip route 172.17.0.0 255.255.128.0 172.32.0.2
routeurdesortie(config)#ip route 172.17.0.0 255.255.128.0 172.33.0.2
routeurdesortie(config)#ip route 192.168.10.0 255.255.255.0 172.32.0.2
routeurdesortie(config)#ip route 192.168.10.0 255.255.255.0 172.33.0.2
routeurdesortie(config)#ip route 192.168.20.0 255.255.255.0 172.32.0.2
routeurdesortie(config)#ip route 192.168.20.0 255.255.255.0 172.33.0.2
routeurdesortie(config)#ip route 172.26.1.0 255.255.255.0 172.32.0.2
routeurdesortie(config)#ip route 172.26.1.0 255.255.255.0 172.33.0.2
routeurdesortie(config)#ip route 192.168.30.0 255.255.255.0 172.32.0.2
routeurdesortie(config)#ip route 192.168.30.0 255.255.255.0 172.33.0.2
routeurdesortie(config)#ip route 192.168.40.0 255.255.255.0 172.32.0.2
routeurdesortie(config)#ip route 192.168.40.0 255.255.255.0 172.33.0.2
```

Puis j'ajoute des routes sur les deux routeurs d'origines et je modifie la route par défaut

```
IOU9(config)#ip route 172.18.0.0 255.255.255.0 172.32.0.1
```

```
IOU9(config)#ip route 0.0.0.0 0.0.0.0 172.32.0.1
```

```
IOU8(config)#ip route 172.18.0.0 255.255.255.0 172.33.0.1
```

```
IOU8(config)#ip route 0.0.0.0 0.0.0.0 172.33.0.1
```

Puis le rajoute les routes static sur les firewalls

<input checked="" type="checkbox"/>	172.32.0.0/24	LAN - 172.18.0.250	LAN	  
<input checked="" type="checkbox"/>	172.33.0.0/24	LAN - 172.18.0.250	LAN	  

<input checked="" type="checkbox"/>	172.32.0.0/24	LAN - 172.21.1.250	LAN	  
<input checked="" type="checkbox"/>	172.33.0.0/24	LAN - 172.21.1.250	LAN	  

Test de fonctionnement

1	1 ms	<1 ms	1 ms	172.17.0.254
2	1 ms	1 ms	1 ms	172.32.0.1
3	1 ms	2 ms	1 ms	172.18.0.2
4	2 ms	2 ms	1 ms	172.21.1.254
5	3 ms	2 ms	2 ms	172.28.1.12
6	6 ms	4 ms	3 ms	192.168.122.1
7	5 ms	4 ms	4 ms	10.0.3.2
8	5 ms	4 ms	4 ms	192.168.1.1

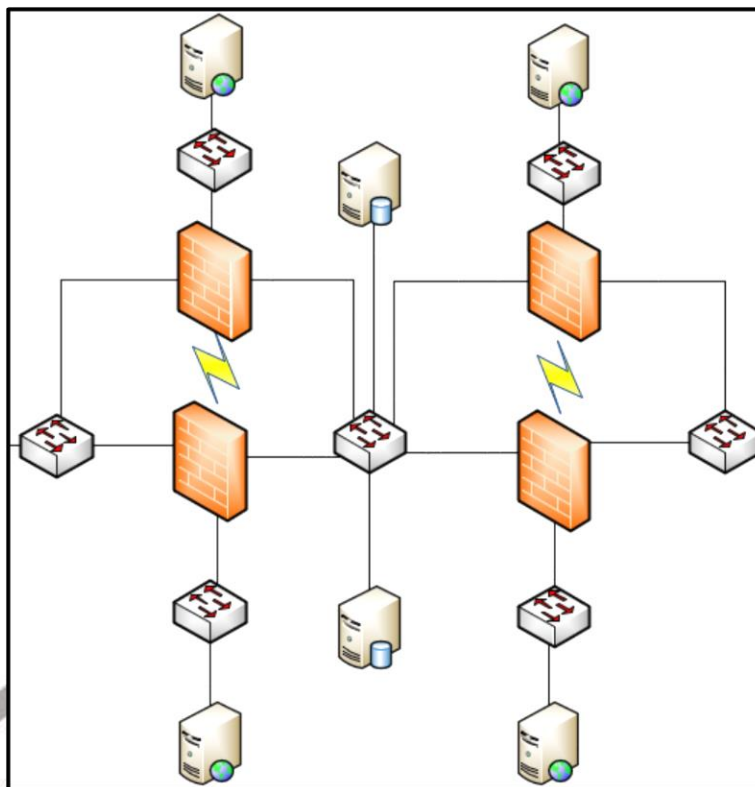
On voit bien le réseau passé par le nouveau routeur

3) Redondance Firewalls

Pour la redondance de firewall j'utilise le protocole CARP qui permet de mettre un firewall en master et l'autre en backup



Je duplique donc les deux firewalls pour en faire deux de redondance



I. Firewalls EXT

- Je mets une IP sur les OPT2

Redondance ext : 172.23.1.2

Firewall ext : 172.23.1.1

- Je mets une IP sur les interfaces LAN des firewalls :

LAN redondance ext : 172.21.1.253

LAN ext : 172.21.1.254

- Puis je prévois la passerelle virtuelle :

IP : 172.21.1.252

Je mets en places les interfaces sur les deux firewalls

EXT :

```
WAN (wan)      -> em2      -> v4/DHCP4: 192.168.122.190/24
LAN (lan)      -> em0      -> v4: 172.21.1.254/24
OPT1 (opt1)    -> em1      -> v4: 172.20.1.254/24
OPT2 (opt2)    -> em3      -> v4: 172.23.1.1/24
```

EXT redondance :

```
WAN (wan)      -> em2      -> v4/DHCP4: 192.168.122.243/24
LAN (lan)      -> em0      -> v4: 172.21.1.253/24
OPT1 (opt1)    -> em1      -> v4: 172.20.1.254/24
OPT2 (opt2)    -> em3      -> v4: 172.23.1.2/24
```

Je déclare la passerelle virtuelle sur les deux routeurs :

Firewall / Virtual IPs				
Virtual IP Address				
Virtual IP address	Interface	Type	Description	Actions
172.21.1.252/24 (vhid: 1)	LAN	CARP		

J'ajoute la règle de l'OPT2 pour le protocole CARP sur chaque Firewalls

Firewall / Rules / OPT2											
Floating WAN LAN OPT1 OPT2 OpenVPN											
Rules (Drag to Change Order)											
<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	✓	0/0 B	IPv4*	OPT2 net	*	OPT2 net	*	*	none		

Puis je mets en place *le High Availability Sync* sur le Firewall qui sera Master

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). 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.

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)

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 Confirm
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!

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)

Puis je le configure sur le Firewall Backup

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). 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 LAN
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 172.23.1.1
Setting this option will force pfsync to synchronize its state table to this IP address. The default is directed multicast.

Je redémarre les Firewalls puis vérifie le status du protocole CARP

Firewall EXT :

CARP Interface	Virtual IP	Status
LAN@1	172.21.1.252/24	MASTER

Firewall EXT redondance :

CARP Interface	Virtual IP	Status
LAN@1	172.21.1.252/24	BACKUP

II. Firewalls INT

- Je mets une IP sur les OPT

Redondance ext : 172.24.1.2

Firewall ext : 172.24.1.1

- Je mets une IP sur les interfaces LAN des firewalls :

LAN redondance int : 172.18.0.5

LAN int : 172.18.0.2

- Je mets une IP sur les interfaces WAN des firewalls :

WAN redondance int : 172.21.1.2

WAN int : 172.21.1.1

- Puis je prévois la passerelle virtuelle :

IP WAN : 172.21.1.250

IP LAN : 172.21.1.250

Je mets en places les interfaces sur les deux firewalls

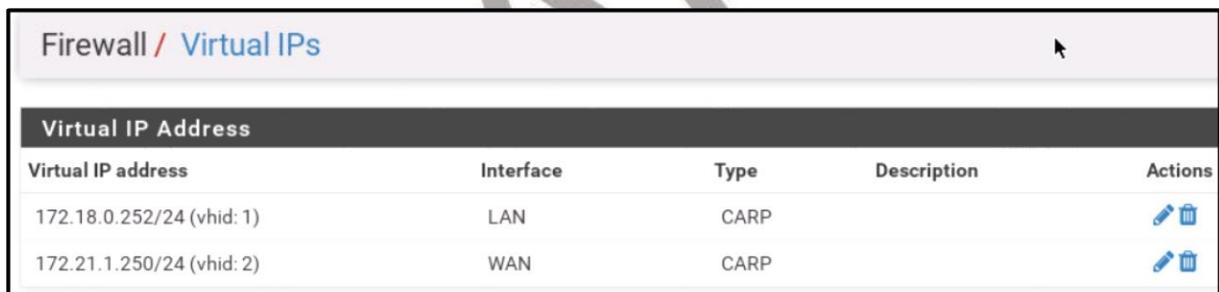
INT redondance :





```
WAN (wan)      -> em2      -> v4: 172.21.1.2/24
LAN (lan)      -> em0      -> v4: 172.18.0.5/24
OPT1 (opt1)   -> em1      -> v4: 172.19.1.254/24
OPT2 (opt2)   -> em3      -> v4: 172.24.1.2/24
```

INT :

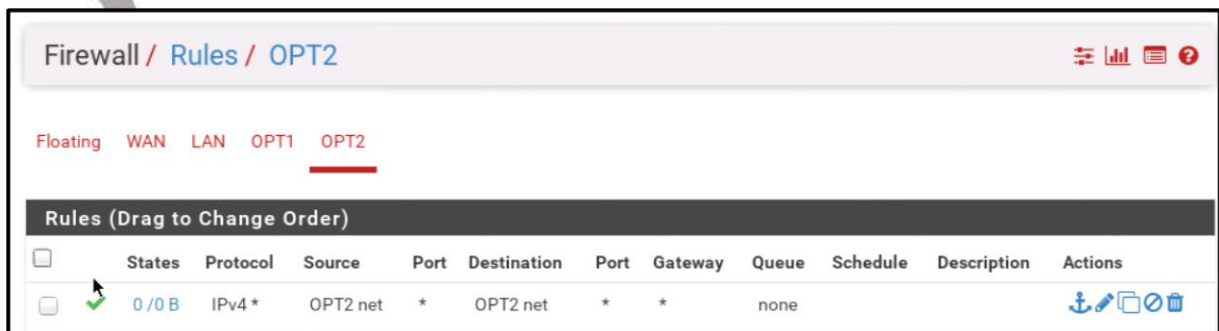
```
WAN (wan)      -> em2      -> v4: 172.21.1.1/24
LAN (lan)      -> em0      -> v4: 172.18.0.2/24
OPT1 (opt1)   -> em1      -> v4: 172.19.1.254/24
OPT2 (opt2)   -> em3      -> v4: 172.24.1.1/24
```




Je déclare les passerelles virtuelles sur les deux routeurs :



Virtual IP address	Interface	Type	Description	Actions
172.18.0.252/24 (vhid: 1)	LAN	CARP		 
172.21.1.250/24 (vhid: 2)	WAN	CARP		 

J'ajoute la règle de l'OPT2 pour le protocole CARP sur chaque Firewalls



States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	0/0 B	IPv4 *	OPT2 net	*	OPT2 net	*	*	none		  

Puis je mets en place *le High Availability Sync* sur le Firewall qui sera Master

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.

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)

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 Confirm
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!

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)

Puis je le configure sur le Firewall Backup

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). 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 LAN
 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 172.24.1.1
 Setting this option will force pfsync to synchronize its state table to this IP address. The default is directed multicast.

Je redémarre les Firewalls puis vérifie le status du protocole CARP

Firewall INT :

CARP Interfaces		
CARP Interface	Virtual IP	Status
LAN@1	172.18.0.252/24	▶ MASTER
WAN@2	172.21.1.250/24	▶ MASTER

Firewall Redondance INT :

CARP Interfaces		
CARP Interface	Virtual IP	Status
LAN@1	172.18.0.252/24	ⓘ BACKUP
WAN@2	172.21.1.250/32	ⓘ BACKUP

Puis je change la route par default sur le routeur

```
Gateway of last resort is 172.18.0.252 to network 0.0.0.0
```

Je test depuis un poste du réseau s'il a bien internet

```
C:\Users\PC40>tracert 8.8.8.8
Détermination de l'itinéraire vers dns.google [8.8.8.8]
avec un maximum de 30 sauts :

 1  1 ms  <1 ms  <1 ms  192.168.40.254
 2  2 ms  1 ms   1 ms   172.18.0.2
 3  2 ms  2 ms   1 ms   172.21.1.254
 4  3 ms  2 ms   2 ms   192.168.122.1
```

```
C:\Users\PC40>ping 8.8.8.8
Envoi d'une requête 'Ping' 8.8.8.8 avec 32 octets de données :
Réponse de 8.8.8.8 : octets=32 temps=16 ms TTL=112
Réponse de 8.8.8.8 : octets=32 temps=15 ms TTL=112
Réponse de 8.8.8.8 : octets=32 temps=16 ms TTL=112
Réponse de 8.8.8.8 : octets=32 temps=16 ms TTL=112
```

Je désactive les deux firewalls principaux pour tester

```
Réponse de 8.8.8.8 : octets=32 temps=16 ms TTL=112
Réponse de 8.8.8.8 : octets=32 temps=16 ms TTL=112
Délai d'attente de la demande dépassé.
Réponse de 8.8.8.8 : octets=32 temps=16 ms TTL=112
Réponse de 8.8.8.8 : octets=32 temps=17 ms TTL=112
```

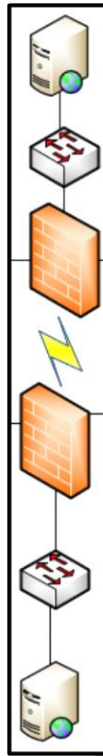
On remarque bien la microcoupure mais qui n'impacte pas la connexion

```
C:\Users\PC40>tracert 8.8.8.8
Détermination de l'itinéraire vers dns.google [8.8.8.8]
avec un maximum de 30 sauts :

 1  1 ms    1 ms    1 ms    192.168.40.254
 2  2 ms    1 ms    1 ms    172.18.0.5
 3  2 ms    2 ms    2 ms    172.21.1.253
 4  3 ms    2 ms    2 ms    192.168.122.1
```

Et on voit bien les deux interfaces de redondance qui ont pris le relais

4) Redondance Serveur WEB



I. Serveur Web INT

Pour faire la Redondance des serveurs web pour éviter d'avoir à saisir les mêmes informations en double j'utilise le logiciel Terminator sur chacune des machines puis plus tard du Load Balancing pour les services WEB



Une fois installé (apt install terminator) je configure le SSH sur chaque machine avec un port SSH différent du port par défaut (dans notre cas 2224)

```
Port 2224
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::

#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_ecdsa_key
#HostKey /etc/ssh/ssh_host_ed25519_key

#LoginGraceTime 2m
PermitRootLogin yes
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10

PubkeyAuthentication yes
```

Puis je modifie les règles sur les deux firewalls pour permettre au SSH de passer et UNIQUEMENT le SSH

Sur le Firewall INT :

- Rules LAN

<input type="checkbox"/>	✓ 0/2 KiB	IPv4 TCP	172.30.1.100	*	172.19.1.100	2224	*	none	
<input type="checkbox"/>	✓ 0/0 B	IPv4 TCP	172.19.1.100	*	172.30.1.100	2224	*	none	

- Rules OPT1

<input type="checkbox"/>	✓ 1/23 KiB	IPv4 TCP	172.19.1.100	*	172.30.1.100	2224	*	none	
--------------------------	------------	----------	--------------	---	--------------	------	---	------	--

- Static Route

<input checked="" type="checkbox"/>	172.30.1.0/24	LAN - 172.18.0.1	LAN	
-------------------------------------	---------------	------------------	-----	--

Sur le Firewall INT Redondance :

- Rules LAN

<input type="checkbox"/>	✓ 1/22 KiB	IPv4 TCP	172.19.1.100	*	172.30.1.100	2224	*	none	
<input checked="" type="checkbox"/>	✓ 0/0 B	IPv4 TCP	172.30.1.100	*	172.19.1.100	2224	*	none	

- Rule OPT1

<input type="checkbox"/>	✓ 0/2 KiB	IPv4 TCP	172.30.1.100	*	172.19.1.100	2224	*	none	
--------------------------	-----------	----------	--------------	---	--------------	------	---	------	--

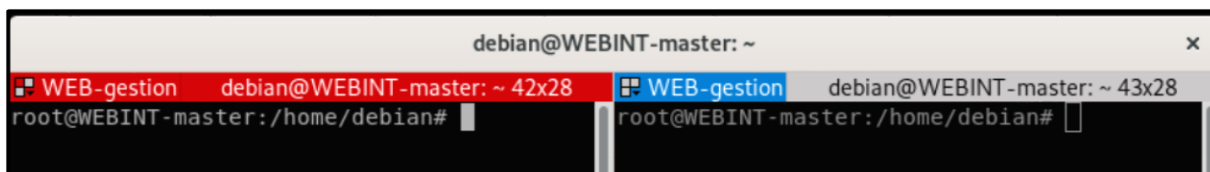
- Static Route

<input checked="" type="checkbox"/>	172.19.1.0/24	LAN - 172.18.0.1	LAN	
-------------------------------------	---------------	------------------	-----	--

Puis j'ajoute les routes sur le routeur de sortie

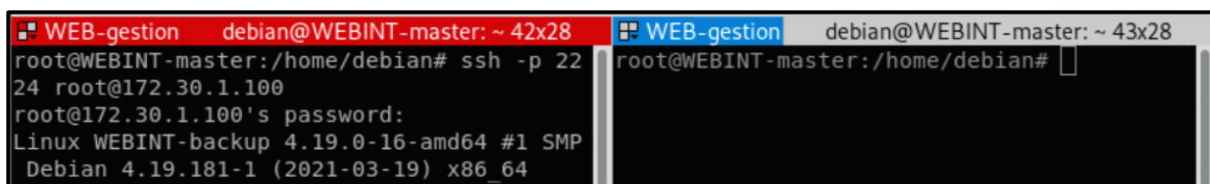
```
routeurdesortie(config)#ip route 172.30.1.0 255.255.255.0 172.18.0.5
routeurdesortie(config)#ip route 172.19.1.0 255.255.255.0 172.18.0.2
```

Puis je lance Terminator sur le Serveur Web master, je e prépare de manière a avoir accès aux deux Serveurs simultanément



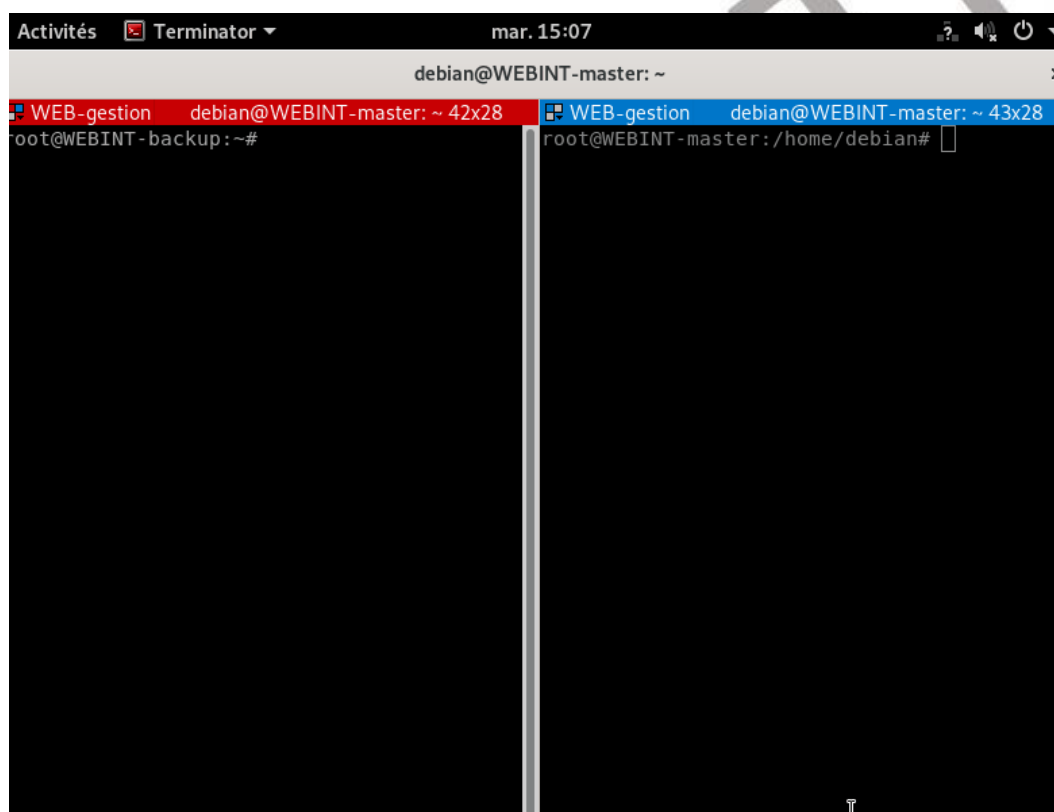
```
debian@WEBINT-master: ~  
WEB-gestion  debian@WEBINT-master: ~ 42x28  WEB-gestion  debian@WEBINT-master: ~ 43x28  
root@WEBINT-master:/home/debian#  root@WEBINT-master:/home/debian#
```

Puis je me connecte en SSH sur le serveur Web backup



```
WEB-gestion  debian@WEBINT-master: ~ 42x28  WEB-gestion  debian@WEBINT-master: ~ 43x28  
root@WEBINT-master:/home/debian# ssh -p 22 root@172.30.1.100  
root@172.30.1.100's password:  
Linux WEBINT-backup 4.19.0-16-amd64 #1 SMP  
Debian 4.19.181-1 (2021-03-19) x86_64
```

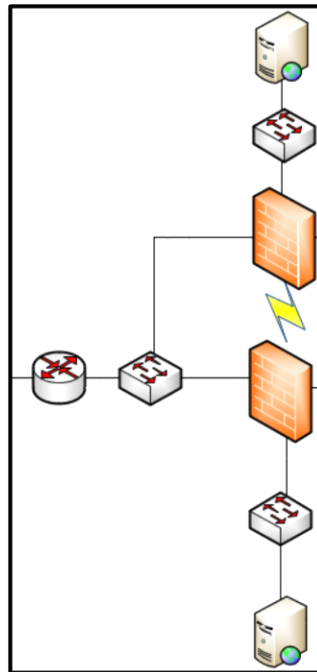
Puis j'active la diffusion simultanée et l'accès aux deux serveurs est simultanée



```
Activités Terminator mar. 15:07  
debian@WEBINT-master: ~  
WEB-gestion  debian@WEBINT-master: ~ 42x28  WEB-gestion  debian@WEBINT-master: ~ 43x28  
root@WEBINT-backup:~#  root@WEBINT-master:/home/debian#
```

II. Serveur Web EXT

Dans le même esprit que les serveur Web INT je suis obligé de rajouté un routeur car le protocole CARP et les VIP ne permettent pas de mettre des routes sur une seul interface physique contenu dans la VIP



J'ajoute donc le routeur et le parametre

```
interface Ethernet0/0
 ip address 172.29.1.10 255.255.255.0
!
interface Ethernet0/1
 ip address 172.28.1.12 255.255.255.0
!
```

Puis je paramètre la nouvelle passerelle du Firewall dual WAN

```
LAN (lan) -> em0 -> v4: 172.29.1.11/24
```

	GW_LAN	LAN	172.29.1.10	172.29.1.10	Interface lan Gateway	
--	--------	-----	-------------	-------------	-----------------------	--

Puis je rajoute la route par default sur le Routeur

```
IOU3(config)#ip route 0.0.0.0 0.0.0.0 172.29.1.11
```

Ensuite la route Static

	172.28.1.0/24	GW_LAN - 172.29.1.11	LAN	
--	---------------	----------------------	-----	--

Et enfin la route vers 172.21.1.0 réseau de la BDD

```
IOU3(config)#ip route 172.21.1.0 255.255.255.0 172.28.1.1
```

Donc le routeur est bien paramétré et internet passe bien dans le réseau GSB. Maintenant je paramètre le SSH pour le fonctionnement de Terminator



J'ajoute tout d'abord les deux fameuses routes sur le routeur

```
routerext(config)#ip route 172.31.1.0 255.255.255.0 172.28.1.11  
routerext(config)#ip route 172.20.1.0 255.255.255.0 172.28.1.10
```

Puis paramètre le SSH sur les deux machines

```
# default value.  
Port 2223  
#AddressFamily any  
#ListenAddress 0.0.0.0  
#ListenAddress ::  
  
#HostKey /etc/ssh/ssh_host_rsa_key  
#HostKey /etc/ssh/ssh_host_ecdsa_key  
#HostKey /etc/ssh/ssh_host_ed25519_key  
█  
#LoginGraceTime 2m  
PermitRootLogin yes  
#StrictModes yes  
#MaxAuthTries 6  
#MaxSessions 10  
  
PubkeyAuthentication yes
```

Ensuite je rajoute les règles sur l'interface WAN en **pensant au NAT de l'interface WAN**

<input type="checkbox"/>	✓	0/0 B	IPv4 TCP	172.20.1.100 *	172.31.1.100	2223	*	none	
<input type="checkbox"/>	✓	0/0 B	IPv4 TCP	172.28.1.11 *	172.20.1.100	2223	*	none	

Puis la règle sur OPT1






<input type="checkbox"/>	✓	0/0 B	IPv4 TCP	172.20.1.100 *	172.31.1.100	2223	*	none	
--------------------------	---	-------	----------	----------------	--------------	------	---	------	--

Et enfin la route static




<input checked="" type="checkbox"/>		172.31.1.0/24		WAN - 172.28.1.12		WAN			
-------------------------------------	--	---------------	--	-------------------	--	-----	--	--	--

Maintenant je fais les paramétrages sur le Firewall de redondance

Je rajoute les Rules WAN en **pensant au NAT de l'interface WAN**

<input type="checkbox"/>	✓	0/0 B	IPv4 TCP	172.31.1.100	*	172.20.1.100	2223	*	none	  
<input type="checkbox"/>	✓	0/0 B	IPv4 TCP	172.28.1.10	*	172.31.1.100	2223	*	none	  

Puis les Rules OPT1

<input type="checkbox"/>	✓	0/0 B	IPv4 TCP	172.31.1.100	*	172.20.1.100	2223	*	none	  
--------------------------	---	-------	----------	--------------	---	--------------	------	---	------	---

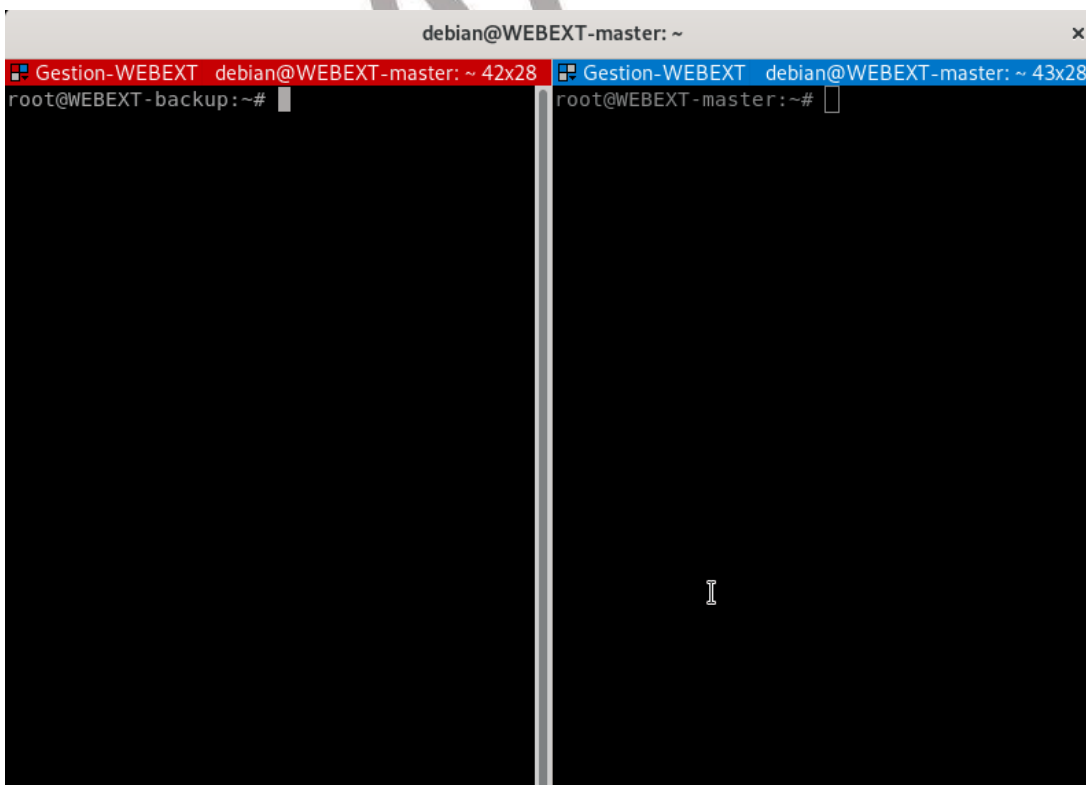
Et enfin la route static

<input checked="" type="checkbox"/>	172.20.1.0/24	WAN - 172.28.1.12	WAN	  
-------------------------------------	---------------	-------------------	-----	---

Puis je fais le test de fonctionnement via Terminator sur le serveur Master

```
root@WEBEXT-master:~# ssh -p 2223 root@172.31.1.100
root@172.31.1.100's password:
Linux WEBEXT-backup 4.19.0-16-amd64 #1 SMP
Debian 4.19.181-1 (2021-03-19) x86_64
```

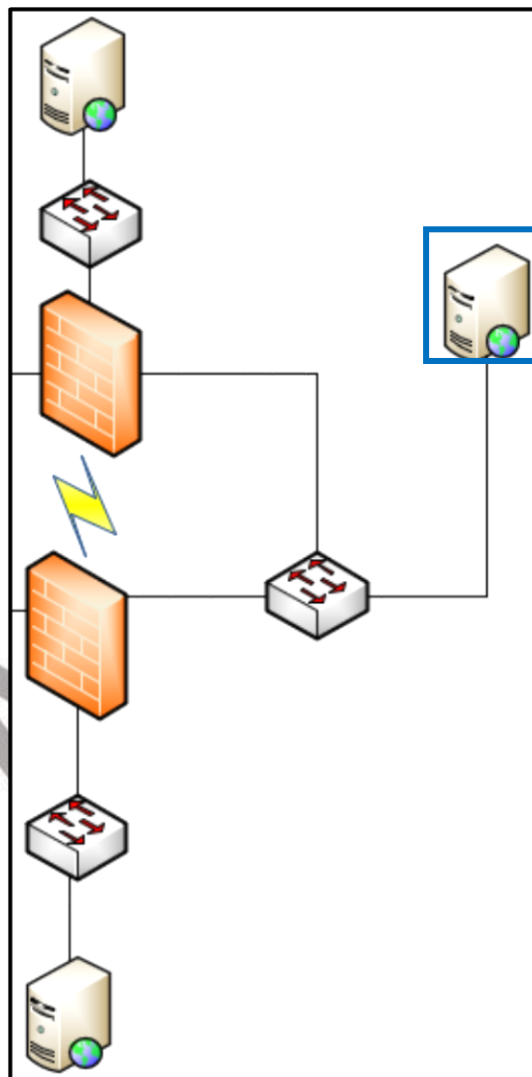
Puis je test le fonctionnement avec la diffusion de groupe



5) Redondance site WEB

I. Site Web internet.gsb.fr

Pour illustrer la redondance de site WEB je vais utiliser le site interne.gsb.fr et rajouter un serveur de Load Balancing



Je parametre le serveur de Load Balancing

```
allow-hotplug enp0s3
iface enp0s3 inet static
    address 172.18.0.4/24
    gateway 172.18.0.1
```

```

GNU nano 3.2 /etc/hosts
127.0.0.1    localhost
127.0.1.1    debian
172.18.0.4   interne.gsb.fr
172.19.1.100 cluster1.gsb.fr cluster1
172.30.1.100 cluster2.gsb.fr cluster2

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

```

```

GNU nano 3.2 /etc/hostname
interne.gsb.fr

```

Puis je paramètre les règles sur les Firewalls

Firewalls INT :

OPT1

<input type="checkbox"/>	✓	0/0 B	IPv4 *	172.19.1.100	*	172.18.0.4	*	*	none				
<input type="checkbox"/>	✓	0/0 B	IPv4 *	172.18.0.4	*	172.19.1.100	*	*	none				

LAN

<input type="checkbox"/>	✓	0/0 B	IPv4 *	172.19.1.100	*	172.18.0.4	*	*	none				
<input type="checkbox"/>	✓	0/0 B	IPv4 *	172.18.0.4	*	172.19.1.100	*	*	none				

Firewall INT RED

LAN

<input type="checkbox"/>	✓	0/0 B	IPv4 *	172.30.1.100	*	172.18.0.4	*	*	none				
<input type="checkbox"/>	✓	0/0 B	IPv4 *	172.18.0.4	*	172.30.1.100	*	*	none				

OPT1

<input type="checkbox"/>	✓	0/0 B	IPv4 *	172.30.1.100	*	172.18.0.4	*	*	none				
<input type="checkbox"/>	✓	0/0 B	IPv4 *	172.18.0.4	*	172.30.1.100	*	*	none				

Puis je mets en place le Load Balancing sur le serveur LB

Je commence par activer les modules apache pour le Load Balancing

Module : `proxy_http, proxy_balancer, lbmethodby_*`

Puis je mets les paramètres de redondance dans 000-default.conf

```
GNU nano 3.2 /etc/apache2/sites-available/000-default.conf
<VirtualHost 172.18.0.4:80>
  ServerName interne.gsb.fr

  #definition du pool de serveurs "backend"
  <Proxy balancer://gsb_cluster>
    BalancerMember http://172.19.1.100
    BalancerMember http://172.30.1.100 status=H
  </Proxy>

  #ajout du header Via
  ProxyVia Full
  #ajout des headers X-forwarded-*
  ProxyAddHeaders On

  #Fonction reverse proxy
  ProxyPass / balancer://gsb_cluster
  ProxyPassReverse / balancer://gsb_cluster

  LogLevel warn

  ErrorLog ${APACHE_LOG_DIR}/error.log
  CustomLog ${APACHE_LOG_DIR}/acces.log combined
</VirtualHost>
```

Puis je paramètre le serveur WEB master

```
GNU nano 3.2 /etc/apache2/sites-available/001-interne.conf
<VirtualHost interne.gsb.fr:80>
  ServerName domain.tld
  ServerAlias www.domain.tld

  DocumentRoot /var/www/html/interneSite/public
  DirectoryIndex /index.php

  <Directory /var/www/html/interneSite/public>
    AllowOverride None
    Order Allow,Deny
    Allow from All

    FallbackResource /index.php
  </Directory>

  # uncomment the following lines if you install assets as symlinks
  # or run into problems when compiling LESS/Sass/CoffeeScript assets
  # <Directory /var/www/project>
  #   Options FollowSymlinks
  # </Directory>

  # optionally disable the fallback resource for the asset directories
  # which will allow Apache to return a 404 error when files are
  # not found instead of passing the request to Symfony
  <Directory /var/www/html/interneSite/public/bundles>
    FallbackResource disabled
  </Directory>
  ErrorLog /var/log/apache2/project_error.log
  CustomLog /var/log/apache2/project_access.log combined

  # optionally set the value of the environment variables used in the application
  #SetEnv APP_ENV prod
```

Puis ensuite je mets en place l'enregistrement DNS sur le serveur AD/DNS/DHCP

Puis je fais de même sur le serveur web de redondance

```
GNU nano 3.2 /etc/apache2/sites-available/001-interne.conf
<VirtualHost interne.gsb.fr:80>
  ServerName domain.tld
  ServerAlias www.domain.tld

  DocumentRoot /var/www/html/interneSite/public
  DirectoryIndex /index.php

  <Directory /var/www/html/interneSite/public>
    AllowOverride None
    Order Allow,Deny
    Allow from All

    FallbackResource /index.php
  </Directory>

  # uncomment the following lines if you install assets as symlinks
  # or run into problems when compiling LESS/Sass/CoffeeScript assets
  # <Directory /var/www/project>
  #   Options FollowSymlinks
  # </Directory>

  # optionally disable the fallback resource for the asset directories
  # which will allow Apache to return a 404 error when files are
  # not found instead of passing the request to Symfony
  <Directory /var/www/html/interneSite/public/bundles>
    FallbackResource disabled
  </Directory>
  ErrorLog /var/log/apache2/project_error.log
  CustomLog /var/log/apache2/project_access.log combined

  # optionally set the value of the environment variables used in the application
  #SetEnv APP_ENV prod
```

Puis je mets l'IP de la BDD dans /etc/apache2/site-available/frontSite/.env

```
DATABASE_URL=mysql://siteExterne:secret@172.21.1.100:3306/siteExterne?serverVer:
###< doctrine/doctrine-bundle ###
```

Je le fais sur les deux serveurs WEB du cluster

Je vérifie déjà que la BDD répond sur le premier serveur WEB

Pour être au plus proche de la configuration que je souhaite la machine cluster2 doit être en backup et de prendre le dessus que si cluster1 tombe

Donc je modifie le fichier apache sur le serveur LB

```
BalancerMember http://172.30.1.100 status=H
```

Puis je test en éteignant le serveur WEB principal



← → ↻ ⚠ Non sécurisé | interne.gsb.fr

Datainterne index

Cle	primaire	Champinterne1	Champinterne2	Champinterne3	actions
1	test	test	test	show edit	

[Create new](#)

Ca fonctionne bien, le basculement est bien opérationnel

Puis j'ajoute le mode sticky et LoadBalancing

Tout d'abord j'active le module headers

```
root@interne:~# a2enmod headers
```

Puis je mets a jour le fichier de configuration

```
<VirtualHost 172.18.0.4:80>
  ServerName interne.gsb.fr

  Header add Set_Cookie "COOKIE_LB=gsb.%(BALANCER_WORKER_ROUTE)e; path=/ env=BALANCER_ROUTE_C$

  Header add X-LB-Backend %(BALANCER_WORKER_NAME)e
  Header add X-LB-Name %(BALANCER_NAME)e

  #definition du pool de serveurs "backend"
  <Proxy balancer://gsb_cluster>
    ProxySet stickysession=COOKIE_LB
    ProxySet lbmethod=bytraffic
    BalancerMember http://172.19.1.100 route=cluster1
    BalancerMember http://172.30.1.100 route=cluster2
  </Proxy>

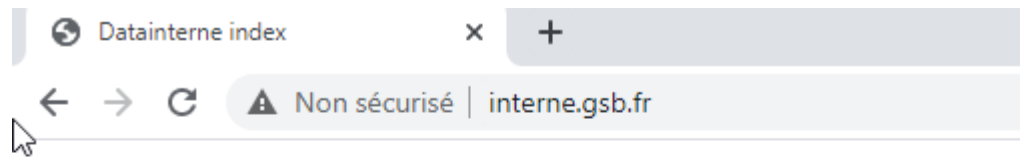
  #ajout du header Via
  ProxyVia Full
  #ajout des headers X-forwarded-*
  ProxyAddHeaders On

  #Fonction reverse proxy
  ProxyPass / balancer://gsb_cluster
  ProxyPassReverse / balancer://gsb_cluster

  LogLevel warn

  ErrorLog ${APACHE_LOG_DIR}/error.log
  CustomLog ${APACHE_LOG_DIR}/acces.log combined
</VirtualHost>
```

Puis je vérifie que la page est toujours joignable

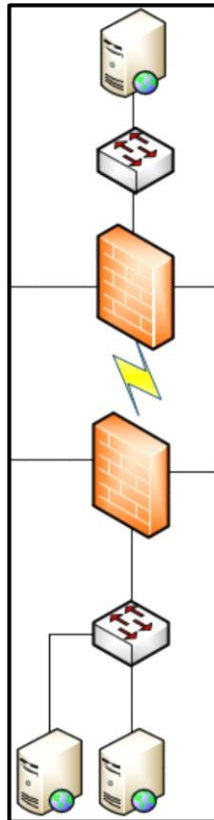


Datainterne index

Cleprimaire	Champinterne1	Champinterne2	Champinterne3	actions
1	test	test	test	show edit
Create new				

JFMARTIN

II. Site Web externe.gsb.fr



Pour le site externe.gsb.fr je reprends la même logique que pour le site interne.gsb.fr en adaptant les IP

Je paramètre le serveur de Load Balancing

```
iface enp0s3 inet static
    address 172.20.1.101/24
    gateway 172.20.1.254
```

```
externe.gsb.fr
```

```
127.0.0.1    localhost
127.0.1.1    debian
172.20.1.101 externe.gsb.fr
172.20.1.100 cluster1ext.gsb.fr cluster1ext
172.31.1.100 cluster2ext.gsb.fr cluster2ext
```

Puis je mets en place le Load Balancing sur le serveur LB

Je commence par activer les modules apache pour le Load Balancing

Module : `proxy_http, proxy_balancer, lbmethodby_*`

Puis je mets les paramètres de redondance dans 000-default.conf

```
<VirtualHost 172.20.1.101:80>
  ServerName externe.gsb.fr

  Header add Set_Cookie "COOKIE_LB=gsb.%(BALANCER_WORKER_ROUTE)e; path=/ env=BALANCER_ROUTE_C$

  Header add X-LB-Backend %(BALANCER_WORKER_NAME)e
  Header add X-LB-Name %(BALANCER_NAME)e

  #definition du pool de serveurs "backend"
  <Proxy balancer://gsb_clusterext>
    ProxySet stickySession=COOKIE_LB
    ProxySet lbmethod=bytraffic
    BalancerMember http://172.20.1.100 route=cluster1ext
    BalancerMember http://172.31.1.100 route=cluster2ext
  </Proxy>

  #ajout du header Via
  ProxyVia Full
  #ajout des headers X-forwarded-*
  ProxyAddHeaders On

  #Fonction reverse proxy
  ProxyPass / balancer://gsb_clusterext
  ProxyPassReverse / balancer://gsb_clusterext

  LogLevel warn

  ErrorLog ${APACHE_LOG_DIR}/error.log
  CustomLog ${APACHE_LOG_DIR}/access.log combined
</VirtualHost>
```

Puis je paramètre les serveurs WEB du cluster

```
GNU nano 3.2 /etc/apache2/sites-available/000-default.conf

<VirtualHost externe.gsb.fr:80>
  ServerName domain.tld
  ServerAlias www.domain.tld

  DocumentRoot /var/www/html/frontSite/public
  DirectoryIndex /index.php






  <Directory /var/www/html/frontSite/public>
    AllowOverride None
    Order Allow,Deny
    Allow from All

    FallbackResource /index.php
  </Directory>
```

Puis je mets la liaison avec la BDD dans /var/www/html/frontSite/.env

```
# Attention: you need configure your server version, check here or in config/p$
DATABASE_URL=mysql://siteExterne:secret@172.21.1.103:3306/siteExterne?serverVer$
###< doctrine/doctrine-bundle ###
```

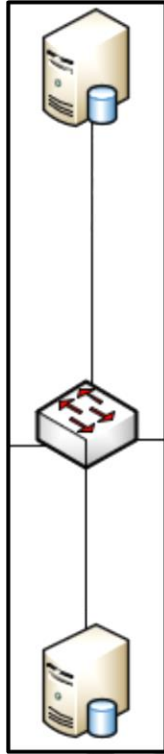
Puis j'ajoute l'enregistrement DNS externe

 (identique au dossier parent)	Source de nom (SOA)	[32], addnsdhcp.galaxy-s...	statique
 (identique au dossier parent)	Serveur de noms (NS)	redondance.galaxy-swiss.l...	statique
 (identique au dossier parent)	Serveur de noms (NS)	addnsdhcp.galaxy-swiss.l...	statique
 externe	Hôte (A)	172.20.1.101	statique
 interne	Hôte (A)	172.18.0.4	statique

Puis je mets les règles du firewall

JEMMARTIN

6) Redondance BDD



Pour faire la Redondance de la BDD j'utiliserais aussi Terminator



Une fois installé (apt install terminator) je configure le SSH sur chaque machine avec un port SSH différent du port par default (dans notre cas 2222)

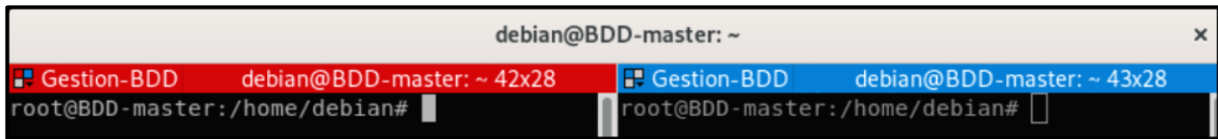
```
Port 2222
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::

#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_ecdsa_key
#HostKey /etc/ssh/ssh_host_ed25519_key

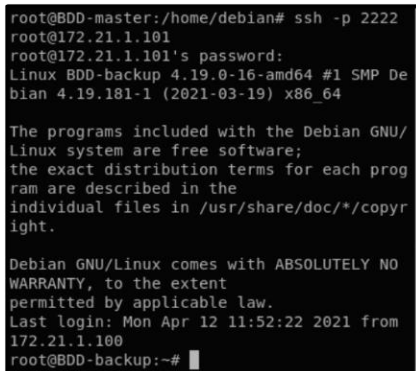
#LoginGraceTime 2m
PermitRootLogin yes
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10

PubkeyAuthentication yes
```

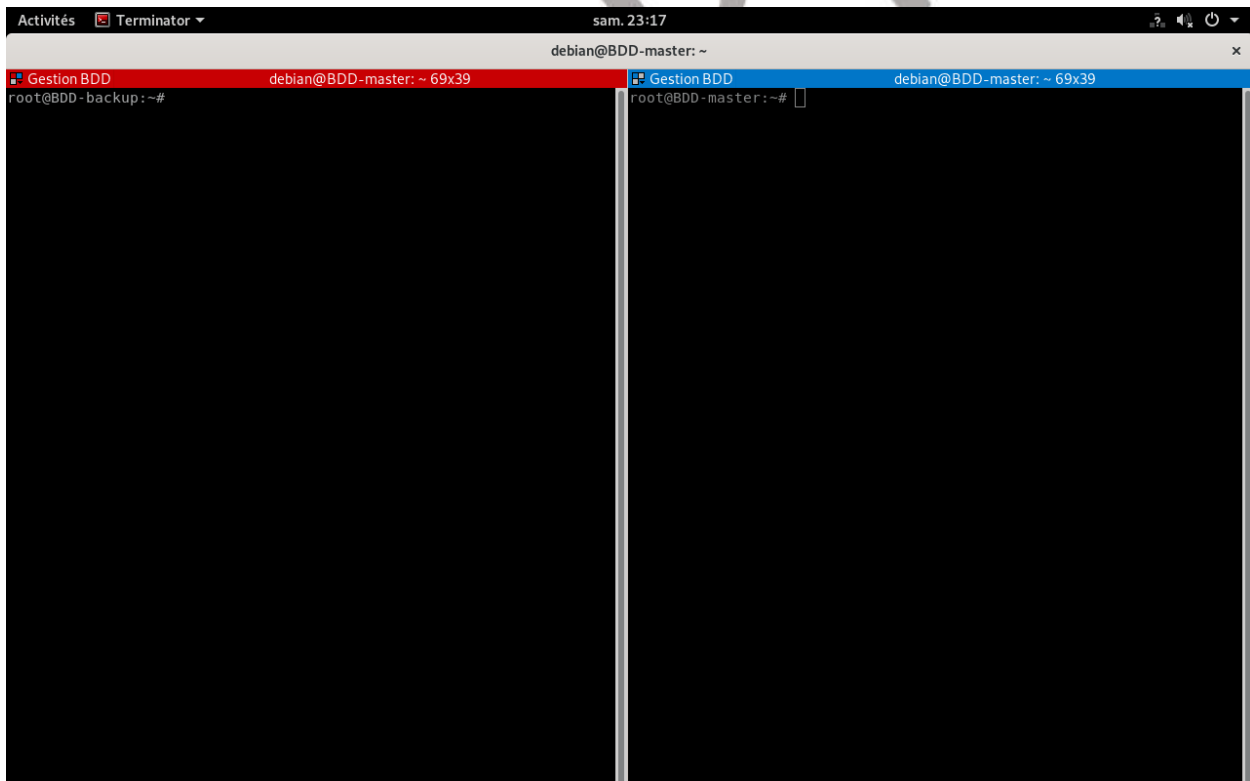
Puis je configure Terminator sur le Poste master en créant un groupe



Puis je me connecte en SSH sur l'autre BDD



Puis j'active la diffusion de groupe et je peux faire une saisie simultanée



Puis je rajoute la règle pour la nouvelle BDD dans le firewall



Puis pour ce qui est de la redondance MySQL et du LoadBalancing je vais utiliser deux solutions **Heartbeat** et **DRBD**. Heartbeat pour la preemption et la haute disponibilité des BDD et DRBD pour la partition ou se trouve MySQL.



Toutes les modifications simultanées sont faite grâce à Terminator en SSh

Modifications faites sur les deux machines

Je commence par mettre tous les hosts

```
127.0.0.1    localhost
127.0.1.1    debian
172.21.1.100 BDD-master
172.21.1.101 BDD-backup
```

Puis je créer la partition /sdb/sdb1 à répliquer

```
Commande (m pour l'aide) : n
Type de partition
  p  primaire (0 primaire, 0 étendue, 4 libre)
  e  étendue (conteneur pour partitions logiques)
Sélectionnez (p par défaut) : p
Numéro de partition (1-4, 1 par défaut) : 1
Premier secteur (2048-16777215, 2048 par défaut) :
Dernier secteur, +/-secteurs ou +/-taille{K,M,G,T,P} (2048-16777215, 16777215
par défaut) :

Une nouvelle partition 1 de type « Linux » et de taille 8 GiB a été créée.

Commande (m pour l'aide) : w
La table de partitions a été altérée.
Appel d'ioctl() pour relire la table de partitions.
Synchronisation des disques.
```

```
root@BDD-backup:~# lsblk
NAME MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
sda   8:0    0   8G  0 disk
├─sda1 8:1    0   6G  0 part /
├─sda2 8:2    0    1K  0 part
├─sda5 8:5    0   2G  0 part [SWAP]
sdb   8:16   0   8G  0 disk
├─sdb1 8:17   0   8G  0 part
sr0   11:0    1 1024M  0 rom
```

Puis j'installe le paquet *drbd-utils*

```
root@BDD-master:~# apt install drbd-utils
```

J'active drbd

```
root@BDD-master:~# modprobe drbd
```

Je crée un fichier de configuration de drbd pour configurer toute les machines du clusters

```
root@BDD-master:~# cd /etc/drbd.d/
root@BDD-master:/etc/drbd.d# ls
global_common.conf
root@BDD-master:/etc/drbd.d# touch drbd.res
```

Je configure le fichier

```
resource r0 {
    protocol C;
    startup {
        wfc-timeout 15;
        degr-wfc-timeout 60;
    }
    net {
        cram-hmac-alg sha1;
        shared-secret "gsb";
    }
    on BDD-master {
        device /dev/drbd0;
        disk /dev/sdb1;
        address 172.21.1.100:7788;
        meta-disk internal;
    }
    on BDD-backup {
        device /dev/drbd0;
        disk /dev/sdb1;
        address 172.21.1.101:7788;
        meta-disk internal;
    }
    syncer {
        rate 100M;
    }
}
```

Puis je mets en fonctionnement drbd

```
root@BDD-master:~# su
root@BDD-master:~# drbdadm create-md r0
initializing activity log
initializing bitmap (256 KB) to all zero
Writing meta data...
New drbd meta data block successfully created.
root@BDD-master:~# drbdadm up r0
root@BDD-master:~#
```

Je vérifie qu'il est bien actif sur les deux machines

```
root@BDD-master:~# drbd-overview
NOTE: drbd-overview will be deprecated soon.
Please consider using drbdtop.

0:r0/0 Connected Secondary/Secondary Inconsistent/Inconsistent
root@BDD-master:~# █
```

```
root@BDD-backup:~# drbd-overview
NOTE: drbd-overview will be deprecated soon.
Please consider using drbdtop.

0:r0/0 Connected Secondary/Secondary Inconsistent/Inconsistent
root@BDD-backup:~# █
```

Les deux sont en Secondary, normal car il n'y a pas encore eu de définition de la machine master

Modification suivante seulement sur la machine master

Je mets la machine « BDD-master » en primaire du cluster

```
root@BDD-master:~# drbdadm -- --overwrite-data-of-peer primary r0
root@BDD-master:~# drbdadm primary r0
```

Modification suivant sur les deux machines

Puis je vérifie si la synchronisation ce fait et si il y a bien Primary/Secondary sur la machine master et Secondary/Primary sur la machine backup

```
Every 2,0s: drbd-overview      BDD-master: Mon May  3 20:26:05 2021
NOTE: drbd-overview will be deprecated soon.
Please consider using drbdtop.

0:r0/0  SyncSource Primary/Secondary UpToDate/Inconsistent
[=====>.....] sync'ed: 45.6% (4464/8188)M

Every 2,0s: drbd-overview      BDD-backup: Mon May  3 20:26:05 2021
NOTE: drbd-overview will be deprecated soon.
Please consider using drbdtop.

0:r0/0  SyncTarget Secondary/Primary Inconsistent/UpToDate
[=====>.....] sync'ed: 45.6% (4464/8188)M
```

Si la synchronisation est bien fini il doit y avoir UpToDate/UpToDate à la fin de la phrase de configuration

Modification suivante seulement sur la machine master

Je formate la partition au bon format

```
root@BDD-master:~# mkfs.ext4 /dev/drbd0
mke2fs 1.44.5 (15-Dec-2018)
Creating filesystem with 2096823 4k blocks and 524288 inodes
Filesystem UUID: 78b202f3-9d73-4bed-83be-359a47d3b893
Superblock backups stored on blocks:
    32768, 98304, 163840, 229376, 294912, 819200, 884736, 1605632

Allocating group tables: done
Writing inode tables: done
Creating journal (16384 blocks): done
Writing superblocks and filesystem accounting information: done
```

Puis je vérifie si la partition est bien présente dans le gestionnaire de partition

```
root@BDD-master:~# lsblk
NAME        MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
sda          8:0    0   8G  0 disk
├─sda1       8:1    0   6G  0 part /
├─sda2       8:2    0   1K  0 part
├─sda5       8:5    0   2G  0 part [SWAP]
sdb          8:16   0   8G  0 disk
├─sdb1       8:17   0   8G  0 part
└─┬drbd0    147:0   0   8G  0 disk
sr0         11:0    1 1024M 0 rom
```

A partir de la je mets en place Heartbeat

Modification suivant sur les deux machines

J'installe le paquet heartbeat

```
apt install heartbeat
```

Pour les fichiers de configuration je récupère les modèles disponible dans /usr/share/doc/heartbeat pour les mettre dans /etc/ha.d/

```
cp: tu cible 'authkeys' n'est pas un répertoire  
root@BDD-master:/usr/share/doc/heartbeat# cp {ha.cf.gz,haresources.gz,authkeys} /etc/ha.d/
```

Je unzip les fichiers de conf

```
root@BDD-master:/etc/ha.d# ls  
authkeys  harc          rc.d          resource.d  
ha.cf.gz  haresources.gz  README.config  shellfuncs  
root@BDD-master:/etc/ha.d# gzip -d haresources.gz  
root@BDD-master:/etc/ha.d# gzip -d ha.cf.gz  
root@BDD-master:/etc/ha.d# ls  
authkeys  harc          rc.d          resource.d  
ha.cf     haresources  README.config  shellfuncs
```

Puis je commence à paramétrer le fichier *ha.cf*

```
GNU nano 3.2 ha.cf  
debugfile /var/log/ha-debug  
logfile /var/log/ha-log  
logfacility local0  
keepalive 2  
deadtime 20  
warntime 10  
initdead 60  
udpport 694  
bcast enp0s3  
auto_failback on  
node BDD-master  
node BDD-backup
```

Puis le fichier *authkeys*, dans notre cas j'utiliserais seulement une sécurité sha1

```
GNU nano 3.2 authkeys  
auth 2  
#1 crc  
2 sha1 gsb  
#3 md5 Hello!
```

Puis je change la sécurisation de authkeys

```
chmod 600 authkeys
```

Ensuite je modifie le fichier haresources

```
GNU nano 3.2 haresources
BDD-master IPaddr::172.21.1.103/24/enp0s3 drbddisk::r0 Filesystem::/dev/drbd0::/mnt::ext4
```

Ensuite je mets chaque service au démarrage de la machine avec systemctl enable

Au redémarrage bien vérifier avec drbd-overview Bien vérifier qu'il y a Connected et

Primary/secondary et surtout /UpToDate/UpToDate.

Pour vérifier le fonctionnement le mets watch drbd-overview sur le backup et je stop heartbeat sur la machine master

```
Every 2,0s: drbd-overview BDD-backup: Mon May 3 22:08:22 2021
NOTE: drbd-overview will be deprecated soon.
Please consider using drbdtop.

0:r0/0 Connected Primary/Secondary UpToDate/UpToDate /mnt ext4 7.9G 36M 7.4G
1%
```

```
root@BDD-backup:/etc/ha.d# watch drbd-overview
root@BDD-backup:/etc/ha.d# df -h
Sys. de fichiers Taille Utilisé Dispo Uti% Monté sur
udev 979M 0 979M 0% /dev
tmpfs 200M 6,1M 194M 4% /run
/dev/sda1 5,9G 4,6G 1,1G 82% /
tmpfs 998M 53M 945M 6% /dev/shm
tmpfs 5,0M 0 5,0M 0% /run/lock
tmpfs 998M 0 998M 0% /sys/fs/cgroup
tmpfs 200M 28K 200M 1% /run/user/117
tmpfs 200M 0 200M 0% /run/user/0
/dev/drbd0 7,9G 36M 7,4G 1% /mnt
root@BDD-backup:/etc/ha.d#
```

La partition est bien remontée est disponible depuis /mnt

Je redémarre heartbeat sur la machine master

```
debian@BDD-master: ~ 78x41
Every 2,0s: drbd-overview BDD-backup: Mon May 3 22:09:58 2021
NOTE: drbd-overview will be deprecated soon.
Please consider using drbdtop.

0:r0/0 Connected Secondary/Primary UpToDate/UpToDate
```

La machine master repasse bien master et la partition n'est plus disponible sur la machine backup

```
sdb 8:16 0 8G 0 disk
└─sdb1 8:17 0 8G 0 part
   └─drbd0 147:0 0 8G 1 disk
sr0 11:0 1 1024M 0 rom
root@BDD-backup:~#
```

Puis je mets en place les liens symboliques pour accéder a la BDD mysql qui est installé sur la partition par default

```
root@BDD-master:/mnt# ln -s /var/lib/mysql/ /mnt

root@BDD-master:/mnt# ls -la
total 24
drwxr-xr-x  3 root root  4096 mai   4 20:57 .
drwxr-xr-x 18 root root  4096 avril  9 01:23 ..
drwx-----  2 root root 16384 mai   3 20:40 lost+found
lrwxrwxrwx  1 root root    15 mai   4 20:57 mysql -> /var/lib/mysql/
root@BDD-master:/mnt#
```

Puis maintenant je modifie la BDD de manière à différencier la BDD master de la BDD backup

```
MariaDB [siteInterne]> UPDATE dataInterne SET champInterne1 ="l'adresse" WHERE cleP
rimaire=1;
Query OK, 1 row affected (0.012 sec)
Rows matched: 1 Changed: 1 Warnings: 0

MariaDB [siteInterne]> select * from dataInterne ;
+-----+-----+-----+-----+
| clePrimaire | champInterne1 | champInterne2 | champInterne3 |
+-----+-----+-----+-----+
|          1 | l'adresse     | test          | test          |
+-----+-----+-----+-----+
1 row in set (0.000 sec)

MariaDB [siteInterne]> UPDATE dataInterne SET champInterne2 ="est" WHERE clePrimair
e=1;
Query OK, 1 row affected (0.055 sec)
Rows matched: 1 Changed: 1 Warnings: 0

MariaDB [siteInterne]> UPDATE dataInterne SET champInterne3 ="172.21.1.100" WHERE c
lePrimaire=1;
Query OK, 1 row affected (0.009 sec)
Rows matched: 1 Changed: 1 Warnings: 0

MariaDB [siteInterne]> select * from dataInterne ;
+-----+-----+-----+-----+
| clePrimaire | champInterne1 | champInterne2 | champInterne3 |
+-----+-----+-----+-----+
|          1 | l'adresse     | est           | 172.21.1.100 |
+-----+-----+-----+-----+
1 row in set (0.000 sec)
```

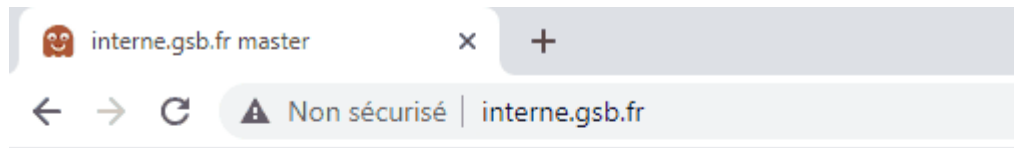
Pour la BDD master dans « champInterne3 » je mets .100 et backup .101

Puis je modifie la page HTML qui affiche la BDD qui se trouve dans /var/www/html/interneSite/Template/dataInterne/index.html.twig sur les serveurs webs

```
{% block title %}interne.gsb.fr master{% endblock %}
{% block body %}
  <h1>interne.gsb.fr BDD master</h1>
{% endblock %}

{% block title %}interne.gsb.fr backup{% endblock %}
{% block body %}
  <h1>interne.gsb.fr BDD backup</h1>
{% endblock %}
```

Puis j'actualise la page pour voir si les informations ont bien été mise à jour



interne.gsb.fr BDD master

	Cleprimaire	Champinterne1	Champinterne2	Champinterne3	actions
1	l'adresse	est	172.21.1.100	show edit	

[Create new](#)

On va bien la page du master et du backup qui alterne avec le load balancing

Maintenant je modifie l'ip de redirection des serveurs web avec la VIP des BDD

```
DATABASE_URL=mysql://siteInterne:secret@172.21.1.103:3306/siteInterne?serverVer$  
###< doctrine/doctrine-bundle ###
```

Puis je rajoute les règles sur les Firewalls pour autoriser la VIP des BDD

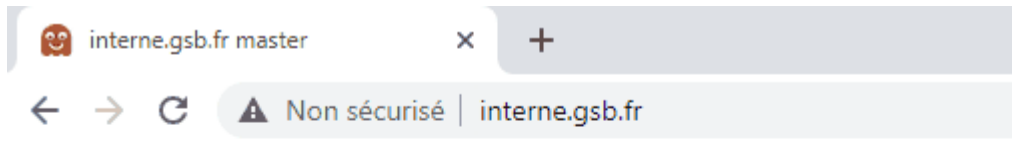
<input type="checkbox"/>	✓	0/0 B	IPv4*	172.30.1.100	*	172.21.1.103	*	*	none	
<input type="checkbox"/>	✓	0/0 B	IPv4*	172.19.1.100	*	172.21.1.103	*	*	none	

Maintenant je coupe heartbeat sur le serveur BDD master

```
Every 2,0s: drbd-overview                               BDD-backup: Fri May 7 16:01:37 2021  
  
NOTE: drbd-overview will be deprecated soon.  
Please consider using drbdtop.  
  
0:r0/0 StandAlone Primary/Unknown UpToDate/DUnknown /mnt ext4 7.9G 36M 7.4G 1%  
  
sdb          8:16    0    8G    0 disk  
└─sdb1       8:17    0    8G    0 part  
   └─drbd0   147:0    0    8G    0 disk /mnt  
sr0         11:0    1 1024M  0 rom  
root@BDD-backup:~#
```

On voit bien que c'est la BDD secondaire qui prend le dessus avec la bonne partition

Je vérifie sur le client que c'est bien la deuxième BDD qui répond



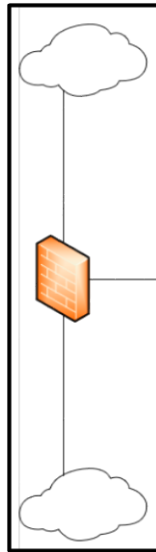
interne.gsb.fr BDD master

Cleprimaire	Champinterne1	Champinterne2	Champinterne3	actions
1	l'adresse	est	172.21.1.100	show edit
Create new				

On voit bien que c'est l'ip 172.21.1.101 qui prend le dessus et que la BDD backup prend la relève

JEMMARTIN

7) Redondance Internet



Je rajoute un NAT pour le deuxième accès internet

Comme le firewall possède seulement 4 sortie (WAN,LAN,OPT1 et OPT2) déjà toute prises je dois rajouter un firewall pour illustrer le Dual WAN (le firewall n'applique donc aucune règle de filtrage)

Puis j'ajoute l'interface WAN2 puis la mets en DHCP

Interfaces / WAN2 (em1) ☰ 📶 ⓘ

General Configuration

Enable Enable interface

Description
Enter a description (name) for the interface here.

IPv4 Configuration Type

```
WAN (wan)      -> em2      -> v4/DHCP4: 192.168.122.190/24
LAN (lan)      -> em0      -> v4: 172.28.1.12/24
WAN2 (opt1)    -> em1      -> v4/DHCP4: 192.168.122.217/24
```

Puis j'active les options pour le Dual-WAN

Gateway Monitoring

State Killing on Gateway Failure Flush all states when a gateway goes down
 The monitoring process will flush all states when a gateway goes down if this box is checked.

Skip rules when gateway is down Do not create rules when gateway is down
 By default, when a rule has a gateway specified and this gateway is down, the rule is created omitting the gateway. This option overrides that behavior by omitting the entire rule instead.

Load Balancing

Load Balancing Use sticky connections

Successive connections will be redirected to the servers in a round-robin manner with connections from the same source being sent to the same web server. This "sticky connection" will exist as long as there are states that refer to this connection. Once the states expire, so will the sticky connection. Further connections from that host will be redirected to the next web server in the round robin. Changing this option will restart the Load Balancing service.

0

Set the source tracking timeout for sticky connections. By default this is 0, so source tracking is removed as soon as the state expires. Setting this timeout higher will cause the source/destination relationship to persist for longer periods of time.

Puis je créer le groupe de gateway avec la priorisation

Edit Gateway Group Entry

Group Name

Gateway Priority

<input type="text" value="WAN_DHCP"/>	Tier 2	Interface Address:	Interface WAN_DHCP Gateway
<input type="text" value="GW_LAN"/>	Never	Interface Address:	Interface lan Gateway
<input type="text" value="WAN2"/>	Tier 1	Interface Address:	Group Name



Gateway	Tier	Virtual IP	Description

Link Priority The priority selected here defines in what order failover and balancing of links will be done. Multiple links of the same priority will balance connections until all links in the priority will be exhausted. If all links in a priority level are exhausted then the next available link(s) in the next priority level will be used.

Virtual IP The virtual IP field selects which (virtual) IP should be used when this group applies to a local Dynamic DNS, IPsec or OpenVPN endpoint.

Trigger Level
 When to trigger exclusion of a member

Gateway Groups

Group Name	Gateways	Priority	Description	Actions
MULTIWAN	WAN_DHCP WAN2	Tier 2 Tier 1		  

Je mets le groupe gateway par défaut

Default gateway

Default gateway IPv4: MULTIWAN ()
Select the gateway or gatewaygroup to use as the default gateway.

Default gateway IPv6: Automatic
Select the gateway or gatewaygroup to use as the default gateway.

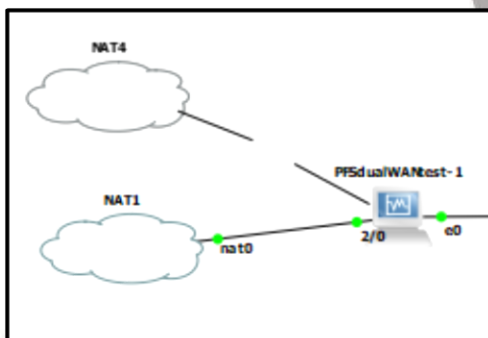
Gateways

Name	Default	Interface	Gateway	Monitor IP	Description	Actions
<input checked="" type="checkbox"/> WAN_DHCP	Tier 2 (IPv4)	WAN	192.168.122.1	192.168.122.1	Interface WAN_DHCP Gateway	
<input type="checkbox"/> GW_LAN		LAN	172.28.1.1	172.28.1.1	Interface lan Gateway	
<input type="checkbox"/> WAN2	Tier 1 (IPv4)	WAN2	192.168.122.1	192.168.122.1		

Puis le mets le groupe gateway sur les règles du LAN

6 / 74 KiB IPv4* * * * * MULTIWAN none

Je coupe une connexion pour tester



C'est bien l'autre interface qui prend le dessus

Gateways

Name	Default	Interface	Gateway	Monitor IP	Description	Actions
<input checked="" type="checkbox"/> WAN_DHCP	Tier 2 (IPv4)	WAN	192.168.122.1	192.168.122.1	Interface WAN_DHCP Gateway	
<input type="checkbox"/> GW_LAN		LAN	172.28.1.1	172.28.1.1	Interface lan Gateway	
<input type="checkbox"/> WAN2	Tier 1 (IPv4)	WAN2	dynamic	dynamic		