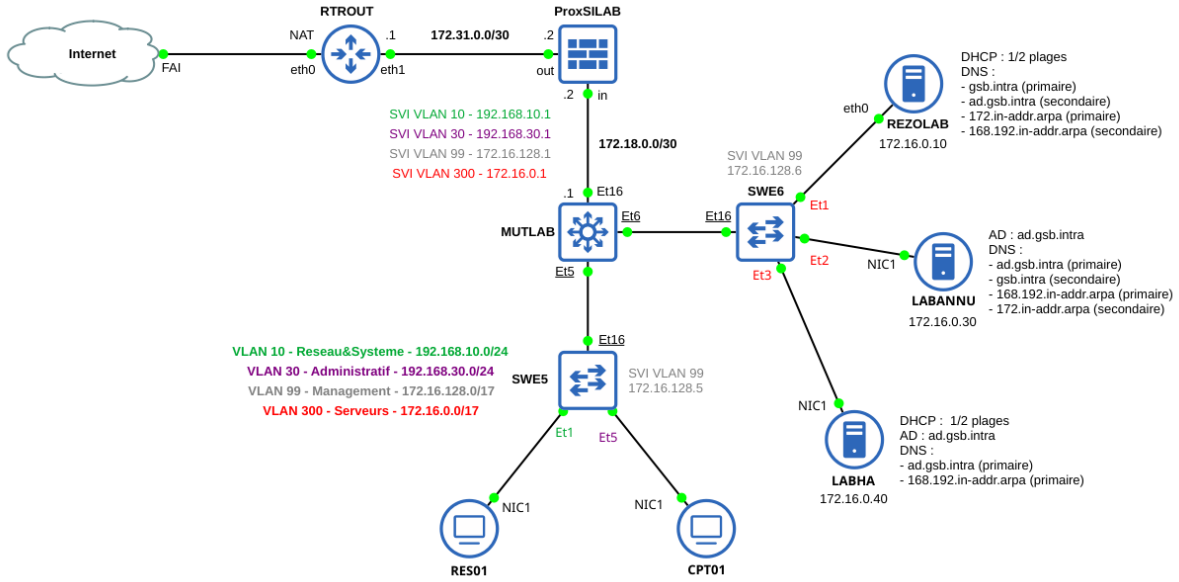
Haute disponibilité et répartition de charge des services AD, DNS et DHCP de GSB

Présentation de la plateforme



Le serveur **REZOLAB** est un serveur Linux Rocky 9 sur lequel les services **DNS** et **DHCP** sont configurés et fonctionnels, en attendant les modifications à apporter pour répondre aux nouveaux besoins.

Les serveurs **LABANNU** et **LABHA** sont des machines sous Windows Server 2022. Aucune configuration n'a encore été effectuée sur ces serveurs.

Les contrôleurs de domaine LABANNU et LABHA

LABANNU et LABHA sont les contrôleurs de domaine du domaine **ad.gsb.intra**.

Le service d'annuaire permet à l'entreprise GSB d'administrer les ordinateurs distribués, les comptes utilisateurs ainsi que l'accès aux ressources du domaine. Ces deux serveurs formeront un cluster Active Directory multimaitre, garantissant une haute disponibilité et une répartition de la charge entre les contrôleurs de domaine.

Pensez à renommer les serveurs en LABANNU et LABHA avant d'installer le service AD DS sur chaque serveur

Utilisateurs du domaine

Services	Utilisateurs
Réseau & Système	FRAZAT Laurent
	CHASTANG Ludovic
Comptabilité	VERNET Pierre
	EDOH Joan

Règles de gestion de l'accès aux ressources

- Chaque utilisateur possède un répertoire personnel. Il en a l'exclusivité.
- Chaque service doit pouvoir échanger des documents par l'intermédiaire d'un dossier commun au service. Les personnels du service peuvent alimenter le répertoire comme ils le souhaitent. Ils sont, bien entendu, les seuls à pouvoir le parcourir. Un fichier ou sous-répertoire ne peut être supprimé que par celui qui l'a créé.
- Le laboratoire met à disposition de tous les employés un certain nombre de documents (charte informatique, organigramme, etc.) grâce à un répertoire commun à tous. Ce dernier ne peut en aucun cas être utiliser par le personnel pour échanger : l'accès s'effectue en lecture uniquement.
- Les utilisateurs accèdent aux dossiers partagés, au travers de lecteurs réseaux connectés automatiquement à l'ouverture de session.

Exemple : L'utilisateur FRAZAT accède, dans l'explorateur de fichiers, aux lecteurs réseaux suivants :
I:\FRAZAT(répertoire personnel)
J:\RES (répertoire d'échange du service Réseau & Système)
K:\COM (répertoire commun à tous les employés)

Déploiement d'applications

Des applications doivent pouvoir être déployées, au besoin, par l'intermédiaire de GPO. Ainsi, par exemple, tous les postes client Windows doivent disposer du navigateur Web Firefox.

Les serveurs DNS REZOLAB, LABANNU et LABHA

Les zones DNS directes gsb.intra et ad.gsb.intra

Le serveur DNS REZOLAB fait autorité sur la zone **gsb.intra**.

```
[sysadmin@rezolab ~]$ sudo cat /etc/named.conf
//
// named.conf
//
...
zone "gsb.intra" {
    type master;
    file "gsb.intra.zone";
    allow-query { any; };
    allow-transfer { none; };
};
...

[sysadmin@rezolab ~]$ sudo cat /var/named/gsb.intra.zone
$TTL 8h
@               IN SOA  rezolab.gsb.intra. hostmaster.gsb.intra. (
                                        2023032801 ; serial number
                                        1d         ; refresh period
                                        3h         ; retry period
                                        3d         ; expire time
                                        3h )       ; minimum TTL

                IN NS   rezolab.gsb.intra.

bdweb           IN      A       172.16.100.100
frais           IN      CNAME   weblab
mutlab          IN      A       172.16.128.1
proxsilab       IN      A       172.18.0.2
rezolab         IN      A       172.16.0.10
rtrout          IN      A       172.31.0.1
swdmz           IN      A       10.0.0.1
swe4            IN      A       172.16.128.4
swe5            IN      A       172.16.128.5
swe6            IN      A       172.16.128.6
```

```
weblab          IN      A       10.0.0.100
```

Après configuration du cluster Active Directory multimaitre, Les serveurs DNS LABANNU et LABHA font tous les 2 autorité sur la zone **ad.gsb.intra**, intégrée à Active Directory. Ils se répartissent la charge de la résolution des requêtes DNS liées à cette zone. En cas de défaillance d'un des serveurs, l'autre pourra toujours répondre aux requêtes DNS, garantissant ainsi la résilience du service.

Notez également que LABANNU appartient également à cette zone :

```
labannu.ad.gsb.intra. IN A 172.16.0.30
```

REZOLAB doit donc déléguer la gestion du sous-domaine **ad.gsb.intra** à LABANNU et LABHA.

Pour des raisons de résilience, la zone **gsb.intra** sera répliquée sur LABANNU. Cela permettra à LABANNU de jouer le rôle de serveur DNS secondaire pour la zone **gsb.intra**. Ainsi, LABANNU maintiendra une copie exacte des enregistrements DNS de la zone principale et pourra répondre aux requêtes DNS en cas de défaillance du serveur primaire, assurant ainsi la continuité du service.

> ⓘ Dans un environnement **DNS principal/secondaires** traditionnel, un serveur DNS est désigné comme le serveur **principal (maître)** et les autres comme le serveurs **secondaires (esclaves).** Chaque serveur secondaire contient une copie répliquée des enregistrements DNS du serveur principal.
> Dans un environnement Active Directory multimaitre, les deux serveurs DNS partagent le même rôle et sont **tous deux considérés comme des serveurs DNS principaux**

Les zones DNS inverses 172.in-addr.arpa 168.192.in-addr.arpa

REOZLAB est actuellement serveur DNS principal pour la zone inverse **172.in-addr.arpa**

LABANNU et LABHA doivent être les serveurs DNS principaux pour la zone inversée **168.192.in-addr.arpa**

REZOLAB doit également être configuré en tant que serveur DNS secondaire pour la zone inversée **168.192.in-addr.arpa**, tandis que L**ABANNU** doit être configuré en tant que serveur DNS secondaire pour la zone inversée **172.in-addr.arpa**.

Cela garantit la répartition des rôles de serveur DNS principal et secondaire entre les différentes zones inversées pour assurer une résilience et une redondance des services DNS.

Les serveurs DHCP REZOLAB et LABHA

Les 2 serveurs DHCP doivent être configurés pour distribuer des configurations IP dans les VLAN existants :

- Les 2 serveurs doivent être actifs et se partager équitablement les plages d'adresses distribuées.
- Les 5 dernières adresses de chaque réseau sont réservées aux adresses fixes.
- Les serveurs DHCP doivent fournir les serveurs DNS REZOLAB, LABHA, et LABANNU en round robin. Cela signifie que lorsque le serveur DHCP attribue des adresses IP aux clients, il doit fournir ces trois serveurs DNS de manière cyclique, afin de répartir la charge de résolution DNS entre eux.

```
[sysadmin@rezolab ~]$ sudo cat /etc/dhcp/dhcpd.conf
#
# DHCP Server Configuration file.
#   see /usr/share/doc/dhcp-server/dhcpd.conf.example
#   see dhcpd.conf(5) man page
#

# Serveur DNS
option domain-name-servers 172.16.0.10;
option domain-name "gsb.intra";

# Bail de 2 heures
default-lease-time 7200;

authoritative;

# VLAN 10 - Reseau&Systeme
subnet 192.168.10.0 netmask 255.255.255.0 {
   range 192.168.10.11 192.168.10.249;
   option routers 192.168.10.1;
}

# VLAN 20 - Direction
subnet 192.168.20.0 netmask 255.255.255.0 {
   range 192.168.20.11 192.168.20.249;
   option routers 192.168.20.1;
}

# VLAN 30 - Administratif
subnet 192.168.30.0 netmask 255.255.255.0 {
   range 192.168.30.11 192.168.30.249;
   option routers 192.168.30.1;
}

# VLAN 150 - Visiteurs
subnet 192.168.150.0 netmask 255.255.255.0 {
   range 192.168.150.11 192.168.150.249;
   option routers 192.168.150.1;
}

# VLAN 300 - Serveurs
subnet 172.16.0.0 netmask 255.255.128.0 {
}
```

Ressources :

Sur Active Directory :

Notions de base de l'Active Directory
Créer un domaine AD avec Windows Server 2016
Active Directory (ADDS) : ajouter un contrôleur de domaine à un domaine existant

Sur le partage de dossiers et les droits NTFS :

Serveurs de fichiers – Créer son premier partage sous Windows Server 2022
Serveur de fichiers – Les permissions NTFS et de partage
AGDLP – Bien gérer les permissions de son serveur de fichiers

Sur les GPO :

Débuter avec les stratégies de groupe sous Windows Server
Comment déployer un logiciel au format MSI par GPO ?

Sur le mappage de lecteur réseau :

3 façons de connecter un lecteur réseau sous Windows 11
Comment mapper un lecteur réseau par GPO ?
Lecteur réseau : comment créer un script de connexion avec net use ?
Connecter un lecteur réseau en PowerShell

Sur le DNS

Mise en place et configuration d'un serveur DNS BIND