

Filière : Cycle d'Ingénieurs en Génie Informatique
Module : Interconnexion et Administration des réseaux

Rapport de projet intitulé :

Services des Réseaux sous Linux

Réalisé par :

- ☐ BANNANY Brahim
- ☐ MAHROUCH Mohamed

Encadré par :

Prof. Fatima AMOUNAS

Présenté le : 29/04/2025

Dédicaces

Toutes les lettres ne sauraient trouver les mots qu'il faut. Tous les mots ne sauraient exprimer la gratitude, l'amour, le respect, la reconnaissance. Avec un énorme plaisir, un cœur ouvert et une immense joie, que nous dédions ce travail :

À nos très chers, respectueux et magnifiques parents, qui nous ont offert sans condition leur soutien tout au long de notre vie.

À notre frère et notre sœur pour leur soutien aux moments difficiles de notre travail.

À tous nos chers amis, pour leurs encouragements permanents, et leur soutien
Moral,

À tous nos enseignants, votre générosité et votre soutien nous obligent à vous témoigner notre profond respect et notre loyale considération

À toutes les personnes qui nous ont aidés ou encouragés tout au long de nos études, nos professeurs et nos encadrants.

À tous ceux qui nous sont chers.

Remerciements

En tout premier lieu, nous remercions le bon Dieu, tout puissant, de nous avoir donné la force pour survivre, ainsi que l'audace pour Dépasser toutes les difficultés. Au nom du dieu le clément et le miséricordieux louange à ALLAH le tout puissant.

Nous tenons à remercier fortement la professeur **Fatima AMOUNAS** pour sa disponibilité et ses conseils qui nous ont permis toujours de poser de nouvelles questions et ainsi pour son suivi et pour son énorme soutien, qu'il n'a cessé de nous prodiguer tout au long de la période d'étude. Nous vous remercions d'avoir partagé avec nous votre passion pour l'enseignement. Nous avons grandement apprécié votre soutien, votre implication et votre expérience.
Merci Infiniment !

Résumé

Ce projet vise à mettre en œuvre une solution pour gérer un réseau qui intègre de manière optimale l'efficacité, la sécurité et la facilité d'administration. Il est structuré en trois phases : la première consiste en la mise en œuvre d'une infrastructure virtualisée comprenant des machines Linux, un routeur, des services DNS/DHCP et un serveur de sauvegarde pour créer les bases techniques du réseau. Dans la deuxième phase, nous ajoutons des fonctionnalités d'interopérabilité avancées (serveurs NIS, NFS, stations de travail Linux et Windows, et sauvegardes améliorées) pour optimiser la centralisation, l'échange et les processus de gestion des ressources. La troisième phase se concentre sur l'amélioration de la cybersécurité en ajoutant Security Onion pour la surveillance proactive, la détection d'intrusions et l'analyse des menaces. Ce système fournit aux administrateurs réseau un environnement d'habilitation robuste qui nécessite un suivi et un contrôle précis des performances tout en anticipant les pannes des dispositifs pour une simplification opérationnelle en temps utile, augmentant ainsi la performance globale et améliorant la résilience face aux incidents.

Table de matière

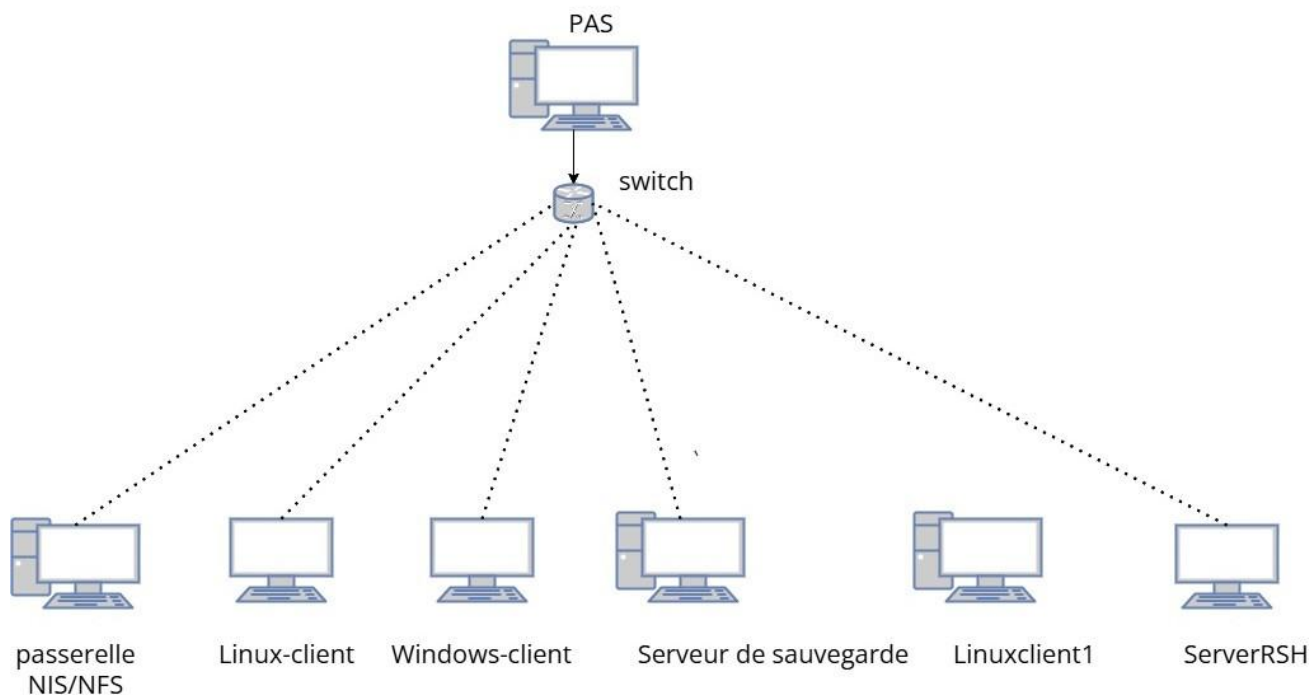
Dédicaces.....	2
Remerciements	3
Résumé.....	4
Table de matière	5
Introduction Générale	6
Chapitre 1 : Services Réseaux sous Linux.....	7
1. Architecture de parc de service informatique et de recherche	8
2. Parc de service Informatique.....	8
2.1. Description.....	8
2.2. Implémentation	9
2.2.1. Configuration DHCP.....	9
2.3.1. Configuration DNS.....	11
2.3.4. Configuration de serveur de sauvegarde Rsnapshot.....	14
2.4. Conclusion :.....	15
3. Parc de service de recherche	16
3.1. Description.....	16
3.2. Architecture de service de recherche	16
3.3. Implémentation de passerelle dotée des services NFS.....	17
3.4 Configuration du serveur NIS	19
Chapitre 2: Sécurité des Réseaux	23
1. Introduction	24
2. Description	24
3. Security Onion	24
3.1. Définition.....	24
3.2. Architecture de logiciel Security Onion	24
4. Implémentation.....	Erreur ! Signet non défini.

Introduction Générale

Dans un environnement dans lequel les réseaux informatiques sont prépondérants et représentent un enjeu fondamental de la communication contemporaine qui plus est exige des gestes techniques et des savoir-faire sécuritaires expertisés, la présente proposition d'architecture intègre l'administration du réseau autour de trois volets, la mise en place des conditions techniques de l'administration à proprement parler accompagné d'une phase de recherche développement afin de faire émerger les solutions les plus satisfaisantes en gestion centralisée des flux (virtualisation sous Linux, interopérabilité Windows) puis dans le volet sécurisation réseau au travers de SecurityOnion, un logiciel permettant de surveiller, détecter les intrusions et analyser les risques en temps réel, offrant ainsi au gestionnaire un ensemble d'outils performants, offrant performance fiabilité et protection contre les menaces dans un contexte de plus en plus exigeant des utilisateurs et incertain dans un monde numérique en perpétuelle mutation.

Chapitre 1 : Services Réseaux sous Linux

1. Architecture de parc de service informatique et de recherche



2. Parc de service Informatique

2.1. Description

Le service informatique central est responsable de la gestion du serveur d'entrée et de sortie du réseau de l'entreprise, ainsi que de certains services informatiques clés comme le DNS, le serveur DHCP et le serveur de sauvegarde.

La passerelle de l'entreprise (appelée « pas ») assure les fonctions de serveur DHCP, et de DNS interne et externe. Toutes les machines du service informatique central fonctionnent sous Linux et sont inscrites dans le domaine DNS « xx.cigi.ma ».

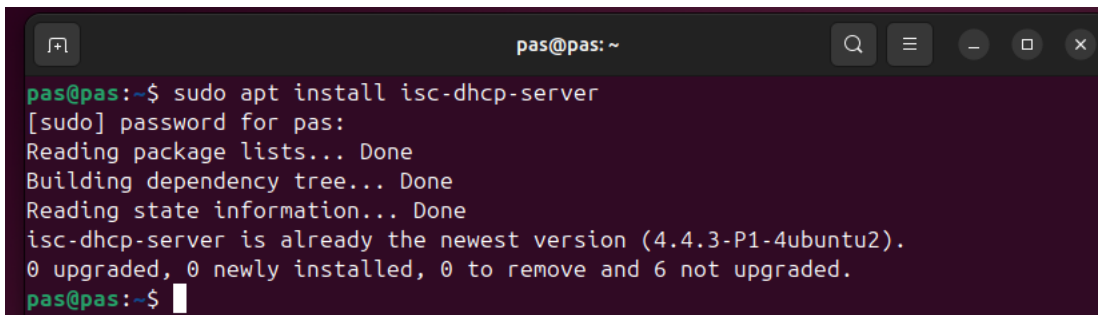
Le serveur de sauvegarde permet de réaliser des sauvegardes automatiques sans intervention humaine. Les données des utilisateurs sont sauvegardées à l'aide de l'outil « rsnapshot ». Les procédures de restauration des données et/ou des systèmes à partir de ces sauvegardes seront mises à disposition.

2.2. Implémentation

Dans la passerelle pas on a configuré le service DNS et DHCP pour une carte réseau, et encore un serveur de sauvegarde dans la carte de service informatique :

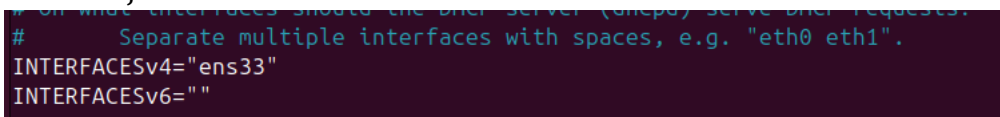
2.2.1. Configuration DHCP

- Installation DHCP



```
pas@pas:~$ sudo apt install isc-dhcp-server
[sudo] password for pas:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
isc-dhcp-server is already the newest version (4.4.3-P1-4ubuntu2).
0 upgraded, 0 newly installed, 0 to remove and 6 not upgraded.
pas@pas:~$
```

- Ajout le nom de carte réseaux



```
# On wide interfaces should the dhcp server (dhcpd) serve other requests.
#       Separate multiple interfaces with spaces, e.g. "eth0 eth1".
INTERFACESv4="ens33"
INTERFACESv6=""
```

- Modification du fichier de configuration du serveur DHCP
/etc/dhcp/dhcpd.conf avec notre éditeur de texte préféré et ajout des lignes suivantes pour configurer les paramètres du serveur DHCP

```
pas@pas: ~  
GNU nano 7.2 /etc/dhcp/dhcpd.conf  
}  
host client-linux1 {  
    hardware ethernet 00:0c:29:8a:be:79;  
    fixed-address 192.168.19.50;  
}  
  
host client-linux2 {  
    hardware ethernet 00:0c:29:11:e9:af;  
    fixed-address 192.168.19.51;  
}  
  
host server-RSH {  
    hardware ethernet 00:0c:29:08:8f:fd;  
    fixed-address 192.168.19.52;  
}  
  
host Passerelle-nfs {  
    hardware ethernet 00:0c:29:ec:94:19;  
    fixed-address 192.168.19.53;  
}
```

- Démarrage et vérification le statut de DHCP

```
pas@pas: ~  
pas@pas:~$ ^C  
pas@pas:~$ sudo systemctl restart isc-dhcp-server  
pas@pas:~$ sudo systemctl status isc-dhcp-server
```

```
pas@pas: ~  
isc-dhcp-server.service - ISC DHCP IPv4 server  
Loaded: loaded (/usr/lib/systemd/system/isc-dhcp-server.service; enabled; preset: enabled)  
Active: active (running) since Mon 2025-04-28 12:18:15 +01; 15s ago  
Docs: man:dhcpd(8)  
Main PID: 2807 (dhcpd)  
Tasks: 1 (limit: 4551)  
Memory: 4.1M (peak: 4.3M)  
CPU: 11ms  
CGroup: /system.slice/isc-dhcp-server.service  
└─2807 dhcpd -user dhcpd -group dhcpd -f -4 -pf /run/dhcp-server/dhcpd.pid -cf /etc/dhcp/dhcpd.conf ens33  
  
Apr 28 12:18:15 pas sh[2807]: Wrote 4 leases to leases file.  
Apr 28 12:18:15 pas dhcpd[2807]: Wrote 0 new dynamic host decls to leases file.  
Apr 28 12:18:15 pas dhcpd[2807]: Wrote 4 leases to leases file.  
Apr 28 12:18:15 pas dhcpd[2807]: Listening on LPF/ens33/00:0c:29:1e:29:ae/192.168.19.0/24  
Apr 28 12:18:15 pas sh[2807]: Listening on LPF/ens33/00:0c:29:1e:29:ae/192.168.19.0/24  
Apr 28 12:18:15 pas sh[2807]: Sending on LPF/ens33/00:0c:29:1e:29:ae/192.168.19.0/24  
Apr 28 12:18:15 pas sh[2807]: Sending on Socket/fallback/fallback-net  
Apr 28 12:18:15 pas dhcpd[2807]: Sending on LPF/ens33/00:0c:29:1e:29:ae/192.168.19.0/24  
Apr 28 12:18:15 pas dhcpd[2807]: Sending on Socket/fallback/fallback-net  
Apr 28 12:18:15 pas dhcpd[2807]: Server starting service.
```

- Tester la réception de ip dans deux clients différents :

```
client1@client1:~$ sudo dhclient -r
[sudo] password for client1:
client1@client1:~$ sudo dhclient -v
Internet Systems Consortium DHCP Client 4.4.3-P1
Copyright 2004-2022 Internet Systems Consortium.
All rights reserved.
For info, please visit https://www.isc.org/software/dhcp/

Listening on LPF/ens33/00:0c:29:8a:be:79
Sending on   LPF/ens33/00:0c:29:8a:be:79
Sending on   Socket/fallback
xid: warning: no netdev with useable HWADDR found for seed's uniqueness enforcement
xid: rand init seed (0x6870678d) built using gethostid
DHCPCDISCOVER on ens33 to 255.255.255.255 port 67 interval 3 (xid=0xf0b4461d)
DHCPOFFER of 192.168.19.50 from 192.168.19.10
DHCPREQUEST for 192.168.19.50 on ens33 to 255.255.255.255 port 67 (xid=0x1d46b4f0)
DHCPACK of 192.168.19.50 from 192.168.19.10 (xid=0xf0b4461d)
Setting LLNMR support level "yes" for "2", but the global support level is "no".
bound to 192.168.19.50 -- renewal in 275 seconds.
client1@client1:~$
```

2.3.1. Configuration DNS

- Affichage des fichiers de configuration de service DNS

```
pas@pas:/etc/bind$ ls
bind.keys      db.empty      named.conf.local  zones.rfc1918
db.0           db.local      named.conf.options
db.127         named.conf    rndc.key
db.255         named.conf.default-zones  zones
pas@pas:/etc/bind$
```

- Fichier de zone direct

```
pas@pas: /etc/bind/zones
GNU nano 7.2 db.xx.cigi.ma
$TTL 86400
@ IN SOA ns1.xx.cigi.ma. admin.xx.cigi.ma. (
    2025032101 ; Serial
    28800      ; Refresh
    7200       ; Retry
    604800     ; Expire
    86400 )    ; Minimum TTL

; Name Servers
@ IN NS ns1.xx.cigi.ma.

; A Records
ns1 IN A 192.168.19.1
pas IN A 192.168.19.1
server-RSH IN A 192.168.19.52
client-linux1 IN A 192.168.19.50

Passerelle-nfs IN A 192.168.19.53
client-linux2 IN A 192.168.19.51
client2 IN A 192.168.19.200

^G Help      ^O Write Out ^W Where Is  ^K Cut       ^T Execute   ^C Location
^X Exit      ^R Read File ^\ Replace   ^U Paste     ^J Justify   ^_ Go To Line
```

- Fichier named.conf

```
// Forward zone
zone "xx.cigi.ma" {
    type master;
    file "/etc/bind/zones/db.xx.cigi.ma";
    // allow-transfer { 192.168.19.131; };
    //allow-query { any; };
};

// Reverse zone
zone "10.168.192.in-addr.arpa" {
    type master;
    file "/etc/bind/zones/db.192.168.10";
    // allow-transfer { 192.168.19.131; };
    //allow-query { any; };
};
```

- Exploration du statut de service DNS

```

pas@pas:~$ sudo systemctl restart bind9
pas@pas:~$ sudo systemctl status bind9
● named.service - BIND Domain Name Server
   Loaded: loaded (/usr/lib/systemd/system/named.service; enabled; preset: enabled)
   Active: active (running) since Mon 2025-04-28 12:38:53 +01; 59s ago
     Docs: man:named(8)
   Main PID: 3069 (named)
    Status: "running"
     Tasks: 8 (limit: 4551)
    Memory: 5.9M (peak: 6.3M)
       CPU: 67ms
    CGroup: /system.slice/named.service
            └─3069 /usr/sbin/named -f -u bind

Apr 28 12:39:06 pas named[3069]: network unreachable resolving './NS/IN': 2001:500:12::d0d#53
Apr 28 12:39:06 pas named[3069]: network unreachable resolving './NS/IN': 2001:dc3::35#53
Apr 28 12:39:07 pas named[3069]: network unreachable resolving './NS/IN': 2001:503:c27::2:30#53
Apr 28 12:39:07 pas named[3069]: network unreachable resolving './NS/IN': 2001:500:2f::f#53
Apr 28 12:39:09 pas named[3069]: network unreachable resolving './NS/IN': 2001:500:9f::42#53
Apr 28 12:39:10 pas named[3069]: network unreachable resolving './NS/IN': 2001:503:ba3e::2:30#53
Apr 28 12:39:11 pas named[3069]: network unreachable resolving './NS/IN': 2001:500:1::53#53
Apr 28 12:39:12 pas named[3069]: network unreachable resolving './NS/IN': 2801:1b8:10::b#53
Apr 28 12:39:12 pas named[3069]: network unreachable resolving './NS/IN': 2001:7fe::53#53
Apr 28 12:39:13 pas named[3069]: resolver priming query complete: timed out
pas@pas:~$

```

- Test de fonctionnement de service DNS

```

client1@client1:~$ nslookup pas.xx.cigi.ma
Server:      127.0.0.53
Address:     127.0.0.53#53

Non-authoritative answer:
Name:   pas.xx.cigi.ma
Address: 192.168.19.1

client1@client1:~$ nslookup client-linux2.xx.cigi.ma
Server:      127.0.0.53
Address:     127.0.0.53#53

Non-authoritative answer:
Name:   client-linux2.xx.cigi.ma
Address: 192.168.19.51

client1@client1:~$

```

2.3.4. Configuration de serveur de sauvegarde Rsnapshot

- Installation du serveur de sauvegarde Rsnapshot

```
brahim@client2: ~  
brahim@client2:~$ sudo apt install rsnapshot  
[sudo] password for brahim:  
Reading package lists... Done  
Building dependency tree... Done  
Reading state information... Done  
rsnapshot is already the newest version (1.4.5-2).  
0 upgraded, 0 newly installed, 0 to remove and 11 not upgraded.  
brahim@client2:~$
```

- Installation d'open-ssh-server

```
brahim@client2: ~  
brahim@client2:~$ sudo apt install openssh-server  
Reading package lists... Done  
Building dependency tree... Done  
Reading state information... Done  
The following additional packages will be installed:  
  ncurses-term openssh-sftp-server ssh-import-id
```

- Le teste de communication avec la machine client

```
brahim@client2:~$ sudo ssh client1@192.168.19.50  
client1@192.168.19.50's password:  
Welcome to Ubuntu 24.04.2 LTS (GNU/Linux 6.11.0-21-generic x86_64)  
  
* Documentation:  https://help.ubuntu.com  
* Management:    https://landscape.canonical.com  
* Support:       https://ubuntu.com/pro  
  
Expanded Security Maintenance for Applications is not enabled.  
  
108 updates can be applied immediately.  
To see these additional updates run: apt list --upgradable  
  
Enable ESM Apps to receive additional future security updates.  
See https://ubuntu.com/esm or run: sudo pro status  
  
The list of available updates is more than a week old.  
To check for new updates run: sudo apt update  
Last login: Sun Apr 27 17:55:50 2025 from 192.168.19.144  
client1@client1:~$
```

- La récupération de fichier « home » de client linux dans notre server :

```
brahim@client2:~/backups$ cd
brahim@client2:~$ sudo rsnapshot alpha
client1@client-linux1.xx.cigi.ma's password:
\brahim@client2:~$ cd backups
brahim@client2:~/backups$ ls
alpha.0
brahim@client2:~/backups$ cd alpha.0/client1/home/client1/backups
brahim@client2:~/backups/alpha.0/client1/home/client1/backups$ ls
brahim.txt
brahim@client2:~/backups/alpha.0/client1/home/client1/backups$ cat brahim.txt
testetetdkjgfeg
brahim@client2:~/backups/alpha.0/client1/home/client1/backups$
```

2.4. Conclusion :

En résumé, le système que nous avons développé offre une solution globale pour la gestion de notre infrastructure réseau. Grâce aux services DNS et DHCP, à un serveur de sauvegarde à l'aide de rsnapshot, nous pouvons assurer une répartition efficace des ressources, une communication sécurisée et une sauvegarde et une récupération fiables des données. Cela nous aidera à maintenir le bon déroulement de l'entreprise, garantissant ainsi la pérennité des activités commerciales.

3. Parc de service de recherche

3.1. Description

Le Service Recherche et Développement est équipé d'une passerelle intégrant les services NIS et NFS, ainsi que de stations de travail sous Linux et Windows. Le domaine DNS attribué à ce service est rd.formation.ma. La passerelle joue un rôle central en fournissant des répertoires personnels aux utilisateurs Linux via NFS et en gérant l'authentification des utilisateurs grâce à NIS.

L'utilisateur principal, "user1", dispose d'une station de travail Windows, depuis laquelle il peut accéder et utiliser les stations de travail Linux. Cela permet à "user1" de bénéficier de l'environnement Linux tout en travaillant sur sa machine Windows. L'accès aux stations de travail Linux depuis le poste Windows est une fonctionnalité clé pour assurer une collaboration fluide et un partage des ressources informatiques au sein du service.

Le stockage des répertoires personnels des utilisateurs Linux sur la passerelle via NFS assure une centralisation des données, facilitant ainsi la gestion et la sauvegarde des informations critiques. De plus, la gestion centralisée des mots de passe via le serveur NIS simplifie l'authentification des utilisateurs, offrant à la fois sécurité et praticité dans la gestion des accès au réseau.

3.2. Architecture de service de recherche

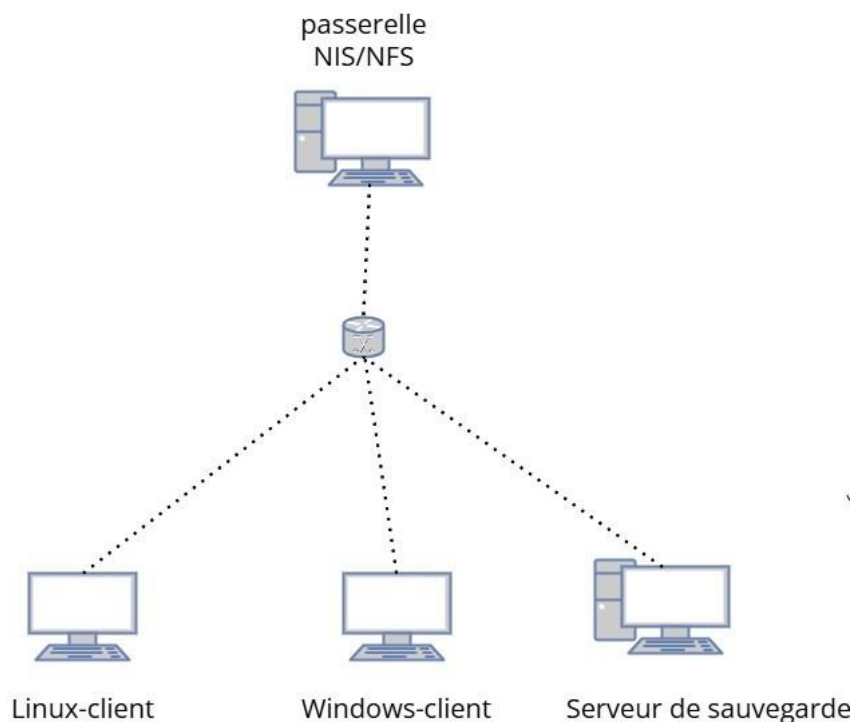


Figure : Architecture de service de développement et de recherche

3.3. Implémentation de passerelle dotée des services NFS

Configuration du Serveur NFS :

- Pour démarrer le service NFS côté serveur il faut installer NFS :

```
serveurnfsnis@serveurnfsnis-VMware-Virtual-Platform: ~  
serveurnfsnis@serveurnfsnis-VMware-Virtual-Platform:~$ sudo apt-get install nfs-kernel-server  
sudo] Mot de passe de serveurnfsnis :  
Lecture des listes de paquets... Fait  
Construction de l'arbre des dépendances... Fait  
Lecture des informations d'état... Fait  
Les paquets supplémentaires suivants seront installés :  
  keyutils libevent-core-2.1-7t64 nfs-common rpcbind  
Paquets suggérés :  
  open-iscsi watchdog  
Les NOUVEAUX paquets suivants seront installés :  
  keyutils libevent-core-2.1-7t64 nfs-common nfs-kernel-server rpcbind  
3 mis à jour, 5 nouvellement installés, 0 à enlever et 100 non mis à jour.  
Il est nécessaire de prendre 612 ko dans les archives.  
Après cette opération, 2 103 ko d'espace disque supplémentaires seront utilisés.  
Souhaitez-vous continuer ? [O/n] o  
Réception de :1 http://ma.archive.ubuntu.com/ubuntu noble/main amd64 libevent-core-2.1-7t64 amd64 2.1.12-stable-9ubuntu2 [91,3 kB]  
Réception de :2 http://ma.archive.ubuntu.com/ubuntu noble/main amd64 rpcbind amd64 1.2.6-7ubuntu2 [46,5 kB]  
Réception de :3 http://ma.archive.ubuntu.com/ubuntu noble/main amd64 keyutils amd64 1.6.3-3build1 [56,8 kB]  
Réception de :4 http://ma.archive.ubuntu.com/ubuntu noble-updates/main amd64 nfs-common amd64 1:2.6.4-3ubuntu5.1 [248 kB]  
Réception de :5 http://ma.archive.ubuntu.com/ubuntu noble-updates/main amd64 nfs-kernel-server amd64 1:2.6.4-3ubuntu5.1 [169 kB]  
12 ko réceptionnés en 8s (77,4 ko/s)  
Sélection du paquet libevent-core-2.1-7t64:amd64 précédemment désélectionné.  
Lecture de la base de données... 149670 fichiers et répertoires déjà installés.)  
Préparation du dépaquetage de .../libevent-core-2.1-7t64_2.1.12-stable-9ubuntu2_amd64.deb ...  
Dépaquetage de libevent-core-2.1-7t64:amd64 (2.1.12-stable-9ubuntu2) ...  
Sélection du paquet rpcbind précédemment désélectionné.  
Préparation du dépaquetage de .../rpcbind_1.2.6-7ubuntu2_amd64.deb ...  
Dépaquetage de rpcbind (1.2.6-7ubuntu2) ...  
Sélection du paquet keyutils précédemment désélectionné.
```

- Lorsqu'un répertoire sur le serveur est accessible à distance par un client, on dit qu'il est exporté. En tant qu'administrateur, il faut créer les répertoires suivants

```
serveurnfsnis@serveurnfsnis-VMware-Virtual-Platform:~/Bureau$ ls  
partage  
serveurnfsnis@serveurnfsnis-VMware-Virtual-Platform:~/Bureau$ cd Partage  
serveurnfsnis@serveurnfsnis-VMware-Virtual-Platform:~/Bureau/Partage$ pwd  
/home/serveurnfsnis/Bureau/Partage  
serveurnfsnis@serveurnfsnis-VMware-Virtual-Platform:~/Bureau/Partage$ sudo chmod 755 /home/serveurnfsnis/Bureau/Partage
```

- Le fichier /etc/exports sur le serveur contient la liste des répertoires exportés, avec un répertoire par ligne. Pour exporter le répertoire de partage avec les options demandées, il faut ajouter les lignes suivantes au fichier /etc/exports :

```
serveurnfsnis@serveurnfsnis-VMware-Virtual-Platform: ~/Bureau/Partage  
GNU nano 7.2 /etc/exports  
#  
# /etc/exports: the access control list for filesystems which may be exported  
# to NFS clients. See exports(5).  
#  
# Example for NFSv2 and NFSv3:  
# /srv/homes hostname1(rw,sync,no_subtree_check) hostname2(ro,sync,no_subtree_check)  
#  
# Example for NFSv4:  
# /srv/nfs4 gss/krb5i(rw,sync,fsid=0,crossmnt,no_subtree_check)  
# /srv/nfs4/homes gss/krb5i(rw,sync,no_subtree_check)  
#  
/home/serveurnfsnis/Bureau/Partage 192.168.229.0/24(rw,sync,no_subtree_check)
```

Dans cet exemple, "192.168.229.0/24" signifie que toutes les machines du réseau du service de recherche sont autorisées à accéder au répertoire de partage en lecture et écriture (option "rw"). L'option "sync" garantit que les écritures sur disque sont synchronisées, assurant ainsi l'intégrité des données. L'option "no_subtree_check" désactive la vérification des sous-répertoires pour améliorer les performances.

- Après avoir modifié le fichier `/etc/exports`, il est nécessaire d'exécuter la commande `"exportfs -ra"` pour que les modifications soient prises en compte :

```
serveurnfsnis@serveurnfsnis-VMware-Virtual-Platform:~/Bureau/Partage$ sudo nano /etc/exports
serveurnfsnis@serveurnfsnis-VMware-Virtual-Platform:~/Bureau/Partage$ sudo nano /etc/exports
serveurnfsnis@serveurnfsnis-VMware-Virtual-Platform:~/Bureau/Partage$ sudo exportfs -ra
serveurnfsnis@serveurnfsnis-VMware-Virtual-Platform:~/Bureau/Partage$ sudo systemctl start nfs-server
serveurnfsnis@serveurnfsnis-VMware-Virtual-Platform:~/Bureau/Partage$ sudo systemctl enable nfs-server
serveurnfsnis@serveurnfsnis-VMware-Virtual-Platform:~/Bureau/Partage$
```

- Création des fichiers pour le test :

```
serveurnfsnis@serveurnfsnis-VMware-Virtual-Platform:~/Bureau/Partage$ sudo nano /etc/exports
serveurnfsnis@serveurnfsnis-VMware-Virtual-Platform:~/Bureau/Partage$ pwd
/home/serveurnfsnis/Bureau/Partage
serveurnfsnis@serveurnfsnis-VMware-Virtual-Platform:~/Bureau/Partage$ nano test.txt
serveurnfsnis@serveurnfsnis-VMware-Virtual-Platform:~/Bureau/Partage$ sudo exportfs -ra
```

- Démarrer et activer le service NFS :

```
serveurnfsnis@serveurnfsnis-VMware-Virtual-Platform:~/Bureau/Partage$ sudo nano /etc/exports
serveurnfsnis@serveurnfsnis-VMware-Virtual-Platform:~/Bureau/Partage$ sudo nano /etc/exports
serveurnfsnis@serveurnfsnis-VMware-Virtual-Platform:~/Bureau/Partage$ sudo exportfs -ra
serveurnfsnis@serveurnfsnis-VMware-Virtual-Platform:~/Bureau/Partage$ sudo systemctl start nfs-server
serveurnfsnis@serveurnfsnis-VMware-Virtual-Platform:~/Bureau/Partage$ sudo systemctl enable nfs-server
serveurnfsnis@serveurnfsnis-VMware-Virtual-Platform:~/Bureau/Partage$
```

Configuration du client NFS :

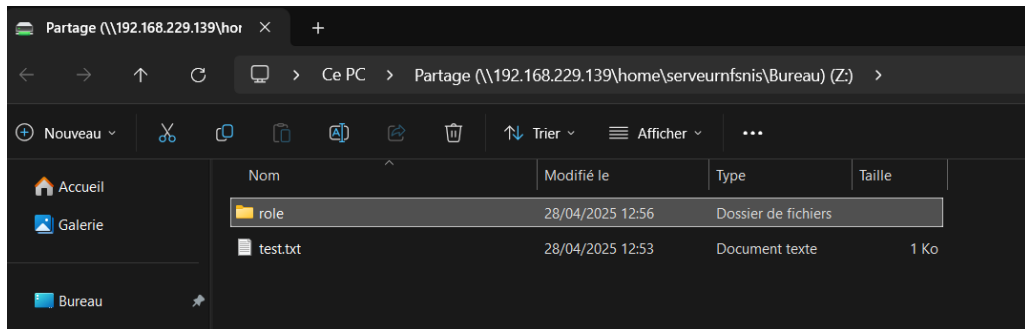
— Installation du client NFS :

```
clientnfs@clientnfs:~$ sudo apt install nfs-common
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
nfs-common est déjà la version la plus récente (1:2.6.4-3ubuntu5.1).
0 mis à jour, 0 nouvellement installés, 0 à enlever et 123 non mis à jour.
clientnfs@clientnfs:~$
```

— Création du dossier de montage de faire le montage et Vérification du fichiers partagé sous le client linux :

```
clientnfs@clientnfs: ~/Bureau/Recu
clientnfs@clientnfs:~/Bureau/Recu$ sudo mount 192.168.229.139:/home/serveurnfsnis/Bureau/Partage /home/clientnfs/Bureau/Recu
clientnfs@clientnfs:~/Bureau/Recu$ ls
test.txt
clientnfs@clientnfs:~/Bureau/Recu$
```

— Vérification et Montage du fichiers partagé sous le client Windows :



3.4 Configuration du serveur NIS

— Installation du NIS :

```
serveurnfsnis@serveurnfsnis-VMware-Virtual-Platform:~$ sudo apt update
[sudo] Mot de passe de serveurnfsnis :
Atteint :1 http://security.ubuntu.com/ubuntu noble-security InRelease
Atteint :2 http://ma.archive.ubuntu.com/ubuntu noble InRelease
Atteint :3 http://ma.archive.ubuntu.com/ubuntu noble-updates InRelease
Atteint :4 http://ma.archive.ubuntu.com/ubuntu noble-backports InRelease
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
100 paquets peuvent être mis à jour. Exécutez « apt list --upgradable » pour les voir.
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
Les paquets supplémentaires suivants seront installés :
  libnsl2 libnss-nis make nscd yp-tools ypbind-mt ypserv
Paquets suggérés :
  make-doc krb5-kdc
Les NOUVEAUX paquets suivants seront installés :
  libnsl2 libnss-nis make nscd yp-tools ypbind-mt ypserv
0 mis à jour, 8 nouvellement installés, 0 à enlever et 100 non mis à jour.
Il est nécessaire de prendre 529 ko dans les archives.
```

La modification du variable NISSERVER sur le fichier /etc/default/nis :

```
server2@server2: ~/Desktop
GNU nano 6.2 /etc/default/nis
# Are we a NIS server and if so what kind (values: false, slave, master)?
NISSERVER=master

NISDOMAIN=rd.forntaion.ma

# Are we a NIS client?

# Location of the master NIS password file (for yppasswdd).
# If you change this make sure it matches with /var/yp/Makefile.
YPPWDDIR=/etc

# Do we allow the user to use ypchsh and/or ypchfn ? The YPCHANGEOK
# fields are passed with -e to yppasswdd, see it's manpage.
# Possible values: "chsh", "chfn", "chsh,chfn"
YPCHANGEOK=chsh

# NIS master server. If this is configured on a slave server then ypinit
# will be run each time NIS is started.
NISMMASTER=master

^G Help      ^O Write Out ^W Where Is  ^K Cut       ^T Execute  ^C Location
^X Exit      ^R Read File ^L Replace  ^U Paste    ^J Justify  ^_ Go To Line
```

L'ajout de configurations au d'autres fichiers :

```
serveurnfsnis@serveurnfsnis-VMware-Virtual-Platform:~$ sudo nano /etc/defaultdomain
serveurnfsnis@serveurnfsnis-VMware-Virtual-Platform:~$ sudo domainname rd.formation.ma
serveurnfsnis@serveurnfsnis-VMware-Virtual-Platform:~$ sudo nano /etc/default/nis
serveurnfsnis@serveurnfsnis-VMware-Virtual-Platform:~$ sudo nano /etc/ypserv.securenets
serveurnfsnis@serveurnfsnis-VMware-Virtual-Platform:~$ sudo /usr/lib/yp/ypinit -m
La commande « udo » n'a pas été trouvée, mais peut être installée avec :
sudo apt install udo
serveurnfsnis@serveurnfsnis-VMware-Virtual-Platform:~$ sudo /usr/lib/yp/ypinit -m

At this point, we have to construct a list of the hosts which will run NIS
servers.  serveurnfsnis-VMware-Virtual-Platform is in the list of NIS server hosts.  Please continue to add
the names for the other hosts, one per line.  When you are done with the
list, type a <control D>.
    next host to add:  serveurnfsnis-VMware-Virtual-Platform
    next host to add:
The current list of NIS servers looks like this:

serveurnfsnis-VMware-Virtual-Platform

Is this correct? [y/n: y] y
We need a few minutes to build the databases...
Building /var/yp/rd.formation.ma/ypservers...
Running /var/yp/Makefile...
gmake[1] : on entre dans le répertoire « /var/yp/rd.formation.ma »
Updating passwd.byname...
failed to send 'clear' to local ypserv: RPC: Program not registeredUpdating passwd.byuid...
failed to send 'clear' to local ypserv: RPC: Program not registeredUpdating group.byname...
failed to send 'clear' to local ypserv: RPC: Program not registeredUpdating group.bygid...
```

L'ajout d'un utilisateur test et mise à jour le NIS :

```
serveurnfsnis@serveurnfsnis-VMware-Virtual-Platform:~$ sudo adduser usertest
info: Ajout de l'utilisateur « usertest » ...
info: Choix d'un UID/GID dans la plage 1000 à 59999 ...
info: Ajout du nouveau groupe « usertest » (1001) ...
info: Ajout du nouvel utilisateur « usertest » (1001) avec le groupe « usertest » (1001) ...
info: Création du répertoire personnel « /home/usertest » ...
info: Copie des fichiers depuis « /etc/skel » ...
Nouveau mot de passe :
MOT DE PASSE INCORRECT : Le mot de passe comporte moins de 8 caractères
Retapez le nouveau mot de passe :
passwd : mot de passe mis à jour avec succès
Modifier les informations associées à un utilisateur pour usertest
Entrer la nouvelle valeur, ou appuyer sur ENTER pour la valeur par défaut
    NOM []:
    Numéro de chambre []:
    Téléphone professionnel []:
    Téléphone personnel []:
    Autre []:
Ces informations sont-elles correctes ? [0/n] o
info: Ajout du nouvel utilisateur « usertest » aux groupes supplémentaires « users » ...
info: Ajout de l'utilisateur « usertest » au groupe « users » ...
serveurnfsnis@serveurnfsnis-VMware-Virtual-Platform:~$ cd /var/yp
serveurnfsnis@serveurnfsnis-VMware-Virtual-Platform:/var/yp$ sudo make
gmake[1] : on entre dans le répertoire « /var/yp/rd.formation.ma »
Updating passwd.byname...
Updating passwd.byuid...
Updating group.byname...
Updating group.bygid...
Updating netid.byname...
Updating shadow.byname...
gmake[1] : on quitte le répertoire « /var/yp/rd.formation.ma »
serveurnfsnis@serveurnfsnis-VMware-Virtual-Platform:/var/yp$
```

Liste des utilisateurs NIS :

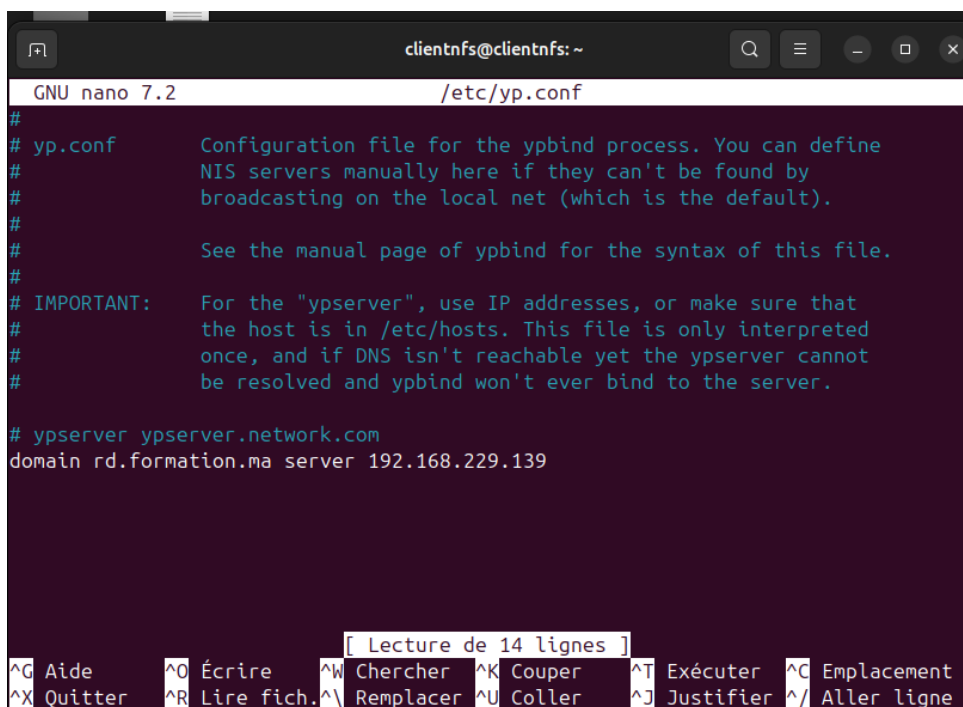
```
serveurnfsnis@serveurnfsnis-VMware-Virtual-Platform:/home$ ypcat passwd
serveurnfsnis:x:1000:1000:SERVEURNfsnis:/home/serveurnfsnis:/bin/bash
usertest:x:1001:1001:,,,:/home/usertest:/bin/bash
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
serveurnfsnis@serveurnfsnis-VMware-Virtual-Platform:/home$
```

8.2.1 Configuration du client NIS

— Installation du NIS :

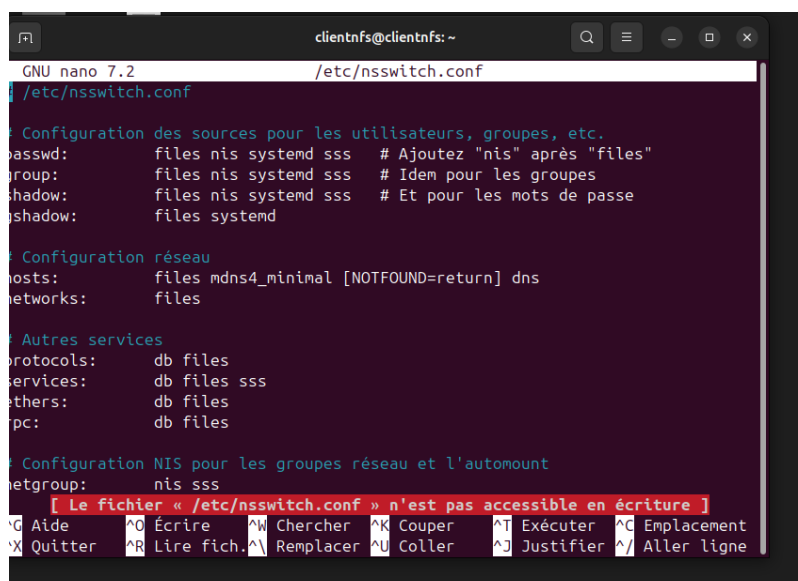
```
clientnfs@clientnfs:~$ sudo apt install nis -y
[sudo] Mot de passe de clientnfs :
Désolé, essayez de nouveau.
[sudo] Mot de passe de clientnfs :
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
nis est déjà la version la plus récente (4.5).
0 mis à jour, 0 nouvellement installés, 0 à enlever et 123 non mis à jour.
clientnfs@clientnfs:~$
```

L'ajout de [nom de domaine] [serveur] [nom d'hôte du serveur NIS] sur le fichier /etc/yp.conf et des modifications sur le fichier /etc/nsswitch.conf :



```
clientnfs@clientnfs: ~
GNU nano 7.2 /etc/yp.conf
#
# yp.conf      Configuration file for the ypbind process. You can define
#              NIS servers manually here if they can't be found by
#              broadcasting on the local net (which is the default).
#
#              See the manual page of ypbind for the syntax of this file.
#
# IMPORTANT:   For the "ypserver", use IP addresses, or make sure that
#              the host is in /etc/hosts. This file is only interpreted
#              once, and if DNS isn't reachable yet the ypserver cannot
#              be resolved and ypbind won't ever bind to the server.
#
# ypserver ypserver.network.com
domain rd.formation.ma server 192.168.229.139

[ Lecture de 14 lignes ]
^G Aide      ^O Écrire   ^W Chercher ^K Couper   ^T Exécuter ^C Emplacement
^X Quitter   ^R Lire fich.^_ Remplacer ^U Coller   ^J Justifier ^/ Aller ligne
```



```
clientnfs@clientnfs: ~
GNU nano 7.2 /etc/nsswitch.conf
/etc/nsswitch.conf
# Configuration des sources pour les utilisateurs, groupes, etc.
passwd:      files nis systemd sss # Ajoutez "nis" après "files"
group:       files nis systemd sss # Idem pour les groupes
shadow:      files nis systemd sss # Et pour les mots de passe
gshadow:     files systemd

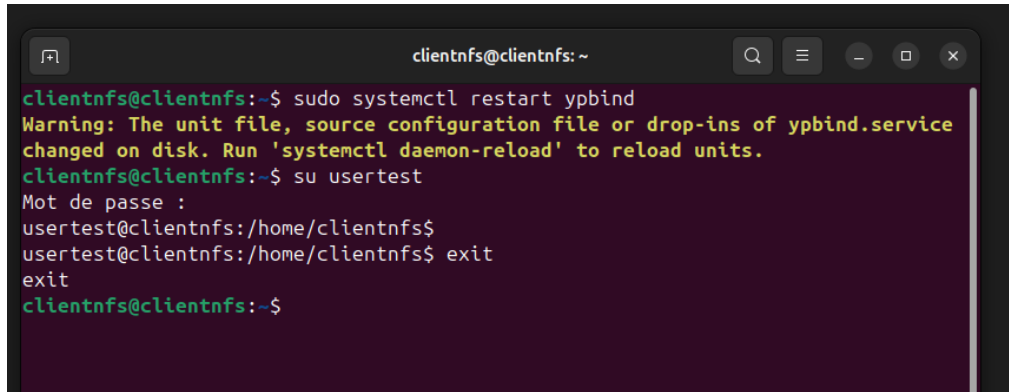
# Configuration réseau
hosts:       files mdns4_minimal [NOTFOUND=return] dns
networks:    files

# Autres services
protocols:   db files
services:    db files sss
ethers:      db files
rpc:         db files

# Configuration NIS pour les groupes réseau et l'automount
netgroup:    nis sss

[ Le fichier « /etc/nsswitch.conf » n'est pas accessible en écriture ]
^G Aide      ^O Écrire   ^W Chercher ^K Couper   ^T Exécuter ^C Emplacement
^X Quitter   ^R Lire fich.^_ Remplacer ^U Coller   ^J Justifier ^/ Aller ligne
```

Redémarrage le service et tester l'utilisateur :

A terminal window titled 'clientnfs@clientnfs: ~' with standard window controls. The terminal shows the following commands and output:

```
clientnfs@clientnfs:~$ sudo systemctl restart ybind
Warning: The unit file, source configuration file or drop-ins of ybind.service
changed on disk. Run 'systemctl daemon-reload' to reload units.
clientnfs@clientnfs:~$ su usertest
Mot de passe :
usertest@clientnfs:/home/clientnfs$
usertest@clientnfs:/home/clientnfs$ exit
exit
clientnfs@clientnfs:~$
```

Pour être sûr que notre serveur NIS fonctionne correctement, on peut vérifier si les clients Linux peuvent s'authentifier. Si le serveur NIS est actif, les utilisateurs devraient pouvoir se connecter sans problème. Cela nous indique que la vérification des mots de passe se fait bien au niveau du serveur, ce qui est une bonne indication que notre NIS est bien configuré et fonctionne comme prévu.

Chapitre 2: Sécurité des Réseaux

1. Introduction

Dans ce chapitre on va entamer la description l'installation et logiciel « Security Onion »

2. Description

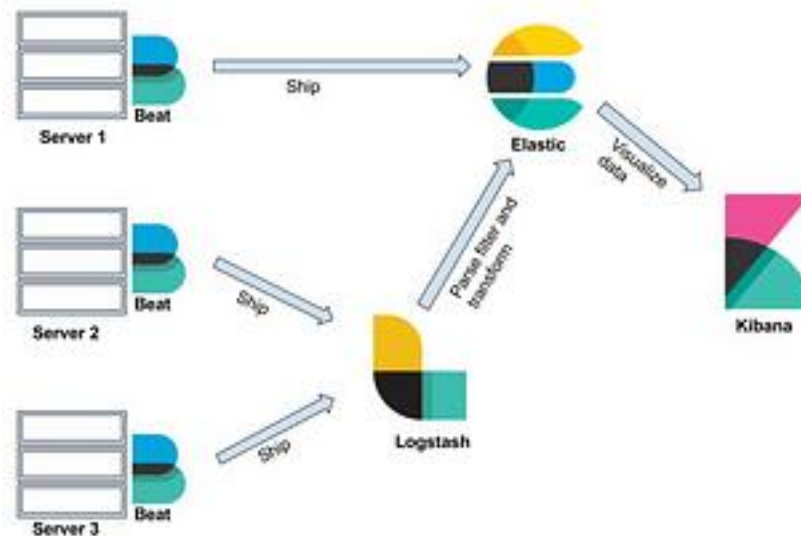
La sécurité des réseaux comprend toutes les mesures prises pour garantir la fonctionnalité et l'intégrité de réseau ainsi que des données. Les technologies matérielles et logicielles qui la composent visent de nombreuses menaces, en les empêchant de pénétrer dans le réseau ou de s'y propager. Il est également possible de gérer l'accès au réseau grâce à des mesures de sécurité efficaces.

3. Security Onion

3.1. Définition

Security Onion est une plateforme gratuite et open-source dédiée à la chasse aux menaces, à la surveillance de la sécurité des entreprises et à la gestion des journaux. Elle intègre ses propres interfaces pour l'alerte, les tableaux de bord, la chasse aux menaces, l'analyse des paquets capturés (PCAP) et la gestion des cas. Elle inclut également d'autres outils tels que Playbook, osquery, CyberChef, Elasticsearch, Logstash, Kibana, Suricata et Zeek.

3.2. Les principaux outils intégrés dans Security Onion :



3.3. Implémentation :

1. Préparation à l'installation

Avant de procéder à l'installation de Security Onion, certaines étapes préparatoires étaient nécessaires pour garantir l'authenticité et l'intégrité de l'image ISO.

a) Télécharger et importer la clé de signature

Pour vérifier les fichiers téléchargés, nous avons récupéré la clé publique officielle de Security Onion :

Commande utilisée : `gpg --keyserver keyserver.ubuntu.com --recv-keys <ID-de-la-clé>`

b) Télécharger le fichier de signature de l'ISO

Nous avons téléchargé le fichier .sig correspondant à l'image ISO depuis le site officiel.

c) Télécharger l'image ISO

Nous avons téléchargé l'image ISO de Security Onion depuis le site officiel.

d) Vérifier l'image ISO téléchargée

Commande utilisée : `gpg --verify securityonion.iso.sig securityonion.iso`

Cette vérification assure que l'ISO n'a pas été modifiée.

2. Tentative d'installation de Security Onion Full

Après la vérification, nous avons tenté l'installation sur une machine virtuelle via VirtualBox.

Configuration : 8 Go RAM, 50 Go disque, 2 CPU, mode réseau Bridged.

Cependant, un problème est survenu : **espace disque insuffisant**.

3. Solution adoptée : Installation de Security Onion Desktop

a) Changement de stratégie

Nous avons opté pour Security Onion Desktop, version plus légère adaptée aux ressources disponibles.

b) Reconfiguration de la machine virtuelle

Nouvelle configuration : 6 Go RAM, 120 Go disque, 2 CPU.

c) Installation de Security Onion Desktop

Installation en mode "Evaluation Setup" avec sélection de composants : Zeek, Suricata, Wazuh, Kibana.

d) Vérification post-installation

Commande utilisée pour vérifier les services : `sudo so-status`.

Accès à l'interface web de Security Onion vérifié.

4. Résumé des difficultés rencontrées

- Problème d'espace disque important (>200 Go pour installation complète).
- Consommation élevée de ressources (RAM et CPU).

En résumé, le projet d'administration réseau a offert la possibilité de mettre en œuvre les divers services lors de l'étude et de la pratique dans les ateliers tels que NFS et DNS. L'objectif du projet était de créer un réseau informatique comprenant des machines virtuelles LINUX, un routeur, des services DNS internes et externes, du DHCP et un serveur de sauvegarde. Un second parc de recherche et développement a également été créé, avec des serveurs NFS. De plus, le projet incluait la mise en place de mesures de sécurité en utilisant un logiciel de sécurité appelé "Security Onion" afin de garantir la sécurité et la protection du réseau. Cela assurait la protection du réseau contre les éventuels dangers tels que les logiciels malveillants et les virus.