Situation 1 sur le projet d'infrastructure réseau Beròi Bòrda secteur Nay

Raphaël Bousquet—Cadena ; SIO2

Sommaire

1. Contexte

L'entreprise **Beròi Bòrda** est une PME spécialisée dans le secteur de la recherche et du développement. Afin de soutenir sa croissance et de moderniser son infrastructure, elle a mis en place un réseau structuré permettant une gestion efficace des services et une communication optimale entre ses différents sites. L'entreprise est répartie sur **deux sites principaux** : **NAY**, qui regroupe l'administration et les services techniques, et **PAU**, dédié à la gestion des utilisateurs et à la messagerie. Une **zone DMZ** est également intégrée pour héberger des services accessibles depuis Internet, tout en garantissant la sécurité du réseau interne.

Le site de **NAY** centralise les services critiques de l'entreprise. Il héberge un **serveur web intranet** pour l'accès aux ressources internes, un **serveur de supervision** pour le suivi du réseau, un **serveur de fichiers** permettant le stockage et le partage des documents, ainsi qu'un **serveur DNS** assurant la résolution des noms de domaine. Un **PC Client Windows** est aussi utilisé pour l'administration et les tests des services. Ce site est relié à Internet via un **routeur principal**, facilitant l'interconnexion avec les autres sites et les ressources externes.

Le site de **PAU** est conçu pour gérer les accès et la communication interne. Un **contrôleur de domaine Active Directory (AD Windows)** permet l'authentification centralisée des employés et la gestion des autorisations sur le réseau. Un **serveur de messagerie** assure la gestion des emails professionnels. Un **PC Admin** est utilisé pour la maintenance du réseau, tandis qu'un **PC Client** est mis à disposition des employés pour accéder aux services internes. Un **routeur dédié** assure une connexion sécurisée entre ce site et le siège, tout en maintenant une séparation des services.

Une **zone DMZ** sécurisée est déployée pour les services accessibles depuis Internet. Un **serveur WordPress maître** héberge le site web de l'entreprise, avec un **serveur WordPress esclave** garantissant la redondance et la disponibilité du service. Une **IP virtuelle** répartit la charge entre les serveurs pour améliorer la performance. Un **routeur dédié** filtre les connexions pour protéger le réseau interne. Cette architecture assure à **Beròi Bòrda** un réseau sécurisé, performant et évolutif, capable de répondre aux exigences de son activité.

2. Description de la situation 1

BTS SERVICES INFORMATIQUES AUX ORGANISATIONS **SESSION 2024**

ANNEXE 9-1-A : Fiche descriptive de réalisation professionnelle

Épreuve E5 - Administration des systèmes et des réseaux (option SISR)

DESCRIPTION D'UNE RÉALISATION PROFESSIONNELLE	**N° réalisation :**
Nom, prénom : Bousquet—Cadena Raphaël	**N° candidat :**
Épreuve ponctuelle ☒ **Contrôle en cours de formation** ☐	**Date :** ..... / ..... /.....
Organisation support de la réalisation professionnelle Lycée Saint-John Perse	
Intitulé de la réalisation professionnelle Beròi Bòrda secteur Nay	
Période de réalisation : ..... **Lieu :** ..... **Modalité :** ☐ **Seul(e)** ☒ **En équipe**	
Compétences travaillées ☒ Concevoir une solution d'infrastructure réseau ☒ Installer, tester et déployer une solution d'infrastructure réseau ☒ Exploiter, dépanner et superviser une solution d'infrastructure réseau	
Conditions de réalisation[1] (ressources fournies, résultats attendus) Salle 23 avec les machines virtuelles sur VirtualBox.	
Description des ressources documentaires, matérielles et logicielles utilisées[2] Le projet Beròi Bòrda secteur Nay comporte un schéma réseau et un plan d'adressage.	
Modalités d'accès aux productions[3] et à leur documentation[4]	

[1] En référence aux *conditions de réalisation et ressources nécessaires* du bloc « Administration des systèmes et des réseaux » prévues dans le référentiel de certification du BTS SIO.

[2] Les réalisations professionnelles sont élaborées dans un environnement technologique conforme à l'annexe II.E du référentiel du BTS SIO.

[3] Conformément au référentiel du BTS SIO « *Dans tous les cas, les candidats doivent se munir des outils et ressources techniques nécessaires au déroulement de l'épreuve. Ils sont seuls responsables de la disponibilité et de la mise en œuvre de ces outils et ressources. La circulaire nationale d'organisation précise les conditions matérielles de déroulement des interrogations et les pénalités à appliquer aux candidats qui ne se seraient pas munis des éléments nécessaires au déroulement de l'épreuve.* ». Les éléments nécessaires peuvent être un identifiant, un mot de passe, une adresse réticulaire (URL) d'un espace de stockage et de la présentation de l'organisation du stockage.

[4] Lien vers la documentation complète, précisant et décrivant, si cela n'a été fait au verso de la fiche, la réalisation, par exemples schéma complet de réseau mis en place et configurations des services.

3. Schéma Réseau

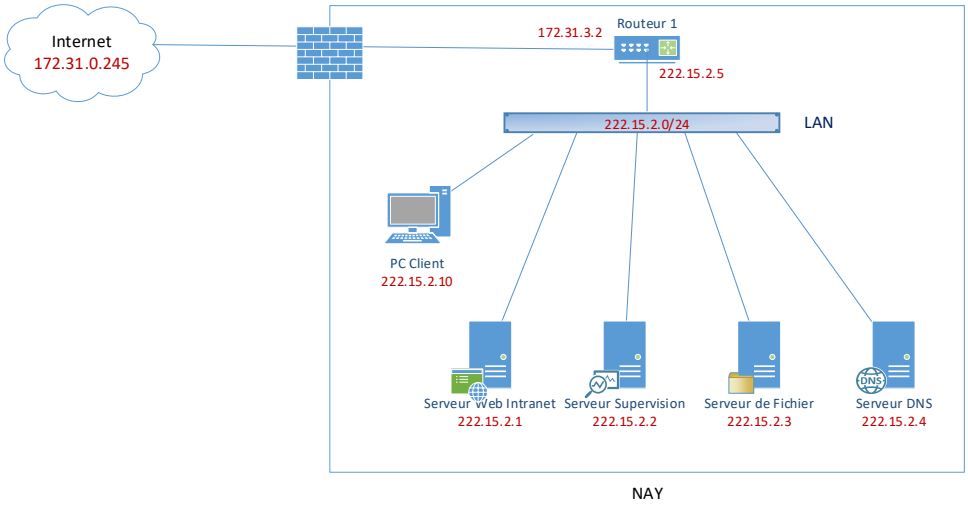


Schéma Réseau de Beròi Bòrda
Secteur Nay
Raphaël Bousquet—Cadena
SIO2
12/12/2024
V4.1

4. Plan d'adressage

Réseaux	Rôles	Outils	Machines
WAN - 172.31.0.0/21	Connexion Internet		Internet
	Routage	Règles NAT SSH : port 22 (nas_ba) ; port 2222 (web_intra_ba) ; port 2224 (dns_ba)	Routeur
LAN NAY - 222.15.2.0/24	Routage	Règles NAT SSH : port 22 (nas_ba) ; port 2222 (web_intra_ba) ; port 2224 (dns_ba)	Routeur
	Client	Windows 11	PC Client
	Serveur Web	Nginx	Serveur Web Intranet
	Supervision	PRTG	Serveur Supervision
	Stockage	NextCloud + Base de Données	Serveur de Fichier
	DNS	nas.beroiborda.fr + intranet.beroiborda.fr	Serveur DNS

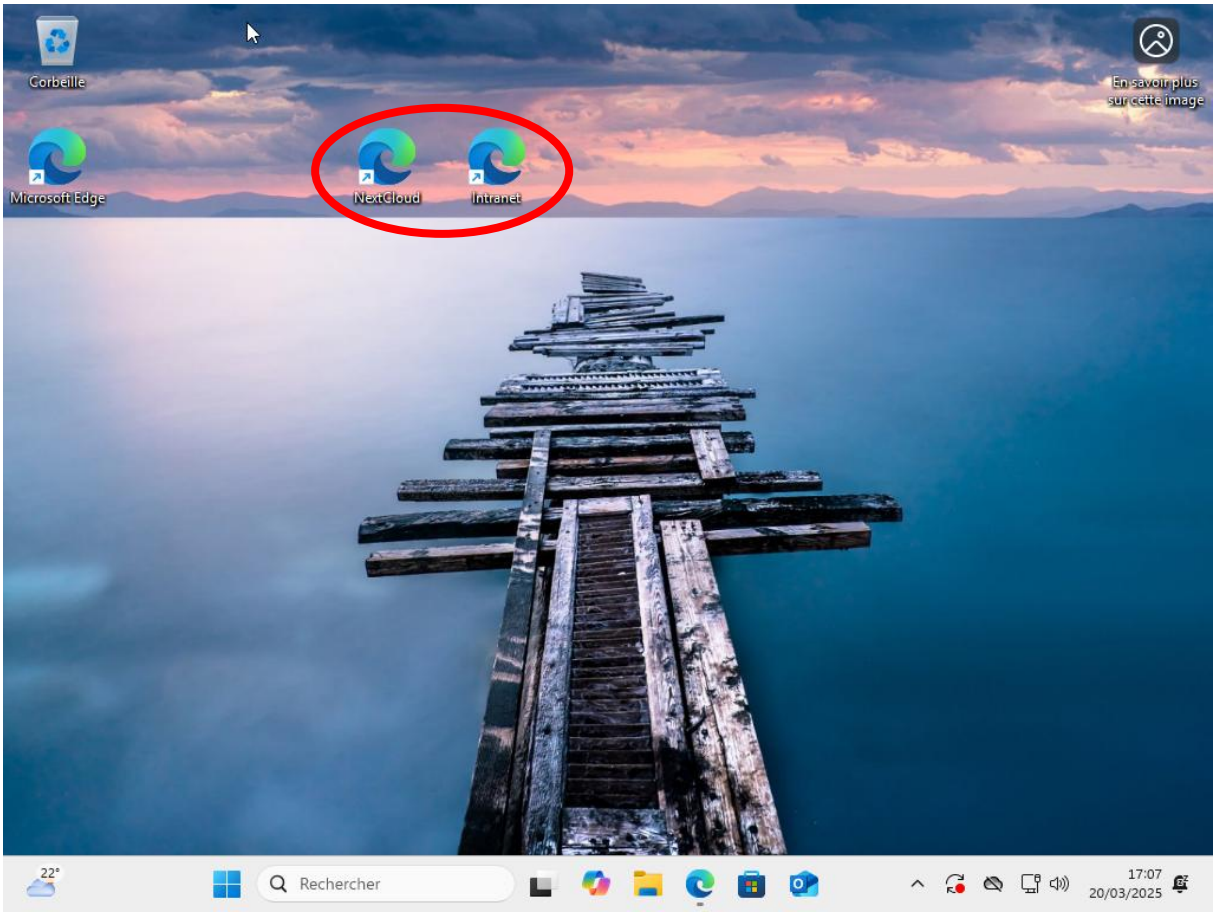
Noms	Adresses IP	Masques de sous-réseau	Passerelles	DNS
Internet	172.31.0.245	255.255.248.0		
Routeur 1	172.31.3.2	255.255.248.0	172.31.0.245	
Routeur 1	222.15.2.5	255.255.255.0		
client_ba2	222.15.2.10	255.255.255.0	222.15.2.5	222.15.2.4
web_intra_ba	222.15.2.1	255.255.255.0	222.15.2.5	222.15.2.4
prtg_ba	222.15.2.2	255.255.255.0	222.15.2.5	
nas_ba	222.15.2.3	255.255.255.0	222.15.2.5	222.15.2.4
dns_ba	222.15.2.4	255.255.255.0	222.15.2.5	

5. Fonctionnalités

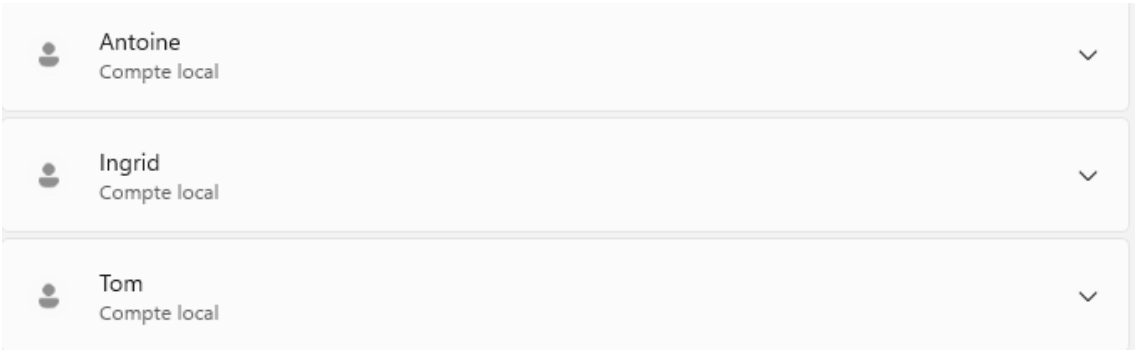
a. Machine Client

La machine client permet d'accéder à l'intranet et le serveur de fichier de l'infrastructure.

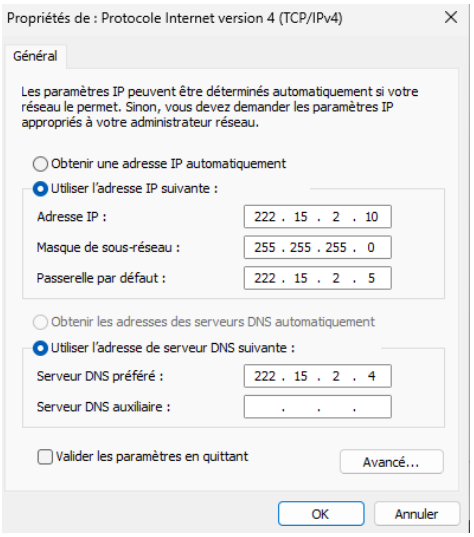
Les URL sont respectivement *http://intranet.beroiborda.fr* et *http://nas.beroiborda.fr*.



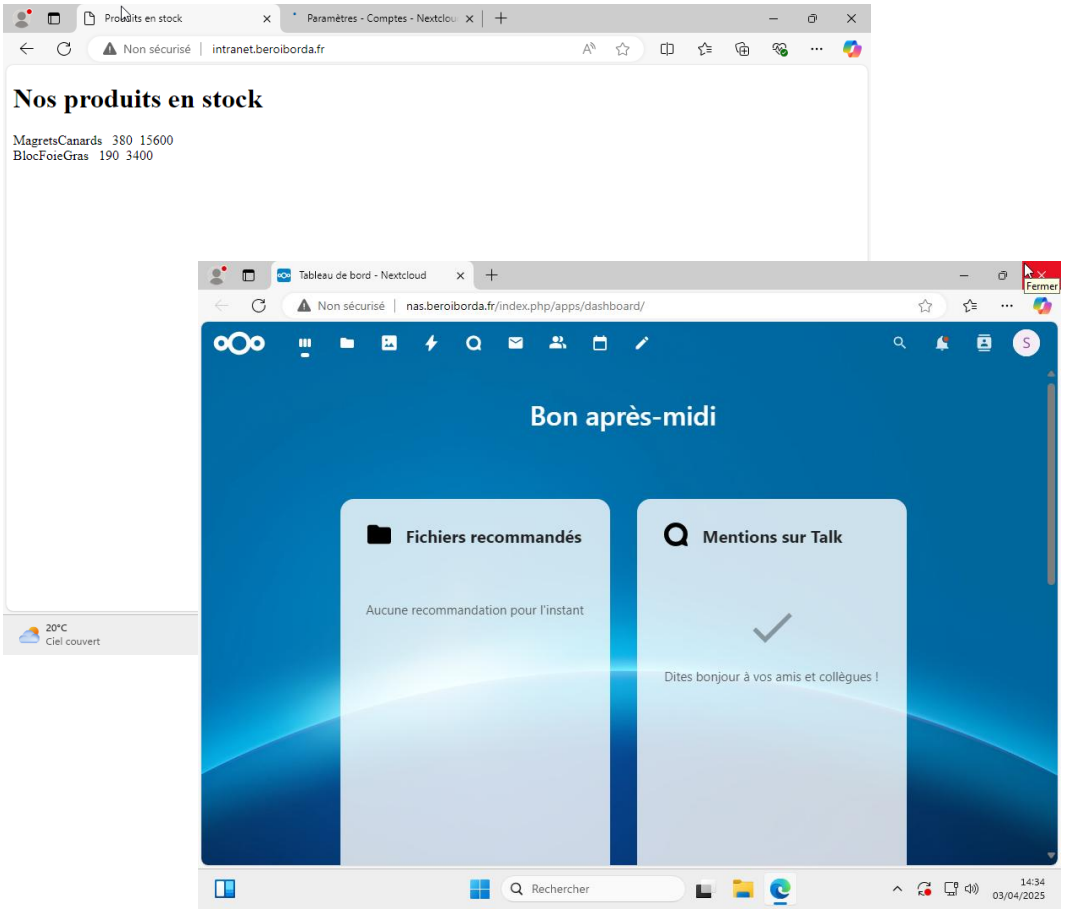
Les utilisateurs sont Antoine, Ingrid et Tom.



Voici les paramètre IP de la machine client :



Le DNS préféré est le serveur DNS du réseau afin que l'on puisse accéder au nas et à l'intranet :



b. Service Web

Le serveur web, dans mon infrastructure, est un intranet, accessible depuis la machine Cliente.

Elle comporte une base de Données pour les stocks de production.

Nous utilisons Nginx pour le service Web et MariaDB pour la Base de Données.

Voici la configuration du */etc/nginx/sites-available/default* :

```
 GNU nano 7.2                                                 default
        #
        # Read up on ssl_ciphers to ensure a secure configuration.
        # See: https://bugs.debian.org/765782
        #
        # Self signed certs generated by the ssl-cert package
        # Don't use them in a production server!
        #
        # include snippets/snakeoil.conf;

        root /var/www/html;

        # Add index.php to the list if you are using PHP
        index index.php index.html index.htm index.nginx-debian.html;

        server_name _;

        location / {
                # First attempt to serve request as file, then
                # as directory, then fall back to displaying a 404.
                try_files $uri $uri/ =404;
        }

        # pass PHP scripts to FastCGI server
        #
        location ~ \.php$ {
                include snippets/fastcgi-php.conf;
        #
        #       # With php-fpm (or other unix sockets):
                fastcgi_pass unix:/run/php/php8.2-fpm.sock;
        #       # With php-cgi (or other tcp sockets):
        #       fastcgi_pass 127.0.0.1:9000;
        }

        # deny access to .htaccess files, if Apache's document root
        # concurs with nginx's one
        #
        #location ~ /\.ht {
        #       deny all;
        #}
}


# Virtual Host configuration for example.com
#
# You can move that to a different file under sites-available/ and symlink that
# to sites-enabled/ to enable it.

^G Aide         ^O Écrire       ^W Chercher     ^K Couper       ^T Exécuter     ^C Emplacement  M-U Annuler     M-A Marquer     M-] -> Crochet  M-Q Précédent
^X Quitter      ^R Lire fich.   ^\ Remplacer    ^U Coller       ^J Justifier    ^_ Aller ligne  M-E Refaire     M-6 Copier      ^Q Retrouver    M-W Suivant
```

La page */var/www/htm/index.php* pour montrer le contenu de la base de données :

```
 GNU nano 7.2                                          /var/www/html/index.php
<!DOCTYPE html>
<html>
<head>
    <title>Produits en stock</title>
</head>
<body>
<h1>Nos produits en stock</h1>
<?php
try {
    // Connexion à la base de données
    $laconnexion = new PDO('mysql:host=localhost;dbname=PRODUCTION', 'toto', 'toto');
    $laconnexion->setAttribute(PDO::ATTR_ERRMODE, PDO::ERRMODE_EXCEPTION);
} catch (PDOException $e) {
    die('Connexion échouée : ' . $e->getMessage());
}

$ordresql = "SELECT * FROM STOCKS";

try {
    $rsql = $laconnexion->query($ordresql);
    $lesTuples = $rsql->fetchAll();

    // Affichage des données
    foreach ($lesTuples as $leTuple) {
        echo $leTuple["Designation"] . "   ";
        echo $leTuple["PoidsUniteGr"] . "  ";
        echo $leTuple["NombreUnitesProduites"] . "<br/>";
    }
} catch (Exception $e) {
    echo "Erreur lors de l'exécution de la requête : " . $e->getMessage();
}
?>
</body>
</html>

                                [ Lecture de 34 lignes ]
^G Aide         ^O Écrire       ^W Chercher     ^K Couper       ^T Exécuter     ^C Emplacement  M-U Annuler     M-A Marquer     M-] -> Crochet  M-Q Précédent
^X Quitter      ^R Lire fich.   ^\ Remplacer    ^U Coller       ^J Justifier    ^_ Aller ligne  M-E Refaire     M-6 Copier      ^Q Retrouver    M-W Suivant
```

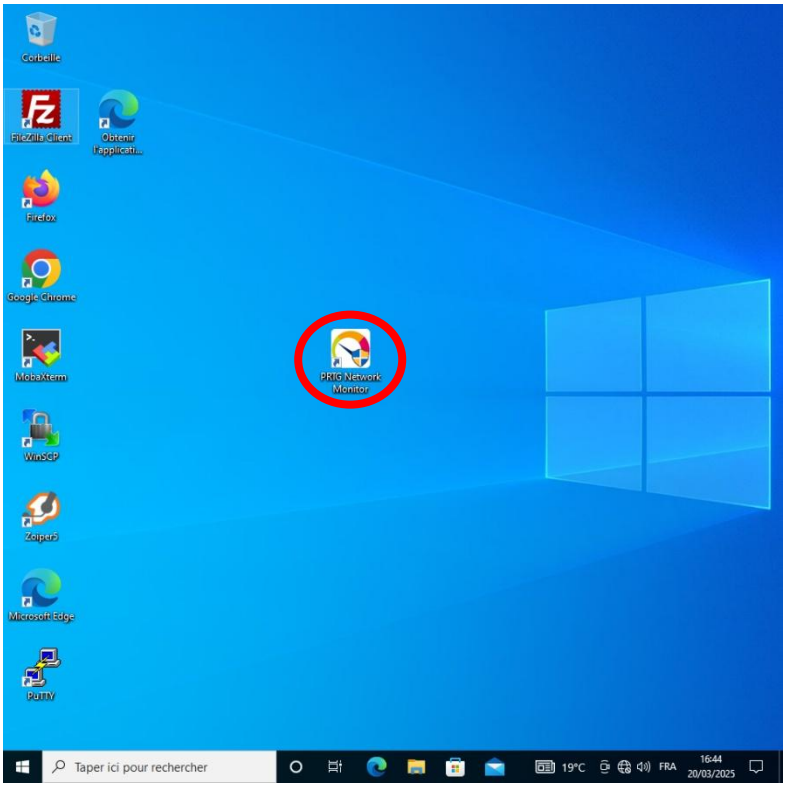
Nous avons la base de données nommée PRODUCTION dans laquelle nous avons la tables STOCKS :

```
MariaDB [(none)]> show databases;
+--------------------+
| Database           |
+--------------------+
| PRODUCTION         |
| information_schema |
| mysql              |
| performance_schema |
| sys                |
+--------------------+
5 rows in set (0,020 sec)

MariaDB [(none)]> _
```

```
Database changed
MariaDB [PRODUCTION]> show tables;
+----------------------+
| Tables_in_PRODUCTION |
+----------------------+
| STOCKS               |
+----------------------+
1 row in set (0,001 sec)

MariaDB [PRODUCTION]> SELECT * STOCKS
    -> ;
ERROR 1064 (42000): You have an error in your SQL syntax; c
CKS' at line 1
MariaDB [PRODUCTION]> SELECT * FROM STOCKS
    -> ;
+---------------+-------------+----------------------+
| Designation   | PoidsUniteGr | NombreUnitesProduites |
+---------------+-------------+----------------------+
| MagretsCanards |         380 |                15600 |
| BlocFoieGras   |         190 |                 3400 |
+---------------+-------------+----------------------+
2 rows in set (0,002 sec)
```

c. Service Supervision

Le service de supervision est configuré sur une machine Windows normale, Il y'a un accès web vers le logiciel PRTG sur le bureau :



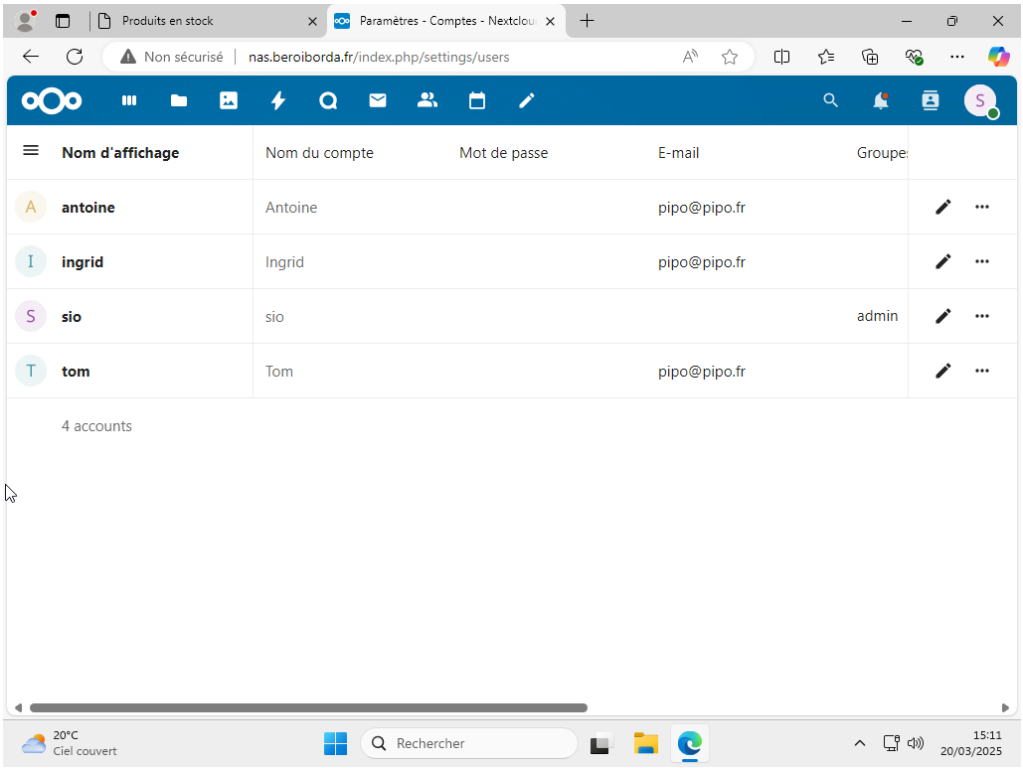
Voici l'état de l'infrastructure d'après PRTG :

d. Service de Stockage

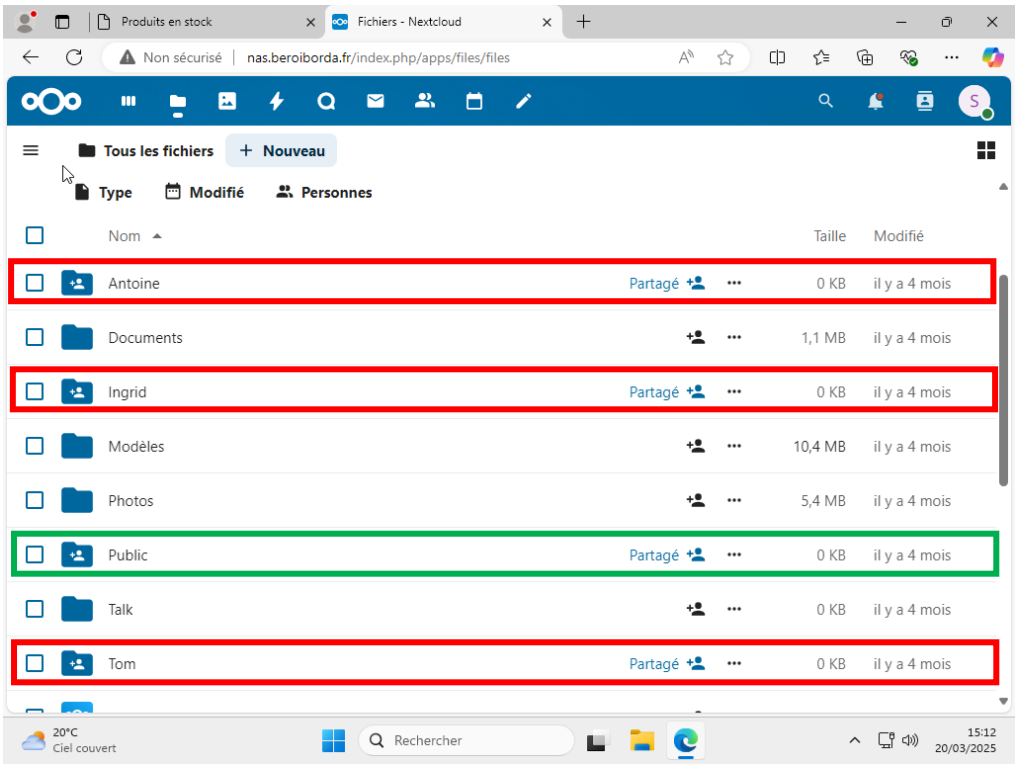
Pour le stockage de fichier, nous avons NextCloud.

Ici, trois utilisateurs : Tom, Antoine et Ingrid (les mêmes utilisateurs que sur la machine client avec les mêmes mots de passe mais pas de stratégie de groupe ni d'AD).

Chaque utilisateur à son dossier personnel, et un dossier en commun auquel tout le monde à accès nommé Public.



Voici les dossiers partagés :



e. Service DNS

On utilise le service bind9 pour le DNS afin d'avoir un URL personnalisé pour le NAS et l'Intranet, voici le fichier */etc/bind/named.conf.local* qui définit quels domaines correspond à quels fichiers de configuration :

```
 GNU nano 7.2                                named.conf.local
//
// Do any local configuration here
//

// Consider adding the 1918 zones here, if they are not used in your
// organization
//include "/etc/bind/zones.rfc1918";

zone "beroiborda.fr" {
    type master;
    file "/etc/bind/db.beroiborda.fr";
};

zone "2.15.222.in-addr.arpa" {
    type master;
    file "/etc/bind/db.reverse";
};
zone "intranet.beroiborda.fr" {
    type master;
    file "/etc/bind/db.intranet.beroiborda.fr";
};
zone "nas.beroiborda.fr" {
    type master;
    file "/etc/bind/db.nas.beroiborda.fr";
};
```

Le fichier de configuration principale pour définir les IP et le domaine *db.beroiborda.fr* :

```
  GNU nano 7.2                                                    db.beroiborda.fr
beroiborda.fr. IN SOA dnsba.beroiborda.fr. root.beroiborda.fr. (
        1 ; Serial
        604800 ; Refresh
        86400 ; Retry
        2419200 ; Expire
        604800 ) ; Negative Cache TTL

beroiborda.fr. IN NS dnsba.beroiborda.fr.
dnsba.beroiborda.fr. IN A 222.15.2.4

intranet.beroiborda.fr. IN A 222.15.2.1
nas.beroiborda.fr.  IN A 222.15.2.3
```

Le fichier de configuration db.reverse qui définit la zone inverse du DNS (sachant que le *hostname* de la machine est *dnsba*) :

```
  GNU nano 7.2                                                      db.reverse
2.15.222.in-addr.arpa. IN SOA dnsba.beroiborda.fr. root.beroiorda.fr. (
        2000102402
        21600
        3600
        604800
        86400
        )

2.15.222.in-addr.arpa. IN NS dnsba.beroiborda.fr.
4 IN PTR dnsba.beroiborda.fr
1 IN PTR intranet.beroiborda.fr.
3 IN PTR nas.beroiborda.fr.

intranet.beroiborda.fr. IN NS dnsba.beroiborda.fr.
1 IN PTR intranet.beroiborda.fr.

nas.beroiborda.fr. IN NS dnsba.beroiborda.fr.
3 IN PTR nas.beroiborda.fr.
```

Maintenant, les fichiers de configuration, respectivement pour l'Intranet et le NAS.

Celui de l'Intranet *db.intranet.beroiborda.fr* :

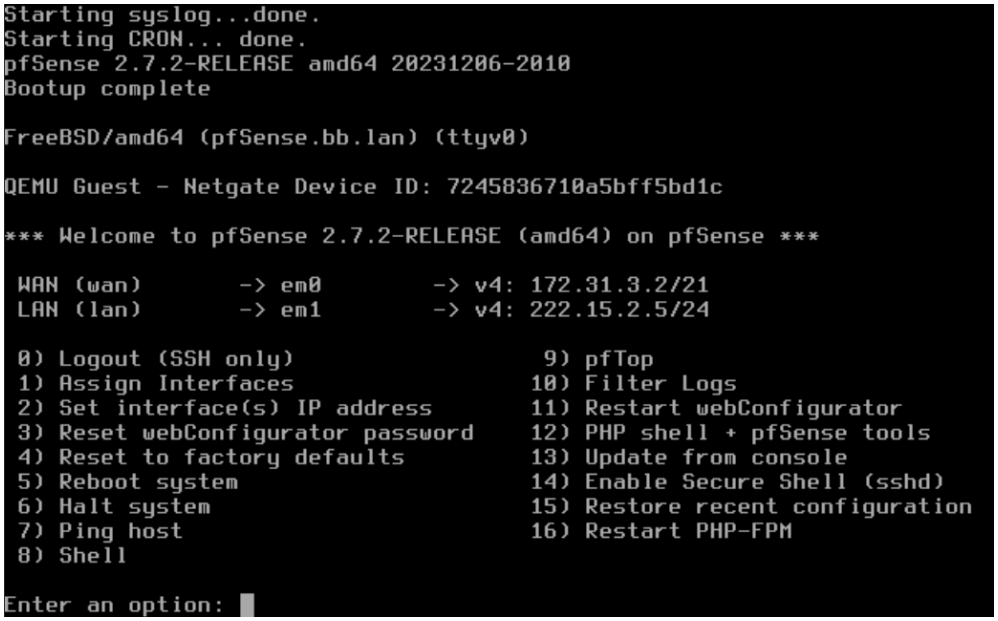
```
  GNU nano 7.2                                              db.intranet.beroiborda.fr
intranet.beroiborda.fr. IN SOA dnsba.beroiborda.fr. root.beroiborda.fr. (
        1 ; Serial
        604800 ; Refresh
        86400 ; Retry
        2419200 ; Expire
        604800 ) ; Negative Cache TTL

intranet.beroiborda.fr. IN NS dnsba.beroiborda.fr.
intranet.beroiborda.fr. IN A 222.15.2.1
```

Celui du NAS *db.nas.beroiborda.fr* :

```
  GNU nano 7.2                                                  db.nas.beroiborda.fr
nas.beroiborda.fr. IN SOA dnsba.beroiborda.fr. root.beroiborda.fr. (
        1 ; Serial
        604800 ; Refresh
        86400 ; Retry
        2419200 ; Expire
        604800 ) ; Negative Cache TTL

nas.beroiborda.fr. IN NS dnsba.beroiborda.fr.
nas.beroiborda.fr. IN A 222.15.2.3
```

f. Service de Routage

On utilise Pfsense pour le routeur qui permet de sortir du réseau local, voici les cartes réseaux du Routeur :



Des règles NAT ont été configurés pour les deux cartes réseaux, l'objectif est de permettre l'accès aux différents serveurs hors du réseau privé, en utilisant de la redirection de port :

Règles

	Interface	Protocole	Adresse source	Ports source	Adresse de destination	Ports dest.	IP NAT	Ports NAT	Description	Actions
✓ ▶	WAN	TCP/UDP	*	*	WAN address	22 (SSH)	222.15.2.3	22 (SSH)	SSH NAS	
✓ ▶	WAN	TCP/UDP	*	*	WAN address	2222	222.15.2.1	22 (SSH)	SSH WEB INTRANET	
✓ ▶	WAN	TCP/UDP	*	*	WAN address	2224	222.15.2.4	22 (SSH)	SSH DNS	

Ces règles NAT ont été configurés de sorte à ce que la connexion SSH se fasse avec l'IP de la carte réseau WAN du routeur et en utilisant des ports que l'on a configurés :

172.31.3.2

NAS : Port 22 (par défaut)

WEB : Post 2222

DNS : Port 2224

6. Description de la situation

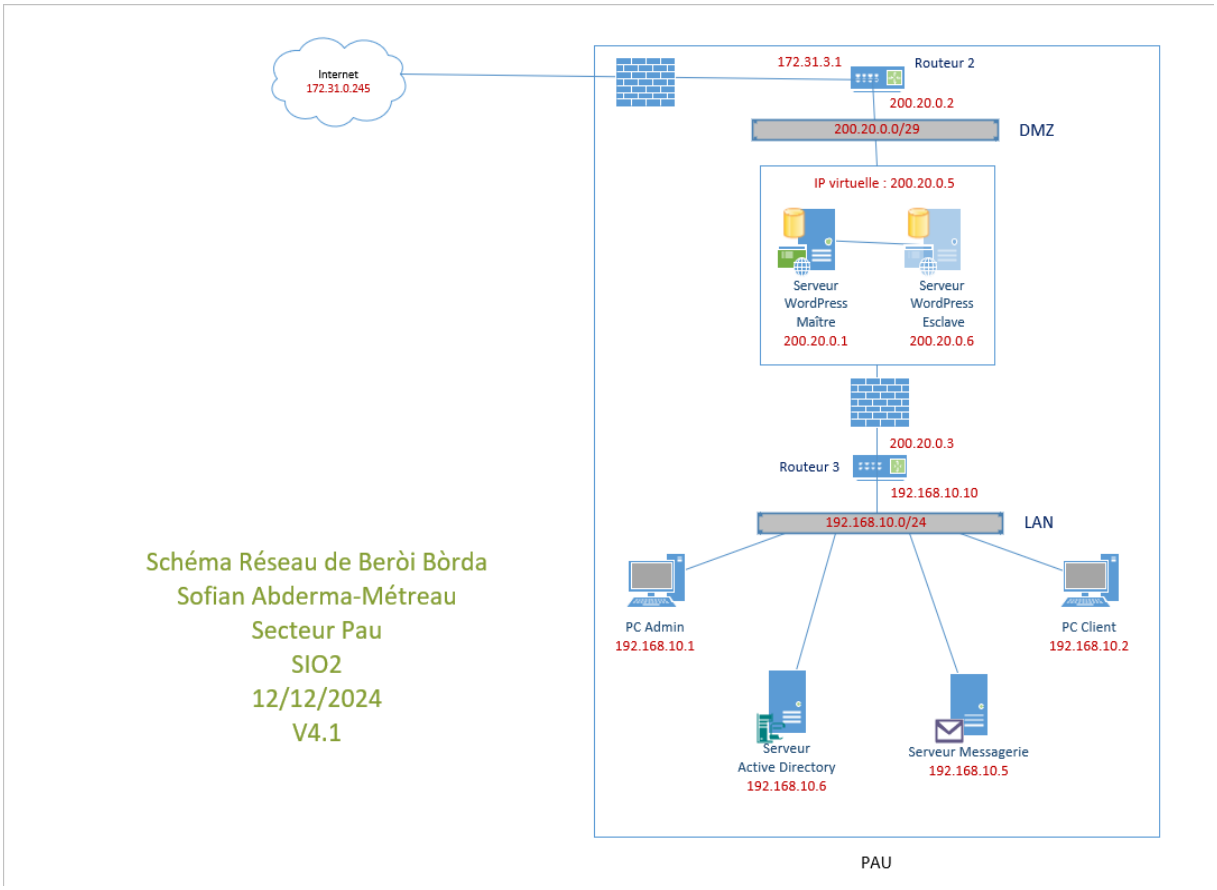
7. BTS SERVICES INFORMATIQUES AUX ORGANISATIONS SESSION 2024
8. ANNEXE 9-1-A : Fiche descriptive de réalisation professionnelle
9. **Épreuve E5 - Administration des systèmes et des réseaux (option SISR)**

DESCRIPTION D'UNE RÉALISATION PROFESSIONNELLE	**N° réalisation :**
Nom, prénom : Bousquet—Cadena Raphaël	**N° candidat :**
Épreuve ponctuelle ☒ **Contrôle en cours de formation** ☐	**Date :** ..... / ..... /.....
Organisation support de la réalisation professionnelle Lycée Saint-John Perse	
Intitulé de la réalisation professionnelle Beròi Bòrda secteur Pau	
Période de réalisation : ..... **Lieu :** ..... **Modalité :** ☐ **Seul(e)** ☒ **En équipe**	
Compétences travaillées ☒ Concevoir une solution d'infrastructure réseau ☒ Installer, tester et déployer une solution d'infrastructure réseau ☒ Exploiter, dépanner et superviser une solution d'infrastructure réseau	
Conditions de réalisation[5] (ressources fournies, résultats attendus) Salle 23 avec les machines virtuelles sur VirtualBox et Proxmox.	
Description des ressources documentaires, matérielles et logicielles utilisées[6] Le projet Beròi Bòrda secteur Pau comporte un schéma réseau et un plan d'adressage.	
Modalités d'accès aux productions[7] et à leur documentation[8]	

[5] En référence aux *conditions de réalisation et ressources nécessaires* du bloc « Administration des systèmes et des réseaux » prévues dans le référentiel de certification du BTS SIO.
[6] Les réalisations professionnelles sont élaborées dans un environnement technologique conforme à l'annexe II.E du référentiel du BTS SIO.
[7] Conformément au référentiel du BTS SIO « *Dans tous les cas, les candidats doivent se munir des outils et ressources techniques nécessaires au déroulement de l'épreuve. Ils sont seuls responsables de la disponibilité et de la mise en œuvre de ces outils et ressources. La circulaire nationale d'organisation précise les conditions matérielles de déroulement des interrogations et les pénalités à appliquer aux candidats qui ne se seraient pas munis des éléments nécessaires au déroulement de l'épreuve.* ». Les éléments nécessaires peuvent être un identifiant, un mot de passe, une adresse réticulaire (URL) d'un espace de stockage et de la présentation de l'organisation du stockage.

[8] Lien vers la documentation complète, précisant et décrivant, si cela n'a été fait au verso de la fiche, la réalisation, par exemples schéma complet de réseau mis en place et configurations des services.

7. Schéma Réseau



8. Plan d'adressage

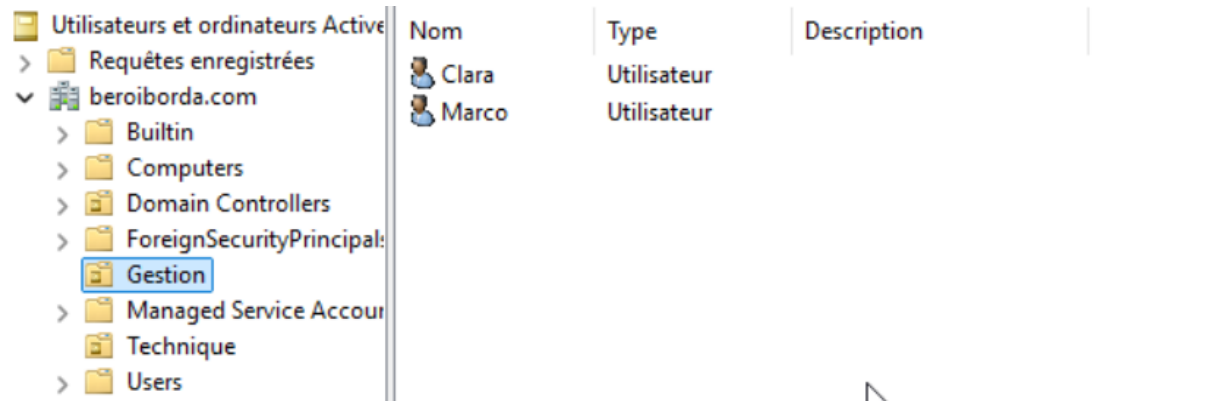
Réseaux	Rôles	Outils	Machines	Noms	Adresses IP	Masques de sous-réseau	Passerelles
WAN - 172.31.0.0/21	Connexion Internet		Internet	Internet	172.31.0.245	255.255.248.0	
	Routage + Filtrage		Routeur	Routeur 2	172.31.3.1	255.255.248.0	172.31.0.245
LAN PAU - 192.168.10.0/24	Routage + Filtrage		Routeur	Routeur 3	192.168.10.10	255.255.255.0	
	Administrateur	Windows 11	PC Admin	admin_ba	192.168.10.1	255.255.255.0	192.168.10.10
	Gestion des groupes et users	Windows Server	Serveur Active Directory	ad_ba	192.168.10.6	255.255.255.0	192.168.10.10
	Messagerie	iRedmail	Serveur Messagerie	mess_ba	192.168.10.5	255.255.255.0	192.168.10.10
	Client	Windows 11	PC Client	client_ba	192.168.10.2	255.255.255.0	192.168.10.10
DMZ - 200.20.0.0/29	Routage + Filtrage	Règles NAT SSH : port 2222 (ad_ba) ; port 2223 (mess_ba)	Routeur	Routeur 2	200.20.0.2	255.255.255.248	
	Routage + Filtrage	Règle NAT : Bloquer tous sauf le web	Routeur	Routeur 3	200.20.0.3	255.255.255.248	200.20.0.2
	Serveur Web + Haute disponibilité	Corosync + Pacemaker + MySQL + WordPress	Serveur Web Maître	maître_wordpress_ba	200.20.0.1	255.255.255.248	200.20.0.2
	Serveur Web + Haute disponibilité	Corosync + Pacemaker + MySQL + WordPress	Sevreur Web Esclave	esclave_wordpress_ba	200.20.0.6	255.255.255.248	200.20.0.2
	Haute disponibilité	Corosync + Pacemaker	IP virtuelle	IP virtuelle	200.20.0.5	255.255.255.248	200.20.0.2

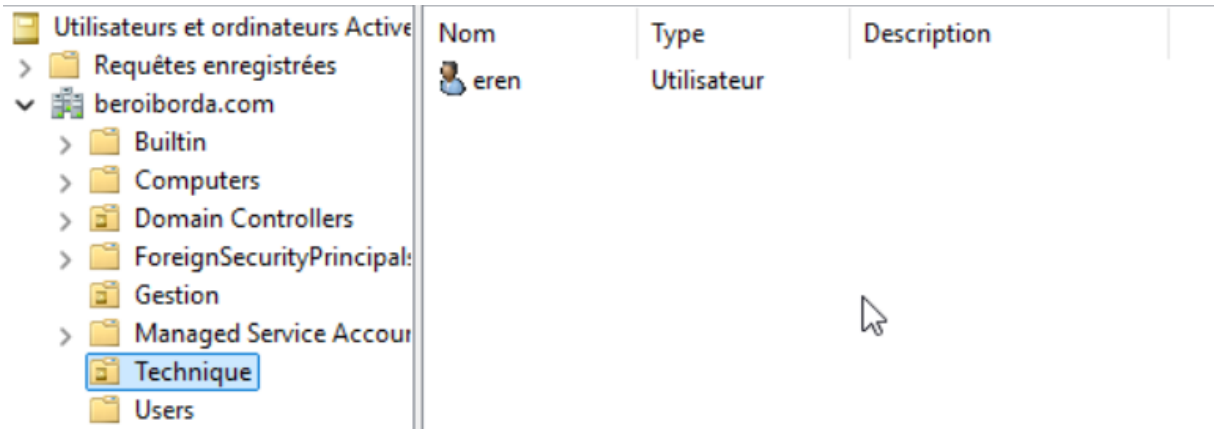
9. Services

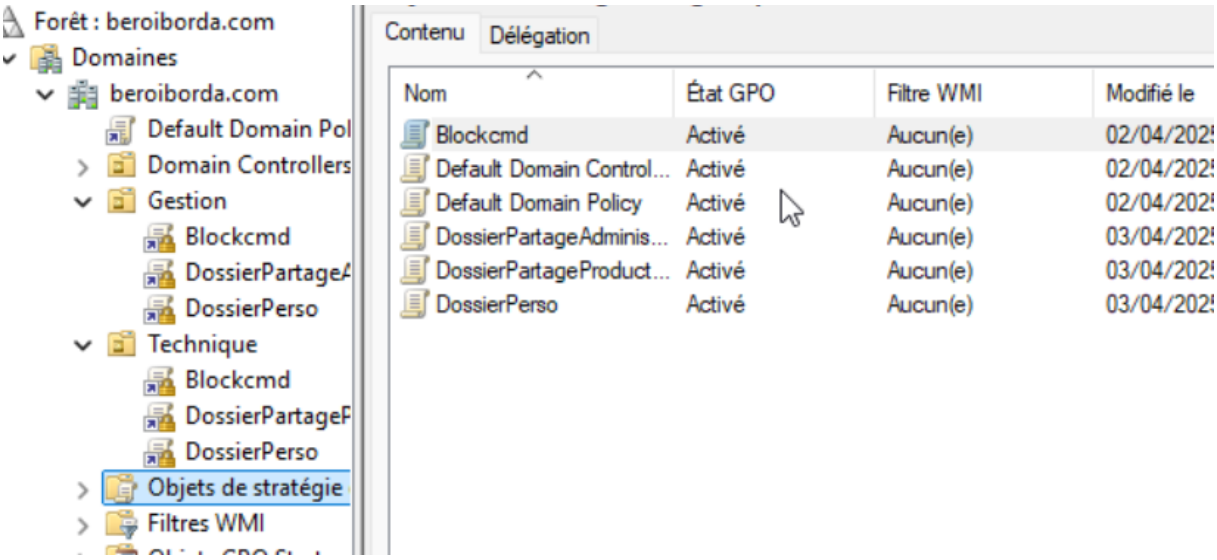
1-LAN

a) **AD Windows**

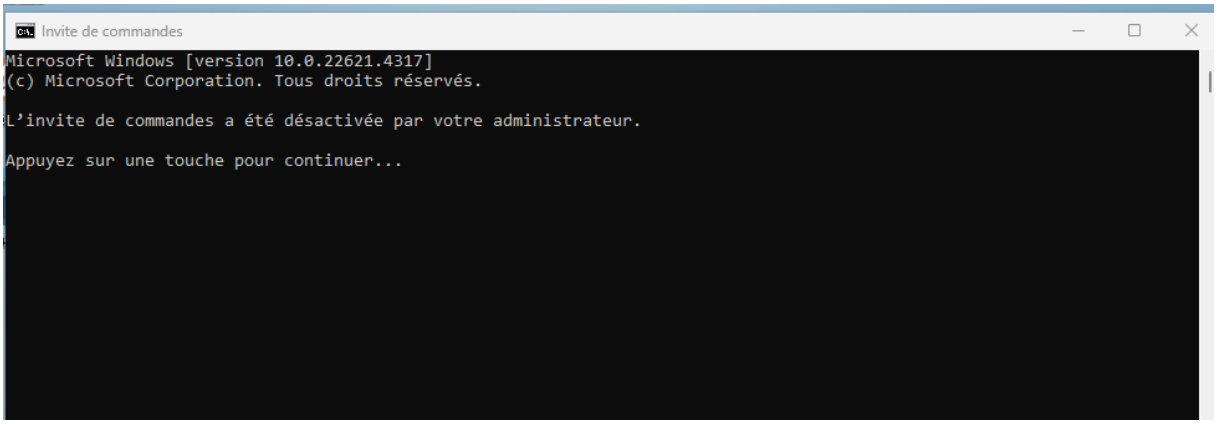
Un **contrôleur de domaine Active Directory (AD Windows)** permet l'authentification centralisée des employés et la gestion des permissions sur le réseau.



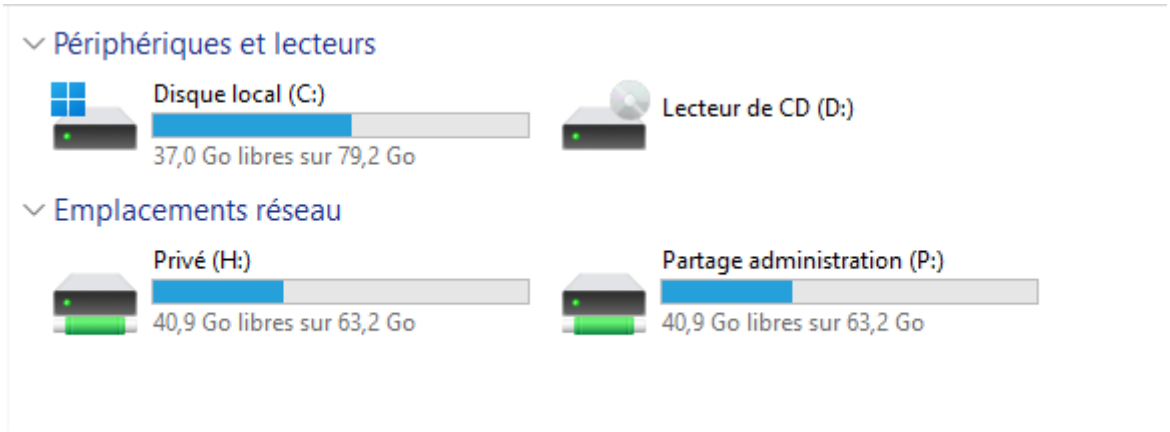




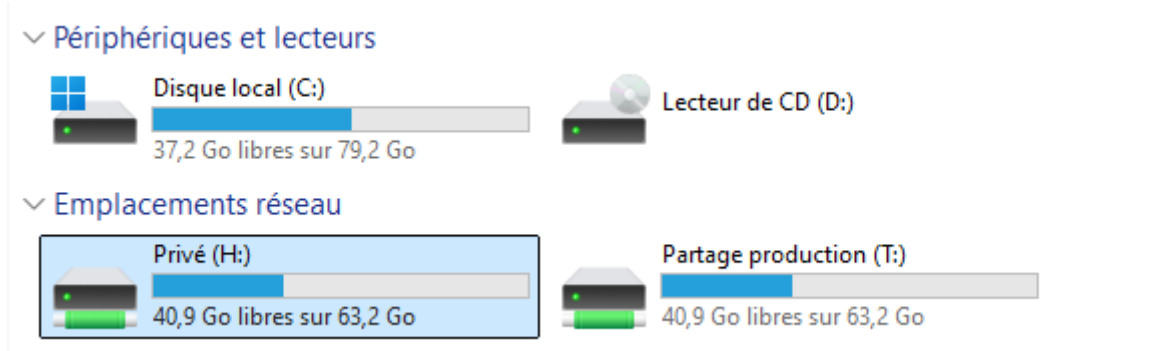
La GPO « Blockcmd » permet de bloquer l'accès à l'invite de commandes.



La GPO « DossierPerso » permet l'obtention d'un dossier personnelle pour tout le monde.

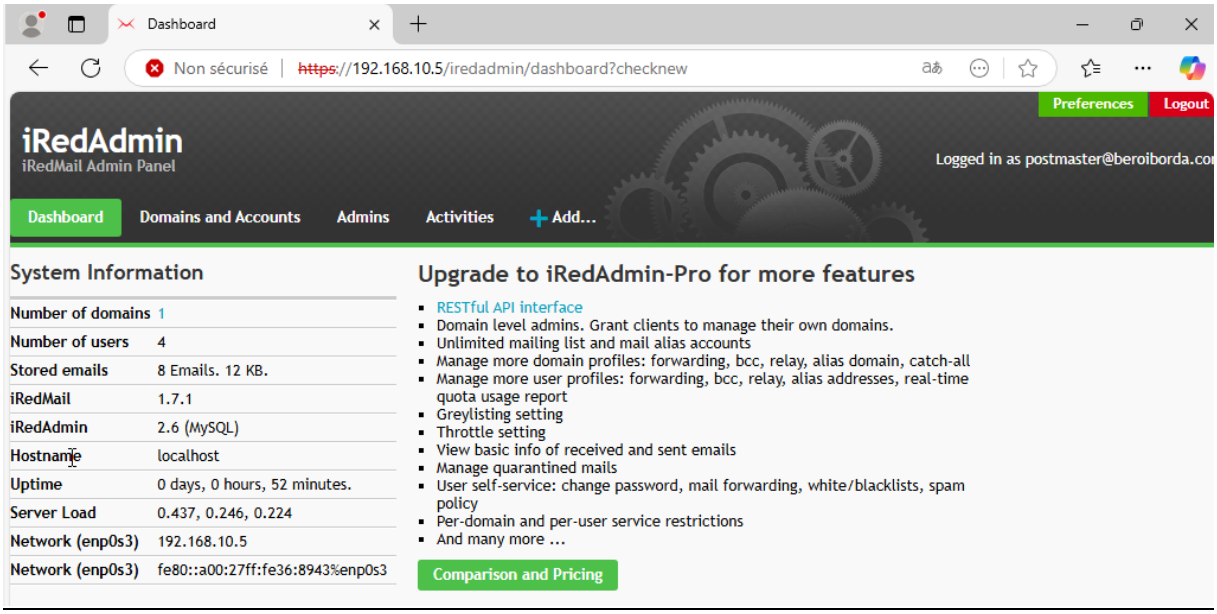


La GPO « DossierpartageProduction » permet de partager un dossier dans l'UO Technique.

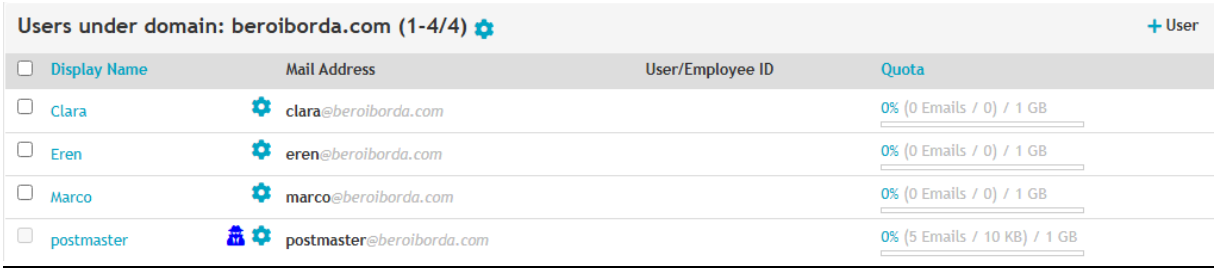


b) **Serveur de messagerie**

Un **serveur de messagerie** permet l'envoi, la réception et le stockage des courriels professionnels. Il facilite la communication interne et externe de l'entreprise.



<u>Liste des utilisateurs ayant un mail :</u>



Fail2Ban protège votre serveur contre les tentatives d'intrusion en bloquant les adresses IP après plusieurs échecs de connexion.

```
[DEFAULT]
# time is in seconds. 3600 = 1 hour, 86400 = 24 hours (1 day)


#La fenêtre de détection des tentatives échouées est de 1 heure.
findtime    = 3600

#Une IP sera bloquée pendant 1 heure après avoir dépassé la limite.
bantime     = 3600

#Après 5 échecs, l'IP est bannie.
maxretry    = 5

#Exclut les IP locales du bannissement
ignoreip    = 127.0.0.1 127.0.0.0/8 10.0.0.0/8 172.16.0.0/12 192.168.0.0/16
```

c)**Routeur(LAN)**

Règles Nat du routeur LAN

Règles

	Interface	Protocole	Adresse source	Ports source	Adresse de destination	Ports dest.	IP NAT	Ports NAT	Description	Actions
☐ ✓ ▶	WAN	TCP/UDP	*	*	WAN address	4432	192.168.10.10	443 (HTTPS)	routeur(LAN vers WAN)	
☐ ✓ ▶	WAN	TCP/UDP	*	*	WAN address	3389 (MS RDP)	192.168.10.6	3389 (MS RDP)	rdp Active Directory	
☐ ✓ ▶	WAN	TCP/UDP	*	*	WAN address	2222	192.168.10.6	22 (SSH)	ssh 2222 Active Directory	
☐ ✓ ▶	WAN	TCP/UDP	*	*	WAN address	2223	192.168.10.5	22 (SSH)	ssh 2223 Serveur Mail	

2-DMZ

Une **zone DMZ** a été mise en place pour héberger les services accessibles depuis Internet tout en garantissant la sécurité du réseau interne.

Un **serveur WordPress maître** héberge le site web de l'entreprise, permettant aux clients et partenaires d'accéder aux informations et aux services en ligne.

Un **serveur WordPress esclave** est mis en place pour assurer une redondance, garantissant la disponibilité du site en cas de panne du serveur principal.

a)Serveur web

Fichier Corosync pour haute disponibilité :

```
totem {
    version: 2
    cluster_name: Wordpress-cluster
    crypto_cipher: aes256
    crypto_hash: sha256
}

logging {
    fileline: off
    to_stderr: yes
    to_logfile: yes
    logfile: /var/log/corosync/corosync.log
    to_syslog: yes
    debug: off
    logger_subsys {
        subsys: QUORUM
        debug: off
    }
}

quorum {
    provider: corosync_votequorum
    expected_votes: 2
    two_nodes: 1
}

nodelist {
    node {
        name: beroiborda-maitre
        nodeid: 1
        ring0_addr: 200.20.0.1
    }

    node {
        name: beroiborda-esclave
        nodeid: 2
        ring0_addr: 200.20.0.6
    }
}
```

Configuration du cluster

```
  * 2 nodes configured
  * 4 resource instances configured

Node List:
  * Online: [ beroiborda-esclave beroiborda-maitre ]

Full List of Resources:
  * IPFailover  (ocf:heartbeat:IPaddr2):         Started beroiborda-maitre
  * serviceWeb  (ocf:heartbeat:nginx):   Started beroiborda-esclave
  * Clone Set: cServiceMySQL [serviceMySQL]:
    * Started: [ beroiborda-esclave beroiborda-maitre ]

root@beroiborda-maitre:~#
```

b)Routeur

Règles NAT Du routeur DMZ :

Règles

	Interface	Protocole	Adresse source	Ports source	Adresse de destination	Ports dest.	IP NAT	Ports NAT	Description	Actions
	WAN	TCP/UDP	*	*	WAN address	22 (SSH)	200.20.0.1	22 (SSH)	ssh Serveur Web maitre	
	WAN	TCP/UDP	*	*	WAN address	2225	200.20.0.6	22 (SSH)	ssh Serveur Web esclave	
	WAN	TCP/UDP	*	*	WAN address	4432	200.20.0.3	4432	Acces routeur public (Lan)	
	WAN	TCP/UDP	*	*	WAN address	4431	200.20.0.2	443 (HTTPS)	Acces routeur public (DMZ)	
	WAN	TCP/UDP	*	*	WAN address	3389 (MS RDP)	200.20.0.3	3389 (MS RDP)	rdp Active Directory	
	WAN	TCP/UDP	*	*	WAN address	80 (HTTP)	200.20.0.5	80 (HTTP)	http wordpress	
	WAN	TCP/UDP	*	*	WAN address	443 (HTTPS)	200.20.0.5	443 (HTTPS)	https Wordpress	
	WAN	TCP/UDP	*	*	WAN address	2222	200.20.0.3	2222	ssh 2222 Active Directory	
	WAN	TCP/UDP	*	*	WAN address	2223	200.20.0.3	2223	ssh 2223 Serveur Mail	