

fbm

Rapport de stage



Nom : Meresse

Prénom : François-Xavier

Classe : BTS SIO 2

Année : 2020-2021

Formation : BTS Service informatique aux organisations

Lieu de scolarité : Ecole de commerce ESICAD

Lieu et date de la PFMP : 20 lotissement porette rn200, Corte

Du 21/12/20 au 15/01/21.

[Introduction : 2](#_Toc62556545)

[Présentation de l’entreprise : 2](#_Toc62556546)

[Activité de la société : 3](#_Toc62556547)

[Compte rendu d’activité : 3](#_Toc62556548)

[Présentation du projet : 3](#_Toc62556549)

[Contexte : 3](#_Toc62556550)

[Objectifs : 3](#_Toc62556551)

[Contexte et objectifs du projet : 4](#_Toc62556552)

[Cahier des charges pour le changement de l’infrastructure informatique 4](#_Toc62556553)

[L’infrastructure informatique : 4](#_Toc62556554)

[Matériel : 4](#_Toc62556555)

[Serveur 4](#_Toc62556556)

[Postes de travail 4](#_Toc62556557)

[Pare-feu (pfsense) 4](#_Toc62556558)

[Réseau 5](#_Toc62556559)

[Paramétrage du réseau 5](#_Toc62556560)

[Configuration du serveur 5](#_Toc62556561)

[Configuration du firewall : 6](#_Toc62556562)

[Tableau d’adressage IP interface firewall : 7](#_Toc62556563)

[Règle pare-feu : 7](#_Toc62556564)

[Configuration des stations de travail 8](#_Toc62556565)

[Switch et Onduleur 9](#_Toc62556566)

[Maintenance du serveur 9](#_Toc62556567)

[Mise en place du Firewall : 10](#_Toc62556568)

[Mise en place et attribution des interfaces : 10](#_Toc62556569)

[Mise en place des règles sur les interfaces : 10](#_Toc62556570)

[Mise en place du serveur AD Samba. 11](#_Toc62556571)

[Initialisation de base : 11](#_Toc62556572)

[Quesque SAMBA AD : 13](#_Toc62556573)

[Mise en place du poste administrateur du réseau Windows 10 : 13](#_Toc62556574)

[Création utilisateurs et groupes : 14](#_Toc62556575)

[Mise en place d’un client Windows 10 sur le domaine : 15](#_Toc62556576)

[Paramètre réseau : 15](#_Toc62556577)

[Entré dans le domaine : 15](#_Toc62556578)

[Connexion session utilisateur du domaine : 16](#_Toc62556579)

[Partage de fichier TrueNas : 17](#_Toc62556580)

[Quesque TrueNas : 17](#_Toc62556581)

[Comment marche TrueNas : 18](#_Toc62556582)

[Mise en place de TrueNas : 18](#_Toc62556583)

[Configuration de TrueNas : 18](#_Toc62556584)

[Mise en place des GPO : 20](#_Toc62556585)

[Déploiement des lecteurs réseau : 20](#_Toc62556586)

[Déploiement logiciel : 20](#_Toc62556587)

[Méthode de sauvegarde : 20](#_Toc62556588)

# Introduction :

Dans le cadre de ma deuxième année de BTS Service informatique aux organisations, j’ai été amené à participer à une période de formation en milieu professionnel afin d’approfondir mes connaissances et mon expérience lors de ma formation et d’agrandir mes connaissances en milieu professionnel.

J’ai choisi d’effectuer cette période de stage dans l’entreprise FBM afin d’avoir une expérience dans une entreprise croissante souhaitant développer une petite architecture réseau afin d’approfondir mes connaissances dans ce milieu.

# Présentation de l’entreprise :

Dénomination : FBM

Effectif : 4 salariés

Siège : 20 lotissements porette rn200, CORTE, Corse

Téléphone : 0601020234

# Activité de la société :

FBM est une entreprise corse et une chaîne distribution et vente de produits agroalimentaire sur éventaires et marchés basé à Corte en Corse.

# Compte rendu d’activité :

## Présentation du projet :

## Contexte :

Le système informatique actuel est obsolète, n’est pas évolutif.

Une nouvelle infrastructure devra répondre à tous les points actuels bloquants et/ou à améliorer.

Les attentes des utilisateurs sont multiples : temps de réponse, faciliter d’accès aux données, sécurisation du matériel et des données par mise en place des droits et sauvegardes.

## Objectifs :

Les objectifs attendus sont les suivants :

* Mettre en œuvre un système performant.
* Sécuriser l’infrastructure matérielle et réseau dans une baie informatique ondulée.
* Respecter le planning d’installation et mise en œuvre afin de ne pas perturber la mise en œuvre des logiciels acquis.

## Contexte et objectifs du projet :

Le projet couvre les domaines suivants :

* Système
* Réseau
* Gestion d’accès et de droits
* Sauvegardes
* Sécurité

Les utilisateurs sont à définir sur le réseau géré sur le nouveau serveur Samba AD.

Un seul site est concerné.

## Cahier des charges pour le changement de l’infrastructure informatique

## L’infrastructure informatique :

## Matériel :

Afin de sécuriser l’infrastructure informatique, il est souhaité un regroupage de tous les éléments dans une baie fermée à clé, où seront stockés :

* Un pare-feu qui sécurisera le réseau
* Un serveur qui supportera le système et logiciels
* Un Switch qui distribuera les différentes interfaces sur des VLANs
* Un onduleur qui protégera l’installation matériel
* Un NAS open source qui partagera/sauvegardera et régulera les droits d’accès aux données

## Serveur

L’espace de données et lecteurs seront redéfinis sur le serveur.

Des lecteurs sont à définir ainsi que la gestion des utilisateurs.

## Postes de travail

Les postes de travail actuels des utilisateurs au nombre de 4 sont à changer.

Afin de faciliter le partage des données et leur sécurité et éviter les données sépares, il faudra veiller à donner l’accès aux utilisateurs sur le lecteur Public du serveur.

Les données seront protégées par droits spécifiques.

## Pare-feu (pfsense)

Le pare-feu Pfsense permettra de sécuriser le réseau via des règle de sécurité.

Il agira sur un WAN, LAN, un LAN2 et une DMZ.

Le LAN2 et la DMZ distribuerons des IP par DHCP.

## Réseau

## Paramétrage du réseau

Le réseau LAN est à mettre en œuvre dont le domaine est « FBMSRV » en remplacement de Workgroup.

Une redéfinition de l’ingénierie Réseau permettra d’améliorer les accès Utilisateurs et droits allouées aux données.

Par sécurité, une vérification des prises réseau est demandée, qui sera retranscrite dans le cahier de recette final.

## Configuration du serveur

|  |  |
| --- | --- |
| Caractéristique | Caractéristique technique |
| Encombrement | Serveur mini tour |
| Dimensions | Hauteur : 36 cm Largeur : 17,5 cm Profondeur : 43,5 cm |
| Processeur | Intel Core™ i5 |
| Chipset | Gamme Intel C236 |
| Système d'exploitation | Debian 10 |
| Mémoire | 16Gb DDR4 2400 MT/s |
| Stockage | SATA HDD 500GB  SARA HDD 2 TO |
| Baies de disques | 4 disques durs 3,5 pouces câblés maximum |
| Emplacements | * 1 emplacement PCIe 3.0 x8 (connecteur x16) * 1 emplacement PCIe 3.0 x4 (connecteur x8) * 1 emplacement PCIe 3.0 x4 (connecteur x8) * 1 emplacement PCIe 3.0 (connecteur x1) |
| Contrôleurs RAID | PERC S130, PERC H330, PERC H730, PERC H830 |
| Contrôleur réseau | Broadcom® BCM5720 |
| Communications | 2 cartes LOM 1 GbE |
| Alimentation | Bloc d’alimentation 290 W câblé |
| Accès des périphériques | 8 ports USB au total : • Ports USB arrière : 2 ports USB 3.0 + 4 ports USB 2.0 • Ports USB avant : 1 port USB 2.0 + 1 port USB 3.0 |
| Static IP | 192.168.3.10 |
| Domaine | Fbmsrv.local |

## Configuration du firewall :

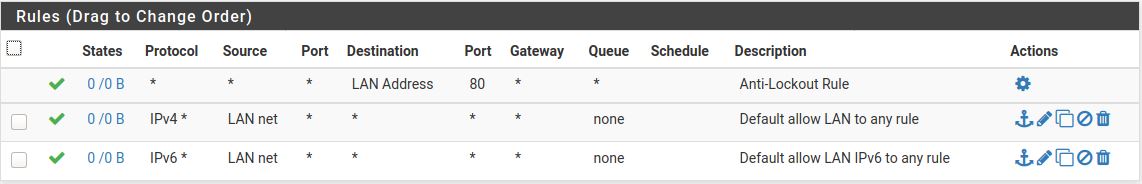
|  |  |
| --- | --- |
| **CPU** | Marvell Armada 3720 (88F3720) ARMv8-A 64-bit Cortex A53 @ 1.2GHz with NEON SIMD and FPU |
| **CPU Cores** | Dual Core |
| **Networking** | One 1 Gigabit Ethernet WAN port (RJ45 / SFP Combo) Four 1 Gigabit Ethernet LAN ports (Marvel 88E6141 switch, uplink at 2.5 Gbps) LAN ports can be repurposed for additional WAN ports |
| **Storage** | 8GB eMMC Flash on board, factory-upgradable to 32 GB M.2 SATA 2242  Solid State Drive (not NVMe compatible) |
| **Memory** | 4 GB DDR4 |
| **Expansion** | 1x M.2 'B' key sockets (SSD, LTE) 1x miniPCIe (WiFi) microSIM slot |
| **Console Port** | MiniUSB (console cable included) |
| **USB Ports** | 1x 2.0 port |
| **LED** | 3 full color RGB LEDs |
| **Enclosure** | Desktop 1.7" (42.2 mm) tall x 4.25" (108 mm) deep x 6.8" (172.7 mm) wide with integrated keyholes for easy wall mounting |
| **Cooling** | Passive |
| **Power** | External ITE P/S AC/DC 100-240V, 50-60 Hz, 12V 2.0A, threaded  barrel connector AC Inlet: IEC320-C7 (2 PIN) One US, UK, EU or ANZ power cord included US Power Cord: NEMA 1-15P to IEC320-C7 UK Power Cord: BS 1363 to IEC320-C7 EU Power Cord: CEE7/16 to IEC320-C7 ANZ Power Cord: AS 3112 (ungrounded) to IEC320-C7 |
| **Environmental** | 32°F (0°C) to 122°F (50°C) |
| **Certifications** | CE, FCC (Class B), RoHS, UL, RCM, VCCI |

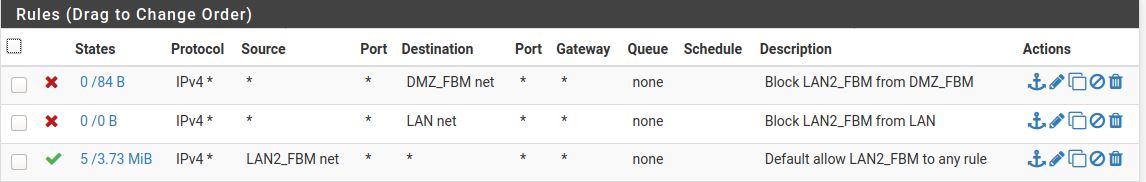
## Tableau d’adressage IP interface firewall :

|  |  |  |
| --- | --- | --- |
| Interface | IP | DHCP |
| WAN | 192.168.1.60 | NO |
| LAN | 10.0.0.254 | 10.0.0.6 ; 10.0.0.240 |
| LAN2\_FBM | 192.168.3.254 | 192.168.3.6 ; 192.168.3.200 |
| DMZ | 172.16.0.1 | 172.16.0.6 ; 172.16.255.200 |

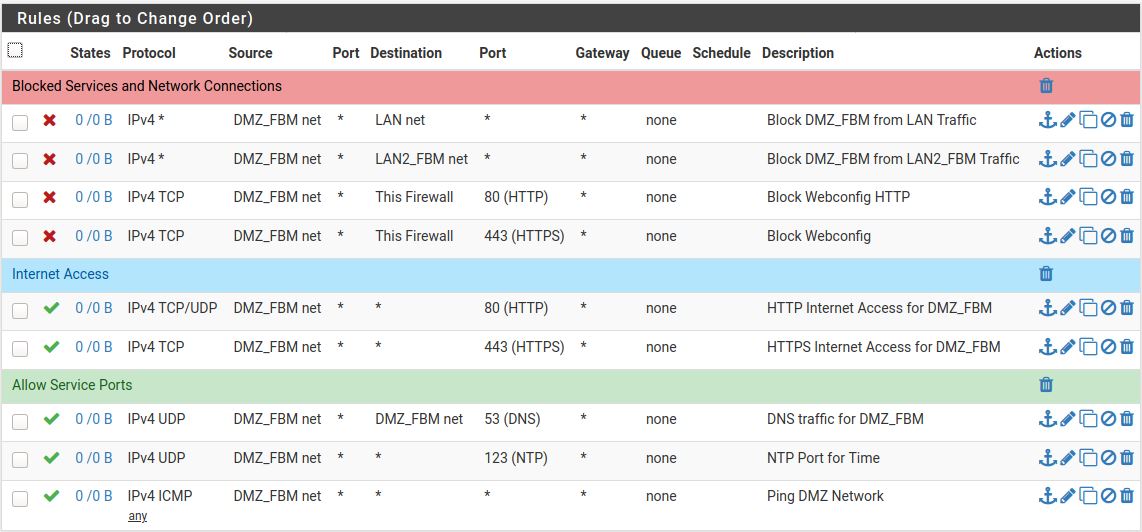
## Règle pare-feu :

LAN :

LAN2\_FBM :



DMZ :



## Configuration des stations de travail

|  |  |
| --- | --- |
| Processeur | Intel Core i5 |
| Système d’exploitation | Windows 10 Pro |
| RAM | 16bg |
| Espace disque | 250Gb |
| Internet / réseau / protocole | Connection Internet LAN2\_FBM (ADSL)   * Protocole TCPIP V4 * Résolution des noms de domaine en adresses IP pour le routage |
| Ecran / Résolution | 24’’ plat et 1920x1080 |
| Clavier + souris | HP |
| Bureautique | Office Microsoft 365 Business Standard |

## Switch et Onduleur

Switch :

NETGEAR (GS724T) :



Onduleur :

APC Smart-UPS SMT - SMT750I :



750 VA

Câblage :

* Cable couleur rouge = prise des éléments réseau et système.
* Cable couleur gris/blanc = prise réseau utilisateur.

Les câbles devront être étiquetés et brassés correctement.

## Maintenance du serveur

La solution doit prévoir :

* Des procédures techniques d’arrêt/redémarrage du serveur applicatif,
* Des procédures de sauvegardes journalières, hebdomadaires, mensuelles et annuelles (pour les données à garder sur plusieurs années) et restauration.
* Un registre des incidents avec les actions correctives apportées, à utiliser par l’utilisateur-clé.

# Mise en place du Firewall :

## Mise en place et attribution des interfaces :

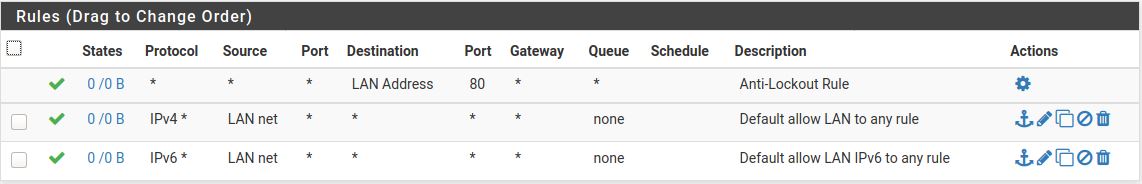
* L’interface WAN qui recevra une arrivé Ethernet du routeur ADSL et qui possèdera une IP fixe 192.168.1.60 un masque de 255.255.255.0 et une passerelle 192.168.1.1 ainsi que le domaine FBMSRV.LOCAL elle disposera par ailleurs deux DNS, un primaire 8.8.8.8 et un secondaire 8.8.4.4.
* L’interface LAN qui elle est relier au switch sur le VLAN 110 possédera une IP fixe 10.0.0.254 et un masque de 255.255.255.0 ainsi qu’une distribution d’adresse IP par DHCP sur une range allant de 10.0.0.6 à 10.0.0.240.
* L’interface LAN2\_FBM qui elle est relier au switch sur le VLAN 120 possédera une IP fixe 192.168.3.254 et un masque de 255.255.255.0 ainsi qu’une distribution d’adresse IP par DHCP sur une range allant de 192.168.3.6 à 192.168.3.200.
* L’interface DMZ\_FBM qui elle est relier au switch sur le VLAN 130 possédera une IP fixe 172.16.0.1 et un masque de 255.255.0.0 ainsi qu’une distribution d’adresse IP par DHCP sur une range allant de 172.16.0.6 à 172.16.255.200.

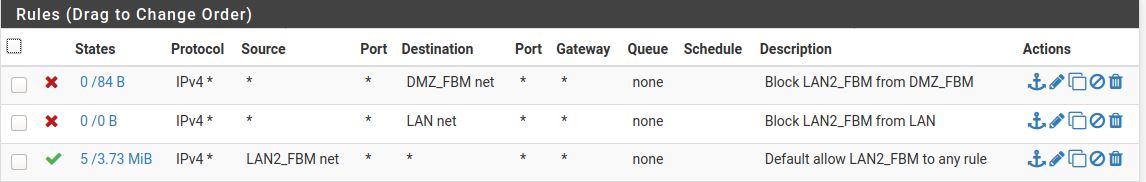
Une série de test ont été effectués afin d’assurer le bon fonctionnement des interfaces et des communications.

***Une documentation technique est mise en place à l’annexe 1.***

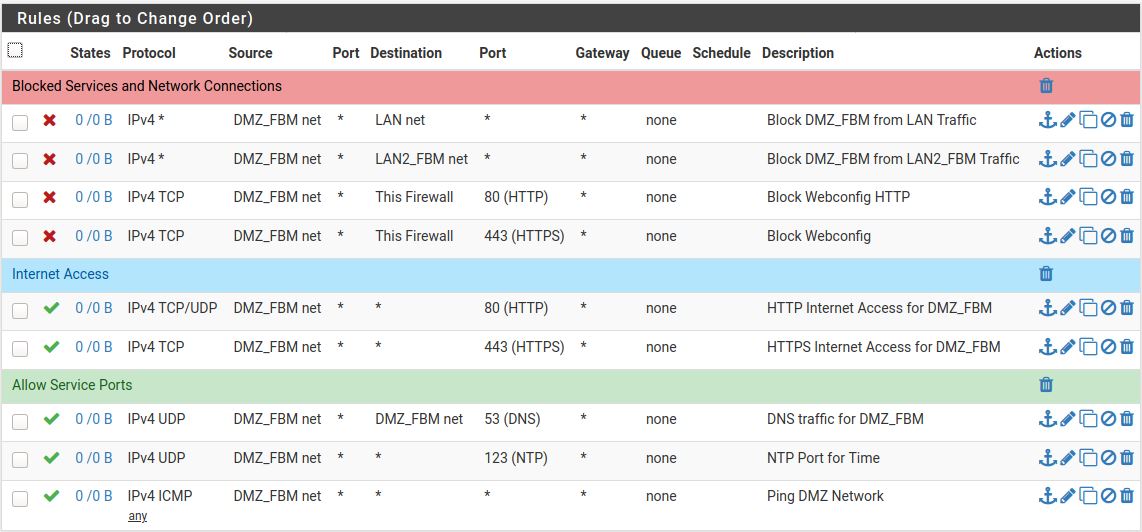
## Mise en place des règles sur les interfaces :

L’interface LAN donne un total accès comme le montre le tableau suivant :



L’interface LAN2\_FBM ne communiquera pas avec la DMZ et le LAN et a un accès complet à l’autre règles comme le montre le tableau suivant : 

L’interface DMZ\_FBM ne communiquera pas avec le LAN et le LAN2\_FBM, bloquera l’accès a l’interface du pare-feu Pfsense en HTTP et en HTTPS.

Elle autorisera les communication internet HTTP et HTTPS ainsi que les service DNS, NTP et ICMP comme le montre le tableau suivant :

***Une documentation technique est mise en place à l’annexe 2.***

# Mise en place du serveur AD Samba.

## Initialisation de base :

Le serveur AD Samba utilisera un système d’exploitation Debian 10.

Le serveur aura un domaine de recherche nommé : fbmsrv.local

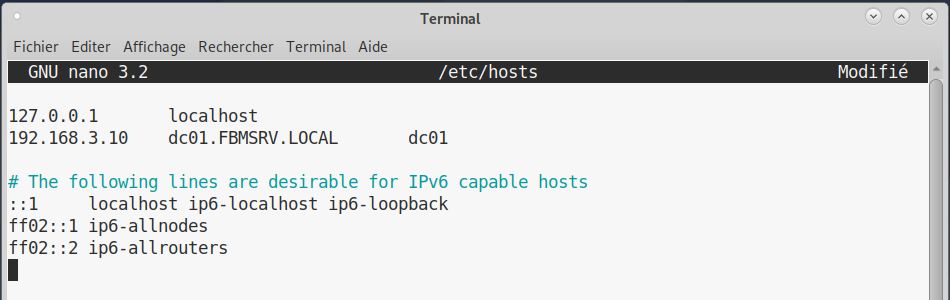
Le nom de serveur est : DC01

L’IP du serveur est : 192.168.3.10 avec un masque 255.255.255.0 /24 et une passerelle pointant sur l’interface Pfsense LAN2\_FBM 192.168.3.254.

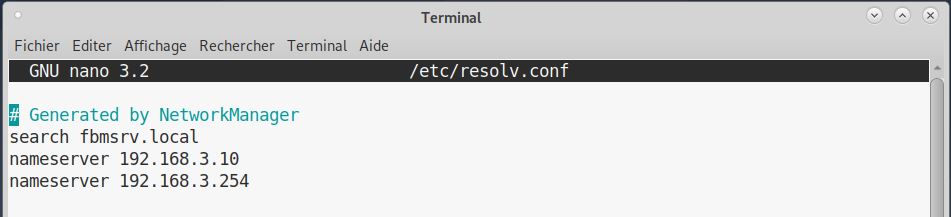
DNS du serveur :

* Primaire : 192.168.3.10 (lui-même)
* Secondaire : 192.168.3.254 (passerelle Pfsense LAN2\_FBM)

Le fichier /etc/hosts sera éditer comme suivant :



Ainsi que le fichier /etc/resolv.conf sera éditer comme ceci :



Les services suivants y seront installés :

acl attr autoconf bind9utils bison build-essential debhelper dnsutils docbook-xml docbook-xsl flex gdb libjansson-dev krb5-user libacl1-dev libaio-dev libarchive-dev libattr1-dev libblkid-dev libbsd-dev libcap-dev libcups2-dev libgnutls28-dev libgpgme-dev libjson-perl libldap2-dev libncurses5-dev libpam0g-dev libparse-yapp-perl libpopt-dev libreadline-dev nettle-dev perl perl-modules pkg-config python-all-dev python-crypto python-dbg python-dev python-dnspython python3-dnspython python-gpgme python3-gpgme python-markdown python3-markdown python3-dev xsltproc zlib1g-dev liblmdb-dev lmdb-utils samba krb5-config krb5-user winbind smbclient

Un utilisateur nommé « vmadvisor » a été créer au préalable afin d’administré le serveur en tant que client Windows 10.

L’installation du domaine se réalisera à partir de l’RFC 2307.

***Une documentation technique est mise en place à l’annexe 3.***

# Quesque SAMBA AD :

Le projet Samba est surtout connu pour le partage de fichiers selon le protocole SMB développé par Microsoft. La version 4 de ce logiciel apporte la fonctionnalité supplémentaire d'un contrôleur de domaine Active Directory (Active Directory Domain Controller - AD DC). Cette fonctionnalité inclue en natif les services DNS, LDAP, Kerberos, RPC et SMB 3.0 ainsi que la distribution et la gestion des GPO. Il simule depuis sa version 4 un serveur Windows 2008 R2.

# Mise en place du poste administrateur du réseau Windows 10 :

L’utilisateur « vmadvisor » précédemment créer permettra l’administration complète du serveur AD.

En premier lieu le client Windows 10 devra se connecter en Ethernet sur le VLAN 120 ainsi que de joindre le domaine FBMSRV.LOCAL précédemment mise en place.

Etant donné que le serveur AD est sous un système d’exploitation différent il devra se munir des fonctionnalité facultative RSAT\* (en GUI ou réalisable en ligne de commande) afin d’administrer le server Samba AD. L’ordinateur permettant d’administrer le serveur est à mettre entre la main d’un technicien agréer et non d’un utilisateur lambda.

Le poste administratif aura une IP qui lui sera attribuer par le DHCP et aura un DNS à incrémenter dans les paramètres réseau qui est (192.168.3.10).

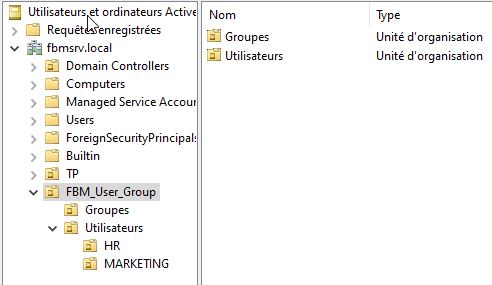
Fonctionnalité RSAT :

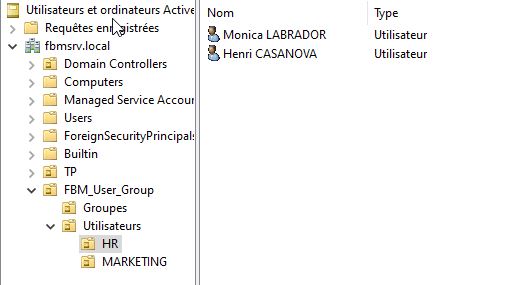
(Pas dans sa globalité)

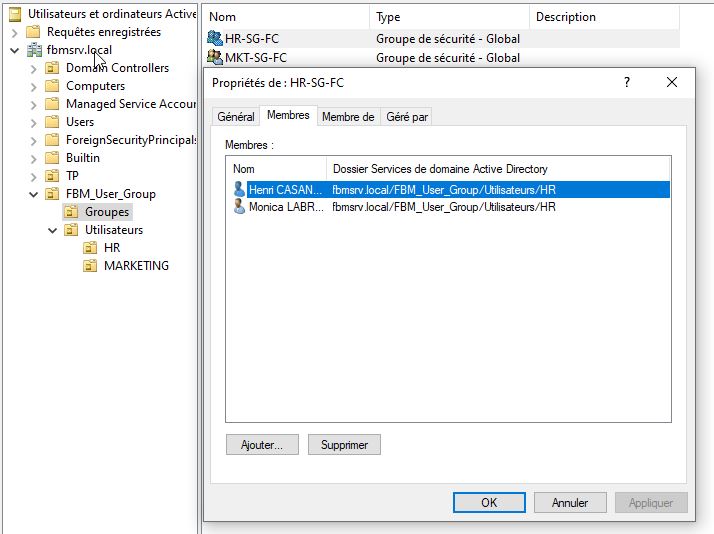
***Une documentation technique est mise en place à l’annexe 4.***

# Création utilisateurs et groupes :

Tout d’abord une nouvelle unité d’organisation sera créée sous le nom de FBM\_User\_Group. Deux sous-unités d’organisation y seront ajoutées, une pour les groupes et une pour les utilisateurs.

L’unité Utilisateurs se composera de deux sous-unité HR et Marketing, c’est ici que les utilisateurs seront créés.

Utilisateur HR étant membre du groupe HR-SG-FC (même chose pour les MARKETING) :

Membre du groupe HR-SG-FC :

***Une documentation technique est mise en place à l’annexe 5.***

# Mise en place d’un client Windows 10 sur le domaine :

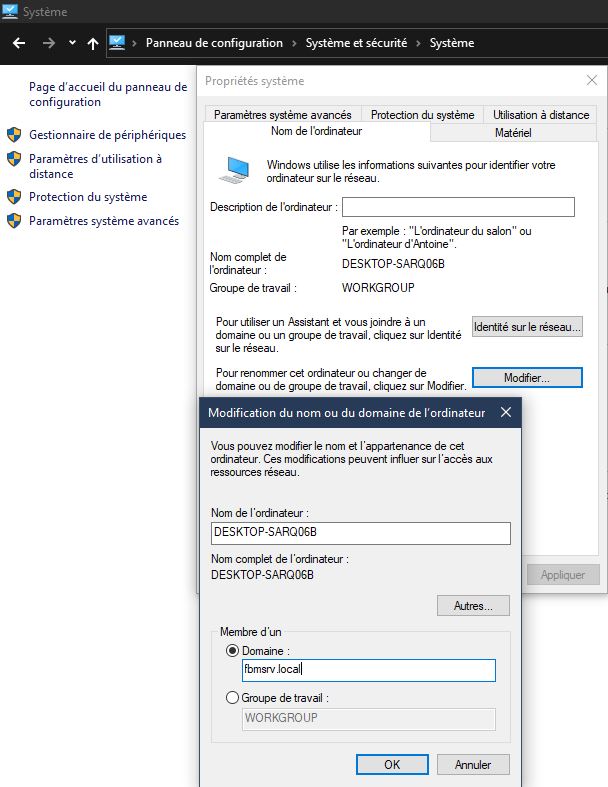
## Paramètre réseau :

Une fois connecter à l’utilisateur local « user1 » il est nécessaire de changer les DNS dans les paramètres réseau afin de pointer l’active directory.

## Entré dans le domaine :

Depuis le poste administrateur un utilisateur sous le nom de « Henri Casanova » sera créer afin de tester la conformité du service.

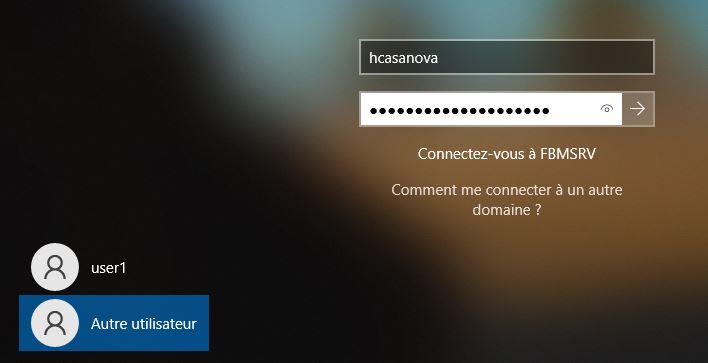
Le client Windows 10 rejoint le domaine fbmsrv.local via les paramètre système (Panneau de configuration\Système et sécurité\Système 🡪 modifier les paramètre 🡪 Modifier 🡪 Domaine). \*Une authentification administrateur est demander.



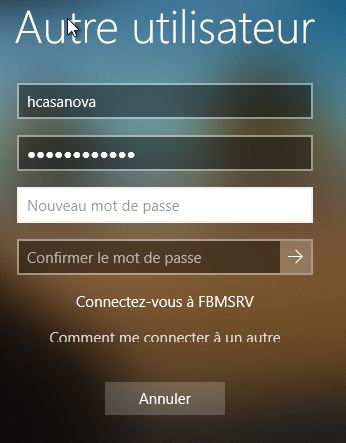
\*redémarrage nécessaire

## Connexion session utilisateur du domaine :

Une fois dans le domaine nous pouvons se connecter sur la session utilisateur précédemment créer sur l’active directory « Henry Casanova » (identifiant de connexion « hcasanova ».



Un changement de mot de passe vous sera demander si en créant l’utilisateur vous avez laisser les valeurs par défauts.



Après le mot de passe changer la connexion à la session s’exécute : 

***Une documentation technique est mise en place à l’annexe 6.***

# Partage de fichier TrueNas :

## Quesque TrueNas :

TrueNAS est un logiciel de stockage en réseau (NAS) qui partage et protège les données des menaces modernes comme les ransomwares et les logiciels malveillants. TrueNAS permet aux utilisateurs et aux appareils clients d’accéder facilement aux données partagées via pratiquement n’importe quel protocole de partage.

## Comment marche TrueNas :

TrueNAS protège les données de différentes manières en fonction de vos besoins domestiques ou professionnels. TrueNAS combine la redondance RAID, OpenZFS, la réplication, les instantanés, la réparation automatique de la corruption et la haute disponibilité en option, pour offrir une protection des données du centre de données.

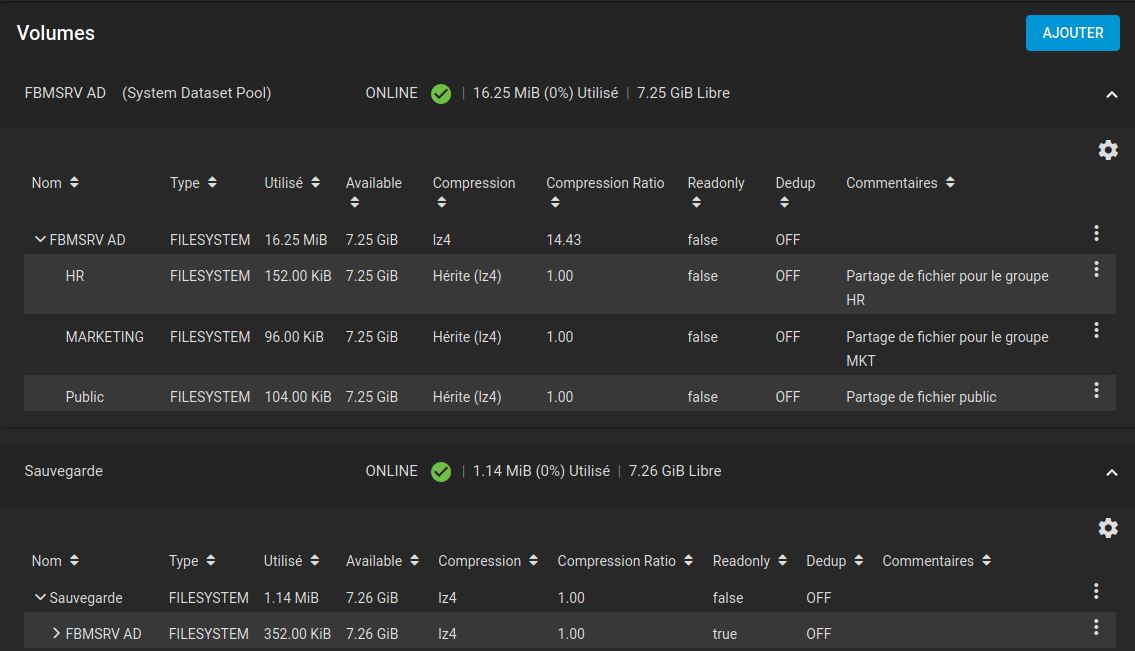
# Mise en place de TrueNas :

## Configuration de TrueNas :

|  |  |
| --- | --- |
| Processeur | Intel Core i5 |
| Système d’exploitation | TrueNas 12 |
| Ram | 16Gb DDR3 |
| Stockage | SSD 120Gb  2x 2TO |
| Domaine | FBMSRV.LOCAL |
| Réseau | 192.168.3.130/24 |
| Volume | * Volume 1 (Partage) * Volume 2 (Backup) |
| Tache | Réplication tous les dimanche soir à 00h00 |
| Partage | * Dossier Public (Pour tous) * Dossier HR (Ressource humaine) * Dossier MARKETING (Maketing) |
| Protocole | SMB |

TrueNas possède une IP fixe 192.168.3.130/24 et est connecter au domaine FBMSRV.LOCAL.

Deux grands volumes primaires, le premier permettant le partage de quatre dossiers et le secondaire permettant de répliquer le premier disque donc un disque BACKUP.

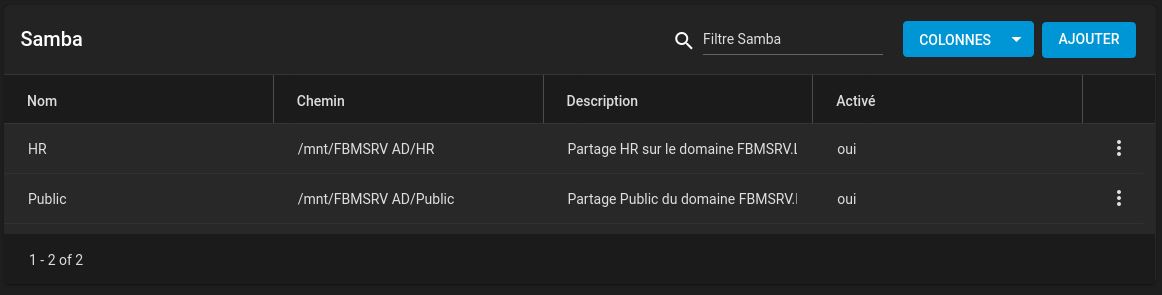


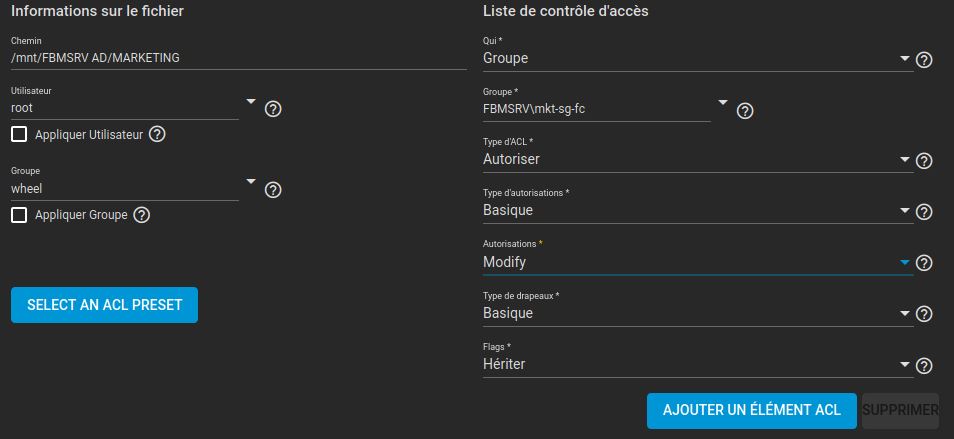
Le dossier Public qui est accessible à tous les utilisateurs du domaine en mode modification.

Le dossier HR est accessible seulement aux l’utilisateurs fessant parti du groupe HR et est bloquer d’accès à l’administrateur.

Le dossier MARKETING est seulement accessible aux utilisateurs fessant parti du groupe MKT et est bloquer d’accès à l’administrateur.

Le dossier sauvegarde permet d’accès au volume de sauvegarde et est réserver à l’administrateur personne d’autre ne peut y accéder.

Les trois dossiers sont partagés grâce au protocole SMB :

TrueNas permet aussi de lui-même définir des ACL (autorisation) sur son interface en étant connecter au domaine dans l’exemple si dessous c’est le dataset (dossier qui est partage ensuite) MARKETING qui est seulement autoriser pour les membres du groupe MKT-SG-FC en modification :

***Une documentation technique est mise en place à l’annexe 7.***

# Mise en place des GPO :

## Déploiement des lecteurs réseau :

## Déploiement logiciel :

# Méthode de sauvegarde :

Truenas replication