

PROJET EVOLUTION



Romain DEMOLLIERE

Franck CESAR

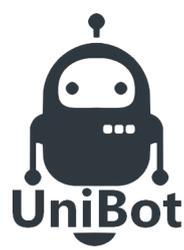
Gabriel ARGENTIERI



TABLE DES MATIERES

Table des matières

- 1. Introduction..... 3
 - 1.0 Présentation de l’entreprise..... 3
 - 1.1 Organigramme..... 3
 - 1.2 Objectifs 3
 - 1.3 Cahier des charges..... 4
 - 1.4 Distribution des tâches..... 5
 - 1.5 Architecture du réseau..... 6
 - 1.6 Solution RAID..... 7
 - 1.7 Back up en Cloud 8
 - 1.8 Plan d’adressage..... 9
- 2. Matériels 10
 - 2.0 Choix des serveurs..... 10
 - 2.1 Choix du système Windows 11
 - 2.2 Choix du système Linux 11
- 3. Serveurs Windows..... 11
 - 3.0 Active directory 11
 - 3.1 DNS..... 12
 - 3.2 DHCP..... 12
 - 3.3 Serveur d’impression..... 12
 - 3.4 Stratégies de groupe 13
 - 3.5 Solution d’accès à distance 15
 - 3.6 Scripts 15
- 4. Serveurs Linux 15
 - 4.0 Debian 15
 - 4.1 Samba 15
 - 4.2 Serveur NFS 16
 - 4.3 Serveur FTP..... 16
 - 4.4 GLPI..... 16
- 5. Conclusion 17



6.	Annexes	18
6.0	Nommage des machines	18
6.1	Politique de mot de passe	18
6.2	Plan des bâtiments	19
6.3	Installation des services Windows	24
6.3.1	Installation contrôleur de domaine physique DC0.....	24
6.3.2	Installation des hyperviseurs physiques.....	28
6.3.3	Installation du serveur physique ISCSI	29
6.3.4	Installation du cluster de basculement	35
6.3.5	Installation du DHCP.....	40
6.3.6	Serveur d'impression.....	45
6.3.7	Stratégies de mot de passe	48
6.3.8	Horaires d'accès	49
6.3.9	Modification de l'horloge	49
6.3.10	Désactivation lecteur CD	50
6.3.11	Lecteurs réseau	51
6.4	Installation des services Linux	56
6.4.1	Installation de Debian	56
6.4.2	Configuration du Debian	61
6.4.3	Samba	63
6.4.4	NFS.....	66
6.4.5	FTP	67
6.4.6	GLPI.....	68
6.5	Scripts	72
6.6	Devis	75



1. Introduction

1.0 Présentation de l'entreprise

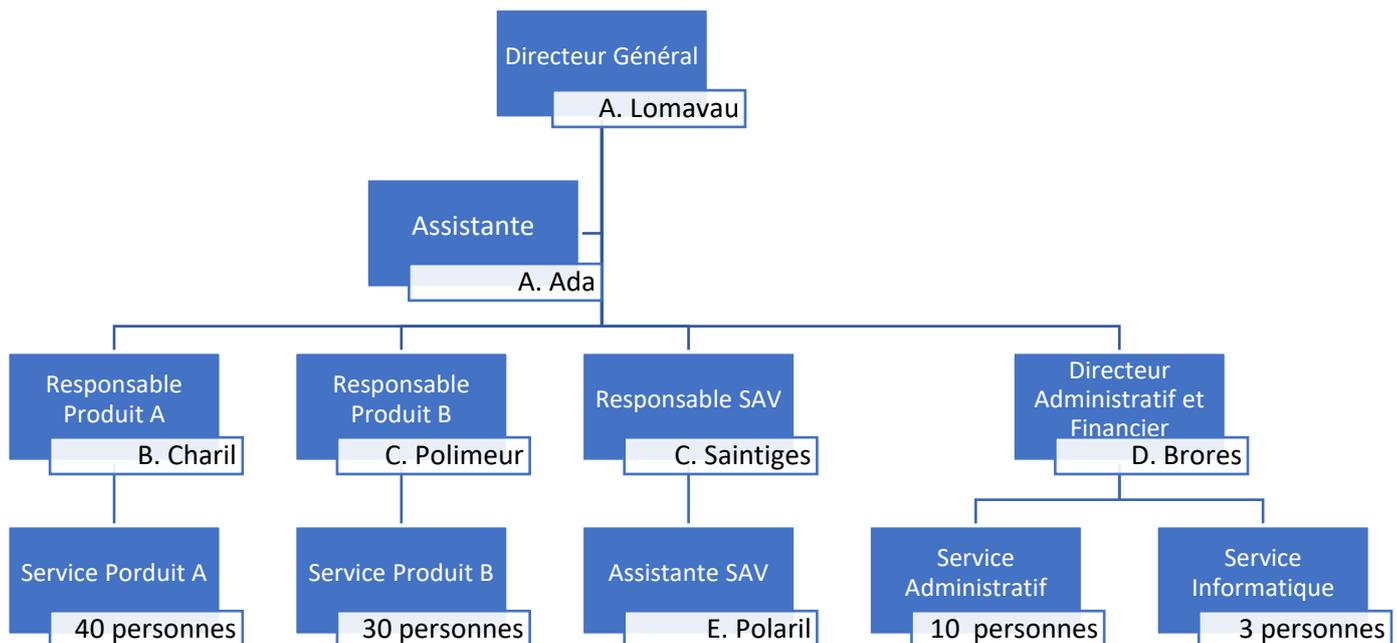
La société « UniBot » est une centrale d'achat qui s'occupe de la distribution de deux modèles de robots IA pour l'assistance humaine.

Créé en 2003, son siège est basé à Ecully (19 Avenue Guy de Collongue, 69130) et compte plus de 90 salariés.

Il y a 6 mois, notre entreprise venait d'acquérir un nouveau site, composé de 3 bâtiments, nous sommes en charge de la mise en place du réseau informatique.

1.1 Organigramme

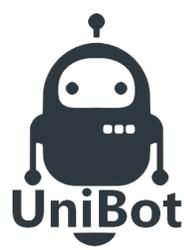
Nous rappelons l'organigramme de l'entreprise qui est composé de 90 personnes :



1.2 Objectifs

Nous devons administrer un parc informatique et pour celui-ci nous avons donc plusieurs objectifs à atteindre :

- Mettre en œuvre les outils d'administration de Windows server.
- Mettre en œuvre les outils d'administration UNIX/LINUX.
- Être capable de sécuriser l'accès au réseau et aux données de l'entreprise.
- Savoir rédiger des rapports écrits adaptés au contexte professionnel.
- Être capable d'automatiser les tâches à l'aide d'un outil de programmation.
- Être capable de créer et gérer une base de données relationnelle.



1.3 Cahier des charges

Dans le but d'optimiser notre réseau informatique au sein de la société, le directeur administratif et financier nous a soumis un cahier des charges.

- Notre équipe informatique se trompe souvent de salle lors de dépannages auprès des utilisateurs, nous n'avons aucune information sur le suivi du matériel actuel sur le parc.
- Il n'y a pas de gestion de droits utilisateurs.
- Le siège social à besoin d'un serveur ftp afin de récupérer des fichiers, un serveur linux sera mis en place.
- L'implémentation de l'Active Directory dans l'entreprise
- Nous avons 6 sessions pour faire aboutir le projet.
- Le DAF souhaite avoir un compte rendu mensuel sur l'avancée du projet.
- Il souhaite également un rapport d'activité globale sur la faisabilité et les solutions mises en place suivant le cahier des charges, les procédures d'installation, de déploiement en suivant la charte de l'entreprise.



1.5 Architecture du réseau

Notre architecture réseau sera composé de 4 serveurs physiques :

- Un serveur sous Windows Server 2016 en tant que contrôleur de domaine principal (EVO-X-N01).
- Un serveur sous Windows Server 2016 en tant qu'hyperviseur pour le fonctionnement du cluster (EVO-X-HV01).
- Un second serveur sous Windows Server 2016 en tant qu'hyperviseur pour le fonctionnement du cluster (EVO-X-HV02).
- Un quatrième serveur sous Windows Server 2016 en tant que SAN ISCSI pour le stockage des machines virtuelles Hyper-V (EVO-X-ISCSI01).

Sur le SAN ISCSI est hébergé 4 machines virtuelles, géré directement sur les deux hyperviseurs :

- Une machine virtuelle sous Windows serveur 2016 servant de contrôleur de domaine et de serveur DNS de secours si le serveur physique tombe en panne.
- Une machine virtuelle sous Windows serveur 2016 en tant que serveur d'impression.
- Une machine virtuelle sous Debian 10 configuré en tant que serveur web, serveur ftp et serveur Nfs.
- Une machine virtuelle sous Debian 10 configuré en tant que client Nfs et serveur web.

Chaque machine physique est installée avec l'OS Windows Server 2016

1^{er} serveur physique :

SERVEUR PHYSIQUE EVO-X-N01 (DC01)	Active Directory DNS
--------------------------------------	-------------------------

2^{ème} serveur physique :

SERVEUR PHYSIQUE EVO-X-ISCSI01 (ISCSI)	Serveur de fichier ISCSI (Stockage des VM)
---	---



3^{ème} serveur physique :

SERVEUR PHYSIQUE EVO-X-HV01 (Hyperviseur 01)	
Hyper-V (Gestionnaire de cluster de basculement)	
EVO-V-N01	Active Directory
	DNS
	DHCP
EVO-V-N02	Serveur d'impression
	Serveur de partage
EVO-V-N03	Samba
	Serveur FTP
	Serveur NFS
EVO-V-N04	Serveur Web
	Client NFS

4^{ème} serveur physique :

SERVEUR PHYSIQUE EVO-X-HV02 (Hyperviseur 02)	
Hyper-V (Gestionnaire de cluster de basculement)	
EVO-V-N01	Active Directory
	DNS
	DHCP
EVO-V-N02	Serveur d'impression
	Serveur de partage
EVO-V-N03	Samba
	Serveur FTP
	Serveur NFS
EVO-V-N04	Serveur Web
	Client NFS

1.6 Solution RAID

Dans un serveur, les données sont contenues dans les disques qui peuvent tomber en panne à tout moment. Afin de préserver les données et la productivité de notre entreprise, nous avons mis en place 4 disques par serveurs montés en raid 5.

Dès lors qu'un disque est amené à être hors-service, le serveur va continuer de fonctionner normalement.

Il nous suffit de remplacer le disque défaillant et le contrôleur RAID s'occupera de l'inclure dans le RAID à l'identique. Pendant tout ce temps, les données sont disponibles normalement avec quelques ralentis.

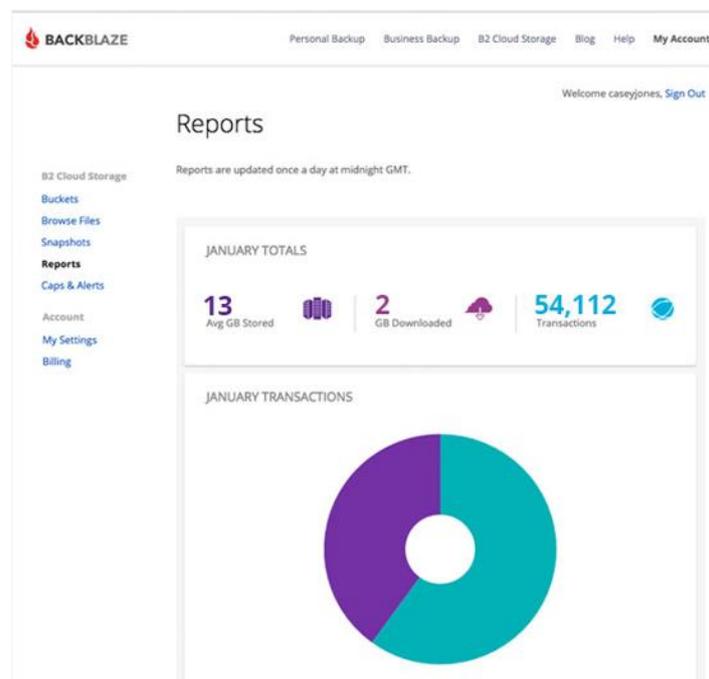
Le devis pour 16 disques de 1To et 2 disques en stock se trouve en annexe.

1.7 Back up en Cloud

Concernant la sauvegarde de données des machines virtuelles hébergé sur notre serveur physique ISCSI, notre choix s'est orienté vers l'outil BackBlaze.



Et plus spécifiquement, sa solution B2 Cloud Storage, qui permet une sauvegarde complète des serveurs. Le tout est administré grâce à une application en interface Web. Ce qui nous permettra une meilleure gestion de l'automatisation des backups. L'édition de rapports et la programmation d'alerte permettent une supervision beaucoup plus ciblée.



Cette solution payante fournit un stockage illimité ainsi qu'une sauvegarde intégrale des données. Nous pouvons également choisir nous-même la vitesse de téléchargement ou la limiter automatiquement si vous ne voulez pas sacrifier toute votre bande passante pour la sauvegarde en ligne. BackBlaze utilise SSL et AES pour le chiffrement. De plus, une authentification à deux facteurs est intégrée au logiciel.



Deux caractéristiques spéciales distinguent BackBlaze : d’une part, il y a les modules de sauvegarde auto-construits. Avec les Storage Pod, nous pouvons créer notre propre matériel. Les plans de construction sont open source et sont offerts gratuitement par BackBlaze dans son blog qui est librement accessible.

Le cloud permet d’avoir une copie dématérialisée de ses fichiers les plus sensibles, que l’on peut restaurer en cas d’incident. On peut aussi tout simplement manquer d’espace local et utiliser ces services pour y stocker ses documents, et assurer ainsi une sauvegarde fiable et accessible à n’importe quel moment. Mais BackBlaze vous propose aussi de vous envoyer les données sous la forme d’une mémoire flash de 128 Go ou d’un disque dur de 4 To.

Provider	Storage (\$/GB/Month)	Download (\$/GB)
BACKBLAZE	\$0.005	\$0.01
amazon S3	\$0.021 +320%	\$0.05+ +400%
Microsoft Azure	\$0.018+ +260%	\$0.05+ +400%
Google Cloud	\$0.020 +300%	\$0.08+ +700%

1.8 Plan d’adressage

Dans un réseau informatique, il est important de déterminer un adressage IP, afin d’organiser et mettre en place correctement ce réseau et éviter différents conflits, voici un tableau récapitulatif du réseau :

Utilisation	Plage IP		IP utilisable
	Première IP	Dernière IP	
Serveurs	192.168.1.1	192.168.1.30	30
Imprimantes	192.168.1.31	192.168.1.40	10
Ordinateurs	192.168.1.41	192.168.1.240	200
Adresses IP disponibles	192.168.1.241	192.168.1.254	14

Nous avons choisi la plage d’adressage 192.168.1.0/24 afin de disposer de 254 adresses.



Serveurs : Nous disposerons de 30 adresses IP fixe pour l'ensemble des appareils du réseau, cela est suffisant pour prévoir une éventuelle évolution.

Imprimantes : Nous avons besoin d'une imprimante par service, avec un total de 6 imprimantes, nous disposerons donc de 10 adresses IP fixe pour l'ensemble des imprimantes du réseau, cela est suffisant afin de prévoir un ajout supplémentaire d'imprimantes.

Ordinateurs : Nous avons prévu une marge d'adresse IP afin de prévoir une évolution possible du nombre de postes. Ces adresses seront distribuées automatiquement par le biais de notre serveur DHCP, nous disposerons donc de 200 adresses IP dans la plage DHCP, pour le moment, 90 adresses IP seront utilisés.

Dans le cadre d'un ajout de matériel supplémentaire, nous disposons de 14 adresses IP vacantes.

2. Matériels

Nous allons mettre en place plusieurs serveurs pour notre infrastructure, avant cela nous allons définir les besoins de l'entreprise.

Concernant ces serveurs, nous avons décidé d'utiliser la virtualisation pour optimiser la puissance. Nous allons donc faire l'acquisition de 4 machines qui hébergeront des machines virtuelles.

2.0 Choix des serveurs

Pour le choix des serveurs, nous avons comparé entre deux marques très connues pour leurs serveurs : Lenovo et HP.

Marque	Lenovo	HP
Modèle	ThinkSystem ST250 (7Y45A02BEA)	HPE ProLiant ML110 Gen10 (P03685-425)
OS	Sans OS	Sans OS
Processeur	Intel Xeon E-2124 (Quad-Core 3.3 GHz / 4.3 GHz Turbo - Cache 8 Mo)	Intel Xeon Bronze 3106 (Octo-Core 1.7 GHz - Cache 11 Mo)
RAM	16 Go	16 Go
Disques	Sans Disques	Sans Disques
Nb de baies pour disques	4	8
Prix HT (à l'unité)	999,13 €	1374,96 €
Prix TTC (à l'unité)	1198,95 €	1649,95 €
Garantie	3 ans	1 an

Après comparaison, nous avons choisi le modèle de la marque LENOVO car c'est une bonne marque, le produit est moins cher pour l'utilisation que nous allons en faire et ce modèle



dispose de 3 ans de garantie comparée à celui de HP qui n'a qu'un an de garantie. Le devis pour 4 serveurs se trouve en annexe.

2.1 Choix du système Windows

Nous avons choisi d'installer Windows Server 2016 car il s'agit de la version la plus récente et la plus pratiquée dans notre service informatique. En effet Windows Server 2012 ne possède pas les nombreux avantages que propose Windows server 2016 et la version 2019 propose de nouvelles fonctionnalités mais inutiles pour notre projet, ce qui augmenterait le coût global.

2.2 Choix du système Linux

Afin de choisir le système linux adapté à notre infrastructure, nous avons fait un comparatif entre deux grandes distributions : CentOS et Debian

Voici quelques avantages de l'utilisation de CentOS :

Elle est basée sur une solution commerciale de qualité stable et qui est testée avant de la rendre disponible au public.

Quant à Debian, il est très stable et sans bug, et dispose d'un support large de l'architecture, mais il présente un cycle lent de mises à jour, mais plus rapide que CentOS.

Nous avons donc choisi la distribution Debian car nous avons plus de connaissances dans cette distribution afin de la paramétrer correctement.

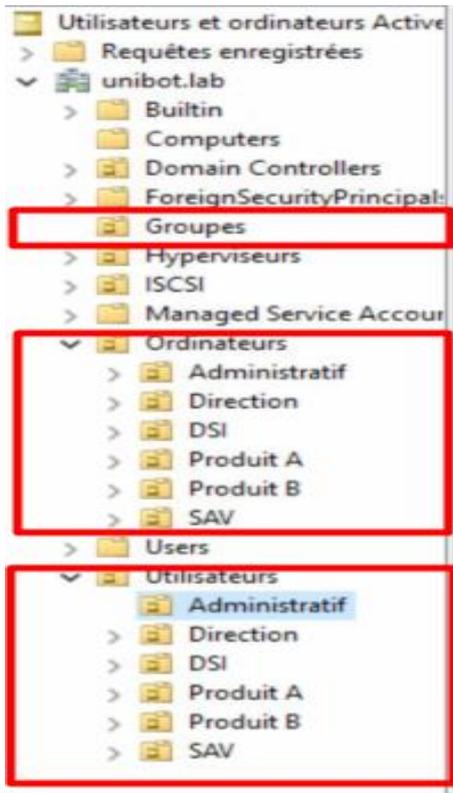
3. Serveurs Windows

3.0 Active directory

L'active directory qui est plus communément appelé AD, est un annuaire qui répertorie et organise les informations concernant les utilisateurs les machines ou les applications d'une entreprise, elle a pour but d'apporter une meilleure gestion du parc informatique.

L'AD permet aux utilisateurs une fois connecter de retrouver et accéder à une ressource du réseau et nous permet aussi de paramétrer des stratégies de groupe (ordinateurs et utilisateurs) qui permettent une gestion précise.

Dans notre cas, nous avons créé des OU (unité organisationnelle)



3.1 DNS

Un serveur DNS (Domain Name System) est un service utilisé pour traduire les noms de domaine en adresse IP.

Le serveur DNS est un rôle important car il permet de faire communiquer toutes les machines entre elles facilement avec le nommage du matériel.

3.2 DHCP

Le DHCP est un protocole qui permet à un périphérique qui se connecte au réseau d'obtenir automatiquement une configuration réseau, le but étant de faciliter l'administration d'un réseau.

Dans notre cas, nous utiliserons le service DHCP sur notre machine virtuelle n°1 sous Windows Server 2016.

Le plan d'adressage a déjà été expliqué la partie Plan d'adressage,

- Les adresses comprises entre 192.168.1.41 et 192.168.1.240

3.3 Serveur d'impression

Un serveur d'impression est une application logicielle, un périphérique réseau ou un ordinateur qui gère les demandes d'impression et rend les informations d'état de la file d'attente d'imprimantes accessibles aux utilisateurs finaux et aux administrateurs réseau. Les serveurs d'impression sont utilisés dans les réseaux des Grandes Entreprises, PME (petites et moyennes entreprises), TPE (très petite entreprise).



- Économise d'espace

Plus besoin d'acheter une imprimante dédiée pour chaque utilisateur, vous pouvez donc économiser de l'espace, de l'électricité et des coûts de maintenance.

- Installation rapide

Ajoutez une imprimante à votre réseau en quelques minutes. Pas besoin d'éteindre votre réseau.

- Éviter les files d'attente ou les retards

Si une imprimante est utilisée avec un gros travail d'impression, un utilisateur peut éviter la file d'attente en utilisant une autre imprimante. Cela pourrait être une solution pour une tâche urgente qui devrait être imprimée en moins de 5 minutes.

- Partage de l'imprimante serveur / poste de travail

Les imprimantes sont configurées sur le serveur et sont ensuite déployé sur les postes.

Voici la liste des imprimantes de l'entreprise :

- 192.168.1.31: PrintDirection
- 192.168.1.32: PrintSAV
- 192.168.1.33: PrintDSI
- 192.168.1.34: PrintProduitA
- 192.168.1.35: PrintProduitB
- 192.168.1.36: PrintAdministratif
- 192.168.1.37: PrintAll

3.4 Stratégies de groupe

Plusieurs stratégies sont à créer :

- Stratégie de mot de passe :

Le mot de passe doit répondre aux exigences de complexité et doit faire au minimum 8 caractères, vous trouverez plus d'informations dans la partie politique de mot de passe de l'annexe.

- Autorisations de connexion selon les horaires



Mme BEZIAT, ELLA, AYO et ACIEN ne peuvent se connecter qu'entre 08 heures et 18 heures et à 19 heures elles doivent être déconnectées (elles sont du service Produit A)

Aucun salarié sauf la direction, le SAV et l'informatique ne peut se connecter entre 20 heures et 07 heures du matin

- Installation des logiciels

En dehors de la direction, des services informatiques, personne ne peut installer de logiciels sur sa machine.

- Modification de l'heure :

En dehors de la direction, des services informatiques, personne ne peut modifier l'heure.

- Gestion de l'espace disque :

Chaque utilisateur a droit à 5Go sur le disque, et nous devons mettre en place des alertes en cas de dépassement.

- Lecteurs réseaux

Chaque service doit avoir un répertoire nommé « Communservice » qui sera attribué à chacun des salariés lors de sa connexion réseau.

A l'intérieur de chaque répertoire, vous créez un dossier pour chaque salarié (contrôle total sur celui-ci et aucun accès sur ceux des collègues).

Seuls la direction et l'informatique peuvent y accéder en plus (juste lire pour la direction).

Attribuer un dossier de base à 2 users locaux au choix.

Attribuer un dossier de base à 2 users du domaine au choix.

Planifier 2 audits au hasard.

Configurer au moins 3 journaux à 3 jours.

- Serveur d'impression

Il faut 1 imprimante pour chaque service nommée Printnom du service.

Une imprimante réseau pour tout le monde (les services Produit 1 et 2 ne peuvent imprimer qu'entre 8 heures du matin et 17 heures).

La direction sont prioritaires sur toutes les impressions et les utilisent 24/24.

Le service informatique a contrôle total sur toutes les impressions.

Mme. LAPORTE et Mlle ADA (les assistantes des services SAV et direction peuvent imprimer chez les Services Informatique, Service Produit A et B.



3.5 Solution d'accès à distance

Pour la solution d'accès à distance, nous allons procéder à l'installation de l'outil OpenVPN sur notre machine virtuelle linux 4 (EVO-V-N04)

Pourquoi utiliser OpenVPN pour l'accès à distance ?

- Il est open source et fiable.
- Il est gratuit.
- Il est compatible Windows et linux.

Le serveur sera installé sur notre machine linux afin d'avoir une meilleure maniabilité sur les configurations.

Le client OpenVPN devra alors être installé sur les postes.

3.6 Scripts

Nous avons mis en place des scripts afin de gérer facilement l'administration serveur.

- Un script pour la création d'utilisateurs depuis un fichier CSV.
- Un script afin d'ajouter des utilisateurs dans les groupes en fonction de leur service.

4. Serveurs Linux

4.0 Debian

Nous utilisons couramment ce nom pour désigner la distribution GNU/Linux de debian, mais depuis 2013, d'autres distributions sont en développement comme Debian GNU/Hurd. Debian est une communauté dont le but est le développement de systèmes d'exploitations avec des logiciels libres. Nous avons choisi cette distribution car c'est celle que l'on connaît mieux.

Voici une liste des paquets que nous aurons à installer :

- krb5-user
- sssd
- samba
- proftpd
- nfs-kernel-server

4.1 Samba



Samba est un logiciel d'interopérabilité (ce qui signifie qu'il fonctionne sous différents systèmes d'exploitation) qui ajoute le protocole propriétaire SMB/CIFS de Windows dans les



ordinateurs fonctionnant sous Linux (ou un de ses dérivés). Il permet aux ordinateurs d'un réseau d'avoir accès aux imprimantes et aux fichiers des ordinateurs sous Unix.

4.2 Serveur NFS

NFS (Network File System) est un protocole développé par Sun Microsystems en 1984 de partage de répertoires sous Linux. Il permet à un ordinateur d'accéder à un système de fichiers à distances par le réseau. Ce dernier permet de partager essentiellement des données entres systèmes Unix, mais existe aussi pour Macintosh ou Windows

4.3 Serveur FTP



Le serveur FTP (File Transfer Protocol) permet de transférer des fichiers par le biais d'un réseau informatique et plus exactement entre un serveur et un fichier. On parlera donc de client et de serveur ftp. Le premier va envoyer une demande au second, qui après vérification des droits (sur le fichier et ceux du client), accepte ou non la demande.

. Nous avons choisi d'utiliser ProFTPD qui est un serveur libre. Ce dernier offre plusieurs avantages comme l'application de quota, la limitation d'accès via chroot et son contrôle précis des partages et des droits. Nous utiliserons Filezilla comme client FTP qui est le plus connu et le plus utilisé des clients FTP.

4.4 GLPI

	GLPI	OCS INVENTORY	RG SUPERVISION	SCCM
OS COMPATIBLE	WINDOWS, LINUX, ANDROID,	WINDOWS, LINUX, ANDROID, MAC OS	WINDOWS, LINUX, ANDROID	WINDOWS, LINUX, ANDROID, MAC OS, IOS
INVENTAIRE				
ORDINATEUR	✓	✓	✓	✓
TABLETTE	✓	✓	✓	✓
DEVIce	✓	✗	✓	✗
CREATION DE TICKET D'INCIDENT	✓	✗	✓	✗
CREATION DE RAPPORT, STATISTIQUE	✓	✗	✓	✗
TELEDIFFUSION	✓	✓	✓	✓
LICENCE	GRATUIT	GRATUIT	PAYANT	PAYANT
CLOUD	✗	✗	✓	✗
SUPERVISION	✗	✗	✓	✗
SUPPORT	COMMUNAUTE	COMMUNAUTE	EDITEUR DU LOGICIEL	EDITEUR DU LOGICIEL
LOCALISATION PHYSIQUE DES UTILISATEURS	✓	✗	✗	✗



Logiciel libre de gestion des services informatiques, glpi signifie gestion libre de parc informatique. Etant une technologie libre, toute personne peut modifier, développer le code pour proposer des améliorations à toute la communauté de ce service. C'est une application web qui permet aux entreprises de gérer plus facilement les systèmes d'informations. Cette dernière contient de nombreuses fonctionnalités : créer et gérer des tickets pour signaler des problèmes, faire l'inventaire des machines ainsi que leur composants et logiciels.

5. Conclusion

Notre objectif était de mettre en place des solutions dans le but de centraliser les ressources de l'entreprise et de faciliter l'administration des utilisateurs. Pour se faire, nous avons mis en place quatre serveurs pour installer un cluster, ainsi que deux Windows serveur 2016 et deux serveurs linux avec de nombreuses fonctionnalités.

Ce cluster nous permet une redondance ainsi qu'un système de basculement, ce qui permet aux serveurs de fonctionner même s'il y a un dysfonctionnement.

Nous avons utilisé un maximum de logiciels libres pour réduire les dépenses liées au projet, cependant, nous avons utilisé des logiciels propriétaires pour avoir un confort au niveau de la sécurité.

Pour ce projet nous avons dépensé au total (il faut rajouter le prix de blackblaze, mais il est minime) :

Coût des serveurs	4861,80 €
Coût des licences	5039,64€
Coût des disques	1505,04€
Coût de blackblaze	XGo*0,0\$
Coût total	11406,49€



6. Annexes

6.0 Nommage des machines

Périphérique	Nommage type	Exemple
Nommage des PC	EVO-D-BXXXXNXX	EVO-D-B1205N35
Nommage des Imprimantes	EVO-P-BXXXXNXX	EVO-P-B2210N12
Nommage des Serveurs	EVO-X-NXX	EVO-X-N02
Nommage des Hyperviseurs	EVO-X-HVXX	EVO-X-HV01
Nommage des ISCSI	EVO-X-ISCSIXX	EVO-X-ISCSI01
Nommage des VM	EVO-V-NXX	EVO-V-N03

BXXXX correspond au numéro du bâtiment et de la salle :

- Exemple : B1105 > Bâtiment 1, Etage 1, Salle 05.

NXX correspond au numéro de l'équipement :

- Exemple : N05 > 5^{ème} équipement.

6.1 Politique de mot de passe

La protection de l'information nécessite des systèmes de sécurité telle que l'utilisation de mots de passe suffisamment difficiles pour être retrouvés par un robot ou une tierce personne. L'utilisation d'un mot de passe unique et régulièrement mis à jour est recommandée, ce qui nécessitera une réinitialisation régulière. Il est également conseillé d'éviter de stocker ces mots de passe dans la base de données de l'ordinateur.

Pour permettre une protection optimale, le mot de passe devrait pouvoir être référencé de la manière suivante :

- Un minimum de 8 caractères pour limiter les risques de récupération du mot de passe de la part d'un tiers.
- Comporter au moins un chiffre, une lettre et un caractère spécial.
- Différent des informations suivantes : Nom/Prénom/Date de Naissance de l'utilisateur ou de l'un de ses proches.

Pour une protection maximale des mots de passes, un ensemble de règles sont à prendre en compte et s'y tenir pour ne pas avoir de fuite.

- Ne pas communiquer son mot de passe par téléphone ou mail sans l'accord du service informatique ;



- Se déconnecter de l'ordinateur ou verrouiller votre session Windows avant de quitter l'ordinateur ;
- Empêcher le navigateur de stocker les mots de passe dans la base de données ;
- Activer la double authentification si le service le permet.

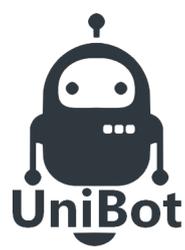
Pour terminer, le mot de passe d'un compte devrait être changé tous les 3 mois. En cas d'échec d'authentification du mot de passe à plusieurs reprises, le compte sera désactivé jusqu'à réactivation du compte avec réinitialisation du mot de passe par le service informatique

6.2 Plan des bâtiments

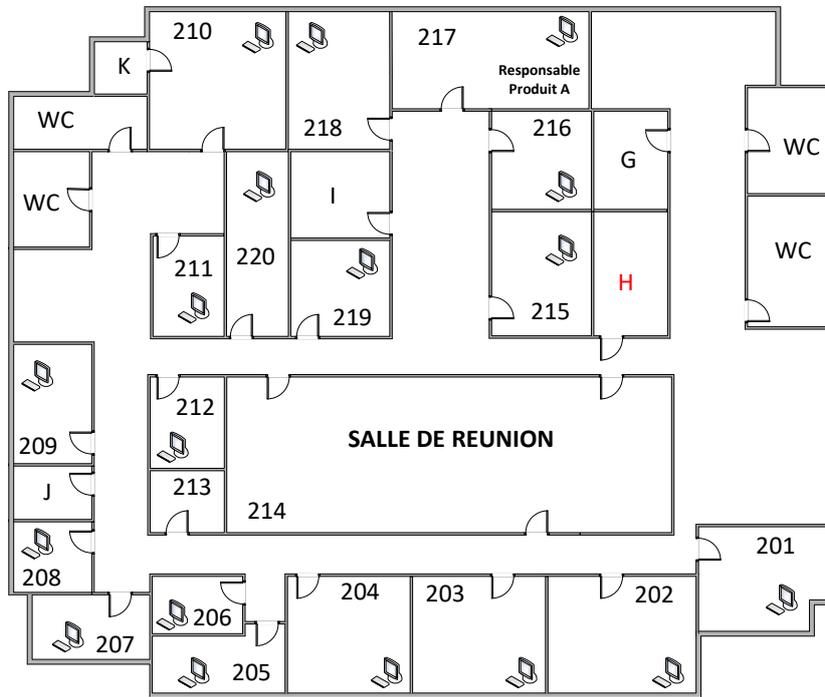
Bâtiment 1 :

- Rez-de-chaussée :



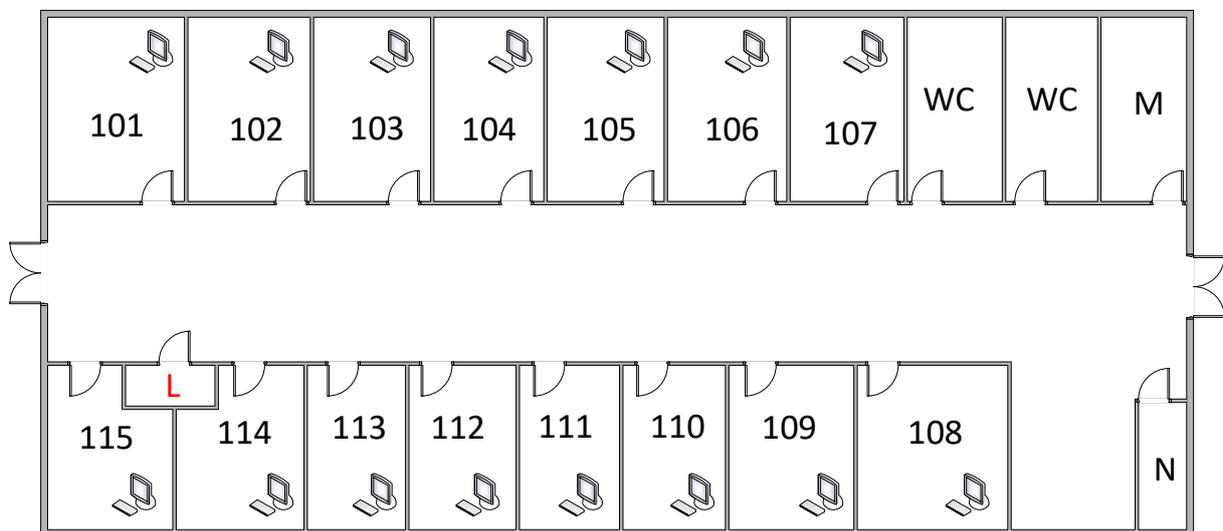


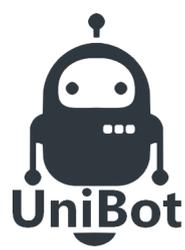
- Etage 1 :



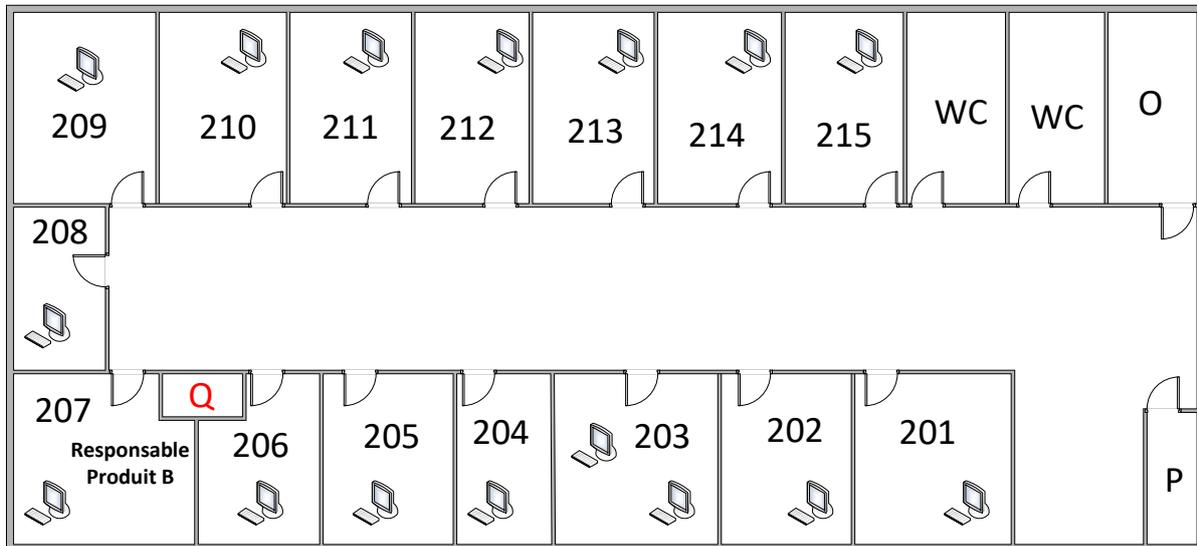
Bâtiment 2 :

- Rez-de-chaussée :



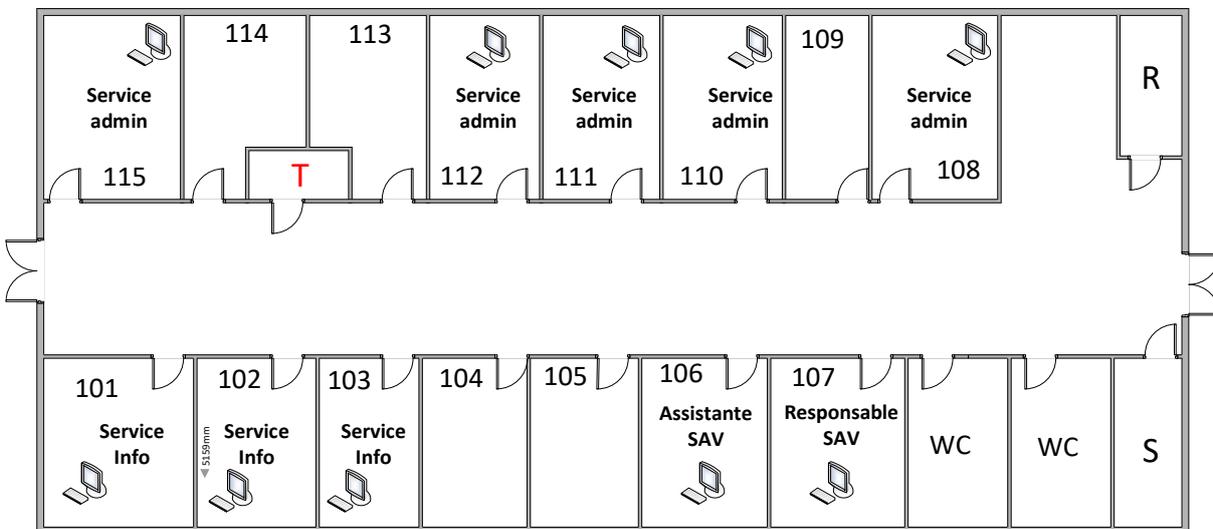


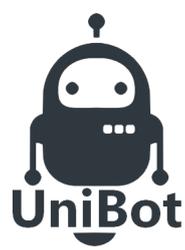
- Etage 1 :



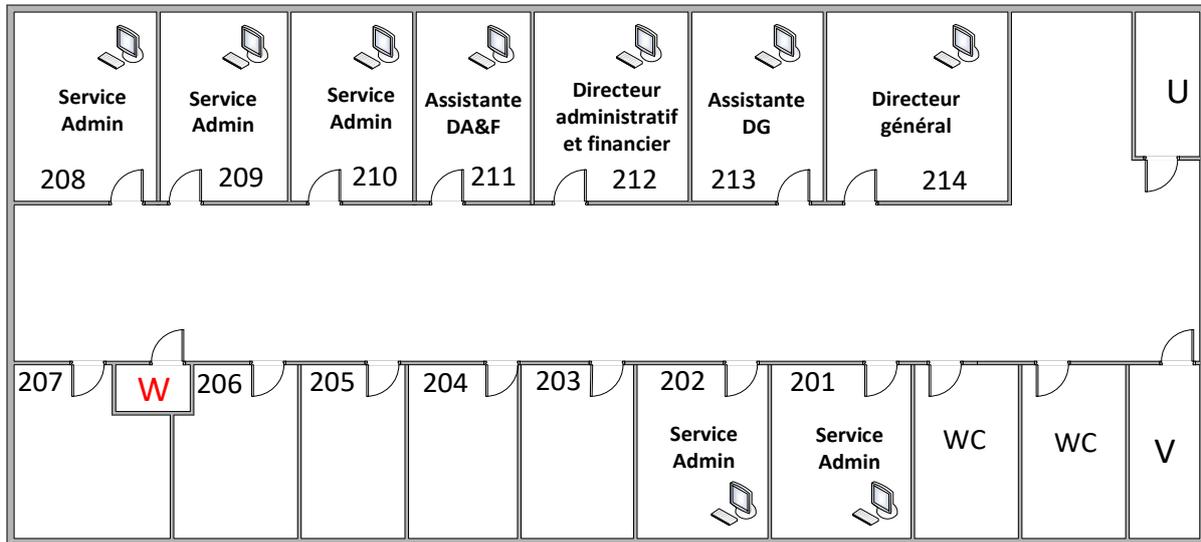
Bâtiment 3 :

- Rez-de-chaussée :



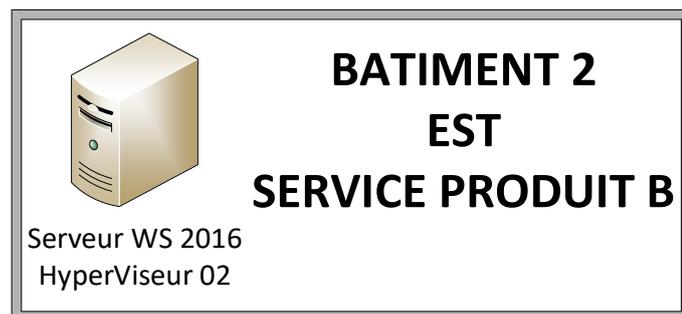
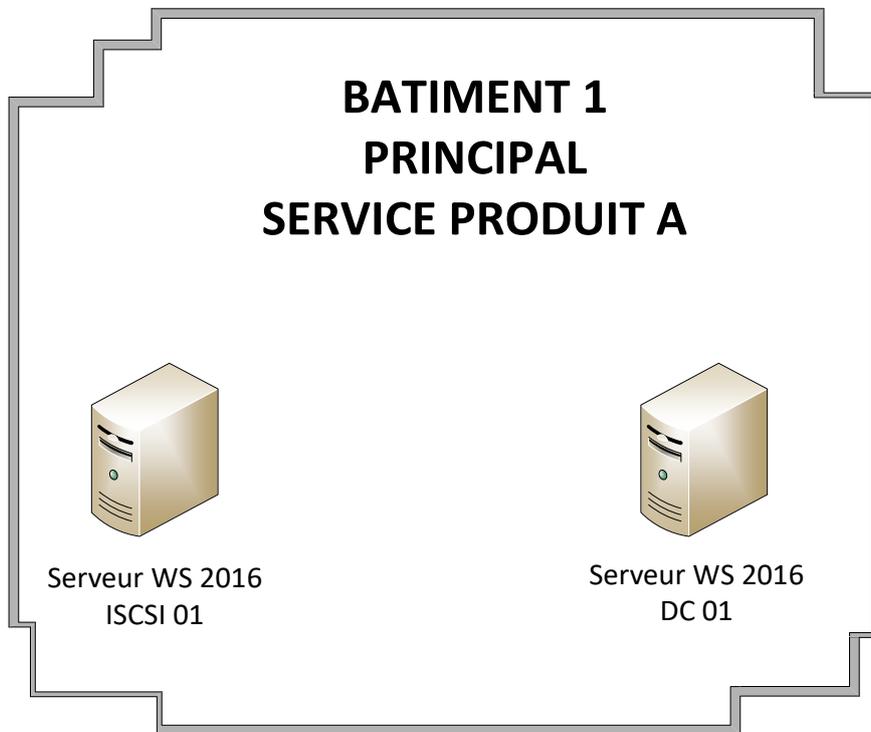
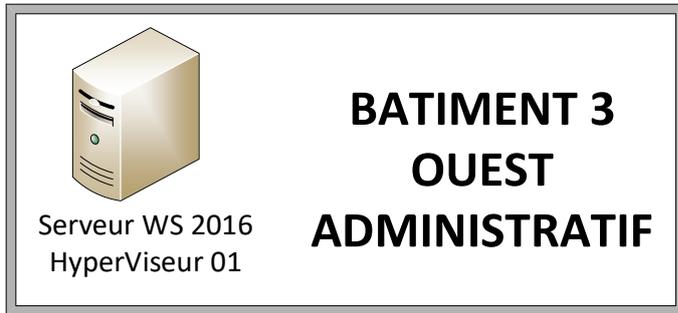


- Etage 1 :





Disposition des serveurs physique sur l'ensemble des bâtiments :

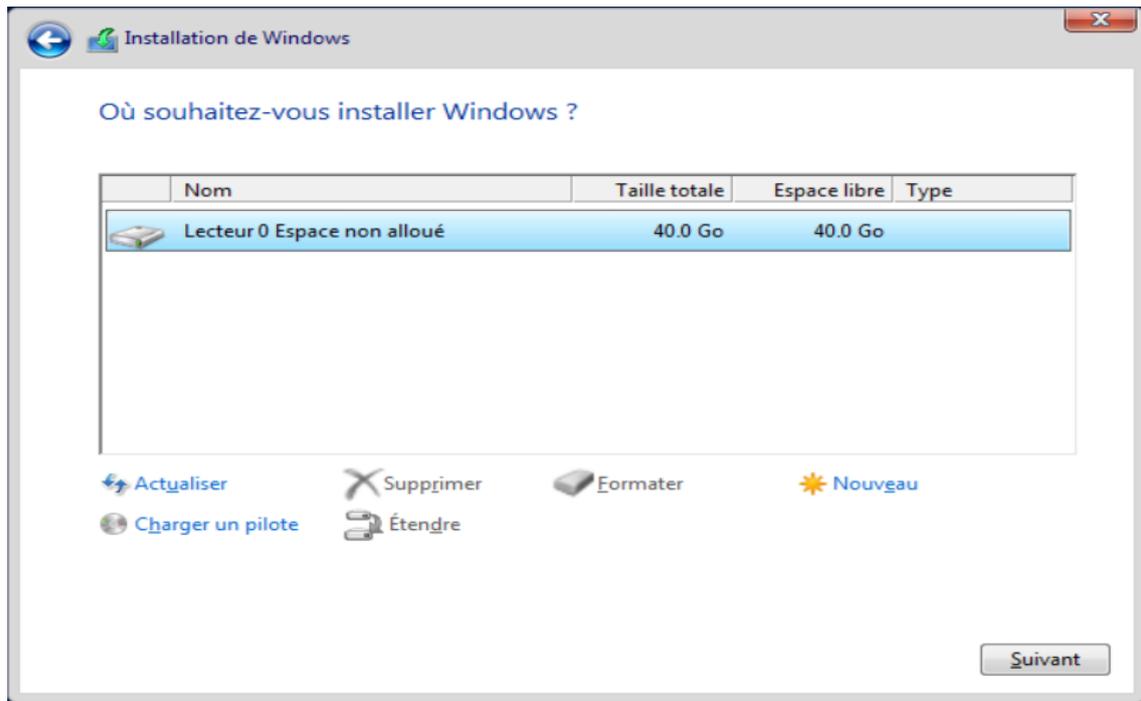


6.3 Installation des services Windows

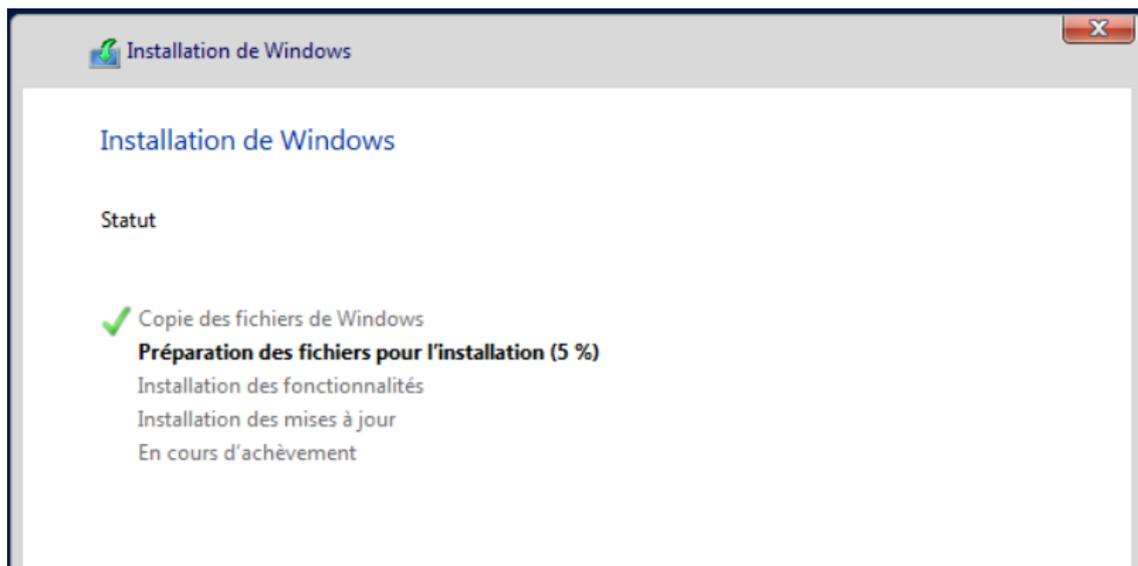
6.3.1 Installation contrôleur de domaine physique DCO

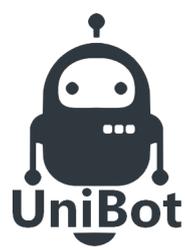
Pour commencer, nous allons démarrer la machine physique DCO et procéder à l'installation de Windows Server 2016 en mode standard avec interface graphique et installer les rôles AD et DNS :

Sélectionner le disque où le système sera installé afin de commencer l'installation :



L'installation est en cours de progression :





Après l'installation de Windows, nous allons modifier le nom du serveur, un redémarrage sera nécessaire après la modification :

Modification du nom ou du domaine de l'ordinateur ✕

Vous pouvez modifier le nom et l'appartenance de cet ordinateur. Ces modifications peuvent influencer sur l'accès aux ressources réseau.

Nom de l'ordinateur :
EVO-X-N01

Nom complet de l'ordinateur :
EVO-X-N01

Autres...

Membre d'un

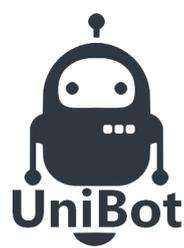
Domaine :

Groupe de travail :
WORKGROUP

OK Annuler

Avant d'installer des rôles, nous allons modifier l'adressage IP du serveur :

- Adresse IP : 192.168.1.5
- Masque de sous réseau : 255.255.255.0
- Passerelle : 192.168.1.1
- DNS 1 : 192.168.1.5
- DNS 2 : 192.168.1.10



Il faudra maintenant installer le rôle AD DS ainsi que le rôle DNS sur le serveur DC0:

Assistant Ajout de rôles et de fonctionnalités

Sélectionner le serveur de destination

SERVEUR DE DESTINATION EVO-X-N01

Avant de commencer
Type d'installation
Sélection du serveur
Rôles de serveurs
Fonctionnalités
Confirmation
Résultats

Sélectionnez le serveur ou le disque dur virtuel sur lequel installer des rôles et des fonctionnalités.

Sélectionner un serveur du pool de serveurs
 Sélectionner un disque dur virtuel

Pool de serveurs

Filtre :

Nom	Adresse IP	Système d'exploitation
EVO-X-N01	192.168.0.38	Microsoft Windows Server 2016 Standard

1 ordinateur(s) trouvé(s)

Cette page présente les serveurs qui exécutent Windows Server 2012 ou une version ultérieure et qui ont été ajoutés à l'aide de la commande Ajouter des serveurs dans le Gestionnaire de serveur. Les serveurs hors connexion et les serveurs nouvellement ajoutés dont la collecte de données est toujours incomplète ne sont pas répertoriés.

< Précédent Suivant > Installer Annuler

Assistant Ajout de rôles et de fonctionnalités

Sélectionner des rôles de serveurs

SERVEUR DE DESTINATION EVO-X-N01

Avant de commencer
Type d'installation
Sélection du serveur
Rôles de serveurs
Fonctionnalités
Serveur DNS
AD DS
Confirmation
Résultats

Sélectionnez un ou plusieurs rôles à installer sur le serveur sélectionné.

Rôles

- Accès à distance
- Attestation d'intégrité de l'appareil
- Expérience Windows Server Essentials
- Hyper-V
- MultiPoint Services
- Serveur de télécopie
- Serveur DHCP
- Serveur DNS
- Serveur Web (IIS)
- Service Guardian hôte
- Services AD DS**
- Services AD LDS (Active Directory Lightweight Directory Services)
- Services AD RMS (Active Directory Rights Management Services)
- Services Bureau à distance
- Services d'activation en volume
- Services d'impression et de numérisation de documents
- Services de certificats Active Directory
- Services de déploiement Windows
- Services de fédération Active Directory (AD FS)

Description

Les services de domaine Active Directory (AD DS) stockent des informations à propos des objets sur le réseau et rendent ces informations disponibles pour les utilisateurs et les administrateurs du réseau. Les services AD DS utilisent les contrôleurs de domaine pour donner aux utilisateurs du réseau un accès aux ressources autorisées n'importe où sur le réseau via un processus d'ouverture de session unique.

< Précédent Suivant > Installer Annuler



L'installation des rôles s'effectue :

Assistant Ajout de rôles et de fonctionnalités

Progression de l'installation

SERVEUR DE DESTINATION
EVO-X-N01

Avant de commencer
Type d'installation
Sélection du serveur
Rôles de serveurs
Fonctionnalités
Serveur DNS
AD DS
AD DS
Confirmation
Résultats

Afficher la progression de l'installation

i Installation de fonctionnalité

Installation démarrée sur EVO-X-N01

- Gestion de stratégie de groupe
- Outils d'administration de serveur distant
 - Outils d'administration de rôles
 - Outils AD DS et AD LDS
 - Module Active Directory pour Windows PowerShell
 - Outils AD DS
 - Centre d'administration Active Directory
 - Composants logiciels enfichables et outils en ligne de commande AD DS
 - Outils du serveur DNS
- Serveur DNS

i Vous pouvez fermer cet Assistant sans interrompre les tâches en cours d'exécution. Examinez leur progression ou rouvrez cette page en cliquant sur Notifications dans la barre de commandes, puis sur Détails de la tâche.

Exporter les paramètres de configuration

< Précédent Suivant > Fermer Annuler

Après l'installation du rôle AD DS et DNS, il faut promouvoir le serveur en contrôleur de domaine, nous allons donc créer la forêt « Unibot.lab » :

Assistant Configuration des services de domaine Active Directory

Configuration de déploiement

SERVEUR CIBLE
EVO-X-N01

Configuration de déploie...

Options du contrôleur de...
Options supplémentaires
Chemins d'accès
Examiner les options
Vérification de la configur...
Installation
Résultats

Sélectionner l'opération de déploiement

- Ajouter un contrôleur de domaine à un domaine existant
- Ajouter un nouveau domaine à une forêt existante
- Ajouter une nouvelle forêt

Spécifiez les informations de domaine pour cette opération

Nom de domaine racine :



A ce moment-là, il faut attribuer un mot de passe afin de procéder à une restauration de l'annuaire AD si besoin et passez les étapes jusqu'à l'installation et puis le serveur va redémarrer :

Assistant Configuration des services de domaine Active Directory

Options du contrôleur de domaine

SERVEUR CIBLE
EVO-X-N01

Configuration de déploiement...
Options du contrôleur de...
Options DNS
Options supplémentaires
Chemins d'accès
Examiner les options
Vérification de la configur...
Installation
Résultats

Sélectionner le niveau fonctionnel de la nouvelle forêt et du domaine racine

Niveau fonctionnel de la forêt : Windows Server 2016

Niveau fonctionnel du domaine : Windows Server 2016

Spécifier les fonctionnalités de contrôleur de domaine

Serveur DNS (Domain Name System)
 Catalogue global (GC)
 Contrôleur de domaine en lecture seule (RODC)

taper le mot de passe du mode de restauration des services d'annuaire (DSRM)

Mot de passe :

Confirmer le mot de passe :

[En savoir plus sur la options du contrôleur de domaine](#)

< Précédent Suivant > Installer Annuler

6.3.2 Installation des hyperviseurs physiques

Nous allons maintenant passer à l'installation des deux hyperviseurs physiques sous Windows Server 2016 en mode standard avec interface graphique avec le rôle Hyper-V afin de procéder à la création du cluster.

Il s'agit de la même installation Windows server que le contrôleur de domaine physique, nous allons donc directement passer au nommage et à la configuration IP du serveur :

Voici le nommage des deux Hyperviseurs :

Nommage de l'hyperviseur n°1 : EVO-X-HV01

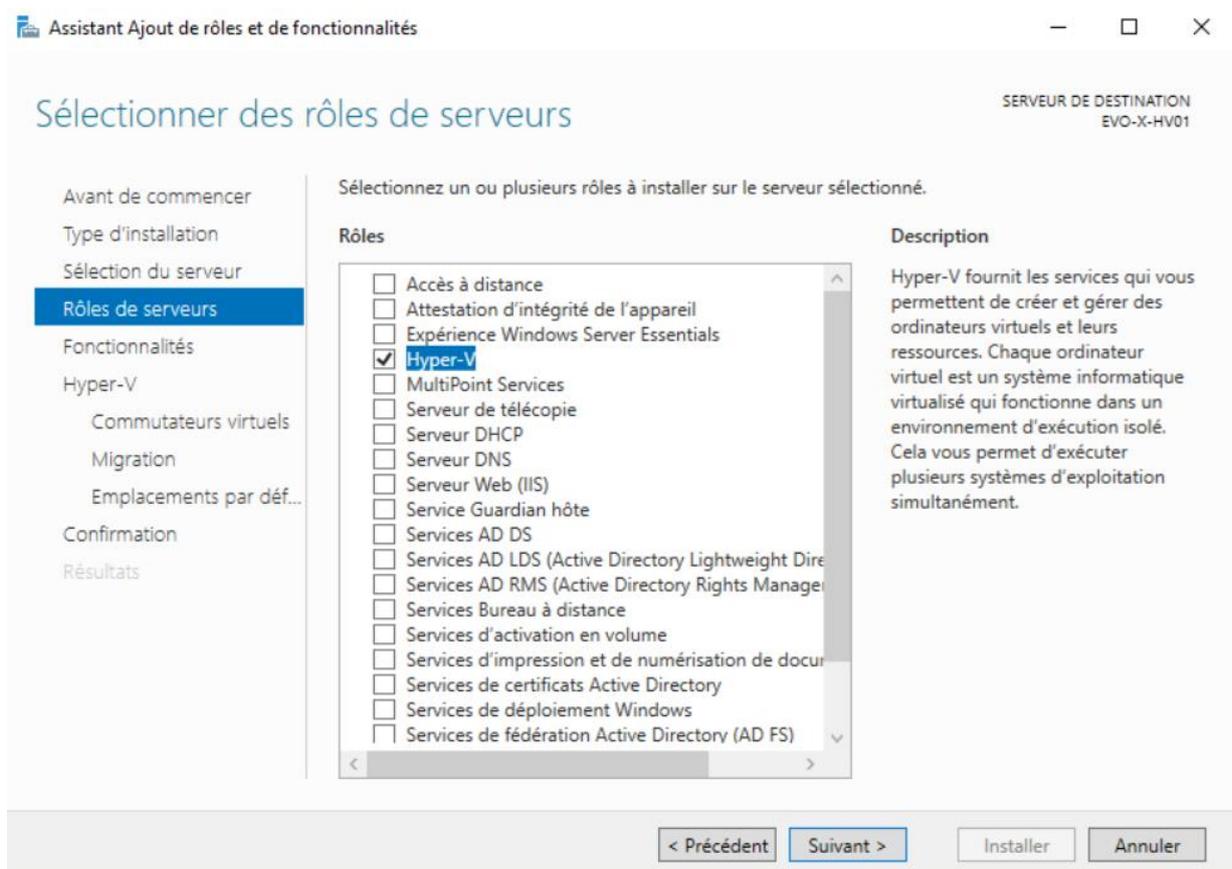
- Adresse IP : 192.168.1.6
- Masque de sous réseau : 255.255.255.0
- Passerelle : 192.168.1.1
- DNS 1 : 192.168.1.5
- DNS 2 : 192.168.1.10



Nommage de l’hyperviseur n°2 : EVO-X-HV02

- Adresse IP : 192.168.1.7
- Masque de sous réseau : 255.255.255.0
- Passerelle : 192.168.1.1
- DNS 1 : 192.168.1.5
- DNS 2 : 192.168.1.10

Nous allons installer le rôle Hyper-V sur les deux machines physiques.



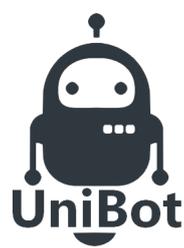
6.3.3 Installation du serveur physique ISCSI

Nous allons maintenant passer à l’installation du serveur ISCSI sous Windows Server 2016 en mode standard avec interface graphique avec le rôle Serveur de fichier et ISCSI afin de procéder à la création du cluster.

Il s’agit de la même installation Windows server que le contrôleur de domaine physique, nous allons donc directement passer au nommage et à la configuration IP du serveur :

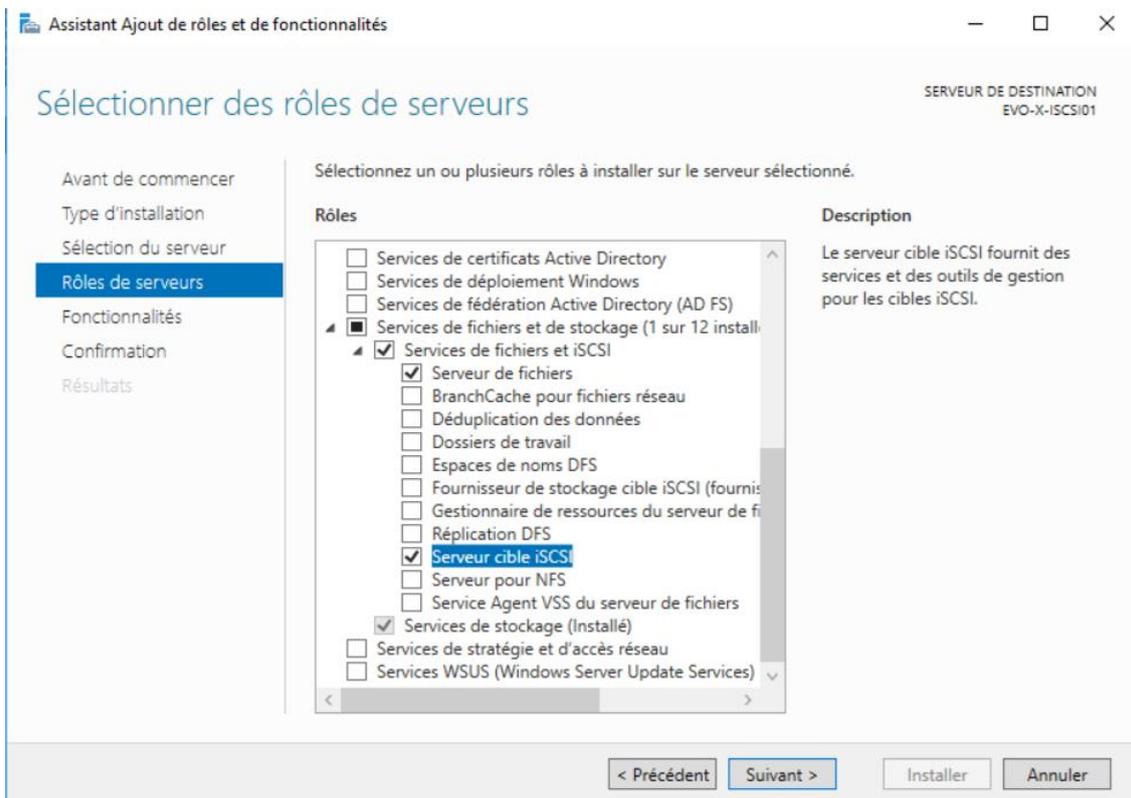
Voici le nommage du serveur ISCSI :

Nommage du serveur ISCSI : EVO-X-ISCSI01

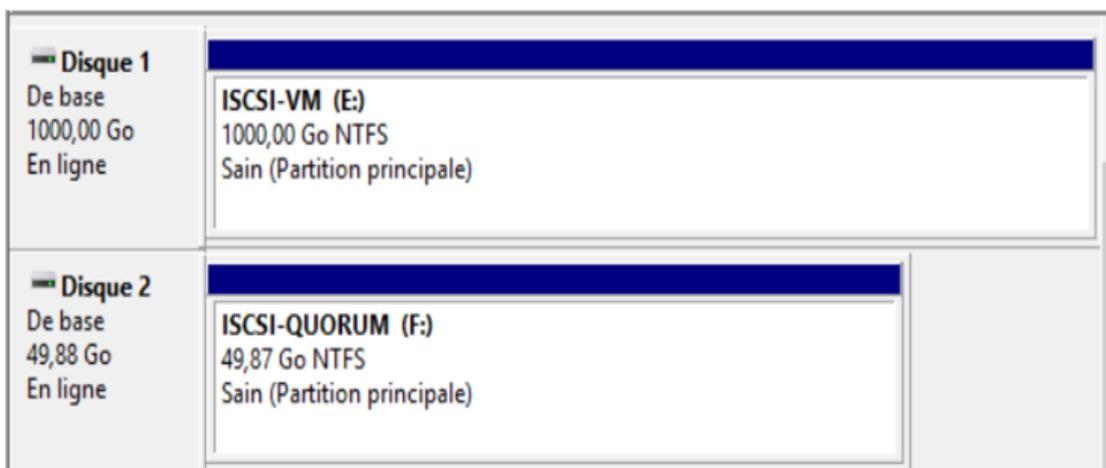


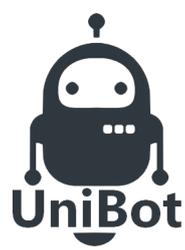
- Adresse IP : 192.168.1.8
- Masque de sous réseau : 255.255.255.0
- Passerelle : 192.168.1.1
- DNS 1 : 192.168.1.5
- DNS 2 : 192.168.1.10

Maintenant que les rôles Hyper-V sont installés sur deux hyperviseurs physiques, nous allons installer le rôle ISCSI :



Nous allons ajouter deux disques pour le stockage des VM :





Lancez le rôle ISCSI et choisissez le disque ISCSI-VM pour le stockage des VM

Sélectionner l'emplacement du disque virtuel iSCSI

Emplacement du disque...

Nom du disque virtuel iS...

Taille du disque virtuel iSC...

Cible iSCSI

Nom de la cible et accès

Serveurs d'accès

Activer les services d'auth...

Confirmation

Résultats

Serveur :

Nom du serveur	Statut	Rôle du cluster	Nœud propriétaire
EVO-X-ISCSI01	En ligne	Non-cluster	

i La liste est filtrée de manière à n'afficher que les serveurs sur lesquels le rôle Serveur cible iSCSI est installé.

Emplacement de stockage :

Sélectionner par volume :

Volume	Espace libre	Capacité	Système de fichiers
C:	19,4 Go	29,5 Go	NTFS
E:	1 000 Go	1 000 Go	NTFS
F:	49,8 Go	49,9 Go	NTFS

Indiquer le nom du disque dur virtuel iSCSI

Emplacement du disque...

Nom du disque virtuel iS...

Taille du disque virtuel iSC...

Cible iSCSI

Nom de la cible et accès

Serveurs d'accès

Activer les services d'auth...

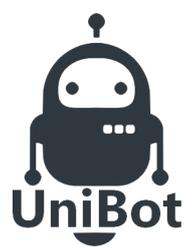
Confirmation

Résultats

Nom :

Description :

Chemin d'accès : E:\iSCSIVirtualDisks\ISCSI-VM.vhdx



Indiquer la taille du disque dur virtuel iSCSI

Emplacement du disque...

Nom du disque virtuel iS...

Taille du disque virtuel iS...

Cible iSCSI

Nom de la cible et accès

Serveurs d'accès

Activer les services d'auth...

Confirmation

Résultats

Espace libre : 1 000 Go

Taille :

Taille fixe

Ce type de disque produit de meilleures perf. et est recommandé pour les serveurs exécutant des applications exigeantes. Le disque dur virtuel est créé à la taille du disque dur virtuel fixe. Sa taille ne change pas avec l'ajout ou la suppr. de données.

Effacer le disque virtuel au moment de l'allocation

Remarque : IL N'EST PAS RECOMMANDÉ de désactiver cette option. L'effacement complet d'un disque supprime les éventuels fragments de données conservés sur le dispositif de stockage sous-jacent, évitant ainsi les fuites d'informations.

Taille dynamique

Ce type permet de mieux exploiter l'espace de stockage physique ; il est recommandé pour les serveurs qui exécutent des applications sollicitant peu le disque. Le fichier .vhdx est petit lors de la création du disque, mais augmente à mesure que des données y sont écrites.

Affecter la cible iSCSI

Emplacement du disque...

Nom du disque virtuel iS...

Taille du disque virtuel iS...

Cible iSCSI

Nom de la cible et accès

Serveurs d'accès

Activer les services d'auth...

Confirmation

Résultats

Affectez ce disque virtuel iSCSI à une cible iSCSI existante ou créez une nouvelle cible pour lui.

Cible iSCSI existante :

Nom de la cible	ID d'initiateur	Description

Nouvelle cible iSCSI



Ajouter les serveurs d'accès :

Indiquer les serveurs d'accès

Emplacement du disque... Cliquez sur Ajouter pour préciser le ou les initiateurs iSCSI devant accéder à ce disque virtuel iSCSI.

Nom du disque virtuel iS...

Taille du disque virtuel iSC...

Cible iSCSI

Nom de la cible et accès

Serveurs d'accès

Activer les services d'auth...

Confirmation

Résultats

Type	Valeur
IQN	iqn.1991-05.com.microsoft:evo-x-hv01.unibot.lab
IQN	iqn.1991-05.com.microsoft:evo-x-hv02.unibot.lab

Et procéder à la création du disque iSCSI-VM:

Confirmer les sélections

Emplacement du disque... Vérifiez que les paramètres suivants sont corrects, puis cliquez sur Créer.

Nom du disque virtuel iS...

Taille du disque virtuel iSC...

Cible iSCSI

Nom de la cible et accès

Serveurs d'accès

Activer les services d'auth...

Confirmation

Résultats

EMPLACEMENT DU DISQUE VIRTUEL iSCSI

Serveur : EVO-X-ISCIO1

Rôle du cluster : Non-cluster

Chemin d'accès : E:\iSCSIVirtualDisks\iSCSI-VM.vhdx

PROPRIÉTÉS DU DISQUE VIRTUEL iSCSI

Nom : iSCSI-VM

Taille : 1 000 Go

PROPRIÉTÉS DE LA CIBLE

Nom : iscsi-vm

SERVEURS D'ACCÈS

Nom qualifié : iqn.1991-05.com.microsoft:evo-x-hv01.unibot.lab

Nom qualifié : iqn.1991-05.com.microsoft:evo-x-hv02.unibot.lab

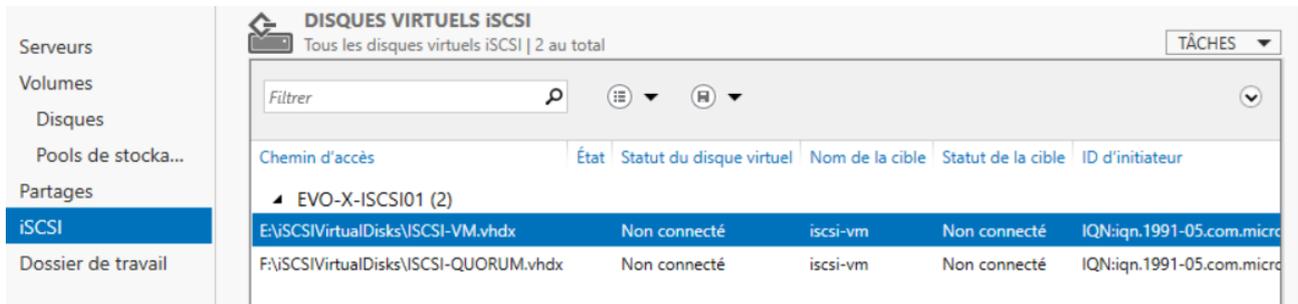
SÉCURITÉ

CHAP : Désactivé

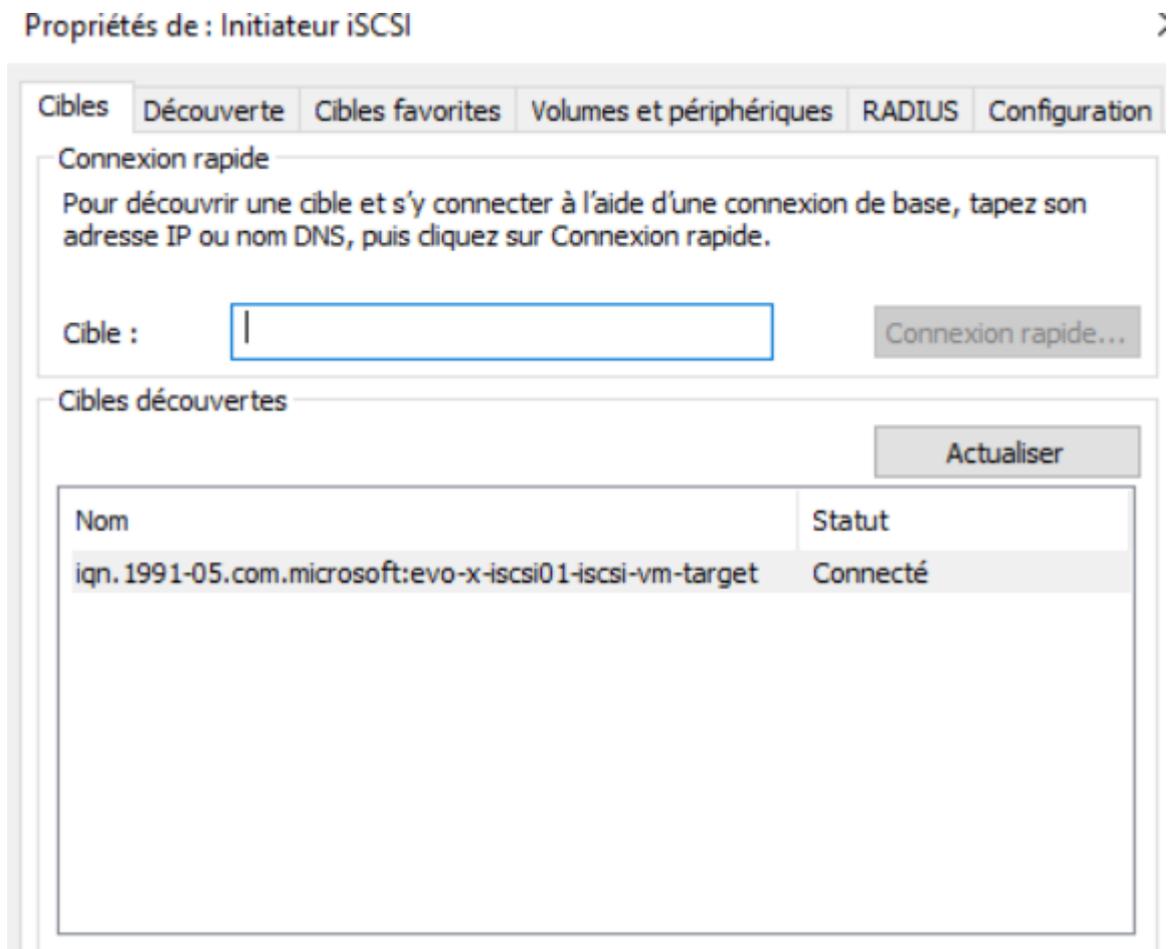
CHAP inversé : Désactivé



Nous allons faire la même chose pour le disque ISCSI-QUORUM.



Nous allons maintenant initialiser la cible ISCSI sur les deux Hyperviseurs physique :



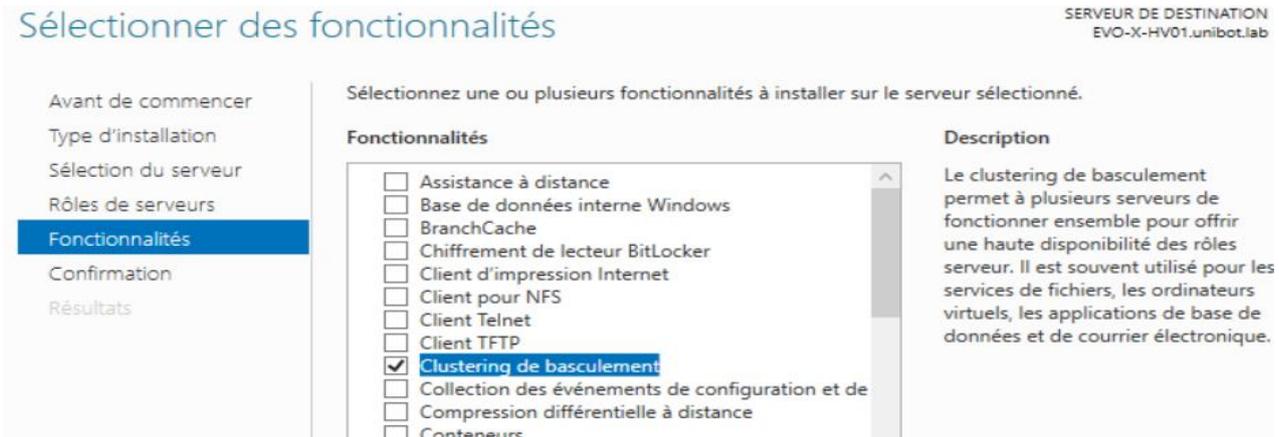
La cible ISCSI est maintenant en place il reste donc à mettre en place de clustering de basculement.



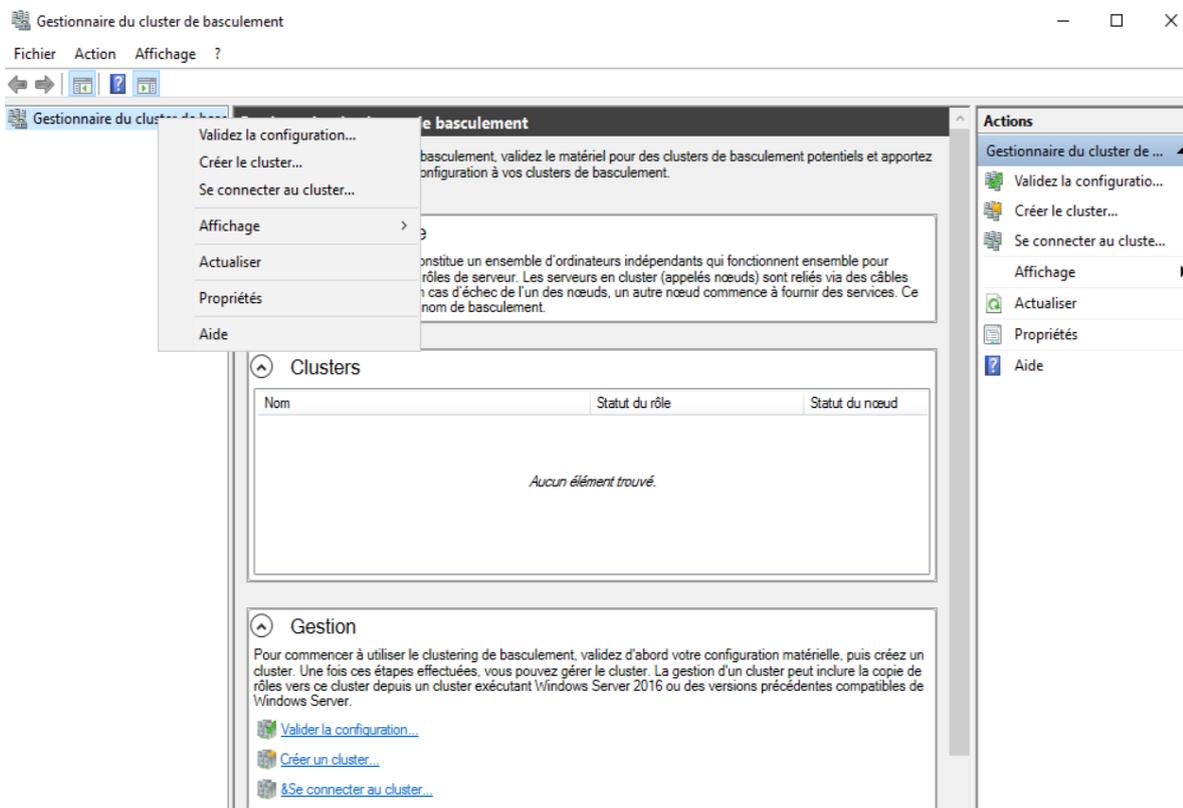
6.3.4 Installation du cluster de basculement

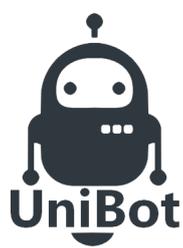
Pour donner suite à la mise en place des deux hyperviseurs et du serveur ISCSI, nous allons pouvoir mettre en place de clustering de basculement afin de pouvoir avoir une redondance des machines virtuelles que nous allons créer.

Nous allons donc installer le rôle Clustering de basculement sur les deux hyperviseurs :



Nous allons maintenant procéder à la création du cluster :





Commencer la création et lors de la sélection des serveurs, sélectionnez les deux hyperviseurs :

Assistant Création d'un cluster X

Sélection des serveurs

Avant de commencer

Sélection des serveurs

Avertissement de validation

Point d'accès pour l'administration du cluster

Confirmation

Création du nouveau cluster

Résumé

Ajoutez le nom des serveurs que vous voulez voir figurer dans le cluster. Vous devez ajouter au moins un serveur.

Nom du serveur :

Serveurs sélectionnés :

EVO-X-HV01.unibot.lab
 EVO-X-HV02.unibot.lab

Faites les tests :

Options de test

Avant de commencer

Options de test

Confirmation

Validation en cours

Résumé

Vous pouvez choisir d'exécuter tous les tests ou seulement des tests sélectionnés.

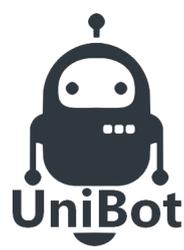
Les tests examinent la configuration du cluster, la configuration d'Hyper-V, l'inventaire, le réseau, le stockage et la configuration du système.

Microsoft prend en charge une solution de cluster seulement si la configuration complète (serveurs, réseau et stockage) réussit tous les tests de cet Assistant. De plus, tous les composants matériels de la solution de cluster doivent comporter la mention « Certifié pour Windows Server 2012 R2 ».

Exécuter tous les tests (recommandé)

Exécuter uniquement les tests que je sélectionne

[En savoir plus sur les tests de validation de cluster](#)



Ajouter un nom et une adresse IP pour le cluster :

Assistant Création d'un cluster

Point d'accès pour l'administration du cluster

Avant de commencer Entrez le nom à utiliser pour administrer le cluster.

Sélection des serveurs

Point d'accès pour l'administration du cluster

Confirmation

Création du nouveau cluster

Résumé

Nom du cluster :

Le nom NetBIOS est limité à 15 caractères. Une ou plusieurs adresses IPv4 n'ont pas pu être configurées automatiquement. Pour chaque réseau à utiliser, vérifiez que le réseau est sélectionné, puis tapez une adresse.

	Réseaux	Adresse
<input checked="" type="checkbox"/>	192.168.1.0/24	192 . 168 . 1 . 9

< Précédent **Suivant >** Annuler

La création du cluster est faite, nous allons maintenant ajouter les disques :

Gestionnaire du cluster de basculement

Fichier Action Affichage ?

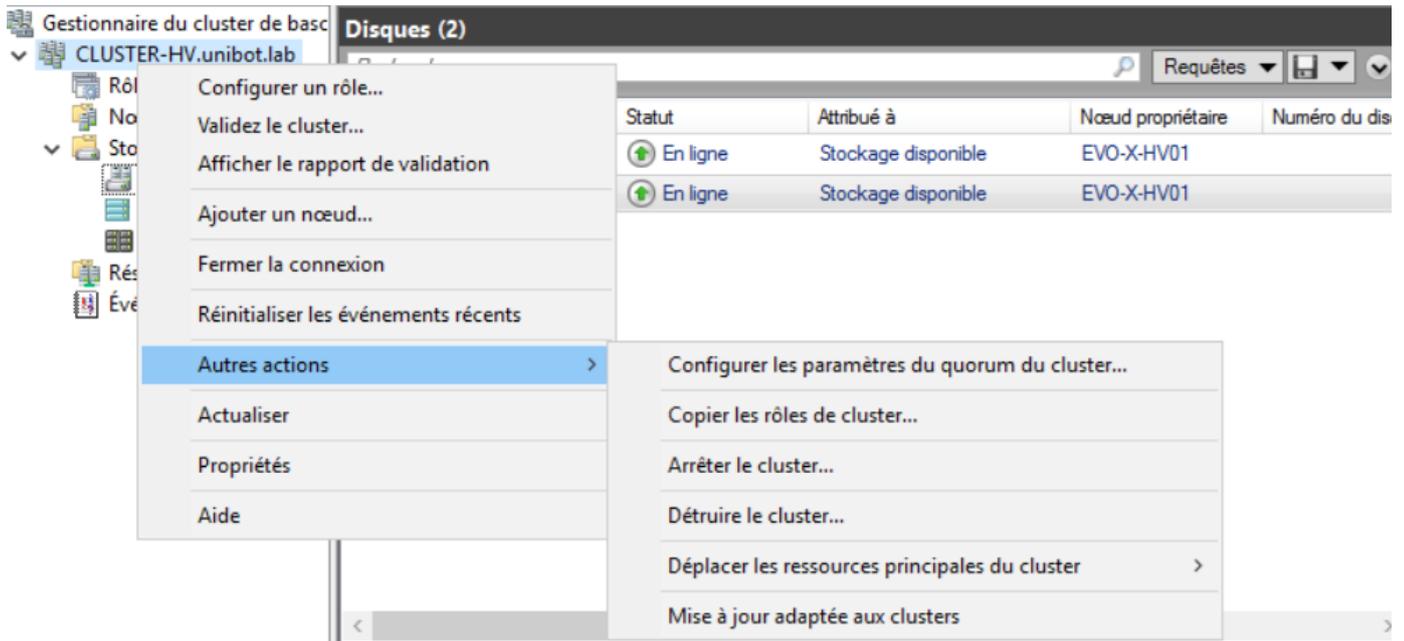
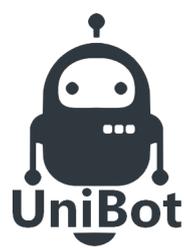
Rechercher Requetes

Nom	Statut	Attribué à	Nœud propriétaire	Numéro du disq
Disque de cluster 1	En ligne	Stockage disponible	EVO-X-HV01	
Disque de cluster 2	En ligne	Stockage disponible	EVO-X-HV01	

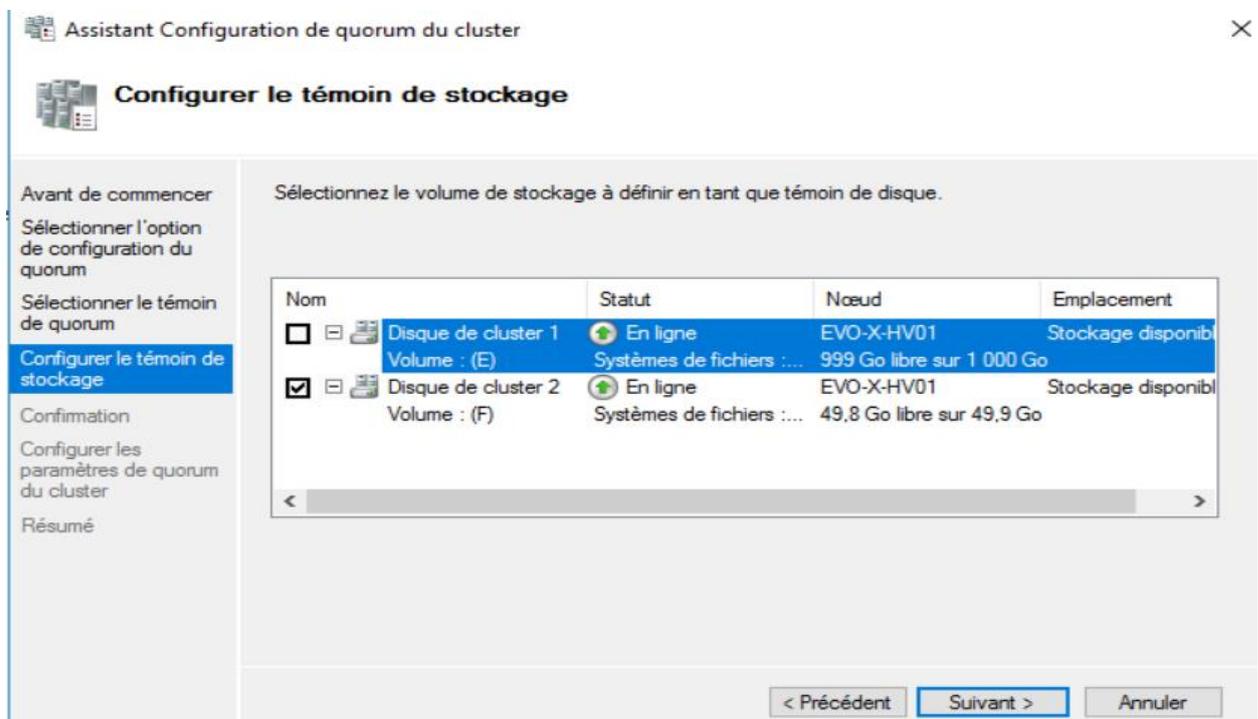
Actions

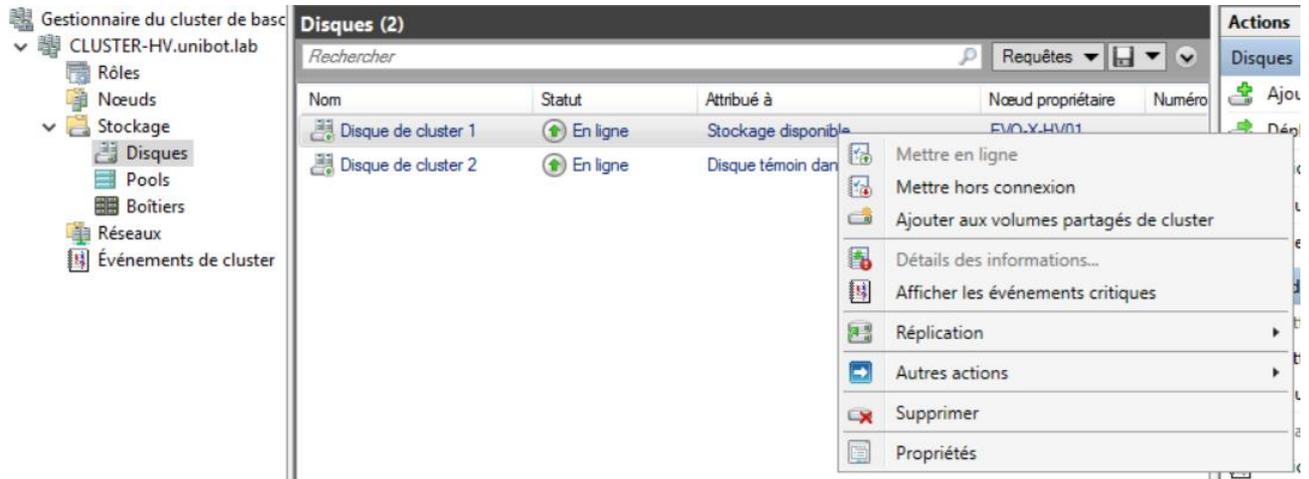
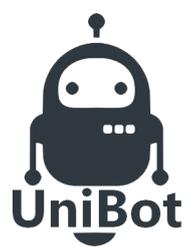
- Disques
 - Ajouter un disque
 - Déplacer le stockage di...
 - Affichage
 - Actualiser
 - Aide
- Disque de cluster 2
 - Mettre en ligne
 - Mettre hors connexion

Nous allons paramétrer le quorum du cluster :



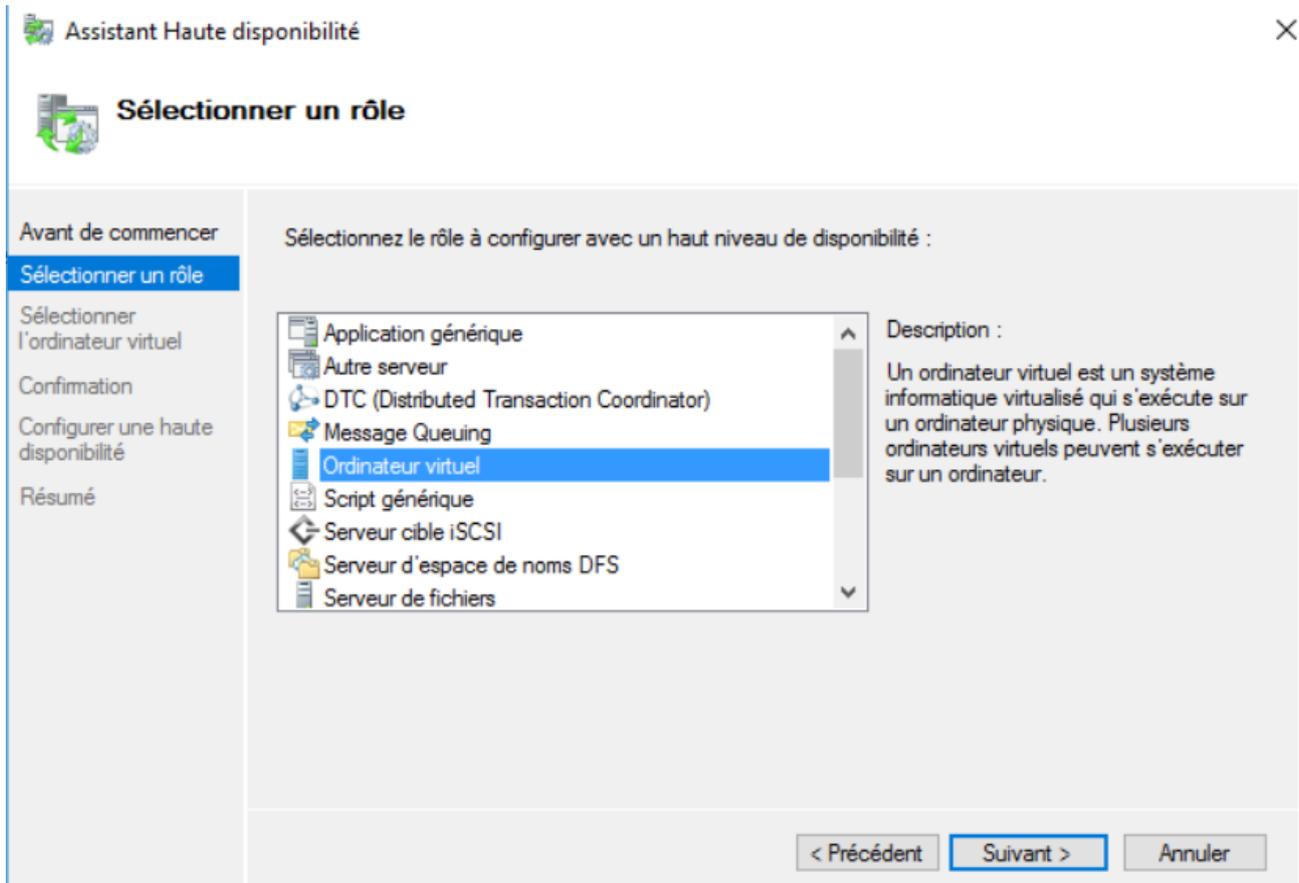
Il faut cliquer sur « Sélectionner le témoin du quorum » et puis nous allons sélectionner le disque qui gère cela :





Nous allons maintenant pouvoir créer les VM, il faudra installer le rôle ordinateur virtuel en faisant clique droite sur Rôle puis configurer un rôle :



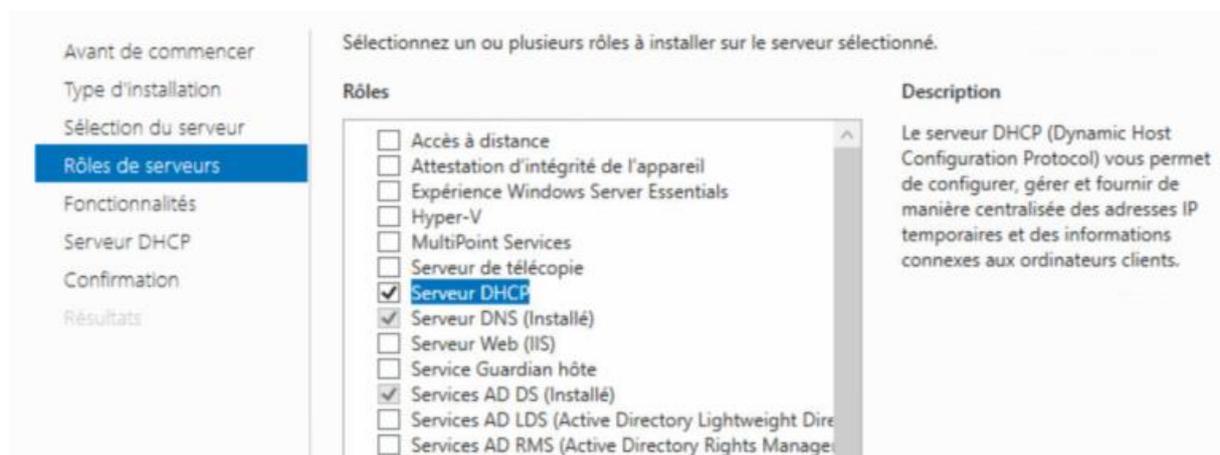


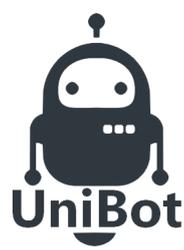
Après l'installation des machines virtuel, le cluster sera en fonctionne, si l'un des deux hyperviseurs tombe en panne, l'autre prend le relais.

6.3.5 Installation du DHCP

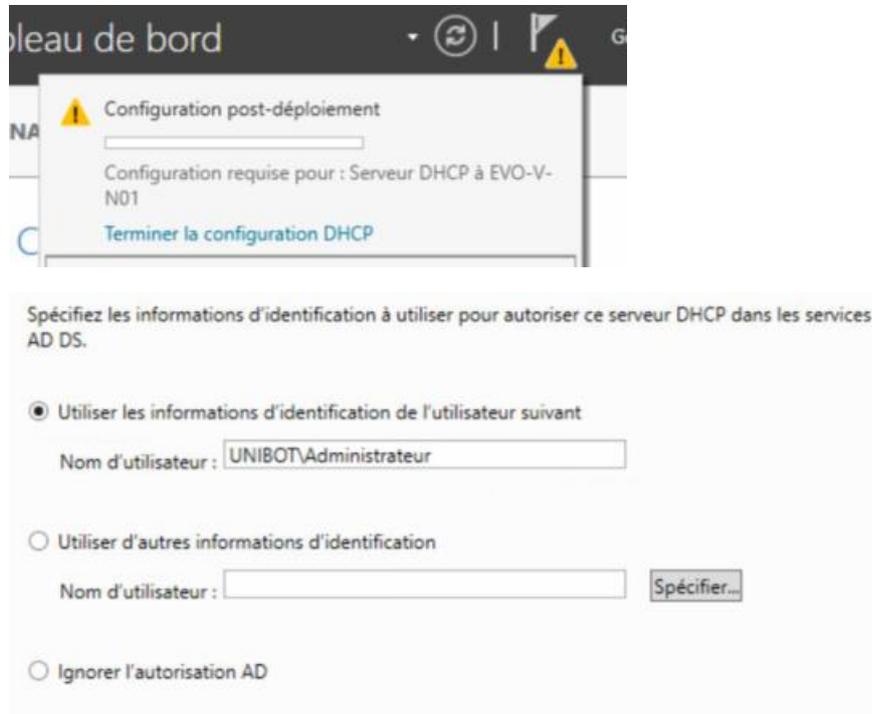
Afin de mettre en marche le serveur DHCP, nous allons l'installer sur notre contrôleur de domaine virtuel EVO-V-N01 :

Pour commencer, nous allons installer le rôle DHCP :

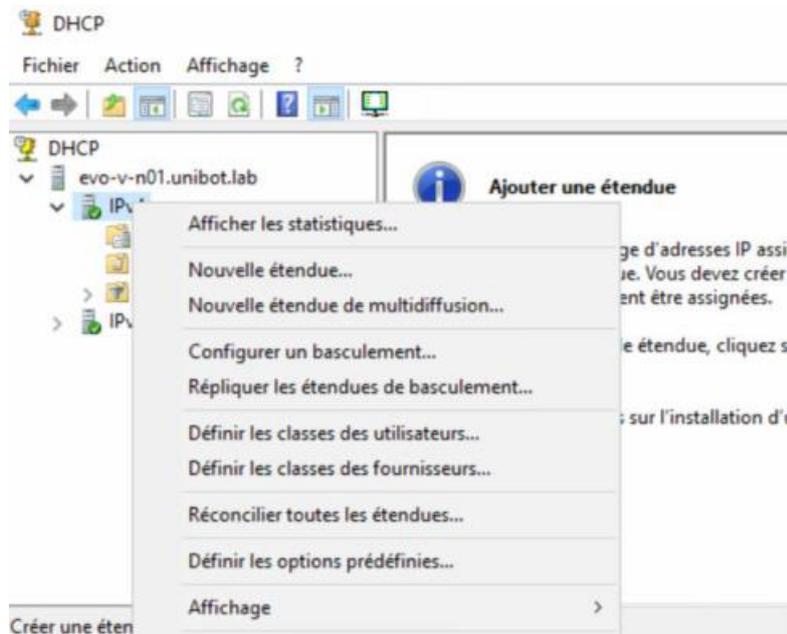




Maintenant que le service DHCP est installé, nous allons passer à la configuration post-install :



La configuration post-install est maintenant terminée, nous allons ouvrir la console DHCP et créer une étendue :





Nous allons nommer notre étendue :

Nom de l'étendue 

Vous devez fournir un nom pour identifier l'étendue. Vous avez aussi la possibilité de fournir une description.

Tapez un nom et une description pour cette étendue. Ces informations vous permettront d'identifier rapidement la manière dont cette étendue est utilisée dans le réseau.

Nom :

Description :

Voici la plage d'adresse IP pour notre étendue :

Plage d'adresses IP 

Vous définissez la plage d'adresses en identifiant un jeu d'adresses IP consécutives.

Paramètres de configuration pour serveur DHCP

Entrez la plage d'adresses que l'étendue peut distribuer.

Adresse IP de début :

Adresse IP de fin :

Paramètres de configuration qui se propagent au client DHCP.

Longueur :

Masque de sous-réseau :

Aucune exclusion a été faite, nous allons paramétrer la durée du bail d'une adresse IP pour la renouveler toutes les 2 jours :

Durée du bail 

La durée du bail spécifie la durée pendant laquelle un client peut utiliser une adresse IP de cette étendue.

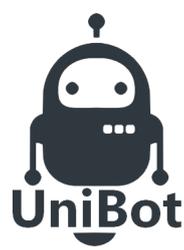
La durée du bail doit théoriquement être égale au temps moyen durant lequel l'ordinateur est connecté au même réseau physique. Pour les réseaux mobiles constitués essentiellement par des ordinateurs portables ou des clients d'accès à distance, des durées de bail plus courtes peuvent être utiles.

De la même manière, pour les réseaux stables qui sont constitués principalement d'ordinateurs de bureau ayant des emplacements fixes, des durées de bail plus longues sont plus appropriées.

Définissez la durée des baux d'étendue lorsqu'ils sont distribués par ce serveur.

Limitée à :

Jours : Heures : Minutes :



Il faut maintenant définir l'adresse IP de la passerelle, ici notre passerelle est la 192.168.1.1 :

Routeur (passerelle par défaut)
Vous pouvez spécifier les routeurs, ou les passerelles par défaut, qui doivent être distribués par cette étendue.

Pour ajouter une adresse IP pour qu'un routeur soit utilisé par les clients, entrez l'adresse ci-dessous.

Adresse IP :

192.168.1.1	Ajouter
	Supprimer
	Monter
	Descendre

Les paramètres DNS sont déjà entrés, ici, nous avons notre serveur DNS sur notre machine physique EVO-X-N01 et notre serveur DNS sur notre machine virtuelle actuelle :

Nom de domaine et serveurs DNS
DNS (Domain Name System) mappe et traduit les noms de domaines utilisés par les clients sur le réseau.

Vous pouvez spécifier le domaine parent à utiliser par les ordinateurs clients sur le réseau pour la résolution de noms DNS.

Domaine parent :

Pour configurer les clients d'étendue pour qu'ils utilisent les serveurs DNS sur le réseau, entrez les adresses IP pour ces serveurs.

Nom du serveur :	Adresse IP :	
<input type="text"/>	<input type="text"/>	Ajouter
<input type="text"/>	192.168.1.5	Supprimer
<input type="text"/>	192.168.1.10	Monter
<input type="text"/>		Descendre

L'étendu est maintenant créé et fonctionnelle, mais avant, nous allons installer le service DHCP sur notre machine physique EVO-X-N01 afin de pratiquer de la haute disponibilité si notre serveur DHCP virtuelle tombe en panne :

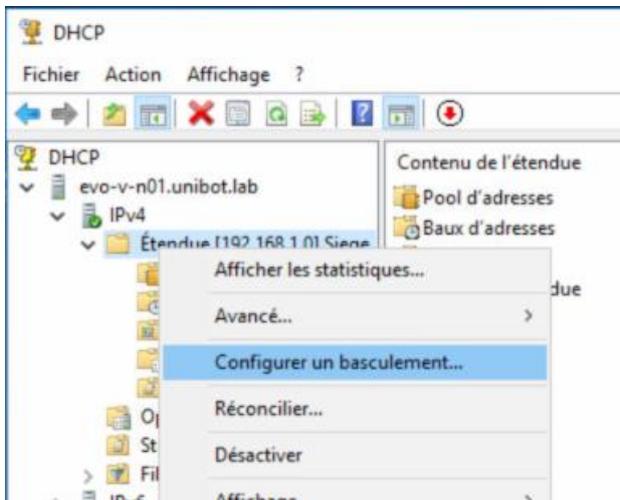
Ajouter une étendue

Une étendue est une plage d'adresses IP assignées aux ordinateurs de manière dynamique. Vous devez créer et configurer une étendue pour que les adresses soient assignées.

Pour ajouter une nouvelle étendue, cliquez sur Nouvelle étendue dans le menu.

Pour plus d'informations sur l'installation d'un serveur DHCP, voir l'aide.

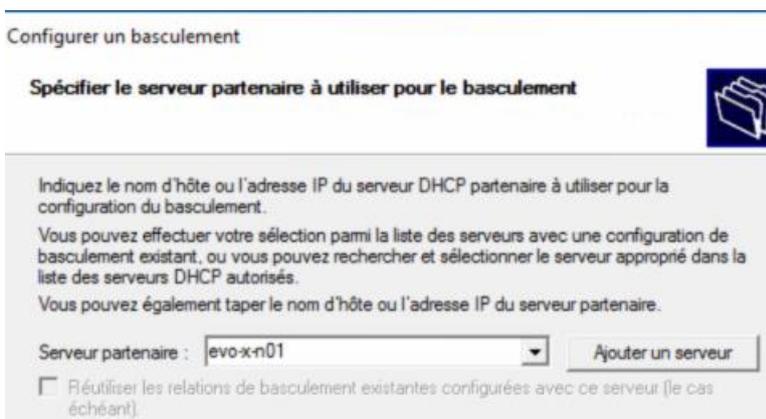
Il faut maintenant configurer le basculement DHCP sur le serveur DHCP principal :



Sélectionner toutes les étendues :



Sélectionner le second serveur DHCP :



Afin de ne pas surcharger l'utilisation du contrôleur de domaine physique principale, nous allons mettre le basculement DHCP en **équilibre de charge** au lieu de **serveur de secours** afin d'utiliser le moins de ressource possible et d'éviter tout type de pannes. Nous devons attribuer un 'secret partagé' complexe qui sera utilisé pour chiffrer les échanges entre les

deux serveurs DHCP concernés, ainsi les échanges de configuration entre les serveurs ne transiteront pas en clair sur le réseau.

Créer une relation de basculement avec le partenaire evo-x-n01

Nom de la relation :

Délai de transition maximal du client (MCLT) : heures minutes

Mode :

Pourcentage d'équilibrage de charge

Serveur local : %

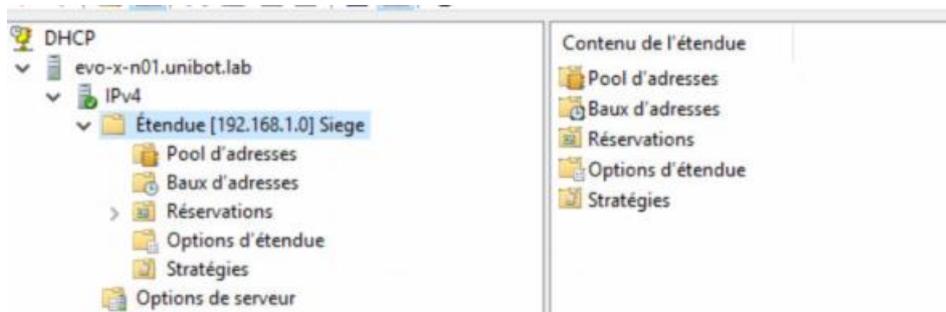
Serveur partenaire : %

Intervalle de basculement d'état : minutes

Activer l'authentification du message

Secret partagé :

Après la création du failover de serveurs DHCP, l'étendu se crée sur la machine physique EVO-X-N01 :



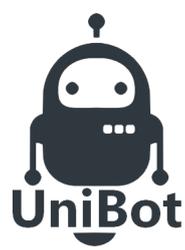
Le serveur DHCP est donc fonctionnel avec une redondance à haute disponibilité.

6.3.6 Serveur d'impression

Le serveur d'impression sera hébergé sur la 2^{ème} machine virtuelle sous Windows server 2016 : Après l'installation du serveur, nous allons renommer le serveur et configurer le réseau :

Nommage de la machine virtuelle EVO-V-N02

- Adresse IP : 192.168.1.11
- Masque de sous réseau : 255.255.255.0
- Passerelle : 192.168.1.1
- DNS 1 : 192.168.1.5
- DNS 2 : 192.168.1.10



Nous allons commencer par installer le rôle de serveur d'impression :

Sélectionnez le serveur ou le disque dur virtuel sur lequel installer des rôles et des fonctionnalités.

Sélectionner un serveur du pool de serveurs
 Sélectionner un disque dur virtuel

Pool de serveurs

Filtre :

Nom	Adresse IP	Systeme d'exploitation
EVO-V-N02	192.168.1.11	Microsoft Windows Server 2016 Standard

Sélectionnez un ou plusieurs rôles à installer sur le serveur sélectionné

Rôles

- Accès à distance
- Attestation d'intégrité de l'appareil
- Expérience Windows Server Essentials
- Hyper-V
- MultiPoint Services
- Serveur de télécopie
- Serveur DHCP
- Serveur DNS
- Serveur Web (IIS)
- Service Guardian hôte
- Services AD DS
- Services AD LDS (Active Directory Lightweight Directory Services)
- Services AD RMS (Active Directory Rights Management Services)
- Services Bureau à distance
- Services d'activation en volume
- Services d'impression et de numérisation de documents
- Services de certificats Active Directory
- Services de déploiement Windows
- Services de fédération Active Directory (AD FS)

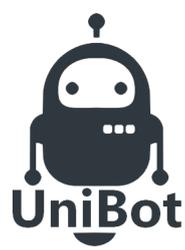
Sélectionner les services de rôle à installer pour Services d'impression et de numérisation de documents

Services de rôle

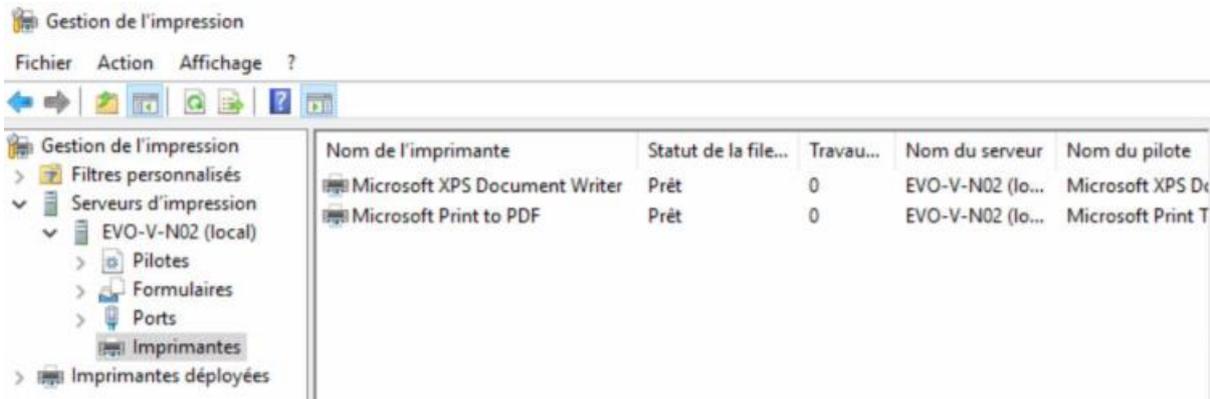
- Serveur d'impression
- Impression Internet
- Serveur de numérisation distribuée
- Service LPD

Détails des services de rôle

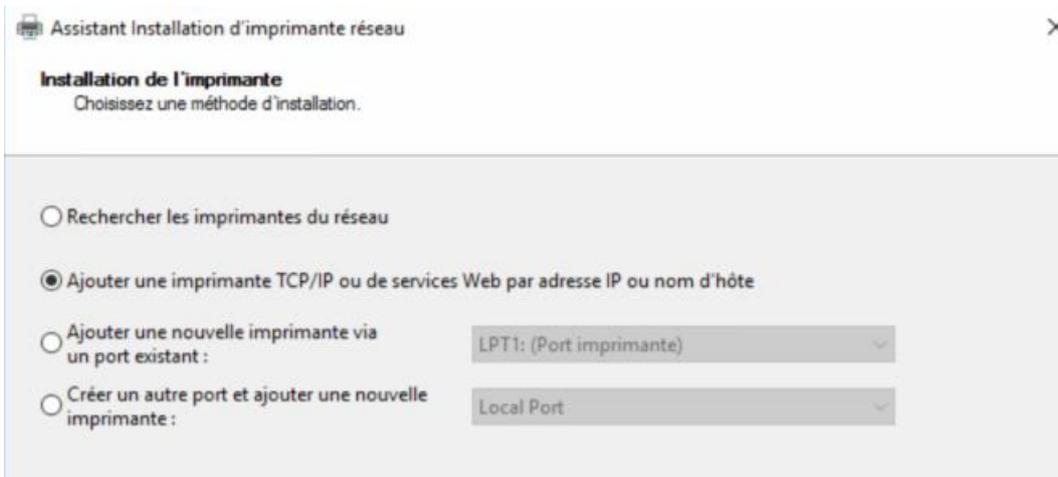
Le serveur d'impression et de numérisation de documents est configuré pour utiliser le service de numérisation de documents.



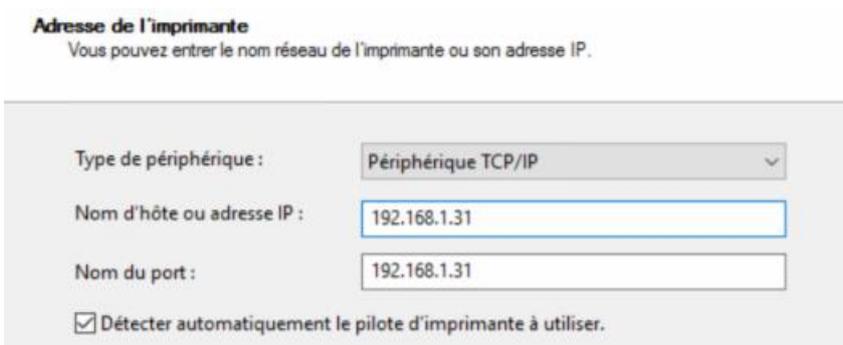
Nous allons maintenant lancer le gestionnaire d'impression afin de créer les imprimantes réseau :



A ce moment-là, il faut choisir d'installer une imprimante en TCP/IP :



Entrez l'adresse IP de l'imprimante en question :



A ce moment-là, il faudra donc renommer l'imprimante : ici PrintDirection, nous allons faire la même chose pour la liste de toutes les imprimantes.



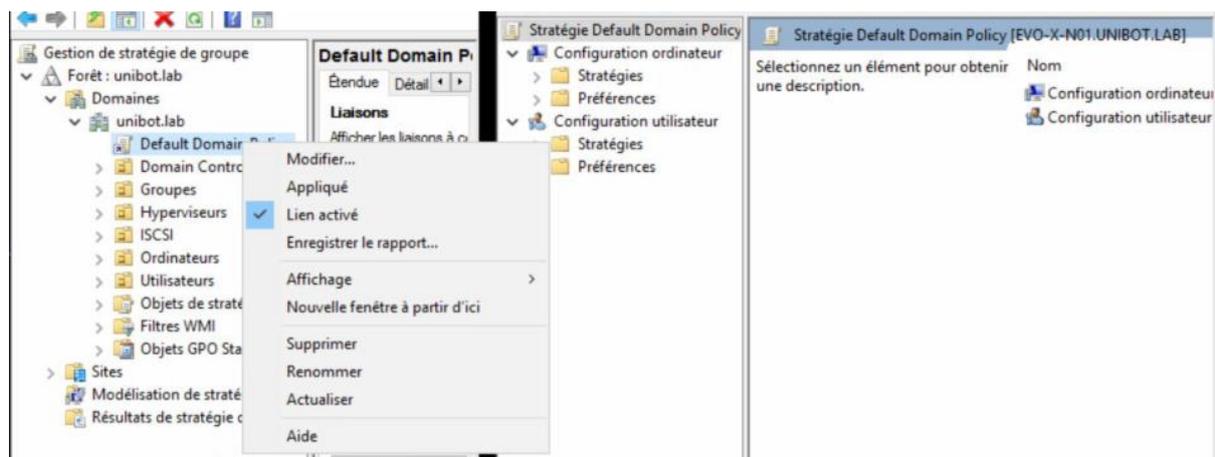
Microsoft Print to PDF	Prêt	0	EVO-V-N02 (lo...	Microsoft Print
Microsoft XPS Document Writer	Prêt	0	EVO-V-N02 (lo...	Microsoft XPS I
PrintAdministratif	Prêt	0	EVO-V-N02 (lo...	HP LaserJet P4C
PrintAll	Prêt	0	EVO-V-N02 (lo...	HP LaserJet P4C
PrintDirection	Prêt	0	EVO-V-N02 (lo...	HP LaserJet P4C
PrintDSI	Prêt	0	EVO-V-N02 (lo...	HP LaserJet P4C
PrintProduitA	Prêt	0	EVO-V-N02 (lo...	HP LaserJet P4C
PrintProduitB	Prêt	0	EVO-V-N02 (lo...	HP LaserJet P4C
PrintSAV	Prêt	0	EVO-V-N02 (lo...	HP LaserJet P4C

Nous allons pouvoir maintenant les déployer par GPO

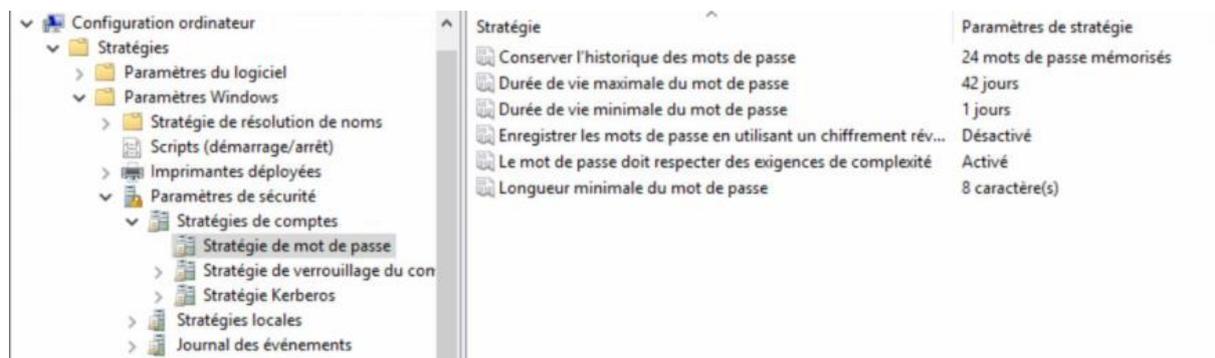
6.3.7 Stratégies de mot de passe

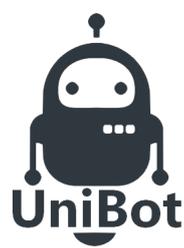
Tout d’abord, une stratégie de mot de passe est obligatoire pour assurer la sécurité de nos utilisateurs, pour se faire, nous allons modifier les stratégies de groupe pour les mots de passes :

Ouvrez donc GPMC.msc, faite un clic droit sur Default Domain Policy et faite modifier :



Dérouler la **Configuration ordinateur** et aller dans : **Stratégies, Paramètres Windows, Paramètres de sécurité, Stratégies de comptes, Stratégie de mot de passe** puis modifier les paramètres comme cela :



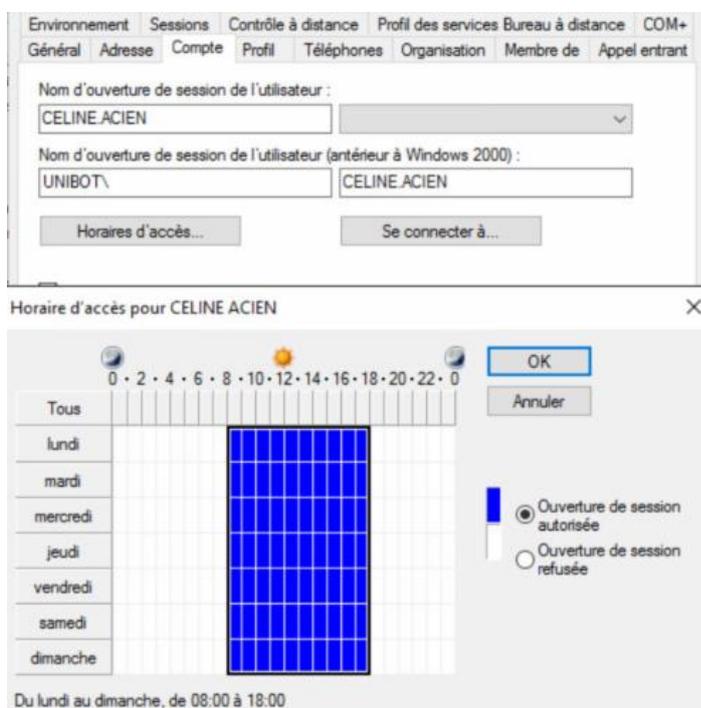


Après l'activation de ces stratégies, nous allons appliquer les modifications avec un **gpupdate /force** dans une invite de commande.

6.3.8 Horaires d'accès

Pour donner suite à des mesures de sécurité, nous devons autoriser la connexion aux postes seulement entre 8h00 et 18h00 pour Mme BEZIAT, ELLA, AYO et ACIEN.

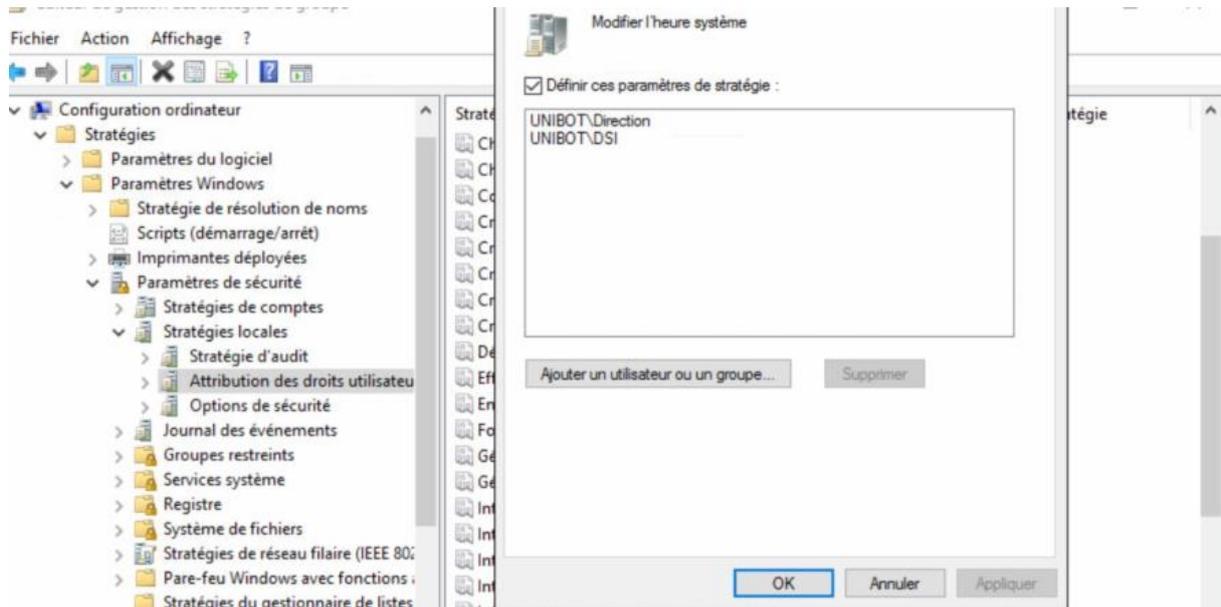
Voici ce que nous avons autorisé pour Mme ACIEN, nous ferons de même pour les 3 autres personnes : Il faut donc faire une clique droite sur la personne en question et aller dans les propriétés du compte, puis Horaires d'accès afin de modifier ces horaires d'accès :



6.3.9 Modification de l'horloge

Afin de pouvoir autoriser que la direction et le service informatique de modifier l'heure, nous avons mis en place une GPO.

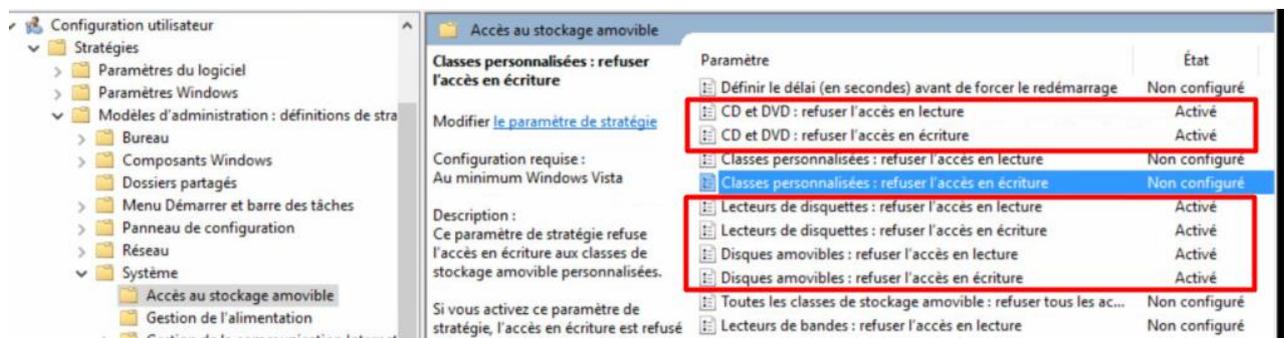
Dans GPMC.msc, Dérouler la **Configuration ordinateur** et aller dans : **Stratégies, Paramètres Windows, Paramètres de sécurité, Stratégies locales, Attribution des droits utilisateurs** puis modifier les paramètres « Modifier l'heure système » comme cela :



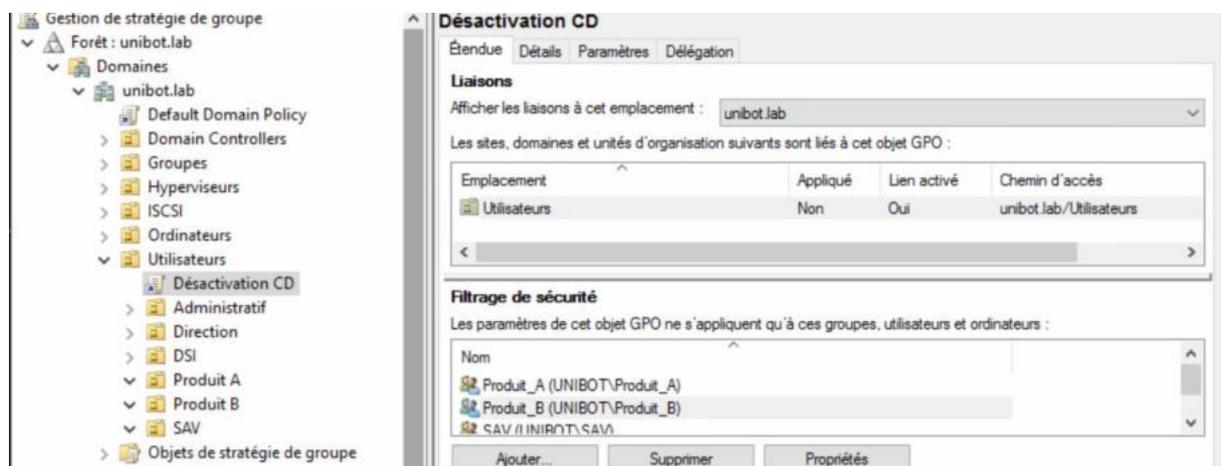
6.3.10 Désactivation lecteur CD

Afin de désactiver le lecteur CD pour les services Produit A et B, nous allons mettre en place une GPO

Dans GPMC.msc, Créer une stratégie « Désactivation CD » puis modifiez là : Dérouler la **Configuration utilisateurs** et aller dans : **Stratégies, Modèles d'administration, Système, Accès au stockage amovible**, puis modifier les paramètres ci-dessous :



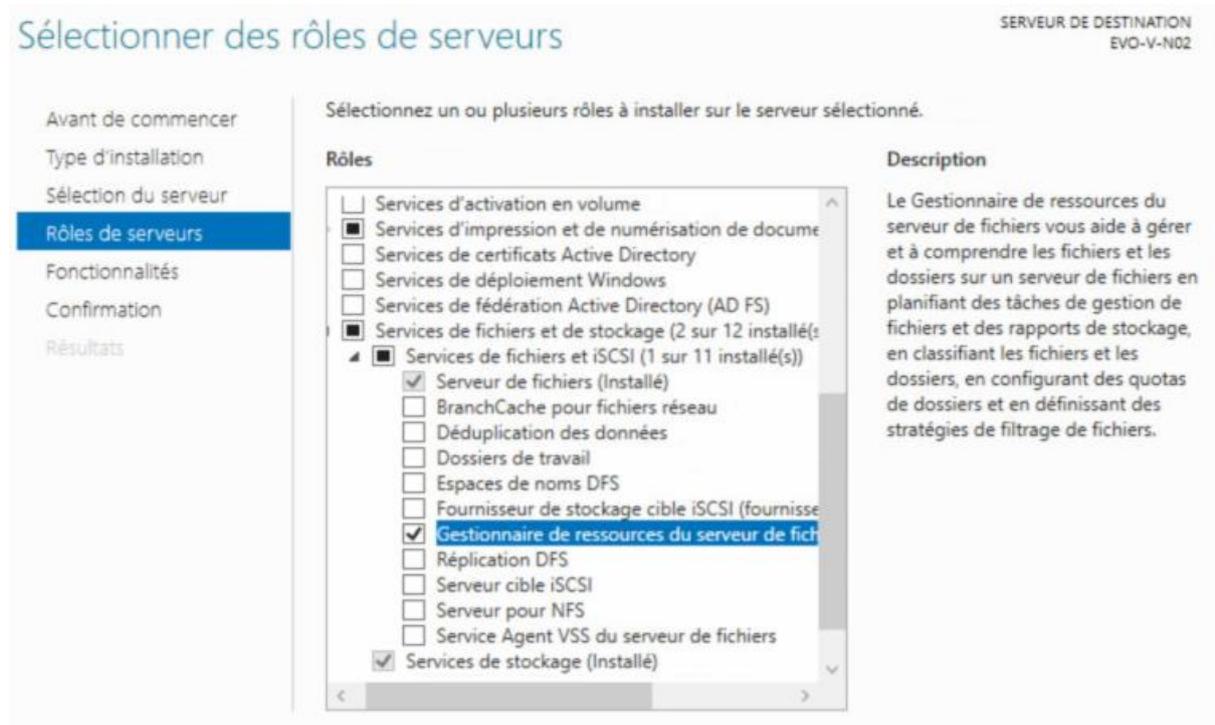
Ajouter les groupes auquel la GPO s'appliquera :



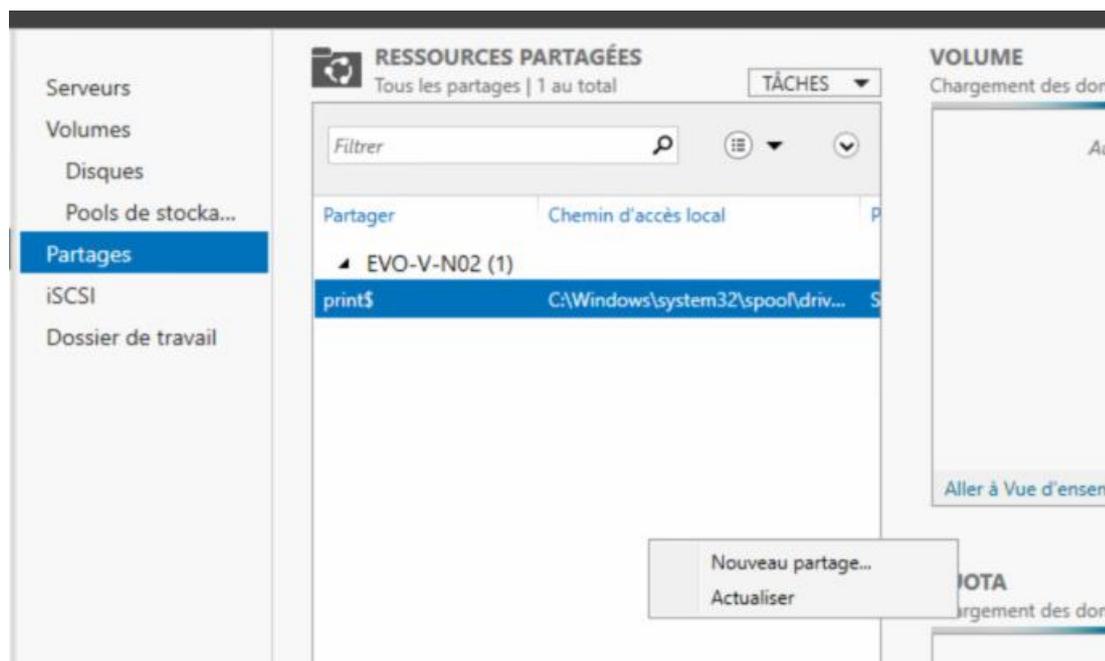


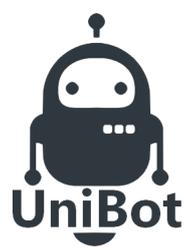
6.3.11 Lecteurs réseau

On commence à installer le service de Gestionnaire de ressources du serveur de fichier sur la machine virtuelle EVO-V-N02 :



Nous allons créer un nouveau dossier partagé : pour cela, nous allons dans l’onglet « Services de fichiers et de stockage » :





Sélectionner le profil de ce partage

Sélectionner un profil

- Emplacement du partage
- Nom de partage
- Autres paramètres
- Autorisations
- Propriétés de gestion
- Quota
- Confirmation
- Résultats

Profil du partage de fichiers :

- Partage SMB - Rapide
- Partage SMB - Avancé**
- Partage SMB - Applications
- Partage NFS - Rapide
- Partage NFS - Avancé

Description :

Ce profil avancé offre des options supplémentaires pour la configuration d'un partage de fichiers SMB.

- Définir les propriétaires du dossier pour une assistance en cas d'accès refusé
- Configurer la classification par défaut des données dans le dossier pour les stratégies de gestion et d'accès
- Activer les quotas

Sélectionner le serveur et le chemin d'accès au partage

Sélectionner un profil

- Emplacement du partage**
- Nom de partage
- Autres paramètres
- Autorisations
- Propriétés de gestion
- Quota
- Confirmation
- Résultats

Serveur :

Nom du serveur	Statut	Rôle du cluster	Nœud propriétaire
EVO-V-N02	En ligne	Non-cluster	

i Cette liste répertorie uniquement les serveurs sur lesquels le Gestionnaire de ressources du serveur de fichiers est installé.

Emplacement du partage :

Sélectionner par volume :

Volume	Espace libre	Capacité	Système de fichiers
C:	17,4 Go	29,5 Go	NTFS

L'emplacement du partage de fichiers sera un nouveau dossier du répertoire \Shares sur le volume sélectionné.

Tapez un chemin personnalisé :



Sélectionner le serveur et le chemin d'accès au partage

Sélectionner un profil

Emplacement du partage

Nom de partage

Autres paramètres

Autorisations

Propriétés de gestion

Quota

Confirmation

Résultats

Serveur :

Nom du serveur	Statut	Rôle du cluster	Noeud propriétaire
EVO-V-N02	En ligne	Non-cluster	

i Cette liste répertorie uniquement les serveurs sur lesquels le Gestionnaire de ressources du serveur de fichiers est installé.

Emplacement du partage :

Sélectionner par volume :

Volume	Espace libre	Capacité	Système de fichiers
C:	17,4 Go	29,5 Go	NTFS

L'emplacement du partage de fichiers sera un nouveau dossier du répertoire \Shares sur le volume sélectionné.

Tapez un chemin personnalisé :

Spécifier les propriétés de gestion des dossiers

Sélectionner un profil

Emplacement du partage

Nom de partage

Autres paramètres

Autorisations

Propriétés de gestion

Quota

Confirmation

Résultats

La propriété Utilisation du dossier spécifie le rôle du dossier et le type de fichiers stockés dans celui-ci. Elle est utilisée par les stratégies de gestion des données, notamment les règles de classification.

Sélectionnez la valeur Utilisation du dossier pour ce dossier :

Fichiers utilisateur

Fichiers de groupe

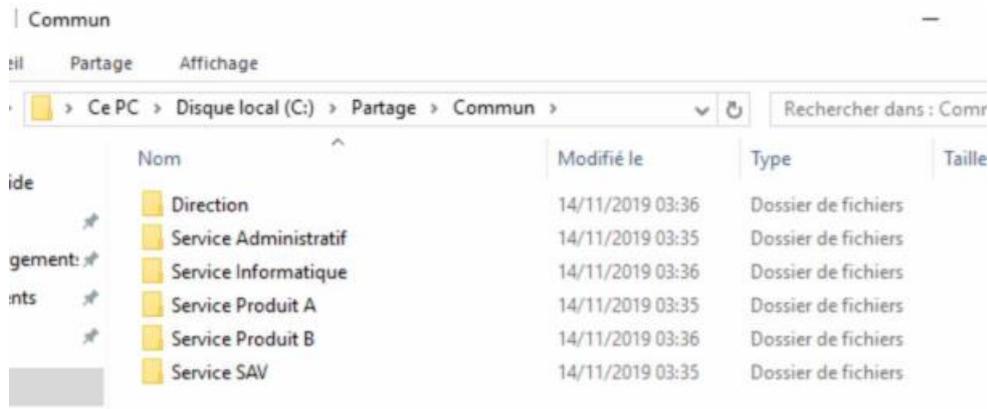
Fichiers d'application

Fichiers de sauvegarde et d'archivage

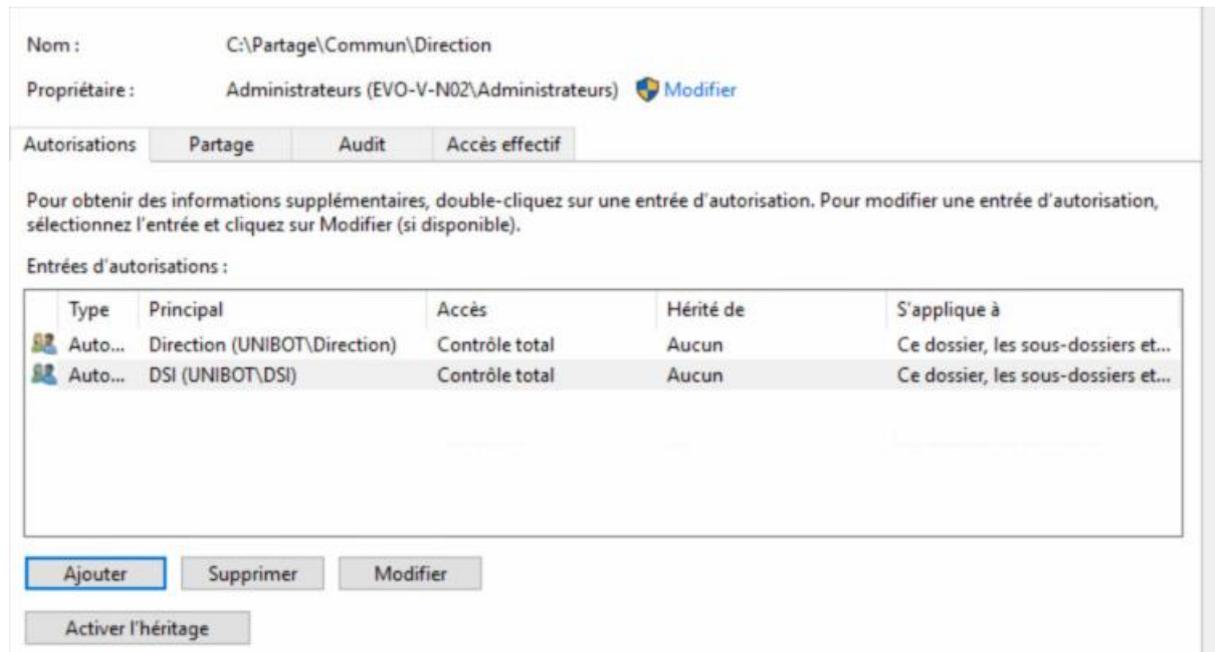
La propriété Adresse de messagerie du propriétaire de dossier spécifie la liste de distribution ou les adresses de messagerie à contacter lorsque les utilisateurs font une demande d'assistance après s'être vus refuser l'accès au dossier.

Spécifiez les adresses de messagerie du propriétaire du dossier (séparées par des points-virgules) :

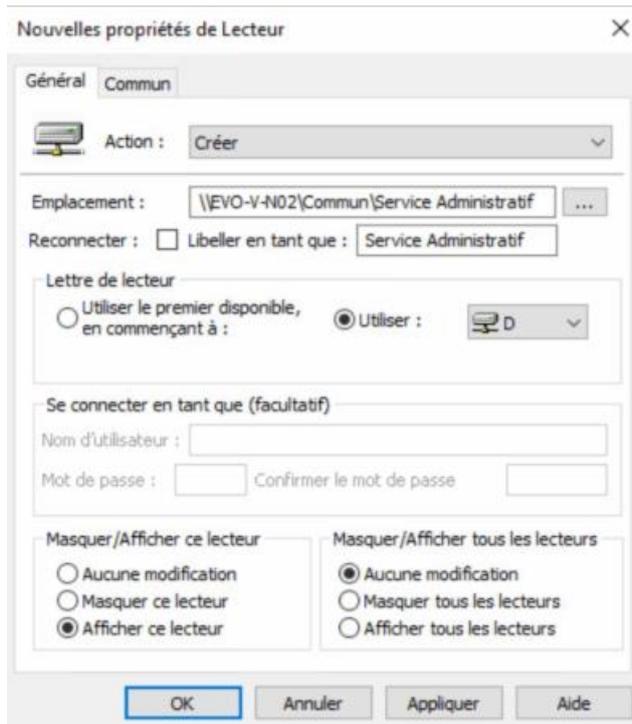
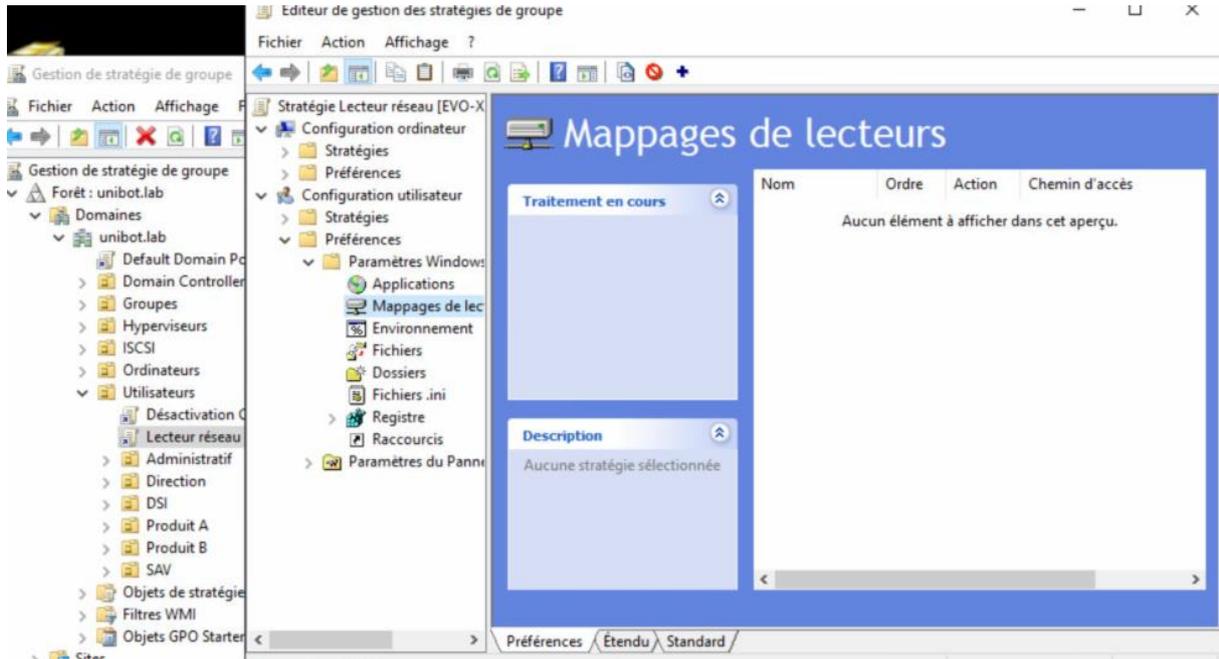
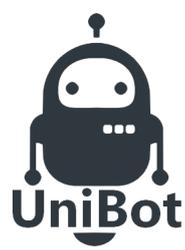
À la suite de la création du dossier partage, nous avons créé des dossiers Commun pour les différents services :



Nous allons maintenant donner les droits à chaque répertoire en fonction des groupes, en autorisant un contrôle total pour le service correspondant ainsi que le service informatique, et en lecture seul pour la direction.



Nous allons maintenant créer une stratégie pour mapper des lecteurs réseaux :

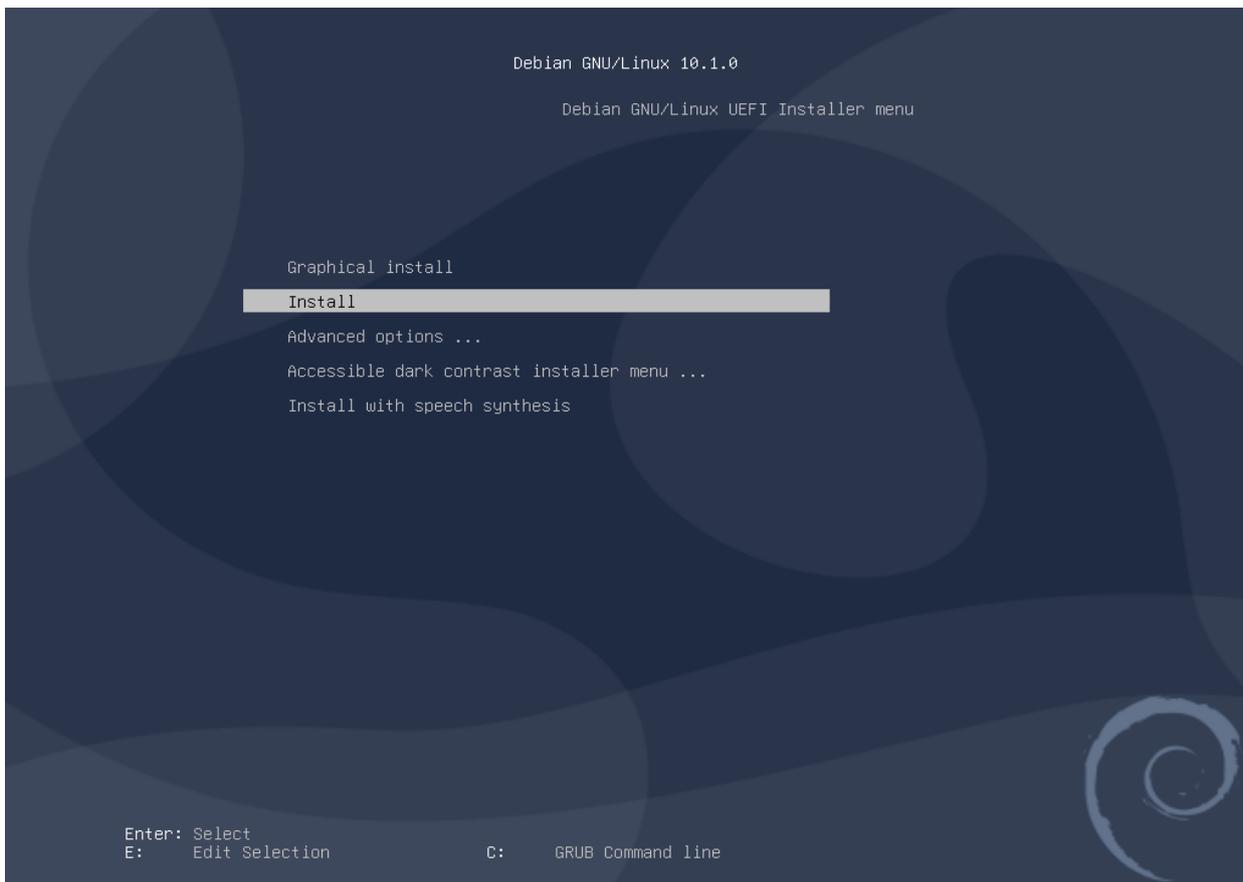




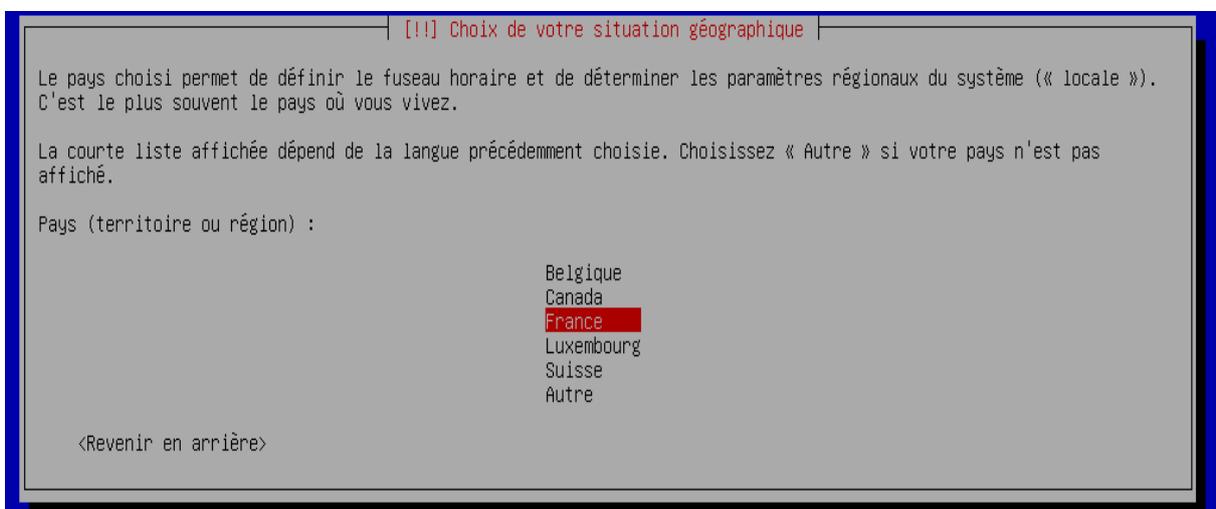
6.4 Installation des services Linux

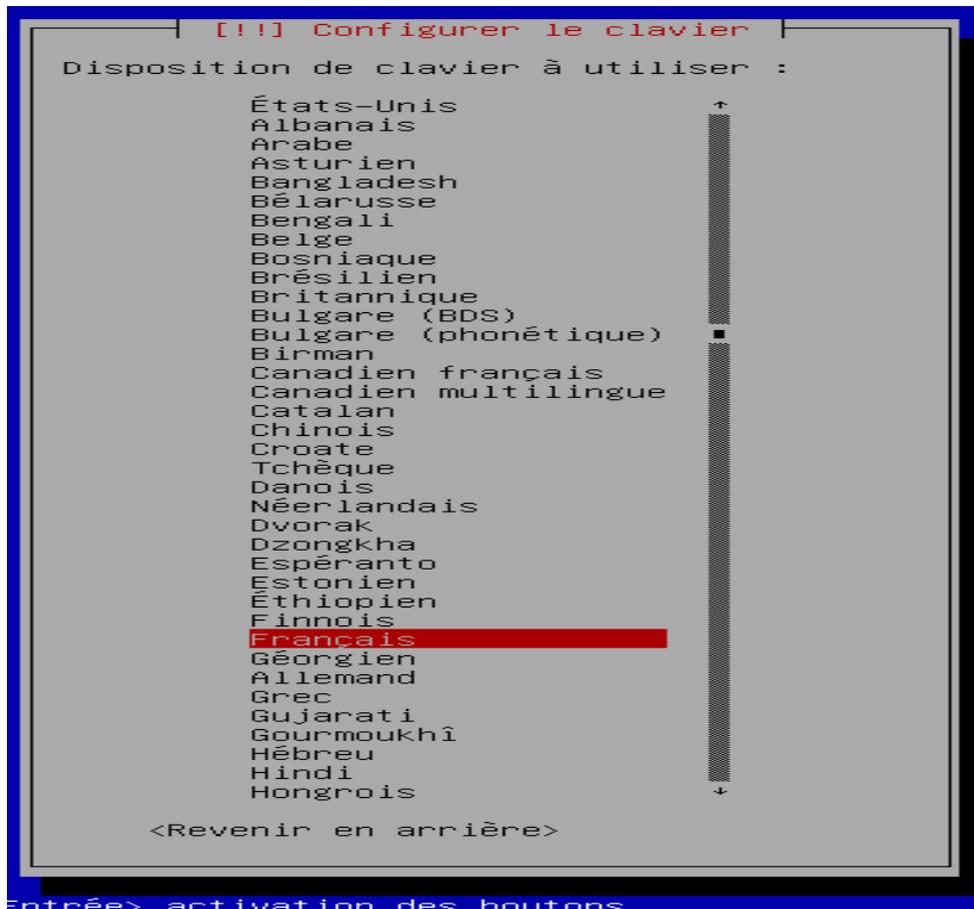
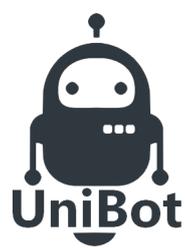
6.4.1 Installation de Debian

Pour commencer, nous devons installer debian sans le mode graphique pour consommer un minimum de ressources :

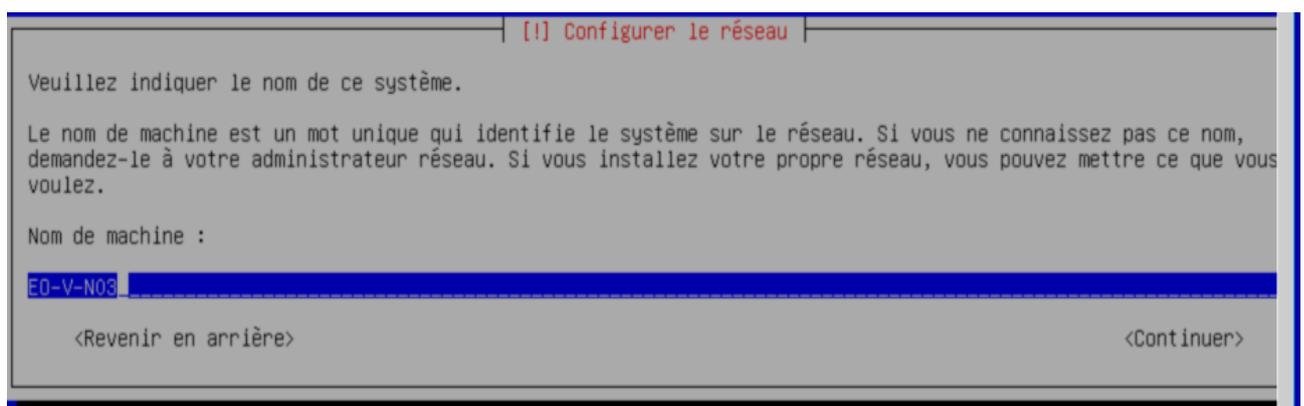


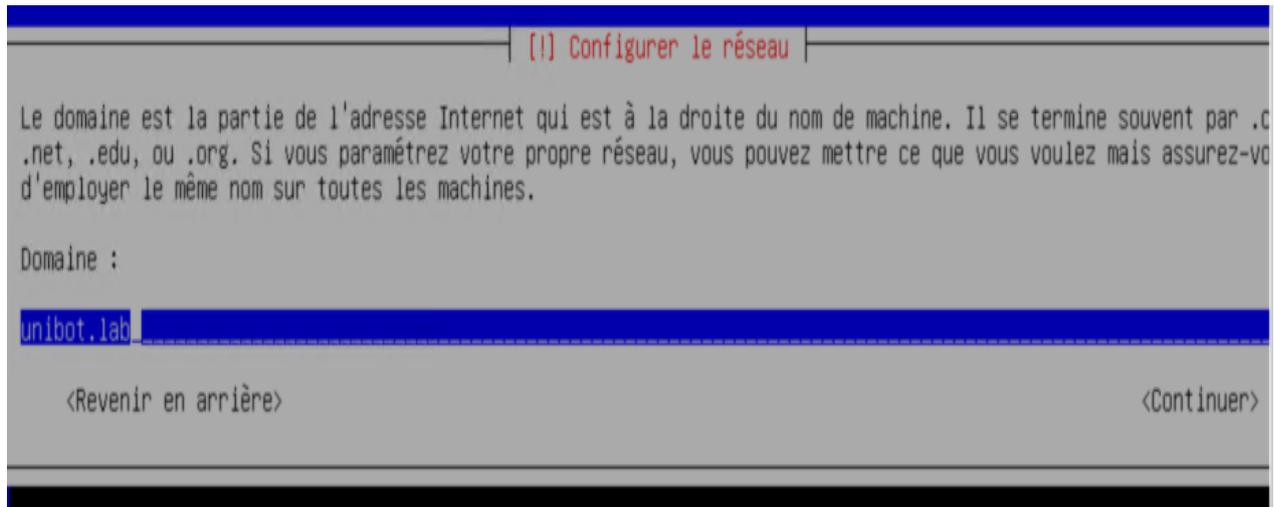
Nous choisissons ensuite notre pays (France) ainsi que la langue du clavier (français).



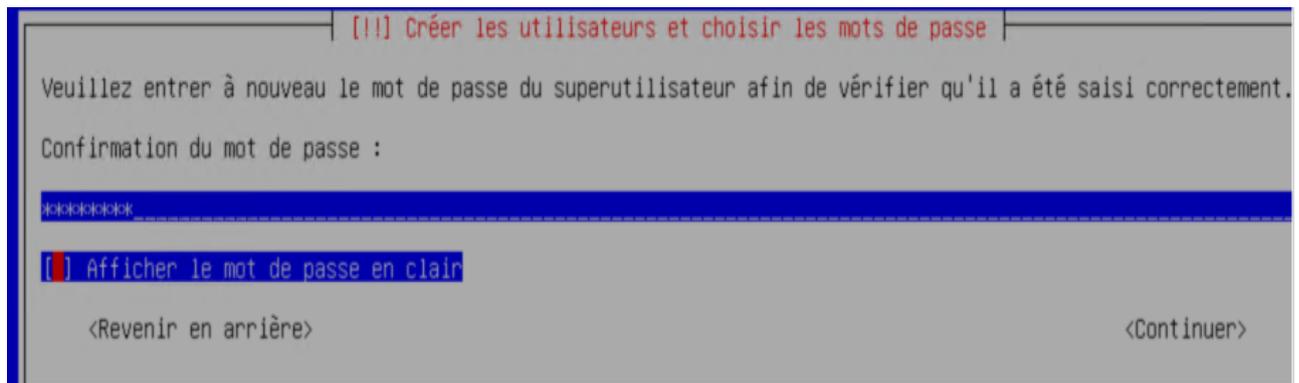


Viens ensuite la configuration réseau : on commence par donner le nom à notre machine (EVO-V-N03) puis on indique le nom du domaine (unibot.lab)

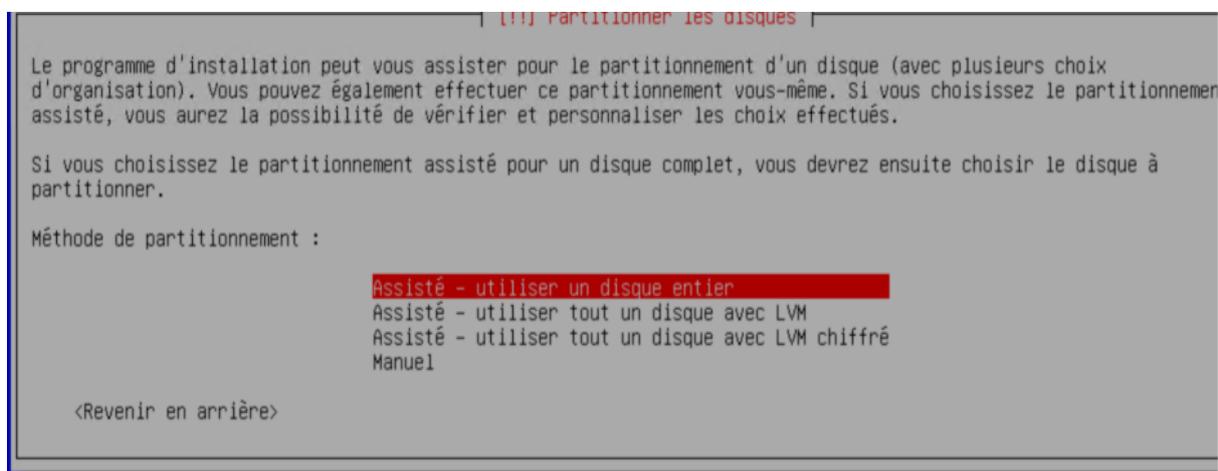




La prochaine étape nécessite seulement de donner le mot de passe au compte administrateur.



Pour la suite, nous sélectionnons assisté (un seul disque) comme méthode de partitionnement et sur une seule partition.





```
[!] Partitionner les disques

Disque partitionné :
SCSI1 (0,0,0) (sda) - Msft Virtual Disk: 21.5 GB

Le disque peut être partitionné selon plusieurs schémas. Dans le doute, choisissez le premier.

Schéma de partitionnement :
    Tout dans une seule partition (recommandé pour les débutants)
    Partition /home séparée
    Partitions /home, /var et /tmp séparées

<Revenir en arrière>
```

La prochaine étape est importante : c'est la configuration de l'outil de gestion de paquet. En effet, pouvoir télécharger des paquets est essentiel pour pouvoir installer des fonctionnalités sur son serveur. On sélectionne France comme pays du miroir de l'archive Debian :

```
[!] Configurer l'outil de gestion des paquets

L'objectif est de trouver un miroir de l'archive Debian qui soit proche de vous du point de vue du réseau. Gardez à l'esprit que le fait de choisir un pays proche, voire même votre pays, n'est peut-être pas le meilleur choix.

Pays du miroir de l'archive Debian :

    Saisie manuelle
    Afrique du Sud
    Allemagne
    Argentine
    Arménie
    Australie
    Autriche
    Belgique
    Brésil
    Bulgarie
    Bélarus
    Canada
    Chili
    Chine
    Corée, République de
    Costa Rica
    Croatie
    Danemark
    Espagne
    Estonie
    Finlande
    France
    Grèce
    Géorgie
    Hong-Kong
    Hongrie
    Inde
    Indonésie
    Iran, République islamique d'
    Israël
    Italie
    Japon
    Kazakhstan
    Kenya

<Revenir en arrière>
```



On choisit ftp.fr.debian.org comme miroir de l'archive Debian.

```

[!] Configurer l'outil de gestion des paquets

Veillez choisir un miroir de l'archive Debian. Vous devriez utiliser un miroir situé dans votre pays ou votre région si vous ne savez pas quel miroir possède la meilleure connexion Internet avec vous.

Généralement, deb.debian.org est un choix pertinent.

Miroir de l'archive Debian :

ftp.fr.debian.org
debian.proxad.net
deb-mir1.naitways.net
debian.univ-lorraine.fr
ftp.u-picardie.fr
ftp.u-strasbg.fr
deb.debian.org
debian-archive.trafficmanager.net
ftp.ec-m.fr
mirror.plusserver.com
debian.mirror.ate.info
debian.univ-tlse2.fr
ftp.rezopole.net
debian.univ-reims.fr
ftp.univ-pau.fr
mirrors.ircam.fr
ftp.crihan.fr
debian.mirrors.ovh.net
ftp.lip6.fr
ftp.iut-bm.univ-fcomte.fr
debian.polytech-lille.fr

<Revenir en arrière>
    
```

Pour terminer l'installation, nous prenons serveur SSH et utilitaires usuels du logiciel comme logiciel à installer.

```

[!] Sélection des logiciels

Actuellement, seul le système de base est installé. Pour adapter l'installation à vos besoins, vous pouvez choisir d'installer un ou plusieurs ensembles prédéfinis de logiciels.

Logiciels à installer :

[ ] environnement de bureau Debian
[ ] ... GNOME
[ ] ... Xfce
[ ] ... KDE Plasma
[ ] ... Cinnamon
[ ] ... MATE
[ ] ... LXDE
[ ] ... LXQt
[ ] serveur web
[ ] serveur d'impression
[*] serveur SSH
[*] utilitaires usuels du système

<Continuer>
    
```

Le serveur linux est maintenant prêt à être utilisé. Il nous faut maintenant rentrer l'adresse ip de la machine. Pour cela nous tapons nano



/etc/network/interfaces en tant que root, et nous configurons le fichier ainsi :

```
# This file describes the network interfaces available on your system
19 and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
allow-hotplug eth0 iface
eth0 inet static
address 192.168.1.13
netmask 255.255.255.0
gateway 192.168.1.1
dns-nameservers 192.168.1.5 192.168.1.10
```

Nous rentrons ensuite la commande `#systemctl restart networking` pour redémarrer la carte réseau avec la nouvelle configuration.

6.4.2 Configuration du Debian

Avant d'installer et de configurer samba, nous devons rentrer la machine linux dans le domaine. Pour se faire, on rentre la commande suivante : `realm join --user=Administrateur@unibot.lab unibot.lab`

Une fois la commande exécutée on effectue un `realm list` pour vérifier que l'intégration au domaine c'est bien fait :

```
root@EVO-V-N03:~# realm list
unibot.lab
  type: kerberos
  realm-name: UNIBOT.LAB
  domain-name: unibot.lab
  configured: kerberos-member
  server-software: active-directory
  client-software: winbind
  required-package: winbind
  required-package: libpam-winbind
  required-package: samba-common-bin
  login-formats: unibot/%U
  login-policy: allow-any-login
root@EVO-V-N03:~#
```

Nous devons maintenant utiliser kerberos pour se connecter à l'AD. Pour se faire, nous devons avoir moins de 5 minutes d'écart entre notre serveur Debian et le contrôleur de domaine.



Il faut commencer par rentrer la commande `apt-get install ntpdate` puis on configure le fichier en lançant la commande `nano /etc/default/ntpdate`.

```
# The settings in this file are used by the program ntpdate-debian, but not
# by the upstream program ntpdate.

# Set to "yes" to take the server list from /etc/ntp.conf, from package ntp,
# so you only have to keep it in one place.
NTPDATE_USE_NTP_CONF=no

# List of NTP servers to use (Separate multiple servers with spaces.)
# Not used if NTPDATE_USE_NTP_CONF is yes.
NTPSERVERS="EVO-X-N01.unibot.lab EVO-V-N01.unibot.lab"

# Additional options to pass to ntpdate
NTPOPTIONS="-u"
```

On lance la synchronisation avec la commande qui nous retourne des données, signifiant que la synchronisation est réussie :

```
root@EVO-V-N03:~# /usr/sbin/ntpdate-debian
14 Nov 16:41:06 ntpdate[2968]: adjust time server 2a02:8429:8230:f701:c5f7:41a4:7167:6bee offset -0.007316 sec
```

Nous installons kerberos et nous configurons le fichier avec la commande `nano /etc/krb5.conf`

```
GNU nano 3.2 /etc/krb5.conf

[libdefaults]
    default_realm = UNIBOT.LAB
    forwardable = true
    proxiable = true
    dns_fallback = no

# The following encryption type specification will be used by MIT Kerberos
# if uncommented. In general, the defaults in the MIT Kerberos code are
# correct and overriding these specifications only serves to disable new
# encryption types as they are added, creating interoperability problems.
#
# The only time when you might need to uncomment these lines and change
# the encyptypes is if you have local software that will break on ticket
# caches containing ticket encryption types it doesn't know about (such as
# old versions of Sun Java).
#
#    default_tgs_encytypes = des3-hmac-sha1
#    default_tkt_encytypes = des3-hmac-sha1
#    permitted_encytypes = des3-hmac-sha1

# The following libdefaults parameters are only for Heimdal Kerberos.
    fcc-mit-ticketflags = true

[realms]
    UNIBOT.LAB = {
        kdc = EVO-X-N01.unibot.lab
        kdc = EVO-V-N01.unibot.lab
        admin_server = EVO-X-N01.unibot.lab
        default_domain = UNIBOT.LAB
    }

[domain_realm]
    .unibot.lab = UNIBOT.LAB
    unibot.lab = UNIBOT.LAB
```



6.4.3 Samba

Nous allons maintenant éditer le fichier de configuration de samba avec la commande nano /etc/samba/smb.conf ,ce qui nous permettra d'accéder aux répertoires partagés depuis les postes clients.

```
[global]
workgroup = unibot
realm = unibot.lab
winbind separator = /
password server = EVO-X-N01.unibot.lab,*
netbios name = debian
os level = 66
#wins server = yes
#wins server = 192.168.1.10
domain master = yes
local master = no
security = ADS
encrypt password = yes

[COMMUN]
writeable = yes
guest ok = yes
public = yes
path = /var/COMMUN
locking = no
write list = @"utilisateurs du domaine@unibot.lab"
browsable = yes
valid users = @"utilisateurs du domaine@unibot.lab"
```



[DIRECTION]

writeable = yes

public = yes

guest ok = no

path = /var/COMMUN DIRECTION

browsable = yes

#read only = no

writeable = no

write list = @"direction@unibot.lab ", @"dsi@unibot.lab "

valid users = @"direction@unibot.lab ", @"dsi@unibot.lab "

[SAV]

writeable = yes

public = yes

guest ok = no

path = /var/COMMUN SAV

browsable = yes

read only = yes

write list = @"dsi@unibot.lab ", @"sav@unibot.lab "

valid users =@"direction@unibot.lab ", @"dsi@unibot.lab ", @"sav@"unibot.lab "

[DSI]

comment = dsi

writeable = yes

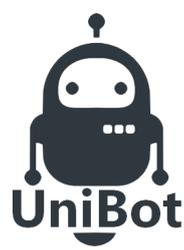
public = yes

guest ok = no

path = /var/DSI

browsable = yes

read only = yes



```
write list = @"dsi@unibot.lab"
```

```
valid users = @"dsi@unibot.lab", @"direction@unibot.lab "
```

```
[PRODUIT_A]
```

```
writeable = yes
```

```
public = yes
```

```
guest ok = no
```

```
path = /var/produit_a
```

```
browsable = yes
```

```
read only = yes
```

```
write list = @"dsi@unibot.lab ", @"produit_a@unibot.lab "
```

```
valid users = @"produit_a@unibot.lab ", @"dsi@unibot.lab ", @"direction@unibot.lab "
```

```
[PRODUIT_B]
```

```
writeable = yes
```

```
public = yes
```

```
guest ok = no
```

```
path = /var/produit_b
```

```
browsable = yes
```

```
read only = yes
```

```
write list = @"dsi@unibot.lab ", @"produit_b@unibot.lab "
```

```
valid users = @"produit_b@unibot.lab ", @"dsi@unibot.lab ", @"direction@unibot.lab "
```

```
[ADMINISTRATIF]
```

```
writeable = yes
```

```
public = yes
```

```
path = /var/administratif
```

```
browsable = yes
```



```
read only = yes
```

```
write list = @"dsi@unibot.lab ", @"administration@unibot.lab "
```

```
valid users = @"administration@unibot.lab ", @"dsi@unibot.lab ", @direction@unibot.lab"
```

Il ne reste plus qu'à donner les permissions aux différents utilisateurs et groupe avec la commande `chmod` ainsi que de mettre en place les ACL sur les différents dossiers personnels des utilisateurs avec la commande `setfacl -m`.

6.4.4 NFS

Commençons par installer paramétrer le serveur nfs :

```
root@EVD-V-N03:/etc/proftpd# apt-get install nfs-kernel-server
```

Avec les commandes suivantes, nous donnons les autorisations aux serveurs clients :

```
chmod 755 /var/          chmod 755 /etc/          chmod 755 /home/
```

Nous allons ensuite rajouter dans le fichier `/etc/exports` les lignes suivantes pour partager le répertoire NFS :

```
/etc 192.168.1.13(sync,no_root_squash)
```

```
/var 192.168.0.13(sync,no_root_squash)
```

```
/home 192.168.0.13(sync,no_root_squash)
```

Pour finir nous mettons à jour la table NFS et nous redémarrons le service :

```
exportfs -r
```

```
systemctl restart nfs
```

Passons maintenant sur le client NFS :

Nous installons nfs avec la même commande que pour le serveur puis nous effectuons un `systemctl enable rpcbind` et `systemctl start rpcbind`.

Avec les commandes suivantes, nous créons les points de montage du répertoire et nous montons le contenu partagé du serveur nfs dans la machine cliente :

```
mkdir /mnt/ home
```

```
mkdir /mnt/var
```

```
mkdir /mnt/etc
```

```
mount 192.168.1.12:/home /mnt/home
```



```
mount 192.168.1.12:/var /mnt/var
```

```
mount 192.168.1.12:/etc /mnt/etc
```

nous vérifions si tout s'est correctement déroulé :

```
mount | grep nfs
```

6.4.5 FTP

Pour commencer nous installons le paquet ProFTPD avec la commande suivante : `apt-get install proftpd`

Nous devons donc configurer le fichier de configuration ProFTPD avec la commande `nano /etc/proftpd/proftpd.conf` :

```
GNU nano 3.2 /etc/proftpd/proftpd.conf Modifie
#
# /etc/proftpd/proftpd.conf -- This is a basic ProFTPD configuration file.
# To really apply changes, reload proftpd after modifications, if
# it runs in daemon mode. It is not required in inetd/xinetd mode.
#
# Includes DSO modules
Include /etc/proftpd/modules.conf

# Set off to disable IPv6 support which is annoying on IPv4 only boxes.
UseIPv6 off
# If set on you can experience a longer connection delay in many cases.
IdentLookups off

ServerName "EVO-X-N01"
# Set to inetd only if you would run proftpd by inetd/xinetd.
# Read README.Debian for more information on proper configuration.
ServerType standalone
DeferWelcome off

MultilineRFC2228 on
DefaultServer on
ShowSymLinks on

TimeoutNoTransfer 600
TimeoutStalled 600
TimeoutIdle 1200

DisplayLogin welcome.msg
DisplayChdir .message true
ListOptions "-l"

DenyFilter \.*/

# Use this to jail all users in their homes
DefaultRoot ~

# Users require a valid shell listed in /etc/shells to login.
# Use this directive to release that constrain.
# RequireValidShell off

# Port 21 is the standard FTP port.
Port 21

# In some cases you have to specify passive ports range to by-pass
# firewall limitations. Ephemeral ports can be used for that, but
# feel free to use a more narrow range.
# PassivePorts 49152 65534
```

```
GNU nano 3.2 /etc/proftpd/proftpd.conf Modifié
#Include /etc/proftpd/ldap.conf
#Include /etc/proftpd/sql.conf

#
# This is used for FTPS connections
#
Include /etc/proftpd/tls.conf

#
# Useful to keep VirtualHost/VirtualRoot directives separated
#
#Include /etc/proftpd/virtuals.conf

# A basic anonymous configuration, no upload directories.

<Anonymous ~ftp>
  User ftp
  Group nogroup
  # We want clients to be able to login with "anonymous" as well as "ftp"
  UserAlias anonymous ftp
  # Cosmetic changes, all files belongs to ftp user
  DirFakeUser on ftp
  DirFakeGroup on ftp

  RequireValidShell off

  # Limit the maximum number of anonymous logins
  MaxClients 10

  # We want 'welcome.msg' displayed at login, and '.message' displayed
  # in each newly chdir'd directory.
  DisplayLogin welcome.msg
  DisplayChdir .message

  # Limit WRITE everywhere in the anonymous chroot
  <Directory *>
    <Limit WRITE>
      DenyAll
    </Limit>
  </Directory>

  # Uncomment this if you're brave.
  # <Directory Incoming>
  # # Umask 022 is a good standard umask to prevent new files and dirs
  # # (second parm) from being group and world writable.
  # Umask <Limit READ WRITE> 022 022
  # #
  # # <Limit READ WRITE>
  # # DenyAll
  # # </Limit>

```

Il suffit de relancer ensuite le serveur ftp avec la commande `systemctl restart proftpd` puis d'installer la version client de filezilla. Pour démarrer le serveur FTP on ouvre Filezilla et on renseigne dans la ligne Hôte le périphérique concerné (192.168.1.12), dans Identifiant (ceux de l'utilisateur avec son domaine, pour notre part se sera utilisateur@unibot.lab), le mot de passe de l'utilisateur ainsi que le Port qui sera en l'occurrence le 22 (SSH). Une fois avoir cliqué sur connexion rapide l'utilisateur sera en possession de son dossier sur le FTP.

6.4.6 GLPI

Pour installer notre glpi nous avons besoin des paquets suivants : apache2 mariadb et php.

```
root@EVO-V-X01N02:~# apt install apache2 php mariadb-server
```

Il faut ensuite modifier le fichier de configuration d'apache avec la commande `nano /etc/apache2/sites-available/000-default.conf`



```

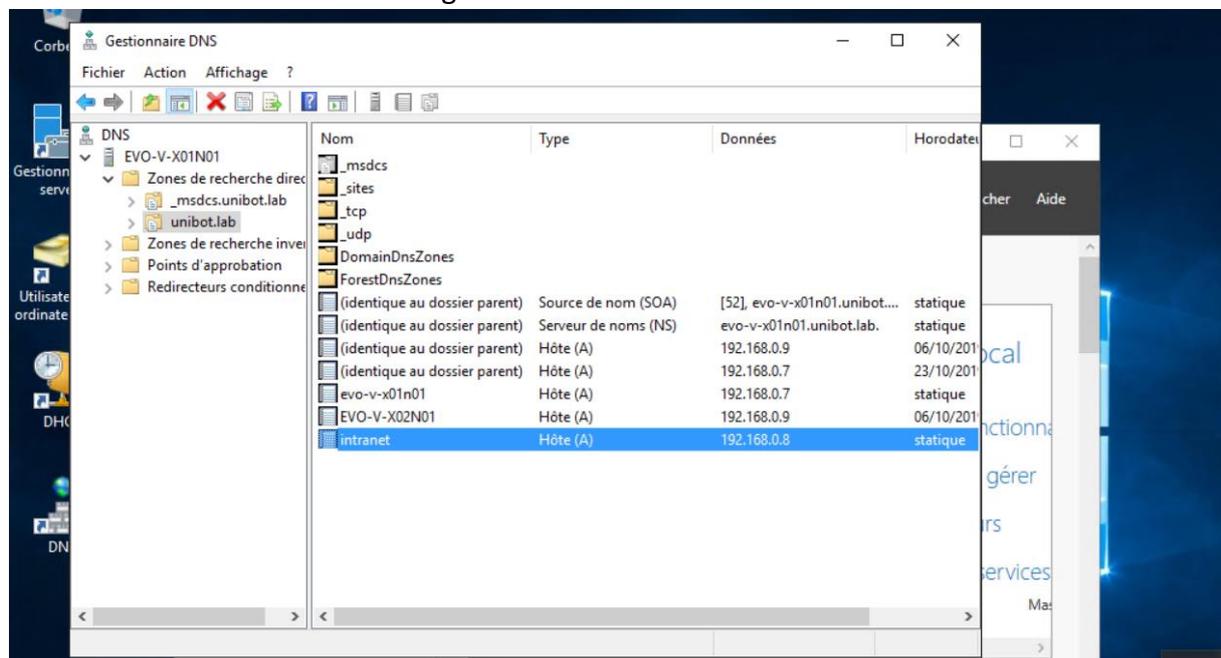
GNU nano 3.2 /etc/apache2/sites-available/000-default.conf Modifié
<VirtualHost *:80>
# The ServerName directive sets the request scheme, hostname and port that
# the server uses to identify itself. This is used when creating
# redirection URLs. In the context of virtual hosts, the ServerName
# specifies what hostname must appear in the request's Host: header to
# match this virtual host. For the default virtual host (this file) this
# value is not decisive as it is used as a last resort host regardless.
# However, you must set it for any further virtual host explicitly.
ServerName intranet.unibot.lab

ServerAdmin webmaster@localhost
DocumentRoot /var/www/glpi

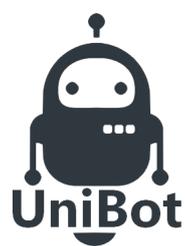
# Available loglevels: trace8, ..., tracel, debug, info, notice, warn,
# error, crit, alert, emerg.
# It is also possible to configure the loglevel for particular
# modules, e.g.
#LogLevel info ssl:warn

[ Lecture de 31 lignes ]
^G Aide      ^O Écrire    ^W Chercher  ^K Couper   ^J Justifier  ^C Pos. cur.
^X Quitter   ^R Lire fich.^\ Remplacer  ^U Coller   ^T Orthograp.^  Aller lig.
    
```

On rajoute le nom du serveur et on modifie le document root pour mettre la page glpi. Il faut ensuite rentrer l'intranet dans le gestionnaire DNS du windows server :



On télécharge ensuite le logiciel glpi, on le décompresse et on finit par l'installation.



```
Debian GNU/Linux 10 EVO-V-X01N02 tty1
EVO-V-X01N02 login: root
Password:
Last login: Wed Oct  9 21:20:02 CEST 2019 on tty1
Linux EVO-V-X01N02 4.19.0-6-amd64 #1 SMP Debian 4.19.67-2+deb10u1 (2019-09-20) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
root@EVO-V-X01N02:~# cd /var/www
root@EVO-V-X01N02:/var/www# wget https://github.com/glpj-project/glpj/releases/download/9.4.4/glpj-9.4.4.tgz
```

```
root@EVO-V-X01N02:/var/www# tar -xzvf glpi-9.4.4.tgz
```

On crée ensuite notre base de données, et on affecte les droits.

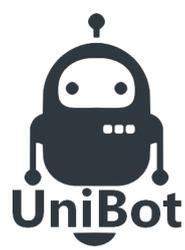
```
MariaDB [(none)]> create DATABASE glpi;
Query OK, 1 row affected (0.000 sec)

MariaDB [(none)]> GRANT ALL PRIVILEGES ON *.* TO 'administrateur'@'localhost' IDENTIFIED BY 'Unibot69';
Query OK, 0 rows affected (0.003 sec)

MariaDB [(none)]>
```

Nous pouvons maintenant nous connecter sur notre glpi en ouvrant une page internet sur notre serveur windows à l'adresse suivante <http://intranet.unibot.lab>



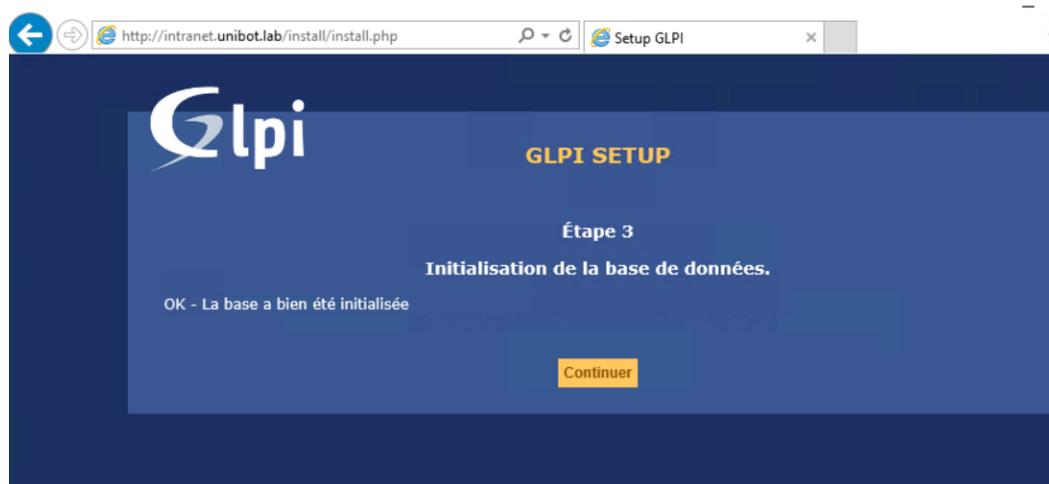


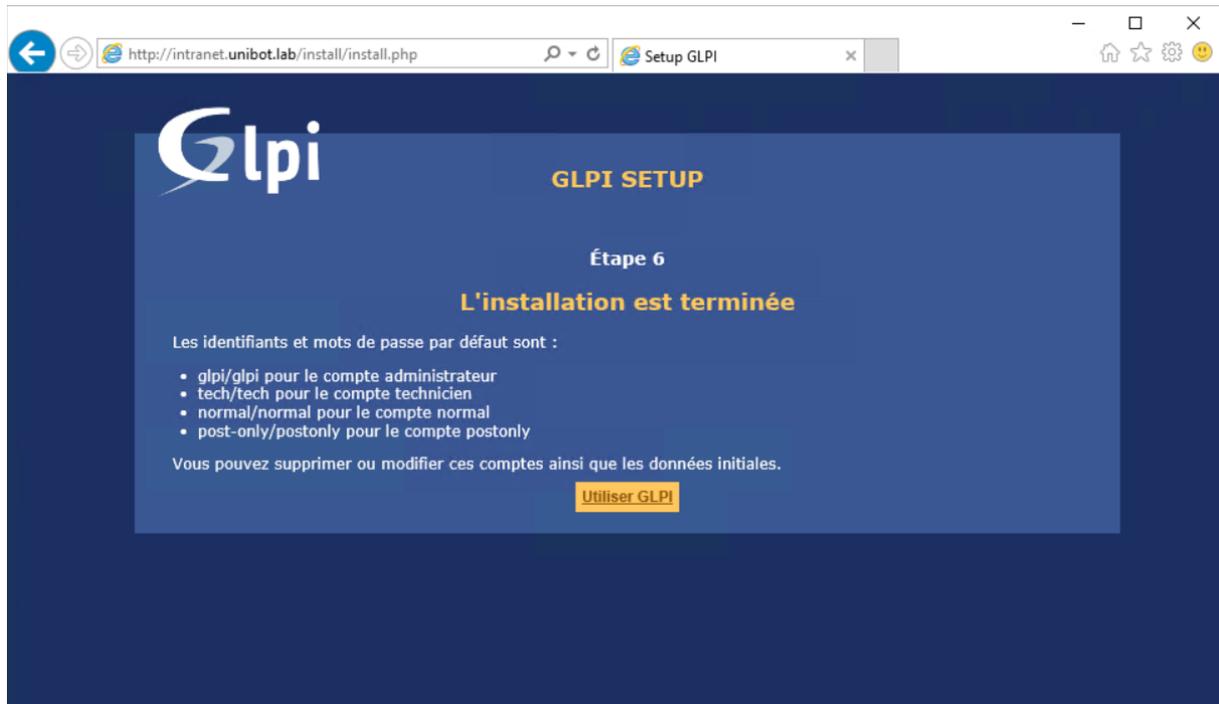
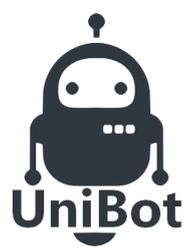
Nous installons les derniers paquets manquant pour l'installation du glpi et on redémarre le service apache.

```
apt install php-mysqli
apt install php-mbstring
apt install php-curl
apt install php-curl
apt install php-gd
apt install php-simplexml

chown -R www-data /var/www/
service apache2 restart
```

On finit par l'installation de glpi





On peut enfin se connecter au glpi.



6.5 Scripts

Afin de mieux gérer l'administration, nous avons mis en place un script permettant de charger une fiche csv avec des informations d'utilisateur et ainsi importer en masse des utilisateurs.

Voici l'affichage du CSV :



	A	B	C	D	E
1	lastName	firstName	password	office	department
2	CHAUVEZE	ABEL	Unibot69	Produit B	Produit_B
3	BRICHASSEC	ADRIEN	Unibot69	Produit B	Produit_B
4	BOISGELOT	AIMERIC	Unibot69	Produit B	Produit_B
5	ROCHEMOND	ALAIN	Unibot69	Produit B	Produit_B
6	BROREL	ALBANIE	Unibot69	Produit B	Produit_B
7	LAURELLI	ALEXANDRA	Unibot69	Produit B	Produit_B
8	MACHELIEU	ALEXINE	Unibot69	Produit B	Produit_B
9	LOMAVAU	ALEXIS	Unibot69	Direction	Direction
10	CAFFAZAC	ALFRED	Unibot69	Produit B	Produit_B
11	RAMBUVILLIE	ALFRED	Unibot69	Produit B	Produit_B
12	ADA	ALICE	Unibot69	SAV	SAV

Voici le script afin d'importer des utilisateurs dans l'AD :

```

Import-Module ActiveDirectory
Import-Module 'Microsoft.PowerShell.Security'

$users = Import-Csv -Delimiter ";" -Path "C:\Users\Administrateur.WIN-0QCSPB33IO5\Desktop\Utilisateurs.csv"

#*****Ajout de chaque utilisateur dans son OU spécifique*****
foreach ($user in $users){

    $name = $user.firstName + " " + $user.lastName
    $fname = $user.firstName
    $lname = $user.lastName
    $login = $user.firstName + "." + $user.lastName
    $password = $user.password
    $dept = $user.department

    switch($user.office){
        "Produit A" {$office = "OU=Produit A,OU=Utilisateurs,DC=unibot,DC=lab"}
        "Produit B" {$office = "OU=Produit B,OU=Utilisateurs,DC=unibot,DC=lab"}
        "SAV" {$office = "OU=SAV,OU=Utilisateurs,DC=unibot,DC=lab"}
        "DSI" {$office = "OU=DSI,OU=Utilisateurs,DC=unibot,DC=lab"}
        "Direction" {$office = "OU=Direction,OU=Utilisateurs,DC=unibot,DC=lab"}
        "Administratif" {$office = "OU=Administratif,OU=Utilisateurs,DC=unibot,DC=lab"}
        default {$office = $null}
    }

    try {
        New-ADUser -Name $name -SamAccountName $login -UserPrincipalName $login -DisplayName $name -GivenName $fname -Surname $lname -AccountPassword (ConvertTo-SecureString $password -AsPlainText -Force) -Path $office -Department $dept -Enabled $true
        echo "Utilisateur ajouté : $name"
    } catch{
        echo "utilisateur non ajouté : $name"
    }
}
    
```



Nous avons créé un script permettant de créer des groupes :

```
New-ADGroup -Name Direction -GroupScope Global -GroupCategory Security -Path
"ou=Groupes,dc=unibot,dc=lab"
New-ADGroup -Name SAV -GroupScope Global -GroupCategory Security -Path
"ou=Groupes,dc=unibot,dc=lab"
New-ADGroup -Name Produit_A -GroupScope Global -GroupCategory Security -Path
"ou=Groupes,dc=unibot,dc=lab"
New-ADGroup -Name Produit_B -GroupScope Global -GroupCategory Security -Path
"ou=Groupes,dc=unibot,dc=lab"
New-ADGroup -Name DSI -GroupScope Global -GroupCategory Security -Path
"ou=Groupes,dc=unibot,dc=lab"
New-ADGroup -Name Administratif -GroupScope Global -GroupCategory Security -Path
"ou=Groupes,dc=unibot,dc=lab"
```

Nous avons aussi préparé un script pour intégrer tous les utilisateurs présents dans un service et les ajouter dans un groupe, voici le script :

```
Import-Module ActiveDirectory
Import-Module 'Microsoft.PowerShell.Security'

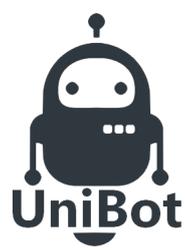
$users = Import-Csv -Delimiter ";" -Path "C:\Users\Administrateur.WIN-
0QCSPB33IO5\Desktop\Utilisateurs.csv"

foreach ($user in $users){

    $name = $user.firstName + " " + $user.lastName
    $fname = $user.firstName
    $lname = $user.lastName
    $login = $user.firstName + "." + $user.lastName
    $upassword = $user.password
    $uoffice = $user.office
    $dept = $user.department

#*****Ajout des utilisateurs dans leurs groupes*****

    if ($dept -eq "Direction"){
        Add-ADGroupMember -Identity 'Direction' -Members $login
    }
    elseif ($dept -eq "SAV"){
        Add-ADGroupMember -Identity 'SAV' -Members $login
    }
    elseif ($dept -eq "DSI"){
        Add-ADGroupMember -Identity 'DSI' -Members $login
    }
    elseif ($dept -eq "Administratif"){
        Add-ADGroupMember -Identity 'Administratif' -Members $login
    }
    elseif ($dept -eq "Produit_A"){
        Add-ADGroupMember -Identity 'Produit_A' -Members $login
    }
    elseif ($dept -eq "Produit_B"){
```



```
Add-ADGroupMember -Identity 'Produit_B' -Members $login
```

```
{
```

6.6 Devis

Devis pour 4 serveurs physiques de chez LENOVO :



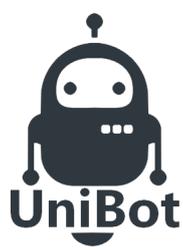
		Votre contact : Pole Internet Pro LDLC.PRO eMail : conseil@ldlc.pro Tél. : 04 27 46 60 05 Fax : 04 26 68 17 98		Référence : E69RESTAR1301 / serveur lenovo Date de l'offre : 13/11/2019 - Délai de validité : 1 semaine GROUPE LDLC 2 RUE DES ERABLES CS21035 69578 LIMONEST CEDEX Tél. : +33 (0) 4 72 52 37 65															
Client Destinataire Restart ARGENTIERI Gabriel 19 Avenue Guy de Collongue 69130 ÉCULLY FRANCE			Client Facturé Restart ARGENTIERI Gabriel 19 Avenue Guy de Collongue 69130 ÉCULLY FRANCE																
Réf	Désignation	Qté	Px Unit. (€)	Remise (%)	Mnt HT (€)														
S0472048	Lenovo ThinkSystem ST250 (7Y45A02BE4)	4	999,12		3 996,50														
Conditions de règlement : A l'ordre de Groupe LDLC Virement Domiciliation : CA St DIDIER Banque Guichet Compte Clé 17806 00679 92903591000 38			GARANTIE : Les étiquettes collées sur les pièces neuves sont nécessaires pour la garantie. Les emballages doivent être conservés.		<table border="1"> <tr><td>Port Liv. Standard :</td><td>55,00</td></tr> <tr><td>Total remise produit HT :</td><td>0,00</td></tr> <tr><td>Remise complémentaire HT :</td><td>0,00</td></tr> <tr><td>Total HT :</td><td>4 051,50</td></tr> <tr><td> Dont éco-participation :</td><td>0,00</td></tr> <tr><td>Total TVA :</td><td>810,30</td></tr> <tr><td>Total TTC (€)</td><td>4 861,80</td></tr> </table>	Port Liv. Standard :	55,00	Total remise produit HT :	0,00	Remise complémentaire HT :	0,00	Total HT :	4 051,50	Dont éco-participation :	0,00	Total TVA :	810,30	Total TTC (€)	4 861,80
Port Liv. Standard :	55,00																		
Total remise produit HT :	0,00																		
Remise complémentaire HT :	0,00																		
Total HT :	4 051,50																		
Dont éco-participation :	0,00																		
Total TVA :	810,30																		
Total TTC (€)	4 861,80																		
Bon pour accord (Signature et cachet) Toute commande est soumise aux conditions générales de vente ci-jointes, dont j'accepte tous les termes et conditions.																			
GROUPE LDLC - SA à directoire et conseil de surveillance au capital de 1 137 979.08 € - 403 554 181 RCS Lyon - NAF 4791B - N° T.V.A. FR 26403554181, N° T.V.A Belge BE 0863283964, N° T.V.A Luxembourg LU 26459700, N° Suisse CHE-136.085.276 TVA, Siret 403 554 181 00178 Page 1/3																			

Devis pour 18 disques dur de 1To pour les serveurs :



		Votre contact : Pole Internet Pro LDLC.PRO eMail : conseil@ldlc.pro Tél. : 04 27 46 60 05 Fax : 04 26 68 17 98		Devis : DV201911130003 Référence : E69RESTAR1301 / DISQUES DUR Date de l'offre : 13/11/2019 - Délai de validité : 1 semaine GROUPE LDLC 2 RUE DES ERABLES CS21035 69578 LIMONEST CEDEX Tél. : +33 (0) 4 72 52 37 65															
Client Destinataire Restart ARGENTIERI Gabriel 19 Avenue Guy de Collongue 69130 ÉCULLY FRANCE			Client Facturé Restart ARGENTIERI Gabriel 19 Avenue Guy de Collongue 69130 ÉCULLY FRANCE																
Réf	Désignation	Qté	Px Unit. (€)	Remise (%)	Mnt HT (€)														
S0121920	Western Digital WD Black Desktop 1 To SATA 6Gb/s	18	71,62		1 289,25														
Conditions de règlement : A l'ordre de Groupe LDLC Virement Domiciliation : CA St DIDIER Banque Guichet Compte Clé 17806 00679 92903591000 38		GARANTIE : Les étiquettes collées sur les pièces neuves sont nécessaires pour la garantie. Les emballages doivent être conservés.		<table border="1"> <tr> <td>Port Liv. Standard :</td> <td>14,95</td> </tr> <tr> <td>Total remise produit HT :</td> <td>0,00</td> </tr> <tr> <td>Remise complémentaire HT :</td> <td>0,00</td> </tr> <tr> <td>Total HT :</td> <td>1 304,20</td> </tr> <tr> <td>Dont éco-participation :</td> <td>0,00</td> </tr> <tr> <td>Total TVA :</td> <td>260,84</td> </tr> <tr> <td>Total TTC (€)</td> <td>1 565,04</td> </tr> </table>		Port Liv. Standard :	14,95	Total remise produit HT :	0,00	Remise complémentaire HT :	0,00	Total HT :	1 304,20	Dont éco-participation :	0,00	Total TVA :	260,84	Total TTC (€)	1 565,04
Port Liv. Standard :	14,95																		
Total remise produit HT :	0,00																		
Remise complémentaire HT :	0,00																		
Total HT :	1 304,20																		
Dont éco-participation :	0,00																		
Total TVA :	260,84																		
Total TTC (€)	1 565,04																		
Bon pour accord (Signature et cachet) Toute commande est soumise aux conditions générales de vente ci-jointes, dont j'accepte tous les termes et conditions.																			
GROUPE LDLC - SA à directeur et conseil de surveillance au capital de 1 137 979.08 € - 403 554 181 RCS Lyon - NAF 4791B - N° T.V.A. FR 26403554181, N° T.V.A Belge BE 0863283964, N° T.V.A Luxembourg LU 26459700, N° Suisse CHE-136.085.276 TVA., Siret 403 554 181 00178 Page 1/3																			

Devis pour 6 licences Windows serveur 2016 standard pour les serveurs physique et virtuel :



	<p>Votre contact : Pole Internet Pro LDLC.PRO eMail : conseil@ldlc.pro Tél. : 04 27 46 60 05 Fax : 04 26 68 17 98</p>	<p>Référence : E69RESTAR1301 /</p> <p>Date de l'offre : 13/11/2019 - Délai de validité : 1 semaine GROUPE LDLC 2 RUE DES ERABLES CS21035 69578 LIMONEST CEDEX Tél. : +33 (0) 4 72 52 37 65</p>			
Client Destinataire	Client Facturé				
<p>Restart ARGENTIERI Gabriel 19 Avenue Guy de Collongue 69130 ÉCULLY FRANCE</p>	<p>Restart ARGENTIERI Gabriel 19 Avenue Guy de Collongue 69130 ÉCULLY FRANCE</p>				
Réf	Désignation	Qté	Px Unit. (€)	Remise (%)	Mnt HT (€)
PB002491	Microsoft Windows Server Standard 2016 (16 coeurs)	6	699,95		4 199,70
<p>Bon pour accord (Signature et cachet)</p> <p><small>Toute commande est soumise aux conditions générales de vente ci-jointes, dont j'accepte tous les termes et conditions.</small></p>					
GROUPE LDLC - SA à directoire et conseil de surveillance au capital de 1 137 979.08 € - 403 554 181 RCS Lyon - NAF 4791B - N° T.V.A. FR 26403554181, N° T.V.A Belge BE 0863283964, N° T.V.A Luxembourg LU 26459700, N° Suisse CHE-136.085.276 TVA., Siret 403 554 181 00178					
Page 1/3					