




Administration Système et Réseau

Le projet :

- 1- Créer une application Web en **Html/Css et JavaScript** et une api en ASP.NET Web API 6.
- 2- Installer et configurer le serveur web **Apache2** sur le serveur linux **Debian 192.168.153.131** afin de pouvoir héberger l'app web.
- 3- Installer et configurer le serveur web **Nginx** pour héberger l'app web sur le serveur **CentOS 192.168.153.133**.
- 4- Installer et configurer le serveur web **IIS** sur le contrôleur de domaine **Windows 192.168.153.130**.
- 5- Installer et configurer un serveur **Jenkins** sur **192.168.153.132** qui permettra de déployer et intégrer de façon continue les sources de l'application web sur les différents nœuds (Linux **Debian**, **CentOS** et **Windows**).
- 6- Faire la même chose que (5) mais déployer sur des workers d'un node master **Kubernetes**.
- 7- Configurer **Jenkins** pour déployer automatiquement sur le serveur linux **Debian et CentOS** les sources de l'application au moment du merge sur la branche master de **GitHub**.
- 8- Ne pas installer docker sur le serveur linux cible **Debian** mais d'ajouter un plugins **Docker** dans **Jenkins** afin de Builder le **Dockerfile** ou même de lancer le conteneur.
- 9- Créer un serveur de base de données **MSSQL** définit dans le contrôleur de domaine **192.168.153.130**.
- 10-Créer une image pour une **API** web en NET6.0 définit dans un service **Docker**.
- 11-Installer et configurer l'utilitaire **Traefik** permettant de concilier dans le même réseau les deux services **Docker (api et App)**.
 -  Caching
 -  Répartition de charges
 -  SSL/TLS
- 12- On va utiliser **Traefik** de deux façons :
 - Avec un fournisseur docker
 - Avec un fournisseur kubernetes
- 13-Installer et configurer un **DOZZLE** permettant de lire les logs des applications isolées dans **Docker**.

14-Utiliser **Ansible** notamment les rôles ansible pour déployer les configurations automatiquement sur le serveur Linux **Debian et CentOS**.

15-Installation de **Grafana** pour contrôler et monitorer les **VM**.

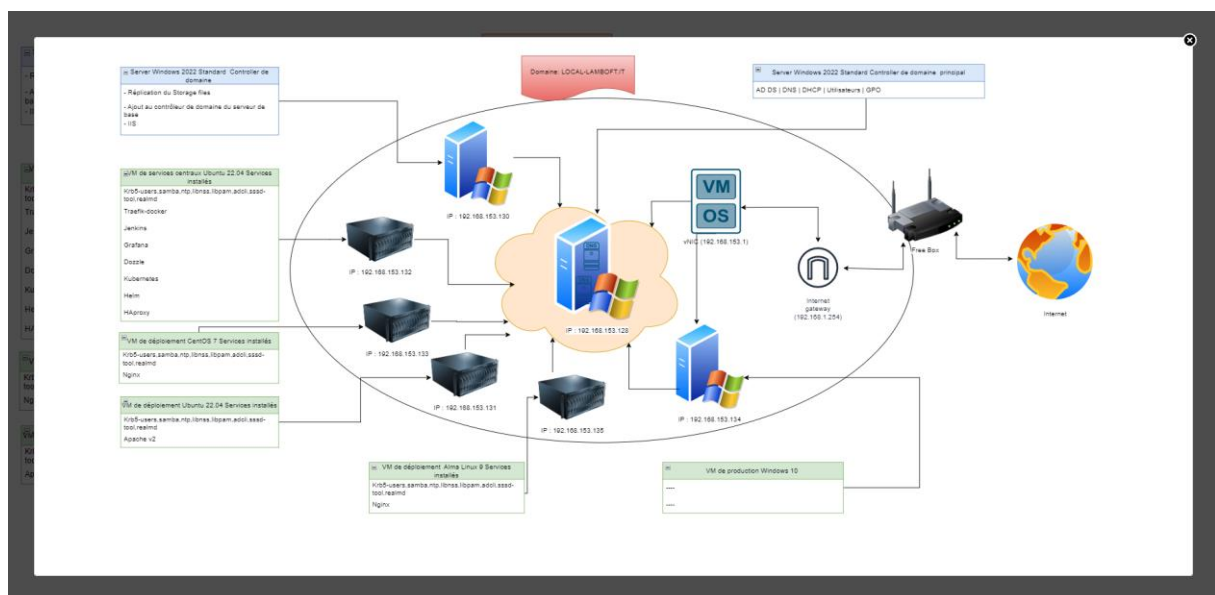
16-Plugger **prométhéums** , **Traefik** et **Grafana** ???

Préparation des serveurs de développement et de production pour le projet

On va se basé sur le schéma suivant pour constituer notre propre écosystème de développement et de déploiement.

Nous allons alterner entre administration de OS et réseau au sein de ces OS. Plusieurs concepts vont être évoqués notamment : DNS , DHCP, ADDS, Passerelle par défaut et Proxy.

I Architecture system



A) Configuration d'hyperviseur VMWare et Installation des serveurs

Dans l'hyperviseur VMware, nous allons créer l'ensemble des machines évoquées dans le schéma ci-haut tout en rajoutant les paramètres réseau et fonctionnalités nécessaires.

❖ Sur le serveur distant **LOCAL-LAMBOFT.IT**

On va configurer **OpenSSH server**

L'objectif est de pouvoir établir une connexion SSH de notre machine de travail TLA vers la machine physique contenant notre hyperviseur.

Ouvrir PowerShell en tant qu'administrateur

Vérifier la présence de OpenSSH Server sur la machine

```
PS C:\Windows\System32> get-windowsCapability -Online | Where-Object Name -like 'OpenSSH*'

Name : OpenSSH.Client~~~~0.0.1.0
State : NotPresent

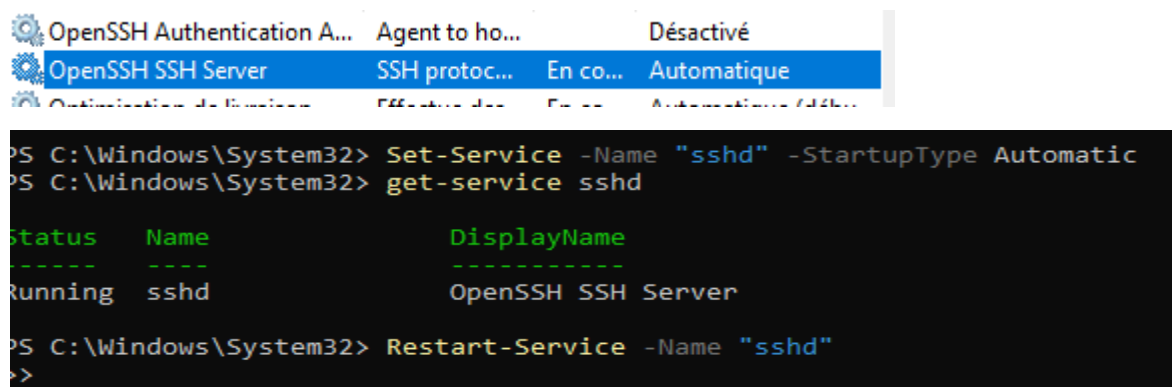
Name : OpenSSH.Server~~~~0.0.1.0
State : NotPresent
```

L'installer via GUI ou en CLI

```
Add-WindowsCapability -Online -Name OpenSSH.Server~~~~0.0.1.0
```



Démarrer le service sshd et setter son démarrage en automatique en CLI ou sur le GUI



Configurer le fichier sshd_config dans C:\ProgramData\ssh et changer le port 22 en 222 puis ajouter une règle au pare-feu Windows

```
PS C:\Windows\System32> New-NetFirewallRule -Name sshd -DisplayName 'OpenSSH Server (sshd) - Port 222' -Enabled True -Direction Inbound -Protocol TCP -Action Allow -LocalPort 222

Name : sshd
DisplayName : OpenSSH Server (sshd) - Port 222
Description :
DisplayGroup :
Group :
Enabled : True
Profile : Any
Platform : {}
Direction : Inbound
Action : Allow
EdgeTraversalPolicy : Block
LooseSourceMapping : False
LocalOnlyMapping : False
Owner :
PrimaryStatus : OK
Status : La règle a été analysée à partir de la banque. (65536)
EnforcementStatus : NotApplicable
PolicyStoreSource : PersistentStore
PolicyStoreSourceType : Local
RemoteDynamicKeywordAddresses :
PolicyApplia :
```

Redémarrer le service sshd

Désactiver ceci

```
#Match Group administrators
#AuthorizedKeysFile __PROGRAMDATA__/ssh/administrators_authorized_keys
```

Cela permettra d'utiliser la directive DenyGroups

```
AllowGroups administrateurs
AllowGroups lft.net\UO_Admin
AllowGroups lft.net\UO_Others
```

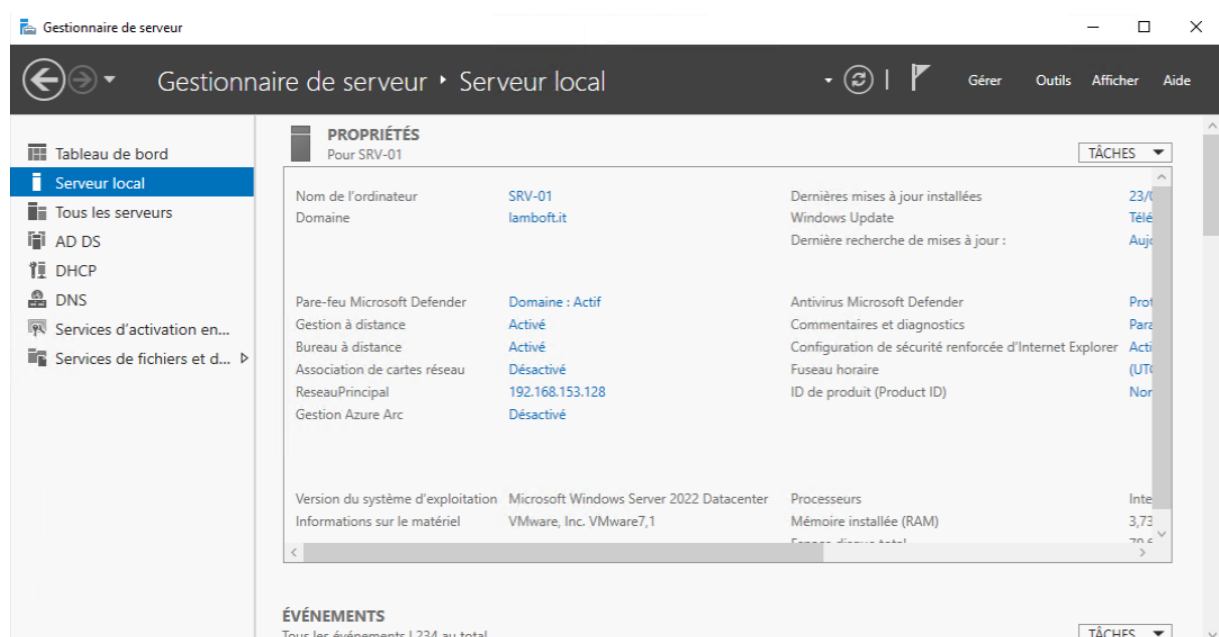
UO_Admin et **UO_Others** sont des groupes créés pour notre domaine AD.

a) Windows server 2022 Standard 192.168.153.128

C'est le serveur de base dans lequel on va créer notre active directory, configurer les serveurs DNS , DHCP, le stockage de fichiers potentiellement les utilisateurs et stratégie de groupe pour ces utilisateurs.

Avant toutes configurations sur les fonctionnalités on va potentiellement changer le nom de l'ordinateur, son adresse IP, le nom du réseau et le domaine.

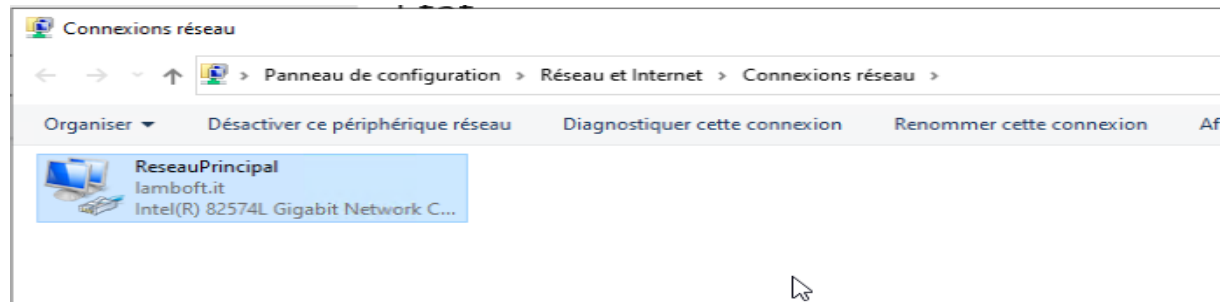
On veut en arriver là :




srvr-01 : Nom du serveur ou de l'ordinateur

LOCAL-LAMBOFT.IT.IT : Nom du domaine ou de la forêt

ReseauPrincipal : le nom que l'on souhaite attribuer à l'interface réseau de cette VM
serveur + IP du serveur



 Serveur DNS <192.168.153.128>

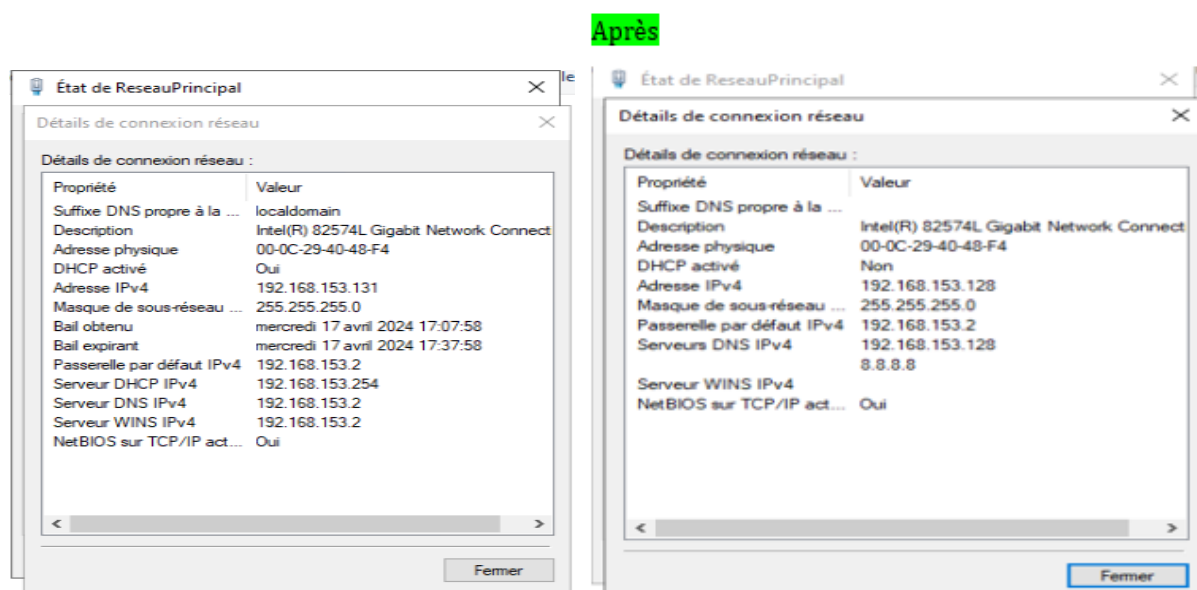
Outils >> Ajouter les fonctionnalités >> Cocher DNS >> Terminer. Ensuite promouvoir au Contrôleur de domaine.

Remarque : Sur la carte Réseau du serveur il est préférable lors de la première connexion de regarder d'abord le statut du réseau. Car de base le réseau est connecté à internet en se basant sur la connectivité local (Box Wifi)

Ce pourquoi : Parceque de base, la VM est créée sur l'hyperviseur et a comme connecteur ou topologie réseau un NAT (qui fait de la translation d'adresse IP de la vm vers une IP publique permettant d'accéder au réseau externe à savoir l'interface réseau de la carte réseau physique de l'hôte sur lequel l'hyperviseur est installé le fameux NIC).

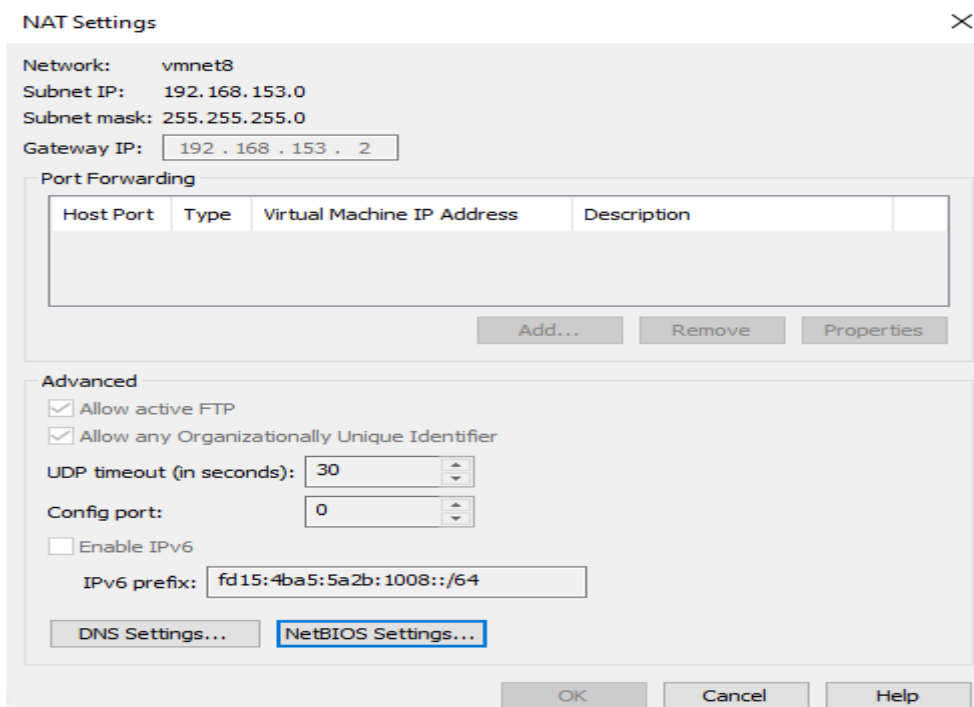
Ça aurait été un Host Only que la VM ne serait pas connecté à internet.

Avant



Conclusion : Au lieu d'attendre de créer la VM d'aller regarder dans sa configuration réseau pour voir l'IP de la passerelle permettant à la machine d'atteindre internet on doit :

- Aller sur **VM Ware >> View >> Virtual Network Editor >> vNIC**
- Vérifier la topologie réseau (NAT ou Bridge afin de se connecter au NIC et ainsi dit avoir accès à internet)
- Cliquer sur NAT settings



A partir de là on voit bien que la passerelle ou la **Gateway** c'est 192.168.153.2

Problème : On arrive plus à pinguer nos VMS depuis l'hôte physique

- Pas de soucis avec le pare-feu sur le protocole ICMP sur les connexions entrantes/sortantes
- Pas de soucis avec la connectivité réseau
- **Pb de route**

Solution : On va créer une route entre notre subnet d'IP 192.168.153.0/24 et la passerelle 192.168.153.2 afin de permettre à notre hôte physique de

Sur le pc 192.168.1.12 :

- route print -4

Pour afficher toutes les routes sur les adresses IPv4

- route -p add 192.168.153.0 mask 255.255.255.0 192.168.153.2 metric 1

Comme on peut bien le voir avec WireShark le trafic passe bien

VMware Network Adapter VMnet8

Fichier Editur Vue Aller Capture Analyser Statistiques Telephonie Wireless Outils Aide

Appliquer un filtre d'affichage ... < Ctrl-/>

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|----------|-----------------|-----------------|----------|--------|---|
| 1 | 0.000000 | 192.168.153.1 | 192.168.153.132 | HTTP | 657 | GET /api/overview HTTP/1.1 |
| 2 | 0.001515 | 192.168.153.132 | 192.168.153.1 | HTTP/1.1 | 647 | HTTP/1.1 200 OK, JSON (application/json) |
| 3 | 0.021414 | 192.168.153.132 | 192.168.153.255 | NBNS | 92 | Name query NB LAMBOFT<Id> |
| 4 | 0.053995 | 192.168.153.1 | 192.168.153.132 | TCP | 54 | 22697 → 9091 [ACK] Seq=604 Ack=594 Win=4101 Len=0 |
| 5 | 1.109207 | 192.168.153.128 | 45.79.47.151 | DNS | 205 | Dynamic update 0x3bba SOA 18e28bbe-f911-4638-be98-15edda5bc3eb._msdcs.lft.net CNAME CNA |
| 6 | 1.195599 | 192.168.153.1 | 192.168.153.132 | ICMP | 74 | Echo (ping) request id=0x0001, seq=22/5632, ttl=128 (reply in 7) |
| 7 | 1.195874 | 192.168.153.132 | 192.168.153.1 | ICMP | 74 | Echo (ping) reply id=0x0001, seq=22/5632, ttl=64 (request in 6) |
| 8 | 2.027716 | 192.168.153.132 | 192.168.153.255 | NBNS | 92 | Name query NB LAMBOFT<Id> |
| 9 | 2.028614 | 192.168.153.132 | 192.168.153.255 | NBNS | 92 | Name query NB LAMBOFT<Id> |
| 10 | 2.206464 | 192.168.153.1 | 192.168.153.132 | ICMP | 74 | Echo (ping) request id=0x0001, seq=23/5888, ttl=128 (reply in 11) |
| 11 | 2.206938 | 192.168.153.132 | 192.168.153.1 | ICMP | 74 | Echo (ping) reply id=0x0001, seq=23/5888, ttl=64 (request in 10) |
| 12 | 3.228026 | 192.168.153.1 | 192.168.153.132 | ICMP | 74 | Echo (ping) request id=0x0001, seq=24/6144, ttl=128 (reply in 13) |
| 13 | 3.221401 | 192.168.153.132 | 192.168.153.1 | ICMP | 74 | Echo (ping) reply id=0x0001, seq=24/6144, ttl=64 (request in 12) |
| 14 | 4.035549 | 192.168.153.132 | 192.168.153.255 | NBNS | 92 | Name query NB LAMBOFT<Id> |
| 15 | 4.036506 | 192.168.153.132 | 192.168.153.255 | BROWSER | 225 | Browser Election Request |
| 16 | 4.235577 | 192.168.153.1 | 192.168.153.132 | ICMP | 74 | Echo (ping) request id=0x0001, seq=25/6400, ttl=128 (reply in 17) |
| 17 | 4.236009 | 192.168.153.132 | 192.168.153.1 | ICMP | 74 | Echo (ping) reply id=0x0001, seq=25/6400, ttl=64 (request in 16) |
| 18 | 4.990999 | 192.168.153.1 | 192.168.153.132 | HTTP | 657 | GET /api/overview HTTP/1.1 |
| 19 | 4.992604 | 192.168.153.132 | 192.168.153.1 | HTTP/1.1 | 647 | HTTP/1.1 200 OK, JSON (application/json) |
| 20 | 5.043530 | 192.168.153.1 | 192.168.153.132 | TCP | 54 | 22697 → 9091 [ACK] Seq=1207 Ack=1187 Win=4106 Len=0 |

Avec cette configuration réseau, notre serveur **srv-01** est en même temps capable d'atteindre internet mais aussi de résoudre les noms de domaine.

Propriétés de : Protocole Internet version 4 (TCP/IPv4)

Général

Les paramètres IP peuvent être déterminés automatiquement si votre réseau le permet. Sinon, vous devez demander les paramètres IP appropriés à votre administrateur réseau.

☐ Obtenir une adresse IP automatiquement

☒ Utiliser l'adresse IP suivante :

Adresse IP : 192 . 168 . 153 . 128

Masque de sous-réseau : 255 . 255 . 255 . 0

Passerelle par défaut : 192 . 168 . 153 . 2

☐ Obtenir les adresses des serveurs DNS automatiquement

☒ Utiliser l'adresse de serveur DNS suivante :

Serveur DNS préféré : 192 . 168 . 153 . 128

Serveur DNS auxiliaire : 8 . 8 . 8 . 8

☐ Valider les paramètres en quittant

Avancé...

OK Annuler

On a changer l'ip de la vm juste la classe D 192.168.153.**131** en 192.168.153.**128**

Ceci dans le but de personnaliser notre propre ip de la VM

On a rajouté la passerelle qui nous avait été proposé au départ 192.168.153.2

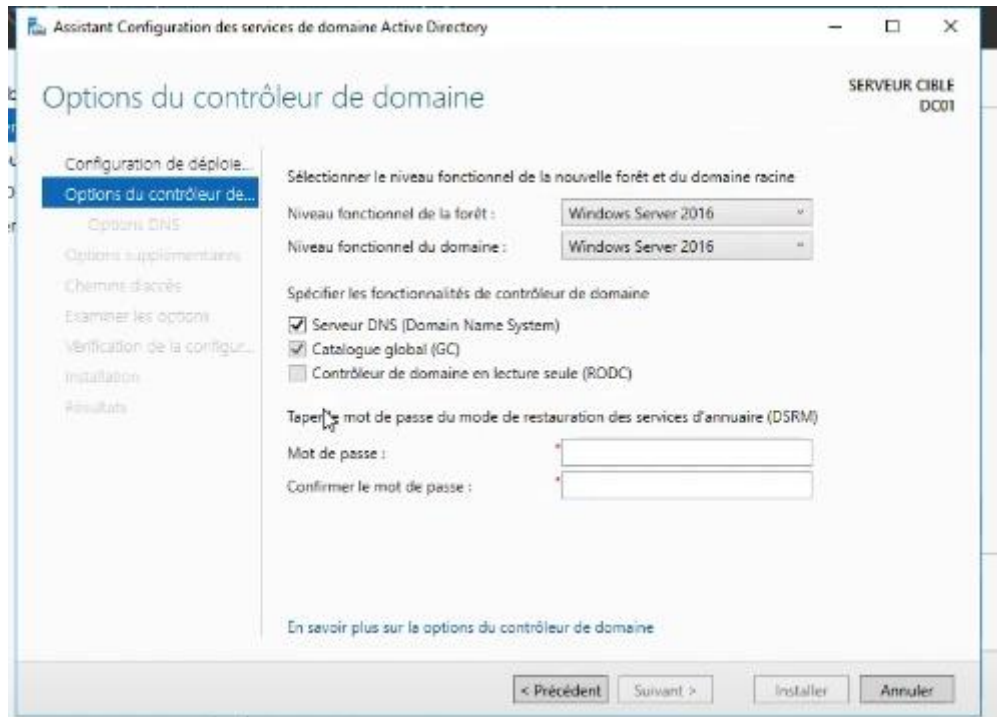
Dans le serveur DNS on veut que la VM soit son propre DNS d'où son IP est le meme que l'IP de la VM

DNS auxiliaire 8.8.8.8 afin de permettre le trafic public entrant.

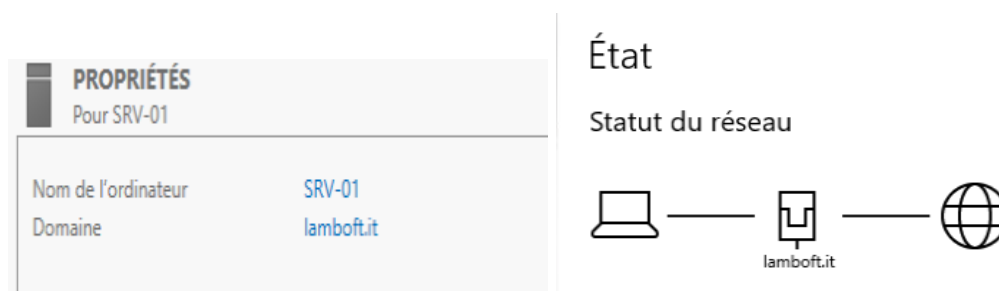
Où on définit le serveur DNS par l'IP du serveur sur lequel on va installer la fonctionnalité DNS.

Pour définir la forêt, on va : **Cliquer Domaine > Modifier > Saisir un nom de domaine**

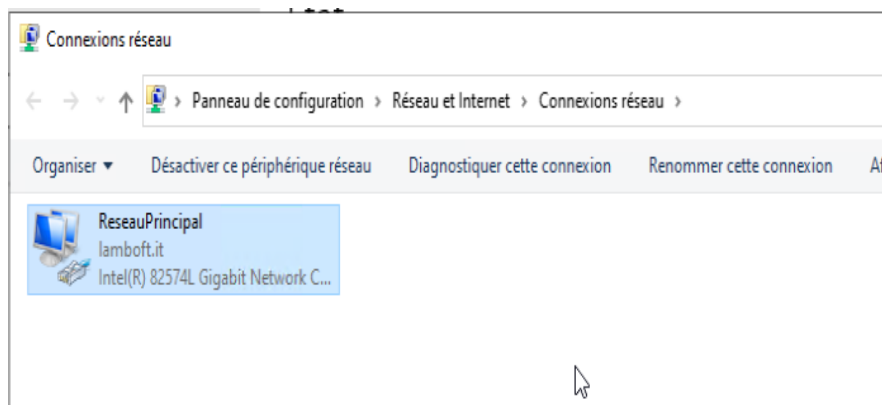
Dans le processus de définition de la forêt, on devra gérer DSRM pour la restauration du service d'annuaire si jamais on a un souci avec AD



A la fin on devra obtenir ceci sur notre serveur local



Et Ceci sur notre carte réseau et sur les paramètres réseau



NB : Dans notre exemple notre serveur ou **vm** sera son propre serveur DNS et passerelle pour les autres machines ajoutées au domaine **LOCAL-LAMBOFT.IT.IT**

- **RRAS** (Remote Route Access Service)

C'est grâce à ce service qu'on va pouvoir faire de notre serveur DNS 192.168.153.128 un routeur.

Configuration du Serveur Windows (RRAS)

1. Installation du rôle RRAS :

- Ouvrez le **Gestionnaire de serveur**.
- Cliquez sur **Ajouter des rôles et des fonctionnalités**.
- Sélectionnez **Installation basée sur un rôle ou une fonctionnalité** et cliquez sur **Suivant**.
- Cochez la case **Routage et accès distant** sous **Services de rôles** du rôle **Accès à distance**, puis cliquez sur **Suivant** et installez.

2. Configurer le RRAS :

- Une fois l'installation terminée, allez dans **Outils d'administration** et ouvrez **Routage et accès distant**.
- Dans la console **RRAS**, cliquez avec le bouton droit sur votre serveur et sélectionnez **Configurer et activer le routage et l'accès distant**.
- Utilisez l'Assistant pour configurer RRAS :
 - Sélectionnez **Configuration personnalisée**.
 - Choisissez **NAT** (pour permettre à votre VM Ubuntu d'accéder à Internet via le serveur Windows).
 - Complétez l'assistant et démarrez le service.

3. Configurer NAT :

- Dans la console **RRAS**, développez **IPv4** puis cliquez sur **NAT**.
- Cliquez avec le bouton droit sur **NAT** et sélectionnez **Nouvelle interface**.
- Sélectionnez l'interface connectée à Internet (celle qui a accès à votre box).
- Dans les propriétés de l'interface, cochez **Public interface connected to the Internet** et **Enable NAT on this interface**.

- Serveur DHCP <192.168.153.128>

Dynamic Host Control Protocol : On va créer soi-même son propre serveur DHCP et définir l'étendue de la plage d'adresses que l'on souhaite.

| Adresse IP de début | Adresse IP de fin | Description |
|---------------------|-------------------|---------------------------------------|
| 192.168.153.125 | 192.168.153.150 | Plage d'adresses pour la distribution |

De 125-150 la plage d'adresse IP que l'on va attribuer des adresse IP à des VM interagissant avec ce serveur DHCP.

ADDS

Active Directory c'est l'annuaire **Windows** qui va nous permettre de stocker des objets et informations sécurisées relatives à la gestion de nos serveurs des comptes utilisateurs et de services.

On va rajouter les **VM** créées (*Linux* et *Windows server*) dans cette AD aussi les comptes utilisateurs.

L'idée est de pouvoir se connecter sur les machines non plus en créant des comptes sur les machines elles-mêmes mais plutôt en utilisant les comptes AD.

Dans le serveur DNS on peut rajouter à la main les machines et leur adresse IP dans le domaine.

| | Nom | Type | Données | Horodateur |
|----------------------|-------------------------------|----------------------|---------------------------------|---------------------|
| Racine de la console | _msdcs | | | |
| DNS | _sites | | | |
| SRV-01 | _tcp | | | |
| | _udp | | | |
| | DomainDnsZones | | | |
| | ForestDnsZones | | | |
| | (identique au dossier parent) | Source de nom (SOA) | [248], srv-01.lft.net., host... | statique |
| | (identique au dossier parent) | Serveur de noms (NS) | srv-01.lft.net. | statique |
| | (identique au dossier parent) | Serveur de noms (NS) | srv-prod.lft.net. | statique |
| | (identique au dossier parent) | Hôte (A) | 192.168.153.130 | 18/04/2024 00:00:00 |
| | (identique au dossier parent) | Hôte (A) | 192.168.153.128 | 15/05/2024 20:00:00 |
| | srv-01 | Hôte (A) | 192.168.153.128 | statique |
| | SRV-PROD | Hôte (A) | 192.168.153.130 | statique |
| | VM-Client | Hôte (A) | 192.168.153.134 | 17/04/2024 17:00:00 |
| | vms-001-ubuntu | Hôte (A) | 192.168.153.131 | statique |
| | vms-002-ubuntu-cemterServices | Hôte (A) | 192.168.153.132 | statique |
| | vms-003-centos7 | Hôte (A) | 192.168.153.133 | |

Dans la zone de recherche inversée on voit qu'on peut rajouter à la main aussi les IP correspondant au hostname de chaque machine.

| | | | | |
|---|-------------------------------|----------------------|---------------------------------|---------------------|
| Racine de la console | Nom | Type | Données | Horodateur |
| DNS | (identique au dossier parent) | Source de nom (SOA) | [9], srv-01.lft.net., hostma... | statique |
| SRV-01 | (identique au dossier parent) | Serveur de noms (NS) | srv-prod.lft.net. | statique |
| Zones de recherche directes | (identique au dossier parent) | Serveur de noms (NS) | srv-01.lft.net. | statique |
| > _msdcs.lft.net | 192.168.153.128 | Pointeur (PTR) | SRV-01.lft.net. | statique |
| > lft.net | 192.168.153.130 | Pointeur (PTR) | lft.net. | statique |
| Zones de recherche inversée | 192.168.153.130 | Pointeur (PTR) | SRV-PROD.lft.net. | statique |
| > 153.168.192.in-addr.arpa | 192.168.153.131 | Pointeur (PTR) | vms-001-ubuntu.lft.net. | statique |
| > Points d'approbation | 192.168.153.132 | Pointeur (PTR) | vms-002-ubuntu-cernterS... | statique |
| > Redirecteurs conditionnels | 192.168.153.133 | Pointeur (PTR) | vms-003-centos7.lft.net. | statique |
| > Dossiers partagés (local) | 192.168.153.134 | Pointeur (PTR) | VM-Client.lft.net. | 17/04/2024 17:00:00 |
| > DHCP | | | | |
| > Gestion des stratégies de groupe | | | | |
| > Utilisateurs et ordinateurs Active Directory [SI] | | | | |
| > Domaines et approbations Active Directory | | | | |

En somme la configuration DNS implique l'attribution d'adresse IP à des noms de serveurs et ce en spécifiant les enregistrements (NS, SOA, PTR, MX) C'est ce qu'on appelle faire une « **résolution de nom de domaine** ».

Ps : Promouvoir au Contrôleur de domaine les VM Windows server : c'est de cette façon qu'on réussit à les rajouter au Contrôleur de domaine ensuite à l'AD.

Utilisateurs

Dans la section Utilisateurs et ordinateurs active directory on pourra créer et donner les droits à un ou groupe d'utilisateurs pouvant se connecter sur les machines.

GPO (Group Policy Objects)



Définition : Ce sont des objets qui permettent de définir une stratégie de configuration de paramètres relatifs à des utilisateurs ou des groupes d'utilisateurs dans un parc informatique.

En quoi c'est important ?

- On veut une configuration homogène entre toutes les machines du parc informatique d'une entreprise. Idem pour la structure des utilisateurs.
- On veut pouvoir renforcer la sécurité d'une machine dans le parc. Pour ce faire, aller dans le contrôleur de domaine et définir des GPO de sécurité comme cela chaque machine qui arrive sur le réseau récupère directement la stratégie.

Cas pratique :

On souhaite renforcer la sécurité du parc informatique grâce aux GPO.

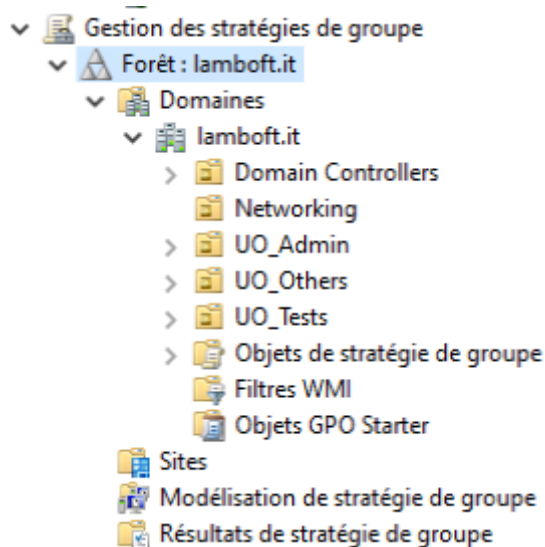
Exemple de GPO de sécurité :

- La gestion de mot de passe (longueur minimale, complexité et l'expiration)
- Paramètres de verrouillage du compte
- La sécurité réseau
- Les permissions et restriction de certains programmes

On va créer une GPO pour la gestion de mot de passe.

Dans notre console on va rajouter le domaine (foret) LOCAL-LAMBOFT.IT.it

Voici l'arborescence de la section stratégie de groupe

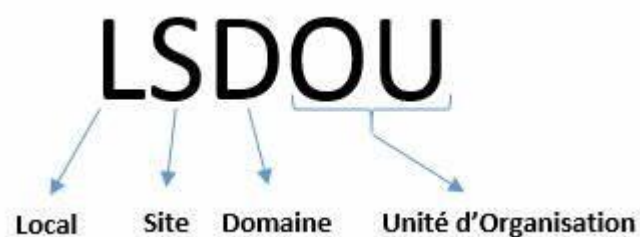


Les types de GPO :

- GPO Locale :
- GPO AD :

La propagation de GPO :

Le principe LSDOU



 Serveur SMTP

On veut pouvoir créer un compte mail pour chaque utilisateur à partir de son compte active directory

Exemple :

artur.lambo@LOCAL-LAMBOFT.IT

yves.makang@LOCAL-LAMBOFT.IT

pecra.cravet@LOCAL-LAMBOFT.IT

On veut que les autres machines puissent utiliser le Dns IP de mon serveur DNS définit dans le **srv-01**.

Première chose à faire aller sur l'hyperviseur **Edit > Virtual Network Editor** et désactiver sur le bridge (dans le cas où le DNS de la machine client a récupérée le IP Dns de localhost) la case **Use local DHCP service**.

Sur le serveur DNS ouvrir l'invite de commande

- ➔ **Ipconfig /release : supp les paramètres du DNS**
- ➔ **Ipconfig /renew : pour ajouter les paramètres du DNS**

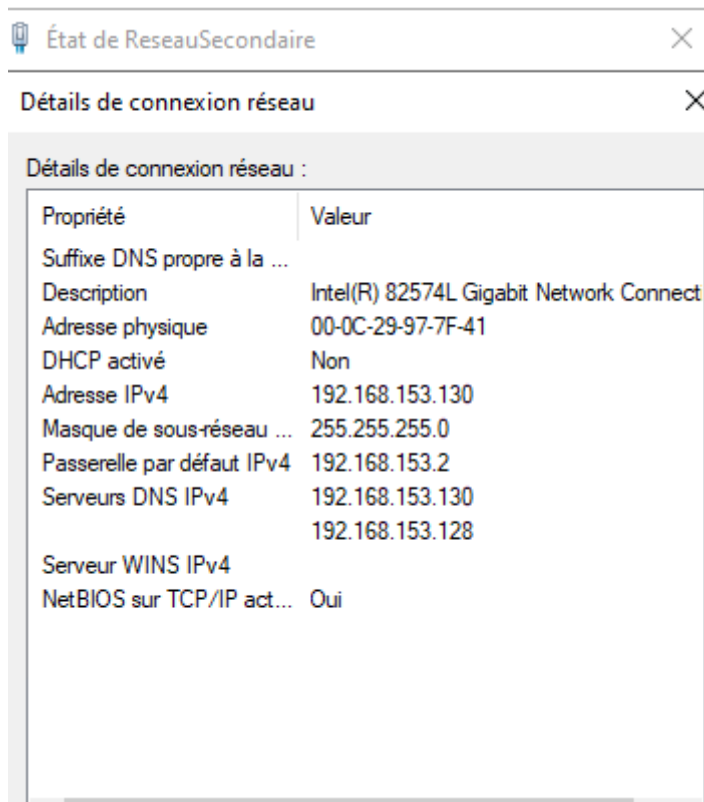
Toutes les prochaines machines qui seront créées devront être rattaché à au domaine **LOCAL-LAMBOFT.IT.IT** et ajouter dans le dossier **computers** de l'AD comme machines du domaine.

| | Nom | Type | Description |
|--|----------------|------------|----------------|
| Racine de la console | | | |
| > DNS | | | |
| > Dossiers partagés (local) | | | |
| > DHCP | | | |
| > Gestion des stratégies de groupe | | | |
| ▼ Utilisateurs et ordinateurs Active Directory [SRV-01.local-lamboft.it] | | | |
| > Requêtes enregistrées | | | |
| ▼ local-lamboft.it | | | |
| > Built-in | | | |
| > Computers | | | |
| > Domain Controllers | | | |
| > ForeignSecurityPrincipals | | | |
| > Managed Service Accounts | | | |
| > Networking | | | |
| > UO_Admin | | | |
| > UO_Others | | | |
| > UO_Tests | | | |
| > Users | | | |
| > Domaines et approbations Active Directory | | | |
| | VMC-CLIENT | Ordinateur | Client windows |
| | VMS-001-UBUNTU | Ordinateur | |
| | VMS-002-SERVER | Ordinateur | |
| | VMS-003-CENTOS | Ordinateur | |

Horodatage :

- L'objectif est de synchroniser la date et l'heure de notre Active Directory à celles des VM qui l'on rejoint

b) Windows server 2022 Standard → 192.168.158.130

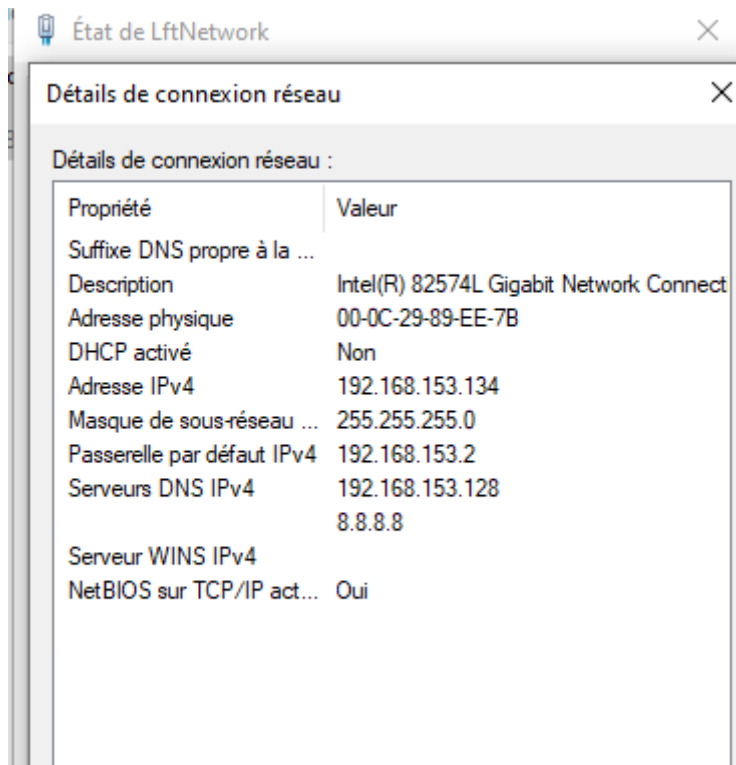


Donc on peut bien voir que cette machine est son propre DNS et a le DNS IP du serveur <192.168.153.128>

c) Windows 10 Pro Client → <192.168.153.134>

Pour permettre à notre client Windows de joindre notre domaine on a :

- Désactivé le DHCP du client ou tout simplement attribuer une adresse IP statique à notre machine.
- On lui a attribué une adresse IP faisant partir de la plage d'adresses IP (125-150) définit dans le DHCP de notre serveur DNS . IP de la VM <192.168.153.134>
- DNS préféré <**192.168.153.128**>
Passerelle <192.168.153.2>
- DNS auxiliaire <192.168.153.130>
- On a redémarré le serveur



Rajouter cette machine au domaine

Informations système générales

Édition Windows

Windows 10 Professionnel

© Microsoft Corporation. Tous droits réservés.



Système

Processeur : Intel(R) Core(TM) i5-4210U CPU @ 1.70GHz 2.39 GHz

Mémoire installée (RAM) : 1,00 Go

Type du système : Système d'exploitation 64 bits, processeur x64

Stylet et fonction tactile : La fonctionnalité d'entrée tactile ou avec un stylet n'est pas disponible sur cet écran.

Paramètres de nom d'ordinateur, de domaine et de groupe de travail

Nom de l'ordinateur : VMC-Client

Nom complet : VMC-Client.lamboft.it

Description de l'ordinateur :

Domaine : lamboft.it

[Modifier les paramètres](#)

d) Ubuntu-22.04 → 192.168.153.131

Pour rajouter notre serveur linux à notre domaine on doit :

- Fixer une adresse IP à notre machine en tenant compte de la plage d'adresses IP définit dans le DHCP de notre serveur DNS.

Dans linux Ubuntu-22.04 la configuration de la carte réseau se trouve dans **/etc/netplan/file.yaml**

Netplan est le gestionnaire réseau par défaut des serveurs Debian depuis la version 17.10

```
# This is the network config written by 'subiquity'
network:
  ethernets:
    ens33:
      dhcp4: no
      addresses: [192.168.153.131/24]
      routes:
        - to: 0.0.0.0/0
          via: 192.168.153.2
      nameservers:
        addresses: [192.168.153.128,192.168.153.130]
  version: 2
```

****ens33** : Est le nom de notre interface réseau

****DHCP** : Est à no pour dire qu'on n'aura pas besoin d'un serveur DHCP pour ce réseau

****addresses** : Est sous forme de liste pour nous dire que si jamais on configurait un serveur DHCP dans cette machine c'est à ce niveau qu'on aurait défini l'étendu ou la plage d'adresses IP qui seront distribuées sur d'autres machines. Dans notre cas il y'a pas de configuration DHCP pour ce serveur d'où on met une seul IP/24

****routes** : C'est pour définir une passerelle afin de se connecter à internet.

****nameservers** : Représentent la liste des serveurs de noms (DNS) qui nous permettront de résoudre un nom de domaine ou une IP à partir de ce client et potentiellement rajouter ce client à notre forêt présent dans le serveur 192.168.153.128

Appliquer le service netplan (netplan Apply) pour prendre en compte les modifications

Dans le fichier **/etc/hosts**

```
lambo@vms-001-ubuntu:~$ less /etc/hosts
127.0.0.1 localhost
127.0.0.2 vms-001-ubuntu.lft.net vms-001-ubuntu


# The following lines are desirable for IPv6 capable hosts
::1      ip6-localhost ip6-loopback
fe00::0  ip6-localnet
ff00::0  ip6-mcastprefix
ff02::1  ip6-allnodes
ff02::2  ip6-allrouters
```

Avec cette configuration on a en même temps accès à internet et la VM peut résoudre le nom de domaine LOCAL-LAMBOFT.IT.IT

Comment configurer la VM linux afin de l'ajouter à l'AD ?

On va commencer par définir les concepts utilisés

| Mots clés | Valeur | Description |
|----------------|---|--|
| DNS_IP_ADDRESS | 192.168.153.128 | Adresse IP de notre serveur de nom DNS |
| mydomain.com | LOCAL-LAMBOFT.IT | Nom DNS de notre domaine Active Directory |
| MYDOMAIN.COM | LOCAL-LAMBOFT.IT | Nom DNS de notre domaine Active Directory en majuscule. |
| myhost | vms-001-ubuntu vms-002-Server vms-003-centos7 | Nom du serveur Linux sur lequel on souhaite joindre au domaine AD. |
| MYDOMAIN | LOCAL-LAMBOFT.IT | Nom DNS du groupe de travail ou domain NT qui inclut votre serveur Samba, en majuscules. |
| ads-hostname | SRV-01.LOCAL-LAMBOFT.IT | Nom d'hôte de notre serveur AD |
| admin-user | administrateur | Nom d'utilisateur de l'administrateur de domaine AD |

 Installation des packages nécessaires pour joindre le domaine Active Directory

sudo apt install samba krb5-config krb5-user winbind libpam-winbind libnss-winbind

samba : C'est un service qui permet à des serveurs linux de communiquer avec des machines Windows en se faisant passer pour une machine Windows

samba assure l'interopérabilité entre linux et Windows c'est grâce à samba que l'on peut configurer l'accès au contrôleur de domaine et rajouter une machine linux au domaine AD de Windows.

krb5-config : Il s'agit du service qui gère la configuration du protocole d'authentification réseau Kerberos.

krb5-user : Third party

winbind : Windows + Bind : Bind est un service sous linux qui permet de configurer un serveur DNS. WinBind est donc un service sous linux qui permet de résoudre un nom de domaine défini dans un active directory sur un serveur Windows.

Pour que WinBind puisse fonctionner correctement, il faudrait que la machine linux sur laquelle on l'installe puisse appartenir au domaine AD

Plus simple si on arrive à résoudre le DNS d'un AD alors on peut utiliser winbind afin de récupérer les utilisateurs et ordinateurs présents dans AD.

libpam-winbind :

libnss-winbind :

- **pam-auth-update** : Cette commande va nous permettre de choisir de créer un répertoire pour l'utilisateur AD qui va se logger.
- Modifier le fichier `/etc/nsswitch.conf`

```
# /etc/nsswitch.conf
#
# Example configuration of GNU Name Service Switch functionality.
# If you have the `glibc-doc-reference' and `info' packages installed, try:
# `info libc "Name Service Switch"' for information about this file.

passwd:         compat winbind
group:          compat winbind
shadow:         compat
gshadow:        files
```

- Modifier le fichier `/etc/hosts`

```
127.0.0.1 localhost
127.0.0.2 vms-001-ubuntu.1ft.net vms-001-ubuntu
```

- Modifier le fichier `/etc/samba/smb.conf`

```
[global]
security = ads
realm = LOCAL-LAMBOFT.IT
workgroup = LOCAL-LAMBOFT
idmap uid = 10000-20000
idmap gid = 10000-20000
winbind enum users = yes
winbind enum groups = yes
template homedir = /home/%D/%G/%U
template shell = /bin/bash
client use spnego = yes
client ntlmv2 auth = yes
encrypt passwords = yes
winbind use default domain = yes
restrict anonymous = 2
kerberos method = secrets and keytab
winbind refresh tickets = true

#-----LOG-----#

log file = /var/log/samba/log.%m
log level = 3
max log size = 1000
/etc/samba/smb.conf (END)
```

- Redémarrer le service `smbd`
- Modifier le fichier `/etc/krb5.conf`

```
[libdefaults]
    default_realm = LOCAL-LAMBOFT.IT
    dns_lookup_realm = false
    dns_lookup_kdc = true

[realms]
    LOCAL-LAMBOFT.IT = {
        kdc = srv-01.local-lamboft.it
        admin_server = srv-01.local-lamboft.it
    }

[domain_realm]
    .local-lamboft.it = LOCAL-LAMBOFT.IT
    local-lamboft.it = LOCAL-LAMBOFT.IT
/etc/krb5.conf (END)
```

- Créer un ticket **Kerberos** pour l'utilisateur admin de l'AD :
`sudo kinit administrateur`
- Créer un fichier **keytab** : `sudo net ads keytab create -U administrateur`
- Joindre le domaine AD avec l'utilisateur administrateur :
`sudo net ads join -U administrateur`

- Redémarrer le service winbind :
`sudo systemctl restart winbind.service`
- Vérifier que l'on a la liste de tous les utilisateurs AD qui s'affiche : `wbinfo -u`
- Redémarrer la VM et se connecter avec n'importe lequel des utilisateurs présents dans l'AD

e) **vms-002-server** → 192.168.153.132

NB : Cette VM on ne va pas la rajouter à l'AD à la Mano mais plutôt via un script Ansible

Rajouter au domaine local-lamboft.it

- installation des paquets
- configuration du fichier krb5.conf identique à celui de la **vm** 192.168.153.131
- dans le gestionnaire de configuration réseau netplan, on rajoute le domaine

```
# This is the network config written by 'subiquity'
network:
  ethernets:
    ens33:
      dhcp4: no
      addresses: [192.168.153.132/24]
      routes:
        - to : 0.0.0.0/0
          via: 192.168.153.2
      nameservers:
        addresses: [192.168.153.128,192.168.153.130]
        search: [lft.net]
  version: 2
```

```
nameserver 127.0.0.53
options edns0 trust-ad
search lft.net
/etc/resolv.conf (END)
```

Pour terminer on doit avoir ceci

```
root@vms-002-ubuntu-server:~# resolvectl query srv-01
srv-01: 192.168.153.128 -- link: ens33
      (srv-01.lft.net)

- Information acquired via protocol DNS in 3.1ms.
- Data is authenticated: no; Data was acquired via local or encrypted transport: no
- Data from: network
```

```

root@vms-002-ubuntu-server:~# kinit administrateur
Password for administrateur@LFT.NET:
root@vms-002-ubuntu-server:~# klist
Ticket cache: FILE:/tmp/krb5cc_0
Default principal: administrateur@LFT.NET

Valid starting    Expires    Service principal
26/05/2024 14:21:38  27/05/2024 00:21:38  krbtgt/LFT.NET@LFT.NET
renew until 27/05/2024 14:21:29

```

Après avoir configuré les fichiers réseaux et résolu le nom de domaine voici les commandes à utiliser pour vérifier que tout se passe bien.

| Outils/services | Commandes | Description |
|-----------------|---|--|
| Kinit | Kinit administrateur | On initialise l'utilisateur administrateur auprès de Kerberos afin de lui créer un keytab (mot de passe demandé) |
| Net ads | Net ads keytab create -U administrateur | Permet de créer un keytab pour administrateur et sera stocké dans /etc/krb5.keytab |
| Net ads join | net ads join -U administrateur | Permet de joindre le domaine lft.net via les credentials du user administrateur |
| Winbind | Systemctl restart winbind | C'est le client logiciel qui utilise l'authentification Kerberos pour se connecter à l'AD /etc/samba/smb.conf |
| smbd | Systemctl restart smbd | Samba est le daemon de winbind |

Cette Vm sera considérée comme le centre de services dans laquelle on va installer l'ensemble des services que l'on va utiliser : **Jenkins, docker, haproxy, kubernetes, traefik, apache**

Jenkins : installé

Apache : installé

Docker : installé

Kube : nécessite docker

Traefik : son installation nécessite Kubernetes 1.22+ et **Helm 3.9.4**

NB : quand on redémarre apache un mot de passe du certificat SSL nous est demandé (Lambo)

On a demandé à apache d'écouter aussi sur le 443 : **https**

f) **vms-003-centos** → 192.168.153.133

On identifie déjà les interfaces réseaux présents avec la commande ip addr : on voit que l'interface réseau c'est ens33 ou on peut aller directement dans le fichier de configuration de base des interfaces sur centos7 dans **/etc/sysconfig/network-scripts/ifcfg-ens33** et on regarde **DEVICE** ou **NAME**

- BOOTPROTO : none veut dire que le DHCP est désactivé
- On peut soit configurer le fichier directement

Ou

```
- sudo nmcli connection add type ethernet ifname ens33 con-name ens33
  ipv4.addresses 192.168.153.133/24 ipv4.gateway 192.168.153.2 ipv4.dns
  "192.168.153.128,192.168.153.130" ipv4.method manual

- sudo nmcli connection up <nom de la connexion>

- sudo systemctl restart NetworkManager
```

```
TYPE=Ethernet
PROXY_METHOD=none
BROWSER_ONLY=no
BOOTPROTO=none
IPADDR=192.168.153.133
PREFIX=24
GATEWAY=192.168.153.2
DNS1=192.168.153.128
DNS2=192.168.153.130
DEFROUTE=yes
IPV4_FAILURE_FATAL=no
IPV6INIT=yes
IPV6_AUTOCONF=yes
IPV6_DEFROUTE=yes
IPV6_FAILURE_FATAL=no
IPV6_ADDR_GEN_MODE=stable-privacy
NAME=ens33
UUID=e462c091-5216-4ff3-8c99-28c913399a73
DEVICE=ens33
ONBOOT=yes
/etc/sysconfig/network-scripts/ifcfg-ens33 (END)_
```

Playbook Ansible

Installation les paquets nécessaires pour joindre l'active directory

```
< <install sssd realmd oddjob oddjob-mkhomedir adcli samba-common samba-common-tools krb5-workstation openldap-clients policycoreutils-python -y>
```

Sur cette machine la configuration est plus aisée dans la mesure où on a plus forcément besoin de modifier les fichiers `krb5.conf` et `sssd.conf`

```
realm join --user=administrator local-lamboft.it
```

Cette commande ci-haut, juste après avoir renseignée le mot de passe du compte administrateur permet effectivement de joindre le domaine AD

Exemple du fichier `sssd.conf`

```
[domain/local-lamboft.it]
default_shell = /bin/bash
krb5_store_password_if_offline = True
cache_credentials = True
krb5_realm = LOCAL-LAMBOFT.IT
realmd_tags = manages-system joined-with-adcli
id_provider = ad
fallback_homedir = /home/%D/%G/%U
ad_domain = local-lamboft.it
use_fully_qualified_names = False
ldap_id_mapping = True
access_provider = ad

[sssd]
domains = local-lamboft.it
config_file_version = 2
services = nss, pam
-----
/etc/sssd/sssd.conf
```

On voit dans la configuration de sssd que le service utilise deux autres services complémentaires (nss et pam)

Dans le répertoire `/etc/pam.d/` on aura plusieurs fichiers dont les plus importants seront :

❑ `system-auth` : Nous intéresse

❑ `password-auth` : C'est ceci qui nous intéresse pour une configuration simple

Dans les deux fichiers ci-haut rajouter :

```
session    optional    pam_mkhomedir.so skel=/etc/skel umask=0077
```

```
systemctl enable oddjobd --now
```

C'est grâce à ce paquet (**oddjobd**) qu'on arrive à créer des répertoires pour chaque utilisateur AD.

❑ sshd : pour la configuration SSH

❑ login : pour des connections SSH

Pour tester un utilisateur de l'AD et voir s'il renvoie bien les informations attendues on peut faire :

```
id <user> ou id <user@domain>
```

Le choix du format d'authentification dépend de la configuration dans sssd.conf

```
use_fully_qualified_names = False
```

cette directive permet de dire à sssd qu'on souhaite se connecter sans rajouter le nom de domaine après le **username**.

D'où la commande `id <user>`

```
[root@vms-005-Alma9 ~]# realm list
local-lamboft.it
  type: kerberos
  realm-name: LOCAL-LAMBOFT.IT
  domain-name: local-lamboft.it
  configured: kerberos-member
  server-software: active-directory
  client-software: sssd
  required-package: oddjob
  required-package: oddjob-mkhomedir
  required-package: sssd
  required-package: adcli
  required-package: samba-common-tools
  login-formats: %U
  login-policy: allow-realm-logins
```

Erreur : l'utilisateur appartient bien au domaine mais on n'arrive pas à se connecter

Contrairement à Ubuntu le client-software ici est sssd

g) vms-005-Alma9 → 192.168.153.135

NB : Cette nouvelle est créée parce qu'on a décidé de déployer nos applications sur les nodes jenkins la 192.168.153.132 est le master node et 192.168.153.131 est le node linux

Du coup on aura besoin de celle-ci pour l'un de nos workers du docker swarm.

Configuration réseau :

Vérifier d'abord l'interface réseau virtuelle présente sur cette machine

```
nmcli connection show
```

```
[root@vms-005-Alma9 ~]# nmcli connection show
```

| NAME | UUID | TYPE | DEVICE |
|--------|--------------------------------------|----------|--------|
| ens160 | 6aff605c-1d23-3b6b-9b33-45fb07684ee0 | ethernet | ens160 |
| lo | cb19d65a-74c0-4ef6-b5fc-ff09df7216c2 | loopback | lo |

A partir de là on a des informations sur le Nom, le type uuid et la device de l'interface réseau qui nous intéresse à savoir celle basée sur ethernet

```
[root@vms-005-Alma9 ~]# cat /etc/sysconfig/network-scripts/ifcfg-ens160
```

TYPE=Ethernet
BROWSER_ONLY=no
BOOTPROTO=None
PROXY_METHOD=None
IPADDR=192.168.153.135
PREFIX=24
GATEWAY=192.168.153.2
DNS1=192.168.153.128
DNS2=192.168.153.130
DEFROUTE=yes
IPV4_FAILURE_FATAL=no
NAME=ens160
DEVICE=ens160
UUID=6aff605c-1d23-3b6b-9b33-45fb07684ee0
ONBOOT=yes

B) Rejoindre le domaine LOCAL-LAMBOFT.IT (Vérification)

Il est facile de faire qu'un client rejoigne le domaine cependant comment faire pour qu'utilisateur active directory puisse se logger à ce client.

Veut dire qu'on a réussi à joindre le domaine AD à partir de la machine linux

```
lambo@vms-001-ubuntu:~$ sudo net ads join -U administrateur
Password for [LFT\administrateur]:
Using short domain name -- LFT
Joined 'VMS-001-UBUNTU' to dns domain 'lft.net'
```

Pour savoir si on a réussi on peut utiliser les commandes suivantes ou

```
wbinfo -g
```

(pour la liste des groupes active directory)

```
root@vms-002-server:~# wbinfo -u
invité
```

```
krbtgt
administrateur
activedirectory
artur
tchinde
yves
jenkinscpteservice
florent.penda
loic.balitoni
tresor.lambo
```

Pour retrouver les infos complètes sur comment LDAP gère la relation entre l'AD et une machine la commande ci-dessous est indicative.

```
root@vms-002-server:~# net ads info
LDAP server: 192.168.153.130
LDAP server name: srv-prod.local-lamboft.it
Realm: LOCAL-LAMBOFT.IT
Bind Path: dc=LOCAL-LAMBOFT,dc=IT
LDAP port: 389
Server time: lun., 23 sept. 2024 10:22:47 UTC
KDC server: 192.168.153.130
Server time offset: 74192
Last machine account password change: dim., 07 juil. 2024 13:05:01 UTC
```

Sur Red Hat on a adcli à la place de net ads info:

```
[root@vms-005-Alma9 ~]# adcli info local-lamboft.it
[domain]
domain-name = local-lamboft.it
domain-short = LOCAL-LAMBOFT
domain-forest = local-lamboft.it
domain-controller = srv-prod.local-lamboft.it
domain-controller-site = Default-First-Site-Name
domain-controller-flags = gc ldap ds kdc closest writable full-secret ads-web
domain-controller-usable = yes
domain-controllers = srv-prod.local-lamboft.it srv-01.local-lamboft.it
[computer]
computer-site = Default-First-Site-Name
```

```
Last machine account password change: dim., 07 juil. 2024 13:05:01 UTC
root@vms-001-ubuntu:~# net ads testjoin
Join is OK
root@vms-001-ubuntu:~# █
```

Les différentes étapes pour joindre une machine au serveur AD

- **Synchronisation de la date et l'heure de la machine sur celle du serveur active directory.**
 - Vérifier si la machine a accès à internet et si les noms de domaine sont bien résolus
 - Vérifier que les paquets ntp et/ou chrony soient installés sur la machine linux

```
apt/yum/dnf install chrony
```

Dans le fichier `/etc/chrony.conf` rajouter ceci :

```
server srv-01.local-lamboft.it iburst prefer
```

où le nom de domaine ci-dessus est celui du serveur AD.

Redémarrer le service `Chronyd`

```
chronyc sources: permet de vérifier si la machine récupère bien la date et l'heure du serveur AD.
```

```
chronyc -a 'makestep' : Permet de forcer la synchronisation
```

- Activer NTP sur le serveur AD

```
w32tm /config /manualpeerlist:"time.windows.com,0x1" /syncfromflags:manual /reliable:YES /update
```

On configure NTP avec une source externe à celle de l'horloge local du serveur basé sur la **montre**.

Redémarrer le service et forcer la synchronisation

```
net stop w32time
net start w32time
```

```
w32tm /resync
```

En revérifiant le status, on voit bien que la source se trouve sur `time.windows.com` (qui est une source externe et fiable)

```
w32tm /query /status
Indicateur de dérive : 0(Aucun avertissement)
Couche : 4 (Référence secondaire, synchronisée par (S)NTP)
Précision : -23 (119.209ns par battement)
Délai de racine : 0.0306906s
Dispersion de racine : 7.8653799s
ID de référence : 0x33917B1D (IP de la source : 51.145.123.29)
Heure de la dernière synchronisation réussie : 30/09/2024 22:00:20
Source : time.windows.com,0x1
Intervalle d'interrogation : 6 (64s)
```

Couche : 4 (Référence secondaire, synchronisée par (S)NTP)

Ceci signifie que le serveur AD utilise le protocole NTP pour se synchroniser à une référence de niveau 3 (time.windows.com).

- Toujours sur le serveur AD vérifier que le port UDP 123 est ouvert

```
Get-NetFirewallRule | Where-Object { $_.DisplayName -like "*NTP*" }
```

- On voit que sur le serveur Alma le **Stratum** est à 4

C'est problématique dans la mesure où il devrait être à **1 ou 2** pour dire qu'il fait lui-même référence à une source d'horloge provenant d'ailleurs par occurrence notre AD

```
chronyc sources
MS Name/IP address           Stratum Poll Reach LastRx Last sample
=====
=
^? time1.google.com          0  6    0    -    +0ns[  +0ns]
+/-    0ns
^? time.cloudflare.com       0  6    0    -    +0ns[  +0ns]
+/-    0ns
^? neel.ch                   0  6    0    -    +0ns[  +0ns]
+/-    0ns
^? ns3051461.ip-51-255-95.eu  3  6    1    1   -3778s[ -3778s]
+/-   60ms
^? SRV-01.local-lamboft.it   4    6    3    2   -3778s[ -3778s] +/-
7890ms
```

On va vérifier s'il n'existe pas une règle de Pare-feu qui ne bloquerait pas le protocole NTP. (notamment le port **udp** 123)

```
firewall-cmd --permanent --add-service=ntp
ET
firewall-cmd --reload
```

- llk

C) Kerberos

Brainstorming

Pour gérer les messages au démarrage

Run-parts /etc/update-motd.d

II Architecture Réseau

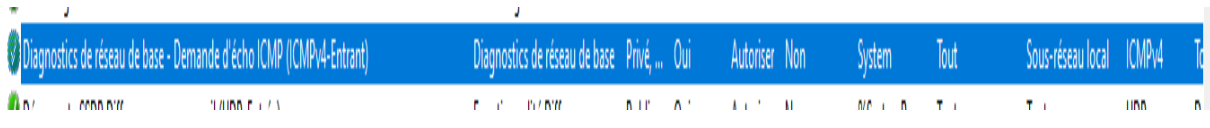
Les bases du modèle OSI et TCP/IP

Brainstorming :

On va voir comment stopper les connexions directes sur la vm mais plutôt se connecter uniquement via SSH.

Le ping -> au protocole ICMP : soit l'host est éteint soit le pare feu bloque les connexions entrantes ou sortantes sur le protocole ICMP il reste donc à identifier de quelle IP il s'agit IPv4 ou IPv6

netstat -ano | findstr :<port> : permet de savoir quel service tourne avec un port connu



The screenshot shows the Windows Network Troubleshooter window. The title bar reads "Diagnostics de réseau de base - Demande d'écho ICMP (ICMPv4-Entrant)". The main area shows a problem with the "Ping de 192.168.1.12 -> 192.168.1.101 ne fonctionne pas". The "Observations" section states "Les deux machines sont sur le même réseau". The "Correctifs" section suggests "vérifier la règle de pare feu ICMP et l'activer pour les connexions entrantes sur la machine de destination". The "Sagesse" section notes "C'est le protocole ICMP qui gère la connectivité réseau entre deux hôtes".

| Problèmes | Observations | Correctifs | Sagesse |
|---|---|---|--|
| Ping de 192.168.1.12 -> 192.168.1.101 ne fonctionne pas | Les deux machines sont sur le même réseau | vérifier la règle de pare feu ICMP et l'activer pour les connexions entrantes sur la machine de destination | C'est le protocole ICMP qui gère la connectivité réseau entre deux hôtes |

ProcessExplorer permet de voir quel service est relié à un port

Nmap est un outil qui nous permet d'analyser en détail la connectivité réseau d'un hôte via son adresse IP

| | | |
|--|--|--|
| | | |
| | | |
| | | |
| | | |

Pour node master jenkins

```
ssh-keyscan -H vms-002-ubuntu-centerServices >> .ssh/known_hosts
9p1 Ubuntu-3ubuntu0.6
9p1 Ubuntu-3ubuntu0.6
9p1 Ubuntu-3ubuntu0.6
9p1 Ubuntu-3ubuntu0.6
9p1 Ubuntu-3ubuntu0.6
cat .ssh/known_hosts
```

Pb sur la 132 avec la résolution dns

Resolvectl status : resolvectl status

Failed to get global data: Unit dbus-org.freedesktop.resolve1.service not found.

Il faut installer systemd-resolved ; car les dns définis dans `/etc/netplan/file.yaml` sont pas prises en compte

DNS fourni par `systemd`.

1. Installer et activer `systemd-resolved`

Pour installer et activer `systemd-resolved`, suivez ces étapes :

1. Installer `systemd-resolved` (si nécessaire)

Sur les versions modernes d'Ubuntu, `systemd-resolved` devrait déjà être installé, mais au cas où il ne le serait pas, vous pouvez l'installer avec :

```
sh Copier le code
sudo apt update
sudo apt install systemd-resolved
```

2. Activer et démarrer `systemd-resolved`

```
sh Copier le code
sudo systemctl enable systemd-resolved
sudo systemctl start systemd-resolved
```

2. Activer et démarrer `systemd-resolved`

```
sh Copier le code  
  
sudo systemctl enable systemd-resolved  
sudo systemctl start systemd-resolved
```

3. Créer un lien symbolique pour `/etc/resolv.conf`

Assurez-vous que `/etc/resolv.conf` pointe vers le fichier de configuration généré par `systemd-resolved` :

```
sh Copier le code  
  
sudo ln -sf /run/systemd/resolve/resolv.conf /etc/resolv.conf
```

2. Vérifier la configuration DNS

Après avoir activé `systemd-resolved`, vérifiez la configuration DNS :

```
sh Copier le code  
  
systemctl status systemd-resolved  
resolvectl status
```

```
oot@vms-002-ubuntu-server:~# resolvectl status  
Global  
    Protocols: -LLMNR -mDNS -DNSOverTLS DNSSEC=no/unsupported  
    resolv.conf mode: foreign  
    DNS Domain: ~.  
  
Link 2 (ens33)  
    Current Scopes: DNS  
        Protocols: +DefaultRoute +LLMNR -mDNS -DNSOverTLS DNSSEC=no/unsupported  
    Current DNS Server: 192.168.153.128  
    DNS Servers: 192.168.153.128 192.168.153.130  
  
Link 3 (docker0)  
    Current Scopes: none  
        Protocols: -DefaultRoute +LLMNR -mDNS -DNSOverTLS DNSSEC=no/unsupported
```

```

root@vms-002-ubuntu-server:~# resolvectl status
Global
  Protocols: -LLMNR -mDNS -DNSOverTLS DNSSEC=no/unsupported
  resolv.conf mode: foreign
  DNS Domain: lft.net

Link 2 (ens33)
  Current Scopes: DNS
  Protocols: +DefaultRoute +LLMNR -mDNS -DNSOverTLS DNSSEC=no/unsupported
  DNS Servers: 192.168.153.128 192.168.153.130
  DNS Domain: lft.net

Link 3 (docker0)
  Current Scopes: none
  Protocols: -DefaultRoute +LLMNR -mDNS -DNSOverTLS DNSSEC=no/unsupported

```

On va changer le nom du contrôleur de domaine/foret de lft.net → LOCAL-LAMBOFT.IT.it

- 1- Backup l'état actuel de la machine
- 2- Modifier le fichier générer par **random /List (NETBIOS -> LOCAL-LAMBOFT.IT)**

6717

Vms-005-rocky

- Créez un point de montage et montez le CD-ROM :

```

sh
sudo mkdir /mnt/cdrom
sudo mount /dev/cdrom /mnt/cdrom

```

• Copiez les fichiers VMware Tools depuis le CD-ROM :

- Copiez le fichier compressé des VMware Tools dans le répertoire `/tmp` :

```

sh
cp /mnt/cdrom/VMwareTools-*.tar.gz /tmp
cd /tmp

```

Étape 3 : Extraire les fichiers et lancer l'installation

• Extrayez le fichier compressé :

```

sh
tar -xzf VMwareTools-*.tar.gz
cd vmware-tools-distrib

```


Avec `gzip` (pour `.gz` files) :

1. Décompressez le fichier `.gz` :

```
sh Copier le code  
gzip -d VMwareTools-*.tar.gz
```

5. Lancez le script d'installation :

```
sh Copier le code  
sudo ./vmware-install.pl
```

Étape 4 : Suivez les instructions de l'assistant d'installation

6. Suivez les instructions à l'écran :

- L'assistant d'installation vous demandera de répondre à plusieurs questions. Acceptez les paramètres par défaut en appuyant sur Entrée pour chaque question, sauf si vous avez des préférences spécifiques.

Étape 5 : Finaliser l'installation

7. Redémarrez la machine virtuelle :

- Après avoir terminé l'installation, il est recommandé de redémarrer la machine virtuelle pour appliquer les modifications :

```
sh Copier le code  
sudo reboot
```