# 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

1. On va utiliser **Traefik** de deux façons :

* Avec un fournisseur docker
* Avec un fournisseur kubernetes

1. Installer et configurer un **DOZZLE** permettant de lire les logs des applications isolées dans **Docker**.
2. Utiliser **Ansible** notamment les rôles ansible pour déployer les configurations automatiquement sur le serveur Linux **Debian et CentOS**.
3. Installation de **Grafana** pour contrôler et monitorer les **VM.**
4. 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.

## Architecture system

Une image contenant texte, capture d’écran, diagramme, logiciel

Description générée automatiquement

### 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

Une image contenant texte, capture d’écran, Police

Description générée automatiquement

L’installer via GUI ou en CLI

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

Une image contenant texte, capture d’écran, Police

Description générée automatiquement

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



Une image contenant texte, capture d’écran, Police

Description générée automatiquement

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

Une image contenant texte, logiciel, Logiciel multimédia, capture d’écran

Description générée automatiquement

Redémarrer le service sshd

Désactiver ceci



Cela permettra d’utiliser la directive DenyGroups

Une image contenant texte, Police, blanc, typographie

Description générée automatiquement

**UO**\_**Admin** et **UO**\_**Others** sont des groupes créés pour notre domaine AD.

1. 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 :

Une image contenant texte, logiciel, Page web, Icône d’ordinateur

Description générée automatiquement

*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

Une image contenant texte, capture d’écran, logiciel, Page web

Description générée automatiquement

* Serveur DNS <192.168.153.128>

**Outils** >> **Ajouter** **les** **fonctionnalités** >> **Cocher** **DNS** >> **Terminer**. Ensuite promouvoir au Controller 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

Une image contenant texte, capture d’écran, affichage, logiciel

Description générée automatiquement Une image contenant texte, capture d’écran, logiciel, nombre

Description générée automatiquement

**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

Une image contenant texte, capture d’écran, affichage, nombre

Description générée automatiquement

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 pouvoir accéder à nos Vms créées dans VMware Workstation

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 trafique passe bien

Une image contenant texte, nombre, Police, ligne

Description générée automatiquement

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

Une image contenant texte, capture d’écran, nombre, Police

Description générée automatiquement

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 aauxiliaire 8.8.8.8 afin de permettre le trafic public entrant.

Ou 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

**Une image contenant texte, capture d’écran, logiciel, Page web

Description générée automatiquement**

A la fin on devra obtenir ceci sur notre serveur local

Une image contenant texte, capture d’écran, Police, ligne

Description générée automatiquement Une image contenant texte, diagramme, capture d’écran, Police

Description générée automatiquement

Et Ceci sur notre carte réseau et sur les paramètres réseau

Une image contenant texte, capture d’écran, logiciel, Page web

Description générée automatiquement

**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.

Une image contenant texte, capture d’écran, Police, document

Description générée automatiquement

Une image contenant texte, capture d’écran, Police, algèbre

Description générée automatiquement

* 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.

Une image contenant texte, capture d’écran, Police, ligne

Description générée automatiquement

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.

Une image contenant texte, capture d’écran, Police, nombre

Description générée automatiquement

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

Une image contenant texte, capture d’écran, Police, nombre

Description générée automatiquement

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 Controller de domaine les VM Windows server : c’est de cette façon qu’on réussit à les rajouter au Controller 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 Objets)

Une image contenant texte, capture d’écran, Police, nombre

Description générée automatiquement

**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

Une image contenant texte, capture d’écran, Police

Description générée automatiquement

**Les types de GPO :**

* GPO Locale :
* GPO AD :

**La propagation de GPO** :

Le principe LSDOU

Une image contenant texte, Police, capture d’écran, Graphique

Description générée automatiquement

* 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](mailto:artur.lambo@LOCAL-LAMBOFT.IT)

[yves.makang@LOCAL-LAMBOFT.IT](mailto:yves.makang@LOCAL-LAMBOFT.IT)

[pecra.cravet@LOCAL-LAMBOFT.IT](mailto: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.

Une image contenant texte, logiciel, nombre, capture d’écran

Description générée automatiquement

Horodatage :

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

1. *Windows server 2022 Standard 🡪 192.168.158.130*

Une image contenant texte, capture d’écran, affichage, Police

Description générée automatiquement

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

1. *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

Une image contenant texte, capture d’écran, affichage, nombre

Description générée automatiquement

Rajouter cette machine au domaine

Une image contenant texte, capture d’écran, Police, nombre

Description générée automatiquement

1. *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

Une image contenant texte, capture d’écran, carte de visite, Police

Description générée automatiquement

\*\****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 foret 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**

Une image contenant texte, capture d’écran, Police, noir

Description générée automatiquement

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 |
| MMYDOMAIN.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 domaine 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 définit 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

Une image contenant texte, capture d’écran, Police, noir

Description générée automatiquement

* Modifier le fichier **/etc/hosts**



* Modifier le fichier **/etc/samba/smb.conf**

Une image contenant texte, capture d’écran, Police

Description générée automatiquement

* Redémarrer le service smbd
* Modifier le fichier **/etc/krb5.conf**

Une image contenant texte, capture d’écran, Police, affichage

Description générée automatiquement

* 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

1. **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

Une image contenant texte, capture d’écran, Police

Description générée automatiquement

Une image contenant texte, Police, capture d’écran, typographie

Description générée automatiquement

Pour terminer on doit avoir ceci

Une image contenant texte, capture d’écran, Police

Description générée automatiquement

Une image contenant texte, capture d’écran, Police

Description générée automatiquement

Après avoir configure r les fichiers réseaux et résoudre 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 crée 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 | Systemclt 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**

1. **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

Une image contenant texte, capture d’écran, Police, conception

Description générée automatiquement

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 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

1. **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

Une image contenant texte, capture d’écran, Police

Description générée automatiquement

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

Une image contenant texte, capture d’écran, Police

Description générée automatiquement

### 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 loger à ce client.

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

Une image contenant texte, capture d’écran, Police, noir

Description générée automatiquement

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

Une image contenant texte, capture d’écran, Police

Description générée automatiquement

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 à 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 voir 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 faitlui-même référenceà 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

### Kerberos

**Brainstorming**

Pour gérer les messages au démarrage

Run-parts /etc/update-motd.d

## 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



|  |  |  |  |
| --- | --- | --- | --- |
| **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 Une image contenant texte, capture d’écran, Police

Description générée automatiquement

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 définit dans /etc/netplan/file.yaml sont pas prises en compte

Une image contenant texte, capture d’écran, logiciel, Page web

Description générée automatiquement

Une image contenant texte, capture d’écran, logiciel, Police

Description générée automatiquement

Une image contenant texte, capture d’écran, Police

Description générée automatiquement

Une image contenant texte, capture d’écran, Police

Description générée automatiquement

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

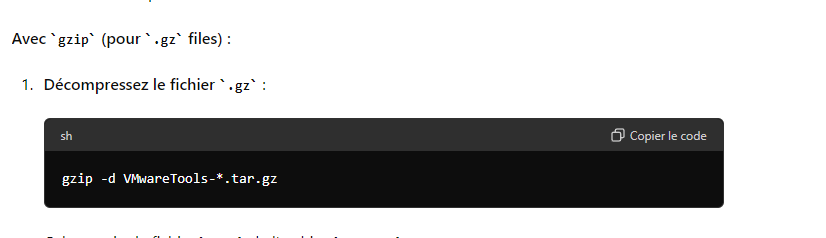
1. Backup l’état actuel de la machine
2. Modifier le fichier générer par **rendom /List (NETBIOS -> LOCAL-LAMBOFT.IT)**

6717

Vms-005-rocky

Une image contenant texte, capture d’écran, logiciel, Police

Description générée automatiquement

Une image contenant texte, capture d’écran, Police

Description générée automatiquement