

Documentation Zimbra



Tables des matières:

1. Introduction	2
2. Besoins pour la réalisation	2
3. Réalisation	3
1- Installation de la machine ubuntu	3
2- Installation des paquets	3
3- Configuration des interfaces réseaux	4
4- Vérification n°1	5
5- Une machine Windows Server 2019	6
6- DNS et DHCP	6
7- Configuration machine Zimbra	8
8- Installation de dnsutils sur Ubuntu	8
9- Validation n°2	8
10- Installation de paquets	9
11- Arrêt du service apparmor	10
12- Téléchargement de Zimbra free open source version VM	10
13- Validation n°3	11
14- Interface d'administration	12
15- Boîte de messagerie administrateur	13
16- Création d'alias m2l.local pointant sur mail.m2l.local	14
17- Configuration de l'authentification AD	15
18- Création d'utilisateur sur DC	16
19- Création d'utilisateur sur Zimbra	17
20- Validation n°4	17
21- Test de l'envoi du mail à l'extérieur	18

1. Introduction :

Zimbra est un serveur de messagerie avec des fonctionnalités de travail collaboratif. La version open source comprend la fonction de serveur de messagerie, de calendriers partagés, de carnets d'adresses gestionnaires partagés, partage de fichiers, de gestionnaire de tâches, wiki, messagerie instantanée, ...

<https://www.zimbra.com/>

lien de téléchargement iso zimbra :

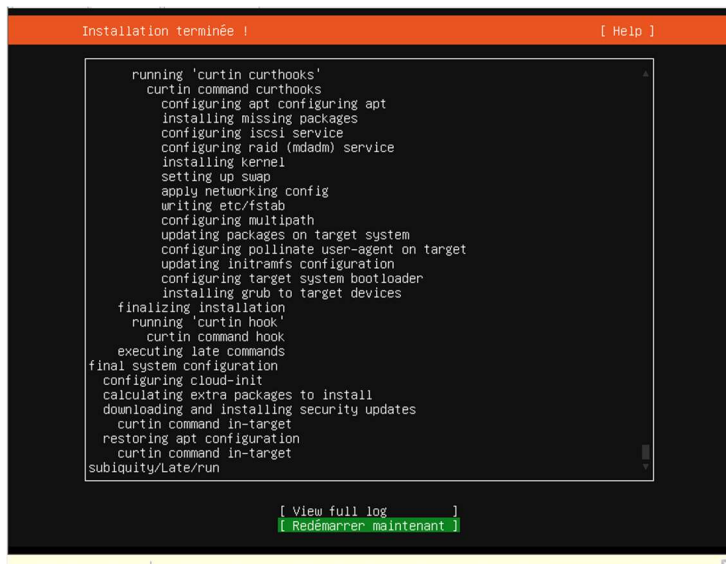
<https://ubuntu.com/download/server#releases>

2. Besoins pour la réalisation :

Poste de travail VMWare Workstation, iso Ubuntu 20.04, iso Windows Server 2019.

3. Réalisation :

1- Installation de la machine ubuntu



```
Installation terminée | [ Help ]

running 'curtin curthooks'
curtin command curthooks
  configuring apt configuring apt
  installing missing packages
  configuring iscsi service
  configuring raid (mdadm) service
  installing kernel
  setting up swap
  apply networking config
  writing etc/fstab
  configuring multipath
  updating packages on target system
  configuring pollinate user-agent on target
  updating initramfs configuration
  configuring target system bootloader
  installing grub to target devices
finalizing installation
  running 'curtin hook'
  curtin command hook
  executing late commands
final system configuration
  configuring cloud-init
  calculating extra packages to install
  downloading and installing security updates
  curtin command in-target
  restoring apt configuration
  curtin command in-target
subiquity/late/run

[ View full log ]
[ Redémarrer maintenant ]
```

Appuyer sur **redémarrer maintenant**.

Le message **FAILED** s'affiche, appuyer sur entrer.

A la fin de l'installation de la machine mail (Ubuntu), se connecter à l'aide du compte utilisateur renseigné au moment de l'installation, ici :

login : user

password : root

2- Installation des paquets

Passer en "root" à l'aide de la commande **sudo su**, puis mettre à jour le système avec **apt update**

Comme ci-dessous :

```
user@mail:~$ sudo su
[sudo] password for user:
root@mail:/home/user# apt update_
```

Puis faire un **apt upgrade -y** et installer l'éditeur nano en faisant **apt install ifupdown**

3- Configuration des interfaces réseaux

Elle doit être équipée de deux interfaces réseaux :

Hostname : mail

Carte 1 : Segment LAN : **172.20.0.30/24**

Carte 2 : DHCP (NAT)

Pour cela, faire **ip a** pour vérifier les noms des interfaces réseaux

```
root@mail:/home/user# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:c7:6e:da brd ff:ff:ff:ff:ff:ff
    inet6 fe80::20c:29ff:fec7:6eda/64 scope link
        valid_lft forever preferred_lft forever
3: ens37: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN group default qlen 1000
    link/ether 00:0c:29:c7:6e:e4 brd ff:ff:ff:ff:ff:ff
```

Puis, éditer le fichier **nano /etc/network/interfaces**

Voici son contenu :

auto lo

iface lo inet loopback

auto ens33

- **iface ens33 inet static**
- **address 172.20.0.30**
- **netmask 255.255.255.0**
-
- **auto ens37**
- **iface ens37 inet dhcp**

Comme ci-dessous :

```

GNU nano 4.8 /etc/network/interfaces
# interfaces(5) file used by ifup(8) and ifdown(8)
# Include files from /etc/network/interfaces.d:
source-directory /etc/network/interfaces.d

auto lo
iface lo inet loopback

auto ens33
iface ens33 inet static
address 172.20.0.30
netmask 255.255.255.0

auto ens37
iface nes37 inet dhcp

```

Enregistrer le fichier, puis :

reboot

ou

ifdown ens33

ifup ens33

ifup ens37

4- Vérification n°1

ifconfig ens33 -> 172.20.0.30

ifconfig ens37 -> adresse obtenue depuis le DHCP de VMware (NAT)

Comme ci-dessous :

```

root@mail:/home/user# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:c7:6e:da brd ff:ff:ff:ff:ff:ff
    inet 172.20.0.30/24 brd 172.20.0.255 scope global ens33
        valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fec7:6eda/64 scope link
        valid_lft forever preferred_lft forever
3: ens37: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:c7:6e:e4 brd ff:ff:ff:ff:ff:ff
    inet 192.168.74.130/24 brd 192.168.74.255 scope global dynamic ens37
        valid_lft 1795sec preferred_lft 1795sec
    inet6 fe80::20c:29ff:fec7:6ee4/64 scope link
        valid_lft forever preferred_lft forever

```

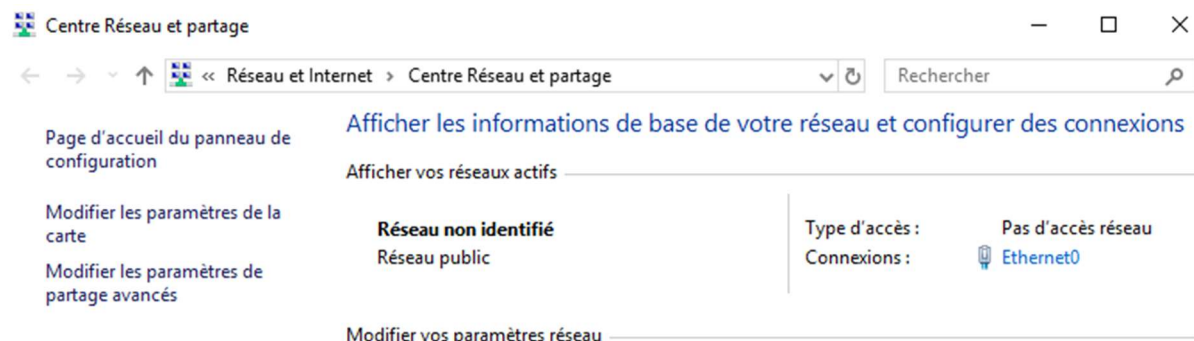
5- Une machine Windows Server 2019

Hostname : DC

Carte 1 : 172.20.0.10/24

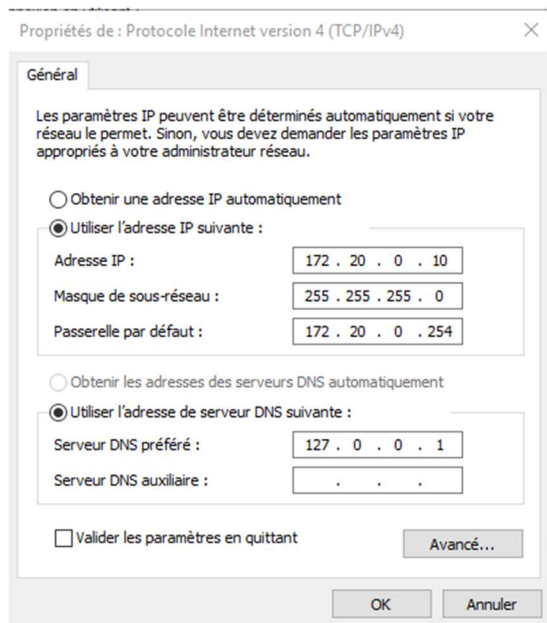
Allumer la machine DC Windows server 2019 (avec le rôle DNS installé pour gérer la zone m2l.local d'adresse 172.20.0.10)

Dans **paramètre réseau & Internet** → **Centre Réseau et partage**



Dans **Ethernet0** → **Propriétés** → **IPv4**

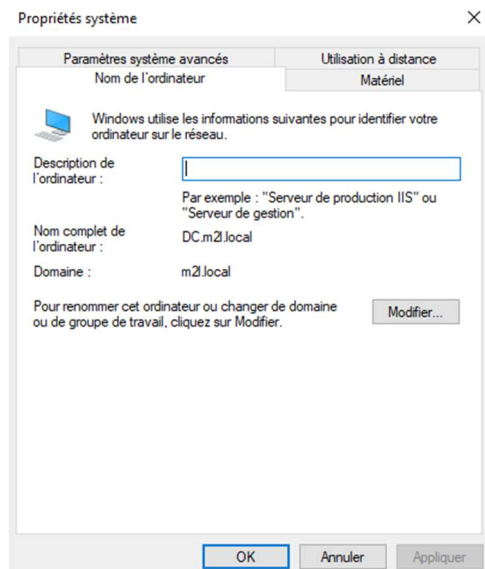
Entrer l'adresse IP, masque de sous-réseau et passerelle souhaités :



6- DNS et DHCP

Dans **Gérer** → **Ajouter des rôles et des fonctionnalités** : Ajouter serveurs **DNS** et **AD DS**

Aller dans **Configurer ce serveur local**, puis appuyer sur **Nom de l'ordinateur**

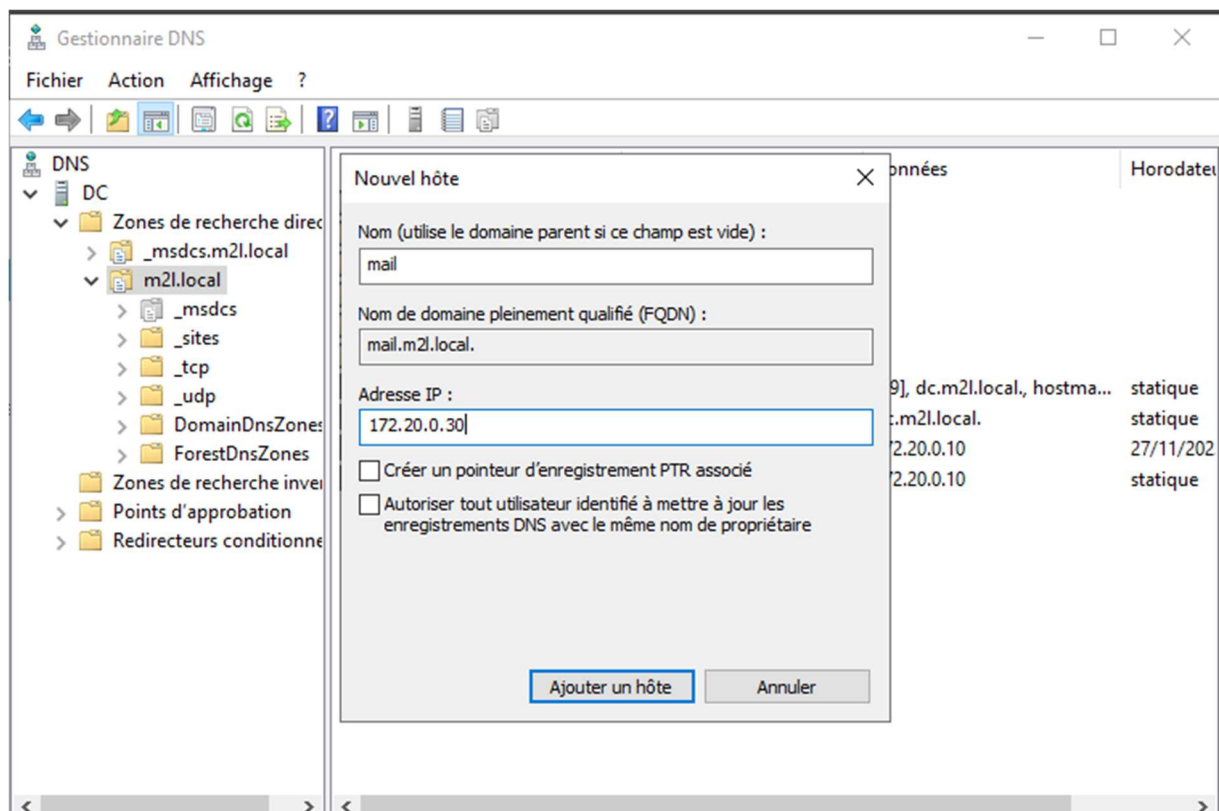


Dans **modifier**, changer le nom de la machine en DC

Dans la console (fenêtre) DNS de cette machine :

Ajouter un enregistrement hôte A faisant correspondre le FQDN : mail.m2l.local à l'adresse 172.20.0.30

Comment : clique droit dans la **console DNS (zone directe)** → Ajouter un enregistrement A (hôte A) → Renseigner le nom d'hôte 'mail' et l'adresse IP 172.20.0.30



Ajouter un autre enregistrement MX (messagerie) au FQDN d'adresse 172.20.0.30

Comment : Cliquez droit dans la console DNS → Ajouter un nouveau serveur de messagerie MX : nom = mail → Parcourir pour aller chercher l'enregistrement mail (A) dans la zone de résolution directe m2l.local puis OK.

mail	Hôte (A)	172.20.0.30
mail	Serveur de messagerie (...)	[10] mail.m2l.local

7- Configuration machine Zimbra

Changer le hostname dans le fichier **/etc/hostname** de la machine mail en FQDN : mail.m2l.local

Supprimer toutes les lignes, Ajouter dans le fichiers **nano /etc/hosts** la ligne suivante :

172.20.0.30 mail.m2l.local mail

```
GNU nano 4.8 /etc/hosts
172.20.0.30 mail.m2l.local mail
```

Supprimer tout ce qui se trouve dans le fichier **/etc/resolv.conf** :

rm /etc/resolv.conf

Editer le fichier **/etc/resolv.conf** :

nano /etc/resolv.conf

changer l'adresse du premier nameserver en 172.20.0.10, puis ajouter une deuxième ligne nameserver 1.1.1.1 et enfin modifier search localdomain en search m2l.local

Comme ici :

```
nameserver 172.20.0.10
nameserver 1.1.1.1
search m2l.local_
```

8- Installation de dnsutils sur Ubuntu

Pour utiliser nslookup sous linux, installer dnsutils avec les commandes :

sudo apt install bind9

sudo apt install dnsutils

9- Validation n°2

Tester la résolution de nom depuis la console DOS de DC puis depuis le Terminal de la machine mail :

nslookup dc.m2l.local doit vous afficher -> **172.20.0.10**

```
root@mail:/home/user# nslookup dc.m2l.local
Server:          172.20.0.10
Address:         172.20.0.10#53

Name:   dc.m2l.local
Address: 172.20.0.10
```

nslookup mail.m2l.local doit vous afficher > **172.20.0.30**

```
root@mail:/home/user# nslookup mail.m2l.local
Server:          172.20.0.10
Address:         172.20.0.10#53

Name:   mail.m2l.local
Address: 172.20.0.30
```

10- Installation de paquets

Installation de quelques paquets nécessaires au fonctionnement de Zimbra :

**apt install netcat-traditional libidn11-dev libgmp10 sysstat sqlite3 libaio1
unzip pax**

NOTE :

netcat-traditional : Utilitaire Unix simple qui lit et écrit des données à travers les connexions réseau en utilisant les protocoles TCP ou UDP. C'est un outil fiable qui peut être utilisé directement ou par d'autres programmes ou scripts. C'est aussi un outil d'exploration et de débogage réseau plein de fonctionnalités car il peut créer

presque toutes les sortes de connexion dont vous pourriez avoir besoin et possède plusieurs capacités incorporées.

libperl5.22 : Files for developing applications which embed a Perl interpreter.

libidn11-dev : GNU Libidn est une mise en œuvre entièrement documentée des spécifications Stringprep, Punycode et IDNA. Libidn permet d'encoder et de décoder les noms de domaine internationalisés. Les profils Nameprep, XMPP, SASLprep, et iSCSI sont pris en charge.

Ce paquet fournit les fichiers d'en-tête, une bibliothèque statique, les informations de pkg-config, les pages de manuel de l'API et le manuel de Libidn.

libgmp10 : GNU MP est une bibliothèque pour les programmes nécessitant une arithmétique à précision arbitraire (c'est-à-dire un paquet pour gérer les grands nombres). Elle peut travailler avec des entiers signés, des rationnels et des nombres à virgule flottante.

Elle possède un grand T

sysstat : Le paquet sysstat contient les outils de performance système suivants :

- sar : collecte et rapport d'informations sur l'activité du système ;
- iostat : rapport d'utilisation CPU et statistiques d'E/S des disques ;
- tapestat : rapport de statistiques pour les lecteurs de bandes connectés au système ;
- mpstat : rapport de statistiques globales et par processeur ;
- pidstat : rapport de statistiques des tâches Linux (processus) ;
- sadf : affichage des données collectées par sar dans divers formats ;
- cifsioat : rapport de statistiques d'E/S pour les systèmes de fichiers CIFS.

Les statistiques rapportées par sar portent entre autres sur les taux de transferts I/O, l'activité de la pagination, l'activité relative aux processus, les interruptions, l'activité du réseau, l'utilisation de la mémoire et de la mémoire virtuelle, l'utilisation du CPU, l'activité du noyau et les statistiques TTY. Les machines SMP et UP sont gérées.

SQLite : est une bibliothèque C qui implémente un moteur de base de données SQL. Les programmes liés avec la bibliothèque SQLite peuvent accéder à des bases de données SQL sans avoir besoin d'un processus séparé de gestion de base de données.

libaio1 : Cette bibliothèque permet aux applications en espace utilisateur d'utiliser les appels système asynchrones d'E/S du noyau Linux, ce qui est important pour les performances des bases de données et d'autres applications avancées.

Ce paquet fournit la bibliothèque partagée.

unzip : Programme d'extraction d'InfoZIP. À l'exception d'archives multivolumes, c.-à-d. des fichiers ZIP qui ont été morcelés sur plusieurs disques (en utilisant l'option « /& » de PKZIP), il peut gérer n'importe quel fichier créé par PKZIP ou par le programme d'InfoZIP correspondant.

Cette version gère le chiffrement.

11- Arrêt du service apparmor

service apparmor stop

NOTE : AppArmor ("Application Armor") est un logiciel libre de sécurité pour Linux. AppArmor permet à l'administrateur système d'associer à chaque programme un profil de sécurité qui restreint les capacités de celui-ci.

Supprimez le chargement automatique de ce dernier au démarrage de la machine :

update-rc.d -f apparmor remove

12- Téléchargement de Zimbra free opensource version VM

wget https://files.zimbra.com/downloads/8.8.15_GA/zcs-8.8.15_GA_4179.UBUNTU20_64.20211118033954.tgz

Décompresser le tgz téléchargé :

tar xvzf zcs-8.8.15_GA_3869.UBUNTU20_64.20190918004220.tgz

```
root@mail:/home/user# tar xvzf zcs-8.8.15_GA_4179.UBUNTU20_64.20211118033954.tgz
```

Accéder au dossier décompressé :

cd zcs-8.8.15_GA_3869.UBUNTU20_64.20190918004220

Lancer l'installation : **./install.sh**

Do you agree with the terms of the software license agreement ? **Y**

Use Zimbra's package repository Y ? **Entrée**

Select the packages to install ? Tapez '**Entrée**' pour tous les paquets à part le **dnscache** et **proxy (N)**

The system will be modified. Continue ? **Y**

Attendre l'affichage du menu :

Choisir **6** pour accéder au menu d'administration (zimbra-store) :

Tapez **4** pour changer le mot de passe de l'administration Zimbra. (Attention 6 caractères au min)

mot de passe : **root123**

Tapez **r** pour previous

Puis **a** pour appliquer

Save configuration data to a file Yes ? **Entrée**

Save config in file (il vous propose un nom de fichier) : **Entrée**

The system will be modified ? **Yes**

Notify Zimbra : **No**

Fin d'installation. Configuration complete - press return to exit - taper **Entrée**

13- Validation n°3

Redémarrer la machine avec un **reboot**

Pensez à vérifier **/etc/resolv.conf**

Ouvrir la session “root” puis changer d'identité en utilisateur zimbra avec **su zimbra**

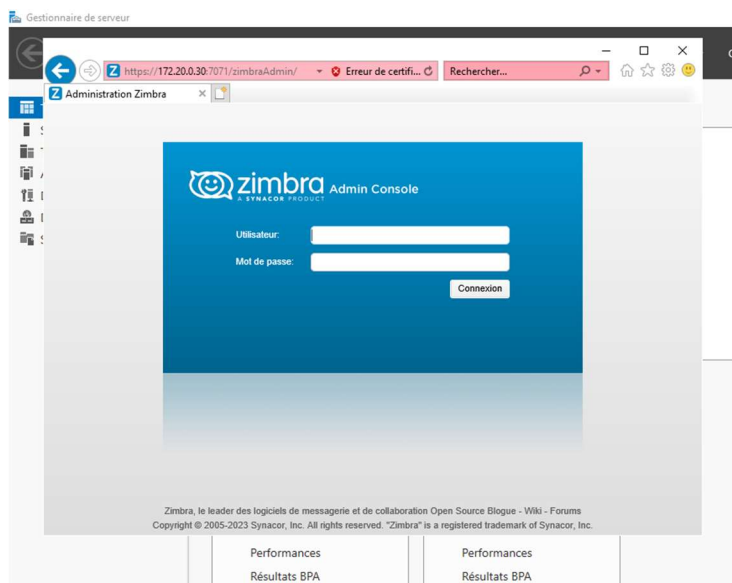
Taper la commande **zmcontrol status** pour vérifier le bon fonctionnement de tous les services installés précédemment

Il faut que tous les services soient en running, comme ici :

```
root@mail:/home/user# su zimbra
zimbra@mail:/home/user$ zmcontrol status
Host mail.m21.local
  amavis           Running
  antispam         Running
  antivirus        Running
  imapd           Running
  ldap            Running
  logger          Running
  mailbox         Running
  memcached       Running
  mta             Running
  opendkim        Running
  service webapp  Running
  snmp            Running
  spell           Running
  stats           Running
  zimbra webapp   Running
  zimbraAdmin webapp Running
  zimlet webapp   Running
  zmconfigd       Running
```

14- Interface d'administration

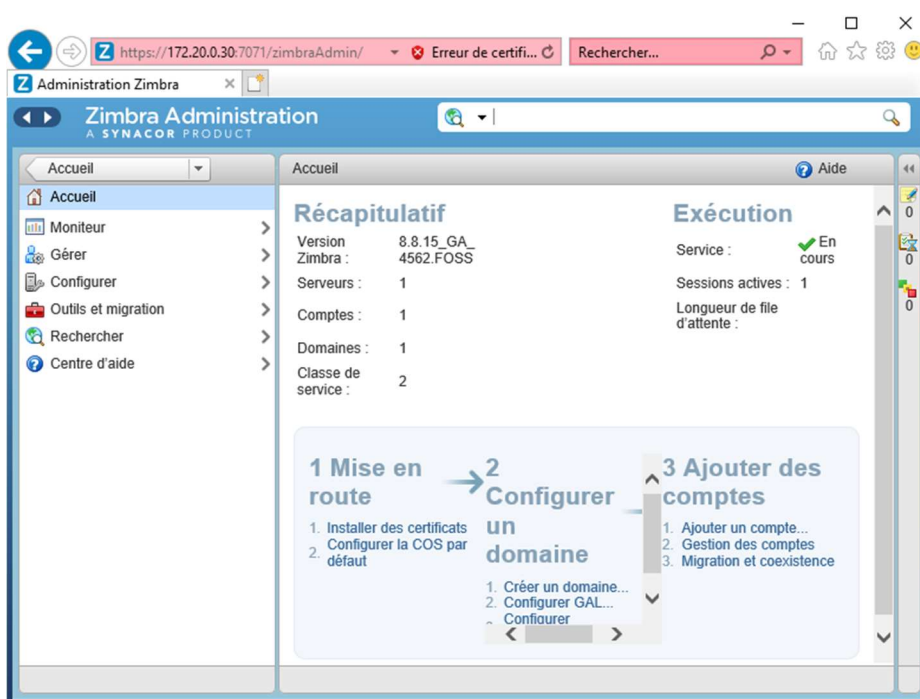
Depuis la machine DC ou la machine physique : <https://172.20.0.30:7071> ou <https://mail.m21.local:7071>



Acceptez le certificat :

Username : **admin**

Password : **root123**



15- Boîte de messagerie administrateur

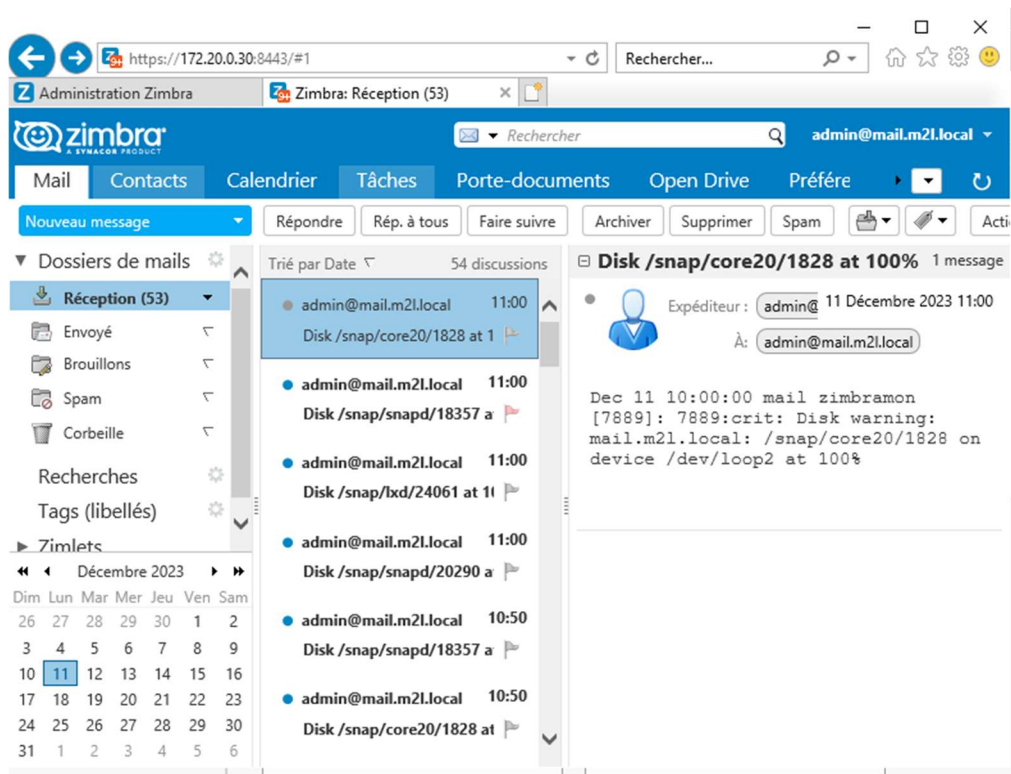
Ouvrez un autre onglet, depuis la machine DC ou depuis la machine physique :

<https://172.20.0.30:8443> ou <https://mail.m2l.loca:8443>

Acceptez le certificat :

Username : **admin**

Password : **root123**



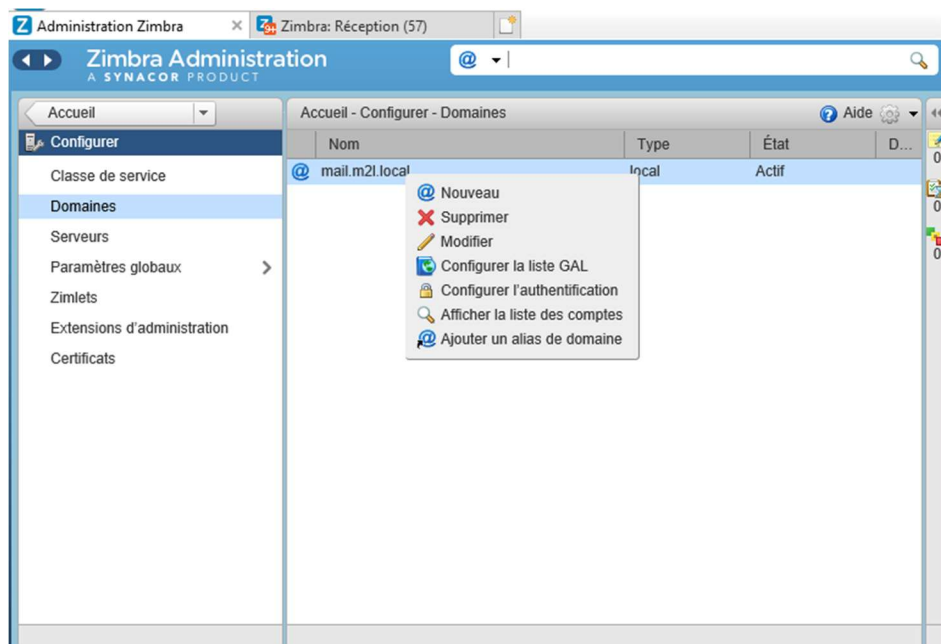
16- Création d'alias m2l.local pointant sur mail.m2l.local

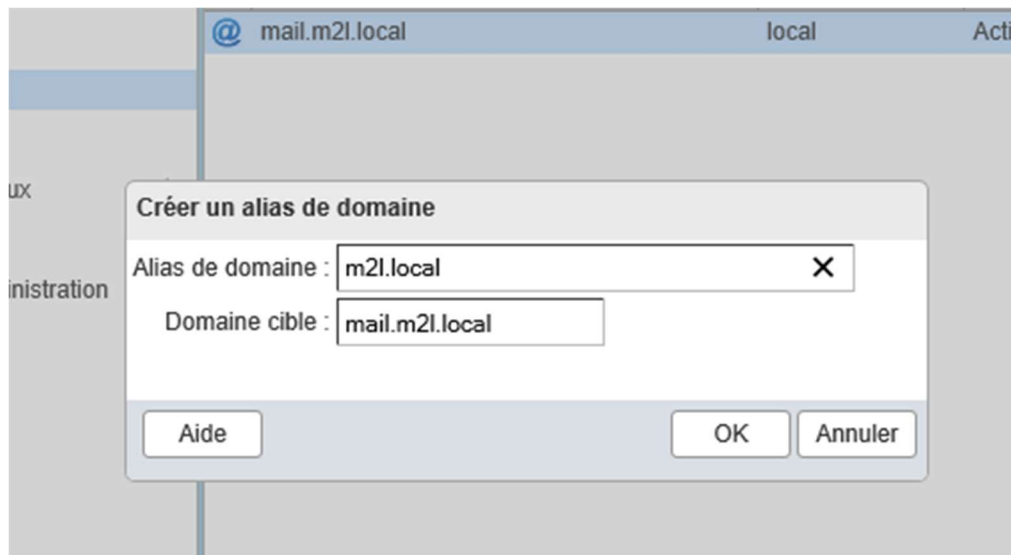
Sur <https://mail.m2l.local:7071> :

Accueil -> Configurer -> Domaine -> Sélectionnez le domaine mail.m2l.local ->
 clic droit, ajouter un alias au domaine:

alias de domaine : m2l.local

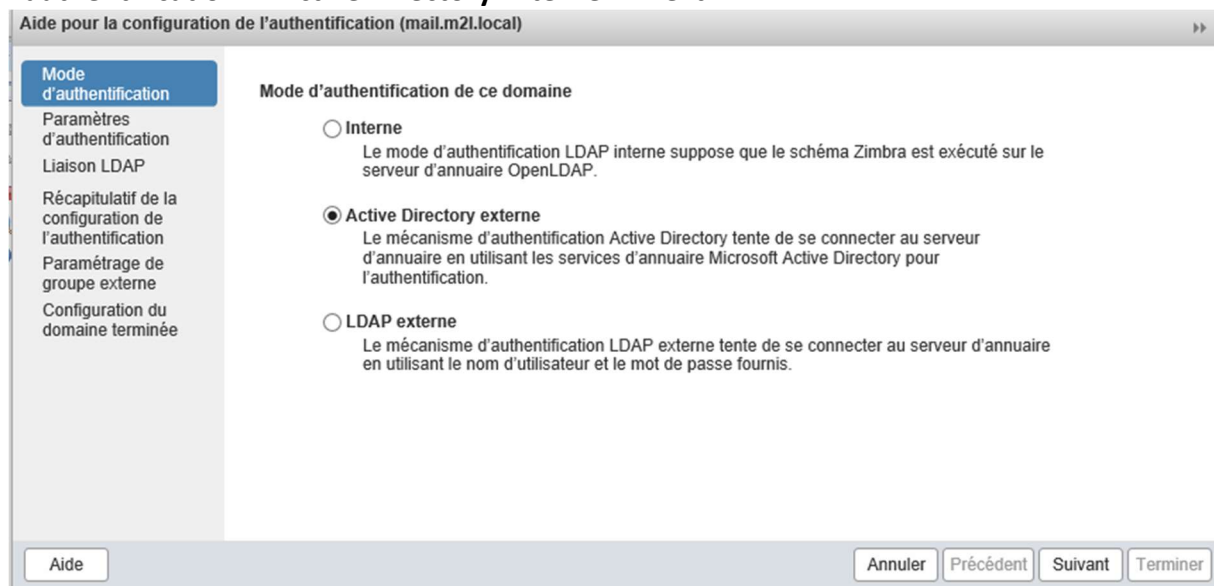
domaine cible : mail.m2l.local





17- Configuration de l'authentification AD

RDV interface web de Zimbra : clique droit sur mail.m2l.local -> **Configurer l'authentification** -> **Active Directory Externe** -> **Next**



Domaine du serveur : m2l.local

Nom du serveur AD : 172.20.0.10 (Adresse IP de DC)

Comme :

Aide pour la configuration de l'authentification (mail.m2l.local)

Mode d'authentification

Paramètres d'authentification

Liaison LDAP

Récapitulatif de la configuration de l'authentification

Paramétrage de groupe externe

Configuration du domaine terminée

Paramètres Active Directory

Domaine du serveur AD :

Serveur AD

Nom du serveur AD : Port : Utiliser SSL : ☐

Ldap:// X

Ajouter une URL

Supprimer

Suivant → Suivant → aller à Récapitulatif de la configuration de l'authentification

Renseignez le compte administrateur AD de la machine DC puis tester avec le bouton **Tester**

-> Suivant -> Suivant -> Terminer

Aide pour la configuration de l'authentification (mail.m2l.local)

Mode d'authentification

Paramètres d'authentification

Liaison LDAP

Récapitulatif de la configuration de l'authentification

Paramétrage de groupe externe

Configuration du domaine terminée

Récapitulatif de la configuration de l'authentification

Mécanisme d'authentification : Active Directory externe

Domaine du serveur AD : m2l.local

URL LDAP : Ldap://172.20.0.10:3268

Veuillez fournir un nom d'utilisateur et un mot de passe pour tester les paramètres d'authentification

Nom d'utilisateur :
Mot de passe :

Tester

Le test d'authentification a réussi

DN de liaison administrateur@m2l.local
calculé :

18- Création d'utilisateur sur DC

Aller sur l'AD de la machine DC pour créer deux utilisateurs dans users : 'user1' et 'user2'

Le mot de passe des utilisateurs est toujours **Bts2024\$**

Nouvel objet - Utilisateur

Créer dans : m2l.local/Users

Quand vous cliquerez sur Terminer, l'objet suivant sera créé :

Nom complet : user1
Nom de connexion de l'utilisateur : user1@m2l.local
L'utilisateur ne peut pas changer de mot de passe.
Le mot de passe n'expire jamais.

< Précédent **Terminer** Annuler

19- Création d'utilisateur sur Zimbra

RDV interface d'administration de Zimbra <https://mail.m2l.local:7071>

Allez dans **Accueil** -> **Gérer**-> **Comptes**-> En haut à droite "petite molette", cliquer sur **nouveau**.

Créer le premier utilisateur de l'AD (le même nom : user1 et nom de famille : famille1), puis cliquer directement sur **Terminer**.

Créer le deuxième utilisateur de l'AD (le même nom : user2 et nom de famille : famille1), puis cliquer directement sur **Terminer**.

Accueil - Gérer			 Aide 
	Adresse mail	Nom affiché	État
	admin@mail.m2l.local		Actif
	user1@mail.m2l.local	famille1	Actif
	user2@mail.m2l.local	famille1	Actif

20- Validation n°4

Se déconnecter de l'interface d'administration, pour se connecter avec l'un des deux utilisateurs à sa boîte de messagerie <https://mail.m2l.local:8443>

Utilisateur : user1/user2

mot de passe : Bts2024\$

Envoyer un mail à user2.

Se déconnecter puis se reconnecter avec l'autre utilisateur pour vérifier la réception du mail.



Bonne réception du mail

21- Test de l'envoi du mail à l'extérieur

Envoyez un mail à votre adresse personnelle : Ça ne s'envoie pas par mesure de sécurité.