

CONFIGURER POUR SECURISER

Notes

Fabrice BODSON

HELMo | BAC 2 | 2020-2021

Table des matières

1. Partie 1 - Windows	2
1.1. Script PowerShell.....	2
1.2 Administration locale	3
1.3 Les partages	7
1.4 Services réseaux	8
1.5 Installation d'Active Directory	12
1.6 Introduction aux GPO	16
1.7 Gestion des GPO.....	17
1.8 Sauvegarde et restauration	21
1.9 Service de bureau à distance	22
2. Partie 2 – Linux.....	26
2.1 Introduction	26
2.2 Scripting Linux	30
2.3 Administration du disque dur	33
2.4 Sauvegardes et planification.....	36
2.5 Configuration réseau	37
2.5.1 Configuration réseau	37
2.5.2 Démarrage système.....	38
2.6 Routage.....	39
2.7 Service SAMBA	39
2.8 Configuration d'Apache	41
2.9 Service DNS	44
2.10 Administration à distance.....	47
2.11 Service FTP	48
2.12 Mail.....	50
2.13 Firewall	53
2.14 DHCP	56

1. Partie 1 - Windows

1.1. Script PowerShell

1. Sur base du fichier « liste-users.csv », on vous demande, pour chaque ligne présente dans le fichier, **d'afficher à l'écran** le contenu de celle-ci en ajoutant deux nouveaux champs : le *login* et le *mot de passe* de l'utilisateur.

1. Le login sera formé comme suit : la 1^{ère} et la dernière lettre de la catégorie (**administratif→af**). Ces lettres seront suivies d'un numéro de séquence par catégorie. Ainsi, s10073 identifie le 73^{ème} utilisateur de la catégorie *social* alors que p10040 identifie le 40^{ème} utilisateur de la catégorie *personnel*.
2. Le mot de passe comptera exactement 8 caractères et comprendra 2 chiffres, deux lettres majuscules et 4 lettres minuscules. Pour composer ce mot de passe, vous pouvez faire appel à la cmdlet `Get-Random` qui fournit un nombre aléatoire. On vous demande de coder vous-même la génération du mot de passe. Pensez que la position des lettres et chiffres dans le mot de passe est aléatoire (il serait incorrect de supposer que le mot de passe commence par une minuscule puis un chiffre, ...). **Attention ! Tous les utilisateurs numérotés 50 (af0050, pl0050, ie0050, ...)** doivent avoir « **P@ssw0rd** » comme mot de passe.

Les lignes commençant par un '#' doivent être ignorées, ce sont des commentaires.

```
$contenu = Get-Content "C:\Users\Administrator\Desktop\Scripts\liste-users.csv"
$compteur = @{}

$number_nb = 2
$upper_letter_nb = 2
$lower_letter_nb = 4

foreach ($ligne in $contenu) {
    # 3 \w afin d'assurer d'avoir 1ere, dernière et d'autres lettre pour créer le login
    if ($ligne -match '^([a-zA-Z]+)([a-zA-Z]+)(\w+)\w+($)' ) {
        ## Création du login
        $key = $Matches[3][0] + $Matches[3][-1]

        if ($compteur.ContainsKey($key)) {
            $compteur[$key]++;
        } else {
            $compteur.Add($key, 0)
        }

        $login = ($key + $($compteur[$key]).ToString("0000"))

        ## Création du mot de passe
        $password = ""

        # Chiffres
        for ($i = 1; $i -le $number_nb; $i++) {
            $random_nb = get-random -Minimum 0 -Maximum 10
            $password += $random_nb
        }

        # Majuscules
        for ($i = 1; $i -le $upper_letter_nb; $i++) {
            [char]$letter = Get-Random -Minimum 65 -Maximum 90
            $password += $letter
        }

        # Minuscules
        for ($i = 1; $i -le $lower_letter_nb; $i++) {
            [char]$letter = Get-Random -Minimum 97 -Maximum 122
            $password += $letter
        }

        $password = ($password -split '') | Sort-Object {Get-Random} -join ''
        Write-Output "$($login) -- $($password)"
    }
}
```

1.2 Administration locale

1. En reprenant le fichier obtenu à l'exercice 1 de la leçon 2, écrivez un script Powershell permettant de créer les comptes des utilisateurs.

- Le script fixera le mot de passe, le chemin d'accès local à C:\UserData\<login> ainsi que le chemin vers le profil à C:\UserData\<login>\myprofile.
- Un groupe particulier sera créé par catégorie¹⁸. Tous les utilisateurs seront membres du groupe *Users* et du groupe spécifique correspondant à sa catégorie (*administratif-communication-comptabilité ...*)
- Les dossiers suivants seront créés:
 - C:\UserData\<login>
 - C:\UserData\<login>\myprofile.V6

Vous ajouterez une autorisation de type *contrôle total* à l'utilisateur sur ces dossiers.

- Vérifiez si tout s'est bien passé ! Tentez de vous connecter avec l'un des comptes créés.

(Conseil : testez votre script sur un nombre très réduit d'utilisateurs : les deux premiers par exemple)

2. Localisez le profil de l'utilisateur avec lequel vous vous êtes connectés. Jetez un œil aux données présentes à l'intérieur

SCRIPT :

```
$listes_users = Get-Content "C:\AdministrationLocale\liste-users.csv"
$compteur = @{}

## Valeur incrémentale pour la création du password
$number_nb = 2
$upper_letter_nb = 2
$lower_letter_nb = 4

$i = 0

foreach ($ligne in $listes_users) {
    ## 3 \w afin d'assurer d'avoir 1ere, dernière et d'autres lettre pour créer le login
    if ($ligne -match '^([^\w]+)([^\w]+)((\w)\w+(\w))$') {

        ## Récupération du nom
        $nom = $Matches[1]

        ## Récupération du prénom
        $prenom = $Matches[2]

        ## Récupération du groupe
        $groupe = $Matches[3]

        ## Création du login

        $key = $Matches[3][0] + $Matches[3][-1]

        if ($compteur.ContainsKey($key)) {
            $compteur[$key]++;
        } else {
            $compteur.Add($key, 0)
        }
    }
}
```

```

$login = ($key + $($compteur[$key]).ToString("0000"))

## Création du mot de passe

if($compteur[$key] -eq 50){
    $password = "P@ssw0rd"
} else {
    $password = ""

## Chiffres

for ($i = 1; $i -le $number_nb; $i++) {
    $random_nb = Get-Random -Minimum 0 -Maximum 10
    $password += $random_nb
}

## Majuscules

for ($i = 1; $i -le $upper_letter_nb; $i++) {
    [char] $letter = Get-Random -Minimum 65 -Maximum 90
    $password += $letter
}

## Minuscules

for ($i = 1; $i -le $lower_letter_nb; $i++) {
    [char] $letter = Get-Random -Minimum 97 -Maximum 122
    $password += $letter
}

$password = ($password -split '' | Sort-Object {Get-Random}) -join ''

write-output "$($login) -- $($password) -- $($nom) -- $($prenom) -- $($groupe)"

## Vérification de l'existence d'un groupe afin de pouvoir le créer dans le cas où il n'existe pas
try {
    Get-LocalGroup -Name $groupe -ErrorAction Stop
}
catch {
    New-LocalGroup -Name $groupe
}

## Vérification de l'existence de l'utilisateur
try {
    Get-LocalUser -Name $login -ErrorAction stop
}
catch {

## Création du chemin
New-Item -ItemType D -Path "C:\UserData\$login"
New-Item -ItemType D -Path "C:\UserData\$login\myprofile"

## Création utilisateur
$utilisateur = New-LocalUser -AccountNeverExpires
>PasswordNeverExpires -UserMayNotChangePassword
-FullName $($prenom + " " + $nom.ToUpper()) -Name $login
-Password (ConvertTo-SecureString -AsPlainText $password -Force)

## Création des chemins des utilisateurs

$userADSI = [ADSI] "WinNT://$env:computername/$login"

$userADSI.Profile = "C:\UserData\$($login)\myprofile"
$userADSI.HomeDirectory = "C:\UserData\$($login)"

$userADSI.SetInfo()
}

```

```

## Vérification de l'appartenance de l'utilisateur aux groupes
try {
    Get-LocalGroupMember -Group $groupe -Member $utilisateur -ErrorAction stop
    Get-LocalGroupMember -Group "Users" -Member $utilisateur -ErrorAction stop
}
catch {
## Ajout de l'utilisateur dans son groupe
    Add-LocalGroupMember -Group $groupe -Member $utilisateur
    Add-LocalGroupMember -Group "Users" -Member $utilisateur
}

```

3. Ecrivez le script qui permet de supprimer les comptes des utilisateurs créés précédemment.
Pour ce faire, utilisez la cmdlet Remove-LocalUser

```

$listes_users = Get-Content "C:\AdministrationLocale\liste-users.csv"
$compteur = @{}
$i = 0
foreach ($ligne in $listes_users){
    if ($ligne -match '^([^\;]+;([^\;]+;((\w)\w+(\w))$') {
        ## Création du login
        $key = $Matches[3][0] + $Matches[3][-1]
        if ($compteur.ContainsKey($key)) {
            $compteur[$key]++
        } else {
            $compteur.Add($key, 0)
        }
        $login = ($key + $($compteur[$key]).ToString("0000"))
        <#
        try {
            Get-LocalUser -Name $login
            Remove-LocalUser -Name $login
            Remove-Item -Path "C:\UserData\$login\myprofile"
        }
        catch {
            Write-Output "User $($login) does not exist" []
        }
        #>
        try {
            Get-LocalGroup -Name $groupe -ErrorAction Stop
            Remove-LocalGroup -Group $login
        }
        catch {
            Write-Output "User $($login) does not exist"
        }
        <#
        if($compteur[$key] -eq 3) {
            break
        }
        #>
    }
}

```

4. (Via l'interface graphique) Créer un compte *helmo*

- Sans mot de passe.
- Fixer le chemin le chemin d'accès local à C:\UserData\helmo et le profil dans C:\UserData\helmo\preconfig
- Créer les dossiers C:\UserData\helmo et C:\UserData\helmo\preconfig.V6.

Fixer les droits pour que *helmo* dispose d'un *contrôle total* sur ces dossiers

- Connectez-vous avec ce login.
- Créer un lien vers le serveur DATA (\\\192.168.128.3) et placez ce raccourci sur le bureau.
- Transformer ce profil standard en profil obligatoire.
- Testez-le!

5. Modifier le script d'ajout des utilisateurs pour que des quotas soient ajoutés en même temps.

Prévoyez deux versions : l'utilisation des quotas disques et l'utilisation des quotas basés sur le chemin. Les quotas à respecter par catégories sont les suivants :

- Administratif, social, comptabilité et direction : quota=400 Mo ; Alerte=390 Mo
- E-Learning, etudiant, juridique et travaux: quota = 300 Mo ; Alerte à 290 Mo
- Informatique, communication et personnel : quota = 800 Mo ; Alerte à 750 Mo

Il sera peut être nécessaire de modifier le script suivant le type de quota à adapter.

- Vérifiez que les quotas sont effectivement appliqués.

QUOTAS (suite du script) :

```

## Création des quotas disques selon les groupes
if($login.Substring(0,2) -eq "af" -or $login.Substring(0,2) -eq "s1" -or $login.Substring(0,2) -eq "ce" -or $login.Substring(0,2) -eq "dn"){
    $quotas_disques = &"fsutil" "quota" "modify" "c:" "390000000" "400000000" "$($login)"
}
if($login.Substring(0,2) -eq "eg" -or $login.Substring(0,2) -eq "et" -or $login.Substring(0,2) -eq "je" -or $login.Substring(0,2) -eq "tx"){
    $quotas_disques = &"fsutil" "quota" "modify" "c:" "290000000" "300000000" "$($login)"
}
if($login.Substring(0,2) -eq "ie" -or $login.Substring(0,2) -eq "cn" -or $login.Substring(0,2) -eq "pl"){
    $quotas_disques = &"fsutil" "quota" "modify" "c:" "750000000" "800000000" "$($login)"
}

## Création des quotas pour le chemin selon les groupes
$fqtm = New-Object -com Fsrm.FsrmQuotaManager
$quota_chemin = $fqtm.CreateQuota("C:\UserData\$($login)")

if($login.Substring(0,2) -eq "af" -or $login.Substring(0,2) -eq "s1" -or $login.Substring(0,2) -eq "ce" -or $login.Substring(0,2) -eq "dn"){
    $quota_chemin.ApplyTemplate("Group a")
    $quota_chemin.Commit()
}
if($login.Substring(0,2) -eq "eg" -or $login.Substring(0,2) -eq "et" -or $login.Substring(0,2) -eq "je" -or $login.Substring(0,2) -eq "tx"){
    $quota_chemin.ApplyTemplate("Group b")
    $quota_chemin.Commit()
}
if($login.Substring(0,2) -eq "ie" -or $login.Substring(0,2) -eq "cn" -or $login.Substring(0,2) -eq "pl"){
    $quota_chemin.ApplyTemplate("Group c")
    $quota_chemin.Commit()
}

## Privilèges de l'utilisateur
$privilege = &"icacls" "C:\UserData\$($login)" "/grant" "$($login):(OI)(CI)(F)"

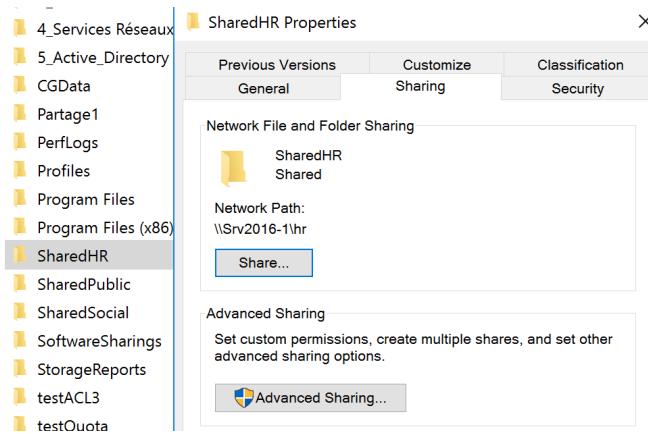
if($compteur[$key] -eq 3) {
    break
}
}

}

```

1.3 Les partages

1. Configurer un partage disque nommé « HR » qui pointe vers le dossier C:\SharedHR que vous aurez créé
 - a. Ce partage doit être accessible en modification aux membres du groupe personnel et en lecture aux membres de direction (voir leçon 3)
 - b. Testez votre configuration en utilisant l'hôte Windows pour y accéder



2. En utilisant la ligne de commande, accéder à votre dossier personnel sur DATA. Déconnectez-vous complètement du serveur en utilisant également la ligne de commande.

```
C:\> net use G: \\192.168.128.3\public
```

3. Pour le compte Administrateur de votre serveur, ajouter un lecteur réseau H: connectant votre dossier personnel sur DATA et activez la reconnexion automatique.

Aller dans PC > Computer (en haut) > Map Network Drive et ajouter :

What network folder would you like to map?

Specify the drive letter for the connection and the folder that you want to connect to:

Drive: H: (\\"192.168.128.3\Users\St...)

Folder: \\\\"192.168.128.3\Users\Students\E190230

Example: \\\server\share

Reconnect at sign-in

Connect using different credentials

[Connect to a Web site that you can use to store your documents and pictures.](#)

1.4 Services réseaux

1. Installer le **service DNS** comme suit :

Avoir IP statique et ajouter le rôle DNS Server. Puis aller dans Tools > DNS > SRV2016-1

- a. Le nom de domaine correspondra à *votre nom de famille* suffixé par « *.local* ». Par exemple `swinnen.local`

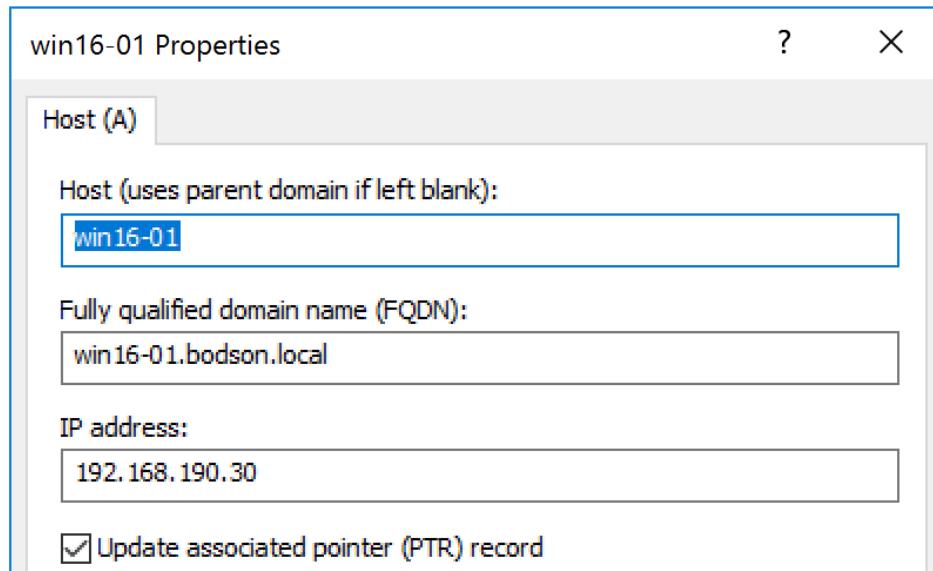
SRV2016-1 > Forward Lookup Zones > New Zone

Primary Zone > bodson.local > New file & changer le nom en `bodson.local` > Do not allow dynamic.

- b. Ajouter les entrées suivantes :

- i. `fw` qui pointera vers l'adresse IP du firewall
- ii. `win16-01` qui pointera vers l'adresse IP de votre serveur
- iii. `host` qui pointera vers l'adresse IP de la machine hôte `192.168.190.1`

 fw	Host (A)	192.168.190.2
 host	Host (A)	192.168.190.1
 win16-01	Host (A)	192.168.190.30



- iv. Créer la zone inverse pour le sous-réseau 192.168.190.0 et ajoutez les entrées PTR pour fw, host et win16-01

Reverse Zone Lookup > clic droit > New zone > Primary zone > ipv4 reverse > IP réseau > New file > not allow dynamic > Finish

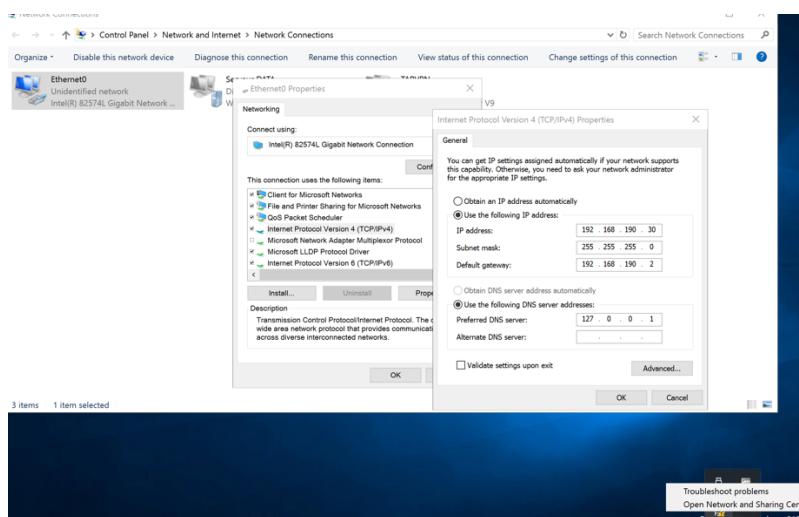
 192.168.190.1	Pointer (PTR)	host.bodson.local.
 192.168.190.2	Pointer (PTR)	fw.bodson.local.
 192.168.190.30	Pointer (PTR)	win16-01.bodson.local.

- c. Configurer le redirecteur pour qu'il pointe vers le serveur DNS 192.168.128.2

Conditional forwarder > Clic droit > New > Ajouter nom et IP

2. Configurer votre serveur Windows pour qu'il soit client du serveur DNS configuré.

- Créer une entrée qui correspond au DNS courant et ajouter l'IP. (Déjà fait avec win16-01)
- Aller dans **This PC > clic droit > Properties > Advanced system settings > Computer name > Change > More > Ajouter le nom DNS configuré comme suffixe DNS principal**
- Reboot
- Modifier les paramètres de la carte réseau pour modifier le serveur DNS à interroger en **localhost**. (**Clic droit sur le truc réseau en bas > Open Network > Change adaptater settings > Clic droit sur ethernet 0 > Double clic sur IPv4**)



3. Installer le service DHCP comme suit :

Il faut ajouter le rôle *DHCP Server*. Sur la notification *Complete DHCP configuration* il faut cliquer sur le lien et appuyer sur *commit*. Puis démarrer le service **Tools > DHCP**.

- Désactiver le serveur DHCP présent dans pfSense (**Services > DHCP Server**)
- Configurer une nouvelle étendue DHCP entre les adresses 192.168.190.150–200
- Précisez toutes les options nécessaires (DNS, ...)

IPv4 > clic droit > Nom + description > 192.168.190.150 + 192.168.190.200 + 255.255.255.0
> IP à ne pas inclure (éventuel) > 4h > Router (Default Gateway) = 192.168.190.30 > DNS Server = 192.168.190.30 (pas localhost !!) > Wins Server (ignorer) > Activate Scope

4. Créer un script Powershell qui va créer des entrées dans le serveur DNS pour chaque adresse comprise dans la plage DHCP (entre 192.168.190.150 et 192.168.190.200). Chaque entrée comprendra un enregistrement dans la zone directe et dans la zone de recherche inversée. Par exemple, voici un nom configuré : ip-192-168-190-200.<votre-nom>.local qui pointera vers l'adresse 192.168.190.200, et ainsi de suite pour toutes les autres adresses.

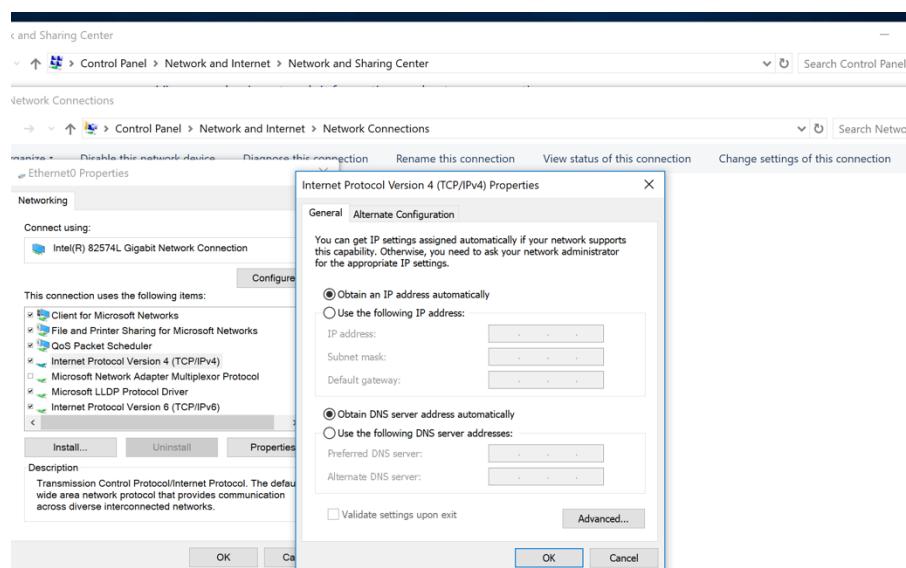
```

1 $ip_start = 150
2 $ip_end = 200
3
4 while($ip_start -le $ip_end) {
5     $dns_forward_entry = &"dnscmd" "SRV2016-1" "/RecordAdd" "bodson.local" "ip-192-168-190-$($ip_start.ToString())" "A" "192.168.190.$($ip_start.ToString())"
6     $dns_reverse_entry = &"dnscmd" "SRV2016-1" "/RecordAdd" "190.168.192.in-addr.arpa" "$($ip_start.ToString())" "PTR" "ip-192-168-190-$($ip_start.ToString()).bodson.local"
7
8     $ip_start++
9 }
10
11 $dns_forward_entry = &"dnscmd" "SRV2016-1" "/RecordAdd" "bodson.local" "ip-192-168-190-155" "A" "192.168.190.155"
12 $dns_reverse_entry = &"dnscmd" "SRV2016-1" "/RecordAdd" "190.168.192.in-addr.arpa" "155" "PTR" "ip-192-168-190-155.bodson.local"

```

5. Installer une nouvelle machine Windows 10²² (mot de passe : rootroot)

- Configurée en mode DHCP
- Vérifiez la configuration réseau reçue et assurez-vous qu'elle a bien accès à Internet



6. A l'aide de **la ligne de commande** :

- a. Ajouter une réservation DHCP pour cette machine avec l'adresse 192.168.190.155 (assurez-vous que le serveur ne distribue plus cette adresse)

Commencer par exclure l'IP qui sera réservée.

```
netsh dhcp server 127.0.0.1 scope 192.168.190.0 add excluderange  
192.168.190.155 192.168.190.155
```

Ensuite, réserver et assigner l'IP :

```
netsh dhcp server 127.0.0.1 scope 192.168.190.0 add reservedip 192.168.190.155  
000C29BD9706 nom_de_lentree_DNS DHCP
```

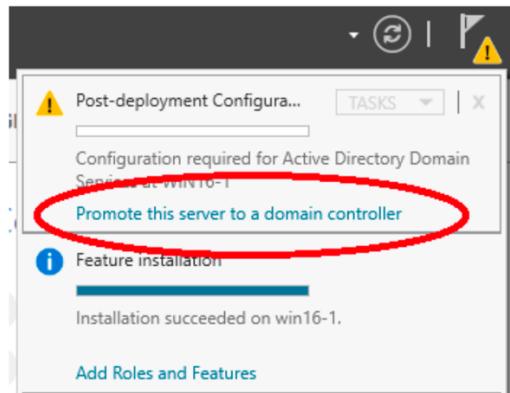
- b. Ajouter un alias DNS (**CNAME**) pour faire pointer le nom suivant : vm10.<votre-nom>.local vers le nom ip-192-168-190-155.<votre-nom>.local.

```
dnscmd bodson.local /RecordAdd ip-192.168.190.155.bodson.local CNAME  
vm10.bodson.local
```

1.5 Installation d'Active Directory

1. Supprimer tous les comptes utilisateurs créés par script (leçon 3, exercice 3)
2. Installer le rôle AD Domain Services et configurer votre contrôleur de domaine AD :

Le rôle s'appelle Active Directory Domain Services > accepter toutes les fonctionnalités proposées. Dans le haut du menu, cliquer sur le lien :



Dans le menu qui suit, ajouter une nouvelle forêt :

- a. Le nom de domaine est `cg01dom.local`
- b. Utiliser le mot de passe `P@ssw0rd` pour le mode restauration
- c. Fixer le niveau fonctionnel de la forêt à Windows 2016
- d. (optionel) Si votre système propose de changer votre mot de passe Administrateur, utilisez `Pa$$w0rd`
- e. Supprimez la stratégie de mot de passe par défaut du domaine

Tools > Group Policy Management > cg01dom.local > Default Domain Policy > clic droit > Edit > Computer Configuration > Policies > Windows Settings > Security Settings > Account Policies > Password Policies > Mettre les valeurs à 0 et disabled.

Policy	Policy Setting
Enforce password history	0 passwords remembered
Maximum password age	0 days
Minimum password age	0 days
Minimum password length	0 characters
Password must meet complexity requirements	Disabled
Store passwords using reversible encryption	Disabled

Si message « A delegation for this DNS server cannot be created ... » ce n'est pas grave, ne pas créer de délégation.

Laisser les options par défaut. Un redémarrage automatique se fait. Si au moins d'entrer les credentials le « `cg01dom.local` » apparaît, c'est bon.

Il faut autoriser le serveur DHCP : **Server Manager > Tools > DHCP > Choisir serveur > Clic droit > Autorize.**

Il faut ensuite **reboot** l'ordinateur.

3. Créer un dossier partagé c:\CGData muni des autorisations adéquates pour stocker les profils des utilisateurs.
4. Créer une unité d'organisation CGComputers et créer un compte d'ordinateur VM-WIN10 pour la machine virtuelle Windows 10.

Tools > AD Users and Computers > cg01dom.local > clic droit > New > Organizational Unit > Nom CGComputers + décocher la case

Clic droit sur CGComputers > VM-WIN10

5. Réécrivez votre script de création des utilisateurs pour :
 - a. Créer des utilisateurs membres du domaine AD
 - b. Les utilisateurs seront créés dans une OU CGUsers et vous créerez une OU par catégorie. Ainsi les utilisateurs de *direction* seront placés dans la branche CGUsers\direction.
 - c. Créer un groupe de sécurité globale par catégorie. Ainsi, dans le groupe de sécurité informatique, on trouvera tous les utilisateurs de la catégorie *informatique*.
 - d. Fixer le chemin vers le profil de l'utilisateur vers le chemin CGData\<login>\netprofile. Fixer également le chemin vers le dossier de base CGData\<login> et connectez un lecteur P: (cf. exercice 3).
 - e. Fixer les ACL vers les dossiers correctement

```
$listes_users = Get-Content "C:\2_AdministrationLocale\liste-users.csv"
$compteur = @{}

## valeur incrémentale pour la création du password
$number_nb = 2
$upper_letter_nb = 2
$lower_letter_nb = 4

$i = 0

foreach ($ligne in $listes_users) {
  ## 3 \w afin d'assurer d'avoir 1ere, dernière et d'autres lettre pour créer le login
  if ($ligne -match '^(\w;+);(\w;+);(\w)\w+(\w)$') {
    ## Récupération du nom
    $nom = $Matches[1]

    ## Récupération du prénom
    $prenom = $Matches[2]

    ## Récupération du groupe
    $groupe = $Matches[3]

    ## Création du login
    $key = $Matches[3][0] + $Matches[3][-1]

    if ($compteur.ContainsKey($key)) {
      $compteur[$key]++;
    } else {
      $compteur.Add($key, 0)
    }

    $login = ($key + $($compteur[$key]).ToString("0000"))
  }
}
```

```

## Création du mot de passe
if($compteur[$key] -eq 50){
    $password = "P@ssw0rd"
} else {
    $password = ""

    ## chiffres
    for ($i = 1; $i -le $number_nb; $i++) {
        $random_nb = Get-Random -Minimum 0 -Maximum 10
        $password += $random_nb
    }

    ## Majuscules
    for ($i = 1; $i -le $upper_letter_nb; $i++) {
        [char]$letter = Get-Random -Minimum 65 -Maximum 90
        $password += $letter
    }

    ## Minuscules
    for ($i = 1; $i -le $lower_letter_nb; $i++) {
        [char]$letter = Get-Random -Minimum 97 -Maximum 122
        $password += $letter
    }

    $password = ($password -split '') | Sort-Object {Get-Random} -join ''
}

## Création du chemin
$new_OU = New-ADOrganizationalUnit -Name "Service $groupe" -Path "OU=CGUsers,DC=cg01dom,DC=local" ` 
-ProtectedFromAccidentalDeletion $false

$new_Security_Group = New-ADGroup -Name $groupe -samAccountName $groupe ` 
-GroupCategory Security -GroupScope Global ` 
-Path "OU=Service $groupe,OU=CGUsers,DC=cg01dom,DC=local"

## Priviléges de l'utilisateur
$privilege = &"icacls" "C:\CGData\$login" "/grant" "$($login):(OI)(CI)(F)"

}

```

6. Ajouter la VM Win10 à votre domaine et tentez une connexion avec un compte utilisateur

- Changez son nom en VM-WIN10 et ajoutez-la dans le domaine

Sur la VM win10 This PC > clic droit > properties > Change settings > Change > Entrer nom + domaine

NB : le client doit utiliser le srv-2016 comme serveur DNS. (via config DHCP, ça c'est fait)

- Vérifiez bien que le profil de l'utilisateur est trouvé

**Se connecter sur la machine en utilisant CG01DOM\Administrator
Vérifier que la machine est ajoutée dans le AD Users and Computers**

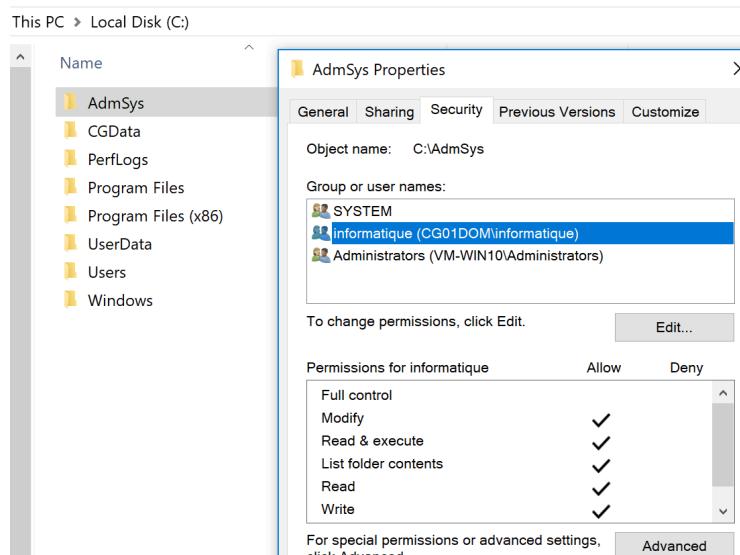
7. Créez un compte `helmodom` avec comme mot de passe `cgdom2016` comme étant un compte de domaine obligatoire. Fixer le chemin vers son profil et son répertoire de base (comme pour les utilisateurs créés à l'étape 5).

8. Connectez-vous avec le compte `Administrator` du domaine sur la VM Win10.

- a. Comment procéder ?

Se connecter sur la machine en utilisant CG01DOM\Administrator

- b. Où est stocké le profil ?
c. Créez un dossier `AdmSys` sur le disque C: uniquement accessible aux utilisateurs de la catégorie *informatique*



1.6 Introduction aux GPO

Aller dans **Tools > Group Policy Management**

Créer la GPO sur une des OU puis sur les autres OU il faut les lier à cette GPO. Ajouter les groupes et supprimer celui par défaut dans Security filtering.

1. Empêcher les membres des catégories *étudiants* et *e-learning* d'avoir accès à l'outil d'édition du registre. **Créez une seule GPO liée aux OUs concernées.**

User Config > Policies > Administrative > System > Prevent access to registry ...

2. Empêcher tous les utilisateurs, excepté les membres de la catégorie *informatique*, de lancer l'invite de commande. **Limitez aux utilisateurs concernés en utilisant les filtrages de sécurité (Security Filtering) uniquement.**

User Config > Policies > Administrative > System > Prevent access to command prompt

3. Créer un partage réseau SharedSocial et connecter les membres de la catégorie *social* à ce partage (lecteur X:, accès en modification pour *social*, inaccessible pour les autres). Ajoutez une GPO Ordinateur « *Configure Logon Script Delay* » à *0 minute*, sur les postes clients (VM Windows 10).
4. Pour protéger la stratégie des mots de passe du domaine, arrangez-vous pour que celle-ci soit toujours prioritaire (en 1^{ère} position dans l'onglet *Group Policy Inheritance*).

Cg01dom.local > Default Domain Policy > clic droit > enforced

5. Permettre aux membres de la catégorie *informatique* d'ouvrir une session locale sur le contrôleur de domaine

Sur cg01dom.local > Computer Config > Policies > Windows Settings > Security Settings > Local Policies > Allow log on locally > Ajouter groupes info et admin

6. Pour des questions de sécurité, on ne souhaite pas voir apparaître le nom de la dernière personne connectée sur les postes clients (VM Windows 10).

GPO sur CG Computers et VM-WIN10 dans le security filtering > Computer Config > Policies > Windows Settings > Security Settings > Local Policies > Security options > Interactive Logon: Do not display last user name

7. Réaliser une redirection de dossier (tous) pour les membres de la catégorie *travaux* de sorte que les dossiers soient placés dans leur profil. Ainsi, leur bureau devra se trouver dans CGData\<login>\Desktop (et ainsi de suite pour tous les dossiers).

Sur OU travaux > User Config > Policies > Windows Settings > Folder Redirection > Sélectionner les dossiers à rediriger

8. Créer un partage réseau SharedPublic et connecter tous les utilisateurs à ce partage (lecteur Q:, tout le monde en lecture, direction en modification).

1.7 Gestion des GPO

1. Créer un groupe de sécurité AdminMachines et ajoutez-y le groupe administratif

AD Users & Computers > clic droit sur cg01dom.local > new > group > AdminMachines + global + security

Clic droit dessus > Properties > Members > Ajouter administratif

2. Déléguer le contrôle de l'OU personnel aux membres du groupe informatique.

Clic droit sur l'OU personnel > Delegate control > sélectionner groupe info > donner les droits

3. Créer les GPO suivantes nommées comme indiqué :

- A. auditObjet - GPO d'audit sur la création / suppression d'utilisateurs dans l'OU personnel (voir exercice 2)

Clic droit sur l'OU personnel > Computer Configuration > Policies > Windows Settings > Security > Local Policies > Audit account management > Success + failure

- B. outilsInstall - GPO d'installation sur les ordinateurs contenus dans l'OU clients. On vous demande de déployer les programmes *firefox 32.0* et *putty 0.69*. Vérifiez que l'installation s'est déroulée correctement sur votre VM Windows 10.

Configuration en mode **Computer**. Partage réseau créé avec les fichiers msi dedans.

Nouvelle GPO sur Clients > Computer Conf > Policies > Software Settings > Software installation > clic droit > New > Package > Sélectionner fichier msi > Assigned > OK

- C. auditEchecConnexion - GPO d'audit sur tous les ordinateurs (clients et servers) du domaine consignant les échecs de connexion.

Clic droit sur CGComputers > Computers Conf > Policies > Windows > Security > Local Policies > Audit account events > Failure + Audit logon events > Failure

- D. boucleRappel – GPO appliquée sur l'OU Servers, activation du mode bld de rappel (en mode *merge*), mais ne pas appliquer aux administrateurs. Imposer les restrictions suivantes :

Clic droit sur Servers > New GPO > Computer Conf > Policies > Administrative > System > Configure user GroupPolicy loopback processing mode > enable + merge

Dans le User Config > Policies > Administrative Templates :

- a. Bureau (... > Desktop) :

- i. Cacher l'icône Emplacements réseau sur le bureau
- ii. Cacher l'icône Internet Explorer sur le Bureau
- iii. Empêcher l'ajout, le glisser-deplacer et la fermeture des barres d'outils de la Barre des tâches

- iv. Empêcher l'utilisateur de rediriger manuellement des dossiers de profils
- v. Empêcher le redimensionnement des barres d'outils du Bureau
- vi. Ne pas enregistrer les paramètres en quittant
- vii. Supprimer le poste de travail du bureau

Desktop	
Policy	Setting
Don't save settings at exit	Enabled
Hide Internet Explorer icon on desktop	Enabled
Hide Network Locations icon on desktop	Enabled
Prevent adding, dragging, dropping and closing the Taskbar's toolbars	Enabled
Prohibit adjusting desktop toolbars	Enabled
Prohibit User from manually redirecting Profile Folders	Enabled
Remove Computer icon on the desktop	Enabled

- b. Composants Windows / Console de gestion Microsoft / Composants logiciels enfichables restreints/autorisés (... > **Windows Components / Microsoft Management** ...) :
- i. Désactiver le gestionnaire de serveur

Windows Components/Microsoft Management Console/Restricted/Permitted snap-ins	
Policy	Setting
Server Manager	Disabled

- c. Menu démarrer et barre des tâches (... > **Start Menu and Taskbar**) :
- i. Désactiver le nettoyage de la zone de notification
 - ii. Effacer l'historique des documents récemment ouverts en quittant
 - iii. Ne pas utiliser la méthode basée sur la recherche pour déterminer les raccourcis du bureau
 - iv. Ne pas utiliser la méthode basée sur la recherche pour déterminer les raccourcis de l'environnement
 - v. Supprimer et empêcher l'accès aux commandes Arrêter, Redémarrer, Mettre en veille et Mettre en veille prolongée
 - vi. Supprimer l'icône de mise en réseau
 - vii. Supprimer l'icône Sécurité et maintenance
 - viii. Supprimer la liste « Récemment ajoutées » du menu Démarrer
 - ix. Supprimer les liens et l'accès à Windows Update
 - x. Supprimer les notifications et le centre de maintenance
 - xi. Verrouiller la barre des tâches

Start Menu and Taskbar	
Policy	Setting
Clear history of recently opened documents on exit	Enabled
Do not use the search-based method when resolving shell shortcuts	Enabled
Do not use the tracking-based method when resolving shell shortcuts	Enabled
Lock the Taskbar	Enabled
Remove and prevent access to the Shut Down, Restart, Sleep, and Hibernate commands	Enabled
Remove links and access to Windows Update	Enabled
Remove Notifications and Action Center	Enabled
Remove Recent Items menu from Start Menu	Enabled
Remove the networking icon	Enabled
Remove the Security and Maintenance icon	Enabled
Turn off notification area cleanup	Enabled

- d. Panneau de configuration / Imprimantes (... > **Control Panel / Printers**) :
- i. Interdire la suppression des imprimantes

Control Panel/Printers	
Policy	Setting
Prevent deletion of printers	Enabled

- e. Panneau de configuration / Personnalisation (... > **Control Panel / Personalization**) :
- i. Empêcher de modifier l'arrière-plan du bureau

Control Panel/Personalization	
Policy	Setting
Prevent changing desktop background	Enabled

- f. Système (... > **System**) :
- i. Désactiver l'accès à l'invite de commandes
 - ii. Empêcher l'accès aux outils de modifications du registre
 - iii. Empêcher l'exécution d'applications spécifiques : powershell.exe et powershell_ise.exe

System	
Policy	Setting
Don't run specified Windows applications	Enabled
List of disallowed applications	
powershell.exe	
powershell_ise.exe	
Policy	Setting
Prevent access to registry editing tools	Enabled
Disable regedit from running silently?	Yes
Policy	Setting
Prevent access to the command prompt	Enabled
Disable the command prompt script processing also?	No

- E. `outilsInstall` - Modifier la GPO, pour faire la mise à jour du programme `firefox` vers la version 52.4.1. Vérifiez que la mise à jour s'est propagée correctement sur la VM Windows 10.

Computer Conf > Policies > Software > Software > clicd roit sur le logiciel à upgrade > Properties > Upgrades > Add le nouveau fichier msi > Choisir Current GPO et désinstaller ancien package

- F. `clientAdmin` - GPO pour déléguer l'administration des machines dans l'OU clients aux membres du groupe AdminMachines (créé à l'exercice 3)

Dans AD Users and Computers > OU Clients > clic droit > Delegate Control > Sélectionner groupe AdminMachines > Sélectionner droits > OK

Créer GPO sur Clients > Computer Config > Policies > Windows Settings > Restricted Group > clic droit > Add group

4. Etablir un audit sur le partage `SharedSocial` créé précédemment (exercice 3.A) pour consigner les ajouts et suppressions de fichiers ou dossiers par un membre du groupe social. Au besoin, vous modifierez la GPO `auditObject` créée à l'exercice 3.A

Création nouvelle GPO sur OU Social > clic droit > Computer Conf > Policies > Windows > Security > Local > Audit directory service access > Success + Audit privilege use > Success

5. En respect du RGPD, on vous demande d'ajouter une GPO `Disclaimer` affichant le texte ci-dessous lors de l'ouverture de session :

Sur cg01dom.local créer la GPO :

- A. Titre du message : « *Politique de confidentialité – Rappel* »
- B. Message : « *En tant qu'utilisateur/trice disposant des accès aux serveurs de l'entreprise dans le cadre de votre fonction au sein de l'organisation, vous êtes tenu.e à observer la plus grande confidentialité à l'égard des informations que vous êtes amené.e à traiter au nom de l'organisation et ne pas en faire un usage à d'autres fins. En cliquant sur "OK" et en poursuivant la connexion, vous reconnaissiez avoir pris connaissance de cette information.* »

Computer Configuration (Enabled)	
Policies	
Windows Settings	
Security Settings	
Local Policies/Security Options	
Interactive Logon	
Policy	Setting
Interactive logon: Message text for users attempting to log on	En tant qu'utilisateur/trice disposant des accès aux serveurs de l'entreprise dans le cadre de votre fonction au sein de l'organisation, vous êtes tenu.e à observer la plus grande confidentialité à l'égard des informations que vous êtes amené.e à traiter au nom de l'organisation et ne pas en faire un usage à d'autres fins. En cliquant sur OK et en poursuivant la connexion, vous reconnaissiez avoir pris connaissance de cette information.
Interactive logon: Message title for users attempting to log on	"POLITIQUE DE CONFIDENTIALITE - RAPPEL"

1.8 Sauvegarde et restauration

- I. Planifier un cliché instantané d'Active Directory, tous les mardi et mercredi à 12h. Vérifier celui-ci avec les outils dsamain et Active Directory Users and Computers.

```
ntdsutil snapshot "activate instance ntds" create quit quit
```

Vérification :

Dsamain :

Entrer les commandes suivantes :

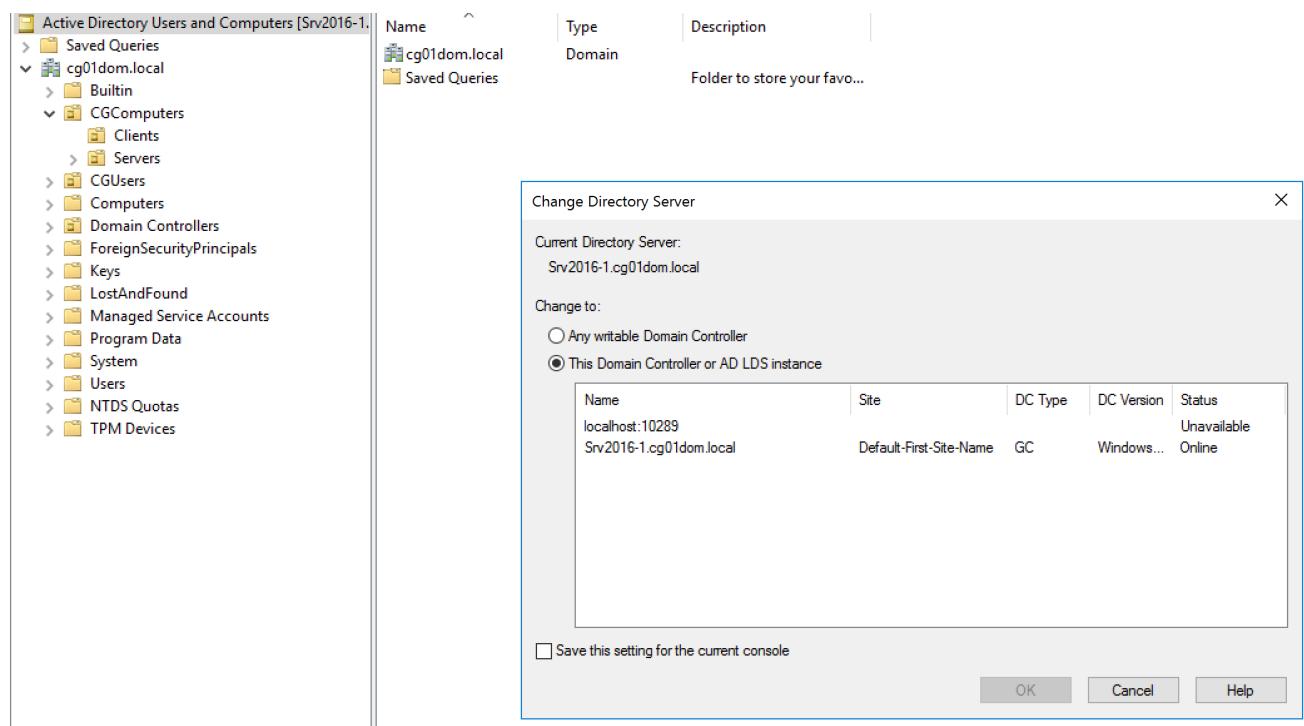
- Ntdsutil snapshot « list all »
- Mount X (X est le n° du snapshot à monter)
- Quit
- Quit
- dsamain -dbpath
"C:\\$SNAP_201710312103_VOLUMEC\$\Windows\NTDS\ntds.dit" -ldapport 10289

Une fois fini, il faut exécuter :

```
ntdsutil snapshot "unmount *" quit quit
```

AD Users and Computers :

AD Users and Computers > Clic droit sur le premier élément > Choisir This domain controller or AD LDS ... > entrer « localhost :10289 »



- II. Arrêter votre serveur *SRV2016-1*. Dans VMware, modifier les paramètres de la VM pour ajouter un nouveau disque dur de 5 Go. Démarrer votre serveur et formatez celui-ci. Il doit être accessible par la lettre « S : »

Tools > Computer Management > Disk Management

- III. Sauvegarder le contenu du dossier *CGData*, en utilisant *Windows Server Backup*. La sauvegarde doit être planifiée tous les mercredi à 11h, vers votre disque « S : »

Tools > Windows Server Backup (ajouter rôle si nécessaire) > Local backup > clic droit Backup schedule > Custom backup > Sélectionner dossier CGData > Once a day at 11 am > Backup to a volume > Sélectionner disque « S: »

- IV. Activer les clichés instantanés sur le volume « C : », le mercredi à 15h. Les clichés doivent être sauvegardés sur le disque « S : »

Tools > Computer Management > Disk Management > Clic droit sur C : > Properties > Shadow copies > Settings > Storage Area = S: > Max size = 5Gb > Schedule > weekly 15:00 Wednesday

Après il faut **Enable** le cliché.

Vérifiez toutes les sauvegardes et tester les clichés instantanés.

1.9 Service de bureau à distance

1. Installer le service Remote Desktop sur la machine *SRV2016-2* (cf. leçon 8, exercice 2).

Connecté avec un compte admin du domaine sur le 2^e serveur.

Ajouter rôle > Type d'installation > Remote Desktop Services installation > Standard Deployment > Session-based desktop deployment > Ajouter le serveur courant dans les ordinateurs sélectionnés > Install the RD Web Access role service on the RD connection Broker server > Next > Ajouter le serveur courant aux serveurs sélectionnés > Next > Restart the destination server automatically if required

Si problème, redémarrer manuellement. Si toujours problème, recommencer + redémarrer.

1. Autoriser les membres elearning et travaux à se connecter au serveur (via la collection de session)

Tasks > Create Session Collection (en haut à droite) > Choisir nom > Sélectionner le serveur > Sélectionner les groupes > Désactiver User profile disk > Create

Dans properties > Tasks > Edit properties > Vérifier que tout correspond bien

2. Tester la connexion depuis la machine VM Windows 10 (par exemple eg0050 + password P@ssw0rd)

Exécuter programme **mstsc.exe**. Cliquer sur **Show Options >**

- Général : Ajouter IP Serveur > Préciser utilisateur CG01DOM\eg0050 > Sauver vers un fichier
- Cliquer sur Connect

2. Modifier la stratégie boucleRappel (exercice 5d, leçon 8) :

1. Empêcher toute redirection du presse-papier et n'autoriser que la redirection de l'imprimante par défaut

User Configuration > Policies > Admin Templates > Windows Components > RD Services > RD Session Host > Device and resource Redirection > Do not allow clipboard redirection = enable

User Configuration > Policies > Admin Templates > Windows Components > RD Services > RD Session Host > Printer Redirection > Redirect only the default client printer = Enable

2. N'autoriser qu'une session par utilisateur

Computer Configuration > Policies > Admin Templates > Windows Components > RD Services > RD Session Host > Connections > Restrict RD Services to a single RD Services session = Enable

3. Définir les délais pour une session inoccupée à 5 minutes. Mentionner qu'une session déconnectée depuis 10 minutes doit être fermée.

Computer Configuration > Policies > Admin Templates > Windows Components > RD Services > RD Session Host > Session Time Limits

- Set time limit for active RD Services sessions = 5min
- Set time limit for disconnected sessions = 10min

4. Autoriser le groupe travaux à ouvrir une session via le service Desktop Services

Computer Configuration > Policies > Admin Templates > Windows Components > RD Services > RD Session Host > Connections > Allow users to connect remotely by using RD Services = Enable

5. Tester la connexion depuis la machine VM Windows 10 (pour tx0050 et eg0050 + P@ssw0rd).

3. Configurer une *RemoteApp*

1. Installer, au préalable, le programme WinSCP sur le serveur SRV2016-2 (cf. leçon 8, exercice 2)

Sur le Server 2 : **Control Panel > Programs > Install application on remote desktop > Sélectionner l'exécutable (WinSCP Setup) > Finish > Suivre installation**

2. Configurer une *RemoteApp* pour permettre l'exécution de ce programme

Server Manager > RD Services > Collections > Collection créée > RemoteApp Programs > TASKS > Publish RemoteApp Programs

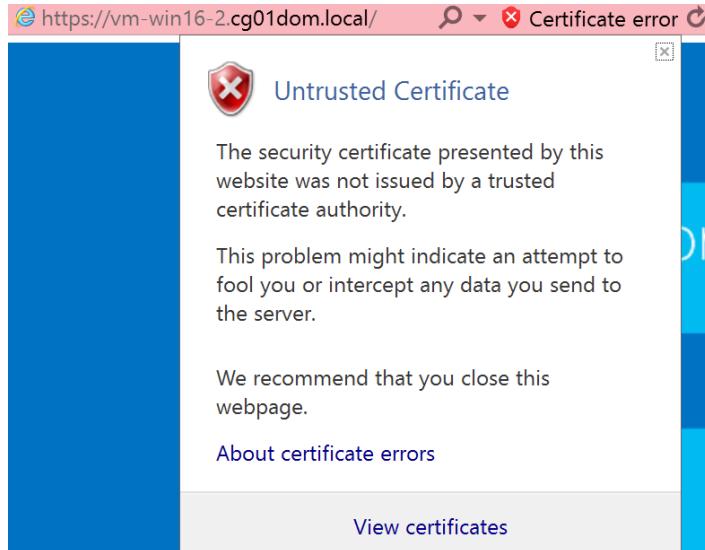
Sélectionner le programme dans la liste et l'ajouter.

Clic droit sur le programme > Edit properties > Spécifier les utilisateurs pouvant exécuter l'application à distance (vu que seuls travaux et e-learning ont accès à la collection, l'option All users est privilégiée) :

The screenshot shows the 'User Assignment' properties dialog. On the left, there is a sidebar with 'Show All' and three collapsed sections: 'General', 'Parameters', and 'User Assignment'. The 'User Assignment' section is currently selected and expanded, indicated by a blue border. To its right, the main pane displays the 'User Assignment' settings. It includes a descriptive text about limiting access to specific users and groups, two radio button options for specifying users ('All users and groups that have access to the collection' or 'Only specified users and groups'), and a 'Users and groups:' input field with 'Add...' and 'Remove' buttons.

Depuis le poste client :

En Admin, aller <https://vm-win16-2.cg01dom.local/> > Go to website > Cliquer sur View certificates



**Install certificate > Local Machine > Place all certificates In the following store:
Trusted Root Certification Authorities > Confirmer > Quitter navigateur et relancer l'opération pour vérifier que l'erreur a disparue.**

Avec un utilisateur autorisé (travaux/e-learning), Control Panel > All Control Panel Items > RemoteApp and Desktop Connections > Access RemoteApp and Desktops > entrer : <https://vm-win16-2.cg01dom.local/RDWeb/Feed/webfeed.aspx>

Si problème de certificat, refaire étape précédente.

Vérifier dans le **Start Menu** du client que le **Work Ressources** est là.

3. Tester la *RemoteApp* depuis votre machine VM Windows 10 avec un membre du groupe travaux (par exemple tx0050). Connectez-vous à *Dartagnan* et copier le contenu de votre dossier `public_html` depuis votre espace vers le disque C:. Quitter la RemoteApp. Trouver les fichiers transférés.

4. Obtenir le fichier `.rdp` permettant de démarrer la RemoteApp. Copier ce dernier sur le bureau de l'utilisateur

RemoteApp and Desktop > View ressources > clic droit sur l'appli > Properties.
Le *Target* indique le chemin vers le fichier `.rdp`

2. Partie 2 – Linux

2.1 Introduction

1. Au moyen de la ligne de commande :

1. Créer un utilisateur local correspondant à votre login HELMo et placer le dans le groupe principal *users*. Précisez également vos informations (nom, prenom, ...) et fixez le mot de passe.

```
[root@localhost ~]# useradd -m -g users -c "Fabrice Bodson" e190230
```

```
[root@localhost ~]# chsh -s /bin/bash e190230
```

```
[root@localhost ~]# passwd e190230
```

2. Créeer un groupe local *friends*

```
[root@localhost ~]# groupadd friends
```

3. Créeer un compte pour votre voisin dans le groupe principal *users* et dans le groupe secondaire *friends*.

```
[root@localhost ~]# useradd -m -g users -G friends -c "Dorian Cerfontaine" dorian
```

```
[root@localhost ~]# chsh -s /bin/bash dorian
```

```
[root@localhost ~]# passwd dorian
```

4. Modifier (usermod) votre compte pour qu'il appartienne également au groupe secondaire *friends*

```
[root@localhost ~]# usermod -G friends e190230
```

- Vérifier avec les commandes et en consultant les fichiers adéquats que tout est correct. Tentez de vous connecter !

```
e190230:x:1001:100:Fabrice BODSON:/home/e190230:/bin/bash
dori:x:1002:100:Dorian CERFONTAINE:/home/dori:/bin/bash
```

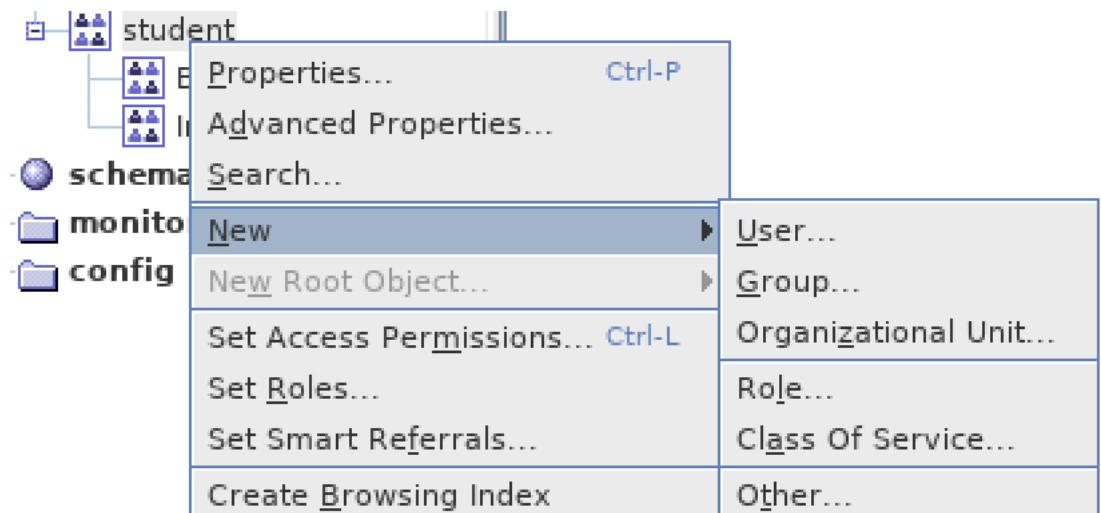
- Au moyen de la **console d'administration LDAP** :

[root@localhost ~]# 389-console

Mot de passe : rootroot

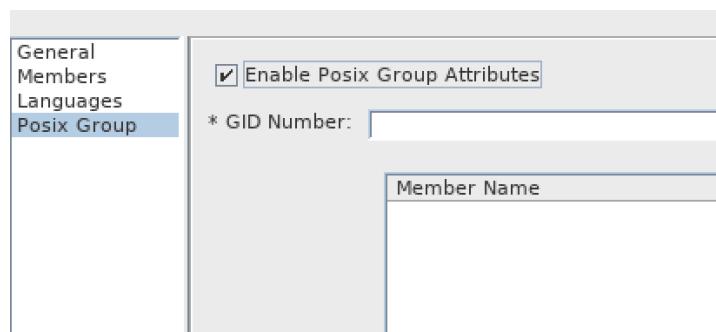
Allez dans *Server Group > Directory Server > localdomain*

- Créez une OU *student* avec, à l'intérieur, une autre unité *BM*



- Dans l'OU *Groups*, créer 4 groupes globaux : *biomed1*, *biomed2*, *biomed3* et *etudiants*

Dans général il faut donner le nom, ensuite dans Posix group il faut déterminer manuellement le GID. Les utilisateurs globaux devront être ajoutés ici manuellement.



3. Dans l'OU *BM*, créer 3 utilisateurs globaux : *bm1*, *bm2*, et *bm3* appartenant au groupe principal *étudiants* et au groupe *biomedX* correspondant.

User
Languages
NT User
Posix User
Account

* First Name: John
* Last Name: Doe
* Common Name(s): John Doe
User ID: bm1
Password:
Confirm Password:
E-Mail: _____
Phone: _____
Fax: _____

User
Languages
NT User
Posix User
Account

Enable Posix User Attributes
* UID Number: 5000
* GID Number: 5003
* Home Directory: /home/bm1
Login Shell: /bin/bash
Gecos: _____

* Indicates a required field

3. Au moyen de la ligne de commande, insérer dans LDAP :

Il faut créer un fichier *.ldif* et y insérer les données. Ensuite exécuter une commande pour créer :

1. Une OU *Info* à l'intérieur de la OU *student*

```
dn: ou=Info,ou=students,dc=localdomain
ou: Info
description: Groupe info
objectClass: top
objectClass: organizationalUnit
```

```
ldapadd -D 'cn=Directory Manager' -f ~/Documents/1_ldap_scripts/infoOU.ldif -x -W
```

2. Dans l'OU *Groups*, les 3 groupes globaux : *info1*, *info2* et *info3*

```
dn: cn=info1, ou=Groups, dc=localdomain
description: info1
objectClass: top
objectClass: groupOfUniqueNames
objectClass: posixGroup
gidNumber: 5004

dn: cn=info2, ou=Groups, dc=localdomain
description: info2
objectClass: top
objectClass: groupOfUniqueNames
objectClass: posixGroup
gidNumber: 5005

dn: cn=info3, ou=Groups, dc=localdomain
description: info3
objectClass: top
objectClass: groupOfUniqueNames
objectClass: posixGroup
gidNumber: 5006
```

```
ldapadd -D 'cn=Directory Manager' -f ~/Documents/1_ldap_scripts/info_global_groups.ldif -x -W
```

3. Dans l'OU *Info*, créer 3 utilisateurs globaux *inf1*, *inf2* et *inf3* appartenant au groupe principal *etudiants* et au groupe *infoX* correspondant. Pour ce faire, créer les fichiers LDIF et importez-les.

```
dn: uid=inf1, ou=Info, ou=student, dc=localdomain
ou: inf1
description: OU user 1 info
objectClass: top
objectClass: inetorgperson
objectClass: posixAccount
cn: Bob LEBOB
sn: LEBOB
givenname: Bob
userPassword: rootroot
gidNumber: 5003
uidNumber: 5003
homeDirectory: /home/inf1
loginShell: /bin/bash

dn: uid=inf2, ou=Info, ou=student, dc=localdomain dn: uid=inf3, ou=Info, ou=student, dc=localdomain
ou: inf2
description: OU user 2 info
objectClass: top
objectClass: inetorgperson
objectClass: posixAccount
cn: Fab
sn: BODSON
givenname: Fab
userPassword: rootroot
gidNumber: 5003
uidNumber: 5004
homeDirectory: /home/inf2
loginShell: /bin/bash
ou: inf3
description: OU user 3 info
objectClass: top
objectClass: inetorgperson
objectClass: posixAccount
cn: Dorian
sn: CERFONTAINE
givenname: Dorian
userPassword: rootroot
gidNumber: 5003
uidNumber: 5005
homeDirectory: /home/inf3
loginShell: /bin/bash
```

```
ldapadd -D 'cn=Directory Manager' -f ~/Documents/1_ldap_scripts/info_global_users.ldif -x -W
```

Pour les ajouter dans les groupes infoX :

```
dn: cn=info1,ou=Groups,dc=localdomain
changetype: modify
add: memberuid
memberuid: inf1

dn: cn=info2,ou=Groups,dc=localdomain
changetype: modify
add: memberuid
memberuid: inf2

dn: cn=info3,ou=Groups,dc=localdomain
changetype: modify
add: memberuid
memberuid: inf3
ldapadd -D 'cn=Directory Manager' -f ~/Documents/1_ldap_scripts/add_groupmember.ldif -x -w[REDACTED]
```

2.2 Scripting Linux

1. Créez un script *Python*, nommé [mklist.py](#), qui va **produire à l'écran** le fichier CSV auquel on aura ajouté 2 colonnes supplémentaires : les logins et mots de passe.
 1. **Les logins** pour les utilisateurs suivront la règle : en fonction de la section de l'étudiant, la 1^{ère} lettre sera a, b, i ou t. Nous aurons ensuite 4 chiffres représentant une séquence. Ainsi, a0001 représente le 1^{er} étudiant de la section automatique, i0054, le 54^{ème} étudiant de la section informatique...
 2. Pour générer le mot de passe de chaque utilisateur, utilisez la commande `mkpasswd`¹. Le mot de passe doit faire 12 caractères et comporter des lettres (majuscules et minuscules) et chiffres (reportez-vous à la documentation pour les paramètres à passer à `mkpasswd`).

Testez votre script et vérifiez si l'information à l'écran est correcte.

```
import csv
import os

def generate_password():
    password = os.popen('mkpasswd -l 12 -c 4 -C 4 -d 4 -s 0').read()
    return password

def main():
    file = "liste-etudiants.csv"
    with open(file, newline='') as list:
        student_list = csv.reader(list, delimiter=";")
        for count, line in enumerate(student_list):
            name = line[0]
            firstname = line[1]
            group = line[2]
            category = line[2][1].lower()

            student_id = f"{category}{count+1:04d}"
            password = generate_password()

            user = f"{name};{firstname};{group};{student_id};{password}".rstrip()
            print(user)

if __name__ == '__main__':
    main()
```

Ensuite seulement, lancez votre script comme suit :

```
$ mklist.py > liste-login-pass.csv
```

Vous obtiendrez ainsi **un nouveau fichier CSV** contenant en plus les logins et mots de passe.

2. Créer un script *Python* nommé [mkuser.py](#) qui va, en se basant sur le fichier CSV obtenu à l'étape précédente, créer les comptes locaux des différents étudiants. On vous demande également de fixer, par ce script, les mots de passe et les données (noms et prénoms) de ces utilisateurs.

On vous demande de placer les étudiants dans le groupe principal (et local) *users* et dans un groupe secondaire correspondant à leur classe (en minuscule).

```
import csv
import os

def create_local_group(group):
    return os.popen(f'groupadd {group}').read()

def create_local_user(name, firstname, group, student_id, password):
    return os.popen(f'useradd -m -g users -G {group} -p {password} -c "{firstname} {name}" {student_id}').read()

def main():
    file = "../liste-login-pass.csv"
    counter = 0
    with open(file, newline='') as list:
        student_list = csv.reader(list, delimiter=";")

        for line in student_list:
            name = line[0]
            firstname = line[1]
            group = line[2].lower()
            student_id = line[3]
            password = line[4]

            create_local_group(group)

            create_local_user(name, firstname, group, student_id, password)

            user = f"{name};{firstname};{group};{student_id};{password}".rstrip()
            print(user)

            if counter == 3:
                break
            else:
                counter += 1

if __name__ == '__main__':
    main()
```

3. Créer un script *Python* nommé `mkuser_ldap.py` permettant d'ajouter facilement un utilisateur dans le LDAP. Pour ce faire l'utilisateur sera ajouté dans le OU=People, il sera configuré comme utilisateur POSIX, aura comme groupe principal, le groupe *users* (*gid=100*) et comme shell *bash* (*/bin/bash*). Le nom, le prénom, l'UID, le login et le mot de passe seront donnés en argument de votre script.

```

import csv
import os
import sys

def create_global_user(name, firstname, uid_number, login, password, file_to_write):
    file_to_write.write(f"dn: uid={login},ou=People,dc=localdomain\n")
    file_to_write.write(f"objectClass: top\n")
    file_to_write.write(f"objectClass: inetorgperson\n")
    file_to_write.write(f"objectClass: posixAccount\n")
    file_to_write.write(f"cn: {firstname} {name}\n")
    file_to_write.write(f"sn: {name}\n")
    file_to_write.write(f"givenname: {firstname}\n")
    file_to_write.write(f"userPassword: {password}\n")
    file_to_write.write(f"gidNumber: 100\n")
    file_to_write.write(f"uidNumber: {uid_number}\n")
    file_to_write.write(f"homeDirectory: /home/{login}\n")
    file_to_write.write(f"loginShell: /bin/bash")

def main():
    file = "liste-login-pass.csv"
    counter = 0

    uid_is_set = False

    with open(file, newline='') as list:
        student_list = csv.reader(list, delimiter=";")

        for line in student_list:
            name = line[0]
            firstname = line[1]
            [REDACTED]
            student_id = line[3]
            password = line[4]

            if uid_is_set is False:
                uid_number = str(sys.argv[1])
                uid_is_set = True
            else:
                uid_number = str(int(uid_number) + 1)

            with open("create_global_user.ldif", "w") as global_students:
                create_global_user(name, firstname, uid_number, student_id, password)
                global_students

            os.popen("ldapadd -D 'cn=Directory Manager' -f /root/Documents/2_scripts
create_global_user.ldif -x -W").read()

            [REDACTED]
            [REDACTED]
            [REDACTED]

            if counter == 3:
                break
            else:
                counter += 1

if __name__ == '__main__':
    main()

```

2.3 Administration du disque dur

1. Installer les quotas sur la partition /home

Dans le fichier `/etc/fstab`, modifier la ligne en ajoutant :

```
/dev/mapper/centos-home /home ext4 defaults,grpquota,usrquota 1 2  
umount /home  
mount /home
```

Après cette commande, pour contrôler que les options **grpquota** et **usrquota** sont bien prises en compte il faut exécuter :

```
mount | grep /home
```

Ensuite il faut créer les fichiers qui contiendront les infos des quotas en exécutant la commande :

```
quotacheck -aucvg9
```

Enfin, il faut informer l'OS que les quotas doivent être vérifiés dans ces fichiers, donc :

```
quotaon /home
```

2. Préciser que :

- Pour le compte créé pour votre voisin la limite est de 250 Mo

```
setquota -u dori 250000 250000 0 0 /home
```

Pour vérifier :

```
edquota -u dori
```

Pour quitter → :q<enter>

- Pour les membres du groupe *etudiant* (voir leçons précédentes), la limite collective est de 500 Mo

```
setquota -g etudiants 500000 500000 0 0 /home
```

Pour vérifier :

```
edquota -g etudiants
```

- c. Pour l'utilisateur *bm1*, la limite est de 150 Mo

```
setquota -u bm1 150000 150000 0 0 /home
```

Pour vérifier :

```
equota -u bm1
```

3. Vérifier que les quotas fonctionnent en copiant un large fichier dans le répertoire d'un utilisateur.
4. Déterminer, à l'aide de la commande *du*, l'espace disque occupé par chaque utilisateur.

La commande est ***cd /home*** puis ***du -h*** :

```
84M      ./dori
```

```
7.5M     ./bm1
```

5. Modifier [le script de création des utilisateurs](#) pour inclure les quotas suivants :
 - a. Chaque étudiant de 1^{ère} année aura un quota de 150 Mo
 - b. Chaque étudiant de 2^{ème} année et 3^{ème} année aura un quota de 200 Mo

```

def main():
    file = "liste-login-pass.csv"
    counter = 0

    uid_is_set = False

    with open(file, newline='') as list:
        student_list = csv.reader(list, delimiter=";")

        for line in student_list:
            name = line[0]
            firstname = line[1]
            current_year = line[2][0]
            student_id = line[3]
            password = line[4]

            if uid_is_set is False:
                uid_number = str(sys.argv[1])
                uid_is_set = True
            else:
                uid_number = str(int(uid_number) + 1)

            with open("create_global_user.ldif", "w") as global_students:
                create_global_user(name, firstname, uid_number, student_id, password)
                global_students

            os.popen("ldapadd -D 'cn=Directory Manager' -f /root/Documents/2_scripts
create_global_user.ldif -x -W").read()

            if current_year == "1":
                os.popen(f"setquota -u {student_id} 150000 150000 0 0 /home").read()
            else:
                os.popen(f"setquota -u {student_id} 200000 200000 0 0 /home").read()

```

Vérifier, avec edquota, que ceux-ci sont effectivement bien configurés.

2.4 Sauvegardes et planification

1. Réaliser une sauvegarde du répertoire `/var` dans un fichier `/tmp/var-back.bz2`. Ce fichier sera compressé par `bzip2`.

```
tar cvjf /tmp/backup-var.tar.bz2 /var
```

2. Réalisez le même exercice que le précédent, en utilisant la commande `zip` : créer l'archive `/tmp/var-back.zip` contenant l'ensemble du dossier `/var`.

```
zip -r /tmp/var-backup.zip /var
```

3. Testez et décompressez l'une des archives précédentes dans votre dossier personnel

```
unzip /tmp/var-backup.zip
```

```
tar xvjf /tmp/backup-var.tar.bz2
```

4. Programmez une tâche ponctuelle, pour le cours prochain, au milieu de celui-ci, et lancer la commande `poweroff`.

```
[root@localhost ~]# at now + 7 day
at> /usr/sbin/poweroff
at> <EOT>
job 1 at Sun May 2 17:08:00 2021
[root@localhost ~]# █
```

5. Programmez une tâche répétitive s'exécutant tous les début de cours et exécutant la commande `ntpdate` (synchronisation d'horloge avec un serveur distant) vers le serveur `time.belnet.be`

```
nano crontab -e
```

```
ntpdate time.belnet.be
```

6. Programmez pour la fin du cours la synchronisation de vos répertoires personnels (`/home`) vers le serveur `dartagnan`. Créer dans votre dossier personnel sur `dartagnan` un dossier `back` qui deviendra le miroir du votre dossier `/home`. Est-ce que cela fonctionne ? Pourquoi ?

```
[root@localhost ~]# at 16:45
at> ~/mirror_home.sh
```

Ecrire dans `mirror_home.sh`:

```
rsync -Cavz /home e190230@dartagnan.cg.helmo.be:~/back -e ssh
```

2.5 Configuration réseau

2.5.1 Configuration réseau

- I. En utilisant Network Manager ou en modifiant les fichiers de configuration :

- a. Prendre note des infos réseaux reçues par DHCP

```
[root@localhost ~]# nmcli device status
DEVICE      TYPE      STATE      CONNECTION
ens33       ethernet  connected  ens33
lo          loopback unmanaged  --
[root@localhost ~]# nmcli -p connection show ens33
=====
                                         Connection profile details (ens33)
=====
connection.id:                         ens33
connection.uuid:                        402bac60-9d8c-4c2c-9ec3-e0de283e597b
connection.stable-id:                   --
connection.type:                       802-3-ethernet
connection.interface-name:              ens33
connection.autoconnect:                yes
connection.autoconnect-priority:      0
connection.autoconnect-retries:        -1 (default)
connection.auth-retries:               -1
connection.timestamp:                 1618302455
connection.read-only:                  no
connection.permissions:               --
connection.zone:                      --
connection.master:                     --
connection.slave-type:                --
connection.autoconnect-slaves:        -1 (default)
connection.secondaries:                --
connection.gateway-ping-timeout:      0
connection.metered:                   unknown
connection.lldp:                      default
connection.mdns:                      -1 (default)
-----
802-3-ethernet.port:                  --
802-3-ethernet.speed:                 0
802-3-ethernet.duplex:                --
802-3-ethernet.auto-negotiate:       no
802-3-ethernet.mac-address:           --
802-3-ethernet.cloned-mac-address:   --
802-3-ethernet.generate-mac-address-mask: --
802-3-ethernet.mac-address-blacklist: --
802-3-ethernet.mtu:                   auto
802-3-ethernet.s390-subchannels:     --
802-3-ethernet.s390-nettype:          --
802-3-ethernet.s390-options:         --
802-3-ethernet.wake-on-lan:           default
802-3-ethernet.wake-on-lan-password:  --
-----
ipv4.method:                          manual
```

- b. Configurer statiquement l'IP de la machine

```
[root@localhost ~]# nmcli connection modify ens33 ipv4.method manual ipv4.address 192.168.190.30/24
ipv4.gateway 192.168.190.2 ipv4.dns 8.8.8.8 ipv4.dns-search localdomain
```

- c. Reboot

```
systemctl restart network
```

- d. Vérifier connexion en surfant sur le web

II. Avec Webmin :

- Ajouter une interface réseau virtuelle
- Spécifier l'IP 10.0.1.X (X est n° de la machine)

The screenshot shows the 'Edit Bootup Interface' page in Webmin. The interface is for the 'ens33' interface. Under 'Boot Time Interface Parameters', 'Activate at boot?' is set to 'Yes'. Under 'IPv4 address', 'Static configuration' is selected with IP 192.168.190.30, Netmask 255.255.255.0, and Broadcast 192.168.190.255. Under 'IPv6 addresses', 'From IPv6 discovery' is selected. Under 'MTU', 'Default' is selected. At the bottom, there are buttons for Save, Save and Apply, Delete and Apply, and Delete.

- Vérifier via ligne de commande que l'interface existe

2.5.2 Démarrage système

III. S'assurer qu'à chaque démarrage l'horloge est synchro avec *ntp1.oma.be*

```
[root@localhost ~]# nano /etc/rc.d/rc.local
[root@localhost ~]# █
```

ntpdate ntp1.oma.be

IV. S'assurer que le service *mariadb* démarre bien au démarrage du système.

(installation était requise : *yum install mariadb-server*)

```
[root@localhost ~]# systemctl enable mariadb
Created symlink from /etc/systemd/system/multi-user.target.wants/mariadb.service to /usr/lib/systemd/
/system/mariadb.service.
```

2.6 Routage

- I. Ajouter interface réseau dans VMware avec IP 192.168.131.0/24.
- II. Connecter cette carte réseau à la CentOS7-Routeur
- III. Installer nouvelle CentOS7-Client connectée sur la nouvelle interface réseau.
- IV. Configurer le routeur.

- a. Créer le fichier suivant et y ajouter :

```
[root@localhost Desktop]# cat /etc/sysctl.d/10-ipforward.conf
# Enabling IP Forwarding
net.ipv4.ip_forward=1
[root@localhost Desktop]#
```

- b. Activer ce mode routeur directement :

```
$ echo 1 > /proc/sys/net/ipv4/ip_forward
```

- V. Pour avoir accès internet sur machine client, il faut sur la machine routeur :

- a. Ajouter règle NAT

```
[root@localhost ~]# iptables -t nat -A POSTROUTING -s 192.168.131.0/24 -j MASQUERADE
$ service iptables save
```

- b. Tester la connexion

2.7 Service SAMBA

- I. Monter le partage *public* du serveur DATA sur la machine Linux (VPN activé)

```
[root@localhost ~]# mount -t cifs //192.168.128.3/Public ~/Desktop/PublicShare/
-o username=e190230, domain=CG, vers=3.0
Password for e190230@//192.168.128.3/Public: *****
```

- II. Configurer le service samba (*/etc/samba/smb.conf*) pour :

- a. Créer un partage */home/documents* accessible en rw pour swila, bm1, bm2, bm3.

```
[documents]
comment = Shared directory for swila, bm1-2-3
path = /home/documents
writable = yes
browseable = yes
write list = @swila bm1 bm2 bm3
```

- b. Permettre aux utilisateurs d'accéder à leurs dossier personnel
chown swila.users /home/documents

- c. Partager le dossier */home/group.biomed* pour que seuls les membres du groupe biomed3 puissent y accéder et en lecture.

```
[group.biomed]
comment = Shared Directory for group.biomed3
path = /home/group.biomed
read only = yes
browseable = yes
read list = @biomed3
```

- d. Créer un dossier `/home/public` accessible en rw à tout le monde. Utiliser les droits de partage et les droits UNIX.

```
# Unix Rights
[public]
    comment = Public share
    path = /home/public
    writable = yes
    create mask = 0755
    directory mask = 0777

# Share autorizations
#[public]
#        comment = Public share
#        path = /home/public
#        writable = yes
#        write list = @users
```

- III. [Script Python](#) pour ajouter les utilisateurs du fichier csv dans la BD des utilisateurs de samba.

```
import csv
import os
import sys

def main():
    file = "../2_scripts/liste-login-pass.csv"
    counter = 0

    with open(file, newline='') as list:
        student_list = csv.reader(list, delimiter=";")

        for line in student_list:
            student_id = line[3]
            password = line[4]

            os.popen(f"smbpasswd -a {student_id}").read()

            if counter == 3:
                break
            else:
                counter += 1

if __name__ == '__main__':
    main()
```

- IV. Vérifier en accédant au serveur samba depuis la machine hôte via l'IP 192.168.190.30.

2.8 Configuration d'Apache

Modifier dans le fichier `/etc/httpd/conf/httpd.conf`:

La ligne `ServerName 192.168.131.2 :80`

- I. Placer une page web de ma création comme page web par défaut

```
[root@localhost conf.d]# pwd  
/etc/httpd/conf.d  
[root@localhost conf.d]# cat default-site.conf  
<VirtualHost 192.168.131.2:80>  
    DocumentRoot /var/www/html/default  
    <Directory "var/www/html/default">  
        Options FollowSymLinks  
        AllowOverride All  
        Require all granted  
    </Directory>  
</VirtualHost>
```

- II. Autoriser les utilisateurs à déployer leur sites web personnels. Les fichiers seront placés dans un dossier web dans leur répertoire personnel.

Dans le fichier `/etc/httpd/conf.d/userdir.conf`: commenter `UserDir disabled`, ajouter nom du dossier.

```
#  
# UserDir is disabled  
# of a username on the  
# permissions).  
#  
# UserDir disabled  
  
#  
# To enable requests to  
# directory, remove the  
# the following line instead.  
#  
UserDir web  
</IfModule>  
  
#  
# Control access to UserDir  
# for a site where these controls  
#  
<Directory "/home/*/*web">
```

Dans l'URL il faut spécifier `ip/~login/default/`

S'assurer que l'utilisateur apache possède le droit en exécution pour tout en web (ACL).

- III. Créer un dossier admin dans le site web par défaut. Ajouter une page web particulière dedans. Protéger le site web avec une authentification simple et ajouter l'utilisateur `letmesee` avec le mot de passe `yesICanREAD`. Utiliser wireshark pour capturer le mot de passe.

- a. Créer fichier `.htaccess` dans le dossier racine où se trouve le/les fichiers à protéger :

```
[root@localhost www]# cat ./html/default/admin/.htaccess
AuthType Basic
AuthName "Message affiché par le navigateur"
AuthBasicProvider file
AuthUserFile "/var/www/admin.passwd"
Require valid-user
```

- b. Créer le fichier *admin.passwd* en ajoutant un utilisateur (-c avant fichier s'il n'existe pas encore):

```
[root@localhost www]# htpasswd -b -B /var/www/admin.passwd letmesee yes1CanREAD
Adding password for user letmesee
```

- IV. Créer un [script Python](#) qui permet d'ajouter les utilisateurs dans le fichier htpasswd protégeant le site web admin.

```
import csv
import os

def main():
    file = "liste-login-pass.csv"
    counter = 0

    with open(file, newline='') as list:
        student_list = csv.reader(list, delimiter=";")

        for line in student_list:
            student_id = line[3]
            password = line[4]

            print(os.popen(f"htpasswd -b -B /var/www/admin.passwd {student_id} {password}").read())

            if counter == 3:
                break
            else:
                counter += 1

if __name__ == '__main__':
    main()
```

- V. Configurer un site SSL *intranet.swilabus.be* en récupérant le certificat. Vérifier que la connexion est sécurisée en se connectant depuis la machine CentOS7-Client.
Ajouter certificats dans */etc/pki/tls/certs*
Ajouter clés dans */etc/pki/tls/private*

Dans le fichiers */etc/httpd/conf.d/ssl.conf*:

```
Listen 443 https
<VirtualHost 192.168.131.2:443>

# General setup for the virtual host
DocumentRoot /var/www/html/default
ServerName intranet.swilabus.be

<Directory "/var/www/html/default">
    AllowOverride All
    Options FollowSymLinks
    Require all granted
</Directory>
SSLEngine on
```

```
SSLProtocol all -SSLv2 -SSLv3

# SSL Cipher Suite:
# List the ciphers that the client is permitted to negotiate.
# See the mod_ssl documentation for a complete list.
SSLCipherSuite "EECDH+ECDSA+AESGCM ECDH+aRSA+AESGCM ECDH+ECDSA+SHA384 ECDH+ECDSA+SHA256 ECDH+aRSA+SHA384 ECDH
+aRSA+SHA256 ECDH+AESGCM ECDH EDH+AESGCM EDH+aRSA HIGH !MEDIUM !LOW !aNULL !eNULL !LOW !RC4 !MD5 !EXP !PSK !SRP
!DSS"
|SSLHonorCipherOrder on
SSLCertificateFile /etc/pki/tls/certs/intranet.swilabus.be.crt
SSLCertificateKeyFile /etc/pki/tls/private/intranet.swilabus.be.key
SSLCertificateChainFile /etc/pki/tls/certs/CA_Intermediate.crt
```

2.9 Service DNS

I. Configurer un serveur DNS pour la zone bodson.cg.helmo.be

Yum install bind-chroot

```
Cd /var/named/chroot/etc  
Cp /usr/share/doc/bind-9.9.4/sample/etc/*.
```

- a. Dans le dossier */var/named/chroot/etc* il faut modifier le fichier *named.conf*:

```
listen-on port 53      { any; };  
//listen-on port 53    { 127.0.0.1; };  
  
listen-on-v6 port 53   { any; };  
//listen-on-v6 port 53  { ::1; };  
allow-query            { any; };  
allow-query-cache      { any; };  
  
version "1234";  
recursion yes;  
Mettre ces lignes en commentaires :  
dnssec-enable yes;  
  
/* Enable DNSSEC validation */  
dnssec-validation yes;  
  
dnssec-lookaside auto;  
/*  
key ddns_key  
{  
    algorithm hmac-md5;  
    secret "use /usr/sbin/dnssec-keygen to generate TSIG keys";  
};  
*/
```

- b. À ajouter dans les vues interne et externe

```
zone "bodson.cg.helmo.be" in {  
    type master;  
    file "bodson.cg.helmo.internal.db";  
    allow-update { none; };  
    allow-transfer { none; };  
};
```

- c. Avant d'entrer les enregistrements suivants, il faut importer le modèle de fichier de zone :

```
$ cd /var/named/chroot/var/named/  
$ cp -a /usr/share/doc/bind-9.9.4/sample/var/named/* .  
$ chown -R named.named *
```

```
$ rm my.* slaves/my.*
```

- d. Vue interne :

- i. Créer le fichier *bodson.cg.helmo.internal.db* dans */var/named/chroot/var/named/*
- ii. Entrée NS : Ns.bodson.cg.helmo.be

- iii. Ns.bodson.cg.helmo.be → 192.168.190.30
- iv. Gate.bodson.cg.helmo.be → ip pfSense
- v. PfSense.bodson.cg.helmo.be → CNAME vers gate

Tabulations!

```
$TTL 86400
@ IN SOA ns.bodson.cg.helmo.be. admin.bodson.cg.helmo.be. (
    20210415 ; Serial
    28800   ; Refresh
    14400   ; Retry
    3600000 ; Expire
    3600 )  ; Name Error

; CRITICAL INFORMATION

; ** Name Server
IN      NS      ns.bodson.cg.helmo.be.

; COMPUTER
bodson.cg.helmo.be.     IN      A      192.168.190.30
ns                  IN      A      192.168.190.30
gate                 IN      A      190.168.190.2
pfSense              IN      CNAME  gate.bodson.cg.helmo.be.
```

e. Vue externe :

- i. Créer le fichier *bodson.cg.helmo.external.db* dans ce répertoire
- ii. Entrée NS : gate.bodson.cg.helmo.be
- iii. Ns.bodson.cg.helmo.be → CNAME gate
- iv. gate.bodson.cg.helmo.be → ip WAN pfSense
- v. pfSense.bodson.cg.helmo.be → CNAME vers gate

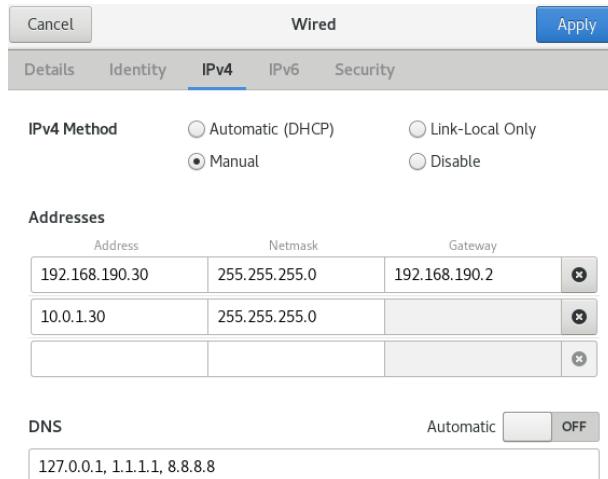
```
$TTL 86400
@ IN SOA gate.bodson.cg.helmo.be.      admin.bodson.cg.helmo.be. (
    20210415 ; Serial
    28800   ; Refresh
    14400   ; Retry
    3600000 ; Expire
    3600 )  ; Name Error

; CRITICAL INFORMATION

; ** Name Server
IN      NS      gate.bodson.cg.helmo.be.

; COMPUTER
ns      IN      CNAME  gate.bodson.cg.helmo.be.
gate    IN      A      192.168.254.10
pfSense IN      CNAME  gate.bodson.cg.helmo.be.
```

f. Configurer le serveur pour qu'il interroge le service DNS qui vient d'être configuré. Activer ce service DNS au démarrage de la machine.



- g. Ouvrir port 53 dans pfSense et le rediriger vers le serveur Linux.
 - h. Tester depuis Windows (nslookup).
- II. Configurer mon serveur DNS pour qu'il soit le serveur secondaire de mon voisin.
Utiliser l'IP WAN.
- III. Ajouter zone DNS inverse pour les ip 192.168.190.X : la machine Windows, le firewall pfSense et le serveur Linux.
- a. Dans `/var/named/chroot/etc/named.conf` :

```
zone "190.168.192.in-addr.arpa" in {
    type master;
    file "reverse.dns.internal.db";
    allow-update { none; };
    allow-transfer { none; };
};
```

 - b. Ajouter dans le fichier `/var/named/chroot/var/named/reverse.dns.internal.db` :

```
$TTL 86400
@ IN SOA ns.bodson.cg.helmo.be. admin.bodson.cg.helmo.be. (
    20210416 ; Serial
    28800 ; Refresh
    14400 ; Retry
    3600000 ; Expire
    3600 ) ; Name Error

; CRITICAL INFORMATION

; ** Name Server
IN NS ns.bodson.cg.helmo.be

; PTR
2 IN PTR gate.bodson.cg.helmo.be
30 IN PTR ns.bodson.cg.helmo.be
```

2.10 Administration à distance

- I. Changer le mot de passe du compte root par mon mot de passe HELMo
- II. Ouvrir le port 22 sur le firewall pfSense

<input checked="" type="checkbox"/>		WAN	TCP	*	*	WAN address	22 (SSH)	192.168.190.30	22 (SSH)	Redirection SSH vers routeur
-------------------------------------	--	-----	-----	---	---	-------------	----------	----------------	----------	------------------------------

- III. Planifier une sauvegarde automatique, en utilisant rsync, de mon dossier /home vers la machine du voisin, en utilisant le compte qu'il m'avait créé.

Crontab -e puis ajouter la commande suivante :

```
rsync -Cavz /home root@192.168.131.15:~/Desktop -e ssh  
(Remplacer root par le nom d'utilisateur et l'IP par l'IP du voisin.)
```

- IV. Configurer un tunnel SSH pour accéder au serveur web du voisin. Pour ce faire, rediriger le port 8080 vers sa machine sur le port 80. Accéder à son site web <http://127.0.0.1:8080>

Remplacer root par le nom d'utilisateur et l'IP par l'IP du voisin

```
[root@localhost ~]# ssh -L 8080:192.168.131.15:80 root@192.168.131.15
```

- V. Sur base des infos sur [ce site](#), ajouter le dépôt Adobe et installer flash player sur ma machine.
- VI. Sur base des infos sur [ce site](#), installer le serveur X2Go sur la CentOS7 Routeur et installer le client sur la CentOS7 Client. Tenter une connexion.
 - a. Remplacer KDE ou GNOME par XFCE

2.11 Service FTP

I. Créer utilisateur backup et son mot de passe

II. Configurer le serveur FTP afin de :

N.B. : *listen=YES, listen_ipv6=NO, pasv_address=<ipWANpfSense>*

/etc/vsftpd/vsftpd.conf

a. Ne pas autoriser l'accès anonyme
anonymous_enable=NO

b. Permettre aux utilisateurs swila et backup de se connecter au serveur FTP.

i. Préciser dans le fichier *user_list* swila et backup puis dans *vsftpd.conf* :

```
### Seuls les utilisateurs listés dans le fichier
### peuvent se connecter
userlist_enable=YES
userlist_deny=NO
userlist_file=/etc/vsftpd/user_list
```

c. Permettre à mon voisin de se connecter au serveur FTP

Ajouter le voisin dans *user_list*

d. Emprisonnez tous les utilisateurs dans leur dossier personnel sauf backup

i. Créer fichier *chroot_list* et y écrire backup puis dans *vsftpd.conf* :

```
### Tous les utilisateurs sont emprisonnés
###sauf ceux mentionnés dans la liste
chroot_local_user=YES
chroot_list_enable=YES
# (default follows)
chroot_list_file=/etc/vsftpd/chroot_list
allow_writeable_chroot=YES
```

e. Activez le mode passif avec les ports compris entre 45000 et 45500

i. Ouvrir les ports dans pfSense (Firewall > NAT) :

Interface : WAN ; Protocol : TCP ; Destination : WAN address ; Destination port range from : (other) 15000 to (other) 15500 ; Redirect target IP : <ip de votre serveur Linux> ; Redirect target port : 15000 ; Cliquer sur SAVE

Interface : WAN ; Protocol : TCP ; Destination : WAN address ; Destination port range from : FTP to FTP ; Redirect target IP : <ip de votre serveur Linux> ; Redirect target port : FTP ; Cliquer sur SAVE

ii. Écrire ce qui suit dans *vsftpd.conf* :

```
pasv_min_port=45000
pasv_max_port=45500
pasv_promiscuous=YES
pasv_address=192.168.1.54 # WAN pfSense
```

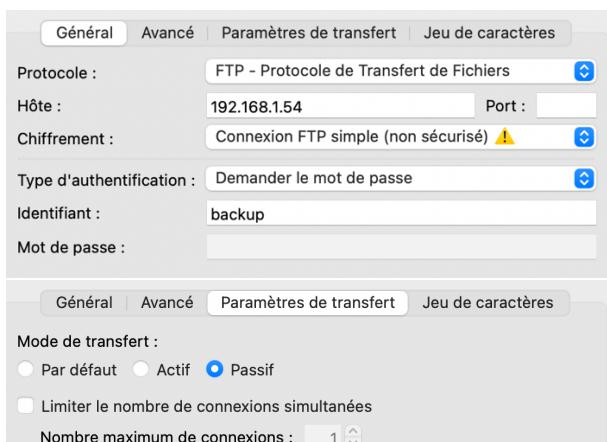
- f. Vérifier en se connectant au serveur en local
 i. Lancer le service

```
$ systemctl start vsftpd
```

- ii. Se connecter

```
[root@localhost vsftpd]# ftp
ftp> open localhost
Trying ::1...
ftp: connect to address ::1Connection refused
Trying 127.0.0.1...
Connected to localhost (127.0.0.1).
220 This is Fab's FTP server.
Name (localhost:root): backup
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> 
```

- III. Configurer pfSense pour ouvrir les ports nécessaires au fonctionnement FTP. Vérifier la configuration en se connectant depuis l'hôte.



- IV. Créer [script Python](#) :

- Qui compresse en zip le contenu de /etc
- Qui transfert le fichier zip vers la machine du voisin en utilisant le compte qu'il m'a créé.

```
import os
import sys
import zipfile

def main():

    directory = str(sys.argv[1])
    dir_to_zip = (directory + "-backup.zip").split("/")[-1]
    zip_file = zipfile.ZipFile(dir_to_zip, 'w', zipfile.ZIP_DEFLATED)

    for root, directories, files in os.walk(directory):
        for file in files:
            zip_file.write(os.path.join(root, file))
    zip_file.close()

    print(os.popen(f'lftp backup@192.168.1.2 -e "put /root/Documents/11_FTP/{dir_to_zip}; exit;"').read())

if __name__ == '__main__':
    main()
```

2.12 Mail

- I. Configurer le serveur mail (sans SSL, ni authentification, ni antispam) pour le domaine configuré.

a. */etc/mail/access*

Connect:localhost.localdomain	RELAY
Connect:localhost	RELAY
Connect:127.0.0.1	RELAY
Connect:192.168.190	RELAY

b. */etc/mail/local-host-names*

bodson.cg.helmo.be

c. */etc/mail/virtusertables*

admin@bodson.cg.helmo.be	root
e190230@bodson.cg.helmo.be	e190230
bm1@bodson.cg.helmo.be	bm1

d. */etc/mail/sendmail.mc*

```
define(`confSMTP_LOGIN_MSG', `$j Sendmail; $b')dnl
define(`SMART_HOST', `smtp.your.provider')dnl
DAEMON_OPTIONS(`Port=smtp, Name=MTA')dnl
```

- II. Installer un serveur POP3/IMAP sur ma machine et le configurer.

a. Installer Dovecot

Yum install dovecot

b. Modifier le fichier */etc/dovecot/dovecot.conf*

```
#####
# Protocols we want to be serving. #
protocols = imap pop3 lmtp
#####

#####
# A comma separated list of IPs or hosts where to listen in for connections.#
# "*" listens in all IPv4 interfaces, ":" listens in all IPv6 interfaces. #
# If you want to specify non-default ports or anything more complex,      #
# edit conf.d/master.conf.                                              #
listen = *, :#
#####

# Base directory where to store runtime data.
#base_dir = /var/run/dovecot/

# Name of this instance. In multi-instance setup dovecadm and other commands
# can use -i <instance_name> to select which instance is used (an alternative
# to -c <config_path>). The instance name is also added to Dovecot processes
# in ps output.
#instance_name = dovecot

#####
# Greeting message for clients.   #
login_greeting = Welcome to Dovecot. #
#####
```

c. Modifier le fichier `/etc/dovecot/conf.d/10-mail.conf`

```
mail_location = mbox:~/mail:INBOX=/var/spool/mail/%u
```

```
mail_access_groups = mail
```

d. Modifier le fichier `/etc/dovecot/conf.d/10-ssl.conf`

```
ssl =no
```

III. Configurer Thunderbird sur le poste Windows pour interroger le serveur mail.

Configurez votre adresse électronique existante
Utilisez votre adresse électronique actuelle

Votre nom complet : Administrateur

Adresse électronique : root@bodson.cg.helmo.be

Mot de passe : Mot de passe

Retenir le mot de passe

✓ Les paramètres suivants ont été trouvés en sondant le serveur indiqué

	ENTRANT	SORTANT
Protocole :	POP3	SMTP
Serveur :	192.168.190.30	.bodson.cg.helmo.be
Port :	110	Automatique
SSL :	Aucune	Autodétection
Authentification:	Mot de passe normal	Autodétection
Identifiant :	root	root

Paramètres du serveur

Type de serveur : Serveur de courrier POP

Nom du serveur : 192.168.190.30 Port : 110 Défaut : 110

Nom d'utilisateur : e190230

Paramètres de sécurité

Sécurité de la connexion : Aucune

Méthode d'authentification : Mot de passe, transmission non sécurisée

Paramètres

Description :

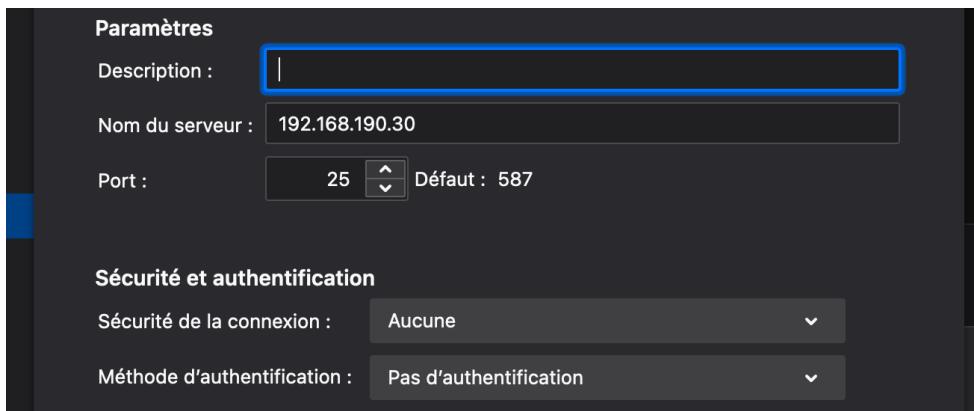
Nom du serveur : 192.168.190.30

Port : 25 Défaut : 587

Sécurité et authentification

Sécurité de la connexion : Aucune

Méthode d'authentification : Pas d'authentification



- IV. Capturer le trafic pour trouver le mot de passe échangé.
- V. Tester la configuration en envoyant des mails à des comptes locaux.
 - a. Installer RoundCube Webmail pour consulter les mails envoyés/reçus.

2.13 Firewall

- I. Configurer un firewall sur la machine routeur :
 - a. Permettre aux machines du réseau interne (192.168.131.0/24) d'accéder à internet via le NAT
 - b. Ouvrir les ports suivants (point d'inspection *untrust2fw*) :
 - i. Autoriser port SSH (tcp/22) depuis l'extérieur
 - ii. Autoriser le port DNS (udp/53 et tcp/53) depuis l'extérieur
 - iii. Autoriser les requêtes ICMP qui viennent des adresses 192.168.190.X
 - c. Limiter le trafic sortant qui provient du réseau interne (point d'inspection *trust2untrust*) au port WEB (tcp/80 et tcp/443) et DNS (udp/53)
 - d. Ouvrir le port 4022 (TCP) et le rediriger vers la machine cliente. Configurer le port SSH de la machine cliente sur 4022. La machine cliente doit être accessible en SSH via ce port.

Création d'un fichier *script fw.sh* :

```
#!/bin/bash
UNTRUST_NET=192.168.190.0/24
UNTRUST_IP=192.168.190.30
UNTRUST_IF=ens33

TRUST_NET=192.168.131.0/24
TRUST_IF=ens36
CLIENT_IP=192.168.131.16

TCP_PORTS=22,53
UDP_PORTS=53

TRUST_TCP_PORTS=80,443

# Effacer toutes les règles afin de ne créer que celles qu'on veut
iptables -t nat -F
iptables -t nat -X
iptables -F
iptables -X

# Création des points d'inspections qui m'intéressent
iptables -N trust2untrust
iptables -N trust2fw
iptables -N untrust2fw
iptables -N untrust2trust
iptables -N fw2trust
iptables -N fw2untrust

### Exercice A ###

# J'accepte le trafic trust2untrust
iptables -A trust2untrust -j ACCEPT

# Autorise la translation d'adresse pour le trafic sortant du réseau interne
iptables -t nat -A POSTROUTING -s $TRUST_NET -j MASQUERADE
```

```

#####
#
#
#
### Exercice B ###

# Autorise le trafic utilisant le protocole TCP dont le port destination est le 22 (SSH) ou le 53 (DNS)
iptables -A untrust2fw -p tcp --destination-port 4022 -j ACCEPT
iptables -A untrust2fw -p tcp --destination-port 53 -j ACCEPT

# Autorise le trafic utilisant le protocole UDP dont le port destination est le 53 (DNS)
iptables -A untrust2fw -p udp --destination-port 53 -j ACCEPT

# Autorise le trafic utilisant le protocole ICMP dont la source vient du réseau untrust (192.168.190.0/24)
iptables -A untrust2fw -p icmp -s $UNTRUST_NET -j ACCEPT

# Autorise le trafic qui serait une réponse à une requête précédemment envoyée
iptables -A untrust2fw -m state --state ESTABLISHED,RELATED -j ACCEPT

# Si le trafic ne remplit pas la condition d'avant, il est journalisé puis droppé
iptables -A untrust2fw -j LOG
iptables -A untrust2fw -j DROP

#####
#
#
#
### Exercice C ###

# Autorise le trafic utilisant les protocoles TCP/UDP sur les ports 53,80 et 443 à sortir
iptables -A trust2untrust -p tcp -m multiport --dports $TRUST_TCP_PORTS -j ACCEPT
iptables -A trust2untrust -p udp -m multiport --dports $TRUST_UDP_PORTS -j ACCEPT

# Autorise le trafic qui serait une réponse à une requête précédemment envoyée
iptables -A trust2untrust -m state --state ESTABLISHED,RELATED -j ACCEPT

# Si le trafic ne remplit pas la condition d'avant, il est journalisé puis droppé
iptables -A trust2untrust -j LOG
iptables -A trust2untrust -j DROP

#####
#
#
#
### Exercice D ###

# Autorise trafic TCP sur le port 4022 (SSH) et le redirige vers la machine client
iptables -t nat -A PREROUTING -i $UNTRUST_IF -d $UNTRUST_IP -p tcp --destination-port 4022 -j DNAT --to-destination $CLIENT_IP:22
iptables -A untrust2trust -m state --state RELATED,ESTABLISHED -j ACCEPT
iptables -A untrust2trust -p tcp --destination-port 22 -j ACCEPT
iptables -A untrust2trust -j LOG
iptables -A untrust2trust -j DROP

#####
#
#
#
iptables -A trust2fw -j ACCEPT
iptables -A fw2trust -j ACCEPT
iptables -A fw2untrust -j ACCEPT

#
#
#
iptables -A INPUT -i lo -j ACCEPT

iptables -A INPUT -i $UNTRUST_IF -j untrust2fw
iptables -A INPUT -i $TRUST_IF -j trust2fw
iptables -A INPUT -j LOG
iptables -A INPUT -j DROP

iptables -A FORWARD -i $UNTRUST_IF -o $TRUST_IF -j untrust2trust
iptables -A FORWARD -i $TRUST_IF -o $UNTRUST_IF -j trust2untrust
iptables -A FORWARD -j LOG
iptables -A FORWARD -j DROP

iptables -A OUTPUT -o lo -j ACCEPT
iptables -A OUTPUT -o $UNTRUST_IF -j fw2untrust
iptables -A OUTPUT -o $TRUST_IF -j fw2trust
iptables -A OUTPUT -j LOG
iptables -A OUTPUT -j DROP

#
#
#
service iptables save

```

- II. Configurer sur votre **machine client** un service FTP comme suit :
- Le port d'écoute doit être le port TCP 4000 (à la place du port 21)
 - Le mode passif doit être configuré sur les ports 63000 à 63500

```
listen_port=4000

pasv_min_port=63000
pasv_max_port=63500
pasv_promiscuous=YES
pasv_address=192.168.131.2
```

- III. Configurer un **firewall** sur votre **machine client** de sorte à :
- Permettre l'accès au port SSH 4022
 - Permettre l'accès au service FTP configuré au point 2 et aux ports configurés pour le mode passif.

```
#!/bin/bash

INTERNAL_NETWORK=192.168.131.0/24
DEVICE_IF=ens33
MY_IP=192.168.131.15

FTP_PORTS=63000:63500

# Effacer toutes les règles afin de ne créer que celles qu'on veut
iptables -t nat -F
iptables -t nat -X
iptables -F
iptables -X

## INPUT
iptables -A INPUT -i lo -j ACCEPT

iptables -A INPUT -i $DEVICE_IF -p tcp --destination-port 4022 -j ACCEPT
iptables -A INPUT -i $DEVICE_IF -p tcp -m multiport --dports $FTP_PORTS -j ACCEPT

iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
iptables -A INPUT -j LOG
iptables -A INPUT -j DROP

## FORWARD
iptables -P FORWARD DROP

## OUTPUT
iptables -P OUTPUT ACCEPT

service iptables save
```

Tester la configuration depuis la machine routeur (pour le FTP) et depuis l'hôte pour le SSH.

2.14 DHCP

- I. Configurer un service DHCP. La plage d'adresses IP : 192.168.131.150-200. IP du routeur sensé être fixe (192.168.131.2). Préciser les options nécessaires pour compléter la configuration DHCP et adapter le firewall si besoin.

- a. Importer un exemple de configuration :

Dans le dossier /etc/dhcp :

```
[root@localhost dhcp]# pwd  
/etc/dhcp
```

```
[root@localhost dhcp]# cp /usr/share/doc/dhcp-4.2.5/dhcpd.conf.example ./dhcpd.conf
```

- b. Dans le fichier /etc/dhcp/dhcpd.conf, il faut écrire seulement ça :

```
# Use this to enable / disable dynamic dns updates globally.  
ddns-update-style none;  
  
# If this DHCP server is the official DHCP server for the local  
# network, the authoritative directive should be uncommented.  
authoritative;  
  
# Use this to send dhcp log messages to a different log file (you also  
# have to hack syslog.conf to complete the redirection).  
log-facility local7;  
shared-network ROUTEUR_CLIENT {  
  
    # option definitions common to all supported networks...  
    option domain-name "bodson.cg.helmo.be";  
    option domain-name-servers ns.bodson.cg.helmo.be;  
  
    # IP est donnée pour 4h  
    default-lease-time 14400;  
  
    # Bail dure maximum 8h  
    max-lease-time 28800;  
  
    # Précise que le service est actif sur la 2e interface réseau  
    subnet 192.168.131.0 netmask 255.255.255.0 {  
  
        # Défini le range  
        range 192.168.131.150 192.168.131.200;  
  
        # Défini l'IP routeur  
        option routers 192.168.131.2;  
    }  
}  
[root@localhost dhcp]# systemctl enable --now dhcpcd
```

- II. Configurer le client en mode DHCP pour recevoir la configuration du serveur DHCP.

```
[root@localhost ~]# nmcli connection modify ens33 ipv4.method auto  
[root@localhost ~]# systemctl restart network  
nmcli device disconnect ens33  
nmcli device connect ens33
```

- III. Ajouter une réservation pour le client afin qu'il reçoive bien toujours l'IP 192.168.131.15.

Il faut ajouter dans le fichier */etc/dhcp/dhcpd.conf*:

```
##### Réservation #####
```

```
host client {  
    hardware ethernet 00:0c:29:7d:af:2a;  
    fixed-address 192.168.131.16;  
}
```