ATELIER ETP CHASSNEUILL

Sommaire

ATELIER ETP CHASSNEUILL

1)Installation de vyos

a)Creation des cartes reseaux

Nous allons tout d'abord machine vyos-router et ajouter les cartes reseaux sur virtual box cloisonner les reseaux et permettre les mises à jours de la vm SRV-AD avec le nettwork translation address (NAT)

1. Carte 1 eth0 sera en nat pour pouvoir mettre a jour le serveur windows
2. Carte 2 eth1 sera en réseau interne et sera dans le lan_serveurs
3. Carte 3 eth2 sera egalement en réseau interne et sera dans le lan_clients
4. Carte 4 eth3 sera enfin en réseau interne et sera dans le lan_dmz

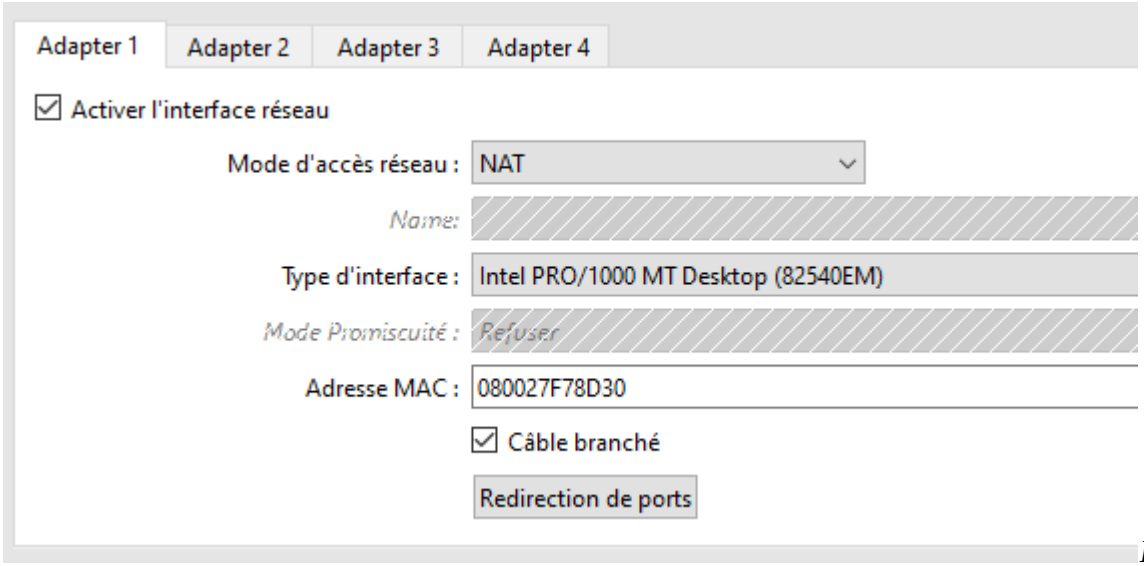


Figure 1: interface nat

ATELIER ETP CHASSNEUILL

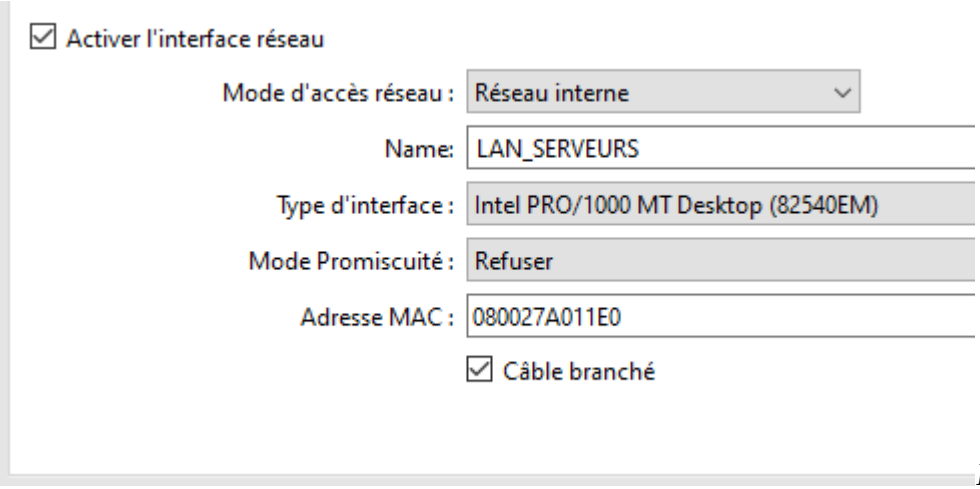


Figure 2: LAN_SERVEURS

ATELIER ETP CHASSNEUILL

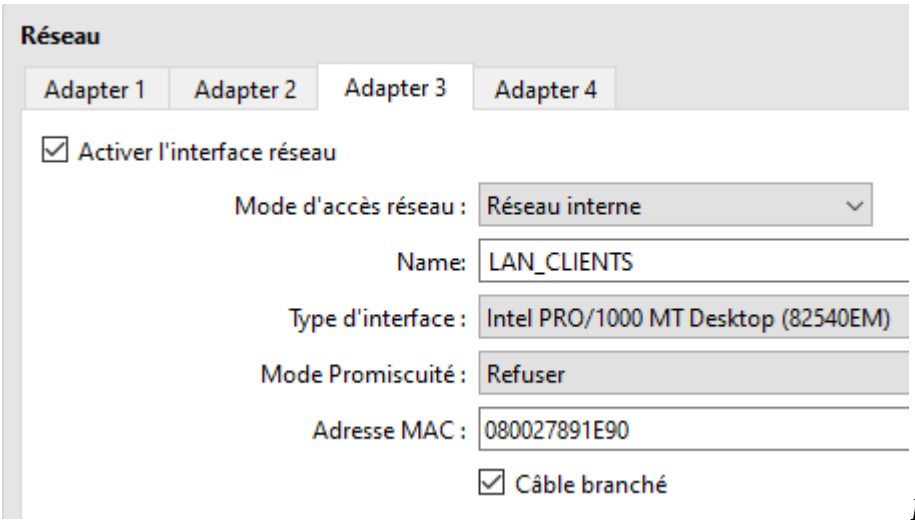


Figure 3: LAN_CLIENTS

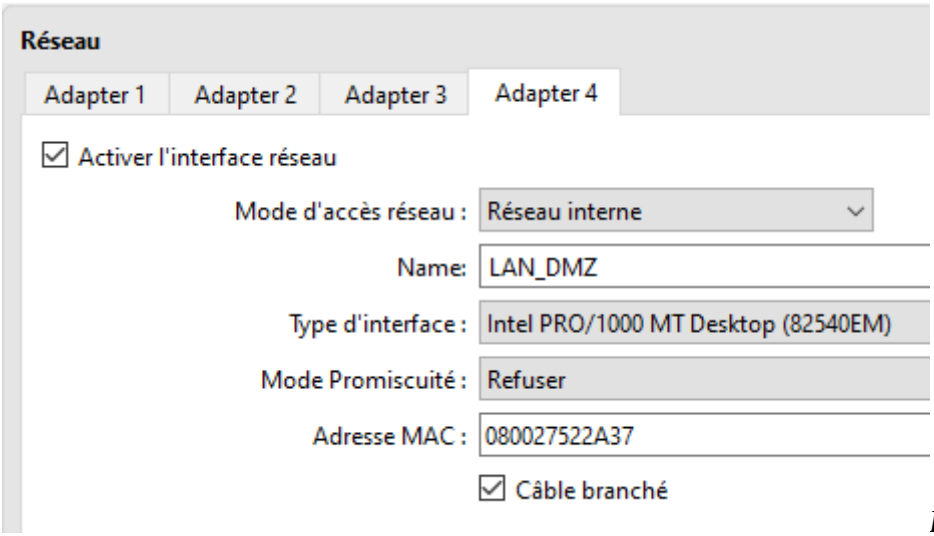


Figure 4: LAN_DMZ

ATELIER ETP CHASSNEUILL

b)configuration de vyos

Nous allons tout d'abord changer le mot de passe par default et créer un compte qui aura les droits admistrateurs pour eviter de se connecter au compte vyos equivalent à root sur linux.

L'utilisateur se nommera talos et aura un mot de passe fort yukinala30!# different du compte vyos.

- set system host-name talos-router
- set system login user talos full-name "Talos"
- set system login user talos authentication plaintext-password "Yukinala10!#

On éffecue les commande commit et save pour sauvegarder les configurations.

Verification des users

ATELIER ETP CHASSNEUILL

```
[edit]
vyos@vyos# show system login
 user talos {
     authentication {
         encrypted-password $6$rounds=656000$Hj8SDQBs5sLQbOBx$mI3GZsAT6x6DjS0mI3
VqjaMbZ5y6LMui/bbXhC7bfuYRyoJxi.gDZh/QRGvCa9RSJL4rY1mBw5RFKXyd6E0AQ/
     }
     full-name talos
 }
 user vyos {
     authentication {
         encrypted-password $6$rounds=656000$7Wb4Iywr3.OHluiw$jCxojX0QStDG7qr70X
3L/A0JDB.ZiW30e3w4DWbgfQc0X/BR97WubBTt.vPF24.jJQJ0Xcf0nkFecJ48MuXCR/
     }
 }
[edit]
vyos@vyos# S
```

c)Configuration des interfaces Vyos-Router

ATELIER ETP CHASSNEUILL

```
[edit]
vyos@vyos# set interfaces ethernet eth0 address dhcp

  Configuration path: [interfaces ethernet eth0 address dhcp] already exists

[edit]
vyos@vyos# set interfaces ethernet eth1 address 10.1.0.254/24
[edit]
vyos@vyos# set interfaces ethernet eth2 address 192.168.1.254/24
[edit]
vyos@vyos# set interfaces ethernet eth3 address 172.16.1.254/24
[edit]
vyos@vyos# commit
[edit]
vyos@vyos# save
[edit]
vyos@vyos#
```

```
 ethernet eth0 {
     address dhcp
     hw-id 08:00:27:f7:8d:30
     offload {
         gro
         gso
         sg
         tso
     }
 }
 ethernet eth1 {
     address 10.1.0.254/24
     hw-id 08:00:27:a0:11:e0
     offload {
         gro
         gso
         sg
         tso
     }
 }
 ethernet eth2 {
     address 192.168.1.254/24
     hw-id 08:00:27:89:1e:90
     offload {
:
```

Figure 5: verification des interfaces

ATELIER ETP CHASSNEUILL

```
        sg
        tso
    }
}
ethernet eth2 {
    address 192.168.1.254/24
    hw-id 08:00:27:89:1e:90
    offload {
        gro
        gso
        sg
        tso
    }
}
ethernet eth3 {
    address 172.16.1.254/24
    hw-id 08:00:27:52:2a:37
    offload {
        gro
        gso
        sg
        tso
    }
}
:_
```

Figure 6: suite

d)Configuration du NAT sur l'interface eth1

Nous allons créer la regle NAT avec un ID 100 (l'identifiant de la regle de NAT) qui va masquer l'adresse ip de ma machine derriere l'ip pubique du routeur avec le nat source masquerade

```
[edit]
vyos@vyos# set nat source rule 100 outbound-interface name eth0
[edit]
vyos@vyos# set nat source rule 100 source address 10.1.0.0/24

  Configuration path: [nat source rule 100 source address 10.1.0.0/24] already e
xists

[edit]
vyos@vyos# set nat source rule 100 translation address masquerade

  Configuration path: [nat source rule 100 translation address masquerade] alrea
dy exists
```

ATELIER ETP CHASSNEUILL

```
[edit]
vyos@vyos# show nat
 source {
     rule 100 {
         outbound-interface {
             name eth0
         }
         source {
             address 10.1.0.0/24
         }
         translation {
             address masquerade
         }
     }
 }
[edit]
```

Figure 7: verification du NAT

e) configuration du dhcp relay vers srv-ad

Nous allons tous d'abord configurer l'agent de relais-dhcp sur eth2 permettant au serveur DHCP situé le reseau 1(server) une IP à des client qui sont sur le meme réseau local 2 (broadcast) .

```
vyos@vyos-router# set service dhcp-relay interface eth2
```

```
service dhcp-relay upstream-interface eth1
```

```
vyos@vyos-router# set service dhcp-relay server 10.1.0.1
```

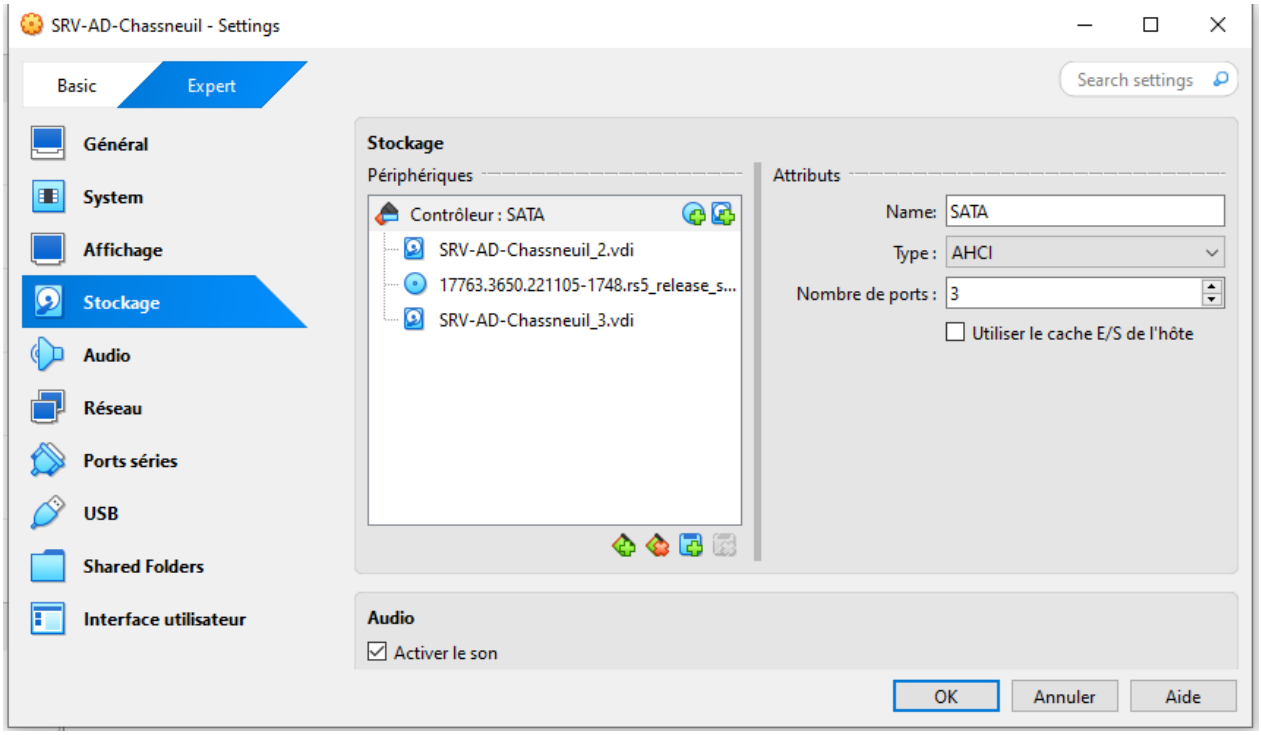
On n'oublit pas d'utiliser commit et save pour sauveagrrder la configuration.

ATELIER ETP CHASSNEUILL

2)Installation et parametrage de windows server 2019

a)installation de la machine virtuelle

Nous allons tout d'abord installer la machine windows server edition datacenter 2019 qui sera controleur de domaine de domaine de chassneuil sur Virtualboxla machine aura 5 gio de ram et 2 disque de 50 gio



nous installerons le systeme sur une partition separée ce qui permettra une meilleur isolation su systeme et facilitera la reinstallation ou la réstauration.

La grande majorité des confiigurations se feront en powershell,pour un soucis de précison et d'efficacité,et pour le plaisir bien sur !

ATELIER ETP CHASSNEUILL

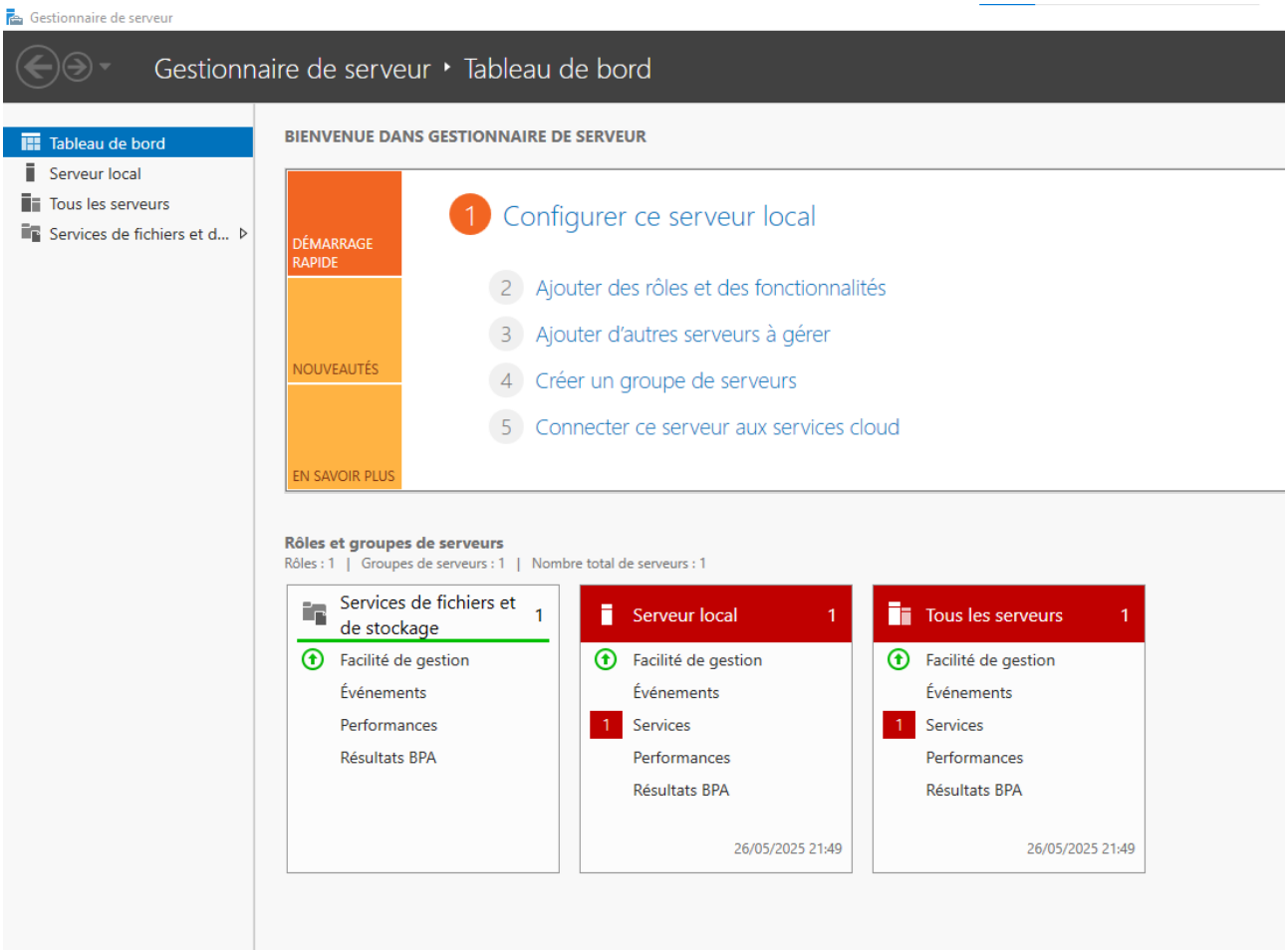


Figure 8: gestionnaire de serveur sur windows serveur 2019

Nous allons renommer le servveur tel quel :

Rename-Computer -NewName "SRV-AD-B2" -Force
Restart-Computer

```
PS C:\Users\Administrateur> Rename-Computer -NewName "SRV-AD-B2" -Force
AVERTISSEMENT : Les modifications seront prises en compte après le redémarrage de l'ordinateur WIN-DLCRB5TCC6T.
```

b)configuration réseau

Configuration de l'adresse ip :
-New-NetIPAddress -InterfaceAlias "Ethernet" -IPAddress "10.1.0.1" -PrefixLength 24 -DefaultGateway "10.1.0.254"

Configuration du dns :

ATELIER ETP CHASSNEUILL

-Set-DnsClientServerAddress -InterfaceAlias "Ethernet" -ServerAddresses "127.0.0.1"

```
PS C:\Users\Administrateur> New-NetIPAddress -InterfaceAlias "Ethernet" -IPAddress "10.1.0.1" -PrefixLength 24 -DefaultGateway "10.1.0.254"


IPAddress         : 10.1.0.1
InterfaceIndex    : 5
InterfaceAlias    : Ethernet
AddressFamily     : IPv4
Type              : Unicast
PrefixLength      : 24
PrefixOrigin      : Manual
SuffixOrigin      : Manual
AddressState      : Tentative
ValidLifetime     : Infinite ([TimeSpan]::MaxValue)
PreferredLifetime : Infinite ([TimeSpan]::MaxValue)
SkipAsSource      : False
PolicyStore       : ActiveStore

IPAddress         : 10.1.0.1
InterfaceIndex    : 5
InterfaceAlias    : Ethernet
AddressFamily     : IPv4
Type              : Unicast
PrefixLength      : 24
PrefixOrigin      : Manual
SuffixOrigin      : Manual
AddressState      : Invalid
ValidLifetime     : Infinite ([TimeSpan]::MaxValue)
PreferredLifetime : Infinite ([TimeSpan]::MaxValue)
SkipAsSource      : False
PolicyStore       : PersistentStore
```

```
PS C:\Users\Administrateur> Set-DnsClientServerAddress -InterfaceAlias "Ethernet" -ServerAddresses "127.0.0.1"
```

Vérification avec les commandes Get-NetIPAddress et Get-DnsClientServerAddress

```
PS C:\Users\Administrateur> Get-NetIPAddress
```

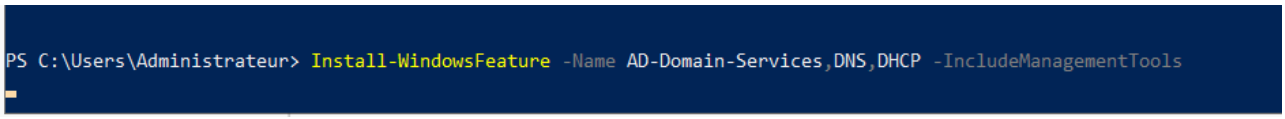
```
PS C:\Users\Administrateur> Get-DnsClientServerAddress

InterfaceAlias               Interface Address ServerAddresses
                             Index     Family
--------------               --------- ------- ---------------
Ethernet                             5 IPv4    {127.0.0.1}
Ethernet                             5 IPv6    {fd00::3}
Loopback Pseudo-Interface 1          1 IPv4    {}
Loopback Pseudo-Interface 1          1 IPv6    {fec0:0:0:ffff::1, fec0:0:0:ffff::2, fec0:0:0:ffff::3}
```

ATELIER ETP CHASSNEUILL

C)Installation des roles

Je vais installer avec cette commande le rôle Active Direcory, le rôle DNS et enfin DHCP

->Install-WindowsFeature -Name AD-Domain-Services, DNS, DHCP -IncludeManagementTools



Verification des roles installés :

Get-WindowsFeature | Where-Object {$_.Installed -eq $true}

ATELIER ETP CHASSNEUILL

```
PS C:\Users\Administrateur> Get-WindowsFeature | Where-Object {$_.Installed -eq $true}

Display Name                                            Name                       Install State
------------                                            ----                       -------------
[X] Serveur DHCP                                        DHCP                           Installed
[X] Serveur DNS                                         DNS                            Installed
[X] Services AD DS                                      AD-Domain-Services             Installed
[X] Services de fichiers et de stockage                 FileAndStorage-Services        Installed
    [X] Services de stockage                            Storage-Services               Installed
[X] Fonctionnalités de .NET Framework 4.7               NET-Framework-45-Fea...        Installed
    [X] .NET Framework 4.7                              NET-Framework-45-Core          Installed
    [X] Services WCF                                    NET-WCF-Services45             Installed
        [X] Partage de port TCP                         NET-WCF-TCP-PortShar...        Installed
[X] Gestion de stratégie de groupe                      GPMC                           Installed
[X] Outils d'administration de serveur distant          RSAT                           Installed
    [X] Outils d'administration de rôles                RSAT-Role-Tools                Installed
        [X] Outils AD DS et AD LDS                      RSAT-AD-Tools                  Installed
            [X] Module Active Directory pour Windows... RSAT-AD-PowerShell             Installed
            [X] Outils AD DS                            RSAT-ADDS                      Installed
                [X] Centre d'administration Active D... RSAT-AD-AdminCenter            Installed
                [X] Composants logiciels enfichables... RSAT-ADDS-Tools                Installed
        [X] Outils du serveur DHCP                      RSAT-DHCP                      Installed
        [X] Outils du serveur DNS                       RSAT-DNS-Server                Installed
[X] Prise en charge WoW64                               WoW64-Support                  Installed
[X] Windows Defender Antivirus                          Windows-Defender               Installed
[X] Windows PowerShell                                  PowerShellRoot                 Installed
    [X] Windows PowerShell 5.1                          PowerShell                     Installed
    [X] Windows PowerShell ISE                          PowerShell-ISE                 Installed
[X] XPS Viewer                                          XPS-Viewer                     Installed
```

Nous allons maintenant promouvoir le serveur en controleur du domaine entrepise tier lieux Pédagogique avec la commande powershell :

```
Install-ADDSForest `
  -DomainName "etp.local" `
  -DomainNetbiosName "ETP" `
  -SafeModeAdministratorPassword (ConvertTo-SecureString "Dsrm@2024" -AsPlainText -Force)`
  -InstallDNS `
  -NoRebootOnCompletion:$false `
  -Force
```

```
PS C:\Users\Administrateur> Install-ADDSForest `
>> -DomainName "etp.local" -DomainNetbiosName "ETP" -SafeModeAdministratorPassword (ConvertTo-SecureString "Yukinala30!#" -AsPlainText -Force) `
>> -InstallDns `
>> -NoRebootOnCompletion:$false `
>> -Force
```

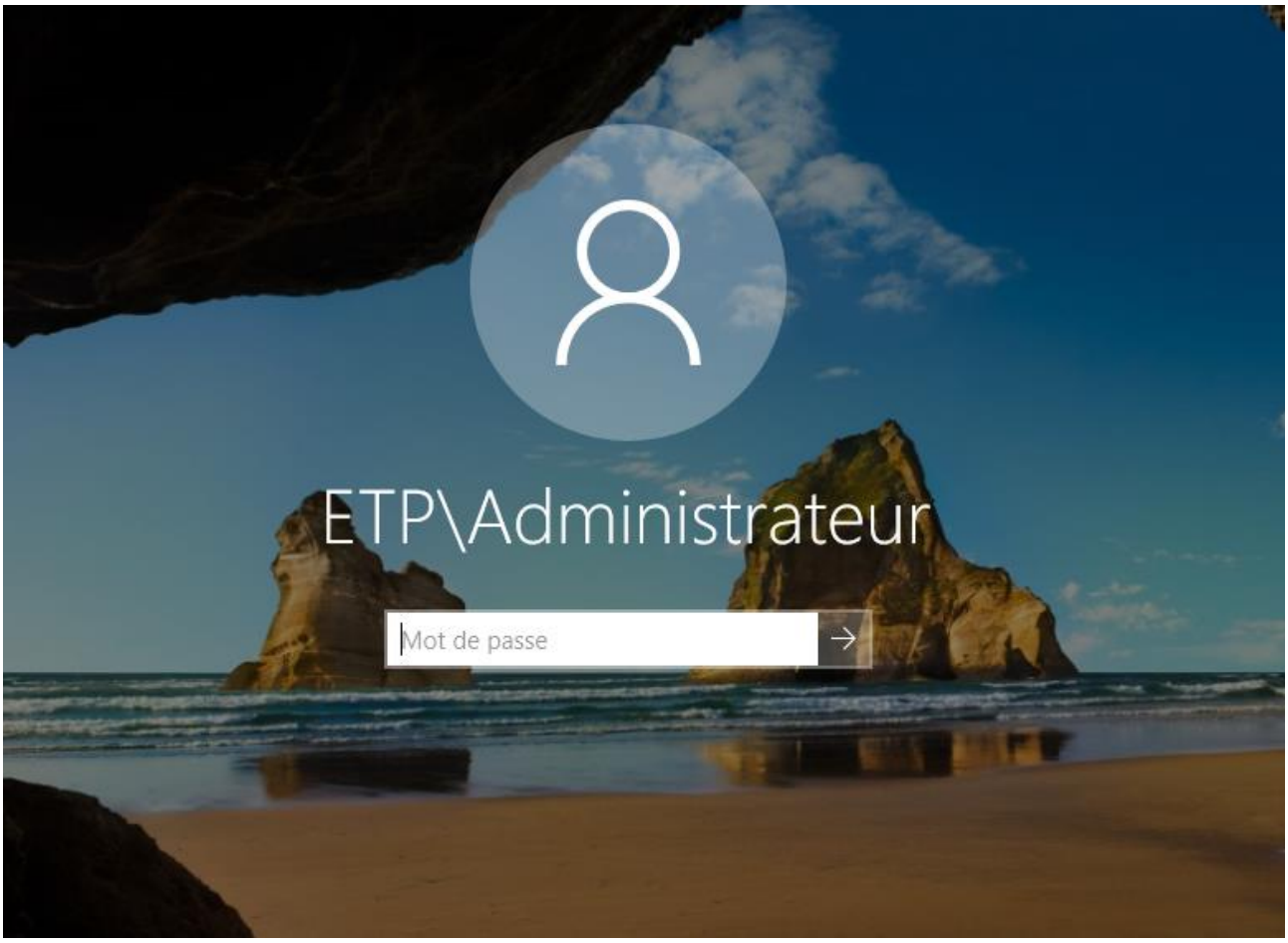


Figure 9: Cela marche!

d) dns

Verification de la zone DNS :

```
PS C:\Users\Administrateur> Get-DnsServerZone

ZoneName                          ZoneType       IsAutoCreated   IsDsIntegrated  IsReverseLookupZone  IsSigned
--------                          --------       -------------   --------------  -------------------  --------
_msdcs.etp.local                  Primary        False           True            False                False
0.in-addr.arpa                    Primary        True            False           True                 False
127.in-addr.arpa                  Primary        True            False           True                 False
255.in-addr.arpa                  Primary        True            False           True                 False
etp.local                         Primary        False           True            False                False
```

Vérification de la résolution DNS :

ATELIER ETP CHASSNEUILL

```
PS C:\Users\Administrateur> Resolve-DnsName SRV-AD-B2.etp.local

Name                                           Type   TTL   Section    IPAddress
----                                           ----   ---   -------    ---------
SRV-AD-B2.etp.local                            AAAA   1200  Question   fe80::73a:3994:a29:af47
SRV-AD-B2.etp.local                            AAAA   1200  Question   fd00::99b1:9b96:ccae:8dd6
SRV-AD-B2.etp.local                            A      1200  Question   10.1.0.1
```

Ajout des redirecteurs DNS Google et journalisation des dns :

```
PS C:\Users\Administrateur> Add-DnsServerForwarder -IPAddress 8.8.8.8,1.1.1.1
PS C:\Users\Administrateur> Set-DnsServerDiagnostics -All $true
```

Création de la zone de recherche inversé utile pour permettre la résolution inverse DNS (utile pour zabbix, les outils réseaux et AD)

```
PS C:\Users\Administrateur> Add-DnsServerPrimaryZone -NetworkId "10.1.0.0/24" -ReplicationScope "Domain" -DynamicUpdate Secure
PS C:\Users\Administrateur>
```

e)dhcp

Création du scope dhcp pour le LAN_CLIENTS qui s'etendra de l'adresse ip 192,168,1,100 à 192,168,1,200 , on évite de donner trop d'adresse au départ pour des raisons de sécurité,moins d'adresses = moins de surface d'attaque.

Nous allons ensuite fournir les informations au scope DHCP, comme l'ip du router vyos et les parametres de notre serveur.

Powershell :

Add-DhcpServerv4Scope -Name "Clients_LAN" -StartRange 192.168.1.100 -EndRange 192.168.1.200 -SubnetMask 255.255.255.0 -State Active

Set-DhcpServerv4OptionValue -ScopeId 192.168.1.0 -Router 192.168.1.254Set-DhcpServerv4OptionValue -ScopeId 192.168.1.0 -DnsServer 10.1.0.1 -DnsDomain etp.local

```
Set-DhcpServerv4OptionValue -ScopeId 192.168.1.0 -Router 192.168.1.254
Set-DhcpServerv4OptionValue -ScopeId 192.168.1.0 -DnsServer 10.1.0.1 -DnsDomain etp.local
```

ATELIER ETP CHASSNEUILL

Puis on autorise le serveur dhcp à distribuer des adresses dans le domaine etp.local car il ny est autorisé par defaut depuis Win Serveur 2008 :

Add-DhcpServerInDC -DnsName "SRV-AD-B2.etp.local" -IPAddress 10.1.0.1

```
Add-DhcpServerInDC -DnsName "SRV-AD-B2.etp.local" -IPAddress 10.1.0.1
```

f)Installation de OpenSSH en powershell

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

```
sc.exe create sshd binPath= "C:\Windows\System32\OpenSSH\sshd.exe" -DisplayName= "OpenSSH Server" start= auto
```

On crée une regle sur le parefeu pour laisser passer le flux ssh sur le port22

```
Start-Service sshd
New-NetFirewallRule -Name sshd -DisplayName 'OpenSSH Server (sshd)' -Enabled True -Direction Inbound -Protocol TCP -Action Allow -LocalPort 22
```

3) connexion du client au domaine et test de connexion

a)connexion au domaine

On va mettre le client dans le bon DNS avec la commande powershell :

ATELIER ETP CHASSNEUILL

```
Set-DnsClientServerAddress -InterfaceAlias "Ethernet" -ServerAddresses 10.1.0.1
```

Puis mettre un ip statique provisoire correspondant au reseau LAN_CLIENTS :

```
PS C:\Windows\system32> New-NetIPAddress -InterfaceAlias "Ethernet" -IPAddress 192.168.1.105 -PrefixLength 24 -DefaultGateway
 192.168.1.254
```

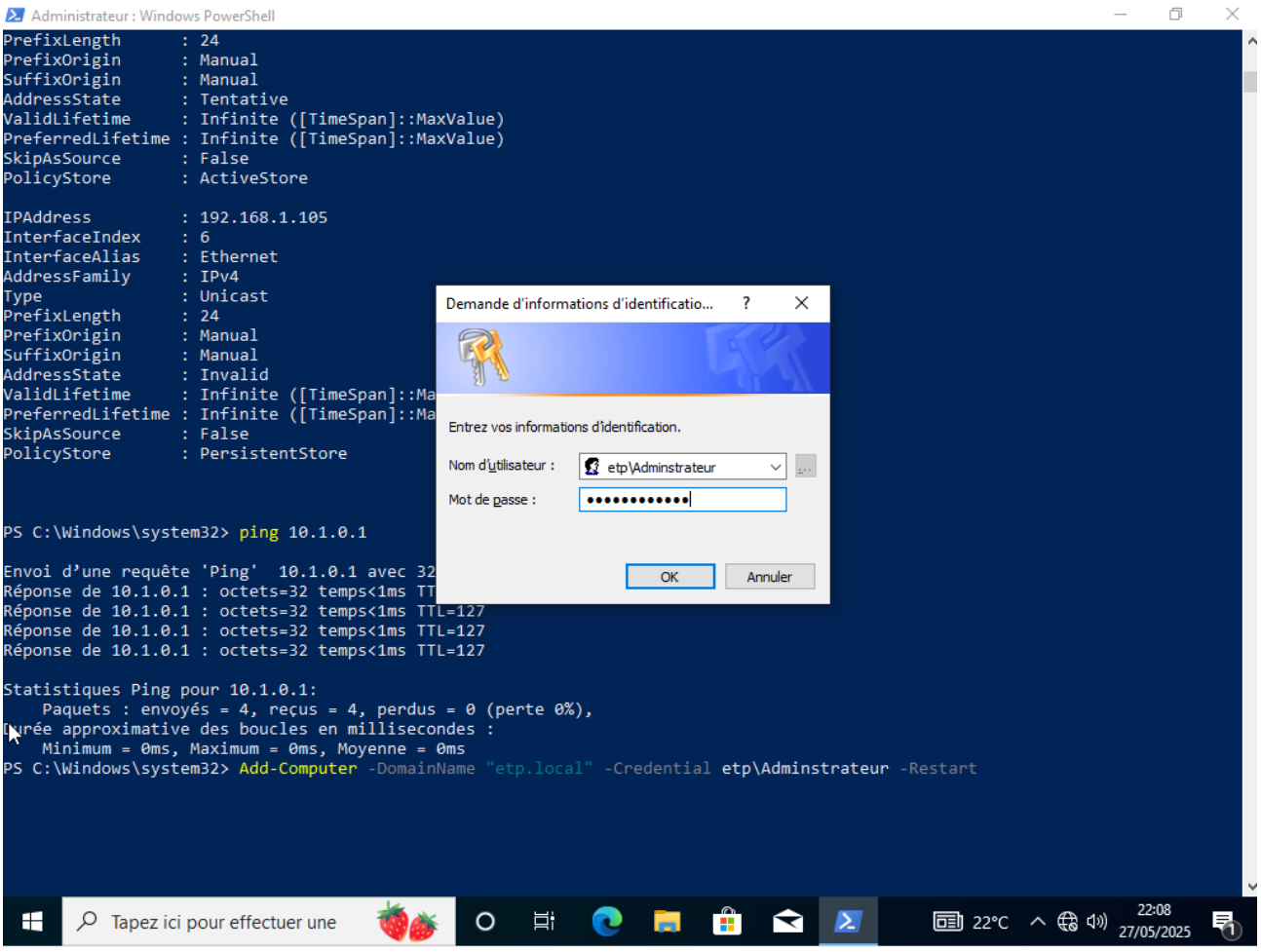
On verifie la bonne connectivité avec le srv-ad avec un ping :

```
PS C:\Windows\system32> ping 10.1.0.1

Envoi d'une requête 'Ping'  10.1.0.1 avec 32 octets de données :
Réponse de 10.1.0.1 : octets=32 temps<1ms TTL=127
Réponse de 10.1.0.1 : octets=32 temps<1ms TTL=127
Réponse de 10.1.0.1 : octets=32 temps<1ms TTL=127
Réponse de 10.1.0.1 : octets=32 temps<1ms TTL=127
```

La connexion peut etre établie :

```
Add-Computer -DomainName "etp.local" -Credential etp\Adminstrateur -Restart
```

ATELIER ETP CHASSNEUILL

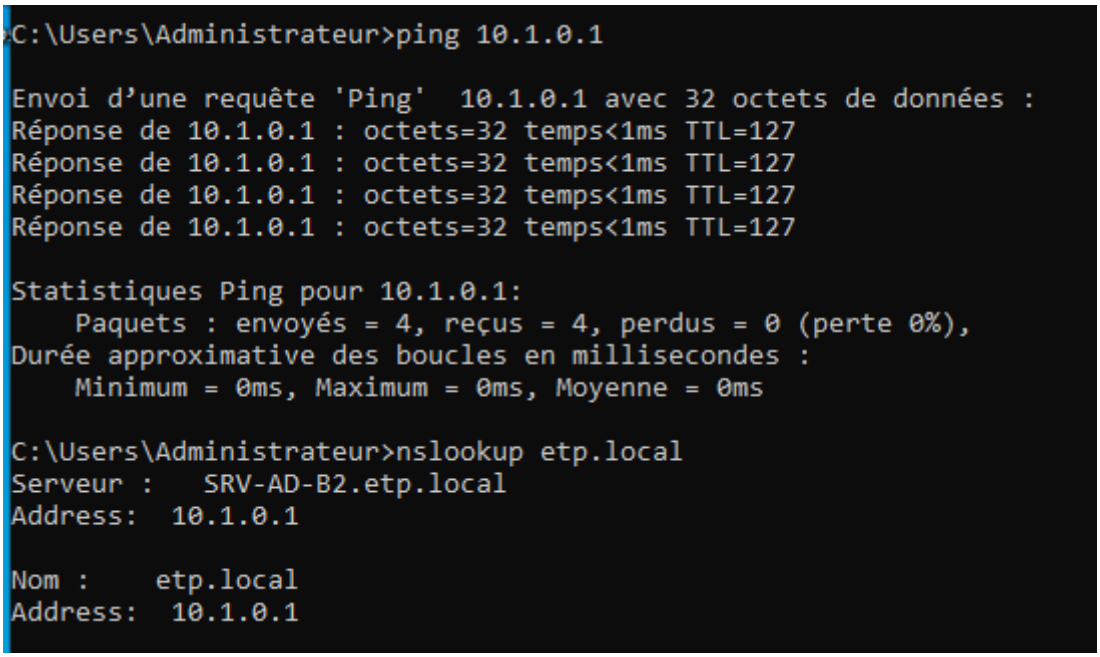


Vérification sur le serveur AD de l'integration du pc

```
PS C:\Users\Administrateur> Get-ADComputer -Filter * | Select Name, Enabled

Name            Enabled
----            -------
SRV-AD-B2          True
DESKTOP-U8OLM5V    True
```

ATELIER ETP CHASSNEUILL

Vérification de la connectivité du client vers le serveur avec ping et nslookup :



b)Script de création de la structure de entreprise tier lieux 86

ATELIER ETP CHASSNEUILL

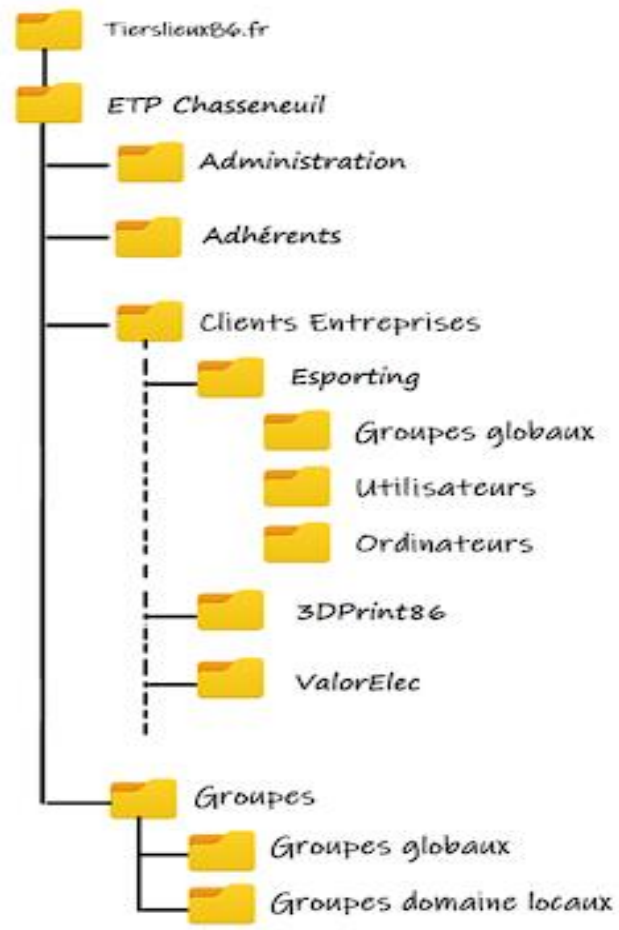
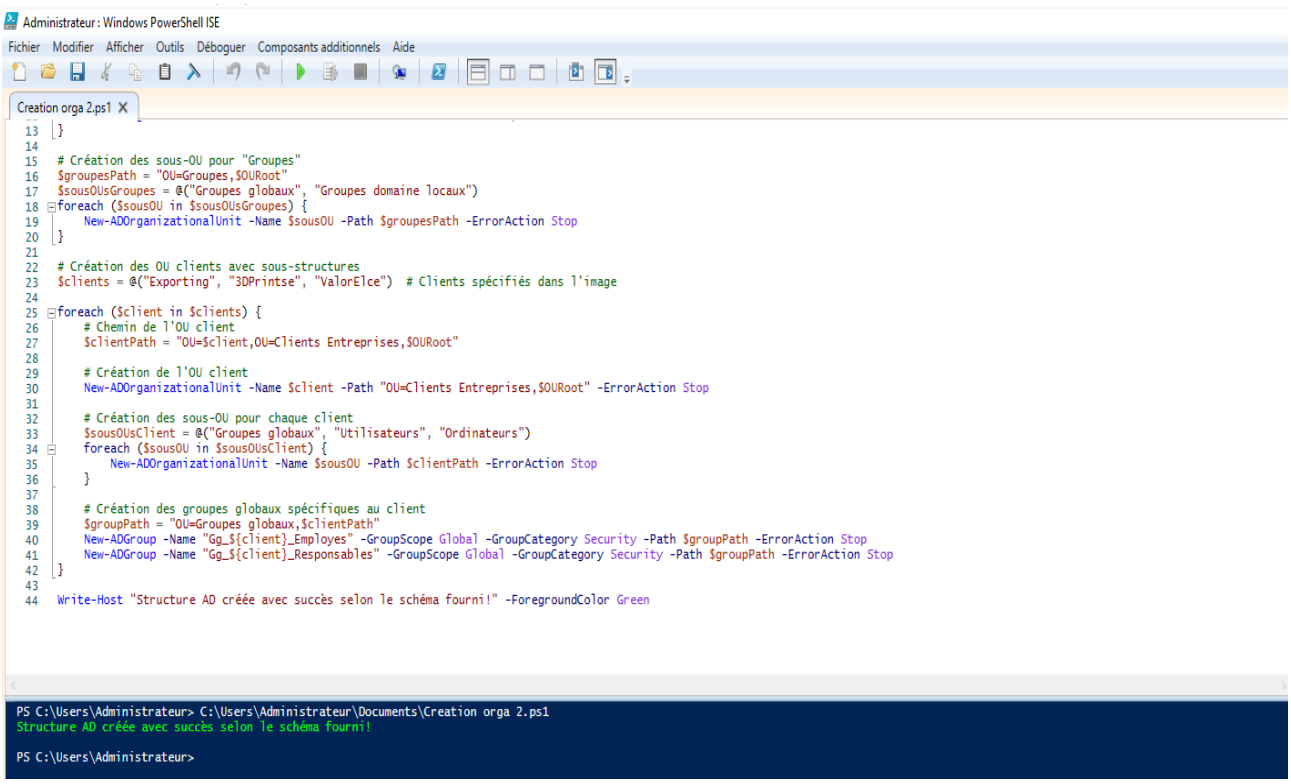


Figure 11: script de création de la structure des groupes et des utilisateurs

```
PS C:\Users\greg> # Racine
New-ADOrganizationalUnit -Name "ETP Chasseneuil" -Path "DC=etp,DC=local"

# Sous-OU
New-ADOrganizationalUnit -Name "Adherents" -Path "OU=ETP Chasseneuil,DC=etp,DC=local"
New-ADOrganizationalUnit -Name "Administration" -Path "OU=ETP Chasseneuil,DC=etp,DC=local"
New-ADOrganizationalUnit -Name "Clients Entreprises" -Path "OU=ETP Chasseneuil,DC=etp,DC=local"
New-ADOrganizationalUnit -Name "Groupes" -Path "OU=ETP Chasseneuil,DC=etp,DC=local"

# Clients
New-ADOrganizationalUnit -Name "3DPrintse" -Path "OU=Clients Entreprises,OU=ETP Chasseneuil,DC=etp,DC=local"
New-ADOrganizationalUnit -Name "Exporting" -Path "OU=Clients Entreprises,OU=ETP Chasseneuil,DC=etp,DC=local"
New-ADOrganizationalUnit -Name "ValorElec" -Path "OU=Clients Entreprises,OU=ETP Chasseneuil,DC=etp,DC=local"

# Groupes
New-ADOrganizationalUnit -Name "Groupes globaux" -Path "OU=Groupes,OU=ETP Chasseneuil,DC=etp,DC=local"
New-ADOrganizationalUnit -Name "Groupes domaine locaux" -Path "OU=Groupes,OU=ETP Chasseneuil,DC=etp,DC=local"

# Groupes globaux
New-ADGroup -Name "GG_Adherents" -GroupScope Global -Path "OU=Groupes globaux,OU=Groupes,OU=ETP Chasseneuil,DC=etp
New-ADGroup -Name "GG_Admin" -GroupScope Global -Path "OU=Groupes globaux,OU=Groupes,OU=ETP Chasseneuil,DC=etp,DC=
New-ADGroup -Name "GG_3DPrintse" -GroupScope Global -Path "OU=Groupes globaux,OU=Groupes,OU=ETP Chasseneuil,DC=etp
New-ADGroup -Name "GG_Exporting" -GroupScope Global -Path "OU=Groupes globaux,OU=Groupes,OU=ETP Chasseneuil,DC=etp
New-ADGroup -Name "GG_ValorElec" -GroupScope Global -Path "OU=Groupes globaux,OU=Groupes,OU=ETP Chasseneuil,DC=etp

# Mot de passe
$password = ConvertTo-SecureString "Yukinala30!#" -AsPlainText -Force

# Création des utilisateurs
New-ADUser -Name "adherent1" -SamAccountName "adherent1" -AccountPassword $password -Enabled $true `
  -Path "OU=Adherents,OU=ETP Chasseneuil,DC=etp,DC=local"
Add-ADGroupMember -Identity "GG_Adherents" -Members "adherent1"

New-ADUser -Name "admin1" -SamAccountName "admin1" -AccountPassword $password -Enabled $true `
  -Path "OU=Administration,OU=ETP Chasseneuil,DC=etp,DC=local"
Add-ADGroupMember -Identity "GG_Admin" -Members "admin1"

New-ADUser -Name "print1" -SamAccountName "print1" -AccountPassword $password -Enabled $true `
  -Path "OU=3DPrintse,OU=Clients Entreprises,OU=ETP Chasseneuil,DC=etp,DC=local"
Add-ADGroupMember -Identity "GG_3DPrintse" -Members "print1"

New-ADUser -Name "exp1" -SamAccountName "exp1" -AccountPassword $password -Enabled $true `
  -Path "OU=Exporting,OU=Clients Entreprises,OU=ETP Chasseneuil,DC=etp,DC=local"
Add-ADGroupMember -Identity "GG_Exporting" -Members "exp1"

New-ADUser -Name "valor1" -SamAccountName "valor1" -AccountPassword $password -Enabled $true `
  -Path "OU=ValorElec,OU=Clients Entreprises,OU=ETP Chasseneuil,DC=etp,DC=local"
Add-ADGroupMember -Identity "GG_ValorElec" -Members "valor1"
```

ATELIER ETP CHASSNEUILL

Le script a etait crée en utilisant Windows powershell IDE pour verifié l'execution pas à pas du script.
Le script permet apres avoir definit les differentes variable de créer la structure de l'organisation et la création des OU et des groupes de etp.local.



ATELIER ETP CHASSNEUILL

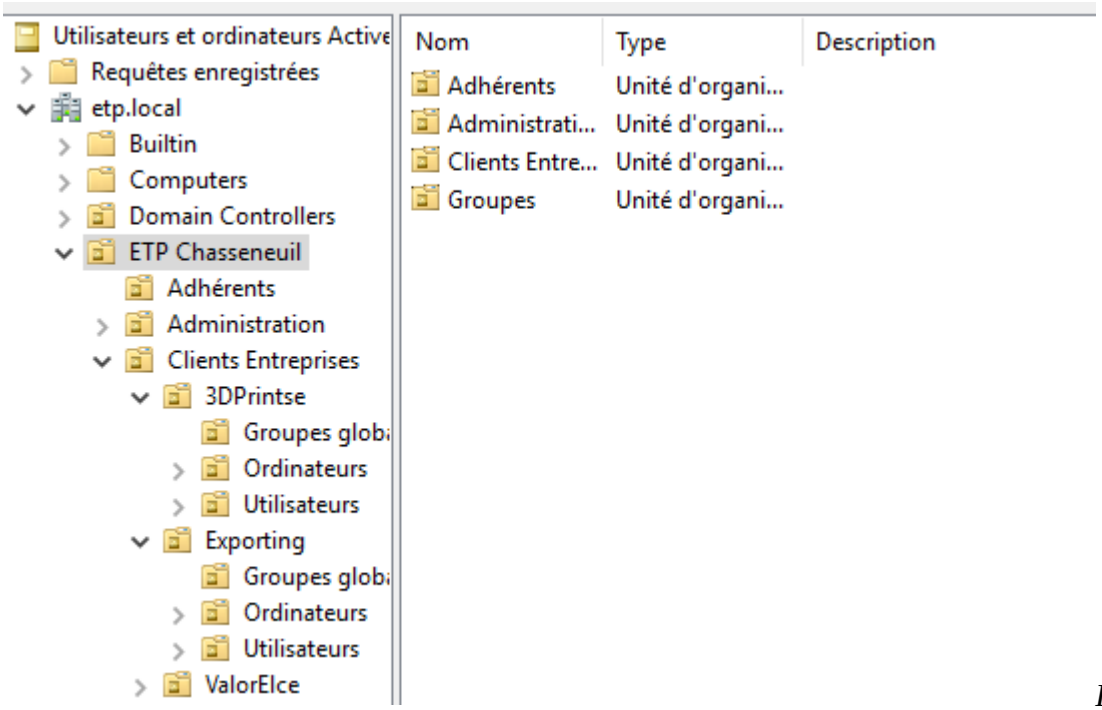


Figure 12: structure crée et fonctionnelle

c)Détails du script

On créé les groupes globaux en powershell

```
New-ADGroup -Name "GG_Admin" -GroupScope Global -Path "OU=Groupes globaux,OU=Groupes,OU=ETP Chasseneuil,DC=etp,DC=local"
New-ADGroup -Name "GG_Adherents" -GroupScope Global -Path "OU=Groupes globaux,OU=Groupes,OU=ETP Chasseneuil,DC=etp,DC=local"
New-ADGroup -Name "GG_3DPrintse" -GroupScope Global -Path "OU=Groupes globaux,OU=Groupes,OU=ETP Chasseneuil,DC=etp,DC=local"
New-ADGroup -Name "GG_Exporting" -GroupScope Global -Path "OU=Groupes globaux,OU=Groupes,OU=ETP Chasseneuil,DC=etp,DC=local"
New-ADGroup -Name "GG_ValorElec" -GroupScope Global -Path "OU=Groupes globaux,OU=Groupes,OU=ETP Chasseneuil,DC=etp,DC=local"
```

ATELIER ETP CHASSNEUILL

On implemente des utilisateurs dans les bonnes OU

```
PS C:\Users\Administrateur> # Administration
PS C:\Users\Administrateur> New-ADUser -Name "admin1" -SamAccountName "admin1" -AccountPassword (ConvertTo-SecureString "P@ssword1002" -AsPlainText -Force) -Enabled $true -Path "OU=Administration,OU=ETP Chasseneuil,DC=etp,DC=local"
PS C:\Users\Administrateur> Add-ADGroupMember -Identity "GG_Admin" -Members "admin1"
PS C:\Users\Administrateur>
PS C:\Users\Administrateur> # Adherents
PS C:\Users\Administrateur> New-ADUser -Name "adherent1" -SamAccountName "adherent1" -AccountPassword (ConvertTo-SecureString "P@ssword1002" -AsPlainText -Force) -Enabled $true -Path "OU=Adherents,OU=ETP Chasseneuil,DC=etp,DC=local"
PS C:\Users\Administrateur> Add-ADGroupMember -Identity "GG_Adherents" -Members "adherent1"
PS C:\Users\Administrateur>
PS C:\Users\Administrateur> # 3DPrintse
PS C:\Users\Administrateur> New-ADUser -Name "print1" -SamAccountName "print1" -AccountPassword (ConvertTo-SecureString "P@ssword1002" -AsPlainText -Force) -Enabled $true -Path "OU=3DPrintse,OU=Clients Entreprises,OU=ETP Chasseneuil,DC=etp,DC=local"
PS C:\Users\Administrateur> Add-ADGroupMember -Identity "GG_3DPrintse" -Members "print1"
PS C:\Users\Administrateur>
PS C:\Users\Administrateur> # Exporting
PS C:\Users\Administrateur> New-ADUser -Name "export1" -SamAccountName "export1" -AccountPassword (ConvertTo-SecureString "P@ssword1002" -AsPlainText -Force) -Enabled $true -Path "OU=Exporting,OU=Clients Entreprises,OU=ETP Chasseneuil,DC=etp,DC=local"
PS C:\Users\Administrateur> Add-ADGroupMember -Identity "GG_Exporting" -Members "export1"
PS C:\Users\Administrateur>
PS C:\Users\Administrateur> # ValorElec
PS C:\Users\Administrateur> New-ADUser -Name "valor1" -SamAccountName "valor1" -AccountPassword (ConvertTo-SecureString "P@ssword1002" -AsPlainText -Force) -Enabled $true -Path "OU=ValorElec,OU=Clients Entreprises,OU=ETP Chasseneuil,DC=etp,DC=local"
PS C:\Users\Administrateur> Add-ADGroupMember -Identity "GG_ValorElec" -Members "valor1"
PS C:\Users\Administrateur>
```

```
New-ADUser -Name "adherent1" -SamAccountName "adherent1" -AccountPassword $password -Enabled $true `
  -Path "OU=Adherents,OU=ETP Chasseneuil,DC=etp,DC=local"
Add-ADGroupMember -Identity "GG_Adherents" -Members "adherent1"
```

```
# Groupes globaux
New-ADGroup -Name "GG_Adherents" -GroupScope Global -Path "OU=Groupes globaux,OU=Groupes,OU=ETP Chasseneuil,DC=etp,DC=local" -PassThru
New-ADGroup -Name "GG_Admin" -GroupScope Global -Path "OU=Groupes globaux,OU=Groupes,OU=ETP Chasseneuil,DC=etp,DC=local" -PassThruS
New-ADGroup -Name "GG_3DPrintse" -GroupScope Global -Path "OU=Groupes globaux,OU=Groupes,OU=ETP Chasseneuil,DC=etp,DC=local" -PassThru
New-ADGroup -Name "GG_Exporting" -GroupScope Global -Path "OU=Groupes globaux,OU=Groupes,OU=ETP Chasseneuil,DC=etp,DC=local" -PassThru
New-ADGroup -Name "GG_ValorElec" -GroupScope Global -Path "OU=Groupes globaux,OU=Groupes,OU=ETP Chasseneuil,DC=etp,DC=local" -PassThru
```

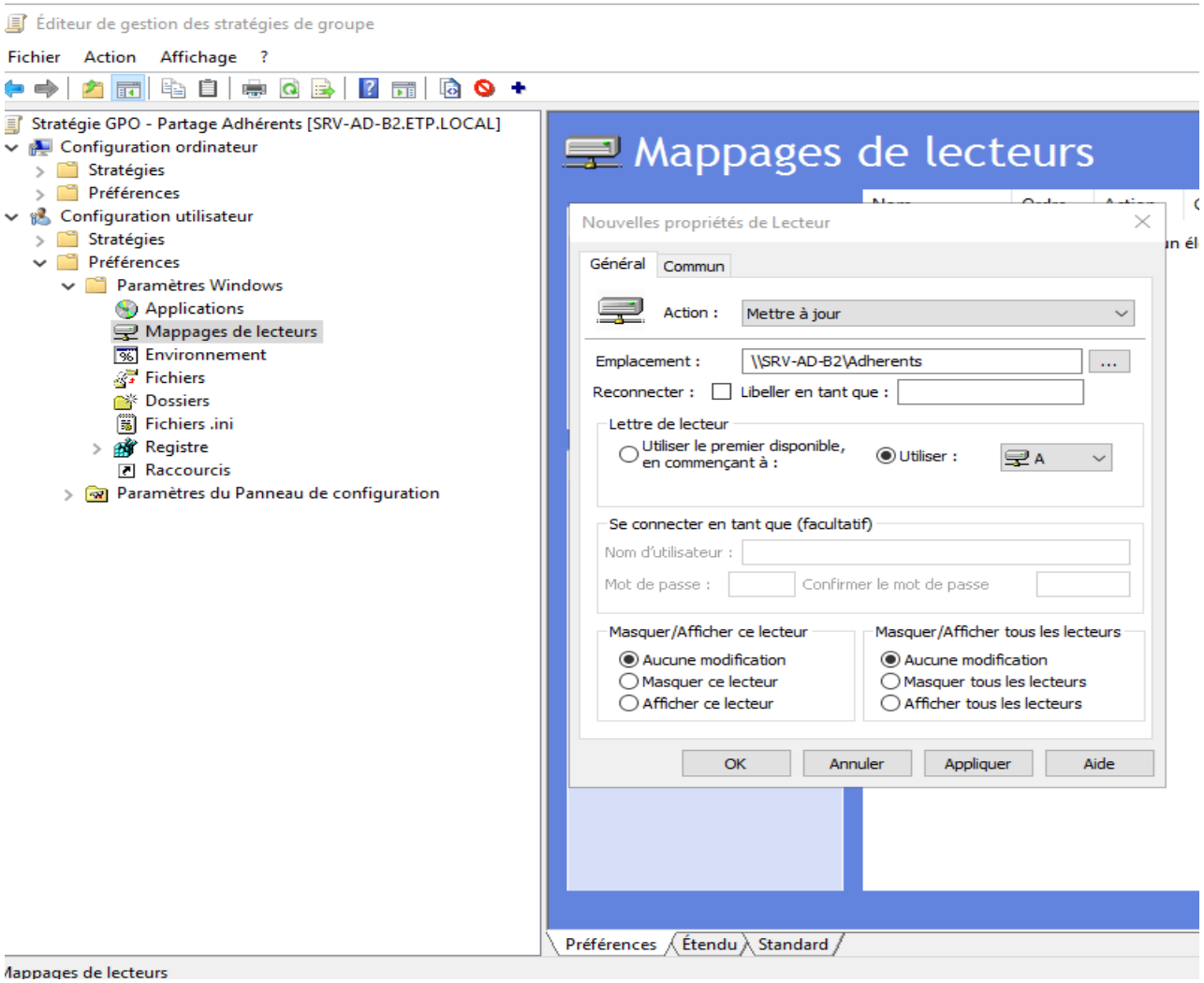
d)Création du dossier de partage pour les adherents et autorisations

- New-Item -ItemType Directory -Path "A:\Adherents"
- New-ADGroup -Name "DL_Adherents_RW" `
  -SamAccountName "DL_Adherents_RW" `
  -GroupScope DomainLocal `
  -GroupCategory Security `
  -Path "OU=Groupes domaine locaux,OU=Groupes,OU=ETP Chasseneuil,DC=etp,DC=local"
- icacls "A:\Adherents" /grant "ETP\DL_Adherents_RW:(OI)(CI)M" /T
- New-SmbShare -Name "Adherents" -Path "A:\Adherents" -FullAccess "ETP\DL_Adherents_RW"

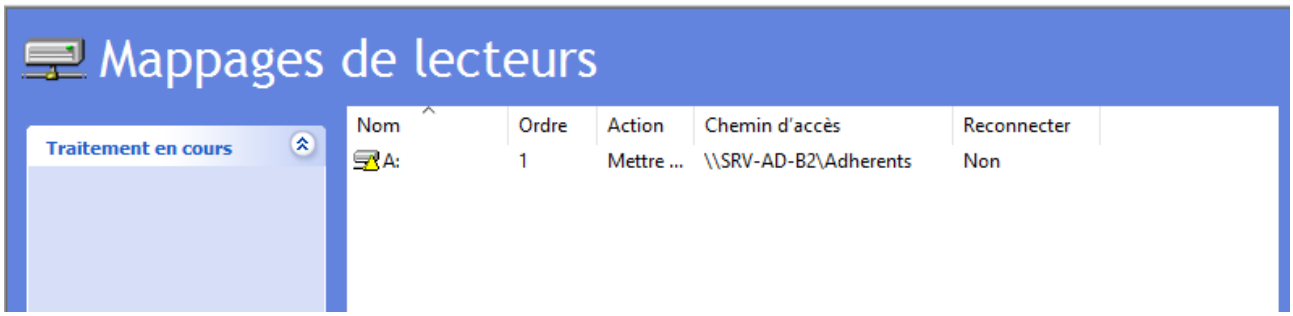
ATELIER ETP CHASSNEUILL

```
PS C:\Users\Administrateur> icacls "A:\Adherents" /grant "ETP\DL_Adherents_RW:(OI)(CI)M" /T
fichier traité : A:\Adherents
1 fichiers correctement traités ; échec du traitement de 0 fichiers
PS C:\Users\Administrateur>
```

On crée une gpo qui s'intitulera GPO – Partages Adhérents à laquelle on va mapper un lecteur



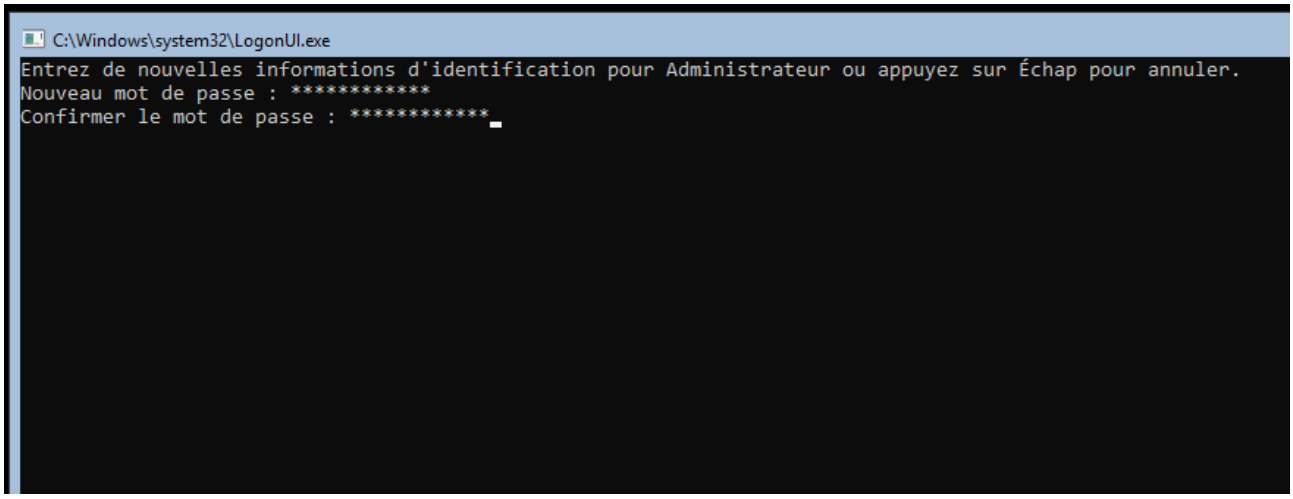
ATELIER ETP CHASSNEUILL



ATELIER ETP CHASSNEUILL

4)Création de la replication de l’active directory

La replication ce fera en windows serveur core pour economiser des ressources (la ram) et limiter la surface d’attaque



ATELIER ETP CHASSNEUILL

```
C:\Users\Administrateur>powershell
Windows PowerShell
Copyright (C) Microsoft Corporation. Tous droits réservés.

PS C:\Users\Administrateur> Get-NetAdapter

Name                      InterfaceDescription                    ifIndex Status       MacAddress             LinkSpeed
----                      --------------------                    ------- ------       ----------             ---------
Ethernet                  Intel(R) PRO/1000 MT Desktop Adapter          6 Up           08-00-27-1D-04-E3         1 Gbps


PS C:\Users\Administrateur> New-NetIPAddress -InterfaceAlias "Ethernet" -IPAddress "10.1.0.2" -PrefixLength 24 -DefaultGatewa
y 10.1.0.254


IPAddress         : 10.1.0.2
InterfaceIndex    : 6
InterfaceAlias    : Ethernet
AddressFamily     : IPv4
Type              : Unicast
PrefixLength      : 24
PrefixOrigin      : Manual
SuffixOrigin      : Manual
AddressState      : Tentative
ValidLifetime     : Infinite ([TimeSpan]::MaxValue)
PreferredLifetime : Infinite ([TimeSpan]::MaxValue)
SkipAsSource      : False
PolicyStore       : ActiveStore

IPAddress         : 10.1.0.2
InterfaceIndex    : 6
InterfaceAlias    : Ethernet
AddressFamily     : IPv4
Type              : Unicast
PrefixLength      : 24
PrefixOrigin      : Manual
SuffixOrigin      : Manual
AddressState      : Invalid
ValidLifetime     : Infinite ([TimeSpan]::MaxValue)
PreferredLifetime : Infinite ([TimeSpan]::MaxValue)
SkipAsSource      : False
PolicyStore       : PersistentStore


PS C:\Users\Administrateur>
```

On va pointer le dns vers le serveurAD principal

```
Set-DnsClientServerAddress -InterfaceAlias "Ethernet" -ServerAddresses 10.1.0.1
```

Puis joindre le domaine etp.local

```
> Add-Computer -DomainName "etp.local" -Credential etp\Administrateur Restart-Computer
```

On va ensuite installer le rôle active directory domains services et importer le module ADDS pour pouvoir effectuer la replication de l'AD.

ATELIER ETP CHASSNEUILL

```
PS C:\Users\Administrateur> Install-WindowsFeature AD-Domain-Services

Success Restart Needed Exit Code      Feature Result
------- -------------- ---------      --------------
True    No             Success        {Services AD DS, Outils d'administration d...


PS C:\Users\Administrateur> Import-Module ADDSDeployment
```

Maintenant on fait la replication :

```
PS C:\Users\Administrateur> Install-ADDSDomainController -DomainName "etp.local" -InstallDns:$true -Credential (Get-Credentia
l) -SiteName "Default-First-Site-Name" -ReplicationSourceDC "SRV-AD-B2.etp.local" -DatabasePath "C:\Windows\NTDS\" -LogPath "
C:\Windows\NTDS\" -SysvolPath "C:\Windows\SYSVOL\" -Force:$true
```

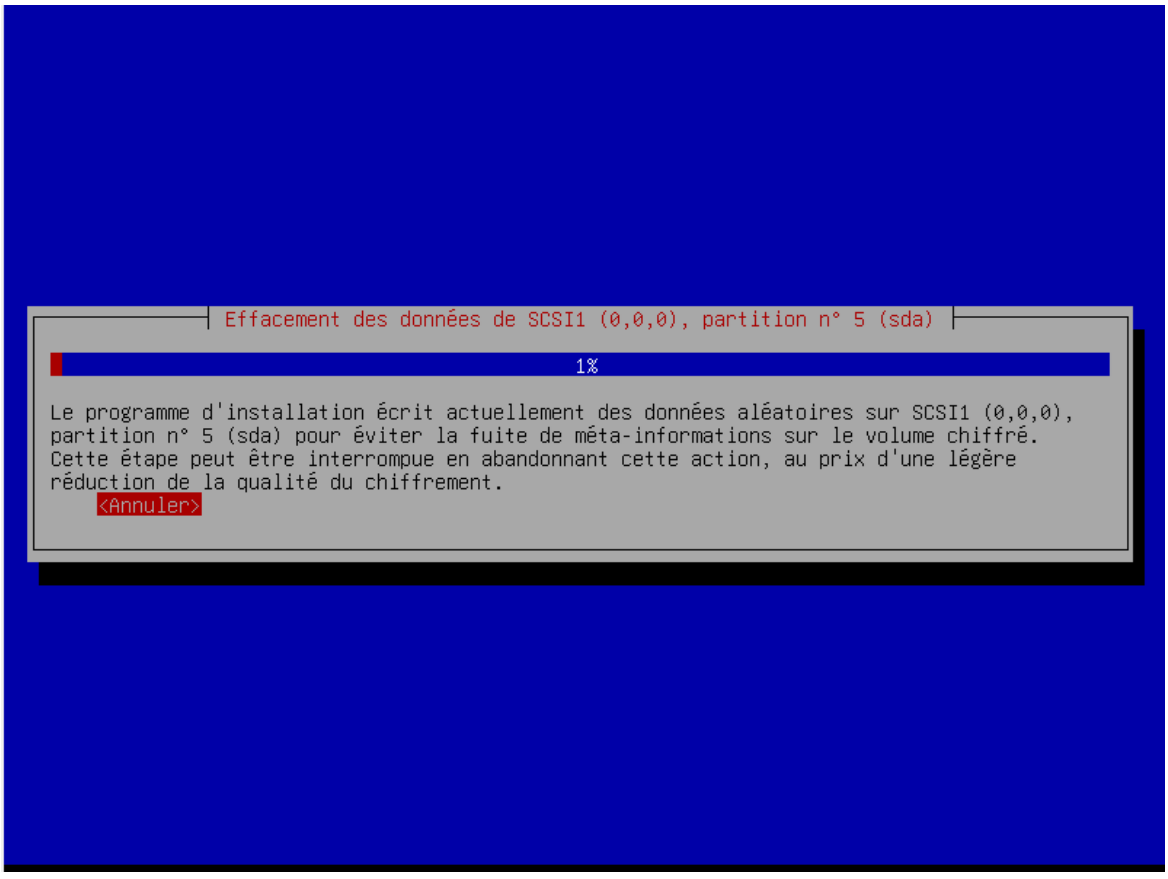
ATELIER ETP CHASSNEUILL

5)Installation de zabbix et des agents

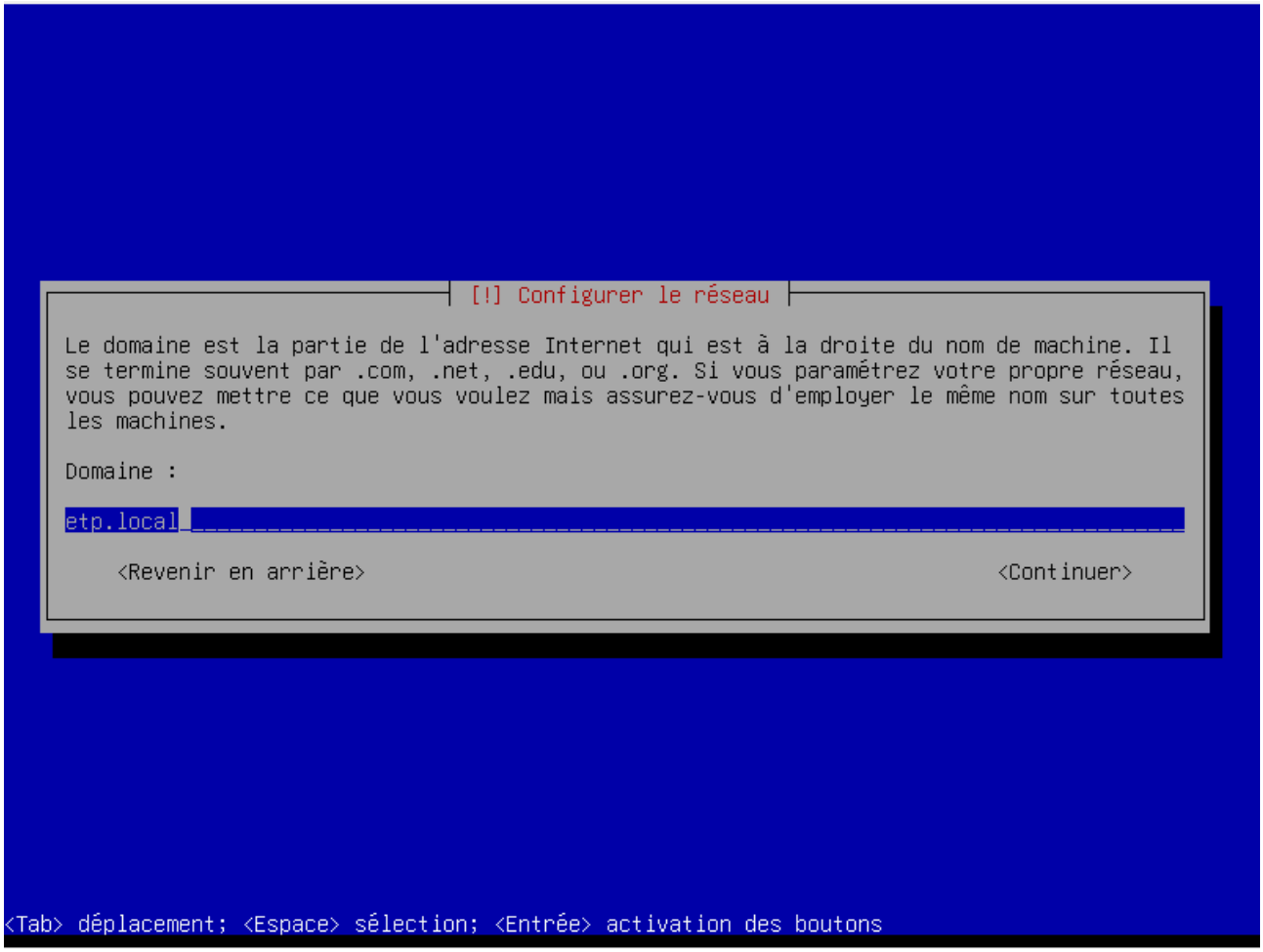
a) configuration et installation

Nous allons procéder dans les etapes suivantes à l'installation de zabbix sur une machine virtuelle debian 12 de 4GO de RAM et 40GO d'espace disque.

L'installation se fera en LVM chiffré pour garantir la confidentialité et l'intégrité des données.



ATELIER ETP CHASSNEUILL



Installation des depots zabbix 7,2 pour Debain 12

```
wget https://repo.zabbix.com/zabbix/7.2/release/debian/pool/main/z/zabbix-release/zabbix-release_latest_7.2+debian12_all.deb
dpkg -i zabbix-release_latest_7.2+debian12_all.deb
apt update
```

Installation du front end,du serveur zabbix et de l'agent

```
apt install zabbix-server-mysql zabbix-frontend-php zabbix-apache-conf zabbix-sql-scripts zabbix-agent
```

ATELIER ETP CHASSNEUILL

Création de la base de données zabbix avec l'utilisateur zabbix mot de passe 1002 (mot de passe faible pour l'atelier,mais en situation de production il en faudrait un plus solide)

```
MariaDB [(none)]> create database zabbix character set utf8mb4 collate utf8mb4_bin;
Query OK, 1 row affected (0,000 sec)

MariaDB [(none)]> create user zabbix@localhost identified by '1002';
Query OK, 0 rows affected (0,002 sec)

MariaDB [(none)]> grant all privileges on zabbix.* to zabbix@localhost;
Query OK, 0 rows affected (0,002 sec)

MariaDB [(none)]>  set global log_bin_trust_function_creators = 1;
Query OK, 0 rows affected (0,000 sec)

MariaDB [(none)]>  quit;
```

Creation du schéma de la base de données zabbix :

zcat /usr/share/zabbix/sql-scripts/mysql/server.sql.gz | mysql --default-character-set=utf8mb4 -uzabbix -p zabbix

Desactiver l'option log_bin_trust_function_creators apres l'importation du schéma de base de données :

mysql> set global log_bin_trust_function_creators = 0;
mysql> quit;

Modification du fichier zabbix.server.conf pour le mot de passe DBPassword=1002

ATELIER ETP CHASSNEUILL

```
DBUser=zabbix

### Option: DBPassword
#       Database password.
#       Comment this line if no password is used.
#
# Mandatory: no
# Default:
# DBPassword=1002
```

On va lancer le processus zabbix et agent au démarage du systeme :

```
# systemctl restart zabbix-server zabbix-agent apache2
# systemctl enable zabbix-server zabbix-agent apache2
```

Installation du module manquant :

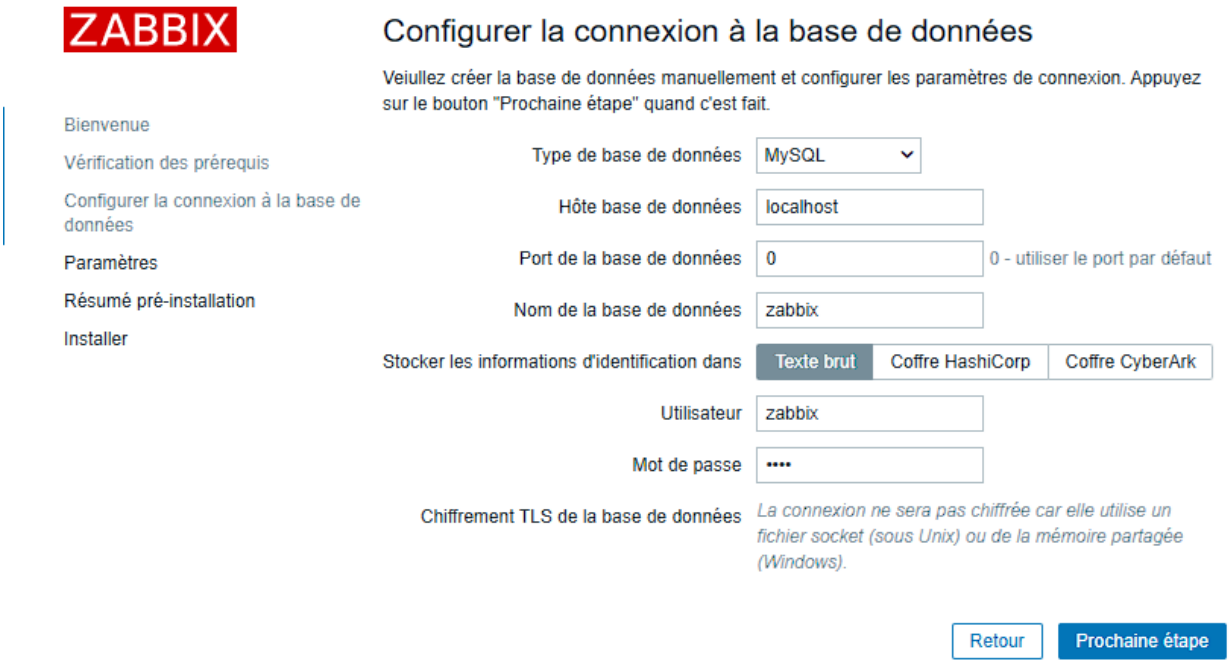
- sudo apt install php-mysql
- sudo systemctl restart apache2

Avec la commande ip a, l'ip du serveur zabbix sera obtenu et nous pourrons nous connecter à l'interface web :

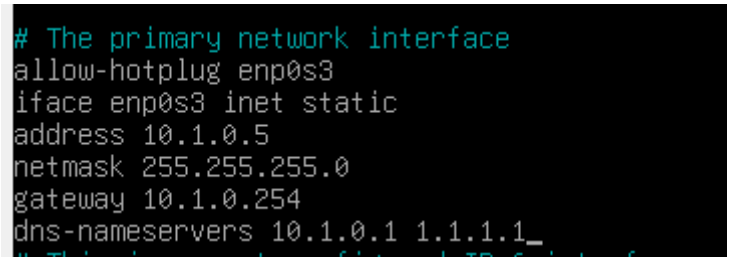
ATELIER ETP CHASSNEUILL

Figure 13: cela marche

ATELIER ETP CHASSNEUILL

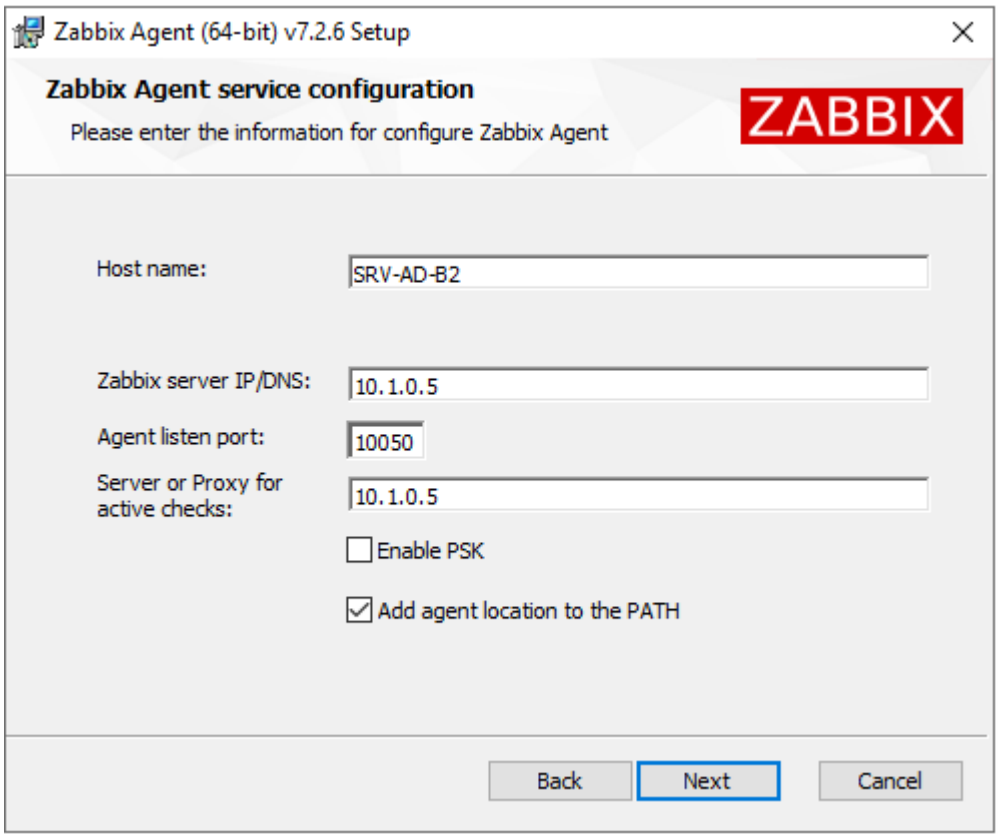


Nous allons maintenant configurer le serveur zabbix en statique avec l'adresse 10.1.0.3

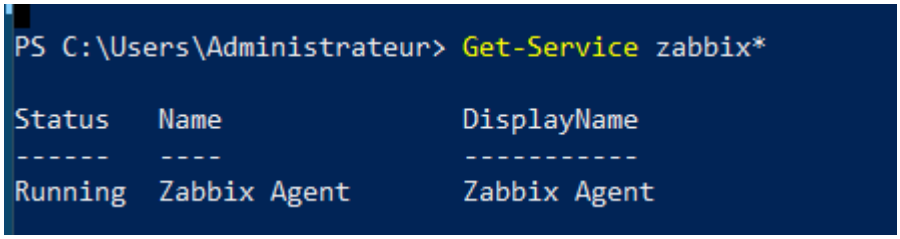


ATELIER ETP CHASSNEUILL

b)Installation de l’agent zabbix

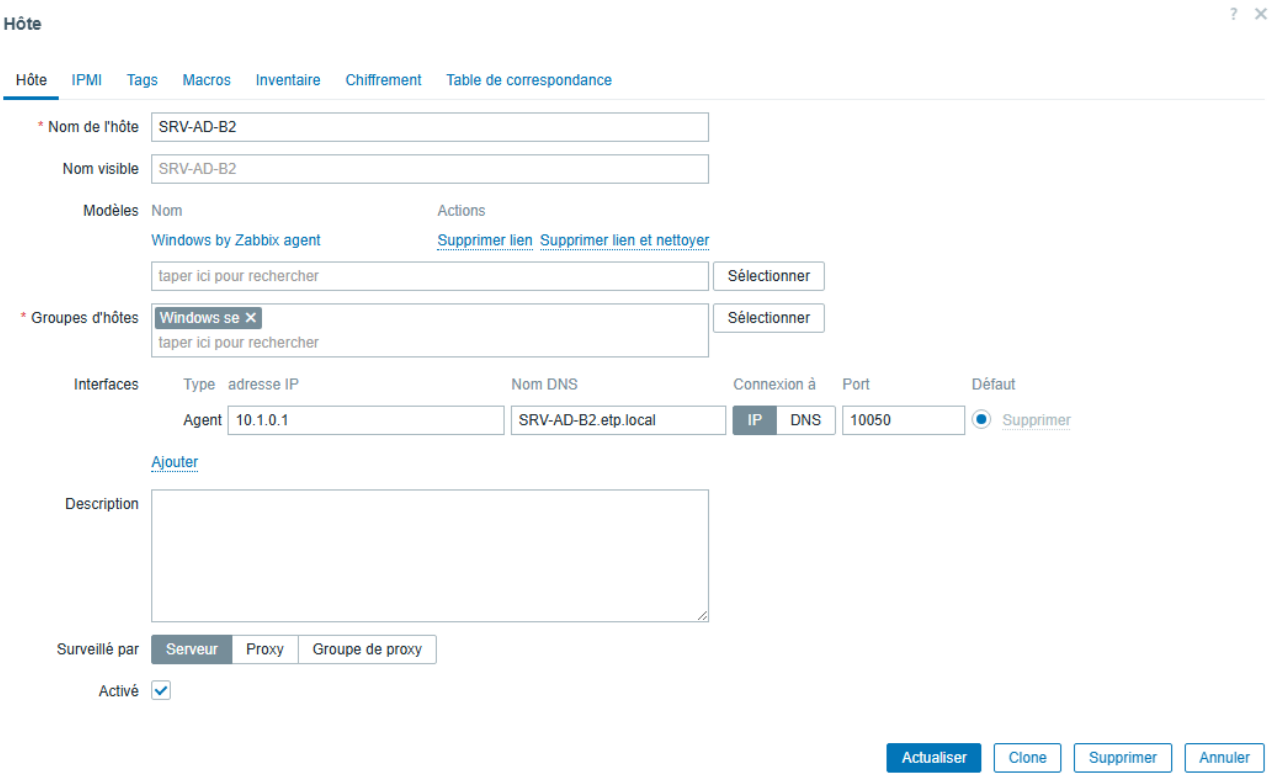


Verification



Configuration de l’hote sur zabbix

ATELIER ETP CHASSNEUILL



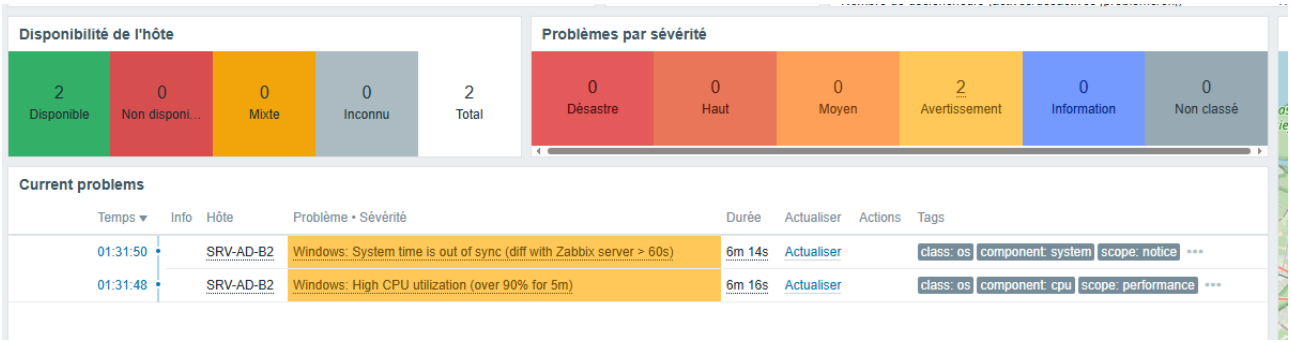


Figure 14: l'agent remonte bien les informations de l'hote

ATELIER ETP CHASSNEUILL

6) Stockage sur TrueNas Core

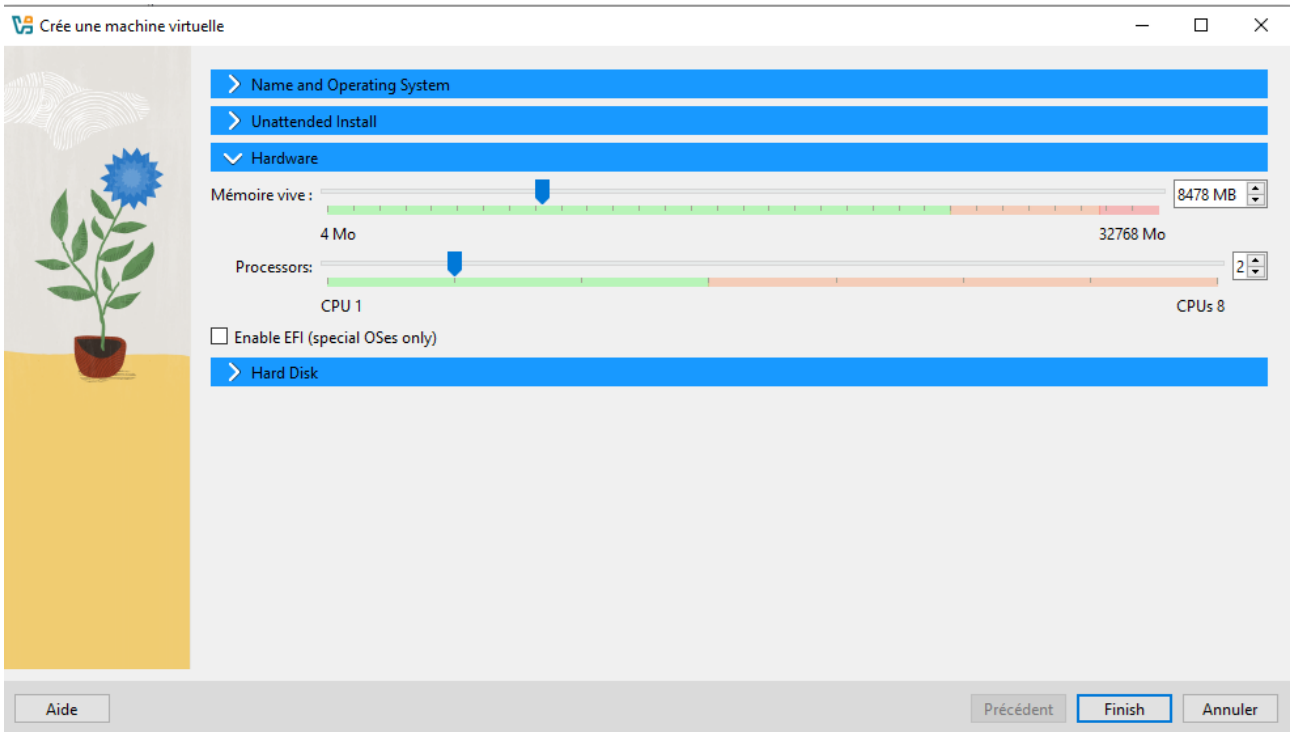
a) Installation

On utilisera true nas core avec 8GO de ram et 2 CPU.

La capacité des 2 disques sera de 20 GO et 150 GO (parrtition systeme et partiton stockage)

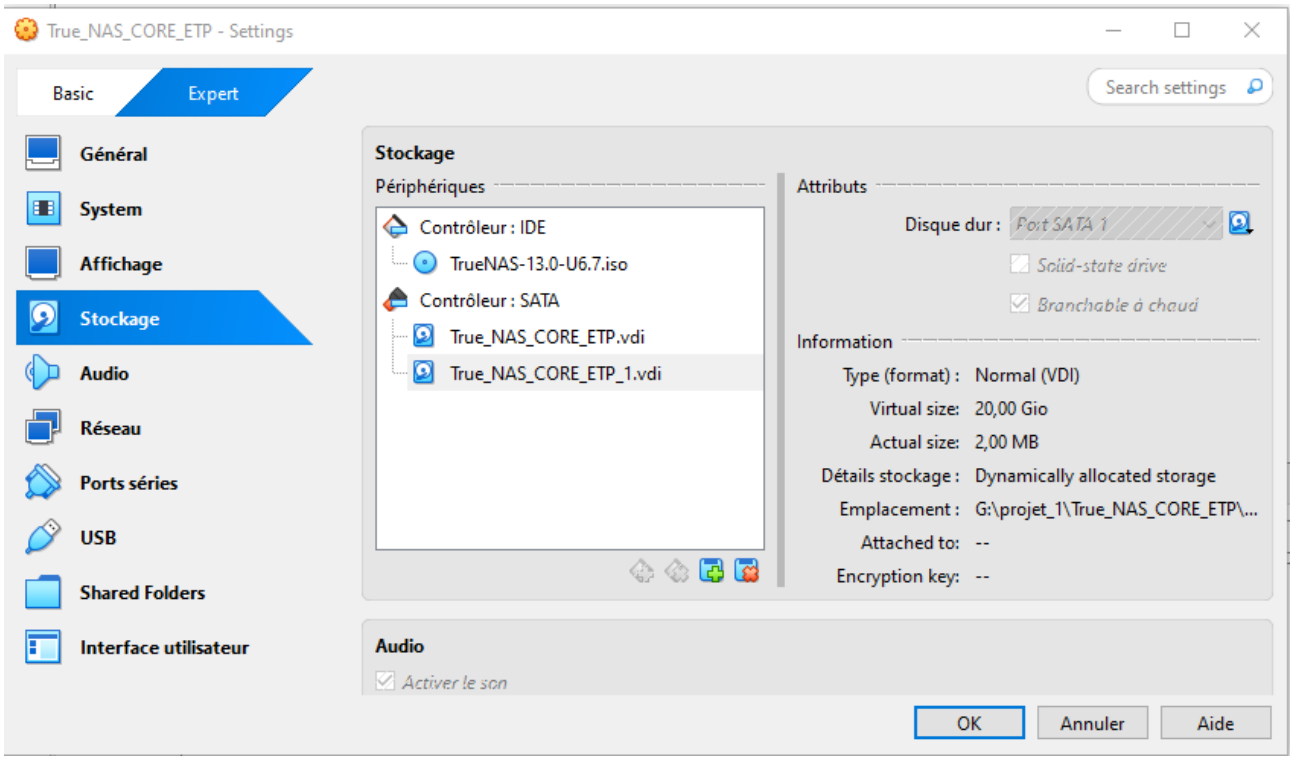
ATELIER ETP CHASSNEUILL

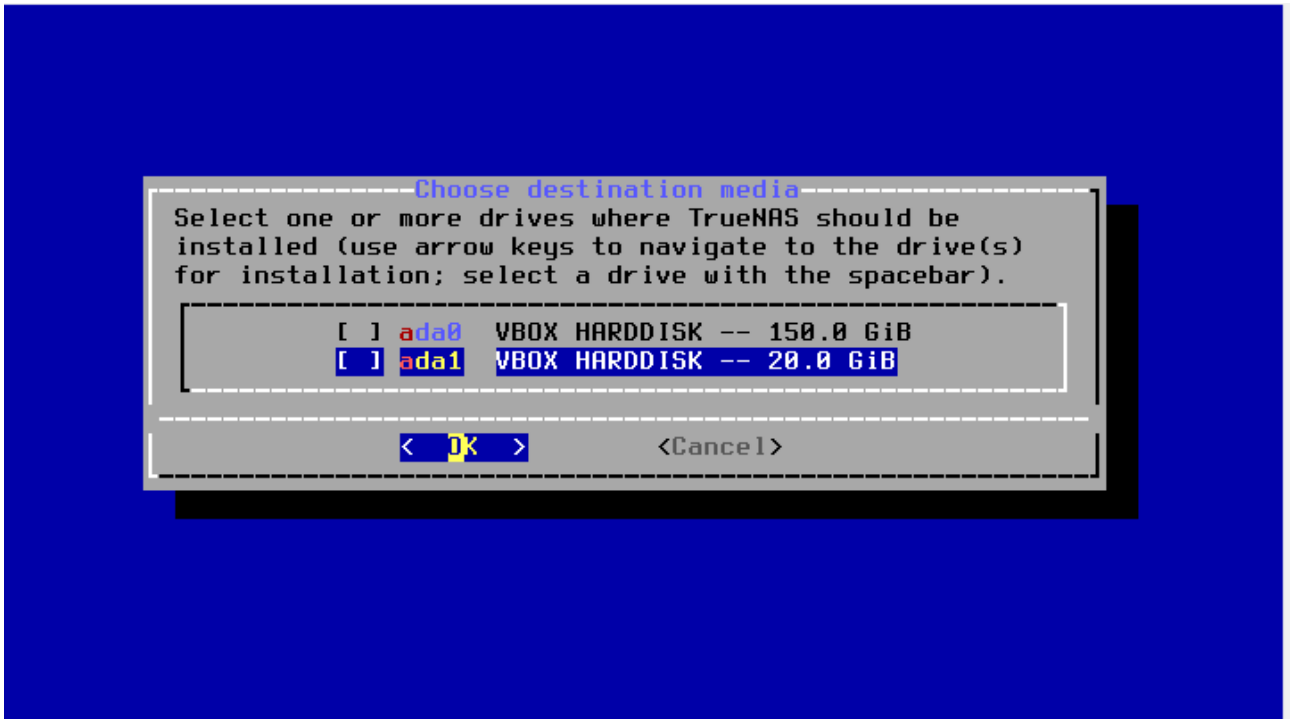
Le serveur sera utilisé pour la sauvegarde windows.



Création de la partition systeme de 20 Go et du disque de 150 Go.

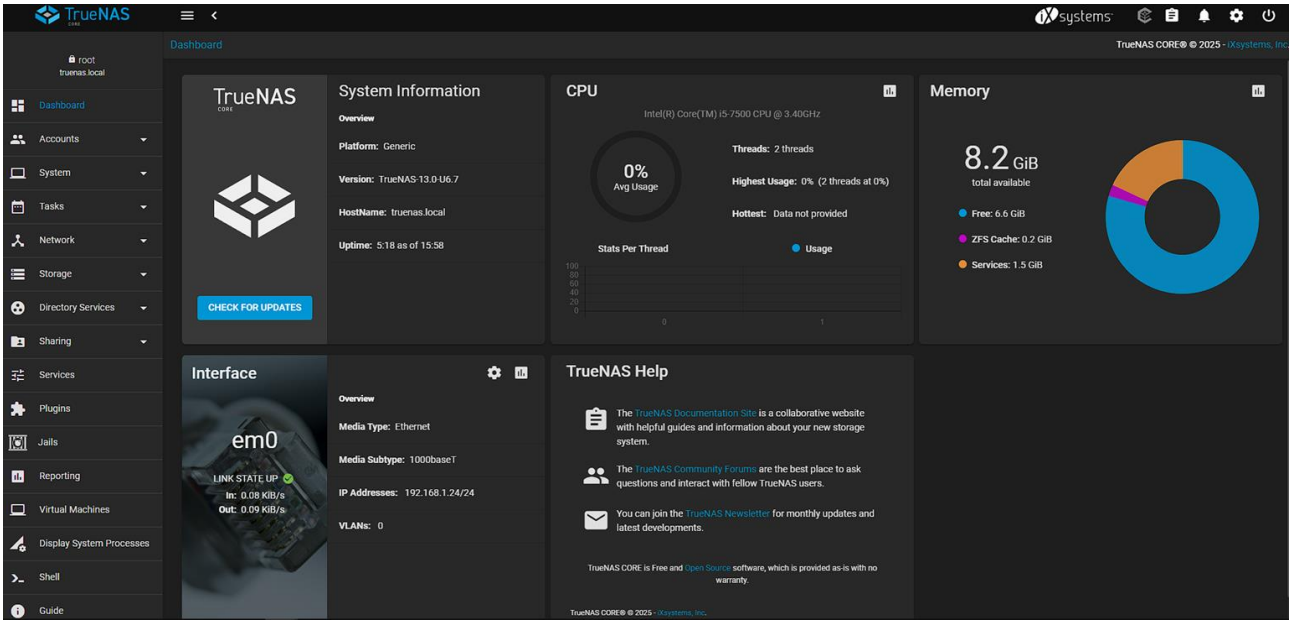
ATELIER ETP CHASSNEUILL





ATELIER ETP CHASSNEUILL

Nous voici dans l'interface web de Truenas core

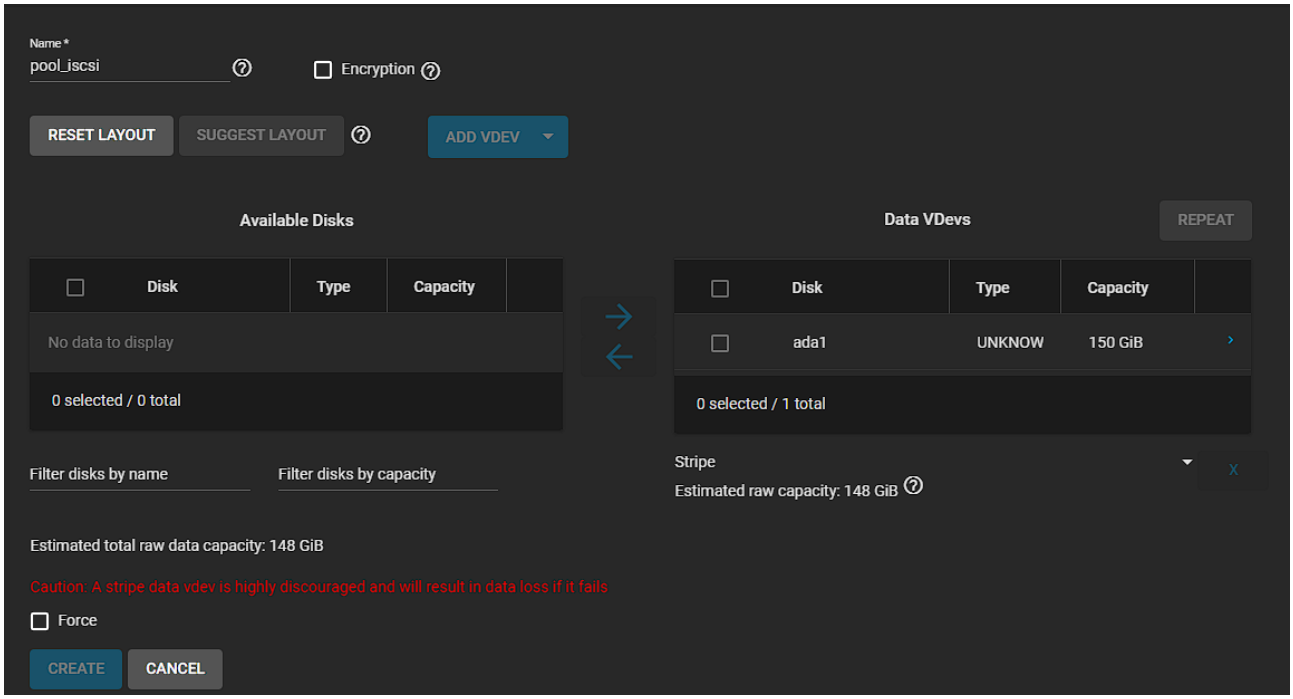


B) Configuration comme cible iSCSI pour le SRV-AD-B2

Nous allons tout d'abord créer un volume logique (zvol) qui servira de disque iSCSI ((**Internet Small Computer Systems Interface**) qui permettra que la stockage distant deviennent un disque à part entiere pour le SRV-AD-B2, on s'en servira ici comme d'un backup distant.

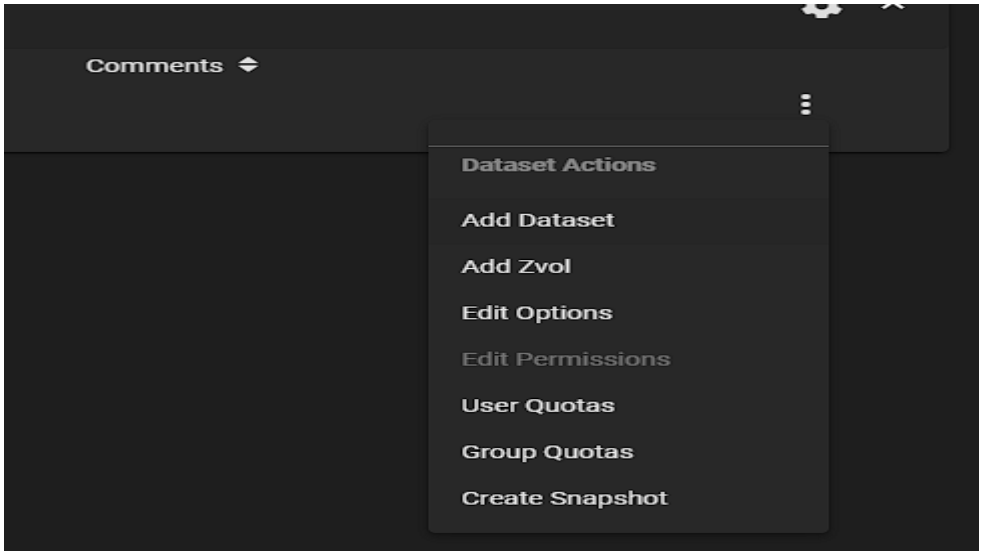
Création du pool_iscsi

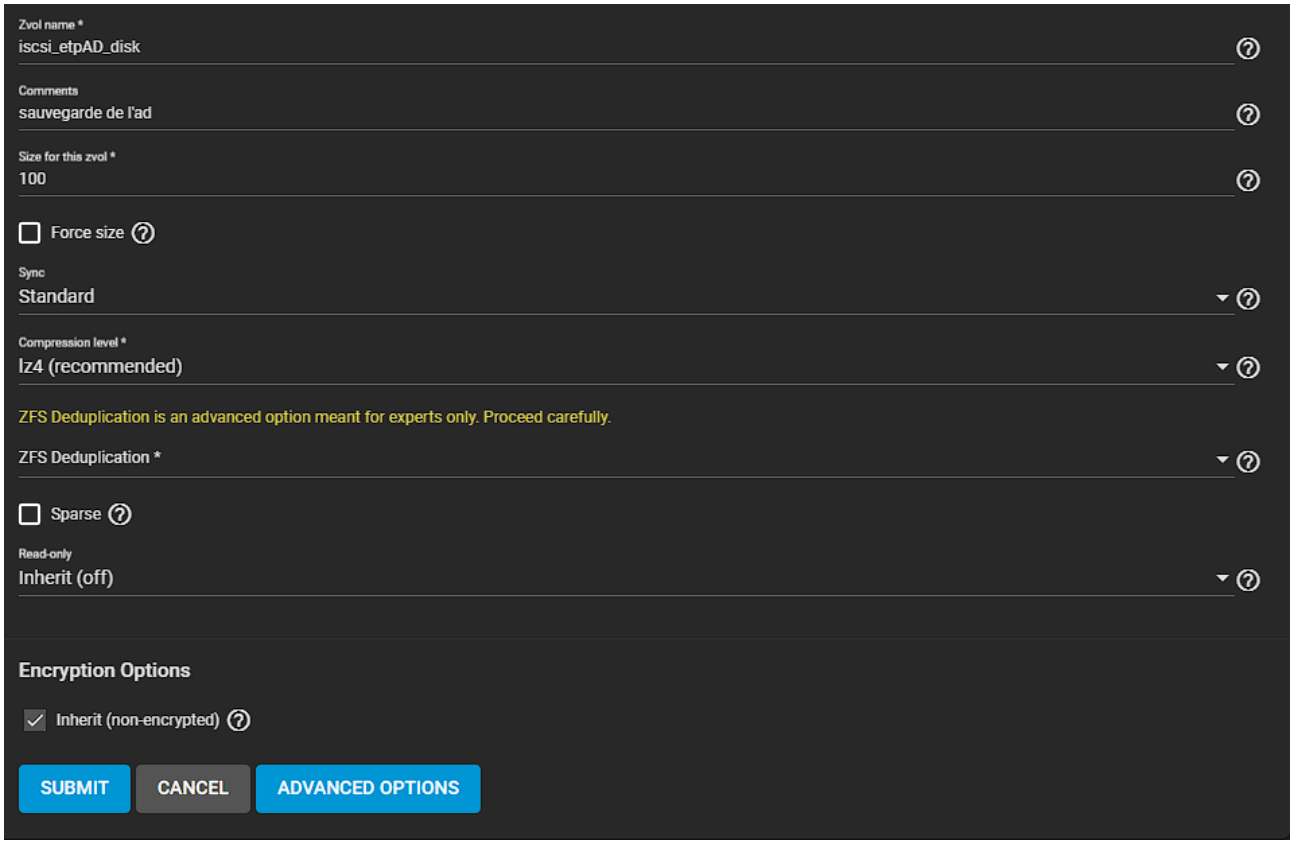
ATELIER ETP CHASSNEUILL



Création du zvol

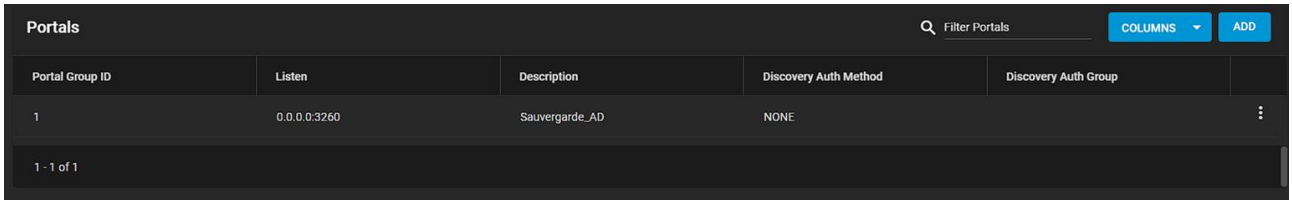
ATELIER ETP CHASSNEUILL

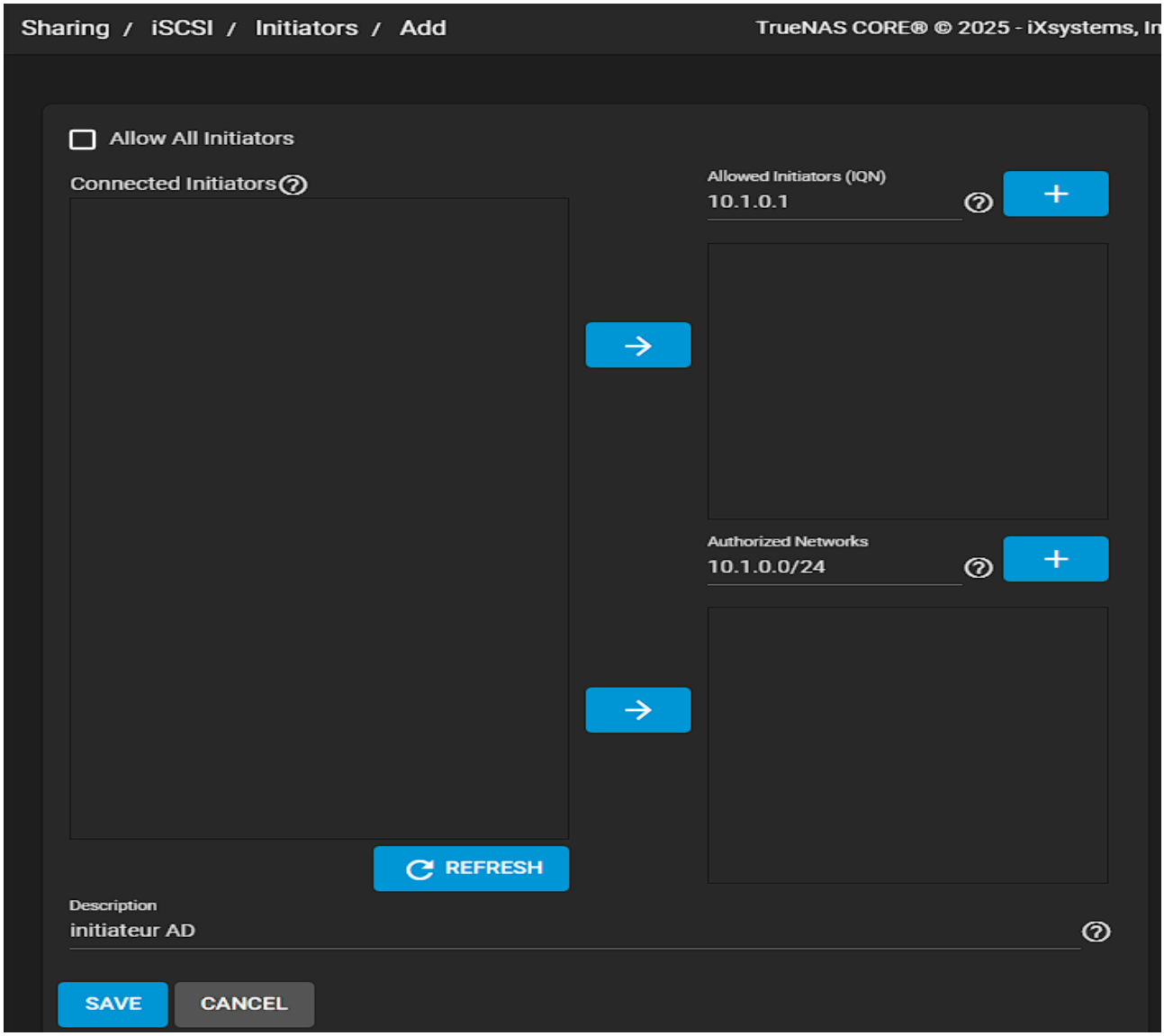




Il s'agira dorénanvant d'effectuer la configuration iscsi du treunas core en créant le portail iSCSi

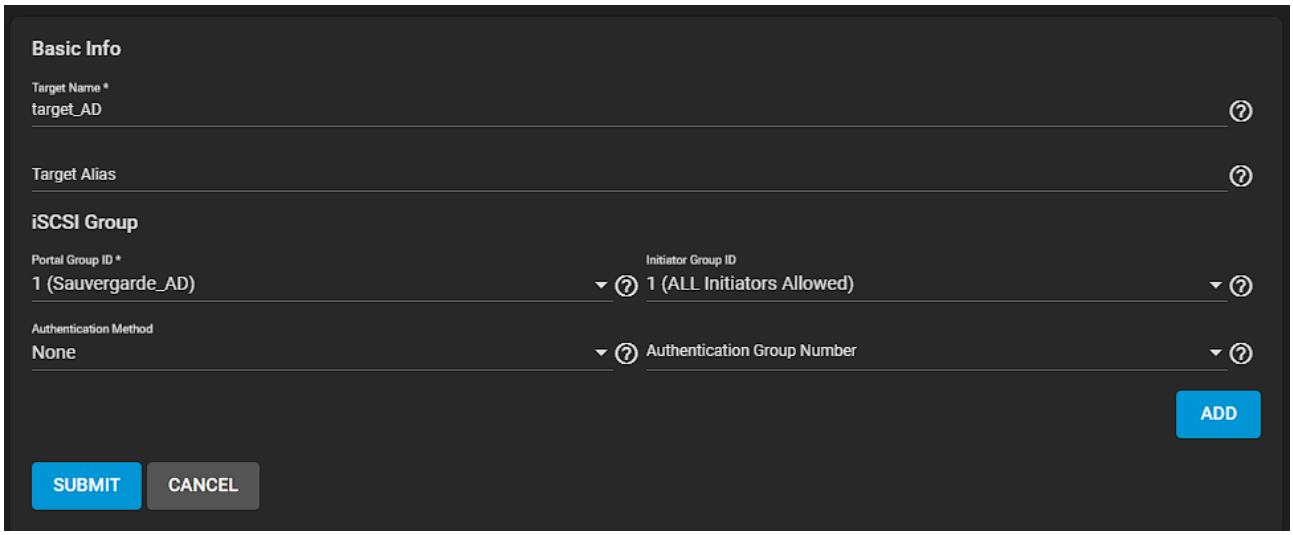
ATELIER ETP CHASSNEUILL



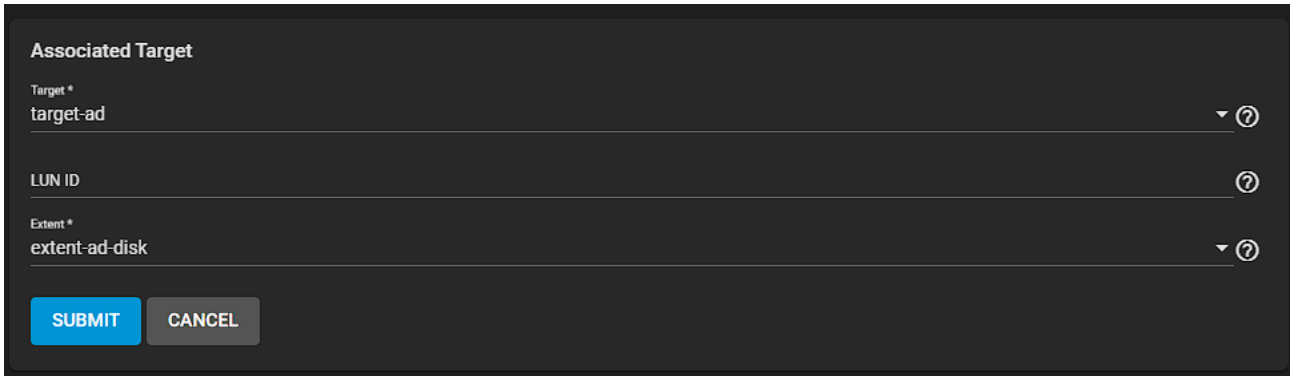


On crée la cible iscsi

ATELIER ETP CHASSNEUILL

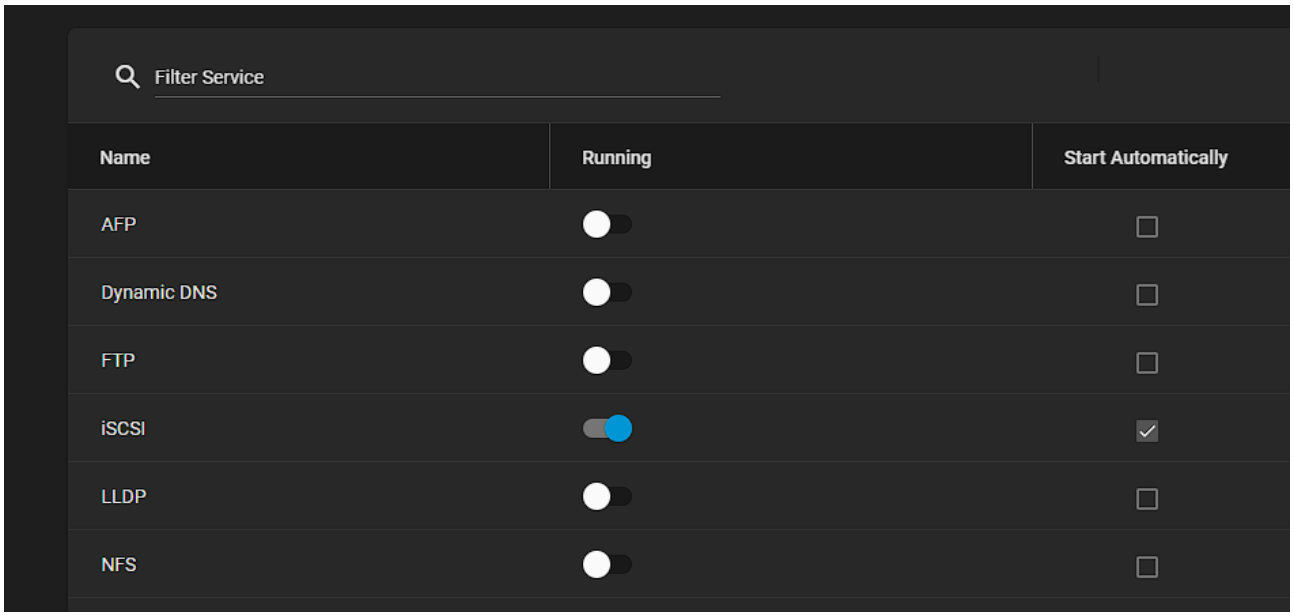


On associe le target et l'extent (la cible 10.1.0.1 vers nos disques configurés



ATELIER ETP CHASSNEUILL

On va enfin activer le service



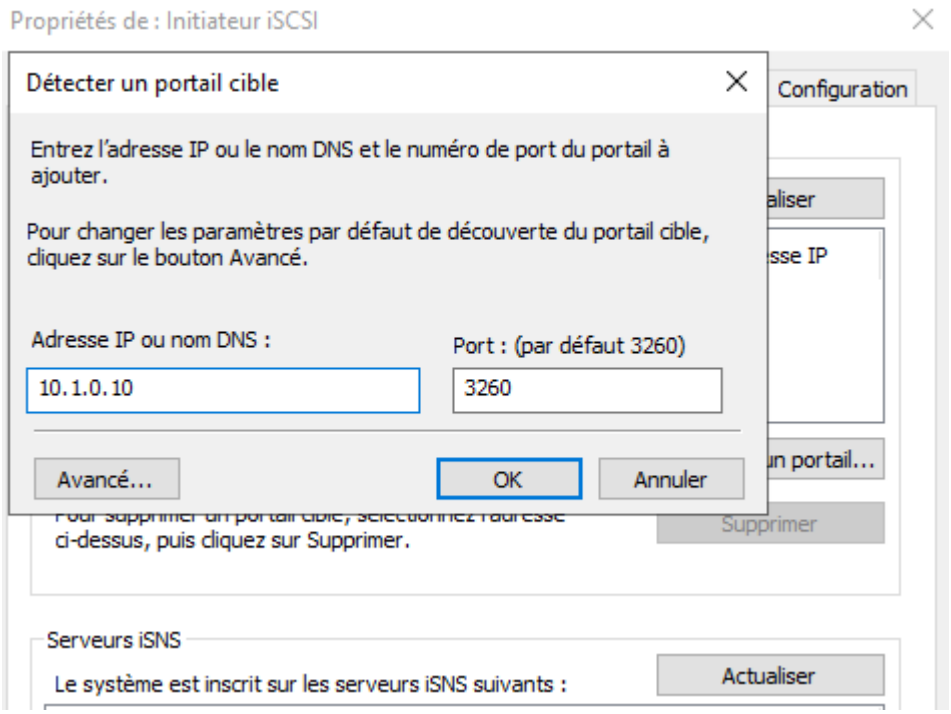
la configuration ip statique sera 10.1.0.10/24 avec une route par defaut à 10.1.0.24,nous allons verifier la connectivité entre le srv-ad-b2et le nas

```
PS C:\Users\Administrateur> ping 10.1.0.10

Envoi d'une requête 'Ping'  10.1.0.10 avec 32 octets de données :
Réponse de 10.1.0.10 : octets=32 temps=1 ms TTL=64
Réponse de 10.1.0.10 : octets=32 temps<1ms TTL=64
Réponse de 10.1.0.10 : octets=32 temps<1ms TTL=64
Réponse de 10.1.0.10 : octets=32 temps<1ms TTL=64

Statistiques Ping pour 10.1.0.10:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 0ms, Maximum = 1ms, Moyenne = 0ms
```

Figure 15: message echo ok

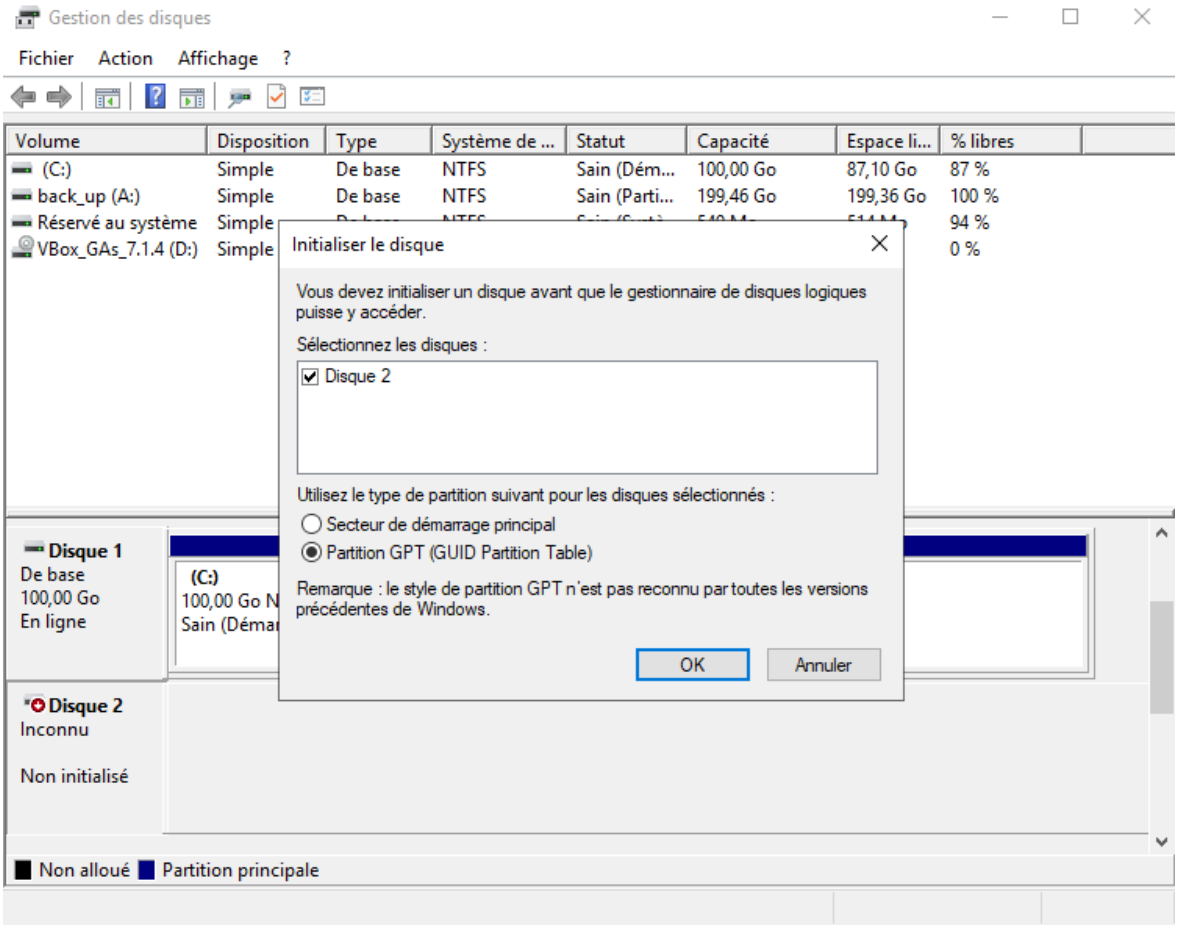
ATELIER ETP CHASSNEUILL

la configuration se fera en activant iSCSI avec la cmd iscsicpl puis en activant la decouverte avec saisie de l'adresse IP 10,1,0,10



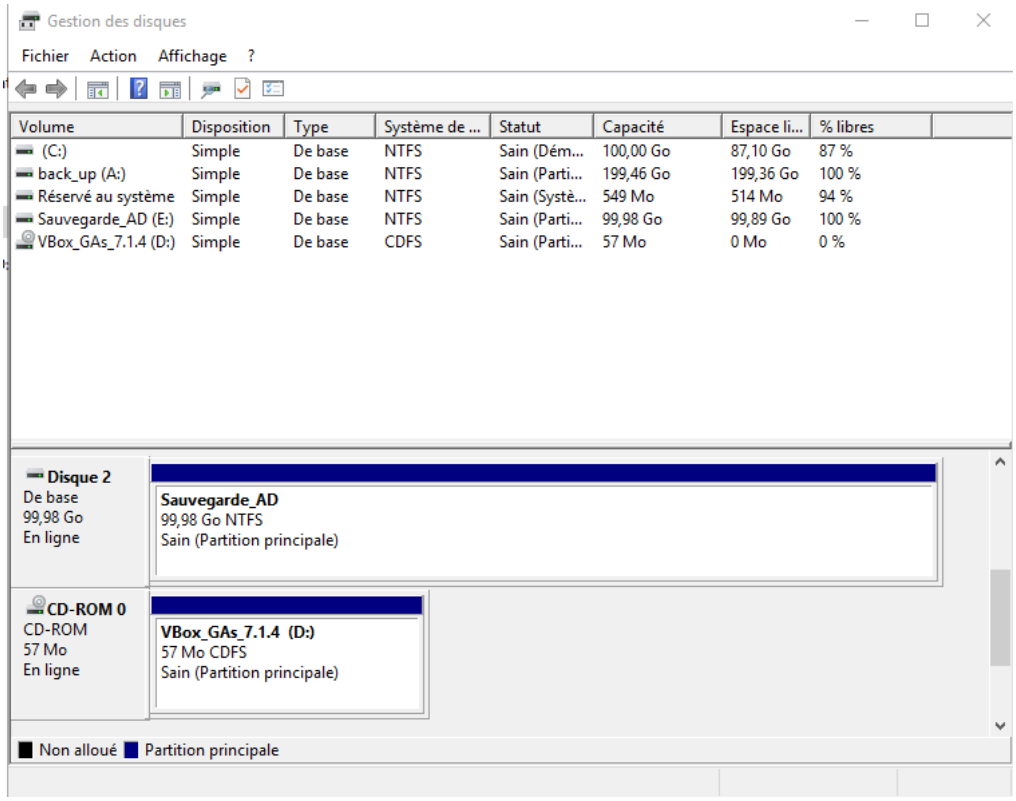
ATELIER ETP CHASSNEUILL

Initialisation du disque dans gestion des disques,on choisis GPT et on crée une nouvelle partition NTFS de sauvegarde_AD



La partition sauvegarde_AD est bien presente dans la gestion des disques windows

ATELIER ETP CHASSNEUILL



c)Mise en place de la sauvegarde de l'AD sur le iscsi

```
PS C:\Users\Administrateur> Install-WindowsFeature Windows-Server-Backup

Success Restart Needed Exit Code      Feature Result
------- -------------- ---------      --------------
True    No             Success        {Sauvegarde Windows Server}
```

```
PS C:\Users\Administrateur> wbadmin start systemstatebackup -backuptarget:E:
```

ATELIER ETP CHASSNEUILL

```
Voulez-vous démarrer l'opération de sauvegarde ?
[O] Oui [N] Non O

Création d'un cliché instantané des volumes spécifiés pour la sauvegarde...
Création d'un cliché instantané des volumes spécifiés pour la sauvegarde...
Création d'un cliché instantané des volumes spécifiés pour la sauvegarde...
Veuillez patienter le temps que les fichiers sur l'état du système à sauvegarder
soient identifiés. Cette opération peut prendre plusieurs minutes...
(250) fichiers trouvés.
(2922) fichiers trouvés.
(3880) fichiers trouvés.
(4674) fichiers trouvés.
(10360) fichiers trouvés.
(19872) fichiers trouvés.
(38512) fichiers trouvés.
(40519) fichiers trouvés.
(42681) fichiers trouvés.
(45074) fichiers trouvés.
```

La sauvegarde sur le disque E : a bien marché

On va planifier une sauvegarde automatique avec les commandes :
wbadmin enable backup `
-addtarget:E: `
-schedule:00:00 `
-include:systemstate `
-quiet

ATELIER ETP CHASSNEUILL

ATELIER ETP CHASSNEUILL

ATELIER ETP CHASSNEUILL

ATELIER ETP CHASSNEUILL

ATELIER ETP CHASSNEUILL

ATELIER ETP CHASSNEUILL

ATELIER ETP CHASSNEUILL

ATELIER ETP CHASSNEUILL

ATELIER ETP CHASSNEUILL

ATELIER ETP CHASSNEUILL

ATELIER ETP CHASSNEUILL

ATELIER ETP CHASSNEUILL

ATELIER ETP CHASSNEUILL

ATELIER ETP CHASSNEUILL

ATELIER ETP CHASSNEUILL

ATELIER ETP CHASSNEUILL

ATELIER ETP CHASSNEUILL

ATELIER ETP CHASSNEUILL

ATELIER ETP CHASSNEUILL

ATELIER ETP CHASSNEUILL

ATELIER ETP CHASSNEUILL

ATELIER ETP CHASSNEUILL

ATELIER ETP CHASSNEUILL

ATELIER ETP CHASSNEUILL

ATELIER ETP CHASSNEUILL

ATELIER ETP CHASSNEUILL

ATELIER ETP CHASSNEUILL

ATELIER ETP CHASSNEUILL

ATELIER ETP CHASSNEUILL

ATELIER ETP CHASSNEUILL

ATELIER ETP CHASSNEUILL

ATELIER ETP CHASSNEUILL