

12/11/2017

# Configuration Windows

Version 1.0 : Version Initiale

Fabien MAUHOURLAT  
[NOM DE LA SOCIETE]

## Configuration et Sécurisation du serveur Windows

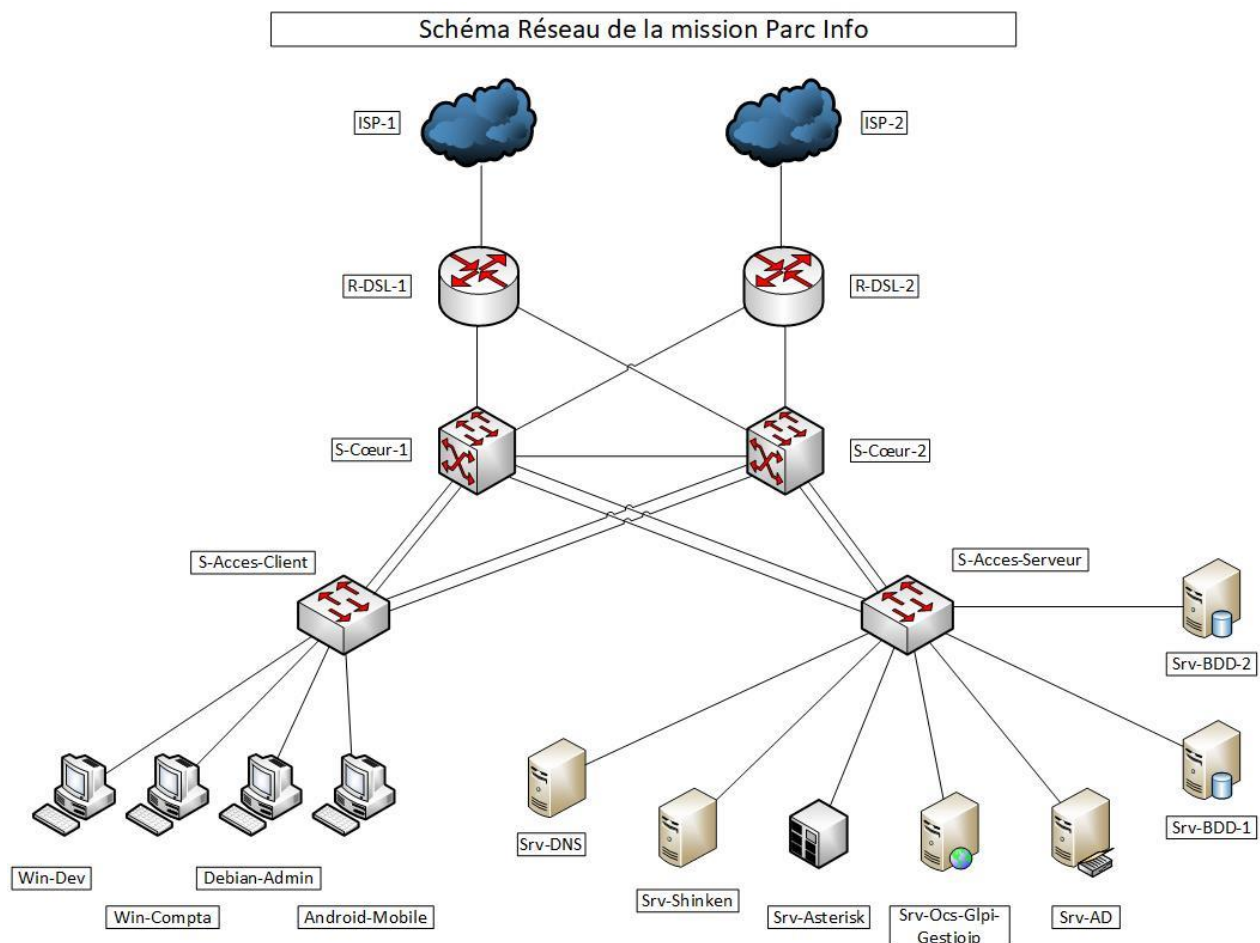
### Contexte :

L'infrastructure Windows est un élément essentiel de toute entreprise. C'est pour cela qu'il est nécessaire de mettre en place des mécanismes pour réduire la surface d'attaque d'un serveur active directory par exemple.

La mise en place du LDAPS est de la partie avec la configuration des logiciels comme OCS et GLPI pour s'authentifier avec ce protocole.

Un serveur Radius a également été mis en place pour sécuriser l'authentification et les autorisations des comptes sur les équipements d'interconnexion qui sont les points d'entrée des attaques.

### Voici l'architecture mise en place :



# Sommaire

- I. Présentation et choix des solutions
- II. Prérequis
- III. Configuration préalable du serveur
- IV. Création du domaine
- V. Intégration des clients au domaine
- VI. Installation de l'agent OCS sur les clients et serveur Windows
- VII. Configuration du service Radius pour authentifier les équipements réseau
- VIII. Configuration du LDAPS
- IX. Annexes

- I. Présentation et choix des solutions
- II. Prérequis
- III. Configuration préalable du serveur

## IV. Création du domaine

Configuration du serveur avec une adresse IP statique :

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

Général

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

☐ Obtenir une adresse IP automatiquement

☒ Utiliser l'adresse IP suivante :

Adresse IP : 192 . 168 . 10 . 235

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

Passerelle par défaut : 192 . 168 . 10 . 250

☐ Obtenir les adresses des serveurs DNS automatiquement

☒ Utiliser l'adresse de serveur DNS suivante :

Serveur DNS préféré : 127 . 0 . 0 . 1

Serveur DNS auxiliaire : . . .

☐ Valider les paramètres en quittant

Avancé...

OK Annuler

Création du domaine à l'aide du script PowerShell :

```

Powershell création Domaine AD.ps1 X
1  #
2  # Script Windows PowerShell pour le déploiement d'AD DS
3  #
4
5  Import-Module ADDSDeployment
6  Install-ADDSForest `
7  -CreateDnsDelegation:$false `
8  -DatabasePath "C:\Windows\NTDS" `
9  -DomainMode "Win2012R2" `
10 -DomainName "bora-bora.nc" `
11 -DomainNetbiosName "BORA-BORA" `
12 -ForestMode "Win2012R2" `
13 -InstallDns:$true `
14 -LogPath "C:\Windows\NTDS" `
15 -NoRebootOnCompletion:$false `
16 -SysvolPath "C:\Windows\SYSVOL" `
17 -Force:$true
18
19

```

Vérifier que le domaine a bien été créé avec la commande : Get-ADDomain bora-bora.nc

```

Administrateur : Windows PowerShell
Windows PowerShell
Copyright (C) 2014 Microsoft Corporation. Tous droits réservés.

PS C:\Users\Administrator> Get-ADDomain bora-bora.nc

AllowedDNSSuffixes      : {}
ChildDomains            : {}
ComputersContainer      : CN=Computers,DC=bora-bora,DC=nc
DeletedObjectsContainer : CN=Deleted Objects,DC=bora-bora,DC=nc
DistinguishedName       : DC=bora-bora,DC=nc
DNSRoot                 : bora-bora.nc
DomainControllersContainer : OU=Domain Controllers,DC=bora-bora,DC=nc
DomainMode              : Windows2012R2Domain
DomainSID                : S-1-5-21-2786526758-1110624492-1588176222
ForeignSecurityPrincipalsContainer : CN=ForeignSecurityPrincipals,DC=bora-bora,DC=nc
Forest                  : bora-bora.nc
InfrastructureMaster     : WIN-KOERN5IEE1U.bora-bora.nc
LastLogonReplicationInterval : 
LinkedGroupPolicyObjects : {CN={31B2F340-016D-11D2-945F-00C04FB984F9},CN=Policies,CN=System,DC=bora-bora,DC=nc}
LostAndFoundContainer   : CN=LostAndFound,DC=bora-bora,DC=nc
ManagedBy              : 
Name                     : bora-bora
NetBIOSName             : BORA-BORA
ObjectClass              : domainDNS
ObjectGUID              : 81e25a14-4e3e-4dd3-bbe6-78bf7fe8811b
ParentDomain            : 
PDCEmulator             : WIN-KOERN5IEE1U.bora-bora.nc
QuotasContainer         : CN=NTDS Quotas,DC=bora-bora,DC=nc
ReadOnlyReplicaDirectoryServers : {}
ReplicaDirectoryServers : {WIN-KOERN5IEE1U.bora-bora.nc}
RIDMaster               : WIN-KOERN5IEE1U.bora-bora.nc
SubordinateReferences   : {DC=ForestDnsZones,DC=bora-bora,DC=nc, DC=DomainDnsZones,DC=bora-bora,DC=nc, CN=Configuration,DC=bora-bora,DC=nc}
SystemsContainer        : CN=System,DC=bora-bora,DC=nc
UsersContainer           : CN=Users,DC=bora-bora,DC=nc

PS C:\Users\Administrator>

```

Création des unités d'organisation :

- Compta, Administrateur, Compte-service et Mobilité

```

PS C:\Users\Administrator> New-ADOrganizationalUnit "Comptabilite"
PS C:\Users\Administrator> New-ADOrganizationalUnit "Administrateur"
PS C:\Users\Administrator> New-ADOrganizationalUnit "Compte-Service"
PS C:\Users\Administrator> New-ADOrganizationalUnit "Mobilité"
PS C:\Users\Administrator>

```

Lister les unités d'organisation du domaine avec la commande Get-ADOrganizationalUnit :

```

PS C:\Users\Administrator> Get-ADOrganizationalUnit -Filter * -SearchBase "DC=bora-bora,DC=nc" | select Name

Name
----
Domain Controllers
Developpeur
Comptabilite
Administrateur
Compte-Service
Mobilité

PS C:\Users\Administrator>

```

Création des utilisateurs en PowerShell avec la commande New-ADUser :

- Name
- SamAccountName
- UserPrincipalName
- Enable
- Path
- AccountPassword

New-ADUser -Name "Fabien Mauhourat" -SamAccountName "fmauhourat" -GivenName "Fabien" -Surname "Mauhourat" -DisplayName "Fabien Mht" -UserPrincipalName "fmauhourat@dom-test.local" -Enabled \$true -Path "OU=Users,DC=dom-test,DC=local" -AccountPassword (ConvertTo-SecureString "Admin2017" -AsPlainText -Force)

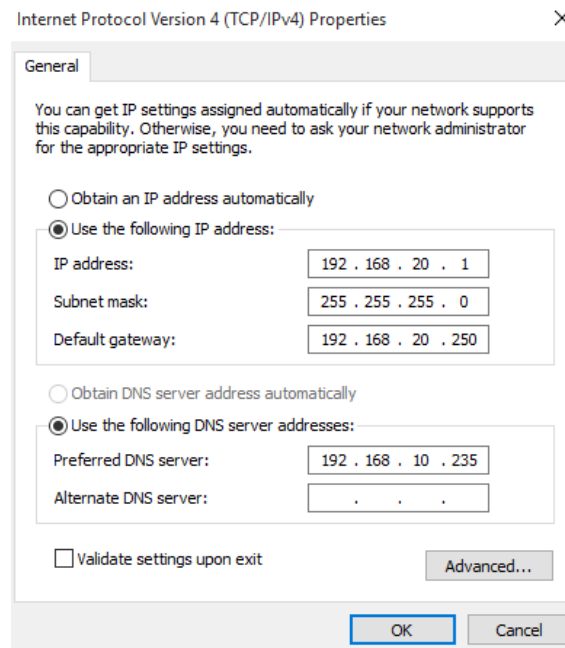
```
PS C:\Users\Administrator> New-ADUser -Name "Fabien Mauhourat" -SamAccountName "fmauhourat" -GivenName "Fabien" -Surname
"Mauhourat" -DisplayName "Fabien Mauhourat" -UserPrincipalName "fmauhourat@bora-bora.nc" -Enabled $true -Path "OU=Admin
istrateur,DC=bora-bora,DC=nc" -AccountPassword (ConvertTo-SecureString "Toor124588*" -AsPlainText -Force)
PS C:\Users\Administrator>
PS C:\Users\Administrator> Get-ADUser -filter * -SearchBase "OU=Administrateur,DC=bora-bora,DC=nc"

DistinguishedName : CN=Fabien Mauhourat,OU=Administrateur,DC=bora-bora,DC=nc
Enabled           : True
GivenName        : Fabien
Name             : Fabien Mauhourat
ObjectClass      : user
ObjectGUID       : 45032196-5a40-444d-a0b4-7865e3e8b875
SamAccountName   : fmauhourat
SID              : S-1-5-21-2786526758-1110624492-1588176222-1105
Surname          : Mauhourat
UserPrincipalName : fmauhourat@bora-bora.nc

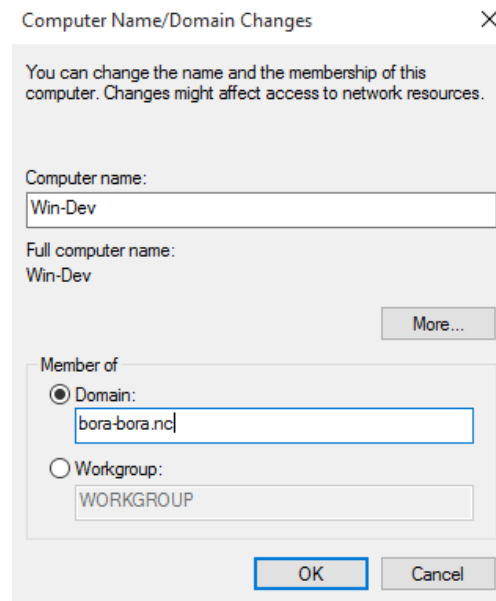
PS C:\Users\Administrator>
```

## V. Intégration des clients au domaine

Il faut configurer le Dns des clients pour qu'il pointe sur le serveur Active Directory :



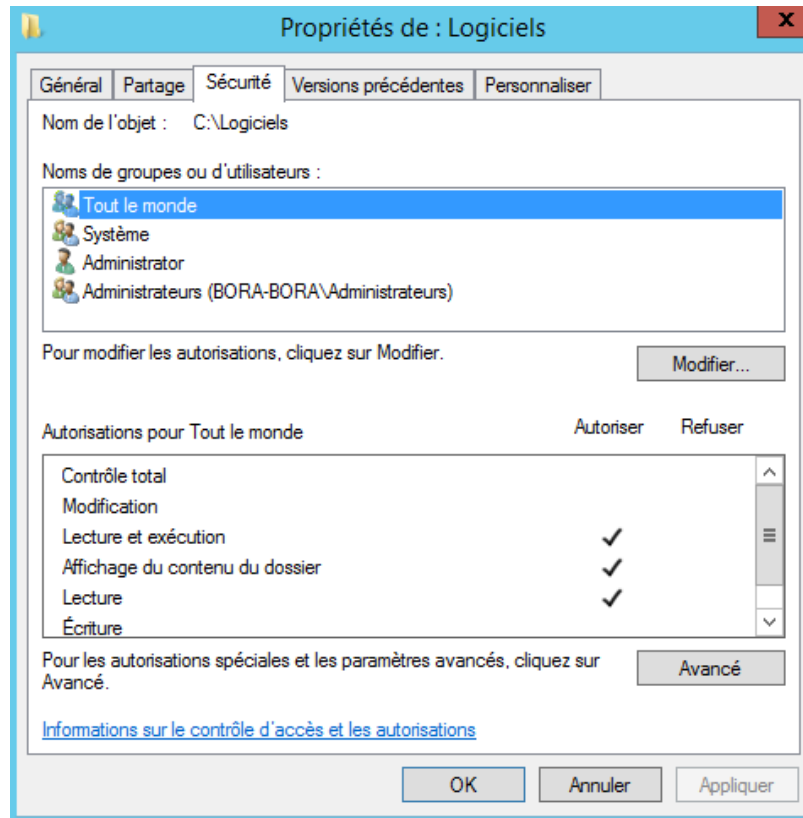
Ensuite Intégrer les clients au domaine :





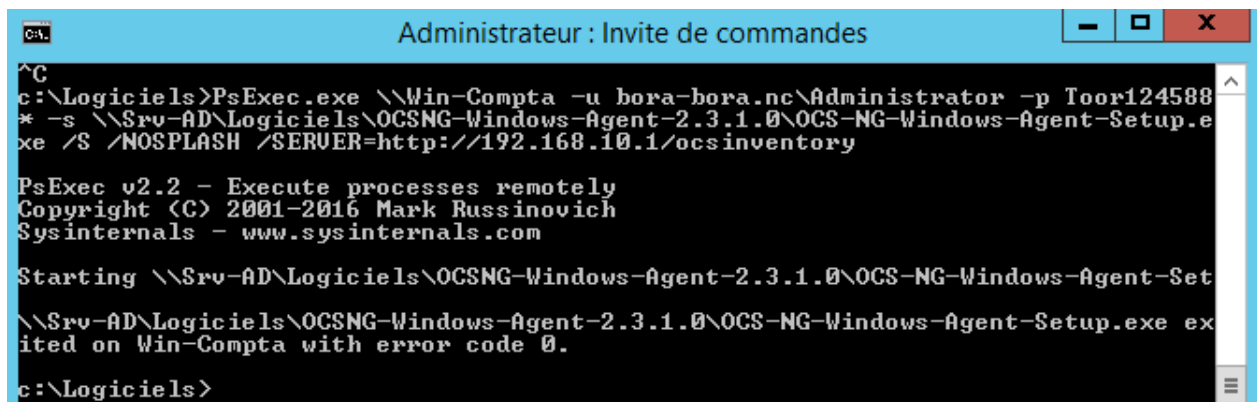
## VI. Installation de l'agent OCS sur les clients et serveur Windows

Créer un partage avec les droits de lecture pour tout le monde :



Ensuite grâce à la commande Psexec qui permet d'exécuter des commandes à distance sur des postes Windows on peut déployer l'agent automatiquement sur une ou plusieurs machines :

```
psexec \\COMPUTER_NAME -s \\Server\NetLogon\OCS-NG-Windows-Agent-Setup.exe /S /NOSPLASH /SERVER=http://my\_ocs\_server/ocsinventory
```



<https://wiki.ocsinventory-ng.org/index.php?title=Documentation:DeployTool>

<https://wiki.ocsinventory-ng.org/index.php?title=Documentation:WindowsAgent/fr>

Vérification du fichier de configuration d'OCS :

```

ocsinventory.ini - Notepad
File Edit Format View Help

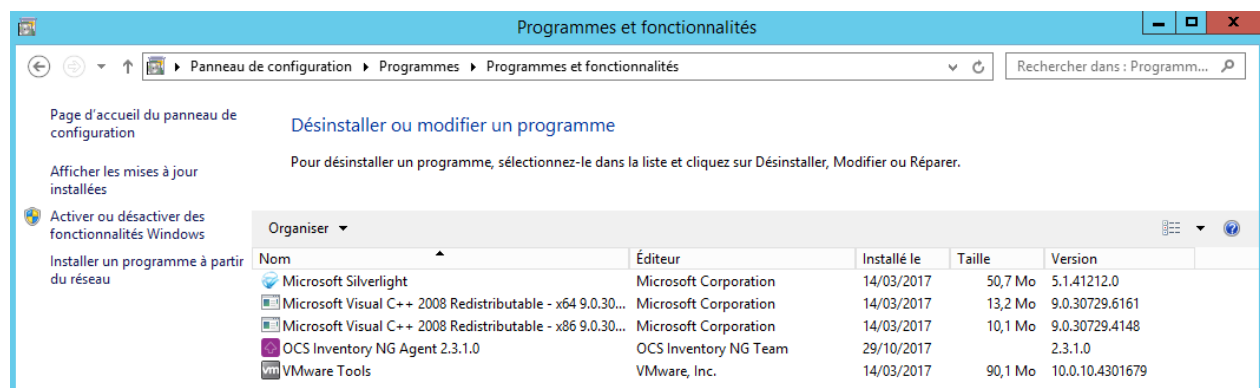
[OCS Inventory Agent]
ComProvider=ComHTTP.dll
Debug=0
Local=
NoSoftware=0
HKCU=0
NoTAG=0
IpDisc=
[HTTP]
Server=http://192.168.10.1/ocsinventory
SSL=1
CaBundle=cacert.pem
AuthRequired=0
User=
Pwd=
ProxyType=0
Proxy=
ProxyPort=0
ProxyAuthRequired=0
ProxyUser=
ProxyPwd=
[OCS Inventory Service]
TTO_WAIT=120
INVENTORY_ON_STARTUP=0
  
```

Installation de l'agent sur le serveur Windows 2012 r2 :

```

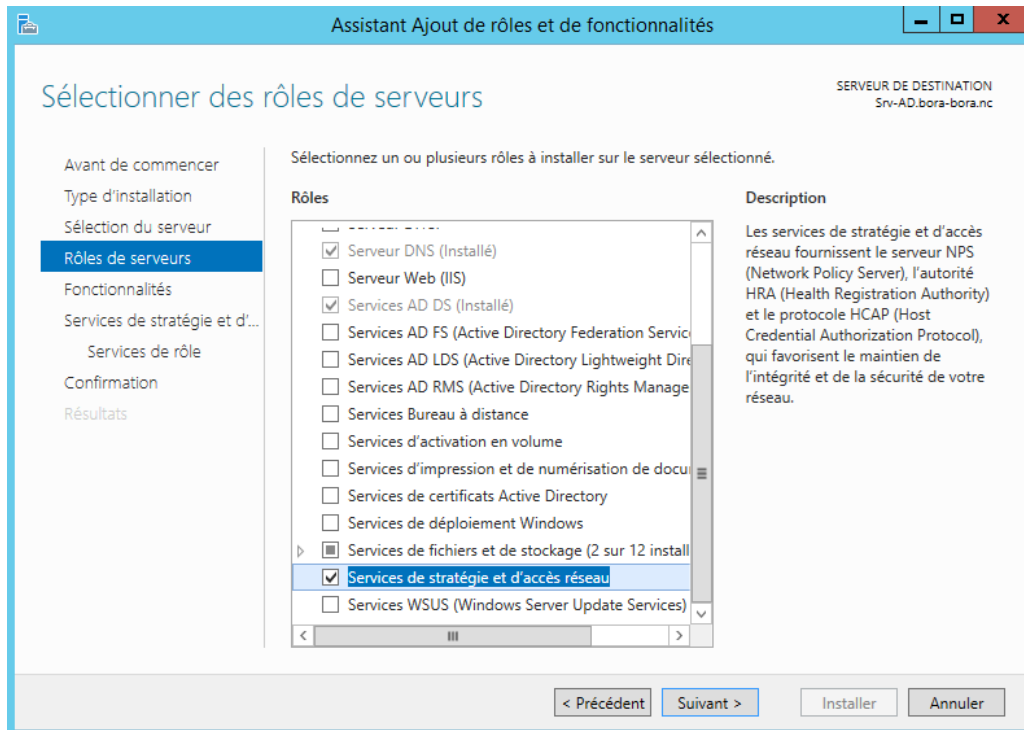
c:\Logiciels>start C:\Logiciels\OCSNG-Windows-Agent-2.3.1.0\OCS-NG-Windows-Agent-Setup.exe /S /NOSPLASH /SERVER=http://192.168.10.1/ocsinventory
c:\Logiciels>
  
```

L'agent OCS a bien été installé :

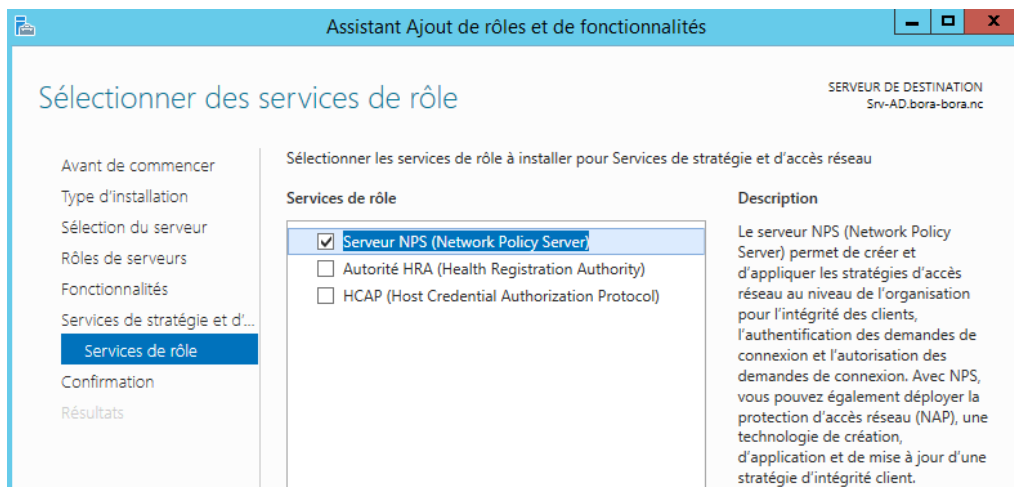


## VII. Configuration du service Radius pour authentifier les équipements réseau

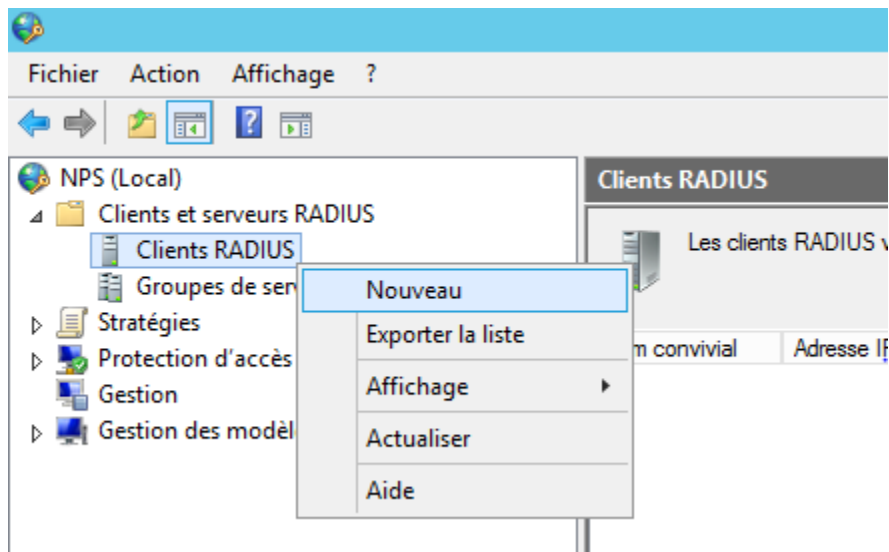
Installer le rôle Stratégies et d'accès réseau :



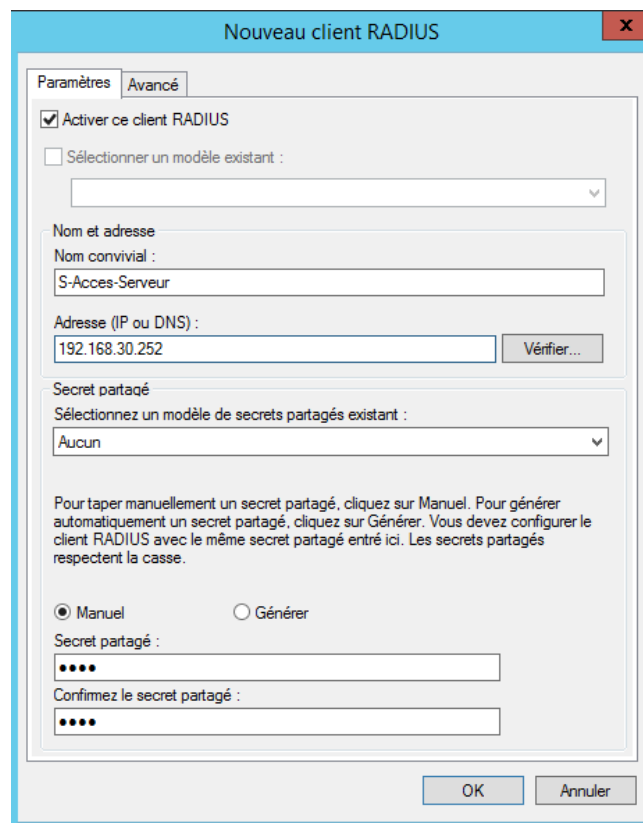
Ensuite cochez NPS pour installer Radius :



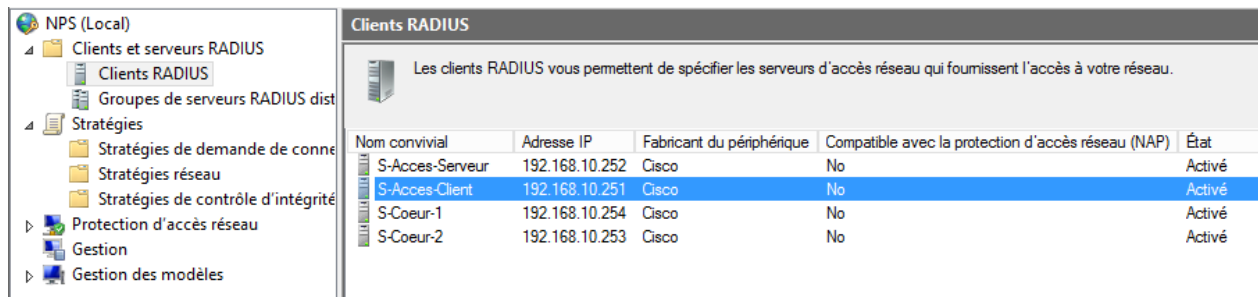
Une fois radius installé il suffit de créer de nouveaux clients :



Entrer l'adresse IP du client radius puis son nom et définissez un secret partagé :

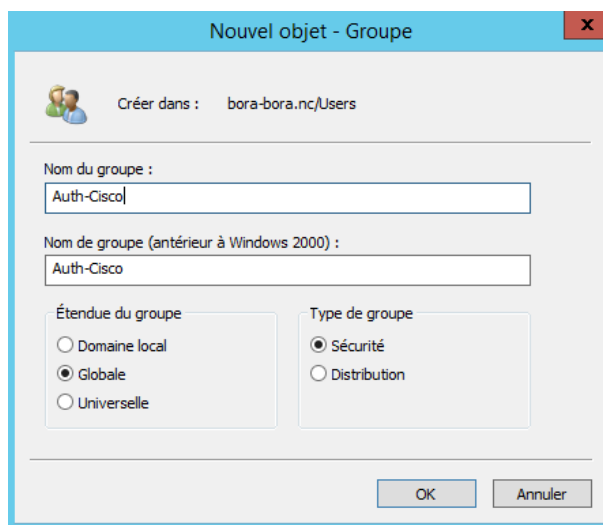


Dans l'onglet client radius, un récapitulatif des clients définis :



Nom convivial	Adresse IP	Fabricant du périphérique	Compatible avec la protection d'accès réseau (NAP)	État
S-Access-Serveur	192.168.10.252	Cisco	No	Activé
S-Access-Client	192.168.10.251	Cisco	No	Activé
S-Coeur-1	192.168.10.254	Cisco	No	Activé
S-Coeur-2	192.168.10.253	Cisco	No	Activé

Créer ensuite un ou plusieurs groupes pour donner les niveaux de privilèges différents en fonction des utilisateurs :



Nouvel objet - Groupe

Créer dans : bora-bora.nc/Users

Nom du groupe :  
Auth-Cisco

Nom de groupe (antérieur à Windows 2000) :  
Auth-Cisco

Étendue du groupe

☐ Domaine local

☒ Globale

☐ Universelle

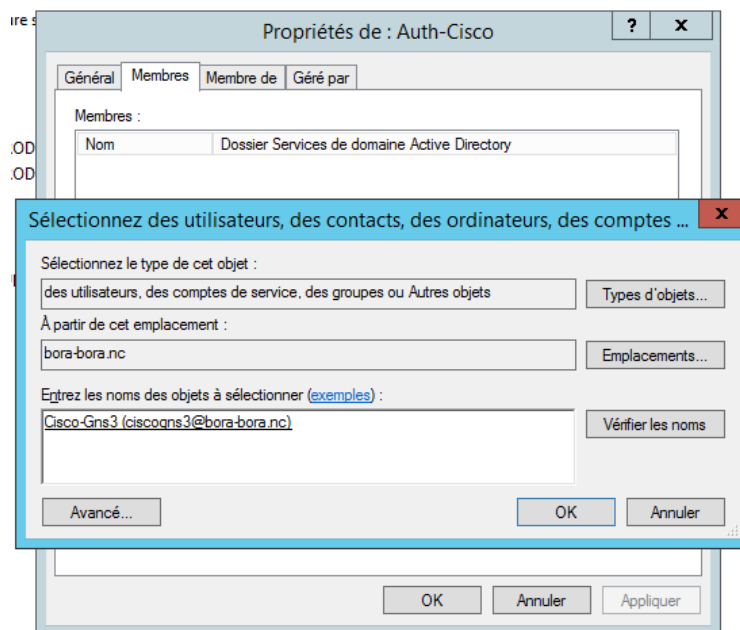
Type de groupe

☒ Sécurité

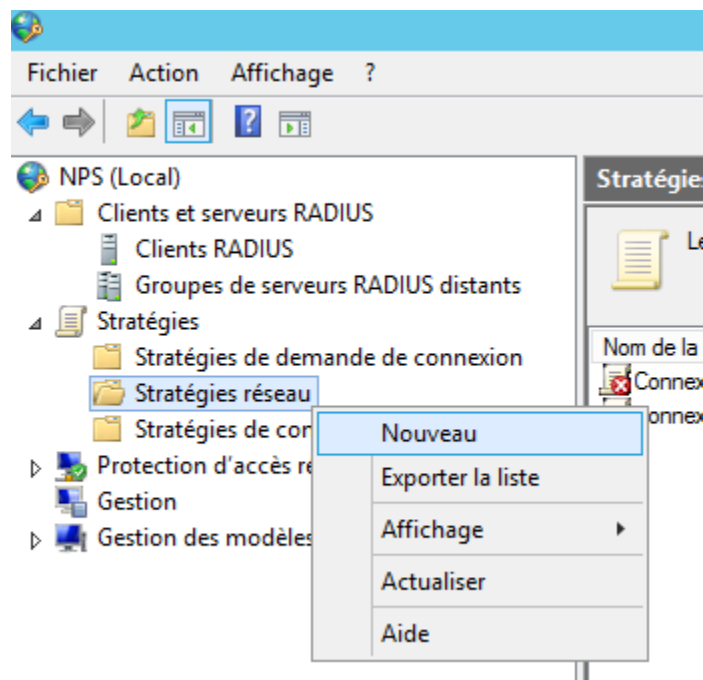
☐ Distribution

OK Annuler

Ensuite ajouter les utilisateurs au bon groupes :



Créer ensuite une nouvelle stratégies réseau :



Nommer cette stratégie :

**Nouvelle stratégie réseau**

**Spécifier le nom de la stratégie réseau et le type de connexion**

Vous pouvez spécifier le nom de votre stratégie réseau ainsi que le type des connexions auxquelles la stratégie s'applique.

**Nom de la stratégie :**

Authentification cisco

**Méthode de connexion réseau**

Sélectionnez le type de serveur d'accès réseau qui envoie la demande de connexion au serveur NPS. Vous pouvez sélectionner une valeur dans Type de serveur d'accès réseau ou bien Spécifique au fournisseur, mais ces paramètres ne sont pas obligatoires. Si votre serveur d'accès réseau est un commutateur d'authentification ou un point d'accès sans fil 802.1X, sélectionnez Non spécifié.

☒ Type de serveur d'accès réseau :

Non spécifié

☐ Spécifique au fournisseur :

10

Choisissez ensuite les groupes windows comme condition :

**Sélectionner une condition**

Sélectionnez une condition, puis cliquez sur Ajouter.

**Groupes**

**Groupes Windows**  
La condition Groupes Windows spécifie que l'utilisateur ou l'ordinateur qui tente d'établir la connexion doit appartenir à l'un des groupes sélectionnés.

**Groupes d'ordinateurs**  
La condition Groupes d'ordinateurs spécifie que l'ordinateur qui tente d'établir la connexion doit appartenir à l'un des groupes sélectionnés.

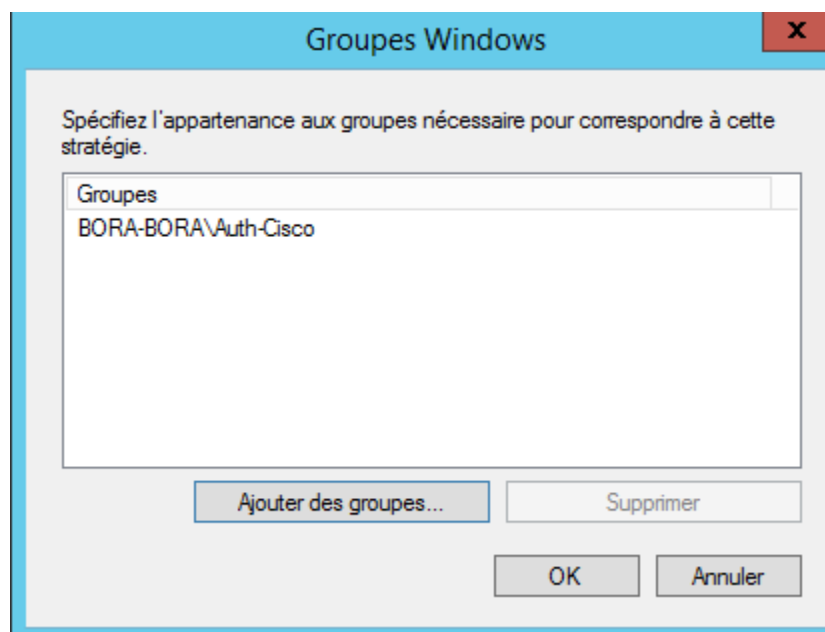
**Groupes d'utilisateurs**  
La condition Groupes d'utilisateurs spécifie que l'utilisateur qui tente d'établir la connexion doit appartenir à l'un des groupes sélectionnés.

**HCAP**

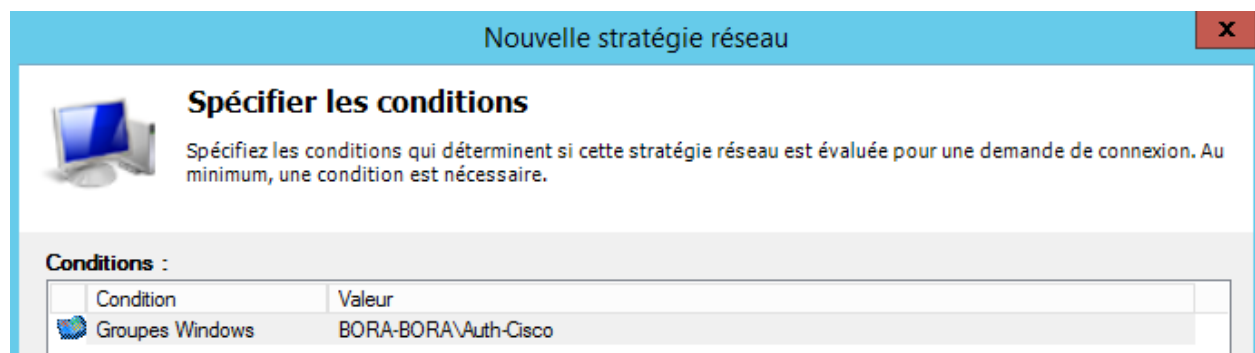
**Groupes d'emplacements**  
La condition Groupes d'emplacements HCAP spécifie les groupes d'emplacements HCAP (Host Credential Authorization Protocol) nécessaires pour correspondre à cette stratégie. Le protocole HCAP sert à la communication entre le serveur NPS et des serveurs NAS tiers. Consultez la documentation de votre serveur NAS avant d'utiliser.

Ajouter... Annuler

Ajouter les groupes windows :

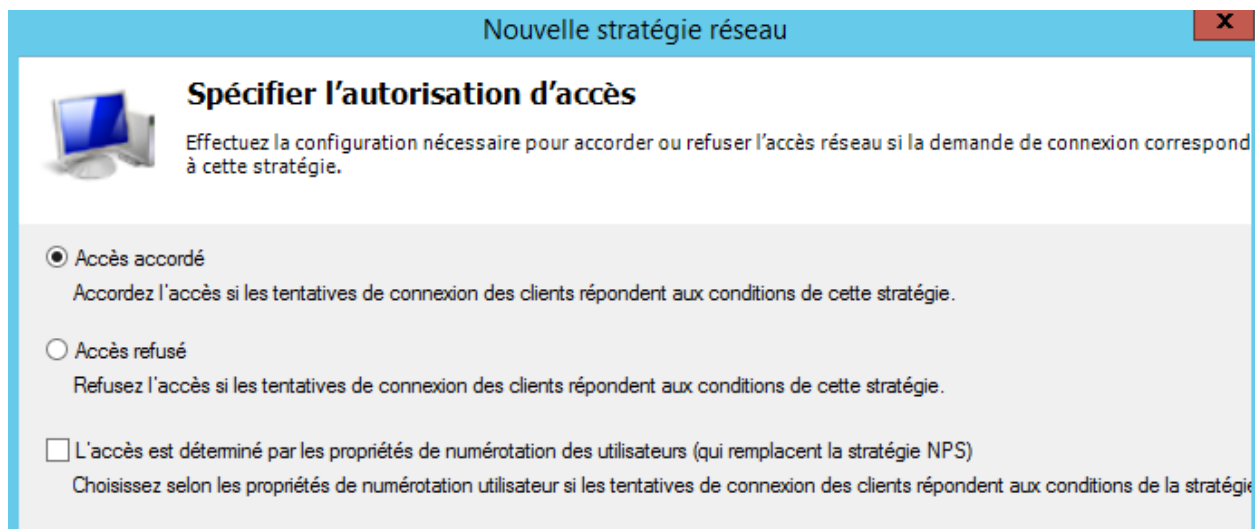


Récapitulatif :





Ensuite il faut accorder l'accès :



**Nouvelle stratégie réseau**

**Spécifier l'autorisation d'accès**

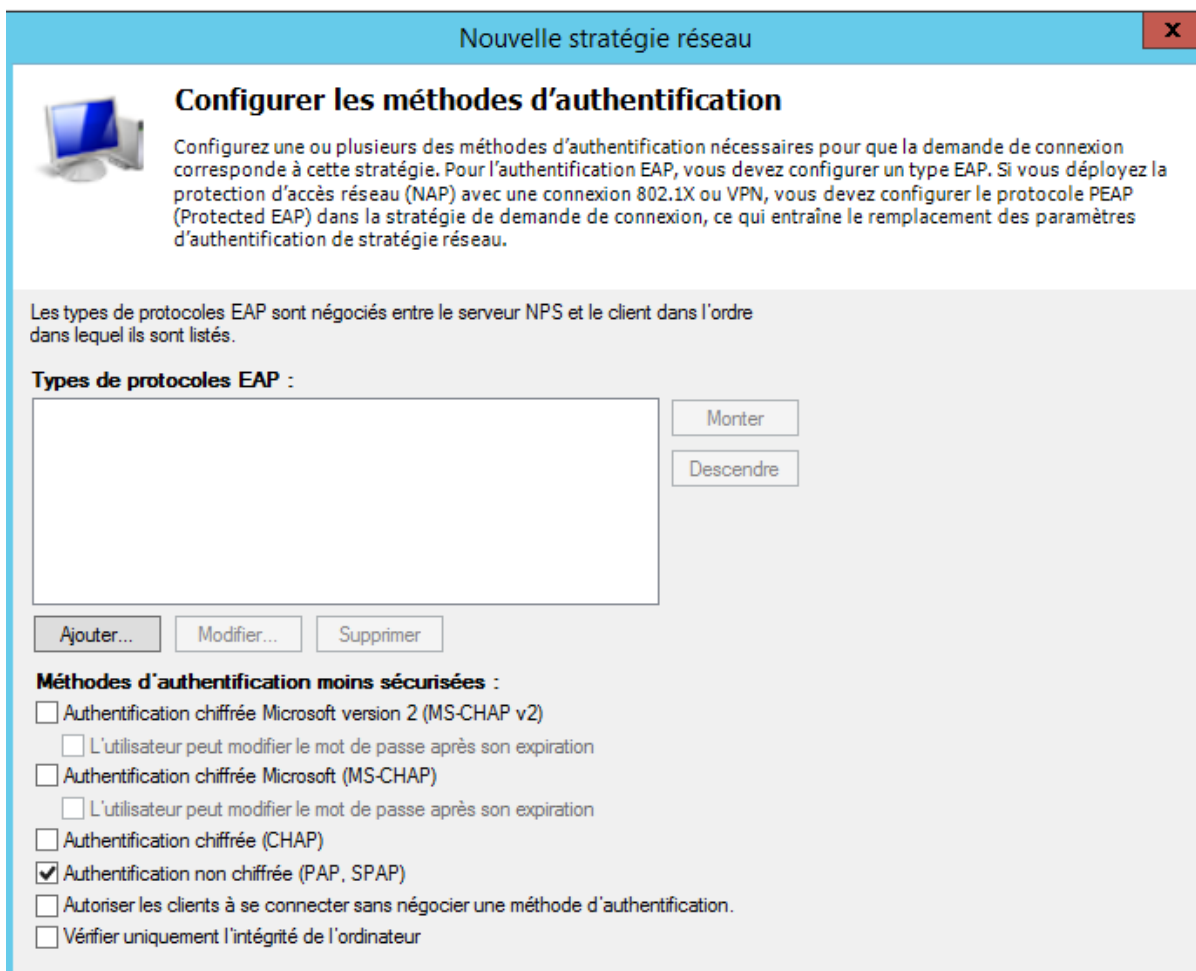
Effectuez la configuration nécessaire pour accorder ou refuser l'accès réseau si la demande de connexion correspond à cette stratégie.

☒ Accès accordé  
Accordez l'accès si les tentatives de connexion des clients répondent aux conditions de cette stratégie.

☐ Accès refusé  
Refusez l'accès si les tentatives de connexion des clients répondent aux conditions de cette stratégie.

☐ L'accès est déterminé par les propriétés de numérotation des utilisateurs (qui remplacent la stratégie NPS)  
Choisissez selon les propriétés de numérotation utilisateur si les tentatives de connexion des clients répondent aux conditions de la stratégie

Concernant les méthode d'authentification il faut tout décocher et choisir authentification non chiffré :



**Nouvelle stratégie réseau**

**Configurer les méthodes d'authentification**

Configurez une ou plusieurs des méthodes d'authentification nécessaires pour que la demande de connexion corresponde à cette stratégie. Pour l'authentification EAP, vous devez configurer un type EAP. Si vous déployez la protection d'accès réseau (NAP) avec une connexion 802.1X ou VPN, vous devez configurer le protocole PEAP (Protected EAP) dans la stratégie de demande de connexion, ce qui entraîne le remplacement des paramètres d'authentification de stratégie réseau.

Les types de protocoles EAP sont négociés entre le serveur NPS et le client dans l'ordre dans lequel ils sont listés.

**Types de protocoles EAP :**

[Liste vide]

Monter  
Descendre

Ajouter... Modifier... Supprimer

**Méthodes d'authentification moins sécurisées :**

☐ Authentification chiffrée Microsoft version 2 (MS-CHAP v2)  
☐ L'utilisateur peut modifier le mot de passe après son expiration

☐ Authentification chiffrée Microsoft (MS-CHAP)  
☐ L'utilisateur peut modifier le mot de passe après son expiration

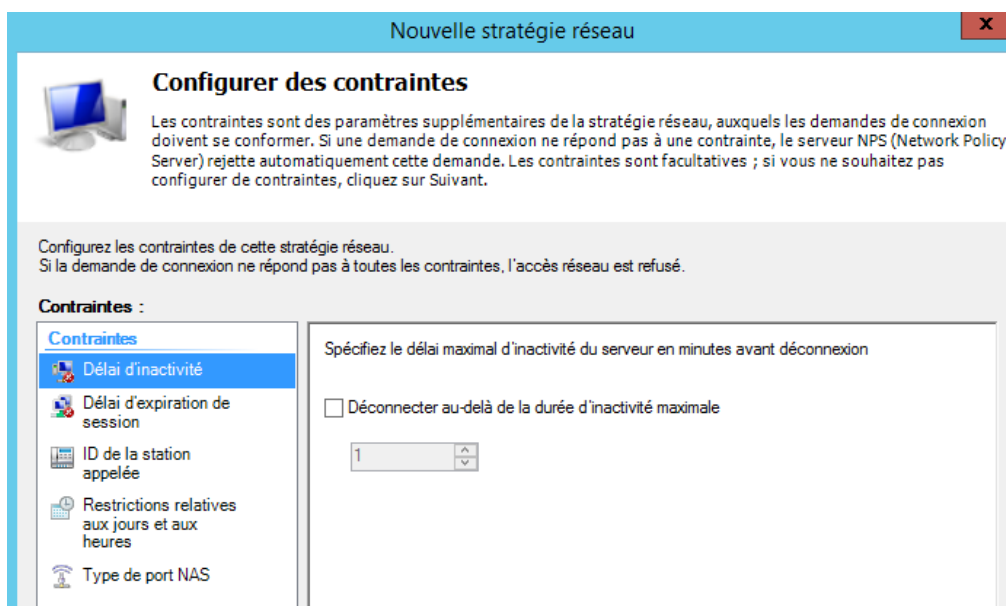
☐ Authentification chiffrée (CHAP)

☒ Authentification non chiffrée (PAP, SPAP)

☐ Autoriser les clients à se connecter sans négocier une méthode d'authentification.

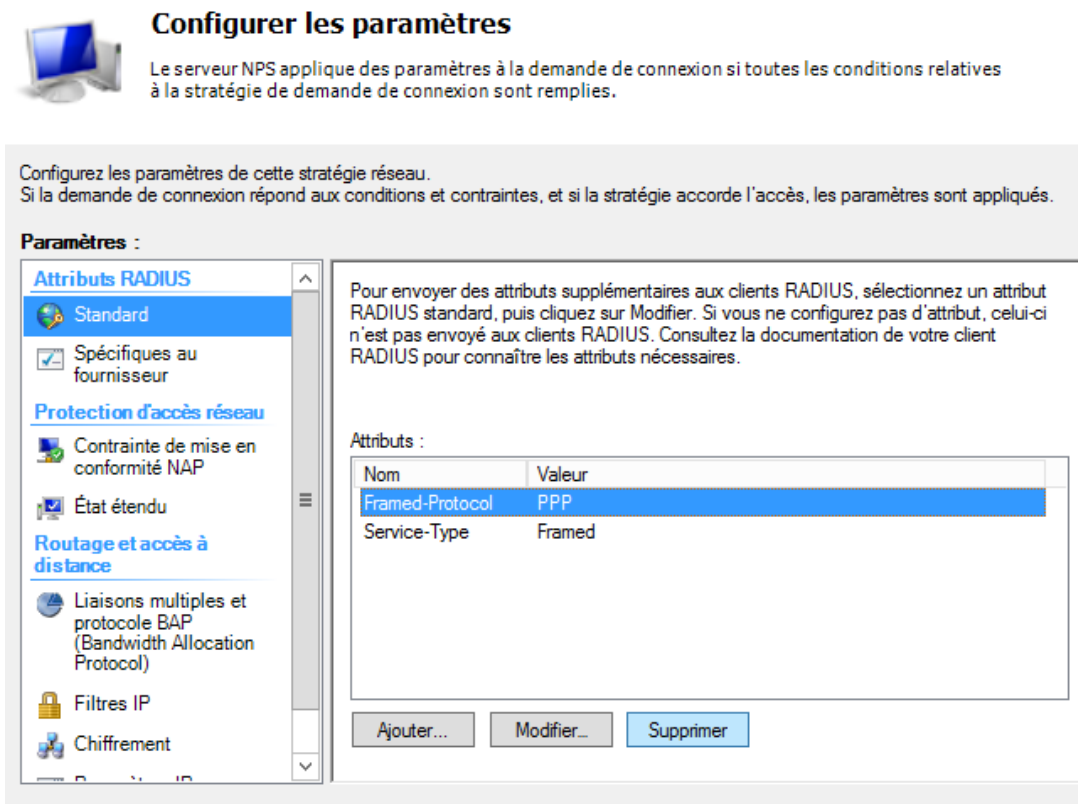
☐ Vérifier uniquement l'intégrité de l'ordinateur

Concernant les contraintes les laisser par défaut :



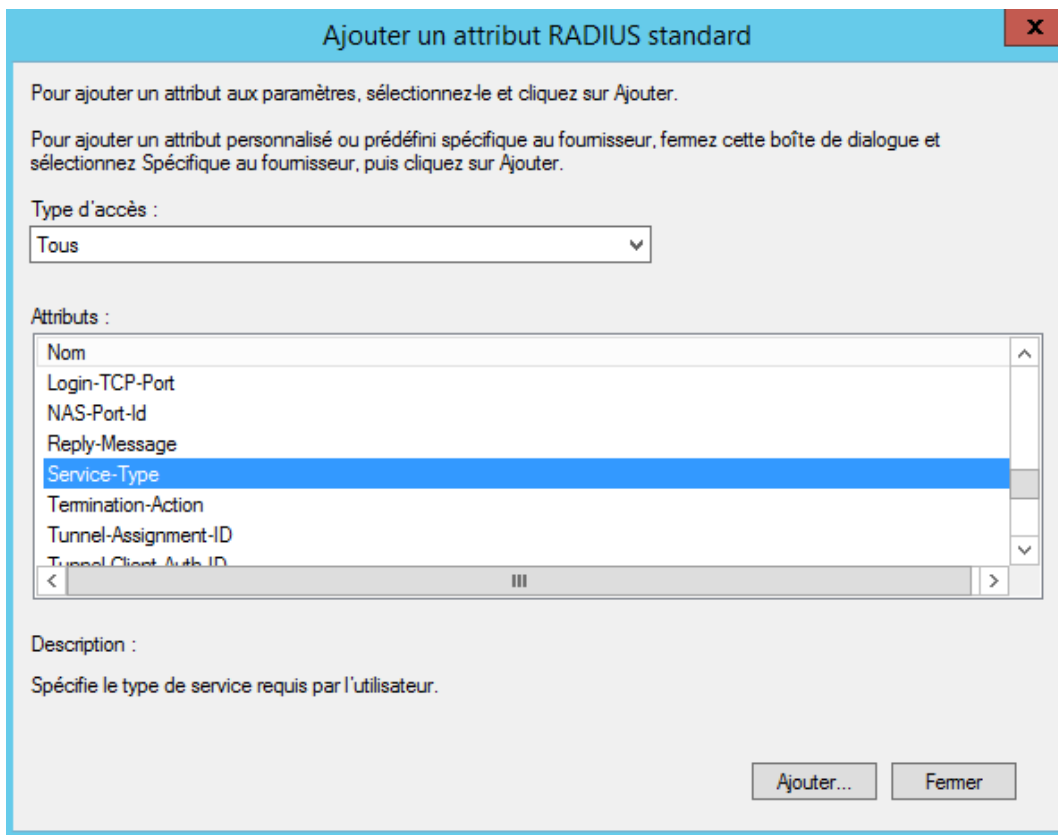
Dans les paramètres il faut supprimer les deux attributs standards :

- Frame-Protocol et service-type



Créer ensuite un nouvel attribut standard :

➤ Service-Type



Ajouter un attribut RADIUS standard

Pour ajouter un attribut aux paramètres, sélectionnez-le et cliquez sur Ajouter.

Pour ajouter un attribut personnalisé ou prédéfini spécifique au fournisseur, fermez cette boîte de dialogue et sélectionnez Spécifique au fournisseur, puis cliquez sur Ajouter.

Type d'accès :  
Tous

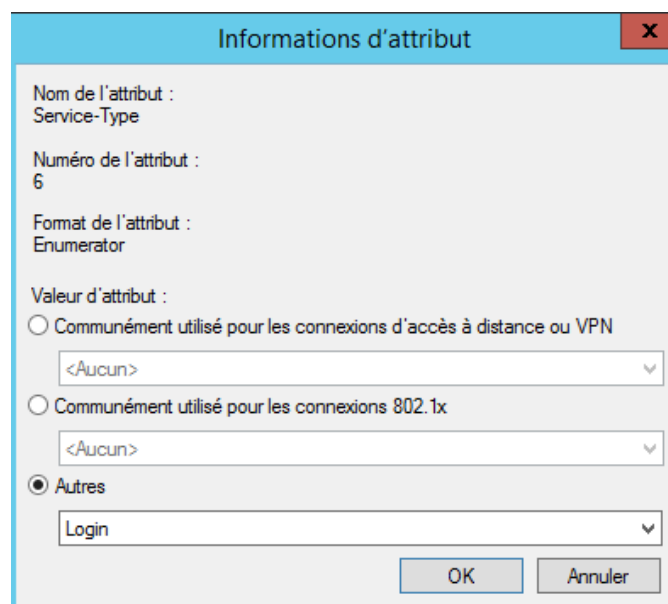
Attributs :

Nom
Login-TCP-Port
NAS-Port-Id
Reply-Message
<b>Service-Type</b>
Termination-Action
Tunnel-Assignment-ID
Tunnel-Client-Auth-ID

Description :  
Spécifie le type de service requis par l'utilisateur.

Ajouter... Fermer

Modifier ensuite l'attribut et spécifier dans la catégorie autres la mention Login :



Informations d'attribut

Nom de l'attribut :  
Service-Type

Numéro de l'attribut :  
6

Format de l'attribut :  
Enumerator

Valeur d'attribut :

☐ Communément utilisé pour les connexions d'accès à distance ou VPN  
<Aucun>

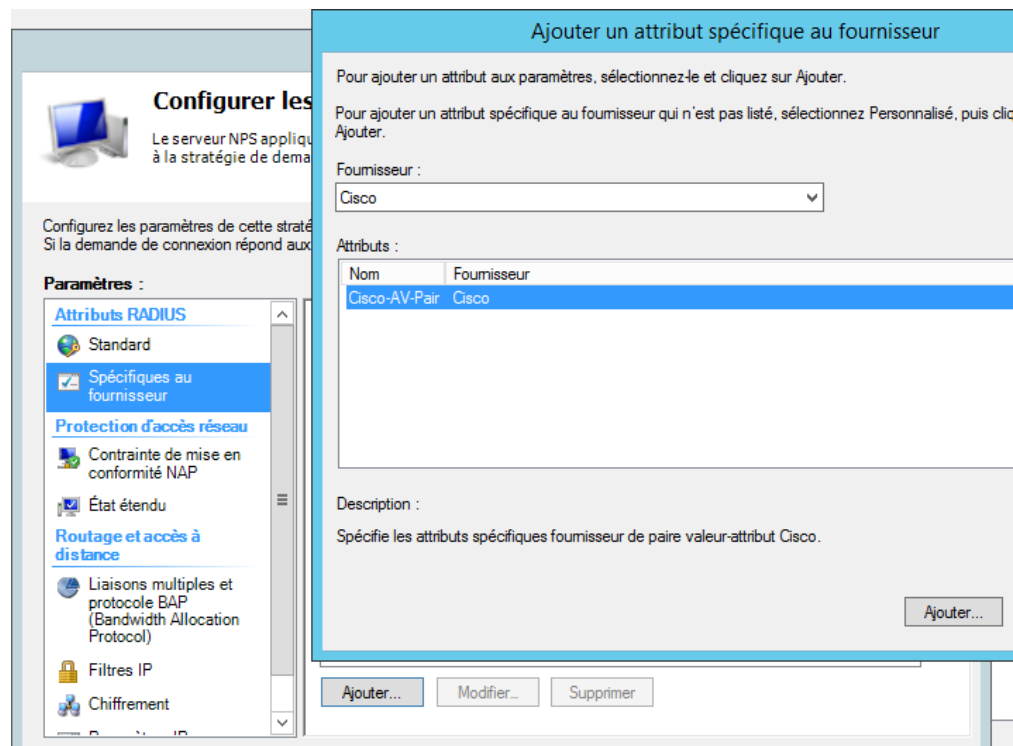
☐ Communément utilisé pour les connexions 802.1x  
<Aucun>

☒ Autres  
Login

OK Annuler

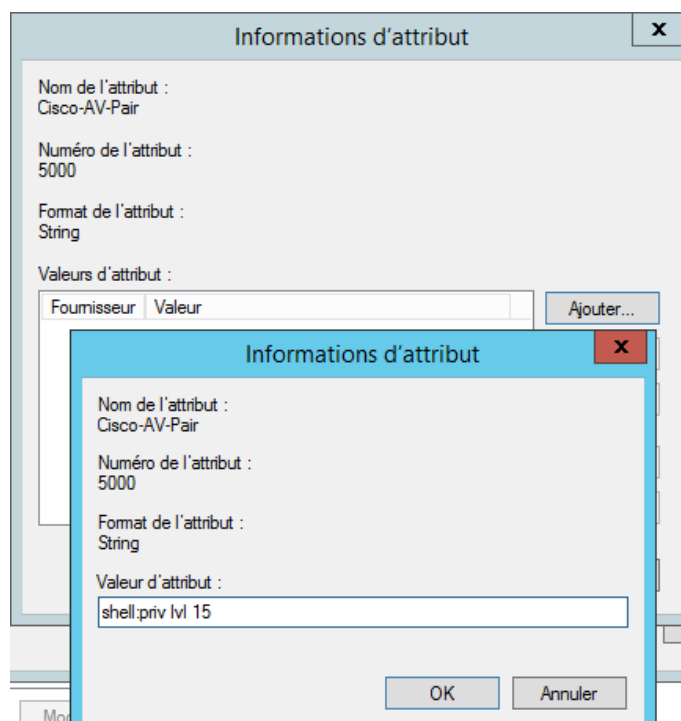
Dans l'onglet spécifique au fournisseur créer un nouvel attribut :

- Choisir Cisco



Dans les paramètres de l'attribut créer une nouvelle valeur :

- Shell :priv-lvl=15





## Configurer les paramètres

Le serveur NPS applique des paramètres à la demande de connexion si toutes les conditions relatives à la stratégie de demande de connexion sont remplies.

Configurez les paramètres de cette stratégie réseau.

Si la demande de connexion répond aux conditions et contraintes, et si la stratégie accorde l'accès, les paramètres sont appliqués.

### Paramètres :

#### Attributs RADIUS

Standard

Spécifiques au fournisseur

#### Protection d'accès réseau

Contrainte de mise en conformité NAP

État étendu

Pour envoyer des attributs supplémentaires aux clients RADIUS, sélectionnez un attribut spécifique au fournisseur, puis cliquez sur Modifier. Si vous ne configurez pas d'attribut, celui-ci n'est pas envoyé aux clients RADIUS. Consultez la documentation de votre client RADIUS pour connaître les attributs nécessaires.

#### Attributs :

Nom	Fournisseur	Valeur
Cisco-AV-Pair	Cisco	shell:priv lvl 15

Vérifier les paramètres de la stratégies réseau et valider :

Nouvelle stratégie réseau X

### Fin de la configuration de la nouvelle stratégie réseau

Vous avez correctement créé la stratégie réseau suivante :

**Authentification cisco**

**Conditions de la stratégie :**

Condition	Valeur
Groupes Windows	BORA-BORA\Auth-Cisco

**Paramètres de la stratégie :**

Condition	Valeur
Méthode d'authentification	Authentification non chiffrée (PAP, SPAP)
Autorisation d'accès	Accorder l'accès
Mettre à jour les clients non conformes	Vrai
Contrainte de mise en conformité NAP	Autoriser un accès réseau complet
Ignorer les propriétés de numérotation des utilisateurs	Faux
Service-Type	Login

Pour fermer cet Assistant, cliquez sur Terminer.

Dans l'exemple deux stratégies réseau ont été déployé :

- La première pour les membre du groupe administrateur : attribut shell :priv-lvl=15
- La deuxième pour ceux qui auront un accès en lecture seul : attribut shell :priv-lvl=1

**Stratégies réseau**

Les stratégies réseau vous permettent d'autoriser les connexions au réseau de manière sélective, et d'indiquer les circonstances dans lesquelles ces connexions peuvent s'effectuer ou non.

Nom de la stratégie	État	Ordre de traitement	Type d'accès	Source
Authentification cisco Admin	Activé	1	Accorder l'accès	Non spécifié
Authentification cisco Read Only	Activé	2	Accorder l'accès	Non spécifié
Connexions au serveur Microsoft de Routage et Accès distants	Activé	999998	Refuser l'accès	Non spécifié
Connexions à d'autres serveurs d'accès	Activé	999999	Refuser l'accès	Non spécifié

**Authentification cisco Admin**

Conditions - Si les conditions suivantes sont réunies :

Condition	Valeur
Groupes Windows	BORA-BORA\Auth-Cisco

Paramètres - Les paramètres suivants sont appliqués :

Paramètre	Valeur
Cisco-AV-Pair	shell:priv-lvl=15
Autorisation d'accès	Accorder l'accès
Méthode d'authentification	Authentification non chiffrée (PAP, SPAP)
Contrainte de mise en conformité NAP	Autoriser un accès réseau complet
Mettre à jour les clients non conformes	Vrai
Service-Type	Login

**Stratégies réseau**

Les stratégies réseau vous permettent d'autoriser les connexions au réseau de manière sélective, et d'indiquer les circonstances dans lesquelles ces connexions peuvent s'effectuer ou non.

Nom de la stratégie	État	Ordre de traitement	Type d'accès	Source
Authentification cisco Admin	Activé	1	Accorder l'accès	Non spécifié
Authentification cisco Read Only	Activé	2	Accorder l'accès	Non spécifié
Connexions au serveur Microsoft de Routage et Accès distants	Activé	999998	Refuser l'accès	Non spécifié
Connexions à d'autres serveurs d'accès	Activé	999999	Refuser l'accès	Non spécifié

**Authentification cisco Read Only**

Conditions - Si les conditions suivantes sont réunies :

Condition	Valeur
Groupes Windows	BORA-BORA\Auth-Cisco-Read

Paramètres - Les paramètres suivants sont appliqués :

Paramètre	Valeur
Cisco-AV-Pair	shell:priv-lvl=1
Autorisation d'accès	Accorder l'accès
Méthode d'authentification	Authentification non chiffrée (PAP, SPAP)
Contrainte de mise en conformité NAP	Autoriser un accès réseau complet
Mettre à jour les clients non conformes	Vrai
Service-Type	Login

**Configuration du protocole radius sur les équipement cisco :**

```
username xxxx privilege 15 secret yyyy
crypto key generate rsa modulus 2048
ip ssh version 2
ip ssh time-out 30
ip ssh dh min size 2048
ip scp server enable
service tcp-keepalives-in
ip ssh logging events
line vty 0 4
transport input ssh
exec -timeout 15
exit
```

```
conf t
username admin priv 15 secret admin
aaa new-model
aaa group server radius BORA
server-private 192.168.10.235 key toor
```

```
aaa authentication login default group BORA local
aaa authorization exec default group BORA local
aa accounting exec default start-stop group BORA
```

```
ip radius source-interface Vlan10
```

```
line vty 0 4
transport input ssh
login authentication default
authorization exec default
```

```
line con 0
transport input ssh
login authentication default
authorization exec default
```

```

S_Coeur_2(config)#ip domain-name bora-bora.nc
S_Coeur_2(config)#crypto key generate rsa modulus 2048
The name for the keys will be: S_Coeur_2.bora-bora.nc

% The key modulus size is 2048 bits
% Generating 2048 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 4 seconds)

S_Coeur_2(config)#
*Oct 29 06:36:51.062: %SSH-5-ENABLED: SSH 1.99 has been enabled
S_Coeur_2(config)#ip ssh version 2
S_Coeur_2(config)#ip shh logging events
      ^
% Invalid input detected at '^' marker.

S_Coeur_2(config)#ip ssh logging events
S_Coeur_2(config)#line vty 0 4
S_Coeur_2(config-line)#transport input ssh
S_Coeur_2(config-line)#exec-timeout 15
S_Coeur_2(config-line)#exit
S_Coeur_2(config)#

```

```

S_Coeur_2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
S_Coeur_2(config)#aaa new-model
S_Coeur_2(config)#aaa group server radius BORA
S_Coeur_2(config-sg-radius)#server-private 192.168.10.235 key toor
S_Coeur_2(config-sg-radius)#exit
S_Coeur_2(config)#aaa authentication login default group BORA
S_Coeur_2(config)#aaa authorization exec default group BORA
S_Coeur_2(config)#
S_Coeur_2(config)#line vty 0 4
S_Coeur_2(config-line)#login authentication default
      ^
% Invalid input detected at '^' marker.

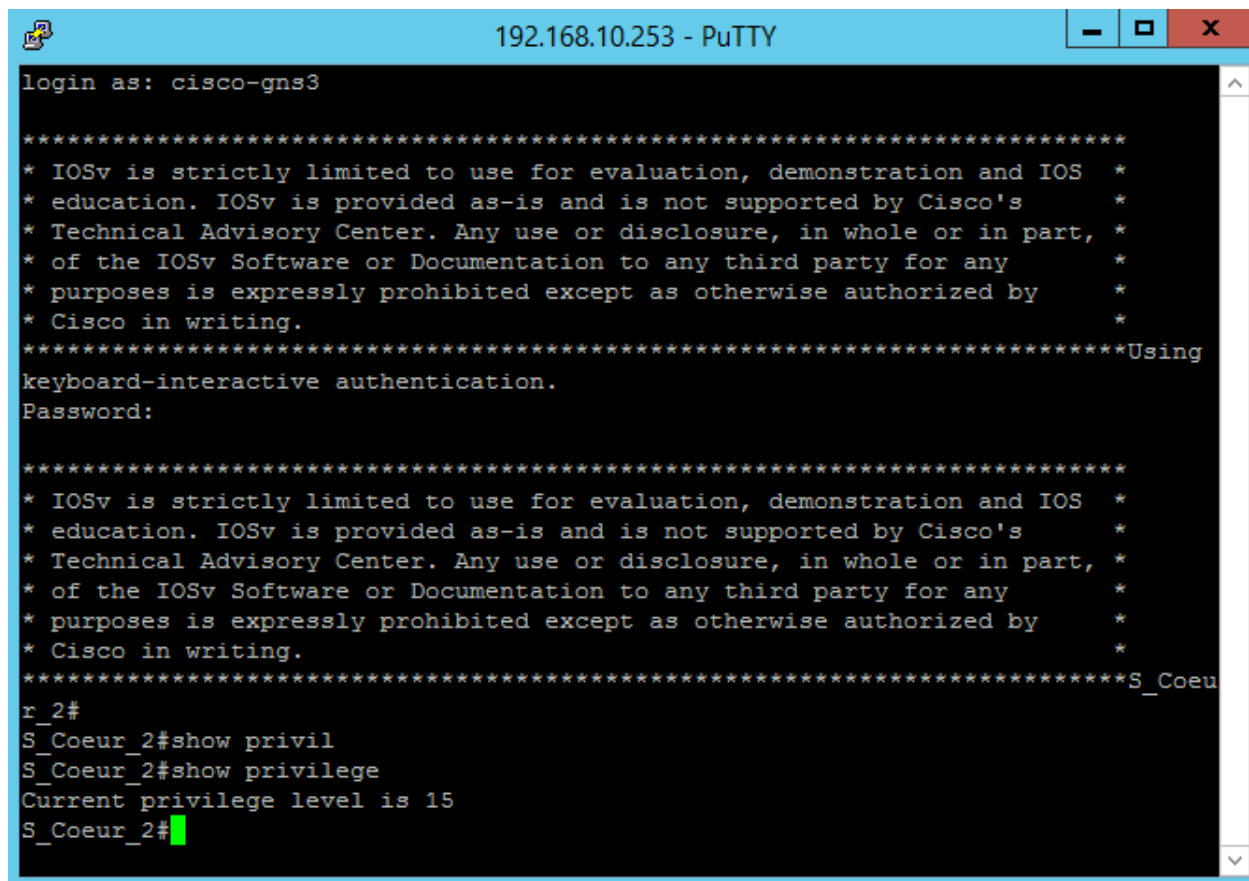
S_Coeur_2(config-line)#login authentication default
*Oct 29 06:40:39.879: %GLBP-6-FWDSTATECHANGE: Vlan40 Grp 1 Fwd 1 state Listen -> Active
*Oct 29 06:40:40.554: %GLBP-6-STATECHANGE: Vlan40 Grp 1 state Standby -> Active
S_Coeur_2(config-line)#login authentication default
S_Coeur_2(config-line)#

```



Connexion en ssh à l'équipement réseau avec le compte associé au groupe administrateur :

- Il a alors les privilèges 15 (maximum)



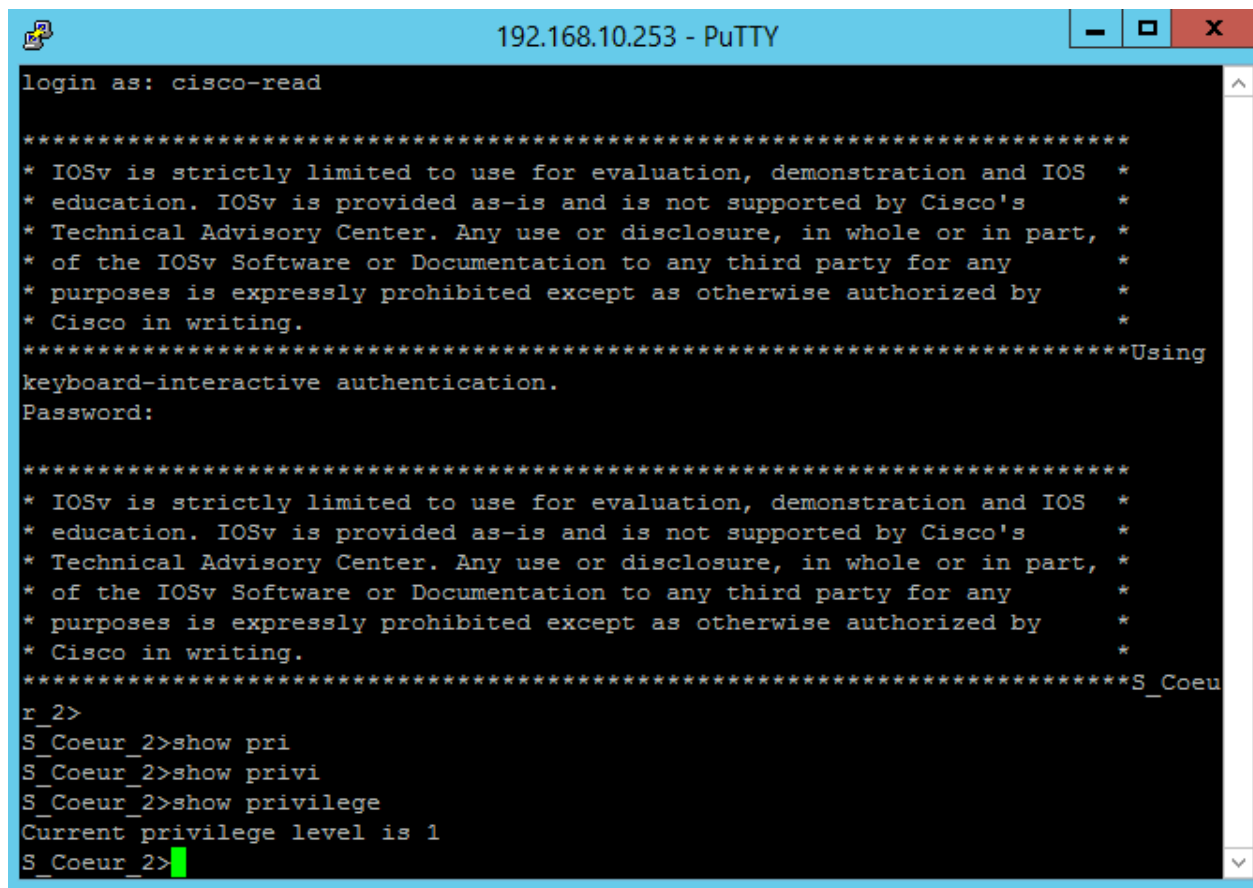
```
192.168.10.253 - PuTTY
login as: cisco-gns3

*****
* IOSv is strictly limited to use for evaluation, demonstration and IOS *
* education. IOSv is provided as-is and is not supported by Cisco's *
* Technical Advisory Center. Any use or disclosure, in whole or in part, *
* of the IOSv Software or Documentation to any third party for any *
* purposes is expressly prohibited except as otherwise authorized by *
* Cisco in writing. *
*****Using
keyboard-interactive authentication.
Password:

*****
* IOSv is strictly limited to use for evaluation, demonstration and IOS *
* education. IOSv is provided as-is and is not supported by Cisco's *
* Technical Advisory Center. Any use or disclosure, in whole or in part, *
* of the IOSv Software or Documentation to any third party for any *
* purposes is expressly prohibited except as otherwise authorized by *
* Cisco in writing. *
*****S_Coeu
r_2#
S_Coeur_2#show privil
S_Coeur_2#show privilege
Current privilege level is 15
S_Coeur_2#
```

Connexion en ssh à l'équipement réseau avec le compte associé au groupe read-only :

- Il a alors les privilèges 15 (minimum)



```

192.168.10.253 - PuTTY
login as: cisco-read

*****
* IOSv is strictly limited to use for evaluation, demonstration and IOS *
* education. IOSv is provided as-is and is not supported by Cisco's *
* Technical Advisory Center. Any use or disclosure, in whole or in part, *
* of the IOSv Software or Documentation to any third party for any *
* purposes is expressly prohibited except as otherwise authorized by *
* Cisco in writing. *
*****Using
keyboard-interactive authentication.
Password:

*****
* IOSv is strictly limited to use for evaluation, demonstration and IOS *
* education. IOSv is provided as-is and is not supported by Cisco's *
* Technical Advisory Center. Any use or disclosure, in whole or in part, *
* of the IOSv Software or Documentation to any third party for any *
* purposes is expressly prohibited except as otherwise authorized by *
* Cisco in writing. *
*****S_Coeur_2>
r_2>
S_Coeur_2>show pri
S_Coeur_2>show privi
S_Coeur_2>show privilege
Current privilege level is 1
S_Coeur_2>

```

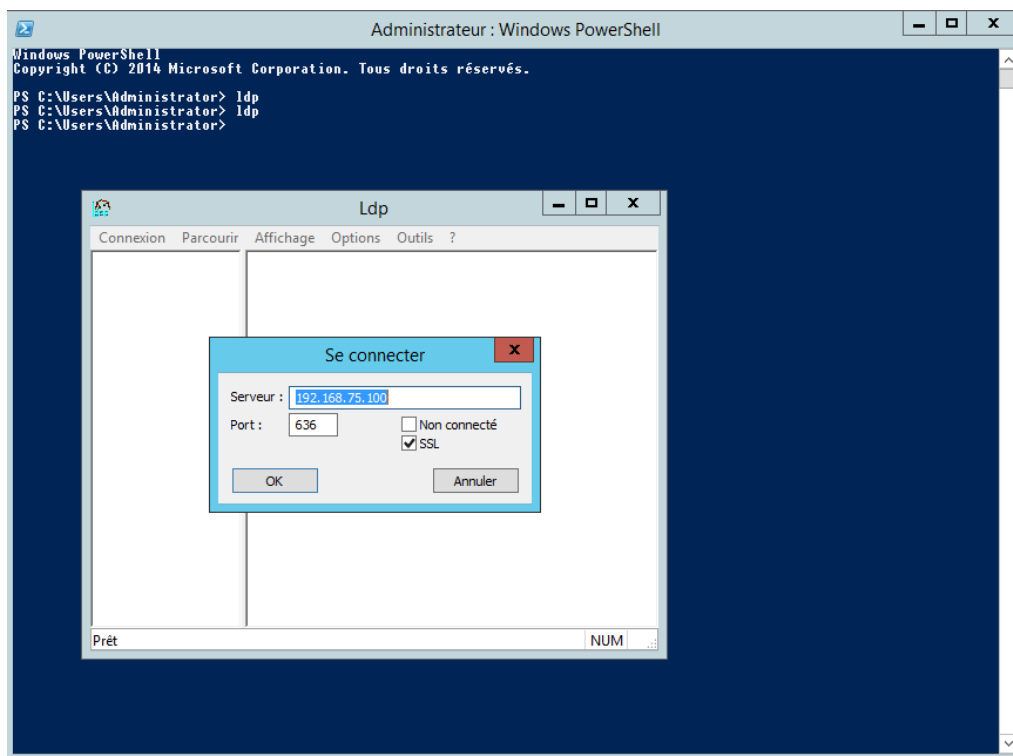
```

SESSION: SSH2 Session request from 192.168.10.235 (tty = 0) using crypto cipher 'aes256-ctr', 1
USERAUTH: User 'cisco-gns3' authentication for SSH2 Session from 192.168.10.235 (tty = 0) using
CLOSE: SSH2 Session from 192.168.10.235 (tty = 0) for user 'cisco-gns3' using crypto cipher 'ae
SESSION: SSH2 Session request from 192.168.10.235 (tty = 0) using crypto cipher 'aes256-ctr', 1
USERAUTH: User 'cisco-read' authentication for SSH2 Session from 192.168.10.235 (tty = 0) using
CLOSE: SSH2 Session from 192.168.10.235 (tty = 0) for user 'cisco-read' using crypto cipher 'ae
SESSION: SSH2 Session request from 192.168.10.235 (tty = 0) using crypto cipher 'aes256-ctr', 1
USERAUTH: User 'cisco-read' authentication for SSH2 Session from 192.168.10.235 (tty = 0) using
CLOSE: SSH2 Session from 192.168.10.235 (tty = 0) for user 'cisco-read' using crypto cipher 'ae

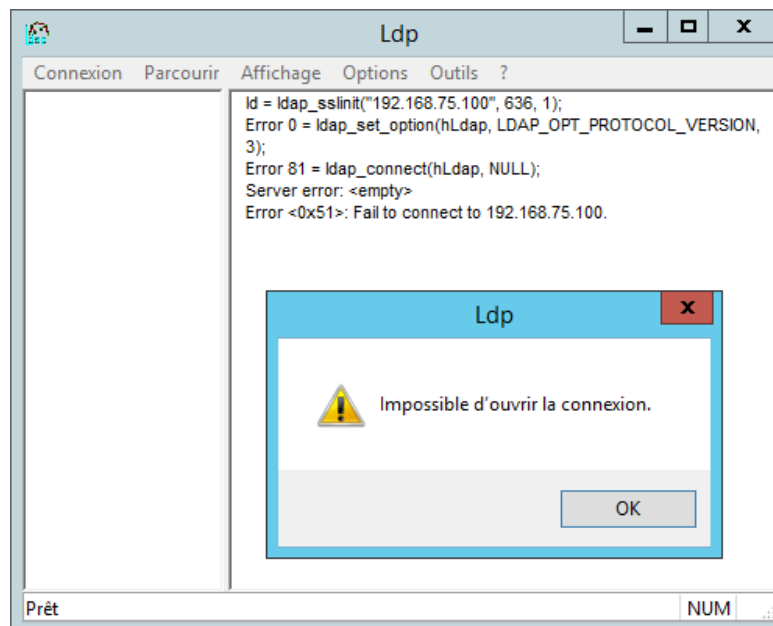
```

## VIII. Configuration du LDAPS

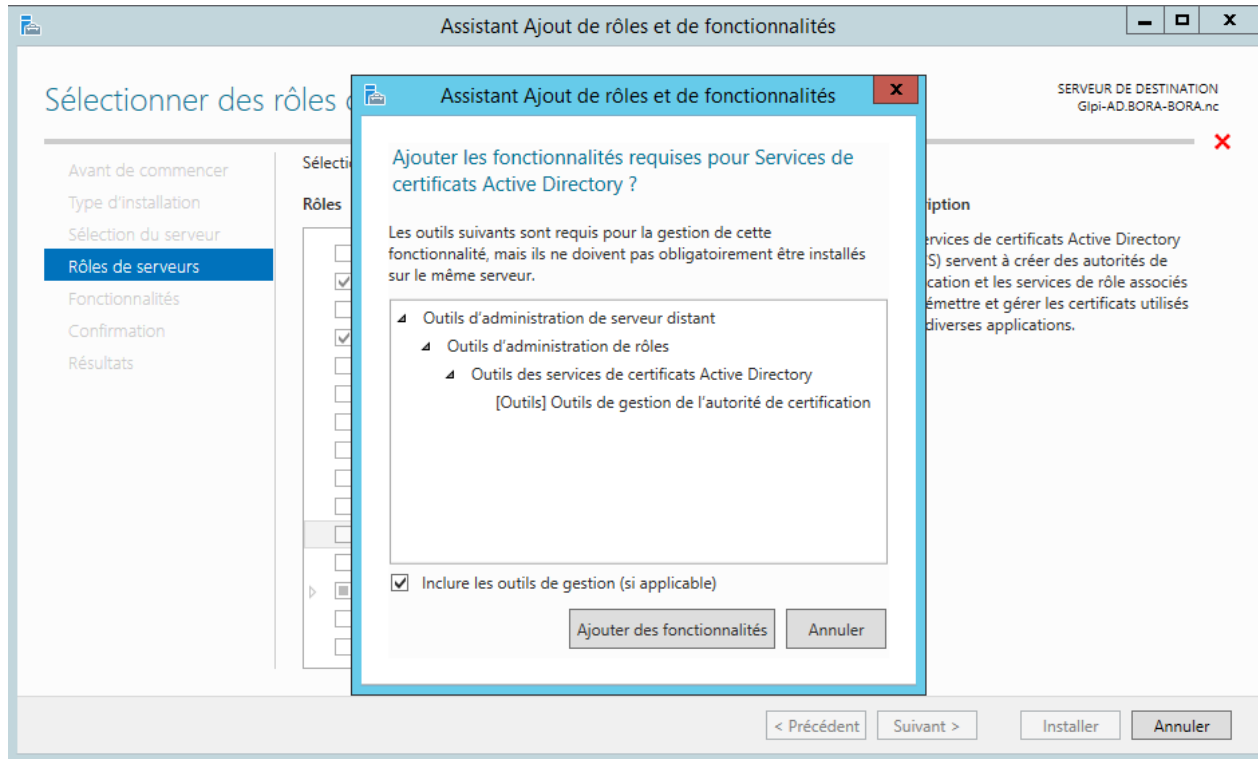
Tentative de connexion en ldaps au serveur AD (Port=636 et SSL activé) :



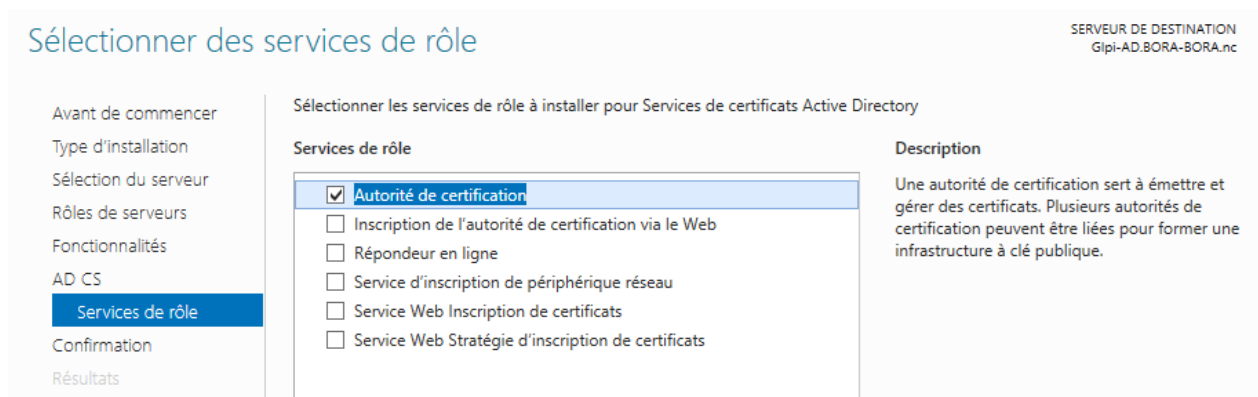
La connexion est impossible :



Ajout du rôle de certificate active directory qui va permettre d'activer après la configuration de la PKI le LDAPS :



Selectionner Autorité de certification :



Configurer l'infrastructure à clé publique :

The screenshot shows the 'Configuration des services de certificats Active Directory' window. The title bar is blue with the text 'Configuration des services de certificats Active Directory'. The main area is titled 'Informations d'identification'. On the right, it says 'SERVEUR DE DESTINATION Glpi-AD.BORA-BORA.nc'. On the left, there is a sidebar with 'Informations d'identification...' selected. The main content area says 'Spécifier les informations d'identification pour configurer les services de rôle'. Below this, it states 'Pour installer les services de rôle suivants, vous devez être membre du groupe Administrateurs local :'. There are two bulleted lists: one for local administrators (Utiliser l'autorité de certification autonome, Inscription de l'autorité de certification via le Web, Répondeur en ligne) and one for enterprise administrators (Autorité de certification d'entreprise, Service Web Stratégie d'inscription de certificats, Service Web Inscription de certificats, Service d'inscription de périphériques réseau). At the bottom, there is a text box for 'Informations d'identification : BORA-BORA\Administrator' and a 'Modifier...' button. At the very bottom, there are navigation buttons: '< Précédent', 'Suivant >', 'Configurer', and 'Annuler'.

Selectionné autorité de certification :

The screenshot shows the 'Configuration des services de certificats Active Directory' window, now at the 'Services de rôle' step. The title bar is the same. The main area is titled 'Services de rôle'. On the right, it says 'SERVEUR DE DESTINATION Glpi-AD.BORA-BORA.nc'. On the left, the sidebar has 'Services de rôle' selected. The main content area says 'Sélectionner les services de rôle à configurer'. There is a list of services with checkboxes: 'Autorité de certification' (checked), 'Inscription de l'autorité de certification via le Web', 'Répondeur en ligne', 'Service d'inscription de périphériques réseau', 'Service Web Inscription de certificats', and 'Service Web Stratégie d'inscription de certificats'. At the bottom, there are navigation buttons: '< Précédent', 'Suivant >', 'Configurer', and 'Annuler'.

Sélectionné autorité de certification d'entreprise ce qui permettra d'ouvrir le port 636 du protocole LDAPS :

## Type d'installation

- Informations d'identificati...
- Services de rôle
- Type d'installation**
- Type d'AC
- Clé privée
  - Chiffrement
  - Nom de l'AC
  - Période de validité
- Base de données de certi...
- Confirmation
- Progression
- Résultats

Spécifier le type d'installation de l'AC

Les autorités de certification d'entreprise peuvent utiliser les services de domaine Active Directory (AD DS) pour simplifier la gestion des certificats. Les autorités de certification autonomes n'utilisent pas AD DS pour émettre ou gérer des certificats.

☒ **Autorité de certification d'entreprise**  
Les autorités de certification d'entreprise doivent être membres d'un domaine et sont généralement en ligne pour émettre des certificats ou des stratégies de certificat.

☐ **Autorité de certification autonome**  
Les autorités de certification autonomes peuvent être membres d'un groupe de travail ou d'un domaine. Les autorités de certification autonomes ne nécessitent pas AD DS et peuvent être utilisées sans connexion réseau (hors connexion).

SERVEUR DE DESTINATION

Glp-AD.BORA-BORA.nc

Sélectionné autorité de certification racine :

## Type d'autorité de certification

- Informations d'identificati...
- Services de rôle
- Type d'installation
- Type d'AC**
- Clé privée
  - Chiffrement
  - Nom de l'AC
  - Période de validité
- Base de données de certi...
- Confirmation
- Progression
- Résultats

Spécifier le type de l'AC

Lorsque vous installez les services de certificats Active Directory (AD CS), vous créez ou étendez une hiérarchie d'infrastructure à clé publique (PKI). Une autorité de certification racine se trouve au sommet de la hiérarchie PKI et émet ses propres certificats auto-signés. Une autorité de certification secondaire reçoit un certificat de l'autorité de certification de rang plus élevé dans la hiérarchie PKI.

☒ **Autorité de certification racine**  
Les autorités de certification racines sont les premières voire les seules autorités de certification configurées dans une hiérarchie PKI.

☐ **Autorité de certification secondaire**  
Les autorités de certification secondaires nécessitent une hiérarchie PKI établie et sont autorisées à émettre des certificats par l'autorité de certification de rang plus élevé dans la hiérarchie.

SERVEUR DE DESTINATION

Glp-AD.BORA-BORA.nc

Créer ensuite la clé privée :

## Clé privée

- Informations d'identificati...
- Services de rôle
- Type d'installation
- Type d'AC
- Clé privée**
- Chiffrement
- Nom de l'AC
- Période de validité
- Base de données de certi...
- Confirmation
- Progression
- Résultats

**SPECIFIEZ LE TYPE DE LA CLÉ PRIVÉE**

Pour générer et émettre des certificats aux clients, une autorité de certification doit posséder une clé privée.

☒ **Créer une clé privée**  
Utilisez cette option si vous n'avez pas de clé privée ou pour en créer une.

☐ **Utiliser la clé privée existante**  
Utilisez cette option pour garantir la continuité avec les certificats émis antérieurement lors de la réinstallation d'une AC.

☐ **Sélectionner un certificat et utiliser sa clé privée associée**  
Sélectionnez cette option s'il existe un certificat sur cet ordinateur ou pour importer un certificat et utiliser sa clé privée associée.

☐ **Sélectionner une clé privée existante sur cet ordinateur**  
Sélectionnez cette option si vous avez conservé les clés privées d'une installation antérieure ou pour utiliser une clé privée d'une autre source.

**SERVEUR DE DESTINATION**  
GlpI-AD.BORA-BORA.nc

Configurer ensuite le chiffrement :

- Configurer la longueur de la clé à 4096 bit
- Puis l'algorithme de hashage en sha256

## Chiffrement pour l'autorité de certification

- Informations d'identificati...
- Services de rôle
- Type d'installation
- Type d'AC
- Clé privée
- Chiffrement**
- Nom de l'AC
- Période de validité
- Base de données de certi...
- Confirmation
- Progression
- Résultats

**SPECIFIEZ LES OPTIONS DE CHIFFREMENT**

Sélectionnez un fournisseur de chiffrement :

Longueur de la clé :

Sélectionnez l'algorithme de hashage pour signer les certificats émis par cette AC :  
  
 SHA384  
 SHA512  
 SHA1

☐ Autorisez l'interaction de l'administrateur lorsque l'autorité de certification accède à la clé privée.

**SERVEUR DE DESTINATION**  
GlpI-AD.BORA-BORA.nc

Spécifier ensuite le nom de l'AC qui doit être le même que celui du serveur :

## Nom de l'autorité de certification

SERVEUR DE DESTINATION  
Glp-AD.BORA-BORA.nc

Informations d'identificati...  
Services de rôle  
Type d'installation  
Type d'AC  
Clé privée  
Chiffrement  
**Nom de l'AC**  
Période de validité  
Base de données de certi...  
Confirmation  
Progression  
Résultats

### Spécifier le nom de l'AC

Tapez un nom commun pour identifier cette autorité de certification. Ce nom est ajouté à tous les certificats émis par l'autorité de certification. Les valeurs des suffixes du nom unique sont générées automatiquement, mais elles sont modifiables.

Nom commun de cette AC :

Suffixe du nom unique :

Aperçu du nom unique :

Configurer 10 ans comme période de validité :

## Période de validité

SERVEUR DE DESTINATION  
Glp-AD.BORA-BORA.nc

Informations d'identificati...  
Services de rôle  
Type d'installation  
Type d'AC  
Clé privée  
Chiffrement  
Nom de l'AC  
**Période de validité**  
Base de données de certi...  
Confirmation  
Progression  
Résultats

### Spécifier la période de validité

Sélectionnez la période de validité du certificat généré pour cette autorité de certification :

Date d'expiration de l'AC : 01/11/2027 13:29:00

La période de validité configurée pour ce certificat d'autorité de certification doit dépasser la période de validité pour les certificats qu'elle émettra.



Laissez les emplacements des bases de données par défaut :

## Base de données de l'autorité de certification

**SERVEUR DE DESTINATION**  
 Glpi-AD.BORA-BORA.nc

Informations d'identificati...

Services de rôle

Type d'installation

Type d'AC

Clé privée

Chiffrement

Nom de l'AC

Période de validité

Base de données de certi...

Confirmation

Progression

Résultats

### Spécifier les emplacements des bases de données

Emplacement de la base de données de certificats :

Emplacement du journal de la base de données de certificats :

Récapitulatif de la configuration de la PKI :

## Confirmation

**SERVEUR DE DESTINATION**  
 Glpi-AD.BORA-BORA.nc

Informations d'identificati...

Services de rôle

Type d'installation

Type d'AC

Clé privée

Chiffrement

Nom de l'AC

Période de validité

Base de données de certi...

Confirmation

Progression

Résultats

Pour configurer les rôles, services de rôle ou fonctionnalités ci-après, cliquez sur Configurer.

^ **Services de certificats Active Directory**

---

**Autorité de certification**

Type d'AC :	Racine d'entreprise
Fournisseur de services de chiffrement :	RSA#Microsoft Software Key Storage Provider
Algorithme de hachage :	SHA1
Longueur de la clé :	2048
Autoriser l'interaction de l'administrateur :	Désactivé
Période de validité du certificat :	01/11/2027 13:29:00
Nom unique :	CN=Parc-Info,DC=BORA-BORA,DC=nc
Emplacement de la base de données de certificats :	C:\Windows\system32\CertLog
Emplacement du journal de la base de données de certificats :	C:\Windows\system32\CertLog

Tentative de connexion en LDAPS et capture de trame avec WireShark :

- Les trames échangées entre le serveur GLPI et le serveur active directory sont bien sécurisé par le protocole TLS1.2 :

\*Standard input [WindowsServer2012r2Srv\_AD Ethernet0 to S\_Acces\_Serveur Gi1/0]

Fichier Editer Vue Aller Capture Analyser Statistiques Telephonie Wireless Outils Aide

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

No.	Time	Source	Destination	Protocol	Length	Info
94	10.361922	00:87:0f:db:dd:04	Spanning-tree-(for-bridges)_00	STP	60	RST. Root = 32768/10/00:87:0f:0f:ab:00 Cost = 3 Port = 0x8005
95	10.383404	Vmware_5e:35:35	Broadcast	ARP	60	Who has 192.168.10.245? Tell 192.168.10.240
96	12.511983	00:87:0f:db:dd:04	Spanning-tree-(for-bridges)_00	STP	60	RST. Root = 32768/10/00:87:0f:0f:ab:00 Cost = 3 Port = 0x8005
97	12.816405	192.168.10.254	224.0.0.102	GLBP	102	G: 1, Hello, IPv4, Request/Response?
98	12.870397	192.168.10.254	224.0.0.5	OSPF	94	Hello Packet
99	12.878006	192.168.10.253	224.0.0.102	GLBP	102	G: 1, Hello, IPv4, Request/Response?
100	13.301524	192.168.10.1	192.168.10.235	TCP	74	58038 → 636 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=4294946637 TSecr=0 WS=128
101	13.302095	Vmware_b1:1f:27	Broadcast	ARP	42	Who has 192.168.10.1? Tell 192.168.10.235
102	13.310162	Vmware_0a:78:4b	Vmware_b1:1f:27	ARP	60	192.168.10.1 is at 00:0c:29:0a:78:4b
103	13.310398	192.168.10.235	192.168.10.1	TCP	74	636 → 58038 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1 TSval=1425952 TSecr=0
104	13.316051	192.168.10.1	192.168.10.235	TCP	66	58038 → 636 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=4294946689 TSecr=1425952
105	13.336267	192.168.10.1	192.168.10.235	TLSv1.2	304	Client Hello
106	13.338508	192.168.10.235	192.168.10.1	TCP	1514	[TCP segment of a reassembled PDU]
107	13.338685	192.168.10.235	192.168.10.1	TLSv1.2	613	Server Hello, Certificate, Server Key Exchange, Certificate Request, Server Hello Done
108	13.344045	192.168.10.1	192.168.10.235	TCP	66	58038 → 636 [ACK] Seq=239 Ack=1449 Win=32128 Len=0 TSval=4294946696 TSecr=1425956
109	13.344875	192.168.10.1	192.168.10.235	TCP	66	58038 → 636 [ACK] Seq=239 Ack=1996 Win=35072 Len=0 TSval=4294946696 TSecr=1425956
110	13.348315	192.168.10.1	192.168.10.235	TLSv1.2	78	Certificate
111	13.349127	192.168.10.1	192.168.10.235	TLSv1.2	141	Client Key Exchange
112	13.349315	192.168.10.235	192.168.10.1	TCP	66	636 → 58038 [ACK] Seq=1996 Ack=326 Win=66304 Len=0 TSval=1425957 TSecr=4294946697
113	13.353574	192.168.10.1	192.168.10.235	TLSv1.2	72	Change Cipher Spec
114	13.354384	192.168.10.1	192.168.10.235	TLSv1.2	167	Encrypted Handshake Message

> Frame 107: 613 bytes on wire (4904 bits), 613 bytes captured (4904 bits) on interface 0

> Ethernet II, Src: Vmware\_b1:1f:27 (00:0c:29:b1:1f:27), Dst: Vmware\_0a:78:4b (00:0c:29:0a:78:4b)

> Internet Protocol Version 4, Src: 192.168.10.235, Dst: 192.168.10.1

> Transmission Control Protocol, Src Port: 636, Dst Port: 58038, Seq: 1449, Ack: 239, Len: 547

> [2 Reassembled TCP Segments (1995 bytes): #106(1448), #107(547)]

Secure Sockets Layer

- ▼ TLSv1.2 Record Layer: Handshake Protocol: Multiple Handshake Messages
  - Content Type: Handshake (22)
  - Version: TLS 1.2 (0x0303)
  - Length: 1990
  - > Handshake Protocol: Server Hello
  - > Handshake Protocol: Certificate
  - > Handshake Protocol: Server Key Exchange
  - > Handshake Protocol: Certificate Request
  - > Handshake Protocol: Server Hello Done